Kaspersky Security Center 10

Лучшие практики

ВЕРСИЯ ПРОГРАММЫ: 10 SERVICE PACK 1

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

Дата редакции документа: 14.09.2015

http://www.kaspersky.ru
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. 9)

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, об управлении мобильными устройствами и о NAC.

Развертывание и первоначальная настройка (см. стр. 23)

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, о настройке и использовании NAC.

Повседневная работа (см. стр. 80)

Этот раздел содержит информацию о повседневном использовании программы. В разделе представлена информация о работе с удаленным доступом к компьютерам, с мобильными устройствами, а также типовые сценарии использования NAC для контроля активности сетевых устройств.

Обращение в Службу технической поддержки (см. стр. 101)

Этот раздел содержит информацию о способах получения технической поддержки и о том, какие условия требуются для получения помощи от Службы технической поддержки.

АО «Лаборатория Касперского» (см. стр. 103)

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

Уведомления о товарных знаках

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: ...	Примеры приведены в блоках на желтом 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 компьютеров;
- наличие организационно или географически обособленных подразделений (офисов, филиалов);
- наличие обособленных сетей, связанных узкими каналами;
- необходимость доступа к Серверу администрирования из интернета (см. раздел Предоставление доступа к Серверу администрирования из интернета (на стр. 10).)

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

Если в составе предприятия есть крупные географически удаленные офисы (филиалы) с собственными администраторами, целесообразно разместить в этих офисах Серверы администрирования. В противном случае такие офисы следует рассматривать как обособленные сети, связанные узкими каналами.

См. раздел Типовая конфигурация: несколько крупных офисов с собственными администраторами (на стр. 14).

При наличии обособленных сетей, связанных узкими каналами, в целях экономии трафика в таких сетях следует один или несколько Агентов администрирования назначить агентами обновлений из расчета один агент обновлений на 100 – 200 клиентских компьютеров. В этом случае все компьютеры обособленной сети будут получать обновления с таких «локальных центров обновлений». Сами же агенты обновлений могут загружать обновления как с Сервера администрирования (поведение по умолчанию), так и с размещенных в интернете серверов «Лаборатории Касперского».

См. раздел Типовая конфигурация: множество небольших удаленных офисов (на стр. 14).

В разделе Типовые конфигурации Kaspersky Security Center (на стр. 13) приведены подробные описания типовых конфигураций Kaspersky Security Center. При планировании развертывания следует, в зависимости от структуры предприятия, выбрать наиболее подходящую типовую конфигурацию.

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

- для инспекции SSL трафика посредством SSL termination proxy или для использования Reverse Proxy;
- для интеграции с инфраструктурой открытых ключей (PKI) предприятия;
- для задания желательных значений полей сертификата;
- для обеспечения желаемой криптографической стойкости сертификата.

См. раздел Задание сертификата Сервера администрирования (на стр. 27).

В этом разделе

О выборе СУБД для Сервера администрирования

При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством компьютеров, 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 тысяч компьютеров. Если Сервер администрирования обслуживает больше 10 тысяч компьютеров, 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.

Если Сервер администрирования обслуживает не более 10 тысяч компьютеров, в качестве СУБД может быть также использован MySQL 5.0.

См. также

Предоставление доступа к Серверу администрирования из интернета

В ряде случаев необходимо предоставить доступ к Серверу администрирования из интернета:

- для управления компьютерами (ноутбуками) автономных пользователей;
- для управления компьютерами, находящимися в удаленных офисах;
- при взаимодействии с главным или подчиненными Серверами администрирования, находящимися в удаленных офисах;
- для управления мобильными устройствами.

В этом разделе рассмотрены типичные способы обеспечения доступа к Серверу администрирования из интернета. Во всех случаях предоставления доступа к Серверу администрирования из интернета может понадобиться задать Серверу администрирования специальный сертификат (см. раздел «Задание сертификата Сервера администрирования» на стр. 27).

В этом разделе

Доступ из интернета: Сервер администрирования в локальной сети

Если Сервер администрирования располагается во внутренней сети предприятия, с помощью механизма «Port Forwarding» порт Сервера администрирования 13000 TCP делается доступным извне. Если требуется управление мобильными устройствами, то делается доступным извне порт 13292 TCP.

Доступ из интернета: Сервер администрирования в демилитаризованной зоне

Если Сервер администрирования располагается в демилитаризованной зоне сети предприятия, у него отсутствует доступ во внутреннюю сеть предприятия. Как следствие, возникают следующие ограничения:

- Сервер администрирования не может самостоятельно обнаруживать новые компьютеры.
- Сервер администрирования не может выполнять первоначальное развертывание Агента администрирования посредством push-инсталляции на компьютеры внутренней сети предприятия.

Речь идет только о первоначальной установке Агента администрирования. Последующие обновления версии Агента администрирования или установка антивируса уже могут быть выполнены Сервером администрирования. Однако первоначальное развертывание Агентов администрирования может быть выполнено иными средствами, например, при помощи групповых политик Microsoft® Active Directory®.

- Сервер администрирования не может посылать управляемым компьютерам уведомления на порт 15000 UDP, что не является критичным для функциональности Kaspersky Security Center.

- Сервер администрирования не может опрашивать Active Directory. Однако результаты опроса Active Directory не нужны в большинстве сценариев.

Если описанные выше ограничения критичны, они могут быть сняты при помощи агентов обновлений, размещенных в сети предприятия:

- Для выполнения первоначального развертывания на компьютеры без Агента администрирования следует предварительно установить Агент администрирования на один из компьютеров и назначить этот компьютер агентом обновлений. В результате первоначальная установка Агента администрирования на прочие компьютеры будет выполняться Сервером администрирования через этот агент обновлений.

- Для обнаружения новых компьютеров во внутренней сети предприятия и для опроса Active Directory следует на одном из агентов обновлений включить желаемые виды опроса сети.

- Для успешной отправки уведомлений управляемым компьютерам, размещенным во внутренней сети предприятия, на порт 15000 UDP, следует покрыть всю сеть предприятия агентами обновлений из расчета по 100 – 200 компьютеров на один агент обновлений. В свойствах назначенных агентов обновлений следует установить флажок **Не разрывать соединение с Сервером администрирования**. В результате Сервер администрирования будет иметь постоянную связь с агентами обновлений, а агенты обновлений смогут посылать уведомления на порт 15000 UDP компьютерам, размещенным во внутренней сети предприятия (см. раздел «Об агентах обновлений» на стр. 15).

Доступ из интернета: Агент администрирования в режиме шлюза в демилитаризованной зоне

Описанный ниже режим доступа применим для Kaspersky Security Center 10 Service Pack 1 и более поздних версий.

Сервер администрирования может располагаться во внутренней сети предприятия, а в демилитаризованной зоне сети может находиться компьютер с Агентом администрирования, работающим в режиме шлюза с обратным направлением подключения (Сервер администрирования устанавливает соединение с Агентом администрирования). В этом случае для организации доступа из интернета нужно выполнить следующие условия:

- На компьютер, находящийся в демилитаризованной зоне, следует установить Агент администрирования. При установке Агента администрирования в окне мастера установки **Шлюз соединений** выбрать вариант **Использовать в качестве шлюза соединений**.

- На Сервере администрирования следует создать отдельную группу администрирования, в свойствах которой назначить по адресу в качестве шлюза соединений указанный выше компьютер из демилитаризованной зоны. В эту группу администрирования не следует добавлять какие-либо компьютеры.

- Для Агентов администрирования, обращающихся к Серверу администрирования из интернета, при установке следует указать созданный выше шлюз с помощью параметра **Подключаться к Серверу через шлюз соединений**.

Для шлюза соединений, находящегося в демилитаризованной зоне, Сервер администрирования создает сертификат, подписанный сертификатом Сервера администрирования. Если администратор принял решение задать Серверу администрирования пользовательский сертификат, то это следует сделать до создания шлюза соединений в демилитаризованной зоне.

При наличии сотрудников с ноутбуками, которые могут подключаться к Серверу администрирования как из локальной сети, так и из интернета, может быть целесообразно создать в политике Агента администрирования правило переключения Агента администрирования.

Типовые конфигурации Kaspersky Security Center

В этом разделе описаны следующие типовые конфигурации размещения компонентов Kaspersky Security Center в сети предприятия:

- один офис;
- несколько крупных географически распределенных офисов с собственными администраторами;
- множество небольших географически распределенных офисов.

В этом разделе

Типовая конфигурация: один офис

В сети предприятия может быть 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. 88), так и в зависимости от общего количества управляемых компьютеров.

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

Серверы администрирования могут быть размещены как во внутренней сети, так и в демилитаризованной зоне, в зависимости от того, нужен ли доступ к Серверам администрирования из интернета.

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

Если Сервер администрирования обслуживает более 5 тысяч компьютеров, то с целью уменьшения нагрузки на сеть и Сервер администрирования желательно назначить в сегментах сети компьютеры–агенты обновлений, из расчета 100 – 200 управляемых компьютеров на один агент обновлений.

См. также

Типовая конфигурация: несколько крупных офисов с собственными администраторами

При наличии нескольких крупных удаленных офисов следует рассмотреть возможность размещения Серверов администрирования в каждом из офисов, по одному и или по несколько Серверов администрирования в каждом, в зависимости от количества клиентских компьютеров и доступного аппаратного обеспечения. В таком случае каждый из офисов может быть рассмотрен как «Типовая конфигурация: один офис». Для упрощения администрирования все Серверы администрирования следует объединить в иерархию, возможно, многоуровневую.

При наличии сотрудников, которые перемещаются между офисами вместе с компьютерами (ноутбуками), в политике Агента администрирования следует создать правила переключения Агента администрирования между Серверами администрирования.

См. также

Типовая конфигурация: один офис 13

Роль иерархии Серверов администрирования 15

Настройка профилей соединения для автономных пользователей 64

Типовая конфигурация: множество небольших удаленных офисов

Эта типовая конфигурация предусматривает один главный офис и множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Возможно, каждый из удаленных офисов находится за Network Address Translation (далее также NAT), то есть подключение из одного удаленного офиса в другой невозможно, офисы изолированы друг от друга.

В главном офисе следует поместить Сервер администрирования, а в остальных офисах назначить по одному или по несколько агентов обновлений. Если связь между офисами осуществляется через интернет, то может быть целесообразным 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 удаленном офисе часть компьютеров не имеет прямого доступа к Серверу администрирования (например, доступ к Серверу администрирования осуществляется через интернет, но доступ в интернет есть не у всех компьютеров), то агенты обновлений следует переключить в режим шлюза (Connection Gateway). В таком случае Агенты администрирования на компьютерах в удаленном офисе будут подключаться (с целью синхронизации) к Серверу администрирования не напрямую, а через шлюз.

Поскольку Сервер администрирования, скорее всего, не сможет опрашивать сеть в удаленном офисе, целесообразно возложить выполнение этой функции на один из агентов обновлений.

Сервер администрирования не сможет посылать уведомления на порт 15000 UDP управляемым компьютерам, размещенным за NAT в удаленном офисе. Для решения этой проблемы целесообразно включить в свойствах компьютеров, являющихся агентами обновлений, режим постоянного соединения с Сервером администрирования (флажок **Не разрывать соединение с Сервером администрирования**). Этот режим доступен, если общее количество агентов обновлений не превышает 200.

См. также

Предоставление доступа к Серверу администрирования из интернета 10

Об агентах обновлений 15

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 компьютера, являющегося агентом обновлений, должна быть создана задача ретрансляции.
- Устанавливать программное обеспечение на другие компьютеры, в том числе и выполнять первоначальное развертывание Агентов администрирования на компьютерах.
- Сканировать сеть с целью обнаружения новых компьютеров и обновления информации об уже известных компьютерах. 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.
- Оптимизировать трафик.
- Предоставить Серверу администрирования доступ к компьютерам в труднодоступных частях сети предприятия. Наличие агента обновлений в находящейся за NAT (по отношению к Серверу администрирования) сети позволяет Серверу администрирования выполнять следующие действия:
  - отправлять компьютерам уведомления по UDP;
  - сканировать сеть;
  - выполнять первоначальное развертывание.

Агент обновлений назначается на группу администрирования. В этом случае областью действия агента обновлений будут компьютеры, находящиеся в такой группе администрирования и всех ее подгруппах. При этом компьютер, являющийся агентом обновлений, не обязан находиться в группе администрирования, на которую он назначен.

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

См. также

Доступ из интернета: Агент администрирования в режиме шлюза в демилитаризованной зоне 12

Типовая конфигурация: множество небольших удаленных офисов 14

Построение структуры групп администрирования и назначение агентов обновлений 33

Роль иерархии Серверов администрирования

В организации 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 компьютеров на главном Сервере могут включать в себя компьютеры 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 распределенных компьютеров с политиками и задачами, каждый виртуальный Сервер администрирования имеет также собственную группу нераспределенных компьютеров, собственные наборы отчетов, выборок компьютеров и событий, инсталляционных пакетов, правил перемещения компьютеров и так далее. Функциональность виртуальных Серверов администрирования может быть использована как сервис-провайдерами (xSP) для максимальной изоляции разных заказчиков друг от друга, так и крупными организациями со сложной структурой и большим количеством администраторов.

