002.11.6

Kaspersky Endpoint Security and Management

Часть I. Внедрение

kaspersky

Учебный курс

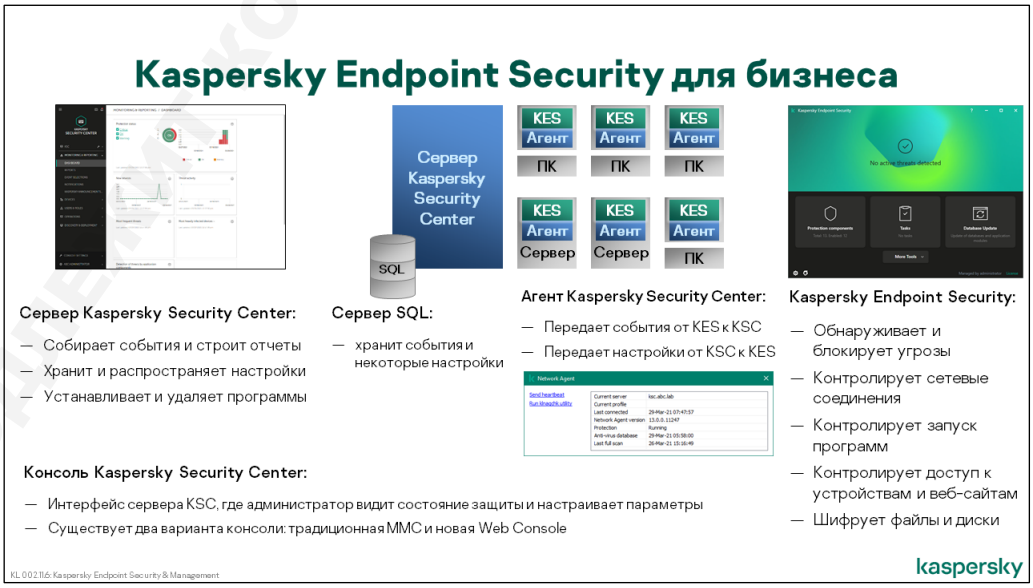
Содержание

1. Введение

Из введения вы узнаете, что это за курс, какие темы он охватывает, а какие нет. Также вы узнаете, какие решения и продукты изучаются в курсе, из чего эти продукты состоят, как взаимодействуют и как лицензируются.

1.1 Основы Kaspersky Endpoint Security для бизнеса

Какие продукты рассматривает курс



Курс рассказывает о решении Kaspersky Endpoint Security для бизнеса, в которое входит много разных продуктов Лаборатории Касперского. Курс не пытается охватить все продукты, а рассказывает только о тех, которые нужны, чтобы защитить не слишком большую сеть на базе Windows. Под не слишком большой сетью курс понимает сеть примерно до 1000 узлов, сосредоточенных в одном месте. Под узлами курс понимает серверы и рабочие станции под управлением Windows.

Чтобы защитить такую сеть, нужно два продукта из состава Kaspersky Endpoint Security для бизнеса:

- Kaspersky Endpoint Security для Windows — защищает компьютеры от угроз
- Kaspersky Security Center — централизованно управляет защитой

Kaspersky Endpoint Security — это одна программа, которая защищает не только от вредоносных программ и хакеров, но также контролирует действия пользователей и шифрует файлы и диски.

Из чего состоит Kaspersky Security Center

Kaspersky Security Center — это несколько программ:

- Сервер администрирования Kaspersky Security Center (далее *Сервер администрирования*, *Сервер KSC* или просто *Сервер*, если это не вызывает разночтений) хранит все настройки, собирает события, составляет отчеты и т.п. Именно Сервер управляет защитой по командам администратора.
- **Сервер баз данных** обслуживает базу данных, в которой Сервер KSC хранит события и некоторые настройки. Остальные настройки Сервер KSC хранит в файлах на диске.
- **Агенты администрирования Kaspersky Security Center** (далее *Агенты администрирования*, *Агенты KSC* или просто *Агенты*) связывают Kaspersky Endpoint Security с Сервером администрирования: получают с Сервера настройки для Kaspersky Endpoint Security, посылают на сервер события
- **Консоль администрирования Kaspersky Security Center** — это интерфейс системы управления для администратора; в консоли администратор настраивает параметры, смотрит на отчеты и события и вообще управляет защитой. Существует два варианта Консоли: традиционная на базе MMC и Web Console.

Из чего состоит Kaspersky Endpoint Security

Kaspersky Endpoint Security — это одна программа, которая включает много разных компонентов.

Компоненты защиты

Kaspersky Security Network	Запрашивает с серверов Лаборатории Касперского репутацию программ и веб-страниц, предоставляет самую свежую информацию об угрозах, защищает от атак нулевого дня и ложных срабатываний
Анализ поведения	Следит за тем, что делают программы, но анализирует не отдельные действия, а что делают программы в целом. Останавливает программы, которые ведут себя как вредоносные. В частности, останавливает программы, которые пытаются шифровать файлы
Защита от эксплойтов	Следит за тем, какие файлы запускают уязвимые программы и блокирует попытки запуска исполняемых файлов, если попытка запуска не была инициирована пользователем
Предотвращение вторжений	Также следит за тем, что делают программы на компьютере. Не дает программам с плохой или неизвестной репутацией менять системные настройки и файлы пользователя. Не даем им вмешиваться в работу операционной системы и других программ
Откат вредоносных действий	Ведет журнал изменений в операционной системе и выполняет откат изменений совершенных подозрительными программами, которые обнаружены компонентами: Анализ поведения, Защита от эксплойтов, Защита от файловых угроз
Защита от файловых угроз	Проверяет файлы, когда их создает, изменяет, копирует или запускает пользователь или программа Блокирует операции с вредоносными файлами, а файлы помещает в карантин
Защита от веб-угроз	Проверяет веб-страницы и файлы, которые пользователь или программы загружают из Интернет. Блокирует опасные и фишинговые веб-сайты, не дает загрузить вредоносные файлы
Защита от почтовых угроз	Перехватывает почтовые сообщения, проверяет текст и вложенные файлы, удаляет вредоносные файлы из письма
Сетевой экран	Контролирует соединения, которые устанавливают программы на компьютере, и пакеты, которые они посылают или отправляют. Блокирует пакеты согласно правилам. Не дает устанавливать соединения программам с плохой репутацией или неизвестной
Защита от сетевых угроз	Проверяет сетевые пакеты, которые получает компьютер. Блокирует соединения, в которых находит признаки сетевых атак
Защита от атак BadUSB	Не дает подключать к компьютеру новые устройства ввода (клавиатуры и т.п.) без разрешения пользователя. Защищает от USB-устройств, которые выдают себя за клавиатуру, и дают компьютеру вредоносные команды
Поставщик AMSI-защиты	Отвечает за интеграцию с Antimalware Scan Interface (AMSI) в Windows 10 и Windows Server 2016. AMSI это компонент Windows, который выполняет роль промежуточного звена между приложениями и антивирусным решением, и позволяет приложению отсылать на проверку файлы, ссылки, скрипты, даже если они не сохраняются на диск, а выполняются в памяти

Компоненты контроля

Контроль программ	Блокирует запуск программ согласно правилам. Позволяет зафиксировать состояние компьютера и блокировать запуск любых новых программ.
Контроль устройств	Блокирует доступ к устройствам согласно правилам. Администратор может запретить доступ ко всем или некоторым сменным носителям, Wi-Fi адаптерам или модемам
Веб-Контроль	Блокирует доступ к веб-страницам согласно правилам. Администратор может запретить доступ к сайтам социальных сетей, поиска работы, новостям и торрент-трекерам и т.п.
Адаптивный контроль аномалий	Содержит набор эвристик для отслеживания опасного поведения, которое обычно характерно для вредоносных программ. Позволяет блокировать подозрительные действия, если они нетипичны для конкретного компьютера. По умолчанию компонент включается в режиме 2-х недельного обучения, за это время он отслеживает активность, информирует об этом администратора и уже администратор принимает решение характерна ли определенная активность для компьютера или нет.

Компоненты шифрования

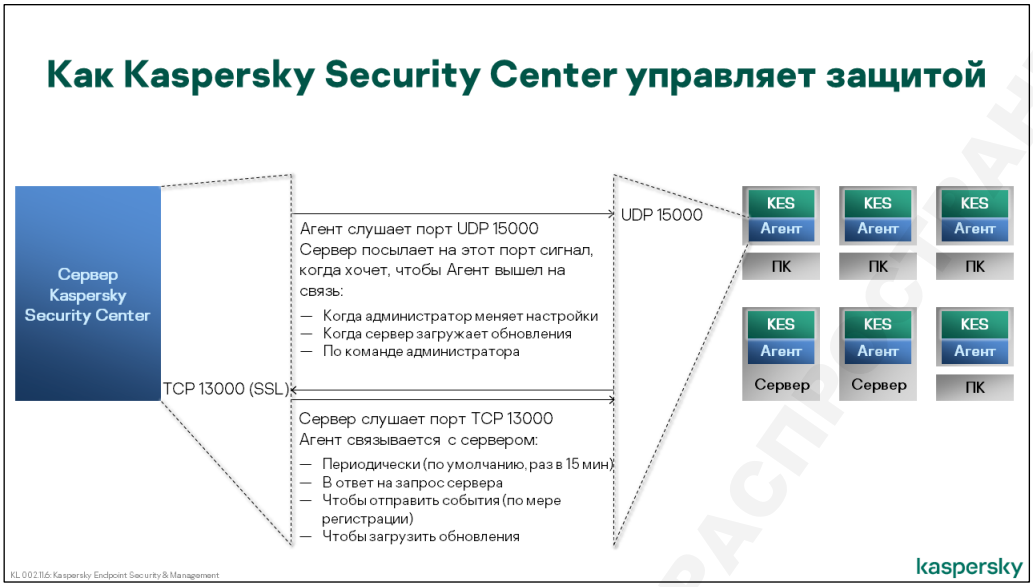
Шифрование дисков	Шифрует все содержимое дисков. Защищает файлы на ноутбуках, которые потеряли или украли
Шифрование файлов	Шифрует отдельные файлы и папки согласно правилам. Защищает файлы на ноутбуках, которые потеряли или украли
Управление Microsoft BitLocker	Управляет шифрованием дисков с помощью Microsoft BitLocker. Защищает файлы на ноутбуках, которые потеряли или украли

Прочие компоненты и задачи

Поиск вирусов	Проверяет файлы по расписанию. Делает это более тщательно, чем файловый антивирус
Обновление	Загружает описания угроз и репутации файлов на компьютеры, обеспечивает защиту, когда нет доступа к Kaspersky Security Network
Endpoint Sensor	Сообщает центральному узлу Kaspersky Anti-Targeted Attack Platform, что делают программы на компьютерах, помогает обнаруживать Advanced Persistent Threats
Проверка целостности	Проверяет, что никто не менял файлы Kaspersky Endpoint Security
Проверка доступности KSN	Проверяет доступность служб KSN с конечных узлов

Подробно о компонентах и их настройках рассказывают части 2 и 3.

Как Kaspersky Security Center управляет компьютерами



Посмотрим, как все компоненты Kaspersky Endpoint Security для бизнеса взаимодействую друг с другом.

В защищенной сети на каждом компьютере установлены две программы:

- Kaspersky Endpoint Security защищает
- Агент администрирования Kaspersky Security Center управляет

Агент администрирования связывается с Сервером администрирования по расписанию, а также по мере необходимости. По умолчанию так называемая синхронизация происходит раз в 15 минут.

Что Сервер получает с компьютеров

Чтобы администратор видел, что происходит в сети, Агент администрирования посылает на сервер следующие данные:

События	По мере регистрации	Когда Kaspersky Endpoint Security находит вредоносную программу, не может загрузить обновления, не может запустить компоненты и т.д.
Статусы	По мере регистрации	Kaspersky Endpoint Security не запущен Базы устарели KSN не доступен Есть необработанные опасные объекты
Списки	Раз в интервал синхронизации	Список известных исполняемых файлов Список уязвимых программ Список вредоносных объектов в карантине Список необработанных угроз Список оборудования Список установленных программ
Настройки Kaspersky Endpoint Security	Во время синхронизации	

В ходе обычной работы Агенты посылают на Сервер только изменения в списках. Раз в несколько часов (3 часа для одних списков, 12 часов для других) Сервер полностью синхронизирует списки с компьютером.

Сервер администрирования принимает соединения от Агентов администрирования на TCP-порт 13000. Агенты сжимают данные и шифруют их по протоколу SSL/TLS с помощью сертификата Сервера администрирования.

Что компьютеры загружают с Сервера

Чтобы Kaspersky Endpoint Security защищал компьютер так, как хочет администратор, Агенты администрирования загружают с Сервера настройки в виде политик и задач для Kaspersky Endpoint Security.

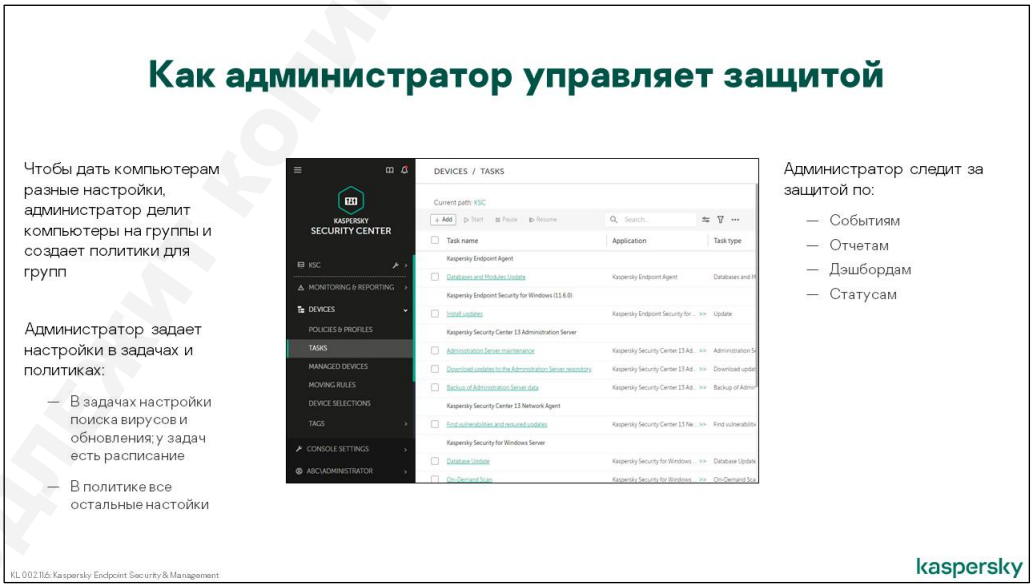
Во время синхронизации Агент администрирования сравнивает задачи и политики на компьютере и на Сервере администрирования и если на Сервере администратор что-то изменил, Агент загружает новые задачи и политики.

Как правило, компьютеры получают задачи и политики раньше, чем при плановой синхронизации. Агенты администрирования принимают пакеты на UDP-порт 15000. Если Сервер хочет, чтобы Агент срочно связался с Сервером, он посылает на этот порт специальный сигнал. Когда администратор меняет задачу или политику, Сервер администрирования просит выйти на связь Агенты на всех компьютерах, к которым относится эта задача или политика. Во время синхронизации политики загружают только те компьютеры, которые не получили сигнал от Сервера.

Запрос на синхронизацию администратор может послать и вручную, через контекстное меню компьютера в Консоли администрирования.

Еще Агенты связываются с Сервером, чтобы загрузить обновления для Kaspersky Endpoint Security. Для этого они тоже подключаются к порту 13000 через SSL-соединение.

Как администратор управляет защитой в консоли



События и статусы, которые посылают Агенты администрирования, помогают администратору понять, что происходит в сети. Сервер администрирования обобщает статусы отдельных

компьютеров и показывает их на главном экране Консоли администрирования — экране **Dashboard**.

Чтобы лучше понять, что происходит, администратор может получать отчеты, которые Сервер администрирования строит на основе событий. В консоли есть много инструментов для поиска и фильтрации событий и компьютеров по разнообразным параметрам.

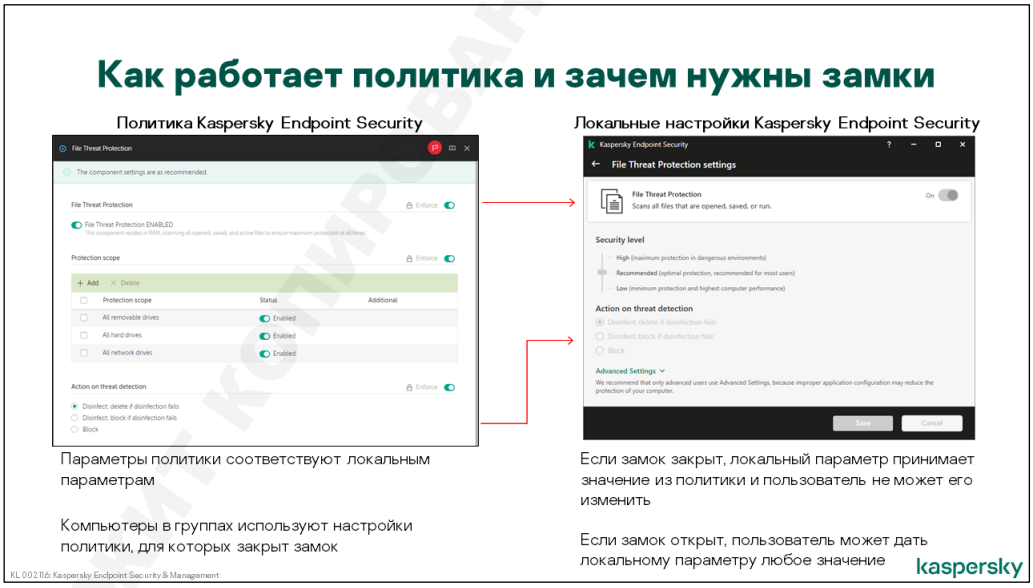
Чтобы задать настройки для защиты компьютеров администратор создает в консоли задачи и политики:

— Задачи — для операций, у которых есть логическое окончание. Например, обновление завершается, когда Kaspersky Endpoint Security получил все новые описания угроз или поиск вирусов завершается, когда в области поиска больше нет файлов. Поэтому обновление и поиск вирусов — это задачи, и у них есть расписание

— Политики — для всех остальных параметров, как проверять файлы, которые пользователь загружает из сети Интернет или получает по почте, или как проверять файлы, которые открывают программы, какие сетевые соединения разрешать, а какие запрещать. Эти настройки должны применяться постоянно, чтобы постоянно защищать компьютер, и поэтому они в политике

Если разным компьютерам нужны разные настройки, администратор разделяет компьютеры на группы и создает отдельные политики или задачи в каждой группе. Например, чтобы выполнять поиск вирусов на серверах по выходным, а на рабочих станциях в фоновом режиме во время рабочего дня, администратор может выделить серверы и рабочие станции в две группы и сделать для них задачи поиска вирусов с разным расписанием.

Как политики применяются к компьютерам



Политика содержит те же параметры, что и локальные настройки Kaspersky Endpoint Security. Когда администратор настраивает политику, он меняет локальные настройки защиты.

В политике у каждого параметр или группы параметров есть кнопка с замком.

Если кнопка нажата и замок закрыт, параметры применяются к компьютерам, на которые действует политика. Пользователь не может изменить значения этих параметров в локальном интерфейсе Kaspersky Endpoint Security.

Если кнопка не нажата и замок открыт, компьютер считает, что этот параметр в политике не задан. Эти параметры пользователь может менять в локальном интерфейсе.

Настройки с закрытым замком называются обязательными.

Как работают политики в группах

Политики применяются к группам компьютеров.

Даже если пользователь не создавал никаких групп, на Сервере администрирования есть корневая группа, которая называется Управляемые устройства. Если пользователь хочет создать свои группы, он их создает как подгруппы в группе Управляемые устройства.

Политики подчиняются правилам:

- В одной группе могут быть политики разных программ, например, политика Агента администрирования и политика Kaspersky Endpoint Security
- В одной группе может быть несколько политик одной программы, но только одна из них может быть активной.

  Активная политика это та, которую Сервер администрирования посылает на компьютеры

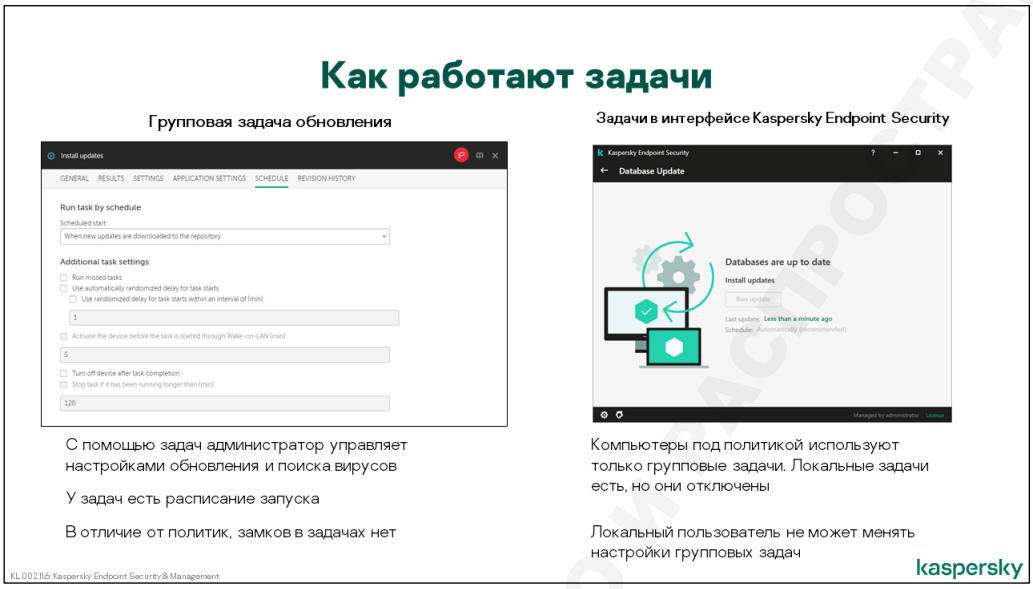
  Неактивная политика ни на что не влияет, но администратор может сделать ее активной и быстро изменить настройки для всех компьютеров

  Если администратор делает политику активной, политика, которая была активной до этого, автоматически становится неактивной

- Если в группе есть политика Kaspersky Endpoint Security, и в этой же группе есть подгруппа, в которой нет политики Kaspersky Endpoint Security, политика группы применяется к компьютерам подгруппы
- Если в группе есть политика Kaspersky Endpoint Security, и в этой же группе есть подгруппа, в которой тоже есть политика Kaspersky Endpoint Security, к компьютерам подгруппы применяется политика подгруппы. Но обязательные параметры из политики группы применяются к политике подгруппы, и администратор не может их изменить. В политике подгруппы администратор может менять только те параметры, которые не закрыты замком в политике родительской группы

— Администратор может не применять политику группы к подгруппам. Для этого нужно в политике подгруппы снять флаг наследовать параметры из политики родительской группы. После этого администратор может менять все параметры в политике подгруппы

Как задачи применяются к компьютерам



Настройками обновления и поиска вирусов администратор управляет не через политику, а через задачи.

Если политика для Kaspersky Endpoint Security одна[1], то разных задач для Kaspersky Endpoint Security много:

— Поиск вирусов
— Обновление
— Откат обновления
— Инвентаризация
— Добавление ключа
— Проверка целостности
— Изменение состава компонентов программы
— Проверка доступности KSN
— Управление учетными записями агента аутентификации

У задач каждого типа свои характерные настройки. У задачи поиска вирусов это область поиска и параметры проверки файлов, у задачи обновления — это источник обновления и какие обновления загружать.

Во всех задачах есть настройки расписания.

В отличие от политик, замков в задачах нет. Все настройки задачи применяются к компьютерам, и пользователь их менять не может.

[1] Одна для одной или нескольких версий. Например, у Kaspersky Endpoint Security 10 SP2 своя политика, а у Kaspersky Endpoint Security 11 своя. Но две политики для одной версии Kaspersky Endpoint Security содержат одинаковые параметры и отличаются только настройками этих параметров.

Задачи может создавать не только администратор на Сервера администрирования, но и пользователь в локальном интерфейсе. Но если на компьютер применяется политика с Сервера администрирования, на нем выполняются только задачи с Сервера администрирования. Локальные задачи не выполняются и не показываются в интерфейсе. И новые локальные задачи пользователь создавать не может.

Как работают задачи в группах

Для регулярных действий, таких как поиск вирусов или обновление, администратор создает задачи в группах.

Как и групповые политики, групповые задачи следуют определенным правилам:

- Если в группе есть подгруппа, то задача группы применяется и к компьютерам подгруппы
- В группе может быть несколько задач одного типа, например, несколько задач поиска вирусов. Они могут отличаться областью поиска и расписанием, например, одна задача может проверять весь компьютер раз в неделю, а другая только критические области, но каждый день.
- Если нужно выполнять поиск вирусов в одной и той же области с разным расписанием на разных компьютерах, разделите компьютеры на группы и создайте отдельные задачи в каждой группе. Например, чтобы выполнять полную проверку компьютера на серверах по выходным, а на рабочих станциях в рабочее время в фоновом режиме.
- Если в группе есть задача, и у группы есть подгруппа с задачей такого же типа, к компьютерам подгруппы применяются обе задачи. Как правило, это значит, что администратор не слишком хорошо продумал, какие задачи ему нужны.

  Особенно осторожным нужно быть, если это задачи обновления. Чтобы обновить Kaspersky Endpoint Security на компьютере, нужна одна задача обновления. Если задача обновления есть и в группе, и в подгруппе, на компьютерах подгруппы получается по две задачи обновления. Если одна задача обновления выполняется, вторая завершается с ошибкой. В результате администратор будет получать ошибки обновления при том, что обновление работает, а ошибка в конфигурации групп и задач

- Подгруппы можно исключить из области действия задачи. Тогда к компьютерам подгруппы будет применяться только задача подгруппы, а задача родительской группы применяться не будет

В отличие от политик, задачи можно создавать не только для групп. Администратор может создать задачу для любого списка компьютеров, от одного компьютера до произвольного набора компьютеров из разных групп.

Как лицензируется Kaspersky Endpoint Security для бизнеса

Какие есть лицензии Kaspersky Endpoint Security для бизнеса

Мы разобрались с тем, как компоненты Kaspersky Endpoint Security для бизнеса взаимодействуют между собой, и как ими управляет администратор.

Теперь разберемся, какие бывают лицензии Kaspersky Endpoint Security для бизнеса, и чем они отличаются.

Лицензия Kaspersky Endpoint Security для бизнеса бывает нескольких уровней:

- Cloud
- Облачное решение, позволяет управлять безопасностью рабочих мест, серверов и мобильных устройств через веб-браузер. Сервер администрирования в этом случае находится в облаке Microsoft Azure и заботу об инфраструктуре берет на себя Лаборатория Касперского, администратор занимается лишь развертыванием и управлением средствами защиты. Подробно об этом решении рассказывает курс KL 040 Kaspersky Endpoint Security Cloud.
- Стандартный
- Расширенный
- Последние два типа лицензий предназначены для on-premises продуктов, которые мы и будем рассматривать в этом курсе.
- Лицензии разного уровня дают право пользоваться разными продуктами Лаборатории Касперского и разными функциями в этих продуктах.

Что активируют лицензии в Kaspersky Endpoint Security для бизнеса

Чтобы использовать Kaspersky Security Center, его не обязательно активировать. Все, что нужно, чтобы управлять защитой рабочих станций, можно использовать без лицензии.

KESB Стандартный разрешает защищать рабочие станции, сервера и мобильные устройства.

Из функций Kaspersky Endpoint Security лицензия KESB Стандартный активирует компоненты защиты и контроля.

В Kaspersky Security Center лицензия KESB Стандартный активирует функции для управления мобильными устройствами. Чтобы управлять только защитой и контролем рабочих станций и серверов, Kaspersky Security Center активировать не обязательно.

KESB Расширенный разрешает защищать те же типы узлов: рабочие станции, сервера и мобильные устройства, но активирует больше функций.

В Kaspersky Endpoint Security для Windows лицензия KESB Расширенный позволяет использовать шифрование.

В Kaspersky Security Center лицензия KESB Расширенный позволяет использовать функции управления системами, в частности автоматически загружать и устанавливать исправления и обновления программ, создавать и разворачивать образы дисков с операционной системой и др.

Адресные лицензии

Если покупателю не нужны все функции KESB Расширенный, он может купить лицензию на отдельную функцию:

- Шифрование
- Управление мобильными устройствами
- Управление системами

Кроме функций, лицензии ограничены количеством устройств (узлов), которые можно защитить. Например, покупатель приобретает лицензию на 100 узлов, а если со временем хочет защитить больше устройств, покупает новую лицензию на, скажем, 150 или 200.

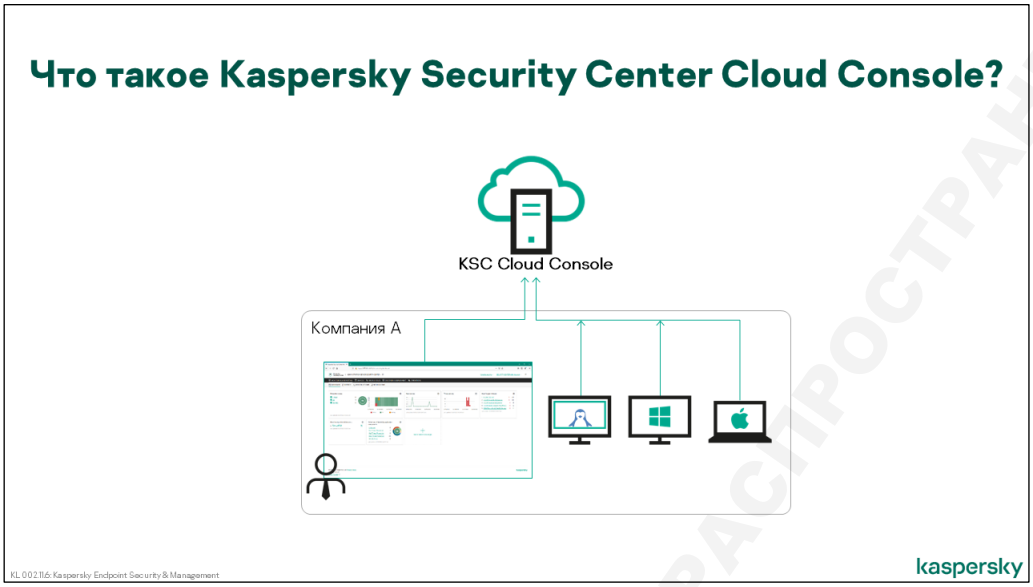
Все перечисленные лицензии, как правило, действуют в течение года. После этого клиент продлевает лицензию еще на год и так далее.

Лицензии по подписке

Кроме этого, Лаборатория Касперского поддерживает лицензии по подписке. Эти лицензии нужно покупать через специальных партнеров, и покупатель оплачивает их ежемесячно. Покупатель может приостановить подписку и продолжить ее позже.

С лицензией по подписке, покупатель может менять уровень функций и количество узлов хоть каждый месяц: расширять или сокращать лицензию в зависимости от того, что ему нужно.

Что такое Kaspersky Security Center Cloud Console



Kaspersky Security Center Cloud Console – это специальный Kaspersky Security Centry, который размещается в облаке (https://ksc.kaspersky.com). Сервер администрирования и СУБД поддерживаются специалистами "Лаборатории Касперского". Администратору не нужно устанавливать Kaspersky Security Center Cloud Console на свой компьютер или сервер, достаточно только зарегистрироваться в Kaspersky Security Center Cloud Console и создать рабочую область своей компании.

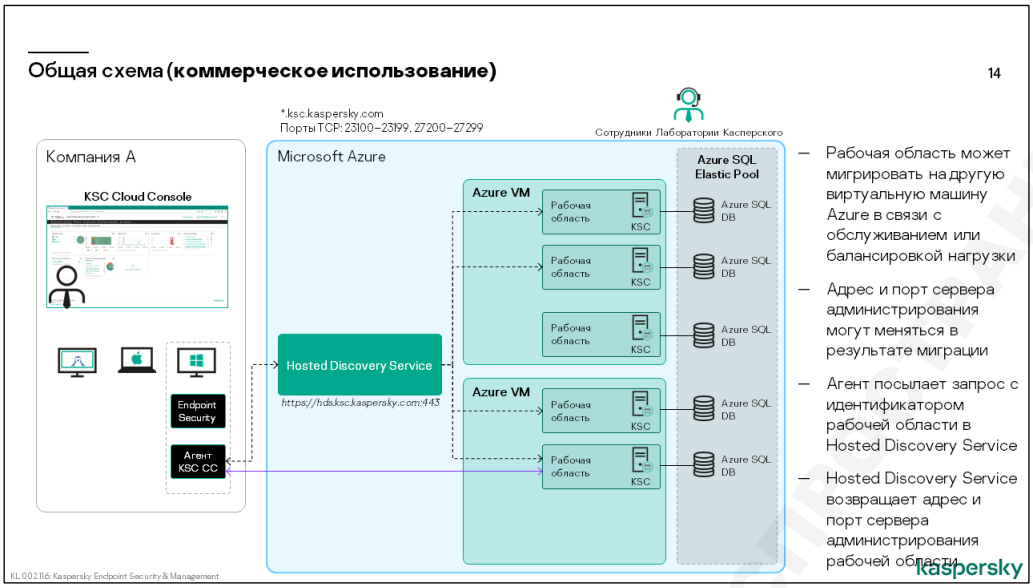
Kaspersky Security Center Cloud Console позволяет администратору устанавливать и управлять следующими программами "Лаборатории Касперского":

- Kaspersky Security для Windows Server
- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac
- Kaspersky Endpoint Agent

Общая схема взаимодействия

Администратор с помощью веб браузера может подключиться к своей рабочей области в облачной консоли Kaspersky Security Center, на устройствах компании установлены средства защиты и агент администрирования.

В облаке MS Azure развёрнуты виртуальные машины – Azure VM, на которых созданы рабочие области компаний. Каждая рабочая область представляет собой специальный сервер администрирования Kaspersky Security Center, у которого есть своя база данных в Azure SQL Elastic Pool.



Сервер администрирования и база данных для него создаются автоматически после того, как пользователь прошел мастер создания рабочей области.

В дальнейшем мы будем использовать термин "рабочая область", когда будем говорить о сервере администрирования и сервере баз данных облачной консоли Kaspersky Security Center.

Всем, кто работал с локальным Kaspersky Security Center или Kaspersky Endpoint Security Cloud, известно, что для того чтобы связаться с сервером администрирования, агент администрирования должен знать адрес сервера администрирования или виртуального сервера, а в случае с Kaspersky Endpoint Security Cloud, и порт подключения.

И эти данные практически никогда не меняются, если в этом нет необходимости у администратора.

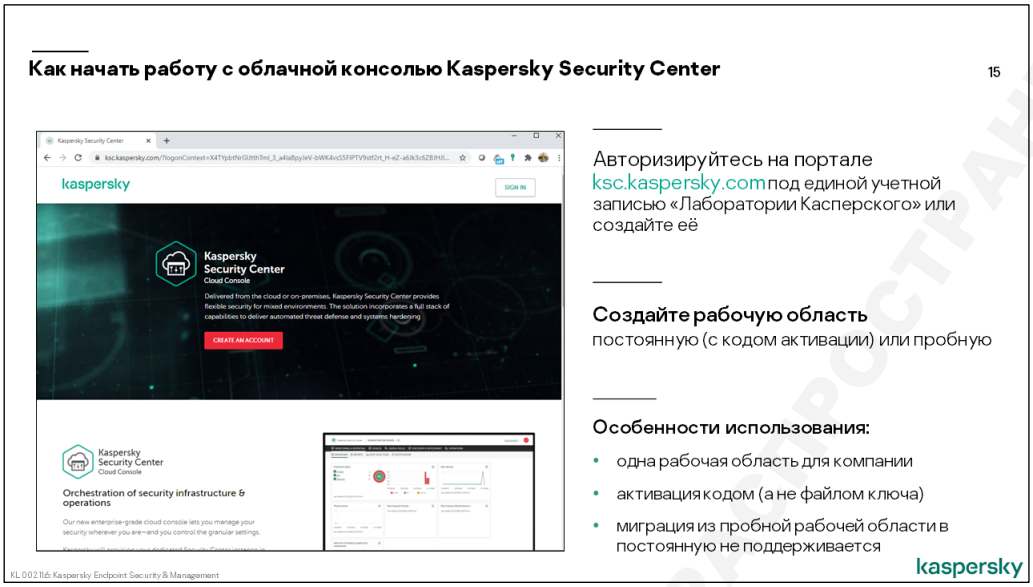
В случае с облачной консолью Kaspersky Security Center это не так. Агент администрирования облачной консоли Kaspersky Security Center не знает адрес и порт своей рабочей области. Он знает только идентификатор своей рабочей области. Чтобы узнать адрес и порт своей рабочей области, агент обращается по 443 порту к специальной службе Hosted Discovery Service (HDS).

Hosted Discovery Service — это специальная служба, развёрнутая в каждом вычислительном центре Microsoft. Она периодически опрашивает рабочие области и ведет список "идентификатор – адрес – порт рабочей области".

Служба Hosted Discovery Service возвращает агенту адрес и порт рабочей области, после чего агент подключается непосредственно к своей рабочей области. Для того чтобы агент смог успешно подключиться к своей рабочей области, необходимо, чтобы в брандмауэре были открыты порты 23100-23199 и 27200-27900 для исходящих TCP-соединений на адрес *ksc.kaspersky.com.

Использование агентом идентификатора обусловлено тем, что рабочая область не привязана жестко к виртуальной машине. Адрес и порт рабочей области могут меняться, например, при миграции на другую виртуальную машину в MS Azure. Миграция рабочей области может быть связана с обслуживанием или балансировкой нагрузки.

Как начать работу с облачной консолью Kaspersky Security Center



Для создания рабочей области необходима единая учетная запись для доступа к решениям «Лаборатории Касперского». Для того чтобы создать единую учетную запись, необходим действующий почтовый адрес.

После создания и активации единой учетной записи необходимо зайти на сайт ksc.kaspersky.com и создать рабочую область:

1. Ознакомиться и принять условия Соглашения, Политик конфиденциальности и Соглашения об обработке данных облачной консоли Kaspersky Security Center

2. Ввести имя компании

3. Задать имя рабочей области

   Текущая версия облачной консоли Kaspersky Security Center поддерживает работу только с одной рабочей областью на компанию

4. Выбрать страну, где расположена Ваша компания

   От выбора страны зависит территориальное расположение вычислительного центра Microsoft, в котором будут храниться и обрабатываться данные компании

5. Указать примерное количество устройств, которое планируется защищать

6. Вести код активации или заказать пробную рабочую область

   Если вы заказываете пробную рабочую область, учтите, что миграция из пробной рабочей области в коммерческую в текущей версии облачной консоли не поддерживается.

Дождаться письма о создании рабочей области (это может занять 10—15 минут). Если вы в течение часа так и не получили письма о создании рабочей области, необходимо обратиться в службу поддержки.

К особенностям использования облачной консоли Kaspersky Security Center можно отнести:

— Одна рабочая область для компании

  Если вы создали учетную запись в облачной консоли Kaspersky Security Center и планируете управлять сразу несколькими компаниями, то на данный момент такой сценарий не поддерживается. У одной рабочей области может быть только один главный администратор.

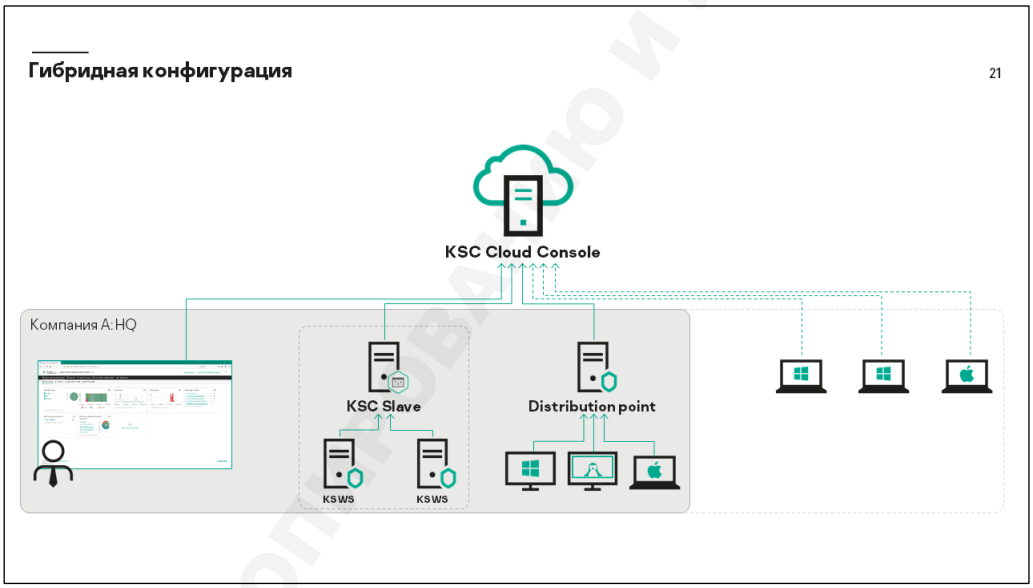
— Активация кодом

  Активировать рабочую область файлом ключа нельзя.

— Миграция пробной рабочей области в постоянную не поддерживается

  Лаборатория Касперского предоставляет тридцатидневный ознакомительный период использования облачной консоли Kaspersky Security Center. После того как ознакомительный период закончится, преобразовать пробную рабочую область в коммерческую нельзя. Чтобы продолжить использование Kaspersky Security Center Cloud Console после истечения срока действия пробной лицензии, необходимо удалить пробную рабочую область и создать другую с коммерческой лицензией.

Гибридная конфигурация



Гибридная конфигурация системы управления представляет собой схему управления, состоящую из локально установленных серверов администрирования Kaspersky Security Center и рабочей области в облачной консоли KSC.

В такой схеме управления рабочая область облачной консоли Kaspersky Security Center выполняет роль главного сервера администрирования, а локально установленные сервера администрирования — роль подчинённых серверов.

Такая схема может использоваться в процессе миграции как промежуточная, до завершения процесса миграции.

Также гибридную схему управления удобно использовать компаниям, имеющим большое количество пользователей, работающих вне офиса компании или находящихся в командировках, но контролировать и защищать их устройства все равно необходимо.

Использование гибридной схемы управления позволит:

- Легко распределить удаленные и локальные офисные устройства по разным серверам администрирования
- Снять вопрос с трудностями, возникающими при организации подключения удаленных устройств к локальному серверу администрирования, связанные с организацией доступа, поддержкой доступности и безопасности сервера администрирования и т.д.

В тоже время такая схема позволит сохранить единую систему управления и все преимущества, с ней связанные.

1.2 О чем этот курс

Что есть и чего нет в этом курсе

В Kaspersky Endpoint Security для бизнеса входит много продуктов и возможностей. Этот курс не пытается рассказать обо всем. Он рассказывает только, как защитить не слишком большую сеть из компьютеров с операционной системой Windows.

Поэтому курс рассказывает не обо всех продуктах, которые входят в Kaspersky Endpoint Security для бизнеса, а только о:

- Kaspersky Endpoint Security для Windows
- Kaspersky Security Center
- И немного о Kaspersky Security для Windows Servers

Курс не касается продуктов:

- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac
- Kaspersky Endpoint Systems Security
- Kaspersky Endpoint Security для Android
- Safe Browser для iOS

— Kaspersky Security для виртуальных сред
— Kaspersky Anti-Targeted Attack Platform / Kaspersky Endpoint Detection and Response

Также курс рассказывает не обо всем, что могут Kaspersky Endpoint Security для Windows и Kaspersky Security Center, а только о том, как:

— Установить защиту на компьютеры
— Управлять защитой компьютеров
— Управлять компонентами контроля
— Использовать один Сервер администрирования Kaspersky Security Center

Курс не касается того, как:

— Управлять шифрованием
— Исправлять уязвимости и обновлять сторонние программы
— Создавать и разворачивать образы компьютеров
— Защищать большие, сложные и распределенные сети с помощью Агентов обновлений, Шлюзов соединений или нескольких Серверов администрирования Kaspersky Security Center

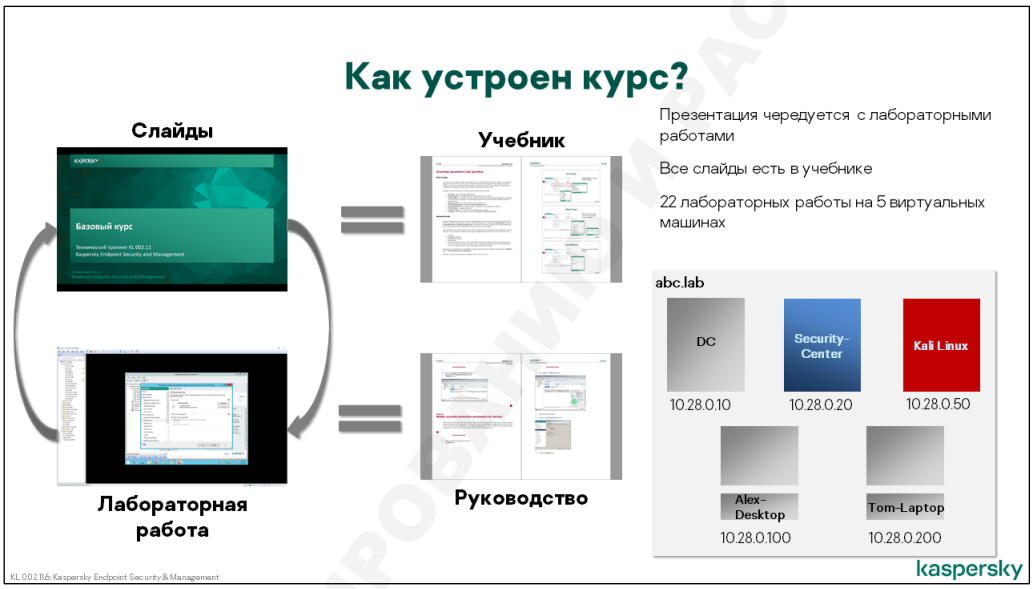
Где узнать больше о том, что не вошло в курс

Все, что не вошло в этот курс, входит в другие курсы, посвященные отдельным продуктам и технологиям:

Как защищать рабочие станции Linux	KL 013	1 день
Как защищать сервера Linux	KL 007	1 день
Как защищать рабочие станции Mac	KL 011	1 день
Как защищать сервера и встраиваемые версии Windows	KL 005	1.5 дня
Как управлять мобильными устройствами	KL 010	1 день
Как управлять шифрованием	KL 008	1 день
Как исправлять уязвимости и устанавливать обновления сторонних программ	KL 009	1 день

Как управлять защитой в больших, сложных и распределенных сетях	KL 302	2 дня
Как защищать виртуальные машины с помощью Kaspersky Security for Virtualization. Agentless	KL 014	1 день
Как защищать виртуальные машины с помощью Kaspersky Security for Virtualization. Light Agent	KL 031	1 день
Как решать проблемы	KL 016	1 день
Как реализовать политику Default Deny	KL 032	1 день
KATA/KEDR	KL 025	2 дня

Из чего состоит курс



Курс состоит из презентаций и лабораторных работ, которые сменяют друг друга. Каждую новую тему сначала инструктор поясняет на слайдах, а потом слушатели пробуют сами в лабораторной работе.

Учебник содержит все слайды и подробно раскрывает все темы и настройки продуктов.

Что делать в лабораторных работах, подробно описывает руководство по лабораторным работам.

Слушатели делают лабораторные работы на виртуальных машинах. Виртуальная среда зависит от класса: это может быть VMware Workstation, VMware vSphere, Microsoft Hyper-V или что-то еще. Руководство по лабораторным работам написано для виртуальной среды VMware Workstation.

В лабораторных слушатели используют пять виртуальных машин с фиксированными ролями:

DC	Предоставляет службы доменов AD, DNS, доступа к файлам
KSC	Является Сервером администрирования Kaspersky Security Center, откуда администратор управляет защитой

Alex-Desktop	Олицетворяет стационарные компьютеры в сети компании
Tom-Laptop	Олицетворяет мобильные компьютеры, которые могут быть вне сети компании
Kali Linux	Предоставляет инструменты для атаки на компьютеры организации

2. Как установить Kaspersky Endpoint Security для бизнеса

2.1 Что и в каком порядке устанавливать

В результате внедрения должна получиться сеть, все компьютеры которой защищены, а администратор имеет возможность управлять защитой централизованно. Для этого нужно установить на компьютеры компоненты Kaspersky Security Center и Kaspersky Endpoint Security для Windows.

Сначала установите Сервер администрирования Kaspersky Security Center. Сервер администрирования централизованно управляет защитой, и помогает устанавливать остальные компоненты.

Консоль администрирования на базе MMC автоматически устанавливается вместе с Сервером администрирования. Чтобы управлять сервером удаленно, используйте удаленный доступ к рабочему столу, или установите Консоль администрирования Kaspersky Security Center на компьютер администратора.

Web Console также может устанавливаться автоматически вместе Сервером администрирования, поэтому по окончании установки у администратора будет выбор, какую консоль управления использовать.

Для защиты сети на каждый компьютер установите Kaspersky Endpoint Security. Сам по себе Kaspersky Endpoint Security не взаимодействует с Kaspersky Security Center, поэтому для централизованного управления на каждый компьютер установите Агент администрирования.

Если нужно дать разным компьютерам разные настройки, разделите компьютеры на группы. Старайтесь не создавать лишние группы. Чтобы легко находить компьютеры, импортируйте структуру из Active Directory.

Подводя итоги, внедряйте защиту в такой последовательности:

1. Установите Сервер администрирования Kaspersky Security Center
2. Установите агенты Kaspersky Security Center и Kaspersky Endpoint Security
3. Разделите компьютеры на группы

2.2 Как организовать процесс

Чтобы просто установить все компоненты Kaspersky Endpoint Security для бизнеса, много времени не нужно. Время уходит на то, чтобы найти и решить проблемы.

Чтобы не тратить лишнего времени, подготовьтесь. Попробуйте то, что вы хотите сделать, в тестовой среде. Если возникнут проблемы, подумайте, как их обойти. Или найдите решение, которое сможете быстро использовать, если проблема возникнет на компьютерах сети.

Вряд ли вы обнаружите все потенциальные проблемы в тестовой среде. Поэтому в рабочей сети начните с небольшого количества компьютеров: 10–20. Постарайтесь выбрать разные компьютеры, чтобы обнаружить как можно больше потенциальных проблем. Если найдете новые проблемы, вернитесь в тестовую среду, воспроизведите их и придумайте, как решить или обойти.

Внедряйте поэтапно, например, по 100 компьютеров за раз. Так вы будете находить новые проблемы постепенно, и количество проблемных компьютеров всегда будет небольшим.

Подводя итоги, внедряйте на компьютеры так:

1. Установите программы в тестовой среде
2. Установите программы на 10-20 характерных компьютеров
3. Установите программы на все компьютеры, поэтапно, по 100 компьютеров за этап

На каждом шаге дайте себе время на то, чтобы найти и решить проблемы. Не переходите к следующему шагу, пока не придумаете, как решить или обойти все проблемы. Ищите решения проблем в тестовой среде, а не на рабочих компьютерах.

Сейчас тестовая среда — это, обычно, виртуальные машины в отделе ИТ. Если виртуальные машины — непозволительная роскошь, используйте для тестов компьютеры администраторов.

3. Как установить Kaspersky Security Center

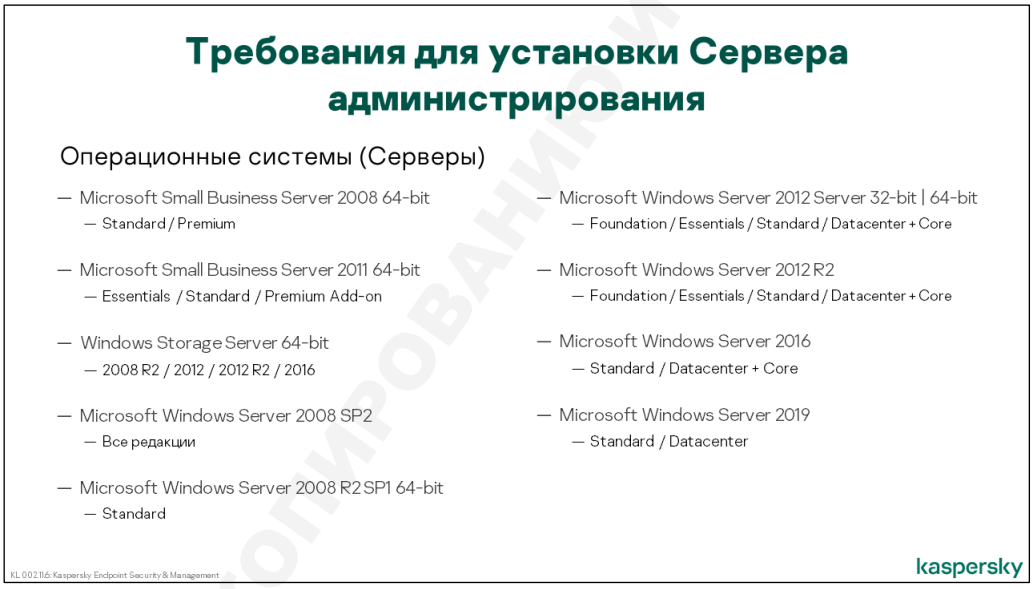
3.1 Требования к Серверу администрирования

Чтобы установить Сервера администрирования Kaspersky Security Center, подготовьте компьютер, который удовлетворяет системным требованиям.

Если узлов в сети меньше 1000, Сервер администрирования и сервер баз данных легко уживутся на одном компьютере. Если узлов больше, используйте более производительный компьютер или используйте отдельный компьютер для сервера баз данных.

Компьютер для Сервера администрирования может быть физический или виртуальный. Если используете виртуальный Сервер, проверьте, что виртуальная среда удовлетворяет системным требованиям.

Поддержка серверных версий Windows



Полный список поддерживаемых серверных операционных систем выглядит так:

- Microsoft Small Business Server 2008 Standard / Premium 64-bit
- Microsoft Small Business Server 2011 Essentials / Standard / Premium Add-on 64-bit
- Windows Storage Server 2008 R2 / 2012 / 2012 R2 / 2016 64-bit
- Microsoft Windows Server 2008 SP2 (все редакции)
- Microsoft Windows Server 2008 Foundation SP2 32-bit / 64-bit
- Microsoft Windows Server 2008 R2 Standard SP1 64-bit
- Microsoft Windows Server 2012 Server Core / Foundation / Essentials / Standard / Datacenter 32-bit / 64-bit
- Microsoft Windows Server 2012 R2 Server Core / Foundation / Essentials / Standard / Datacenter
- Microsoft Windows Server 2016 Server Core / Standard / Datacenter
- Microsoft Windows Server 2019 Server Core / Standard / Datacenter

Поддержка рабочих станций Windows

Лучше устанавливать Сервер администрирования на серверную версию Windows. Но в сетях небольшого размера (до пары сотен компьютеров) можно использовать и производительную рабочую станцию. Также можете использовать рабочую станцию в тестовой среде.

Сервер администрирования можно установить на такие несерверные версии Windows:

- Microsoft Windows 10 Pro / Enterprise / Education / Mobile RS5 32-bit / 64-bit
- Microsoft Windows 10 Pro / Enterprise / Education / Mobile RS4 32-bit / 64-bit
- Microsoft Windows 10 Pro / Enterprise / Education / Mobile RS3 32-bit / 64-bit

Microsoft Windows 10 Pro for Workstations RS3 / RS4 / RS5 / 19H1 / 19H2 / 20H1 / 20H2

- Microsoft Windows 10 Enterprise 2015 LTSC 32-bit / 64-bit
- Microsoft Windows 10 Enterprise 2016 LTSC 32-bit / 64-bit
- Microsoft Windows 8.1 Pro / Enterprise 32-bit / 64-bit
- Microsoft Windows 8 Pro / Enterprise 32-bit / 64-bit
- Microsoft Windows 7 Professional / Enterprise / Ultimate SP1 32-bit / 64-bit

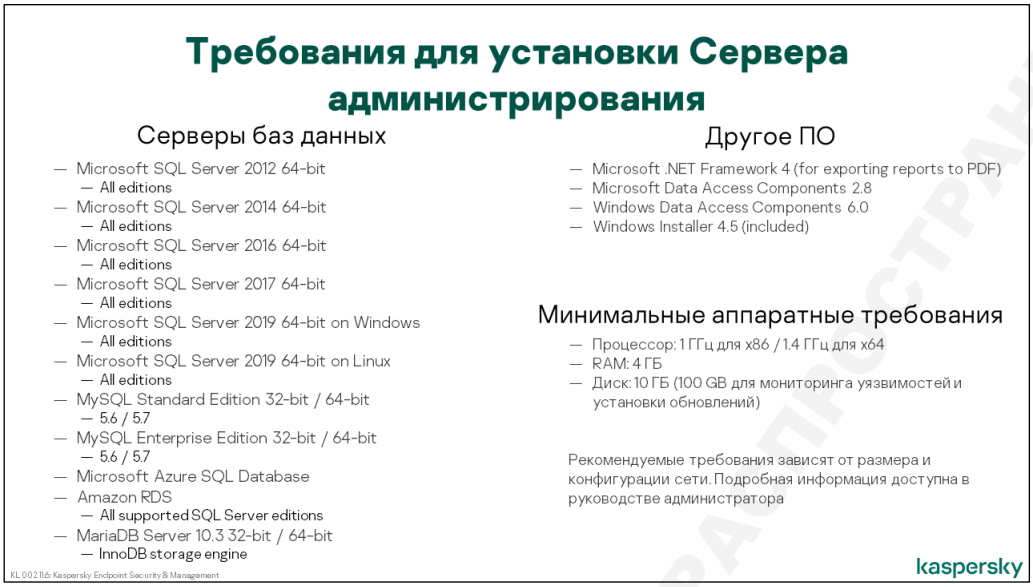
Поддержка виртуальных платформ

Чтобы установить Сервер администрирования на виртуальную машину, используйте одну из следующих платформ виртуализации:

- VMware vSphere 6.7 / 7.1
- VMware Workstation 15 Pro / 16 Pro
- Microsoft Hyper-V Server 2012 / 2012 R2 / 2016 / 2019
- Citrix XenServer 7.1 LTSR / 8.x
- Parallels Desktop 16
- Oracle VM VirtualBox 6.x (поддерживаются гостевые операционные системы Windows)

Виртуальная машина должна соответствовать требования к операционной системе, программному и аппаратному обеспечению.

Поддержка серверов управления базами данных



Сервер администрирования в работе использует базу данных, для хранения которой необходим SQL-сервер. Поддерживается хранение базы данных на следующих версиях SQL-серверов:

- **Microsoft SQL Server**
  - **Microsoft SQL Server 2012 (all editions) 64-bit**
  - **Microsoft SQL Server 2014 (all editions) 64-bit**
  - **Microsoft SQL Server 2016 (all editions) 64-bit**
  - **Microsoft SQL Server 2019 (all editions) 64-bit**
  - **Microsoft SQL Server 2016 (all editions) 64-bit on Windows**
  - **Microsoft SQL Server 2016 (all editions) 64-bit on Linux**
- **MySQL**
  - MySQL Standard Edition 5.6 / 5.7 32-bit / 64-bit
  - MySQL Enterprise Edition 5.6 / 5.7 32-bit / 64-bit
- **Microsoft Azure SQL Database**
- **Amazon RDS** — all supported SQL Server editions
- **MariaDB Server**
  - MariaDB Server 10.3 32-bit / 64-bit
  - InnoDB storage engine

Microsoft SQL Server Express больше не входит в поставку Kaspersky Security Center.

Начиная с версии Kaspersky Security Center 10 SP3, Microsoft SQL Server Express необходимо загружать и устанавливать самостоятельно. Помните, что Express-редакции имеют ограничения и не должны использоваться для управления большим числом компьютеров (больше 5000). Подробнее об этом рассказывается в курсе KL 302.

SQL-сервер может быть установлен на том же компьютере, что и Сервер администрирования или на любом другом компьютере в сети. Важно, чтобы Сервер администрирования имел доступ с правами чтения и записи в базу, расположенную на SQL-сервере. При установке Сервера администрирования и SQL-сервера на одном компьютере проблем с доступом нет в принципе.

Дополнительные требования к ПО

Помимо требований к ОС, на компьютере также должны быть установлены:

- Microsoft .NET Framework 4 (установите, как компонент Windows)
- Microsoft Data Access Components 2.8
- Windows Data Access Components 6.0
- Windows Installer 4.5 (включено в поставку)

Выделите для Сервера администрирования новый компьютер. Если это невозможно, проверьте, что на компьютере нет Агента администрирования Kaspersky Security Center. Программа установки автоматически обнаруживает установленный Агент и просит администратора удалить его.

