KASPERSKY lab

Kaspersky Security Center 10

Руководство по внедрению

Версия программы: 10 Service Pack 2, Maintenance Release 1

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, «Лаборатория Касперского» ответственности не несет.

Дата редакции документа: 07.12.2016

http://www.kaspersky.ru
https://help.kaspersky.com
http://support.kaspersky.ru

Содержание

Об этом документе

Руководство по внедрению Kaspersky Security Center 10 (далее «Kaspersky Security Center») адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security Center, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security Center.

Вы можете применять информацию в этом руководстве для выполнения следующих задач:

- планирование установки программы (учитывая принципы работы программы, системные требования, типовые схемы развертывания, особенности совместимости с другими программами);
- подготовка к установке, установка и активация Kaspersky Security Center;
- настройка программы после установки.

Также из этого руководства вы можете узнать об источниках информации о программе и способах получения технической поддержки.

В этом разделе

В этом документе

Руководство по внедрению Kaspersky Security Center содержит введение, разделы с описанием установки компонентов программы и настройки их взаимодействия, разделы, описывающие развертывание антивирусной защиты сети, разделы с информацией о нагрузочном тестировании, а также глоссарий.

Источники информации о программе (см. стр. 14)

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

Kaspersky Security Center (см. стр. 17)

В этом разделе представлена информация о назначении, ключевых возможностях и составе программы Kaspersky Security Center.

Архитектура программы (см. стр. 19)

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

Аппаратные и программные требования (см. стр. 20)

Этот раздел содержит сведения о программных и аппаратных требованиях к клиентским устройствам сети.

Сведения о производительности Сервера администрирования (см. стр. 36)

В разделе представлены результаты тестирования производительности Сервера администрирования для разных аппаратных конфигураций.

Типовые схемы развертывания системы защиты (см. стр. 40)

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

Развертывание системы защиты внутри организации (см. стр. 42)

В этом разделе описаны процессы развертывания системы защиты внутри организации, соответствующие типовым схемам развертывания.

Развертывание системы защиты в сети организации-клиента (см. стр. 46)

В этом разделе описаны процессы развертывания системы защиты в сети организации-клиента, соответствующие типовым схемам развертывания.

Развертывание Сервера администрирования (см. стр. 51)

В этом разделе описаны этапы развертывания Сервера администрирования.

Настройка системы защиты сети организации-клиента (см. стр. 93)

В этом разделе описаны особенности настройки системы защиты через Консоль администрирования в сети организации-клиента.

Удаленная установка программ (см. стр. 99)

В этом разделе описаны способы удаленной установки программ «Лаборатории Касперского» и их удаления с устройств сети.

Локальная установка программ (см. стр. 124)

В этом разделе описана процедура установки программ, которые могут быть установлены на устройства только локально.

Развертывание систем управления мобильными устройствами (см. стр. 134)

В этом разделе описано развертывание систем управления мобильных устройств по протоколам Exchange ActiveSync®, iOS MDM и Kaspersky Endpoint Security.

Развертывание Self Service Portal (см. стр. 156)

В этом разделе описаны подготовка к развертыванию Self Service Portal и шаги развертывания Self Service Portal.

Настройка SMS-рассылки в Kaspersky Security Center (см. стр. 162)

В этом разделе описана установка утилиты Kaspersky SMS Broadcasting на мобильное устройство, синхронизация утилиты с Сервером администрирования и настройка SMS-рассылки в Консоли администрирования.

Нагрузка на сеть (см. стр. 166)

В этом разделе приводится информация об объеме сетевого трафика, которым обмениваются между собой клиентские устройства и Сервер администрирования в ходе выполнения ключевых административных операций.

Скорость заполнения событиями базы данных Сервера администрирования (см. стр. 173)

В этом разделе приведены примеры скорости заполнения базы данных Сервера администрирования событиями, возникающими в работе управляемых программ.

Обращение в Службу технической поддержки (см. стр. 174)

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Глоссарий

В разделе перечислены термины, используемые в этом документе.

АО «Лаборатория Касперского» (см. стр. 187)

В этом разделе приведена информация об АО «Лаборатория Касперского».

Информация о стороннем коде (см. стр. 190)

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках (см. стр. 191)

В этом разделе приведены уведомления о зарегистрированных товарных знаках.

Предметный указатель

С помощью этого раздела вы можете быстро найти необходимые сведения в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком «Пример».
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.

Пример текста	Описание условного обозначения
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком «стрелка».
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В этом разделе

Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Security Center:

- страница Kaspersky Security Center на веб-сайте «Лаборатории Касперского»;
- страница Kaspersky Security Center на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 174).

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Security Center на веб-сайте «Лаборатории Касперского»

На странице Kaspersky Security Center (http://www.kaspersky.ru/security-center) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security Center содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Security Center в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Security Center в Базе знаний (http://support.kaspersky.ru/ksc10) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Security Center, но и к другим программам «Лаборатории Касперского». Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

Программа содержит файлы полной и контекстной справки.

В полной справке вы можете найти информацию о настройке и использовании Kaspersky Security Center.

В контекстной справке вы можете найти информацию об окнах Kaspersky Security Center: описание параметров Kaspersky Security Center и ссылки на описания задач, в которых используются эти параметры.

Справка может быть включена в состав программы либо располагаться онлайн на веб-ресурсе «Лаборатории Касперского». Если справка расположена онлайн, то при ее вызове будет открыто окно браузера. Для отображения онлайн-справки требуется соединение с интернетом.

Документация

В состав документации к программе входят файлы руководств.

В руководстве администратора вы можете найти информацию о настройке и использовании Kaspersky Security Center.

В руководстве по внедрению вы можете найти информацию для выполнения следующих задач:

- планирование установки программы (учитывая принципы работы программы, системные требования, типовые схемы развертывания, особенности совместимости с другими программами);
- подготовка к установке, установка и активация Kaspersky Security Center;
- настройка программы после установки.

В руководстве «Начало работы» вы можете найти информацию для быстрого начала работы с программой (описание интерфейса и основных задач, которые можно выполнять с помощью Kaspersky Security Center).

Обсуждение программ «Лаборатории Касперского» на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме (http://forum.kaspersky.com).

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Kaspersky Security Center

В этом разделе представлена информация о назначении, ключевых возможностях и составе программы Kaspersky Security Center.

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

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

При помощи Kaspersky Security Center вы можете:

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

  Под *организациями-клиентами* здесь подразумеваются организации, антивирусную защиту которых обеспечивает сервис-провайдер.

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

- Управлять системой антивирусной безопасности, построенной на основе программ «Лаборатории Касперского».

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

- Удаленно управлять программами «Лаборатории Касперского» и других производителей, установленными на клиентских устройствах: устанавливать обновления, искать и закрывать уязвимости.

- Централизованно распространять ключи программ «Лаборатории Касперского» на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.
- Получать статистику и отчеты о работе программ и устройств.
- Получать уведомления о критических событиях в работе программ «Лаборатории Касперского».
- Управлять мобильными устройствами, поддерживающими протоколы Kaspersky Security для Android™, Exchange ActiveSync® или iOS Mobile Device Management (iOS MDM).
- Управлять шифрованием информации, хранящейся на жестких дисках устройств и съемных дисках, и доступом пользователей к зашифрованным данным.
- Проводить инвентаризацию оборудования, подключенного к сети организации.
- Централизованно работать с файлами, помещенными программами защиты на карантин или в резервное хранилище, а также с файлами, обработка которых программами защиты отложена.

Архитектура программы

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

Программа Kaspersky Security Center включает в себя следующие основные компоненты:

- **Сервер администрирования** (далее также *Сервер*). Осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.
- **Агент администрирования** (далее также *Агент*). Осуществляет взаимодействие между Сервером администрирования и программами «Лаборатории Касперского», установленными на сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех программ, разработанных для систем Microsoft® Windows®. Для программ «Лаборатории Касперского», разработанных для систем Novell® и Unix™, существуют отдельные версии Агента администрирования.
- **Консоль администрирования** (далее также *Консоль*). Предоставляет пользовательский интерфейс к административным службам Сервера и Агента. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC). Консоль администрирования позволяет подключаться к удаленному Серверу администрирования через интернет.
- **Сервер мобильных устройств**. Предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.
- **Kaspersky Security Center 10 Web Console**. Предназначена для контроля состояния системы защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center.

Аппаратные и программные требования

Сервер администрирования

Аппаратные требования:

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

Программные требования:

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

Операционная система:

- Microsoft Windows 10 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro RS1 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS1 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS1 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Pro RS2 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS2 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS2 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Professional SP1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Enterprise SP1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Ultimate SP1 32-разрядная / 64-разрядная;
- Microsoft Small Business Server 2008 Standard 64-разрядная;
- Microsoft Small Business Server 2008 Premium 64-разрядная;
- Microsoft Small Business Server 2011 Essentials 64-разрядная;
- Microsoft Small Business Server 2011 Premium Add-on 64-разрядная;
- Microsoft Small Business Server 2011 Standard 64-разрядная;
- Microsoft Windows Server® 2008 Datacenter SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008;
- Windows Server 2008 SP1;

- Microsoft Windows Server 2008 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-разрядная;
- Microsoft Windows Server 2008 R2 Standard 64-разрядная;
- Microsoft Windows Server 2008 R2 Standard SP1 64-разрядная;
- Microsoft Windows Server 2012 Server Core 64-разрядная;
- Microsoft Windows Server 2012 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 Essentials 64-разрядная;
- Microsoft Windows Server 2012 Foundation 64-разрядная;
- Microsoft Windows Server 2012 Standard 64-разрядная;
- Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
- Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2012 R2 Standard 64-разрядная;
- Windows Storage Server 2008 R2 64-разрядная;
- Windows Storage Server 2012 64-разрядная;

- Windows Storage Server 2012 R2 64-разрядная;
- Windows Server 2016 Datacenter Edition 64-разрядная;
- Windows Server 2016 Standard Edition 64-разрядная.

Сервер баз данных (может быть установлен на другом компьютере):

- Microsoft SQL Server® 2008 Express 32-разрядная;
- Microsoft SQL 2008 R2 Express 64-разрядная;
- Microsoft SQL 2012 Express 64-разрядная;
- Microsoft SQL 2014 Express 64-разрядная;
- Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная;
- Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная;
- Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная;
- Microsoft SQL Server 2012 (все редакции) 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft Azure SQL Database;
- MySQL 5.5 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.5 32-разрядная / 64-разрядная;
- MySQL 5.6 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.6 32-разрядная / 64-разрядная;
- MySQL 5.7 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.7 32-разрядная / 64-разрядная.

Поддерживаются следующие виртуальные платформы:

- VMware vSphere™ 5.5;
- VMware vSphere 6;
- VMware™ Workstation 12.x Pro;
- Microsoft Hyper-V® Server 2008;
- Microsoft Hyper-V Server 2008 R2;
- Microsoft Hyper-V Server 2008 R2 SP1;
- Microsoft Hyper-V Server 2012;
- Microsoft Hyper-V Server 2012 R2;
- Microsoft Virtual PC 2007 (6.0.156.0);
- Citrix® XenServer® 6.2;
- Citrix XenServer 6.5;
- Citrix XenServer 7;
- Parallels Desktop 11;
- Oracle® VM VirtualBox 4.0.4-70112 (поддерживаются гостевые операционные системы Windows).

Для установки Сервера администрирования на устройства с операционной системой Microsoft Windows Server 2008 необходимо использовать пакет установки «lite». Перед установкой Сервера администрирования необходимо самостоятельно установить базу данных, например, Microsoft SQL Server 2014.

Kaspersky Security Center 10 Web Console

Аппаратные требования:

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

Программные требования:

- Для работы под управлением операционных систем Microsoft Windows с установленным Сервером администрирования Kaspersky Security Center версии Service Pack 2:
  - Microsoft Windows 10 Pro 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Enterprise 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Education 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Pro RS1 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Enterprise RS1 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Education RS1 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Pro RS2 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Enterprise RS2 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Education RS2 32-разрядная / 64-разрядная;
  - Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
  - Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
  - Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;
  - Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная;
  - Microsoft Windows 7 Professional SP1 32-разрядная / 64-разрядная;

- Microsoft Windows 7 Enterprise SP1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Ultimate SP1 32-разрядная / 64-разрядная;
- Microsoft Small Business Server 2008 Standard 64-разрядная;
- Microsoft Small Business Server 2008 Premium 64-разрядная;
- Microsoft Small Business Server 2011 Essentials 64-разрядная;
- Microsoft Small Business Server 2011 Premium Add-on 64-разрядная;
- Microsoft Small Business Server 2011 Standard 64-разрядная;
- Microsoft Windows Server® 2008 Datacenter SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008;
- Windows Server 2008 SP1;
- Microsoft Windows Server 2008 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-разрядная;
- Microsoft Windows Server 2008 R2 Standard 64-разрядная;

- Microsoft Windows Server 2008 R2 Standard SP1 64-разрядная;
- Microsoft Windows Server 2012 Server Core 64-разрядная;
- Microsoft Windows Server 2012 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 Essentials 64-разрядная;
- Microsoft Windows Server 2012 Foundation 64-разрядная;
- Microsoft Windows Server 2012 Standard 64-разрядная;
- Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
- Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2012 R2 Standard 64-разрядная;
- Windows Storage Server 2008 R2 64-разрядная;
- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Windows Server 2016 Datacenter Edition 64-разрядная;
- Windows Server 2016 Standard Edition 64-разрядная;
- Debian GNU/Linux® 7.x 32-разрядная;
- Debian GNU/Linux 7.x 64-разрядная;
- Ubuntu Server 14.04 LTS 32-разрядная;
- Ubuntu Server 14.04 LTS 64-разрядная;
- CentOS 6.x (до 6.6) 64-разрядная.

Kaspersky Security Center 10 Web Console не поддерживает версии операционных систем, работающих с systemd, например, Fedora® 17.

Веб-сервер:

- Apache 2.4.25 (для Windows) 32-разрядный;
- Apache 2.4.25 (для Linux) 32-разрядный / 64-разрядный.

Для работы с Kaspersky Security Center 10 Web Console можно использовать следующие браузеры:

- Microsoft Internet Explorer® 9 и выше;
- Microsoft® Edge;
- Chrome™ 53 и выше;
- Firefox™ 47 и выше;
- Safari® 8 под управлением Mac OS X 10.10 (Yosemite);
- Safari 9 под управлением Mac OS X 10.11 (El Capitan).

Сервер мобильных устройств iOS Mobile Device Management (iOS MDM)

Аппаратные требования:

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

Программные требования: операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования).

Сервер мобильных устройств Exchange ActiveSync

Программные и аппаратные требования для Сервера мобильных устройств Exchange ActiveSync полностью включены в требования для сервера Microsoft Exchange Server.

Поддерживается работа с Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 и Microsoft Exchange Server 2013.

Консоль администрирования

Аппаратные требования:

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

Программные требования:

- Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования);
- Microsoft Management Console 2.0;
- Microsoft Windows Installer 4.5;
- Microsoft Internet Explorer 7.0 и выше при работе с Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 или Microsoft Windows Vista®;
- Microsoft Internet Explorer 8.0 и выше при работе с Microsoft Windows 7;
- Microsoft Internet Explorer 10.0 и выше при работе с Microsoft Windows 8 и 10;
- Microsoft Edge при работе с Microsoft Windows 10.

Агент администрирования

Аппаратные требования:

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

Если устройство, на котором установлен Агент администрирования, будет дополнительно выполнять роль агента обновлений, это устройство должно удовлетворять следующим аппаратным требованиям:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 1 ГБ.
- Объем свободного места на диске: 4 ГБ.

Программные требования:

- Windows Embedded POSReady 7 32-разрядная / 64-разрядная;
- Windows Embedded Standard 7 SP1 32-разрядная / 64-разрядная;
- Windows Embedded 8 Standard 32-разрядная / 64-разрядная;
- Windows Embedded 8 Industry Pro 32-разрядная / 64-разрядная;
- Windows Embedded 8 Industry Enterprise 32-разрядная / 64-разрядная;
- Windows Embedded 8.1 Industry Pro 32-разрядная / 64-разрядная;
- Windows Embedded 8.1 Industry Enterprise 32-разрядная / 64-разрядная;
- Windows Embedded 8.1 Industry Update 32-разрядная / 64-разрядная;
- Windows 10 Home 32-разрядная / 64-разрядная;
- Windows 10 Pro 32-разрядная / 64-разрядная;
- Windows 10 Enterprise 32-разрядная / 64-разрядная;
- Windows 10 Education 32-разрядная / 64-разрядная;
- Windows 10 Home RS1 32-разрядная / 64-разрядная;
- Windows 10 Pro RS1 32-разрядная / 64-разрядная;
- Windows 10 Enterprise RS1 32-разрядная / 64-разрядная;
- Windows 10 Education RS1 32-разрядная / 64-разрядная;

- Windows 10 Home RS2 32-разрядная / 64-разрядная;
- Windows 10 Pro RS2 32-разрядная / 64-разрядная;
- Windows 10 Enterprise RS2 32-разрядная / 64-разрядная;
- Windows 10 Education RS2 32-разрядная / 64-разрядная;
- Microsoft Windows 2000 Server;
- Windows 8.1 Pro 32-разрядная / 64-разрядная;
- Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
- Windows 8 Pro 32-разрядная / 64-разрядная;
- Windows 8 Enterprise 32-разрядная / 64-разрядная;
- Windows 7 Professional SP1 32-разрядная / 64-разрядная;
- Windows 7 Enterprise SP1 32-разрядная / 64-разрядная;
- Windows 7 Ultimate SP1 32-разрядная / 64-разрядная;
- Windows 7 Professional 32-разрядная / 64-разрядная;
- Windows 7 Enterprise 32-разрядная / 64-разрядная;
- Windows 7 Ultimate 32-разрядная / 64-разрядная;
- Windows 7 Home Basic 32-разрядная / 64-разрядная;
- Windows 7 Premium 32-разрядная / 64-разрядная;
- Windows Vista Business SP1 32-разрядная / 64-разрядная;
- Windows Vista Enterprise SP1 32-разрядная / 64-разрядная;
- Windows Vista Ultimate SP1 32-разрядная / 64-разрядная;
- Windows Vista Business SP2 32-разрядная / 64-разрядная;
- Windows Vista Enterprise SP2 32-разрядная / 64-разрядная;
- Windows Vista Ultimate SP2 32-разрядная / 64-разрядная;

- Windows XP Professional SP3 32-разрядная;
- Windows XP Professional SP2 32-разрядная / 64-разрядная;
- Windows XP Home SP3 32-разрядная;
- Essential Business Server 2008 64-разрядная;
- Small Business Server 2003 Standard SP1 32-разрядная;
- Small Business Server 2003 Premium SP1 32-разрядная;
- Small Business Server 2008 Standard 64-разрядная;
- Small Business Server 2008 Premium 64-разрядная;
- Small Business Server 2011 Essentials 64-разрядная;
- Small Business Server 2011 Premium Add-on 64-разрядная;
- Small Business Server 2011 Standard 64-разрядная;
- Windows Home Server 2011 64-разрядная;
- Windows MultiPoint™ Server 2011 64-разрядная;
- Windows Server 2003 Enterprise SP2 32-разрядная / 64-разрядная;
- Windows Server 2003 Standard SP2 32-разрядная / 64-разрядная;
- Windows Server 2003 R2 Enterprise SP2 32-разрядная / 64-разрядная;
- Windows Server 2003 R2 Standard SP2 32-разрядная / 64-разрядная;
- Windows Server 2008 Datacenter SP1 32-разрядная / 64-разрядная;
- Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная;
- Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная;
- Windows Server 2008 SP1 Server Core 32-разрядная / 64-разрядная;
- Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная;
- Windows Server 2008 32-разрядная / 64-разрядная;

- Windows Server 2008 R2 Server Core 64-разрядная;
- Windows Server 2008 R2 Datacenter 64-разрядная;
- Windows Server 2008 R2 Datacenter SP1 64-разрядная;
- Windows Server 2008 R2 Enterprise 64-разрядная;
- Windows Server 2008 R2 Enterprise SP1 64-разрядная;
- Windows Server 2008 R2 Foundation 64-разрядная;
- Windows Server 2008 R2 Foundation SP1 64-разрядная;
- Windows Server 2008 R2 SP1 Core Mode 64-разрядная;
- Windows Server 2008 R2 Standard 64-разрядная;
- Windows Server 2008 R2 Standard SP1 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная;
- Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2012 Essentials 64-разрядная;
- Windows Server 2012 Foundation 64-разрядная;
- Windows Server 2012 Standard 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2012 R2 Datacenter 64-разрядная;
- Windows Server 2012 R2 Essentials 64-разрядная;
- Windows Server 2012 R2 Foundation 64-разрядная;
- Windows Server 2012 R2 Standard 64-разрядная;
- Windows Server 2016 Datacenter Edition;
- Windows Server 2016 Standard Edition;
- Windows Nano Server 2016;

- Windows Storage Server 2008 R2 64-разрядная;
- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Debian GNU / Linux 8.x 32-разрядная;
- Debian GNU / Linux 8.x 64-разрядная;
- Debian GNU / Linux 7.x (до 7.8) 32-разрядная;
- Debian GNU / Linux 7.x (до 7.8) 64-разрядная;
- Ubuntu Server 16.04 LTS x32 32-разрядная;
- Ubuntu Server 16.04 LTS x64 64-разрядная;
- Ubuntu Server 14.04 LTS x32 32-разрядная;
- Ubuntu Server 14.04 LTS x64 64-разрядная;
- Ubuntu Desktop 16.04 LTS x32 32-разрядная;
- Ubuntu Desktop 16.04 LTS x64 64-разрядная;
- Ubuntu Desktop 14.04 LTS x32 32-разрядная;
- Ubuntu Desktop 14.04 LTS x64 64-разрядная;
- CentOS 6.x (до 6.6) 64-разрядная;
- CentOS 7.0 64-разрядная;
- Red Hat Enterprise Linux Server 7.0 64-разрядная;
- SUSE Linux Enterprise Server 12 64-разрядная;
- SUSE Linux Enterprise Desktop 12 64-разрядная;
- Mac OS X® 10.4 (Tiger®);
- Mac OS X 10.5 (Leopard®);
- Mac OS X 10.6 (Snow Leopard®);

- OS X 10.7 (Lion);
- OS X 10.8 (Mountain Lion);
- OS X 10.9 (Mavericks);
- OS X 10.10 (Yosemite);
- OS X 10.11 (El Capitan);
- macOS® Sierra (10.12);
- VMware vSphere™ 5.5;
- VMware vSphere 6;
- VMware Workstation 9.x;
- VMware Workstation 10.x;
- VMware Workstation 11.x;
- VMware Workstation 12.x Pro;
- Microsoft Hyper-V Server 2008;
- Microsoft Hyper-V Server 2008 R2;
- Microsoft Hyper-V Server 2008 R2 SP1;
- Microsoft Hyper-V Server 2012;
- Microsoft Hyper-V Server 2012 R2;
- Citrix XenServer 6.2;
- Citrix XenServer 6.5;
- Citrix XenServer 7.