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

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

Установка образов операционных систем

Kaspersky Security Center позволяет разворачивать на компьютеры сети предприятия wim-образы настольных и серверных версий операционных систем Windows®.

Образ операционной системы, пригодный для развертывания средствами Kaspersky Security Center, может быть получен следующими способами:

- импортом из файла install.wim, который входит в состав дистрибутива Windows;
- захватом образа с эталонного компьютера.

Поддерживаются два сценария развертывания образа операционной системы:

- развертывание на «чистый» компьютер, то есть на компьютер без установленной на нем операционной системы;
- развертывание на компьютер, работающий под управлением операционной системы Windows.

В составе Сервера администрирования неявно присутствует служебный образ WinPE (Windows Preinstallation Environment), который всегда используется как при захвате, так и во время развертывания образов операционной системы. В WinPE следует добавить все драйверы, необходимые для правильной работы всех целевых компьютеров. Как правило, требуется добавить драйверы чипсета, необходимые для работы сетевого интерфейса Ethernet.

Для реализации сценариев развертывания и захвата образов должны быть выполнены следующие требования:

- На Сервер администрирования должен быть установлен Windows Automated Installation Kit (WAIK) версии 2.0. и выше или Windows Assessment and Deployment Kit (WADK). Если предполагаются работы по установке или захвату образов на Windows XP, следует установить WAIK.
- В сети, в которой расположен целевой компьютер, должен присутствовать DHCP-сервер.
- Папка общего доступа Сервера администрирования должна быть доступна для чтения из сети, в которой находится целевой компьютер. Если папка общего доступа расположена на Сервере администрирования, то доступ нужен для учетной записи KlPxeUser. Если папка расположена вне Сервера администрирования, то доступ нужен для всех.

При выборе образа операционной системы для установки, администратор должен явно указать архитектуру процессора целевого компьютера: x86 или x86-64.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ

В ЭТОМ РАЗДЕЛЕ

СЕРВЕР МОБИЛЬНЫХ УСТРОЙСТВ EXCHANGE ACTIVESYNC

Сервер мобильных устройств Exchange ActiveSync® позволяет управлять мобильными устройствами, которые подключаются к Серверу администрирования по протоколу Exchange ActiveSync (EAS-устройствами).

В ЭТОМ РАЗДЕЛЕ

Способы развертывания Сервера мобильных устройств Exchange ActiveSync

Если в организации развернуто несколько серверов Microsoft Exchange с ролью клиентского доступа, объединенных в массив (Client Access Server Array), то Сервер мобильных устройств Exchange ActiveSync следует устанавливать на каждый сервер в массиве. В мастере установки Сервера мобильных устройств Exchange ActiveSync необходимо выбрать **Режим кластера**. В этом случае совокупность экземпляров Сервера мобильных устройств Exchange ActiveSync, установленных на серверы массива, будет называться кластером Серверов мобильных устройств Exchange ActiveSync.

Если в организации не развернут массив серверов Microsoft Exchange с ролью клиентского доступа, то Сервер мобильных устройств Exchange ActiveSync следует устанавливать на сервер Microsoft Exchange, имеющий роль Client Access. При этом в мастере установки Сервера мобильных устройств Exchange ActiveSync необходимо выбрать **Обычный режим**.

Вместе с Сервером мобильных устройств Exchange ActiveSync на компьютер необходимо установить Агент администрирования, с помощью которого осуществляется интеграция Сервера с Kaspersky Security Center.

По умолчанию область сканирования Сервера мобильных устройств Exchange ActiveSync – это текущий домен Active Directory, в котором он установлен. В случае развертывания Сервера мобильных устройств Exchange ActiveSync на сервере Microsoft Exchange 2010 – 2013 имеется возможность расширить область сканирования на весь лес доменов (см. раздел Настройка области сканирования (на стр. 82)). Запрашиваемая при сканировании информация включает в себя учетные записи пользователей сервера Microsoft Exchange, политики Exchange ActiveSync и мобильные устройства пользователей, подключенные к серверу Microsoft Exchange по протоколу Exchange ActiveSync.

В пределах одного домена недопустима установка нескольких экземпляров Сервера мобильных устройств Exchange ActiveSync, работающих в **Обычном режиме** и управляемых одним и тем же Сервером администрирования.

В пределах одного леса доменов Active Directory также недопустима установка нескольких экземпляров Сервера мобильных устройств Exchange ActiveSync (или нескольких кластеров Сервера мобильных устройств Exchange ActiveSync), работающих в **Обычном режиме**, с расширенной областью сканирования на весь лес доменов и подключенных к одному и тому же Серверу администрирования.

См. также

Инсталляция Сервера мобильных устройств Exchange ActiveSync 65

Настройка области сканирования 82

Необходимые права для развертывания Сервера мобильных устройств Exchange ActiveSync

Для развертывания Сервера мобильных устройств Exchange ActiveSync на серверах Microsoft Exchange 2010 – 2013 требуются права доменного администратора и роль Organization Management. Для развертывания Сервера мобильных устройств Exchange ActiveSync на сервере Microsoft Exchange 2007 требуются права доменного администратора и членство в группе безопасности Exchange Organization Administrators.

Учетная запись для работы службы Exchange ActiveSync

В процессе установки Сервера мобильных устройств Exchange ActiveSync в Active Directory автоматически создается учетная запись:

- на сервере Microsoft Exchange 2010—2013 – учетная запись KLMDM4ExchAdmin***** с ролью KLMDM Role Group;
- на сервере Microsoft Exchange 2007 – учетная запись KLMDM4ExchAdmin*****, являющаяся членом группы безопасности KLMDM Secure Group.

Под этой учетной записью работает служба Сервера мобильных устройств Exchange ActiveSync.

Если вы хотите отказаться от автоматического создания учетной записи, то необходимо создать собственную учетную запись, обладающую следующими правами:

- В случае использования сервера Microsoft Exchange 2010—2013, учетная запись должна обладать ролью, для которой разрешено выполнение следующих командлетов:
  - Get-CASMailbox;
  - Set-CASMailbox;
  - Remove-ActiveSyncDevice;
  - Clear-ActiveSyncDevice;
  - Get-ActiveSyncDeviceStatistics;
  - Get-AcceptedDomain;
  - Set-AdServerSettings;
  - Get-ActiveSyncMailboxPolicy;
  - New-ActiveSyncMailboxPolicy;
  - Set-ActiveSyncMailboxPolicy;
  - Remove-ActiveSyncMailboxPolicy.
- В случае использования сервера Microsoft Exchange 2007, для учетной записи должны быть назначены права доступа к объектам Active Directory (см. таблицу ниже).

Таблица 2. Права доступа к объектам Active Directory

Доступ	Объект	Командлет
Полный	Ветка «CN=Mobile Mailbox Policies,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>»	`Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=Mobile Mailbox Policies,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericAll`
Чтение	Ветка «CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>»	`Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericRead`
Чтение и запись	Свойства msExchMobileMailboxPolicyLink и msExchOmaAdminWirelessEnable для объектов в Active Directory	`Add-ADPermission -User <Имя пользователя или группы> -Identity "DC=<Имя домена>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`
Расширенное право ms-Exch-Store-Active	Хранилища почтовых ящиков Exchange-сервера, ветка «CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>»	`Get-MailboxDatabase | Add-ADPermission -User <Имя пользователя или группы> -ExtendedRights ms-Exch-Store-Admin`

Сервер мобильных устройств iOS MDM

Сервер мобильных устройств iOS MDM позволяет осуществлять управление iOS-устройствами путем установки на них специализированных iOS MDM-профилей. Поддерживаются следующие функции:

- блокирование устройства;
- сброс пароля;
- очистка устройства;
- установка или удаление приложений;
- применение iOS MDM-профиля с дополнительными параметрами (такими как параметры VPN, почты, Wi-Fi, камеры, сертификаты, и так далее).

Сервер мобильных устройств iOS MDM представляет собой веб-сервис, который принимает входящие соединения от мобильных устройств на свой TLS-порт (по умолчанию порт 443) и управляется со стороны Kaspersky Security Center с помощью Агента администрирования. Агент администрирования устанавливается локально на компьютере с развернутым Сервером мобильных устройств iOS MDM.

В процессе развертывания Сервера мобильных устройств iOS MDM администратору необходимо выполнить следующие действия:

- обеспечить Агенту администрирования доступ к Серверу администрирования;
- обеспечить мобильным устройствам доступ к TCP-порту Сервера мобильных устройств iOS MDM.

В этом разделе рассмотрены две типовые конфигурации Сервера мобильных устройств iOS MDM.

В этом разделе

Типовая конфигурация: Kaspersky Mobile Device Management в демилитаризованной зоне

Сервер мобильных устройств iOS MDM располагается в демилитаризованной зоне сети предприятия с доступом в интернет. Особенностью данного подхода является отсутствие проблем с доступностью веб-сервиса iOS MDM из интернета со стороны устройств.

Так как для управления Сервером мобильных устройств iOS MDM требуется локально установленный Агент администрирования, необходимо обеспечить взаимодействие этого Агента администрирования с Сервером администрирования. Это можно сделать следующими способами:

- Поместить Сервер администрирования в демилитаризованную зону.
- Использовать шлюз соединений (см. раздел «Доступ из интернета: Агент администрирования в режиме шлюза в демилитаризованной зоне» на стр. 12):
  a. На компьютере с развернутым Сервером мобильных устройств iOS MDM подключить Агент администрирования к Серверу администрирования через шлюз соединений.
  b. На компьютере с развернутым Сервером мобильных устройств iOS MDM назначить Агент администрирования шлюзом соединений.

См. также

Типовая конфигурация: Сервер мобильных устройств iOS MDM в локальной сети предприятия

Сервер мобильных устройств iOS MDM располагается во внутренней сети предприятия. Порт 443 (порт по умолчанию) делается доступным извне. Например, посредством публикации веб-сервиса iOS MDM на Microsoft Forefront® Threat Management Gateway (далее TMG) (см. раздел «Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)» на стр. 71).

В любой типовой конфигурации потребуется обеспечить доступность для Сервера мобильных устройств веб-сервисов Apple (диапазон адресов 17.0.0.0/8) по порту TCP 2195. Этот порт используется для оповещения устройств о новых командах через специализированный сервис APN (см. раздел «Настройка доступа к сервису Apple Push Notification» на стр. 69).

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 компьютерами:
  - 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 10

Задание сертификата Сервера администрирования 27

О Network Access Control (NAC)

По умолчанию Network Access Control (NAC) используется для получения и аудита информации о доступе устройств в сеть Ethernet. С помощью NAC можно получить ряд базовых сетевых характеристик устройств, таких как MAC-адрес, IP-адрес, NetBIOS-имя, а также ряд дополнительных характеристик, полученных в результате активного сканирования: версия операционной системы, тип устройства, список открытых сетевых портов и тому подобное.

С созданием политик разграничения доступа появляется возможность задавать критерии и правила, по которым то или иное устройство получит полный или частичный доступ к ресурсам сети, либо не получит доступ вовсе. Набор критериев, описывающий одно или несколько устройств, называется *сетевым объектом*. Критерии сетевого объекта содержат базовые сетевые характеристики, а также дополнительные характеристики, полученные в результате активного сканирования. Правила, в свою очередь, определяют вид доступа устройств (удовлетворяющих критериям) к ресурсам сети.

Аудит доступа устройств к сети и применение политик осуществляется Агентами администрирования. Агент администрирования с работающей функциональностью NAC называется *NAC-агентом*. Для обеспечения работы NAC требуется наличие одного действующего NAC-агента в каждом широковещательном домене сети. К примеру, если в сети, включающей в себя суммарно 50000 сетевых устройств, имеется 50 широковещательных доменов, то в каждом таком домене требуется наличие одного действующего NAC-агента – итого 50 действующих NAC-агентов. Действующим является NAC-агент, работающий в режиме «Основной». В случаях, когда действующий NAC-агент не может нормально функционировать (например, компьютер перезагружается), функции действующего NAC-агента может временно взять на себя резервный NAC-агент (штатно работает в режиме «Резервный»). Резервный NAC-агент (при его наличии) должен работать в том же широковещательном домене, что и основной.

NAC-агент используют технологию активного сканирования портов (NMAP), поэтому, если на устройстве закрыто большинство популярных портов, то результаты сканирования могут быть не точными или могут отсутствовать вовсе.

В текущей реализации NAC, входящий в состав Kaspersky Security Center, построен на технологии манипуляций и анализа ARP-трафика. Если NAC работает в режиме «Симуляция», используется лишь анализ ARP-трафика, и манипуляция ARP-трафиком не производится.

