kaspersky

Kaspersky Security для виртуальных сред 6.2 Легкий агент

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 6.2

kaspersky

Уважаемый пользователь!

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

Внимание! Права на этот документ являются собственностью АО "Лаборатория Касперского" (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

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

Документ может быть изменен без предварительного уведомления.

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

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

Дата редакции документа: 24.01.2025

© 2025 АО "Лаборатория Касперского"

https://www.kaspersky.ru
https://support.kaspersky.ru

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

kaspersky

Содержание

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Security для виртуальных сред 6.2 Легкий агент" (далее также "Kaspersky Security", "решение").

Подготовительные процедуры изложены в разделах "Подготовка к установке решения", "Установка решения" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки решения, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки решения.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование решения, а также инструкции и указания по безопасному использованию решения.

В документе также содержатся разделы с дополнительной информацией о решении.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Security, а также поддержка организаций, использующих Kaspersky Security. Технические специалисты должны иметь опыт работы с операционными системами Microsoft® Windows® и Linux®, с виртуальными инфраструктурами и системой удаленного централизованного управления приложениями "Лаборатории Касперского" Kaspersky Security Center.

Kaspersky Security обеспечивает защиту виртуальных машин на следующих платформах виртуализации:

- VMware™ vSphere.
- XenServer®.
- Microsoft® Hyper-V®.
- KVM (Kernel-based Virtual Machine).
- Proxmox VE.
- Базис.
- Скала-Р.
- HUAWEI FusionSphere.
- Nutanix Acropolis.
- Enterprise Cloud Platform VeiL.
- SharxBase.
- Облачная платформа ТИОНИКС.
- OpenStack®.
- Альт Сервер Виртуализации.
- Программный комплекс средств виртуализации Брест.
- Среда виртуализации zVirt.
- Система управления средой виртуализации ROSA Virtualization.
- РЕД Виртуализация.
- Astra Linux.

- Облачная платформа SpaceVM.
- Облачная платформа Базис.DynamiX.
- VMmanager Infrastructure.
- Numa vServer.
- Облачная платформа VK Cloud.
- Система серверной виртуализации "Р-Виртуализация".

Имеются ограничения в установке и работе решения в виртуальных инфраструктурах на платформах Enterprise Cloud Platform VeiL, SharxBase, Программный комплекс средств виртуализации Брест, Среда виртуализации zVirt, Система управления средой виртуализации ROSA Virtualization, РЕД Виртуализация, VMmanager Infrastructure, Облачная платформа SpaceVM, Облачная платформа Базис.DynamiX и Система серверной виртуализации "Р-Виртуализация". Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).

Решение Kaspersky Security оптимизировано для обеспечения максимальной производительности виртуальных машин, которые находятся под защитой решения.

Решение позволяет защищать виртуальные машины с гостевыми операционными системами для серверов и гостевыми операционными системами для рабочих станций.

Решение Kaspersky Security может использоваться в *режиме мультитенантности* (см. раздел "*Использование Kaspersky Security для виртуальных сред 6.2 Легкий агент в режиме мультитенантности*" на стр. 191). Этот вариант использования решения позволяет обеспечивать защиту изолированных виртуальных инфраструктур организаций-тенантов или подразделений одной организации (далее также "тенантов").

В состав решения входят следующие компоненты:

- Сервер защиты Kaspersky Security (далее также "*Сервер защиты*"). Компонент представляет собой службу, установленную на специальной виртуальной машине – SVM (secure virtual machine, виртуальная машина защиты). SVM требуется развернуть на гипервизорах в виртуальной инфраструктуре в ходе установки решения Kaspersky Security.
- Легкий агент Kaspersky Security (далее также "*Легкий агент*"). Компонент представляет собой приложение, предназначенное для установки на виртуальные машины. Легкий агент требуется установить на каждую виртуальную машину, которую вы хотите защищать с помощью решения Kaspersky Security.

  В качестве Легкого агента для Linux в составе решения Kaspersky Security используется приложение Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).

  В качестве Легкого агента для Windows в составе решения Kaspersky Security используется приложение Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).
- Сервер интеграции Kaspersky Security для виртуальных сред Легкий агент (далее также "*Сервер интеграции*"). Компонент представляет собой приложение, предназначенное для установки на устройстве с операционной системой Linux или на устройстве с операционной системой Windows в вашей инфраструктуре. Сервер интеграции осуществляет взаимодействие между компонентами решения Kaspersky Security и виртуальной инфраструктурой.

Для установки и управления работой решения Kaspersky Security требуется система удаленного централизованного управления приложениями "Лаборатории Касперского" Kaspersky Security Center. Вы можете использовать Kaspersky Security Center Windows или Kaspersky Security Center Linux.

kaspersky

Источники информации о Kaspersky Security

Указанные источники информации о решении Kaspersky Security (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

Страница Kaspersky Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security (http://www.kaspersky.ru/business-security/virtualization-light-agent) вы можете получить общую информацию о решении, его возможностях и особенностях работы.

Страница Kaspersky Security в Базе знаний

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

На странице Kaspersky Security в Базе знаний (https://support.kaspersky.ru/ksv-light-agent/6.2?page=kb) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании решения.

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

Обсуждение приложений "Лаборатории Касперского" на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме (https://forum.kaspersky.com/forum/%D1%80%D1%83%D1%81%D1%81%D0%BA%D0%BE%D1%8F%D0%B7%D1%8B%D1%87%D0%BD%D1%8B%D0%B9-%D1%84%D0%BE%D1%80%D1%83%D0%BC-162/).

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

kaspersky

О решении

Решение представляет собой средство антивирусной защиты и средство контроля подключения съемных машинных носителей информации и предназначено для применения на серверах и автоматизированных рабочих местах информационных систем под управлением ОС семейства Linux и Windows.

Основными угрозами, для противостояния которым используется Kaspersky Security, являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и(или) съемных машинных носителей информации, компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации.