Вы можете получить сведения о последней версии аппаратных и программных требований на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center, в разделе «Системные требования» (http://support.kaspersky.ru/ksc10#requirements).

Сведения о производительности Сервера администрирования

В разделе представлены результаты тестирования производительности Сервера администрирования для разных аппаратных конфигураций.

Результаты тестов производительности Сервера администрирования позволили определить максимальные количества клиентских устройств, с которыми Сервер администрирования может выполнить синхронизацию за указанные периоды времени. Эта информация может использоваться для выбора оптимальных схем развертывания антивирусной защиты в компьютерных сетях организаций.

Для тестирования использовались следующие аппаратные конфигурации Сервера администрирования:

- 32-разрядная операционная система (двухъядерный процессор Intel® Core™2 Duo E8400 с тактовой частотой 3,00 ГГц, 4 ГБ ОЗУ, жесткий диск SATA 500 ГБ);
- 64-разрядная операционная система (четырехъядерный процессор Intel Xeon® E5450 с тактовой частотой 3,00 ГГц, 8 ГБ ОЗУ, жесткий диск SAS 2x320 RAID 0).

Сервер базы данных Microsoft SQL 2005x32 Enterprise Edition был установлен на том же клиентском устройстве, что и Сервер администрирования.

Сервер администрирования обеих аппаратных конфигураций поддерживал создание 200 виртуальных Серверов администрирования.

Таблица 2. Обобщенные результаты нагрузочного тестирования Сервера администрирования на 32-разрядной операционной системе

Период синхронизации, мин.	Количество управляемых устройств
15	5 000
30	10 000
45	15 000
60	20 000

Таблица 3. Обобщенные результаты нагрузочного тестирования Сервера администрирования на 64-разрядной операционной системе

Период синхронизации, мин.	Количество управляемых устройств
15	10 000
30	20 000
45	30 000
60	40 000

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать программу для управления более чем 5 000 устройств.

Выбор структуры системы защиты организации

Выбор структуры системы защиты организации определяют следующие факторы:

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

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

Для анализа сетевой и аппаратной инфраструктуры рекомендуется следующий порядок действий:

1. Определить следующие параметры сети, в которой будет развертываться защита:
    - число сегментов сети;
    - скорость каналов связи между отдельными сегментами сети;
    - число управляемых устройств в каждом из сегментов сети;
    - пропускную способность каждого канала связи, которая может быть выделена для функционирования защиты.

2. Определить допустимое время выполнения ключевых операций администрирования для всех управляемых устройств.

3. Проанализировать информацию из пунктов 1 и 2, а также данные нагрузочного тестирования системы администрирования (см. раздел «Нагрузка на сеть» на стр. 166). На основании проведенного анализа ответить на следующие вопросы:

   - Возможно ли обслуживание всех клиентов одним Сервером администрирования или требуется иерархия Серверов администрирования?
   - Какая аппаратная конфигурация Серверов администрирования требуется для обслуживания всех клиентов за время, определенное в пункте 2?
   - Требуется ли использование агентов обновлений для снижения нагрузки на каналы связи?

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

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

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

Типовые схемы развертывания системы защиты

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

Необходимо обеспечить защиту системы от несанкционированного доступа всех видов. Рекомендуется перед установкой программы на устройство установить все доступные обновления безопасности операционной системы.

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

- Развертывание системы защиты средствами Kaspersky Security Center одним из следующих способов:
  - через Консоль администрирования;
  - через Kaspersky Security Center 10 Web Console.

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

  Основной схемой развертывания является развертывание системы защиты через Консоль администрирования. Использование Kaspersky Security Center 10 Web Console позволяет запускать установку программ «Лаборатории Касперского» через браузер.
- Развертывание системы защиты вручную с помощью автономных пакетов установки, сформированных в Kaspersky Security Center.

Установка программ «Лаборатории Касперского» на клиентские устройства и рабочее место администратора производится вручную, параметры подключения клиентских устройств к Серверу администрирования задаются при установке Агента администрирования.

Этот вариант развертывания рекомендуется применять в случаях, когда невозможно провести удаленную установку.

Kaspersky Security Center также позволяет разворачивать систему защиты с помощью групповых политик Active Directory®. Подробнее см. в полной справке Kaspersky Security Center.

Развертывание системы защиты внутри организации

В этом разделе описаны процессы развертывания системы защиты внутри организации, соответствующие типовым схемам развертывания.

В этом разделе

Развертывание системы защиты через Консоль администрирования внутри организации

Удаленную установку необходимого программного обеспечения через Консоль администрирования проводит администратор Kaspersky Security Center (далее также администратор). Процесс развертывания в этом случае состоит из следующих основных шагов:

1. Администратор разворачивает Сервер администрирования следующим образом:
   a. устанавливает Kaspersky Security Center на выбранное устройство;
   b. устанавливает Консоль администрирования на рабочее место администратора (если требуется);
   c. настраивает параметры Сервера администрирования.
2. Если требуется, администратор создает иерархию Серверов администрирования в Kaspersky Security Center.

3. Администратор формирует структуру групп администрирования и распределяет клиентские устройства организации по группам администрирования.
4. Администратор создает и настраивает в Kaspersky Security Center инсталляционные пакеты Агента администрирования и необходимых программ «Лаборатории Касперского».
5. Администратор выбирает в Консоли администрирования устройства, на которые требуется установить выбранные программы.
6. Администратор создает и запускает задачи удаленной установки выбранных программ через Консоль администрирования.
7. При необходимости администратор выполняет дополнительную настройку установленных программ через Консоль администрирования с помощью политик и локальных параметров программ.

Развертывание системы защиты средствами Kaspersky Security Center 10 Web Console внутри организации

Удаленную установку необходимого программного обеспечения средствами Kaspersky Security Center 10 Web Console проводит администратор Kaspersky Security Center (далее также администратор). Процесс развертывания в этом случае состоит из следующих основных шагов:

1. Администратор разворачивает Сервер администрирования следующим образом:
    a. устанавливает Kaspersky Security Center на выбранное устройство;
    b. устанавливает на то же устройство Kaspersky Security Center 10 Web Console;
    c. устанавливает Консоль администрирования на рабочее место администратора (если требуется);
    d. настраивает Сервер администрирования для работы с Kaspersky Security Center 10 Web Console.

2. Администратор создает в Kaspersky Security Center виртуальный Сервер администрирования для управления клиентскими устройствами.
3. Администратор выбирает в сети организации устройство, которое будет играть роль агента обновлений, и локально устанавливает на него Агент администрирования.

   В результате Kaspersky Security Center автоматически назначает устройство, на котором установлен Агент администрирования, агентом обновлений и настраивает его в качестве шлюза соединений при первом соединении с Сервером администрирования.
4. Администратор создает и настраивает на виртуальном Сервере администрирования инсталляционные пакеты Агента администрирования и необходимых программ «Лаборатории Касперского».
5. Администратор запускает Kaspersky Security Center 10 Web Console.
6. Администратор запускает в Kaspersky Security Center 10 Web Console установку выбранных программ на устройства.
7. При необходимости администратор выполняет дополнительную настройку установленных программ через Консоль администрирования с помощью политик и локальных параметров программ.

Развертывание системы защиты вручную внутри организации

Установку необходимого программного обеспечения вручную при помощи автономных пакетов установки проводит администратор Kaspersky Security Center (далее также администратор). Процесс развертывания в этом случае состоит из следующих основных шагов:

1. Администратор разворачивает Сервер администрирования следующим образом:
   a. устанавливает Kaspersky Security Center на выбранное устройство;
   b. устанавливает Консоль администрирования на рабочее место администратора (если требуется);
   c. настраивает параметры Сервера администрирования.

2. Если требуется, администратор создает иерархию Серверов администрирования в Kaspersky Security Center.

3. Администратор формирует структуру групп администрирования.

4. Администратор создает и настраивает в Kaspersky Security Center инсталляционные пакеты Агента администрирования и необходимых программ «Лаборатории Касперского».

5. Администратор создает автономные пакеты установки для выбранных программ.

6. Администратор передает на клиентские устройства автономные пакеты установки, например, публикуя ссылку на автономные пакеты.

7. Пользователи клиентских устройств запускают установку программ с помощью полученных автономных пакетов установки.

8. После установки связи с Сервером администрирования клиентские устройства перемещаются в группы администрирования, указанные в свойствах автономных пакетов установки.

Развертывание системы защиты в сети организации-клиента

В этом разделе описаны процессы развертывания системы защиты в сети организации-клиента, соответствующие типовым схемам развертывания.

В этом разделе

Развертывание системы защиты через Консоль администрирования в сети организации-клиента

Удаленную установку необходимого программного обеспечения через Консоль администрирования проводит администратор Kaspersky Security Center (далее также администратор). Процесс развертывания в этом случае состоит из следующих основных шагов:

1. Администратор Kaspersky Security Center разворачивает Сервер администрирования следующим образом:
   a. устанавливает Kaspersky Security Center на выбранное устройство;
   b. устанавливает на то же устройство Kaspersky Security Center 10 Web Console;

c. устанавливает Консоль администрирования на рабочее место администратора (если требуется);

d. настраивает Сервер администрирования для работы с Kaspersky Security Center 10 Web Console.

2. Администратор Kaspersky Security Center создает в Kaspersky Security Center виртуальный Сервер администрирования для управления клиентскими устройствами организации-клиента.

3. Администратор Kaspersky Security Center выбирает в сети организации устройство, которое будет играть роль агента обновлений, и локально устанавливает на него Агент администрирования.

   В результате Kaspersky Security Center автоматически назначает клиентское устройство, на котором установлен Агент администрирования, агентом обновлений и настраивает его в качестве шлюза соединений при первом соединении с Сервером администрирования.

4. Администратор Kaspersky Security Center создает и настраивает на виртуальном Сервере администрирования инсталляционные пакеты Агента администрирования и необходимых программ «Лаборатории Касперского».

5. Администратор Kaspersky Security Center выбирает в Консоли администрирования устройства, на которые требуется установить выбранные программы.

6. Администратор создает и запускает задачи удаленной установки выбранных программ через Консоль администрирования.

7. При необходимости администратор выполняет дополнительную настройку установленных программ через Консоль администрирования с помощью политик и локальных параметров программ.

Развертывание системы защиты средствами Kaspersky Security Center 10 Web Console в сети организации-клиента

Удаленную установку необходимого программного обеспечения средствами Kaspersky Security Center 10 Web Console проводят совместно администратор Kaspersky Security Center и администратор организации-клиента. Процесс развертывания в этом случае состоит из следующих основных шагов:

1. Администратор Kaspersky Security Center разворачивает Сервер администрирования следующим образом:

   a. устанавливает Kaspersky Security Center на выбранное устройство;

   b. устанавливает на то же устройство Kaspersky Security Center 10 Web Console;

   c. устанавливает Консоль администрирования на рабочее место администратора (если требуется);

   d. настраивает Сервер администрирования для работы с Kaspersky Security Center 10 Web Console.

2. Администратор Kaspersky Security Center создает в Kaspersky Security Center виртуальный Сервер администрирования для управления клиентскими устройствами организации-клиента.

3. Администратор организации-клиента выбирает в сети организации устройство, которое будет играть роль агента обновлений, и локально устанавливает на него Агент администрирования.

   В результате Kaspersky Security Center автоматически назначает клиентское устройство, на котором установлен Агент администрирования, агентом обновлений и настраивает его в качестве шлюза соединений при первом соединении с Сервером администрирования.

4. Администратор Kaspersky Security Center создает и настраивает на виртуальном Сервере администрирования инсталляционные пакеты Агента администрирования и необходимых программ «Лаборатории Касперского».

5. Администратор организации-клиента запускает в Kaspersky Security Center 10 Web Console установку выбранных программ на клиентские устройства.

6. При необходимости администратор Kaspersky Security Center выполняет дополнительную настройку установленных программ через Консоль администрирования с помощью политик и локальных параметров программ.

Развертывание системы защиты вручную в сети организации-клиента

Установку необходимого программного обеспечения вручную при помощи автономных пакетов установки проводят совместно администратор Kaspersky Security Center и администратор организации-клиента. Процесс развертывания в этом случае состоит из следующих основных шагов:

1. Администратор Kaspersky Security Center разворачивает Сервер администрирования следующим образом:

   a. устанавливает Kaspersky Security Center на выбранное устройство;

   b. устанавливает на то же устройство Kaspersky Security Center 10 Web Console;

   c. устанавливает Консоль администрирования на рабочее место администратора (если требуется);

   d. настраивает Сервер администрирования для работы с Kaspersky Security Center 10 Web Console.

2. Администратор Kaspersky Security Center создает в Kaspersky Security Center виртуальный Сервер администрирования для управления клиентскими устройствами организации-клиента.

3. Администратор организации-клиента выбирает в сети организации устройство, которое будет играть роль агента обновлений, и локально устанавливает на него Агент администрирования.

   В результате Kaspersky Security Center автоматически назначает клиентское устройство, на котором установлен Агент администрирования, агентом обновлений и настраивает его в качестве шлюза соединений при первом соединении с Сервером администрирования.

4. Администратор Kaspersky Security Center создает и настраивает на виртуальном Сервере администрирования инсталляционные пакеты Агента администрирования и необходимых программ «Лаборатории Касперского».

5. Администратор Kaspersky Security Center создает автономные пакеты установки для выбранных программ.

6. Администратор Kaspersky Security Center передает организации-клиенту автономный пакет установки, например, публикуя ссылку на автономный пакет установки в Kaspersky Security Center 10 Web Console.

7. Администратор организации-клиента через Kaspersky Security Center 10 Web Console передает на выбранные устройства автономный пакет установки.

8. Пользователи клиентских устройств запускают установку программы с помощью полученного автономного пакета установки.

9. После установки связи с Сервером администрирования клиентские устройства перемещаются в группу администрирования, указанную в свойствах автономного пакета установки.

Развертывание Сервера администрирования

В этом разделе описаны этапы развертывания Сервера администрирования.

Этапы развертывания описаны для двух вариантов работы с программой:

- развертывание Сервера администрирования внутри организации;
- развертывание Сервера администрирования для защиты сети организации-клиента.

> Если вам требуется развернуть Сервер администрирования внутри организации, которая включает в себя удаленные офисы, не входящие в сеть организации, вы можете следовать порядку развертывания системы защиты для сервис-провайдеров.

Kaspersky Security Center предоставляет возможность интеграции в платформу Microsoft Network Access Protection (NAP), которая позволяет регулировать доступ клиентских устройств в сеть. Для того чтобы обеспечить проверку работоспособности операционной системы при совместной работе программы Kaspersky Security Center с Microsoft NAP, необходимо дополнительно установить компонент System Health Validator (см. раздел «Установка и настройка Kaspersky Security Center SHV» на стр. 83).

Далее в разделе описаны действия, входящие в перечисленные этапы развертывания защиты.

В этом разделе

Этапы развертывания Сервера администрирования внутри организации

► *Чтобы развернуть Сервер администрирования внутри организации, выполните следующие действия:*

1. Установите Kaspersky Security Center на рабочее место администратора.
2. Настройте параметры Сервера администрирования.

Этапы развертывания Сервера администрирования для защиты сети организации-клиента

► *Чтобы развернуть Сервер администрирования для защиты сети организации-клиента, выполните следующие действия:*

1. Установите Kaspersky Security Center на рабочее место администратора.
2. Установите Kaspersky Security Center 10 Web Console на рабочее место администратора.
3. Настройте параметры Сервера администрирования для работы с Kaspersky Security Center 10 Web Console.

Обновление предыдущей версии Kaspersky Security Center

Вы можете установить Сервер администрирования версии 10 на устройство, на котором установлена предыдущая версия Сервера администрирования. При обновлении до версии 10 данные и параметры предыдущей версии Сервера администрирования сохраняются.

Перед обновлением Kaspersky Security Center необходимо расшифровать зашифрованные диски устройств, на которых установлены компоненты программы (Серверы администрирования, Агенты администрирования). После обновления Kaspersky Security Center расшифрованные диски можно зашифровать повторно.

► *Чтобы обновить Сервер администрирования версии 9.0 до версии 10, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe для версии 10.

   Откроется окно с выбором программ «Лаборатории Касперского» для установки.

   В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте указаниям мастера.

2. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и «Лабораторией Касперского». Если вы согласны со всеми его пунктами, установите флажок **Я принимаю условия Лицензионного соглашения**.

   Установка программы будет продолжена. Мастер установки предложит вам создать резервную копию данных Сервера администрирования для Kaspersky Security Center 9.0.

   Kaspersky Security Center поддерживает восстановление данных из резервной копии данных Сервера администрирования, сформированной более ранней версией программы.

3. Если требуется создать резервную копию, в открывшемся окне **Создание резервной копии Сервера администрирования** установите флажок **Создать резервную копию Сервера администрирования**.

Резервная копия данных Сервера администрирования создается при помощи утилиты klbackup. Эта утилита входит в состав дистрибутива программы и располагается в корне папки установки Kaspersky Security Center.

> Подробную информацию о работе утилиты резервного копирования и восстановления данных см. в полной справке Kaspersky Security Center в разделе «Приложения».

4. Установите Сервер администрирования версии 10, следуя указаниям мастера установки.

> Не рекомендуется прерывать работу мастера установки. Прерывание процесса обновления на стадии установки Сервера администрирования может привести к неработоспособности Kaspersky Security Center 9.0.

5. Для устройств, на которых был установлен Агент администрирования предыдущей версии, создайте и запустите задачу удаленной установки новой версии Агента администрирования (см. раздел «Установка программ с помощью задачи удаленной установки» на стр. 102).

   После выполнения задачи удаленной установки версия Агента администрирования будет обновлена.

Если при установке Сервера администрирования возникли проблемы, вы можете восстановить предыдущую версию Сервера администрирования, используя созданную перед обновлением резервную копию данных Сервера.

Если в сети установлен хотя бы один Сервер администрирования новой версии, обновление других Серверов администрирования в сети можно проводить с помощью задачи удаленной установки, в которой используется инсталляционный пакет Сервера администрирования.

Установка и удаление Kaspersky Security Center

В этом разделе описывается локальная установка компонентов Kaspersky Security Center. Доступны два типа установки:

- **Стандартная**. В этом случае будет установлен минимальный набор необходимых компонентов программы. Этот тип установки рекомендуется для сетей, содержащих до 200 устройств.
- **Выборочная**. В этом случае вы сможете выбрать отдельные компоненты для установки и настроить дополнительные параметры программы. Этот тип установки рекомендуется для сетей, содержащих более 200 устройств. Выборочную установку рекомендуется проводить опытным пользователям.

Если в сети установлен хотя бы один Сервер администрирования, Серверы на других устройствах сети могут быть установлены с помощью задачи удаленной установки методом форсированной установки (см. раздел «Установка программ с помощью задачи удаленной установки» на стр. 102). При формировании задачи удаленной установки следует использовать инсталляционный пакет Сервера администрирования.

В этом разделе

Подготовка к установке

Перед началом установки нужно убедиться, что аппаратное и программное обеспечение устройства соответствует требованиям, предъявляемым к Серверу администрирования и Консоли администрирования.

Kaspersky Security Center хранит информацию в базе данных SQL-сервера. Для этого совместно с Kaspersky Security Center по умолчанию устанавливается программа Microsoft SQL Server 2014 Express SP1. Для хранения информации можно использовать и другие SQL-серверы. В этом случае они должны быть установлены в сети до начала установки Kaspersky Security Center.

Для установки Kaspersky Security Center необходимо наличие прав локального администратора на устройстве, где осуществляется установка.

Чтобы в результате установки компоненты программы работали верно, на устройствах должны быть открыты все необходимые порты (см. таблицу ниже).

Таблица 4. Порты, используемые Kaspersky Security Center

Номер порта	Протокол	Описание
Устройство, на котором установлен Сервер администрирования		
8060	HTTP	Используется для подключения к Веб-серверу для работы Kaspersky Security Center 10 Web Console и организации внутреннего портала предприятия.
8061	HTTPS	Используется для подключения к Веб-серверу для работы Kaspersky Security Center 10 Web Console и организации внутреннего портала предприятия. При подключении используется шифрование.
13000	TCP	Используется для следующих целей: • получения данных с клиентских устройств; • подключения агентов обновлений; • подключения подчиненных Серверов администрирования. При этом используется защищенное SSL-соединение.

Номер порта	Протокол	Описание
13000	UDP	Используется для передачи информации о выключении устройств.
13111	TCP	Используется для подключения к прокси-серверу KSN.
13291	TCP	Используется для подключения Консоли администрирования к Серверу администрирования. При этом используется защищенное SSL-соединение.
13292	TCP	Используется для подключения мобильных устройств.
14000	TCP	Используется для следующих целей: • получения данных с клиентских устройств; • подключения агентов обновлений; • подключения подчиненных Серверов администрирования. При этом защищенное SSL-соединение не используется.
17000	TCP	Используется для подключения к прокси-серверу активации. При этом используется защищенное SSL-соединение.
17100	TCP	Используется для подключения к прокси-серверу активации для активации мобильных клиентов.
Устройство, назначенное агентом обновлений		
13000	TCP	Используется клиентскими устройствами для подключения к агенту обновлений.
13001	TCP	Используется клиентскими устройствами для подключения к агенту обновлений, если им является устройство с установленным Сервером администрирования.

Номер порта	Протокол	Описание
14000	TCP	Используется клиентскими устройствами для подключения к агенту обновлений.
14001	TCP	Используется клиентскими устройствами для подключения к агенту обновлений, если им является устройство с установленным Сервером администрирования.
Клиентское устройство с установленным Агентом администрирования		
7	UDP	Используется функцией Wake On Lan.
9	UDP	
67	UDP	Используются на устройстве, которое назначено PXE-сервером, при развертывании образов операционных систем.
69	UDP	
15000	UDP	Используется для получения запроса на подключение к Серверу администрирования, что позволяет получать информацию об устройстве в режиме реального времени.
15001	UDP	Используется для взаимодействия с агентом обновлений.

Для исходящих соединений клиентских устройств с Сервером администрирования и агентами обновлений используется диапазон портов 1024–5000 (протокол TCP). В Microsoft Windows Vista и Microsoft Windows Server 2008 исходящий диапазон портов по умолчанию – 49152–65535 (протокол TCP).

Стандартная установка

► *Чтобы провести стандартную установку Kaspersky Security Center на локальном устройстве, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ «Лаборатории Касперского» для установки.

   В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте указаниям мастера.

2. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и «Лабораторией Касперского». Если вы согласны со всеми его пунктами, установите флажок **Я принимаю условия Лицензионного соглашения**. Установка программы будет продолжена.

   Мастер установки также может предложить вам ознакомиться с Лицензионными соглашениями на доступные в дистрибутиве Kaspersky Security Center плагины управления программами и принять условия этих Лицензионных соглашений.

3. Выберите тип установки **Стандартная** и нажмите на кнопку **Далее**.

В результате мастер установки распакует из дистрибутива необходимые файлы и запишет их на жесткий диск устройства.

