KASPERSKY lab

Kaspersky Security Center 10

Лучшие практики для поставщиков услуг

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.

Дата редакции документа: 07.12.2016

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

Содержание

Об этом документе

Руководство администратора 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.

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

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

В этом разделе

В этом документе

Документ «Лучшие практики» Kaspersky Security Center содержит рекомендации по развертыванию, настройке и использованию программы, а также способы решения типичных проблем, возникающих при работе программы.

Планирование развертывания Kaspersky Security Center (см. стр. 10)

Этот раздел содержит информацию о выборе СУБД для Сервера администрирования, о предоставлении доступа к Серверу администрирования из интернета, о типовых конфигурациях Kaspersky Security Center. В разделе представлена информация о роли агентов обновлений и роли иерархии Серверов администрирования. Также представлена информация о виртуальных Серверах администрирования, об установке образов операционных систем и об управлении мобильными устройствами.

Развертывание и первоначальная настройка (см. стр. 18)

В этом разделе представлена информация о развертывании Сервера администрирования, о развертывании Агента администрирования и антивируса и о первоначальной настройке Kaspersky Security Center. Также раздел содержит информацию о резервном копировании и восстановлении параметров Сервера администрирования, о поддержке автономных пользователей.

Повседневная работа (см. стр. 93)

Этот раздел содержит информацию о повседневном использовании программы. В разделе представлена информация о работе с удаленным доступом к устройствам.

Обращение в Службу технической поддержки (см. стр. 111)

АО «Лаборатория Касперского» (см. стр. 114)

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

Уведомления о товарных знаках (см. стр. 116)

В этом разделе приведены уведомления о зарегистрированных товарных знаках.

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 текста	Описание условного обозначения
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.
► *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.

Планирование развертывания Kaspersky Security Center

Планируя размещение компонентов Kaspersky Security Center в сети предприятия, следует принимать во внимание следующие факторы:

- общее количество устройств;
- количество MSP-клиентов.

Один Сервер администрирования может обслуживать не более чем 50 000 устройств. Если общее количество устройств в сети предприятия превышает 50 000, следует разместить на стороне MSP несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

На одном Сервере администрирования может быть создано до 200 виртуальных серверов, следовательно, на каждые 200 MSP-клиентов необходим отдельный Сервер администрирования.

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

- для инспекции SSL трафика посредством SSL termination proxy или для использования Reverse Proxy;
- для задания желательных значений полей сертификата;
- для обеспечения желаемой криптографической стойкости сертификата.

См. раздел «Задание сертификата Сервера администрирования» (на стр. 21).

В этом разделе

О выборе СУБД для Сервера администрирования

При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством устройств, которые обслуживает Сервер администрирования. Поставляемая вместе с Kaspersky Security Center СУБД Microsoft® SQL Server® 2008 R2 Express Edition может использовать только один процессор и не более одного гигабайта памяти. Размер базы данных ограничен десятью гигабайтами. СУБД не может использоваться, если Сервер администрирования обслуживает более 10 000 устройств. Если Сервер администрирования обслуживает больше 10 000 устройств, следует использовать версии SQL Server с меньшими ограничениями: SQL Server Workgroup Edition, SQL Server® Web Edition, SQL Server Standard Edition, или SQL Server Enterprise Edition.

Такое же ограничение действует при работе в сети более 50 устройств и использовании компонента Контроль запуска программ программы Kaspersky Endpoint Security для Windows.

Если Сервер администрирования обслуживает не более 10 000 устройств или если не используется компонент Контроль запуска программ, в качестве СУБД может быть также использован MySQL 5.0.

См. также

Аппаратные требования для СУБД и Сервера администрирования 99

Выбор СУБД 20

Предоставление доступа к Серверу администрирования из интернета

Для того чтобы устройства, размещенные в сети клиента, могли обращаться к Серверу администрирования через интернет, необходимо сделать доступным следующие порты Сервера администрирования:

- 13000 TCP – порт TLS Сервера администрирования, к данному порту подключается Агенты администрирования, размещенные в сети клиента;
- 8061 TCP – порт HTTPS, используется для публикации автономных пакетов средствами Консоли администрирования;
- 8060 TCP – порт HTTP, используется для публикации автономных пакетов средствами Консоли администрирования;
- 13292 TCP – данный TLS порт нужен, только если требуется управлять мобильными устройствами.

В случае если необходимо предоставить клиентам базовые возможнсти по администрированию своей сети посредством Web Console, то также необходимо открыть порты Web Console:

- 8081 TCP – порт HTTPS;
- 8080 TCP – порт HTTP.

Типовая конфигурация Kaspersky Security Center

На стороне MSP размещен один или несколько Серверов администрирования. Количество Серверов может быть выбрано как исходя из наличия доступного аппаратного обеспечения (см. раздел «Аппаратные требования для СУБД и Сервера администрирования» на стр. 99), так и в зависимости от количества обслуживаемых MSP-клиентов или же общего количества управляемых устройств.

Один Сервер администрирования может обслуживать до 50 000 устройств. Нужно учесть возможность увеличения количества управляемых устройств в ближайшем будущем: может оказаться желательным подключение несколько меньшего количества устройств к одному Серверу администрирования.

На одном Сервере администрирования может быть создано до 200 виртуальных серверов, следовательно, на каждые 200 MSP-клиентов необходим отдельный Сервер администрирования.

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

На каждом виртуальном сервере, соответствующем MSP-клиенту, следует назначить по одному или по несколько агентов обновлений. Так как связь между MSP-клиентами и Сервером администрирования осуществляется через интернет, целесообразно создать для агентов обновлений задачу ретрансляции обновлений, так, чтобы агенты обновлений загружали обновления не с Сервера администрирования, а непосредственно с серверов «Лаборатории Касперского».

Если в сети MSP-клиента часть устройств не имеет прямого доступа в интернет, то агенты обновлений следует переключить в режим шлюза (Connection Gateway). В таком случае Агенты администрирования на устройствах в сети MSP-клиента будут подключаться (с целью синхронизации) к Серверу администрирования не напрямую, а через шлюз.

Поскольку Сервер администрирования не может выполнять опрос сети MSP-клиента, целесообразно возложить выполнение этой функции на один из агентов обновлений.

Сервер администрирования не сможет посылать уведомления на порт 15000 UDP управляемым устройствам, размещенным за NAT в сети MSP-клиента. Для решения этой проблемы целесообразно включить в свойствах устройств, являющихся агентами обновлений и работающих в режиме шлюза (Connection Gateway), режим постоянного соединения с Сервером администрирования (флажок **Не разрывать соединение с Сервером администрирования**). Режим постоянного соединения доступен, если общее количество агентов обновлений не превышает 300.

Об агентах обновлений

Агент администрирования может быть использован в качестве агента обновлений. В этом режиме Агент администрирования может выполнять следующие функции:

- Раздавать обновления, причем обновления могут быть получены как с Сервера администрирования, так и с серверов «Лаборатории Касперского». В последнем случае для устройства, являющегося агентом обновлений, должна быть создана задача ретрансляции.
- Устанавливать программное обеспечение на другие устройства, в том числе и выполнять первоначальное развертывание Агентов администрирования на устройствах.
- Сканировать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Агент обновлений может выполнять те же виды сканирования сети, что и Сервер администрирования.

Размещение агентов обновлений в сети предприятия преследует следующие цели.

- Уменьшить нагрузку на Сервер администрирования в случае, если источником обновлений служит Сервер администрирования.
- Оптимизировать интернет-трафик, так как в этом случае каждому устройству в сети MSP-клиента не придется обращаться за обновлениями к серверам «Лаборатории Касперского» или к Серверу администрирования.

- Предоставить Серверу администрирования доступ к устройствам за NAT (по отношению к Серверу администрирования) сети MSP-клиента позволяет Серверу администрирования выполнять следующие действия:
  - отправлять устройствам уведомления по UDP;
  - сканировать сеть;
  - выполнять первоначальное развертывание.

Агент обновлений назначается на группу администрирования. В этом случае областью действия агента обновлений будут устройства, находящиеся в такой группе администрирования и всех ее подгруппах. При этом устройство, являющееся агентом обновлений, не обязано находиться в группе администрирования, на которую оно назначено.

Агент обновлений может быть назначен шлюзом соединений. В этом случае находящиеся в его области действия устройства будут подключаться к Серверу администрирования не напрямую, а через шлюз. Данный режим полезен в сценариях, когда между устройствами с Агентом администрирования и Сервером администрирования невозможно прямое соединение.

См. также

Построение структуры групп администрирования и назначение агентов обновлений 30

Роль иерархии Серверов администрирования

У MSP может быть более одного Сервера администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Взаимодействие «главный – подчиненный» между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики и задачи, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов;
- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.

Виртуальные Серверы администрирования

В рамках физического Сервера администрирования можно создать несколько виртуальных Серверов администрирования, во многом подобных подчиненным Серверам. По сравнению с моделью разделения доступа, основанной на списках контроля доступа (ACL), модель виртуальных Серверов более функциональна и предоставляет большую степень изоляции. Помимо собственной структуры групп администрирования для управляемых устройств с политиками и задачами, каждый виртуальный Сервер администрирования имеет также собственную группу нераспределенных устройств, собственные наборы отчетов, выборок устройств и событий, инсталляционных пакетов, правил перемещения устройств и так далее. Для достижения максимальной изоляции MSP-клиентов друг от друга рекомендуется использовать именно функциональность виртуальных Серверов администрирования. Кроме того, создание виртуального Сервера для каждого MSP-клиента позволяет предоставить клиентам базовые возможности по администрированию своей сети посредством Kaspersky Security Center Web Console.

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

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

Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android

Управление мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android™ (далее KES-устройства) осуществляется с помощью Сервера администрирования. В программе Kaspersky Security Center 10 Service Pack 1 поддерживаются следующие возможности по управлению KES-устройствами:

- работа с мобильными устройствами как с клиентскими устройствами:
  - членство в группах администрирования;
  - статусы, события, отчеты и прочее;
  - изменение локальных параметров и назначение политик для приложения Kaspersky Endpoint Security для Android;
- централизованная отправка команд;
- удаленная установка пакетов мобильных приложений.

Обслуживание KES-устройств осуществляется Сервером администрирования по протоколу TLS, порт TCP 13292.

См. также

Предоставление доступа к Серверу администрирования из интернета 12

Задание сертификата Сервера администрирования 21

Развертывание и первоначальная настройка

Kaspersky Security Center представляет собой распределенное приложение. В состав Kaspersky Security Center входят следующие программы:

- Сервер администрирования – центральный компонент, ответственный за управление устройствами предприятия и хранение данных в СУБД.
- Консоль администрирования – основной инструмент администратора. Консоль администрирования поставляется вместе с Сервером администрирования, но может быть также установлена отдельно на один или несколько устройств администратора.
- Kaspersky Security Center Web Console — веб-интерфейс к Серверу администрирования для выполнения простейших операций. Необходимо инсталлировать данный компонент вместе с Сервером администрирования, если требуется предоставить MSP-клиентам базовые возможности по администрированию своей сети.
- Агент администрирования – служит для управления установленной на устройстве программой защиты, а также для получения информации об устройстве. Агенты администрирования устанавливаются на устройства предприятия.

Развертывание Kaspersky Security Center в сети предприятия осуществляется следующим образом:

- установка Сервера администрирования;
- установка Kaspersky Security Center Web Console на устройстве с Сервером администрирования;
- установка Консоли администрирования на устройстве администратора;
- установка Агента администрирования и программы защиты на устройства организации.

В этом разделе

Установка Сервера администрирования

В этом разделе содержатся рекомендации, касающиеся установки Сервера администрирования. В разделе также содержатся сценарии использования папки общего доступа на устройстве с Сервером администрирования для развертывания Агента администрирования на клиентских устройствах.

В этом разделе

Создание учетных записей для служб Сервера администрирования

По умолчанию инсталлятор самостоятельно создает непривилегированные учетные записи для служб Сервера администрирования. Такое поведение наилучшим образом подходит для установки Сервера администрирования на обычное устройство.

Однако при установке Сервера администрирования на контроллер домена или на отказоустойчивый кластер следует поступить иначе:

1. Создать в Active Directory® глобальные доменные группы с именами KLAdmins и KLOperators;
2. Создать непривилегированные доменные учетные записи для служб Сервера администрирования и сделать их членами глобальной доменной группы безопасности KLAdmins;
3. Задать в инсталляторе Сервера администрирования созданные доменные учетные записи.

Выбор СУБД

В процессе инсталляции Сервера администрирования необходимо выбрать СУБД, которую будет использовать Сервер администрирования. Можно либо установить SQL Server Express Edition, входящий в состав поставки, либо выбрать уже существующую СУБД. В таблице ниже перечислены допустимые варианты СУБД и ограничения их использования.

Таблица 2. Ограничения СУБД

СУБД	Ограничения
SQL Server Express Edition, входящий в состав поставки Kaspersky Security Center	Не рекомендуется, если планируется обслуживание одним Сервером администрирования более 10 тысяч устройств или использование компонента Контроль запуска программ.
Локальный SQL Server Edition, отличный от Express	Нет ограничений.
Удаленный SQL Server Edition, отличный от Express	Допустимо только в случае, если оба устройства находятся в одном домене Windows®. Если домены разные, то между ними должно быть установлено двустороннее отношение доверия.
Локальный или удаленный MySQL 5.0	Сервер администрирования может обслуживать не более 10 000 устройств, если не используется компонент Контроль запуска программ.

Недопустимо совместное использование СУБД Server Express Edition Сервером администрирования и каким-либо другим приложением.

См. также

О выборе СУБД для Сервера администрирования..... 11

Указание адреса Сервера администрирования

При установке Сервера администрирования необходимо задать внешний адрес Сервера администрирования. Этот адрес по умолчанию используется при создании инсталляционных пакетов Агента администрирования. В дальнейшем адрес Сервера администрирования можно будет изменить средствами Консоли администрирования, однако при этом он не изменится автоматически в уже созданных инсталляционных пакетах Агента администрирования.

Задание сертификата Сервера администрирования

В случае необходимости можно задать Серверу администрирования специальный сертификат при помощи утилиты командной строки klsetsrvcert.

При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой «Ошибка аутентификации Сервера администрирования».

Следует учитывать, что сертификат Сервера администрирования часто помещают в пакеты Агента администрирования при их создании. В этом случае замена сертификата Сервера при помощи утилиты klsetsrvcert не приведет к замене сертификата Сервера администрирования в уже существующих пакетах Агента администрирования.