В решении реализованы следующие функции безопасности:

- разграничение доступа к управлению;
- управление работой;
- управление параметрами;
- управление установкой обновлений (актуализации) БД ПКВ;
- аудит безопасности;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация;
- контроль целостности;
- контроль подключения съемных машинных носителей информации.

Основные функции защиты и контроля виртуальных машин обеспечиваются функциональными компонентами и задачами Легкого агента для Linux и Легкого агента для Windows.

В качестве Легкого агента для Linux в составе решения Kaspersky Security используется приложение Kaspersky Endpoint Security для Linux. Описание функций приложения Kaspersky Endpoint Security для Linux см. в справке приложения (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).

В качестве Легкого агента для Windows в составе решения Kaspersky Security используется приложение Kaspersky Endpoint Security для Windows. Описание функций приложения Kaspersky Endpoint Security для Windows см. в справке приложения (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Имеются следующие особенности работы приложений Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows в режиме Легкого агента:

- Активация приложения выполняется на стороне Сервера защиты.
- Управление обновлением баз и программных модулей приложения выполняется на стороне Сервера защиты. Приложение получает обновления из папки на SVM. Выбрать другой источник обновления невозможно.
- Не поддерживается использование облачных баз.
- Приложение взаимодействует с серверами KSN с помощью прокси-сервера KSN. Взаимодействие с KSN напрямую не поддерживается.

- Использование прокси-сервера приложения при подключении к Серверу интеграции, к SVM и к серверам KSN не поддерживается.
- Недоступно управление приложением с помощью Kaspersky Security Center Cloud Console.
- Только для приложения Kaspersky Endpoint Security для Linux: недоступно управление приложением с помощью графического пользовательского интерфейса.
- Только для приложения Kaspersky Endpoint Security для Windows:
  - Невозможно установить компоненты шифрования данных и Адаптивный контроль аномалий.
  - Встроенный агент EDR Expert не работает в режиме Легкого агента.

Для поддержки компонентов решения Kaspersky Security в актуальном состоянии и расширения возможностей использования решения предусмотрены дополнительные функции решения:

- **Активация**. Использование решения по коммерческой лицензии обеспечивает полнофункциональную работу компонентов решения и доступ к обновлению баз и программных модулей решения.
- **Обновление баз и программных модулей**. Обновление баз и программных модулей решения обеспечивает актуальность защиты виртуальных машин от вирусов и других приложений, представляющих угрозу.
- **Использование Kaspersky Security Network в работе компонентов решения**. Использование облачной базы знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения позволяет повысить эффективность защиты виртуальных машин и данных пользователей, обеспечивает более высокую скорость реакции на различные угрозы и снижение количества ложных срабатываний.
- **Отчеты и уведомления** (на стр. 172). В процессе работы компонентов решения возникают различного рода события. Вы можете получать уведомления о событиях и формировать на основе событий отчеты.

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

В этом разделе

О подключении Легкого агента к SVM

Для функционирования решения Kaspersky Security требуется постоянное взаимодействие между Легким агентом и Сервером защиты. Если соединение с Сервером защиты отсутствует, Легкий агент не может передавать фрагменты файлов на проверку Серверу защиты, проверка не выполняется. Если в ходе

выполнения запущенных задач проверки Легкий агент теряет соединение с Сервером защиты более чем на 5 минут, выполнение задач проверки приостанавливается, задачи завершаются с ошибкой.

Для взаимодействия с Сервером защиты Легкий агент устанавливает и поддерживает подключение к SVM, на которой установлен этот Сервер защиты.

Легкий агент может подключаться только к SVM, версия которой совместима с версией Легкого агента.

Чтобы подключиться к SVM, Легкий агент должен получить информацию об SVM, к которым доступно подключение (см. раздел "Об обнаружении SVM" на стр. 15). Легкий агент выбирает оптимальную для подключения SVM из числа доступных для подключения в соответствии с алгоритмом выбора SVM (см. раздел "Об алгоритмах выбора SVM" на стр. 16).

Независимо от используемого алгоритма при выборе SVM Легкие агенты также учитывают следующие параметры:

- Наличие действующей лицензии (см. раздел "О лицензии" на стр. 79) (на SVM добавлен лицензионный ключ, который не находится в списке запрещенных ключей, и срок действия лицензии, связанной с ключом, не истек). Легкий агент в первую очередь подключается к SVM, на которой решение активировано (добавлен ключ).
- Тип лицензионного ключа, добавленного на SVM. Если вы используете схему лицензирования по количеству виртуальных машин, защищаемых с помощью решения (ключи для серверов и ключи для рабочих станций), Легкий агент в первую очередь подключается к SVM, на которой тип ключа соответствует операционной системе, установленной на виртуальной машине с Легким агентом.
- Защита соединения между Легким агентом и Сервером защиты (на стр. 144). Легкий агент, для которого включена защита соединения, может подключаться только к тем SVM, на которых включено шифрование канала передачи данных между Легким агентом и Сервером защиты. Легкий агент, для которого выключена защита соединения, может подключаться только к тем SVM, на которых шифрование канала выключено или разрешено незащищенное соединение между Легким агентом и Сервером защиты.
- Теги для подключения к SVM (см. раздел "Настройка использования тегов для подключения" на стр. 142). Если Легкому агенту назначен тег, Легкий агент может подключаться только к тем SVM, на которых настроено использование этого тега для подключения.

Возможность подключения Легкого агента к SVM также зависит от параметров загрузки обновлений на SVM (см. раздел "Настройка параметров загрузки обновлений на SVM" на стр. 157), которые задаются в политике для Сервера защиты. Подключиться к SVM могут только те Легкие агенты, для которых на эту SVM загружаются обновления баз.