В последнем окне мастера установки вам будет предложено запустить Консоль администрирования. При первом запуске Консоли вы можете выполнить первоначальную настройку программы (подробнее см. *Руководство администратора Kaspersky Security Center*).

По окончании работы мастера установки следующие компоненты программы будут установлены на жесткий диск, на котором установлена операционная система:

- Сервер администрирования (совместно с серверной версией Агента администрирования);
- Консоль администрирования;
- доступные в дистрибутиве плагины управления программами.

Кроме того, будут установлены следующие программы, если они не были установлены ранее:

- Microsoft Windows Installer версии 4.5;
- Microsoft .NET Framework 2.0 SP2;
- Microsoft SQL Server® 2008 R2 Express Edition SP2.

Выборочная установка

► *Чтобы провести выборочную установку Kaspersky Security Center на локальном устройстве,*

запустите исполняемый файл setup.exe.

Откроется окно с выбором программ «Лаборатории Касперского» для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте указаниям мастера.

Далее описаны шаги мастера установки программы, а также действия, которые вы можете выполнить на каждом из этих шагов.

Шаги мастера

Шаг 1. Просмотр Лицензионного соглашения

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Вам также может быть предложено ознакомиться с Лицензионными соглашениями на доступные в дистрибутиве Kaspersky Security Center плагины управления программами.

Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, установите флажок **Я принимаю условия Лицензионного соглашения**. Установка программы на ваше устройство будет продолжена.

Если вы не согласны с Лицензионным соглашением, то отмените установку программы, нажав на кнопку **Отмена**.

Шаг 2. Выбор типа установки

Укажите тип установки **Выборочная**.

Шаг 3. Выбор компонентов для установки

Выберите компоненты Сервера администрирования Kaspersky Security Center, которые вы хотите установить:

- **Поддержка мобильных устройств**. Этот компонент обеспечивает управление защитой мобильных устройств через Kaspersky Security Center.
- **Агент SNMP**. Получает статистическую информацию для Сервера администрирования по протоколу SNMP. Компонент доступен при установке программы на устройство с установленным компонентом SNMP.

  После установки Kaspersky Security Center необходимые для получения статистической информации mib-файлы будут расположены в папке установки программы во вложенной папке SNMP.

В диалоговом окне мастера приводится справочная информация о выбранном компоненте и необходимом для его установки объеме дискового пространства.

Компоненты Агент администрирования и Консоль администрирования не отображаются в списке компонентов. Эти компоненты устанавливаются автоматически, их установку отменить нельзя.

Вместе с компонентом Сервер администрирования на устройство будет установлена серверная версия Агента администрирования. Его совместная установка с обычной версией Агента администрирования невозможна. Если серверная версия Агента администрирования уже установлена на вашем устройстве, требуется удалить ее и запустить установку Сервера администрирования повторно.

На этом шаге мастера также следует указать папку для установки компонентов Сервера администрирования. По умолчанию компоненты устанавливаются в папку <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Если папки с таким названием нет, она будет создана автоматически в процессе установки. Вы можете сменить папку назначения с помощью кнопки **Обзор**.

Шаг 4. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса программы.

В таблице ниже перечислены параметры установки программы и отображения интерфейса при выборе разных размеров сети.

Таблица 5. Зависимость параметров установки от выбора размеров сети

Параметры	1–100 устройств	100–1000 устройств	1000–5000 устройств	Более 5000 устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами	отсутствует	отсутствует	присутствует	присутствует
Отображение разделов **Безопасность** в окнах свойств Сервера и групп администрирования	отсутствует	отсутствует	присутствует	присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать программу для управления более чем 5000 устройств.

Шаг 5. Выбор учетной записи

Выберите учетную запись, под которой Сервер администрирования будет запускаться как служба на этом устройстве:

- **Учетная запись системы**. Сервер администрирования будет запускаться под учетной записью и с правами *Учетная запись системы*.

  Для правильной работы Kaspersky Security Center требуется, чтобы учетная запись для запуска Сервера администрирования обладала правами администратора ресурса для размещения информационной базы Сервера администрирования.

  В Microsoft Windows Vista и операционных системах Microsoft Windows более поздних версий Сервер администрирования не может быть установлен под учетной записью системы. В этих случаях для выбора доступен вариант **Автоматически созданная учетная запись (<Имя учетной записи>)**.

- **Учетная запись пользователя**. Сервер администрирования будет запускаться под учетной записью пользователя. В этом случае Сервер администрирования будет инициировать все операции с правами этой учетной записи. С помощью кнопки **Выбрать** определите пользователя, чья учетная запись будет использоваться, и укажите пароль.

При использовании SQL-сервера в режиме аутентификации учетной записи пользователя средствами Microsoft Windows требуется обеспечить доступ к базе данных. Учетная запись пользователя должна быть владельцем базы данных Антивируса Касперского. По умолчанию требуется использовать схему dbo.

Если в дальнейшем вы захотите изменить учетную запись Сервера администрирования, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования (*klsrvswch*). Подробную информацию см. в *Руководстве администратора Kaspersky Security Center*.

Шаг 6. Настройка учетной записи для запуска служб

Выберите учетную запись, под которой будут запускаться службы Kaspersky Security Center на этом устройстве:

- **Автоматически созданная учетная запись**. Kaspersky Security Center создает учетную запись в группе kladmins. Службы Kaspersky Security Center будут запускаться под созданной учетной записью.
- **Задать учетную запись**. Службы Kaspersky Security Center будут запускаться под заданной учетной записью пользователя. По кнопке **Выбрать** укажите учетную пользователя и введите пароль.

Шаг 7. Выбор базы данных

На этом шаге мастера установки требуется выбрать ресурс Microsoft SQL Server (SQL Express) или MySQL, который будет использоваться для размещения информационной базы данных Сервера администрирования.

Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), для него не предусмотрена возможность установки Microsoft SQL Server (SQL Express). В этом случае для правильной установки Kaspersky Security Center рекомендуется использовать ресурс MySQL.

Структура базы данных Сервера администрирования описана в файле klakdb.chm, который расположен в папке установки программы Kaspersky Security Center.

Шаг 8. Настройка параметров SQL-сервера

На этом шаге мастера установки выполняется настройка параметров SQL-сервера.

В зависимости от выбранной базы данных возможны следующие варианты настройки параметров SQL-сервера:

- Если на предыдущем этапе вы выбрали SQL Express или Microsoft SQL Server, выберите один из следующих вариантов:

  - Если в сети организации установлен SQL-сервер, укажите его имя в поле **Имя SQL-сервера**.

    В поле **Имя SQL-сервера** по умолчанию указано имя SQL-сервера, если он обнаружен на устройстве, с которого осуществляется установка Kaspersky Security Center. При помощи кнопки **Обзор** вы можете вывести список всех SQL-серверов, установленных в сети.

    > Если Сервер администрирования запускается под учетной записью локального администратора или под учетной записью системы, кнопка **Обзор** недоступна.

    Задайте имя базы данных, которая будет создана для размещения информации Сервера администрирования, в поле **Имя базы данных**. По умолчанию база данных создается под именем **KAV**.

    > Если с помощью Kaspersky Security Center вы предполагаете управлять устройствами в количестве менее 5000, можно использовать Microsoft SQL Express 2005 / 2008. Если планируемое количество устройств под управлением Kaspersky Security Center превышает 5000, рекомендуем использовать Microsoft SQL 2005 / 2008.

    > Рекомендуется использовать SQL Server Edition, отличный от Express, если планируется использовать компонент Контроль активности программ для управления более чем 50 устройствами.

- Если в сети организации не установлен SQL-сервер, выберите вариант **Установить Microsoft SQL Server 2014 Express SP1**.

  Мастер установки программы установит Microsoft SQL Server 2014 Express SP1. Необходимые параметры будут настроены автоматически.

- Если на предыдущем этапе был выбран сервер MySQL, укажите его имя в поле **Имя SQL-сервера** (по умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center) и порт для подключения в поле **Порт** (по умолчанию используется порт 3306).

  В поле **Имя базы данных** задайте имя базы данных, которая будет создана для размещения информации Сервера администрирования (по умолчанию база данных создается под именем **KAV**).

Если вы хотите вручную установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите вручную установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL-сервер и вернитесь к установке Kaspersky Security Center.

Шаг 9. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к SQL-серверу.

В зависимости от выбранной базы данных вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:

  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.

- **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись**, **Пароль** и **Подтверждение пароля**.

  Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью Локальная система.

- Для сервера MySQL укажите учетную запись и пароль.

Шаг 10. Определение папки общего доступа

Определите место размещения и название папки общего доступа, которая будет использоваться для следующих целей:

- хранения файлов, необходимых для удаленной установки программ (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);
- размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

К этому ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать папку общего доступа**. Создание новой папки. Укажите путь к папке в расположенном ниже поле.
- **Выбрать существующую папку общего доступа**. Выбор папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на устройстве, с которого производится установка, так и удаленно, на любом из клиентских устройств, входящих в состав сети организации. Вы можете указать папку общего доступа с помощью кнопки **Обзор** или вручную, введя в соответствующем поле UNC-путь (например, \\server\Share).

По умолчанию создается локальная папка Share в папке, заданной для установки программных компонентов Kaspersky Security Center.

Шаг 11. Настройка параметров подключения к Серверу администрирования

Настройте параметры подключения к Серверу администрирования:

- **Номер порта**. Номер порта для подключения к Серверу администрирования. По умолчанию используется порт 14000.
- **Номер SSL-порта**. Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL. По умолчанию используется порт 13000.

Если Сервер администрирования работает под управлением Microsoft Windows XP с Service Pack 2, то встроенный межсетевой экран блокирует TCP-порты с номерами 13000 и 14000. Поэтому для обеспечения доступа на устройстве, на котором установлен Сервер администрирования, эти порты нужно открыть вручную.

Шаг 12. Задание адреса Сервера администрирования

Задайте адрес Сервера администрирования. Вы можете выбрать один из следующих вариантов:

- **Имя DNS-домена**. Этот вариант используется в том случае, когда в сети присутствует DNS-сервер, и клиентские устройства могут получить с его помощью адрес Сервера администрирования.
- **NetBIOS-имя**. Этот вариант используется, если клиентские устройства получают адрес Сервера администрирования с помощью протокола NetBIOS, или в сети присутствует WINS-сервер.
- **IP-адрес**. Этот вариант используется, если Сервер администрирования имеет статический IP-адрес, который в дальнейшем не будет изменяться.

Шаг 13. Настройка параметров для мобильных устройств

Этот шаг мастера установки доступен в случае, если вы выбрали для установки компонент Поддержка мобильных устройств.

Укажите имя Сервера администрирования для подключения мобильных устройств.

Шаг 14. Выбор плагинов управления программами

Выберите плагины управления программами «Лаборатории Касперского», которые требуется установить совместно с Kaspersky Security Center.

Шаг 15. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные программы, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые программы будут установлены автоматически после нажатия на кнопку **Далее**.

Установка в неинтерактивном режиме

Kaspersky Security Center может быть установлен в неинтерактивном режиме, то есть без интерактивного ввода параметров установки.

► *Чтобы установить Kaspersky Security Center на локальном устройстве в неинтерактивном режиме,*

выполните команду

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 <setup_parameters>"
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PRO1=PROP1VAL PROP2=PROP2VAL`). Файл setup.exe расположен на дистрибутивном компакт-диске программы Kaspersky Security Center в папке Server.

Имена и возможные значения параметров, которые можно использовать при установке Сервера администрирования в неинтерактивном режиме, приведены в таблице ниже.

Таблица 6. Параметры установки Сервера администрирования в неинтерактивном режиме

Имя параметра	Описание параметра	Возможные значения
EULA	Согласие с условиями Лицензионного соглашения	• 1 – согласны с условиями Лицензионного соглашения • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется)
INSTALLATIONMODETYPE	Тип установки Сервера администрирования	• Standard – стандартная установка • Custom – выборочная установка
INSTALLDIR	Путь к папке установки Сервера администрирования	Строковое значение
ADDLOCAL	Список компонентов (через запятую) Сервера администрирования для установки	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86 Минимальный достаточный для корректной установки Сервера администрирования список компонентов: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole,KSNProxy ,Microsoft_VC90_CRT_x86,Mi crosoft_VC100_CRT_x86`

Имя параметра	Описание параметра	Возможные значения
NETRANGETYPE	Размер сети (количество устройств в сети)	• NRT_1_100 – от 1 до 100 устройств • NRT_100_1000 – от 100 до 1000 устройств • NRT_GREATER_1000 – более 1000 устройств
SRV_ACCOUNT_TYPE	Способ задания учетной записи, под которой Сервер администрирования будет запускаться как служба	• SrvAccountDefault – учетная запись создается автоматически • SrvAccountUser – учетная запись задается вручную; в этом случае следует задать значения параметров SERVERACCOUNTNAME и SERVERACCOUNTPWD
SERVERACCOUNTNAME	Имя учетной записи, под которой Сервер администрирования будет запускаться как служба; значение параметра задается, если SRV_ACCOUNT_TYPE=SrvAccountUser	Строковое значение
SERVERACCOUNTPWD	Пароль учетной записи, под которой Сервер администрирования будет запускаться как служба; значение параметра задается, если SRV_ACCOUNT_TYPE=SrvAccountUser	Строковое значение

Имя параметра	Описание параметра	Возможные значения
SERVERCER	Длина ключа для сертификата Сервера администрирования (в битах)	• 1 – длина ключа для сертификата Сервера администрирования 2048 бит • Значение не задано – длина ключа для сертификата Сервера администрирования 1024 бит
DBTYPE	Тип базы данных, которая будет использоваться для размещения информационной базы данных Сервера администрирования	• MySQL – будет использоваться база данных MySQL; в этом случае следует задать значения параметров MYSQLSERVERNAME, MYSQLSERVERPORT, MYSQLDBNAME, MYSQLACCOUNTNAME, MYSQLACCOUNTPWD • MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Express); в этом случае следует задать значения параметров MSSQLCONNECTIONTYPE и MSSQLAUTHTYPE
MYSQLSERVERNAME	Полное имя SQL-сервера; значение параметра задается, если DBTYPE=MySQL	Строковое значение
MYSQLSERVERPORT	Номер порта для подключения к SQL-серверу; значение параметра задается, если DBTYPE=MySQL	Строковое значение

Имя параметра	Описание параметра	Возможные значения
MYSQLDBNAME	Имя базы данных, которая будет создана для размещения информации Сервера администрирования; значение параметра задается, если DBTYPE=MySQL	Строковое значение
MYSQLACCOUNTNAME	Имя учетной записи для подключения к базе; значение параметра задается, если DBTYPE=MySQL	Строковое значение
MYSQLACCOUNTPWD	Пароль учетной записи для подключения к базе; значение параметра задается, если DBTYPE=MySQL	Строковое значение
MSSQLCONNECTIONTYPE	Тип использования базы данных MSSQL; значение параметра задается, если DBTYPE=MSSQL	• InstallMSSEE – установить Microsoft SQL Server 2014 Express SP1; необходимые параметры будут настроены автоматически • ChooseExisting – использовать SQL-сервер, установленный в сети организации; в этом случае следует задать значения параметров MSSQLSERVERNAME и MSSQLDBNAME
MSSQLSERVERNAME	Полное имя SQL-сервера; значение параметра задается, если MSSQLCONNECTIONTYPE=ChooseExisting	Строковое значение

Имя параметра	Описание параметра	Возможные значения
MSSQLDBNAME	Имя базы данных; значение параметра задается, если MSSQLCONNECTIONTYPE=ChooseExisting	Строковое значение
MSSQLAUTHTYPE	Тип авторизации при подключении к SQL-серверу; значение параметра задается, если DBTYPE=MSSQL	• Windows – режим аутентификации Microsoft Windows • SQLServer – режим аутентификации SQL-сервера; в этом случае следует задать значения параметров MSSQLACCOUNTNAME и MSSQLACCOUNTPWD
MSSQLACCOUNTNAME	Имя учетной записи для подключения к SQL-серверу; значение параметра задается, если MSSQLAUTHTYPE=SQLServer	Строковое значение
MSSQLACCOUNTPWD	Пароль учетной записи для подключения к SQL-серверу; значение параметра задается, если MSSQLAUTHTYPE=SQLServer	Строковое значение
CREATE_SHARE_TYPE	Способ задания папки общего доступа	• Create – создать новую папку общего доступа; в этом случае следует задать значения параметров SHARELOCALPATH и SHAREFOLDERNAME • ChooseExisting – выбрать существующую папку; в этом случае следует задать значение параметра EXISTSHAREFOLDERNAME

Имя параметра	Описание параметра	Возможные значения
SHARELOCALPATH	Полный путь к локальной папке; значение параметра задается, если CREATE_SHARE_TYPE=Create	Строковое значение
SHAREFOLDERNAME	Сетевое имя папки общего доступа; значение параметра задается, если CREATE_SHARE_TYPE=Create	Строковое значение
EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа; значение параметра задается, если CREATE_SHARE_TYPE=ChooseExisting	Строковое значение
SERVERPORT	Номер порта для подключения к Серверу администрирования	Числовое значение
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL	Числовое значение
SERVERADDRESS	Адрес Сервера администрирования	Строковое значение
MOBILESERVERADDRESS	Адрес Сервера администрирования для подключения мобильных устройств	Строковое значение

Подробно параметры установки Сервера администрирования описаны в разделе «Выборочная установка» (на стр. 60).

Изменения в системе после установки

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

Сервер администрирования и Агент администрирования будут установлены на устройстве в качестве служб с атрибутами, указанными в таблице ниже. В таблице также указаны атрибуты других служб, которые выполняются на устройстве после установки Сервера администрирования.

Таблица 7. Атрибуты служб

Компонент	Имя службы	Отображаемое имя службы	Тип запуска	Учетная запись
Сервер администрирования	kladminserver	Сервер администрирования Kaspersky Security Center	Автоматически при старте операционной системы	Указанная пользователем или специальная, созданная при установке, учетная запись вида KL-AK-*
Агент администрирования	klnagent	Агент администрирования Kaspersky Security Center	Автоматически при старте операционной системы	Локальная система
Веб-сервер для работы Веб-консоли и организации внутреннего портала предприятия	klwebsrv	Веб-сервер «Лаборатории Касперского»	Автоматически при старте операционной системы	Специальная непривилегированная учетная запись вида KlScSvc-*
Прокси-сервер активации	klactprx	Прокси-сервер активации «Лаборатории Касперского»	Автоматически при старте операционной системы	Специальная непривилегированная учетная запись вида KlScSvc-*

Компонент	Имя службы	Отображаемое имя службы	Тип запуска	Учетная запись
Веб-портал авторизации доступа	klnsacwsrv	Портал авторизации «Лаборатории Касперского»	Вручную	Локальная система
Прокси-сервер KSN	ksnproxy	Прокси-сервер Kaspersky Security Network	Вручную	Специальная непривилегированная учетная запись вида KlScSvc-*
Сервер iOS MDM	KLIOSMdmServiceSrv2	iOS MDM Mobile devices server	Автоматически при старте операционной системы	Network Service
COM+ объект для взаимодействия с Exchange сервером	KasperskyMdmService	Kaspersky MDM for Exchange	Автоматически при обращении к объекту	Учетная запись пользователя, входящая в группы Domain User и KLMDM Role Group (KLMDM Secure Group)

Вместе с Сервером администрирования на устройство будет установлена серверная версия Агента администрирования. Она входит в состав Сервера администрирования, устанавливается и удаляется в его составе и может взаимодействовать только с локально установленным Сервером администрирования. Настраивать параметры подключения Агента к Серверу администрирования не требуется: настройка реализована программно с учетом того, что компоненты установлены на одном устройстве. Эти параметры будут недоступны также в локальных параметрах Агента администрирования на этом устройстве. Такая конфигурация позволяет избежать дополнительной настройки параметров и возможных конфликтов в работе компонентов при их отдельной установке.

Серверная версия Агента администрирования устанавливается с теми же атрибутами и выполняет те же функции управления программами, что и стандартный Агент администрирования. На эту версию будет действовать политика группы администрирования, в которую включено клиентское устройство Сервера администрирования. Для серверной версии Агента администрирования создаются все задачи, предусмотренные для Агента администрирования, за исключением задачи смены Сервера.

Отдельная установка Агента администрирования на устройство Сервера администрирования не требуется. Его функции выполняет серверная версия Агента администрирования.

Вы можете просматривать свойства служб Сервера, Агента администрирования и Сервера политик «Лаборатории Касперского», а также следить за их работой при помощи стандартных средств администрирования Microsoft Windows – Управление компьютером\Службы. Информация о работе службы Сервера администрирования сохраняется в системном журнале Microsoft Windows на устройстве, где установлен Сервер администрирования, в отдельной ветви журнала Kaspersky Event Log.

На устройстве, где установлен Сервер администрирования, также автоматически создаются группы локальных пользователей KLAdmins и KLOperators. Если Сервер администрирования запускается под учетной записью пользователя, входящего в домен, то группы пользователей KLAdmins и KLOperators добавляются в список групп доменных пользователей. Изменение состава групп пользователей осуществляется при помощи стандартных средств администрирования Microsoft Windows.

Для настройки почтовых уведомлений, администратору может потребоваться заведение учетной записи на почтовом сервере для ESMTP-аутентификации.

Удаление программы

Вы можете удалить Kaspersky Security Center стандартными средствами установки и удаления программ Microsoft Windows. Для удаления программы запускается мастер, в результате работы которого с устройства будут удалены все компоненты программы (включая плагины). Если во время работы мастера вы не задали удаление папки общего доступа (Share), то после завершения всех связанных с ней задач вы можете удалить ее вручную.

Мастер удаления программы предложит вам сохранить резервную копию Сервера администрирования.

При удалении программы с операционных систем Microsoft Windows 7 и Microsoft Windows 2008 возможно преждевременное завершение работы программы удаления. Чтобы избежать этого, отключите в операционной системе службу контроля учетных записей (UAC) и повторно запустите удаление программы.

Установка Консоли администрирования на рабочее место администратора

Вы можете установить Консоль администрирования отдельно на рабочее место администратора и управлять Сервером администрирования по сети с помощью этой Консоли.

► *Чтобы установить Консоль администрирования на рабочее место администратора, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ «Лаборатории Касперского» для установки.

   В окне с выбором программ по ссылке **Установить Консоль администрирования Kaspersky Security Center** запустите мастер установки Консоли администрирования. Следуйте указаниям мастера.

   Процесс установки Консоли администрирования с дистрибутива, полученного через интернет, совпадает с процессом установки Консоли администрирования с дистрибутивного компакт-диска.

2. Выберите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете сменить папку назначения с помощью кнопки **Обзор**.

3. В завершающем окне мастера установки нажмите на кнопку **Начать**, чтобы начать процесс установки Консоли администрирования.

По окончании работы мастера Консоль администрирования будет установлена на рабочем месте администратора.