Целесообразно заменять сертификат сразу после инсталляции Сервера администрирования, до завершения мастера первоначальной настройки.

Подробную информацию об условиях, при которых необходима замена сертификата, смотрите в разделе Планирование развертывания с учетом организационной структуры предприятия и топологии сетей (см. раздел «Планирование развертывания Kaspersky Security Center» на стр. 10).

Для замены сертификата следует создать новый сертификат (например, средствами инфраструктуры открытых ключей предприятия) в формате PKCS#12, и передать его на вход утилиты klsetsrvcert (значения параметров утилиты см. в таблице ниже). Задаваемый посредством утилиты сертификат должен содержать всю цепочку доверия.

Синтаксис утилиты:

klsetsrvcert [-l LOGFILE] -t TYPE [-p PASSWORD] -i FILE

Таблица 3. Значения параметров утилиты klsetsrvcert

Параметр	Значение
-t TYPE	Тип сертификата, который следует заменить. Возможные значения параметра TYPE: • C – заменить сертификат для портов 13000 и 13291; • CR – заменить резервный сертификат для портов 13000 и 13291; • M – заменить сертификат для мобильных устройств порта 13292.
-i FILE	Контейнер с сертификатом в формате PKCS#12 (файл с расширением p12 или pfx).
-p PASSWORD	Пароль, при помощи которого защищен p12-контейнер с сертификатом.
-l LOGFILE	Файл вывода результатов. По умолчанию вывод осуществляется в стандартный поток вывода.

Первоначальная настройка

После завершения инсталляции Сервера администрирования запускается Консоль администрирования, которая предлагает выполнить первоначальную настройку с помощью мастера. Во время работы мастера первоначальной настройки в корневой группе администрирования создаются следующие политики и задачи:

- политика Kaspersky Endpoint Security;
- групповая задача обновления Kaspersky Endpoint Security;
- групповая задача проверки устройства Kaspersky Endpoint Security;
- политика Агента администрирования;
- задача поиска уязвимостей (задача Агента администрирования);
- задача установки обновлений и закрытия уязвимостей (задача Агента администрирования).

Политики и задачи создаются с параметрами по умолчанию, которые могут оказаться неоптимальными или даже непригодными для данной организации. Поэтому следует просмотреть свойства созданных объектов и, в случае необходимости, внести изменения вручную.

В этом разделе содержится информация о первоначальной настройке политик, задач и других параметров Сервера администрирования.

В этом разделе

Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security, которую создает мастер первоначальной настройки Kaspersky Security Center. Настройка выполняется в окне свойств политики.

При изменении параметра следует помнить, что для того, чтобы значение параметра использовалось на рабочей станции, следует нажать на кнопку с «замком» над параметром.

В этом разделе

Настройка политики в разделе Антивирусная защита

Ниже описаны действия по дополнительной настройке, которую рекомендуется выполнить в окне свойств политики Kaspersky Endpoint Security в разделе **Антивирусная защита**.

Раздел Антивирусная защита, подраздел Сетевой экран

Следует проверить список сетей в свойствах политики. В списке могут отображаться не все сети.

► *Чтобы проверить список сетей, выполните следующие действия:*

1. В свойствах политики в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.
2. В блоке **Доступные сети** нажмите на кнопку **Настройка**.

   Откроется окно **Сетевой экран**. Список сетей отображается в этом окне на закладке **Сети**.

Раздел Антивирусная защита, подраздел Файловый Антивирус

Включенная проверка сетевых дисков может создавать значительную нагрузку на сетевые диски. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

► *Чтобы выключить проверку сетевых дисков, выполните следующие действия:*

1. В свойствах политики в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
3. В открывшемся окне **Файловый Антивирус** на закладке **Общие** снимите флажок **Все сетевые диски**.

Настройка политики в разделе Дополнительные параметры

Ниже описаны действия по дополнительной настройке, которые рекомендуется выполнить в окне свойств политики Kaspersky Endpoint Security в разделе **Дополнительные параметры**.

Раздел Дополнительные параметры, подраздел Отчеты и хранилища

В блоке **Информировать Сервер администрирования** следует обратить внимание на следующие параметры:

- Флажок **О найденных уязвимостях** – этот параметр нужен главным образом для обеспечения обратной совместимости с Kaspersky Security Center 9. Обнаружение уязвимостей встроено в Kaspersky Security Center начиная с версии 10. Поэтому, если используется Сервер администрирования и Агенты администрирования версии 10 и выше, этот флажок целесообразно снять.
- Флажок **О запускаемых программах** – если флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех модулей приложений на устройствах в сети предприятия. Указанная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятки

гигабайт). Поэтому в политике верхнего уровня флажок **О запускаемых программах** следует снять, если он оказался установлен.

Раздел Дополнительные параметры, подраздел Интерфейс

Если защита в сети предприятия должна управляться полностью централизованно через Консоль администрирования, то следует выключить отображение пользовательского интерфейса Kaspersky Endpoint Security на рабочих станциях (снять флажок **Отображать интерфейс программы** в разделе **Взаимодействие с пользователем**), а также включить защиту паролем (установить флажок **Включить защиту паролем** в разделе **Защита паролем**).

Раздел Дополнительные параметры, подраздел Параметры KSN

Целесообразно выключить использование прокси-сервера KSN (установить флажок **Использовать прокси-сервер KSN**).

Настройка политики в разделе События

В разделе **События** следует отключить сохранение на Сервере администрирования всех событий, за исключением перечисленных ниже:

- На закладке **Информационное сообщение**:
  - Объект вылечен.
  - Объект удален.
  - Запуск программы запрещен в тестовом режиме.
  - Объект помещен на карантин.
  - Объект восстановлен из карантина.
  - Создана резервная копия объекта.
- На закладке **Предупреждение**:
  - Самозащита программы выключена.
  - Компоненты защиты выключены.
  - Некорректный резервный код активации.

- Пользователь отказался от политики шифрования.
- Жалоба на запрет запуска программы.
- Жалоба на запрет доступа к устройству.
- Жалоба на запрет доступа к веб-контенту;
- Обнаружена программа, которая может быть использована злоумышленником.

- На закладке **Отказ функционирования**:
  - Ошибка в параметрах задачи. Параметры задачи не применены.
- На закладке **Критическое событие**:
  - Автозапуск программы выключен.
  - Доступ запрещен.
  - Запрещено.
  - Запуск программы запрещен.
  - Лечение невозможно.
  - Нарушено Лицензионное соглашение.
  - Не удалось загрузить модуль шифрования.
  - Невозможен запуск двух задач одновременно.
  - Обнаружен возможно зараженный объект.
  - Обнаружен вредоносный объект.
  - Обнаружена активная угроза. Требуется запуск процедуры лечения.
  - Обнаружена ранее открытая фишинговая ссылка.
  - Обнаружена ранее открытая вредоносная ссылка.
  - Обнаружена сетевая атака.

- Обновлены не все компоненты.
- Операция с устройством запрещена.
- Ошибка активации.
- Ошибка активации портативного режима.
- Ошибка взаимодействия с Kaspersky Security Center.
- Ошибка деактивации портативного режима.
- Ошибка изменения состава программы.
- Ошибка применения шифрования / расшифровки файлов.
- Политика не может быть применена.
- Процесс завершен.
- Сетевая активность запрещена.
- Сетевая ошибка обновления.

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Информация в этом подразделе применима для Kaspersky Security Center 10 MR1 и более поздних версий.

В случае, если источником обновлений является Сервер администрирования, то для групповых задач обновления Kaspersky Endpoint Security версии 10 и выше оптимальным и рекомендуемым является расписание **При загрузке обновлений в хранилище** при установленном флажке **Автоматически определять интервал для распределения запуска задачи**.

Для групповой задачи обновления Kaspersky Endpoint Security версии 8 следует явно указать период запуска (1 час или больше) и установить флажок **Автоматически определять интервал для распределения запуска задачи**.

В случае, если на каждом агенте обновлений будет создана локальная задача загрузки обновлений в хранилище с серверов «Лаборатории Касперского», то для групповой задачи обновления Kaspersky Endpoint Security оптимальным и рекомендуемым является периодическое расписание. Значение периода рандомизации следует в этом случае установить в 1 час.

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства. По умолчанию для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**.

Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. Следует настроить оптимальное расписание этой задачи исходя из принятого в организации регламента работы.

Ручная настройка расписания задачи поиска уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу поиска уязвимостей. По умолчанию для задачи выбрано расписание **Запускать по вторникам в 19:00** с автоматической рандомизацией и установлен флажок **Запускать пропущенные задачи**.

Если регламент работы организации предусматривает выключение устройств в это время, то задача поиска уязвимостей будет запущена после включения устройства (в среду утром). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует задать

оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы.

Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу установки обновлений и поиска уязвимостей. По умолчанию настроен запуск задачи ежедневно в 1:00 с автоматической рандомизацией, флажок **Запускать пропущенные задачи** снят.

Если регламент работы организации предусматривает отключение устройств на ночь, то задача установки обновлений никогда не будет запущена. Следует задать оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы. Кроме того, следует учитывать, что в результате установки обновлений может потребоваться перезагрузка устройства.

Построение структуры групп администрирования и назначение агентов обновлений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область действия политик задается с помощью тегов, местоположения устройств в подразделениях Active Directory, членства в группах безопасности Active Directory и прочего (см. раздел «Иерархия политик, использование профилей политик» на стр. 34).

- Задание области действия групповых задач.

Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.
- Назначение агентов обновлений.

При построении структуры групп администрирования следует учитывать топологию сети предприятия для оптимального назначения агентов обновлений. Оптимальное распределение агентов обновлений позволяет уменьшить сетевой трафик внутри сети предприятия.

В зависимости от организационной структуры MSP-клиента и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- один офис;
- множество небольших изолированных офисов.

В этом разделе

Типовая конфигурация MSP-клиента: один офис

В типовой конфигурации «один офис» все устройства находятся в сети предприятия и «видят» друг друга. Сеть предприятия может состоять из нескольких выделенных «частей» (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали

какие-либо группы администрирования. Можно использовать автоматическое назначение агентов обновлений, либо назначать агенты обновлений вручную.

- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение агентов обновлений, и в каждой выделенной части сети назначить одно или несколько устройств агентами обновлений на корневую группу администрирования, например, на группу **Управляемые устройства**. Все агенты обновлений окажутся на одном уровне и будут иметь одинаковую область действия «все устройства сети предприятия». Каждый Агент администрирования версии 10 SP1 или более поздней версии в таком случае будет подключаться к тому агенту обновлений, маршрут к которому является самым коротким. Маршрут к агенту обновлений можно определить с помощью утилиты tracert.

Назначать агенты обновлений вручную следует из расчета 100 – 200 обслуживаемых устройств на каждый агент обновлений. Агентами обновлений следует назначать мощные устройства с достаточным количеством свободного места на диске (см. раздел «Оценка места на диске для агента обновлений» на стр. 101). Агенты обновлений не следует часто выключать, на них должен быть выключен «спящий режим».

Типовая конфигурация MSP-клиента: множество небольших изолированных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).

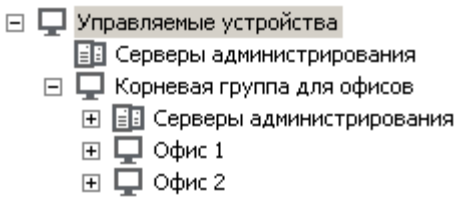

Рисунок 1. Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить один или несколько агентов обновлений. Агентами обновлений нужно назначать устройства удаленного офиса, имеющие достаточно места на диске (см. раздел «Оценка места на диске для агента обновлений» на стр. 101). Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к агентам обновлений, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше агентам обновлений выбрать два и или более устройств и назначить их агентами обновлений на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Например, имеется ноутбук, размещенный в группе администрирования **Офис 1**, но физически переехавший в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к агентам обновлений, назначенным на группу **Офис 1**, но эти агенты обновлений окажутся недоступны. Тогда Агент администрирования начнет обращаться к агентам обновлений, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех агентов обновлений, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к агентам обновлений, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать агента обновлений того офиса, в котором в данный момент находится физически.

Иерархия политик, использование профилей политик

В этом разделе содержится информация об особенностях применения политик к устройствам в группах администрирования. В разделе также содержится информация о профилях политик, которые поддерживаются в Kaspersky Security Center начиная с версии 10 SP1.

В этом разделе

Иерархия политик

В Kaspersky Security Center политики предназначены для задания одинакового набора параметров на множестве устройств. Например, областью действия политики продукта P, определенной для группы G, являются управляемые устройства с установленным продуктом P, размещенные в группе администрирования G и всех ее подгруппах, исключая те подгруппы, в свойствах которых снят флажок **Наследовать из родительской группы**.

Политика отличается от локальных параметров наличием «замков» возле содержащихся в ней параметров. Установленный «замок» в свойствах политики означает, что соответствующий ему параметр (или группа параметров) должен, во-первых, быть использован при формировании эффективных параметров, во-вторых, должен быть записан в нижележащую политику.

Формирование на устройстве действующих параметров можно представить следующим образом: из политики берутся значения параметров с неустановленным «замком», затем поверх них записываются значения локальных параметров, затем поверх полученных значений записываются взятые из политики значения параметров с установленным «замком».

Политики одного и того же продукта действуют друг на друга по иерархии групп администрирования: параметры с установленным «замком» из вышележащей политики переписывают одноименные параметры из нижележащей политики.

Существует особый вид политики – политика для автономных пользователей. Эта политика вступает в силу на устройстве, когда устройство переходит в автономный режим. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

Политика для автономных пользователей не будет поддерживаться в будущих версиях Kaspersky Security Center. Вместо политик для автономных пользователей следует использовать профили политик.

Профили политик

Применение политик к устройствам исходя только из иерархии групп администрирования во многих случаях неудобно. Может возникнуть необходимость создать в разных группах администрирования нескольких копий политики, отличающихся одним-двумя параметрами, и в дальнейшем вручную синхронизировать содержимое этих политик.

Во избежание подобных проблем в Kaspersky Security Center, начиная с версии 10 SP1, поддерживаются *профили политики*. Профиль политики представляет собой именованное подмножество параметров политики, которое распространяется на устройства вместе с политикой и дополняет политику при выполнении некоторого условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от «базовой» политики, действующей на клиентском устройстве (компьютере, мобильном устройстве). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политик сейчас имеют следующие ограничения:

- в политике может быть не более 100 профилей;
- профиль политики не может содержать другие профили;
- профиль политики не может содержать параметры уведомлений.