Рекомендуется учитывать, что объем доступной на Легком агенте функциональности зависит от лицензии, по которой решение активировано на SVM:

- Если вы хотите использовать функциональность Легких агентов, включенную в лицензию Enterprise, вам нужно подключить Легкий агент к SVM, на которой решение активировано по лицензии Enterprise. При подключении к SVM, на которой решение активировано по лицензии Standard, объем доступной на Легком агенте функциональности уменьшается.
- Если вы хотите использовать дополнительную функциональность Легких агентов (например, интеграцию с решениями Detection and Response от "Лаборатории Касперского" или интеграцию с Kaspersky Unified Monitoring and Analysis Platform), вам нужно подключить Легкий агент к SVM, на которой решение активировано по лицензии, включающей эту дополнительную функциональность, или к SVM, на которую добавлен отдельный лицензионный ключ для активации нужной

дополнительной функциональности. При отключении Легкого агента от текущей SVM и подключении к SVM, на которой не активирована дополнительная функциональность, на Легком агенте эта функциональность становится недоступна.

Чтобы предотвратить переключение Легких агентов между SVM с разными видами лицензий, вы можете ограничить для Легкого агента количество доступных SVM с помощью тегов для подключения (см. раздел "Настройка использования тегов для подключения" на стр. 142) или списка SVM для подключения (см. раздел "Настройка параметров обнаружения SVM" на стр. 140).

Вы можете получить информацию о состоянии подключения Легкого агента к SVM следующими способами:

- Для Легкого агента для Linux: с помощью команды приложения Kaspersky Endpoint Security для Linux `kesl-control --svm-info`. Подробнее см. в справке приложения Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).
- Для Легкого агента для Windows:
  - в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows;
  - с помощью команды приложения Kaspersky Endpoint Security для Windows `avp.com SVMINFO`.

  Подробнее см. в справке приложения Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Информация об отсутствии подключения Легкого агента к SVM отображается в Kaspersky Security Center с помощью статуса клиентского устройства: если подключение к SVM не установлено, статус защищенной виртуальной машины изменяется на *Критический*. Информация о потере и восстановлении соединения Легкого агента с SVM сохраняется в виде событий в Kaspersky Security Center.

Не рекомендуется использовать для SVM и виртуальных машин с установленным Легким агентом для Linux снимки виртуальных машин, сделанные на запущенной гостевой ОС (live-snapshots). Восстановление из такого снимка приводит к потере соединения между Легкими агентами и SVM и к снижению производительности виртуальной инфраструктуры. Вы можете использовать снимки виртуальных машин, сделанные на запущенной гостевой ОС, только если в параметрах Легкого агента включен информирующий режим работы. См. подробнее в справке Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).

Об обнаружении SVM

Легкий агент может обнаруживать SVM, работающие в сети, одним из следующих способов:

- С помощью Сервера интеграции. SVM передают информацию о себе на Сервер интеграции. Сервер интеграции формирует список доступных для подключения SVM и предоставляет его Легким агентам.

  В виртуальной инфраструктуре большого размера под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС вы можете ограничивать размер списка доступных для подключения SVM, который Сервер интеграции передает Легким агентам. Сервер интеграции может передавать информацию только о том количестве доступных

для подключения SVM, которое вы указали в конфигурационном файле Сервера интеграции (см. раздел "Настройка параметров обнаружения SVM" на стр. 140).

Для использования этого способа обнаружения SVM требуется подключение SVM и Легких агентов к Серверу интеграции.

- С использованием списка адресов SVM. Вы можете задать список адресов SVM, к которым могут подключаться Легкие агенты.

Если для Легкого агента применяется расширенный алгоритм выбора SVM (см. раздел "Об алгоритмах выбора SVM" на стр. 16), а на SVM включен режим защиты больших инфраструктур (см. раздел "Защита больших инфраструктур" на стр. 153), в качестве способа обнаружения SVM Легкими агентами рекомендуется выбрать Сервер интеграции.

Каждый Легкий агент может использовать только один из двух возможных способов обнаружения SVM.

Вы можете настраивать параметры обнаружения SVM Легкими агентами следующими способами:

- Для Легкого агента для Linux: в политике приложения Kaspersky Endpoint Security для Linux (см. раздел "Настройка параметров обнаружения SVM" на стр. 140).
- Для Легкого агента для Windows:
  - в политике приложения Kaspersky Endpoint Security для Windows (см. раздел "Настройка параметров обнаружения SVM" на стр. 140);
  - в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows.

Об алгоритмах выбора SVM

Легкие агенты могут применять один из следующих алгоритмов выбора SVM для подключения:

- **Стандартный алгоритм выбора SVM**

  Если применяется этот алгоритм, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является *локальной* для Легкого агента.

  Локальность SVM относительно Легкого агента определяется в зависимости от вида виртуальной инфраструктуры:

  - В виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer локальной для Легкого агента считается SVM, которая развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом.
  - В виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС вы можете указывать, как определяется локальность SVM относительно Легкого агента, с помощью параметра `StandardAlgorithmSvmLocality` в секции `HypervisorSpecificSettings:Openstack` в конфигурационном файле Сервера интеграции appsettings.json. В зависимости от версии Сервера интеграции файл расположен по следующему пути:
    - /var/opt/kaspersky/viis/common/ – файл Сервера интеграции на базе Linux.

- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ – файл Сервера интеграции на базе Windows.

Параметр `StandardAlgorithmSvmLocality` может принимать следующие значения:

- `ServerGroup` – если установлено это значение, локальной для Легкого агента считается SVM, которая находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом. Это значение используется по умолчанию.
- `Project` – если установлено это значение, локальной для Легкого агента считается SVM, которая развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом.
- `AvailabilityZone` – если установлено это значение, локальной для Легкого агента считается SVM, которая расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом.

Если нет доступных для подключения локальных SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре.

Локальность SVM относительно Легкого агента не определяется, если для Сервера защиты на этой SVM включен режим защиты больших инфраструктур (см. раздел "Защита больших инфраструктур" на стр. 153). В этом случае рекомендуется использовать расширенный алгоритм выбора SVM и выбрать Сервер интеграции в качестве способа обнаружения SVM (см. раздел "Об обнаружении SVM" на стр. 15).