После установки Консоли администрирования следует подключиться к Серверу администрирования. Для этого нужно запустить Консоль администрирования и в открывшемся окне указать имя устройства или IP-адрес устройства, на котором установлен Сервер администрирования, а также параметры учетной записи для подключения к нему. После установления соединения с Сервером администрирования можно управлять системой антивирусной защиты с помощью этой Консоли администрирования.

Вы можете удалить Консоль администрирования стандартными средствами установки и удаления программ Microsoft Windows.

Настройка подключения Консоли администрирования к Серверу администрирования

В предыдущих версиях Kaspersky Security Center Консоль администрирования подключалась к Серверу администрирования, используя SSL-порт TCP 13291, а также SSL-порт TCP 13000. Начиная с версии Kaspersky Security Center 10 Service Pack 2 SSL-порты, используемые программой, строго разделены, и использование портов не по назначению невозможно:

- SSL-порт TCP 13291 могут использовать только Консоль администрирования и объекты автоматизации утилиты klakaut.
- SSL-порт TCP 13000 могут использовать только Агент администрирования, подчиненный Сервер и главный Сервер администрирования, размещенный в демилитаризованной зоне.

Порт TCP 14000 может использоваться для подключения Консоли администрирования, агентов обновлений, подчиненных Серверов администрирования и объектов автоматизации утилиты klakaut, а также для получения данных с клиентских устройств.

В некоторых случаях может быть необходимо подключение Консоли администрирования по SSL-порту 13000:

- если предпочтительно использовать один и тот же SSL-порт как для Консоли администрирования, так и для других активностей (для получения данных с клиентских устройств, подключения агентов обновлений, подключения подчиненных Серверов администрирования),
- если объект автоматизации утилиты klakaut подключается к Серверу администрирования не напрямую, а через агент обновлений, размещенный в демилитаризованной зоне.

► *Чтобы разрешить подключение Консоли администрирования по порту 13000, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM

   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Для ключа LP_ConsoleMustUsePort13291 (DWORD) установите значение 00000000.

   По умолчанию для этого ключа указано значение 1.

4. Перезапустите службу Сервера администрирования.

В результате Консоль администрирования сможет подключаться к Серверу администрирования, используя порт 13000.

Установка и настройка Kaspersky Security Center SHV

Kaspersky Security Center предоставляет возможность интеграции в платформу Microsoft Network Access Protection (NAP). Microsoft NAP позволяет регулировать доступ клиентских устройств в сеть. Microsoft NAP предполагает, что в сети выделен сервер с установленной операционной системой Microsoft Windows Server 2008, на который установлена служба PVS (Posture Validation Server), а на клиентских устройствах установлены NAP-совместимые операционные системы: Microsoft Windows Vista, Microsoft Windows XP с установленным Пакетом обновлений 3, Microsoft Windows 7.

При совместной работе программы Kaspersky Security Center с Microsoft NAP проверку работоспособности операционной системы осуществляет System Health Validator (далее – Kaspersky Security Center SHV).

► *Чтобы установить Kaspersky Security Center SHV на устройство локально, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ «Лаборатории Касперского» для установки.

   В окне с выбором программ по ссылке **Установить Kaspersky Security Center SHV** запустите мастер установки Kaspersky Security Center SHV. Следуйте указаниям мастера.

   > Процесс установки Kaspersky Security Center SHV с дистрибутива, полученного через интернет, совпадает с процессом установки Kaspersky Security Center SHV с дистрибутивного компакт-диска.

2. Определите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center SHV. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете сменить папку назначения с помощью кнопки **Обзор**.

3. В завершающем окне мастера установки нажмите на кнопку **Начать**, чтобы начать процесс установки Kaspersky Security Center SHV.

По окончании работы мастера Kaspersky Security Center SHV будет установлен на вашем устройстве.

Вы можете удалить Kaspersky Security Center SHV стандартными средствами установки и удаления программ Microsoft Windows. При этом запускается мастер, в результате работы которого с устройства будут удалены все компоненты программы.

Установка Kaspersky Security Center 10 Web Console

На устройстве, где планируется установить Kaspersky Security Center 10 Web Console, должна быть установлена Консоль администрирования (см. раздел «Установка Консоли администрирования на рабочее место администратора» на стр. 80).

На устройствах с операционными системами Windows 7, Windows Server 2008 и Windows Vista дополнительно должно быть установлено исправление KB2533623 (https://support.microsoft.com/en-us/kb/2533623).

Для установки Kaspersky Security Center 10 Web Console необходимы права локального администратора.

► *Чтобы установить Kaspersky Security Center 10 Web Console на локальном устройстве,*

запустите файл install.exe на дистрибутивном компакт-диске программы Kaspersky Security Center 10 Web Console.

Установка сопровождается мастером. Мастер установки предложит вам настроить параметры установки. Следуйте его указаниям.

Процесс установки Kaspersky Security Center 10 Web Console с дистрибутива, полученного через интернет, совпадает с процессом установки программы с дистрибутивного компакт-диска.

Шаги мастера

Шаг 1. Просмотр Лицензионного соглашения

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, установите флажок **Я принимаю условия Лицензионного соглашения**. Установка программы на ваше устройство будет продолжена.

Если вы не согласны с Лицензионным соглашением, то отмените установку программы, нажав на кнопку **Отмена**.

Удаленная установка Kaspersky Security Center 10 Web Console с помощью инсталляционного пакета или локальная установка в неинтерактивном режиме означает автоматическое согласие с условиями Лицензионного соглашения на устанавливаемую программу. Просмотреть Лицензионное соглашение на конкретную программу можно в комплекте поставки этой программы или на сайте поддержки «Лаборатории Касперского».

Шаг 2. Подключение к Kaspersky Security Center

Выберите способ подключения Kaspersky Security Center 10 Web Console к Kaspersky Security Center. Доступны следующие способы подключения:

- **Использовать сервер Apache, установленный на локальном устройстве**. Если выбран этот вариант, подключение Kaspersky Security Center 10 Web Console к Kaspersky Security Center будет выполняться через сервер Apache, установленный на локальном устройстве (выбрать установку сервера Apache можно на следующем шаге мастера).

- **Использовать сервер Apache, установленный на удаленном устройстве**. Вы можете выбрать этот вариант, если сервер Apache уже установлен на удаленном устройстве. В этом случае локально будет установлена только серверная часть Kaspersky Security Center 10 Web Console. Чтобы подключить Kaspersky Security Center 10 Web Console к Kaspersky Security Center, на удаленном устройстве необходимо установить клиентскую часть Kaspersky Security Center 10 Web Console. При выборе этого варианта мастер установки переходит к Шагу 8 (см. раздел «Шаг 8. Запуск установки Kaspersky Security Center 10 Web Console» на стр. 89).

► *Чтобы установить клиентскую часть Kaspersky Security Center 10 Web Console на удаленное устройство на платформе Linux,*

в зависимости от типа системы запустите один из следующих файлов:

- Для 32-битных систем:
  - kscwebconsole-10.<номер_сборки>.i386.rpm;
  - kscwebconsole_10.<номер_сборки>_i386.deb.
- Для 64-битных систем:
  - kscwebconsole-10.<номер_сборки>.x86_64.rpm;
  - kscwebconsole_10.<номер_сборки>_x86_64.deb.

Шаг 3. Выбор папки назначения

Определите папку назначения для установки Kaspersky Security Center 10 Web Console. По умолчанию папкой назначения является папка <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console. Если такой папки нет, она будет создана автоматически. Вы можете сменить папку назначения с помощью кнопки **Обзор**.

Шаг 4. Выбор установки сервера Apache

Если на устройстве не установлен сервер Apache, на этом шаге мастер установки предложит вам установить Apache HTTP Server 2.4.25.

По умолчанию выбран вариант установки Apache HTTP Server 2.4.25. Если вы не хотите устанавливать сервер Apache с помощью мастера установки Kaspersky Security Center 10 Web Console, снимите флажок **Установить Apache HTTP Server 2.4.25.**

Во время установки сервера Apache может потребоваться перезагрузка устройства.

Шаг 5. Установка сервера Apache

На этом шаге мастера выполняется установка и настройка Apache HTTP Server 2.4.25.

Перед началом установки задайте сертификат, который будет использовать для шифрования соединения сервера Apache с браузером пользователя. Выберите один из следующих вариантов:

- **Сформировать новый**. Сформировать сертификат для работы по HTTPS.
- **Выбрать существующий**. Использовать имеющийся сертификат для работы по HTTPS. Задайте сертификат одним из предложенных способов:
  - **Выбрать файл сертификата**. Вы можете выбрать имеющийся сертификат, нажав на кнопку **Обзор**.
  - **Выбрать файл закрытого ключа**. Вы можете задать сертификат файлом его закрытого ключа, нажав на кнопку **Обзор**.

Шаг 6. Выбор портов

Настройте следующие параметры:

- Номер SSL-порта для защищенного подключения устройства к Серверу администрирования. По умолчанию используется порт 13291.
- Номер порта для подключения устройства к серверу Apache. По умолчанию используется порт 9000.
- Адрес устройства, на котором установлен Сервер администрирования. По умолчанию указан адрес localhost.

  Если устройство, на которое устанавливается Kaspersky Security Center 10 Web Console и Self Service Portal, находится в демилитаризованной зоне, установите флажок **Шлюз соединения**, а в поле **Адрес сервера** укажите адрес шлюза соединения.
- Номер порта для подключения устройства к Kaspersky Security Center 10 Web Console. По умолчанию используется порт 8080.
- Номер порта для подключения устройства к Self Service Portal. По умолчанию используется порт 8081.

После установки Kaspersky Security Center 10 Web Console и Self Service Portal вы можете изменить номера портов, заданные по умолчанию (см. раздел «Изменение номера порта для подключения устройства» на стр. 90).

Шаг 7. Выбор учетной записи

Укажите доменную учетную запись пользователя, от имени которой с помощью QR-кодов установочные пакеты будут загружаться на мобильные устройства пользователей. Учетную запись нужно указывать в формате <Имя домена>\<Имя учетной записи>.

По кнопке **Проверить** вы можете проверить подключение к Серверу администрирования.

Шаг 8. Запуск установки Kaspersky Security Center 10 Web Console

Нажмите на кнопку **Установить** для запуска установки Kaspersky Security Center 10 Web Console.

Процесс установки отображается в окне мастера.

Шаг 9. Завершение установки Kaspersky Security Center 10 Web Console

Если на устройстве уже был установлен сервер Apache версии 2.4.25 или выше или автоматическая установка сервера Apache завершилась с ошибкой, на этом шаге мастера установки Kaspersky Security Center 10 Web Console вам будет предложено открыть файл с инструкциями по настройке сервера Apache. Чтобы после завершения работы мастера открыть файл с инструкциями, требуется установить флажок **Открыть файл readme.txt**.

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

Дополнительная настройка Kaspersky Security Center 10 Web Console и Self Service Portal

После установки Kaspersky Security Center 10 Web Console и Self Service Portal вы можете выполнить их дополнительную настройку:

- Создать файлы с текстом Лицензионного соглашения и часто задаваемыми вопросами, которые пользователи могут просматривать при доступе к Kaspersky Security Center 10 Web Console и Self Service Portal (см. раздел «Настройка файла Лицензионного соглашения и файла с часто задаваемыми вопросами» на стр. 91).
- Добавить логотип вашей организации в интерфейс Kaspersky Security Center 10 Web Console и Self Service Portal (см. раздел «Настройка логотипа» на стр. 92).

Изменение номера порта для подключения устройства

► *Чтобы изменить номер порта 8080 для подключения устройства к Kaspersky Security Center 10 Web Console, выполните следующие действия:*

1. Откройте файл httpd.conf, расположенный в рабочей папке сервера Apache.

   Например, "<Диск>:\Program Files (x86)\KSC Apache 2.4\Apache2.4\conf\httpd.conf".

2. Замените значение порта 8080 на требуемый порт в трех местах:

   - Строка 1: `Listen 8080`;
   - Строка 38: `<VirtualHost *:8080>`;
   - Строка 54: `RewriteCond %{SERVER_PORT} !^8080$`.

3. Перезапустите службу сервера Apache.
4. Перезапустите Kaspersky Security Center 10 Web Console.

Пример:

Если необходимо заменить порт 8080 на 443, то результат должен выглядеть так:

Строка 1: `Listen 443`

Строка 38: `<VirtualHost *:443>`

Строка 54: `RewriteCond %{SERVER_PORT} !^443$`

► *Чтобы изменить номер порта 8081 для подключения устройства к Self Service Portal, выполните следующие действия:*

1. Откройте файл httpd.conf, расположенный в рабочей папке сервера Apache.

   Например, "<Диск>:\Program Files (x86)\KSC Apache 2.4\Apache2.4\conf\httpd.conf" с помощью notepad++.

2. Замените значение порта 8081 на требуемый порт в трех местах:

   - Строка 2: `Listen 8081`;

- Строка 139: `<VirtualHost *:8081>`;
- Строка 149: `RewriteCond %{SERVER_PORT} !^8081$`.

3. Перезапустите службу сервера Apache.
4. Перезапустите Self Service Portal.

Не рекомендуется использовать порт 80 для подключения устройств к Kaspersky Security Center 10 Web Console или к Self Service Portal, так как порт 80 по умолчанию назначен для протокола HTTP, а для подключения устройств к Kaspersky Security Center 10 Web Console и к Self Service Portal используется протокол HTTPS.

Настройка файла Лицензионного соглашения и файла с часто задаваемыми вопросами

► *Чтобы текст Лицензионного соглашения и ответы на часто задаваемые вопросы пользователей были доступны в интерфейсе Kaspersky Security Center 10 Web Console и / или в интерфейсе Self Service Portal, выполните следующие действия:*

1. Создайте файл Лицензионного соглашения (eula.txt или eula.html) и файл с ответами на часто задаваемые вопросы (faq.txt или faq.html).
2. Поместите созданные файлы в папку установки сервера Apache, во вложенную папку htdocs\help.

Тексты Лицензионного соглашения и ответы на часто задаваемые вопросы будут доступны по ссылкам из главного окна Kaspersky Security Center 10 Web Console и / или из главного окна Self Service Portal.

Настройка логотипа

► *Чтобы логотип вашей организации отображался в интерфейсе Kaspersky Security Center 10 Web Console и / или в интерфейсе Self Service Portal, выполните следующие действия:*

1. Подготовьте файл логотипа, отвечающий следующим требованиям:
   - формат файла: PNG;
   - название файла: logo.png;
   - размер логотипа: 220×72 пикселя.
2. Поместите файл логотипа в папку установки сервера Apache:
   - Если сервер Apache установлен на Microsoft Windows, путь к папке установки по умолчанию: C:\Program Files\Apache Software Foundation\Apache2.2\htdocs\images\custom_logo.
   - Если сервер Apache установлен на Linux, путь к директории установки по умолчанию: /opt/kaspersky/kscwebconsole/share/htdocs/images/custom_logo.

Настройка системы защиты сети организации-клиента

В этом разделе описаны особенности настройки системы защиты через Консоль администрирования в сети организации-клиента.

Настройка системы защиты является частью процесса развертывания защиты в сети организации-клиента. В процедуру настройки системы защиты входят следующие шаги:

1. Выбор устройства, которое будет играть роль агента обновлений в сети организации-клиента.
2. Локальная установка Агента администрирования на устройство, выбранное агентом обновлений.
3. Удаленная установка Агента администрирования и необходимых программ «Лаборатории Касперского» на устройства организации-клиента.

   > В этом разделе рассмотрены необходимые условия для удаленной установки программ на устройства организации-клиента. Процедура удаленной установки Агента администрирования и антивирусных программ «Лаборатории Касперского» подробно описана в разделе «Удаленная установка программ» (см. стр. 99).

4. Создание иерархии групп администрирования, подчиненных виртуальному Серверу администрирования.

В этом разделе

Назначение устройства агентом обновлений. Настройка параметров агента обновлений

Вы можете управлять устройствами организации-клиента, не имеющими прямой связи с виртуальным Сервером администрирования, через шлюз соединений.

Вы также можете вручную назначить устройство агентом обновлений для группы администрирования и настроить его как шлюз соединений в Консоли администрирования.

► *Чтобы назначить устройство агентом обновлений группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел Сервер администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Агенты обновлений** нажмите на кнопку **Добавить**.

   В результате откроется окно **Добавление агента обновлений**.
4. В окне **Добавление агента обновлений** выполните следующие действия:

   a. Выберите устройство, которое будет выполнять роль агента обновлений, раскрыв список с помощью кнопки , расположенной справа от кнопки **Добавить**. Доступны следующие способы добавления устройства:

      - **Добавить устройство из группы**. Добавление устройства из папки **Управляемые устройства**.
      - **Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**. Ввод адреса шлюза соединений.

      Этот вариант следует использовать для добавления в качестве агента обновлений устройства, защищенного межсетевым экраном, поскольку его невозможно напрямую включить в группу администрирования.

      При выборе устройства учитывайте особенности работы агентов обновлений и требования к устройству, которое выполняет роль агента обновлений.

b. Укажите набор устройств, на которые агент обновлений будет распространять обновления. Вы можете указать группу администрирования или подсеть Network Location Awareness (NLA-подсеть).

5. Нажмите на кнопку **ОК**.

Добавленный агент обновлений отобразится в списке агентов обновлений в разделе Агенты обновлений.

> Первое устройство с установленным Агентом администрирования, которое подключится к виртуальному Серверу, будет автоматически назначено агентом обновлений и настроено в качестве шлюза соединений.

В результате добавления агента обновлений по IP-адресу Сервер администрирования обнаружит его при очередном сканировании сети и поместит в папку **Нераспределенные устройства**. Поскольку агент обновлений защищен межсетевым экраном, для его настройки требуется выполнить следующие действия:

1. Добавить это устройство в выбранную группу администрирования.
2. Снова открыть окно свойств Сервера администрирования на разделе **Агенты обновлений**.
3. Удалить устройство, добавленное по адресу, из списка агентов обновлений.
4. Добавить это же устройство из папки **Управляемые устройства** с помощью кнопки **Добавить** или **Добавить устройство из группы**.
5. В окне свойств этого агента обновлений в разделе **Дополнительно** проверить, установлены ли флажки **Шлюз соединений** и **Инициировать создание соединения с шлюзом со стороны Сервера администрирования**.

Локальная установка Агента администрирования на устройство, выбранное агентом обновлений

Чтобы устройство, выбранное агентом обновлений, могло напрямую связаться с виртуальным Сервером администрирования для выполнения роли шлюза соединений, на это устройство требуется локально установить Агент администрирования.

Порядок локальной установки Агента администрирования на устройство, выбранное агентом обновлений, совпадает с порядком локальной установки Агента администрирования на любое устройство сети.

Для устройства, выбранного агентом обновлений, должны быть выполнены следующие условия:

- В процессе локальной установки Агента администрирования в окне мастера установки **Сервер администрирования** в поле **Адрес сервера** требуется указать адрес виртуального Сервера администрирования, под управлением которого находится устройство. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.

  Используется следующая форма записи адреса виртуального Сервера: <Полный адрес физического Сервера администрирования, которому подчинен виртуальный Сервер>/<Имя виртуального Сервера администрирования>**.**

- Для выполнения роли шлюза соединений на устройстве должны быть открыты все порты, необходимые для связи с Сервером администрирования.

В результате установки на устройство Агента администрирования с указанными параметрами программа Kaspersky Security Center автоматически выполняет следующие действия:

- включает это устройство в группу **Управляемые устройства** виртуального Сервера администрирования;

- назначает это устройство агентом обновлений группы **Управляемые устройства** виртуального Сервера администрирования.

Необходимо и достаточно выполнить локальную установку Агента администрирования на устройстве, назначенное агентом обновлений группы **Управляемые устройства** в сети организации. На устройства, выполняющие роль агентов обновлений во вложенных группах администрирования, Агент администрирования можно установить удаленно, используя агент обновлений группы **Управляемые устройства** в качестве шлюза соединений.

См. также

Локальная установка Агента администрирования 126

Удаленная установка программ 99

Необходимые условия для установки программ на устройства организации-клиента

Процесс удаленной установки программ на устройства организации-клиента совпадает с процессом удаленной установки программ внутри организации (см. раздел Удаленная установка программного обеспечения (см. стр. 99)).

Для установки программ на устройства организации-клиента необходимо выполнение следующих условий:

- Перед первой установкой программ на устройства организации-клиента требуется установить на них Агент администрирования.

  При настройке инсталляционного пакета Агента администрирования на стороне сервис-провайдера в программе Kaspersky Security Center в окне свойств инсталляционного пакета требуется настроить следующие параметры:

  - В разделе **Подключение** в строке **Адрес сервера** требуется указать тот же адрес виртуального Сервера администрирования, что и при локальной установке Агента администрирования на агент обновлений.

  - В разделе **Дополнительно** требуется установить флажок **Подключаться к Серверу администрирования через шлюз соединений**. В строке **Адрес шлюза соединений** нужно указать адрес агента обновлений. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.

- В качестве способа загрузки инсталляционного пакета Агента администрирования необходимо выбрать **Средствами операционной системы с помощью агентов обновлений**. Выбор способа загрузки осуществляется следующим образом:
  - При установке программ с помощью задач удаленной установки способ загрузки можно выбрать двумя способами:
    - при создании задачи удаленной установки в окне **Параметры**;
    - в окне свойств задачи удаленной установки в разделе **Параметры**.
  - При установке программ с помощью мастера удаленной установки способ загрузки можно выбрать в окне мастера **Параметры**.
- Учетная запись, под которой работает агент обновлений, должна иметь доступ к ресурсу Admin$ на клиентских устройствах.

Создание иерархии групп администрирования, подчиненных виртуальному Серверу администрирования

После создания виртуального Сервера администрирования он по умолчанию содержит группу администрирования **Управляемые устройства**.

Процедура создания иерархии групп администрирования, подчиненных виртуальному Серверу администрирования, совпадает с процедурой создания иерархии групп администрирования, подчиненных физическому Серверу администрирования. Эта процедура описана в *Руководстве администратора Kaspersky Security Center*.

> В состав групп администрирования, подчиненных виртуальному Серверу администрирования, нельзя добавлять подчиненные и виртуальные Серверы администрирования. Это связано с ограничениями виртуальных Серверов администрирования, описанными в *Руководстве администратора Kaspersky Security Center*.

Удаленная установка программ

В этом разделе описаны способы удаленной установки программ «Лаборатории Касперского» и их удаления с устройств сети.

Перед началом установки программ на клиентские устройства требуется убедиться в том, что аппаратное и программное обеспечение устройств соответствует предъявляемым к нему требованиям.

В этом разделе рассмотрена удаленная установка программ через Консоль администрирования.

Связь Сервера администрирования с клиентскими устройствами обеспечивает Агент администрирования. Поэтому его необходимо установить на каждое клиентское устройство, которое будет подключено к системе удаленного централизованного управления.

На устройстве, где установлен Сервер администрирования, может использоваться только серверная версия Агента администрирования. Она входит в состав Сервера администрирования и устанавливается и удаляется вместе с ним. Устанавливать Агент администрирования на это устройство не требуется.