Учитывая ограничения протокола ARP, активность NAC-агента не распространяется за границы широковещательного домена. Границей такого домена, как правило, является маршрутизатор. Для работы NAC требуется отключение защиты от ARP-spoofing на маршрутизаторах.

Работа в сетях стандартов IEEE 802.11 (Wi-Fi) в данный момент не поддерживается.

См. также

Настройка и использование NAC 76

NAC: события и типовые сценарии работы 84

Проблемы с управлением доступом в сеть (NAC) 99

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 компьютерами 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 компьютеров администратора.
- Агент администрирования – служит для управления установленным на компьютере антивирусом, а также для получения информации о компьютере. Агенты администрирования устанавливаются на компьютеры предприятия.

Развертывание Kaspersky Security Center в сети предприятия осуществляется следующим образом:

- установка Сервера администрирования;
- выборочная установка Консоли администрирования на компьютере администратора;
- установка Агента администрирования и антивируса на компьютеры 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 компьютере с Сервером администрирования для развертывания Агента администрирования на клиентских компьютерах.

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 обычный компьютер.

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 3. Ограничения СУБД

СУБД	ОГРАНИЧЕНИЯ
SQL Server Express Edition, входящий в состав поставки Kaspersky Security Center	Не рекомендуется обслуживание одним Сервером администрирования более 10 тысяч компьютеров.
Локальный SQL Server Edition, отличный от Express	Нет ограничений.
Удаленный SQL Server Edition, отличный от Express	Допустимо только в случае, если оба компьютера 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 тысяч компьютеров.

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

См. также

О выборе СУБД для Сервера администрирования 10

ЗАДАНИЕ ПАПКИ ОБЩЕГО ДОСТУПА

Во время установки Сервера администрирования (а также и после установки, в свойствах Сервера) можно задать местоположение папки общего доступа. По умолчанию папка общего доступа создается на компьютере с Сервером администрирования (с доступом на чтение для встроенной группы **Everyone**). Однако в некоторых случаях (высокая нагрузка, необходимость доступа из изолированной сети и прочее) целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Папка общего доступа используется в нескольких сценариях развертывания Агента администрирования.

В этом разделе

Удаленная инсталляция средствами Сервера администрирования с помощью групповых политик Active Directory 26

Удаленная инсталляция рассылкой UNC-пути на автономный пакет 26

Обновление из папки 26

Установка образов операционных систем 26

Удаленная инсталляция средствами Сервера администрирования с помощью групповых политик Active Directory

В случае если целевые компьютеры находятся в домене Windows (нет рабочих групп), первоначальное развертывание (установку Агента администрирования и антивируса на пока еще не управляемые компьютеры) целесообразно выполнять при помощи групповых политик Active Directory. Развертывание выполняется с помощью штатной задачи удаленной инсталляции Kaspersky Security Center. Если размер сети велик, с целью уменьшения нагрузки на дисковую подсистему компьютера с Сервером администрирования, целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Удаленная инсталляция рассылкой UNC-пути на автономный пакет

В случае если пользователи компьютеров сети предприятия имеют права локального администратора, еще одним способом первоначального развертывания является создание автономного пакета Агента администрирования (или даже «спаренного» пакета Агента администрирования совместно с антивирусом). После создания автономного пакета нужно отправить пользователям компьютеров сети ссылку на пакет, находящийся в папке общего доступа. Инсталляция запускается по ссылке.

Обновление из папки

В задаче обновления антивируса можно настроить обновление из папки общего доступа Сервера администрирования. Если задача назначена для большого количества компьютеров, целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Установка образов операционных систем

Установка образов операционных систем всегда выполняется с использованием папки общего доступа: целевые компьютеры читают из папки образы операционных систем. Если планируется развертывание образов на большом количестве компьютеров предприятия, то целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

См. также

Развертывание Агента администрирования и антивируса 42

Указание адреса Сервера администрирования

При установке Сервера администрирования можно задать адрес Сервера администрирования. Этот адрес по умолчанию используется при создании инсталляционных пакетов Агента администрирования. По умолчанию используется NetBIOS-имя компьютера с Сервером администрирования. Если в сети предприятия настроена и правильно работает DNS, то следует здесь задать FQDN-имя компьютера с Сервером администрирования. Если Сервер администрирования установлен в демилитаризованной зоне, то может быть целесообразным указать внешний адрес Сервера 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.

См. также

Доступ из интернета: Сервер администрирования в демилитаризованной зоне 11

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. 9).

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).

Синтаксис утилиты:

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

Таблица 4. 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 компьютера 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 компьютерах 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 антивирусная 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 включить использование KSN Proxy (установить флажок **Использовать KSN Proxy**), так как это существенно повышает надежность обнаружения вредоносного программного обеспечения.

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.

Для групповых задач обновления Kaspersky Endpoint Security версий 10 и / или 10 SP1 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**.

Ручная настройка групповой задачи проверки компьютера Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки компьютера. 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 компьютеры организации выключаются по пятницам, например, в 18:30, то задача проверки компьютера 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 компьютеров в это время, то задача поиска уязвимостей будет запущена после включения компьютера (в среду утром). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему компьютера. 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 компьютеров 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 компьютера.

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 компьютерах с помощью *профилей политик*. В этом случае область действия политик задается с помощью тегов, местоположения компьютеров в подразделениях Active Directory, членства в группах безопасности Active Directory и прочего (см. раздел «Иерархия политик, использование профилей политик» на стр. 35).

- Задание области действия групповых задач.

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

- Задание прав доступа к компьютерам, 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 предприятия и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- один офис;

- множество небольших изолированных офисов.

В этом разделе

Типовая конфигурация: один офис

В типовой конфигурации «один офис» все компьютеры 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 один или несколько компьютеров агентами обновлений на корневую группу администрирования, например, на группу **Управляемые компьютеры**. Все агенты обновлений окажутся на одном уровне и будут иметь одинаковую область действия «все компьютеры 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 компьютеров на каждый агент обновлений. Агентами обновлений следует назначать мощные компьютеры с достаточным количеством свободного места на диске (см. раздел «Оценка места на диске для агента обновлений» на стр. 89). Агенты обновления не следует часто выключать, на них должен быть выключен «спящий режим».

Типовая конфигурация: 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).

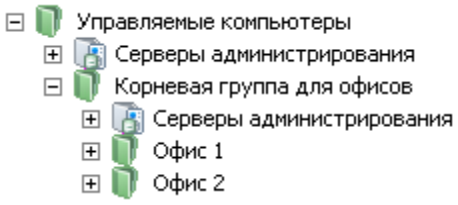

Рисунок 1. Создание задачи рассылки отчета

На каждую группу администрирования, соответствующую офису, нужно назначить один или несколько агентов обновлений. Агентами обновлений нужно назначать компьютеры удаленного офиса, имеющие достаточно места на диске (см. раздел «Оценка места на диске для агента обновлений» на стр. 89). Компьютеры, 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 компьютеров 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 обновления, 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 компьютерам 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 компьютеров. Например, областью действия политики продукта P, определенной для группы G, являются управляемые компьютеры 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 компьютере 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 компьютере, когда компьютер 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 компьютерам 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 целевые компьютеры 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 ста 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 компьютера. 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 компьютера:
  - состояние автономного режима;
  - свойства сетевого окружения – имя активного правила подключения Агента администрирования; (см. раздел «Настройка профилей соединения для автономных пользователей» на стр. 64)
  - наличие или отсутствие у компьютера указанных тегов;
  - местоположение компьютера в подразделении Active Directory: явное (компьютер находится непосредственно в указанном подразделении), или неявное (компьютер находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности);
  - членство компьютера в группе безопасности Active Directory (явное или неявное);
  - членство владельца компьютера 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 **Компьютер 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 компьютер 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 компьютерах. Локальные задачи могут быть изменены не только администратором на стороне Kaspersky Security Center средствами Консоли администрирования, но и пользователем удаленного компьютера (например, в интерфейсе антивируса). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом компьютере, 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 компьютеры, подключенные к размещенным в этой группе и подгруппах подчиненным и виртуальным Серверам администрирования.

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

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

  Запуск по расписанию задач для выборок компьютеров всегда осуществляет Сервер администрирования. Такие задачи не запустятся на компьютерах, не имеющих связи с Сервером администрирования. Задачи будут запускаться не по локальному времени целевого компьютера, а по локальному времени Сервера администрирования.

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

Правила перемещения компьютеров

Размещение компьютеров в группах администрирования целесообразно автоматизировать при помощи *правил перемещения компьютеров*. Правило перемещения состоит из трех основных частей: имени, условия выполнения (логического выражения над атрибутами компьютера) и целевой группы администрирования. Правило перемещает компьютер в целевую группу администрирования, если атрибуты компьютера удовлетворяют условию выполнения правила.

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

Правила перемещения компьютеров могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должен попасть компьютер 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.**

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

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

Наличие правил перемещение, действующих на компьютеры, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

Можно создать правило перемещения, способное многократно действовать на один и тот же компьютер.

Настоятельно рекомендуется избегать подхода к работе с управляемыми компьютерами, при котором один и тот же компьютер многократно перемещается из группы в группу – например, с целью применения к компьютеру 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 компьютеров (см. раздел «Задачи» на стр. 37), назначать Агенты администрирования согласно методике (см. раздел «Построение структуры групп администрирования и назначение агентов обновлений» на стр. 33) 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 компьютеры.

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 компьютеров, 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 компьютеров, что создаст риск безвозвратной потери зашифрованных данных на компьютерах 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 компьютере, 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 компьютеров 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

Вышел из строя компьютер с Сервером администрирования

Если в результате сбоя вышел из строя компьютер 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 компьютере.
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 антивируса

Для управления компьютерами предприятия требуется установить на компьютеры Агент администрирования. Развертывание распределенного приложения Kaspersky Security Center на компьютерах предприятия обычно начинается с установки на них Агента администрирования.

В этом разделе

Первоначальное развертывание

Если на компьютере уже установлен Агент администрирования, удаленная инсталляция приложений на такой компьютер 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 обновления, многоадресную рассылку и так далее. Подробные сведения об установке приложений на управляемые компьютеры, на которых уже установлен Агент администрирования, см. далее в этом разделе.

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

- С помощью сторонних средств удаленной установки приложений.
- Путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования: средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков, или сторонними средствами.
- Через механизм групповых политик Microsoft Windows: с помощью штатных средств управления групповыми политиками Microsoft Windows, или автоматизированно, с помощью соответствующей опции в задаче удаленной установки приложений Kaspersky Security Center.
- Принудительно с помощью соответствующих опций в задаче удаленной установки приложений Kaspersky Security Center.

- Путем рассылки пользователям компьютеров 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 продуктов на целевых компьютерах.

На платформах, отличных от Microsoft Windows, первоначальную установку Агента администрирования на управляемых компьютерах следует осуществлять имеющимися сторонними средствами. 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 компьютерах 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 «Типовые конфигурации Kaspersky Security Center» на стр. 13);

- общее количество компьютеров;

- наличие в сети предприятия компьютеров, не являющихся членами доменов Active Directory, и наличие унифицированных учетных записей с административными правами на таких компьютерах;

- ширину канала между Сервером администрирования и целевыми компьютерами;

- характер связи между Сервером администрирования и удаленными подсетями и ширину сетевых каналов внутри таких подсетей;

- используемые на момент начала развертывания параметры безопасности на удаленных компьютерах (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, 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 выбранный компьютер), необходимые параметры можно задать с помощью пользовательского интерфейса инсталлятора.

Этот способ настройки параметров не подходит для неинтерактивной «тихой» установки программ на группы компьютеров. В типичном случае администратор должен централизованно указать значения параметров, которые в дальнейшем могут быть использованы для неинтерактивной установки на выбранные компьютеры 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. В случае удаленной установки приложений средствами Kaspersky Security Center инсталляционные пакеты доставляются на целевые компьютеры таким образом, что при запуске инсталлятора приложения ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки приложений «Лаборатории Касперского» достаточно обеспечить доступность на целевом компьютере всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center в соответствующей подпапке папки общего доступа (см. раздел «Задание папки общего доступа» на стр. 25).

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. 46).

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

Несмотря на то, что ключ лицензии на приложение можно задать в свойствах инсталляционного пакета, желательно не использовать этот способ распространения лицензий из-за широкой доступности инсталляционных пакетов на чтение. Следует использовать автоматически распространяемые 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 в следующих случаях:

- при установке через групповые политики Windows при помощи штатных средств Microsoft или иных сторонних инструментов для работы с групповыми политиками Windows;
- при установке с помощью сторонних средств, ориентированных на работу с инсталляторами в формате Microsoft Installer (см. раздел «Настройка параметров инсталляторов» на стр. 54).

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.
- В случае установки из папки общего доступа убедиться в достаточной производительности этого файлового ресурса.