Минимальные требования к оборудованию

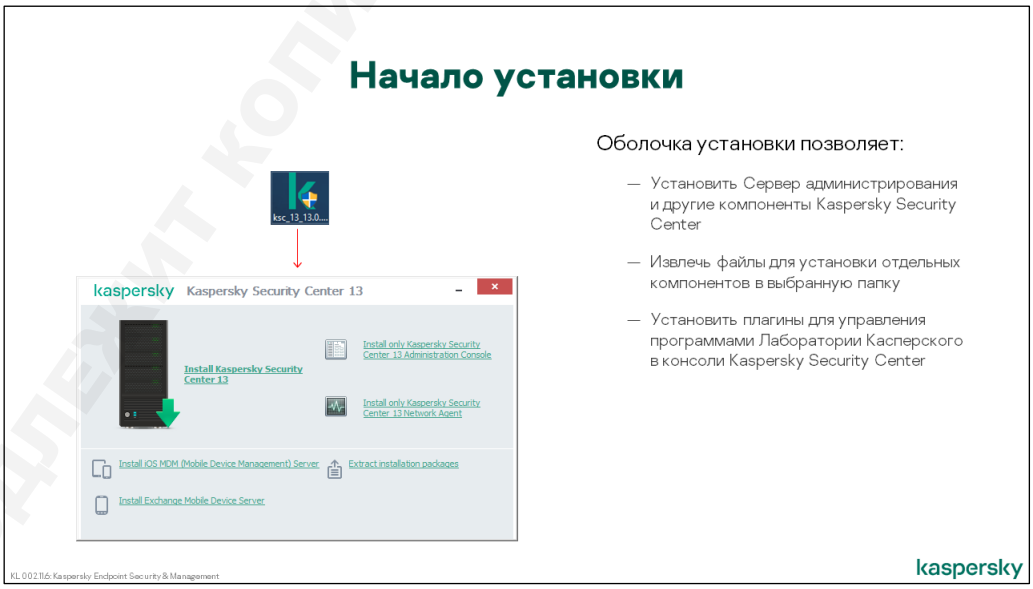
Минимальные требования к аппаратной конфигурации:

- Процессор с частотой не менее 1 ГГц (1.4 ГГц для 64-битных систем)
- 4 ГБ оперативной памяти
- 10 ГБ свободного дискового пространства (для использования функционала Управление системами потребуется не меньше 100 ГБ свободного места)

Для обслуживания большого числа клиентов потребуется более производительный сервер. Рекомендации можно найти в руководстве администратора. Обсуждение практического опыта использования Сервера администрирования в крупных сетях находится в курсе KL 302. Kaspersky Endpoint Security and Management. Масштабирование.

3.2 Установка Сервера администрирования

Где взять дистрибутив Kaspersky Security Center



Чтобы установить Kaspersky Security Center, запустите программу установки.

Прежде чем приступать к установке Kaspersky Security Center, необходимо установить и настроить сервер баз данных.

Программу установки Kaspersky Security Center можно загрузить с веб-сайта Лаборатории Касперского (*https://www.kaspersky.com/small-to-medium-business-security/downloads/security-center*) или со страницы о продукте на сайте технической поддержки (*http://support.kaspersky.ru/ksc13#downloads*).

Есть две программы установки:

- **ksc_13_13.0.0.1147_full_ru.exe** — полный дистрибутив Kaspersky Security Center, включающий все собственные компоненты, инсталляционные пакеты Агента администрирования и Kaspersky Endpoint Security 11.6 для Windows, Microsoft .NET Framework и другие вспомогательные программы, а также плагины управления всеми поддерживаемыми продуктами. Размер дистрибутива составляет около 1 ГБ
- **ksc_13_13.0.0.1147_lite_ru.exe** — облегченная версия дистрибутива, в которой отсутствует инсталляционный пакет Kaspersky Endpoint Security для Windows, Microsoft .NET Framework и некоторые вспомогательные программы, а из плагинов имеются только плагины управления компонентами Kaspersky Security Center 13. Размер дистрибутива составляет около 140 МБ. Такой дистрибутив можно использовать для обновления версии компонентов Kaspersky Security Center

Оболочка инсталлятора Kaspersky Security Center

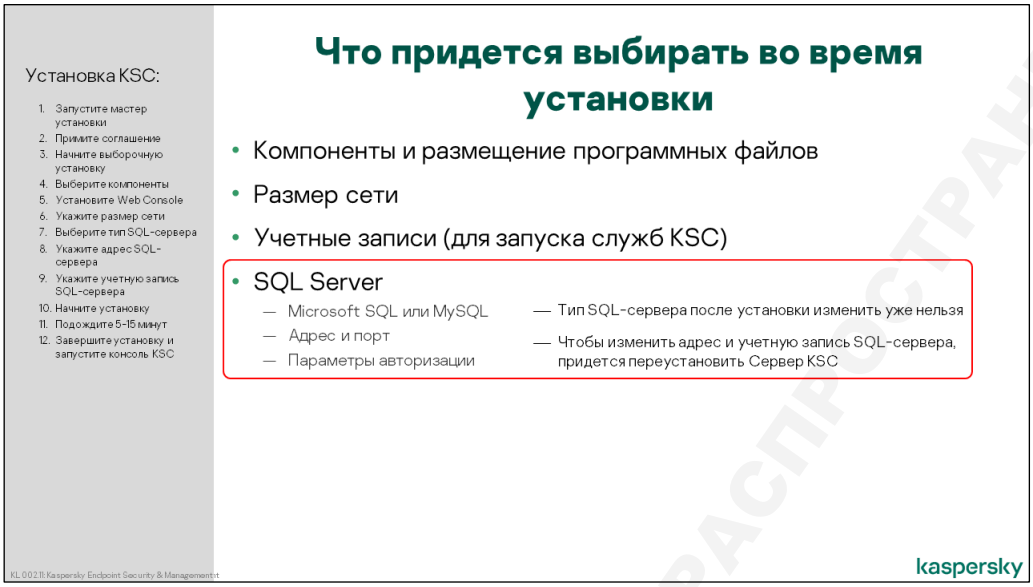
При запуске полной версии дистрибутива запускается оболочка программы установки. Из окна оболочки можно запустить установку отдельных компонентов, например, Сервера администрирования или Консоли администрирования. Также можно извлечь инсталляционные файлы для выбранных компонентов в папку, указанную администратором.

Из программы-оболочки можно извлечь или установить такие продукты:

- Сервер администрирования Kaspersky Security Center
- Консоль администрирования Kaspersky Security Center
- Агент администрирования Kaspersky Security Center
- Kaspersky Endpoint Security 11.6 для Windows (только извлечь)
- iOS MDM Server (компонент Kaspersky Security Center для управления мобильными устройствами)
- Kaspersky Endpoint Security for Android (только извлечь)
- Microsoft Exchange Mobile Devices Server (компонент Kaspersky Security Center для управления мобильными устройствами)
- Плагины управления программами

Этот курс рассматривает только Сервер, Консоль и Агент администрирования, а также Kaspersky Endpoint Security.

Что нужно знать перед установкой



В ходе установки администратор выбирает:

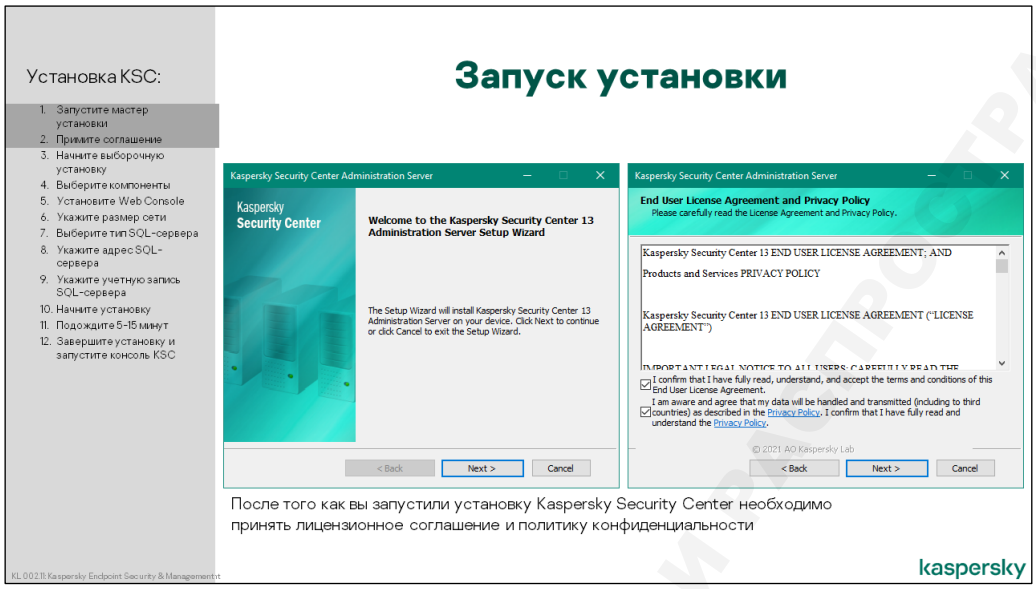
- Компоненты Kaspersky Security Center (в том числе новая Web Console)
- Папку установки
- Тип SQL-сервера и параметры подключения к нему
- Путь к общей папке Сервера администрирования
- Порты и адрес подключения к Серверу администрирования
- Плагины для управления продуктами

Почти все значения можно будет изменить после установки. Нельзя изменить только тип SQL-сервера. Если выбрать Microsoft SQL, то потом перейти на MySQL без потери данных нельзя.

Выбрать другой SQL-сервер того же типа без потери данных можно, но непросто. Нужно создать резервную копию данных Сервера администрирования. Переустановить Сервер администрирования и выбрать другой SQL-сервер. И после этого восстановить данные из резервной копии.

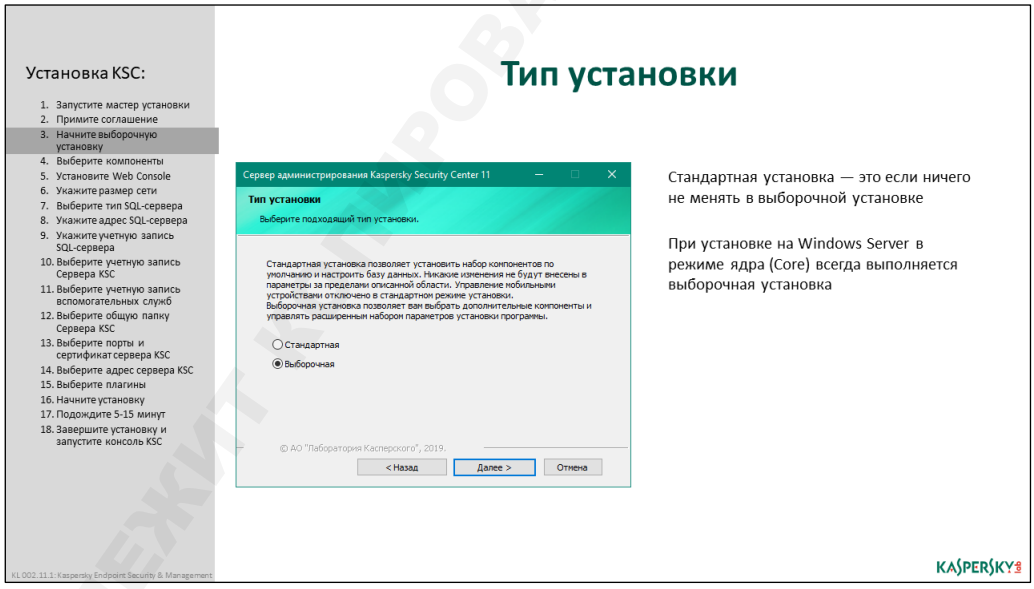
Мастер установки

Запуск установки



На первом шаге установки Kaspersky Security Center 13 от Администратора требуется принять лицензионное соглашение и политику конфиденциальности.

Типы установки



Установку Сервера администрирования можно выполнить в выборочном или стандартном режиме[2].

[2] На Windows Server в режиме Core, доступна только выборочная установка

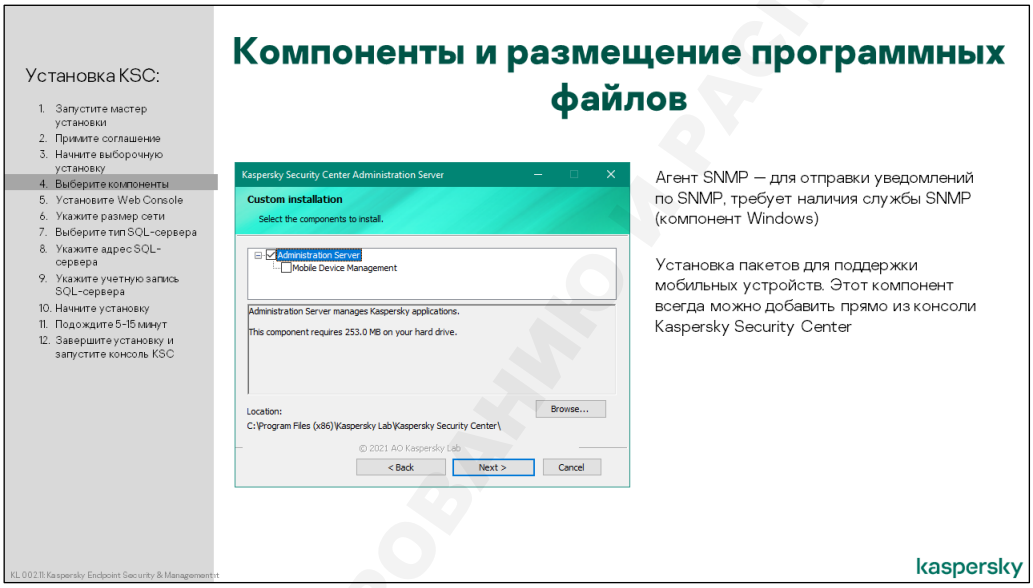
В стандартной установке от администратора требуется:

- Принять лицензионное соглашение Kaspersky Security Center
- Указать размер сети
- Выбрать тип сервера баз данных
- Настроить параметры подключения к серверу баз данных

В дистрибутив Kaspersky Security Center больше не входит дистрибутив Microsoft SQL-сервера. Поэтому, прежде чем приступить к установке Сервера Администрирования, в сети желательно развернуть и настроить сервер баз данных Microsoft SQL или MySQL

Если пойти по пути Выборочной установки и оставить все настройки по умолчанию, результат будет такой же, как и у Стандартной установки.

Компоненты и размещение программных файлов

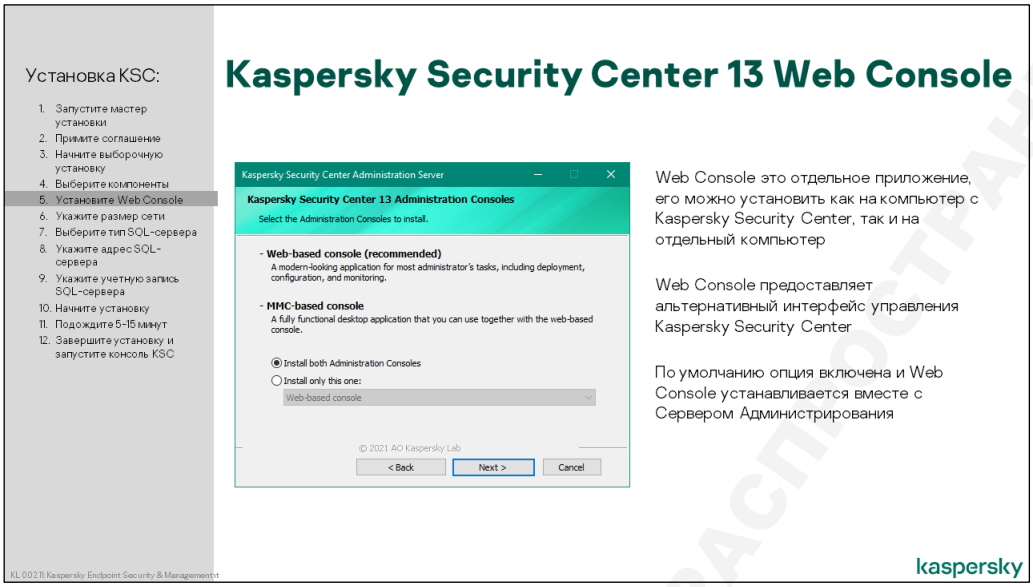


Вместе с Сервером администрирования можно установить компонент **Управление мобильными устройствами**. **Он** необходим для управления продуктом Kaspersky Endpoint Security for Mobile через Kaspersky Security Center. Подробности содержатся в курсе KL 010.

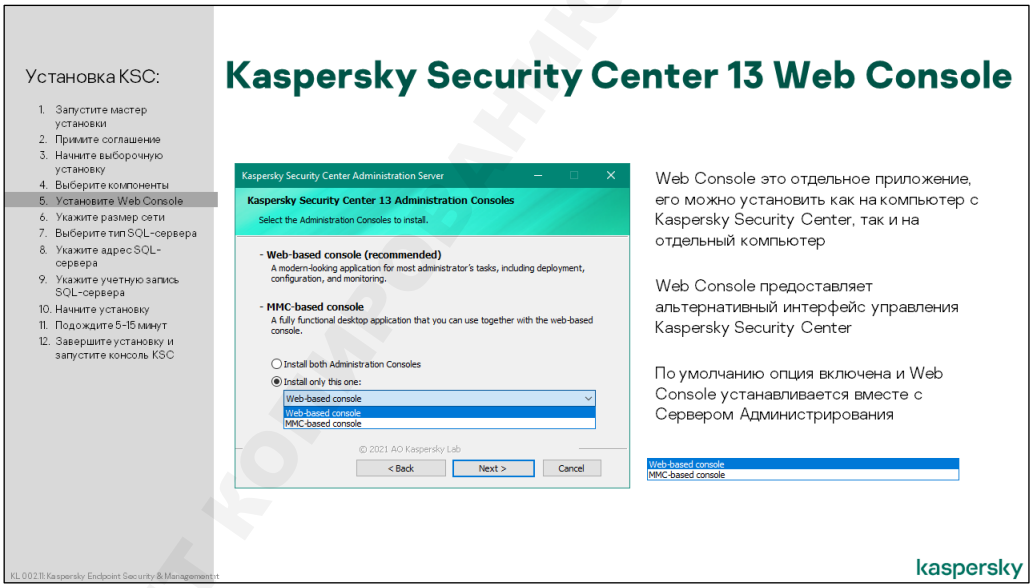
Здесь же под списком компонентов можно изменить размещение программных файлов Сервера администрирования. Если вы хотите перенести файлы, потому что на диске C: мало места, подумайте о том, чтобы перенести только общую папку Сервера администрирования. Ее можно перенести независимо от программных файлов, и она занимает значительно больше места, чем остальные программные файлы вместе взятые. Путь к общей папке вы выбираете дальше в мастере установки.

Помните, что резервные копии Сервера администрирования хранятся в папке данных – *%ProgramData%\KasperskySC*. Резервные копии имеют значительный объем: до нескольких гигабайт, в зависимости от количества узлов.

Web Console

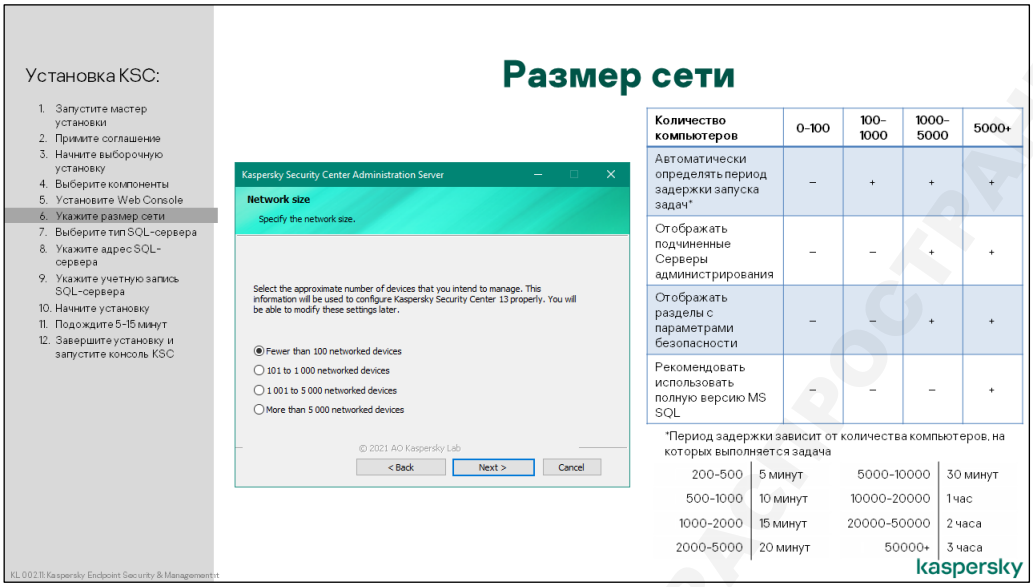


Web Console — это отдельное приложение, его можно установить как на компьютер с Kaspersky Security Center, так и на отдельный компьютер.



Web Console входит в состав дистрибутива Kaspersky Security Center 13 и на одном из шагов мастер установки спрашивает, хотите ли вы установить Web Console вместе с Kaspersky Security Center. Если ничего не менять, то Web Console установится с параметрами по умолчанию, в частности, порт подключения к Web Console будет 8080.

Размер сети



Размер сети можно выбрать из четырех вариантов:

- Менее 100 компьютеров в сети
- От 100 до 1000 компьютеров в сети
- От 1000 до 5000 компьютеров в сети
- Более 5000 компьютеров в сети

От ответа администратора зависят следующие параметры Сервера администрирования:

Количество компьютеров в сети	Менее 100	От 100 до 1000	От 1000 до 5000	Более 5000
Автоматически определять период задержки запуска задач	–	+	+	+
Отображать подчиненные Серверы администрирования	–	–	+	+
Отображать разделы с параметрами безопасности	–	–	+	+

Автоматическое определение периода задержки при запуске задач относится к расписанию групповых задач поиска вирусов, обновления, поиска уязвимостей и пр.

При одновременном запуске задачи на большом количестве компьютеров резко возрастает загрузка сети и нагрузка на Сервер администрирования. Чтобы сгладить скачок, задача может запускаться на компьютерах не строго в указанное время, а после случайной задержки.

Администратор может включить случайный разброс времени запуска и затем выбрать интервал задержки вручную или положиться на автоматическое определение интервала. На каждом компьютере независимо выбирается случайное значение задержки в пределах заданного или автоматически выбранного интервала.

Как работает автоматическое распределение периода задержки

При автоматическом определении периода задержки его величина зависит от количества компьютеров, на которых запускается задача.

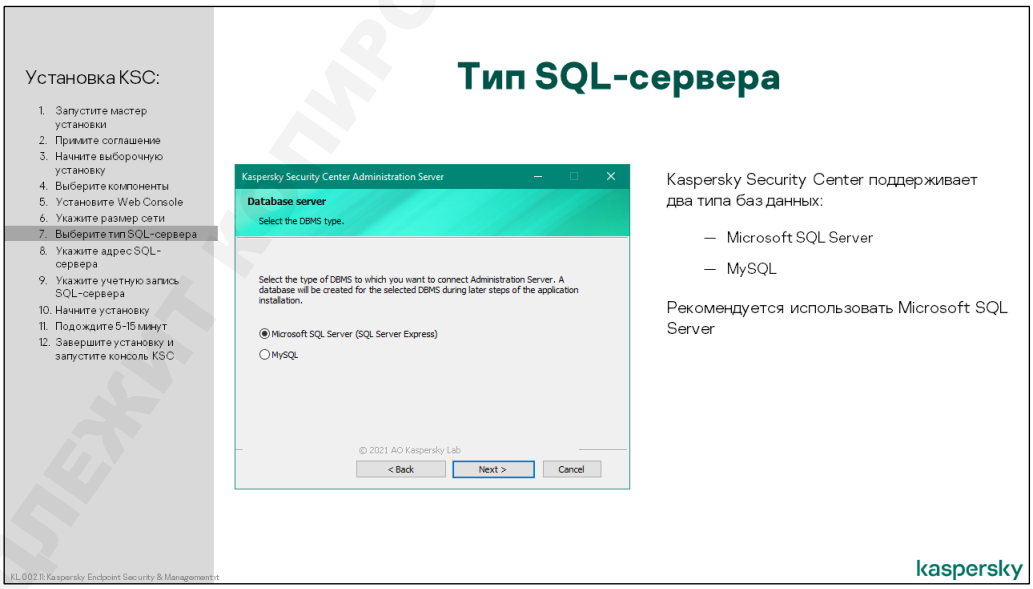
Количество компьютеров	Период задержки
0–200	0 минут
200–500	5 минут
500–1000	10 минут
1000–2000	15 минут
2000–5000	20 минут
5000–10000	30 минут
10000–20000	1 час
20000–50000	2 часа
50000+	3 часа

О подчиненных серверах администрирования и параметрах безопасности рассказывает курс KL 302. «Kaspersky Endpoint Security and Management. Масштабирование». В небольших и средних сетях эти функции используются редко.

Разницы в настройках по умолчанию между выбором сети от 1000 до 5000 компьютеров и сети с более 5000 компьютеров нет. При выборе более 5000 компьютеров в сети мастер установки не рекомендует использовать бесплатную версию сервера Microsoft SQL. О работе в больших сетях рассказывает курс KL 302. «Kaspersky Endpoint Security and Management. Масштабирование».

Выбор размера сети влияет только на пару настроек интерфейса, которые можно легко изменить после установки. При этом разница есть только между выбором сети до 1000 компьютеров и больше 1000 компьютеров. Никакие рабочие параметры Сервера администрирования этот выбор не затрагивает.

Выбор типа SQL-сервера



Сервер администрирования хранит события, информацию о компьютерах и часть настроек в базе данных SQL.

Хранить базу данных Сервер администрирования может в одном из двух типов SQL-серверов:

- Microsoft SQL Server
- MySQL

Что выбрать, зависит от предпочтений компании и администратора.

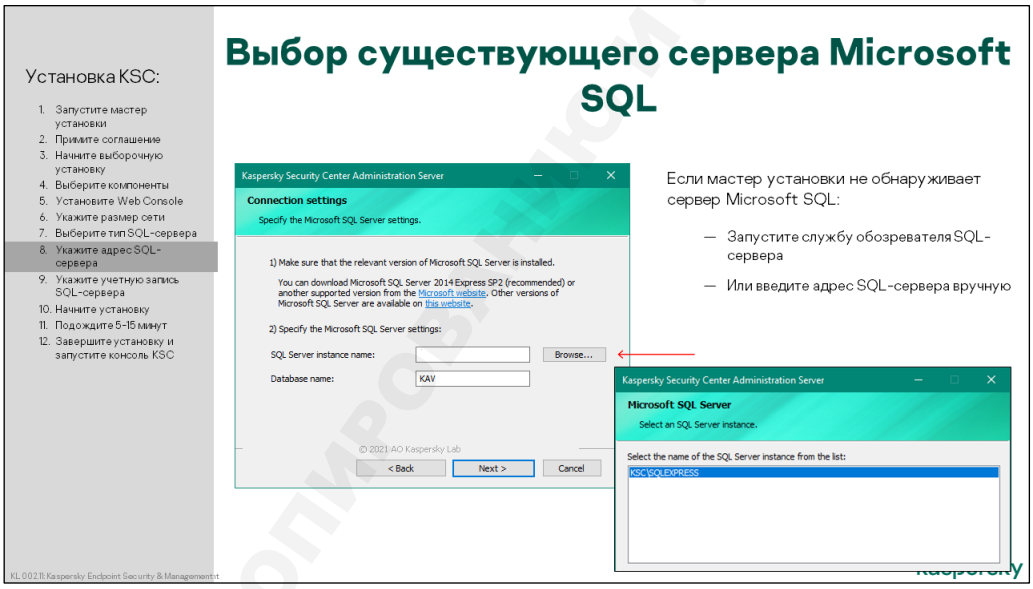
Microsoft SQL Server является индустриальным стандартом и рекомендуется для больших сетей от 5000 узлов и выше.

MySQL-сервер имеет открытый исходный код и может работать на операционной системе Linux. Поэтому MySQL иногда выбирают государственные структуры.

В состав Kaspersky Security Center, начиная с версии 10 SP3, больше не входит Microsoft SQL Server Express. Поэтому администратору необходимо самостоятельно установить и настроить SQL-сервер. Желательно сделать это до начала установки Kaspersky Security Center.

Выбор существующего сервера Microsoft SQL

Если вы решили использовать Microsoft SQL-сервер, укажите полное имя экземпляра SQL-сервера и имя базы данных для Сервера администрирования.

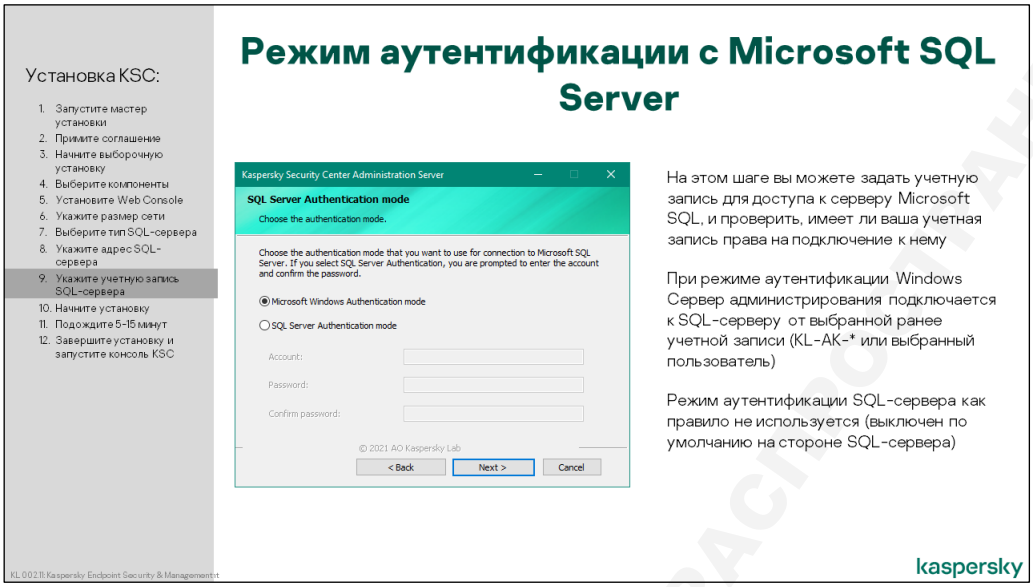


Чтобы найти нужный экземпляр в сети, используйте кнопку **Обзор…**. Если экземпляра нет в списке, проверьте, что на SQL-сервере запущена служба *SQL Server Browser*. По умолчанию она отключена.

Если вы не установили сервер Microsoft SQL заранее, можете установить его не закрывая мастер установки KSC. В окне выбора параметров SQL-сервера есть две ссылки на веб-страницы Microsoft:

- Ссылка на страницу загрузки Microsoft SQL Server 2014 SP2 Express, бесплатной версии, рекомендуемой для небольших сетей до 5000 узлов
- Ссылка на страницу Microsoft SQL Server, где можно найти описания разных редакций и выбрать подходящую

Как подключиться к серверу Microsoft SQL



Базу данных для Сервера администрирования создает программа установки. Впоследствии Сервер администрирования подключается к базе, чтобы записывать и извлекать из нее события.

Инсталлятору нужны права, чтобы создать базу. Серверу администрирования нужны права чтобы записывать и читать из базы.

Если выбрать **Режим аутентификации Microsoft Windows**, инсталлятор подключается к SQL-серверу от имени текущего пользователя Windows. При этом Сервер администрирования подключается к базе от имени учетной записи своей службы (*KL-AK-<*>*), которую администратор выбрал на одном из предыдущих шагов.

Следовательно, у текущего пользователя должны быть права на SQL-сервере, чтобы создать базу.

Если администратор Kaspersky Security Center не может получить права создавать базы на SQL-сервере, пусть администратор SQL-сервера создаст пустую базу, а администратор Kaspersky Security Center укажет имя экземпляра и базы в мастере установки.

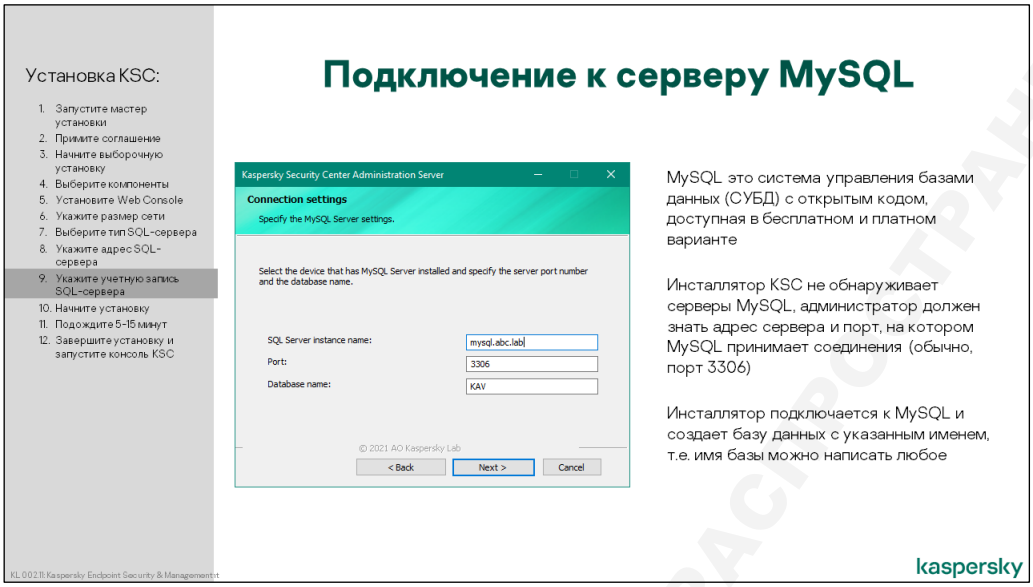
У учетной записи *KL-AK-<*>* (или другой записи, которую выбрал администратор), должны быть права читать и писать в базу. До установки это проверить нельзя, но после установки можно дать выбранной записи недостающие права или вообще выбрать другую запись для службы Сервера администрирования.

Если выбрать **Режим аутентификации SQL-сервера**, укажите учетную запись SQL-сервера (не Windows). Инсталлятор и Сервер администрирования оба будут использовать эту запись, чтобы создать базу и записывать в нее события.

По умолчанию во всех поддерживаемых версиях SQL-сервера режим аутентификации SQL-сервера отключен. Такая аутентификация считается устаревшей и небезопасной. Microsoft и Лаборатория Касперского рекомендуют режим аутентификации Microsoft Windows Authentication Mode.

Если экземпляр SQL-сервера находится на другом компьютере, проверьте, что SQL-сервер разрешает подключения по сети, и что порты не блокируются сетевым экраном.

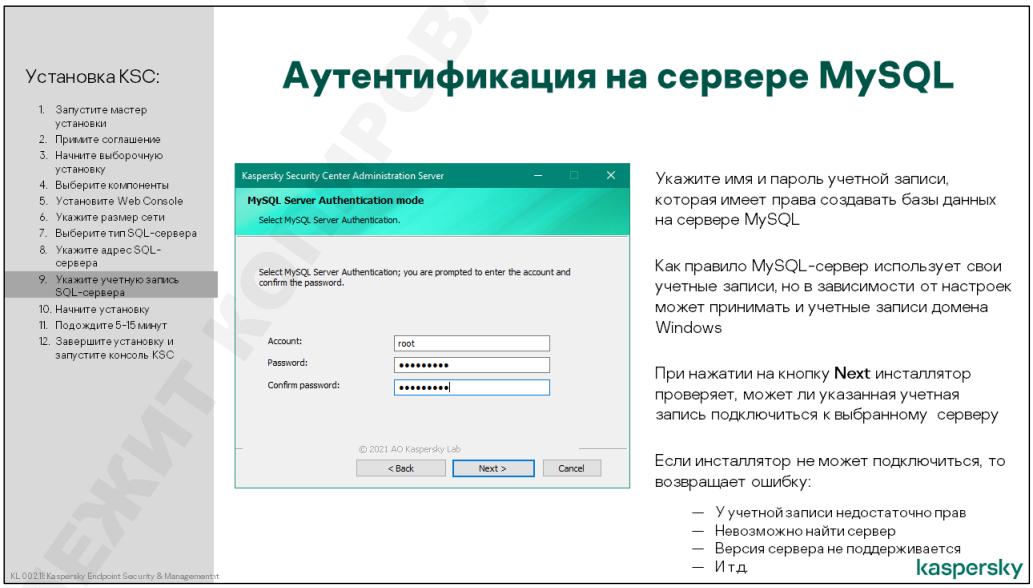
Как указать сервер MySQL



Если вы выбрали MySQL-сервер, укажите адрес сервера баз данных, порт MySQL-сервера (как правило, 3306) и имя базы данных.

В окне настройки параметров нет ссылки на страницу загрузки MySQL. Чтобы загрузить дистрибутив MySQL, используйте веб-сайт *www.mysql.org*

Как подключиться к серверу MySQL

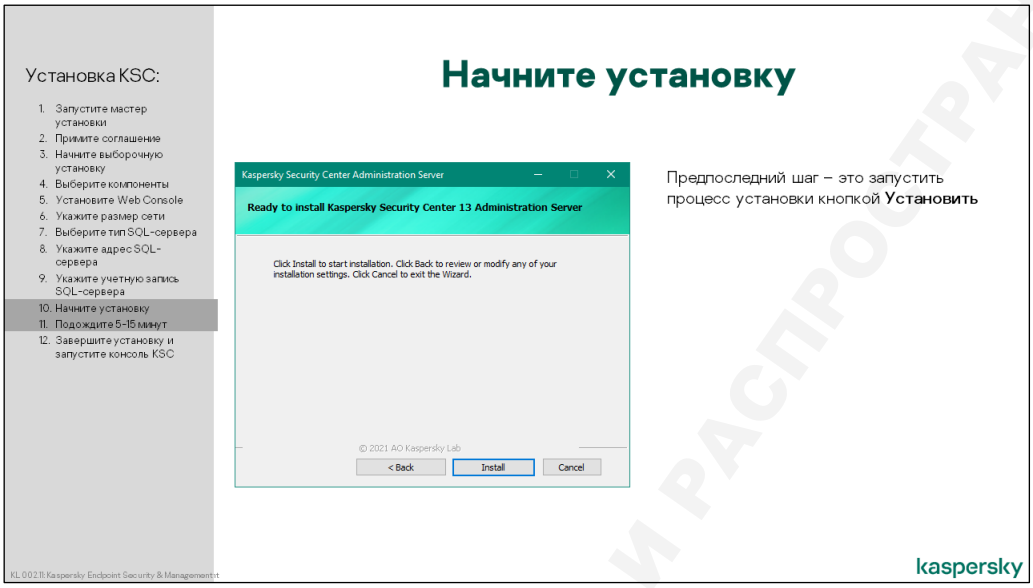


Также укажите имя и пароль для аутентификации на MySQL-сервере. Эти имя и пароль будут использовать и инсталлятор, чтобы создать базу, и Сервер администрирования, чтобы в нее писать.

В новых версиях MySQL-сервер, чтобы учетная запись могла подключиться к серверу, нужно со стороны SQL-сервера разрешить использовать ее с конкретного адреса или имени компьютера. Подробности ищите в документации MySQL.

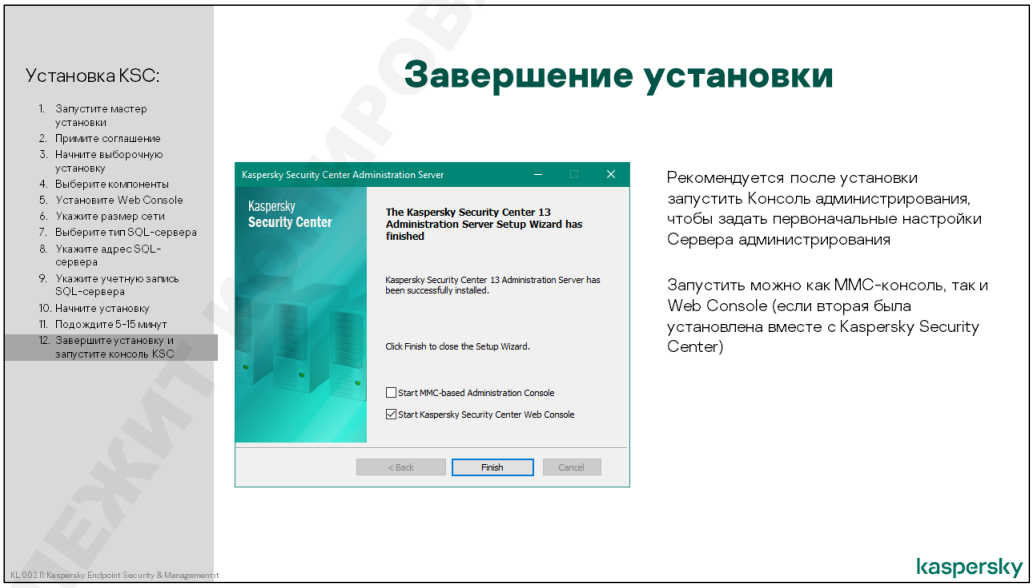
При нажатии кнопки **Next**, мастер пытается подключиться к указанному серверу от имени этой учетной записи. Если подключиться не удастся, то мастер выдаст ошибку с описанием причины.

Начните установку



В предпоследнем окне мастер предлагает начать установку. Установка может занять от 5 до 15 минут в зависимости от вычислительных мощностей аппаратных средств.

Завершение установки



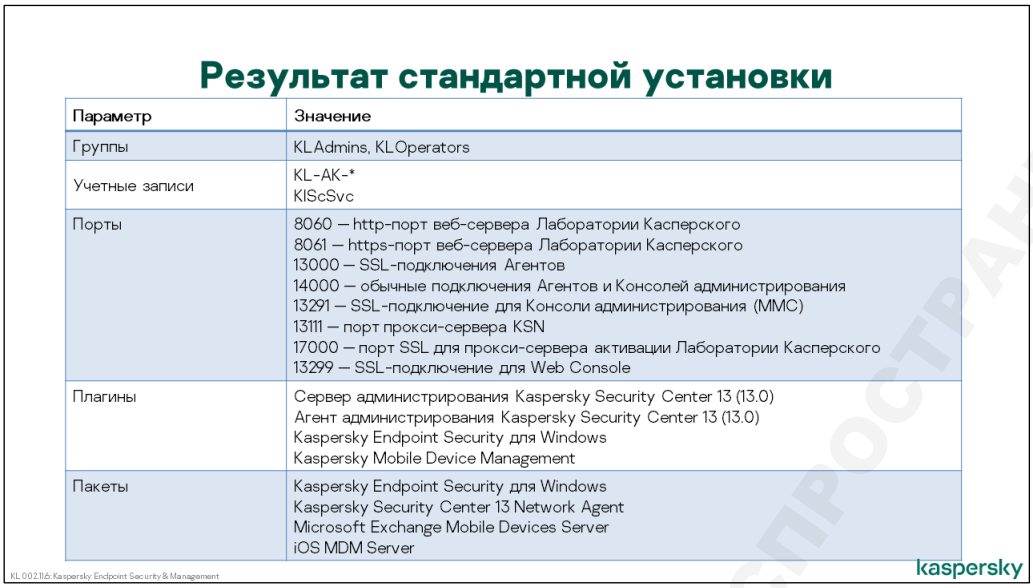
В последнем окне мастер предлагает сразу запустить локальную MMC-консоль администрирования или Web Console и продолжить установку в мастере первоначальной настройки Сервера администрирования. По умолчанию запустится Web Console, если она была установлена.

Как правило, Серверу администрирования нужно несколько минут, чтобы начать работать и принимать соединения.

Результаты установки

Если выбрать вариант установки **Выборочная**, но во всех окнах мастера принять настройки по умолчанию, результат будет точно такой же, как и при выборе варианта установки **Стандартная**, а именно:

Компоненты	Сервер администрирования Агент администрирования Консоль администрирования на базе MMC Web Console
Пути установки	*%ProgramFiles(x86)%***Kaspersky Lab\Kaspersky Security Center** — программные файлы *%ProgramFiles%***Kaspersky Lab\Kaspersky Security Center Web Console 13** — программные файлы *%ProgramData%***KasperskyLab\adminkit** — настройки *%ProgramData%***KasperskySC\SC_Backup** — папка для резервных копий
Службы	Сервер администрирования Kaspersky Security Center Агент администрирования Kaspersky Security Center Объект автоматизации Kaspersky Security Center Прокси-сервер Kaspersky Security Network Веб-сервер «Лаборатории Касперского» Прокси-сервер активации «Лаборатории Касперского» Kaspersky Security Center 13 Management Service Kaspersky Security Center 13 Web Console Kaspersky Security Center 13 Web Console Message Queue
Общая папка	KLSHARE — локальный путь *%ProgramData%***KasperskyLab\adminkit\1093\.working\Share**



Группы	**KLAdmins** **KLOperators** (зачем они нужны, рассказывает курс KL 302)
Учетные записи	**KL-AK-<*>** — запускает службу Сервер администрирования Kaspersky Security Center **KlScSvc** — запускает службы Прокси-сервер активации «Лаборатории Касперского», Прокси-сервер Kaspersky Security Network и Веб-сервер «Лаборатории Касперского». Записи **KL-AK-<*>** и **KlScSvc** имеют права, эквивалентные правам локального администратора, хотя и не входят во встроенную группу администраторов **KlPxeUser** — служебный пользователь для PXE-сервера (см. курс KL 009)
Порты для подключений	8060 — http-порт Веб-сервера «Лаборатории Касперского» 8061 — https-порт Веб-сервера «Лаборатории Касперского» 13000 — для SSL-подключений Агентов 14000 — для обычных подключений Агентов и Консолей администрирования 13291 — для SSL-подключений Консолей администрирования 13111 — порт службы Kaspersky Security Network proxy server 17000 — порт прокси-сервера активации 13299 — для SSL-подключений Kaspersky Security Center Web Console
SQL-сервер	Имя базы — **KAV**
Адрес для подключений	DNS-имя сервера
Плагины	Сервер администрирования Kaspersky Security Center 13 (13.0) Агент администрирования Kaspersky Security Center 13 (13.0) Kaspersky Endpoint Security 11.6 для Windows Kaspersky Mobile Device Management 11
Инсталляционные пакеты	Kaspersky Endpoint Security 11.6 for Windows Агент администрирования Kaspersky Security Center 13 (13.0) Microsoft Exchange Mobile Devices Server iOS MDM Server

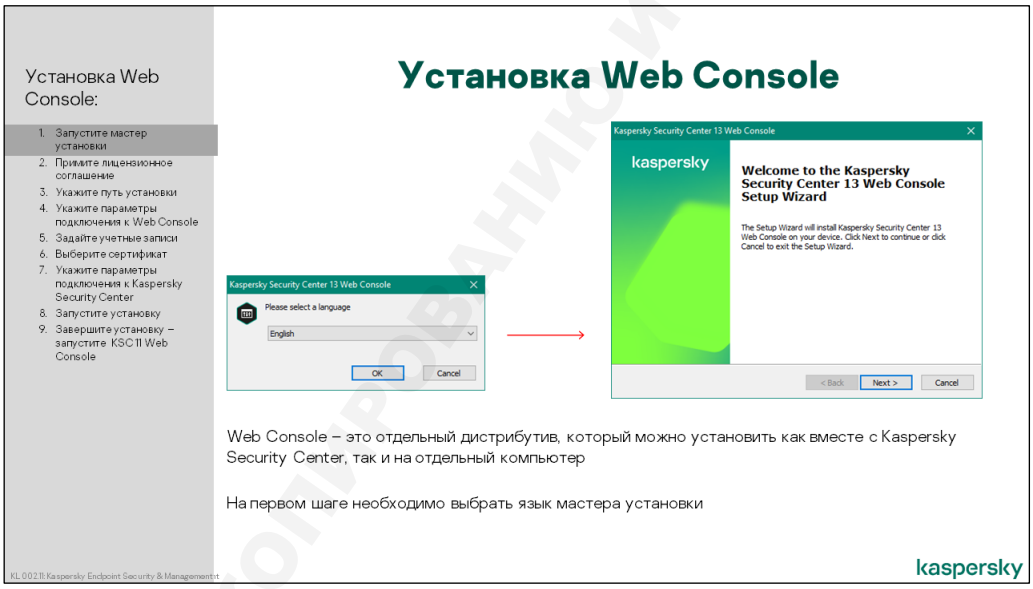
Большинство этих настроек можно изменить или в рамках выборочной установки, или в настройках продукта после того, как установка выполнена, или и там, и там. Но небольшое количество настроек поменять после установки либо нельзя вовсе, либо очень тяжело. Эти исключения нужно знать и продумать их значения до установки:

- Путь к файлам данных нельзя изменить в принципе — он установлен в соответствии с требованиями Microsoft.
- Путь к программным файлам и адрес SQL-сервера без переустановки изменить нельзя.
- Тип SQL-сервера (Microsoft или MySQL) изменить нельзя. Во всяком случае, штатными способами.

3.3 Установка Kaspersky Security Center Web Console

Мастер установки

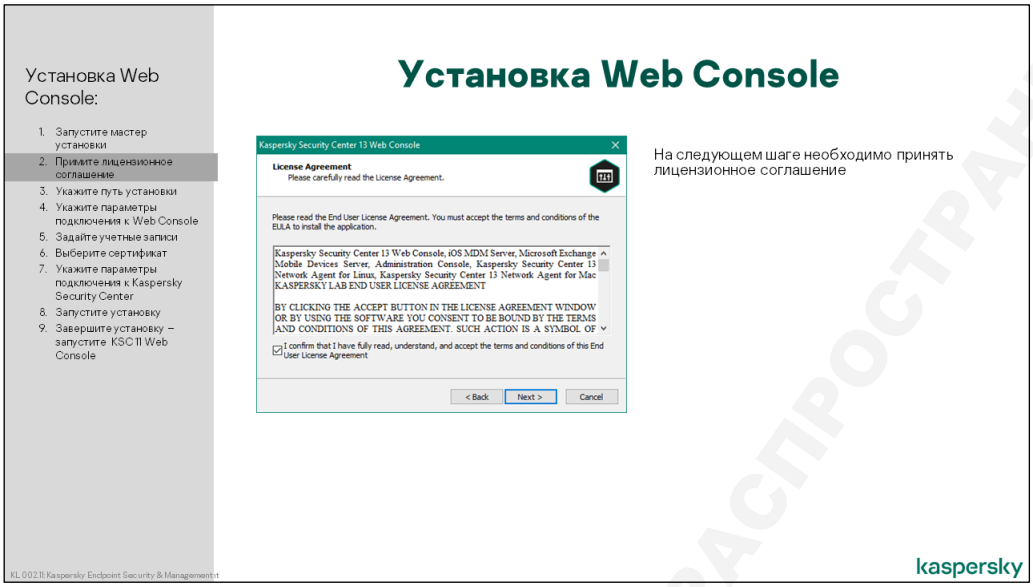
Выбор языка установки и приветствие



Web Console не обязательно устанавливать вместе с Kaspersky Security Center, она вполне может существовать на отдельном компьютере, для этого нужно установить Web Console как обычную программу. Дистрибутив Web Console находится в распакованной папке Сервера администрирования — **Server\Packages\Web Console**.

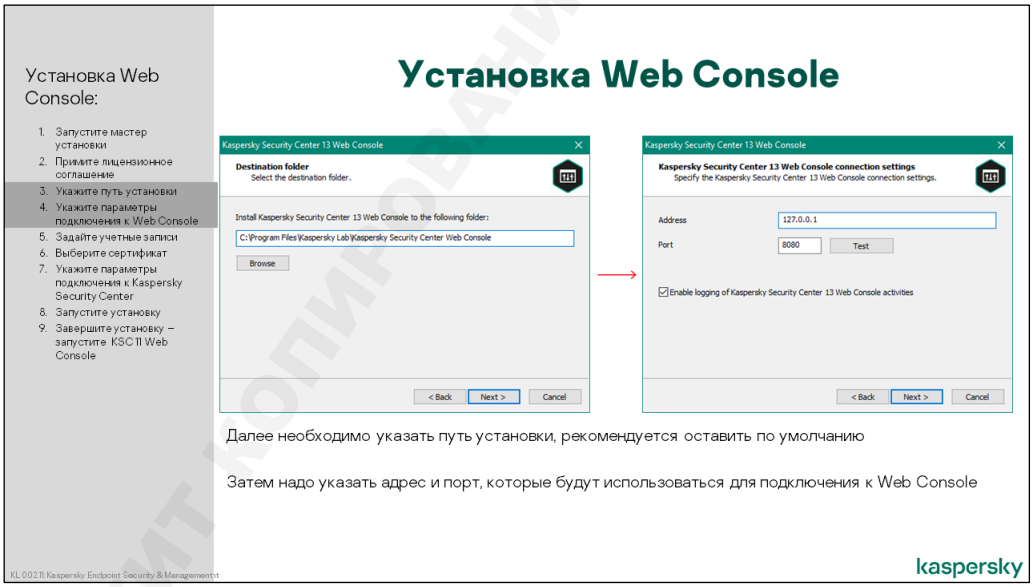
Запустите программу установки и на первом шаге можно выбрать язык, на котором продолжится мастер установки.

Лицензионное соглашение и список локализаций Web Console



Теперь нужно принять лицензионное соглашение.

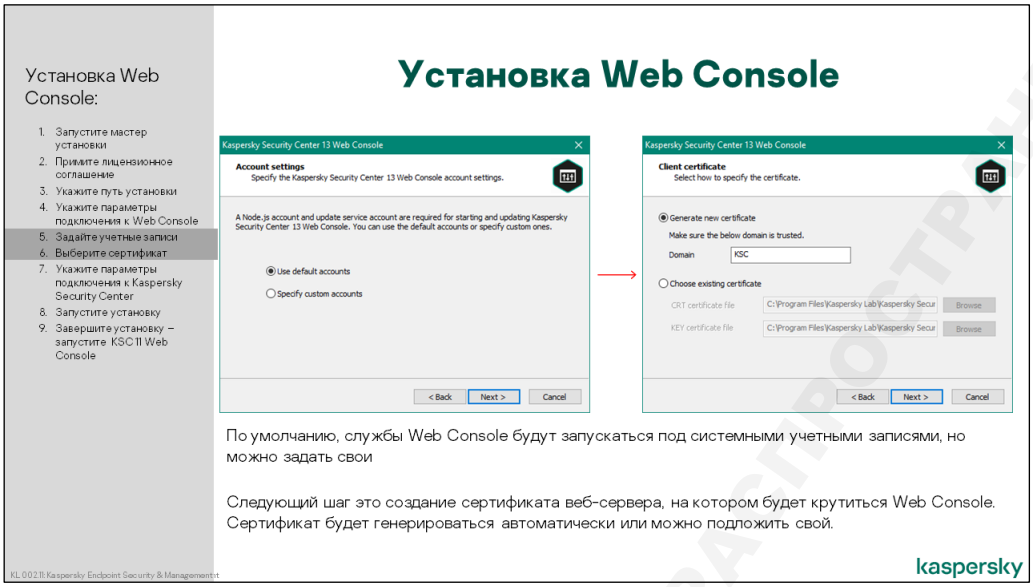
Путь установки и адрес подключения



Путь установки рекомендуется оставить по умолчанию.

Порт для подключения к Web Console можно изменить. Сейчас по умолчанию используется порт 8080.

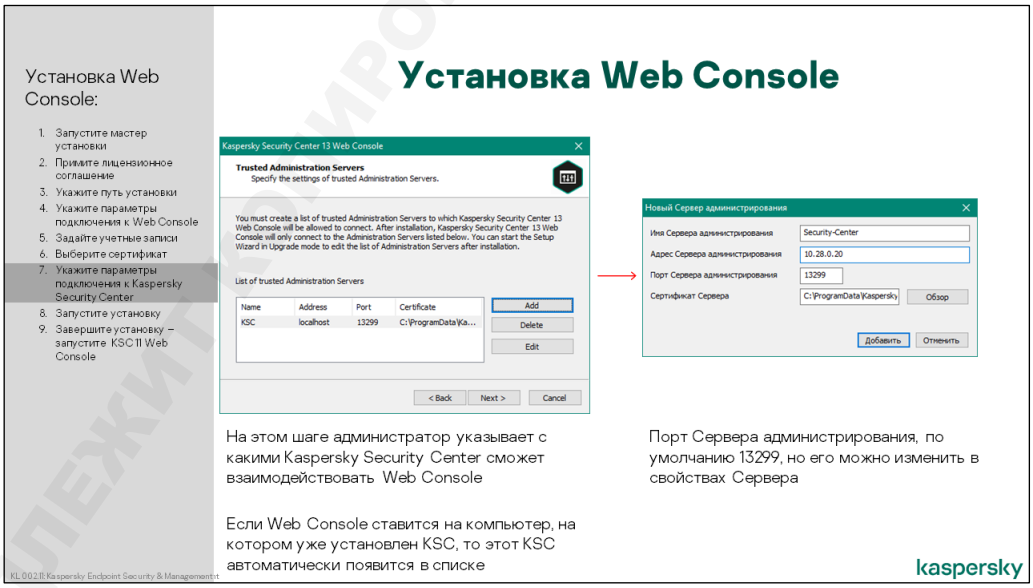
Учетные записи и выбор сертификата



Web Console устанавливает в систему несколько служб, на этом шаге предлагается выбрать учетные записи, из-под которых будут запускаться службы. Мы рекомендуем оставить значение по умолчанию, в таком случае службы Web Console будут запускаться под Local System и Network Service.

Теперь нужно разобраться с сертификатом. Мастер установки может сгенерировать самоподписанный сертификат автоматически или можно использовать уже существующий.

Подключение к Kaspersky Security Center

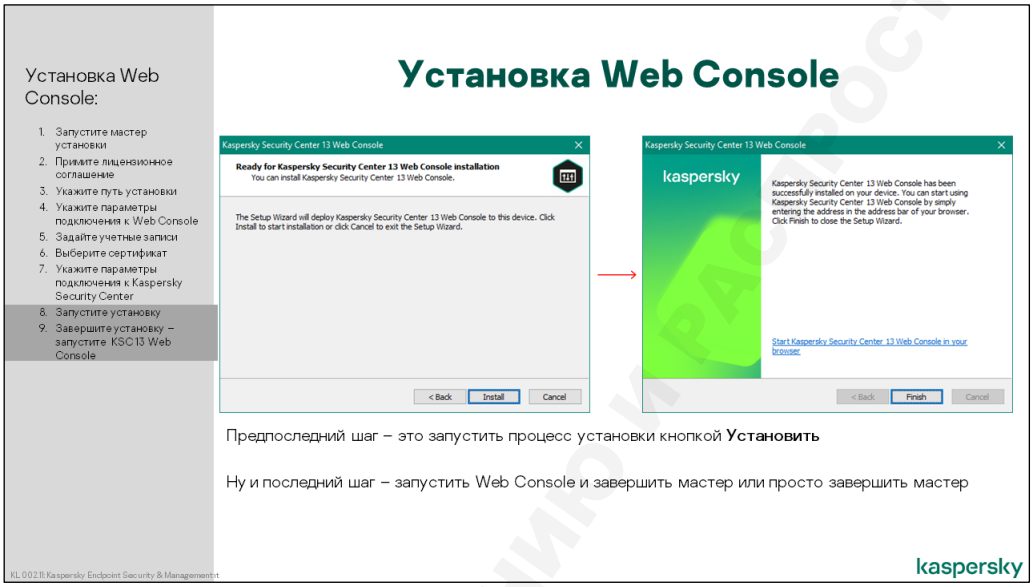


Самый важный шаг — это добавление доверенных Серверов администрирования. Тут администратор указывает с каким Kaspersky Security Center сможет взаимодействовать Web Console.

Если Web Console устанавливается на компьютер, на котором уже установлен Kaspersky Security Center, то этот Сервер администрирования автоматически появится в списке доверенных. Если нет, то нужно ручками добавить сервер — указать адрес, порт и обязательно путь к сертификату Сервера администрирования. Это сертификат потом скопируется в папку установки Web Console.

Web Console по умолчанию использует порт 13299 для подключения к Kaspersky Security Center, но его при необходимости можно изменить в свойствах Сервера администрирования.