Состав профиля

Профиль политики содержит следующие составные части:

- Имя. Профили с одинаковыми именами действуют друг на друга по иерархии групп администрирования с общим правилами.
- Подмножество параметров политики. В отличие от политики, где содержатся все параметры, в профиле присутствуют лишь те параметры, которые действительно нужны (на которых установлен «замок»).
- Условие активации – логическое выражение над свойствами устройства. Профиль активен (дополняет политику), только когда условие активации профиля становится истинным. В остальных случаях профиль неактивен и игнорируется. В логическом выражении могут участвовать следующие свойства устройства:
  - состояние автономного режима;
  - свойства сетевого окружения – имя активного правила подключения Агента администрирования; (см. раздел «Настройка профилей соединения для автономных пользователей» на стр. 81);
  - наличие или отсутствие у устройства указанных тегов;
  - местоположение устройства в подразделении Active Directory: явное (устройство находится непосредственно в указанном подразделении), или неявное (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности);
  - членство устройства в группе безопасности Active Directory (явное или неявное);
  - членство владельца устройства в группе безопасности Active Directory (явное или неявное).

- Флажок отключения профиля. Отключенные профили всегда игнорируются, условия их активации не проверяются на истинность.

- Приоритет профиля. Условия активации профилей независимы, поэтому одновременно могут активироваться сразу несколько профилей. Если активные профили содержат непересекающиеся наборы параметров, то никаких проблем не возникает. Но если два активных профиля содержат разные значения одного и того же параметра, возникает неоднозначность. Неоднозначность устраняется при помощи приоритетов профилей: значение неоднозначной переменной будет взято из профиля с большим приоритетом (из того профиля, который располагается выше в списке профилей).

Поведение профилей при действии политик друг на друга по иерархии

Одноименные профили объединяются согласно правилам объединения политик. Профили верхней политики приоритетнее профилей нижней политики. Если в «верхней» политике запрещено изменение параметров (кнопка «замок» нажата), в «нижней» политике используются условия активации профиля из «верхней» политики. Если в «верхней» политике разрешено изменение параметров, то используются условия активации профиля из «нижней» политики.

Поскольку профиль политики может в условии активации содержать свойство **Устройство в автономном режиме**, профили полностью заменяют функциональность политик для автономных пользователей, которая в дальнейшем не будет поддерживаться.

Политика для автономных пользователей может содержать профили, но активация ее профилей может произойти не ранее, чем устройство перейдет в автономный режим.

Задачи

В зависимости от области действия задачи, в Kaspersky Security Center можно выделить следующие виды задач:

- Локальные задачи – создаются непосредственно на управляемых устройствах. Локальные задачи могут быть изменены не только администратором на стороне Kaspersky Security Center средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе программы защиты). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором как более приоритетные.

- Групповые задачи – действуют на группу администрирования и все ее подгруппы. Групповые задачи также действуют (опционально) и на устройства, подключенные к размещенным в этой группе и подгруппах подчиненным и виртуальным Серверам администрирования.

- Задачи для наборов устройств – действуют на ограниченный набор устройств, указанный при создании задачи.

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

  > Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования.

- Задачи кластера (массива серверов) – действуют на узлы данного кластера или массива серверов.

Правила перемещения устройств

Размещение устройств в группах администрирования на виртуальном сервере, соответствующем MSP-клиенту, целесообразно автоматизировать при помощи *правил перемещения устройств*. Правило перемещения состоит из трех основных частей: имени, условия выполнения (логического выражения над атрибутами устройства) и целевой группы администрирования. Правило перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Сервер администрирования проверяет атрибуты устройства на соответствие условию выполнения каждого правила, в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют условию выполнения правила, то устройство перемещается в целевую группу, и на этом обработка правил для данного устройства прекращается. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Правила перемещения устройств могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должно попасть устройство после установки на нем Агента администрирования. Также правила перемещения могут быть созданы администратором Kaspersky Security Center в явном виде, в списке правил перемещения. Список расположен в Консоли администрирования в свойствах группы **Нераспределенные устройства.**

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает только один раз устройства, находящиеся в группе **Нераспределенные устройства**. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу **Нераспределенные устройства**. Это рекомендуемый способ использования правил перемещения.

Можно перемещать устройства, уже размещенные в группах администрирования. Для этого в свойствах правила нужно снять флажок **Перемещать только устройства, не размещенные в группах администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенных в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенного агента обновлений.

Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и по сетевому трафику, а также противоречат модели работы Kaspersky Security Center (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик (на стр. 35), задачи для выборок устройств (см. раздел «Задачи» на стр. 38), назначать Агенты администрирования согласно методике (см. раздел «Построение структуры групп администрирования и назначение агентов обновлений» на стр. 30) и так далее.

Категоризация программного обеспечения

Основным средством контроля запуска приложений являются *категории «Лаборатории Касперского»* (далее также *KL-категории*). KL-категории облегчают администратору Kaspersky Security Center работу по поддержанию категоризации ПО и минимизируют объем трафика, передаваемого на управляемые устройства.

Пользовательские категории следует создавать только для программ, не подпадающих ни под одну KL-категорию (например, для программ, разработанных на заказ). Пользовательские категории создаются на основе дистрибутива продукта (MSI) или на основе папки с дистрибутивами.

В случае если имеется большая пополняемая коллекция программного обеспечения, не категоризированного при помощи KL-категорий, может быть целесообразным создать автоматически обновляемую категорию. Такая категория будет автоматически пополняться контрольными суммами исполняемых файлов при изменении папки с дистрибутивами.

Нельзя создавать автоматически обновляемые категории программного обеспечения на основе папок Мои документы, %windir%, %ProgramFiles%. Файлы в этих папках часто меняются, что приводит к увеличению нагрузки на Сервер администрирования и к увеличению трафика в сети. Следует создать отдельную папку с коллекцией программного обеспечения и время от времени пополнять ее.

Резервное копирование и восстановление параметров Сервера администрирования

Для резервного копирования параметров Сервера администрирования и используемой им базы данных предусмотрены задача резервного копирования и утилита klbackup. Резервная копия включает в себя все основные параметры и объекты Сервера администрирования: сертификаты Сервера администрирования, мастер-ключи шифрования дисков управляемых устройств, ключи для лицензий, структуру групп администрирования со всем содержимым, задачи, политики и так далее. Имея резервную копию, можно восстановить работу Сервера администрирования в кратчайшие сроки – от десятков минут до двух часов.

Ни в коем случае не следует отказываться от регулярного создания резервных копий Сервера администрирования с помощью штатной задачи резервного копирования.

В случае отсутствия резервной копии сбой может привести к безвозвратной потере сертификатов и всех параметров Сервера администрирования. Это повлечет необходимость заново настраивать Kaspersky Security Center, а также заново выполнять первоначальное развертывание Агента администрирования в сети предприятия. Кроме того, будут потеряны и мастер-ключи шифрования дисков управляемых устройств, что создаст риск безвозвратной потери зашифрованных данных на устройствах с Kaspersky Endpoint Security.

Мастер первоначальной настройки программы создает задачу резервного копирования параметров Сервера администрирования с ежедневным запуском в три часа ночи. Резервные копии по умолчанию сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskySC.

Если в качестве СУБД используется экземпляр Microsoft SQL Server, установленный на другом устройстве, следует изменить задачу резервного копирования: указать в качестве папки для хранения сделанных резервных копий UNC-путь, доступный на запись как службе Сервера администрирования, так и службе SQL Server. Это неочевидное требование является следствием особенности резервного копирования в СУБД Microsoft SQL Server.

Если в качестве СУБД используется локальный экземпляр Microsoft SQL Server, также целесообразно сохранять резервные копии на отдельном носителе, чтобы обезопасить их от повреждения одновременно с Сервером администрирования.

Поскольку резервная копия содержит важные данные, в задаче резервного копирования и в утилите klbackup предусмотрена защита резервных копий паролем. По умолчанию задача резервного копирования создается с пустым паролем. Следует обязательно задать пароль в свойствах задачи резервного копирования. Несоблюдение этого требования приведет к тому, что ключи сертификатов Сервера администрирования, ключи для лицензий и мастер-ключи шифрования дисков управляемых устройств окажутся незашифрованными.

Помимо регулярного резервного копирования, следует также создавать резервную копию перед всеми значимыми изменениями, в том числе перед обновлением Сервера администрирования до новой версии, и перед установкой патчей Сервера администрирования.

Для уменьшения размеров резервных копий целесообразно установить флажок **Сжимать резервные копии** (**Compress backup**) в параметрах SQL Server.

Восстановление из резервной копии выполняется с помощью утилиты klbackup на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Инсталляция Сервера администрирования, на которую выполняется восстановление, должна использовать СУБД того же типа (тот же SQL Server или MySQL) той же самой или более новой версии. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

В этом разделе описаны типовые сценарии восстановления параметров и объектов Сервера администрирования.

В этом разделе

Вышло из строя устройство с Сервером администрирования

Если в результате сбоя вышло из строя устройство с Сервером администрирования, рекомендуется выполнить следующие действия:

- Новому Серверу назначить тот же самый адрес: NetBIOS-имя, FQDN-имя, статический IP – смотря по тому, что было задано при развертывании Агентов администрирования.
- Установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
- Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Повреждены параметры Сервера администрирования или база данных

Если Сервер администрирования стал неработоспособен в результате повреждения параметров или базы данных (например, из-за сбоя питания), рекомендуется использовать следующий сценарий восстановления:

1. Выполнить проверку файловой системы на пострадавшем устройстве.
2. Деинсталлировать неработоспособную версию Сервера администрирования.

3. Заново установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.

4. Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Совершенно недопустимо восстанавливать Сервер администрирования любым другим способом кроме штатной утилиты klbackup.

Во всех случаях восстановления Сервера с помощью стороннего программного обеспечения неизбежно произойдет рассинхронизация данных на узлах распределенного приложения Kaspersky Security Center и, как следствие, неправильная работа продукта.

Развертывание Агента администрирования и программы защиты

Для управления устройствами предприятия требуется установить на устройства Агент администрирования. Развертывание распределенного приложения Kaspersky Security Center на устройствах предприятия обычно начинается с установки на них Агента администрирования.

В этом разделе

Первоначальное развертывание

Если на устройстве уже установлен Агент администрирования, удаленная инсталляция приложений на такое устройство осуществляется с помощью самого Агента администрирования. При этом передача дистрибутива устанавливаемого приложения вместе с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентами администрирования и Сервером администрирования. Для передачи дистрибутива можно использовать промежуточные центры распространения в виде агентов обновлений, многоадресную рассылку и так далее. Подробные сведения об установке приложений на управляемые устройства, на которых уже установлен Агент администрирования, см. далее в этом разделе.

Первоначальную установку Агента администрирования на устройства на платформе Microsoft Windows можно осуществлять следующими способами:

- С помощью сторонних средств удаленной установки приложений, через механизм групповых политик Microsoft Windows: с помощью штатных средств управления групповыми политиками Microsoft Windows.
- Через механизм групповых политик Microsoft Windows.
- Принудительно с помощью соответствующих опций в задаче удаленной установки приложений Kaspersky Security Center.
- Путем рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных программ с настроенными параметрами.
- Вручную, запуская инсталляторы программ на устройствах.

На платформах, отличных от Microsoft Windows, первоначальную установку Агента администрирования на управляемых устройствах следует осуществлять имеющимися сторонними средствами либо вручную путем отправки пользователям архива с предварительно сконфигурированным дистрибутивом. Обновлять Агент администрирования до новой версии, а также устанавливать другие приложения «Лаборатории Касперского» на этих платформах можно с помощью задач удаленной установки приложений, используя уже имеющиеся на устройствах Агенты администрирования. Установка в этом случае происходит аналогично установке на платформе Microsoft Windows.

Выбирая способ и стратегию развертывания продуктов в управляемой сети, следует принимать во внимание ряд факторов (неполный список):

- конфигурацию сети предприятия (см. раздел «Типовая конфигурация Kaspersky Security Center» на стр. 13);
- общее количество устройств;
- наличие доменов Windows в управляемой сети, возможность внесения изменений в групповые политики Active Directory в таких доменах;
- знание учетной записи (записей) с правами локального администратора на тех устройствах, где предстоит провести первоначальное развертывание программ «Лаборатории Касперского» (то есть доступность доменной учетной записи с правами локального администратора либо наличие унифицированных локальных учетных записей с административными правами на таких устройствах);
- характер связи и ширину сетевых каналов между Сервером администрирования и сетями MSP-клиентов и ширину сетевых каналов внутри этих сетей;
- используемые на момент начала развертывания параметры безопасности на удаленных устройствах (в частности, использование UAC и режима Simple File Sharing).

Настройка параметров инсталляторов

Прежде чем приступать к развертыванию в сети программ «Лаборатории Касперского», следует определить параметры инсталляции – те параметры, которые настраиваются в ходе установки программы. При установке Агента администрирования требуется задать по крайней мере, адрес для подключения к Серверу администрирования, параметры proxy, а возможно и некоторые дополнительные параметры. В зависимости от выбранного способа установки параметры можно задавать различными способами. В простейшем случае (при интерактивной установке вручную на выбранное устройство) необходимые параметры можно задать с помощью пользовательского интерфейса инсталлятора, так что в некоторых случаях первоначальное развертывание может даже осуществляться путем отправки пользователям ссылки на дистрибутив Агента администрирования с указанием параметров (адреса Сервера администрирования и тому подобное), которые пользователь должен будет ввести в интерфейсе инсталлятора (см. раздел «Возможности ручной установки приложений» на стр. 58).

Этот способ настройки параметров не рекомендуется к использованию на практике ввиду неудобства для пользователей и высокой вероятности ошибок при ручном задании ими параметров и не подходит для неинтерактивной тихой установки программ на группы устройств. В типичном случае администратор должен централизованно указать значения параметров, которые в дальнейшем могут быть использованы для формирования автономных пакетов. Автономные пакеты являются самораспаковывающимися архивами дистрибутивов с заданными администратором параметрами. Автономные пакеты могут быть расположены на ресурсах, доступных для загрузки конечными пользователями (например, на Веб-сервере Kaspersky Security Center) и для неинтерактивной установки на выбранные устройства в сети.

Инсталляционные пакеты

Первый и основной способ настройки инсталляционных параметров приложений является универсальным и подходит для всех способов установки приложений: как средствами Kaspersky Security Center, так и с помощью большинства сторонних средств. Этот способ подразумевает создание в Kaspersky Security Center инсталляционных пакетов приложений.