См. также

Задание папки общего доступа 25

Настройка параметров инсталляторов 54

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 (принудительная установка, установка с помощью копирования образа жесткого диска, установка с помощью групповых политик Microsoft Windows). Создать задачу удаленной установки можно как для указанной группы администрирования, так и для набора компьютеров или для выборки компьютеров (такие задачи отображаются в Консоли администрирования в папке **Задачи для наборов компьютеров**). При создании задачи можно выбрать инсталляционные пакеты (Агента администрирования и / или другого приложения), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки. Кроме того, можно воспользоваться мастером удаленной установки приложений, в основе которого также лежит создание задачи удаленной установки приложений и мониторинг результатов.

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

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

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

Развертывание захватом и копированием образа жесткого диска компьютера

Если нужно инсталлировать Агент администрирования на компьютеры, на которые также предстоит установить (или переустановить) операционную систему и прочее программное обеспечение, можно воспользоваться механизмом захвата и копирования образа жесткого диска компьютера.

Развертывание путем захвата и копирования образа жесткого диска нужно выполнять следующим образом:

1. Создать «эталонный» компьютер с установленной операционной системой и необходимым для работы набором программного обеспечения, включая Агент администрирования и антивирус.

2. Захватить образ «эталонного» компьютера и далее распространять этот образ на новые компьютеры посредством задачи Kaspersky Security Center.

   Для захвата и установки образов диска можно воспользоваться как имеющимися на предприятии сторонними средствами, так и функциональностью, предоставляемой (при наличии лицензии Systems Management) Kaspersky Security Center (см. раздел «Установка образов операционных систем» на стр. 16).

Если для работы с образами диска используются сторонние инструменты, необходимо при развертывании на целевой компьютер из эталонного образа обеспечить удаление информации, с помощью которой Kaspersky Security Center идентифицирует управляемый компьютер. В противном случае Сервер администрирования не сможет в дальнейшем корректно различать компьютеры, созданные путем копирования одного и того же образа (см. http://support.kaspersky.com/9334).

При захвате образа диска средствами Kaspersky Security Center эта проблема решается автоматически.

Копирование образа жесткого диска сторонними инструментами

При использовании сторонних инструментов для захвата образа компьютера с установленным Агентом администрирования следует воспользоваться одним из следующих методов:

- Рекомендуемый метод. При установке Агента администрирования на эталонный компьютер выбрать вариант **Не запускать службу по завершении инсталляции** и захватить образ компьютера до первого старта службы Агента администрирования (так как уникальная информация, идентифицирующая компьютер, создается при первом подключении Агента администрирования к Серверу администрирования). В дальнейшем рекомендуется не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.

- На эталонном компьютере остановить службу Агента администрирования и запустить утилиту klmover с ключом -dupfix. Утилита klmover входит в состав инсталляционного пакета Агента администрирования. В дальнейшем не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.

- Обеспечить запуск утилиты klmover с ключом -dupfix до (это важно) первого запуска службы Агента администрирования на целевых компьютерах при первом старте операционной системы после развертывания образа. Утилита klmover входит в состав инсталляционного пакета Агента администрирования.

Если копирование образа жесткого диска было выполнено неправильно, см. раздел Неверно выполнено копирование образа жесткого диска (на стр. 93).

Можно применять альтернативный вариант развертывания Агента администрирования на новые компьютеры с использованием образов операционной системы:

- Захваченный образ не содержит установленный Агент администрирования,

- В список исполняемых файлов, запускаемых по завершении развертывания образа на целевых компьютерах, добавлен автономный пакет Агента администрирования, расположенный в папке общего доступа Kaspersky Security Center.

Этот вариант развертывания дает большую гибкость: можно использовать один образ операционной системы совместно с различными вариантами установки Агента и / или антивирусного продукта, включая правила перемещения компьютера, связанные с автономным пакетом. При этом несколько усложняется процесс развертывания, требуется обеспечить доступ к сетевой папке с автономными пакетами с целевого компьютера (см. раздел «Установка образов операционных систем» на стр. 16).

Развертывание с помощью механизма групповых политик Microsoft Windows

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

- целевые компьютеры являются членами домена Active Directory;

- план развертывания позволяет дождаться штатной перезагрузки целевых компьютеров до начала развертывания на них Агентов администрирования, или к целевым компьютерам 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 целевых компьютеров).
- 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 целевые компьютеры.
- При очередном входе целевого компьютера в домен (до входа в систему пользователей компьютера) 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 целевые компьютеры 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 компьютеров (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 целевые компьютеры при применении групповой политики Windows.

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

Самым простым способом инсталляции приложений при помощи групповых политик Microsoft Windows является установка флажка **Назначить установку инсталляционного пакета в групповых политиках Active Directory** в свойствах задачи удаленной установки приложений Kaspersky Security Center. В этом случае при запуске задачи Сервер администрирования самостоятельно выполнит следующие действия:

- Создаст необходимые объекты в групповой политике Microsoft Windows.
- Создаст специальные группы безопасности, в которые включит целевые компьютеры, и назначит установку выбранных приложений для этих групп безопасности. Состав групп безопасности будет актуализироваться при каждом запуске задачи в соответствии с набором целевых компьютеров на момент запуска.

Для обеспечения работоспособности данной функции, следует указать в параметрах задачи учетную запись, имеющую права на редактирование групповых политик Active Directory.

Если с помощью одной задачи предполагается установить и Агент администрирования, и другое приложение, установка флажка **Назначить установку инсталляционного пакета в групповых политиках Active Directory** приведет к созданию в политике Active Directory объекта установки только для Агента администрирования. Второе выбранное в задаче приложение будет устанавливаться уже средствами Агента администрирования, как только он будет установлен на целевом компьютере. Если по какой-то причине необходимо установить отличное от Агента администрирования приложение именно с помощью групповых политик Windows, то нужно создать задачу установки только для этого инсталляционного пакета (без пакета Агента администрирования).

В случае, когда необходимые объекты создаются в групповой политике средствами Kaspersky Security Center, в качестве источника инсталляционного пакета будет использована папка общего доступа Kaspersky Security Center. При планировании развертывания следует соотнести скорость чтения из этой папки с количеством целевых компьютеров и размером устанавливаемого дистрибутива. Возможно, будет целесообразно расположить папку общего доступа Kaspersky Security Center в мощном специализированном файловом хранилище (см. раздел «Задание папки общего доступа» на стр. 25).

Помимо простоты, автоматическое создание групповых политик Windows средствами Kaspersky Security Center имеет еще одно преимущество: при планировании установки Агента администрирования легко указать группу администрирования Kaspersky Security Center, в которую будут автоматически перемещаться компьютеры по завершении установки. Группу можно указать в мастере создания задачи или в окне параметров задачи удаленной установки.

При работе с групповыми политиками Windows средствами Kaspersky Security Center задание целевых компьютеров для объекта групповой политики осуществляется путем создания группы безопасности. Kaspersky Security Center синхронизирует состав группы безопасности с текущим набором целевых компьютеров задачи. При использовании иных средств для работы с групповыми политиками можно привязывать объекты групповых политик непосредственно к выбранным подразделениям Active Directory.

Самостоятельная установка приложений с помощью политик Microsoft Windows

Администратор может самостоятельно создать в групповой политике Windows объекты, необходимые для установки. В этом случае можно сослаться на пакеты, лежащие в папке общего доступа Kaspersky Security Center, или выложить пакеты на отдельный файловый сервер и сослаться на них.

Возможны следующие сценарии установки:

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Объект групповой политики ссылается на msi-файл этого сконфигурированного пакета, лежащего в папке общего доступа Kaspersky Security Center.

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Затем администратор копирует целиком подпапку EXEC этого пакета из папки общего доступа Kaspersky Security Center в папку на специализированном файловом ресурсе 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. 54).

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center

В случае если требуется начать развертывание Агентов администрирования или других необходимых приложений немедленно, без ожидания очередного входа целевых компьютеров в домен, или же при наличии целевых компьютеров, не являющихся членами домена Active Directory, можно использовать принудительную (форсированную) установку выбранных инсталляционных пакетов при помощи задачи удаленной установки приложений Kaspersky Security Center.

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

Данный способ установки осуществляется путем копирования файлов на административный ресурс admin$ каждого из целевых компьютеров и удаленной регистрации на них вспомогательных служб. При этом должны выполняться следующие условия:

- Целевые компьютеры должны быть доступны для подключения либо со стороны Сервера администрирования, либо со стороны агента обновлений.
- В сети должно корректно работать разрешение имен для целевых компьютеров.
- На управляемых компьютерах не должны быть отключены административные ресурсы общего доступа admin$.
- На целевых компьютерах должна быть запущена системная служба Server (по умолчанию данная служба запущена).
- На целевых компьютерах должны быть открыты следующие порты для удаленного доступа к компьютерам средствами Windows: TCP 139, TCP 445, UDP 137, UDP 138.
- На целевых компьютерах должен быть выключен режим Simple File Sharing.
- На целевых компьютерах 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*).
- Целевые компьютеры должны быть членами домена, либо на целевых компьютерах должны быть заблаговременно созданы унифицированные учетные записи с административными правами.

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

При создании групповой задачи необходимо помнить, что групповая задача действует на компьютеры 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 компьютерах этой группы. В результате на всех компьютерах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период времени, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества компьютеров в сети.

Принудительная установка может быть использована и в случае, если целевые компьютеры не доступны Серверу администрирования непосредственно: например, компьютеры расположены в изолированных сетях, или компьютеры расположены в локальной сети, а Сервер администрирования – в демилитаризованной зоне. Для работоспособности принудительной установки необходимо обеспечить наличие агентов обновлений в каждой такой изолированной сети.

Использование агентов обновлений в качестве локальных центров установки может быть удобно и для установки на компьютеры в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между компьютерами внутри подсети. Однако следует учитывать, что данный способ установки создает значительную нагрузку на компьютеры, назначенные агентами обновлений. Поэтому нужно выбирать в качестве агентов обновлений достаточно мощные компьютеры 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. 89).

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 размещается в папке общего доступа Kaspersky Security Center.

При помощи Kaspersky Security Center можно разослать по электронной почте выбранным пользователям ссылку на этот файл в папке общего доступа с просьбой запустить файл (интерактивно или с ключом «тихой» установки «-s»). Автономный пакет установки можно прикрепить к сообщению электронной почты для пользователей компьютеров, не имеющих доступ к папке общего доступа Kaspersky Security Center. Администратор может скопировать автономный пакет на внешнее устройство и доставить пакет на нужный компьютер с целью его последующего запуска.

Автономный пакет можно создать из пакета Агента администрирования, пакета другого (например, антивирусного) 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 компьютеры (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, расположенного в папке общего доступа Kaspersky Security Center, сначала произойдет копирование пакета во временную локальную папку, затем из локальной справки будет запущен инсталлятор приложения.

Удаленная установка приложений на компьютеры с установленным Агентом администрирования

Если на компьютере установлен работоспособный Агент администрирования, подключенный к главному Серверу администрирования или к одному из его подчиненных Серверов, то на этом компьютере 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. 45).

Если флажок установлен, то передача на целевые компьютеры 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 целевыми компьютерами 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. 15) и Построение структуры групп администрирования и назначение агентов обновлений (на стр. 33)). В этом случае распространение инсталляционных пакетов и параметров инсталлятора осуществляется с Сервера администрирования на целевые компьютеры 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 целевые компьютеры 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\$FTCITmp.

Удалять файлы из папки $FTCITmp 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 целевые компьютеры.

УПРАВЛЕНИЕ ПЕРЕЗАГРУЗКОЙ ЦЕЛЕВЫХ КОМПЬЮТЕРОВ В ЗАДАЧЕ УДАЛЕННОЙ УСТАНОВКИ

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

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

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

- **Спросить у пользователя**. В этом случае на экране клиентского компьютера будет выводиться сообщение о том, что компьютер должен быть перезагружен 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 антивирусной защиты необходимо учитывать возможность обновления антивирусных баз (включая модули автопатчей), распространяемых вместе с дистрибутивом антивирусного приложения. 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 антивирусной защиты на целевых компьютерах.

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

Для установки антивирусной программы «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 антивирусной программы несовместимые с ней программы удаляются автоматически, если в окне свойств инсталляционного пакета антивирусной программы (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 целевых компьютерах непосредственно перед задачей установки антивирусной программы. 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 антивирусной программы не может успешно удалить какую-либо из несовместимых программ.

Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых компьютерах 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 целевых компьютерах 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:

```
[SetupProcessResult]

Wait=0
```

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

```
[SetupProcessResult]

WaitJob=0
```

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

```
[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:

```
[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 компьютера (если перезагрузка необходима для завершения операции), нужно дополнительно перечислить коды возврата процесса, означающие необходимость перезагрузки, в секции [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]

3010=
```

Мониторинг развертывания

Для контроля развертывания Kaspersky Security Center, а также для контроля наличия на управляемых компьютерах антивирусной программы и Агента администрирования, следует обращать внимание на «семафор» **Развертывание**, расположенный в рабочей области узла Сервер администрирования в главном окне Консоли администрирования (см. раздел «»Семафоры» в Консоли администрирования» на стр. 80).

«Семафор» отображает текущее состояние развертывания. Рядом с «семафором» отображается количество компьютеров с установленными Агентами администрирования и антивирусными программами. При наличии активных задач установки отображается их прогресс. При наличии ошибок установки отображается количество ошибок с возможностью перейти по ссылке для просмотра детальной информации об ошибке.

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

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 целевых компьютерах, а в нижнем – список событий задачи на компьютере, который в данный момент выбран 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.

Установка в тихом режиме (без файла ответов)

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 5. 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, CiscoNACServer, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86

Свойство MSI	Описание	Возможные значения
NETRANGETYPE	Размер сети	• NRT_1_100 – от 1 до 100 компьютеров • NRT_100_1000 – от 100 до 1000 компьютеров • NRT_GREATER_1000 – более 1000 компьютеров
SRV_ACCOUNT_TYPE	Способ задания пользователя для работы сервиса Сервера администрирования	• SrvAccountDefault – учетная запись пользователя будет создана автоматически • SrvAccountUser – учетная запись пользователя задана вручную
SERVERACCOUNTNAME	Имя пользователя для сервиса	
SERVERACCOUNTPWD	Пароль пользователя для сервиса	
DBTYPE		• MySQL • MSSQL
MYSQLSERVERNAME	Полное имя mysql-сервера	
MYSQLSERVERPORT	Номер порта для подключения к 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 SQLServer	

Свойство MSI	Описание	Возможные значения
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	
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 6. Свойства MSI

Свойство MSI	Описание	Возможные значения
DONT_USE_ANSWER_FILE	Читать параметры установки из файла ответов	• 1 • Пусто
INSTALLDIR	Папка установки	
INSTALL_NSAC	Устанавливать ли NAC	• 1 • Пусто
SERVERADDRESS	Адрес Сервера администрирования (обязательный параметр)	
SERVERPORT	Номер порта подключения к Серверу администрирования	

Свойство MSI	Описание	Возможные значения
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	
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	

Свойство MSI	Описание	Возможные значения
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 антивируса на каждую виртуальную машину и защита виртуальных машин на уровне гипервизора. В первом случае для защиты виртуальных машин может использоваться как обычный антивирус, 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 компьютеров с Агентом администрирования» на стр. 63).

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 компьютера 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 компьютеры.

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 компьютеров** 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 (см. раздел «Развертывание захватом и копированием образа жесткого диска компьютера» на стр. 45).

Однако в описанных ниже двух случаях Агент администрирования обнаруживает факт копирования автоматически, и выполнять сложные действия, описанные в разделе «Развертывание захватом и копированием жесткого диска компьютера», 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 компьютером, 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 компьютеров с Агентом администрирования

Kaspersky Security Center является распределенной программой. Откат файловой системы в предыдущее состояние на одном из компьютеров 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 компьютерах 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 компьютеров, в Kaspersky Security Center, начиная с версии 10 MR1 (Сервер администрирования и Агенты администрирования должны быть версии 10 MR1 или более новой), была добавлена поддержка обнаружения отката файловой системы на компьютерах с установленным Агентом администрирования. В случае обнаружения такие компьютеры 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 функциональности следует на компьютере с Сервером администрирования импортировать в Реестр представленный ниже reg-файл и перезапустить службу Сервера администрирования.

Операционная система на компьютере 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 компьютере 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 SP1 поддержка обнаружения отката файловой системы включена по умолчанию.

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

Для компьютера 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. 39).

Настройка профилей соединения для автономных пользователей

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

Использование различных адресов одного и того же Сервера администрирования

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

Компьютеры 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. При этом 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 (на стр. 12)), 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 компьютеров с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится компьютер.

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 10

Доступ из интернета: Агент администрирования в режиме шлюза в демилитаризованной зоне 12

Развертывание функциональности Управление мобильными устройствами

В этом разделе

Инсталляция Сервера мобильных устройств Exchange ActiveSync

Настройка веб-сервера Internet Information Services

При использовании Microsoft Exchange Server версий 2010 и 2013 в настройках веб-сервера Internet Information Services (IIS) необходимо активировать механизм аутентификации Windows для виртуальной директории Windows PowerShell™. Активация этого механизма аутентификации выполняется автоматически, если в мастере установки Сервера мобильных устройств Exchange ActiveSync установлен флажок **Автоматическая настройка IIS** (поведение по умолчанию).

В противном случае необходимо активировать механизм аутентификации самостоятельно.

Чтобы активировать механизм аутентификации Windows для виртуальной директории PowerShell вручную, выполните следующие действия:

1. В консоли Internet Information Services Manager откройте свойства виртуальной директории PowerShell.
2. Перейдите в раздел **Authentication**.
3. Выберите **Windows authentication**, нажмите на кнопку **Enable**.
4. Откройте дополнительные параметры **Advanced Settings**.
5. Установите флажок **Enable Kernel-mode authentication**.
6. В раскрывающемся списке **Extended Protection** выберите **Required**.

При использовании Microsoft Exchange Server версии 2007 настройка веб-сервера IIS не требуется.

Локальная установка Сервера мобильных устройств Exchange ActiveSync

Для локальной установки Сервера мобильных устройств Exchange ActiveSync администратор должен выполнить следующие действия:

1. Из дистрибутива Kaspersky Security Center скопировать содержимое папки \Server\Packages\MDM4Exchange\ на клиентский компьютер.

2. Запустить исполняемый файл setup.exe.

Локальная установка подразумевает два типа инсталляции:

- Стандартная установка – упрощенная установка, не требующая со стороны администратора настройки каких-либо параметров, рекомендуется в большинстве случаев;

- Расширенная установка – установка, требующая от администратора настройки следующих параметров:

  - путь для установки Сервера мобильных устройств Exchange ActiveSync;

  - режим работы Сервера мобильных устройств Exchange ActiveSync: обычный или в режиме кластера (см. раздел «Способы развертывания Сервера мобильных устройств Exchange ActiveSync» на стр. 18);

  - возможность указания учетной записи, под которой будет работать служба Сервера мобильных устройств Exchange ActiveSync (см. раздел «Учетная запись для работы службы Exchange ActiveSync» на стр. 18);

  - включение / выключение автоматической настройки веб-сервера IIS.

Мастер установки Сервера мобильных устройств Exchange ActiveSync следует запускать под учетной записью, обладающей необходимыми правами (см. раздел «Необходимые права для развертывания Сервера мобильных устройств Exchange ActiveSync» на стр. 18).

Удаленная установка Сервера мобильных устройств Exchange ActiveSync

Для настройки удаленной установки Сервера мобильных устройств Exchange ActiveSync администратор должен выполнить следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выбрать папку **Удаленная установка**, в ней вложенную папку **Инсталляционные пакеты**.

2. Во вложенной папке **Инсталляционные пакеты** открыть свойства пакета **Сервер мобильных устройств Exchange ActiveSync.**

3. Перейти в раздел **Параметры**.

   В разделе содержатся те же параметры, что и для локальной установки продукта.

После настройки удаленной установки можно приступить к установке Сервера мобильных устройств Exchange ActiveSync.

Для установки Сервера мобильных устройств Exchange ActiveSync необходимо выполнить следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выбрать папку **Удаленная установка**, в ней вложенную папку **Инсталляционные пакеты**.

2. Во вложенной папке **Инсталляционные пакеты** выбрать пакет **Сервер мобильных устройств Exchange ActiveSync**.

3. Открыть контекстное меню пакета и выбрать пункт **Установить программу**.

4. В открывшемся мастере удаленной установки выбрать один компьютер (или несколько компьютеров при установке в режиме кластера).

5. В поле **Запускать инсталлятор программы под указанной учетной записью** указать учетную запись, под которой будет запущен процесс установки на удаленном компьютере.

   Учетная запись должна обладать необходимыми правами (см. раздел «Необходимые права для развертывания Сервера мобильных устройств Exchange ActiveSync» на стр. 18).

ИНСТАЛЛЯЦИЯ СЕРВЕРА МОБИЛЬНЫХ УСТРОЙСТВ IOS MDM

Количество установленных копий Сервера мобильных устройств iOS MDM может быть выбрано как исходя из наличия доступного аппаратного обеспечения, так и в зависимости от общего количества обслуживаемых мобильных устройств.

Однако следует учесть, что на одну установку Kaspersky Mobile Device Management, рекомендуется не более 50000 мобильных устройств. С целью уменьшения нагрузки, все множество устройств можно распределить между несколькими серверами с установленным Сервером мобильных устройств iOS MDM.

Аутентификация iOS MDM-устройств осуществляется при помощи сертификатов пользователей (профиль, устанавливаемый на устройство, содержит сертификат того пользователя, которому оно принадлежит). Поэтому возможны две схемы развертывания Сервера мобильных устройств iOS MDM:

- упрощенная схема;
- схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD).

Ниже рассмотрены обе схемы развертывания.

УПРОЩЕННАЯ СХЕМА РАЗВЕРТЫВАНИЯ

При развертывании Сервера мобильных устройств iOS MDM по упрощенной схеме мобильные устройства напрямую подключаются к веб-сервису iOS MDM. При этом для аутентификации устройств могут быть использованы только пользовательские сертификаты, выпущенные Сервером администрирования. Интеграция с Public Key Infrastructure (PKI) для пользовательских сертификатов невозможна (см. раздел «Типовая конфигурация: Kaspersky Mobile Device Management в демилитаризованной зоне» на стр. 21).

Схема развертывания с использованием принудительного делегирования Kerberos (KCD)

Для использования схемы развертывания с принудительным делегированием Kerberos Сервер администрирования и Сервер мобильных устройств iOS MDM должны располагаться во внутренней сети предприятия.

Эта схема развертывания предполагает:

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

При использовании этой схемы развертывания следует учесть следующее:

- В Консоли администрирования в настройках веб-сервиса iOS MDM необходимо установить флажок **Обеспечить совместимость с Kerberos Constrained Delegation**.
- В качестве сертификата веб-сервиса iOS MDM следует указать особый (кастомизированный) сертификат, заданный на TMG при публикации веб-сервиса iOS MDM.
- Пользовательские сертификаты для iOS-устройств должны выписываться доменным Центром сертификации (Certification authority, далее CA). Если в домене несколько корневых CA, то пользовательские сертификаты должны быть выписаны CA, указанным при публикации веб-сервиса iOS MDM на TMG.

  Обеспечить соответствие пользовательского сертификата указанному требованию возможно несколькими способами:

  - Указать пользовательский сертификат в мастере создания iOS MDM-профиля и в мастере установки сертификатов.
  - Интегрировать Сервер администрирования с доменным PKI и настроить соответствующий параметр в правилах выписки сертификатов:

    1. В 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 PKI** настройте интеграцию с инфраструктурой открытых ключей.
    3. В разделе **Выпуск сертификатов общего типа** укажите источник сертификатов.

См. разделы:

- Типовая конфигурация: Kaspersky Mobile Device Management в локальной сети предприятия (см. раздел «Типовая конфигурация: Сервер мобильных устройств iOS MDM в локальной сети предприятия» на стр. 21);
- Интеграция с PKI (Public Key Infrastructure) (см. раздел «Интеграция с Public Key Infrastructure» на стр. 75).

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- веб-сервис iOS MDM запущен на 443 порте;
- имя компьютера с TMG – tmg.mydom.local;
- имя компьютера с веб-сервисом iOS MDM – iosmdm.mydom.local;
- имя внешней публикации веб-сервиса iOS MDM – iosmdm.mydom.global.

Service Principal Name для http/iosmdm.mydom.local

В домене требуется прописать Service Principal Name (SPN) для компьютера с веб-сервисом iOS MDM (iosmdm.mydom.local):

setspn -a http/iosmdm.mydom.local iosmdm

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

Для делегирования трафика доверить компьютер с TMG (tmg.mydom.local) службе, определенной по SPN (http/iosmdm.mydom.local).

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

1. В оснастке MMC «Active Directory Users and Computers» необходимо выбрать компьютер с установленным TMG (tmg.mydom.local).
2. В свойствах компьютера 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/iosmdm.mydom.local.

Особый (кастомизированный) сертификат для публикуемого веб-сервиса (iosmdm.mydom.global)

Требуется выписать особый (кастомизированный) сертификат для веб-сервиса iOS MDM на FQDN iosmdm.mydom.global и указать его взамен сертификата по умолчанию в настройках веб-сервиса iOS MDM в Консоли администрирования.

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

Публикации веб-сервиса iOS MDM на TMG

На TMG для трафика, идущего со стороны мобильного устройства на 443 порт iosmdm.mydom.global, необходимо настроить KCD на SPN http/iosmdm.mydom.local с использованием сертификата, выписанного для FQDN iosmdm.mydom.global. При этом следует учесть, что как на публикации, так и на публикуемом веб-сервисе должен быть один и тот же серверный сертификат.

Настройка доступа к сервису Apple Push Notification

Для корректной работы веб-сервиса iOS MDM, а также для обеспечения своевременного реагирования устройств на команды администратора, в параметрах Сервера мобильных устройств iOS MDM следует указать сертификат Apple Push Notification Service (далее APNs-сертификат).

О том, как получить APNs-сертификат см. статью в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.com/11077.

Взаимодействуя с сервисом Apple Push Notification (далее APNs), веб-сервис iOS MDM подключается к внешнему адресу gateway.push.apple.com по порту 2195 (исходящий). Поэтому веб-сервису iOS MDM необходимо предоставить доступ к порту TCP 2195 для диапазона адресов 17.0.0.0/8. Со стороны iOS устройства – доступ к порту TCP 5223 для диапазона адресов 17.0.0.0/8.

Если доступ к APNs со стороны веб-сервиса iOS MDM предполагается осуществлять через прокси-сервер, то на компьютере с установленным веб-сервисом iOS MDM необходимо выполнить следующие действия:

1. Прописать в Реестр следующие строки:

   - Для 32-разрядной операционной системы:

     [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset]

     «ApnProxyHost»=«<Proxy Host Name>»

     «ApnProxyPort»=«<Proxy Port>»

     «ApnProxyLogin»=«<Proxy Login>»

     «ApnProxyPwd»=«<Proxy Password>»

   - Для 64-разрядной операционной системы:

     [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset]

     «ApnProxyHost»=«<Proxy Host Name>»

     «ApnProxyPort»=«<Proxy Port>»

     «ApnProxyLogin»=«<Proxy Login>»

     «ApnProxyPwd»=«<Proxy Password>»

2. Перезапустить службу веб-сервиса iOS MDM.

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. 10)).

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 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. 75);

- Предоставление доступа к Серверу администрирования из интернета (на стр. 10).

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- точка доступа к мобильному протоколу на стороне Сервера администрирования поднята на 13292 порте;

- имя компьютера с TMG – tmg.mydom.local;

- имя компьютера 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 часть 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 компьютера с Сервером администрирования. Для компьютера kes4mob.mydom.local с Сервером администрирования, это будет выглядеть следующим образом:

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

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

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

Чтобы доверить компьютер 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 компьютер с установленным TMG (tmg.mydom.local).
2. В свойствах компьютера 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 Cloud Messaging

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

Чтобы включить использование GCM, 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 Cloud Messaging**.
4. В полях **Идентификатор отправителя** и **Ключ API** укажите параметры GCM: SENDER_ID и API Key.

Сервис GCM 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 GCM.

Настройка GCM: получение SENDER_ID, API Key

Для настройки работы с GCM 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 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 компьютере 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 компьютера 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 компьютер 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, iOS MDM-профилей, а также файлов из папки общего доступа.

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

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

Настройки веб-сервера

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

Настройка и использование NAC

В разделе содержатся рекомендации по первичной настройке и использованию NAC. Описаны требования к компьютерам, которые планируется использовать как NAC-агенты, приоритеты ограничений для сетевых устройств, указанных в правилах NAC.

Приведены примеры настройки NAC для нескольких типовых конфигураций сети.

В этом разделе

См. также

Назначение NAC-агентов

В качестве NAC-агента следует выбирать компьютер, соответствующий следующим критериям:

- есть свободные ресурсы, не загружен как по ЦПУ, так и по сетевым сервисам;
- наиболее мощный;
- очень редко перезагружается и / или выключается.

Назначение NAC-агентом компьютера, соответствующего этим требованиям, позволит быстрее собрать данные и выполнить сканирование, а также более качественно применять NAC-политики. Если NAC-агент включен для работы в широковещательном домене, в котором уже работают сетевые устройства (активность которых предполагается ограничивать), то может пройти некоторое время, прежде чем сеть будет проанализирована и NAC-политика вступит в силу. Как правило, политика вступает в действие через 10 – 15 минут для широковещательного домена размером в 300 устройств.

Количество устройств, которое может быть обслужено одним NAC-агентом, зависит от инфраструктуры и размеров широковещательного домена сети, а также от количества сетевых объектов и правил. NAC уверенно функционирует при наличии 1000 устройств на один NAC-агент.

Для тестирования работоспособности политики NAC предусмотрен режим работы NAC-агента «Симуляция». Суть режима «Симуляция» состоит в том, что политика NAC транслируется в драйвер, однако фактически сетевая активность устройств, попадающих под ограничения доступа, никак не ограничивается. В режиме «Симуляция» NAC-драйвер сообщает Агенту администрирования лишь информацию о необходимости применить то или иное правило в отношении устройства. Эта информация доступна в файле $klnac.log (см. раздел «Определение работоспособности правила NAC» на стр. 86). В остальном этот режим не отличается от рабочего режима (режим «Обычный»).

NAC-агент для работы создает дополнительные виртуальные адаптеры (по одному на каждый физический адаптер в системе), MAC-адреса которых случайно генерируются на Сервере администрирования. Этот список MAC-адресов генерируется один раз при первоначальном запуске Сервера администрирования и в дальнейшем не изменяется. На этапе инициализации, используя один из доступных MAC-адресов из списка, адаптер NAC-агента делает несколько попыток DHCP-конфигурирования. Если в инфраструктуре сети не предусмотрен DHCP-сервер или конфигурация DHCP-сервера использует статическую привязку MAC – IPv4, то для работы NAC-агента требуется ручное конфигурирование интерфейса.

Ручное конфигурирование адаптеров NAC-агента (не рекомендуется)

Выполнить ручное конфигурирование можно через Реестр Windows на NAC-агенте путем импорта следующего файла.

Для 32-разрядной версии Windows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags]

«EnfUseDHCP»=dword:00000000

«EnfIpv4»=«10.16.72.2»

«EnfSubnetMask»=«255.255.252.0»

«EnfIpv4Gateway»=«10.16.72.1»
```