Установка Агента администрирования осуществляется точно так же, как и установка программ, и может быть проведена как удаленно, так и локально. При централизованной установке программ защиты через Консоль администрирования вы можете установить Агент администрирования совместно с программами защиты.

Агенты администрирования могут различаться в зависимости от программ «Лаборатории Касперского», для совместной работы с которыми они должны быть установлены. В некоторых случаях возможна только локальная установка Агента администрирования (подробнее см. в Руководствах к соответствующим программам). Агент администрирования устанавливается на клиентское устройство один раз.

Управление программами «Лаборатории Касперского» через Консоль администрирования выполняется при помощи плагинов управления. Поэтому для получения доступа к управлению программой через Kaspersky Security Center плагин управления этой программой должен быть установлен на рабочее место администратора.

Вы можете выполнить удаленную установку программ с рабочего места администратора в главном окне программы Kaspersky Security Center.

> Некоторые программы «Лаборатории Касперского» можно установить на клиентские устройства только локально (подробнее см. в Руководствах к соответствующим программам). Удаленное управление этими программами с помощью Kaspersky Security Center доступно.

Для удаленной установки программного обеспечения следует создать задачу удаленной установки.

Сформированная задача удаленной установки будет запускаться на выполнение в соответствии со своим расписанием. Вы можете прервать процедуру установки, остановив выполнение задачи вручную.

> Если удаленная установка программы завершается с ошибкой, вы можете проверить, чем вызвана эта проблема, и устранить ее с помощью утилиты подготовки устройства к удаленной установке (см. раздел «Подготовка устройства к удаленной установке. Утилита riprep.exe» на стр. 119).

Вы можете отслеживать процесс установки программ защиты «Лаборатории Касперского» в сети с помощью отчета о развертывании.

Kaspersky Security Center поддерживает удаленное управление следующими программами компании «Лаборатория Касперского»:

- Для рабочих станций:
  - Kaspersky Endpoint Security 10 для Windows (поддерживаются все версии);
  - Kaspersky Endpoint Security 8 для Linux (поддерживаются все версии);
  - Kaspersky Endpoint Security 10 для Linux (выход планируется во второй половине 2016 года);

- Kaspersky Endpoint Security 8 для Mac (поддерживаются все версии);
- Kaspersky Endpoint Security 10 для Mac (выход планируется во второй половине 2016 года);
- Kaspersky Embedded Systems Security для Windows (выход планируется в ноябре 2016 года).

- Для мобильных устройств:
  - Kaspersky Security 10 для мобильных устройств (установка доступна при активации функциональности Управление мобильными устройствами);
- Для файловых серверов:
  - Kaspersky Endpoint Security 10 для Windows (поддерживаются все версии);
  - Антивирус Касперского 8.0 для Windows Servers Enterprise Edition (поддерживаются все версии);
  - Kaspersky Security 10 для Windows Server (выход планируется во второй половине 2016 года);
  - Антивирус Касперского 8.0 для Linux File Server (поддерживаются все версии);
  - Антивирус Касперского 10 для Linux File Server (выход планируется во второй половине 2016 года).
- Для виртуальных машин:
  - Kaspersky Security для виртуальных сред 3.0 Защита без агента;
  - Kaspersky Security для виртуальных сред 3.0. Легкий агент (поддерживаются все версии).
- Kaspersky Industrial Cyber Security:
  - Kaspersky Industrial Cyber Security for Nodes.

Вы можете получить сведения о последних версиях программ на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center, в разделе Общие понятия (http://support.kaspersky.ru/12029).

Подробную информацию об управлении перечисленными программами через Kaspersky Security Center см. в Руководствах к соответствующим программам.

В этом разделе

Установка программ с помощью задачи удаленной установки

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

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.

- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

Для правильной работы задачи удаленной установки на устройстве, на котором не установлен Агент администрирования, необходимо открыть порты TCP 139 и 445, UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке (см. раздел «Подготовка устройства к удаленной установке. Утилита riprep.exe» на стр. 119).

В этом разделе

Установка программы на выбранные устройства

► *Чтобы установить программу на выбранные устройства, выполните следующие действия:*

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

2. В дереве консоли выберите папку **Задачи**.

3. Запустите процесс создания задачи по ссылке **Создать задачу**.

   В результате запускается мастер создания задачи. Следуйте его указаниям.

В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** выберите тип задачи **Удаленная установка программы**.

В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на выбранные устройства.

Установка программы на клиентские устройства группы администрирования

► *Чтобы установить программу на клиентские устройства группы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области группы выберите закладку **Задачи**.
4. Запустите процесс создания задачи по ссылке **Создать задачу**.

   В результате запускается мастер создания задачи. Следуйте его указаниям.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** выберите тип задачи **Удаленная установка программы**.

   В результате работы мастера создания задачи будет создана групповая задача удаленной установки выбранной программы. Созданная задача отображается в рабочей области группы администрирования, на закладке **Задачи**.

5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на клиентские устройства группы администрирования.

Установка программы с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать программы «Лаборатории Касперского» с помощью групповых политик Active Directory.

Установка программ с помощью групповых политик Active Directory возможна только при использовании инсталляционных пакетов, в состав которых входит Агент администрирования.

► *Чтобы установить программу с помощью групповых политик Active Directory, выполните следующие действия:*

1. Запустите процесс создания групповой задачи удаленной установки или задачи удаленной установки для набора устройств.
2. В окне мастера создания задачи **Параметры** установите флажок **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.
3. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:
   - групповая политика с именем **Kaspersky_AK{GUID}**;
   - связанная с групповой политикой группа безопасности **Kaspersky_AK{GUID}**. Эта группа безопасности содержит клиентские устройства, на которые распространяется задача. Состав группы безопасности определяет область действия групповой политики.
2. Установка программ на клиентские устройства осуществляется непосредственно из сетевой папки общего доступа программы Share. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msi для устанавливаемой программы.

3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи установлен флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.

4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.

5. При удалении задачи из Active Directory будут удалены политика, ссылка на политику и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной безопасности прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением msi, расположенный во вложенной папке exec в папке инсталляционного пакета нужной программы.
- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки exec, так как помимо файла с расширением msi в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы ключ был установлен вместе с программой, в эту папку следует также скопировать файл ключа.

Установка программ на подчиненные Серверы администрирования

► *Чтобы установить программу на подчиненные Серверы администрирования, выполните следующие действия:*

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

2. Убедитесь в том, что соответствующий устанавливаемой программе инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если инсталляционного пакета нет на каком-либо из подчиненных Серверов, распространите его с помощью задачи распространения инсталляционного пакета (см. раздел «Распространение инсталляционных пакетов на подчиненные Серверы администрирования» на стр. 115).

3. Запустите создание задачи установки программы на подчиненные Серверы администрирования одним из следующих способов:

   - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи удаленной установки для этой группы (см. раздел «Установка программы на клиентские устройства группы администрирования» на стр. 104).
   - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи удаленной установки для набора устройств (см. раздел «Установка программы на выбранные устройства» на стр. 103).

   В результате запустится мастер создания задачи удаленной установки. Следуйте его указаниям.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная установка программы на подчиненные Серверы администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы на выбранные подчиненные Серверы администрирования.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на выбранные подчиненные Серверы администрирования.

Установка программ с помощью мастера удаленной установки

Для установки программ компании вы можете воспользоваться мастером удаленной установки. Мастер удаленной установки позволяет проводить удаленную установку программ как с использованием сформированных инсталляционных пакетов, так и с дистрибутивов.

Для правильной работы задачи удаленной установки на клиентском устройстве, на котором не установлен Агент администрирования, необходимо открыть следующие порты: TCP 139 и 445; UDP 137 и 138. Эти порты по умолчанию открыты для всех устройств, включенных в домен, и открываются автоматически с помощью утилиты подготовки устройства к удаленной установке (см. раздел «Подготовка устройства к удаленной установке. Утилита riprep.exe» на стр. 119).

► *Чтобы установить программу с помощью мастера удаленной установки, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.

2. В дереве консоли выберите группу администрирования.

3. В рабочей области группы нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите пункт **Установить программу.**

   В результате запустится мастер удаленной установки. Следуйте его указаниям.

4. На последнем шаге мастера нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

В результате работы мастера удаленной установки Kaspersky Security Center выполняет следующие действия:

- Создает инсталляционный пакет для установки программы (если он не был создан раньше). Инсталляционный пакет размещается в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты** с именем, соответствующим названию и версии программы. Вы можете использовать этот инсталляционный пакет для установки программы в дальнейшем.

- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Сформированная задача удаленной установки размещается в папке **Задачи** или добавляется к задачам группы администрирования, для которой она была создана. Вы можете запускать эту задачу в дальнейшем вручную. Имя задачи соответствует имени инсталляционного пакета для установки программы: **Установка <Имя инсталляционного пакета>**.

Просмотр отчета о развертывании защиты

Для отслеживания процесса развертывания защиты в сети можно использовать отчет о развертывании защиты.

► *Чтобы просмотреть отчет о развертывании защиты, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите закладку **Отчеты**

3. В рабочей области закладки **Отчеты** выберите шаблон отчета **Отчет о развертывании защиты**.

В рабочей области будет сформирован отчет, содержащий информацию о развертывании защиты на всех устройствах сети.

Вы можете сформировать новый отчет о развертывании защиты и указать, информацию какого типа в него следует включать:

- для группы администрирования;
- для набора устройств;
- для выборки устройств;
- для всех устройств.

Подробную информацию о создании нового отчета см. в *Руководстве администратора Kaspersky Security Center*.

В рамках Kaspersky Security Center считается, что на устройстве развернута защита в том случае, когда на нем установлена программа защиты и включена постоянная защита.

Удаленная деинсталляция программ

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

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

В этом разделе

Удаленная деинсталляция программы с клиентских устройств группы администрирования

► *Чтобы удаленно деинсталлировать программу с клиентских устройств группы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области группы выберите закладку **Задачи**.
4. Запустите процесс создания задачи по ссылке **Создать задачу**.

   В результате запускается мастер создания задачи. Следуйте его указаниям.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция программы**.

   В результате работы мастера создания задачи будет создана групповая задача удаленной деинсталляции выбранной программы. Созданная задача отображается в рабочей области группы администрирования, на закладке **Задачи**.
5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранная программа будет удалена с клиентских устройств группы администрирования.

Удаленная деинсталляция программы с выбранных устройств

► *Чтобы удаленно деинсталлировать программу с выбранных устройств, выполните следующие действия:*

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

2. В дереве консоли выберите папку **Задачи**.

3. Запустите процесс создания задачи по кнопке **Создать задачу**.

   В результате запускается мастер создания задачи. Следуйте его указаниям.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция программы**.

   В результате работы мастера создания задачи будет создана задача удаленной деинсталляции выбранной программы для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет удалена с выбранных устройств.

Работа с инсталляционными пакетами

При создании задач удаленной установки используются инсталляционные пакеты, которые содержат набор параметров, необходимых для установки программы.

> Инсталляционные пакеты могут содержать в себе файл ключа. Не рекомендуется размещать в открытом доступе инсталляционные пакеты, содержащие в себе файл ключа.

Вы можете использовать один и тот же инсталляционный пакет многократно.

Сформированные для Сервера администрирования инсталляционные пакеты размещаются в дереве консоли в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

В этом разделе

Создание инсталляционного пакета

► *Чтобы создать инсталляционный пакет, выполните следующие действия:*

1. Подключитесь к нужному Серверу администрирования.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Запустите процесс создания инсталляционного пакета одним из следующих способов:
   - в контекстном меню папки **Инсталляционные пакеты** выберите пункт **Создать → Инсталляционный пакет**;
   - в контекстном меню списка инсталляционных пакетов выберите пункт **Создать → Инсталляционный пакет**;
   - по ссылке **Создать инсталляционный пакет** в блоке управления списком инсталляционных пакетов.

В результате запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

В процессе создания инсталляционного пакета для программы «Лаборатории Касперского» вам может быть предложено ознакомиться с Лицензионным соглашением на

эту программу. Внимательно прочитайте Лицензионное соглашение. Если вы согласны со всеми его пунктами, установите флажок **Принимаю условия Лицензионного соглашения**. После этого создание инсталляционного пакета будет продолжено. Путь к файлу Лицензионного соглашения задается в файле с расширением kud или kpd, входящем в состав дистрибутива программы, для которой создается инсталляционный пакет.

> При создании инсталляционного пакета для программы Kaspersky Endpoint Security для Mac вы можете выбрать язык Лицензионного соглашения.

Во время создания инсталляционного пакета для программы из базы программ «Лаборатории Касперского» вы можете включить автоматическую установку общесистемных компонентов (пререквизитов), необходимых для установки этой программы. Мастер создания инсталляционного пакета отображает список всех возможных общесистемных компонентов для выбранной программы. Если инсталляционный пакет создается для патча (неполный дистрибутив), то в список общесистемных компонентов будут включены все необходимые для развертывания патча составляющие, вплоть до версии с полным дистрибутивом. Впоследствии вы можете ознакомиться с этим списком в свойствах инсталляционного пакета.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей области папки **Инсталляционные пакеты** в дереве консоли.

Инсталляционный пакет для удаленной установки Агента администрирования не нужно создавать вручную. Он формируется автоматически при установке программы Kaspersky Security Center и располагается в папке **Инсталляционные пакеты**. Если пакет для удаленной установки Агента администрирования был удален, то для его повторного формирования в качестве файла с описанием следует выбрать файл nagent10.kud, расположенный в папке NetAgent дистрибутива Kaspersky Security Center.

> Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

При создании инсталляционного пакета Сервера администрирования в качестве файла с описанием следует выбрать файл sc10.kud, расположенный в корневой папке дистрибутива Kaspersky Security Center.

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

► *Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Запустите создание задачи распространения инсталляционного пакета на подчиненные Серверы администрирования одним из следующих способов:
   - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи для этой группы.
   - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи для набора устройств.

   В результате запустится мастер создания задачи. Следуйте его указаниям.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Распространение инсталляционного пакета**.

   В результате работы мастера создания задачи будет создана задача распространения выбранных инсталляционных пакетов на выбранные подчиненные Серверы администрирования.
3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи выбранные инсталляционные пакеты будут скопированы на выбранные подчиненные Серверы администрирования.

Распространение инсталляционных пакетов с помощью агентов обновлений

Для распространения инсталляционных пакетов в пределах группы администрирования вы можете использовать агенты обновлений.

После получения инсталляционных пакетов с Сервера администрирования агенты обновлений автоматически распространяют их на клиентские устройства с помощью многоадресной IP-рассылки. IP-рассылка новых инсталляционных пакетов в пределах группы администрирования производится один раз. Если в момент рассылки клиентское устройство было отключено от сети организации, то при запуске задачи установки Агент администрирования клиентского устройства автоматически скачивает необходимый инсталляционный пакет с агента обновлений.

Передача в Kaspersky Security Center информации о результатах установки программы

После создания инсталляционного пакета программы вы можете настроить инсталляционный пакет таким образом, чтобы диагностическая информация о результатах установки программы передавалась в Kaspersky Security Center. Для инсталляционных пакетов программ «Лаборатории Касперского» передача диагностической информации о результате установки программы настроена по умолчанию, дополнительная настройка не требуется.

► *Чтобы настроить передачу в Kaspersky Security Center диагностической информации о результате установки программы, выполните следующие действия:*

1. Перейдите в папку инсталляционного пакета, сформированного средствами Kaspersky Security Center для выбранной программы. Эта папка расположена в папке общего доступа, которая была указана при установке Kaspersky Security Center.
2. Откройте файл с расширением kpd или kud для редактирования (например, с помощью текстового редактора Блокнот Microsoft Windows).

   Файл имеет формат обычного конфигурационного ini-файла.
3. Добавьте в файл следующие строки:

   ```
   [SetupProcessResult]

   Wait=1
   ```

   Эта команда настраивает программу Kaspersky Security Center таким образом, чтобы она ожидала окончания установки программы, для которой сформирован инсталляционный пакет и анализировала код возврата программы установки. Если нужно отключить передачу диагностической информации, установите для ключа Wait значение 0.

4. Внесите описание кодов возврата успешной установки. Для этого добавьте в файл следующие строки:

   ```
   [SetupProcessResult_SuccessCodes]

   <код возврата>=[<описание>]

   <код возврата 1>=[<описание>]

   …
   ```

   > В квадратных скобках приводятся необязательные ключи.

   Синтаксис строк:

   - `<код возврата>`. Любое число, соответствующее коду возврата программы установки. Количество кодов возврата может быть произвольным.
   - `<описание>`. Текстовое описание результата установки. Описание может отсутствовать.

5. Внесите описание кодов возврата для установки, завершенной с ошибкой. Для этого добавьте в файл следующие строки:

   ```
   [SetupProcessResult_ErrorCodes]

   <код возврата>=[<описание>]

   <код возврата 1>=[<описание>]

   …
   ```

   Синтаксис строк соответствует синтаксису строк кодов возврата при успешной установке.

6. Закройте kpd- или kud-файл, сохранив внесенные изменения.

Информация о результатах установки программы, указанной пользователем, будет записываться в журналах Kaspersky Security Center и отображаться в списке событий, в отчетах и в результатах выполнения задач.

Получение актуальных версий программ

Kaspersky Security Center позволяет получать актуальные версии корпоративных программ, выложенные на интернет-серверах «Лаборатории Касперского».

► *Чтобы получить актуальные версии корпоративных программ «Лаборатории Касперского», выполните следующие действия:*

1. Откройте главное окно Kaspersky Security Center.
2. Откройте окно **Актуальные версии программ** по ссылке **Вышли новые версии программ «Лаборатории Касперского» в** блоке **Развертывание**.

   Ссылка **Вышли новые версии программ «Лаборатории Касперского»** становится доступна, когда Сервер администрирования обнаруживает очередную версию корпоративной программы на интернет-сервере «Лаборатории Касперского».

3. Выберите в списке нужную вам программу.
4. Загрузите дистрибутив программы по ссылке в строке **Веб-адрес дистрибутива**.

   Если для выбранной программы отображается кнопка **Загрузить программы и создать инсталляционные пакеты**, вы можете нажать на эту кнопку для загрузки дистрибутива программы и автоматического создания инсталляционного пакета. В этом случае Kaspersky Security Center загружает дистрибутив программы на Сервер администрирования в папку общего доступа, заданную при установке Kaspersky Security Center. Автоматически созданный инсталляционный пакет отображается в папке **Удаленная установка** дерева консоли, во вложенной папке **Инсталляционные пакеты**.

После закрытия окна **Актуальные версии программ** ссылка **Вышли новые версии программ «Лаборатории Касперского»** исчезает из блока **Развертывание**.

Вы можете создавать инсталляционные пакеты новых версий программ и работать с созданными инсталляционными пакетами в папке **Удаленная установка** дерева консоли, во вложенной папке **Инсталляционные пакеты**.

Вы также можете открыть окно **Актуальные версии программ** по ссылке **Просмотреть актуальные версии программ «Лаборатории Касперского» в** рабочей области папки **Инсталляционные пакеты**.

См. также

Подготовка устройства к удаленной установке. Утилита riprep.exe

Удаленная установка программы на клиентском устройстве может завершаться с ошибкой по следующим причинам:

- Задача ранее уже была успешно выполнена на этом устройстве. В этом случае ее повторное выполнение не требуется.
- Во время запуска задачи устройство было выключено. В этом случае требуется включить устройство и запустить задачу еще раз.
- Отсутствует связь между Сервером администрирования и Агентом администрирования, установленным на клиентском устройстве. Для определения причины проблемы вы можете воспользоваться утилитой удаленной диагностики устройства (klactgui). Подробную информацию об использовании этой утилиты см. в *Руководстве администратора Kaspersky Security Center*.

- Если на устройстве не установлен Агент администрирования, при удаленной установке программы могут возникнуть следующие проблемы:
  - на клиентском устройстве включен параметр **Простой общий доступ к файлам**;
  - на клиентском устройстве не работает служба Server;
  - на клиентском устройстве закрыты необходимые порты;
  - у учетной записи, под которой выполняется задача, недостаточно прав.

  Для решения проблем, возникших при установке программы на клиентское устройство, на котором не установлен Агент администрирования, вы можете воспользоваться утилитой подготовки устройства к удаленной установке (riprep).

В этом разделе описывается утилита подготовки устройства к удаленной установке (riprep). Она расположена в папке установки Kaspersky Security Center на устройстве с установленным Сервером администрирования.

Утилита подготовки устройства к удаленной установке не работает под управлением операционной системы Microsoft Windows XP Home Edition.

В этом разделе

Подготовка устройства к удаленной установке в интерактивном режиме

► *Чтобы подготовить устройство к удаленной установке в интерактивном режиме, выполните следующие действия:*

1. На клиентском устройстве запустите файл riprep.exe.
2. В открывшемся главном окне утилиты подготовки к удаленной установке установите следующие флажки:
   - **Отключить простой общий доступ к файлам**.

- **Запустить службу Server**.
- **Открыть порты**.
- **Добавить учетную запись**.
- **Отключить контроль учетных записей (UAC)**. Этот параметр доступен для операционных систем Microsoft Windows Vista, Microsoft Windows 7 и Microsoft Windows Server 2008.

3. Нажмите на кнопку **Запустить**.

В результате в нижней части главного окна утилиты отображаются этапы подготовки устройства к удаленной установке.

Если вы установили флажок **Добавить учетную запись**, при создании учетной записи будет выведен запрос на ввод имени учетной записи и пароля. В результате будет создана локальная учетная запись, принадлежащая группе локальных администраторов.

Если вы установили флажок **Отключить контроль учетных записей**, попытка отключения контроля учетных записей будет выполняться и в том случае, когда до запуска утилиты контроль учетных записей был отключен. После отключения контроля учетных записей будет выведен запрос на перезагрузку устройства.

Подготовка устройства к удаленной установке в неинтерактивном режиме

► *Чтобы подготовить устройство к удаленной установке в неинтерактивном режиме,*

на клиентском устройстве запустите файл riprep.exe из командной строки с необходимым набором ключей.

Синтаксис утилиты:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Описание ключей:

- `-silent` – запуск утилиты в неинтерактивном режиме.
- `-cfg CONFIG_FILE` – определение конфигурации утилиты, где `CONFIG_FILE` – путь к файлу конфигурации (файл с расширением .ini).
- `-tl traceLevel` – задание уровня трассировки, где `traceLevel` – число от 0 до 5. Если ключ не задан, то используется значение 0.

В результате запуска утилиты в неинтерактивном режиме вы можете выполнить следующие задачи:

- отключение простого общего доступа к файлам;
- запуск службы Server на клиентском устройстве;
- открытие портов;
- создание локальной учетной записи;
- отключение контроля учетных записей (UAC).