Инсталляционные пакеты создаются следующими способами:

- автоматически из указанных дистрибутивов на основании входящих в их состав *описателей* (файлов с расширением kud, содержащих правила установки и анализа результата и другую информацию);
- из исполняемых файлов инсталляторов или инсталляторов в формате Microsoft Windows Installer (MSI) – для стандартных или поддерживаемых приложений.

Созданные инсталляционные пакеты представляют собой папки с вложенными подпапками и файлами. Помимо исходного дистрибутива, в состав инсталляционного пакета входят редактируемые параметры (включая параметры самого инсталлятора и правила обработки таких ситуаций, как необходимость перезагрузки операционной системы для завершения инсталляции), а также небольшие вспомогательные модули.

Значения параметров инсталляции, специфичные для конкретного поддерживаемого приложения, можно задавать в пользовательском интерфейсе Консоли администрирования при создании инсталляционного пакета (еще больше параметров для настройки может быть доступно в свойствах уже созданного инсталляционного пакета). В случае удаленной установки программ средствами Kaspersky Security Center инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора программы ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки программ «Лаборатории Касперского» достаточно обеспечить доступность на устройстве всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center в соответствующей папке каталога общих данных.

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

О том, как именно можно воспользоваться этим способом настройки параметров для приложений «Лаборатории Касперского» перед их развертыванием сторонними средствами, смотрите в разделе «Развертывание с помощью механизма групповых политик Microsoft Windows» (см. раздел «Развертывание с помощью механизма групповых политик Microsoft Windows» на стр. 53).

Сразу после установки Kaspersky Security Center автоматически создается несколько инсталляционных пакетов, готовых к установке, в том числе пакеты Агента администрирования и программы защиты для платформы Microsoft Windows.

Использование инсталляционных пакетов для развертывания приложений в сети MSP-клиента в ряде случаев подразумевает необходимость создания инсталляционных пакетов на виртуальных Серверах, соответствующих MSP-клиентам. Создание инсталляционных пакетов на виртуальных Серверах позволяет использовать в инсталляционных пакетах для разных MSP-клиентов различные параметры инсталляции. В первую очередь это необходимо в инсталляционных пакетах Агента администрирования, так как Агенты администрирования, развернутые в сетях разных MSP-клиентов, используют различные адреса подключения к Серверу администрирования. Собственно, адрес подключения и определяет, к какому виртуальному Серверу подключается Агент администрирования.

Помимо наличия возможности создания новых инсталляционных пакетов непосредственно на виртуальном Сервере, основным режимом работы с инсталляционными пакетами на виртуальных Серверах является «ретрансляция» инсталляционных пакетов главного Сервера на виртуальные. Ретранслировать выбранные (или все) пакеты на выбранные виртуальные Серверы (в том числе все Серверы, входящие в выбранную группу администрирования) можно с помощью соответствующей задачи Сервера администрирования. Также при создании нового виртуального Сервера в мастере можно выбрать список инсталляционных пакетов главного Сервера. Выбранные пакеты будут сразу ретранслированы на вновь созданный виртуальный Сервер.

При ретрансляции инсталляционного пакета не происходит полного копирования его содержимого. В файловом хранилище, соответствующем ретранслированному инсталляционному пакету на виртуальном Сервере, хранятся только файлы параметров, специфичных для данного виртуального Сервера. Основная, неизменная часть инсталляционного пакета (включая сам дистрибутив устанавливаемого приложения) хранится только в хранилище главного Сервера. Это позволяет существенно повысить производительность системы и снизить объем требуемого дискового пространства. При работе с инсталляционными пакетами, ретранслированными на виртуальные Серверы (то есть, при работе задач удаленной установки или при создании автономных инсталляционных пакетов) происходит «сложение» данных из исходного инсталляционного пакета главного Сервера и файлов с параметрами, соответствующих ретранслированному пакету на виртуальном Сервере.

Несмотря на то, что ключ для лицензии на приложение можно задать в свойствах инсталляционного пакета, желательно не использовать этот способ распространения лицензий из-за потенциальной возможности чтения файлов, расположенных в каталоге. Следует использовать автоматически распространяемые ключи или продуктовые задачи установки ключей.

Свойства MSI и файлы трансформации

Другим способом настроить параметры инсталляции на платформе Windows является задание свойств MSI и файлов трансформации. Этот способ может быть использован при установке с помощью сторонних средств, ориентированных на работу с инсталляторами в формате Microsoft Installer (см. раздел «Настройка параметров инсталляторов» на стр. 66), а также при установке через групповые политики Windows при помощи штатных средств Microsoft или иных сторонних инструментов для работы с групповыми политиками Windows.

Развертывание при помощи сторонних средств удаленной установки приложений

При наличии на предприятии каких-либо средств удаленной установки приложений (например, Microsoft System Center) целесообразно выполнять первоначальное развертывание при помощи этих средств.

Нужно выполнить следующие действия:

- Выбрать способ настройки параметров инсталляции, наиболее подходящий для используемого средства развертывания.
- Определить механизм синхронизации между изменением параметров инсталляционных пакетов через интерфейс Консоли администрирования и работой выбранных сторонних средств развертывания приложений из данных инсталляционных пакетов.

См. также

Настройка параметров инсталляторов 66

Общие сведения о задачах удаленной установки приложений Kaspersky Security Center

Kaspersky Security Center предоставляет разнообразные механизмы удаленной установки приложений, реализованные в виде задач удаленной установки приложений. Создать задачу удаленной установки можно как для указанной группы администрирования, так и для набора устройств или для выборки устройств (такие задачи отображаются в Консоли администрирования в папке **Задачи**). При создании задачи можно выбрать инсталляционные пакеты (Агента администрирования и / или другого приложения), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки.

Задачи для групп администрирования действуют не только на устройства, принадлежащие этой группе, но и на все устройства всех подгрупп выбранной группы. Если в параметрах задачи включен соответствующий параметр, задача распространяется на устройства подчиненных Серверов администрирования, расположенных в данной группе или ее подгруппах.

Задачи для наборов устройств актуализируют список клиентских устройств при каждом запуске в соответствии с составом выборки устройств на момент запуска задачи. Если в выборке устройств присутствуют устройства, подключенные к подчиненным Серверам администрирования, задача будет запускаться и на этих устройствах. Подробнее об этих параметрах и способах установки будет рассказано далее в этом разделе.

Для успешной работы задачи удаленной установки на устройствах, подключенных к подчиненным Серверам администрирования, следует при помощи задачи ретрансляции предварительно ретранслировать используемые задачей инсталляционные пакеты на соответствующие подчиненные Серверы администрирования.

Развертывание с помощью механизма групповых политик Microsoft Windows

Первоначальное развертывание Агентов администрирования рекомендуется осуществлять с помощью групповых политик Microsoft Windows при выполнении следующих условий:

- устройства являются членами домена Active Directory;
- разрешен доступ к контроллеру домена с правами администратора, позволяющими создавать и модифицировать групповые политики Active Directory;
- имеется возможность переноса настроенных инсталляционных пакетов в сеть управляемых устройств (в папку общего доступа, доступную на чтение для всех устройств);
- план развертывания позволяет дождаться штатной перезагрузки устройств до начала развертывания на них Агентов администрирования, или к устройствам можно принудительно применить групповую политику Windows.

Суть данного способа развертывания заключается в следующем:

- Дистрибутив приложения в формате Microsoft Installer (MSI-пакет) размещается в папке общего доступа (в папке, к которой имеют доступ на чтение учетные записи LocalSystem устройств).
- В групповой политике Active Directory создается объект установки данного дистрибутива.
- Область действия установки задается привязкой к organization unit и / или к группе безопасности, в которую входят устройства.
- При очередном входе устройства в домен (до входа в систему пользователей устройства) выполняется проверка наличия требуемого приложения среди установленных приложений. Если приложение отсутствует, происходит загрузка дистрибутива с заданного в политике ресурса и его установка.

Одним из преимуществ этого способа развертывания является то, что назначенные приложения устанавливаются на устройства при загрузке операционной системы еще до входа пользователя в систему. Даже если пользователь, имеющий необходимые права, удалит приложение, при следующей загрузке операционной системы оно будет установлено снова. Недостатком этого способа развертывания является то, что произведенные администратором изменения в групповой политике не вступят в силу до перезагрузки устройств (без применения дополнительных средств).

С помощью групповых политик можно устанавливать как Агент администрирования, так и другие приложения, инсталляторы которых имеют формат Windows Installer.

При выборе этого способа развертывания, помимо прочего, необходимо оценить нагрузку на файловый ресурс, с которого будет осуществляться копирование файлов на устройства при применении групповой политики Windows, а также способ доставки на этот ресурс сконфигурированного инсталляционного пакета (и синхронизации производимых изменений в его параметрах).

Работа с политиками Microsoft Windows с помощью задачи удаленной установки приложений Kaspersky Security Center

Данный способ развертывания возможен только в том случае, если доступ к контроллеру домена, в которую входят устройства, возможен с устройства, где установлен Сервер администрирования, а с устройств доступна для чтения папка общего доступа Сервера администрирования (в которой расположены инсталляционные пакеты). Поэтому данный способ развертывания не рассматривается в контексте MSP.

Самостоятельная установка приложений с помощью политик Microsoft Windows

Администратор может самостоятельно создать в групповой политике Windows объекты, необходимые для установки. В этом случае нужно выложить пакеты на отдельный файловый сервер и сослаться на них.

Возможны следующие сценарии установки:

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Затем администратор копирует целиком подпапку EXEC этого пакета из папки общего доступа Kaspersky Security Center в папку на специализированном файловом ресурсе предприятия. Объект групповой политики ссылается на msi-файл этого сконфигурированного пакета, лежащего в подпапке на специализированном файловом ресурсе предприятия.

- Администратор загружает дистрибутив приложения (в том числе дистрибутив Агента администрирования) из интернета и выкладывает его на специализированный файловый ресурс предприятия. Объект групповой политики ссылается msi-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе предприятия. Настройка параметров инсталляции осуществляется путем настройки свойств MSI или настройкой файлов трансформации MST (см. раздел «Настройка параметров инсталляторов» на стр. 66).

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center

Для первоначального развертывания Агентов администрирования или других необходимых приложений при наличии учетной записи (записей) с правами локального администратора на устройствах и наличии в каждой подсети устройств хотя бы одного устройства с уже установленным Агентом администрирования, исполняющим роль агента обновлений (см. раздел «Об агентах обновлений» на стр. 14), можно использовать принудительную (форсированную) установку выбранных инсталляционных пакетов при помощи задачи удаленной установки приложений Kaspersky Security Center.

Устройства при этом могут задаваться явно (списком), либо выбором группы администрирования Kaspersky Security Center, которой они принадлежат, либо созданием выборки устройств по определенному условию. Момент начала установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

Принудительная установка осуществляется путем доставки инсталляционных пакетов на агенты обновлений, последующего копирования файлов на административный ресурс admin$ каждого из устройств, и удаленной регистрации на них вспомогательных служб. Доставка инсталляционных пакетов на агенты обновлений выполняется с помощью функции Kaspersky Security Center, отвечающей за сетевое взаимодействие. При этом должны выполняться следующие условия:

- Устройства должны быть доступны со стороны агента обновлений.
- В сети должно корректно работать разрешение имен для устройств.
- На управляемых устройствах не должны быть отключены административные ресурсы общего доступа admin$.
- На устройствах должна быть запущена системная служба Server (по умолчанию данная служба запущена).
- На устройствах должны быть открыты следующие порты для удаленного доступа к устройствам средствами Windows: TCP 139, TCP 445, UDP 137, UDP 138.
- На устройствах должен быть выключен режим Simple File Sharing.
- На устройствах модель совместного доступа и безопасности для локальных учетных записей должна находиться в состоянии *Обычная – локальные пользователи удостоверяются как они сами* (*Classic – local users authenticate as themselves*), и ни в коем случае не в состоянии *Гостевая – локальные пользователи удостоверяются как гости* (*Guest only – local users authenticate as Guest*).
- Устройства должны быть членами домена, либо на устройствах должны быть заблаговременно созданы унифицированные учетные записи с административными правами.

Устройства, расположенные в рабочих группах, могут быть приведены в соответствие указанным выше требованиям при помощи утилиты riprep.exe, которая описана на портале Службы технической поддержки «Лаборатории Касперского» (http://support.kaspersky.com/7434).

При установке на новые устройства, еще не размещенные в группах администрирования Kaspersky Security Center, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Можно использовать упрощенный способ создания задач принудительной установки приложений – автоматическую установку. Для этого в свойствах группы администрирования нужно выбрать в списке инсталляционных пакетов те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Для работоспособности принудительной установки необходимо обеспечить наличие агентов обновлений в каждой изолированной сети, в которой находятся устройства.

Следует учитывать, что данный способ установки создает значительную нагрузку на устройства, назначенные агентами обновлений. Поэтому нужно выбирать в качестве агентов обновлений достаточно мощные устройства с быстрыми накопителями. Также необходимо, чтобы объем свободного места в разделе с папкой *%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit* многократно превосходил суммарный объем дистрибутивов устанавливаемых приложений (см. раздел «Оценка места на диске для агента обновлений» на стр. 101).

Запуск автономных пакетов, сформированных Kaspersky Security Center

Описанные выше способы первоначального развертывания Агента администрирования и приложений могут быть реализованы не всегда из-за невозможности выполнить все необходимые условия. В таких случаях из подготовленных администратором инсталляционных пакетов с необходимыми параметрами установки средствами Kaspersky Security Center можно создать единый исполняемый файл, который называется *автономным пакетом установки*. Автономный пакет установки может быть опубликован как на внутреннем Веб-сервере (входящем в состав Kaspersky Security Center), если это имеет смысл (настроен доступ к этому Веб-серверу извне для пользователей устройств), так и на специально развернутом Веб-сервере, входящем в состав Kaspersky Security Center Web Console. Также можно скопировать автономные пакеты на другой Веб-сервер.

При помощи Kaspersky Security Center можно разослать по электронной почте выбранным пользователям ссылку на файл автономного пакета на используемом Веб-сервере с просьбой запустить файл (интерактивно или с ключом «тихой» установки «-s»). Автономный пакет установки можно прикрепить к сообщению электронной почты для пользователей устройств, не имеющих доступ к Веб-серверу. Администратор может также скопировать автономный пакет на внешнее устройство и доставить пакет на нужное устройство с целью его последующего запуска.