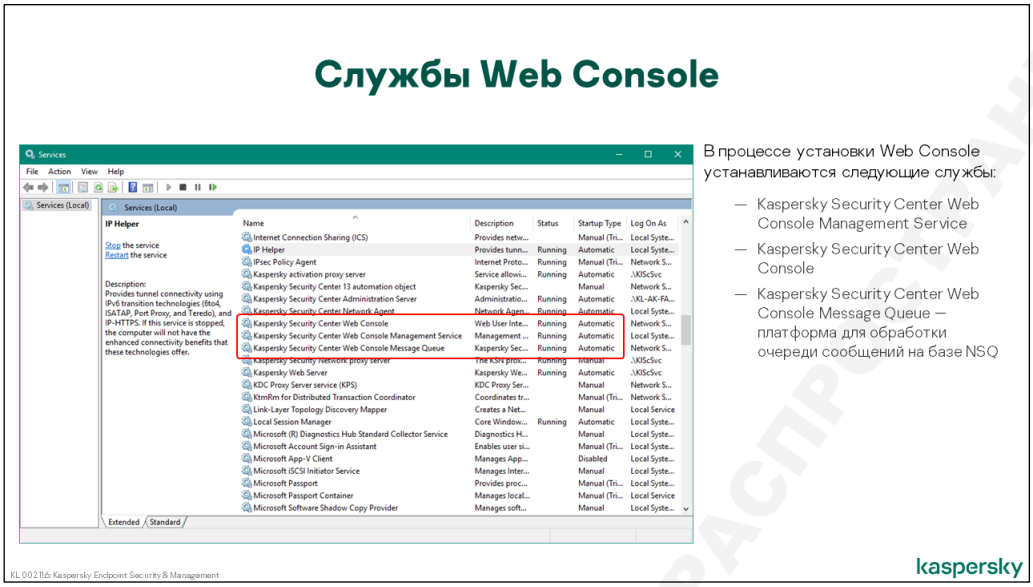
Установка и завершение мастера



Запускаем установку кнопкой **Установить** и ждем 5-7 минут пока установится Web Console.

Теперь можно либо завершить мастер, либо запустить Web Console по ссылке. Чтобы подключиться с рабочего места администратора или любой другой удаленной машины нужно ввести в браузере —*https://<IP-адрес>:8080* или другой порт, если он менялся во время установки.

Службы Web Console



Архитектура Web Console состоит из множества компонентов и процессов, которые скрыты от пользователя и не имеет смысла их подробно разбирать. Можно сказать, что основным компонентом является Сервер Веб-Консоли на базе Node.js, запускается в отдельном процессе **node.exe**. Также есть другие компоненты, которые запускаются в отдельных процессах **node.exe**, например, для каждого плагина выделяется отдельный процесс.

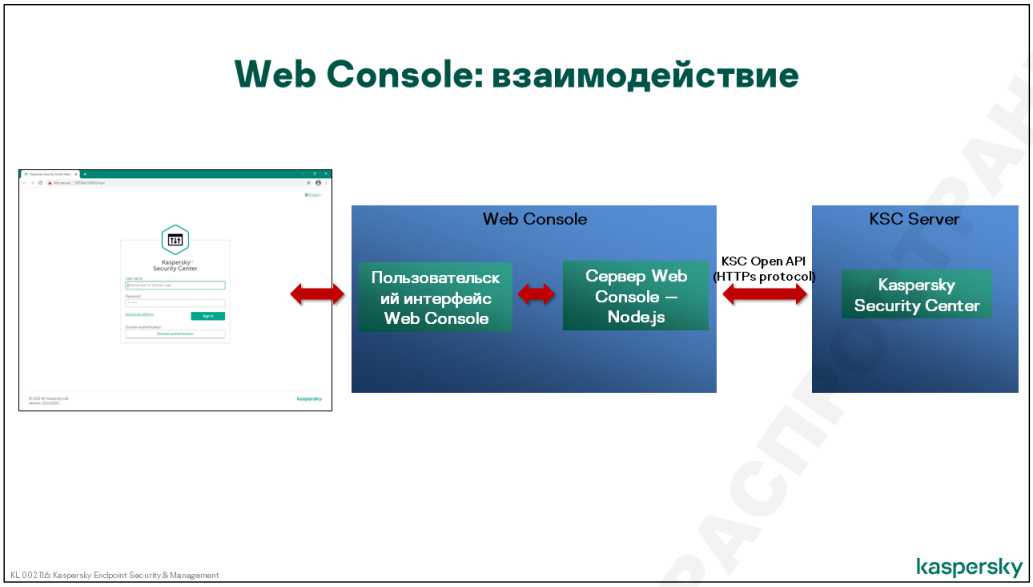
Отдельные процессы используются для подсистемы обработки очереди сообщений (**nsqd.exe**) и логирования (**nsq_to_file.exe**).

Для мониторинга и управления процессами используется стандартный для среды Node.js менеджер процессов. Из-за ограничений операционной системы, менеджер процессов запускает процессы под той учетной записью, под которой запущен он сам. По этой причине запускается два менеджера процессов, один под системной (Local System), другой под сетевой (Network Service) учетной записью. Для большинства процессов достаточно ограниченных прав, но бывают сценарии, для которых нужны расширенные права.

Теперь посмотрим какие службы устанавливает в систему Web Console:

- Kaspersky Security Center 13 Web Console Management Service — **SrvLauncher.exe** — служба используется исключительно для обеспечения автозапуска менеджера процессов под учетной записью Local System
- Kaspersky Security Center 13 Web Console — **SrvLauncher.exe** — служба используется исключительно для обеспечения автозапуска менеджера процессов под учетной записью Network Service
- Kaspersky Security Center 13 Web Console Message Queue — **nsqd.exe** — платформа для обработки очереди сообщений на базе NSQ

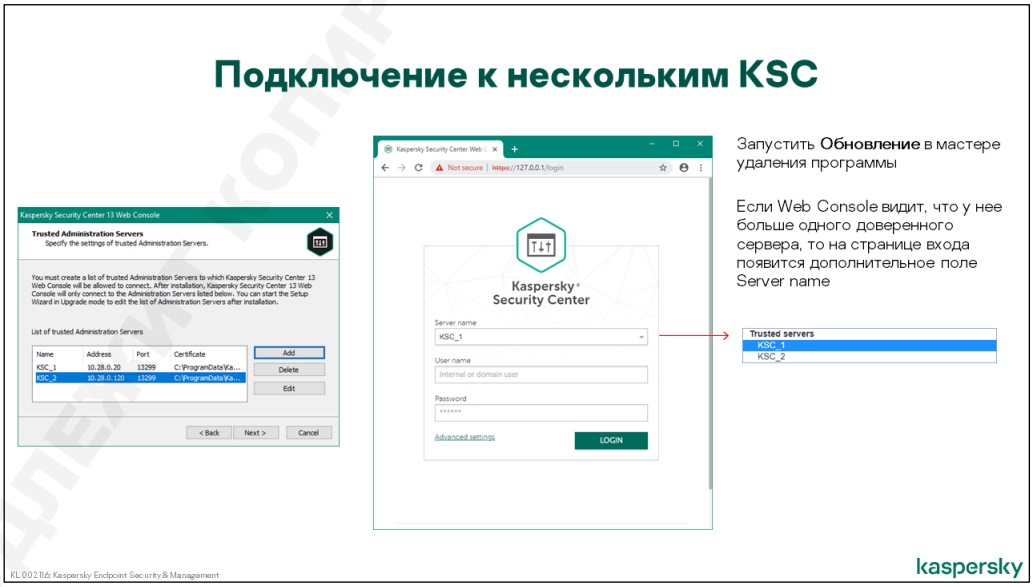
Взаимодействие с Kaspersky Security Center



Web Console представляет собой веб-сервер на платформе Node.js. Серверная часть Web Console подключается к Kaspersky Security Center по новому протоколу KSC Open API на базе HTTPs.

Клиентская часть представляет собой SPA (Single Page Application). В простейшем варианте SPA это веб-приложение, компоненты которого загружаются один раз на странице, а контент подгружается по необходимости. Т.е. когда мы кликаем в Web Console на какой-либо элемент интерфейса, запускается JavaScript, который подгружает модули и визуализирует то, что мы запросили. Для пользователя все будет выглядеть так, как будто мы перешли на другую страницу.

Подключение к нескольким Серверам администрирования



А если в компании несколько Серверов администрирования и мы хотим ко всем подключаться через браузер, как быть?

Самый простой вариант — для каждого Kaspersky Security Center установить свою Web Console и работать с разными Серверами администрирования в разных вкладках браузера.

Однако можно использовать одну Web Console как точку входа и управлять несколькими Серверами администрирования. В этом сценарии нужно добавить в Web Console несколько доверенных Серверов администрирования.

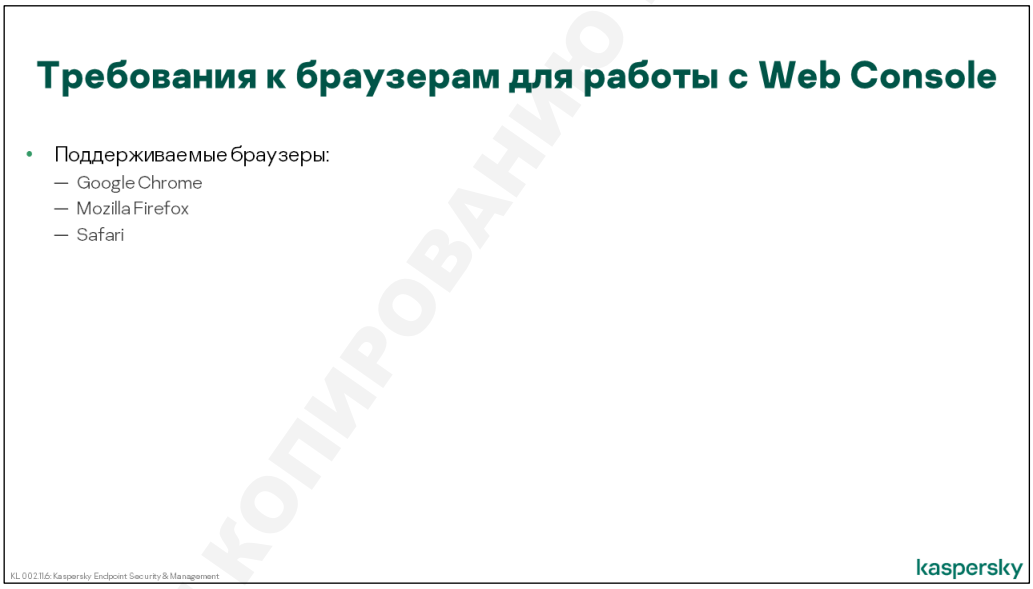
Это можно сделать двумя способами:

- Либо запустить **Изменить | Обновление** в оснастке **Программы и компоненты** (рекомендуемый вариант)
- Либо вручную поправить конфигурационный файл – config.json в папке установки Web Console (нерекомендуемый вариант)

В этом случае, если у Web Console есть несколько доверенных Серверов администрирования, то в окне ввода логина-пароля появится дополнительное поле — Server name (окно авторизации пока только на английском языке).

И администратору нужно будет выбрать Сервер администрирования, к которому он хочет подключиться.

Требования к браузерам



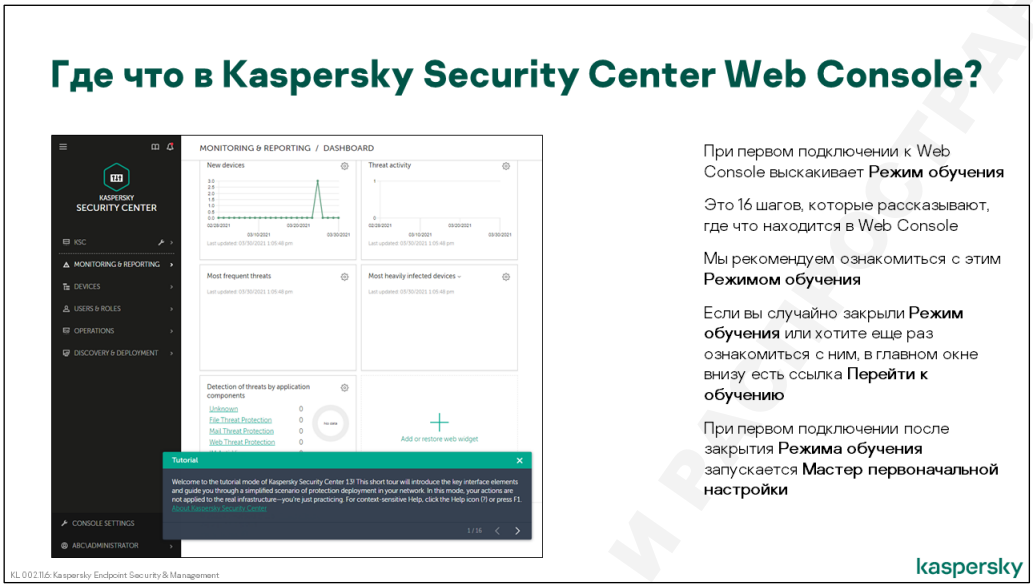
Для работы с Web Console необходимо использовать следующие браузеры:

- Google Chrome версии 88 и выше
- Mozilla Firefox версии 78 и выше
- Safari версии 14

Обратите внимание, что Internet Explorer не поддерживается.

3.4 Мастер первоначальной настройки

Режим обучения

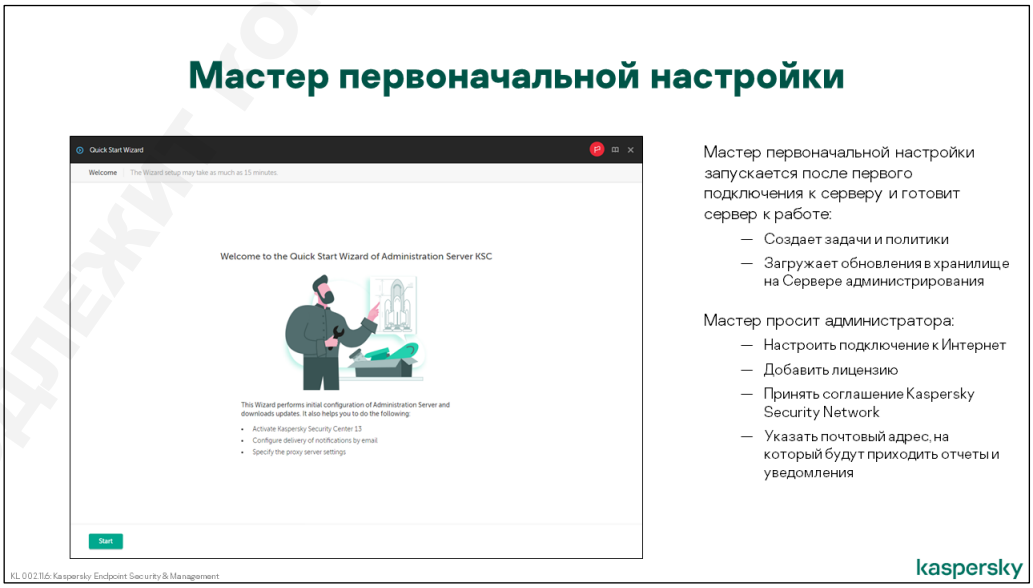


При первом подключении Web Console к Серверу выскакивает Режим обучения. Это небольшая демонстрация, которая рассказывает, где что находится в Web Console.

Если вы до этого использовали MMC-консоль, то поначалу будет очень непривычно работать с Web Console и мы настоятельно рекомендуем пройти обучение, чтобы получить начальную информацию.

Если вы случайно закрыли Режим обучения или хотите еще раз ознакомиться с ним, в главном окне внизу есть ссылка **Пройти обучение**.

При первом подключении после того, как вы пройдете или закроете Режим обучения, запустится Мастер первоначальной настройки.



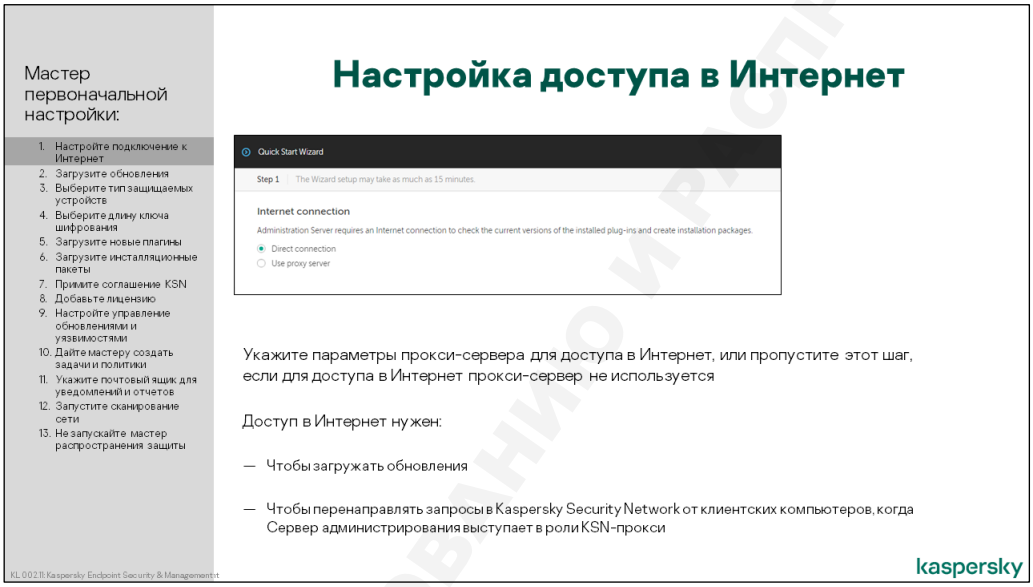
Мастер первоначальной настройки готовит Сервер к работе:

- Загружает необходимые плагины
- Создает политики и задачи
- Загружает обновления в хранилище Сервера администрирования

В процессе работы мастер просит администратора:

- Настроить прокси-сервер для выхода в Интернет
- Добавить лицензию
- Включить Kaspersky Security Network
- Настроить почтовые уведомления и доставку отчетов

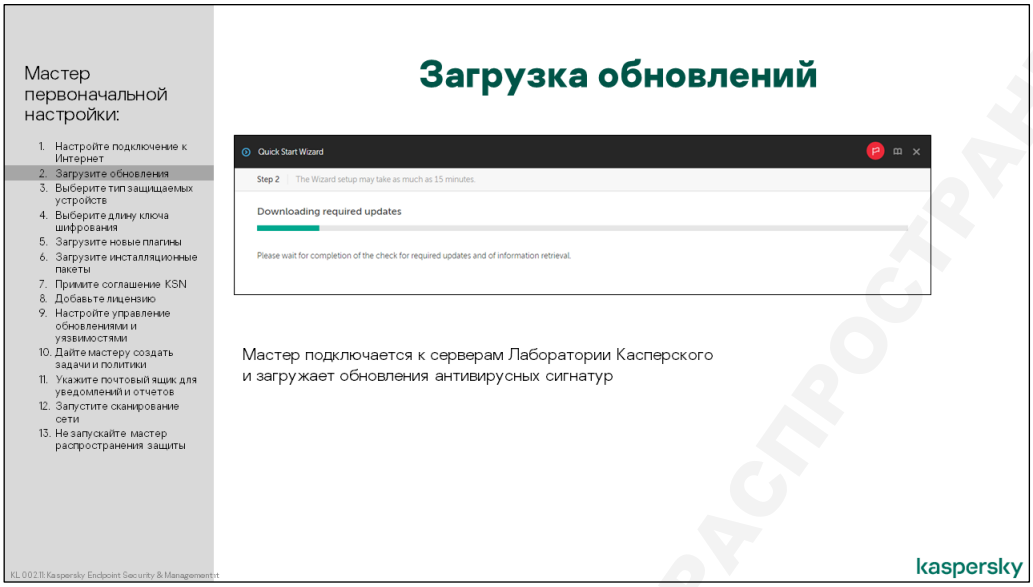
Настройка доступа в Интернет



Следующий шаг просит настроить параметры прокси-сервера для доступа в Интернет. Серверу администрирования нужен выход в Интернет для загрузки обновлений и для связи с KSN-серверами Лаборатории Касперского. Обе функции будут использовать общие параметры прокси.

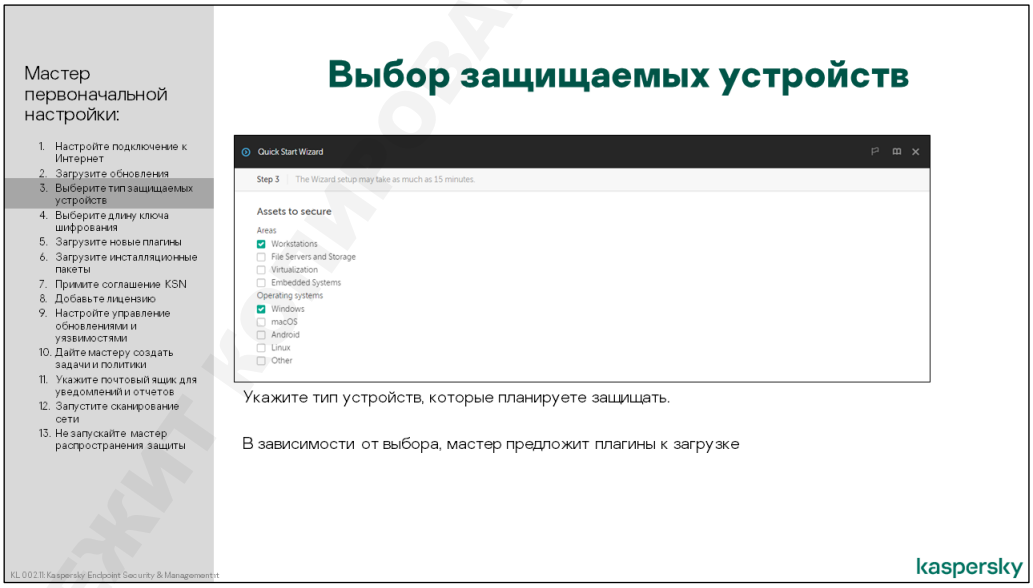
Сами параметры вполне стандартны: адрес и порт сервера, опциональные имя и пароль пользователя для аутентификации, возможность отключить использование прокси для локальных адресов.

Загрузка обновлений



Мастер подключается к серверам Лаборатории Касперского и загружает актуальную версию антивирусных сигнатур. Дожидаться пока завершиться обновление не обязательно, загрузка баз продолжится в фоновом режиме.

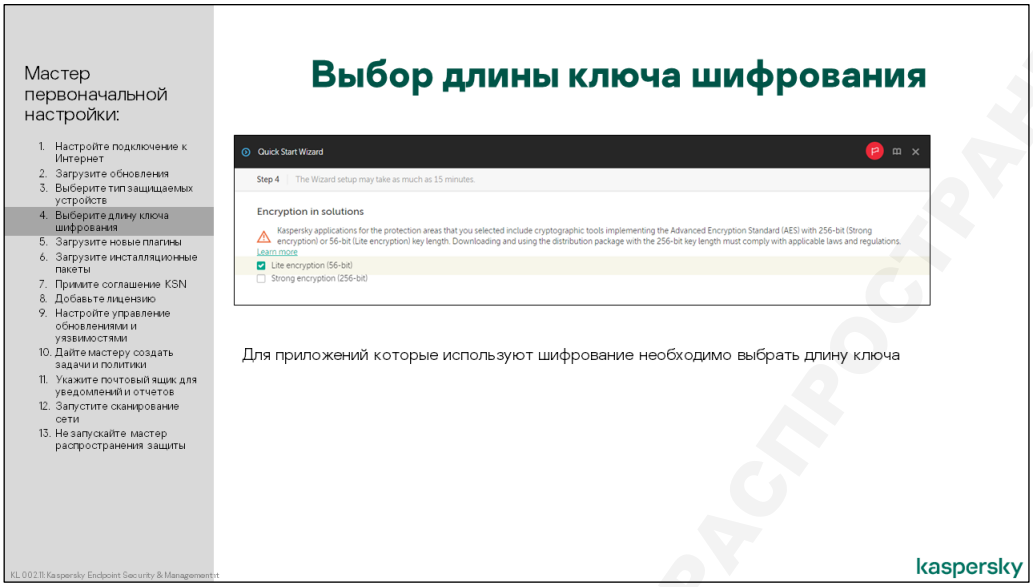
Выбор защищаемых устройств



Следующий и самый важный шаг – выбор типа защищаемых устройств и защищаемых операционных систем. В зависимости от выбранных типов устройств Kaspersky Security Center предложит администратору, какие плагины управления для Web Console и инсталляционные пакеты доступны для загрузки. По умолчанию Kaspersky Security Center предлагает защищать рабочие станции под управлением Windows.

Если по какой-то причине Администратор решил защищать другие устройства, то нужно заново запустить Мастер первоначальной настройки и выбрать необходимые активы.

Выбор длины ключа шифрования



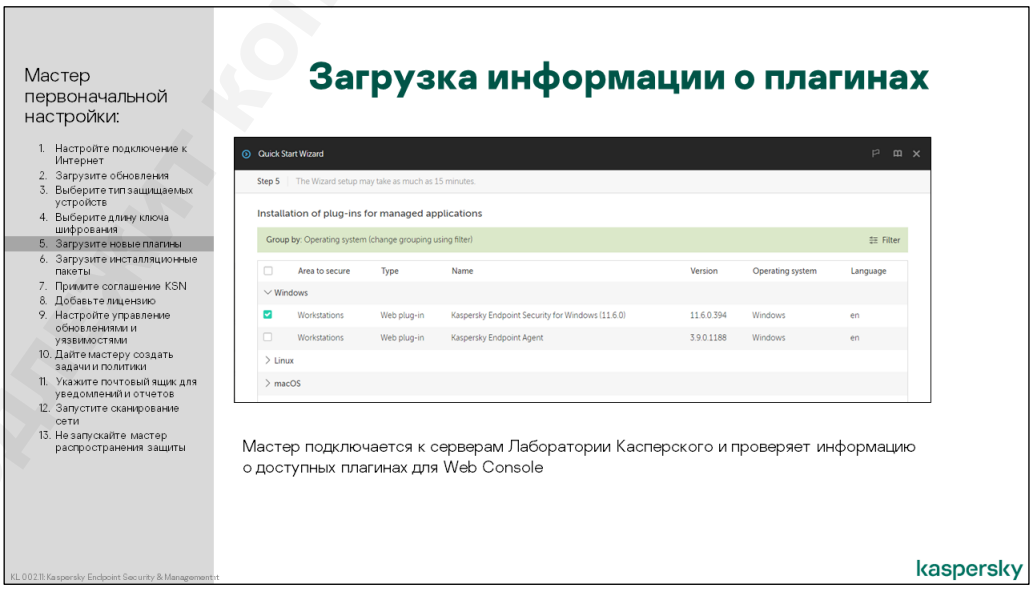
Следующий шаг – выбор длины ключа шифрования. Kaspersky Endpoint Security использует алгоритм шифрования Advanced Encryption Standard (AES) и позволяет шифровать файлы и папки, хранящиеся на локальных дисках компьютера и съемных дисках, съемные и жесткие диски целиком.

В окне Тип шифрования необходимо выбрать один из следующих типов шифрования:

- Упрощенное шифрование. Для этого типа шифрования используется 56-разрядный ключ.
- Стойкое шифрование. Для этого типа шифрования используется 256-разрядный ключ.

При выборе длины ключа шифрования ознакомьтесь с местными законами и требованиями регуляторов. В ряде стран использовать стойкое шифрование (256-бит) запрещено законом

Загрузка информации о плагинах



Следующий шаг – выбор плагинов для управляемый программ.

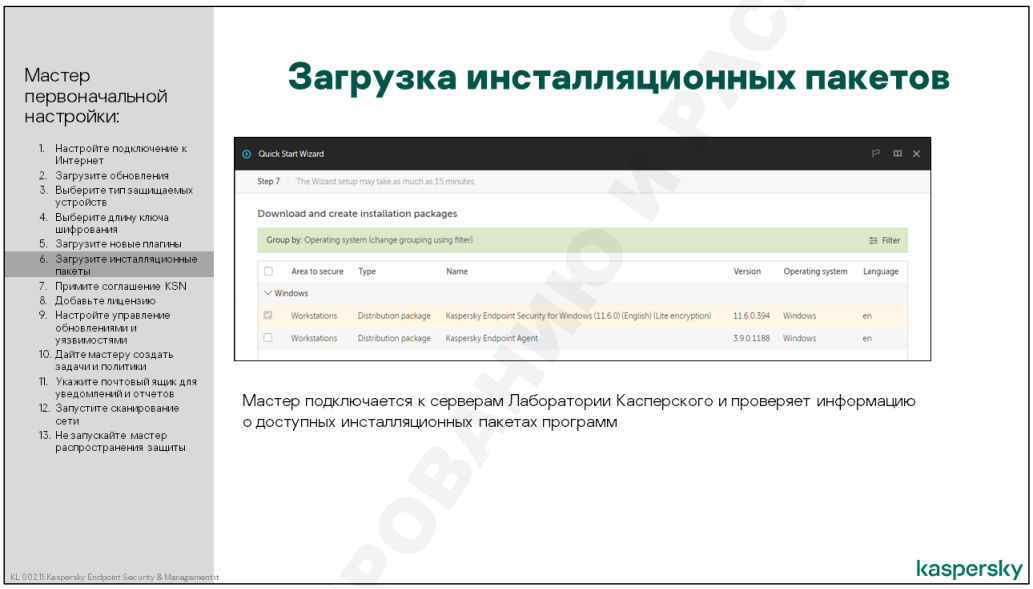
По умолчанию Web Console устанавливается с двумя плагинами:

— для Сервера администрирования
— для Агента администрирования

Мастер первоначальной настройки проверяет, актуальный список плагинов, расположенных на серверах "Лаборатории Касперского". Список отфильтрован в соответствии с, выбранными устройствами и операционными системами, указанными на предыдущих шагах мастера.

После выбора плагинов, их установка начинается автоматически в фоновом режиме. Для установки некоторых плагинов администратор должен принять условия Лицензионного соглашения и Политики конфиденциальности.

Загрузка инсталляционных пакетов



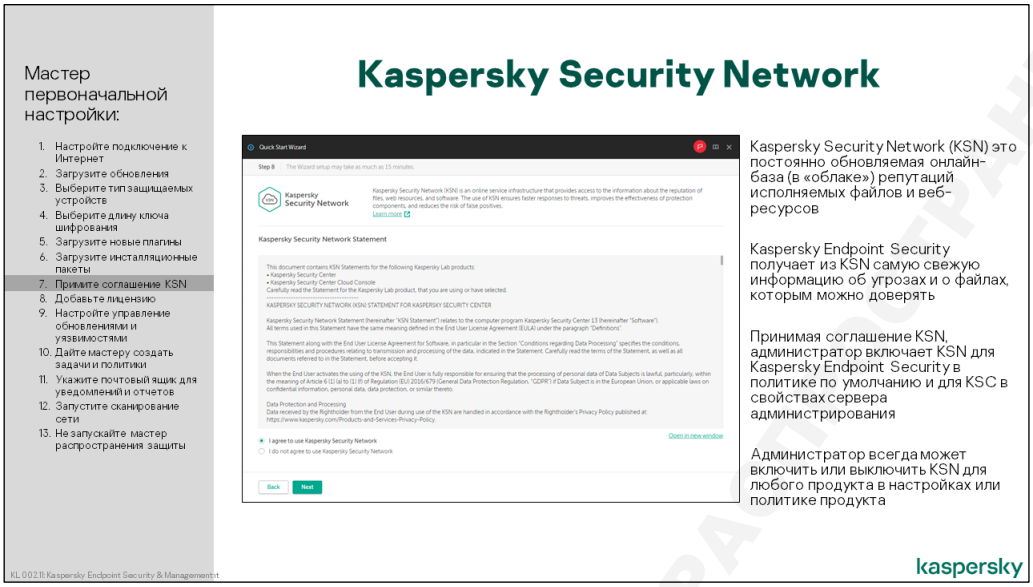
Следующий шаг – загрузка инсталляционных пакетов управляемых программ Лаборатории Касперского.

Мастер первоначальной настройки подключается к серверам Лаборатории Касперского и проверяет информацию о доступных версиях дистрибутивов, соответствующих ранее выбранным типам защищаемых устройств и операционных систем. Обычно в списке программ присутствуют только те приложения, которые официально поддерживаются. Устаревшие или неподдерживаемые программ Мастер первоначальной настройки не скачивает. После того, как администратор выбрал дистрибутивы (к примеру, Kaspersky Endpoint Security для Windows 11), начинается загрузка,

Чтобы завершить загрузку некоторых дистрибутивов администратор должен принять Лицензионное соглашение и Политику конфиденциальности.

После завершения работы Мастера первоначальной настройки инсталляционные пакеты Агента администрирования и управляемых программ Лаборатории Касперского можно обнаружить в хранилище Сервера администрирования **Обнаружение устройств и развертывание | Развертывание и назначение | Инсталляционные пакеты**.

Kaspersky Security Network



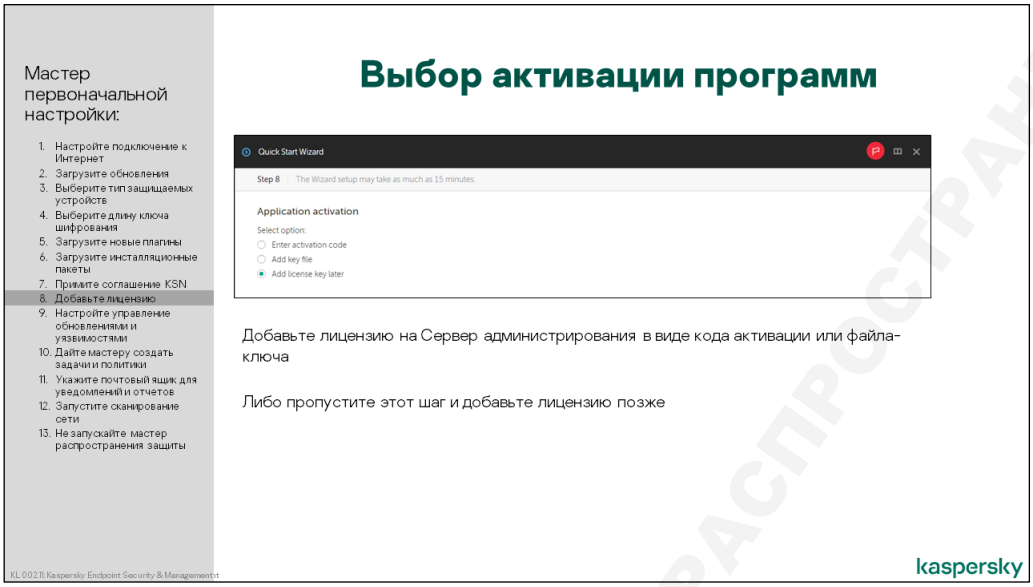
Мастер предлагает администратору принять соглашение Kaspersky Security Network (далее, KSN). KSN — это название облачных (in-the-cloud) защитных технологий Лаборатории Касперского.

Участие в KSN позволяет использовать для защиты компьютеров оперативную информацию о новых угрозах, не дожидаясь появления этой информации в традиционных антивирусных базах. Взамен на это согласие, Лаборатория Касперского будет получать обезличенную информацию о файлах и URL-адресах, обработанных на компьютерах клиента. Подробнее о службе KSN рассказывается во Вступлении и в Части 2 Управление защитой.

Согласие на участие в KSN активирует в политике опции использования KSN и KSN-прокси. Если отказаться от участия в KSN, использование KSN в политике Kaspersky Endpoint Security 11.6 будет отключено, но использование KSN-прокси останется включенным.

Использование KSN-прокси в политике связано с функцией KSN-прокси Сервера администрирования. Функция KSN-прокси в Сервере администрирования реализована в виде дополнительной службы — Прокси-сервер Kaspersky Security Network. По умолчанию в свойствах Сервера администрирования использование KSN-прокси включено.

Установка лицензии



Следующий шаг — активация продукта. Большинство продуктов Лаборатории Касперского требует активации, а некоторые, в частности, Kaspersky Security Center и Kaspersky Endpoint Security, могут быть активированы до разного уровня функциональности. То есть, в зависимости от лицензии, некоторые возможности могут быть недоступны.

Ключи и коды активации

Чтобы активировать продукт, нужен ключ или код. Оба могут олицетворять лицензию покупателя со всеми ее ограничениями.

Ключ — это специальный файл с параметрами лицензии, подлинность которого продукт может установить локально. Код — это просто строка и для выяснения ее подлинности и параметров соответствующей лицензии продукт должен подключиться к Серверам активации Лаборатории Касперского в Интернет.

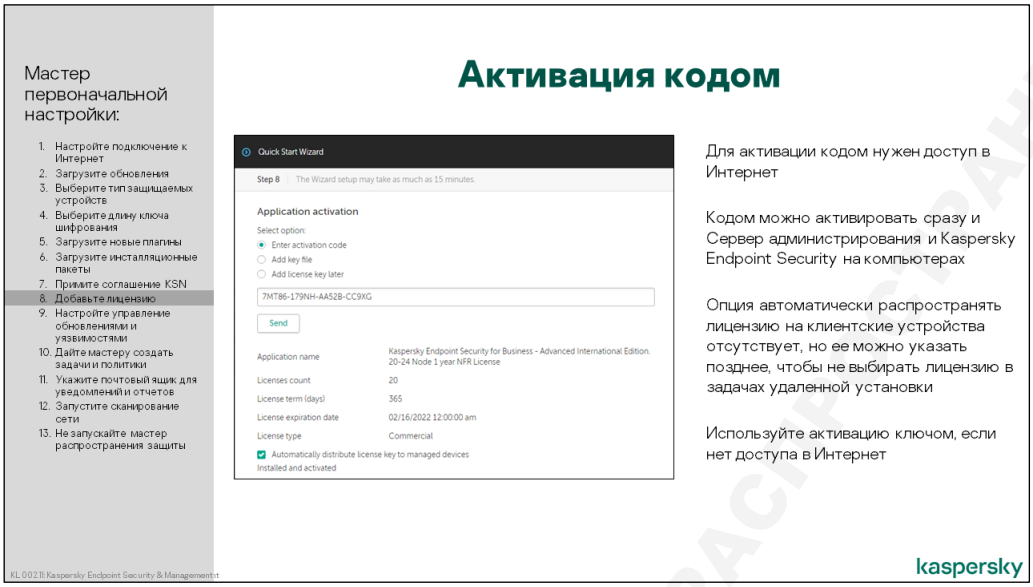
Старые версии продуктов Лаборатории Касперского можно активировать только ключом. Все актуальные версии можно активировать и ключом, и кодом.

Коды удобнее, потому что один код активирует все продукты по лицензии. Чтобы активировать эти же продукты ключом, часто в лицензию входит несколько разных ключевых файлов. Ключом для Kaspersky Security Center нельзя активировать Kaspersky Endpoint Security, и наоборот. А код у них один.

Ключи нужны, когда нужно активировать продукт на компьютере без доступа в Интернет. Если у вас есть только код, но нет ключа, добавьте код в хранилище ключей на Сервере администрирования (вкладка **Операции | Лицензирование | Лицензии Лаборатории Касперского** в Web Console). Сервер автоматически загрузит соответствующие ключи, которые вы сможете экспортировать в файлы.

Если у компьютеров нет доступа в Интернет, но они подключены к Серверу администрирования, у которого доступ есть, продукты на компьютерах можно будет активировать кодом. Продукты верифицируют код через службу Сервера администрирования: Прокси-сервера активации «Лаборатории Касперского».

Активация кодом



В мастере первоначальной настройки можно указать либо ключ, либо код. Если у покупателя есть только код, все просто, нужно выбрать подходящий способ активации, ввести код и дождаться его верификации. На этом этапе Серверу администрирования требуется доступ в Интернет.

Подробнее о том, как активировать Kaspersky Endpoint Security на клиентских компьютерах, рассказывает глава 3 в этой части.

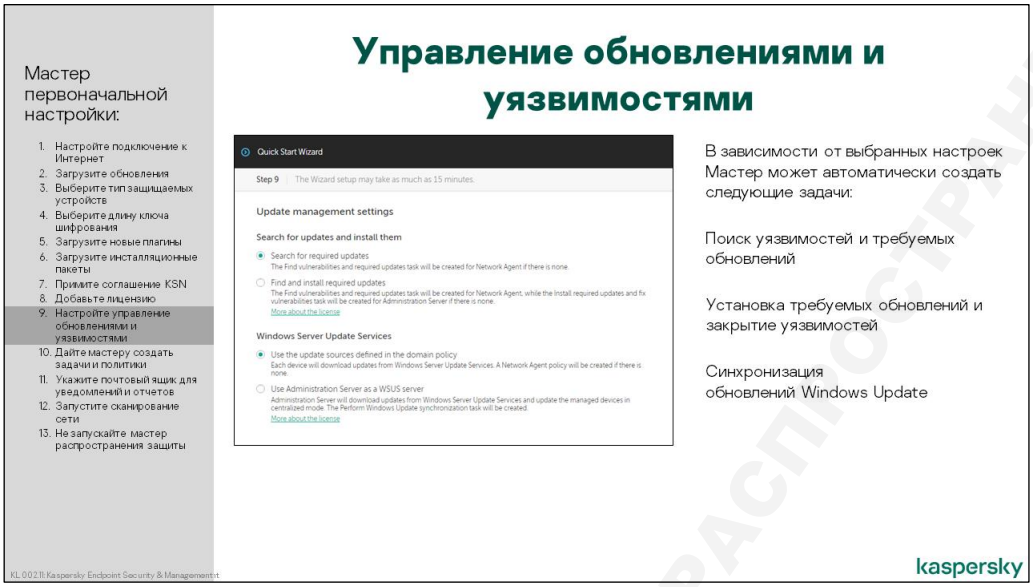
Активация ключом

Если у покупателя вместо кода есть ключ, то, как правило, он есть не один и нужно решить, какой ключ указать в мастере.

Чаще всего рекомендуется указывать ключ для активации Kaspersky Endpoint Security. Узнать, какой из ключей подходит для этой цели можно из файла *CompatibilityList.txt*, который обычно поставляется вместе с ключом или кодом. Остальные ключи можно добавить позже на вкладке **Операции | Лицензирование | Лицензии Лаборатории Касперского** в Web Console или в свойствах Сервера администрирования.

Ключ можно назначить для автоматической установки на клиентские компьютеры. Для этого отметьте флаг **Автоматически распространять ключ на управляемые устройства**. Если Сервер администрирования обнаружит управляемый компьютер, на котором Kaspersky Endpoint Security не активирован, он автоматически пошлет туда ключ, выбранный для автоматической установки.

Управление обновлениями и уязвимостями



Следующий шаг – настройка параметров управления обновления и уязвимостями.

Этот функционал не имеет отношения к антивирусной защите и к Kaspersky Endpoint Security, а касается управления компьютерами силами Агента администрирования. Для использования функционала Systems Management достаточно установленного на клиентских компьютерах Агента администрирования. Более подробней о возможностях управления уязвимостями и обновления рассказывается в курсе KL 009.

В мастере первоначальной настройки Kaspersky Security Center можно выбрать, в каких режимах Systems Management будет работать сервер администрирования:

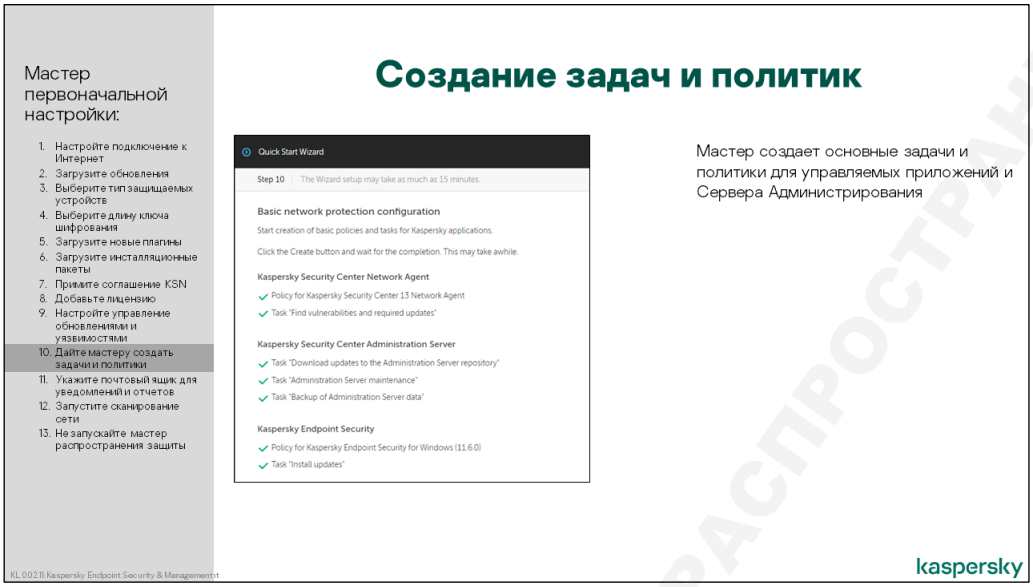
— Поиск уязвимостей и доступных обновлений — используя базу уязвимостей Лаборатории Касперского, Агент администрирования в рамках одноименной задачи ищет уязвимости и доступные обновления на клиентских компьютерах

— Исправление уязвимостей и установка обновлений — Kaspersky Security Center позволяет автоматически исправлять уязвимости и устанавливать обновления программ с помощью специальной задачи. Задача работает на основе правил, в которых необходимо задать условия, что и где исправлять

— Использовать настройки обновлений, определяемые доменной политикой — Kaspersky Kaspersky Security Center никак не влияет на работу Windows Update Agent (WUA).

— Синхронизация обновлений Windows Update — Kaspersky Security Center может выступать в роли локального WSUS-сервера, т.е. клиентские компьютеры будут скачивать обновления Windows не из Интернет, а с Сервера администрирования

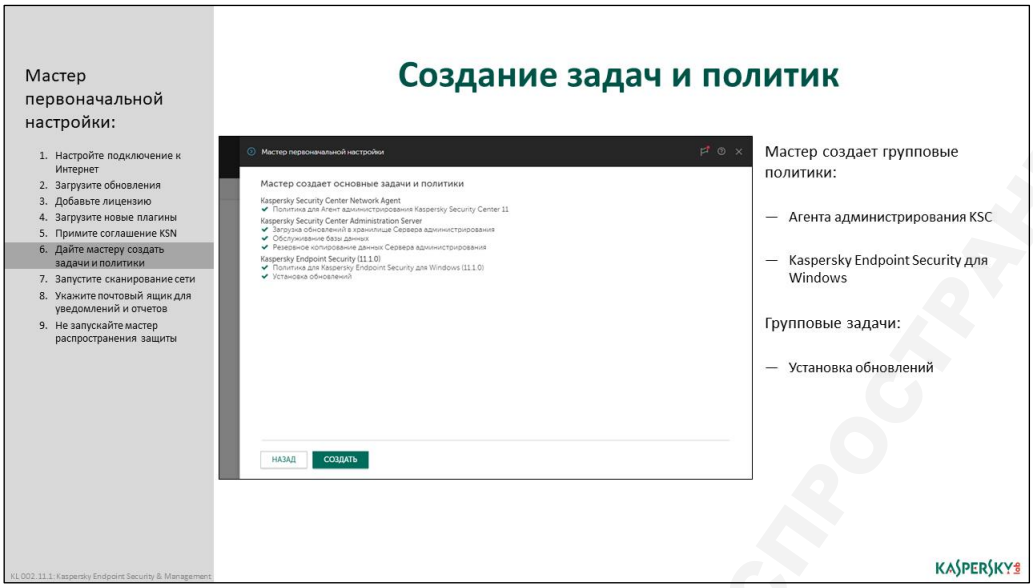
Создание задач и политик



На этом этапе мастер первоначальной настройки создает политики и задачи, необходимые для защиты узлов. Следующие политики и задачи создаются всегда:

Задачи Сервера администрирования

Задача	Область действия	Расписание	Параметры
Загрузка обновлений в хранилище	Сервер администрирования	Каждый час	Источник: Сервера обновлений Лаборатории Касперского
Обслуживание базы данных	Сервер администрирования	Каждую субботу в 1:00 ночи	Оптимизирует, но не сжимает базу
Резервное копирование данных Сервера администрирования	Сервер администрирования	Раз в два дня в 2:00 утра	Хранит 3 последние копии, пароль не задан



Политики

Политика	Область действия
Kaspersky Endpoint Security 11.6 for Windows	Группа Управляемые устройства
Агент администрирования Kaspersky Security Center 13	Группа Управляемые устройства

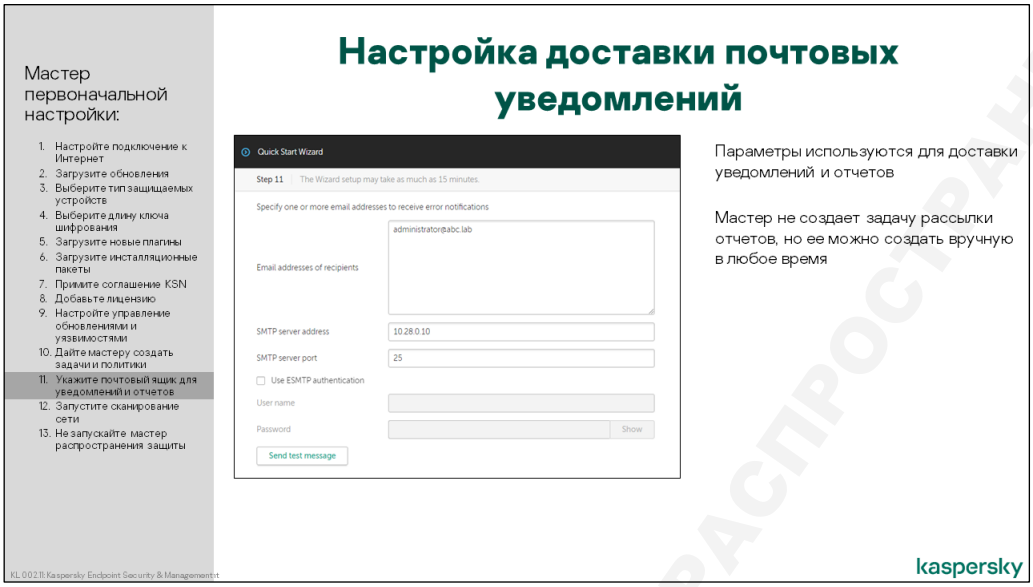
Задачи

Задача	Область действия	Расписание	Параметры
Установка обновлений	Управляемые устройства	При загрузке обновлений в хранилище	Источник: Сервер администрирования Устанавливает только одобренные обновления модулей

Обратите внимание, что групповая задача Быстрый поиск вирусов больше не создается по умолчанию. Вместо нее включается **Фоновая проверка**, которая сканирует системные области во время простоя компьютера. Опция находится в политике на вкладке **Параметры программы | Локальные задачи**.

Если администратор хочет полноценно управлять проверкой по требованию, ему нужно будет самому создать групповую задачу проверки с необходимыми настройками.

Настройка почтовых уведомлений



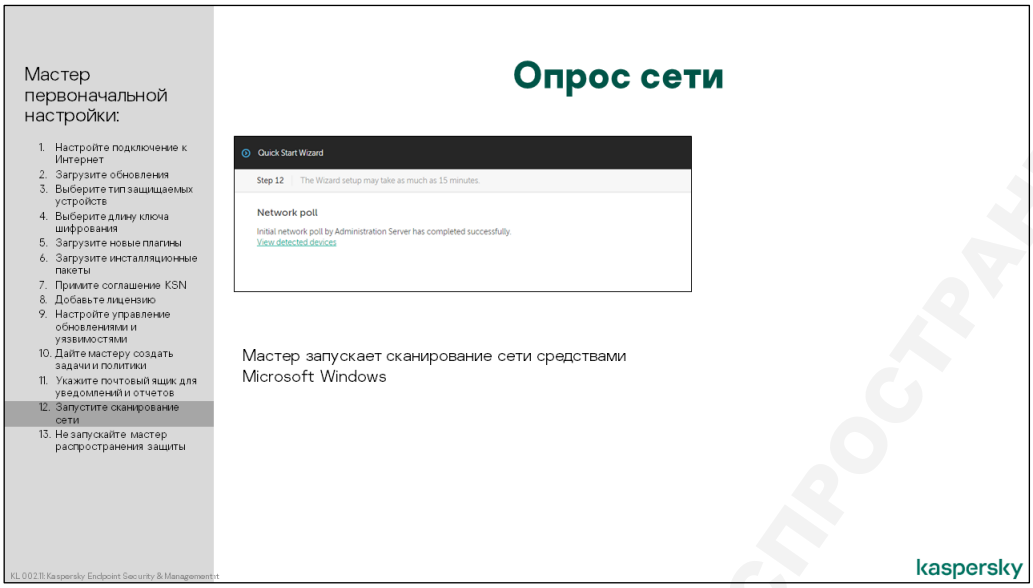
Следующий шаг — настройка почтовых уведомлений и доставки отчетов. Чтобы получать уведомления о важных событиях в почтовый ящик, нужно указать адрес получателя и параметры SMTP-сервера: адрес, порт и, если требуется, данные для авторизации. Заданные здесь параметры будут использоваться для отправки уведомлений и отчетов.

По умолчанию отправка уведомлений о событиях не включена. Чтобы действительно получать информацию о событиях в почтовый ящик, нужно включить отправку уведомлений в свойствах событий. События Kaspersky Security Center доступны через свойства Сервера администрирования. События Kaspersky Endpoint Security — через политику Kaspersky Endpoint Security.

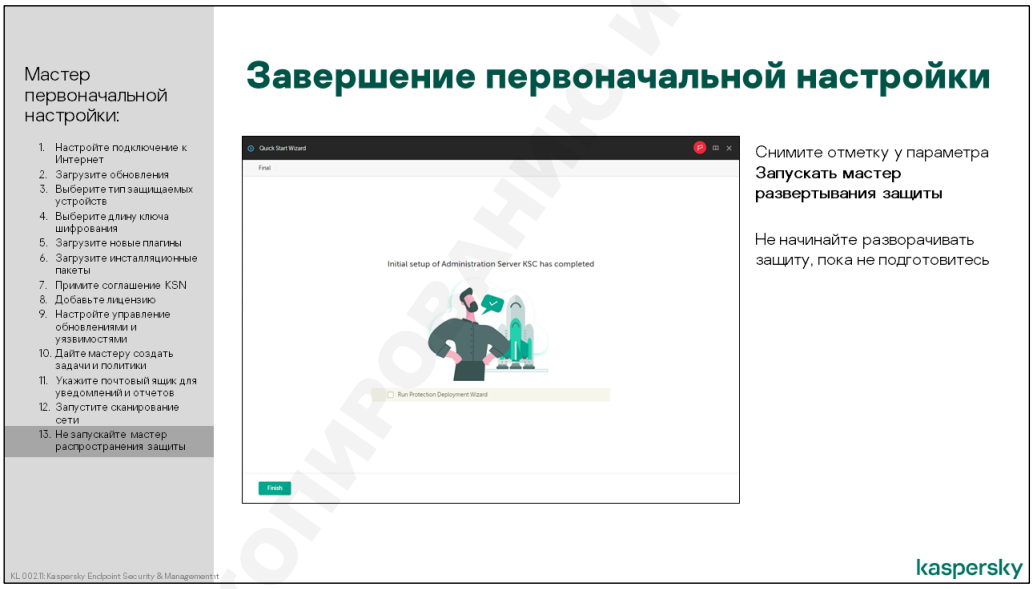
Мастер не проверяет корректность настроек, но позволяет сделать это администратору с помощью кнопки **Отправить пробное сообщение**. Администратор может воспользоваться ей для отправки тестового сообщения по указанным реквизитам. Если мастеру не удастся подключиться к почтовому серверу или пройти аутентификацию, будет сообщение об ошибке. Для завершения проверки администратору нужно дополнительно убедиться, что сообщение пришло в почтовый ящик.

Сканирование сети

Следующий шаг — сканирование сети средствами Windows. Этот тип сканирования работает через сетевое окружение в проводнике Windows, которое по умолчанию выключено в операционной системе. Этот шаг можно пропустить; сканирование будет выполняться в фоновом режиме.



Что делать дальше



В последнем окне мастера первоначальной настройки есть возможность немедленно перейти к мастеру удаленной установки для внедрения Kaspersky Endpoint Security на компьютеры сети. По умолчанию эта опция включена, но лучше с внедрением не спешить, а действовать по плану:

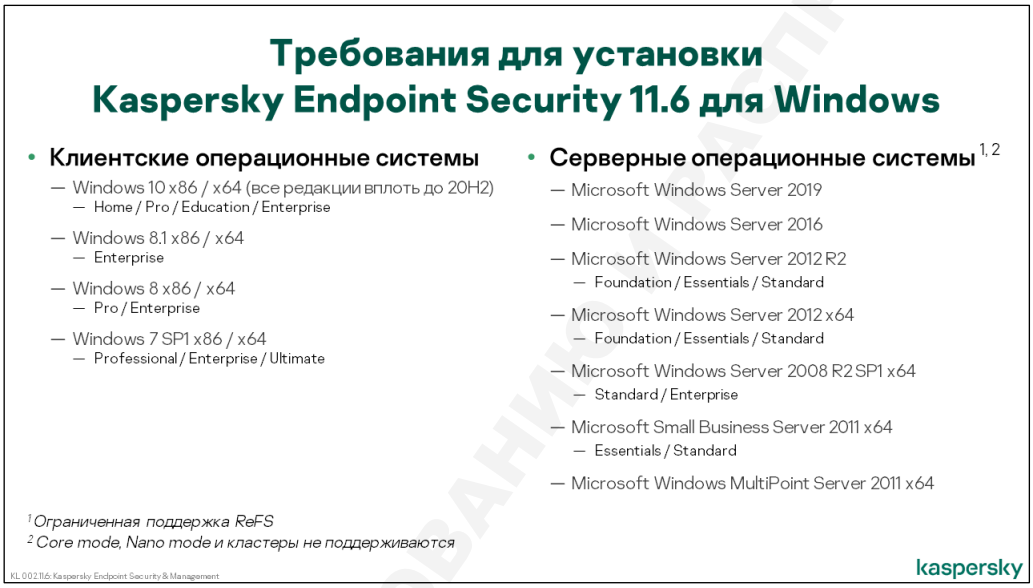
4. Дать Серверу время обнаружить компьютеры в сети
5. Проверить настройки инсталляционных пакетов, чтобы установить именно то, что нужно
6. Попробовать разные методы установки в тестовой среде

При желании администратор может повторно запустить мастер первоначальной настройки. При последующих запусках мастер создает только те задачи и политики, которых не хватает.

4. Как установить Kaspersky Endpoint Security на компьютеры

4.1 Требования к клиентским компьютерам

Требования Kaspersky Endpoint Security 11 к операционным системам



Kaspersky Endpoint Security можно установить на следующие операционные системы Microsoft Windows:

Пользовательские

- Windows 10 Pro x86 / x64 (все редакции до 20H2)[3]
- Windows 10 Education x86 / x64 (все редакции)[3]
- Windows 10 Enterprise x86 / x64 (все редакции)[3]
- Windows 8.1 Enterprise x86 / x64
- Windows 8 Pro x86 / x64
- Windows 8 Enterprise x86 / x64
- Windows 7 Professional SP1 x86 / x64
- Windows 7 Enterprise SP1 x86 / x64
- Windows 7 Ultimate SP1 x86 / x64

[3] Ограничения при работе на разных версиях Windows 10 описаны в статье базы знаний по ссылке https://support.kaspersky.ru/13036

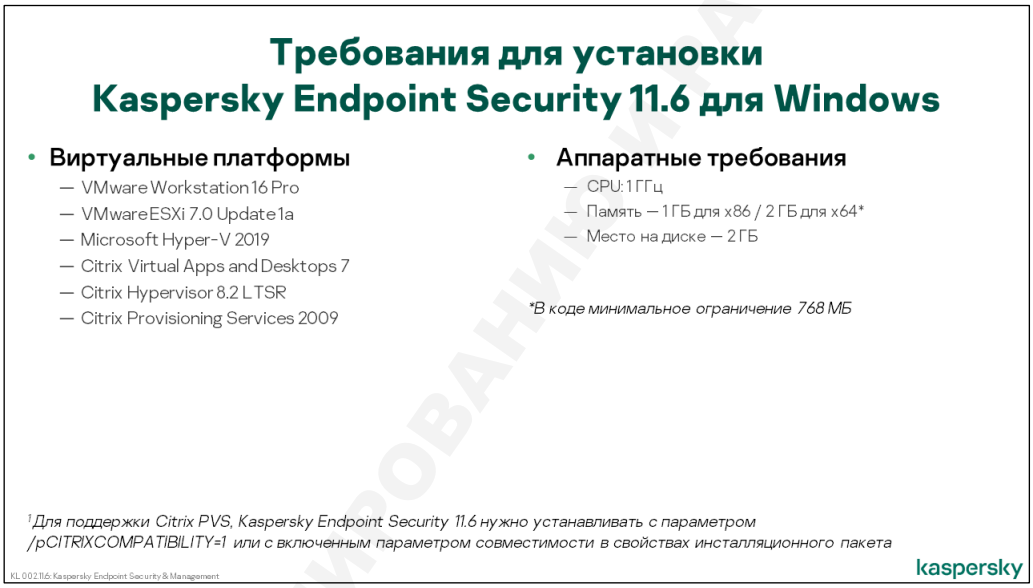
Серверные

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2 Foundation / Essential / Standard
- Microsoft Windows Server 2012 Foundation / Essential / Standard x64
- Microsoft Small Business Server 2011 Essential / Standard x64
- Microsoft Windows Server 2008 R2 SP1 Standard / Enterprise x64 SP1
- Microsoft Windows MultiPoint Server 2011x64

Стоит обратить внимание, что Datacenter-редакции Windows Server не поддерживаются. Для их защиты нужно использовать Kaspersky Security для Windows Server.