Вы можете задать параметры подготовки устройства к удаленной установке в конфигурационном файле, указанном в ключе `-cfg`. Чтобы задать эти параметры, в конфигурационный файл нужно добавить следующую информацию:

- В разделе `Common` указать, какие задачи следует выполнять:
  - `DisableSFS` – отключение простого общего доступа к файлам (0 – задача выключена; 1 – задача включена).
  - `StartServer` – запуск службы Server (0 – задача выключена; 1 – задача включена).
  - `OpenFirewallPorts` – открытие необходимых портов (0 – задача выключена; 1 – задача включена).
  - `DisableUAC` – отключение контроля учетных записей (0 – задача выключена; 1 – задача включена).

- `RebootType` – определение поведения при необходимости перезагрузки при отключении контроля учетных записей. Вы можете использовать следующие значения параметра:
  - 0 – никогда не перезагружать устройство;
  - 1 – перезагружать устройство, если до запуска утилиты контроль учетных записей был включен;
  - 2 – перезагружать устройство принудительно, если до запуска утилиты контроль учетных записей был включен;
  - 4 – всегда перезагружать устройство;
  - 5 – всегда принудительно перезагружать устройство.

- В разделе `UserAccount` указать имя учетной записи (`user`) и ее пароль (`Pwd`).

Пример содержимого конфигурационного файла:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1

[UserAccount]
user=Admin
Pwd=Pass123
```

По окончании работы утилиты в папке запуска создаются следующие файлы:

- riprep.txt – отчет о работе, в котором перечислены этапы работы утилиты с причинами их проведения;
- riprep.log – файл трассировки (создается, если заданный уровень трассировки больше 0).

Локальная установка программ

В этом разделе описана процедура установки программ, которые могут быть установлены на устройства только локально.

Для проведения локальной установки программ на выбранном клиентском устройстве вам необходимо обладать правами администратора на этом устройстве.

► *Чтобы установить программы локально на выбранное клиентское устройство, выполните следующие действия:*

1. Установите на клиентское устройство Агент администрирования и настройте связь клиентского устройства с Сервером администрирования.
2. Установите на устройство необходимые программы согласно описаниям, изложенным в Руководствах к этим программам.
3. Установите на рабочее место администратора плагин управления для каждой из установленных программ.

Kaspersky Security Center также поддерживает возможность локальной установки программ с помощью автономного пакета установки.

Создание автономных пакетов установки доступно для следующих программ:

- Для рабочих станций:
  - Kaspersky Endpoint Security 10 для Windows (поддерживаются все версии);
  - Kaspersky Endpoint Security 10 для Linux (выход планируется во второй половине 2016 года);
  - Kaspersky Endpoint Security 8 для Linux (поддерживаются все версии);
  - Kaspersky Endpoint Security 10 для Mac (выход планируется во второй половине 2016 года);
  - Kaspersky Endpoint Security 8 для Mac (поддерживаются все версии);
  - Kaspersky Embedded Systems Security для Windows (выход планируется в ноябре 2016 года).

- Для мобильных устройств:
  - Kaspersky Security 10 для мобильных устройств (установка доступна при активации функциональности Управление мобильными устройствами).
- Для почтовых систем и серверов совместной работы:
  - Kaspersky Security 8.0 для Linux Mail Server Maintenance Pack 1 (и выше);
  - Kaspersky Secure Mail Gateway 1.0;
  - Kaspersky Security для Microsoft Exchange Servers (выход планируется во второй половине 2016 года);
  - Kaspersky Security для SharePoint Server (выход планируется во второй половине 2016 года).
- Для файловых серверов:
  - Kaspersky Endpoint Security 10 для Windows (поддерживаются все версии);
  - Антивирус Касперского 8.0 для Windows Servers Enterprise Edition (поддерживаются все версии);
  - Kaspersky Security 10 для Windows Server (выход планируется во второй половине 2016 года);
  - Антивирус Касперского 8.0 для Linux File Server (поддерживаются все версии).
  - Антивирус Касперского 10 для Linux File Server (выход планируется во второй половине 2016 года).
- Для виртуальных машин:
  - Kaspersky Security для виртуальных сред 3.0 Защита без агента;
  - Kaspersky Security для виртуальных сред 4.0 Защита без агента (выход планируется в ноябре 2016 года);
  - Kaspersky Security для виртуальных сред 3.0 Легкий агент (поддерживаются все версии);
  - Kaspersky Security для виртуальных сред 4.0 Легкий агент (выход планируется в ноябре 2016 года).

- Kaspersky Industrial Cyber Security:
  - Kaspersky Industrial Cyber Security for Networks;
  - Kaspersky Industrial Cyber Security for Nodes.

Вы можете получить сведения о последних версиях программ на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center 10, в разделе Общие понятия (http://support.kaspersky.ru/12029).

В этом разделе

Локальная установка Агента администрирования

► *Чтобы установить Агент администрирования на устройство локально, выполните следующие действия:*

1. На устройстве запустите файл setup.exe с дистрибутивного компакт-диска или дистрибутива, полученного через интернет.

   Откроется окно с выбором программ «Лаборатории Касперского» для установки.

2. В окне с выбором программ по ссылке **Установить только Агент администрирования Kaspersky Security Center** запустите мастер установки Агента администрирования. Следуйте указаниям мастера.

   Во время работы мастера установки вы можете настроить дополнительные параметры Агента администрирования (см. ниже). Процесс установки Агента администрирования с дистрибутива, полученного через интернет, совпадает с процессом установки Агента администрирования с дистрибутивного компакт-диска.

3. Чтобы использовать устройство в качестве шлюза соединений для выбранной группы администрирования, в окне **Шлюз соединений** мастера установки выберите вариант **Использовать в качестве шлюза соединений в демилитаризованной зоне**.

4. Чтобы настроить Агент администрирования при установке на виртуальную машину, выполните следующие действия:

   a. Включите динамический режим Агента администрирования для Virtual Desktop Infrastructure (VDI). Для этого в окне мастера установки **Дополнительные параметры** установите флажок **Включить динамический режим для VDI**.

   b. Оптимизируйте работу Агента администрирования для виртуальной инфраструктуры. Для этого в окне мастера установки **Дополнительные параметры** установите флажок **Оптимизировать параметры Агента администрирования Kaspersky Security Center для виртуальной инфраструктуры.**

      В результате будет выключена проверка исполняемых файлов на наличие уязвимостей при запуске устройства. Также будет выключена передача на Сервер администрирования следующей информации:

      - о реестре оборудования;
      - о программах, установленных на устройстве;
      - об обновлениях Microsoft Windows, которые необходимо установить на локальном клиентском устройстве;
      - об уязвимостях программного обеспечения, обнаруженных на локальном клиентском устройстве.

      В дальнейшем вы сможете включить передачу этой информации в свойствах Агента администрирования или в параметрах политики Агента администрирования.

   По окончании работы мастера установки Агент администрирования будет установлен на устройстве.

Вы можете просматривать свойства службы Агента администрирования Kaspersky Security Center, запускать, останавливать и следить за работой Агента администрирования при помощи стандартных средств администрирования Microsoft Windows – Управление компьютером\Службы.

Установка Агента администрирования в неинтерактивном режиме

Агент администрирования может быть установлен в неинтерактивном режиме, то есть без интерактивного ввода параметров установки. Для неинтерактивной установки используется установочный msi-пакет Агента администрирования, расположенный в дистрибутиве программы Kaspersky Security Center в папке Packages\NetAgent\exec.

► *Чтобы установить Агент администрирования на локальном устройстве в неинтерактивном режиме,*

выполните команду

```
msiexec /i "Kaspersky Network Agent.msi"
/qn <setup_parameters>
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PRO1=PROP1VAL PROP2=PROP2VAL`).

Имена и возможные значения параметров, которые можно использовать при установке Агента администрирования в неинтерактивном режиме, приведены в таблице ниже.

Таблица 8. Параметры установки Агента администрирования в неинтерактивном режиме

Имя параметра	Описание параметра	Возможные значения
INSTALLDIR	Путь к папке установки Агента администрирования.	Строковое значение.
SERVERADDRESS	Адрес Сервера администрирования.	Строковое значение.
SERVERPORT	Номер порта для подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL.	Числовое значение.

Имя параметра	Описание параметра	Возможные значения
USESSL	Использовать ли SSL-соединение.	• 1 – использовать; • другое значение или не задано – не использовать.
OPENUDPPORT	Открывать ли UDP-порт.	• 1 – открывать; • другое значение или не задано – открывать.
UDPPORT	Номер UDP-порта.	Числовое значение
USEPROXY	Использовать ли прокси-сервер.	• 1 – использовать; • другое значение или не задано – не использовать.
PROXYADDRESS	Адрес прокси-сервера.	Строковое значение.
PROXYPORT	Номер порта для подключения к прокси-серверу.	Числовое значение.
PROXYLOGIN	Имя учетной записи для подключения к прокси-серверу.	Строковое значение.
PROXYPASSWORD	Пароль учетной записи для подключения к прокси-серверу. Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.	Строковое значение.

Имя параметра	Описание параметра	Возможные значения
GATEWAYMODE	Режим использования шлюза соединений.	• 0 – не использовать шлюз соединений; • 1 – использовать устройство, на котором устанавливается Агент администрирования, в качестве шлюза соединений; • 2 – подключаться к Серверу администрирования через другой шлюз соединений.
GATEWAYADDRESS	Адрес шлюза соединений.	Строковое значение.
CERTSELECTION	Способ получения сертификата.	• GetOnFirstConnection – получить сертификат Сервера администрирования; • GetExistent – выбрать существующий сертификат.
CERTFILE	Путь к файлу сертификата.	Строковое значение.
VMVDI	Включать ли динамический режим для VDI.	• 1 – включать; • другое значение или не задано – не включать.
LAUNCHPROGRAM	Запускать ли службу Агента администрирования после окончания установки.	• 1 – запускать; • другое значение или не задано – не запускать.

Удаленная установка Агента администрирования с помощью инсталляционного пакета или локальная установка в неинтерактивном режиме означает согласие с условиями Лицензионного соглашения на устанавливаемую программу. Просмотреть Лицензионное соглашение на конкретную программу можно в комплекте поставки этой программы или на веб-сайте Службы технической поддержки «Лаборатории Касперского».

Локальная установка плагина управления программой

► *Чтобы установить плагин управления программой,*

на устройстве, где установлена Консоль администрирования, запустите исполняемый файл klcfginst.exe, входящий в дистрибутивный пакет этой программы.

Файл klcfginst.exe входит в состав всех программ, которыми может управлять Kaspersky Security Center. Установка сопровождается мастером и не требует настройки параметров.

Установка программ в неинтерактивном режиме

► *Чтобы провести установку программы в неинтерактивном режиме, выполните следующие действия:*

1. Откройте главное окно программы Kaspersky Security Center
2. В папке дерева консоли **Удаленная установка** во вложенной папке **Инсталляционные пакеты** выберите инсталляционный пакет нужной программы или сформируйте для этой программы новый инсталляционный пакет.

   Инсталляционный пакет будет сохранен на Сервере администрирования в папке общего доступа в служебной папке Packages. При этом каждому инсталляционному пакету соответствует отдельная вложенная папка.

3. Откройте папку нужного инсталляционного пакета одним из следующих способов:

   - Скопируйте папку, соответствующую нужному инсталляционному пакету, с Сервера администрирования на клиентское устройство. Затем откройте скопированную папку на клиентском устройстве.
   - С клиентского устройства откройте на Сервере администрирования папку общего доступа, соответствующую нужному инсталляционному пакету.

Если папка общего доступа расположена на устройстве с установленной операционной системой Microsoft Windows Vista, необходимо установить значение **Отключен** для параметра **Управление учетными записями пользователей: все администраторы работают в режиме одобрения администратором** (**Пуск** → **Панель управления** → **Администрирование** → **Локальная политика безопасности** → **Параметры безопасности**).

4. В зависимости от выбранной программы выполните следующие действия:

   - Для Антивируса Касперского для Windows Workstations, Антивируса Касперского для Windows Servers и Kaspersky Security Center перейдите во вложенную папку exec и запустите исполняемый файл (файл с расширением exe) с ключом /s.
   - Для остальных программ «Лаборатории Касперского» запустите из открытой папки исполняемый файл (файл с расширением exe) с ключом /s.

   Запуск исполняемого файла с ключом `EULA=1` означает, что вы принимаете положения Лицензионного соглашения. Текст Лицензионного соглашения входит в комплект поставки Kaspersky Security Center. Согласие с положениями Лицензионного соглашения является необходимым условием для установки программы или обновления предыдущей версии программы.

Установка программ с помощью автономных пакетов

Kaspersky Security Center позволяет формировать автономные пакеты установки программ. Автономный пакет установки представляет собой исполняемый файл, который можно разместить на Веб-сервере, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки программы без участия Kaspersky Security Center.

► *Чтобы установить программу с помощью автономного пакета установки, выполните следующие действия:*

1. Подключитесь к нужному Серверу администрирования.
2. В папке дерева консоли **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В рабочей области выберите инсталляционный пакет нужной программы.
4. Запустите процесс создания автономного пакета установки одним из следующих способов:
   - в контекстном меню инсталляционного пакета выберите пункт **Создать автономный пакет установки**;
   - по ссылке **Создать автономный пакет установки** в блоке работы с инсталляционным пакетом.

   В результате запускается мастер создания автономного пакета установки. Следуйте его указаниям.

   На завершающем шаге мастера выберите способ передачи автономного пакета установки на клиентское устройство.
5. Передайте автономный пакет установки программы на клиентское устройство.
6. Запустите автономный пакет установки на клиентском устройстве.

В результате программа будет установлена на клиентском устройстве с параметрами, указанными в автономном пакете.

При создании автономный пакет установки автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных пакетов установки. При необходимости вы можете отменить публикацию выбранного автономного пакета и снова опубликовать его на Веб-сервере. По умолчанию для загрузки автономных пакетов установки используется порт 8060.

Развертывание систем управления мобильными устройствами

В этом разделе описано развертывание систем управления мобильных устройств по протоколам Exchange ActiveSync, iOS MDM и Kaspersky Endpoint Security.

В этом разделе

Управление с помощью iOS MDM-протокола и протокола Microsoft Exchange ActiveSync

Kaspersky Security Center позволяет управлять мобильными устройствами, которые подключаются к Серверу администрирования по протоколу Exchange ActiveSync. Мобильными устройствами Exchange ActiveSync (EAS-устройствами) называются мобильные устройства, подключенные к Серверу мобильных устройств Exchange ActiveSync и находящиеся под управлением Сервера администрирования.

Протокол Exchange ActiveSync поддерживают следующие операционные системы:

- Windows Mobile;
- Windows CE;
- Windows Phone® 7;

- Windows Phone 8;
- Android;
- Bada;
- BlackBerry® 10;
- iOS®;
- Symbian.

Набор параметров управления устройством Exchange ActiveSync зависит от операционной системы, под управлением которой находится мобильное устройство. С особенностями поддержки протокола Exchange ActiveSync для конкретной операционной системы можно ознакомиться в документации для этой операционной системы.

Развертывание системы управления мобильными устройствами по протоколу Exchange ActiveSync выполняется в следующей последовательности:

1. Администратор устанавливает на выбранное клиентское устройство Сервер мобильных устройств Exchange ActiveSync (см. раздел «Установка Сервера мобильных устройств Exchange ActiveSync» на стр. 136).
2. Администратор создает в Консоли администрирования профиль (профили) управления EAS-устройствами и добавляет профиль к почтовым ящикам пользователей Exchange ActiveSync.

   Профиль управления мобильными устройствами Exchange ActiveSync – это политика ActiveSync, которая используется на сервере Microsoft Exchange для управления мобильными устройствами Exchange ActiveSync. Почтовому ящику Microsoft Exchange можно назначить только один профиль управления EAS-устройствами.

   Инструкцию по созданию профиля управления EAS-устройствами см. в *Руководстве администратора Kaspersky Security Center*.

Пользователи мобильных EAS-устройств подключаются к своим почтовым ящикам Exchange. Профиль управления накладывает ограничения на мобильные устройства (см. раздел «Подключение мобильных устройств к Серверу мобильных устройств Exchange ActiveSync» на стр. 138).

Информацию о добавлении профиля управления EAS-устройствами и об управлении мобильными устройствами Exchange ActiveSync см. в *Руководстве администратора Kaspersky Security Center*.

Установка Сервера мобильных устройств Exchange ActiveSync

Сервер мобильных устройств Exchange ActiveSync устанавливается на клиентское устройство с установленным сервером Microsoft Exchange. Рекомендуется устанавливать Сервер мобильных устройств Exchange ActiveSync на сервер Microsoft Exchange с ролью Client Access. Если в одном домене несколько серверов Microsoft Exchange с ролью Client Access объединены в массив (Client Access Array), то рекомендуется устанавливать Сервер мобильных устройств Exchange ActiveSync в режиме кластера на каждый сервер Microsoft Exchange в массиве.

► *Чтобы установить Сервер мобильных устройств Exchange ActiveSync на локальном устройстве, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ «Лаборатории Касперского» для установки.

2. В окне с выбором программ по ссылке **Установить Сервер мобильных устройств Exchange ActiveSync** запустите мастер установки Сервера мобильных устройств Exchange ActiveSync.

3. В окне **Настройка установки** выберите тип установки Сервера мобильных устройств Exchange ActiveSync:

   - Если вы хотите установить Сервер мобильных устройств Exchange ActiveSync с использованием параметров по умолчанию, выберите вариант **Стандартная установка** и нажмите на кнопку **Далее**.

- Если вы хотите задать вручную значения параметров установки Сервера мобильных устройств Exchange ActiveSync, выберите вариант **Расширенная установка** и нажмите на кнопку **Далее**. Затем выполните следующие действия:

  a. В окне **Папка назначения** выберите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Mobile Device Management for Exchange. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете сменить папку назначения с помощью кнопки **Обзор**.

  b. В окне **Режим установки** выберите режим установки Сервера мобильных устройств Exchange ActiveSync: обычный режим или режим кластера.

  c. В окне **Выбор учетной записи** выберите учетную запись, которая будет использоваться для управления мобильными устройствами:

  - **Создать учетную запись и ролевую группу автоматически**. Учетная запись будет создана автоматически.
  - **Указать учетную запись**. Учетную запись следует выбрать вручную. С помощью кнопки **Выбрать** укажите пользователя, чья учетная запись будет использоваться, и пароль. Выбранный пользователь должен входить в группу с правами на управление мобильными устройствами через ActiveSync.

  d. В окне **Настройка IIS** разрешите или запретите автоматическую настройку параметров веб-сервера Internet Information Services (IIS).

  > Если вы запретили автоматическую настройку параметров IIS, включите вручную механизм аутентификации «Windows authentication» в параметрах IIS для виртуальной директории PowerShell. Если механизм аутентификации «Windows authentication» не будет включен, установленный Сервер мобильных устройств Exchange ActiveSync будет неработоспособен. Информацию о работе с параметрами IIS можно прочитать в документации для этого веб-сервера.

  e. Нажмите на кнопку **Далее**.

4. В открывшемся окне проверьте значения параметров установки Сервера мобильных устройств Exchange ActiveSync и нажмите на кнопку **Установить**.

В результате работы мастера будет выполнена установка Сервера мобильных устройств Exchange ActiveSync на локальное устройство. Сервер мобильных устройств Exchange ActiveSync будет отображаться в папке **Управление мобильными устройствами** дерева консоли.

Подключение мобильных устройств к Серверу мобильных устройств Exchange ActiveSync

Перед подключением мобильных устройств должен быть настроен Microsoft Exchange Server для возможности соединения устройств по протоколу ActiveSync.

Чтобы подключить мобильное устройство к Серверу мобильных устройств Exchange ActiveSync, пользователь с мобильного устройства подключается к своему почтовому ящику Microsoft Exchange, используя ActiveSync. При подключении пользователь в клиенте ActiveSync должен указать параметры подключения, например, адрес электронной почты, пароль электронной почты.

Мобильное устройство пользователя, подключенное к серверу Microsoft Exchange, отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

После подключения мобильного устройства Exchange ActiveSync к Серверу мобильных устройств Exchange ActiveSync администратор может управлять подключенным мобильным устройством Exchange ActiveSync. Информацию об управлении мобильными устройствами Exchange ActiveSync см. в *Руководстве администратора Kaspersky Security Center*.

Развертывание системы управления по протоколу iOS MDM

Kaspersky Security Center позволяет управлять мобильными устройствами на платформе iOS. Мобильными устройствами iOS MDM называются мобильные устройства iOS, подключенные к Серверу iOS MDM и находящиеся под управлением Сервера администрирования.

Подключение мобильных устройств к Серверу iOS MDM выполняется в следующей последовательности:

1. Администратор устанавливает на выбранное клиентское устройство Сервер iOS MDM. Установка Сервера iOS MDM выполняется штатными средствами операционной системы.

2. Администратор получает сертификат Apple® Push Notification Service (APNs-сертификат) (см. раздел «Получение APNs-сертификата» на стр. 147).

   APNs-сертификат позволяет Серверу администрирования подключаться к серверу APNs для отправки push-уведомлений на мобильные устройства iOS MDM.

3. Администратор устанавливает на Сервере iOS MDM APNs-сертификат (см. раздел «Установка сертификата APNs на Сервер iOS MDM» на стр. 149).

4. Администратор формирует iOS MDM-профиль для пользователя мобильного устройства iOS.

   iOS MDM-профиль содержит набор параметров подключения мобильных устройств iOS к Серверу администрирования.

5. Администратор выписывает пользователю общий сертификат (см. раздел «Выписка и установка общего сертификата на мобильное устройство» на стр. 150).

   Общий сертификат необходим для подтверждения того, что мобильное устройство принадлежит пользователю.

6. Пользователь переходит по ссылке, высланной администратором, и загружает установочный пакет на мобильное устройство.

   Установочный пакет содержит сертификат и iOS MDM-профиль.

   После загрузки iOS MDM-профиля и синхронизации с Сервером администрирования мобильное устройство iOS MDM отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

7. Администратор добавляет конфигурационный профиль на Сервер iOS MDM и после подключения мобильного устройства устанавливает на него конфигурационный профиль.

   Конфигурационный профиль содержит набор параметров и ограничений для мобильного устройства iOS MDM, например, параметры установки приложений и использования различных функций мобильного устройства, параметры работы с электронной почтой и календарем. Конфигурационный профиль позволяет настраивать мобильные устройства iOS MDM в соответствии с политиками безопасности организации.

8. При необходимости администратор добавляет на Сервер iOS MDM provisioning-профили, а затем устанавливает provisioning-профили на мобильные устройства.

   Provisioning-профиль – это профиль, который используется для управления приложениями, распространяемыми не через App Store®. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

Информацию об управлении мобильными устройствами iOS MDM см. в *Руководстве администратора Kaspersky Security Center*.

В этом разделе

Установка Сервера iOS MDM

► *Чтобы установить Сервер iOS MDM на локальное устройство, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ «Лаборатории Касперского» для установки.

   В окне с выбором программ по ссылке **Установить Сервер iOS MDM** запустите мастер установки Сервера iOS MDM.

2. Выберите папку назначения.