Автономный пакет можно создать из пакета Агента администрирования, пакета другого (например, программы защиты) приложения или сразу из обоих пакетов. Если автономный пакет создан из Агента администрирования и другого приложения, установка начнется с Агента администрирования.

При создании автономного пакета с Агентом администрирования можно указать группу администрирования, в которую будут автоматически перемещаться новые устройства (ранее не размещенные в группах администрирования) по завершении установки на них Агента администрирования.

Автономные пакеты могут работать интерактивно (по умолчанию), с отображением результата установки входящих в них приложений, или в «тихом» режиме (при запуске с ключом «-s»). «Тихий» режим может быть использован для установки из каких-либо скриптов (например, из скриптов, настраиваемых для запуска по завершении развертывания образа операционной системы, и тому подобное). Результат установки в «тихом» режиме определяется кодом возврата процесса.

Возможности ручной установки приложений

Администраторы или опытные пользователи могут устанавливать приложения вручную в интерактивном режиме. При этом можно использовать как исходные дистрибутивы, так и сформированные из них инсталляционные пакеты, расположенные в папке общего доступа Kaspersky Security Center. Инсталляторы по умолчанию работают в интерактивном режиме, запрашивая у пользователя все необходимые значения параметров. Но при запуске процесса setup.exe из корня инсталляционного пакета с ключом «-s» инсталлятор будет работать в «тихом» режиме с параметрами, заданными при настройке инсталляционного пакета.

При запуске setup.exe из корня инсталляционного пакета, сначала произойдет копирование пакета во временную локальную папку, затем из локальной справки будет запущен инсталлятор приложения.

Удаленная установка приложений на устройства с установленным Агентом администрирования

Если на устройстве установлен работоспособный Агент администрирования, подключенный к главному Серверу администрирования или к одному из его подчиненных Серверов, то на этом устройстве можно обновлять версию Агента администрирования, а также устанавливать, обновлять или удалять с помощью Агента администрирования любые поддерживаемые приложения.

Эта функция включается флажком **С помощью Агента администрирования** в свойствах задачи удаленной установки приложений (см. раздел «Общие сведения о задачах удаленной установки приложений Kaspersky Security Center» на стр. 52).

Если флажок установлен, то передача на устройства инсталляционных пакетов с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентом администрирования и Сервером администрирования.

Для оптимизации нагрузки на Сервер администрирования и минимизации трафика между Сервером администрирования и устройствами целесообразно назначать в каждой удаленной сети или в каждом широковещательном домене агенты обновлений (см. разделы Роль агентов обновлений (см. раздел «Об агентах обновлений» на стр. 14) и Построение структуры групп администрирования и назначение агентов обновлений (на стр. 30)). В этом случае распространение инсталляционных пакетов и параметров инсталлятора осуществляется с Сервера администрирования на устройства через агенты обновлений.

Также с использованием агентов обновлений можно выполнять широковещательную (многоадресную) рассылку инсталляционных пакетов, что позволяет многократно снизить сетевой трафик в ходе развертывания приложений.

При передаче инсталляционных пакетов на устройства по каналам связи между Агентами администрирования и Сервером администрирования, подготовленные к передаче

инсталляционные пакеты дополнительно кешируются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. При использовании большого числа различных инсталляционных пакетов большого размера и при большом количестве агентов обновлений размер этой папки может существенно увеличиваться.

Удалять файлы из папки FTServer вручную нельзя. При удалении исходных инсталляционных пакетов соответствующие данные будут автоматически удаляться и из папки FTServer.

Данные, принимаемые на стороне агентов обновлений, сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTClTmp.

Удалять файлы из папки $FTClTmp вручную нельзя. По мере завершения задач, использующих данные из папки, содержимое этой папки будет удаляться автоматически.

Поскольку инсталляционные пакеты распространяются по каналам связи между Сервером администрирования и Агентами администрирования из промежуточного хранилища в оптимизированном для передачи по сети формате, нельзя вносить изменения в инсталляционные пакеты в исходной папке инсталляционного пакета. Такие изменения не будут автоматически учтены Сервером администрирования. Если необходимо изменить вручную файлы инсталляционных пакетов (хотя делать это не рекомендуется), нужно обязательно изменить какие-либо параметры инсталляционного пакета в Консоли администрирования. Изменение параметров инсталляционного пакета в Консоли администрирования заставит Сервер администрирования обновить образ пакета в кеше, подготовленном для передачи на устройства.

Управление перезагрузкой устройств в задаче удаленной установки

Часто для завершения удаленной установки приложений (особенно на платформе Windows) требуется перезагрузка устройства.

Если используется задача удаленной установки приложений Kaspersky Security Center, в мастере создания задачи или в окне свойств созданной задачи (раздел **Перезагрузка ОС**) можно выбрать вариант действия при необходимости перезагрузки:

- **Не перезагружать устройство**. В этом случае автоматическая перезагрузка не будет выполнена. Для завершения установки потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки будет сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач установки на серверы и другие устройства, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**. В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения установки. Этот вариант подходит для задач установки на устройства, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Спросить у пользователя**. В этом случае на экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Вариант **Спросить у пользователя** наиболее подходит для рабочих станций, пользователи которых должны иметь возможность выбрать наиболее подходящий момент для перезагрузки.

Целесообразность обновления баз в инсталляционном пакете антивирусного приложения

Перед началом развертывания защиты необходимо учитывать возможность обновления антивирусных баз (включая модули автопатчей), распространяемых вместе с дистрибутивом программы защиты. Целесообразно перед началом развертывания принудительно обновить базы в составе инсталляционного пакета приложения (например, с помощью соответствующей команды в контекстном меню выбранного инсталляционного пакета). Это уменьшит количество перезагрузок, требующихся для завершения развертывания защиты на устройствах. В случае использования для удаленной установки инсталляционных

пакетов, ретранслированных на виртуальные Серверы с главного Сервера, обновлять базы нужно только в самом исходном пакете на главном Сервере. Обновлять базы в ретранслированных пакетах на виртуальных Серверах в этом случае не следует.

Выбор способа деинсталляции несовместимых приложений при установке программы защиты «Лаборатории Касперского»

Для установки программ защиты «Лаборатории Касперского» средствами Kaspersky Security Center может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемой программой. Существуют два основных способа выполнить эту задачу.

Автоматическое удаление несовместимых программ с помощью инсталлятора

Поддерживается при различных видах установки. Перед установкой программы защиты несовместимые с ней программы удаляются автоматически, если в окне свойств инсталляционного пакета программы защиты (раздел **Несовместимые программы**) установлен флажок **Удалять несовместимые программы автоматически**.

Удаление несовместимых программ с помощью отдельной задачи

Для удаления несовместимых программ используется задача **Удаленная деинсталляция программы**. Задачу следует запускать на устройствах перед задачей установки программы защиты. Например, в задаче установки можно выбрать расписание типа **По завершению другой задачи**, где другой задачей является задача **Удаленная деинсталляция программы**.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор программы защиты не может успешно удалить какую-либо из несовместимых программ.

Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых устройствах произвольных исполняемых файлов

С помощью мастера создания инсталляционного пакета можно выбрать произвольный исполняемый файл и задать для него параметры командной строки. При этом в инсталляционный пакет можно поместить как сам выбранный файл, так и всю папку, в которой этот файл содержится. Затем следует создать задачу удаленной установки и выбрать созданный инсталляционный пакет.

В ходе работы задачи на устройствах будет запущен указанный при создании исполняемый файл с заданными параметрами командной строки.

Если используются инсталляторы в формате Microsoft Windows Installer (MSI), Kaspersky Security Center использует штатные возможности по анализу результата установки.

Если есть лицензия Systems Management, при создании инсталляционного пакета для одного из поддерживаемых приложений, распространенных в корпоративной среде, Kaspersky Security Center также использует правила установки и анализа результатов установки, имеющиеся в его обновляемой базе.

В иных случаях для исполняемых файлов задача по умолчанию дожидается завершения запущенного процесса и всех порожденных им дочерних процессов. По завершении запущенных процессов задача будет завершена успешно независимо от кода возврата исходного процесса. Чтобы изменить такое поведение задачи, перед созданием задачи следует изменить вручную kud-файл, сформированный Kaspersky Security Center в папке созданного инсталляционного пакета.

Для того чтобы задача не ожидала завершения запущенного процесса, в секции [SetupProcessResult] нужно задать значение 0 для параметра Wait:

Пример:

[SetupProcessResult]

Wait=0

Для того чтобы на платформе Windows задача ожидала только завершения исходного процесса, но не порожденных им дочерних процессов, нужно в секции [SetupProcessResult] задать значение 0 для параметра WaitJob, например:

Пример:

[SetupProcessResult]

WaitJob=0

Для того чтобы задача завершалась успешно или с ошибкой в зависимости от кода возврата запущенного процесса, нужно перечислить успешные коды возврата в секции [SetupProcessResult_SuccessCodes], например:

Пример:

[SetupProcessResult_SuccessCodes]

0=

3010=

В этом случае любой код, отличный от перечисленных, будет означать ошибку.

Для того чтобы в результатах задачи отображалась строка с комментарием об успешном завершении задачи или сообщения об ошибках, нужно задать краткие описания ошибок, соответствующих кодам возврата процесса, в секциях [SetupProcessResult_SuccessCodes] и [SetupProcessResult_ErrorCodes], например:

Пример:

[SetupProcessResult_SuccessCodes]

0= Installation completed successfully

3010=A reboot is required to complete the installation

[SetupProcessResult_ErrorCodes]

1602=Installation cancelled by the user

1603=Fatal error during installation

Для того чтобы задействовать средства Kaspersky Security Center по управлению перезагрузкой устройства (если перезагрузка необходима для завершения операции), нужно дополнительно перечислить коды возврата процесса, означающие необходимость перезагрузки, в секции [SetupProcessResult_NeedReboot]:

Пример:

[SetupProcessResult_NeedReboot]

3010=

Мониторинг развертывания

Для контроля развертывания Kaspersky Security Center, а также для контроля наличия на управляемых устройствах программы защиты и Агента администрирования, следует обращать внимание на цветовой индикатор в блоке **Развертывание**. Индикатор расположен в рабочей области узла Сервер администрирования в главном окне Консоли администрирования (см. раздел «Цветовые индикаторы в Консоли администрирования» на стр. 93). Индикатор отображает текущее состояние развертывания. Рядом с индикатором отображается количество устройств с установленными Агентами администрирования и программами защиты. При наличии активных задач установки отображается прогресс выполнения задач. При наличии ошибок установки отображается количество ошибок с возможностью просмотреть детальную информацию об ошибке по ссылке.

Также можно воспользоваться диаграммой развертывания в рабочей области папки **Управляемые устройства** на закладке **Группы**. Диаграмма отражает процесс развертывания: количество устройств без Агента администрирования, с Агентом администрирования, с Агентом администрирования и программой защиты.

Более детальное описание хода развертывания (или работы конкретной задачи установки) можно увидеть в окне результатов выполнения соответствующей задачи удаленной установки. Окно результатов доступно из контекстного меню задачи (пункт **Результаты**). В окне отображаются два списка: в верхнем списке содержится список состояний задачи на устройствах, а в нижнем – список событий задачи на устройстве, которое в данный момент выбрано в верхнем списке.

Информация об ошибках при развертывании записываются в Kaspersky Event Log Сервера администрирования. Информация об ошибках также доступна в соответствующей выборке событий в папке **Отчеты и уведомления**, в подпапке **События**.

Настройка параметров инсталляторов

В разделе содержится информация о файлах инсталляторов Kaspersky Security Center и параметрах установки, а также рекомендации по установке Сервера администрирования и Агента администрирования в «тихом» режиме.

В этом разделе

Общая информация

Инсталляторы компонентов Kaspersky Security Center 10 – Сервера администрирования, Агента администрирования, Консоли администрирования построены на технологии Windows Installer. Ядром инсталлятора является msi-пакет. Этот формат упаковки дистрибутива позволяет использовать все преимущества технологии Windows Installer: масштабируемость, возможность использовать систему патчевания, систему трансформации, возможность установки централизованно сторонними решениями, прозрачность регистрации в операционной системе.

Установка в «тихом» режиме (с файлом ответов)

В инсталляторах Сервера администрирования и Агента администрирования реализована возможность работы с файлом ответов (ss_install.xml), в котором записаны параметры для установки в тихом режиме без участия пользователя. Файл ss_install.xml расположен в той же папке, что и msi-пакет, и используется автоматически при установке в «тихом» режиме. «Тихий» режим установки включается ключом командной строки «/s».

Пример запуска:

```
setup.exe /s
```

Файл ss_install.xml представляет собой внутренний формат параметров инсталлятора Kaspersky Security Center. В составе дистрибутивов поставляется файл ss_install.xml с параметрами по умолчанию.

Не следует изменять файл ss_install.xml вручную. Этот файл изменяется средствами Kaspersky Security Center при изменении параметров установочных пакетов в Консоли администрирования.

Установка в тихом режиме (без файла ответов)

Агент администрирования можно установить при помощи одного только msi-пакета, задавая при этом значения свойств MSI стандартным образом. Такой сценарий позволяет устанавливать Агент администрирования, используя групповые политики. Для того чтобы не возникал конфликт между параметрами, заданными с помощью свойств MSI, и параметрами, заданными в файле ответов, предусмотрена возможность отключения файла ответов путем задания свойства DONT_USE_ANSWER_FILE=1. Ниже приведен пример запуска инсталлятора Агента администрирования с помощью msi-пакета.

Пример:

msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com

Также параметры инсталляции msi-пакета можно задать, подготовив предварительно файл трансформации (файл с расширением mst). Команда будет выглядеть следующим образом:

Пример:

msiexec /I "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst

В одной команде можно указать более одного файла трансформации.

Частичная настройка параметров установки через setup.exe

Запуская установку продуктов через setup.exe, можно передавать в msi-пакет значения любых свойств MSI.

Команда будет выглядеть следующим образом:

Пример:

/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"

Параметры установки Сервера администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Сервера администрирования. Все параметры являются опциональными, кроме EULA.

Таблица 4. Свойства MSI

Свойство MSI	Описание	Возможные значения
EULA	Согласие с условиями лицензии (обязательный параметр)	• 1 • Пусто
INSTALLATIONMODETYPE	Тип установки Сервера администрирования	• Стандартная • Выборочная
INSTALLDIR	Папка установки продукта	
ADDLOCAL	Список компонентов для установки (через запятую)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.