- **Расширенный алгоритм выбора SVM**

Если применяется этот алгоритм, вы можете определять следующие параметры выбора SVM:

- учитывать или игнорировать расположение SVM в инфраструктуре при выборе SVM для подключения;
- если расположение SVM учитывается, как определять локальность SVM относительно Легкого агента.

Если Легкие агенты игнорируют расположение SVM в инфраструктуре, то Легкие агенты смогут подключаться к любым доступным для подключения SVM.

Если Легкие агенты должны учитывать расположение SVM в инфраструктуре, вам нужно выбрать тип расположения SVM (см. раздел "Настройка алгоритма выбора SVM" на стр. 147), который будет учитываться при определении локальности SVM относительно Легкого агента. Локальность SVM относительно Легкого агента определяется по-разному в зависимости от виртуальной инфраструктуры.

В виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer SVM может считаться локальной для Легкого агента в одном из следующих случаев:

- SVM развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом.
- SVM развернута на том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом.

- SVM развернута в том же дата-центре, что и виртуальная машина с установленным Легким агентом.

В виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС SVM может считаться локальной для Легкого агента в одном из следующих случаев:

- SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом.
- SVM развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом.
- SVM расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом.

Если Легкие агенты учитывают расположение SVM в инфраструктуре при выборе SVM для подключения, то Легкие агенты могут подключаться только к тем SVM, которые являются локальными.

Например, если вы указали в качестве типа расположения SVM кластер гипервизоров, то локальными для Легкого агента будут считаться все SVM, развернутые на этом кластере гипервизоров, и Легкий агент сможет подключаться к только к одной из этих SVM. Если в том же кластере, в котором работает Легкий агент, нет доступных для подключения SVM, Легкий агент не будет подключаться к SVM.

При выборе SVM Легкие агенты также учитывают количество подключенных Легких агентов, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM.

Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM (см. раздел "Об обнаружении SVM" на стр. 15) выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур (см. раздел "Защита больших инфраструктур" на стр. 153), то подключение Легкого агента к этой SVM возможно, только если Легкий агент игнорирует расположение SVM.

Вы можете указать, какой алгоритм выбора SVM (см. раздел "Настройка алгоритма выбора SVM" на стр. 147) будут использовать Легкие агенты, и настроить параметры применения расширенного алгоритма выбора SVM.

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы решения, а также указания по эксплуатации и требования к среде.

В этом разделе

Требования к компонентам Kaspersky Security Center

Для установки и управления работой решения Kaspersky Security требуется Kaspersky Security Center Windows или Kaspersky Security Center Linux.

Kaspersky Security Center Linux имеет в составе версию Сервера администрирования, предназначенную для установки на устройство с операционной системой Linux. Взаимодействие с Сервером администрирования Kaspersky Security Center Linux осуществляется с помощью Kaspersky Security Center Web Console. Подробнее о Kaspersky Security Center Linux см. в справке Kaspersky Security Center Linux.

Вы можете использовать приложение Kaspersky Security Center одной из следующих версий:

- Kaspersky Security Center Linux:
  - Kaspersky Security Center 15.2 Linux. Поддерживается управление компонентами решения Kaspersky Security (см. раздел "Об управлении решением через Kaspersky Security Center" на стр. 104) через Kaspersky Security Center Web Console с помощью веб-плагина управления.
  - Kaspersky Security Center 15.1 Linux. Поддерживается управление компонентами решения Kaspersky Security через Kaspersky Security Center Web Console с помощью веб-плагина управления.
  - Kaspersky Security Center 15 Linux. Поддерживается управление компонентами решения Kaspersky Security через Kaspersky Security Center Web Console с помощью веб-плагина управления.
- Kaspersky Security Center Windows:
  - Kaspersky Security Center 15.1 Windows. Поддерживается управление компонентами решения Kaspersky Security через Консоль администрирования с помощью MMC-плагина управления и через Kaspersky Security Center Web Console с помощью веб-плагина управления.

- Kaspersky Security Center 14.2 Windows. Поддерживается управление компонентами решения Kaspersky Security через Консоль администрирования с помощью MMC-плагина управления и через Kaspersky Security Center Web Console с помощью веб-плагина управления.

Для работы Kaspersky Security требуются следующие компоненты Kaspersky Security Center:

- Сервер администрирования.

  На Сервере администрирования должны быть настроены следующие службы:

  - Служба прокси-сервера активации – используется при активации решения Kaspersky Security. Настройка службы прокси-сервера активации выполняется в свойствах Сервера администрирования Kaspersky Security Center. Если служба прокси-сервера активации выключена, активация решения с помощью кода активации невозможна.
  - Служба прокси-сервера KSN – обеспечивает обмен данными между компонентами решения Kaspersky Security и Kaspersky Security Network. Настройка службы прокси-сервера KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center.

  Подробнее о службе прокси-сервера активации и службе прокси-сервера KSN см. в справке Kaspersky Security Center.

- Агент администрирования. Агент администрирования осуществляет взаимодействие между Сервером администрирования и виртуальными машинами с установленными компонентами решения Kaspersky Security.

  Агент администрирования требуется установить на все виртуальные машины, которые вы хотите защищать (см. раздел "Об установке Агента администрирования Kaspersky Security Center на виртуальные машины" на стр. 89), и на SVM (см. раздел "Установка Сервера защиты" на стр. 61). Дистрибутив Агента администрирования входит в комплект поставки решения.

- Консоль управления (см. раздел "Об управлении решением через Kaspersky Security Center" на стр. 104) Kaspersky Security Center. Независимо от версии Kaspersky Security Center вы можете использовать Kaspersky Security Center Web Console (далее также "Web Console"). Для взаимодействия с Kaspersky Security Center Windows вы также можете использовать Консоль администрирования на основе MMC (далее также "Консоль администрирования").

Сведения об установке компонентов Kaspersky Security Center см. в справке Kaspersky Security Center.