   Папка назначения по умолчанию <Диск>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

3. В окне мастера **Параметры подключения к Серверу iOS MDM** в поле **Внешний порт подключения к службе iOS MDM** укажите внешний порт для подключения мобильных устройств к службе iOS MDM.

   Внешний порт 5223 используется мобильными устройствами для связи с APNs-сервером. Убедитесь, что в сетевом экране открыт порт 5223 для подключения к диапазону адресов 17.0.0.0/8.

   Для подключения устройства к Серверу iOS MDM по умолчанию используется порт 443. Если порт 443 уже используется другим сервисом или приложением, то его можно изменить, например, на порт 9443.

   Сервер iOS MDM использует внешний порт 2195 для отправки уведомлений на APNs-сервер.

   APNs-серверы работают в режиме сбалансированной нагрузки. Мобильные устройства не всегда подключаются к одним и тем же IP-адресам для получения уведомлений. Диапазон адресов 17.0.0.0/8 назначен компании Apple, поэтому рекомендуется указать весь этот диапазон как разрешенный в параметрах сетевого экрана.

4. Если вы хотите вручную настроить порты для взаимодействия между компонентами программы, установите флажок **Настроить локальные порты вручную**, а затем укажите значения следующих параметров:

   - **Порт подключения к Агенту администрирования**. Укажите в поле порт подключения службы iOS MDM к Агенту администрирования. По умолчанию используется порт 9799.

   - **Порт подключения к службе iOS MDM**. Укажите в поле локальный порт подключения Агента администрирования к службе iOS MDM. По умолчанию используется порт 9899.

   > Рекомендуется использовать значения по умолчанию.

5. В окне мастера **Внешний адрес Сервера мобильных устройств** в поле **Веб-адрес удаленного соединения с Сервером мобильных устройств** укажите адрес клиентского устройства, на котором будет установлен Сервер iOS MDM.

   Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Клиентское устройство должно быть доступно для подключения к нему iOS MDM-устройств.

   Вы можете указать адрес клиентского устройства в одном из следующих форматов:

   - FQDN-имя устройства (например, mdm.example.com);

   - NetBIOS-имя устройства;

   - IP-адрес устройства.

   > Не следует включать в строку с адресом URL-схему и номер порта: эти значения будут добавлены автоматически.

В результате работы мастера Сервер iOS MDM будет установлен на локальное устройство. Сервер iOS MDM отображается в папке **Управление мобильными устройствами** дерева консоли.

Установка Сервера iOS MDM в неинтерактивном режиме

Kaspersky Security Center позволяет устанавливать Сервер iOS MDM на локальное устройство в неинтерактивном режиме, то есть без интерактивного ввода параметров установки.

► *Чтобы установить Сервер iOS MDM на локальное устройство в неинтерактивном режиме,*

выполните команду

```
.\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1
<setup_parameters>"
```

где `setup_parameters` – перечень параметров и их значений, отделенных друг от друга пробелом (`PRO1=PROP1VAL PROP2=PROP2VAL`). Файл setup.exe расположен на дистрибутивном компакт-диске программы Kaspersky Security Center в папке Server.

Имена и возможные значения параметров, которые можно использовать при установке Сервера iOS MDM в неинтерактивном режиме, приведены в таблице ниже. Параметры можно указывать в любом порядке.

Таблица 9. Параметры установки Сервера iOS MDM в неинтерактивном режиме

Имя параметра	Описание параметра	Возможные значения
EULA	Согласие с условиями Лицензионного соглашения. Параметр является обязательным.	• 1 – согласны с условиями Лицензионного соглашения; • другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
DONT_USE_ANSWER_FILE	Использовать xml-файл с параметрами установки Сервера iOS MDM или нет. xml-файл идет в комплекте с инсталляционным пакетом или находится на Сервере администрирования.	• 1 – не использовать xml-файл с параметрами; • другое значение или не задано – использовать xml-файл с параметрами.

Имя параметра	Описание параметра	Возможные значения
	Дополнительно путь к файлу указывать не нужно. Параметр является обязательным.	
INSTALLDIR	Папка установки Сервера iOS MDM. Параметр не является обязательным.	Строковое значение, например, `INSTALLDIR=\"C:\install\".`
CONNECTORPORT	Локальный порт подключения службы iOS MDM к Агенту администрирования. По умолчанию используется порт 9799. Параметр не является обязательным.	Числовое значение.
LOCALSERVERPORT	Локальный порт подключения Агента администрирования к службе iOS MDM. По умолчанию используется порт 9899. Параметр не является обязательным.	Числовое значение.
EXTERNALSERVERPORT	Порт для подключения устройства к Серверу iOS MDM. По умолчанию используется порт 443. Параметр не является обязательным.	Числовое значение.

Имя параметра	Описание параметра	Возможные значения
EXTERNAL_SERVER_URL	Внешний адрес клиентского устройства, на котором будет установлен Сервер iOS MDM. Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Клиентское устройство должно быть доступно для подключения к нему iOS MDM. Адрес не должен включать URL-схему и номер порта: эти значения будут добавлены автоматически. Параметр не является обязательным.	• FQDN-имя устройства (например, mdm.example.com); • NetBIOS-имя устройства; • IP-адрес устройства.
WORKFOLDER	Рабочая папка Сервера iOS MDM. Если рабочая папка не указана, данные будут записаны в папку по умолчанию. Параметр не является обязательным.	Строковое значение, например, `WORKFOLDER=\"C:\work\".`
MTNCY	Использование Сервера iOS MDM несколькими виртуальными Серверами. Параметр не является обязательным.	• 1 – Сервер iOS MDM будет использоваться несколькими виртуальными Серверами администрирования; • другое значение или не задано – Сервер iOS MDM не будет использоваться несколькими виртуальными Серверами администрирования.

Пример:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443
EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Параметры установки Сервера iOS MDM подробно описаны в разделе «Установка Сервера iOS MDM» (на стр. 141).

Использование Сервера iOS MDM несколькими виртуальными Серверами

► *Чтобы включить использование Сервера iOS MDM несколькими виртуальными Серверами администрирования, выполните следующие действия:*

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер iOS MDM, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0
3. Для ключа ConnectorFlags (DWORD) установите значение 02102482.
4. Перейдите в раздел:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0
5. Для ключа ConnInstalled (DWORD) установите значение 00000001.
6. Перезапустите службу Сервера iOS MDM.

Задавать значения ключей необходимо в указанной последовательности.

Получение APNs-сертификата

После создания Certificate Signing Request (далее CSR-запрос) на первом шаге мастера получения APNs-сертификата приватная часть будущего сертификата (private key) сохраняется в оперативной памяти устройства. Поэтому все шаги мастера должны быть завершены в рамках одной сессии работы с программой.

► *Чтобы получить APNs-сертификат, выполните следующие действия:*

1. В дереве консоли в папке **Мобильные устройства** выберите Сервер iOS MDM.

   Папка **Мобильные устройства по** умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.

3. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.

4. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Запросить новый**.

   Запустится мастер получения APNs-сертификата, откроется окно **Запросить новый**.

5. Создайте Certificate Signing Request (далее CSR-запрос). Для этого выполните следующие действия:

   a. Нажмите на кнопку **Создать CSR**.

   b. В открывшемся окне **Создание CSR** укажите название запроса, название компании и департамента, город, область и страну.

   c. Нажмите на кнопку **Сохранить** и укажите имя файла, в котором будет сохранен CSR-запрос.

   Приватная часть (private key) будущего сертификата будет сохранена в памяти устройства.

6. Отправьте созданный файл с CSR-запросом на подпись в «Лабораторию Касперского» через ваш CompanyAccount.

Подписание CSR-запроса доступно только после загрузки на портал CompanyAccount ключа, разрешающего использование функциональности Управление мобильными устройствами.

После обработки вашего электронного запроса вы получите файл CSR-запроса, подписанный «Лабораторией Касперского».

7. Отправьте подписанный файл CSR-запроса на веб-сайт Apple Inc. https://identity.apple.com/pushcert, используя произвольный Apple ID.

   Не рекомендуется использовать персональный Apple ID. Создайте отдельный Apple ID, чтобы использовать его как корпоративный. Созданный Apple ID привяжите к почтовому ящику организации, а не отдельного сотрудника.

   После обработки CSR-запроса в Apple Inc. вы получите публичную часть APNs-сертификата. Сохраните полученный файл на диск.

8. Экспортируйте APNs-сертификат вместе с приватным ключом, созданным при формировании CSR-запроса, в файл формата PFX. Для этого выполните следующие действия:

   a. В окне **Запрос нового APNs-сертификата** нажмите на кнопку **Завершить CSR**.

   b. В открывшемся окне **Открыть** выберите файл с публичной частью сертификата, полученный после обработки CSR-запроса в Apple Inc., и нажмите на кнопку **Открыть**.

      Запустится экспорт сертификата.

   c. В открывшемся окне введите пароль для приватного ключа, нажмите на кнопку **ОК**.

      Заданный пароль будет использоваться для установки APNs-сертификата на Сервер iOS MDM.

   d. В открывшемся окне **Сохранение APNs-сертификата** укажите имя файла для сохранения APNs-сертификата, выберите папку, в которую он будет сохранен, и нажмите на кнопку **Сохранить**.

Приватная и публичная части сертификата будут объединены, APNs-сертификат будет сохранен в файл формата PFX. После этого можно установить полученный APNs-сертификат на Сервер iOS MDM (см. раздел «Установка сертификата APNs на Сервер iOS MDM» на стр. 149).

Подробнее о создании файла CSR-запроса и отправке его в Apple Inc. можно прочитать в Базе знаний на веб-сайте Службы технической поддержки «Лаборатории Касперского» http://support.kaspersky.ru/11077.

Установка сертификата APNs на Сервер iOS MDM

После получения APNs-сертификата необходимо установить APNs-сертификат на Сервер iOS MDM.

► *Чтобы установить APNs-сертификат на Сервер iOS MDM, выполните следующие действия:*

1. В дереве консоли в папке **Мобильные устройства** выберите Сервер iOS MDM.

   Папка **Мобильные устройства по** умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.

3. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.

В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Установить**.

1. Выберите файл формата PFX, содержащий APNs-сертификат.

2. Введите пароль приватного ключа, указанный при экспорте APNs-сертификата (см. раздел «Получение APNs-сертификата» на стр. 147).

В результате APNs-сертификат будет установлен на Сервер iOS MDM. Информация о сертификате будет отображаться в окне свойств Сервера iOS MDM в разделе **Сертификаты**.

Выписка и установка общего сертификата на мобильное устройство

► *Чтобы выписать общий сертификат пользователю, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите учетную запись пользователя.

2. В контекстном меню учетной записи пользователя выберите пункт **Установить сертификат**.

Будет запущен мастер установки сертификата. Следуйте его указаниям.

В результате работы мастера сертификат будет создан и добавлен в список сертификатов пользователя.

Выписанный сертификат пользователь загружает вместе с установочным пакетом, в котором содержится iOS MDM-профиль.

После подключения мобильного устройства к Серверу iOS MDM на устройстве пользователя будут применены параметры iOS MDM-профиля. Администратор сможет управлять подключенным устройством.

Мобильное устройство пользователя, подключенное к Серверу iOS MDM, отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Подробнее о выписке сертификатов и об управлении мобильными устройствами iOS MDM см. в *Руководстве администратора Kaspersky Security Center*.

Добавление iOS MDM-устройства в список управляемых устройств

► *Чтобы добавить iOS MDM-устройство пользователя в список управляемых устройств с помощью ссылки на App Store, выполните следующие действия:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. Выберите учетную запись пользователя, мобильное устройство которого вы хотите добавить в список управляемых устройств.

3. В контекстном меню учетной записи пользователя выберите пункт **Добавить устройство**.

   Запустится мастер добавления устройства. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на устройство;
   - указать файл общего сертификата.

4. В окне мастера **Тип устройства** выберите вариант **Ссылка на App Store**.

5. В окне мастера **Способ уведомления пользователей** настройте уведомление пользователя мобильного устройства о создании сертификата (с помощью SMS-сообщения или по электронной почте).

6. В окне мастера **Информация о сертификате** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате работы мастера на устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Safe Browser с App Store. Пользователь переходит по ссылке или сканирует QR-код. После этого операционная система устройства запрашивает у пользователя согласие на установку Kaspersky Safe Browser. Пользователь устанавливает Kaspersky Safe Browser на мобильное устройство. После установки Kaspersky Safe Browser пользователь повторно сканирует QR-код для получения параметров подключения к Серверу администрирования. В результате повторного сканирования QR-кода в Safe Browser пользователь получает параметры подключения к Серверу администрирования и общий сертификат. Мобильное устройство подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Если Kaspersky Safe Browser был ранее установлен на мобильное устройство, параметры подключения к Серверу администрирования нужно вводить самостоятельно. С помощью функции сканирования приложения Kaspersky Safe Browser пользователь сканирует QR-код и получает параметры подключения устройства к Серверу администрирования. Полученные параметры пользователь сохраняет на устройстве. Далее мобильное устройство автоматически подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли. Повторная загрузка и установка Kaspersky Safe Browser в этом случае не выполняется.

Если на iOS MDM-устройстве ранее был установлен iOS MDM-профиль, то после установки на устройстве Kaspersky Safe Browser и общего сертификата это устройство отображается в списке устройств в папке **Мобильные устройства** дважды (дублируется). Устройство дублируется в списке из-за наличия на нем двух общих (идентификационных) сертификатов.

Развертывание системы управления по KES-протоколу с помощью Self Service Portal

Kaspersky Security Center позволяет пользователям самостоятельно управлять своими мобильными устройствами, которые подключаются к Серверу администрирования по KES-протоколу, с помощью Self Service Portal.

Self Service Portal поддерживает мобильные устройства с операционными системами iOS и Android.

Развертывание системы управления по KES-протоколу с помощью Self Service Portal состоит из следующих этапов:

1. Подготовка к установке Self Service Portal:
   a. Администратор устанавливает на выбранное клиентское устройство Self Service Portal (см. раздел «Установка Self Service Portal» на стр. 156).
   b. Администратор сообщает адрес Self Service Portal пользователю.
2. Подключение мобильного устройства к Self Service Portal:
   a. Пользователь открывает главную страницу портала.

      Self Service Portal создает установочный пакет, после чего отображает на странице портала одноразовую ссылку для скачивания пакета и QR-код, в котором зашифрована ссылка. Установочный пакет необходим для установки на устройство агента управления, и применения корпоративных политик.
   b. Пользователь переходит на страницу загрузки установочного пакета с мобильного устройства, которое нужно добавить на Self Service Portal, загружает установочный пакет и устанавливает агент управления на мобильное устройство.
   c. После установки агента управления устройство подключается к Серверу администрирования.

В результате устройство будет добавлено в список управляемых устройств и к нему будут применены корпоративные политики. Ссылка на информацию о подключении к Серверу администрирования отправляется на электронную почту пользователя.

Информацию о добавлении устройства на Self Service Portal см. в *Руководстве администратора Kaspersky Security Center*.

Добавление KES-устройства в список управляемых устройств

► *Чтобы добавить KES-устройство пользователя в список управляемых устройств с помощью ссылки на Google Play™, выполните следующие действия:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. Выберите учетную запись пользователя, мобильное устройство которого вы хотите добавить в список управляемых устройств.

3. В контекстном меню учетной записи пользователя выберите пункт **Добавить устройство**.

   Запустится мастер добавления устройства. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на устройство;
   - указать файл общего сертификата.

4. В окне мастера **Тип устройства** выберите вариант **Ссылка на Google Play**.

5. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата (с помощью SMS-сообщения, по электронной почте или информация будет отображена после окончания работы мастера).

6. В окне мастера **Информация о сертификате** нажмите на кнопку **Готово для** завершения работы мастера установки сертификатов.

В результате работы мастера на устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Endpoint Security для Android с Google Play. Пользователь переходит в магазин приложений Google Play по ссылке или отсканировав QR-код. После этого операционная система устройства запрашивает у пользователя согласие на установку Kaspersky Endpoint Security для Android. После загрузки и установки Kaspersky Endpoint Security для Android мобильное устройство подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство, мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Если приложение Kaspersky Endpoint Security для Android уже установлено на устройство, пользователю нужно самостоятельно ввести параметры подключения к Серверу администрирования, получив их у администратора. После настройки параметров подключения мобильное устройство подключается к Серверу администрирования. Администратор выписывает общий сертификат для устройства и отправляет пользователю сообщение электронной почты или SMS с именем пользователя и паролем для загрузки сертификата. Пользователь загружает и устанавливает общий сертификат. После установки сертификата на мобильное устройство, мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли. Повторная загрузка и установка Kaspersky Endpoint Security для Android в этом случае не выполняются.

Установка Self Service Portal

В этом разделе описаны подготовка к установке Self Service Portal и шаги установки.

Клиентское устройство, на котором планируется развернуть Self Service Portal, должно соответствовать следующим требованиям:

- На устройстве должен быть установлен Сервер администрирования (см. раздел «Развертывание Сервера администрирования» на стр. 51).
- На устройстве должен быть установлен Сервер iOS MDM (см. раздел «Развертывание системы управления по протоколу iOS MDM» на стр. 138).

Для установки Self Service Portal необходимы права локального администратора на устройстве, где осуществляется установка.

► *Чтобы установить Self Service Portal на локальном устройстве, выполните следующие действия:*

1. В дереве консоли выберите папку Self Service Portal, вложенную в папку **Управление мобильными устройствами**.
2. В рабочей области папки нажмите на кнопку **Установить Self Service Portal**.
3. В окне **Актуальные версии программ** выберите и загрузите нужный дистрибутив по кнопке **Загрузить дистрибутив**.
4. Запустите загруженный файл.

   Запустится мастер распаковки дистрибутива. Следуйте шагам мастера.
5. Распакуйте дистрибутив в нужную вам папку.
6. В указанной вами папке запустите файл install.exe.

   Запустится мастер установки программы. Следуйте его указаниям.

Также вы можете запустить файл install.exe, расположенный на дистрибутивном компакт-диске программы Kaspersky Security Center 10 Web Console.

Процесс установки Self Service Portal с дистрибутива, полученного через интернет, совпадает с процессом установки с дистрибутивного компакт-диска.

Шаг 1. Просмотр Лицензионного соглашения

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, установите флажок **Я принимаю условия Лицензионного соглашения**. Установка программы на ваше устройство будет продолжена.

Если вы не согласны с условиями Лицензионного соглашения, то отмените установку программы, нажав на кнопку **Отмена**.

Удаленная установка Self Service Portal с помощью инсталляционного пакета или локальная установка в неинтерактивном режиме означает автоматическое согласие с условиями Лицензионного соглашения на устанавливаемую программу. Просмотреть Лицензионное соглашение можно в комплекте поставки программы в файле license.txt или на сайте технической поддержки «Лаборатории Касперского».

Шаг 2. Подключение к Kaspersky Security Center

Выберите способ подключения Self Service Portal к Kaspersky Security Center. Доступны следующие способы подключения:

- **Использовать сервер Apache, установленный на локальном устройстве**. Если выбран этот вариант, подключение Self Service Portal к Kaspersky Security Center будет выполняться через сервер Apache, установленный на локальном устройстве (выбрать установку сервера Apache можно на следующем шаге мастера).

- **Использовать сервер Apache, установленный на удаленном устройстве**. Вы можете выбрать этот вариант, если сервер Apache уже установлен на удаленном устройстве. В этом случае локально будет установлена только серверная часть Self Service Portal. Чтобы подключить Self Service Portal к Kaspersky Security Center, на удаленном устройстве необходимо установить клиентскую часть Self Service Portal. При выборе этого варианта мастер установки переходит к Шагу 7 (см. раздел «Шаг 6. Выбор портов» на стр. 160).

► *Чтобы установить клиентскую часть Self Service Portal на удаленное устройство на платформе Linux,*

в зависимости от типа операционной системы запустите на удаленном устройстве следующие файлы:

- Для 32-разрядных систем:
  - kscwebconsole-10.<номер_сборки>.i386.rpm;
  - kscwebconsole_10.<номер_сборки>_i386.deb.
- Для 64-разрядных систем:
  - kscwebconsole-10.<номер_сборки>.x86_64.rpm;
  - kscwebconsole_10.<номер_сборки>_x86_64.deb.

Запустите файл с расширением rpm, если на устройстве установлена rpm-based операционная система. Запустите файл с расширением deb, если на устройстве установлена deb-based операционная система.

Шаг 3. Выбор папки назначения

Укажите папку назначения для установки Self Service Portal. По умолчанию папкой назначения является папка <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center Self Service Portal. Если такой папки нет, она будет создана автоматически. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

Шаг 4. Выбор установки сервера Apache

Если на устройстве не установлен сервер Apache, на этом шаге мастер установки предложит вам установить Apache HTTP Server 2.4.25.

По умолчанию выбран вариант установки Apache HTTP Server 2.4.25. Если вы не хотите устанавливать сервер Apache с помощью мастера установки Kaspersky Security Center 10 Web Console, снимите флажок **Установить Apache HTTP Server 2.4.25.**

Во время установки сервера Apache может потребоваться перезагрузка устройства.

Шаг 5. Установка сервера Apache

На этом шаге мастера выполняется установка и настройка Apache HTTPS Server 2.4.25.

Перед началом установки укажите сертификат, который Self Service Portal будет использовать для связи с сервером Apache. Выберите один из следующих вариантов:

- **Сформировать новый**. Сформировать новый сертификат для работы по протоколу HTTPS. В этом случае будет создан самоподписанный сертификат для работы по протоколу HTTPS.
- **Выбрать существующий**. Использовать имеющийся сертификат для работы по протоколу HTTPS. Задайте сертификат одним из следующих способов:
  - **Выбрать файл сертификата**. Выберите имеющийся файл сертификата по кнопке **Обзор**.
  - **Выбрать файл закрытого ключа**. Задайте сертификат файлом его закрытого ключа по кнопке **Обзор**.

В случае использования самоподписанных или пользовательских недоверенных сертификатов, на некоторых устройствах возможно возникновение проблемы с доступом к Self Service Portal. Проблема решается установкой корневого сертификата в список доверенных на устройстве.

Если необходимо, вы можете настроить работу Self Service Portal не по протоколу HTTPS, а по протоколу HTTP. Подробную информацию о настройке работы Self Service Portal по протоколу HTTP смотрите в Базе знаний Службы технической поддержки «Лаборатории Касперского» http://support.kaspersky.ru/11452.

После выбора сертификата нажмите на кнопку **Далее**. В результате будет запущена установка Apache HTTPS Server 2.4.25. Следуйте указаниям мастера.

Шаг 6. Выбор портов

Настройте следующие параметры:

- Номер SSL-порта для защищенного подключения устройства к Серверу администрирования. По умолчанию используется порт 13291.
- Номер порта для подключения устройства к серверу Apache. По умолчанию используется порт 9000.
- Адрес устройства, на котором установлен Сервер администрирования. По умолчанию указан адрес localhost.