Перечень операционных систем включает большинство версий Windows, начиная с Windows 7 / Windows Server 2008 SP2 и до Windows 10 20H2 / Windows Server 2019.

Поддержка Kaspersky Endpoint Security виртуальных платформ



Kaspersky Endpoint Security 11.6 для Windows можно установить на следующие виртуальные платформы:

- VMware Workstation 16 Pro
- VMware ESXi 7.0 Update 1a
- Microsoft Hyper-V 2019
- Citrix Virtual Apps and Desktops 7
- Citrix Hypervisor 8.2 LTSR
- Citrix Provisioning Services 2009

Для корректной работы с Citrix PVS нужно устанавливать Kaspersky Endpoint Security с параметром /pCITRIXCOMPATIBILITY=1. В Kaspersky Endpoint Security 11.6 для Windows этот параметр можно включить в свойствах инсталляционного пакета, а не только через командную строку.

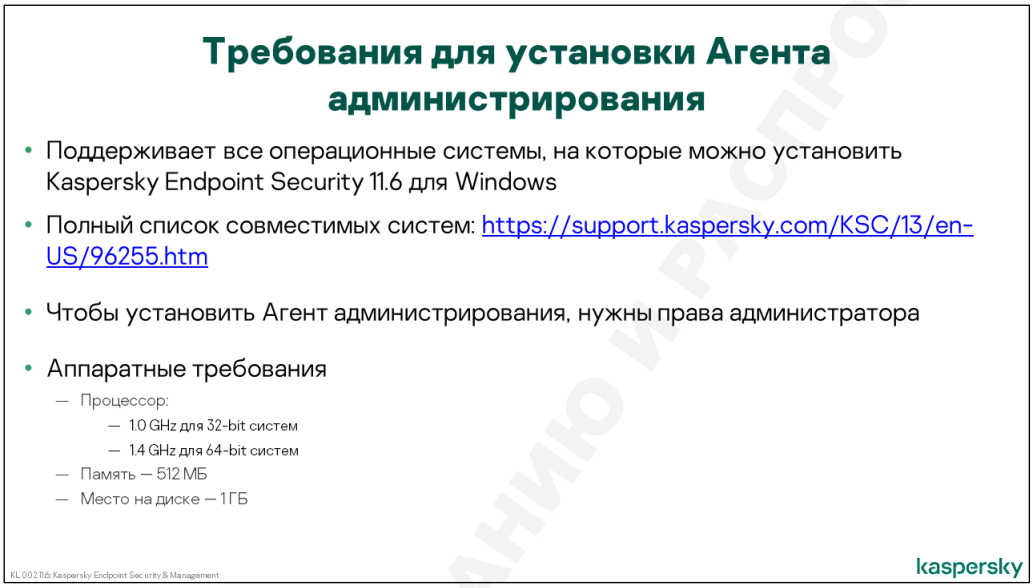
Чтобы установить Kaspersky Endpoint Security, нужны права администратора.

Минимальные требования к оборудованию

Общие аппаратные требования для установки Kaspersky Endpoint Security 11.6 таковы:

- Процессор с частотой 1 ГГц (и поддержкой набора инструкций SSE2)
- 1 ГБ оперативной памяти[4] (для x86)
- 2 ГБ оперативной памяти (для x64)
- 2 ГБ свободного места на диске

Требования для установки Агента администрирования



Агент администрирования Kaspersky Security Center поддерживает установку на все системы, поддерживаемые Kaspersky Endpoint Security 11.6для Windows.

Аппаратные требования для установки Агента администрирования следующие:

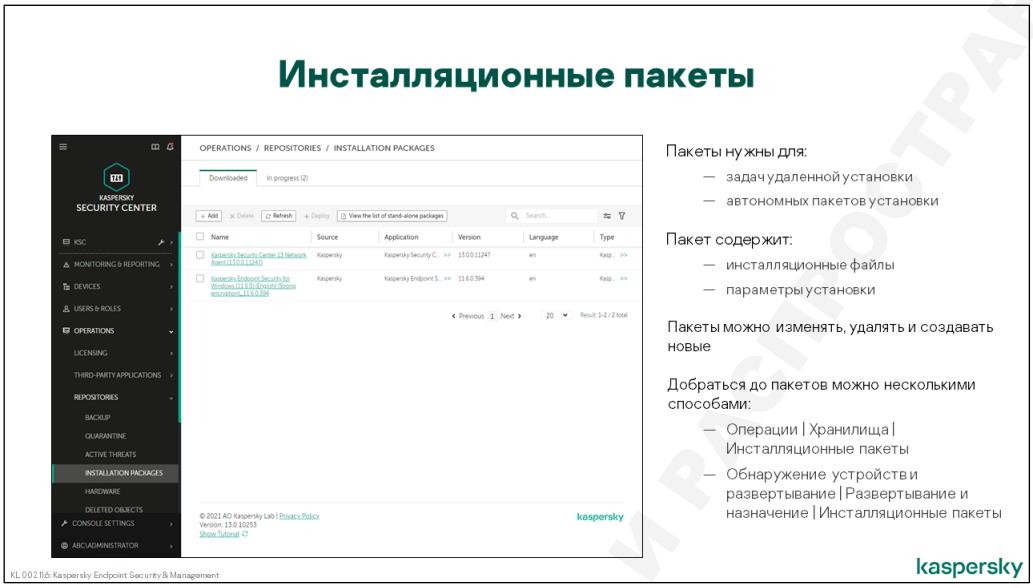
- Процессор:
  - 1 ГГц или выше для 32-битных систем
  - 1.4 ГГц или выше для 64-битных
- Память: 512 МБ
- Место на диске: 1 ГБ

Требования к памяти следует воспринимать как рекомендацию. Установку можно выполнить и на компьютер с меньшим объемом памяти.

[4] Минимальный объем оперативной памяти при котором можно выполнить установку составляет 768 МБ

4.2 Как изменить состав компонентов KES

Инсталляционные пакеты



Инсталляционные пакеты в Kaspersky Security Center — это готовые к установке продукты. В пакете объединяются инсталляционные файлы, параметры установки и некоторые параметры работы продукта. Параметры инсталляционного пакета призваны заменить мастер установки и мастер первоначальной настройки продукта. У каждого продукта свои настройки. Как уже было видно, инсталляционные пакеты используются в мастере и задачах удаленной установки, а также при создании автономных пакетов установки.

В поставку Kaspersky Security Center входят все необходимые пакеты для внедрения системы защиты:

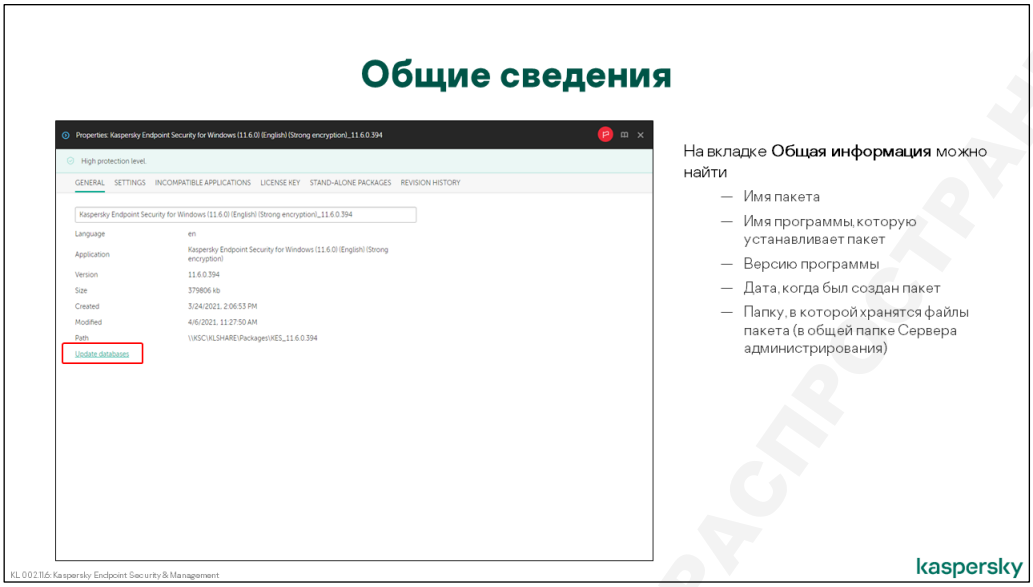
- Пакет Агента администрирования
- Пакет Kaspersky Endpoint Security для Windows
- Пакет Сервера iOS MDM
- Пакет Сервера мобильных устройств Exchange ActiveSync

Список имеющихся пакетов доступен на вкладке **Обнаружене устройств и развертывание | Развертывание и назначение | Инсталляционные пакеты**. Кроме названия и версии устанавливаемого приложения у каждого пакета есть уникальное имя. Эти данные, а также язык пакета отображаются в виде таблицы. Если открыть свойства пакета, то можно увидеть его размер — суммарный размер всех файлов.

Пакеты можно создавать, изменять и удалять. Если пакет используется в задаче установки, удалить его нельзя. Сначала удалите все задачи, которые используют пакет, затем удаляйте пакет.

В Kaspersky Security Center можно создавать и использовать инсталляционные пакеты разных видов и назначения. С помощью инсталляционных пакетов можно устанавливать операционные системы, сторонние программы, обновления и исправления к сторонним программам. С помощью инсталляционных пакетов можно также запускать на компьютерах скрипты и утилиты. Об использовании этих видов инсталляционных пакетов больше говорится в курсе KL 009 Управление системами. Настоящая глава ограничивается рассмотрением пакетов для установки программ Лаборатории Касперского.

Настройки пакета Kaspersky Endpoint Security

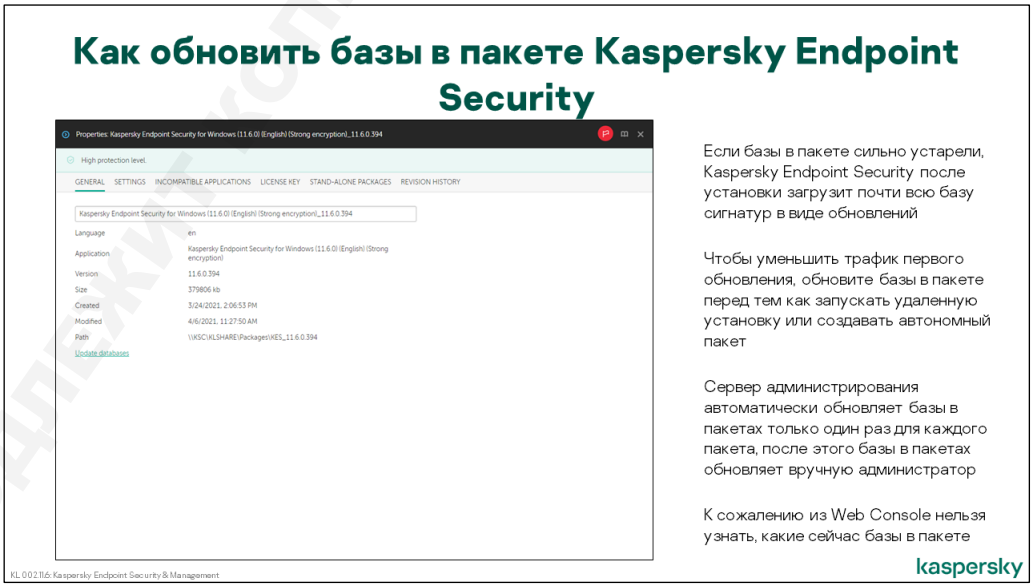


Общие свойства

У каждого пакета есть общие свойства и настройки, которые зависят от программы, для которой создан пакет. Чтобы увидеть настройки пакета, нужно чтобы в консоли был установлен плагин программы. Плагин можно загрузить прямо из интерфейса Web Console, для этого надо в правом верхнем углу выбрать **Параметры консоли | Веб-плагины**.

В общих свойствах пакета повторяется информация о версии программы и размере файлов, а также приводится путь к файлам пакета в общей папке Сервера администрирования. При необходимости, сотрудник ИТ–департамента может загрузить инсталляционные файлы по сети и выполнить локальную установку программы.

Как обновить базы в пакете



В общих свойствах пакета Kaspersky Endpoint Security есть еще кнопка **Обновить базы**. Она обновляет базу сигнатур внутри пакета.

Чтобы Kaspersky Endpoint Security мог работать сразу после установки, в состав инсталляционных файлов входят базы. Со временем они устаревают. Это не является большой проблемой, поскольку сразу после установки Kaspersky Endpoint Security запустится задача обновления и загрузит новые базы.

Но в некоторых случая целесообразно, чтобы установка выполнялась с максимально свежими базами. Например, сотрудник ИТ может взять с собой автономный пакет установки для внедрения на компьютерах небольшого офиса с плохим доступом в Интернет. В этом случае не столь важен размер пакета, который сотрудник принесет с собой на сменном носителе. Важнее уменьшить трафик задачи обновления, который может составить несколько десятком мегабайт, если базы в пакете старые.

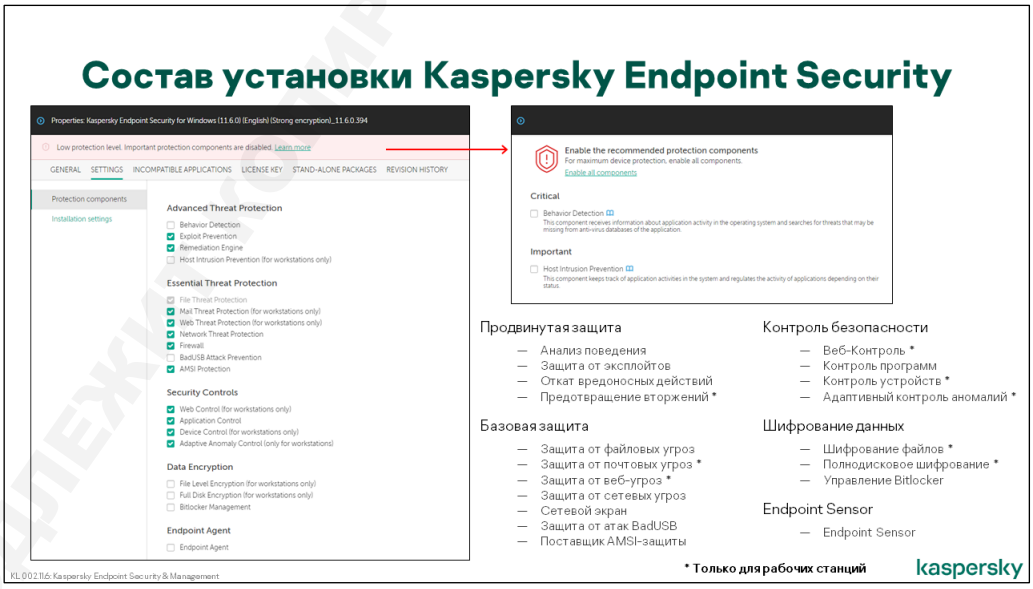
Для таких случаев предусмотрена возможность обновить базы в самом пакете перед установкой. Дата последнего такого обновления, к сожалению, не видна в Web Console, но это можно посмотреть в MMC-консоли, в общих свойствах пакета, в графе **Базы обновлены**.

Кнопка **Обновить базы** копирует в пакет полный набор баз для Kaspersky Endpoint Security из хранилища Сервера. В исходной версии пакета базы представлены архивом *bases.cab*. После обновления баз кнопкой **Обновить базы**, архив заменяется папкой *bases*. Суммарный объем папки сравним с размером архива, поскольку файлы баз зашифрованы и не поддаются сжатию.

Kaspersky Security Center автоматически обновляет базы в пакетах после загрузки новых обновлений в хранилище. Но делает это только один раз для каждого пакета. Если базы в пакете уже однажды были обновлены автоматически, при последующей загрузке обновлений в хранилище базы они больше автоматически не обновляются.

Фактически автоматическое обновление применяется вскоре после установки Сервера администрирования к предустановленному пакету Kaspersky Endpoint Security, и точно также к каждому новому созданному пакету Kaspersky Endpoint Security вскоре после его создания.

Как выбрать компоненты в пакете



Остальные параметры пакета Kaspersky Endpoint Security дублируют параметры интерактивной установки. Это в первую очередь список компонентов и папка размещения программных файлов.

Компоненты, доступные для установки:

- **Продвинутая защита**
  - Анализ поведения
  - Защита от эксплойтов
  - Откат вредоносных действий
  - Предотвращение вторжений *
- **Базовая защита**
  - Защита от файловых угроз
  - Защита от почтовых угроз *
  - Защита от веб-угроз *
  - Защита от сетевых угроз
  - Сетевой экран
  - Защита от атак BadUSB
  - Поставщик AMSI-защиты
- **Контроль безопасности**
  - Веб-Контроль *
  - Контроль программ
  - Контроль устройств *
  - Адаптивный контроль аномалий *
- **Шифрование данных**
  - Шифрование файлов *
  - Полнодисковое шифрование *
  - Управление Bitlocker
- **Endpoint Sensor**
  - Endpoint Sensor

По умолчанию выбраны в основном компоненты, которые соответствуют лицензии Стандартная. При этом нужно помнить, что, хотя пакет может быть установлен на любую поддерживаемую операционную систему, многие компоненты работают только на рабочих станциях. На серверных системах устанавливаются только следующие компоненты:

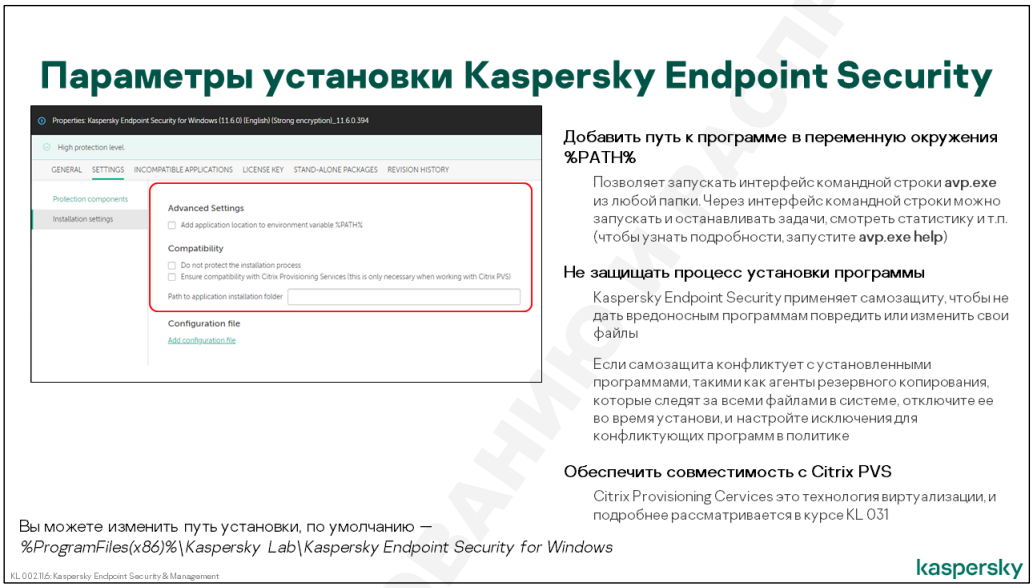
- Анализ поведения
- Защита от эксплойтов
- Откат вредоносных действий
- Защита от файловых угроз
- Защита от сетевых угроз
- Сетевой экран
- Защита от атак BadUSB
- Поставщик AMSI-защиты
- Контроль программ
- Управление Bitlocker
- Endpoint Sensor

Несмотря на то, что настройки компонента *Предотвращение вторжений* отображаются в интерфейсе Kaspersky Endpoint Security на серверах, компонент на самом деле не устанавливается. Kaspersky Endpoint Security на серверах не контролирует активность программ, и, в частности, не блокирует запуск программ, имеющих статус *Недоверенные*. Настройки *Предотвращения вторжений* отображаются на серверах потому, что часть этих настроек относится к работе компонента *Сетевой экран*. Подробнее о компонентах *Предотвращение вторжений* и *Сетевой экран* рассказывается в части II этого курса.

Кроме компонентов устанавливаются также локальные задачи. Они недоступны для выбора в свойствах пакета и устанавливаются на любые операционные системы:

- Обновление
- Откат обновления
- Проверка целостности
- Задачи поиска вирусов:
  - Полная проверка
  - Проверка важных областей
  - Выборочная проверка
  - Проверка из контекстного меню

Настройки совместимости



По умолчанию компоненты Kaspersky Endpoint Security устанавливаются в папку *%ProgramFiles(x86)%***Kaspersky Lab\Kaspersky Endpoint Security for Windows**.

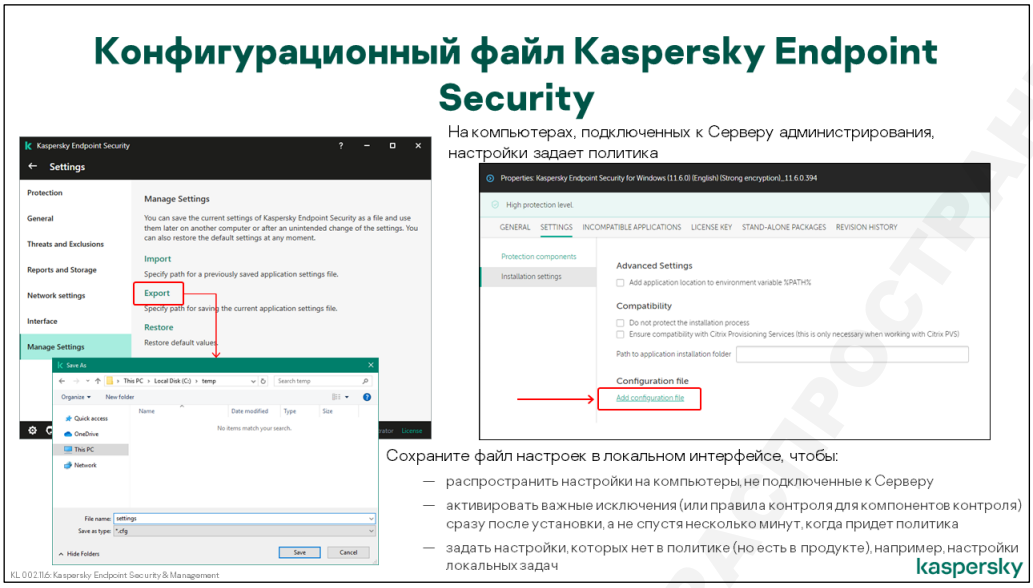
При желании администратор может изменить этот путь на любой другой.

Администраторы, часто использующие интерфейс командной строки, могут включить флаг автоматического добавления папки установки в переменную среды *%PATH%*. Тогда они смогут вызывать команды управления продуктом просто через **avp.com**, без необходимости указывать полный путь.

В пакете есть два дополнительных параметра имеющих статус настроек совместимости. Один из них — **Не защищать процесс установки программы** — отключает самозащиту в процессе установки. Самозащита не дает менять инсталляционные файлы сторонним программам, в первую очередь вредоносным. Она также блокирует доступ к папке, куда устанавливаются файлы Kaspersky Endpoint Security, и к разделу реестра с ключами программ Лаборатории Касперского. Иногда самозащита конфликтует со сторонними программами, например, с агентами резервного копирования. Поэтому ее можно отключить.

Второй параметр — **Обеспечить совместимость с Citrix Provisioning Services**. Если вы хотите установить Kaspersky Endpoint Security на образ для виртуальных машин в среде Citrix PVS, включите эту опцию.

Как добавить в пакет файл с настройками



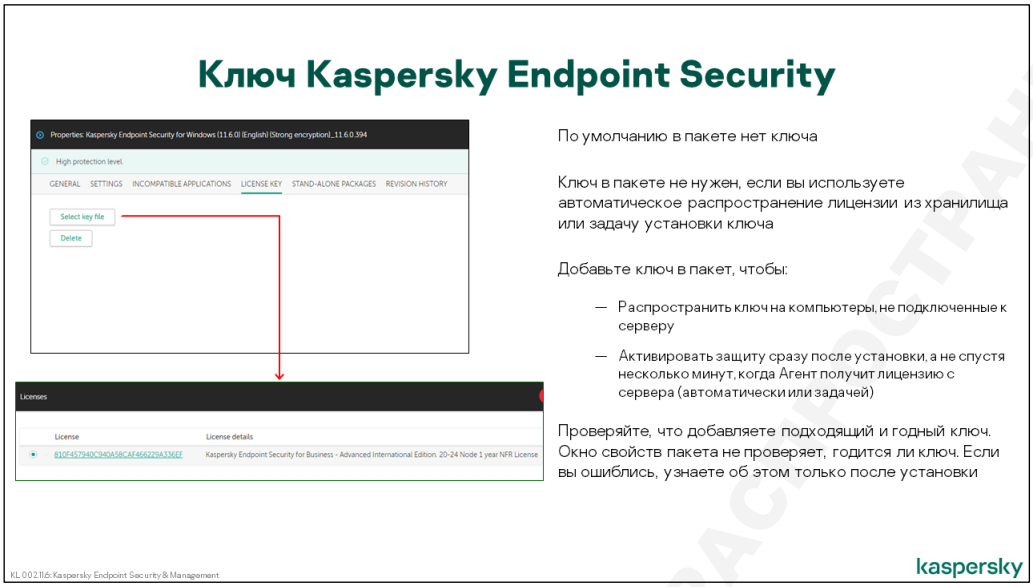
Еще одним параметром является **Конфигурационный файл**. Этот файл задает параметры работы Kaspersky Endpoint Security после установки

Конфигурационный файл заменяет собой мастер первоначальной настройки Kaspersky Endpoint Security. Если конфигурационный файл не задан, продукт будет работать с заводскими настройками. Впрочем, при первом же соединении Агента с Сервером будет загружена политика Kaspersky Endpoint Security, которая переопределит настройки защиты. Так что конфигурационный файл нужен, если политика форсирует не все настройки продукта, или для использования на неуправляемых компьютерах.

Чтобы создать конфигурационный файл, установите Kaspersky Endpoint Security на компьютер, но не подключайте его к Серверу администрирования, иначе групповая политика не даст вам менять локальные настройки.

Настройте Kaspersky Endpoint Security через локальный интерфейс, как вам нужно, и сохраните эти настройки в файл. Кнопка **Сохранить…** находится в окне **Настройка** в разделе **Общие параметры | Управление параметрами.**

Как добавить в пакет ключ



Kaspersky Endpoint Security не работает без активации. При интерактивной установке ключ задается в ходе выполнения мастера первоначальной настройки. При удаленной установке есть несколько способов активировать установленный продукт. Один из них — указать файл ключа в свойствах инсталляционного пакета.

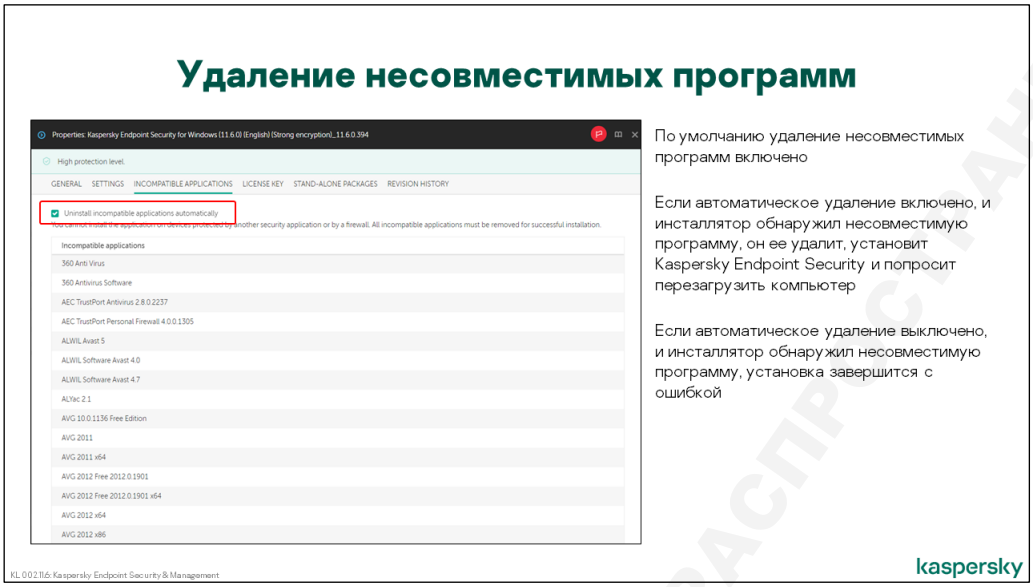
В свойствах пакета можно добавить только ключ, код добавить нельзя.

Кроме этого, ключ или код можно распространить специальной задачей на выбранные компьютеры.

Третий вариант: включить флаг **Автоматически распространяемый ключ** в свойствах ключа или кода на вкладке **Операции | Лицензирование | Лицензии Лаборатории Касперского** в веб-консоли.

В крайнем случае код или ключ можно добавить через локальный интерфейс Kaspersky Endpoint Security.

Где выключить удаление несовместимых программ

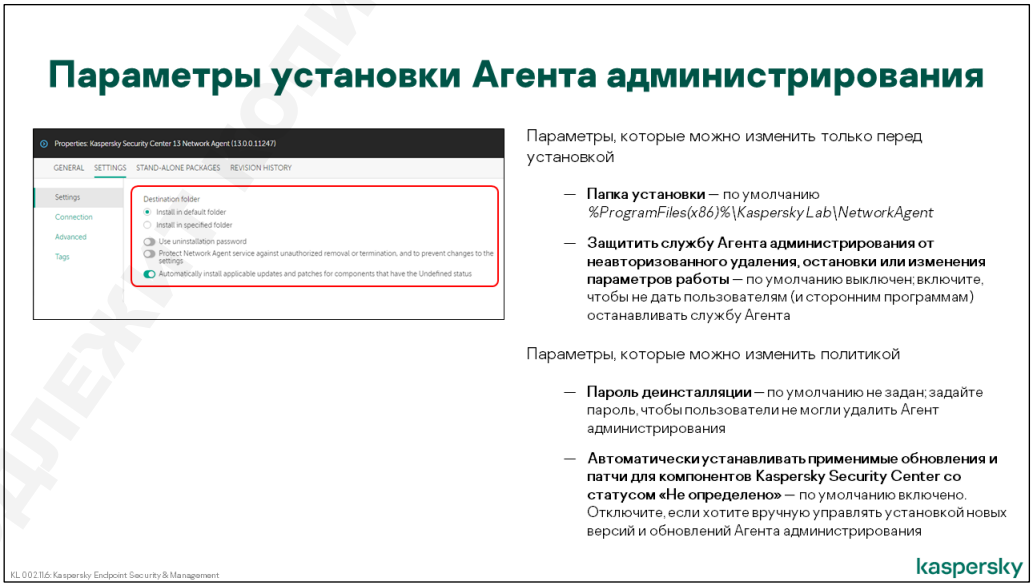


По умолчанию инсталлятор Kaspersky Endpoint Security ищет и удаляет несовместимые программы: сторонние антивирусы и сетевые экраны.

Список программ, которые может удалить Kaspersky Endpoint Security, довольно большой, но не исчерпывающий. В нем, как правило, нет самых свежих версий сторонних средств защиты, а также нет программ, которые не слишком широко распространены. Как удалить программы, которые Kaspersky Endpoint Security не обнаружил, рассказывает раздел в конце этой главы.

Если Kaspersky Endpoint Security некорректно удаляет несовместимую программу, отключите автоматическое удаление, и удалите программу самостоятельно.

Параметры пакета Агента администрирования



Путь установки

Общие сведения о пакете Агента администрирования такие же, как и Kaspersky Endpoint Security, но без кнопки **Обновить базы**. У Агента администрирования нет баз.

В разделе **Параметры** можно изменить каталог установки, а также задать пароль на деинсталляцию. Если каталог не указан в явном виде, используется стандартное значение

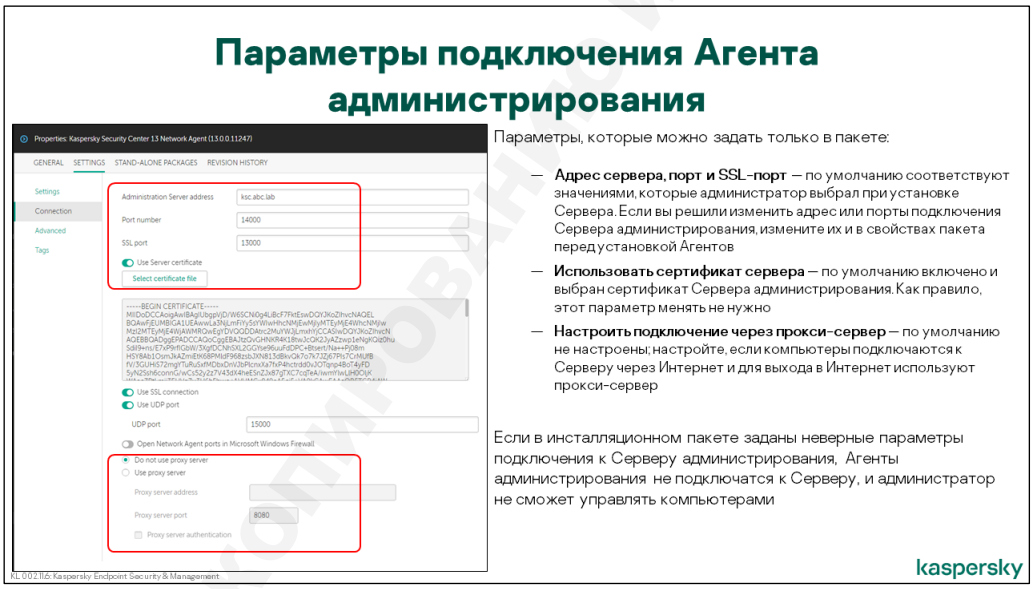
*%ProgramFiles%***Kaspersky Lab\NetworkAgent**

Защита паролем

В свойствах пакета можно включить защиту Агента от деинсталляции и указать пароль. В этом случае даже пользователь с правами администратора не сможет удалить Агент штатными средствами, не зная пароля. Впрочем, при большом желании пользователь с правами администратора всегда может привести Агент в неработоспособное состояние.

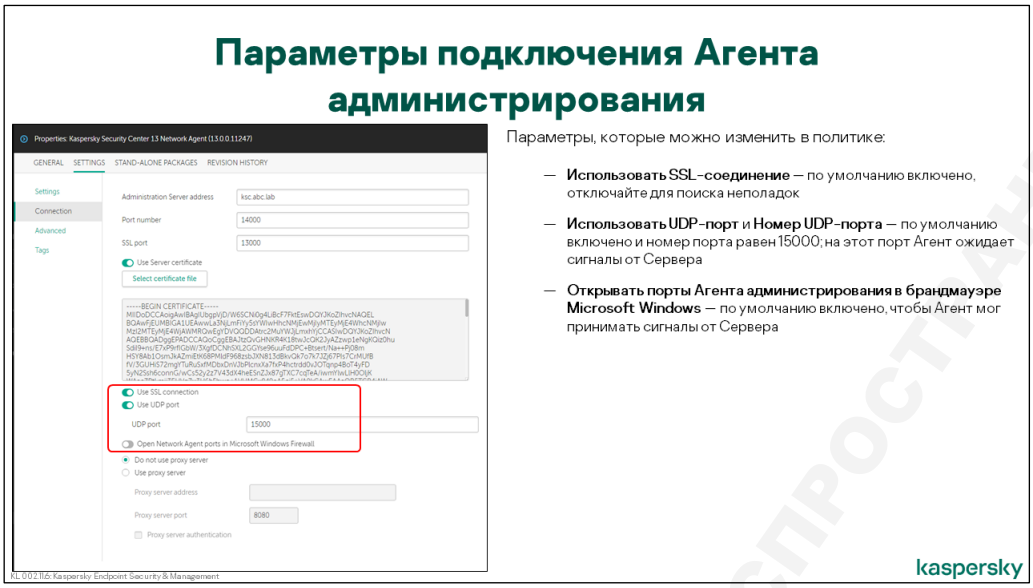
Если вы не включили защиту паролем в инсталляционном пакете Агента, включите ее в политике Агента, где она тоже есть.

Параметры подключения к Серверу администрирования



В разделе **Подключение** в свойствах инсталляционного пакета Агента администрирования расположены параметры подключения к Серверу администрирования. Эти же настройки спрашивает мастер установки Агента при выполнении локальной инсталляции в интерактивном режиме.

Основные параметры подключения — это адрес и порты Сервера администрирования. Исходно они принимают значения, заданные при установке Сервера администрирования. Если клиентские компьютеры и Сервер администрирования находятся в разных подсетях, связь между которыми осуществляется через прокси-сервер, параметры прокси-сервера тоже можно задать в свойствах инсталляционного пакета. Эти стандартные параметры включают адрес и порт прокси-сервера, а также имя и пароль для аутентификации. Следует иметь в виду, что эти параметры будут использованы Агентами при подключении к Серверу, а не наоборот.



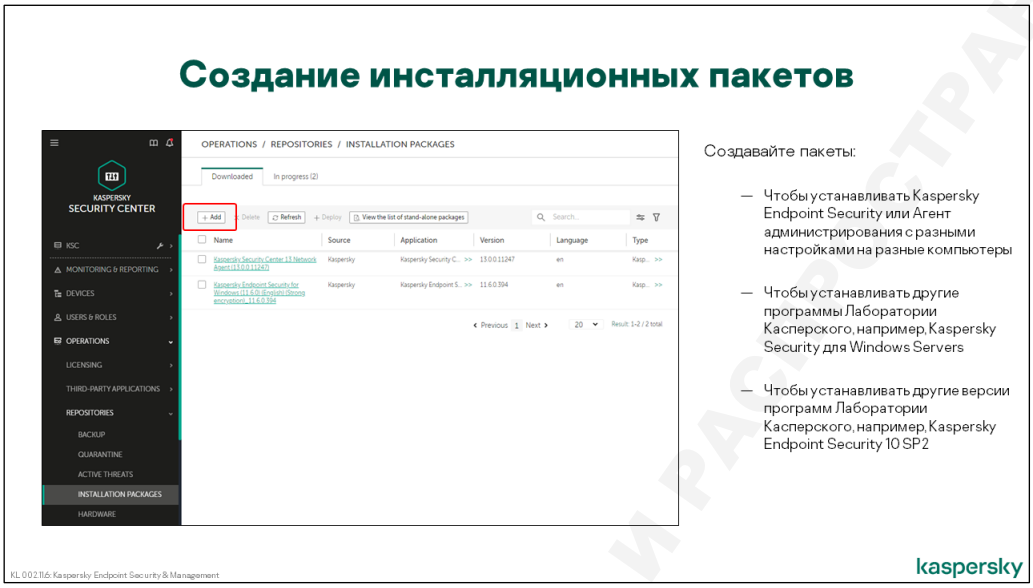
Когда соединение с клиентским компьютером инициируется Сервером, например, для экстренного применения политики, Сервер обращается к Агенту администрирования через UDP-порт. Чтобы брандмауэр Windows не блокировал поступающие на этот порт запросы, Агент может автоматически создать необходимые исключения. Такое поведение Агента регулируется опцией **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**. По умолчанию Агент принимает соединения на UDP-порт 15000. Значение можно поменять как в свойствах пакета, так и позже в политике Агента.

Как и Консоль администрирования, Агенты могут связываться с Сервером по шифрованному (SSL) или нешифрованному каналу. По умолчанию использование SSL включено. При этом Агенты автоматически загружают и используют сертификат Сервера администрирования. Возможность задать сертификат вручную может использоваться в сетях с повышенными требованиями к безопасности, чтобы исключить вариант подмены Сервера администрирования.

Дополнительные параметры в инсталляционном пакете Агента востребованы скорее в сетях со сложной инфраструктурой. Они рассмотрены в курсах KL 009. Управление системами и KL 302. Kaspersky Endpoint Security and Management. Масштабирование.

4.3 Как создать новый пакет установки

Зачем создавать пакеты установки



Инсталляционных пакетов, входящих в стандартную поставку Kaspersky Security Center, вполне достаточно для организации защиты в большинстве сетей. Создание дополнительных пакетов может потребоваться в следующих случаях:

— Вышла новая версия Kaspersky Endpoint Security. Для обновления версии, как и для первоначальной установки, нужен инсталляционный пакет. Администратор может создать пакет самостоятельно или загрузить новую версию Kaspersky Security Center, включающую обновленную версию пакета, и переустановить Сервер администрирования поверх существующего (все настройки сохранятся).

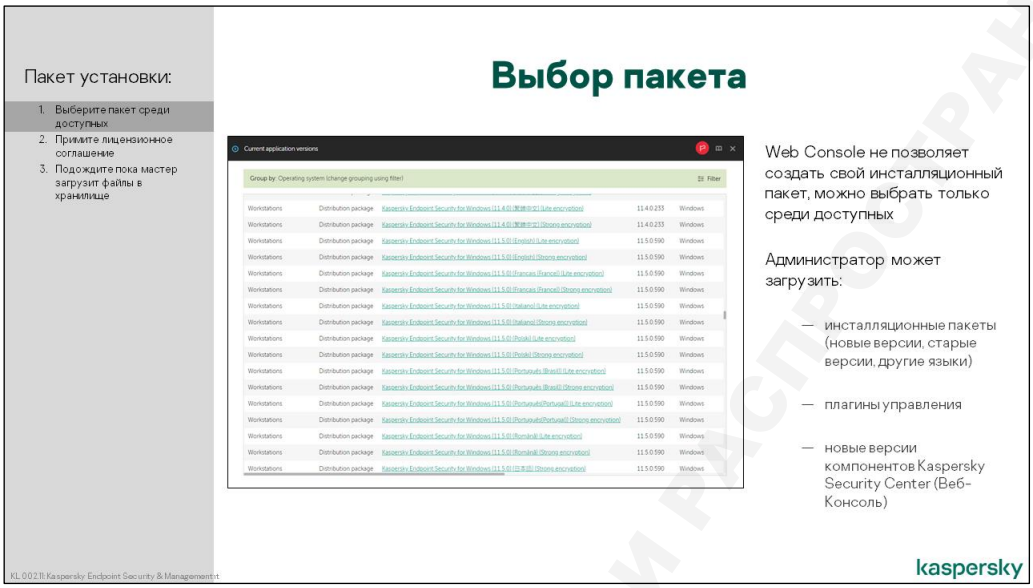
— Нужно выполнить удаленную установку продукта Лаборатории Касперского, не входящего в стандартную поставку Kaspersky Security Center, например, Kaspersky Security для Windows Server. Такой пакет нужно создавать вручную.

— В разных частях сети установку нужно выполнять с разными параметрами. Например, согласно плану внедрения, часть компьютеров может не нуждаться в компонентах *Защита от веб-угроз* и *Защита от почтовых угроз*. Чтобы иметь возможность выполнять внедрение параллельно на обе категории компьютеров, нужно создать дополнительный инсталляционный пакет с нестандартными настройками.

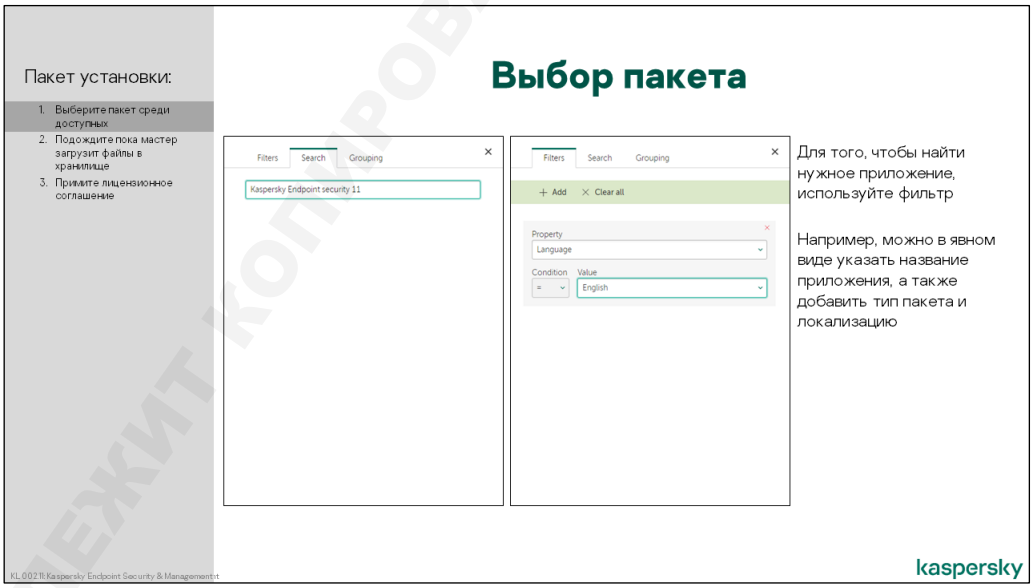
Чтобы создать инсталляционный пакет, нажмите кнопку **Добавить** во вкладке **Операции | Хранилища | Инсталляционные пакеты**. После этого открывается список доступных дистрибутивов различных версий и локализаций.

Мастер создания пакета

Выбор пакета



Администратору не нужно самому искать и загружать инсталляционные файлы. Kaspersky Security Center отслеживает текущие версии Kaspersky Security Center, Kaspersky Endpoint Security и Kaspersky Security для Windows Server и другие, и позволяет администратору создавать инсталляционные пакеты прямо из дистрибутивов, доступных на серверах Лаборатории Касперского.



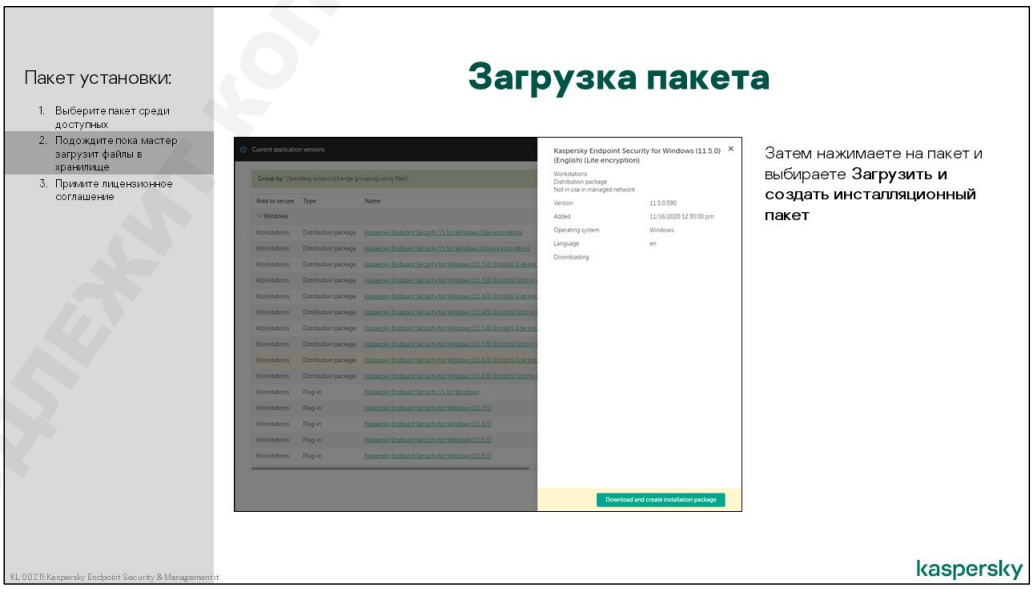
Для поиска нужного приложения среди огромного количества лучше всего воспользоваться фильтром, в котором указать хотя бы название и язык.

Kaspersky Security Center управляет многими программами Лаборатории Касперского. А список обновлений содержит не только новые версии программ, но и обновления к ним, новые версии плагинов, разные локализации одной и той же программы. В итоге список получается длинный.

Чтобы найти то, что нужно, используйте фильтр. В фильтре можно выбрать:

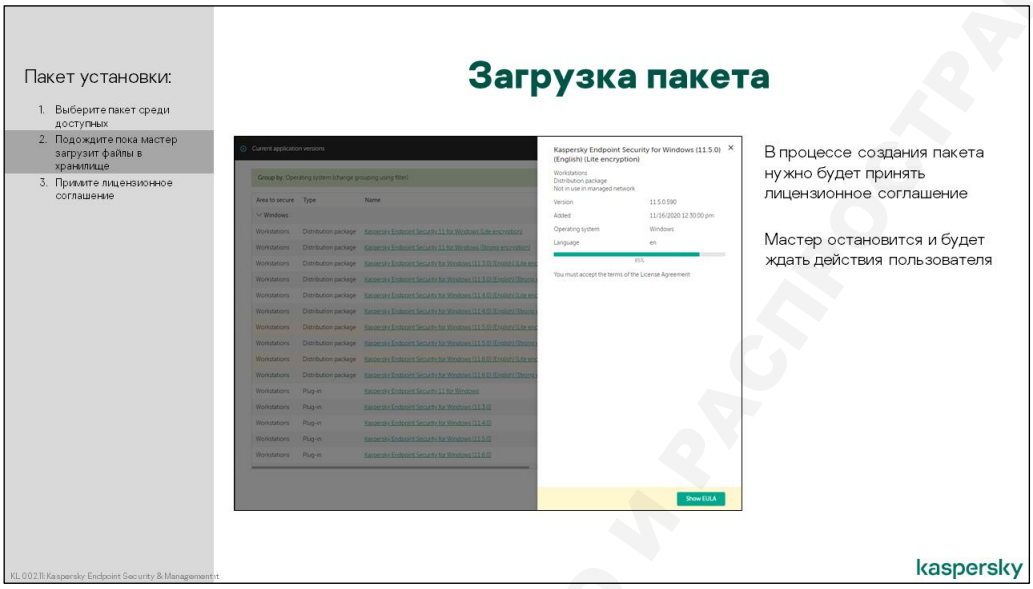
- Тип программы:
  - Инструменты управления — компоненты Kaspersky Security Center
  - Рабочие станции— программы для защиты рабочих станций. Сюда относится Kaspersky Endpoint Security для Windows
  - Файловые сервера и системы хранения данных— программы для защиты серверов и хранилищ. Сюда относится, например, Kaspersky Security для Windows Server
  - Виртуальные среды— разные версии Kaspersky Security для виртуальных сред
  - Мобильные устройства— программы Лаборатории Касперского для смартфонов и планшетов Android и iOS
  - Банкоматы и POS-системы — Kaspersky Embedded Systems Security
- Тип обновления:
  - Полный дистрибутив
  - Плагин для управления
  - Обновление программы
- Показывать не все обновления:
  - Только самые последние версии
  - Обновление только к используемым программам
  - Обновления к программам, плагины которых установлены в консоли
- Язык:
  - Все языки
  - Язык консоли администрирования и базовый набор языков (английский, немецкий, французский)
  - Язык консоли и еще один язык, на выбор из списка

После того, как вы примените фильтр, в окне останутся только обновления, которые удовлетворяют условиям. Вы также можете сортировать результаты по имени, типу, языку и другим параметрам.

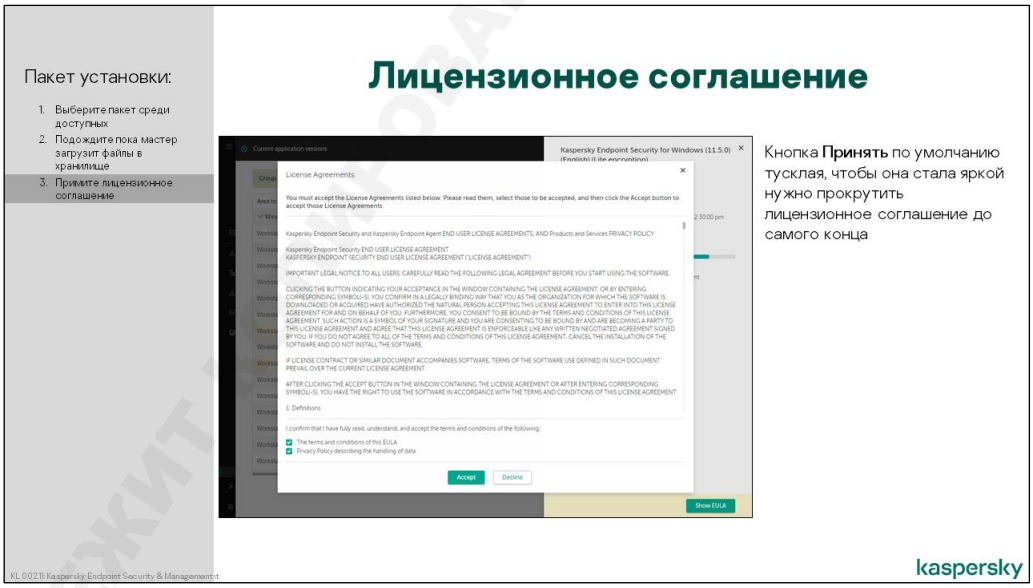


Когда выбрали нужный дистрибутив, просто нажимаете кнопку **Загрузить и создать пакет** — все остальное Сервер администрирования выполнит автоматически: загрузит файлы и создаст из них инсталляционный пакет.

Лицензионное соглашение



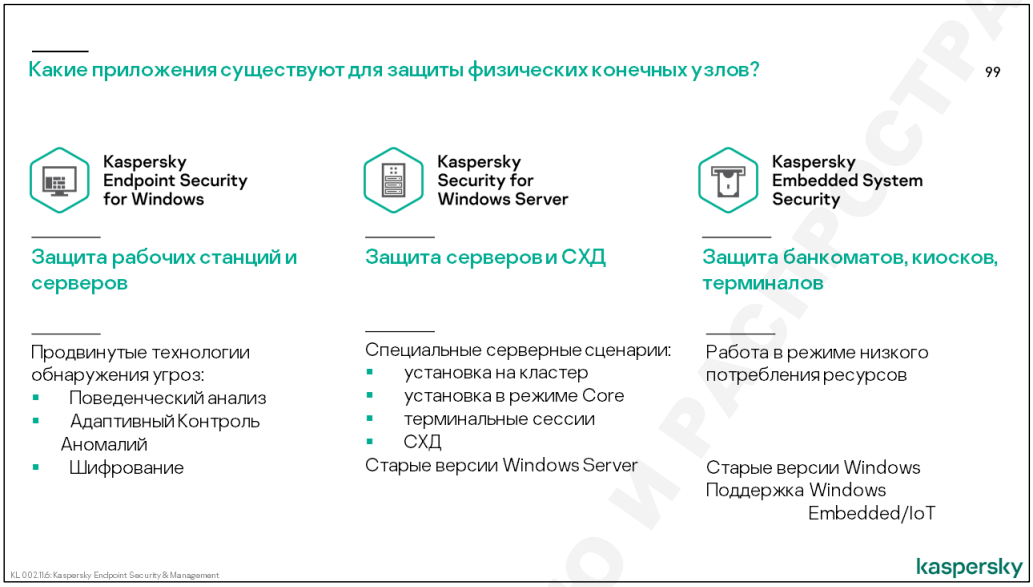
Индикатор выполнения остановится примерно на 85% и будет ждать, пока примет лицензионное соглашение.



Кнопка **Принять** по умолчанию неактивна, чтобы она стала активной нужно прокрутить лицензионное соглашение до самого низа

4.4 Kaspersky Security для Windows Server

Какие еще есть приложения существуют для защиты Windows Servers



У Лаборатории Касперского есть несколько приложений класса EPP для защиты физических конечных узлов:

— Kaspersky Endpoint Security для Windows
— Kaspersky Security для Windows Server
— Kaspersky Embedded Systems Security

Здесь мы хотим сделать акцент именно на физических устройствах, поскольку для защиты виртуальных машин у Лаборатории Касперского есть специализированные приложения.

Данное утверждение не значит, что вышеперечисленные приложения нельзя устанавливать на виртуальные машины. Можно. Но возможен не оптимальный расход системных ресурсов.

Давайте же разберемся, чем отличаются все три приложения, в чём преимущества каждого из них, какие у них сильные стороны и сценарии использования в корпоративной инфраструктуре.

— Kaspersky Endpoint Security для Windows

  Спроектирован для защиты рабочих станций и серверов Windows.

  Является флагманским и самым передовым приложением от Лаборатории Касперского так как сочетает в себе продвинутые технологии для обнаружения вредоносного программного обеспечения, например, Поведенческий анализ и Адаптивный контроль аномалий. Позволяет использовать полнодисковое или файловое шифрование для соблюдения конфиденциальности данных на защищаемом устройстве.

— Kaspersky Security для Windows Server

  Создан для защиты серверов Windows и систем хранения данных. Вот небольшой перечень уникальных возможностей Kaspersky Security для Windows Server по сравнению с Kaspersky Endpoint Security:

При работе на отказоустойчивом кластере умеет корректно воспринимать смену активного узла и применять те же параметры проверки к общим кластерным ресурсам, которые перемещаются при смене узла.

Kaspersky Security для Windows Server по умолчанию устанавливается без интерфейса, чтобы им управлять, можно использовать: Консоль управления Kaspersky Security, Kaspersky Security Center или утилиту управления командной строки (kavshell.exe) Эта особенность позволяет устанавливать Kaspersky Security for Windows Server на сервера Windows в режиме ядра (Server Core).

Умеет корректно распознавать режим терминальной сессии или сеанс удалённого рабочего стола, и при обнаружении угрозы уведомлять только конкретного пользователя, который работает в сессии.

Защищает системы хранения данных, речь идет о NAS-хранилищах, которые в основном используют собственную операционную систему и подключаются к серверу по специфическим протоколам. Т.е. проверка стандартными средствами в этом случае работать не будет.

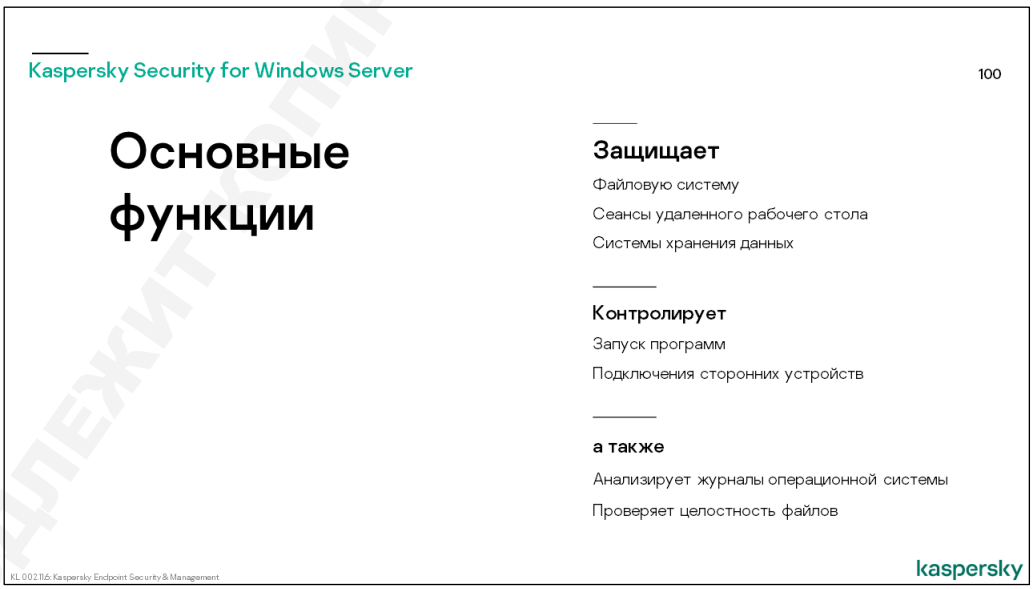
Поддерживает все актуальные платформы Microsoft Windows Server, а также устаревшие версии, такие как Microsoft Windows Server 2003.

— Kaspersky Embedded Systems Security

  Приложение создано на основе кодовой базы Kaspersky Security для Windows Server и во многом функции и возможности продуктов пересекаются. Основным отличием от вышеперечисленных программ KESS является установка на Embedded устройства (банкоматы, терминалы, киоски). KESS был спроектирован таким образом, чтобы наименьшим образом влиять на работу устройств с весьма ограниченным количеством вычислительных системных ресурсов.