Требования для установки Сервера интеграции на базе Windows

Для установки и функционирования Сервера интеграции на базе Windows и Консоли Сервера интеграции на устройстве должна быть установлена одна из следующих операционных систем:

- Windows Server 2022 Standard / Datacenter / Essentials.
- Windows Server 2019 Standard / Datacenter / Essentials.
- Windows Server 2016 Standard / Datacenter.
- Windows Server 2012 R2 Standard / Datacenter / Essentials.
- Windows Server 2012 Standard / Datacenter / Essentials.

На устройстве, на котором вы планируете установить Консоль Сервера интеграции, операционная система должна быть установлена в режиме Desktop experience.

Для установки Сервера интеграции на базе Windows и Консоли Сервера интеграции, а также для работы Консоли Сервера интеграции требуется платформа Microsoft .NET Framework 4.6.2, 4.7 или 4.8. Вы можете установить платформу Microsoft .NET Framework предварительно, или при наличии доступа в интернет мастер установки компонентов Kaspersky Security предложит ее установить в ходе установки Сервера интеграции и Консоли Сервера интеграции.

Для установки и работы Сервера интеграции на базе Windows и Консоли Сервера интеграции устройство должно удовлетворять следующим минимальным аппаратным требованиям:

- четырехъядерный виртуальный процессор с частотой 2 ГГц;
- объем свободного места на диске:
  - для Консоли Сервера интеграции – 4 ГБ;
  - для Сервера интеграции – 4 ГБ;
- объем оперативной памяти:
  - для Консоли Сервера интеграции – 4 ГБ;
  - для Сервера интеграции – 4 ГБ.

В зависимости от размера виртуальной инфраструктуры может изменяться необходимый объем оперативной памяти и объем свободного места на диске. Для увеличения производительности работы Сервера интеграции рекомендуется 10 ГБ свободного места на диске.

Требования для установки Сервера интеграции на базе Linux

Для установки и функционирования Сервера интеграции на базе Linux на устройстве должна быть установлена одна из следующих 64-разрядных операционных систем:

- Ubuntu 22.04 LTS.
- Операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-37 (очередное обновление 7.7).

На устройстве должны быть установлены следующие пакеты:

- независимо от установленной операционной системы:
  - libc6;
  - libgssapi-krb5-2;
  - zlib1g;
- в операционной системе Ubuntu 22.04 LTS:
  - ca-certificates;
  - libssl3;
  - libunwind8;
- в операционной системе Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7): libssl1.1;

Для установки и работы Сервера интеграции на базе Linux устройство должно удовлетворять следующим минимальным аппаратным требованиям:

- четырехъядерный виртуальный процессор с частотой 2500 МГц;
- объем свободного места на диске – 4 ГБ;
- объем оперативной памяти – 8 ГБ.

Аппаратные требования могут изменяться в зависимости от размера виртуальной инфраструктуры. Для увеличения производительности работы Сервера интеграции рекомендуется 10 ГБ свободного места на диске и 12 ГБ оперативной памяти.

Требования к виртуальной инфраструктуре

Поддерживается установка и работа решения Kaspersky Security на следующих платформах виртуализации:

- **Платформа Microsoft Hyper-V**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен один из следующих гипервизоров:

  - Гипервизор Microsoft Windows Server 2022 Hyper-V (Desktop experience / Core).
  - Гипервизор Microsoft Windows Server 2019 Hyper-V (Desktop experience / Core).
  - Гипервизор Microsoft Windows Server 2016 Hyper-V (Desktop experience / Core) со всеми доступными обновлениями.

  Поддерживается установка и работа решения на гипервизорах Microsoft Windows Server (Hyper-V), входящих в состав кластера гипервизоров под управлением службы Windows Failover Clustering. На узлах кластера должна быть включена технология Cluster Shared Volumes.

  Если для управления Сервером интеграции вы используете Консоль Сервера интеграции, во время развертывания SVM на гипервизорах Microsoft Windows Server (Hyper-V) вы можете использовать сервер управления виртуальной инфраструктурой Microsoft System Center Virtual Machine Manager (далее "Microsoft SCVMM") одной из следующих версий:

  - Microsoft SCVMM 2022 с последними обновлениями.
  - Microsoft SCVMM 2019 с последними обновлениями.
  - Microsoft SCVMM 2016 с последними обновлениями.

  Если для управления Сервером интеграции вы используете Веб-консоль Сервера интеграции или REST API, подключение к Microsoft SCVMM не поддерживается.

  > Для Сервера интеграции на базе Linux не поддерживается подключение к виртуальной инфраструктуре на платформе Microsoft Hyper-V. Используйте Сервер интеграции на базе Windows.

- **Платформа XenServer**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор XenServer 8.

  > В виртуальной инфраструктуре на платформе XenServer не поддерживается развертывание SVM с указанием статического IP-адреса. Используйте динамическую IP-адресацию.

- **Платформа VMware vSphere™**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен один из следующих гипервизоров:

  - Гипервизор VMware ESXi™ 8.0 с последними обновлениями.
  - Гипервизор VMware ESXi 7.0 с последними обновлениями.

  В виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой VMware vCenter Server® версии 8.0 или 7.0 со всеми доступными обновлениями. Поддерживается установка и работа решения в инфраструктуре под управлением как автономных серверов VMware vCenter Server, так и группы серверов VMware vCenter Server, работающих в режиме Linked mode.

  Если в инфраструктуре на платформе VMware vSphere вы используете VMware NSX Manager™, Kaspersky Security может назначать теги безопасности (см. раздел "О тегах безопасности (Security Tags)" на стр. 134) (Security Tags) защищенным виртуальным машинам. Kaspersky Security поддерживает совместимость с VMware NSX Manager, входящим в состав одного из следующих пакетов:

  - VMware NSX 4.0.1.
  - VMware NSX-T Data Center 3.2.