  Если устройство, на которое устанавливается Kaspersky Security Center 10 Web Console и Self Service Portal, находится в демилитаризованной зоне, установите флажок **Шлюз соединения**, а в поле **Адрес сервера** укажите адрес шлюза соединения.
- Номер порта для подключения устройства к Kaspersky Security Center 10 Web Console. По умолчанию используется порт 8080.
- Номер порта для подключения устройства к Self Service Portal. По умолчанию используется порт 8081.

После установки Kaspersky Security Center 10 Web Console и Self Service Portal вы можете изменить номера портов, заданные по умолчанию (см. раздел «Изменение номера порта для подключения устройства» на стр. 90).

Шаг 7. Выбор учетной записи

Укажите доменную учетную запись пользователя, от имени которой с помощью QR-кодов установочные пакеты будут загружаться на мобильные устройства пользователей. Учетную запись нужно указывать в формате <Имя домена>\<Имя учетной записи>.

По кнопке **Проверить** вы можете проверить подключение к Серверу администрирования.

Шаг 8. Запуск установки Self Service Portal

Нажмите на кнопку **Начать** для запуска установки Self Service Portal.

Процесс установки отображается в окне мастера.

Шаг 9. Завершение установки Self Service Portal

Если на устройстве до установки Self Service Portal был установлен сервер Apache версии 2.4.25 или выше, или автоматическая установка сервера Apache завершилась с ошибкой, на этом шаге мастер установки предложит открыть файл с инструкциями по настройке сервера Apache. Чтобы после завершения работы мастера просмотреть текстовый файл с инструкциями, установите флажок **Открыть файл readme.txt**.

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

Настройка SMS-рассылки в Kaspersky Security Center

Kaspersky Security Center может использоваться для отправки пользователям мобильных устройств SMS-уведомлений.

SMS-рассылка может использоваться в следующих случаях:

- Для получения администратором SMS-уведомлений о событиях в работе Сервера администрирования и программ, установленных на клиентских устройствах.
- Для установки программ на мобильные устройства пользователей. Пользователь мобильного устройства получает SMS, в котором содержится ссылка на скачивание программы, которую необходимо установить.
- Для оповещения сотрудников организации.

Развертывание SMS-рассылки выполняется в следующей последовательности:

1. Администратор устанавливает утилиту Kaspersky SMS Broadcasting на мобильное устройство Android.

   > Утилита Kaspersky SMS Broadcasting устанавливается только на мобильные устройства на платформе Android.

2. После установки утилиты Kaspersky SMS Broadcasting на мобильное устройство администратор синхронизирует мобильное устройство с Сервером администрирования.
3. Администратор назначает мобильное устройство, на котором установлена утилита Kaspersky SMS Broadcasting, отправителем SMS в Консоли администрирования.

В этом разделе

Получение и установка утилиты Kaspersky SMS Broadcasting

Утилита Kaspersky SMS Broadcasting входит в состав пакета установки Kaspersky Endpoint Security 10 для мобильных устройств. Вы можете загрузить пакет установки Kaspersky Endpoint Security 10 для мобильных устройств с сайта «Лаборатории Касперского».

► *Чтобы установить утилиту Kaspersky SMS Broadcasting, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Дополнительные действия** и из выпадающего списка выберите пункт **Управлять пакетами мобильных приложений**.

3. В окне **Управление пакетами мобильных приложений** выберите пакет мобильного приложения, содержащего утилиту Kaspersky SMS Broadcasting.

   Если пакет не создавался, нажмите на кнопку **Новый** и создайте пакет мобильного приложения для утилиты Kaspersky SMS Broadcasting.

4. В окне **Управление пакетами мобильных приложений** нажмите на кнопку **Опубликовать на веб-сервере**.

   Ссылка на скачивание пакета мобильного приложения с утилитой Kaspersky SMS Broadcasting будет опубликована на веб-сервере.

5. В окне **Управление пакетами мобильных приложений** нажмите на кнопку **Послать по почте**, чтобы отправить пользователю мобильного устройства ссылку на скачивание пакета мобильных приложений, содержащего утилиту Kaspersky SMS Broadcasting.

6. Скачайте с веб-сервера на мобильное устройство пакет мобильных приложений, содержащий утилиту Kaspersky SMS Broadcasting.

7. Выполните установку утилиты Kaspersky SMS Broadcasting штатными средствами мобильного устройства.

Вы также можете скачать утилиту Kaspersky SMS Broadcasting на мобильное устройство с сайта «Лаборатории Касперского» или подключить мобильное устройство к клиентскому устройству и скопировать уже скачанную утилиту Kaspersky SMS Broadcasting на мобильное устройство.

Синхронизация мобильного устройства с Сервером администрирования

► *Чтобы синхронизировать мобильное устройство с Сервером администрирования, выполните следующие действия:*

1. В дереве консоли Kaspersky Security Center в контекстном меню папки Сервер **администрирования** выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.

2. В окне свойств Сервера администрирования в разделе **Параметры** установите флажок **Открывать порт для мобильных устройств**.

3. В разделе **Параметры** в поле **Порт для мобильных устройств** укажите порт синхронизации мобильного устройства с Сервером администрирования. По умолчанию используется порт 13292.

4. Запустите утилиту Kaspersky SMS Broadcasting на мобильном устройстве.

5. В главном окне утилиты Kaspersky SMS Broadcasting нажмите на кнопку **Параметры синхронизации**.

6. В окне **Параметры синхронизации** в поле **Адрес сервера** укажите IP-адрес Сервера администрирования.

7. В поле **Порт** укажите порт подключения к Серверу администрирования. По умолчанию используется порт 13292.

8. Нажмите на кнопку **ОК**.

Когда мобильное устройство синхронизируется с Сервером администрирования, вы можете назначить это мобильное устройство отправителем SMS-сообщений.

Назначение мобильного устройства отправителем SMS-сообщений

► *Чтобы назначить мобильное устройство отправителем SMS-сообщений, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить список отправителей SMS**.

   Откроется окно свойств событий на разделе **Отправители SMS**.
4. В разделе **Отправители SMS** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор устройства**.
5. В окне **Выбор устройства** укажите мобильное устройство, которое будет использоваться в качестве отправителя SMS-сообщений.
6. Нажмите на кнопку **ОК**.

На устройстве, которое назначено отправителем SMS-сообщений, должна быть установлена утилита Kaspersky SMS Broadcasting.

Нагрузка на сеть

В этом разделе приводится информация об объеме сетевого трафика, которым обмениваются между собой клиентские устройства и Сервер администрирования в ходе выполнения ключевых административных сценариев.

Основная нагрузка на сеть связана с выполнением следующих административных сценариев:

- первоначальное развертывание антивирусной защиты;
- первоначальное обновление антивирусных баз;
- синхронизация клиентского устройства с Сервером администрирования;
- регулярное обновление антивирусных баз;
- обработка событий на клиентских устройствах Сервером администрирования.

В этом разделе

Первоначальное развертывание антивирусной защиты

В этом разделе приведен расход трафика при установке на клиентском устройстве Агента администрирования версии 10 и Kaspersky Endpoint Security 10 для Windows (см. таблицу ниже).

Агент администрирования устанавливается путем форсированной установки, когда требуемые для установки файлы копируются Сервером администрирования в папку общего доступа на клиентском устройстве. После установки Агент администрирования получает дистрибутив Kaspersky Endpoint Security 10 для Windows, используя соединение с Сервером администрирования.

Таблица 10. Расход трафика

Сценарий	Установка Агента администрирования для одного клиентского устройства	Установка Kaspersky Endpoint Security 10 для Windows для одного клиентского устройства (с обновленными базами)	Совместная установка Агента администрирования и Kaspersky Endpoint Security 10 для Windows
Трафик от клиентского устройства к Серверу администрирования, КБ	386,70	1 841,3	2 253,8
Трафик от Сервера администрирования к клиентскому устройству, КБ	14 801,13	269 994,5	284 768,7
Общий трафик (для одного клиентского устройства), КБ	15 187,83	271 835,8	287 022,5

После установки Агентов администрирования на клиентские устройства можно назначить одно из устройств в группе администрирования на роль агента обновлений. Он будет использоваться для распространения инсталляционных пакетов. В этом случае объем трафика, передаваемого при первоначальном развертывании антивирусной защиты, существенно отличается в зависимости от того, используется ли многоадресная IP-рассылка.

В случае использования многоадресной IP-рассылки инсталляционные пакеты будут разосланы всем включенным устройствам в группе администрирования один раз. Таким образом, общий трафик уменьшится примерно в N раз, где N – общее число включенных устройств в группе администрирования. Если многоадресная IP-рассылка не используется, общий трафик совпадает с трафиком в случае получения инсталляционных пакетов с Сервера администрирования, но источником инсталляционных пакетов является не Сервер администрирования, а агент обновлений.

Первоначальное обновление антивирусных баз

В этом разделе приведена информация о расходе трафика при первом запуске задачи обновления баз на клиентском устройстве (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии баз.

Таблица 11. Расход трафика

Сценарий	Первоначальное обновление антивирусных баз
Трафик от клиентского устройства к Серверу администрирования, КБ	1 357,1
Трафик от Сервера администрирования к клиентскому устройству, КБ	33 917,0
Общий трафик (для одного клиентского устройства), КБ	35 274,1

Синхронизация клиента с Сервером администрирования

Этот сценарий характеризует состояние системы администрирования в случае, когда происходит активная синхронизация данных между клиентским устройством и Сервером администрирования. Клиентские устройства подключаются к Серверу администрирования с периодом, заданным администратором. Сервер администрирования сравнивает состояние данных на клиентском устройстве с состоянием данных на Сервере, регистрирует данные о последнем подключении клиентского устройства в базе данных и проводит синхронизацию данных.

В разделе приведена информация о расходе трафика для основных административных сценариев при подключении клиента к Серверу администрирования с синхронизацией (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии баз.

Таблица 12. Расход трафика

Сценарий	Трафик от клиентских устройств к Серверу администрирования, КБ	Трафик от Сервера администрирования к клиентским устройствам, КБ	Общий трафик (для одного клиентского устройства), КБ
Первоначальная синхронизация до обновления баз на клиентском устройстве	368,6	463,7	832,3
Первоначальная синхронизация после обновления баз на клиентском устройстве	1 748,3	34 388,3	36 136,6
Синхронизация при отсутствии изменений на клиентском устройстве и на Сервере администрирования	8,7	6,6	15,3
Синхронизация при изменении одного параметра в политике группы	11,1	13,3	24,4
Синхронизация при изменении одного параметра в групповой задаче	10,0	12,5	22,5
Принудительная синхронизация при отсутствии изменений на клиентском устройстве	47,3	15,5	62,8

Объем общего трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Объем трафика при первоначальной синхронизации до и после обновления баз указан для следующих случаев:

- установка на клиентское устройство Агента администрирования и программы защиты;
- перенос клиентского устройства в группу администрирования;
- применение к клиентскому устройству политики и задач, созданных для группы по умолчанию.

В таблице указан объем трафика при изменении одного из параметров защиты, входящих в параметры политики Kaspersky Endpoint Security. Данные для других параметров политики могут отличаться от данных, представленных в таблице.

Добавочное обновление антивирусных баз

В этом разделе приведена информация о расходе трафика при инкрементальном обновлении антивирусных баз через 20 часов после предыдущего обновления (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии баз.

Таблица 13. Расход трафика

Сценарий	Инкрементальное обновление антивирусных баз
Трафик от клиентского устройства к Серверу администрирования, КБ	436,9
Трафик от Сервера администрирования к клиентскому устройству, КБ	9 979,2
Общий трафик (для одного клиентского устройства), КБ	10 416,1

Объем трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Обработка событий клиентов Сервером администрирования

В этом разделе приведен расход трафика при возникновении на клиентском устройстве события «Найден вирус», информация о котором передается на Сервер администрирования и регистрируется в базе данных (см. таблицу ниже).

Таблица 14. Расход трафика

Сценарий	Передача на Сервер администрирования данных при наступлении события «Найден вирус»	Передача на Сервер администрирования данных при наступлении девяти событий «Найден вирус»
Трафик от клиентского устройства к Серверу администрирования, КБ	27,2	100,4
Трафик от Сервера администрирования к клиентскому устройству, КБ	25,8	52,5
Общий трафик (для одного клиентского устройства), КБ	53,0	152,9

Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусной программы и в зависимости от того, какие именно события определены в политике как требующие регистрации в базе данных Сервера администрирования.

Расход трафика за сутки

В этом разделе приведена информация о расходе трафика за сутки работы системы администрирования в состоянии «покоя», когда не происходит изменений данных ни со стороны клиентских устройств, ни со стороны Сервера администрирования (см. таблицу ниже).

Данные, приведенные в таблице, характеризуют состояние сети после стандартной установки Kaspersky Security Center и завершения работы мастера первоначальной

настройки. Период синхронизации клиентского устройства с Сервером администрирования составлял 20 минут, загрузка обновлений в хранилище Сервера администрирования происходила каждый час.

Таблица 15. Расход трафика

Сценарий	Состояние «покоя» системы администрирования
Трафик от клиентского устройства к Серверу администрирования, КБ	2 162,2
Трафик от Сервера администрирования к клиентскому устройству, КБ	51 000,2
Общий трафик (для одного клиентского устройства), КБ	53 162,4

Скорость заполнения базы данных событиями Kaspersky Endpoint Security

В этом разделе приведены примеры скорости заполнения базы данных Сервера администрирования событиями, возникающими в работе управляемых программ.

Информация о событиях в работе управляемых программ передается с клиентского устройства и регистрируется в базе данных Сервера администрирования.

В базу данных поступает (Ne*Nh) событий в день (см. таблицу ниже). Здесь Nh – количество клиентских устройств, на которых установлены управляемые программы, Ne – количество событий в день, информацию о которых передает с клиентского устройства установленная на нем управляемая программа.

Таблица 16. Скорость заполнения базы данных событиями

Количество устройств, на которых установлены управляемые программы	**Количество событий, передаваемое в базу данных в день**
100	≤ 2 000
1000	≤ 20 000
10 000	≤ 200 000

В таблице приведены данные для штатной работы управляемых программ, когда от одного клиентского устройства поступает не более 20 событий в день.

Максимальное количество событий, хранящихся в базе данных, определяется в разделе **Хранение событий** окна свойств Сервера администрирования. По умолчанию в базе данных хранится не более 400 000 событий.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе (см. раздел «Источники информации о программе» на стр. 14), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (http://support.kaspersky.ru/support/contacts);
- отправить запрос в Службу технической поддержки «Лаборатории Касперского» с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru/support/contacts).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы «Лаборатории Касперского». Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами «Лаборатории Касперского» с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами «Лаборатории Касперского» и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в «Лабораторию Касперского», а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (http://support.kaspersky.ru/faq/companyaccount_help).

Глоссарий

E

EAS-устройство

Мобильное устройство, которое подключается к Серверу администрирования по протоколу Exchange ActiveSync.

I

iOS MDM-профиль

Набор параметров подключения мобильных устройств iOS к Серверу администрирования. iOS MDM-профиль устанавливается пользователем на мобильное устройство, после чего это мобильное устройство подключается к Серверу администрирования.

iOS MDM-устройство

Мобильное устройство на платформе iOS, находящееся под управлением Сервера iOS MDM (см. раздел «Сервер iOS MDM» на стр. 183).

K

Kaspersky Security Center System Health Validator (SHV)

Компонент программы Kaspersky Security Center, предназначенный для проверки работоспособности операционной системы при совместной работе программы Kaspersky Security Center с Microsoft NAP.

P

Provisioning-профиль

Набор параметров для работы приложений на мобильных устройствах iOS. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

A

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами «Лаборатории Касперского», установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех программ компании для Windows. Для программ «Лаборатории Касперского» для Novell, Unix и Mac существуют отдельные версии Агента администрирования.

Агент обновлений

Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки программ, получения информации об устройствах в составе группы администрирования и / или широковещательного домена. Агенты обновлений предназначены для уменьшения нагрузки на Сервер администрирования при распространении обновлений и для оптимизации трафика в сети. Агенты обновлений могут быть назначены автоматически Сервером администрирования или вручную администратором.

Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных «Лаборатории Касперского» на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами «Лаборатории Касперского» и обновляются каждый час.

Веб-сервер Kaspersky Security Center

Компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

Восстановление данных Сервера администрирования

Восстановление данных Сервера администрирования при помощи утилиты резервного копирования на основании информации, сохраненной в резервном хранилище. Утилита позволяет восстанавливать:

- информационную базу Сервера администрирования (политики, задачи, параметры программы, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ «Лаборатории Касперского». Устройства группируются для удобства управления ими как единым целым. В состав группы

могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских устройствах, входящих в состав этой группы администрирования.

Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

Доступное обновление

Пакет обновлений модулей программы «Лаборатории Касперского», в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

Задача

Функции, выполняемые программой «Лаборатории Касперского», реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Задача для набора устройств

Задача, определенная для набора клиентских устройств из произвольных групп администрирования и выполняемая на них.

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы «Лаборатории Касперского» при помощи системы удаленного управления Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию.

Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы.

Клиент Сервера администрирования (Клиентское устройство)

Устройство, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые программы «Лаборатории Касперского».

Консоль администрирования

Компонент программы Kaspersky Security Center, предоставляющий пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

Конфигурационный профиль

Политика, содержащая набор параметров и ограничений для мобильного устройства iOS MDM.

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском устройстве.

Непосредственное управление программой

Управление программой через локальный интерфейс.

Несовместимая программа

Антивирусная программа стороннего производителя или программа «Лаборатории Касперского», не поддерживающая управление через Kaspersky Security Center.

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

Оператор Kaspersky Security Center

Пользователь, который ведет наблюдение за состоянием и работой системы защиты, управляемой при помощи Kaspersky Security Center.

Параметры задачи

Параметры работы программы, специфичные для каждого типа задач.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

Плагин управления программой

Специализированный компонент, предоставляющий интерфейс для управления работой программы через Консоль администрирования. Для каждой программы существует свой плагин управления. Он входит в состав всех программ «Лаборатории Касперского», управление которыми может осуществляться при помощи Kaspersky Security Center.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на компьютерах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Порог вирусной активности

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в

периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Профиль

Набор параметров поведения мобильных устройств Exchange ActiveSync при подключении к серверу Microsoft Exchange.

Рабочее место администратора

Устройство, на котором установлен компонент, предоставляющий интерфейс управления программой. Для Антивирусных продуктов это Консоль Антивируса, для программы Kaspersky Security Center – Консоль администрирования.

С рабочего места администратора выполняются настройка серверной части программы и управление ею, а для Kaspersky Security Center – построение системы централизованной антивирусной защиты сети организации, сформированной на базе программ «Лаборатории Касперского», и управление ею.

Резервное копирование данных Сервера администрирования

Копирование данных Сервера администрирования для резервного хранения и последующего восстановления, осуществляемое при помощи утилиты резервного копирования. Утилита позволяет сохранять:

- информационную базу Сервера администрирования (политики, задачи, параметры программы, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Сервер iOS MDM

Компонент Kaspersky Security Center, который устанавливается на клиентское устройство и позволяет подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью сервиса Apple Push Notifications (APNs).

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах «Лаборатории Касперского» и управления ими.

Сервер мобильных устройств

Компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования.

Сервер мобильных устройств Exchange ActiveSync

Компонент Kaspersky Security Center, который позволяет подключать мобильные устройства Exchange ActiveSync к Серверу администрирования. Устанавливается на клиентском устройстве.

Серверы обновлений «Лаборатории Касперского»

HTTP-серверы «Лаборатории Касперского», с которых программы «Лаборатории Касперского» получают обновления баз и модулей программы.

Сертификат Сервера администрирования

Сертификат, на основании которого осуществляется аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с клиентскими устройствами. Сертификат Сервера администрирования создается при установке Сервера администрирования и хранится на Сервере администрирования в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности устройства.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

Удаленная установка

Установка программ «Лаборатории Касперского» при помощи инструментов, предоставляемых программой Kaspersky Security Center.

Уровень важности события

Характеристика события, зафиксированного в работе программы «Лаборатории Касперского». Существуют четыре уровня важности:

- Критическое событие.
- Отказ функционирования.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Установка с помощью сценария входа

Метод удаленной установки программ «Лаборатории Касперского», который позволяет закрепить запуск задачи удаленной установки за конкретной учетной записью пользователя (нескольких пользователей). При регистрации пользователя в домене предпринимается попытка провести установку программы на клиентском устройстве, с которого пользователь зарегистрировался. Данный метод рекомендуется для установки программ

компании на устройства, работающие под управлением операционных систем Microsoft Windows 98 / Me.

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать программу «Лаборатории Касперского» по пробной или коммерческой лицензии. Вы можете использовать программу только при наличии файла ключа.

Форсированная установка

Метод удаленной установки программ «Лаборатории Касперского», который позволяет провести удаленную установку программного обеспечения на конкретные клиентские устройства. Для успешного выполнения задачи методом форсированной установки учетная запись для запуска задачи должна обладать правами на удаленный запуск программ на клиентских устройствах. Данный метод рекомендуется для установки программ на устройства, работающие под управлением операционных систем Microsoft Windows NT / 2000 / 2003 / XP, в которых поддерживается такая возможность, либо на устройства под управлением Microsoft Windows 98 / Me, на которых установлен Агент администрирования.

Хранилище резервных копий

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

Централизованное управление программой

Удаленное управление программой при помощи сервисов администрирования, предоставляемых Kaspersky Security Center.

АО «Лаборатория Касперского»

«Лаборатория Касперского» – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году «Лаборатория Касперского» вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). В России, по данным IDC, «Лаборатория Касперского» – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей («IDC Endpoint Tracker 2014»).

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с 34 офисами в 31 стране мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты «Лаборатории Касперского» сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами «Лаборатории Касперского».

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно «Лабораторией Касперского». Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, «Лаборатория Касперского» стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Вирусная лаборатория:	http://newvirus.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com

Дополнительная защита с использованием Kaspersky Security Network

«Лаборатория Касперского» предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков «Лаборатории Касперского» обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте «Лаборатории Касперского».

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory, ActiveSync, Edge, Internet Explorer, Hyper-V, Microsoft, MultiPoint, SharePoint, SQL Server, Windows, Windows Server, Windows Phone, Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Android, Chrome, Google Play – товарные знаки Google, Inc.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Apple, App Store, Leopard, Mac, Mac OS, macOS, Safari, Snow Leopard, OS X, Tiger – товарные знаки Apple Inc., зарегистрированные в США и других странах.

Cisco – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и / или ее аффилированных компаний.

Citrix, XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Intel, Core, Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS, Fedora, Red Hat Enterprise Linux – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Firefox – товарный знак Mozilla Foundation.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Oracle и Java – зарегистрированные товарные знаки Oracle Corporation и / или ее аффилированных компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Novell, Netware – товарные знаки Novell Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Ubuntu – зарегистрированный товарный знак Canonical Ltd.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

VMware – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

Товарный знак BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Предметный указатель

A

C

E

K

P

R

S

А

Б

В

Г

Д

З

И

К

М

Н

О

П

Р

С

У

Ф

Х