  Kaspersky Embedded Systems Security можно устанавливать не только на современные версии Microsoft Windows, но и устаревшие, такие как Windows XP. Также программа поддерживает установку на специальные редакции Microsoft Windows: Embedded и IoT.

Основные функции Kaspersky Security для Windows Server



Лаборатория Касперского разработала Kaspersky Security для Windows Server, которая имеет следующие основные функции.

Защищает:

- Серверную файловую систему от вредоносных файлов, вирусов шифровальщиков-вымогателей и эксплойтов.
- Сеансы удаленного рабочего стола от веб и почтовых угроз, а также помогает контролировать доступ к сторонним веб-ресурсам.
- Системы хранения данных от передачи вредоносных данных через папки общего доступа, а также предотвращает попытки зашифровать данные на защищаемых хранилищах NetApp.

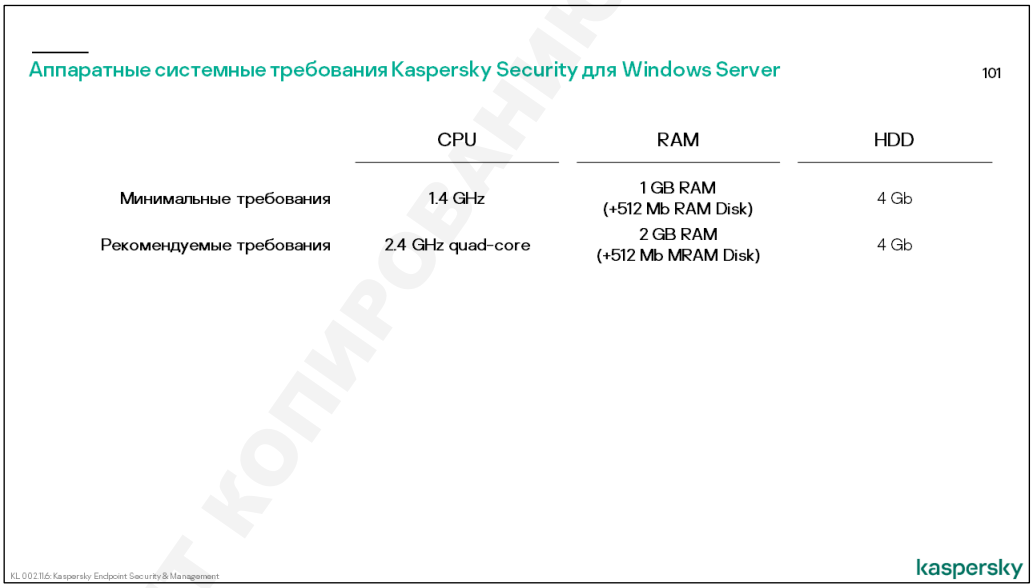
Контролирует:

- Запуск всех программ, и блокирует запуск тех, которых нет в разрешенном списке.
- Подключение внешних устройств (USB, CD, MTP) к защищаемому серверу.

А также:

- Анализирует журналы операционный системы, чтобы выявить аномалии в работе и попытки взлома сервера.
- Отслеживает изменения файлов, чтобы предоставить администратору информацию о файловых операциях

Системные требования Kaspersky Security для Windows Server


Аппаратные системные требования Kaspersky Security для Windows Server 101

	CPU	RAM	HDD
Минимальные требования	1.4 GHz	1 GB RAM (+512 Mb RAM Disk)	4 Gb
Рекомендуемые требования	2.4 GHz quad-core	2 GB RAM (+512 Mb MRAM Disk)	4 Gb

KL 002.11.6: Kaspersky Endpoint Security & Management
kaspersky

Минимальные системные требования:

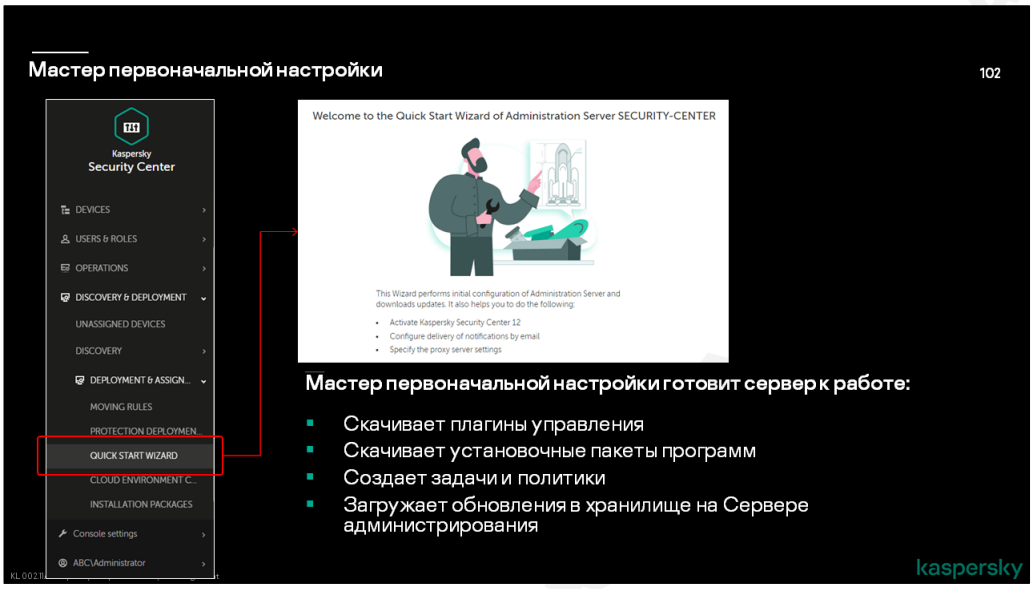
- Процессор: с 1 ядром, тактовой частотой 1.4 GHz
- Память: 1Gb + дополнительные 512 Mb необходимы если включена опция KL RAM Disk в настройках задачи обновления
- Жесткий диск: с 4Gb свободного места

Рекомендуемые системные требования:

- Процессор: с 1 ядром, тактовой частотой 2.4 GHz
- Память: 2Gb + дополнительные 512 MB необходимы если включена опция KL RAM Disk в настройках задачи обновления
- Жесткий диск: с 4Gb свободного места

4.5 Как создать инсталляционный пакет Kaspersky Security для Windows Server

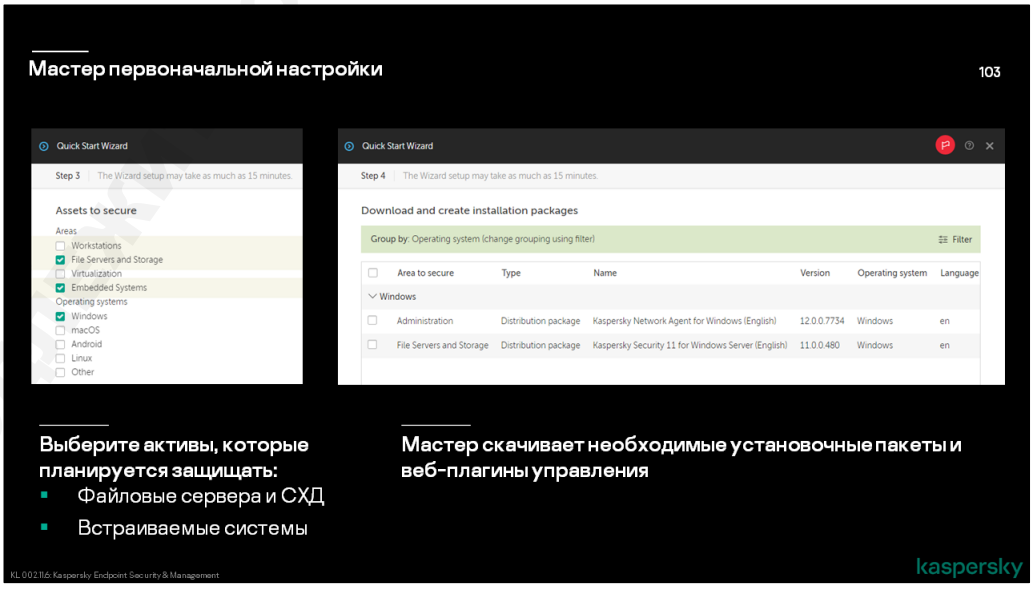
Мастер первоначальной настройки



Мы подразумеваем, что компания уже использует Kaspersky Security Center, который позволяет централизованно управлять продуктами Лаборатории Касперского, в том числе и Kaspersky Security для Windows Server.

Чтобы администратору было удобнее управлять процессом внедрения Kaspersky Security для Windows Server он может воспользоваться мастером первоначальной настройки сервера администрирования Kaspersky Security Center.

Мастер первоначальной настройки может быть использован не только для первичной настройки сервера администрирования Kaspersky Security Center, но и когда необходимо расширить список используемых программ Лаборатории Касперского.



Какие функции выполняет Мастер первоначальной настройки:

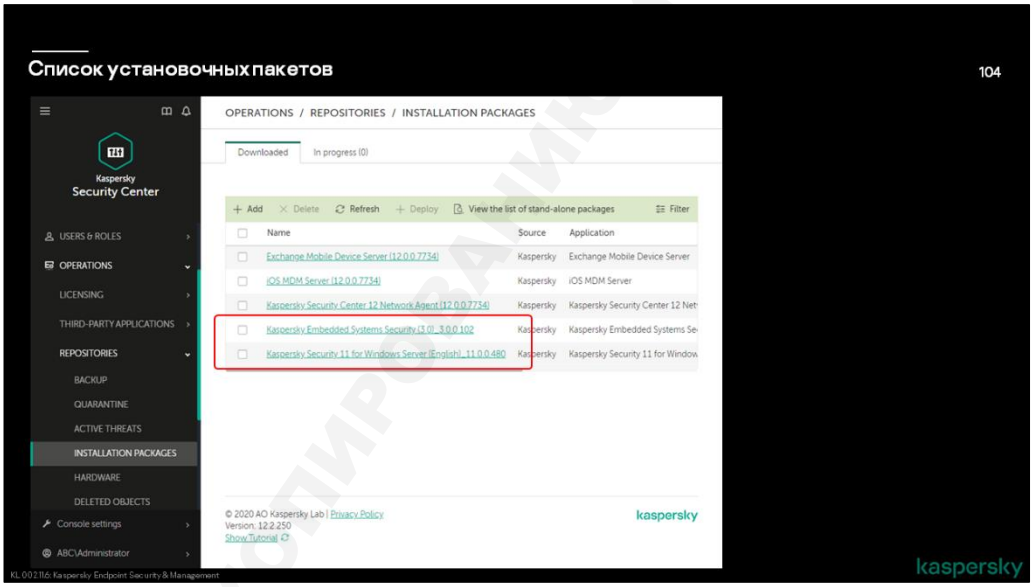
- Скачивает плагины управления
- Скачивает установочные пакеты программ Лаборатории Касперского
- Создает политики и задачи
- Загружает обновления в хранилище Сервера Администрирования

Если администратор по какой-то причине не желает использовать Мастер первоначальной настройки, то он может самостоятельно скачать дистрибутив Kaspersky Security для Windows Server можно скачать с официального сайта технической поддержки – *https://support.kaspersky.ru/ksws11#downloads*

Там же можно скачать документацию к продукту, и плагин для управления через Kaspersky Security Center. Kaspersky Security для Windows Server, и документация доступны на разных языках: English, Russian, German.

Для того чтобы запустить Мастер первоначальной настройки, надо перейти в контейнер **Обнаружение и развертывание | Хранилища | Мастер первоначальной настройки** и нажать соответствующую ссылку.

Список установочных пакетов

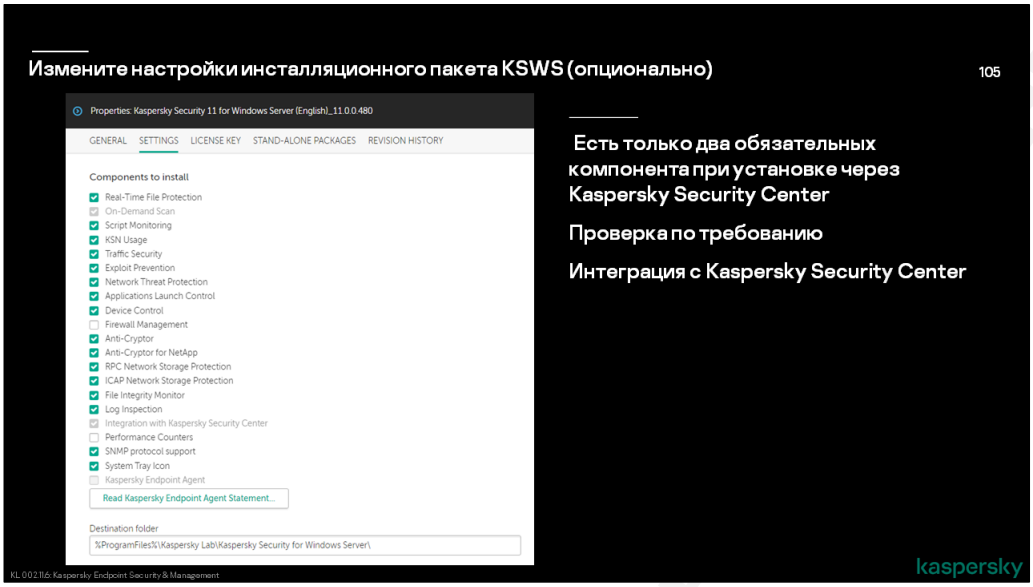


Как только Мастер первоначальной настройки завершил свою работу в Хранилище инсталляционных пакетов Kaspersky Security Center появятся установочные пакеты Kaspersky Security для Windows Server и Kaspersky Embedded Systems Security.

Список установочных пакетов можно посмотреть в контейнере **Обнаружение устройств и развертывание | Развертывание и назначение | Инсталляционные пакеты.** Здесь же администратор может просмотреть или при необходимости отредактировать свойства инсталляционного пакета.

Осталось дождаться загрузки пакета в хранилище и завершить работу мастера.

Компоненты Kaspersky Security для Windows Server



В свойствах инсталляционного пакета администратор может выбрать компоненты защиты, которые будут установлены в составе Kaspersky Security для Windows Server.

Вы всегда можете отредактировать инсталляционный пакет и добавить или удалить компоненты, которые вы не планируете устанавливать. При установке средствами Kaspersky Security Center есть только два компонента обязательных к установке: **Интеграция с Kaspersky Security Center** и **Проверка по требованию**. По умолчанию компоненты: **Проверка скриптов** и **Управление Сетевым Экраном** не устанавливаются.

На самом деле очень сложно представить ситуацию, где пришлось бы тщательно выбирать компоненты для установки. Мы рекомендуем использовать полный набор компонентов для установки, а будут ли они задействованы, чтобы обеспечивать защиту или нет, можно регулировать с помощью настроек политики.

Компоненты защиты операционной системы сервера

Под компонентами защиты операционной системы сервера мы подразумеваем защиту не только файлов и данных непосредственно операционной системы, но и защиту сервера от различных векторов современных кибер-угроз. Компоненты защиты операционной системы являются ключевыми для предотвращения компрометации: доставки вредоносного кода по сети, эксплуатации уязвимости, исполнения вредоносного кода, повышения привилегий и т.д.

- Постоянная защита файлов
- Защита от шифрования
- Защита от эксплойтов
- Защита от сетевых атак
- Мониторинг скриптов

Постоянная защита файлов защищает сервер от файловых угроз, выполняет перехват файлов при операциях запуска или чтения. Тем не менее данный компонент можно не устанавливать, если используется Контроль запуска программ и регулярно выполняется задача полной проверки, или проверки критических областей.

Защита от шифрования позволяет обнаружить активность вымогателей шифровальщиков в папках общего доступа на целевом сервере.

Защита от эксплойтов - защищает память процессов от эксплуатации уязвимостей защищает память процессов от эксплуатации уязвимостей

Защита от сетевых угроз – выполняет проверку входящего сетевого трафика на соответствие шаблонов поведений характерных для сетевых атак.

Проверка скриптов – проверяет объекты и скрипты, созданные с использованием технологий Microsoft Windows Script Technologies.

Компоненты защиты терминальных сессий

Постоянная защита файлов в рамках сеансов удалённого рабочего стола или терминальных сессий защищает от файловых угроз.

Компоненты защиты **Защита трафика** (Защита от Веб-угроз, Защита от Почтовых угроз, Веб-Контроль) перехватывают и проверяют объекты на наличие известных угроз в сетевом и почтовом трафике. Выполняют антивирусную и антифишинговую проверку.

Веб Контроль позволяет разрешать или запрещать доступ к веб-ресурсам на основе категорий, сертификатов или просто по ссылке.

Контроль сервера

Контроль запуска программ отслеживает попытки запуска программ на сервере и в зависимости от имеющихся правил разрешает или запрещает запуск

Контроль устройств Kaspersky Security для Windows Server контролирует регистрацию и использование запоминающих устройств и устройств чтения/записи CD/DVD, USB флеш накопителей или MTP-устройств в целях защиты сервера от угроз безопасности, которые могут возникнуть во время файлового обмена с внешним устройством, а также ограничить доступ к данным типам устройств.

Управление сетевым экраном предоставляет возможность настраивать параметры и передавать правила сетевого экрана операционной системы.

Контроль целостности файлов отслеживает изменения в файлах, которые могут свидетельствовать о нарушении безопасности на защищаемом сервере

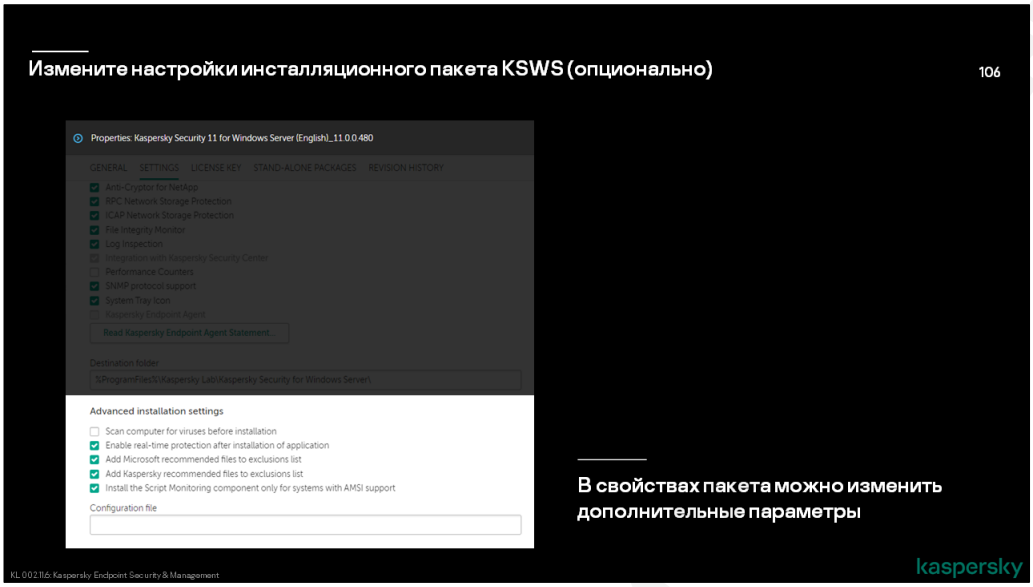
Анализ журналов контролирует целостность защищаемого сервера, выполняя поиск аномалий в журналах событий Windows

Компоненты защиты систем хранения данных

ICAP-СХД и **RPC-СХД —** аналог **постоянной защиты файлов** работает по протоколам ICAP и RPC

Защита от шифрования для NetApp выполняет защиту общих сетевых папок СХД NetApp от вредоносного шифрования

Дополнительные настройки пакета Kaspersky Security для Windows Server

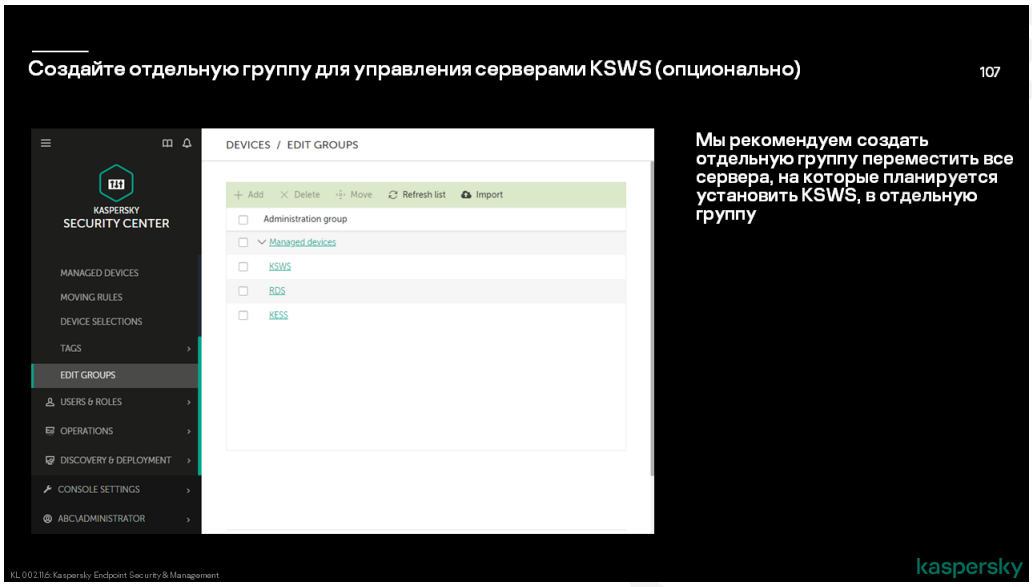


В свойствах пакета можно указать дополнительные настройки, которые будут использоваться при установке:

- **Выполнить антивирусную проверку компьютера перед началом установки** — по умолчанию данный параметр отключен, т.к. предварительное сканирование может занять дополнительное время. При включении опции, будет просканирована только системная память сервера, а не диски и их загрузочная область. Рекомендуется использовать данный параметр в случае, если сервер долгое время использовался без антивируса, был установлен антивирус стороннего производителя, или имеется подозрение на заражение компьютера.
- **Включить постоянную защиту после установки программы** — запускать или не запускать постоянную защиту файлов. Если ее запустить, она охватит все диски сервера, что может быть нежелательно. Вместо этого можно не запускать ее сразу после установки, изменить область и параметры защиты и запустить позже. По умолчанию, защита файлов запускается.
- **Добавить к исключениям файлы, рекомендуемые Microsoft** — существует ряд статей в базе знаний Microsoft с перечнем рекомендаций по настройке антивируса при работе на различных версиях Windows и совместно с различными серверными продуктами Microsoft (Exchange, Forefront TMG и пр.). Включение этой опции автоматически создает в доверенной зоне Kaspersky Security for Windows Server исключения для файлов и каталогов согласно этим рекомендациям.
- **Добавить к исключениям файлы, рекомендуемые Лабораторией Касперского** — аналогичные по назначению рекомендации есть и у Лаборатории Касперского. Они касаются совместной работы файлового антивируса и программ для защиты серверных продуктов Microsoft (Exchange, Forefront TMG и пр.). Например, рекомендуется исключать из проверки файловым антивирусом временные каталоги Kaspersky Security для Microsoft Exchange Servers.
- **Установить компонент Проверка скриптов только на системах с поддержкой технологии AMSI** позволяет Kaspersky Security для Windows Server лучше взаимодействовать с AMSI (Antimalware Scan Interface), и за счет этого повысить уровень обнаружения целого ряда атак, например, бесфайловых атак.

Данные параметры повторяют параметры установки, используемые локальным мастером установки.

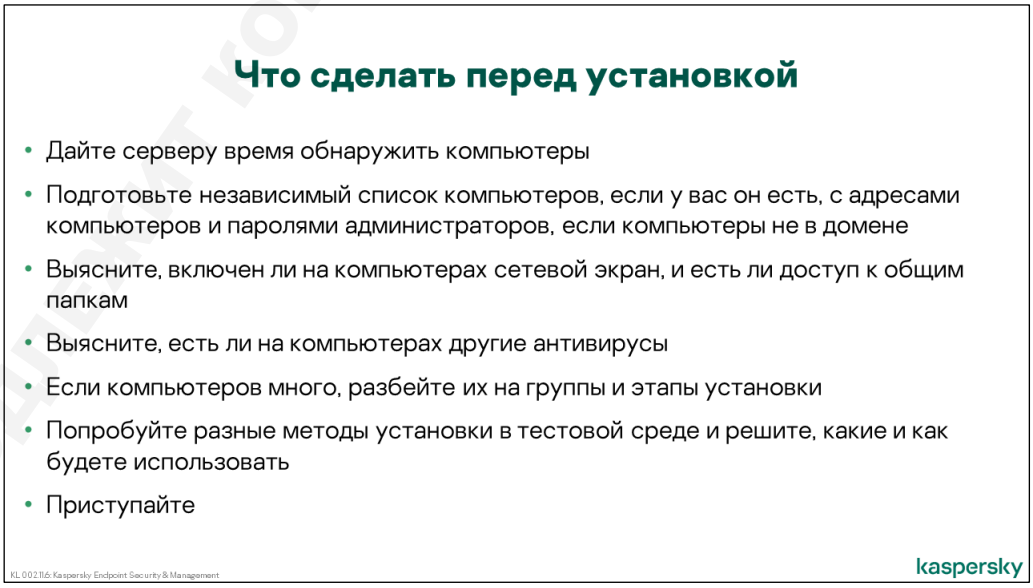
Создайте отдельную группу для управления серверами Kaspersky Security для Windows Server



Обычно с помощью Kaspersky Security Center администратор управляет разными продуктами Лаборатории Касперского или разными версиями одного продукта. Для каждого продукта в Kaspersky Security Center используются собственные политики и задачи. В таких случаях проще всего группировать компьютеры по приложению, которое используется для защиты. Поэтому заранее подготовим группу “Серверы”, в которую автоматически будут перемещаться компьютеры, на которых мы решим установить Kaspersky Security для Windows Server.

4.6 Методы установки

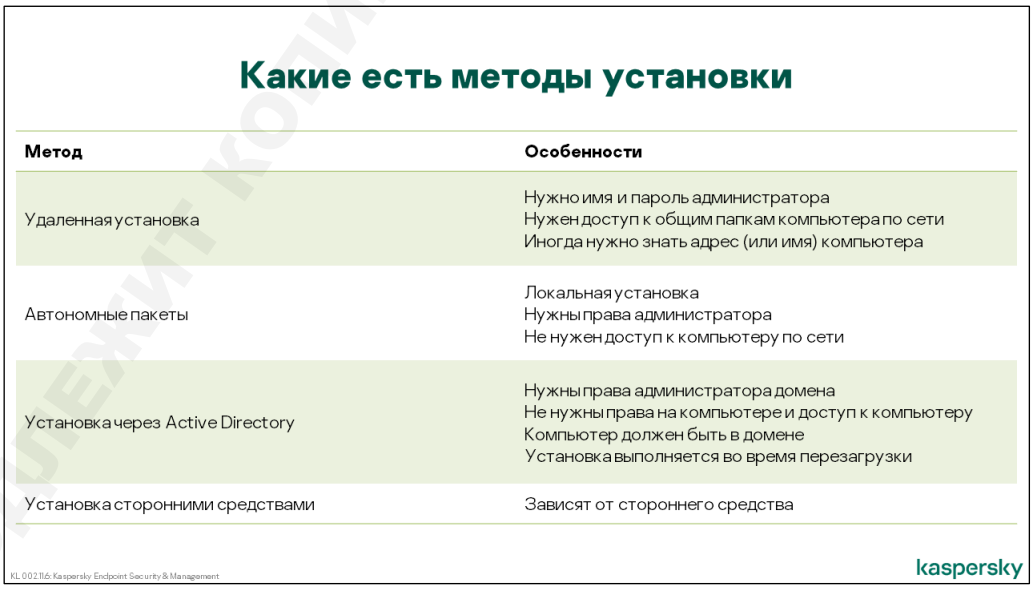
Что делать перед установкой



Перед тем, как устанавливать Kaspersky Endpoint Security на компьютеры, подготовьтесь:

Что делать	Зачем
Дайте серверу время обнаружить компьютеры	Вам не придется искать и вводить имена или адреса
Подготовьте независимый список компьютеров	Сервер может обнаружить не все компьютеры, лучше иметь под рукой эталонный список, в котором отмечать прогресс
Узнайте адреса компьютеров,	Если Сервер администрирования не обнаружил компьютер, но вы знаете его адрес, вы все равно сможете запустить удаленную установку
Узнайте имена и пароли администраторов	Если компьютеры в домене, достаточно знать пароль администратора домена На компьютерах вне домена все равно нужно знать пароль администратора и для удаленной и для локальной установки
Выясните, есть ли на компьютерах сторонние антивирусы, и какие	Kaspersky Endpoint Security может не обнаружить и не удалить сторонние антивирусы, и тогда вам придется удалить их самостоятельно
Если компьютеров много, разбейте их на этапы установки	Чем больше компьютеров, тем с большим количеством проблем вы столкнетесь, тем больше вы будете их решать, и тем дольше отдельные пользователи будут простаивать
Попробуйте разные методы установки в тестовой среде	Вы обнаружите как минимум часть из тех проблем, которые потом возникнут в сети, и сможете решить, как их быстро устранить или вообще обойти Выберите методы установки, которые создают меньше проблем
Приступайте	

Какие есть методы установки



Есть разные способы установить Kaspersky Endpoint Security, каждый со своими особенностями и преимуществами.

Удаленная установка с помощью Kaspersky Security Center	Не нужно ходить к каждому компьютеру, можно устанавливать на много компьютеров одновременно, что экономит время Установку можно начать в любой момент и начать получать результаты через считанные минуты. Но нужно знать пароль администратора на компьютерах, и нужно, чтобы общие папки компьютеров были доступны по сети. Часто сетевые экраны или настройки безопасности Windows блокируют доступ к общим папкам
Установка через Active Directory	Тоже не нужно ходить к компьютерам и можно устанавливать на много сразу. Более того, не нужен доступ к общим папкам компьютеров и пароли администратора на компьютерах. Компьютеры сами загружают и устанавливают программы. С другой стороны, компьютеры должны быть в домене и администратору нужны права в домене, чтобы опубликовать пакет. Компьютеры начинают установку не сразу, а только при следующем входе в домен, т.е. при следующей перезагрузке.
Установка сторонними средствами	Администраторы устанавливают не только Kaspersky Endpoint Security, и у них вполне могут быть сторонние средства для установки и управления программами. Особенности зависят от конкретного средства, но как правило администратор может установить программы удаленно на много компьютеров сразу.
Локальная установка из автономного пакета	Ни один из методов удаленной установки не гарантирует успех на 100% компьютеров. Компьютеры могут быть не в домене, их общие папки могут быть закрыты сетевым экраном и у администратора может не быть сторонних средств управления компьютерами. Иногда проще прийти к компьютеру и установить программу локально, чем добиться того, чтобы сработала удаленная установка. Автономные пакеты в Kaspersky Security Center экономят время при локальной установке: администратору не нужно проходить мастер установки и настраивать параметры, нужно просто запустить инсталлятор и подождать

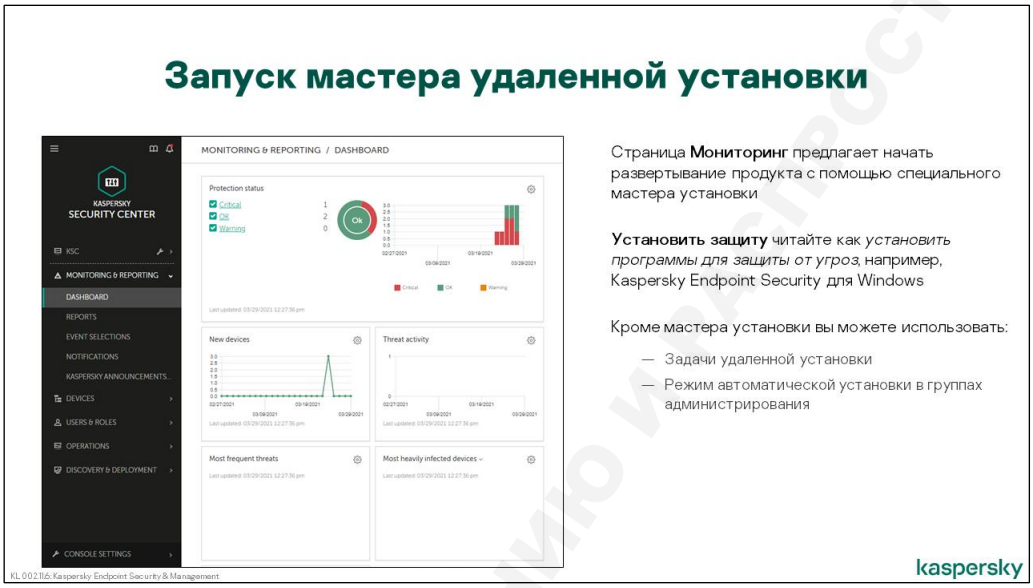
Выполняйте установку удаленно тем методом, который лучше подходит для вашей сети.

На тех компьютерах, где удаленная установка не удалась, устанавливайте локально с помощью автономных пакетов.

4.7 Как удаленно установить Агент администрирования и Kaspersky Endpoint Security

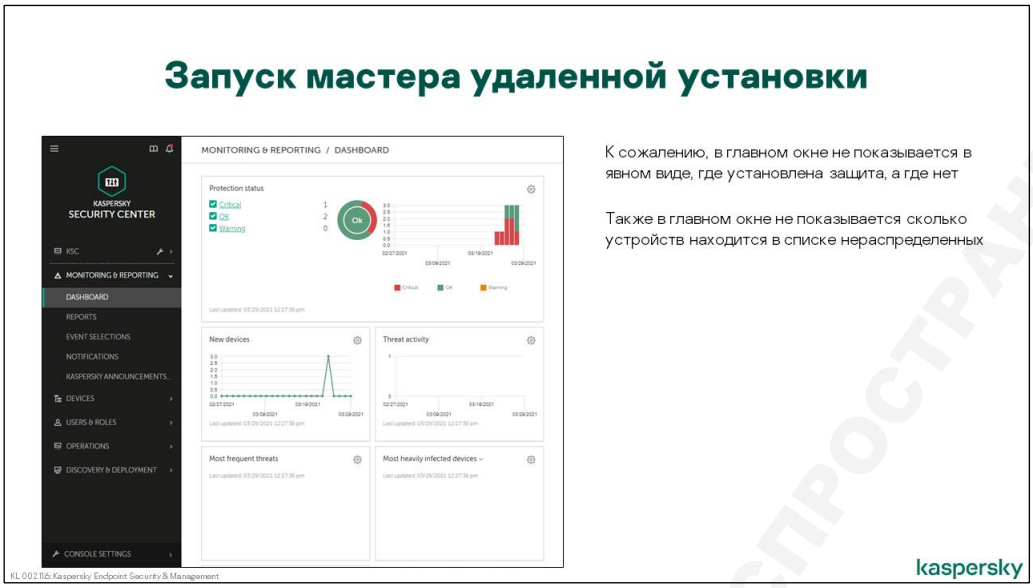
Информация на главном окне консоли управления

Web-консоль



В Kaspersky Security Center есть много способов запустить удаленную установку. Они все используют один и тот же базовый механизм. Разница между способами заключается в количестве настроек и в том, где в консоли ими можно воспользоваться. Наиболее стандартный способ, особенно для новичков, заключается в использовании общего мастера удаленной установки. Характерный сценарий его использования описан ниже.

Сервер администрирования обнаруживает в сети компьютеры, на которых не установлены средства защиты. Этот факт отображается на закладке **Мониторинг** узла Сервера администрирования в секции **Развертывание** — предупреждающим цветом индикатора и поясняющими надписями. Для исправления ситуации администратору предлагается нажать на ссылку **Установить защиту**.



К сожалению, в главном окне Web Console представлена минимальная информация по сравнению с MMC-консолью и невозможно сказать везде ли установлена защита и сколько устройств находится среди нераспределенных.

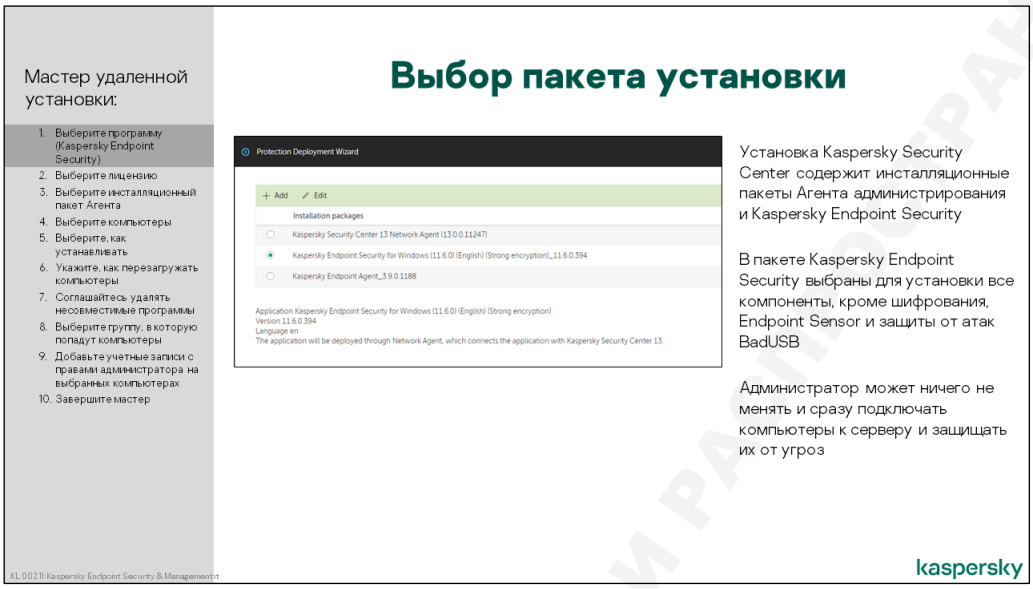
Запустить мастер удаленной установки можно разными способами:

- **Обнаружение устройств и развертывание | Развертывание и назначение | Мастер первоначальной настройки**
- Перейти на страницу **Обнаружение устройств и развертывание | Развертывание и назначение | Инсталляционные пакеты**, выбрать нужный пакет и нажать **Развернуть**
- Перейти во вкладку **Устройства | Задачи**, нажать **Добавить** и выбрать тип задачи **Удаленная установка программы**

Кроме мастера можно воспользоваться режимом автоматической установки в группах администрирования.

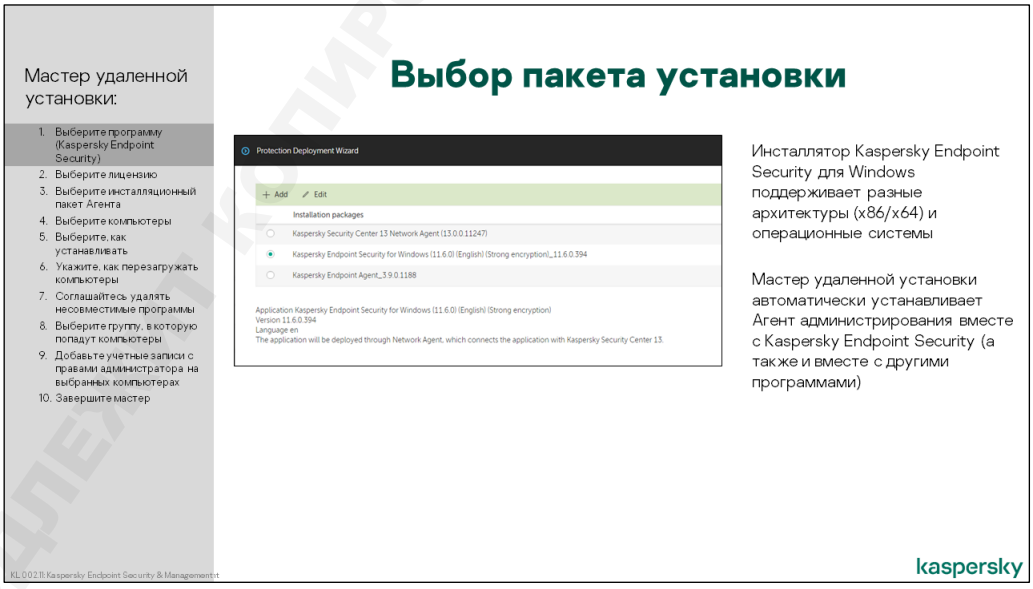
Мастер удаленной установки

Выбор пакета установки



Продукт для установки выбирается из списка доступных инсталляционных пакетов. В стандартную поставку Kaspersky Security Center входят инсталляционные пакеты текущих версий Агента администрирования и Kaspersky Endpoint Security для Windows.

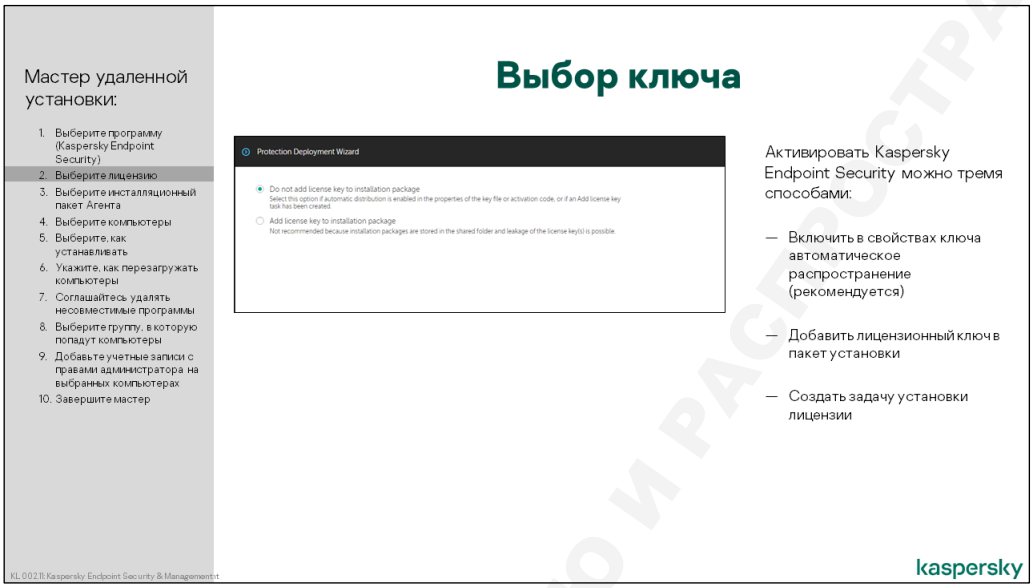
Если в мастере удаленной установки выбрать Kaspersky Endpoint Security, он будет установлен вместе с Агентом администрирования. Мастер не только устанавливает выбранный пакет, но и подключает компьютеры к Серверу администрирования путем установки на них Агента. Если компьютеры уже подключены, Агент повторно не устанавливается.



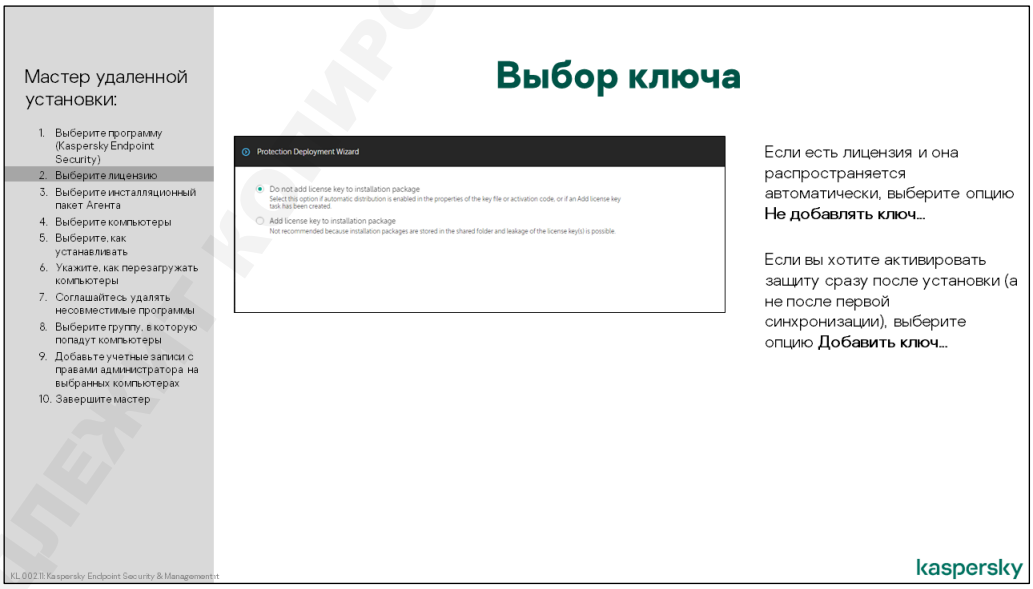
Инсталляционные пакеты Kaspersky Endpoint Security для Windows и Агента администрирования годятся для установки на любую поддерживаемую операционную систему: сервер, рабочую станцию, 32-битную или 64-битную.

Из-за этой универсальности, инсталляционный пакет Kaspersky Endpoint Security 11 имеет сравнительно большой объем: чуть меньше 200 МБ. Штатных способов уменьшить размер инсталляционного пакета не предусмотрено. Пакет Агента администрирования имеет куда меньший объем — около 40 МБ.

Добавление лицензии



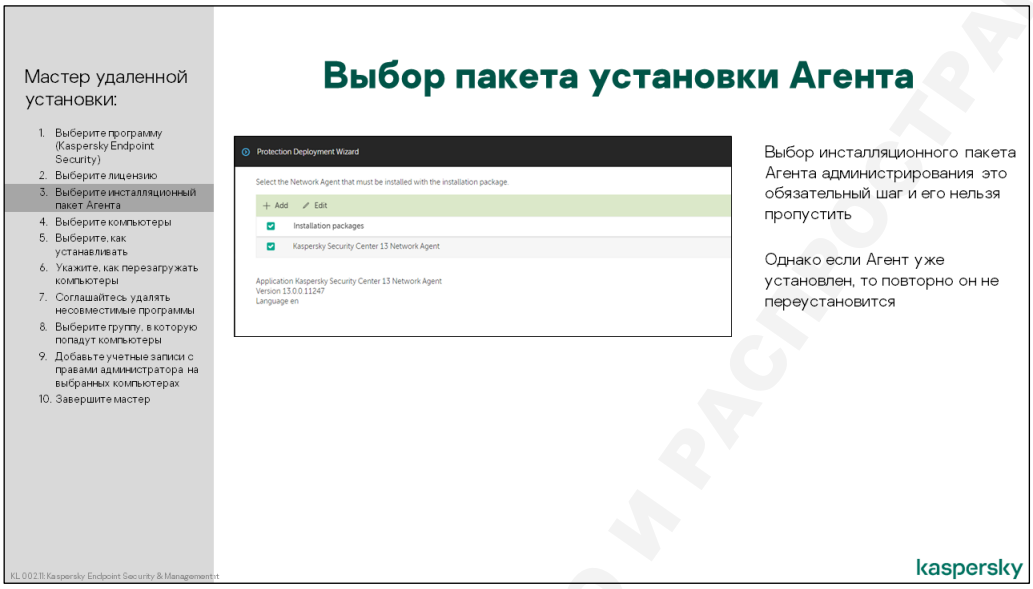
Kaspersky Endpoint Security, в отличие от Агента администрирования, для функционирования нужна активация. В мастере установки можно явно указать, какой код или ключ использовать для активации продукта. На выбор предоставляется список кодов и ключей, уже добавленных в хранилище Сервера администрирования. При необходимости этот список можно пополнить, не прекращая работу мастера.



Выбирать нужно ключ. Мастер не просто использует выбранный ключ для этой установки, но и сохранит его в свойствах пакета Kaspersky Endpoint Security. Плагин Kaspersky Endpoint Security не поддерживает коды активации в свойствах инсталляционного пакета.

Чтобы активировать Kaspersky Endpoint Security кодом, а не ключом, не выбирайте ничего в мастере установки. Вместо этого включите параметр **Автоматически распространяемый ключ** в свойствах кода активации.

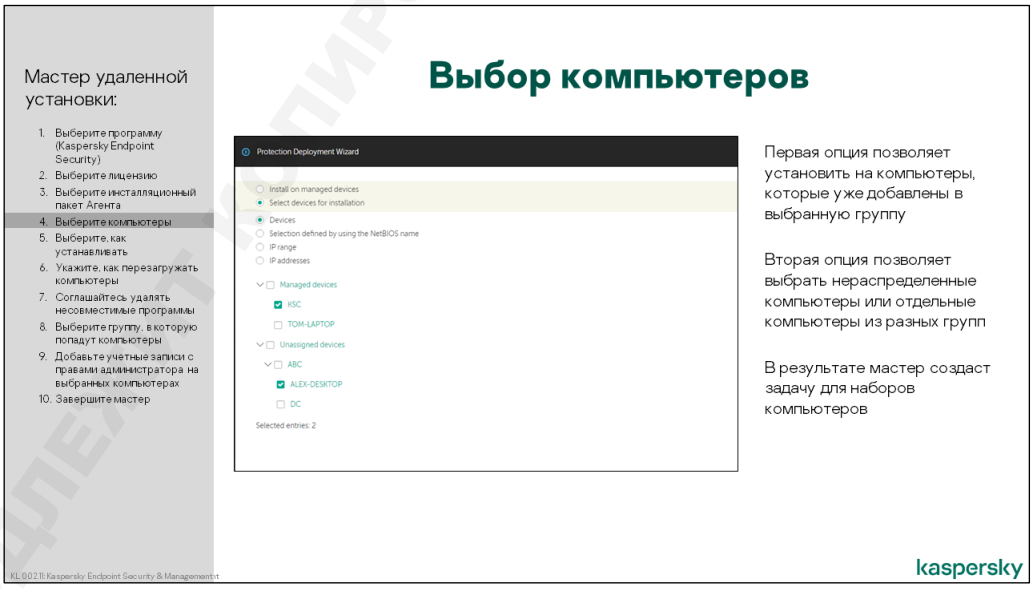
Выбор пакета установки Агента



Даже если вы хотите установить только Kaspersky Endpoint Security, мастер все равно попросит указать пакет Агента администрирования, этот шаг обязательный и пропустить его нельзя.

Однако если Агент уже установлен, то повторно он не переустановится.

Выбор компьютеров



После пакета, выберите, на какие компьютеры его устанавливать.

В мастере можно выбрать управляемые компьютеры, группы компьютеров или отдельные компьютеры.

Если вы запустили мастер сразу после того, как установили Сервер администрирования, в группах у вас есть только один компьютер — сам Сервер администрирования. Все остальные компьютеры, которые обнаружил Сервер администрирования, находятся во вкладке **Обнаружение устройств | Нераспределенные устройства**. Еще могут быть компьютеры, которые Сервер администрирования не обнаружил: их нет нигде в консоли.

Зачем тогда мастер предлагает выбирать группы, если в них нет компьютеров? Например, если перед установкой защиты вы импортировали структуру компьютеров из Active Directory. Тогда у вас уже есть группы, наполненные компьютерами, и вы можете устанавливать Kaspersky Endpoint Security по группе за раз. Как импортировать группы и компьютеры из Active Directory, читайте в Главе 4 этой части.

Вернемся к сценарию, когда у вас нет групп. Чтобы выбрать компьютеры из списка **Нераспределенные устройства** или указать адреса необнаруженных компьютеров, переключитесь на опцию **Выбор устройств для установки**.

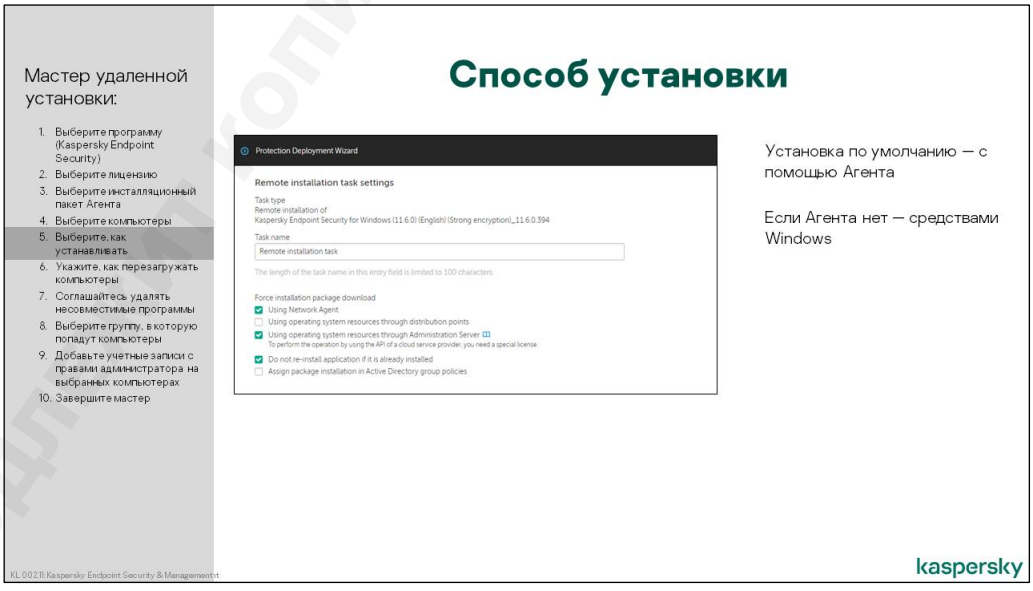
Как будет видно чуть позже, мастер удаленной установки в результате собранных сведений создает задачу удаленной установки. Если на этом шаге выбрать группу, мастер создаст групповую задачу, если выбрать компьютеры, мастер создаст задачу для наборов компьютеров.

Если выбрать опцию **Выбор устройств для установки | Устройства**, мастер показывает все обнаруженные компьютеры: и те, которые уже в группах в узле **Управляемые устройства**, и те, которые еще в узле **Нераспределенные устройства**. В узле **Нераспределенные устройства** компьютеры сгруппированы в домены и рабочие группы.

Чтобы выбрать компьютеры, поставьте возле них отметки. Если поставить отметку на группе, домене или узле верхнего уровня, вы выберете сразу все компьютере в группе, домене или узле.

Чтобы установить Kaspersky Endpoint Security на компьютеры, которые Сервер администрирования не обнаружил, их нужно добавить вручную по IP-адресу или имена компьютеров. Чтобы ввести сразу много адресов, укажите диапазон адресов.

Способ установки



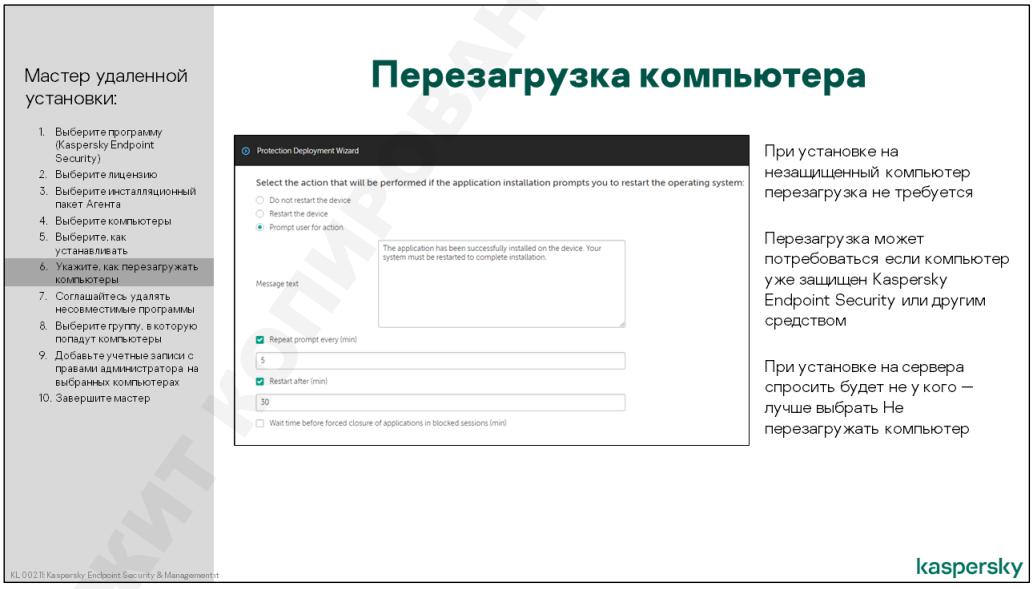
На следующем шаге мастер спрашивает, как выполнять удаленную установку. Есть два способа:

С помощью Агента администрирования	Агент администрирования уже должен быть на компьютере и должен быть подключен к этому Серверу. Сервер посылает команду Агенту, Агент загружает файлы пакетов во временную папку и выполняет установку от имени локальной системы. Имя и пароль администратора указывать не нужно, доступ к общим папкам на компьютере не нужен.
Средствами операционной системы	Нужен доступ к общим папкам компьютера по сети. Сервер администрирования копирует файлы пакетов в системную общую папку \\<*имя компьютера*>\admin$ Затем сервер использует протокол Remote Procedure Call (RPC), чтобы удаленно запустить служебный процесс, который выполнит установку и сообщит результат на Сервер. Чтобы скопировать файлы и запустить установку, нужно указать имя и пароль администратора компьютера.

Мастер всегда пытается выполнить установку с помощью Агента администрирования. Если Агент на компьютере еще не установлен, применяется установка средствами Windows.

При установке на компьютер Kaspersky Endpoint Security и Агента администрирования, мастер сначала устанавливает Агент средствами Windows, а затем устанавливает Kaspersky Endpoint Security 11 с помощью Агента.

Перезагрузка компьютера

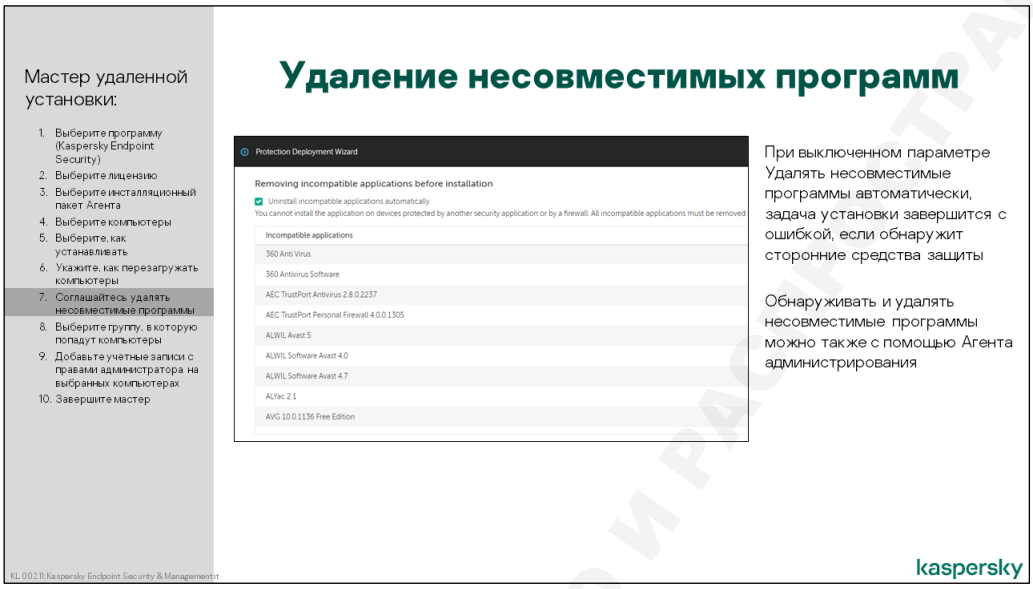


Мастер предлагает выбрать параметры перезагрузки, однако в большинстве случаев при установке Агента и Kaspersky Endpoint Security 11 перезагрузка не нужна. При установке Агента она не нужна практически никогда. При установке Kaspersky Endpoint Security необходимость в перезагрузке возникает, если на компьютере до этого была установлена другая защитная программа.

Выбор по умолчанию — **Спросить у пользователя** — годится для установки на рабочие станции. При установке на сервера лучше выбрать **Не перезагружать**. За сервером, как правило, нет пользователя, и ответить на запрос будет некому.

Чтобы пользователь не тянул с перезагрузкой, по умолчанию задача показывает предупреждение каждые 5 минут. И через 30 минут принудительно перезагружает компьютер. Администратор может изменить эти интервалы и текст предупреждения.