  Если для управления Сервером интеграции вы используете Консоль Сервера интеграции, во время развертывания SVM на гипервизорах VMware ESXi вы можете использовать сервер управления виртуальной инфраструктурой Microsoft SCVMM одной из следующих версий:

  - Microsoft SCVMM 2022 с последними обновлениями.
  - Microsoft SCVMM 2019 с последними обновлениями.
  - Microsoft SCVMM 2016 с последними обновлениями.

  Если для управления Сервером интеграции вы используете Веб-консоль Сервера интеграции или REST API, подключение к Microsoft SCVMM не поддерживается.

- **Платформа KVM (Kernel-based Virtual Machine)**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор KVM на базе одной из следующих операционных систем:

  - Debian GNU/Linux 12.0.
  - Debian GNU/Linux 11.0.
  - Ubuntu 22.04 LTS.
  - Red Hat Enterprise Linux® Server 8.0.
  - CentOS Stream 9.

Для развертывания SVM на гипервизорах KVM под управлением операционной системы CentOS требуется удалить или закомментировать строку Defaults requiretty в конфигурационном файле /etc/sudoers операционной системы гипервизора.

- **Платформа Proxmox VE**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор Proxmox VE 8.

  > Поддерживается только Proxmox VE на базе KVM. Не поддерживается работа решения на гипервизоре Proxmox VE с использованием LXC (Linux Containers).

- **Платформа Базис**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор Р-Виртуализация 7.0.13.

  Для развертывания и работы SVM на гипервизорах Р-Виртуализация в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой Базис.vControl версии 2.2.1.

- **Платформа Скала-Р**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор Р-Виртуализация 7.0.13.

  Для развертывания и работы SVM на гипервизорах Р-Виртуализация в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой Скала-Р Управление версии 1.98.

- **Платформа HUAWEI FusionSphere**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор HUAWEI FusionCompute CNA версии 8.0.

  Для развертывания и работы SVM на гипервизорах HUAWEI FusionCompute CNA в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой HUAWEI FusionCompute VRM версии 8.0.

- **Платформа Nutanix Acropolis**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор Nutanix AHV 6.5.1.5.

  Для развертывания и работы SVM на гипервизорах Nutanix AHV в виртуальной инфраструктуре должен быть установлен сервер управления виртуальной инфраструктурой Nutanix Prism 6.5.1.5.

- **Платформа Enterprise Cloud Platform VeiL**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор VeiL Node 5.1.2.

  > Имеются ограничения в установке и работе решения в виртуальной инфраструктуре на платформе Enterprise Cloud Platform VeiL. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).

- **Платформа SharxBase**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор SharxBase 5.10.

  > Имеются ограничения в установке и работе решения в виртуальной инфраструктуре SharxBase. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).

- **Облачная платформа ТИОНИКС**.

  Для установки и работы решения Kaspersky Security требуется Облачная платформа ТИОНИКС версии 2.9 или 3.0.

  В составе Облачной платформы ТИОНИКС должны быть установлены следующие микросервисы:

  - Keystone – микросервис аутентификации.
  - Compute (Nova) – микросервис, используемый для создания виртуальных машин и работы с инфраструктурой.
  - Cinder – микросервис, используемый для работы с хранилищами.
  - Glance – микросервис, используемый для работы с образами виртуальных машин.
  - Neutron – микросервис, используемый для работы с сетями.

  В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

- **Платформа OpenStack**.

  Для установки и работы решения Kaspersky Security требуется платформа OpenStack одной из следующих серий релизов: Havana, Stein, Newton, Victoria, Zed, Antelope, Bobcat.

  В составе платформы OpenStack должны быть установлены следующие микросервисы:

  - Keystone – микросервис аутентификации.
  - Compute (Nova) – микросервис, используемый для создания виртуальных машин и работы с инфраструктурой.
  - Cinder – микросервис, используемый для работы с хранилищами.
  - Glance – микросервис, используемый для работы с образами виртуальных машин.
  - Neutron – микросервис, используемый для работы с сетями.

  В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

- **Платформа Альт Сервер Виртуализации**.

  Для установки и работы решения Kaspersky Security требуется платформа Альт Сервер Виртуализации 10.0.

  В составе платформы должен быть установлен базовый гипервизор платформы Альт Сервер Виртуализации 10.0 (гипервизор на базе KVM).

- **Платформа Программный комплекс средств виртуализации Брест**.

  Для установки и работы решения Kaspersky Security требуется платформа Программный комплекс средств виртуализации Брест версии 3.2 или 3.3.

  В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

Имеются ограничения в установке и работе решения в виртуальной инфраструктуре на платформе Программный комплекс средств виртуализации Брест. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).

- **Среда виртуализации zVirt**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор zVirt Node версии 3.1, 3.3, 4.0, 4.1, 4.2 или zVirt Max.

  Имеются ограничения в установке и работе решения в виртуальной инфраструктуре Среда виртуализации zVirt. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).

- **Платформа Система управления средой виртуализации ROSA Virtualization**.

  Для установки и работы решения Kaspersky Security требуется платформа Система управления средой виртуализации ROSA Virtualization версии 2.1 или 3.0.

  В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

  Имеются ограничения в установке и работе решения в виртуальной инфраструктуре на платформе Система управления средой виртуализации ROSA Virtualization. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).
  Вы можете устранить ограничения, связанные с использованием Сервера интеграции в виртуальной инфраструктуре на платформе Система управления средой виртуализации ROSA Virtualization. Если вы хотите использовать расширенный функционал по обнаружению Легкими агентами SVM (использование Сервера интеграции и расширенного алгоритма выбора SVM), вы можете вручную добавить информацию об инфраструктуре на Сервер интеграции. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16006).

- **Платформа РЕД Виртуализация**.

  Для установки и работы решения Kaspersky Security требуется платформа РЕД Виртуализация 7.3.

  В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

  Имеются ограничения в установке и работе решения в виртуальной инфраструктуре на платформе РЕД Виртуализация. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).

- **Платформа Astra Linux**.