Свойство MSI	Описание	Возможные значения
		Минимальный достаточный для корректной установки Сервера администрирования список компонентов: `ADDLOCAL=CSAdminKitServer,CSAdminKitConsole,KSNProxy,Microsoft_VC90_CRT_x86,Microsoft_VC100_CRT_x86`
NETRANGETYPE	Размер сети	• NRT_1_100 – от 1 до 100 устройств • NRT_100_1000 – от 100 до 1000 устройств • NRT_GREATER_1000 – более 1000 устройств
SRV_ACCOUNT_TYPE	Способ задания пользователя для работы службы Сервера администрирования	• SrvAccountDefault – учетная запись пользователя будет создана автоматически • SrvAccountUser – учетная запись пользователя задана вручную
SERVERACCOUNTNAME	Имя пользователя для службы	
SERVERACCOUNTPWD	Пароль пользователя для службы	
DBTYPE		• MySQL • MSSQL
MYSQLSERVERNAME	Полное имя mysql-сервера	
MYSQLSERVERPORT	Номер порта для подключения к	

Свойство MSI	Описание	Возможные значения
	mysql-серверу	
MYSQLDBNAME	Имя базы данных mysql-сервера	
MYSQLACCOUNTNAME	Имя пользователя для подключения к базе mysql-сервера	
MYSQLACCOUNTPWD	Пароль пользователя для подключения к базе mysql-сервера	
MSSQLCONNECTIONTYPE	Тип использования базы данных MSSQL	• InstallMSSEE – инсталлировать из пакета • ChooseExisting –использовать установленный сервер
MSSQLSERVERNAME	Полное имя экземпляра SQL Server	
MSSQLDBNAME	Имя базы данных SQL Server	
MSSQLAUTHTYPE	Способ аутентификации при подключении к SQL Server	• Windows • SQLServer
MSSQLACCOUNTNAME	Имя пользователя для подключения к SQL Server в режиме SQLServer	
MSSQLACCOUNTPWD	Пароль пользователя для подключения к SQL Server в режиме	

Свойство MSI	Описание	Возможные значения
	SQLServer	

CREATE_SHARE_TYPE	Способ задания папки общего доступа	• Create – создать новую папку общего доступа. В этом случае должны быть заданы свойства:
		  • SHARELOCALPATH – путь к локальной папке
		  • SHAREFOLDERNAME – сетевое имя папки
		• Пусто – должно быть задано свойство EXISTSHAREFOLDERNAME

EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа	
SERVERPORT	Номер порта для подключения к Серверу администрирования	
SERVERSSLPORT	Номер порта для установки SSL-соединения с Сервером администрирования	
SERVERADDRESS	Адрес Сервера администрирования	

Свойство MSI	Описание	Возможные значения
SERVERCERT2048BITS	Длина ключа для сертификата Сервера администрирования (в битах)	• 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит • 0 – длина ключа для сертификата Сервера администрирования составляет 1024 бит • Если параметр не задан, длина ключа для сертификата Сервера администрирования составляет 1024 бит
MOBILESERVERADDRESS	Адрес Сервера администрирования для подключения мобильных устройств; игнорируется, если не выбран компонент MobileSupport	

Параметры установки Агента администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Агента администрирования. Все параметры являются опциональными, кроме SERVERADDRESS.

Таблица 5. Свойства MSI

Свойство MSI	Описание	Возможные значения
DONT_USE_ANSWER_FILE	Читать параметры установки из файла ответов	• 1 • Пусто
INSTALLDIR	Папка установки	

Свойство MSI	Описание	Возможные значения
SERVERADDRESS	Адрес Сервера администрирования (обязательный параметр)	
SERVERPORT	Номер порта подключения к Серверу администрирования	
SERVERSSLPORT	Номер порта для SSL-соединения	
USESSL	Использовать ли SSL-соединение	• 1 • Пусто
OPENUDPPORT	Открыть ли UDP-порт	• 1 • Пусто
UDPPORT	Номер UDP-порта	
USEPROXY	Использовать ли прокси-сервер	• 1 • Пусто
PROXYADDRESS	Адрес прокси-сервера	
PROXYPORT	Номер порта для подключения к прокси-серверу	
PROXYLOGIN	Учетная запись для подключения к прокси-серверу	
PROXYPASSWORD	Пароль учетной записи для подключения к прокси-серверу. Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.	

Свойство MSI	Описание	Возможные значения
GATEWAYMODE	Режим использования шлюза соединения	• 0 – не использовать шлюз соединений • 1 – использовать данный Агент администрирования в качестве шлюза соединений • 2 – подключаться к Серверу администрирования через шлюз соединений
GATEWAYADDRESS	Адрес шлюза соединений	
CERTSELECTION	Способ получения сертификата	• GetOnFirstConnection – получить сертификат от Сервера администрирования • GetExistent – задать существующий сертификат. Если выбран этот вариант, должно быть задано свойство CERTFILE
CERTFILE	Путь к файлу сертификата	
VMVDI	Включить динамический режим для VDI	• 1 • Пусто
LAUNCHPROGRAM	Запускать ли службу Агента администрирования после установки	• 1 • Пусто

Виртуальная инфраструктура

Kaspersky Security Center поддерживает работу с виртуальными машинами. Поддерживается установка Агента администрирования и программы защиты на каждую виртуальную машину и защита виртуальных машин на уровне гипервизора. В первом случае для защиты виртуальных машин может использоваться как обычная программа защиты, так и Kaspersky Security для виртуальных сред / Легкий агент (см. http://support.kaspersky.ru/ksv3). Во втором случае для защиты виртуальных машин используется Kaspersky Security для виртуальных сред / Защита без агента (см. http://support.kaspersky.com/ksv).

Начиная с версии 10 MR1, Kaspersky Security Center поддерживает откат виртуальных машин в предыдущее состояние (см. раздел «Поддержка отката файловой системы для устройств с Агентом администрирования» на стр. 79).

В этом разделе

Рекомендации по снижению нагрузки на виртуальные машины

В случае инсталляции Агента администрирования на виртуальную машину следует рассмотреть возможность отключения той части функциональности Kaspersky Security Center, которая малополезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, целесообразно выполнить следующие действия:

- если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**) установить флажок **Оптимизировать параметры для VDI (Virtual Desktop Infrastructure)**;
- если выполняется интерактивная установка с помощью мастера, в окне мастера установить флажок **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Установка флажков изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Консоли администрирования.

Поддержка динамических виртуальных машин

Kaspersky Security Center поддерживает динамические виртуальные машины. Если в сети предприятия развернута виртуальная инфраструктура, то в некоторых случаях могут использоваться динамические (временные) виртуальные машины. Такие машины создаются с уникальными именами из заранее подготовленного администратором шаблона. Пользователь работает с созданной машиной некоторое время, а после выключения виртуальная машина удаляется из виртуальной инфраструктуры. Если в сети предприятия развернут Kaspersky Security Center, то виртуальная машина с установленным на ней Агентом администрирования добавляется в базу данных Сервера администрирования. После выключения виртуальной машины запись о ней должна быть также удалена и из базы данных Сервера администрирования.

Чтобы функциональность автоматического удаления записей о виртуальных машинах работала, при установке Агента администрирования на шаблон, из которого будут созданы динамические виртуальные машины, нужно установить флажок **Включить динамический режим для VDI**:

- в случае удаленной установки – в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**);
- в случае интерактивной установки – в окне мастера установки Агента администрирования.

> Флажок **Включить динамический режим для VDI** не следует устанавливать при установке Агента администрирования на физические устройства.

Если нужно, чтобы события с динамических виртуальных машин сохранялись на Сервере администрирования некоторое время после удаления машин, то следует в окне свойств Сервера администрирования в разделе **Хранение событий** установить флажок **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

Поддержка копирования виртуальных машин

Копирование виртуальной машины с установленным на нее Агентом администрирования или ее создание из шаблона с установленным Агентом администрирования эквивалентно развертыванию Агентов администрирования захватом и копированием образа жесткого диска. Поэтому, в общем случае, при копировании виртуальных машин нужно выполнять те же действия, что и при развертывании копированием образа диска.

Однако в описанных ниже двух случаях Агент администрирования обнаруживает факт копирования автоматически. Поэтому выполнять сложные действия, описанные в разделе «Развертывание захватом и копированием жесткого диска устройства», не обязательно:

- При установке Агента администрирования был установлен флажок **Включить динамический режим для VDI**: после каждой перезагрузки операционной системы такая виртуальная машина будет считаться новым устройством, независимо от факта ее копирования.
- Используется один из следующих гипервизоров: VMware™, HyperV® или Xen®: Агент администрирования определит факт копирования виртуальной машины по изменившимся идентификаторам виртуального аппаратного обеспечения.

Анализ изменений виртуального аппаратного обеспечения не абсолютно надежен. Прежде чем широко использовать данный метод, следует предварительно проверить его работоспособность на небольшом количестве виртуальных машин для используемой на предприятии версии гипервизора.

Поддержка отката файловой системы для устройств с Агентом администрирования

Kaspersky Security Center является распределенной программой. Откат файловой системы в предыдущее состояние на одном из устройств с установленным Агентом администрирования приведет к рассинхронизации данных и неправильной работе Kaspersky Security Center.

Откат файловой системы (или ее части) в предыдущее состояние может происходить в следующих случаях:

- при копировании образа жесткого диска;
- при восстановлении состояния виртуальной машины средствами виртуальной инфраструктуры;
- при восстановлении данных из резервной копии или точки восстановления.

Для Kaspersky Security Center критичны только те сценарии, при которых стороннее программное обеспечение на устройствах с установленным Агентом администрирования затрагивает папку %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\. Поэтому, при наличии возможности, следует всегда исключать эту папку из процедуры восстановления.

Поскольку на ряде предприятий регламент работы предполагает выполнение отката состояния файловой системы устройств, в Kaspersky Security Center, начиная с версии 10 MR1 (Сервер администрирования и Агенты администрирования должны быть версии 10 MR1 или выше), была добавлена поддержка обнаружения отката файловой системы на устройствах с установленным Агентом администрирования. В случае обнаружения такие устройства автоматически переподключаются к Серверу администрирования с полной очисткой и полной синхронизацией данных.

> В Kaspersky Security Center 10 MR1 поддержка обнаружения отката файловой системы по умолчанию выключена.
>
> Для включения этой функции следует на устройстве с Сервером администрирования импортировать в Реестр представленный ниже reg-файл и перезапустить службу Сервера администрирования.

Операционная система на устройстве с установленным Сервером администрирования (32-разрядная):

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]

"KLSRV_HST_VM_REVERT_DETECTION"=dword:00000001
```

Операционная система на устройстве с установленным Сервером администрирования (64-разрядная):

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\ServerFlags]

"KLSRV_HST_VM_REVERT_DETECTION"=dword:00000001
```

В Kaspersky Security Center 10 Service Pack 2 поддержка обнаружения отката файловой системы включена по умолчанию.

Следует при любой возможности избегать отката папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ на устройствах с установленным Агентом администрирования, так как полная повторная синхронизация данных требует большого количества ресурсов.

Для устройства с установленным Сервером администрирования откат состояния системы недопустим. Недопустимым также является откат в предыдущее состояние базы данных, используемой Сервером администрирования.

Восстановить состояние Сервера администрирования из резервной копии можно только при помощи штатной утилиты klbackup (см. раздел «Резервное копирование и восстановление параметров Сервера администрирования» на стр. 41).

Настройка профилей соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также «устройства») может понадобиться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Использование различных адресов одного и того же Сервера администрирования

> Описанное ниже применимо только для Kaspersky Security Center 10 SP1 и выше.

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети предприятия, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования (раздел **Сеть**, вложенный раздел **Подключение**) нужно добавить профиль подключения к Серверу администрирования из интернета. В окне создания профиля необходимо снять флажок **Использовать только для получения обновлений** и установить флажок **Синхронизировать параметры подключения с параметрами Сервера**, указанными в этом профиле. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center вида Доступ из интернета: Агент администрирования в режиме шлюза в демилитаризованной зоне), в профиле подключения следует указать адрес шлюза соединений в соответствующем поле.

Переключение между Серверами администрирования в зависимости от текущей сети

> Описанное ниже применимо для Kaspersky Security Center 10 MR1 и выше.

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования следует создать профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения следует указать адреса соответствующих Серверов администрирования и установить либо снять флажок **Использовать только для получения обновлений**:

- установить флажок, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- снять флажок, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая «домашний офис». Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

См. также

Предоставление доступа к Серверу администрирования из интернета 12

Развертывание функциональности Управление мобильными устройствами

В этом разделе

Подключение KES-устройств к Серверу администрирования

В зависимости от способа подключения устройств к Серверу администрирования существует две схемы развертывания Kaspersky Mobile Device Management для KES-устройств:

- схема развертывания с использованием прямого подключения устройств к Серверу администрирования;
- схема развертывания с использованием Forefront® Threat Management Gateway (TMG).

Прямое подключение устройств к Серверу администрирования

KES-устройства могут напрямую подключаться к порту 13292 Сервера администрирования.

В зависимости от способа аутентификации существуют два варианта подключения KES-устройств к Серверу администрирования:

- подключение устройств с использованием пользовательского сертификата;
- подключение устройств без пользовательского сертификата.

Подключение устройства с использованием пользовательского сертификата

При подключении устройства с использованием пользовательского сертификата происходит привязка этого устройства к учетной записи пользователя, для которой средствами Сервера администрирования назначен соответствующий сертификат.

В этом случае будет использована двусторонняя аутентификация SSL (2-way SSL authentication, mutual authentication). Как Сервер администрирования, так и устройство будут аутентифицированы с помощью сертификатов.

Подключение устройства без пользовательского сертификата

При подключении устройства без пользовательского сертификата оно не будет привязано ни к одной учетной записи пользователя на Сервере администрирования. Но при получении устройством любого сертификата будет произведена привязка этого устройства к пользователю, которому средствами Сервера администрирования назначен соответствующий сертификат.

При подключении устройства к Серверу администрирования будет использована односторонняя SSL-аутентификация (1-way SSL authentication), при которой только Сервер администрирования аутентифицируется с помощью сертификата. После получения устройством пользовательского сертификата, тип аутентификации будет изменен на двустороннюю аутентификацию SSL (2-way SSL authentication, mutual authentication (см. раздел «Предоставление доступа к Серверу администрирования из интернета» на стр. 12)).

Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)

Схема подключения KES-устройств к Серверу администрирования с использованием Kerberos Constrained Delegation (KCD) предполагает:

- интеграцию с Microsoft Forefront Threat Management Gateway (далее TMG);
- использование принудительного делегирования Kerberos Constrained Delegation (далее KCD) для аутентификации мобильных устройств;
- интеграцию с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) для использования пользовательских сертификатов.

При использовании этой схемы подключения следует учесть следующее:

- Тип подключения KES-устройств к TMG должен быть «2-way SSL authentication», то есть устройство должно подключаться к TMG по своему пользовательскому сертификату. Для этого в инсталляционный пакет Kaspersky Endpoint Security для Android, который установлен на устройстве, необходимо интегрировать пользовательский сертификат. Этот KES-пакет должен быть создан Сервером администрирования специально для данного устройства (пользователя).
- Вместо серверного сертификата по умолчанию для мобильного протокола следует указать особый (кастомизированный) сертификат:
  1. В окне свойств Сервера администрирования в разделе **Параметры** установить флажок **Открывать порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.
  2. В открывшемся окне указать тот же сертификат, что задан на TMG при публикации точки доступа к мобильному протоколу на Сервере администрирования.

- Пользовательские сертификаты для KES-устройств должны выписываться доменным Certificate Authority (CA). Причем, следует учесть, что если в домене несколько корневых CA, то пользовательские сертификаты должны быть выписаны тем CA, который прописан в публикации на TMG.

  Обеспечить соответствие пользовательского сертификата заявленному выше требованию возможно несколькими способами:

  - Указать особый пользовательский сертификат в мастере создания инсталляционных пакетов и в мастере установки сертификатов.
  - Интегрировать Сервер администрирования с доменным PKI и настроить соответствующий параметр в правилах выписки сертификатов:

    1. В Консоли администрирования в рабочей области папки **Управление мобильными устройствами / Сертификаты** по ссылке **Интегрировать с инфраструктурой открытых ключей** перейдите в окно **Правила выписки сертификатов**.
    2. В разделе **Интеграция с PKI** настройте интеграцию с инфраструктурой открытых ключей.
    3. В разделе **Выпуск сертификатов общего типа** укажите источник сертификатов.

См. разделы:

- Интеграция с PKI (Public Key Infrastructure) (см. раздел «Интеграция с Public Key Infrastructure» на стр. 90);
- Предоставление доступа к Серверу администрирования из интернета (на стр. 12).

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- точка доступа к мобильному протоколу на стороне Сервера администрирования поднята на 13292 порте;
- имя устройства с TMG – tmg.mydom.local;
- имя устройства с Сервером администрирования – ksc.mydom.local;
- имя внешней публикации точки доступа к мобильному протоколу – kes4mob.mydom.global.

Доменная учетная запись для Сервера администрирования

Необходимо создать доменную учетную запись (например, KSCMobileSrvcUsr), под которой будет работать служба Сервера администрирования. Указать учетную запись для службы Сервера администрирования можно при установке Сервера администрирования или с помощью утилиты klsrvswch. Утилита klsrvswch расположена в папке установки Сервера администрирования.

Указать доменную учетную запись необходимо по следующим причинам:

- функциональность по управлению KES-устройствами является неотъемлемой частью Сервера администрирования;
- для правильной работы принудительного делегирования (KCD) принимающая сторона, которой является Сервер администрирования, должна работать под доменной учетной записью.

Service Principal Name для http/kes4mob.mydom.local

В домене под учетной записью KSCMobileSrvcUsr требуется прописать Service Principal Name (SPN) для публикации сервиса мобильного протокола на 13292 порту устройства с Сервером администрирования. Для устройства kes4mob.mydom.local с Сервером администрирования это будет выглядеть следующим образом:

setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr

Настройка доменных свойств устройства с TMG (tmg.mydom.local)

Для делегирования трафика нужно доверить устройство с TMG (tmg.mydom.local) службе, определенной по SPN (http/kes4mob.mydom.local:13292).

Чтобы доверить устройство с TMG службе, определенной по SPN (http/kes4mob.mydom.local:13292), администратор должен выполнить следующие действия:

1. В оснастке MMC «Active Directory Users and Computers» необходимо выбрать устройство с установленным TMG (tmg.mydom.local).
2. В свойствах устройства на закладке **Delegation** для переключателя **Trust this computer for delegation to specified service only** выбрать вариант **Use any authentication protocol**.
3. В список **Services to which this account can present delegated credentials** добавить SPN http/kes4mob.mydom.local:13292.

Особый (кастомизированный) сертификат для публикации (kes4mob.mydom.global)

Для публикации мобильного протокола Сервера администрирования требуется выписать особый (кастомизированный) сертификат на FQDN kes4mob.mydom.global и указать его взамен серверного сертификата по умолчанию в параметрах мобильного протокола Сервера администрирования в Консоли администрирования. Для этого в окне свойств Сервера администрирования в разделе **Параметры** необходимо установить флажок **Открывать порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.

Следует учесть, что в контейнере с серверным сертификатом (файл с расширением p12 или pfx) должна также присутствовать цепочка корневых сертификатов (публичные части).

Настройка публикации на TMG

На TMG для трафика, идущего со стороны мобильного устройства на 13292 порт kes4mob.mydom.global, необходимо настроить KCD на SPN http/kes4mob.mydom.local:13292 с использованием серверного сертификата, выписанного для FQND kes4mob.mydom.global. При этом следует учесть, что как на публикации, так и на публикуемой точке доступа (13292 порт Сервера администрирования) должен быть один и тот же серверный сертификат.

Использование Google Firebase Cloud Messaging

Для обеспечения своевременного реагирования KES-устройств под управлением Android на команды администратора в свойствах Сервера администрирования следует включить использование сервиса Google™ Firebase Cloud Messaging (далее GFCM).

► *Чтобы включить использование GFCM, выполните следующие действия:*

1. В Консоли администрирования выберите узел **Управление мобильными устройствами**, папку **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В свойствах папки выберите раздел **Параметры сервиса Google Firebase Cloud Messaging**.
4. В полях **Идентификатор отправителя** и **Ключ API** укажите параметры GFCM: SENDER_ID и API Key.

Сервис GFCM работает на следующих диапазонах адресов:

- Со стороны KES-устройства необходим доступ на порты 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) следующих адресов:
  - google.com;
  - android.googleapis.com;
  - android.apis.google.com;
  - либо на все IP из списка Google's ASN of 15169.
- Со стороны Сервера администрирования необходим доступ на порт 443 (HTTPS) следующих адресов:
  - android.googleapis.com;
  - либо на все IP из списка «Google ASN 15169».

В случае если в Консоли администрирования в свойствах Сервера администрирования заданы параметры прокси-сервера (**Дополнительно / Настройки доступа к сети интернет**), то они будут использованы для взаимодействия с GFCM.

Настройка GFCM: получение SENDER_ID, API Key

Для настройки работы с GFCM администратор должен выполнить следующие действия:

1. Зарегистрироваться на портале google https://accounts.google.com.
2. Перейти на портал для разработчиков https://console.developers.google.com/project.
3. Создать новый проект по кнопке **Create Project**, указать имя проекта, указать ID.
4. Дождаться создания проекта.

   На первой странице проекта, в верхней части страницы, в поле **Project Number** указан искомый SENDER_ID.
5. Перейти в раздел **APIs & auth / APIs**, включить **Google Firebase Cloud Messaging for Android**.

6. Перейти в раздел **APIs & auth / Credentials**, нажать на кнопку **Create New Key**.

7. Нажать на кнопку **Server key**.

8. Если есть, задать ограничения, нажать на кнопку **Create**.

9. Получить API Key из свойств только что созданного ключа (поле **API key**).

Интеграция с Public Key Infrastructure

Интеграция с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) в первую очередь предназначена для упрощения выпуска доменных пользовательских сертификатов Сервером администрирования.

Администратор может назначить для пользователя доменный сертификат в Консоли администрирования. Это можно сделать одним из следующих способов:

- назначить пользователю особый (кастомизированный) сертификат из файла в мастере подключения нового устройства либо в мастере установки сертификатов;
- выполнить интеграцию с PKI и назначить PKI источником сертификатов для конкретного типа сертификатов либо для всех типов сертификатов.

Параметры интеграции с PKI доступны в рабочей области папки **Управление мобильными устройствами / Сертификаты** по ссылке **Интегрировать с инфраструктурой открытых ключей**.

Общий принцип интеграции с PKI для выпуска доменных сертификатов пользователей

В Консоли администрирования по ссылке **Интегрировать с инфраструктурой открытых ключей** в рабочей области папки **Управление мобильными устройствами / Сертификаты** следует задать доменную учетную запись, которая будет использована Сервером администрирования для выписки доменных пользовательских сертификатов посредством доменного CA (далее – учетная запись, под которой производится интеграция с PKI).

При этом следует учесть следующее:

- В параметрах интеграции с PKI существует возможность указать шаблон по умолчанию для всех типов сертификатов. Тогда как в правилах выпуска сертификатов (правила доступны в рабочей области папки **Управление мобильными устройствами / Сертификаты** по ссылке **Правила выпуска сертификатов)** присутствует возможность задать шаблон для каждого типа сертификата отдельно.

- На устройстве с установленным Сервером администрирования в хранилище сертификатов учетной записи, под которой производится интеграция с PKI, должен быть установлен специализированный сертификат Enrollment Agent (EA). Сертификат Enrollment Agent (EA) выписывает администратор доменного CA (Certificate Authority).

Учетная запись, под которой производится интеграция с PKI, должна соответствовать следующим критериям:

- Является доменным пользователем.

- Является локальным администратором устройства с установленным Сервером администрирования, с которого производится интеграция с PKI.

- Обладает правом **Вход в качестве службы**.

- Под этой учетной записью необходимо хотя бы один раз запустить устройство с установленным Сервером администрирования, чтобы создать постоянный профиль пользователя.

Веб-сервер Kaspersky Security Center

Веб-сервер Kaspersky Security Center (далее веб-сервер) – это компонент Kaspersky Security Center. Веб-сервер предназначен для публикации автономных пакетов установки, автономных инсталляционных пакетов для мобильных устройств, а также файлов из папки общего доступа.

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

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

Параметры Веб-сервера

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

Повседневная работа

В этом разделе

Цветовые индикаторы в Консоли администрирования

В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Securuity Center и управляемых устройств с помощью цветовых индикаторов. Индикаторы отображаются в рабочей области узла **Сервер администрирования** на закладке **Начало работы**. На закладке имеется шесть информационных блоков с цветовыми индикаторами. Каждый блок с индикатором отвечает за отдельную функциональную область Kaspersky Security Center (см. таблицу ниже).

Таблица 6. Области ответственности цветовых индикаторов в Консоли администрирования

Название блока	Область ответственности цветового индикатора
Развертывание	Установка Агента администрирования и программ защиты на устройства сети предприятия
Управление устройствами	Структура групп администрирования. Сканирование сети. Правила перемещения устройств
Защита устройств и поиск вирусов	Функции программы защиты: состояние защиты, поиск вирусов
Обновление	Обновления и патчи
Мониторинг	Состояние защиты
Сервер администрирования	Функции и свойства Сервера администрирования

Индикатор может быть одного из пяти цветов (см. таблицу ниже). Цвет индикатора зависит от текущего состояния Kaspersky Security Center и от зарегистрированных событий.

Таблица 7. Цветовые кодировки индикаторов

Состояние	Цвет индикатора	Значение цвета индикатора
Информационное	Зеленый	Вмешательство администратора не требуется
Предупреждение	Желтый	Требуется вмешательство администратора
Критическое	Красный	Имеются серьезные проблемы. Требуется вмешательство администратора для их решения
Информационное	Голубой	Зарегистрированы события, не связанные с потенциальными или фактическими угрозами для безопасности управляемых устройств
Информационное	Серый	Информация о событиях недоступна или еще не получена

Следует поддерживать все индикаторы блоков зелеными.

Удаленный доступ к управляемым устройствам

В этом разделе

Доступ к локальным задачам и статистике, флажок «Не разрывать соединение с Сервером администрирования»

По умолчанию в Kaspersky Security Center нет постоянных соединений между управляемыми устройствами и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Продолжительность периода такой синхронизации (по умолчанию 15 минут) задается в политике Агента администрирования. Если необходима досрочная синхронизация (например, для ускорения применения политики), то Сервер администрирования посылает Агенту администрирования подписанный сетевой пакет на порт UDP 15000. Если доступ по UDP от Сервера администрирования к управляемому устройству по какой-то причине невозможен, то синхронизация произойдет при очередном периодическом подключении Агента администрирования к Серверу в течение периода синхронизации.

Некоторые операции не могут быть выполнены без досрочного подключения Агента администрирования к Серверу: запуск и остановка локальных задач, получение статистики управляемого продукта (программы защиты или Агента администрирования), создание тоннеля и прочее. Для решения этой проблемы в свойствах управляемого устройства (раздел **Общие**) нужно установить флажок **Не разрывать соединение с Сервером администрирования**. Если управляемое устройство осуществляет доступ к Серверу администрирования не напрямую, а через агент обновлений, работающий в режиме «шлюза», то флажок следует установить в свойствах устройства, который является агентом обновлений и выполняет роль шлюза. Общее количество устройств с установленным флажком **Не разрывать соединение с Сервером администрирования** не может превышать 300.

Проверка времени соединения устройства с Сервером администрирования

При выключении устройства Агент администрирования уведомляет о выключении Сервер администрирования. В Консоли администрирования такое устройство отображается как выключенное. Однако Агенту удается уведомить Сервер администрирования не во всех случаях. Поэтому Сервер администрирования для каждого устройства периодически анализирует атрибут **Время последнего соединения** (значение атрибута отображается в Консоли администрирования в свойствах устройства в разделе **Общие**) и сопоставляет его с периодом синхронизации из действующих параметров Агента администрирования. Если устройство не выходило на связь более чем три периода синхронизации, то такое устройство отмечается как выключенное.

Форсирование синхронизации

Несмотря на то, что Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору нужно точно знать, что в данный момент времени для данного устройства синхронизация выполнена.

В контекстном меню управляемых устройств в Консоли администрирования устройства в пункте меню **Все задачи** имеется команда **Синхронизировать принудительно**. В Kaspersky Security Center 10 Service Pack 2 при выполнении этой команды в свойствах устройства устанавливается флажок **Назначена принудительная синхронизация**, затем Сервер администрирования пытается связаться с устройством. Если это удается, то выполняется принудительная синхронизация, и флажок снимается. В противном случае принудительная синхронизация и снятие флажка произойдет лишь после очередного выхода Агента администрирования на связь с Сервером. Исчезновение флажка является сигналом для администратора о том, что синхронизация выполнена.