Для 64-разрядной версии Windows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags]

«EnfUseDHCP»=dword:00000000

«EnfIpv4»=«10.16.72.2»

«EnfSubnetMask»=«255.255.252.0»

«EnfIpv4Gateway»=«10.16.72.1»
```

Ручное конфигурирование возможно только на NAC-агентах с одним активным физическим интерфейсом. Если активных физических интерфейсов несколько, то данная конфигурация будет применена к виртуальному адаптеру первого случайно выбранного интерфейса.

Ограничения в правилах NAC

Ограничения в правилах NAC имеют следующие приоритеты (от самого высокого к самому низкому):

- NAC-агенты (самый высокий приоритет, для внутреннего использования).

  Компьютеры с NAC-агентами всегда доступны для сетевого взаимодействия с устройствами, независимо от ограничений, накладываемых на активность устройств.

- Белый список. NAC-агенты никак не ограничивают устройства в этом списке.

- Заблокированные вручную из Консоли администрирования.

- Авторизованные через Портал Авторизации. NAC-агенты никак не ограничивают устройства в этом списке.

- Заблокированные. Доступ к устройствам сети будет заблокирован.

- Заблокированные, кроме списка специальных адресов (тип ограничения «Разрешить доступ к сервисным адресам»).

  Устройства в списке получат доступ только к списку специальных адресов правила. Доступ к прочим адресам будет заблокирован.

- Устройства под действием ограничения «Перенаправлять на Портал авторизации» (самый низкий приоритет).

  Сразу после выполнения авторизации устройство добавляется в список «Авторизованные через Портал авторизации» и никак более не ограничивается NAC-агентом. До успешной авторизации на портале устройствам, попавшим под действие такого ограничения, всегда доступен список DNS-серверов сети.

При задании сетевых объектов следует обратить особое внимание на соответствие устройства типу сетевого объекта. Например, если сетевой объект относится к типу «Компьютеры», то критериям такого объекта будут удовлетворять только устройства, тип которых был определен в результате активного сканирования как «Компьютеры».

Включение NAC

Для включения NAC нужно выполнить следующую последовательность действий:

1. В Консоли администрирования создать политику Агента администрирования и в свойствах политики (раздел **Параметры**, блок параметров **Режим работы NAC**) включить NAC в режиме **Обычный**.
2. Назначить NAC-агенты в тех широковещательных доменах, в которых находятся устройства, сетевую активность которых предполагается ограничивать.
3. В свойствах Агента администрирования на соответствующих NAC-агентах выбрать режим работы NAC-агента **Основной**.

Типовые конфигурации NAC

Рассмотрим настройку NAC в нескольких типовых конфигурациях сети.

Конфигурация «Только корпоративные устройства»

В широковещательный домен Ethernet-сети подключается множество сетевых устройств: компьютеры, ноутбуки, сетевые принтеры. Администратору известно происхождение этих устройств, поэтому в Консоли администрирования в узле **Хранилища/Оборудование** он присваивает устройствам признак «Корпоративное». Администратор желает полностью ограничить доступ к ресурсам сети всем устройствам, не отмеченным как «Корпоративные» (компьютерам, файловым серверам, принтерам и так далее).

Для этого администратор должен выполнить следующие действия:

1. Включить NAC (см. раздел «Включение NAC» на стр. 78).

2. В свойствах политики создать сетевой объект «Некорпоративные устройства» (имя объекта может быть любым) с типом «Устройства любого типа». В список критериев добавить критерий «Устройства, не отмеченные как Корпоративные».

3. Создать правило ограничения доступа вида «Запретить доступ в сеть». В списке сетевых объектов правила добавить объект «Некорпоративные устройства».

Конфигурация «Доступ только к сетевому принтеру»

В широковещательный домен Ethernet-сети подключается множество сетевых устройств: компьютеры, ноутбуки, сетевые принтеры. Администратору не известно происхождение этих устройств, однако ему требуется разрешить доступ к сетевому принтеру с IP-адресом 192.168.1.135 всем устройствам, отмеченным как «Компьютер» в этом сегменте.

Для этого администратор должен выполнить следующие действия:

1. Включить NAC (см. раздел «Включение NAC» на стр. 78).

2. В свойствах политики создать объект «Сетевые адреса» с именем «Printer 192.168.1.135», описывающий IP-адрес 192.168.1.135.

3. Создать сетевой объект «Все компьютеры сегмента» с типом «Компьютеры». В список критериев добавить критерий «По сетевым атрибутам», описывающий диапазон IP-адресов сегмента (например, 192.168.1.2 – 192.168.1.254).

4. Создать правило ограничения доступа вида «Разрешить доступ к сетевым адресам». В список сетевых объектов правила добавить объект «Все компьютеры сегмента», а в список разрешенных сетевых адресов добавить объект «Printer 192.168.1.135».

Конфигурация «Доступ через Портал авторизации»

В широковещательный домен Ethernet-сети подключается множество сетевых устройств. Администратору не известно происхождение этих устройств, однако ему требуется разрешить доступ к ресурсам сети тем компьютерам, пользователи которых авторизовались на Портале авторизации.

Для этого администратор должен выполнить следующие действия:

1. Включить NAC (см. раздел «Включение NAC» на стр. 78).

2. В свойствах политики создать учетную запись Портала авторизации с именем «Guest».

3. Создать сетевой объект «Все компьютеры сегмента» с типом «Компьютеры». В список критериев добавить критерий «По сетевым атрибутам», описывающий диапазон IP-адресов сегмента (например, 192.168.1.2 – 192.168.1.254).

4. Создать правило ограничения доступа вида «Перенаправлять на Портал авторизации». В список сетевых объектов правила добавить объект «Все компьютеры сегмента».

На NAC-агенте автоматически запускается служба Kaspersky Captive Portal. Сетевой трафик устройств (определенных как «Компьютеры») будет перенаправлен на Портал авторизации, в результате чего в браузере пользователя будет открываться страница авторизации. Если пользователь введет в ней данные учетной записи Guest, то компьютер будет отмечен как авторизованный и пользователь получит полный доступ к ресурсам сети.

В браузерах пользователей Портала авторизации должен быть включен JavaScript.

ПОВСЕДНЕВНАЯ РАБОТА

В ЭТОМ РАЗДЕЛЕ

«СЕМАФОРЫ» В КОНСОЛИ АДМИНИСТРИРОВАНИЯ

Главным индикатором состояния Kaspersky Security Center и управляемых компьютеров является набор «семафоров» в рабочей области узла **Сервер администрирования** в Консоли администрирования (**Начало работы**). Всего имеется шесть «семафоров». Каждый «семафор» отвечает за отдельную область функциональности Kaspersky Security Center.

Таблица 7. Области ответственности «семафоров» в Консоли администрирования

Имя «семафора»	**Область ответственности «семафора»**
Развертывание	Установка Агента администрирования и антивируса на компьютеры сети предприятия
Управление компьютерами	Структура групп администрирования. Сканирование сети. Правила перемещения компьютеров
Защита компьютеров и поиск вирусов	Функциональность антивируса: состояние защиты, поиск вирусов
Обновление	Обновления и патчи
Мониторинг	Состояние защиты
Сервер администрирования	Функциональность и свойства Сервера администрирования

Каждый из «семафоров» имеет три состояния, которые кодируются цветами:

Таблица 8. Цветовые кодировки «семафоров»

Состояние	**Цветовая кодировка**	**Значение кодировки**
Информационное	Зеленый	Вмешательство администратора не требуется
Предупреждение	Желтый	Требуется вмешательство администратора
Критический	Красный	Имеются серьезные проблемы. Требуется вмешательство администратора для их решения

Следует поддерживать все шесть «семафоров» зелеными.

Удаленный доступ к управляемым компьютерам

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 компьютерами и Сервером администрирования. Агенты администрирования на управляемых компьютерах 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 подключение по UDP от Сервера администрирования к управляемому компьютеру по какой-то причине невозможно, 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 (антивируса или Агента администрирования), создание тоннеля и прочее. Для решения этой проблемы в свойствах управляемого компьютера (раздел **Общие**) нужно установить флажок **Не разрывать соединение с Сервером администрирования**. Общее количество компьютеров с установленным флажком **Не разрывать соединение с Сервером администрирования** не может превышать 300.

Проверка времени соединения компьютера с Сервером администрирования

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

Форсирование синхронизации

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

В контекстном меню управляемых компьютеров в Консоли администрирования компьютера в пункте меню **Все задачи** имеется команда **Синхронизировать принудительно**. В Kaspersky Security Center 10 SP1 при выполнении этой команды в свойствах компьютера устанавливается флажок **Назначена принудительная синхронизация**, затем Сервер администрирования пытается связаться с компьютером. 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 компьютере. Туннелирование используется для подключения клиентского приложения, находящегося на компьютере с установленной Консолью администрирования, к TCP-порту на управляемом компьютере если прямое соединение компьютера с Консолью администрирования с целевым компьютером 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.

Управление мобильными устройствами

В этом разделе

Сервер мобильных устройств Exchange ActiveSync

После успешной установки Сервер мобильных устройств Exchange ActiveSync отображается в Консоли администрирования Kaspersky Security Center в папке **Управление мобильными устройствами**.

Работа с политиками Exchange ActiveSync

После установки Сервера мобильных устройств Exchange ActiveSync в разделе **Почтовые ящики** окна свойств этого Сервера вы можете посмотреть информацию об учетных записях сервера Microsoft Exchange, полученных в результате опроса текущего домена либо леса доменов.

Кроме того, в окне свойств Сервера мобильных устройств Exchange ActiveSync вы можете использовать следующие кнопки:

- **Изменить профили** – позволяет открыть окно **Профили политики**, содержащее список политик, полученных с сервера Microsoft Exchange. В этом окне можно создавать, изменять или удалять политики Exchange ActiveSync. Окно **Профили политик** почти полностью соответствует окну редактирования политик в консоли Exchange Management Console.

- **Назначить профили мобильным устройствам** – позволяет назначить выбранную политику Exchange ActiveSync одной или нескольким учетным записям.

- **Вкл/выкл ActiveSync** – позволяет включить или выключить HTTP протокол Exchange ActiveSync для одной или нескольких учетных записей.

Настройка области сканирования

В свойствах установленного Сервера мобильных устройств Exchange ActiveSync в разделе **Параметры** вы можете настроить область сканирования. По умолчанию область сканирования – это текущий домен, в котором установлен Сервер мобильных устройств Exchange ActiveSync. При выборе значения **Весь лес доменов** область сканирования расширится на весь лес доменов.

Работа с EAS-устройствами

Устройства, полученные в результате сканирования сервера Microsoft Exchange, попадают в единый список устройств, который находится в узле **Управление мобильными устройствами** в папке **Мобильные устройства**.

Если вы хотите, чтобы в папке **Мобильные устройства** отображались только устройства Exchange ActiveSync (далее EAS-устройства), отфильтруйте список устройств по ссылке **Exchange ActiveSync (EAS)**, расположенной над ним.

Вы можете управлять EAS-устройствами с помощью команд. Например, команда **Удалить данные** позволяет удалить все данные с устройства и сбросить настройки устройства до заводских. Эта команда полезна в случае кражи или потери устройства, когда необходимо избежать попадания корпоративных или личных данных к третьим лицам.

Если с устройства были удалены все данные, то при следующем подключении этого устройства к серверу Microsoft Exchange с него снова будут удалены все данные. Команда будет повторяться до тех пор, пока устройство не будет удалено из списка устройств. Такое поведение обусловлено особенностями работы сервера Microsoft Exchange.

Чтобы удалить EAS-устройство из списка, в контекстном меню устройства выберите пункт **Удалить**. Если с EAS-устройства не будет удалена учетная запись Exchange ActiveSync, то при последующей синхронизации устройства с сервером Microsoft Exchange оно снова появится в списке устройств.

Сервер мобильных устройств iOS MDM

В этом разделе рассмотрены основные возможности работы с устройствами под управлением Сервера мобильных устройств iOS MDM (далее iOS MDM-устройства).

В этом разделе

Добавление нового устройства посредством публикации ссылки на профиль

В Консоли администрирования с помощью мастера подключения нового устройства администратор создает новый iOS MDM-профиль. В результате работы мастера будут выполнены следующие действия:

- iOS MDM-профиль автоматически опубликуется на веб-сервере.
- Пользователю будет отправлена ссылка на iOS MDM-профиль в SMS-сообщении или по электронной почте. После получения ссылки пользователь установит iOS MDM-профиль на устройстве.
- Устройство будет подключено к Серверу мобильных устройств iOS MDM.

См. также

Добавление нового устройства посредством установки профиля администратором

Чтобы подключить устройство к Серверу мобильных устройств iOS MDM с помощью установки iOS MDM-профиля на устройство, администратор должен выполнить следующие действия:

1. В Консоли администрирования открыть мастер подключения нового устройства.
2. Создать новый iOS MDM-профиль, установив в окне мастера создания профиля флажок **Показать сертификат по окончании ввода**.
3. Сохранить iOS MDM-профиль.
4. Установить iOS MDM-профиль на устройство пользователя с помощью утилиты Apple Configurator.

В результате устройство будет подключено к Серверу мобильных устройств iOS MDM.

См. также

Веб-сервер Kaspersky Security Center..... 75