  Для установки и работы решения Kaspersky Security требуется платформа Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) с установленным обновлением Бюллетень № 2022-1221SE17MD (оперативное обновление 1.7.3.UU.1).

  В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

- **Облачная платформа SpaceVM**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре требуется Облачная платформа SpaceVM 6.2.

Имеются ограничения в установке и работе решения в виртуальной инфраструктуре Облачная платформа SpaceVM. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).

- **Облачная платформа Базис.DynamiX**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре требуется Облачная платформа Базис.DynamiX версии 3.8.5, 3.8.8 или 4.0.0.

  Имеются ограничения в установке и работе решения в виртуальной инфраструктуре Облачная платформа Базис.DynamiX. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).

- **Платформа VMmanager Infrastructure**.

  Для установки и работы решения Kaspersky Security требуется платформа VMmanager Infrastructure 2023.11.1-1.

  В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

  Имеются ограничения в установке и работе решения в виртуальной инфраструктуре на платформе VMmanager Infrastructure. Подробнее см. в Базе знаний (https://support.kaspersky.ru/16007).

- **Платформа Numa vServer**.

  Для установки и работы решения Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор Numa vServer 1.1.

- **Облачная платформа VK Cloud**.

  Для установки и работы решения Kaspersky Security требуется платформа VK Cloud одной из следующих серий релизов: Havana, Stein, Newton, Victoria, Zed, Antelope, Bobcat.

  В составе платформы VK Cloud должны быть установлены следующие микросервисы:

  - Keystone – микросервис аутентификации.
  - Compute (Nova) – микросервис, используемый для создания виртуальных машин и работы с инфраструктурой.
  - Cinder – микросервис, используемый для работы с хранилищами.
  - Glance – микросервис, используемый для работы с образами виртуальных машин.
  - Neutron – микросервис, используемый для работы с сетями.

  В виртуальной инфраструктуре должен быть установлен гипервизор KVM.

- **Система серверной виртуализации "Р-Виртуализация"**.

  Для установки и работы программы Kaspersky Security в виртуальной инфраструктуре должен быть установлен гипервизор Р-Виртуализация версии 7.0.13.

  Имеются ограничения в установке и работе программы в виртуальной инфраструктуре на платформе Система серверной виртуализации "Р-Виртуализация". Подробнее см. в Базе знаний (https://support.kaspersky.ru/ksv5la/install/15809).

Решение Kaspersky Security может защищать виртуальные машины в составе инфраструктуры, в которой используются следующие решения для виртуализации:

- VMware Horizon 8.
- Huawei FusionAccess 8 (только виртуальные машины с гостевой операционной системой Windows).
- Citrix Virtual Apps and Desktops 7 2402 LTSR с последними установленными обновлениями.
- Citrix Provisioning Services 7.
- Citrix XenApp and XenDesktop 7.15.
- Citrix App Layering 2009 (только виртуальные машины с гостевой операционной системой Windows).
- Termidesk VDI 3.3.
- Базис.WorkPlace 1.98.2.
- Remote Desktop Host Services на базе Microsoft и на базе Citrix.

Имеются ограничения в работе решения в инфраструктуре VDI на базе Termidesk и Базис.WorkPlace.

Требования к ресурсам SVM

Для функционирования решения для SVM требуется выделить следующее минимальное количество системных ресурсов:

- двухъядерный виртуальный процессор;
- объем свободного места на диске – 30 ГБ;
- объем оперативной памяти – 2 ГБ;
- виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

Требования к виртуальной машине для установки Легкого агента

Требования Легкого агента для Linux

На виртуальных машинах с операционными системами Linux в качестве Легкого агента используется приложение Kaspersky Endpoint Security для Linux, установленное в режиме Легкого агента.

Минимальные аппаратные требования и список поддерживаемых операционных систем для приложения Kaspersky Endpoint Security для Linux в режиме Легкого агента см. в справке приложения Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).

Имеются ограничения в случае использования приложения Kaspersky Endpoint Security для Linux в режиме Легкого агента для защиты виртуальных сред. Использование Kaspersky Endpoint Security для Linux в режиме Легкого агента не поддерживается:

- на устройствах с операционными системами для архитектуры Arm;

- на устройствах с операционными системами Astra Linux в режимах мандатного разграничения доступа и замкнутой программной среды.

Требования Легкого агента для Windows

На виртуальных машинах с операционными системами Windows в качестве Легкого агента используется приложение Kaspersky Endpoint Security для Windows, установленное в режиме Легкого агента.

Минимальные аппаратные требования и список поддерживаемых операционных систем для приложения Kaspersky Endpoint Security для Windows в режиме Легкого агента см. в справке приложения Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Общие требования Легкого агента

Перед установкой Легкого агента на виртуальных машинах должны быть установлены следующие пакеты, в зависимости от виртуальной инфраструктуры:

- В инфраструктуре Microsoft Hyper-V на виртуальных машинах должен быть установлен пакет служб интеграции (Integration Services).
- В инфраструктуре VMware vSphere на виртуальных машинах должен быть установлен пакет VMware Tools.
- В инфраструктуре XenServer на виртуальных машинах должна быть установлена программа XenTools.
- В инфраструктуре HUAWEI FusionSphere на виртуальных машинах должен быть установлен пакет HUAWEI Tools.
- В инфраструктуре KVM, OpenStack, Облачная платформа VK Cloud, Облачная платформа ТИОНИКС, Astra Linux и Альт Сервер Виртуализации на виртуальных машинах должен быть установлен QEMU Guest Agent.

Поддерживаемые версии приложений в режиме Легкого агента

В составе решения Kaspersky Security для виртуальных сред 6.2 Легкий агент в качестве Легких агентов используются следующие приложения:

- Kaspersky Endpoint Security для Linux 12.2 (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).
- Kaspersky Endpoint Security для Windows 12.8 (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Для других компонентов решения Kaspersky Security поддерживается совместимость только с указанными версиями приложений.

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление решением должны осуществляться в соответствии с эксплуатационной документацией.