Туннелирование

Kaspersky Security Center позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

В частности, туннелирование используется для подключения к удаленному рабочему столу: как для подключения к существующей сессии, так и для создания новой удаленной сессии.

Также туннелирование может быть использовано при помощи механизма внешних инструментов. В частности, администратор может запускать таким образом утилиту putty, VNC-клиент и прочие инструменты.

Приложения

В этом разделе содержится справочная и дополнительная информация, касающаяся использования Kaspersky Security Center:

- сведения об ограничениях текущей версии программы (максимальные количества управляемых устройств, политик, задач и прочее);
- аппаратные требования для установки Сервера администрирования и СУБД;
- справочная информация о количестве места на диске, необходимого для работы компонентов программы;
- справочная информация о среднесуточном объеме трафика между Агентом администрирования и Сервером администрирования;
- информация о решении типовых проблем, возникающих при использовании Kaspersky Security Center, в том числе о решении проблем с управлением мобильными устройствами пользователей.

В этом разделе

Ограничения Kaspersky Security Center

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center 10 Service Pack 2.

Таблица 8. Ограничения Kaspersky Security Center 10 Service Pack 2

Тип ограничения	Значение
Максимальное количество управляемых устройств	50 000
Максимальное количество устройств с установленным флажком **Не разрывать соединение с Сервером администрирования**	300
Максимальное количество групп администрирования	10 000
Максимальное количество хранимых событий	15 000 000
Максимальное количество политик	2000
Максимальное количество задач	2000
Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, устройств и групп безопасности)	1 000 000
Максимальное количество профилей в политике	100
Максимальное количество подчиненных Серверов у одного главного Сервера администрирования	500
Максимальное количество виртуальных Серверов администрирования	200
Максимальное количество устройств, которые может обслуживать один агент обновлений	500

Аппаратные требования для СУБД и Сервера администрирования

В таблицах ниже приведены минимальные аппаратные требования СУБД и Сервера администрирования для обслуживания 50 000 устройств.

Сервер администрирования и SQL Server находятся на одном устройстве

Таблица 9. Аппаратные требования к устройству

Процессор	8 ядер 2500 – 3000 МГц
Память	16 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит
Операционная система	Windows x86 – 64

Сервер администрирования и SQL Server находятся на разных устройствах

Таблица 10. Аппаратные требования к устройству с Сервером администрирования

Процессор	4 ядра 2500 – 3000 МГц
Память	8 ГБ
Жесткий диск	300 ГБ, желателен RAID
Сетевой адаптер	1 Гбит
Операционная система	Windows x86 – 64

Таблица 11. Аппаратные требования к устройству с SQL Server

Процессор	4 ядра 2500 – 3000 МГц
Память	16 ГБ
Жесткий диск	200 ГБ SATA RAID
Сетевой адаптер	1 Гбит
Операционная система	Windows x86-64

При этом сделаны следующие предположения:

- в сети предприятия назначены агенты обновлений, каждый из которых обслуживает по 100 – 200 устройств;
- задача резервного копирования сохраняет резервные копии на файловый ресурс, расположенный на отдельном сервере;
- период синхронизации Агентов администрирования настроен в соответствии с таблицей ниже.

Таблица 12. Период синхронизации Агентов администрирования

Период синхронизации, минуты	Количество управляемых устройств
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000

Оценка места на диске для агента обновлений

Для работы агента обновлений необходимо не менее 4 ГБ свободного места на диске.

При наличии на Сервере администрирования задач удаленной инсталляции, на устройстве с агентом обновлений дополнительно потребуется количество места на диске, равное суммарному размеру устанавливаемых инсталляционных пакетов.

При наличии на Сервере администрирования одного или нескольких экземпляров задачи установки обновлений (патчей) и закрытия уязвимостей, на устройстве с агентом обновлений дополнительно потребуется количество места на диске, равное удвоенному суммарному размеру всех устанавливаемых патчей.

Предварительный расчет места в базе данных и на диске для Сервера администрирования

Оценка места в базе данных Сервера администрирования

Место, которое будет занято в базе данных, можно приблизительно оценить по следующей формуле:

(200 * C + 2,3 * E + 2,5 * A), КБ

где:

«C»	Количество устройств.
«E»	Количество сохраняемых событий.
«A»	Суммарное количество объектов Active Directory: учетных записей устройств; учетных записей пользователей; учетных записей групп безопасности; подразделений Active Directory. Если сканирование Active Directory выключено, то «A» следует считать равным нулю.

Если Сервер администрирования распространяет обновления Windows (играет роль WSUS-сервера), то в базе данных дополнительно потребуется 2,5 ГБ.

Следует учитывать, что в ходе работы в базе данных всегда образуется так называемое «незанятое пространство» (unallocated space). Поэтому реальный размер файла базы данных (по умолчанию файл KAV.MDF в случае использования СУБД «SQL Server») часто оказывается, примерно в два раза больше, чем занятое в базе данных место.

Размер журнала транзакций (по умолчанию файл KAV_log.LDF в случае использования СУБД «SQL Server») может достигать 2 ГБ.

Оценка места на диске для устройства с Сервером администрирования

Место на диске в директории %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit на устройстве с Сервером администрирования можно приблизительно оценить по формуле:

(220 * C + 0,15 * E + 0,17 * A), КБ

Значения переменных «C», «E» и «A» см. в таблице выше.

Обновления

В папке общего доступа требуется не менее 4 ГБ для хранения обновлений.

Инсталляционные пакеты

При наличии на Сервере администрирования инсталляционных пакетов в папке общего доступа дополнительно потребуется место, равное суммарному размеру имеющихся инсталляционных пакетов.

Задачи удаленной установки

При наличии на Сервере администрирования задач удаленной установки на устройстве с Сервером администрирования дополнительно потребуется количество места на диске (в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit), равное суммарному размеру устанавливаемых инсталляционных пакетов.

Патчи

Если Сервер администрирования используется для установки патчей, то потребуется дополнительное место на диске:

- В папке для хранения патчей – количество места, равное суммарному размеру всех скачанных патчей. Папкой для хранения патчей по умолчанию является %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\wusfiles. Папка может быть изменена при помощи утилиты klsrvswch. Если Сервер администрирования используется в качестве WSUS, то рекомендуется зарезервировать под эту папку не менее 100 ГБ.
- В директории %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit – количество места, равное суммарному размеру патчей, на которые ссылаются имеющиеся экземпляры задачи установки обновлений (патчей) и закрытия уязвимостей.

Оценка трафика между Агентом администрирования и Сервером администрирования

В таблице ниже приведен среднесуточный трафик между Сервером администрирования Kaspersky Security Center 10 MR1 сборка 10.1.249 и управляемым устройством (на устройстве установлены Агент администрирования Kaspersky Security Center 10 MR1 сборка 10.1.249 и Kaspersky Endpoint Security 10 MR1 сборка 10.2.1.23).

Таблица 13. Среднесуточный трафик: Kaspersky Security Center 10 MR1

	От Сервера к управляемому устройству (download)	**От управляемого устройства к Серверу (upload)**
Средний ежесуточный трафик с параметрами задачи обновления по умолчанию	27 МБ	2,7 МБ
Средний ежесуточный трафик с выключенной задачей обновления	0,8 МБ	1 МБ

В таблице ниже приведен среднесуточный трафик между Сервером администрирования Kaspersky Security Center 10 Service Pack 2 и управляемым устройством (установлены Агент администрирования Kaspersky Security Center 10 Service Pack 2 и Kaspersky Endpoint Security 10 Service Pack 1).

Таблица 14. Среднесуточный трафик: Kaspersky Security Center 10 Service Pack 2

	От Сервера к управляемому устройству (download)	**От управляемого устройства к Серверу (upload)**
Средний ежесуточный трафик с параметрами задачи обновления по умолчанию	17 МБ	3,5 МБ
Средний ежесуточный трафик с выключенной задачей обновления	0,8 МБ	1 МБ

Решение проблем

В этом разделе содержится информация о наиболее распространенных ошибках и проблемах при развертывании и использовании Kaspersky Security Center, а также рекомендации по решению проблем.

В этом разделе

Проблемы при удаленной установке программ

В таблице ниже перечислены проблемы, возникающие при удаленной установке программ, и типовые причины возникновения этих проблем.

Таблица 15. Проблемы при удаленной установке программ

Проблема	Типовая причина проблемы и вариант решения
Недостаточно прав для установки	Учетная запись, под которой запущена установка, не имеет достаточно прав для выполнения операций, необходимых для установки программы.
Недостаточно места на диске	Недостаточно свободного места на диске для завершения установки. Освободите место на диске и повторите операцию.
Произошла незапланированная перезагрузка ОС	Во время установки произошла незапланированная перезагрузка ОС, точный результат установки может быть неизвестен. Проверьте правильность параметров запуска инсталляционного приложения или обратитесь в Службу технической поддержки.
Не найден необходимый файл	В инсталляционном пакете не найден необходимый файл. Проверьте целостность используемого инсталляционного пакета.

Проблема	Типовая причина проблемы и вариант решения
Несовместимая платформа	Инсталляционный пакет не предназначен для данной платформы. Используйте соответствующий инсталляционный пакет.
Несовместимая программа	На устройстве установлена программа, несовместимая с устанавливаемой программой. Перед установкой удалите все программы, входящие в список несовместимых.
Недостаточные системные требования	Инсталляционный пакет требует наличия в системе дополнительного программного обеспечения. Проверьте соответствие конфигурации системы системным требованиям устанавливаемой программы.
Незавершенная установка	Предыдущая установка или удаление программы не было штатно завершено. Для завершения предыдущей установки или удаления программы, выполненного на данном устройстве, необходимо перезагрузить ОС и повторить процесс установки.
Не та версия инсталляционного приложения	Установка данного инсталляционного пакета не поддерживается версией инсталляционного приложения, установленного на устройстве.
Инсталляция уже запущена	На устройстве уже запущена установка другого приложения.
Не удалось открыть инсталляционный пакет	Не удалось открыть инсталляционный пакет. Возможные причины: пакет отсутствует, пакет повреждён, недостаточно прав для доступа к пакету.
Несовместимая локализация	Инсталляционный пакет не предназначен для установки на данную локализацию ОС.
Установка запрещена политикой	Установка программ на данном устройстве запрещена политикой.

Проблема	Типовая причина проблемы и вариант решения
Ошибка записи файла	Во время установки программы произошла ошибка записи. Проверьте наличие прав у учётной записи, под которой выполняется установка, и наличие свободного места на диске.
Неверный пароль деинсталляции	Пароль для удаления программы задан неверно.
Недостаточные аппаратные требования	Аппаратные требования системы не удовлетворяют требованиям программы (объем оперативной памяти, свободное место на диске и так далее).
Недопустимый каталог установки	Установка программы в указанный каталог запрещена политикой инсталляционного приложения.
Требуется повторная попытка установки после перезагрузки устройства	Требуется повторный запуск инсталлятора программы после перезагрузки устройства.
Для продолжения установки требуется перезагрузка устройства	Для продолжения работы инсталлятора продукта требуется перезагрузка устройства.

Неверно выполнено копирование образа жесткого диска

Если копирование образа жесткого диска с установленным Агентом администрирования было выполнено без учета правил развертывания, часть устройств в Консоли администрирования может отображаться как один значок устройства, постоянно меняющий имя.

Можно использовать следующие способы решения этой проблемы:

- Удаление Агента администрирования.

  Этот способ является самым надежным. На устройствах, которые были скопированы из образа неправильно, нужно при помощи сторонних средств удалить Агент администрирования, а затем установить его заново. Удаление Агента администрирования не может быть выполнено средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

- Запуск утилиты klmover с ключом «-dupfix».

  На проблемных устройствах (на всех, которые были скопированы из образа неправильно) необходимо при помощи сторонних средств однократно запустить утилиту klmover с ключом «-dupfix» (klmover -dupfix), расположенную в папке установки Агента администрирования. Запуск утилиты не может быть выполнен средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

  Затем следует удалить значок, на который отображались проблемные устройства до запуска утилиты.

- Ужесточение правила обнаружения неправильно скопированных устройств.

  > Этот способ можно использовать только в случае, если установлены Сервер администрирования и Агенты администрирования версии 10 SP1 или новее.

  Следует ужесточить правило обнаружения неправильно скопированных Агентов администрирования таким образом, чтобы изменение NetBIOS-имени устройства приводило к автоматической «починке» таких Агентов администрирования (предполагается, что скопированные устройства имеют различные NetBIOS-имена).

На устройстве с Сервером администрирования нужно импортировать в Реестр представленный ниже reg-файл и перезапустить службу Сервера администрирования.

- Если на устройстве с Сервером администрирования установлена 32-разрядная операционная система:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]

"KLSRV_CheckClones"=dword:00000003
```

- Если на устройстве с Сервером администрирования установлена 64-разрядная операционная система:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\ServerFlags]

"KLSRV_CheckClones"=dword:00000003
```

Проблемы с KES-устройствами

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием KES-устройств, а также о способах их решения.

В этом разделе

Портал support.kaspersky.com

Информация о проблемах, возникающих при работе с KES-устройствами, приведена в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.com/ks10mob.

Проверка настроек сервиса Google Firebase Cloud Messaging

Проверка настроек сервиса Google Firebase Firebase Cloud Messaging может быть выполнена на портале Google https://code.google.com/apis/console/#project:[YOUR.

Проверка доступности сервиса Google Firebase Cloud Messaging

Для проверки доступности сервиса Google Firebase Cloud Messaging со стороны Kaspersky Security Center (см. раздел «Использование Google Firebase Cloud Messaging» на стр. 88) вы можете использовать команду утилиты Telnet:

```
telnet android.googleapis.com 443
```

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, 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).

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apple, iPhone, – товарные знаки Apple Inc., зарегистрированные в США и других странах.

Xen – товарный знак Citrix Systems, Inc. и / или дочерних компаний, зарегистрированный в патентном офисе США и других стран.

Android, Google – товарные знаки Google, Inc.

JavaScript– зарегистрированный товарный знак Oracle Corporation и / или ее аффилированных компаний.

Active Directory, ActiveSync, Forefront, Microsoft, HyperV, SQL Server, Windows, Windows PowerShell – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

VMware и ESXi – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.