Удаление несовместимых программ



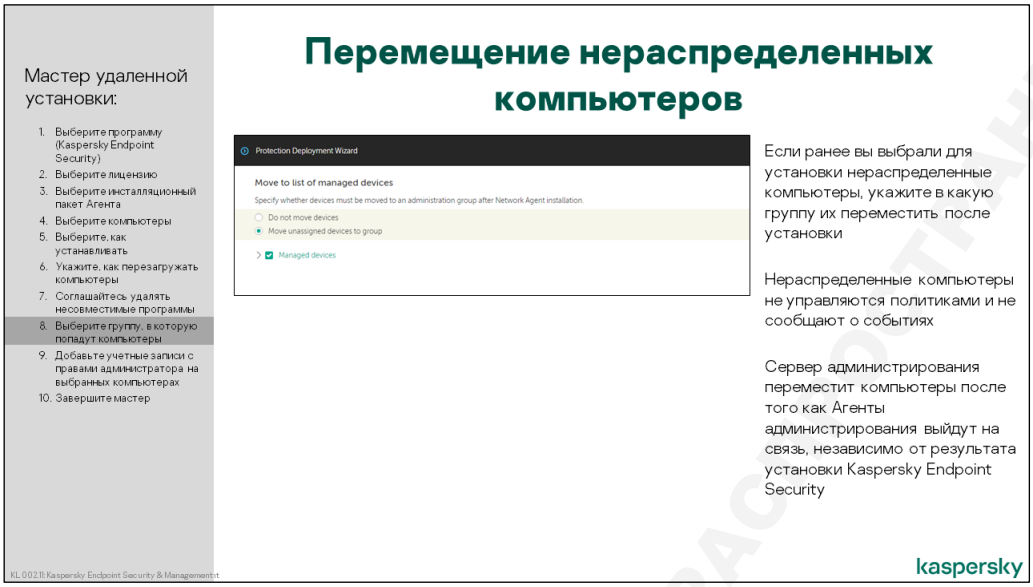
Одной из возможностей программы установки Kaspersky Endpoint Security 11 является обнаружение и удаление с компьютера несовместимых программ. Имеются в виду средства защиты — антивирусы, сетевые экраны и т.п. — совместное использование которых с Kaspersky Endpoint Security крайне не рекомендуется, т.к. может привести к серьезным проблемам в работе пользователей и компьютеров.

В общем случае администратор должен сам знать, какие потенциально несовместимые средства защиты имеются в сети, и должен заранее побеспокоиться об их удалении. Деинсталляцию рекомендуется выполнять штатными средствами соответствующих программ или средствами Windows. Возможности инсталлятора Kaspersky Endpoint Security стоит рассматривать лишь как защиту от непредвиденных ситуаций.

Обнаружение несовместимых программ отключить нельзя[5], т.к. оно призвано защитить от конфликтных ситуаций. В мастере удаленной установки можно изменить настройки удаления, но подробнее они будут рассмотрены в конце этой главы.

[5] Нельзя отключить в графическом интерфейсе. Существует параметр командной строки, который отключает обнаружение несовместимых программ, и при необходимости его можно задать в файле описания пакета удаленной установки.

Куда поместить компьютеры после установки



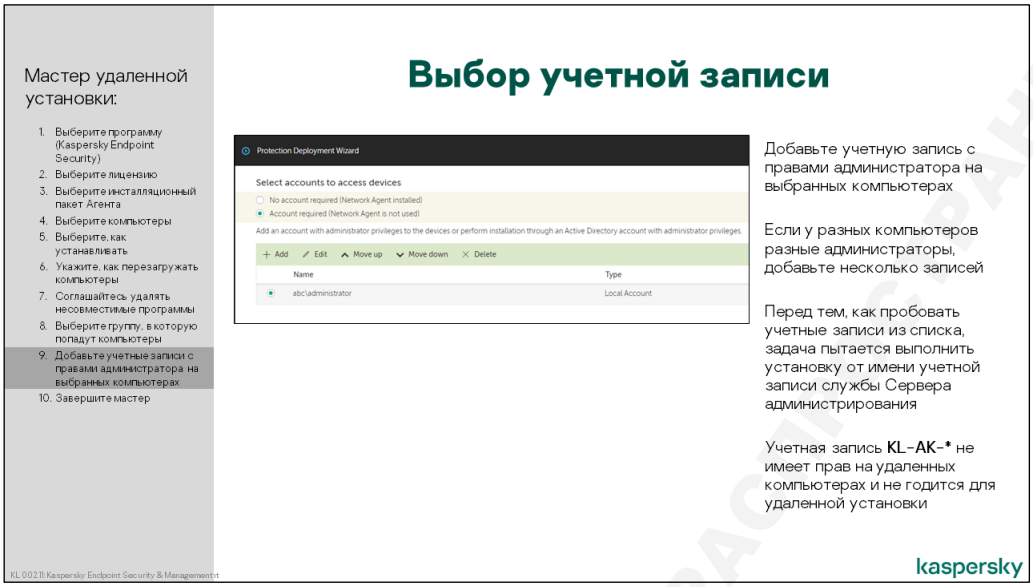
Установка Агента и средств защиты предполагает, что компьютеры после установки должны быть управляемыми: использовать настройки политик и задач с Сервера администрирования. Для этого компьютеры должны быть в списке **Управляемые устройства**, а не в списке **Нераспределенные устройства**.

Если на компьютере есть Агент администрирования, но компьютер не входит в группу администрирования, такой компьютер не пересылает свои события на Сервер администрирования, не отображается в отчетах и не использует заданные администратором централизованные настройки. Он является управляемым только номинально, но не фактически.

Если администратор выбирает компьютеры не группами, а по отдельности, мастер установки дополнительно запрашивает, нужно ли перемещать компьютеры после установки в группу администрирования, и если да, то в какую.

Выбор влияет только на нераспределенные компьютеры. Если в список установки попали и нераспределенные, и управляемые компьютеры, управляемые останутся на своих местах. Этот шаг возникает, только если совместно с Kaspersky Endpoint Security 11 выполняется установка Агента администрирования.

Учетная запись администратора

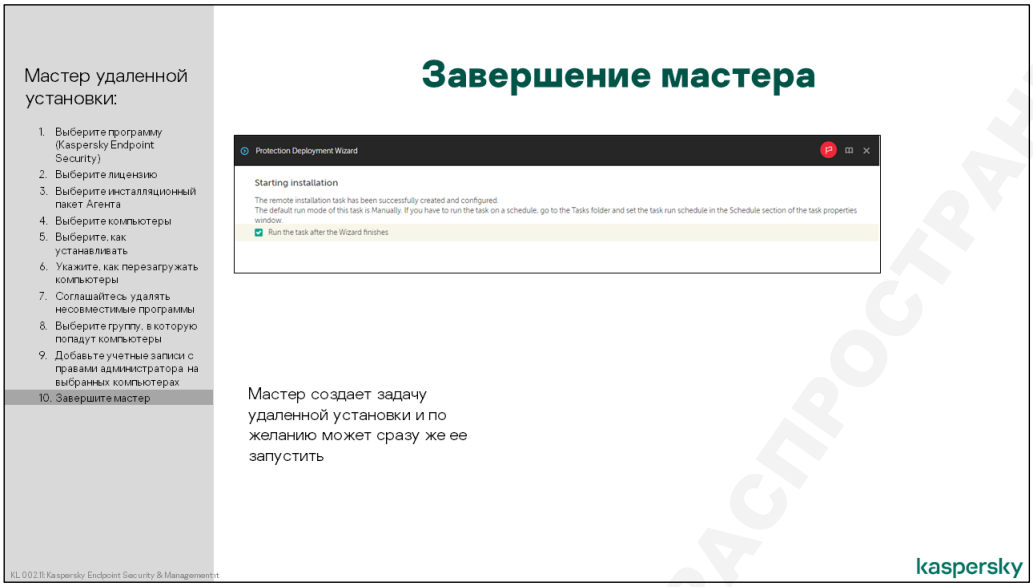


Первоначальная установка Агента выполняется средствами Windows и нуждается в учетной записи для доступа к компьютерам. Мастер установки позволяет задать несколько учетных записей, на случай если пароли администратора на компьютерах не совпадают. Попытки доступа от имени разных учетных записей выполняются в порядке перечисления. Если одна учетная запись не подходит, используется следующая и так до конца списка.

Перед использованием явно заданных учетных записей всегда выполняется попытка установки от имени учетной записи Сервера администрирования. Можно считать, что она незримо присутствует в самом начале списка. Впрочем, если при инсталляции Сервера администратор использовал настройки по умолчанию, учетная запись службы Сервера для удаленной установки не подойдет. В результате установки с настройками по умолчанию служба Сервера запускается от имени учетной записи **KL-AK-***, которая создается автоматически и наделяется правами локального администратора (не буквально, но эквивалентными). На удаленных компьютерах она прав не имеет.

Таким образом, в большинстве случаев учетную запись для доступа к компьютерам задавать нужно. В доменной среде для использования при удаленной установке удобно использовать учетную запись администратора домена. В крупных компаниях, как правило, есть специальная учетная запись для выполнения удаленной установки, либо необходимые права есть у учетных записей персонала ИТ.

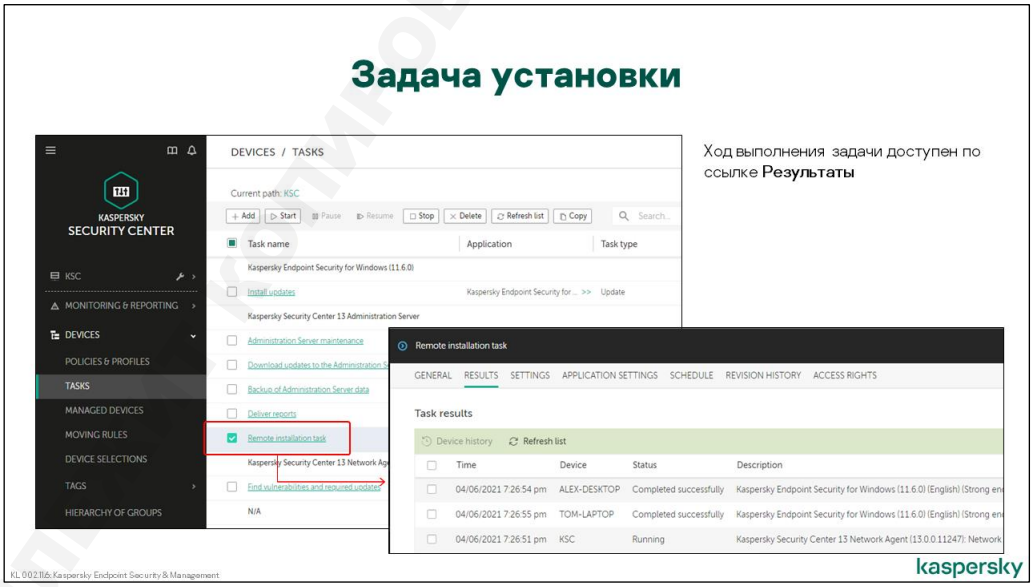
Завершение мастера



На последнем шаге мастер позволяет запустить задачу немедленно. Часто это именно то, что вы и так собираетесь сделать. Чтобы запустить задачу, включите опцию **Запустить задачу после завершения работы мастера**.

Где следить за ходом установки

Задача установки

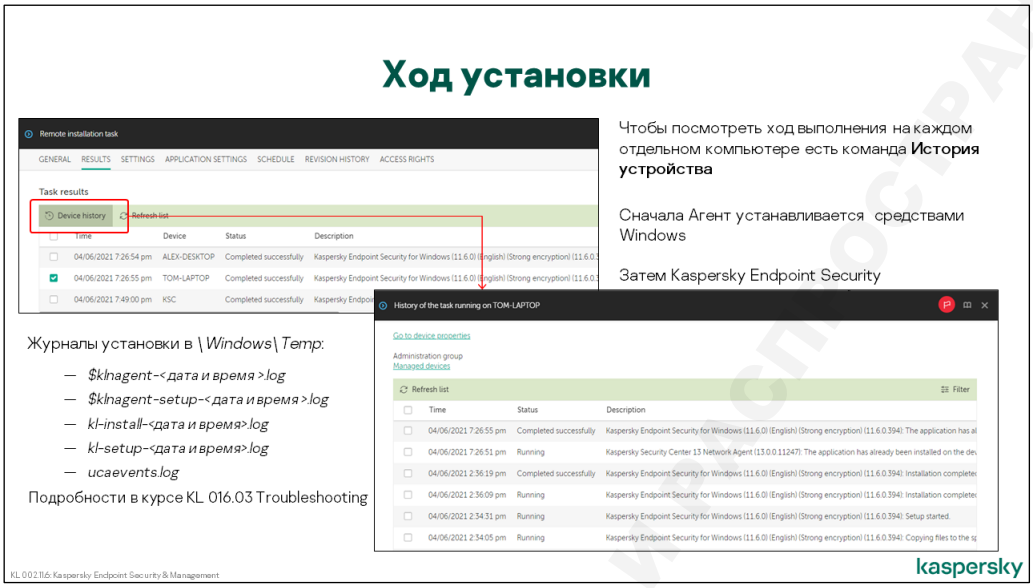


Мастер установки, исходя из заданных администратором настроек, создает и немедленно запускает задачу установки продукта на выбранные компьютеры. После чего автоматически отрывает экран задачи в Web Console.

На этом экране отображается ход выполнения задачи на выбранных компьютерах. Установка может ожидать выполнения, выполняться, ожидать перезагрузки, завершиться успешно или с

ошибкой. Количество компьютеров в каждом из состояний показывается в виде секторной диаграммы и таблицы.

Журнал задачи

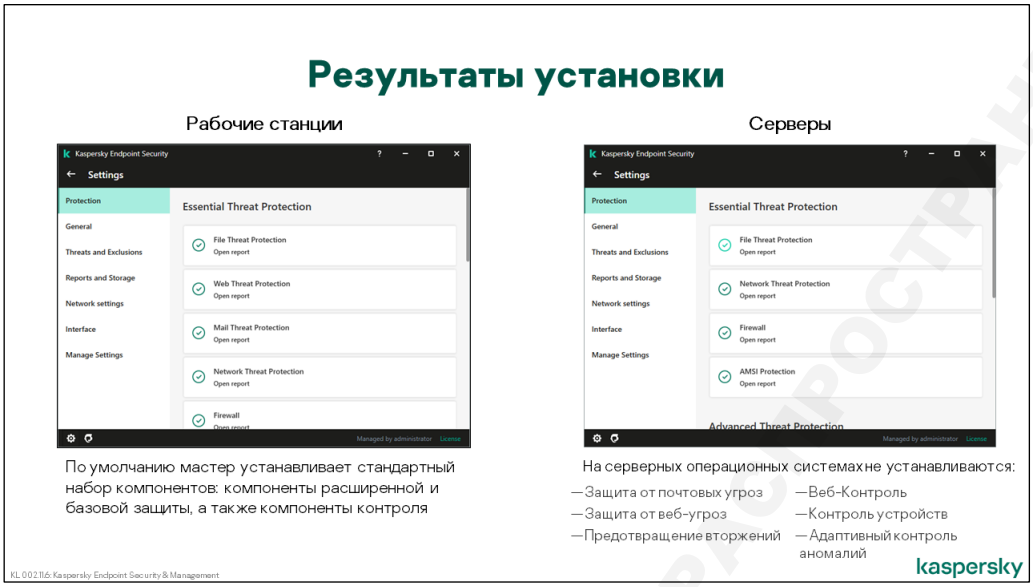


Чтобы посмотреть ход выполнения на каждом отдельном компьютере, нужно отметить компьютер и выполнить команду **История устройства**.

Журнал выполнения представляет собой историю изменения статуса задачи на компьютере. При этом общий статус может оставаться таким же, а меняться только его описание. Так в задаче установки журнал может содержать несколько записей со статусом **Выполняется**, где первая будет говорить о начале копирования файлов на удаленный компьютер, вторая о запуске программы установки, третья о выполнении установки.

Характерная история выполнения установки на отдельном компьютере показывает, что сначала устанавливается Агент, а потом Kaspersky Endpoint Security. При этом для установки Агента файлы копируются в общую папку **admin$** на компьютере, а для установки Kaspersky Endpoint Security Сервер администрирования ожидает соединения с установленным Агентом.

Результат установки



Хотя пакет Kaspersky Endpoint Security один для всех версий Windows, результаты установки на серверы и рабочие станции отличаются.

- На рабочие станции устанавливаются все компоненты, выбранные в свойствах инсталляционного пакета.
- На серверы устанавливаются только компоненты (те из них, которые выбраны в пакете):
  - Анализ поведения
  - Защита от эксплойтов
  - Откат вредоносных действий
  - Защита от файловых угроз
  - Защита от сетевых угроз
  - Сетевой экран
  - Защита от атак BadUSB
  - Поставщик AMSI-защиты
  - Контроль программ
  - Управление BitLocker
  - Endpoint Sensor

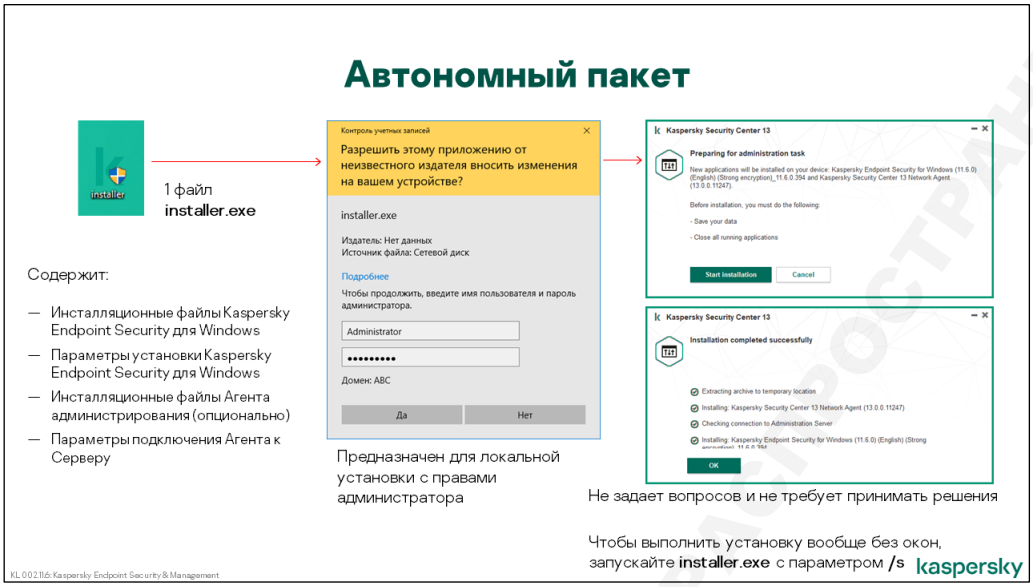
4.8 Как сделать проще локальную установку

Зачем устанавливать локально

Если на компьютеры не получается установить программы удаленно, часто проще не пытаться устранить препятствия, а прийти к компьютеру и установить программы локально. Особенно если таких компьютеров сравнительно мало.

Если устанавливать обычными программами установки, нужно проходить мастер установки. Это хоть и не слишком долго, но быстро надоедает, и легко опечататься, указывая адрес Сервера администрирования. Проще подготовить на Сервере администрирования автономный пакет со всеми настройками, и устанавливать из него.

Автономные пакеты установки



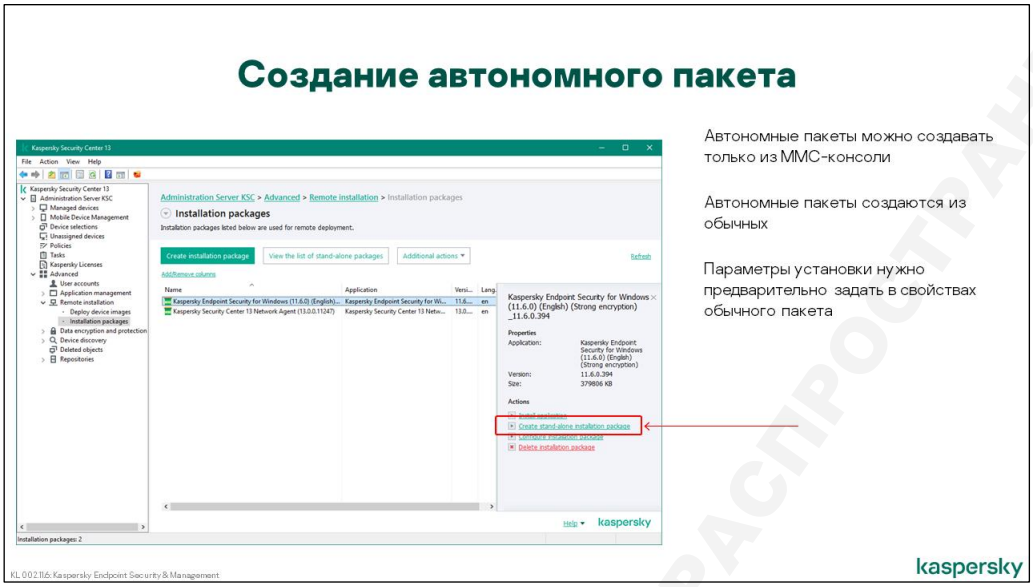
Автономный пакет в Kaspersky Security Center — это один файл *setup.exe*, который включает в себя инсталляционные файлы и параметры установки продукта, например, Kaspersky Endpoint Security. Автономный пакет может дополнительно включать инсталляционные файлы Агента администрирования и параметры соединения с Сервером администрирования.

Такой пакет предназначен для локальной установки администраторами и сотрудниками ИТ, а также пользователями, у которых есть достаточные для этого права с целью экономии времени и снижения количества ошибок.

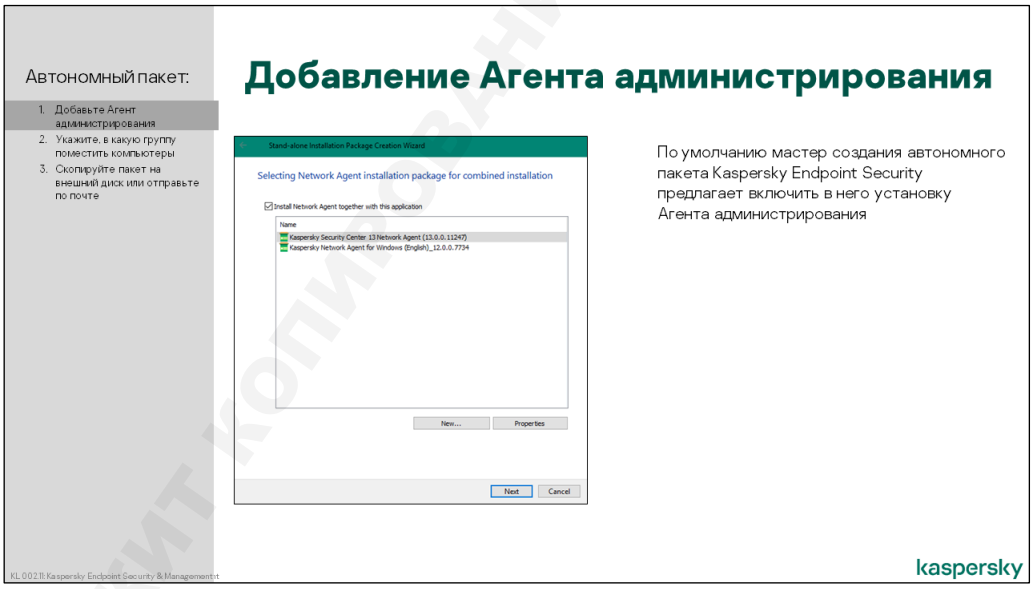
Очевидным преимуществом автономных пакетов является очень простая процедура установки. Во время установки не нужно настраивать никакие параметры, все они уже включены в пакет. Это экономит время и исключает ошибки, например, при указании адреса Сервера для подключения Агента администрирования.

Кроме того, поскольку автономный пакет — это всего лишь один файл, с ним проще обращаться, чем со стандартным дистрибутивом. Нет опасности недокопировать часть файлов, и в целом операции с ним занимают меньше времени.

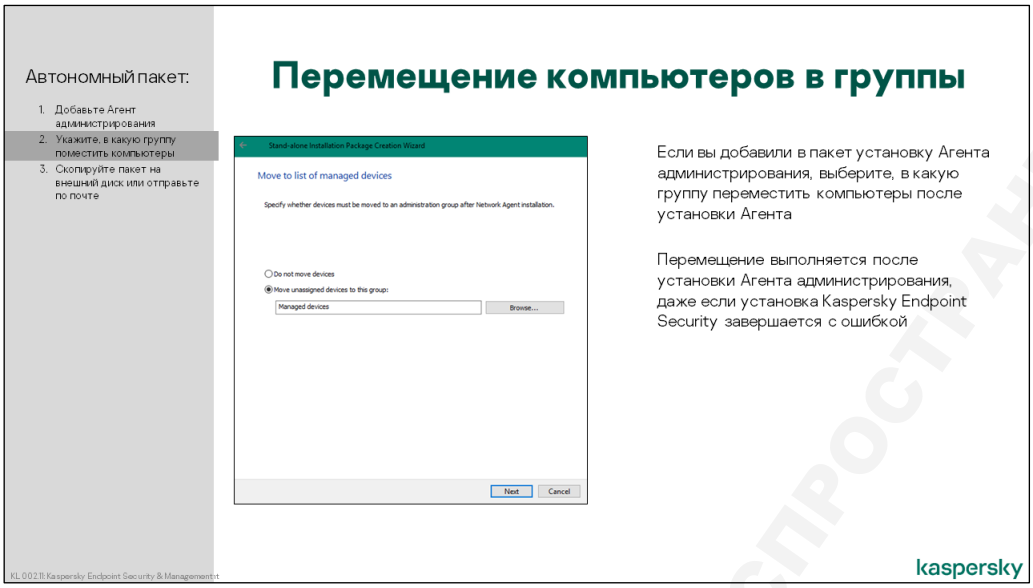
Как создать автономный пакет



Автономные пакеты можно создавать пока только в MMC-консоли. Автономные пакеты создаются из обычных инсталляционных пакетов, доступных на Сервере администрирования в контейнере **Инсталляционные пакеты**. Это делает специальный мастер, который перед созданием автономного пакета уточняет некоторые параметры установки.



Если создается автономный инсталляционный пакет Kaspersky Endpoint Security, мастер предлагает включить в пакет установку Агента администрирования, чтобы защищенный компьютер был немедленно подключен к Серверу администрирования.



Как и при удаленной установке, компьютеры после установки можно сразу переместить в категорию управляемых. Оставлять защищенные компьютеры в категории нераспределенных смысла не имеет.

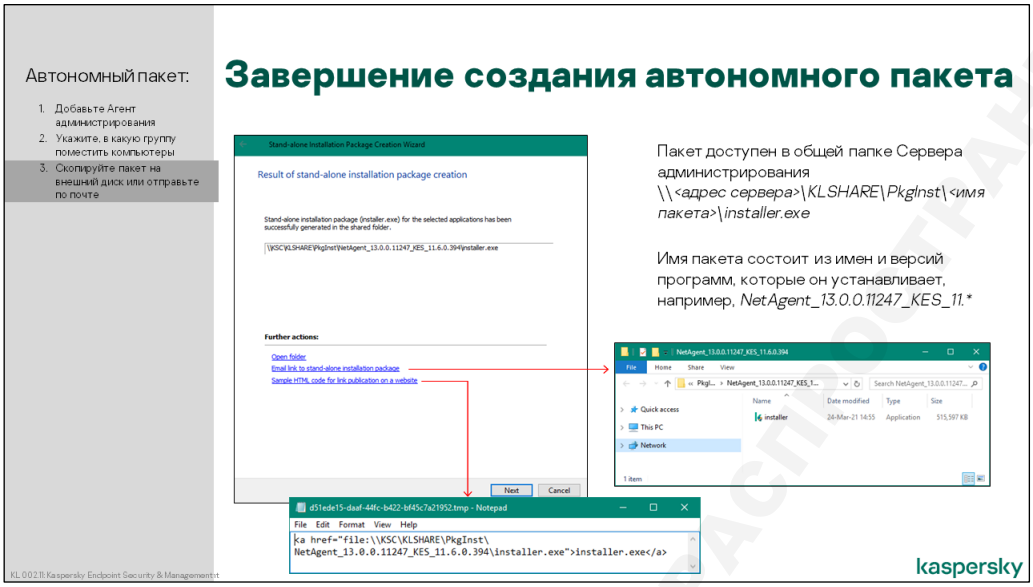
Этот шаг появляется в мастере при выборке установки Агента администрирования совместно с основным пакетом.

Если кроме указанных параметров нужно изменить исходные параметры работы Kaspersky Endpoint Security или состав устанавливаемых компонентов, это нужно сделать предварительно в свойствах обычного пакета, перед тем как запускать для него мастер создания автономного пакета установки. Параметры инсталляционных пакетов описаны раньше в этой главе.

После уточнения параметров мастер формирует файл **setup.exe**, выполняющий установку, и помещает его в специальный подкаталог *PkgInst* общей папки Сервера администрирования. Имя папки с файлом *setup.exe* совпадает с именем пакета. Позже вы легко найдете пакет по сетевому пути*: \\<имя сервера администрирования>\KLSHARE\PkgInst\<имя автономного пакета>\setup.exe*.

По умолчанию Сервер администрирования подписывает автономные пакеты своим сертификатом. Это самоподписанный сертификат и Windows при запуске пакета покажет предупреждение. Администратор может подписать пакеты своим сертификатом. Сертификат нужно указать в свойствах узла **Дополнительно | Удаленная установка | Инсталляционные пакеты**, в разделе **Подпись автономных пакетов**.

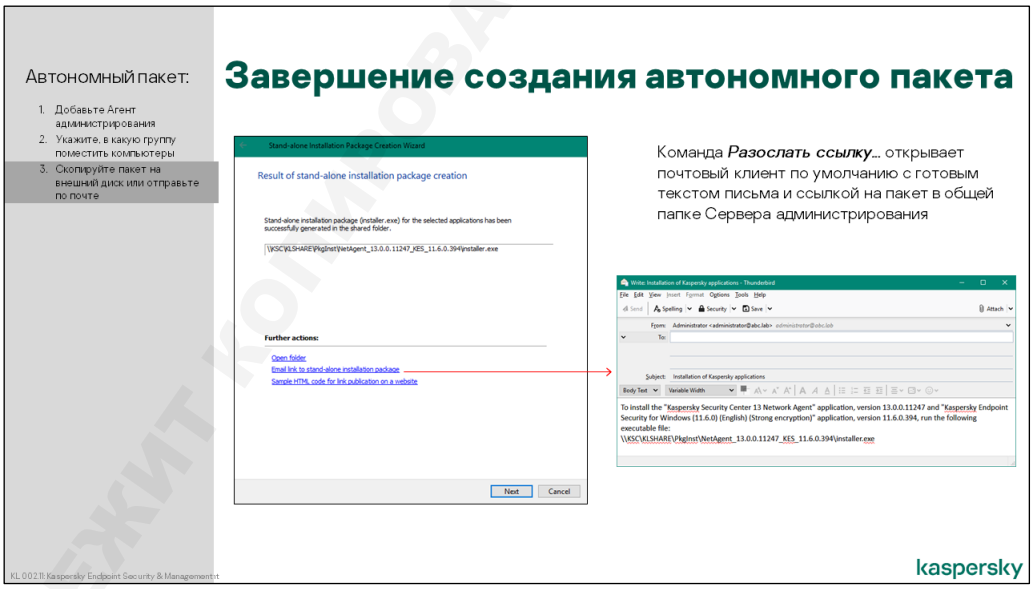
Что делать с автономными пакетами



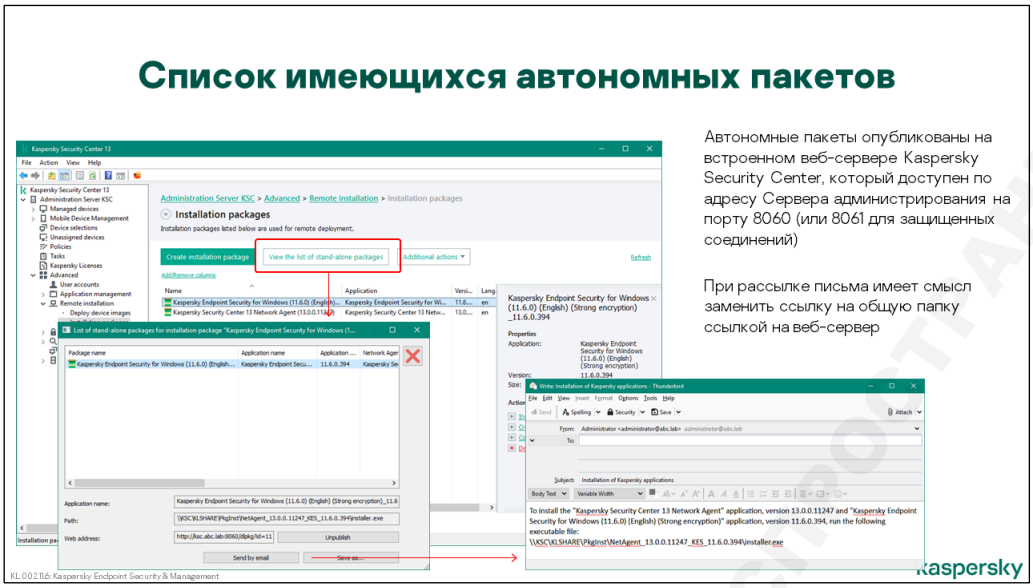
При этом администратору предлагается три варианта дальнейших действий:

— **Открыть папку** — например, чтобы скопировать на Flash-накопитель

— **Пример HTML-кода для размещения ссылки на веб-сайте** — открывается текстовое окно с фрагментом HTML-кода, который можно добавить на веб-страницу, чтобы на ней отображалась ссылка на пакет



— **Разослать ссылку на автономный пакет установки по электронной почте** — Сервер администрирования запускает почтовый клиент по умолчанию и автоматически формирует тему и текст приглашения со ссылкой на расположение пакета в общей папке, адреса получателей администратору нужно заполнить самостоятельно



Впоследствии список созданных автономных пакетов можно открыть по кнопке **Просмотреть список автономных пакетов** на странице узла **Инсталляционные пакеты**. В окне списка можно удалить ненужные пакеты или повторить рассылку письма пользователям.

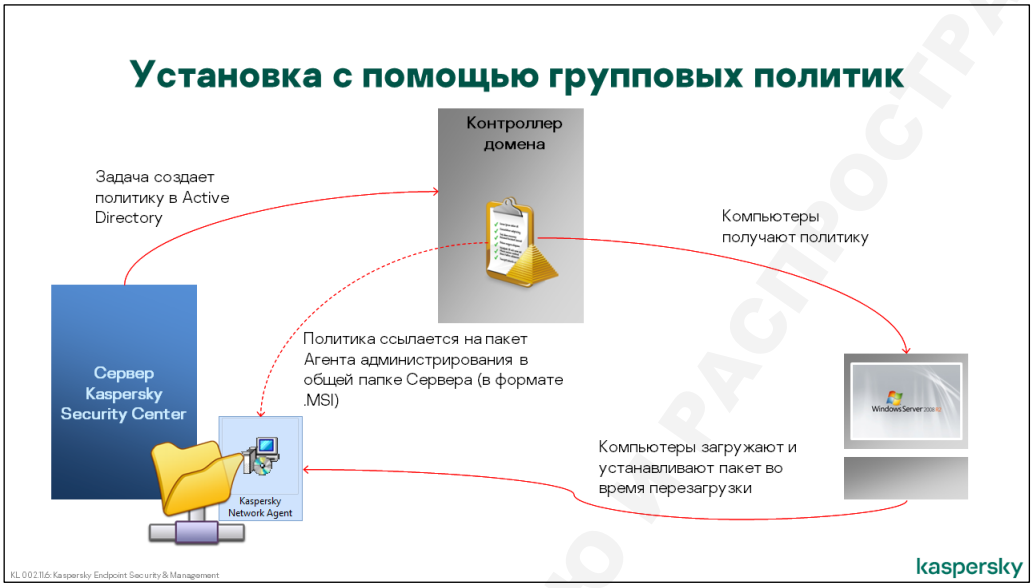
Предлагаемая мастером создания пакета ссылка для отправки по почте содержит путь к сетевой папке Сервера администрирования. Если по ссылке попытается пойти пользователь, не входящий в домен и не зарегистрированный на Сервере администрирования, он может не получить доступа.

Вместо ссылки на сетевую папку лучше использовать http-ссылку на пакет, которую можно скопировать из свойств пакета. На Сервере администрирования имеется встроенный веб-сервер, через который любой пользователь может загрузить пакет. Каждый автономный пакет получает уникальную ссылку, основанную на идентификаторе пакета. Администратор может найти эту ссылку в свойствах пакета в общем списке автономных пакетов.

При повторном запуске мастера создания автономного пакета из обычного пакета, для которого автономный пакет ранее уже создавался, у администратора есть выбор: пересоздать автономный пакет или создать отдельный новый автономный пакет.

4.9 Как установить Агент администрирования через Active Directory

Как устанавливать программы через Active Directory

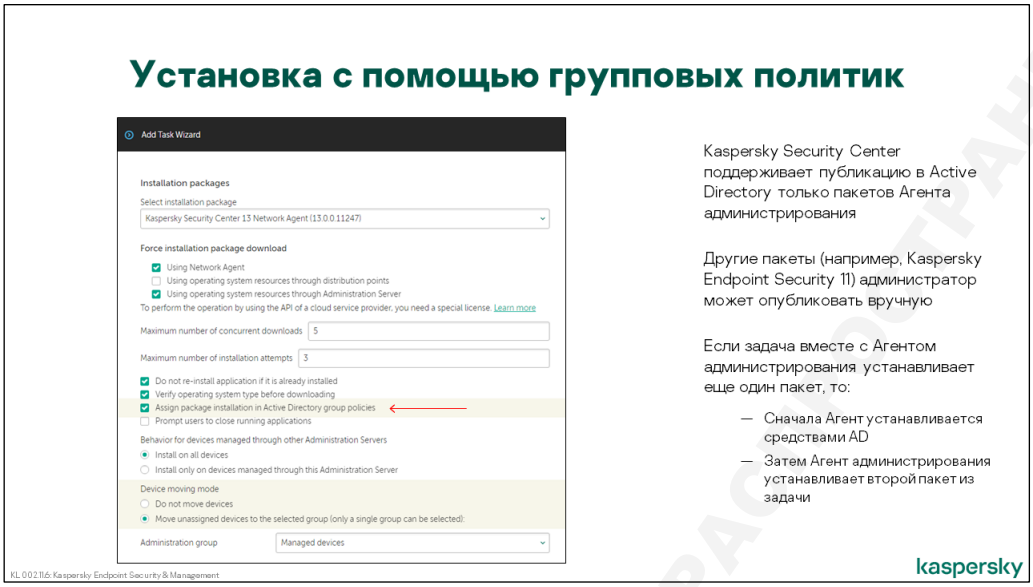


Устанавливать программы с помощью групповых политик Active Directory можно и без Kaspersky Security Center.

Принцип заключается в следующем. Инсталляционный пакет продукта в формате Microsoft Installer (.msi) помещается в общую папку, доступную для чтения компьютерам домена. Размещенный пакет регистрируется в разделе установки в групповой политике Active Directory, которая распространяется на доменные компьютеры. При следующем входе в домен, компьютеры в соответствии с политикой загружают инсталляционный пакет из общей папки и выполняют его установку еще до входа пользователя в систему.

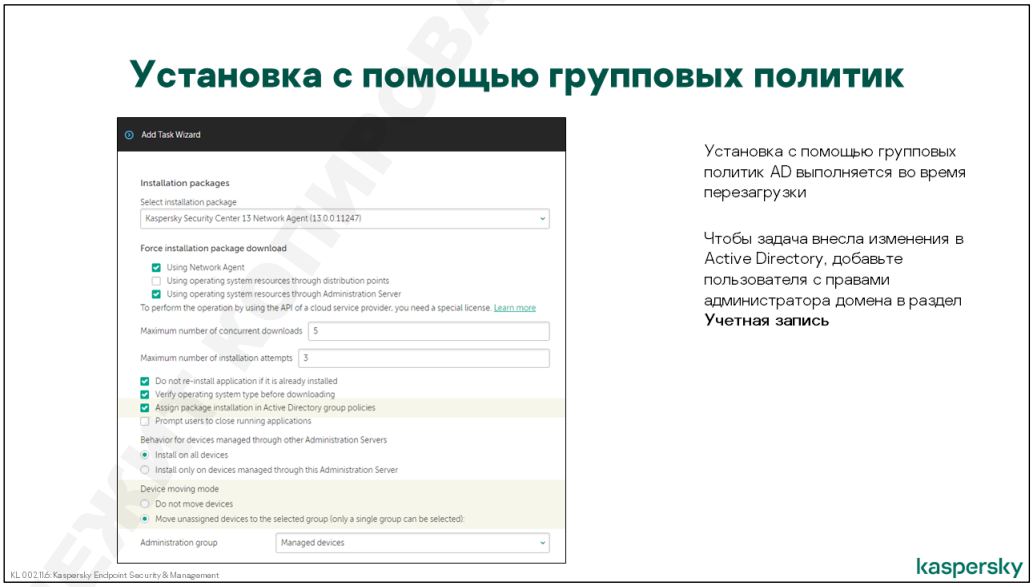
Этот метод сравнительно несложно осуществить вручную. Тем не менее, через Kaspersky Security Center его использовать удобнее.

Как задачей опубликовать пакет Агента в Active Directory



Чтобы опубликовать пакет Агента администрирования в групповой политике домена, включите в задаче (или в мастере установки) опцию **Назначить установку Агента администрирования в групповых политиках Active Directory**.

Метод распространяется только на Агент администрирования, поскольку считается, что после установки Агента, остальные программы будут инсталлироваться с помощью Агента, а не другими методами.

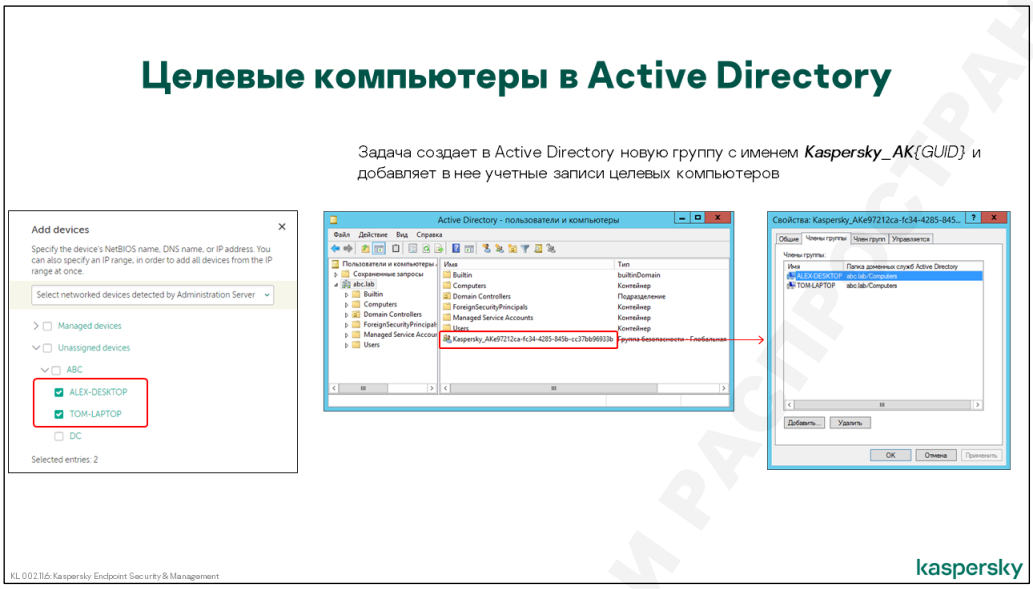


Установка с помощью групповых политик AD выполняется во время перезагрузки

Также не стоит забывать, чтобы задача завершилась успешно, запускайте ее с правами администратора домена. Для этого добавьте учетную запись администратора домена в раздел **Учетная запись** в настройках задачи.

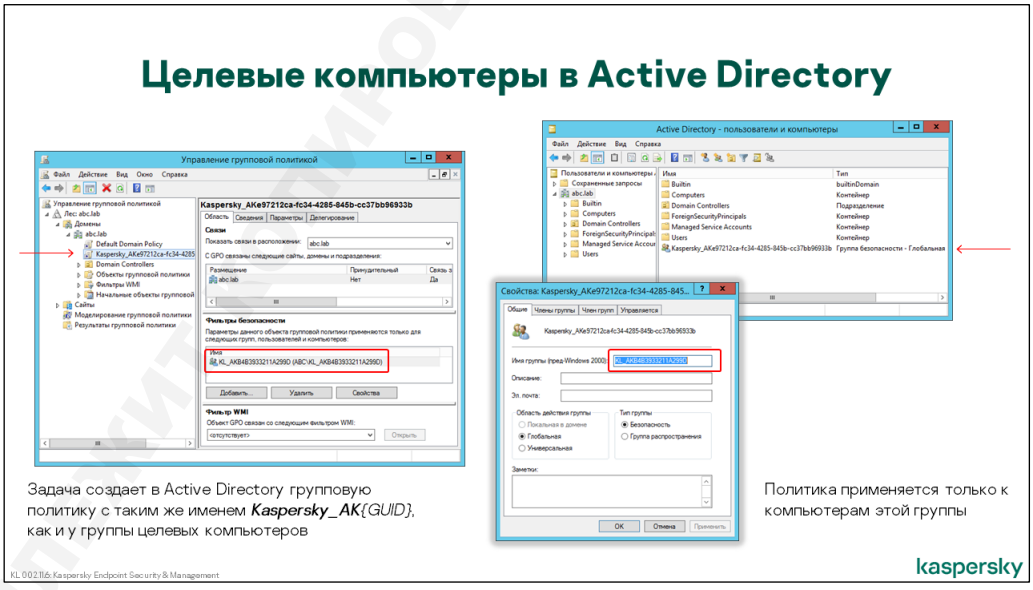
Что задача меняет в Active Directory

Группа целевых компьютеров



Результат у включения опции следующий. Сервер администрирования создает в Active Directory новую группу с именем **Kaspersky_AK***{GUID}* и включает в нее учетные записи компьютеров, на которые распространяется задача.

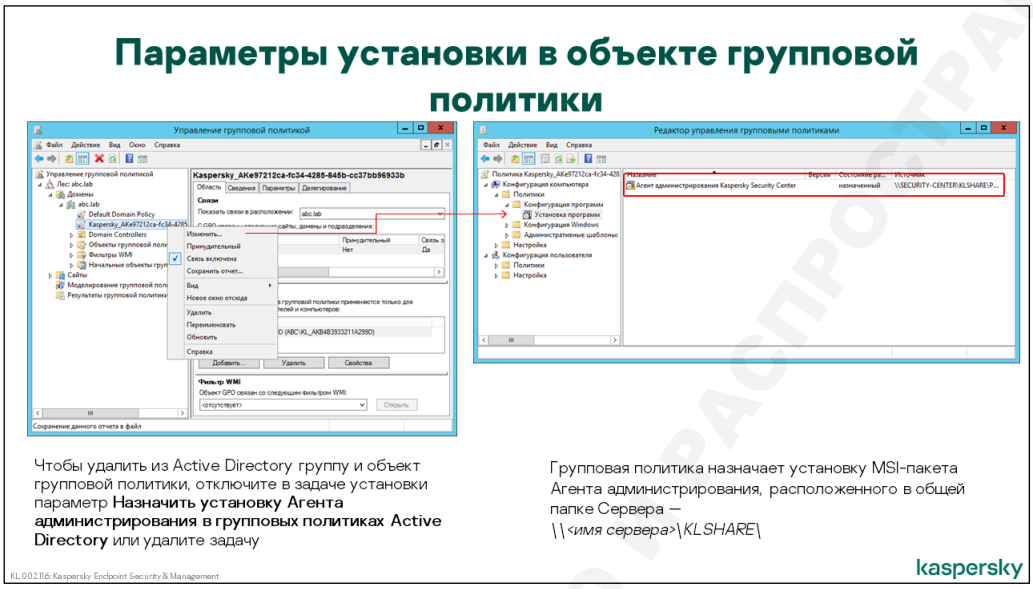
Объект групповой политики



Сервер администрирования также создает в Active Directory новый объект групповой политики уровня домена с именем **Kaspersky_AK***{тот же GUID}* и назначает в нем установку MSI-пакета Агента администрирования, расположенного в общей папке Сервера.

Право применения политики дается только ранее созданной группе с учетными записями целевых компьютеров задачи. Таким образом, политика уровня домена будет применена не на всех компьютерах домена, а только на выбранных компьютерах.

Параметры объекта групповой политики



После этого установка выполняется в стандартном ключе. Политика со временем распространяется на компьютеры. При очередной перезагрузке компьютеры загружают MSI-пакет Агента администрирования из общей папки Сервера администрирования и устанавливают его. Параметры установки, среди которых находится адрес и порты Сервера, берутся из файла ответов, который находится рядом с MSI-пакетом. Таким образом, компьютеры автоматически подключаются к Серверу администрирования.

Если в задаче установки был выбран не только Агент, но и другая программа, например, Kaspersky Endpoint Security, установка продолжится после первого подключения Агента к Серверу.

Созданные задачей группа безопасности и объект групповой политики остаются в Active Directory до тех пор, пока либо задача не будет удалена из Kaspersky Security Center, либо не будет отключена опция **Назначить установку Агента администрирования в групповых политиках Active Directory** в свойствах задачи.

4.10 Как удалять несовместимые программы

Какие программы несовместимые и зачем их удалять

Kaspersky Endpoint Security несовместим с другими средствами защиты. Перед его установкой конфликтующие программы нужно удалить. Если этого не сделать, компьютер может работать медленно и нестабильно. В худших, хотя и редких случаях, компьютер может зависать, спонтанно перегружаться и показывать синий экран.

Средства защиты плохо работают вместе из-за драйверов, которые они устанавливают, чтобы перехватывать операции с файлами, сетевые соединения и системные вызовы. Агент администрирования никаких драйверов не устанавливает, поэтому со сторонними средствами защиты не конфликтует.

Как удалять несовместимые программы

Чтобы удалить сторонние средства защиты, лучше использовать штатные средства:

— Программы со своей системой централизованного управления удаляйте через эту систему
— Если это приемлемо, удаляйте сторонние средства защиты средствами Windows

Если удалить несовместимые программы штатными средствами не удается, у администратора есть два способа сделать это с помощью Kaspersky Security Center:

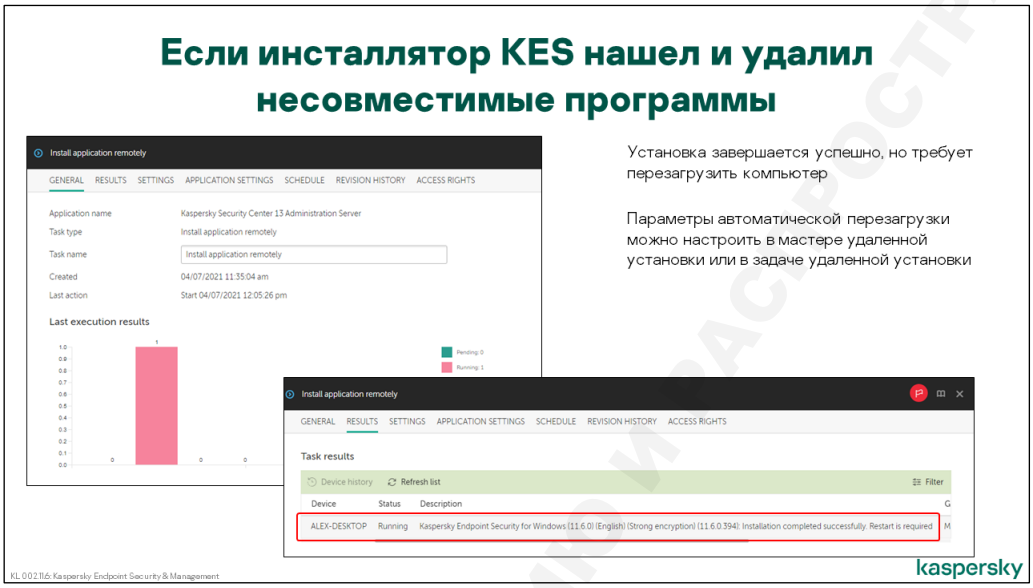
— Воспользоваться опцией **Удалять несовместимые программы автоматически** в пакете установки Kaspersky Endpoint Security
— Использовать задачу Агента администрирования: **Удаленная деинсталляция программы**

Опция в инсталляционном пакете включена всегда и надежно удаляет многие распространенные версии сторонних антивирусов и сетевых экранов. Но если у вас не слишком распространенный сторонний антивирус или свежая версия стороннего антивируса, инсталлятор Kaspersky Endpoint Security может его пропустить.

Кроме этого, некоторые несовместимые программы инсталлятор может обнаружить, но не может удалить.

Что бывает, если есть несовместимые программы

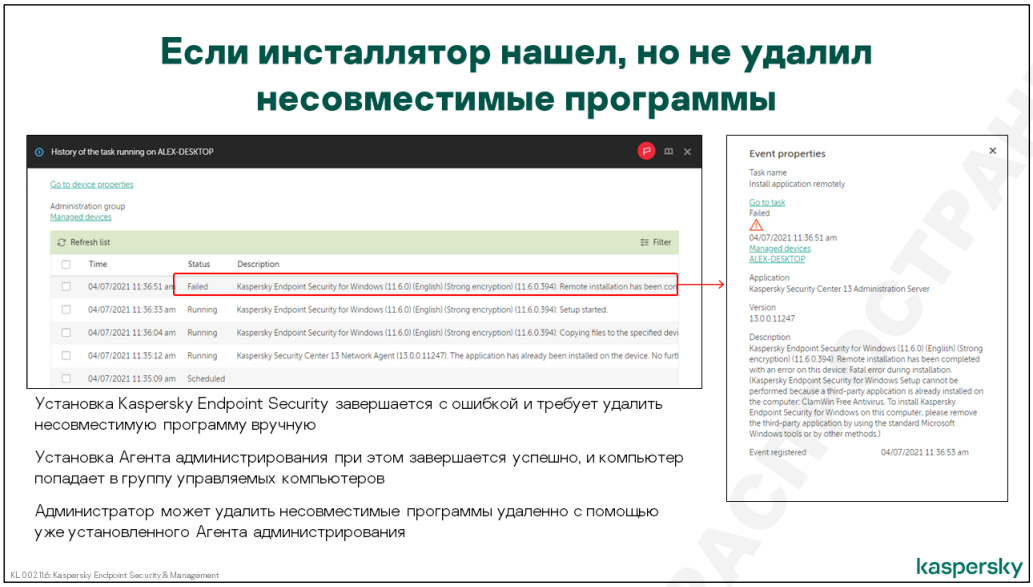
Kaspersky Endpoint Security обнаружил и удалил несовместимые программы



Если инсталлятор обнаружил и удалил несовместимые программы, он потребует перезагрузить компьютер, чтобы завершить установку Kaspersky Endpoint Security. Это единственное отличие от обычной установки. Если на компьютере не было несовместимых программ, инсталлятор все установит без перезагрузки.

Специально для таких ситуаций в задаче установки есть параметры перезагрузки. По умолчанию задача будет показывать пользователю сообщение, что нужно перезагрузить компьютер, каждые 5 минут, и принудительно перезагрузит компьютер через 30 минут. Все эти интервалы администратор может поменять в свойствах задачи удаленной установки.

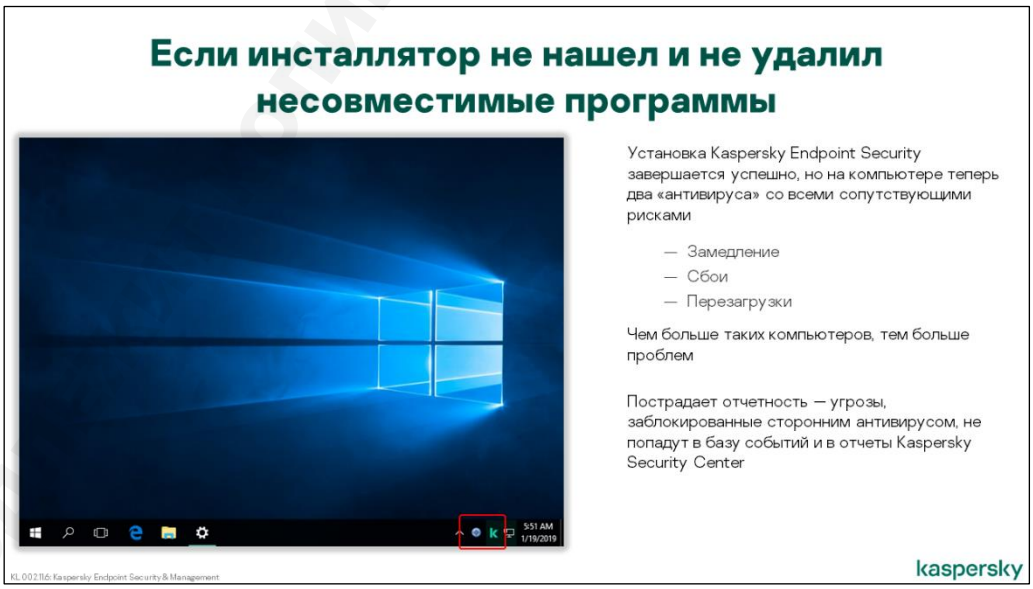
Kaspersky Endpoint Security обнаружил, но не удалил несовместимые программы



Если при отключенном удалении в ходе установки Kaspersky Endpoint Security 11.6 обнаруживается несовместимая программа, инсталлятор завершается с ошибкой. В описании ошибки сказано, что установка невозможна, пока на компьютере присутствуют несовместимые программы. Администратору предлагается удалить конфликтующие программы и повторить попытку установки.

Если это задача, которая устанавливает Kaspersky Endpoint Security вместе с Агентом администрирования, она установит Агент администрирования и только потом сообщит об ошибке. Это удобно, потому что позволит использовать Агент, чтобы удалить несовместимую программу специальной задачей.

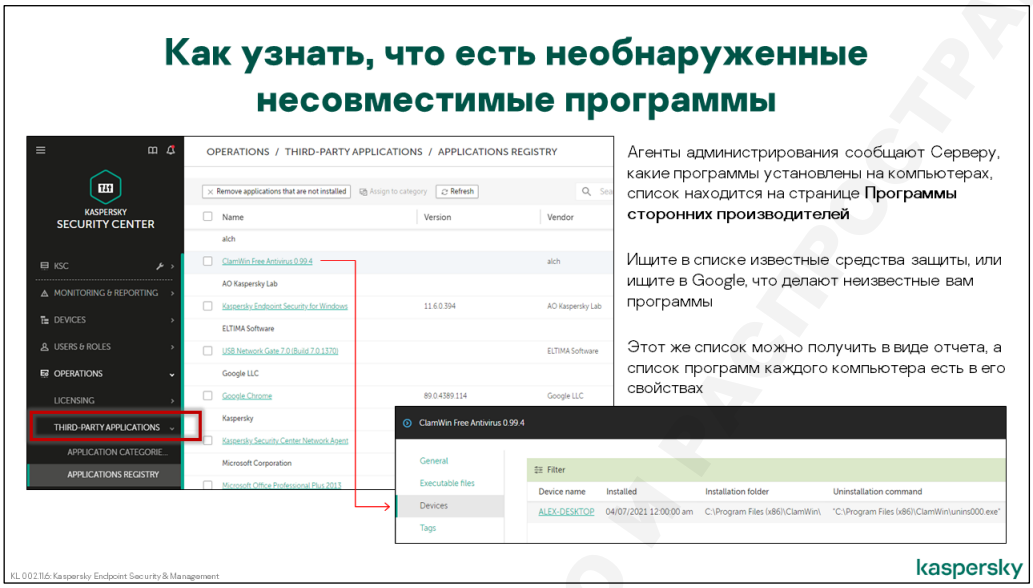
Kaspersky Endpoint Security не обнаружил несовместимые программы



Если на компьютере есть несовместимые программы, но инсталлятор их не нашел, он завершит установку так, как будто их нет. В этом случае администратор может не сразу узнать о том, что

есть конфликт. Рано или поздно пользователи начнут жаловаться на то, что компьютер работает медленно или со сбоями. Выясняя в чем дело, администратор обнаружит, что на компьютере несколько средств защиты.

Как узнать, что есть несовместимые программы



Узнать о том, что на компьютерах есть сторонние средства зашиты, администратор может из консоли администрирования. Агенты администрирования посылают на Сервер списки установленных программ, и обобщенный список находится в Web Console на вкладке **Операции | Программы сторонних производителей | Реестр программ**.