Отправка команд на устройство

- *Чтобы отправить команду на iOS MDM-устройство, администратор должен выполнить следующие действия:*

1. В Консоли администрирования открыть узел **Управление мобильными устройствами**.
2. Выбрать папку **Мобильные устройства**.
3. В папке **Мобильные устройства** выбрать устройство, на которое необходимо отправить команды.
4. В контекстном меню устройства выбрать пункт **Команды для iOS-устройств** или **Управление устройством**, во всплывающем списке выбрать необходимую команду для отправки на устройство.

Проверка статуса исполнения отправленных команд

- *Чтобы проверить статус выполнения отправленной команды на устройстве, администратор должен выполнить следующие действия:*

1. В Консоли администрирования открыть узел **Управление мобильными устройствами**.
2. Выбрать папку **Мобильные устройства**.
3. В папке **Мобильные устройства** выбрать устройство, на котором необходимо проверить статус выполнения отправленных команд.
4. В контекстном меню устройства выбрать пункт **Показать журнал команд**.

NAC: события и типовые сценарии работы

Этот раздел содержит описания событий NAC, которые публикуют NAC-агенты, а также рекомендации по использованию NAC в рамках типовых сценариев работы с этой функциональностью.

События NAC

Доступны два вида событий, публикуемых NAC-агентами:

- Устройство обнаружено. Событие публикуется при первом обнаружении устройства NAC-агентом. Текст события содержит MAC-адрес и IP-адрес устройства (актуальный в момент обнаружения);
- Устройство авторизовано. Событие публикуется при каждой успешной авторизации устройства на Портале авторизации. Текст события содержит MAC-адрес и IP-адрес устройства (актуальный в момент обнаружения).

Типовые сценарии работы с NAC

В этом разделе описаны типовые сценарии использования NAC для контроля активности сетевых устройств.

В этом разделе

Аудит активности сетевых устройств

Аудит активности сетевых устройств можно проводить в режиме онлайн в Консоли администрирования в папке **Нераспределенные устройства/Сетевые устройства**. В рабочей области этой папки отображается список устройств, когда-либо обнаруженных в сети. Используя контекстное меню, можно заблокировать или разблокировать устройство вручную.

Также аудит активности сетевых устройств можно проводить в режиме оффлайн в Консоли администрирования в папке **Отчеты и уведомления/События**.

Ограничение сетевой активности устройства

Ограничить сетевую активность устройства можно двумя способами:

- В Консоли администрирования найти устройство в рабочей области папки **Нераспределенные устройства** и в контекстном меню устройства выбрать пункт **Заблокировать**;
- В политике Агента администрирования создать сетевой объект с типом **Устройства любого типа** и в список критериев добавьте известный набор критериев. Если известен MAC-адрес устройства, то это критерий **По сетевым атрибутам** со значением атрибута, равным MAC-адресу устройства.

Снятие ограничения сетевой активности устройства

Разблокировать устройство можно также двумя способами:

- Если устройство было вручную заблокировано администратором, то отменить блокировку можно, сняв флажок в пункте **Блокировка** контекстного меню устройства в папке **Нераспределенные устройства** в Консоли администрирования.

- Если сетевая активность устройства ограничена в результате действия правил NAC, то снять ограничение можно, добавив соответствующий сетевой объект в Белый список устройств в параметрах Агента администрирования (раздел **Управление доступом (NAC)**), либо изменив сетевой объект так, чтобы устройство более не удовлетворяло его критериям.

Определение работоспособности правила NAC

По завершению настройки политика с правилами NAC (далее также «NAC-политика») доставляется на NAC-агенты. Применение политики к конкретному устройству начинается сразу после обнаружения какой-либо исходящей сетевой активности этого устройства.

Чтобы определить, действует ли правило NAC (и какое именно правило действует) на устройство в сети, необходимо знать, в рамках какого широковещательного домена работает это устройство и иметь удаленный доступ к NAC-агенту, применяющему NAC-политику в этом сегменте.

Например, в широковещательном домене *X* работает устройство *Y* с MAC-адресом *Z*. В политике Агента администрирования это устройство описано (с помощью сетевого объекта) и для него создано правило ограничения доступа в сеть *R*. В широковещательном домене *X* работает NAC-агент *E*. Аудит активности NAC-агента можно провести с помощью файла $klnac.log. Порядок аудита NAC-агента E описан ниже.

Аудит активности NAC-агента

Чтобы провести аудит активности NAC-агента E, администратор должен выполнить следующие действия:

1. Получить удаленный доступ к файловой системе NAC-агента E.

2. В папке %WINDIR%\Temp файл найти файл $klnac.log, затем открыть его любым текстовым редактором, поддерживающим формат Unix®, например, wordpad.

3. В текстовом файле найти строки вида Rule activity, где после строки RuleName: следует имя применяемого правила *R*, и далее после знака минус описаны сетевые атрибуты устройства, активность которого ограничена: MAC SRC, IPv4 SRC. Если MAC-адрес *Z* найден, значит, правило *R* применено и работает.

   Также в файле $klnac.log можно увидеть, когда устройство впервые было обнаружено, и к какому сетевому ресурсу оно на тот момент обращалось (в строках вида Device discovery).

ПРИЛОЖЕНИЯ

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

- сведения об ограничениях текущей версии программы (максимальные количества управляемых компьютеров, 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 SP1.

Таблица 9. Ограничения Kaspersky Security Center 10 SP1

Тип ограничения	Значение
Максимальное количество управляемых компьютеров	50 000
Максимальное количество компьютеров 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	2 000

Тип ограничения	Значение
Максимальное количество задач	2 000
Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, компьютеров 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 компьютеров, которых 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 тысяч компьютеров.

Сервер администрирования и SQL Server находятся на одном компьютере

Таблица 10. Аппаратные требования к компьютеру

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 компьютерах

Таблица 11. Аппаратные требования к компьютеру 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 12. Аппаратные требования к компьютеру 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 компьютеров;
- задача резервного копирования сохраняет резервные копии на файловый ресурс, расположенный на отдельном сервере;
- период синхронизации Агентов администрирования настроен в соответствии с таблицей ниже.

Таблица 13. Период синхронизации Агентов администрирования

Период синхронизации, минуты	Количество управляемых компьютеров
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 компьютере 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 компьютере 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 компьютеров.
«E»	Количество сохраняемых событий.
«A»	Суммарное количество объектов Active Directory: • учетных записей компьютеров; • 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 компьютера с Сервером администрирования

Место на диске в директории %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit на компьютере 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 компьютере 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 компьютером (на компьютере установлены Агент администрирования Kaspersky Security Center 10 MR1, сборка 10.1.249 и Kaspersky Endpoint Security 10 MR1, сборка 10.2.1.23).

Таблица 14. Среднесуточный трафик: Kaspersky Security Center 10 MR1

	От Сервера к управляемому компьютеру (download)	От управляемого компьютера 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 SP1 и управляемым компьютером (установлены Агент администрирования Kaspersky Security Center 10 SP1 и Kaspersky Endpoint Security 10 SP1).

Таблица 15. Среднесуточный трафик: Kaspersky Security Center 10 SP1

	От Сервера к управляемому компьютеру (download)	От управляемого компьютера 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 16. 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.
Несовместимая платформа	Инсталляционный пакет не предназначен для данной платформы. Используйте соответствующий инсталляционный пакет.
Несовместимая программа	На компьютере 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.

Проблема	Типовая причина проблемы и вариант решения
Незавершенная установка	Предыдущая установка или удаление программы не было штатно завершено. Для завершения предыдущей установки или удаления программы, выполненного на данном компьютере, необходимо перезагрузить ОС и повторить процесс установки.
Не та версия инсталляционного приложения	Установка данного инсталляционного пакета не поддерживается версией инсталляционного приложения, установленного на компьютере.
Инсталляция уже запущена	На компьютере 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 компьютере запрещена политикой.
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 (объём 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 компьютера	Требуется повторный запуск инсталлятора программы после перезагрузки компьютера.
Для продолжения установки требуется перезагрузка компьютера	Для продолжения работы инсталлятора продукта требуется перезагрузка компьютера.

Неверно выполнено копирование образа жесткого диска

Если копирование образа жесткого диска с установленным Агентом администрирования было выполнено без учета правил развертывания (см. раздел «Развертывание захватом и копированием образа жесткого диска компьютера» на стр. 45), часть компьютеров в Консоли администрирования может отображаться как один значок компьютера, постоянно меняющий имя.

Можно использовать следующие способы решения этой проблемы:

- Удаление Агента администрирования.

  Этот способ является самым надежным. На компьютерах, 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 компьютеры неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

- Запуск утилиты klmover с ключом «-dupfix».

  На проблемных компьютерах (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 компьютеры неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

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

- Ужесточение правила обнаружения неправильно скопированных компьютеров.

  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 компьютера приводило к автоматической «починке» таких Агентов администрирования (предполагается, что скопированные компьютеры имеют различные NetBIOS-имена).

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

  - Если на компьютере 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 компьютере 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 Сервером мобильных устройств Exchange ActiveSync

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием Сервера мобильных устройств Exchange ActiveSync.

Ошибка во время установки Сервера мобильных устройств Exchange ActiveSync

Если во время локальной или удаленной установки возникла ошибка, то причину ошибки можно узнать, открыв файл error.log, который расположен на компьютере, где производилась установка продукта, по пути C:\Windows\Temp\klmdm4exch-2014-11-28-15-56-37\ (где цифры – это дата и время установки продукта). Как правило, информации из файла error.log достаточно для решения возникшей проблемы.

В таблице ниже приведены примеры типичных ошибок, регистрируемых в файле error.log.

Таблица 17. Типичные ошибки

Ошибка	Описание	Причина
Error occurred on installation step: 'Test connection to PowerShell'	Error: Processing data from remote server failed with the following error message: The user «oreh-security.ru/Users/TestInstall» isn't assigned to any management roles.	Аккаунт, под которым производилась установка продукта, не обладает ролью Organization Management.
Error occurred on installation step: 'Test connection to PowerShell'	Connecting to remote server failed with the following error message: The WinRM client cannot process the request. The authentication mechanism requested by the client is not supported by the server or unencrypted traffic is disabled in the service configuration. Verify the unencrypted traffic setting in the service configuration or specify one of the authentication mechanisms supported by the server. To use Kerberos, specify the computer name as the remote destination. Also verify that the client computer and the destination computer are joined to a domain. To use Basic, specify the computer name as the remote destination, specify Basic authentication and provide user name and password. Possible authentication mechanisms reported by server: Digest For more information, see the about_Remote_Troubleshooting Help topic.	Механизм аутентификации Windows в настройках веб-сервера IIS для виртуальной директории PowerShell не включен.

Список устройств и почтовых аккаунтов пуст

Причину, из-за которой не удается получить список устройств и почтовых аккаунтов, можно узнать из событий, сохраненных в Консоли администрирования в папке **Отчеты и уведомления/События/Отказы функционирования**. Если в событиях нет информации, необходимо проверить подключение между Агентом администрирования компьютера, на котором развернут Сервер мобильных устройств Exchange ActiveSync и Сервером администрирования.

Проблемы с Сервером мобильных устройств iOS MDM

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием Сервера мобильных устройств iOS MDM, а также о способах их решения.

В этом разделе

Портал support.kaspersky.com

Информация о некоторых проблемах, возникающих при использовании Сервера мобильных устройств iOS MDM, приведена в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.com/ks10mob.

Проверка доступности сервиса APN

Для проверки доступности сервиса APN вы можете использовать следующие команды утилиты Telnet:

- Со стороны веб-сервиса iOS MDM:

```
$ telnet gateway.push.apple.com 2195
```

- Со стороны iOS MDM-устройства (проверку необходимо провести из сети, в которой находится устройство):

```
$ telnet 1-courier.push.apple.com 5223
```

Рекомендуемая последовательность действий для решения проблем с веб-сервисом iOS MDM

Если при использовании веб-сервиса iOS MDM возникают проблемы, выполните следующие действия:

1. Проверьте, что сертификаты корректны.
2. Проверьте события Консоли администрирования на наличие ошибок и невыполненных команд со стороны Сервера мобильных устройств iOS MDM.
3. Проверьте устройство с помощью консоли приложения iPhone Configuration Utility.
4. Проверьте файлы трассировок веб-сервиса iOS MDM: внутренние сервисы, такие как RPC-сервис и веб-сервис (100 потоков), должны быть успешно запущены.

Проверка корректности сертификата веб-сервиса iOS MDM с помощью мультиплатформенной утилиты OpenSSL

Пример команды:

$ openssl s_client -connect mymdm.mycompany.com:443

Результат выполнения:

CONNECTED(00000003)

...

Certificate chain

0 s:/C=RU/ST=Msk/L=Msk/O=My Company/OU=AdminKit/CN=mymdm.mycompany.com

i:/CN=Kaspersky iOS MDM Server CA

...

.

Проверка трассировок веб-сервиса iOS MDM

О том, как получить трассировки веб-сервиса iOS MDM, см. статью в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.com/9792.

Пример успешных трассировок:

I1117 20:58:39.050226 7984] [MAIN]: Starting service...

I1117 20:58:39.050226 7984] [RPC]: Starting rpc service...

...

I1117 20:58:39.081428 7984] [RPC]: Rpc service started

I1117 20:58:39.081428 3724] [WEB]: Starting web service...

I1117 20:58:39.455832 3724] [WEB]: Starting thread [T000]

I1117 20:58:39.455832 3724] [WEB]: Starting thread [T001]

...

I1117 20:58:39.455832 3724] [WEB]: Starting thread [T099]

Пример трассировок с занятым портом:

[WEB]: Starting web service...

Error 28 fault: SOAP-ENV:Server [no subcode] «Only one usage of each socket address (protocol/network address/port) is normally permitted.»

Detail: [no detail]

[WEB]: Web service terminated

Проверка трассировок с помощью консоли приложения iPhone Configuration Utility

Пример успешных трассировок:

Службы, отвечающие за MDM – profiled, mdmd

mdmd[174] <Notice>: (Note) MDM: mdmd starting...

mdmd[174] <Notice>: (Note) MDM: Looking for managed app states to clean up

profiled[175] <Notice>: (Note) profiled: Service starting...

mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note) MDM: Polling MDM server https://10.255.136.71 for commands

mdmd[174] <Notice>: (Note) MDM: Transaction completed. Status: 200

mdmd[174] <Notice>: (Note) MDM: Attempting to perform MDM request: DeviceLock

mdmd[174] <Notice>: (Note) MDM: Handling request type: DeviceLock

mdmd[174] <Notice>: (Note) MDM: Command Status: Acknowledged

profiled[175] <Notice>: (Note) profiled: Recomputing passcode requirement message

profiled[175] <Notice>: (Note) profiled: Locking device

mdmd[174] <Notice>: (Note) MDM: Transaction completed. Status: 200

mdmd[174] <Notice>: (Note) MDM: Server has no commands for this device.

mdmd[174] <Notice>: (Note) MDM: mdmd stopping...

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 Cloud Messaging

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

Проверка доступности сервиса Google Cloud Messaging

Для проверки доступности сервиса Google Cloud Messaging со стороны Kaspersky Security Center (см. раздел «Использование Google Cloud Messaging» на стр. 73) вы можете использовать команду утилиты Telnet:

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

Проблемы с управлением доступом в сеть (NAC)

Этот раздел содержит информацию об ошибках и проблемах, связанных с управлением доступом в сеть (NAC).

NAC-агент на Агенте администрирования не запускается

Вероятная причина:

- компоненты NAC не установлены или установлены с ошибками. Описание ошибки должно присутствовать в Kaspersky Event Log.

Вариант решения:

- устраните причину ошибки (если это возможно) и перезапустите службу Kaspersky Network Agent.

NAC в политике настроен, NAC-агент включен, но правило NAC не применяется (активность устройства не ограничена NAC-агентом)

Вероятная причина:

- неверная настройка правил NAC в политике.

Варианты решения:

- проверьте, что устройство удовлетворяет критериям, описанным в сетевом объекте;
- проверьте, что NAC-агент включен в режиме «Обычный» и в Kaspersky Event Log на хосте нет никаких сообщений об ошибках;
- проверьте, что компьютер с NAC-агентом работает в том же широковещательном домене, что и устройство.

NAC в политике настроен, NAC-агент работает, правило применяется, однако доступ устройства к сетевым ресурсам все равно не ограничен (в виртуальной среде)

Вероятная причина:

- неверные параметры сетевой инфраструктуры.

Варианты решения:

- Для виртуальной среды VMware ESXi™:
  - на виртуальных свитчах опции Promiscuous Mode, MAC Address Changes и Forged Transmits должны быть настроены в режиме Accept.
- Для виртуальной среды Microsoft Hyper-V:
  - на сервере с установленной ролью Hyper-V для каждой виртуальной машины <vm_name> необходимо выполнить: Set-VMNetworkAdapter –VMName <vm_name> –MacAddressSpoofing On.

Высокая загрузка ЦПУ в режиме ядра

Вероятная причина:

- слишком высокая широковещательная активность в домене сети (несколько тысяч устройств) или NAC-агент сильно загружен другими низкоуровневыми операциями (дисковый ввод-вывод, файловые сетевые сервисы и тому подобное).

Варианты решения:

- перенесите NAC-агент на другой, менее загруженный компьютер;
- перенесите или отключите сервисы, требовательные к ЦПУ в режиме ядра.

Правило «Перенаправлять на Портал авторизации» не работает

Вероятная причина:

- неверно настроены параметры NAC в политике;
- неверные настройки сетевой инфраструктуры.

Варианты решения:

- проверьте, что правило работоспособно и применяется в отношении устройства (см. раздел «Определение работоспособности правила NAC» на стр. 86);
- проверьте, что на NAC-агенте работает служба Kaspersky Captive Portal и в Kaspersky Event Log нет ошибок связанных с ней;
- проверьте, что порт TCP 80 (по умолчанию используемый службой Kaspersky Captive Portal) не занят другими веб-серверами. Если порт занят, то освободите его (перенесите веб-сервер на другой хост в сети) и перезапустите службу Kaspersky Captive Portal. Освободив порт и запустив службу, проверьте, что в браузере на компьютере с NAC-агентом при переходе по ссылке вида http://<enforcer_host> открывается страница авторизации.

Сканирование завершено, однако тип устройства или версия ОС не определены

Вероятная причина:

- служба Kaspersky Network Scanner не работает;
- сетевые порты на устройстве закрыты.

Варианты решения:

- проверьте, что служба KNS запускается и в Kaspersky Event Log отсутствует описание ошибки. Если ошибка есть, то попробуйте устранить ее (если это возможно) и перезапустить службу;
- убедитесь, что на устройстве выключен сетевой экран, препятствующий активному сканированию сетевых портов.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

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

В ЭТОМ РАЗДЕЛЕ

О ТЕХНИЧЕСКОЙ ПОДДЕРЖКЕ

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки «Лаборатории Касперского». 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 «Лаборатории Касперского» по телефону;
- отправить запрос в Службу технической поддержки «Лаборатории Касперского» через портал Kaspersky CompanyAccount.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ПО ТЕЛЕФОНУ

В большинстве регионов вы можете позвонить специалистам Службы технической поддержки «Лаборатории Касперского». 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). Эти правила содержат информацию о том, в какие часы вы можете позвонить в Службу технической поддержки «Лаборатории Касперского», а также о том, какие данные потребуются специалисту Службы технической поддержки «Лаборатории Касперского», чтобы помочь вам.

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 их 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, General Dynamics, Facebook, Juniper Networks, Lenovo, H3C, 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.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Вирусная лаборатория:	http://newvirus.kaspersky.ru (для проверки подозрительных файлов и веб-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.