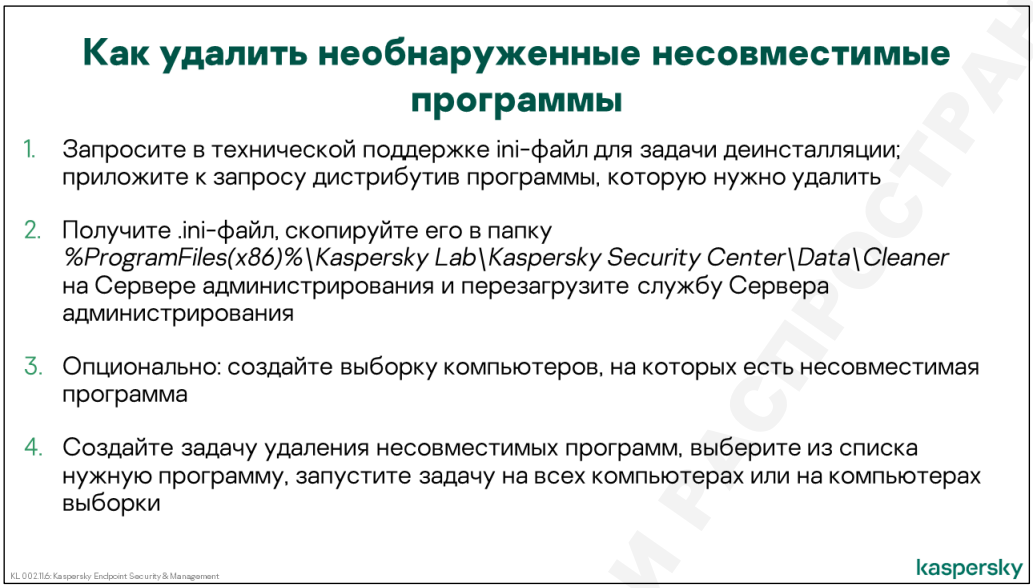
Если администратор подозревает, что в сети могут быть средства защиты других производителей, он может поискать их в списке по имени производителя. Например, Symantec, McAfee и другие.

В свойствах программы администратор найдет список компьютеров, на которых она установлена. После этого останется только ее удалить.

Для этого есть задача Агента администрирования: **Удаленная деинсталляция программы**. Но сразу она не поможет. Список программ, которые может удалить Агент, обычно совпадает со списком программ, которые может удалить инсталлятор Kaspersky Endpoint Security. Этот список общий и в составе продуктов обновляется только при выпуске новых версий или пакетов исправлений (Service Pack). А новые версии и пакеты исправлений для Kaspersky Endpoint Security и Kaspersky Security Center почти всегда выходят одновременно.

Как удалить неизвестные несовместимые программы

Что делать



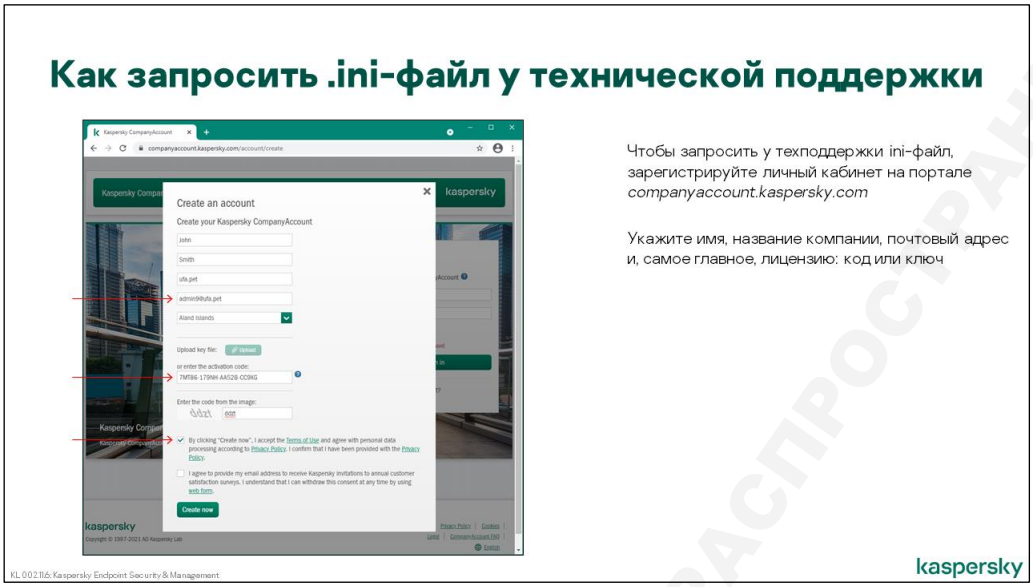
Для каждой программы из списка есть ini-файл, в котором написано, как ее обнаруживать и как ее удалять.

Чтобы удалить программу, которой нет в списке, отправьте дистрибутив программы в службу поддержки и запросите ini-файл для нее. Специалистам Лаборатории Касперского понадобится время, чтобы изучить программу и разработать для нее ini-файл. Эта услуга доступна только для сравнительно больших клиентов.

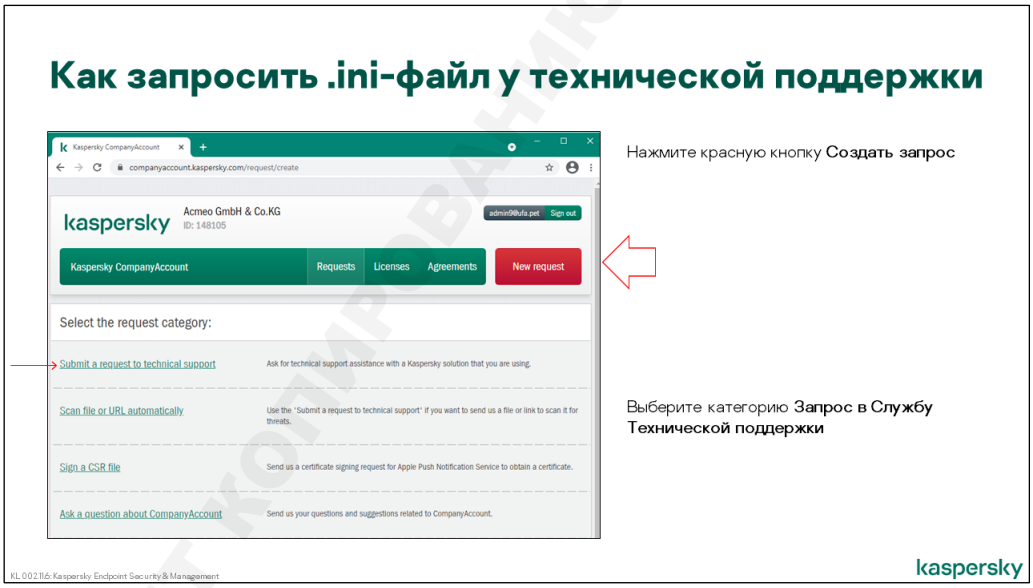
Полученный ini-файл скопируйте в папку с остальными ini-файлами на Сервере администрирования: *%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Data\Cleaner*. После этого перезагрузите службу Сервера администрирования.

Теперь задача Агента администрирования — **Удаленная деинсталляция программ** — сможет удалять новую несовместимую программу. Запустите задачу, чтобы удалить все несовместимые программы на всех компьютерах. Или, чтобы сэкономить ресурсы, сделайте выборку только тех компьютеров, на которых есть несовместимая программа, и запустите на них задачу деинсталляции только для этой несовместимой программы.

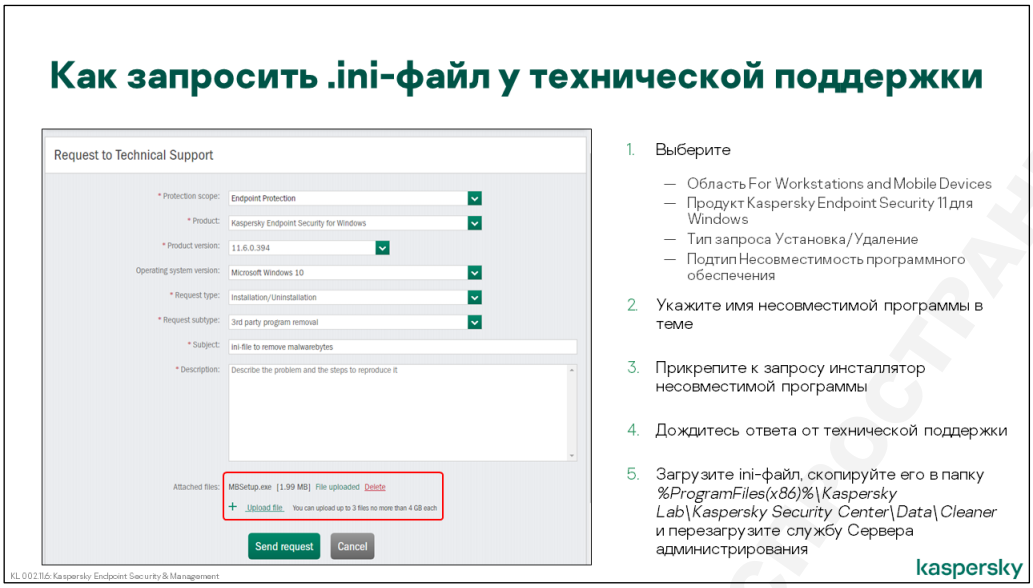
Как обратиться в поддержку



Чтобы обратиться в техническую поддержку, используйте портал *companyaccount.kaspersky.com*. Чтобы зарегистрироваться, укажите свой почтовый ящик и лицензию: ключ или код активации.



Чтобы запросить ini-файл, создайте новый запрос и выберите категорию *Запрос в Службу Технической поддержки*.



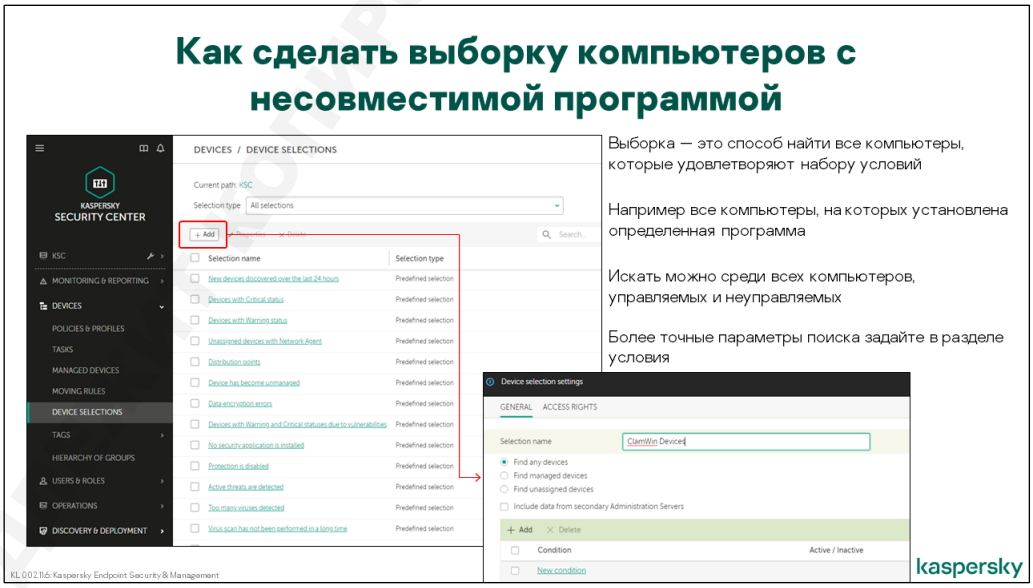
В запросе выберите

- Область — для рабочих станций
- Название и версию программы — Kaspersky Endpoint Security для Windows 11.x.x.xxxx
- Тип и подтип запроса — установка и несовместимые программы

После этого опишите ситуацию и обязательно прикрепите к запросу инсталлятор сторонней программы, которую вы хотите удалить.

Как отобрать компьютеры с несовместимой программой

Как создать выборку



Чтобы удалить несовместимые программы, нужно создать задачу деинсталляции и запустить ее на компьютерах, где эти программы обнаружены.

Чтобы отобрать компьютеры с несовместимой программой, создайте выборку компьютеров на вкладке **Устройства | Выборки устройств**. Там есть предустановленные выборки, которые показывают проблемные компьютеры:

- Базы устарели
- Давно не выполнялся поиск вирусов
- Давно не подключались
- Есть необработанные объекты
- Найдено много вирусов
- Не включена защита
- Не установлена программа защиты
- Нераспределенные устройства с Агентом администрирования
- Новые устройства в сети
- Ошибки шифрования данных
- Потеряно соединение с устройством
- Устройства со статусом «Критический»
- Устройства со статусом «Предупреждение»
- Устройства со статусом «Предупреждение» и «Критический» из-за наличия уязвимостей
- Точки распростанения (бывшая Агенты обновления)

Это предустановленные выборки: их нельзя ни изменить, ни удалить. Выборки компьютеров с несовместимыми устройствами среди них нет.

Чтобы создать выборку нажмите кнопку **Добавить**.

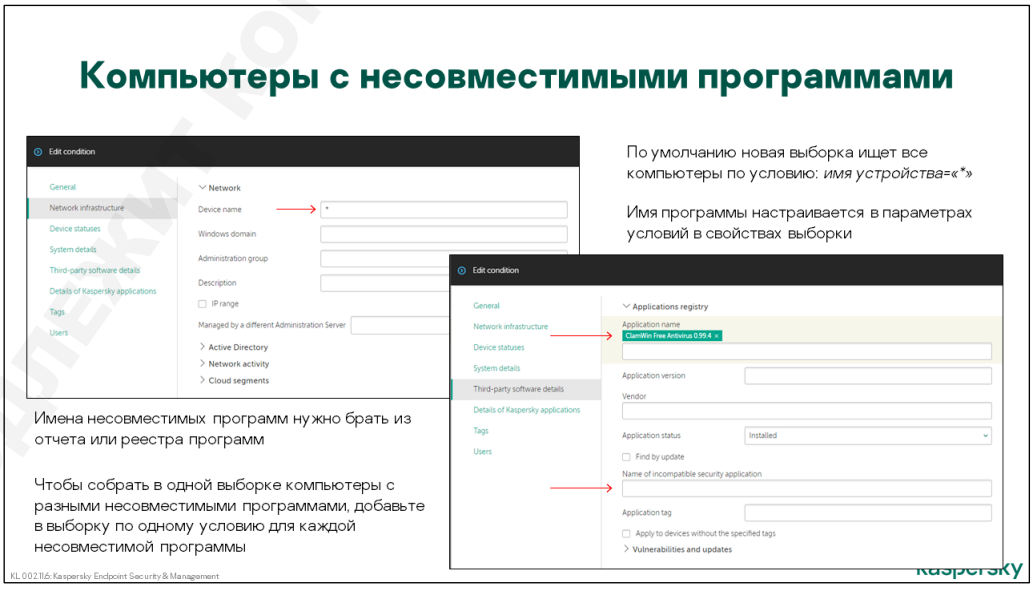
В выборке можно искать:

- среди всех компьютеров
- только среди управляемых
- только среди нераспределенных

Нераспределенные компьютеры не передают на сервер списки установленных программ. Поэтому ищите компьютеры с несовместимыми программами либо среди управляемых, либо среди всех.

По умолчанию в выборке не заданы никакие условия, и она находит все компьютеры в области поиска.

Параметры выборки



Чтобы найти компьютеры с несовместимой программой, измените ее условия.

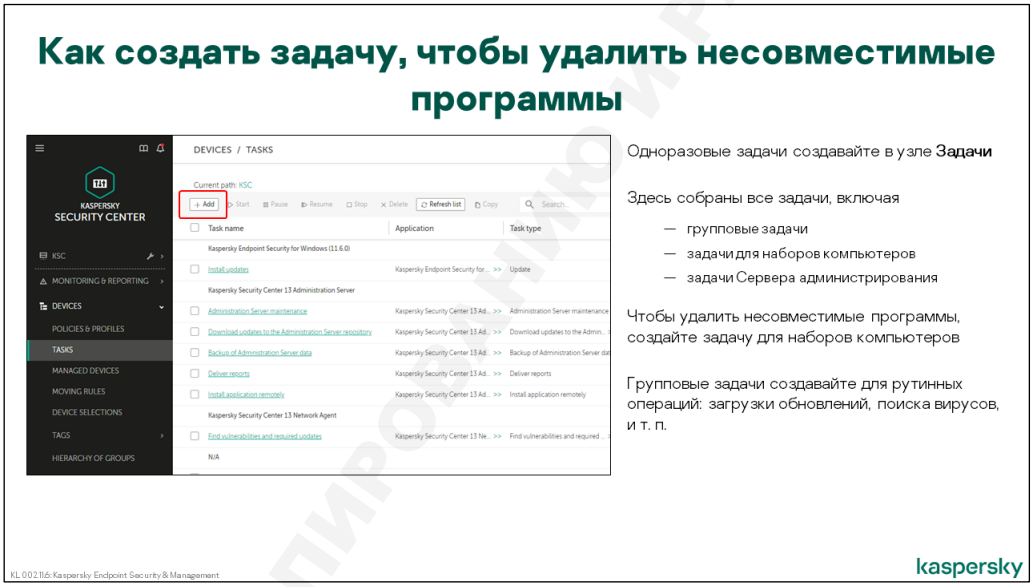
По умолчанию в каждой выборке есть одно макроусловие с множеством микроусловий. Все микроусловия в макроусловии объединяются логическим И. Макроусловия между собой объединяются логическим ИЛИ.

Чтобы найти компьютеры с одной несовместимой программой, достаточно одного макроусловия. Откройте его свойства и перейдите в раздел **Информация о программах сторонних производителей**. Выберите имя искомой программы в списке *Название несовместимого средства защиты*. Сохраните условие и выборку. В результате выборка будет содержать только компьютеры, где обнаружена эта программа.

Чтобы отобразить в одной выборке компьютеры с разными несовместимыми программами, добавьте макроусловия и выберите в них остальные несовместимые программы.

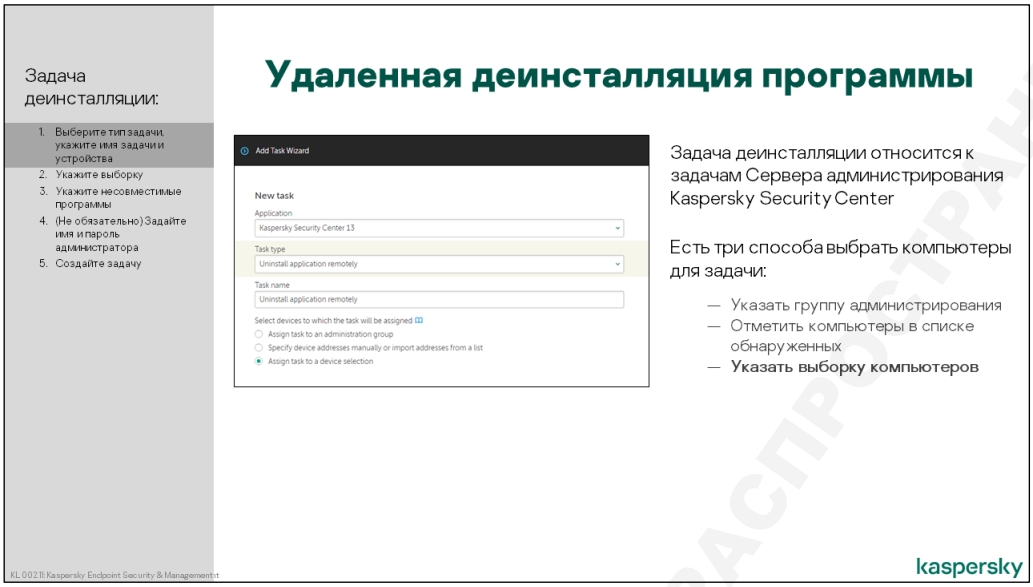
Как удалить несовместимые программы задачей

Где в консоли создавать задачи



Теперь создайте для этой выборки задачу деинсталляции. Для этого запустите мастер создания задачи во вкладке **Устройства | Задачи**, и на шаге выбора компьютеров укажите созданную выборку. Такая задача при каждом запуске будет проверять текущее содержимое выборки и обновлять свой список целевых компьютеров соответствующим образом.

Типы задач



Мастер создания показывает все задачи, которые вы можете создать. Каждый плагин, установленный в консоли, добавляет к списку задачи того или иного приложения. После стандартной установки Сервера администрирования вы сможете создавать задачи для Kaspersky Security Center и Kaspersky Endpoint Security 11.6. Задача удаленной установки и задача деинсталляции — это задачи Kaspersky Security Center.

Для удаления несовместимых программ выберите тип задачи Сервер администрирования **Kaspersky Security Center 13** | **Удаленная деинсталляция программы** в мастере создания задачи.

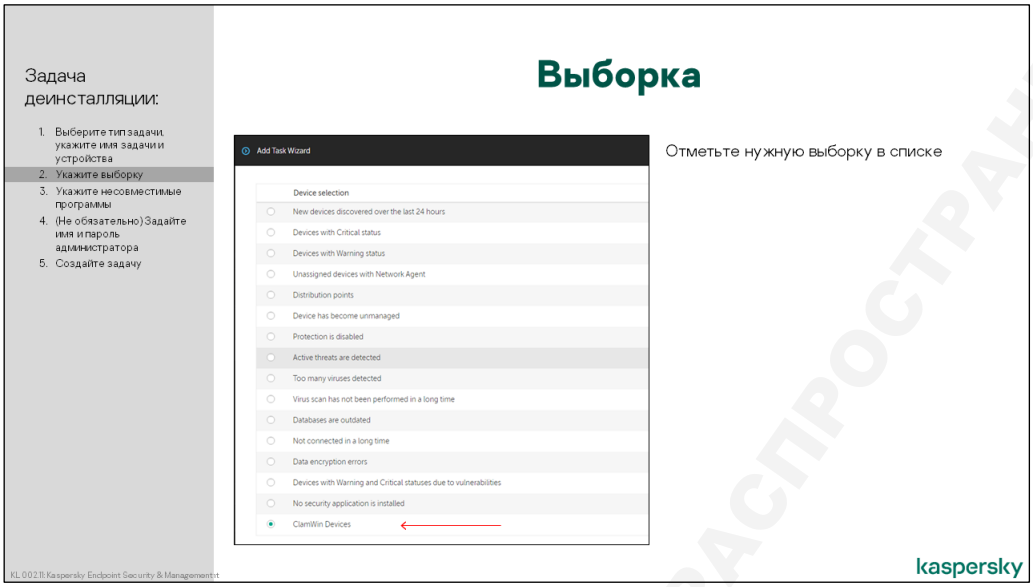
По умолчанию мастер предлагает имя задачи, которое совпадает с типом задачи: **Удаленная деинсталляция программы**. Если вы удаляете одну программу, укажите ее имя в имени задачи. Так вам будет проще понимать в будущем, нужна еще эта задача, или ее можно удалить.

Выберите компьютеры для задачи. Доступны следующие варианты выбора:

- Указать имя группы компьютеров
- Отметить компьютеры в группе *Управляемые устройства* и в узле *Нераспределенные устройства*
- Указать имя выборки компьютеров

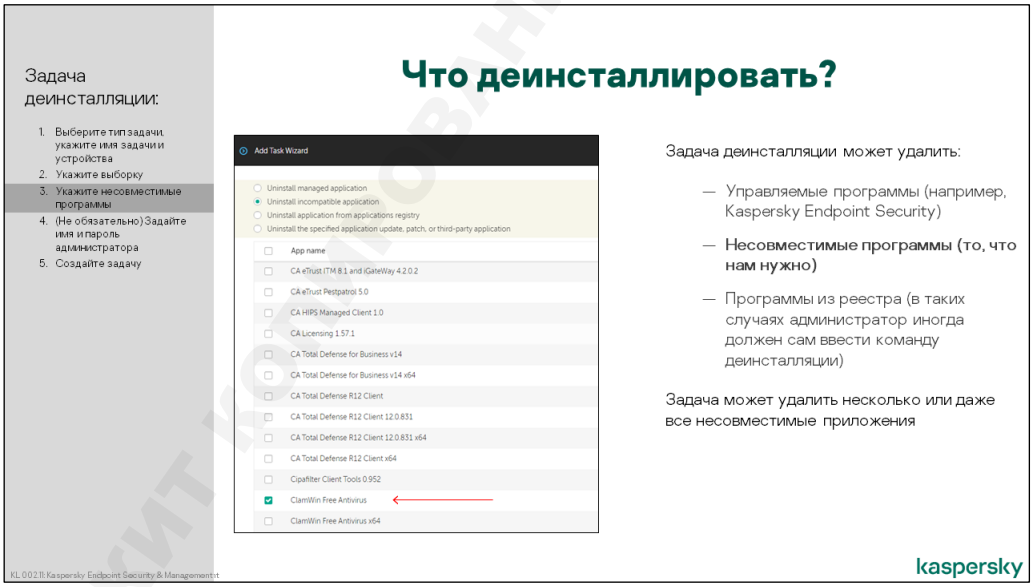
Последняя опция удобна, когда компьютеры можно сравнительно легко описать набором условий. Например, компьютеры, на которых обнаружены несовместимые программы.

Выбор компьютеров



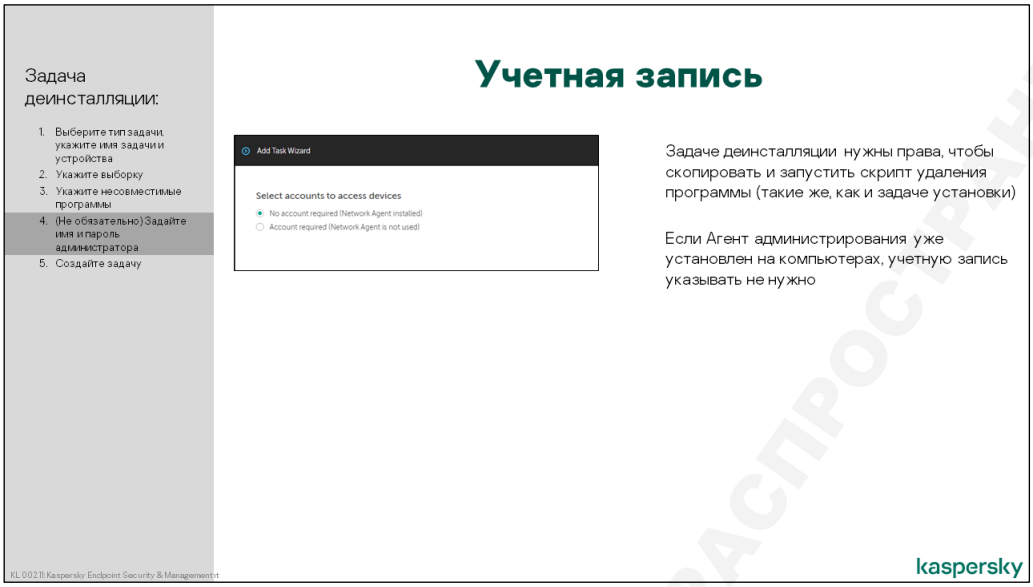
Отметьте нужную выборку, чтобы задача при запуске получила актуальный список устройств с несовместимыми программами.

Выбор программы



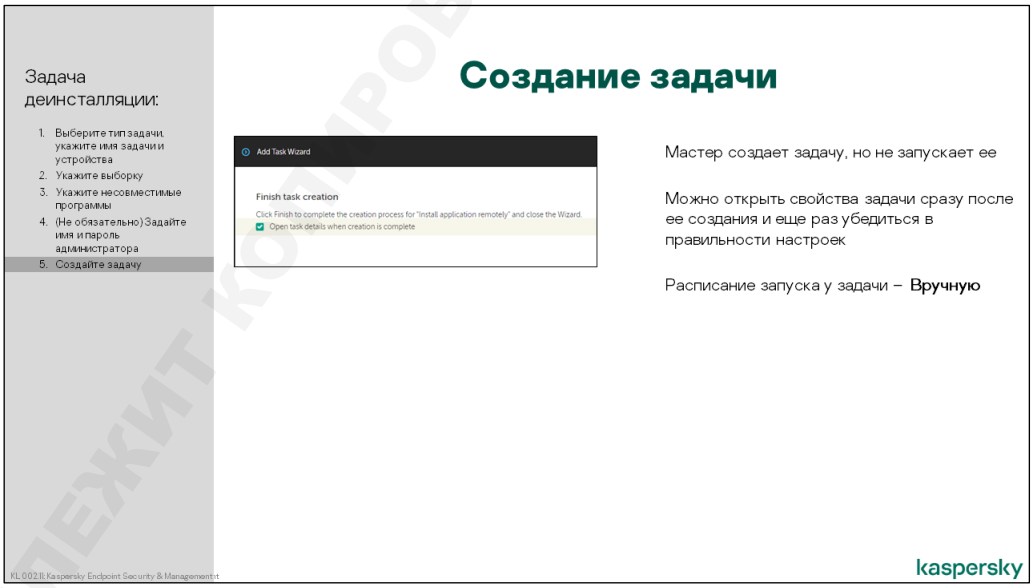
После этого укажите имя несовместимой программы, которую нужно удалить. Потенциально можно указать несколько программ для удаления или даже все программы из поддерживаемого списка. Выбор больше, чем одной программы для деинсталляции увеличивает время выполнения задачи, поскольку задача последовательно выполняет сценарии удаления для всех программ из списка.

Учетная запись



Еще мастер создания задачи запрашивает у администратора учетную запись. В описываемом сценарии учетную запись задавать не нужно, т.к. на компьютерах уже есть Агент администрирования, который загрузит и выполнит задачу деинсталляции от имени локальной системы. Учетную запись нужно задавать, только если задача будет выполняться на компьютерах без Агента администрирования, либо на компьютерах, где Агент администрирования не имеет прав администратора. И тот, и другой случай встречается редко.

Завершение мастера



На последнем шаге мастер предлагает перейти к свойствам задачи после ее создания. Администратор может еще раз убедиться в правильности настроек и запустить ее.

5. Как организовать компьютеры в группы

5.1 Как понять, что внедрение закончилось

Теперь вы знаете все, что нужно, чтобы установить защиту на всех компьютерах сети:

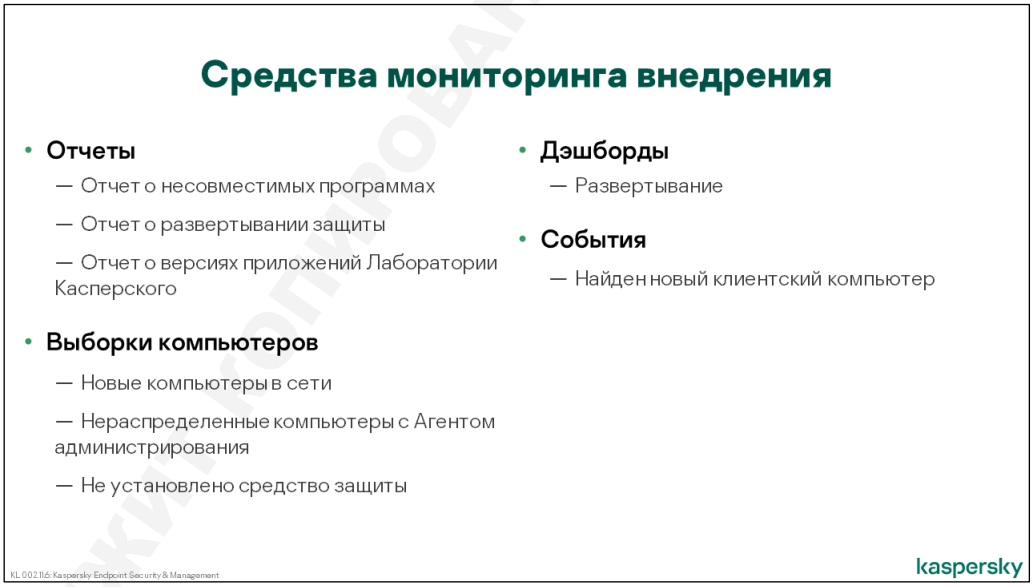
- Как выбрать компоненты и параметры установки Kaspersky Endpoint Security
- Как установить Kaspersky Endpoint Security и Агент администрирования удаленно
- Как установить Kaspersky Endpoint Security и Агент администрирования средствами Active Directory
- Как создать автономный пакет для локальной установки
- Как создать несколько разных пакетов с разными параметрами
- Как установить на обнаруженные и необнаруженные компьютеры

К этому списку полезно добавить инструменты мониторинга:

- Как понять, какие программы установлены на каких компьютерах
- Как понять, что установка в сети закончилась

Для этого можно использовать результаты задач установки, а также отчеты, выборки компьютеров и выборки событий.

Где искать информацию о внедрении



Результаты задачи или просмотр группы **Управляемые устройства** не обязательно дают полную информацию о развертывании защиты в сети. Внедрение одной задачей на все компьютеры характерно только для небольших сетей, как и управление всеми компьютерами, используя только одну группу.

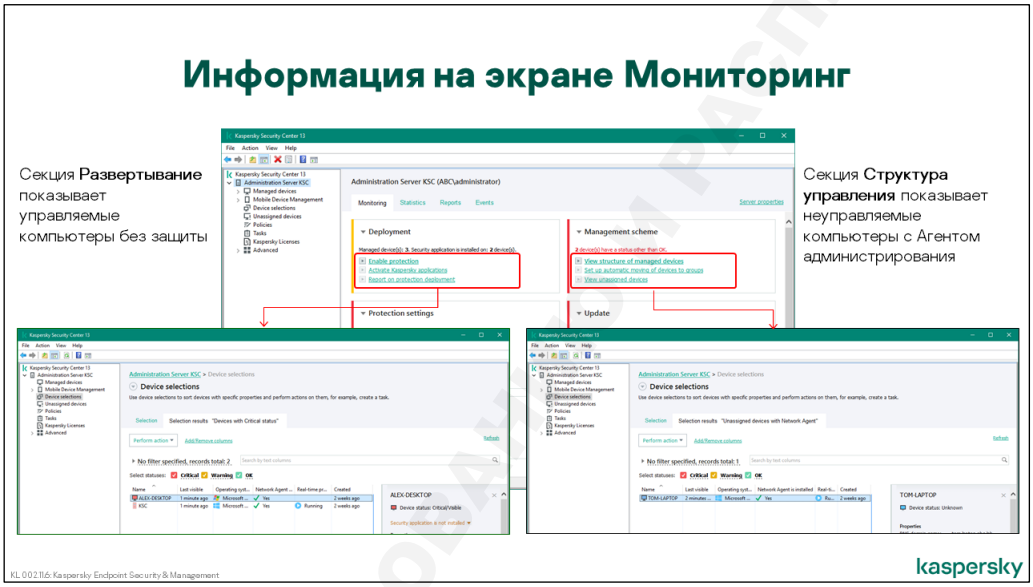
Для составления полной картины, естественным источником информации являются отчеты. На стадии внедрения полезны отчеты:

- Отчет о несовместимых программах
- Отчет о версиях программ Лаборатории Касперского
- Отчет о развертывании защиты

Кроме того, полезными инструментами на этапе внедрения являются выборки:

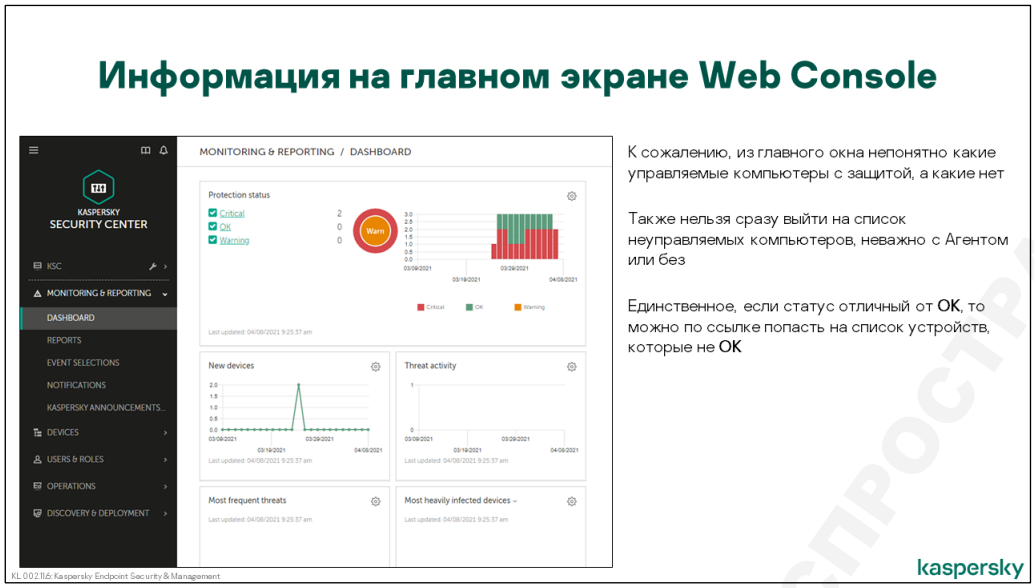
- Новые устройства в сети
- Не установлена программа защиты
- Нераспределенные устройства с Агентом администрирования

Общие статусы



В ММС-консоли информация о развертывании защиты доступна сразу на главной закладке **Мониторинг** Сервера администрирования. В секции **Развертывание** приводится количество управляемых компьютеров, не оснащенных Kaspersky Endpoint Security. Если их больше нуля, отображается ссылка на выборку всех таких компьютеров.

Если в узле **Нераспределенные устройства** есть компьютеры с установленным Агентом администрирования, это отражается в области **Структура управления**, со ссылкой на соответствующую выборку компьютеров.



Если говорить о Web Console, то, к сожалению, информация на главном окне довольно скудная. Определить на каких управляемых устройствах установлен Kaspersky Endpoint Security, а на каких нет, так просто нельзя.

Приводится только список управляемых устройств, распределенных по статусу. Но статус **Критический** может быть у устройства, на котором вообще не установлен Kaspersky Endpoint Security, а может быть устройства, где Kaspersky Endpoint Security установлен, но по какой-то причине не запущен.

Единственный плюс — это можно сразу попасть на список устройств, статус которых отличается от **OK** и изучить состояние этих устройств.

Выборки устройств

Компьютеры с Агентом администрирования должны быть в узле **Управляемые устройства**. Если они находятся в узле **Нераспределенные устройства**, они не посылают события на Сервер администрирования и не получают с Сервера задачи и политики.

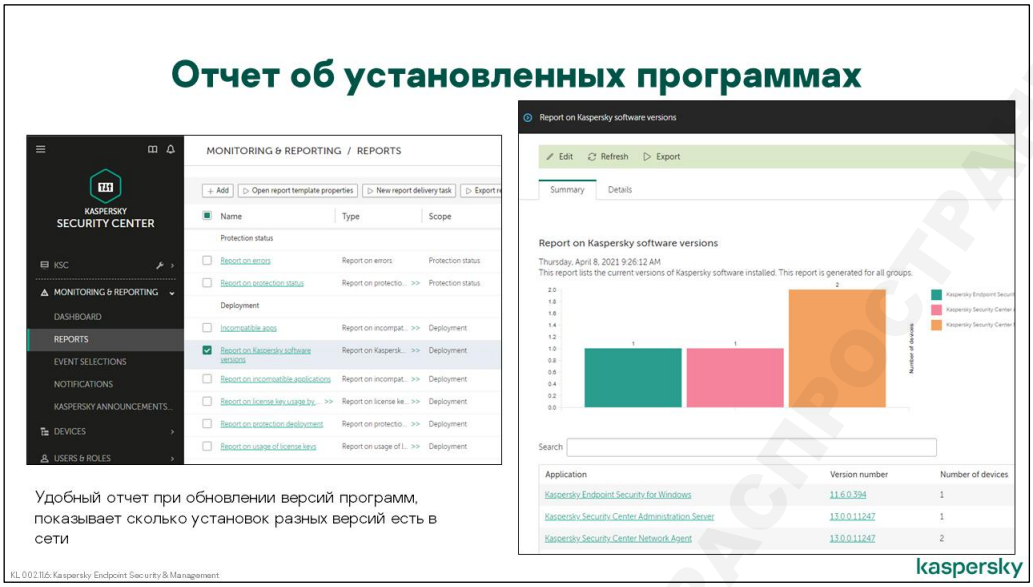
Поэтому Сервер администрирования показывает такие компьютеры на экране мониторинг ММС-консоли и в соответствующей выборке.

Отчеты

Где искать отчеты

Отчеты доступны в разделе **Мониторинг и отчеты** на соответствующей вкладке — **Отчеты**.

Отчет об установленных программах



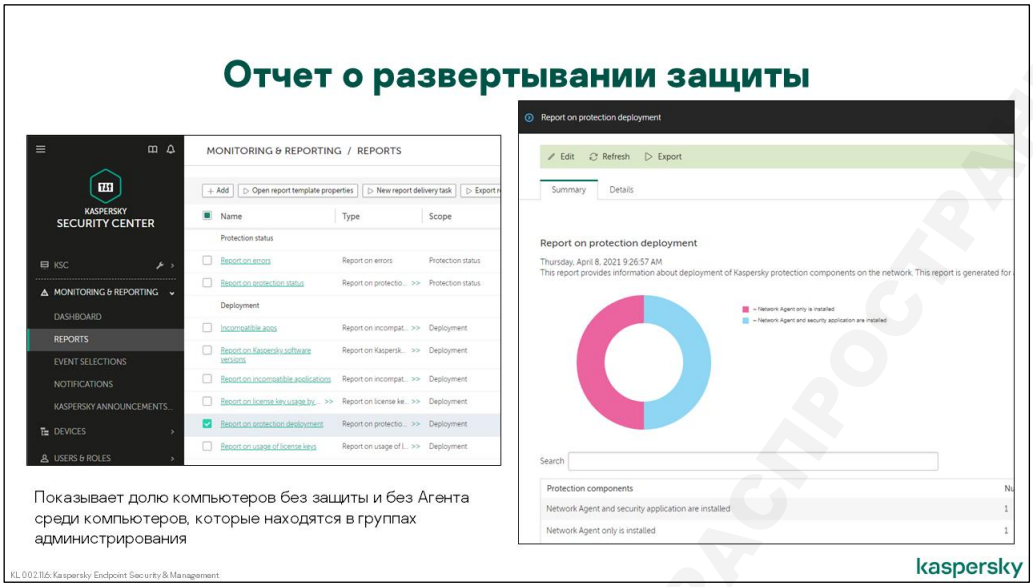
Отчет о версиях установленных программ показывает количество установленных экземпляров программ Лаборатории Касперского на управляемых компьютерах. В частности, количество установленных Агентов администрирования, Серверов администрирования и экземпляров Kaspersky Endpoint Security.

Различные версии (сборки) продуктов учитываются отдельно, что удобно при переходе на новую версию. В отчете хорошо видно, сколько компьютеров уже используют актуальные версии программ, а сколько — еще старые.

Графическая часть отчета является визуализацией таблицы статистики, которая перечисляет разные версии управляемых продуктов и количество установок каждой из них.

Таблица детализации приводит информацию по каждому компьютеру: какие продукты установлены, каких версий и т.д.

Отчет о развертывании защиты



Этот отчет делит компьютеры на три категории:

- Компьютеры с Агентом и средствами защиты
- Компьютеры с Агентом, но без средств защиты
- Компьютеры без Агента

Компьютеры со средствами защиты, но без Агента попадают в последнюю категорию. Если Агент не установлен, Сервер администрирования не знает, есть ли на компьютере средства защиты. В эту же категорию попадают компьютеры, на которых Агент установлен, но не подключен к Серверу администрирования. Например, компьютеры, где Агенты используют неправильный адрес Сервера.

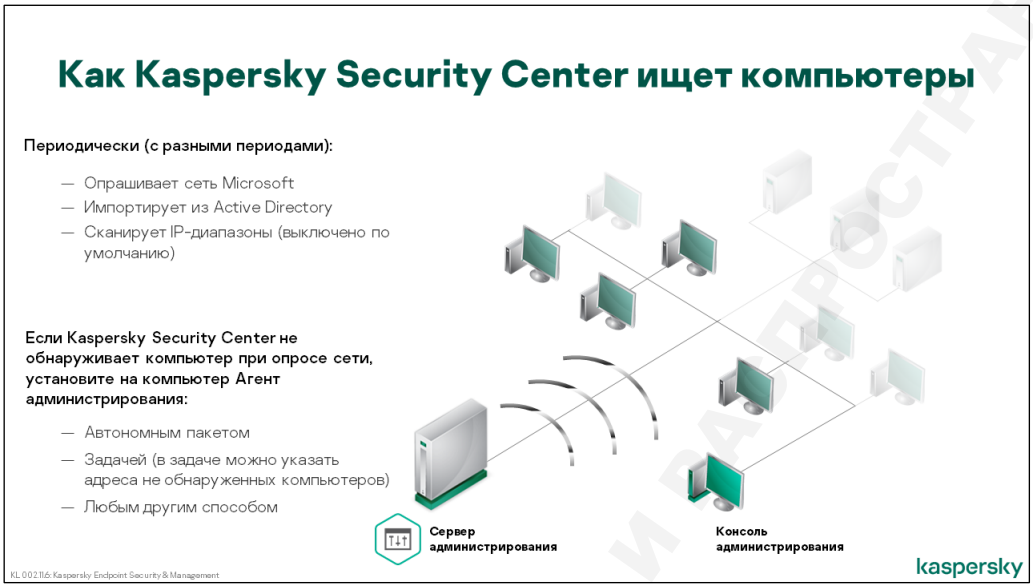
Диаграмма и статистическая таблица приводят число компьютеров в каждой из категорий. Таблица детализации, как и в отчете о версиях установленных программ, приводит версию Агента и Kaspersky Endpoint Security на каждом из компьютеров.

Этот отчет особенно удобен, если для внедрения администратор сначала перенес все компьютеры в группу управляемых, а потом начал внедрение с использованием задач. В этом случае отчет явно показывает, сколько еще управляемых компьютеров не подключено к Серверу, и сколько из подключенных еще не защищены Kaspersky Endpoint Security.

Если для внедрения администратор использует мастер удаленной установки, и каждый раз выбирает компьютеры из нераспределенных, этот отчет оказывается менее полезным. Информация о нераспределенных компьютерах в отчет не включена.

5.2 Как сервер администрирования ищет компьютеры

Виды опросов



В ходе работы мастера удаленной установки или при создании задачи установки администратор имеет возможность выбирать компьютеры из некоторого списка. Этот список формируется Сервером администрирования путем опроса сети. Опрос осуществляется периодически несколькими разными способами:

— Опросом сети Microsoft
— Опросом Active Directory
— Опросом IP-подсетей

Сеть опрашивает не служба Сервера администрирования, а служба Агента администрирования, установленная на сервере администрирования. Агенты администрирования на обычных компьютерах сеть не опрашивают.

Где настроить опросы

Результаты опроса отображаются на вкладке **Обнаружение устройств и развертывание | Обнаружение устройств** отдельно для каждого метода обнаружения:

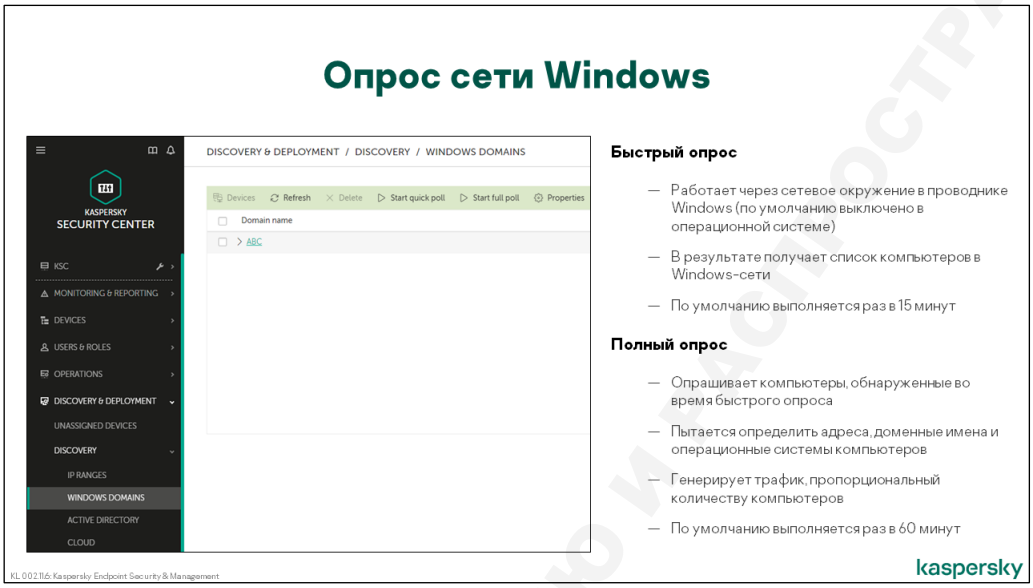
— **IP-диапазоны** — папками представлены IP-подсети
— **Windows-домены** — компьютеры, обнаруженные в ходе опроса сети Windows; рабочие группы и домены представлены папками, в которых содержатся компьютеры
— **Active Directory** — домены и организационные подразделения представлены папками, в которых содержатся компьютеры

В упрощенном виде найденные компьютеры отображаются на вкладке **Обнаружение устройств и развертывание | Нераспределенные устройства**.

Один компьютер может отображаться в нескольких представлениях. Если компьютер обнаружен в домене HQ и его адрес *192.168.0.1*, его будет видно и в узле **Домены**, и в узле **IP-диапазоны** в соответствующих папках.

Администратор может изменить параметры опроса для каждого из методов. Для этого нужно перейти на вкладку **Обнаружение устройств и развертывание | Обнаружение устройств**, выбрать нужный способ и воспользоваться командой **Свойства**. На этом же экране он может запустить любой из опросов вручную.

Опрос сети Windows



Что делает быстрый опрос

Сервер администрирования собирает списки компьютеров сети Windows точно так же, как это делает сама операционная система. Когда пользователь открывает на компьютере сетевое окружение, он видит список соседних компьютеров, сгруппированных в домены и рабочие группы. Точно такой же список может получать и Сервер администрирования.

Этот способ опроса называется быстрым опросом сети Windows. В ходе такого сканирования Сервер практически не создает нагрузки на сеть. За составление и предоставление списка компьютеров отвечает служба Computer Browser. В каждом сегменте сети есть главный компьютер, хранящий общий список и предоставляющий его по запросу. Чтобы получить список, Серверу администрирования достаточно послать один запрос.

В последних версиях Windows служба *Обозреватель компьютеров* по умолчанию отключена или вообще не установлена. Если Сервер администрирования не может получить список компьютеров от службы *Обозреватель компьютеров*, он выполняет запрос в Active Directory и пытается получить список компьютеров оттуда. Конечно, при условии, что Сервер администрирования входит в домен Active Directory.

Быстрый опрос выполняется раз в 15 минут. В результате быстрого опроса Сервер получает список NetBIOS-имен компьютеров, доменов и рабочих групп.

Что делает полный опрос

При полном опросе Сервер администрирования пытает получить как можно больше информации о каждом компьютере из результатов быстрого опроса.

Для каждого имени, Сервер выполняет разрешение имени в IP-адрес, используя протоколы NetBIOS, DNS и LLMNR. Для полученных адресов сервер выполняет обратное разрешение в имя, и, если имя не совпадает с исходным, получает IP-адрес для нового имени.

Сервер проверяет, доступны ли IP-адреса, с помощью ICMP-запросов, и в конце пытается соединиться с компьютерами по протоколам SMB и RPC, чтобы выяснить операционную систему.

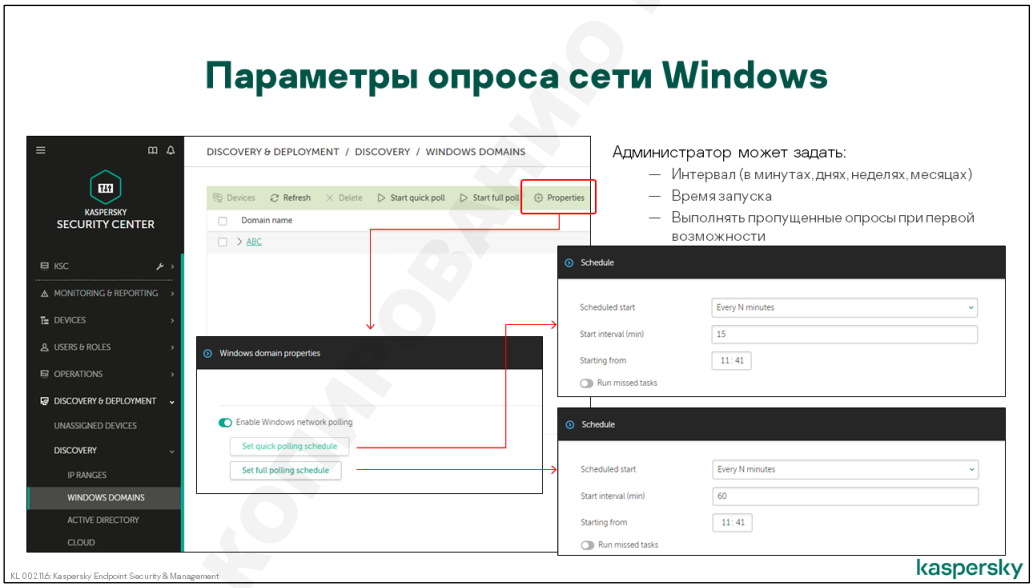
Все эти многочисленные запросы нужны, чтобы учесть, что имена и адреса компьютеров могут меняться. С помощью прямых и обратных проверок имен и IP-адресов Сервер администрирования отличает новые компьютеры в сети от старых компьютеров, которые просто поменяли имя или IP-адрес.

Поскольку количество запросов пропорционально количеству компьютеров, сетевая активность при полном опросе заметно выше, чем при быстром. Как следствие период такого опроса по умолчанию составляет 60 минут.

Как сервер отображает результаты опроса

В результатах опроса Сервер показывает все, что смог выяснить о компьютере: его имя, адрес, операционную систему и т.д.

Параметры опроса сети Windows

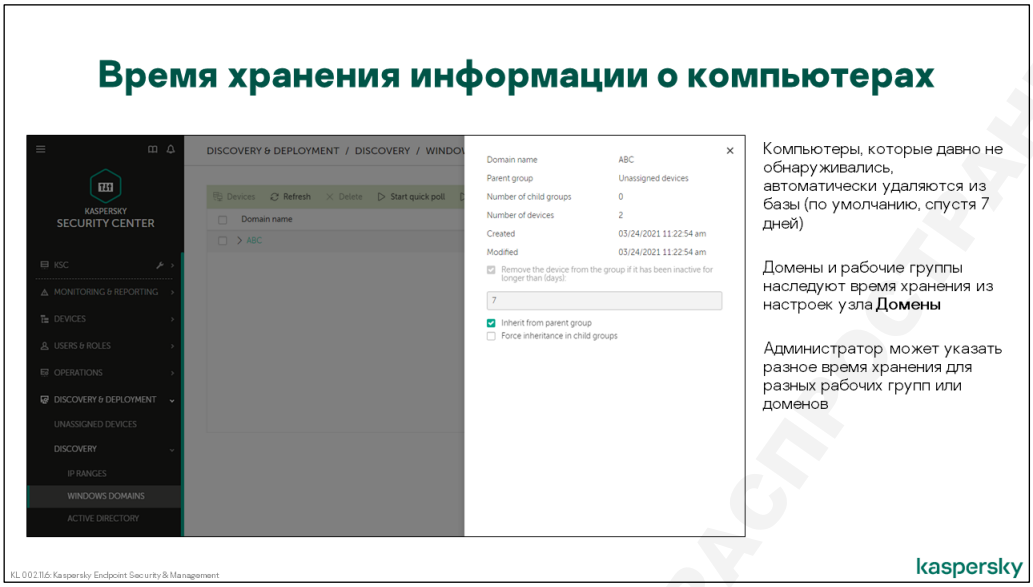


Для каждого типа опроса администратор может:

- Включить или выключить опрос вообще
- Включить или выключить опрос для части сети (что такое часть сети, зависит от типа опроса)
- Выбрать расписание опроса
- Выбрать, когда данные опроса устаревают

Расписание опроса определяется временем начала и интервалом. Интервал можно задать в минутах, часах, днях и даже неделях. Также можно включить запуск пропущенных опросов. При частом опросе это вряд ли потребуется, но не будет лишним, если опрос выполняется раз в неделю или раз в месяц.

Время хранения информации о компьютерах



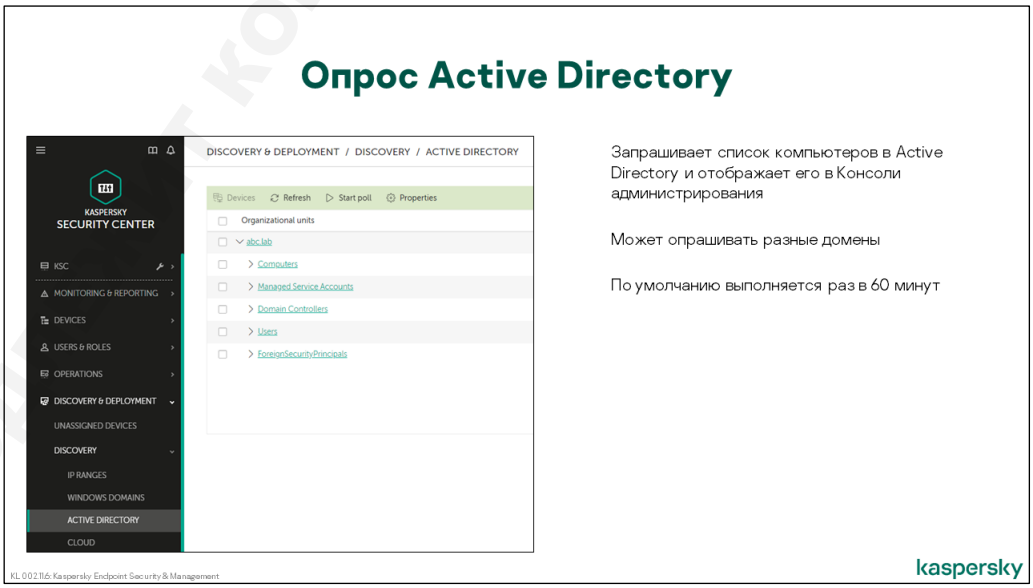
Кроме того, для опроса сети Windows администратор может указать время жизни информации о найденных компьютерах. По умолчанию этот период составляет 7 дней. Если в течение семи дней найденный ранее компьютер не обнаруживается при опросе сети Windows, информация о нем удаляется из базы данных Сервера.

Этот интервал можно задать независимо для каждого домена или рабочей группы. Или же можно задать общее время жизни и использовать его для всей сети Windows.

Кроме того, в свойствах домена или рабочей группы можно отключить опрос только для этого участка сети.

Опрос Active Directory

Что делает опрос Active Directory

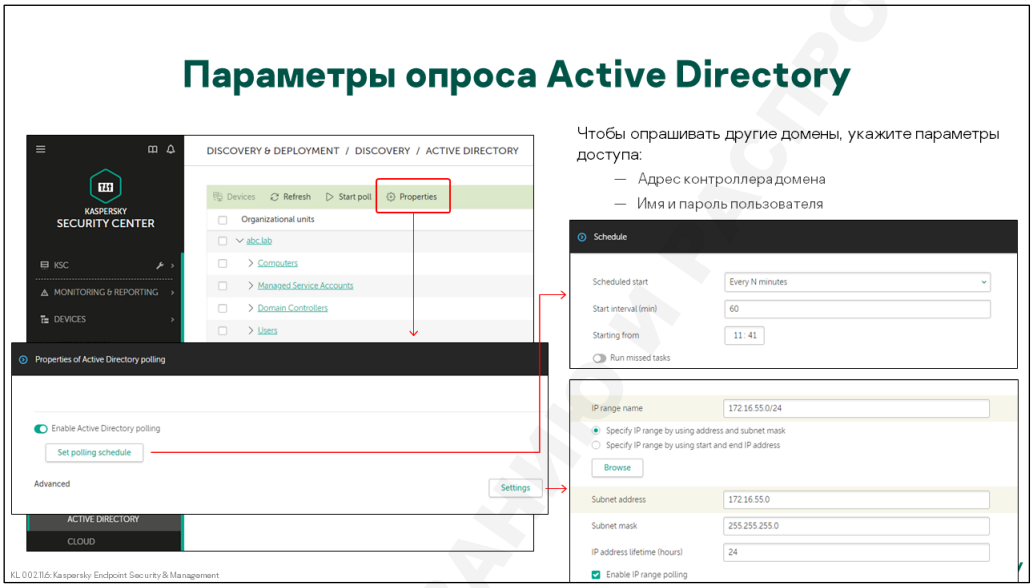


Сервер администрирования запрашивает в Active Directory структуру контейнеров (подразделений) и списки компьютеров в каждом из них.

Кроме этого, Сервер администрирования запрашивает список пользователей и групп безопасности. В этом курсе мы не касаемся того, как использовать пользователей AD. Смотрите курсы KL 010 и KL 302

В большой сети общий объем всех списков (компьютеров, пользователей, групп) может быть большим, поэтому по умолчанию опрос Active Directory выполняется раз в 60 минут.

Параметры опроса Active Directory



Параметры опроса для Active Directory похожи на параметры опроса сети Windows. Есть возможность полностью отключить этот метод опроса, и есть настройки расписания опроса, если опрос включен.

Явно заданного времени жизни у полученных данных нет. Каждый следующий опрос заменяет результаты предыдущего:

— добавляет недостающие подразделения и компьютеры
— удаляет компьютеры и подразделения, которых больше нет в Active Directory

В дополнительных параметрах опроса администратор может выбрать область сканирования:

— Домен, куда входит Сервер администрирования (выбрано по умолчанию)
— Весь лес доменов, куда входит Сервер администрирования
— Явно заданный список доменов

Чтобы добавить домен для опроса, нужно указать адрес контроллера домена, а также имя и пароль учетной записи для доступа к нему.

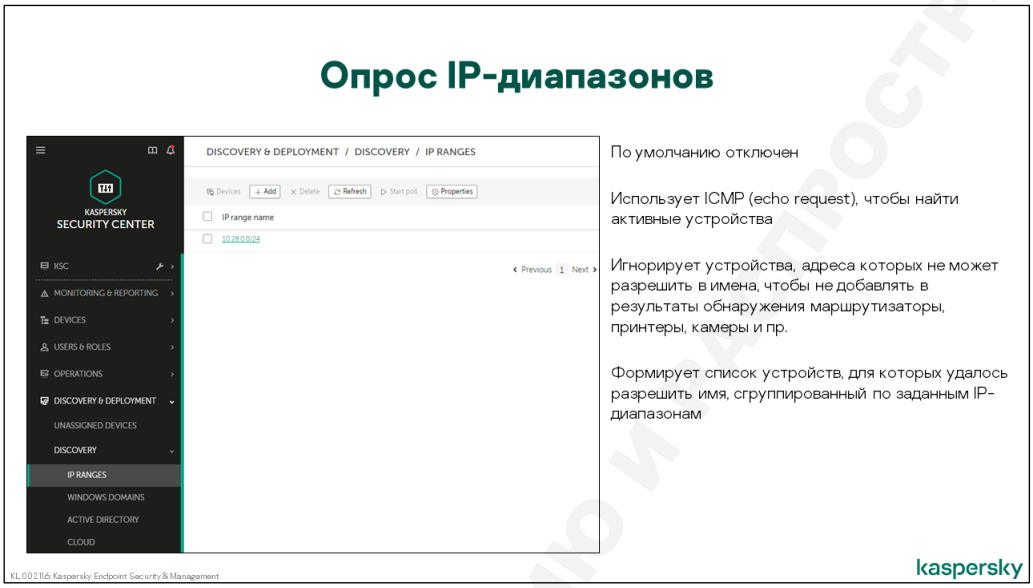
Опрос отдельных подразделений можно отключить в свойствах этих подразделений.

После того, как администратор меняет область опроса, после следующего опроса Сервер показывает только содержимое новой области. Например, если администратор отключил сканирование подразделения, после очередного опроса этого Сервер администрирования удалит всю информацию о содержимом этого подразделения из своей базы данных. Точно так же, если

ранее Сервер сканировал несколько доменов и администратор удалил один из доменов из списка, после следующего опроса Сервер удалит все данные этого домена из базы.

Опрос IP-подсетей

Что делает опрос IP-подсетей



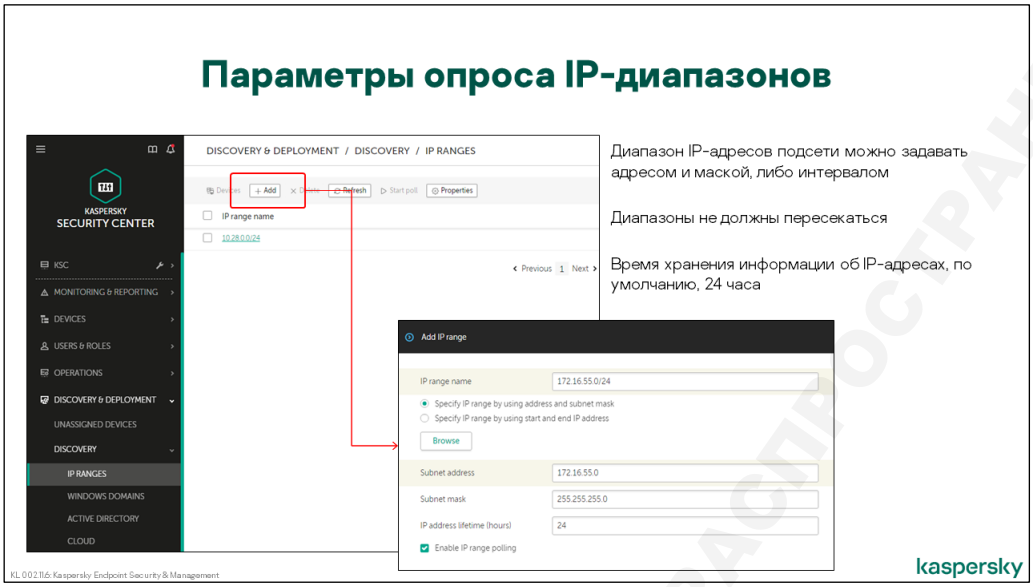
Опрос IP-диапазонов работает почти так же, как полный опрос сети Windows. Но исходный список компьютеров — это не результаты быстрого опроса, а список IP-адресов из заданных администратором IP-диапазонов.

Каждый адрес сервер пытается разрешить в имя, имя опять в адрес, проверяет, отвечает ли адрес на запросы ICMP ECHO REQUEST и т.д.

Чтобы выяснить тип устройства, Сервер также отправляет SNMP-запросы.

В результаты опроса попадают только те компьютеры, которые ответили на ICMP-запрос.

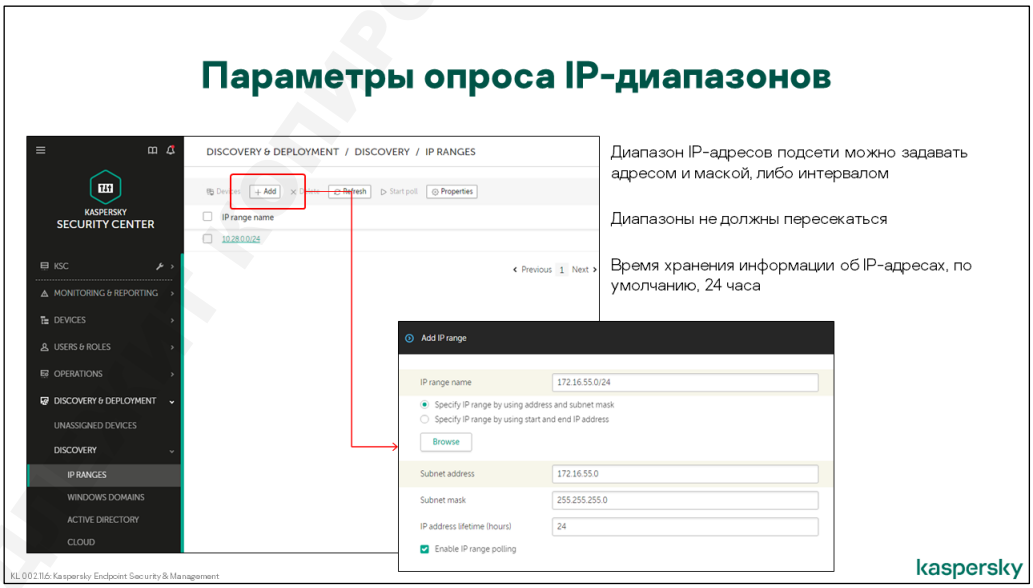
Параметры опроса IP-подсетей



Исходно IP-диапазоны для опроса Сервер администрирования берет из сетевых настроек компьютера, на котором установлен. Если адрес компьютера *192.168.0.1* и маска подсети *255.255.255.0*, Сервер администрирования автоматически включит сеть *192.168.0.0/24* в список сканируемых и проведет опрос всех адресов от *192.168.0.1* до *192.168.0.254*.

Параметры опроса IP-диапазонов включают список опрашиваемых IP-подсетей, разрешающий флаг и расписание. Если включить этот тип опроса, интервалом по умолчанию будет 420 минут (7 часов).

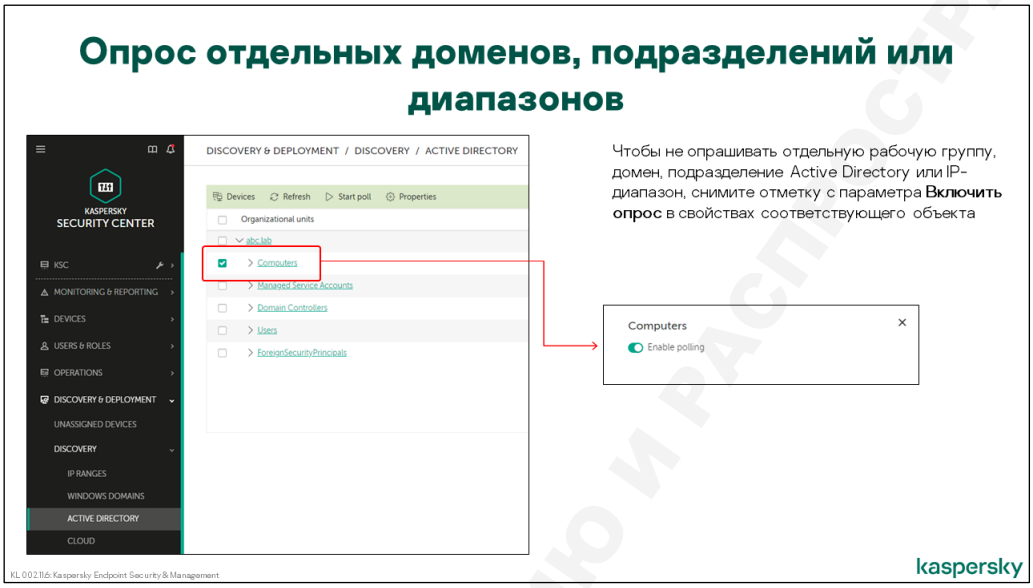
Как добавить сеть для опроса



Чтобы опрашивать подсети, в которые Сервер администрирования не входит, их нужно добавить в список вручную. Задать подсеть можно либо ее адресом и маской, либо начальным и конечным IP-адресом, как IP-диапазон. Кроме этого, нужно указать имя создаваемой подсети.

Время жизни результатов опроса по умолчанию составляет 24 часа. Если IP-адрес не подтверждается опросами в течение суток, он удаляется из базы. Такой короткий период жизни пытается учесть динамические IP-адреса (полученные по протоколу DHCP), которые могут меняться часто. При изменении настроек главное, чтобы время хранения информации не было меньше интервала опроса.

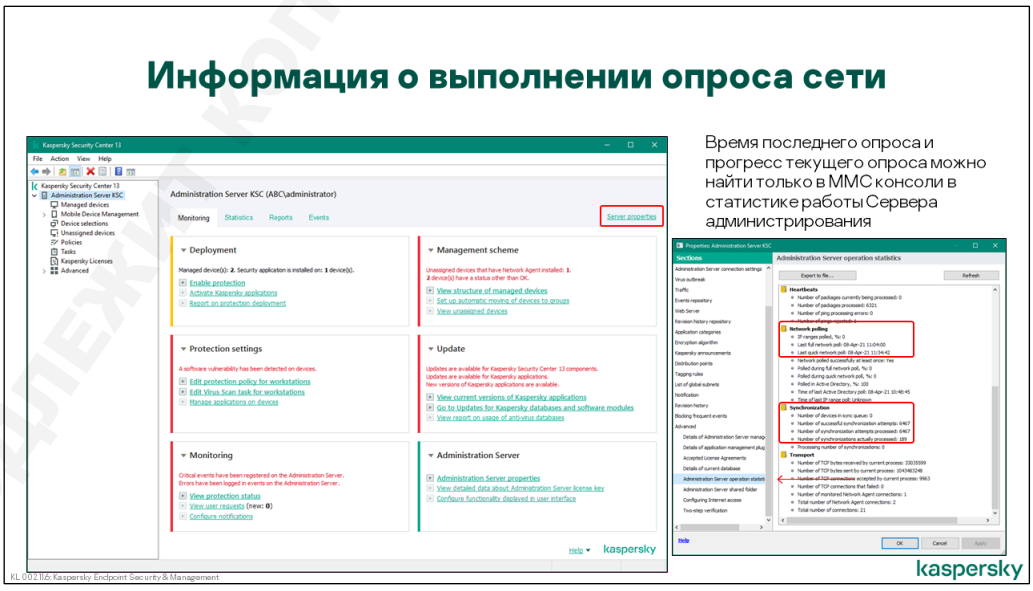
Как изменить диапазоны в IP-подсети



Под одним именем можно объединить несколько разных IP-диапазонов. Дополнительные диапазоны настраиваются в свойствах подсети. Именованные подсети не могут пересекаться друг с другом. Диапазоны внутри одной подсети пересекаться могут.

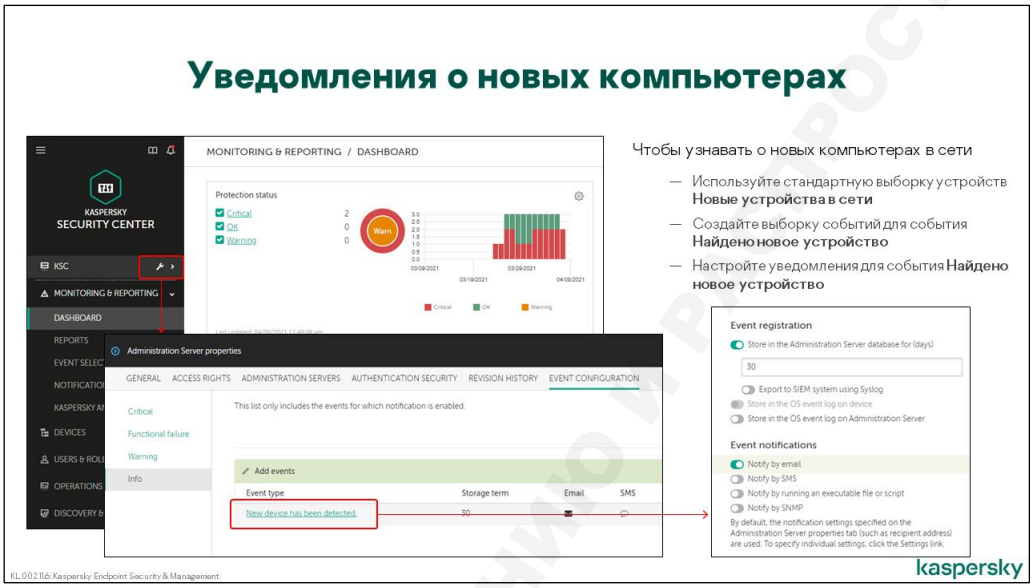
Разрешать и отключать сканирование можно независимо для каждой подсети.

Где следить за ходом опросов сети



Если администратор хочет следить за ходом опроса, то сделать это можно только в MMC-консоли. При выполнении опроса сети на экране узла **Дополнительно | Опрос сети** отображается прогресс опроса. Более подробная информация доступна в статистике Сервера администрирования (свойства Сервера администрирования: *Дополнительно | Статистика работы Сервера администрирования*). Из статистики можно узнать время последнего опроса каждым из методов, прогресс выполнения опроса в процентах и имя опрашиваемого домена при опросе сети Microsoft.

Как узнать, что Сервер нашел новые компьютеры



Администратор может настроить уведомление о событии обнаружения новых компьютеров в сети. Событие находится в свойствах Сервера администрирования и администратору нужно просто включить в его параметрах отправку почтового сообщения.

Чтобы получать уведомления о новых компьютерах, перейдите на вкладку **Настройка событий** в свойствах Сервера администрирования. Найдите событие **Найдено новое устройство** в разделе **Информационное сообщение**. Откройте свойства события и включите опцию **Уведомлять по электронной почте**.

Для доставки уведомлений Сервер использует параметры, которые вы задачи в мастере первоначальной настройки, когда устанавливали Сервер администрирования. Если вы не уверены, что указали верные параметры, проверьте их на вкладке **Общие** в разделе **Параметры доставки уведомлений** в окне свойств Сервера.

5.3 Как создать или импортировать группы

Зачем создавать группы

После установки на Сервере администрирования есть только одна группа — **Управляемые устройства**. При такой организации администратор вынужден использовать одну политику защиты и общее расписание задач для всех компьютеров, что не всегда удобно.

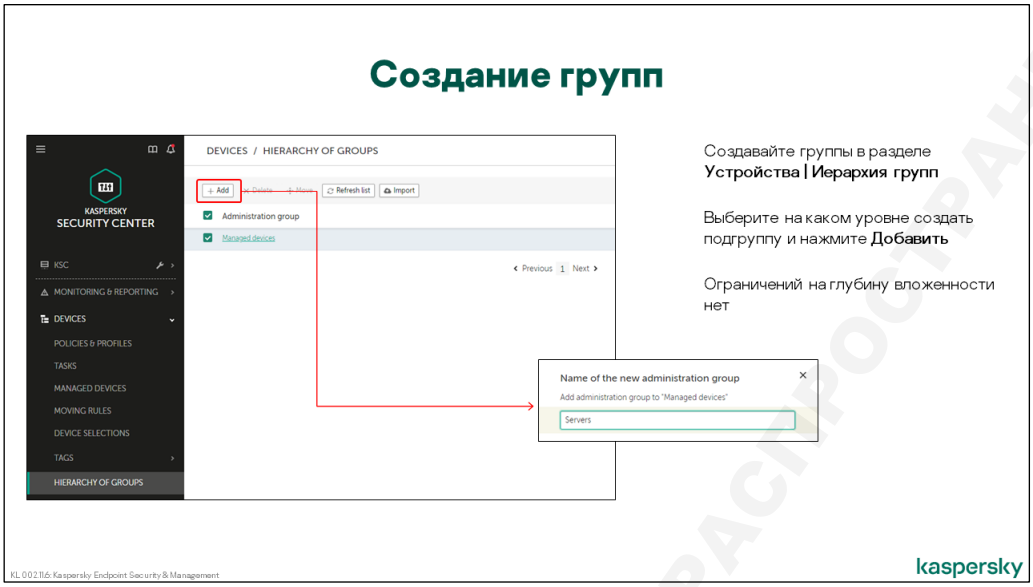
Даже в небольших сетях бывает удобно или даже необходимо использовать разные настройки защиты для серверов и пользовательских компьютеров. А в крупных сетях, где разные группы пользователей используют разные специализированные программы, возможность создавать политики с разными исключениями для разных пользователей очень удобна. А для того, чтобы применять разные политики, нужно поместить компьютеры в разные группы.[6]

С практической точки зрения бывает удобно, когда компьютеры в Kaspersky Security Center организованы в такие же группы, как и в Active Directory, или в группы, соответствующие IP-подсетям, используемым в организации. Так администратору проще понимать, где расположен компьютер, чтобы послать к нему сотрудника ИТ-департамента.

Есть и другие примеры использования групп. Нередко, особенно в больших сетях, администраторы создают группы для организации процесса внедрения. Компьютеры без Агента и средств защиты помещают в группу **Deploy Agent**, где создана задача автоматической установки Агента администрирования. Компьютеры с установленным Агентом перемещают в группу **Remove Incompatible Apps**, где созданы задачи удаления несовместимых программ. Компьютеры без несовместимых программ перемещают в группу **Deploy KES**, где создана задача автоматической установки Kaspersky Endpoint Security. Наконец, полностью защищенные компьютеры перемещают в постоянную структуру управления.

[6] Начиная с Kaspersky Security Center 10 Service Pack 1 есть возможность применять разные профили настроек к компьютерам в одной группе. Эта тема раскрыта в курсе KL 302

Как добавить группу



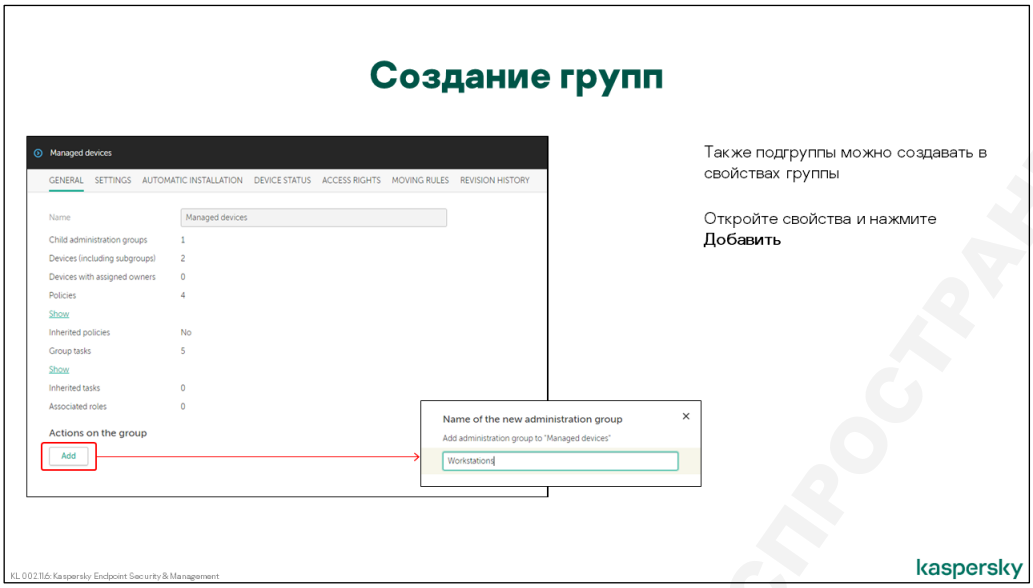
В отличие от MMC-консоли, где группы создаются так же просто как папки в Обозревателе Windows, в Web Console придется некоторое время привыкать к тому, как создавать группы. Первые группы создаются прямо в узле **Управляемые устройства**. Последующие группы можно создавать там же или в созданных ранее группах.

Чтобы создать новую группу в Web Console перейдите на вкладку **Устройства | Иерархия групп.** Затем нужно выбрать на каком уровне вы хотите создать группу и нажать **Добавить**.

В открывшемся окне нужно ввести имя группы, после чего она появится в виде подпапки в структуре управляемых компьютеров.

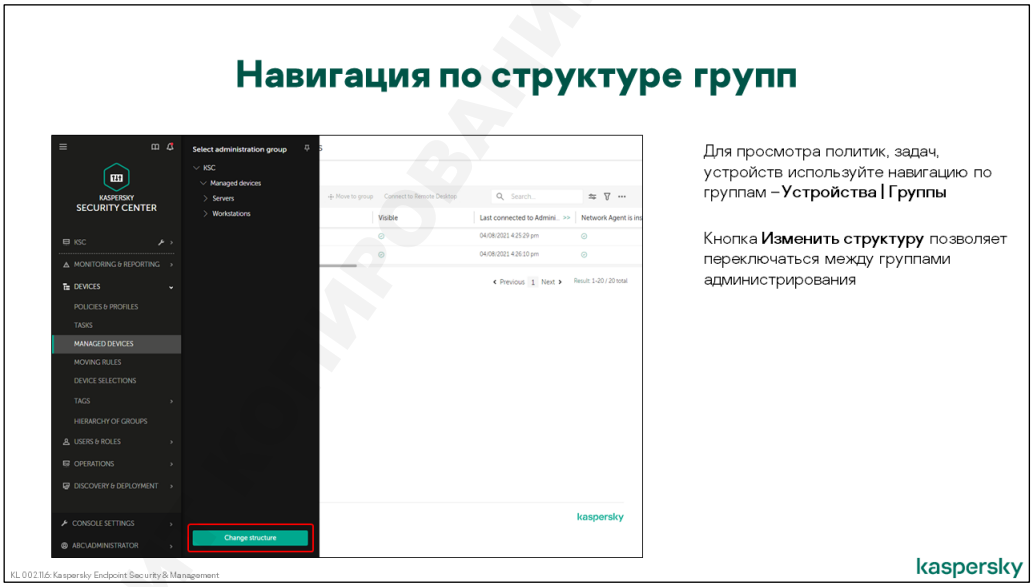
Если созданная ранее группа больше не нужна, ее можно удалить. Для этого должно выполняться одно требование — в группе, с учетом возможных подгрупп, не должно быть компьютеров. Это обычно и означает, что группа не нужна.

Группы можно перемещать внутри структуры управляемых компьютеров. Например, если структура групп отражает территориальное расположение компьютеров и отдел кадров переехал из корпуса 1 в корпус 2, подгруппу отдела кадров вместе со всеми компьютерами можно легко переместить из группы корпуса 1 в группу корпуса 2. Для этого нужно выбрать группу, которую хотите переместить, нажать **Переместить** и указать группу, в которую надо переместить.



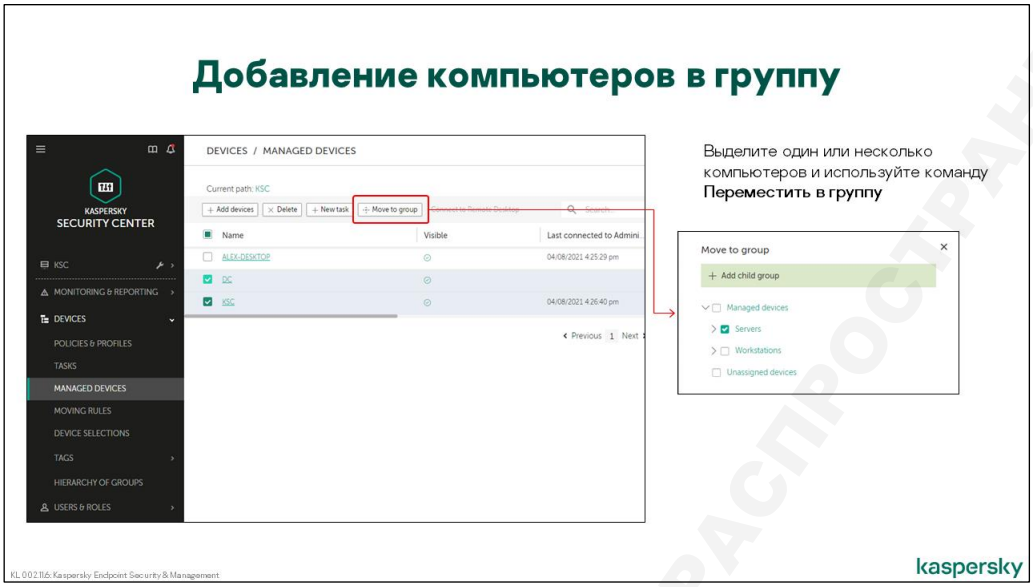
Еще один способ создания подгруппы — непосредственно в свойствах родительской группы. Если открыть свойства любой группы, то на вкладке **Общие** есть кнопка **Добавить**, которая создает подгруппу.

Навигация по структуре групп



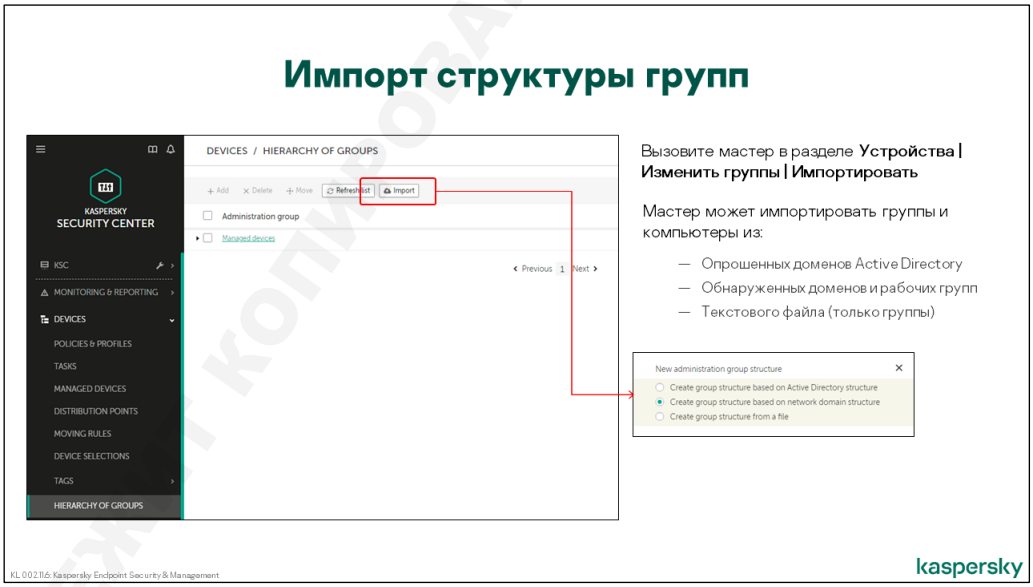
В Web Console на первый взгляд не совсем понятно, как путешествовать по группам. Но есть почти незаметная кнопка навигации — **Устройства | Группы**, которая позволяет отобразить существующую структуру групп, а при выборе группы перекидывает на список политик для этой группы. Также кнопка **Изменить структуру** перенаправляет на вкладку **Изменить группы**.

Как добавить компьютеры в группу



В Web Console администрирования перемещать компьютеры можно только одним способом, это касается и распределенных и нераспределенных устройств. Нужно выделить один или несколько компьютеров и выбрать команду **Переместить в группу**, после чего указать нужную группу.

Как импортировать структуру групп



Если сеть большая и планируемая структура управляемых компьютеров предполагает большое количество групп, создание такой структуры вышеописанными методами может оказаться весьма трудоемкой задачей. Иногда проще импортировать структуру групп из результатов опроса сети или из тестового файла.

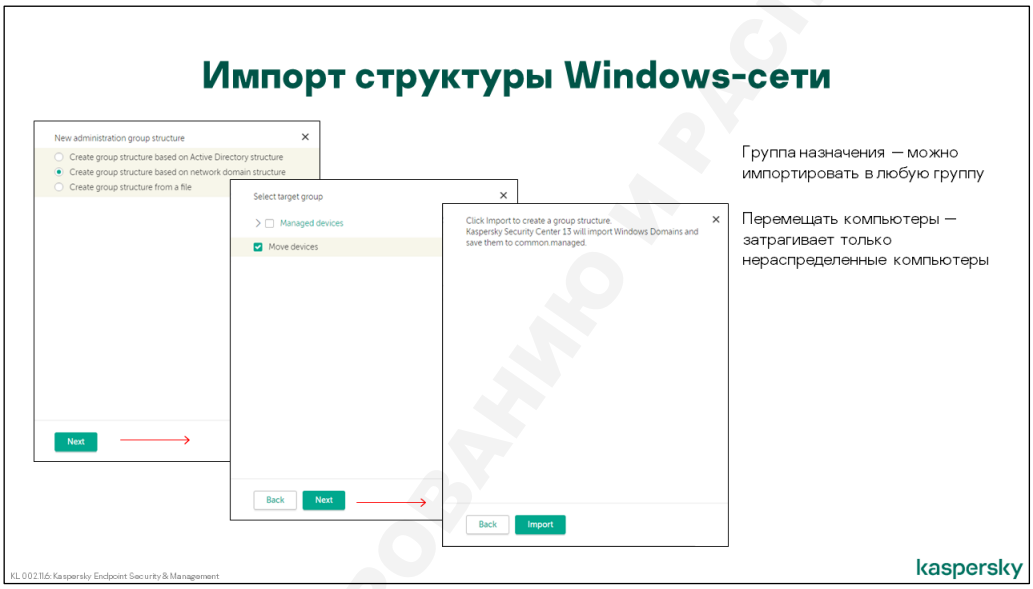
Нередко бывает, что администратор хочет организовать управляемые компьютеры точно так же, как организована его сеть — чтобы компьютеры были разбиты на такие же рабочие группы или

домены и подразделения. Для этого администратор может воспользоваться функцией импорта структуры.

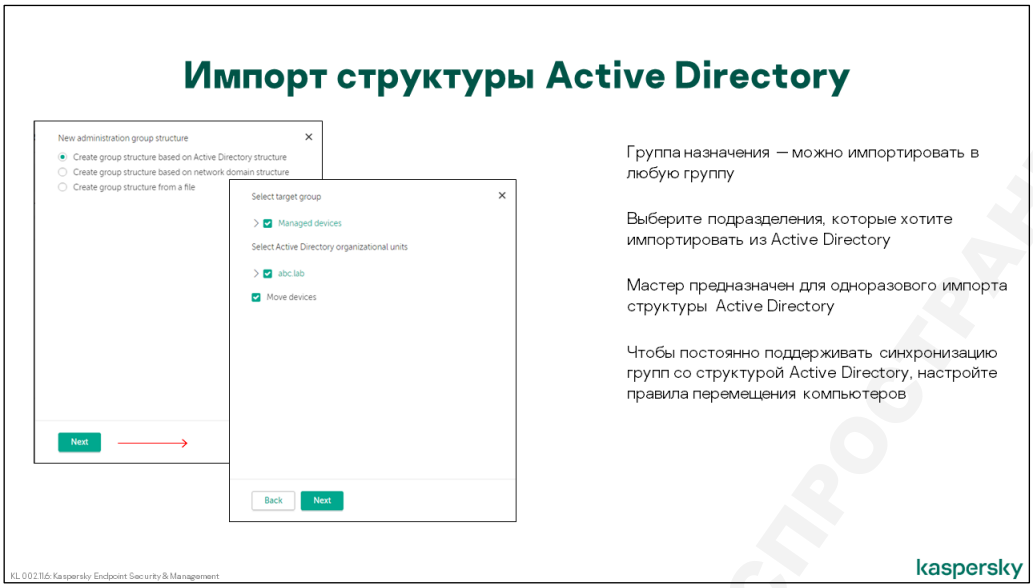
Импортировать можно структуру Windows-сети, структуру Active Directory и структуру, заданную текстовым файлом. В первых двух случаях импортировать можно или структуру целиком — группы с компьютерами, или только группы. При импорте структуры из текстового файла создаются только группы.

Импорт компьютеров затрагивает только нераспределенные компьютеры. Если часть компьютеров импортируемой рабочей группы или подразделения Active Directory уже находится в одной из групп управляемых компьютеров, в результате работы мастера они свое расположение не изменят.

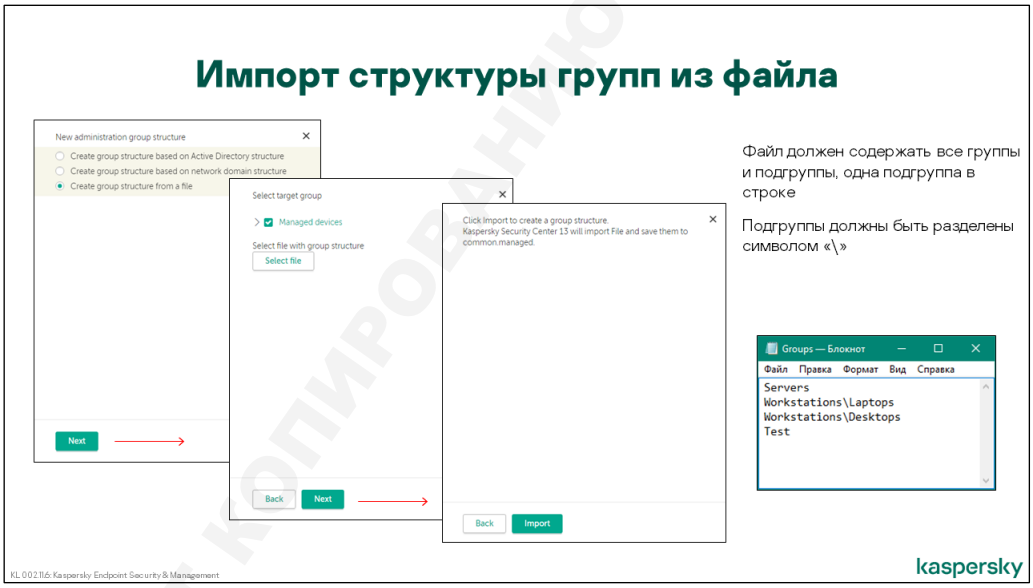
Чтобы запустить мастер, нужно выбрать группу **Управляемые устройства** выполнить команду **Импортировать**. В мастере нужно последовательно указать, какую структуру импортировать, и в какую группу. При импорте структуры Windows-сети или Active Directory можно отказаться от импорта компьютеров.



Структура Windows-сети и структура, заданная текстовым файлом, импортируются целиком. При импорте структуры Active Directory можно выбрать, какой домен или какое подразделение импортировать. Соседние домены и подразделения будут проигнорированы.



Мастер предназначен для облегчения первоначального создания структуры управляемых компьютеров. Он не предназначен для регулярной синхронизации структуры в Kaspersky Security Center, например, с Active Directory. Если стоит задача синхронизации, ее можно решить при помощи правил переноса компьютеров.



Текстовый файл для импорта нужно готовить вручную. Каждая группа или подгруппа задается отдельной строкой. Подгруппы задаются полным путем через «\», например:

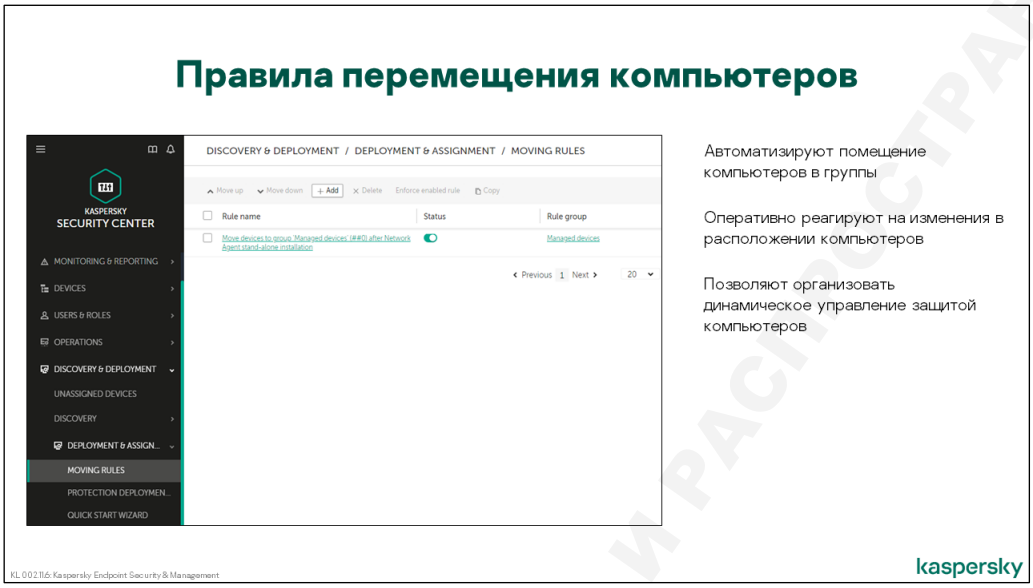
Офис1\Подразделение1\Отдел1
Офис1\Подразделение1\Отдел2
Офис2
Офис3\Подразделение1

Если в полном пути подгруппы есть еще не созданные группы, они автоматически создаются.

Созданные при импорте группы ничем не отличаются от созданных вручную. Их можно переименовывать, перемещать, удалять и т. д.

5.4 Как автоматически добавлять компьютеры в группы

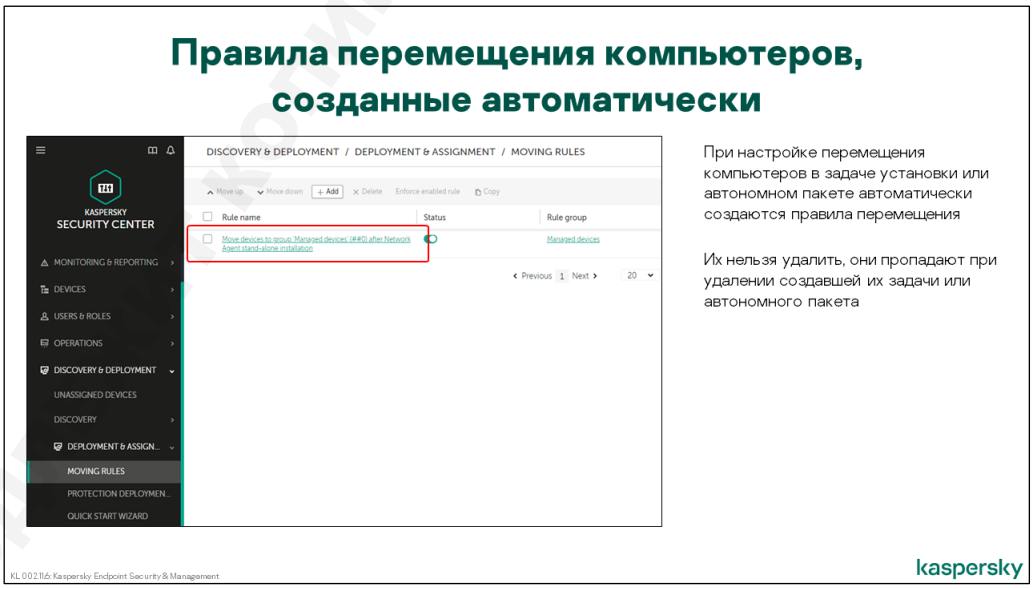
Правила перемещения компьютеров



Если группы в Kaspersky Security Center соответствуют IP-подсетям или подразделениям Active Directory, администратор может легко автоматизировать распределение компьютеров по группам. Для этого существуют правила перемещения компьютеров.

Список правил перемещения доступен на вкладке **Обнаружение устройств и развертывание | Развертывание и назначение | Правила перемещения**

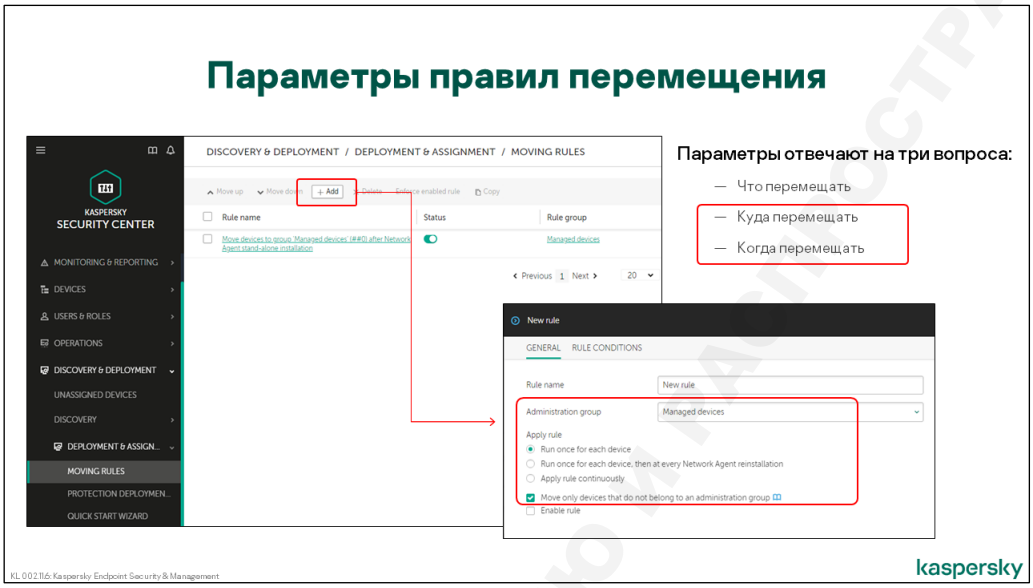
Правила, созданные задачами



В ряде сценариев Kaspersky Security Center автоматически создает правила перемещения компьютеров. Например, когда администратор в мастере удаленной установки или при создании

автономного пакета выбирает перемещать нераспределенные компьютеры в группу, Сервер администрирования для выполнения этой операции создает правило перемещения. Эти правила можно увидеть в списке и можно отключить, но нельзя удалить или отредактировать. Сервер удаляет их автоматически при удалении породившей их задачи или автономного пакета.

Настройки правил перемещения



Правило перемещения состоит из следующих естественных настроек:

— Что перемещать — набор условий, который применяется к компьютерам, чтобы решить, нужно их перемещать или нет

— Куда перемещать — имя группы в структуре управляемых компьютеров, куда будут перемещаться компьютеры, удовлетворяющие условиям правила

— Когда перемещать — при каких условиях правило будет применено автоматически

При создании правила нужно выбрать ему имя. Лучше, чтобы оно отражало суть правила, поскольку в списке видны только имена. Также нужно выбрать группу назначения — куда перемещать.

Когда применяются правила

После этого нужно решить, когда применять правило к компьютерам. Есть три возможности:

— Один раз для каждого устройства — в момент включения такое правило применяется ко всем компьютерам в базе Сервера, после чего применяется к каждому новому компьютеру при его обнаружении

— Один раз для каждого устройства и после каждой переустановки Агента — отличается от предыдущего тем, что если на каком-то компьютере Агент был переустановлен, правило применяется к нему повторно

— Постоянно — правило действует перманентно, если удовлетворяющий правилу компьютер переместить в другую группу, Сервер администрирования тут же вернет его на место согласно правилу. Или если атрибуты компьютера изменились, постоянно действующее правило на это отреагируют, а однократное — нет.

Правила, которые Сервер администрирования создает автоматически для задач установки и автономных пакетов, применяются в режиме **Один раз для каждого устройства и после каждой переустановки Агента**.

На практике постоянно действующие правила могут быть удобнее, но сопряжены с постоянной загрузкой вычислительных ресурсов Сервера администрирования.

Условия в правилах перемещения

Перемещать управляемые компьютеры

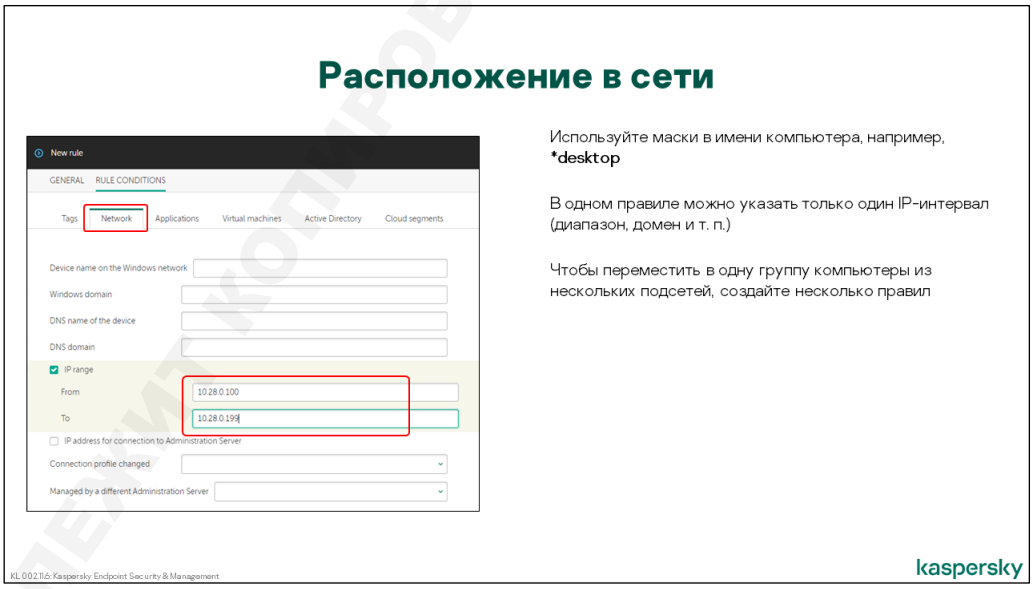
Остальные настройки правила задают условия, которым должен удовлетворять компьютер, чтобы правило на него подействовало. Первое такое условие находится в разделе **Общие** и называется **Перемещать только устройства, не размещенные в группах администрирования**.

С этой опцией правило — даже постоянного действия — не будет мешать администратору вручную перемещать компьютеры между группами. Оно затронет только нераспределенные компьютеры. Чтобы применить такое правило к отдельному компьютеру, уже находящемуся в группе, достаточно компьютер из группы удалить. При удалении из структуры управляемых компьютеров компьютер снова становится нераспределенным и попадает под действие правила.

Без опции **Перемещать только устройства, не размещенные в группах администрирования** правило действует на все компьютеры в базе и намертво привязывает компьютеры к назначенной им группе. Впрочем, намертво только в том смысле, что их нельзя переместить в другую группу. Удалить их из базы Сервера администрирования можно без препятствий.

Остальные условия расположены в дополнительных секциях в свойствах правила.

Перемещать компьютеры по именам и IP-адресам



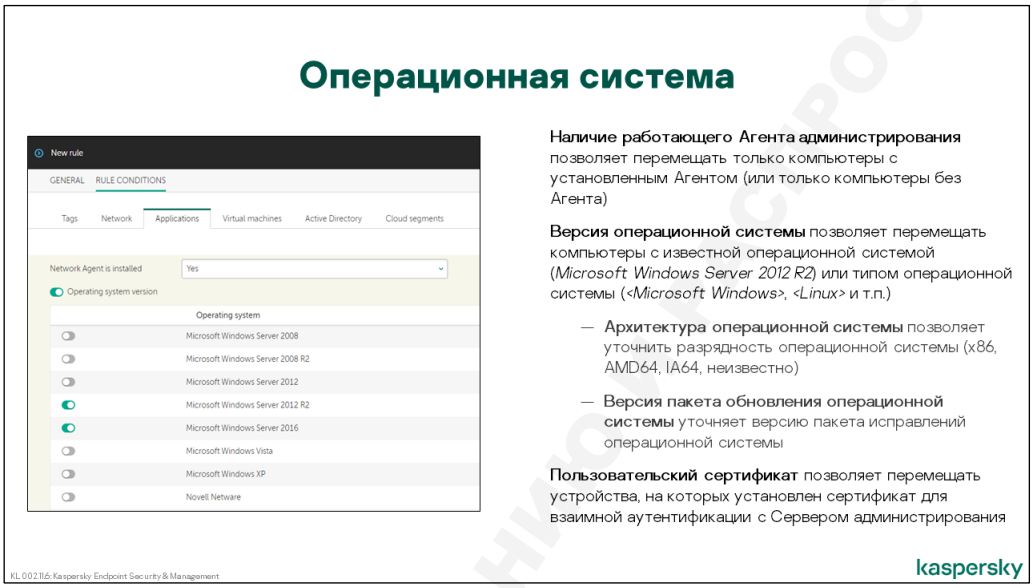
Многие условия для перемещения касаются сетевых атрибутов компьютера:

- NetBIOS-имя
- Имя домена или рабочей группы
- DNS-имя
- DNS-домен

— IP-адрес
— IP-адрес подключения к Серверу (если компьютер находится за NAT-шлюзом, адресом подключения будет адрес шлюза)

Чтобы охватить правилом не один компьютер, а несколько, для IP-адресов можно указать интервал, а в именах можно использовать маски: «*» и «?». Если этих параметров недостаточно, можно создать несколько правил с разными условиями, которые будут помещать компьютеры в одну группу.

Перемещать компьютеры по операционным системам



Условия для устройств могут включать версию операционной системы, а также ее архитектуру и номер пакета обновлений (Service Pack). В одном правиле можно указать несколько операционных систем. Если администратор хочет автоматически перемещать все сервера в группу Servers, ему будет достаточно одного правила для всех серверных версий Windows, используемых в сети. Например, для Windows Server 2008 R2 и Windows Server 2012 R2.

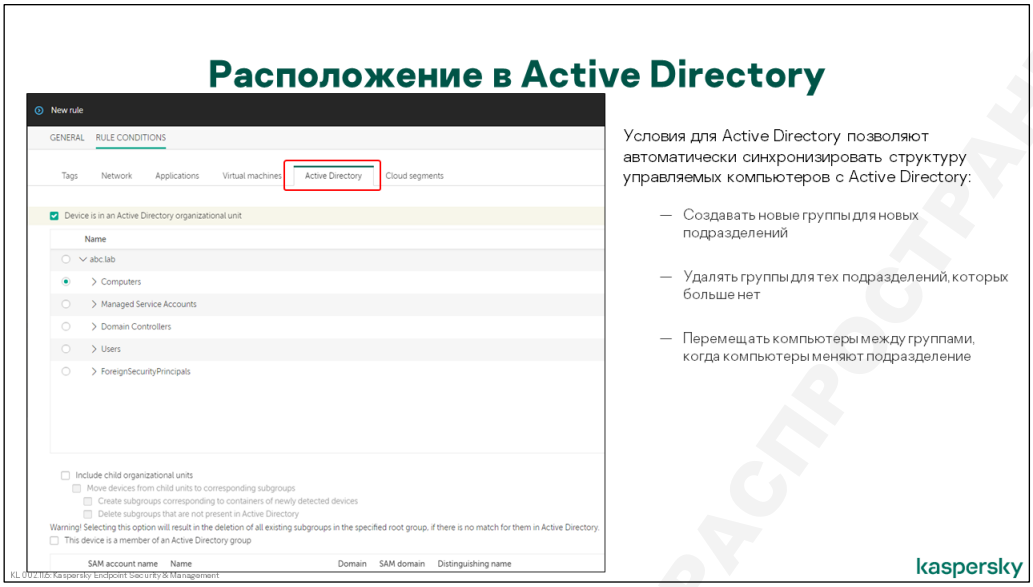
Также условия для компьютеров могут включать наличие работающего Агента администрирования. Этим условием можно отделить компьютеры, уже подключенные к Серверу администрирования, от компьютеров, ожидающих подключения.

Остальные условия

В правиле перемещения есть условия для виртуальных машин. Виртуальные машины на разных платформах виртуализации можно переместить в разные группы. О защите виртуальных машин рассказывает курс KL 031 Kaspersky Security для виртуальных сред. Легкий агент.

Если этих условий не хватает, компьютеры можно пометить метками (тегами) и настроить условия по тегам. Эта тему раскрывает курс KL 302.

Как синхронизировать группы с Active Directory



Есть аналогичные условия и для расположения компьютеров в структуре Active Directory:

— Имя подразделения Active Directory
— Имя группы в Active Directory

Правила перемещения позволяют организовать полную синхронизацию с Active Directory. Для этого нужно включить дополнительные опции, относящиеся к условию **Применить правило к подразделению Active Directory**:

— **Включая дочерние подразделения** — если в выбранном подразделении есть дочерние подразделения, компьютеры из них будут перемещены в группу назначения

— **Перемещать компьютеры из дочерних организационных единиц в соответствующие подгруппы** — если в выбранном подразделении есть дочернее подразделение, а в группе назначения есть одноименная подгруппа, компьютеры из дочернего подразделения будут перемещены в одноименную подгруппу

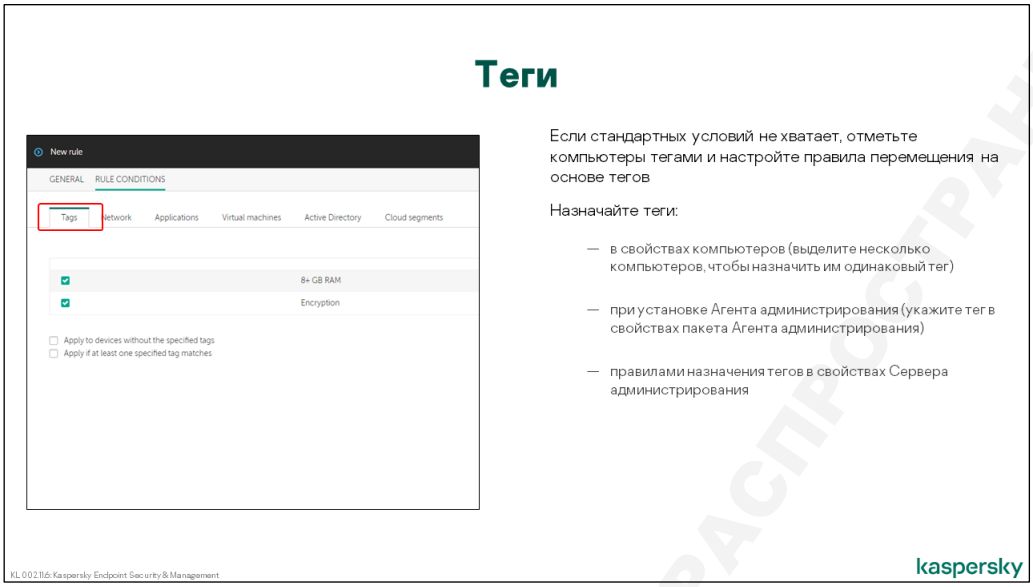
— **Создавать отсутствующие подгруппы** — если в выбранном подразделении есть дочернее подразделение, а в группе назначения нет одноименной подгруппы, Сервер администрирования создаст такую подгруппу и переместит в нее компьютеры дочернего подразделения

— **Удалять подгруппы, отсутствующие в Active Directory** — антипод предыдущей опции. Когда подразделение удаляется из Active Directory, эта опция удалит соответствующую группу из Kaspersky Security Center.

Если включить все четыре этих опции, в группе назначения будет создана постоянно обновляемая копия структуры Active Directory. Если в Active Directory будут появляться или исчезать подразделения, или компьютеры будут перемещаться из одного подразделения в другое, Kaspersky Security Center автоматически отразит эти изменения в структуре группы назначения.

Кроме подразделений в Active Directory есть группы, куда могут входить учетные записи компьютеров. Чтобы перенести в группы компьютеры, которые входят в доменную группу, отметьте условие **Устройство является членом группы Active Directory** и выберите имя группы.

Теги



Теги — это дополнительный атрибут, который администратор может назначить устройствам, и использовать для более гибкой настройки правил перемещения. Администратор может назначать теги вручную одному или сразу нескольким выбранным устройствам, а может настроить правила автоматического назначения тегов. Одному устройству может быть назначено несколько тегов.

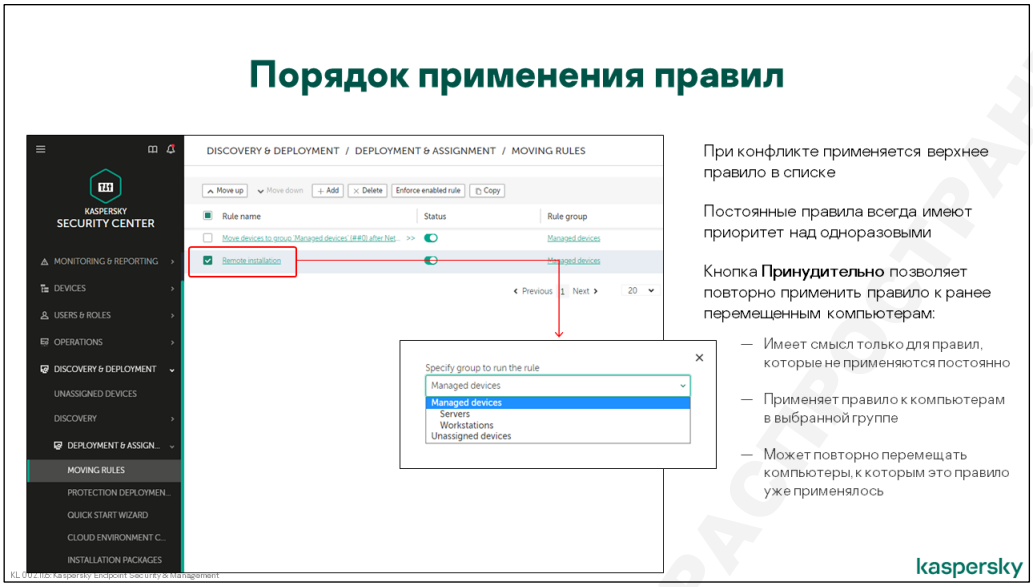
Правила перемещения могут применяться к устройствам без выбранных тегов или к устройствам, у которых есть хотя бы один из выбранных тегов.

Чтобы назначить теги, выберите одно или несколько устройств, откройте окно свойств и перейдите во вкладку **Теги**. В этой же вкладке есть ссылка *Настроить правила автоматического назначения тегов.* Правила автоматического назначения тегов можно настроить на вкладке **Устройства | Теги | Правила автоматического назначения тегов**.

В ряде случаев теги имеет смысл назначать сразу при развертывании средств защиты. Сделать это можно в свойствах пакета Агента администрирования. Чтобы при установке назначить компьютерам разные теги, сделайте несколько пакетов установки Агента администрирования, включите в каждом пакете нужный тег, и используйте пакеты с разными тегами для установки на разные компьютеры.

Вне зависимости, на каком устройстве и как был добавлен тег, он будет доступен для выбора в свойствах любого устройства.

Порядок применения правил



Созданные правила организованы в список и порядок правил имеет значение. Постоянно действующие правила, очевидно, имеют приоритет над остальными. Среди правил одного типа применяется верхнее из подходящих. Иными словами, если компьютер удовлетворяет условиям нескольких правил, сработает только самое верхнее.

Порядок правил можно менять стрелками. Кроме этого правила можно применять вручную с помощью кнопки **Принудительно**. Это позволяет повторно применить непостоянное правило. Постоянным правилам эта кнопка ничего не дает, поскольку постоянные правила и так непрерывно форсируются.

Мастер форсирования просит выбрать группу, в которой нужно применить правило, и переместит компьютеры, которые удовлетворяют условиям правила из выбранной группы в группу, заданную в правиле. Есть возможность пропускать компьютеры, к которым правило уже было применено, и применять его только к новым компьютерам.