2. Решение должно эксплуатироваться на устройствах, отвечающих минимальным требованиям, приведенным в разделе "Требования".
3. Перед установкой и началом эксплуатации решения необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ решения ко всем объектам информационной системы, которые необходимы решению для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость решения с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы решения со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлено решение.
8. Должна быть обеспечена поддержка средств аудита, используемых в решении (расширенные возможности по хранению и анализу информации аудита безопасности).
9. Должны быть обеспечены надлежащий источник меток времени и синхронизация по времени между компонентами решения, а также между решением и средой его функционирования.
10. Персонал, ответственный за функционирование решения, должен обеспечивать надлежащее функционирование решения, руководствуясь эксплуатационной документацией.
11. Должна быть обеспечена доверенная связь между решением и уполномоченными субъектами информационной системы (администраторами безопасности).
12. Функционирование решения должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности решения.
13. Администратор должен установить в среде ИТ максимальное число неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
14. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.
15. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
16. Должна быть обеспечена защищенная область для выполнения функций безопасности решения.
17. Управление атрибутами безопасности, связанными с доступом к функциям и данным решения, должно предоставляться только уполномоченным ролям (администраторам решения и информационной системы).
18. Должна быть обеспечена возможность периодического контроля целостности программы и БД ПКВ.
19. Должен осуществляться контроль вноса в контролируемую зону или выноса из контролируемой зоны съемных машинных носителей информации.

kaspersky

Подготовка к установке программы

Перед началом установки Kaspersky Security вам нужно выполнить следующие действия.

Общие действия

- Установить Kaspersky Security Center одной из поддерживаемых версий (см. раздел "Требования к компонентам Kaspersky Security Center" на стр. 19).
- Проверить соответствие компонентов виртуальной инфраструктуры аппаратным и программным требованиям решения Kaspersky Security.
- Подготовить файлы, необходимые для установки решения (на стр. 34).
- Убедиться в том, что на устройствах, где установлены компоненты решения и объекты виртуальной инфраструктуры, к которым подключается Сервер интеграции, используются только безопасные криптографические алгоритмы, наборы шифров и протоколы (см. раздел "Настройка использования безопасных криптографических алгоритмов, шифров и протоколов" на стр. 47).
- Убедиться в том, что в настройках сетевого оборудования или программного обеспечения, обеспечивающего контроль трафика между виртуальными машинами, разрешено прохождение сетевого трафика через порты, используемые при установке и работе решения (см. раздел "Настройка используемых портов" на стр. 35).
- Убедиться в том, что настроены параметры учетных записей (см. раздел "Учетные записи для установки и работы решения" на стр. 42), которые требуются для установки и работы решения.
- Если в сети используется динамическая IP-адресация, обеспечить возможность маршрутизации сетевого трафика от SVM до устройства, на котором установлен Сервер администрирования Kaspersky Security Center.
- Установить последние обновления Windows на устройствах, где будут установлены Сервер интеграции на базе Windows, Консоль Сервера интеграции и MMC-плагины управления.
- Если вы хотите, чтобы виртуальные машины с установленными компонентами Kaspersky Security автоматически перемещались в группы администрирования после установки компонентов, создать группы администрирования в Консоли администрирования Kaspersky Security Center и настроить правила автоматического перемещения виртуальных машин в группы администрирования (см. раздел "Настройка правил перемещения виртуальных машин в группы администрирования" на стр. 48).

Подготовка к установке Легкого агента для Linux на виртуальные машины

Перед началом установки Легкого агента для Linux вам нужно выполнить следующие действия:

- Проверить соответствие виртуальных машин, которые вы планируете защищать, аппаратным и программным требованиям приложения Kaspersky Endpoint Security для Linux (см. раздел "Требования к виртуальной машине для установки Легкого агента" на стр. 28), которое используется в роли Легкого агента для Linux, установить необходимые для работы приложения пакеты и утилиты.
- Выполнить подготовительные действия, необходимые для установки приложения Kaspersky Endpoint Security для Linux в режиме Легкого агента (см. подробнее в справке приложения Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm)).

Подготовка к установке Легкого агента для Windows на виртуальные машины

Перед началом установки Легкого агента для Windows вам нужно выполнить следующие действия:

- Проверить соответствие виртуальных машин, которые вы планируете защищать, аппаратным и программным требованиям приложения Kaspersky Endpoint Security для Windows (см. раздел "Требования к виртуальной машине для установки Легкого агента" на стр. 28), которое используется в роли Легкого агента для Windows, установить необходимые для работы приложения пакеты и утилиты.
- Выполнить подготовительные действия, необходимые для установки приложения Kaspersky Endpoint Security для Windows в режиме Легкого агента (см. подробнее в справке приложения Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm)).

  Для поддержки совместимости Легкого агента для Windows с некоторыми решениями для виртуализации требуются дополнительные действия во время установки (см. раздел "Поддержка совместимости Легкого агента для Windows с решениями для виртуализации" на стр. 93).

Дополнительные действия для платформы Microsoft Hyper-V

В виртуальной инфраструктуре на платформе Microsoft Hyper-V вам нужно также выполнить следующие действия перед началом установки решения Kaspersky Security:

- Убедиться в том, что на виртуальных машинах, которые вы хотите защищать, установлен пакет служб интеграции (Integration Services).
- Убедиться в том, что на гипервизоре включен общий сетевой ресурс ADMIN$. На гипервизорах Microsoft Windows Server 2012 R2 Hyper-V для включения общего сетевого ресурса ADMIN$ требуется предварительно установить роль файлового сервера (File Server) с помощью мастера настройки сервера.
- Убедиться в том, что на гипервизорах, не входящих в домен Active Directory, установлено программное обеспечение удаленного управления Windows Remote Management (WinRM) версии 3.0. Windows Remote Management (WinRM) версии 3.0 входит в состав инсталляционного пакета Windows Management Framework 3.0, доступного для загрузки с сайта Microsoft.
- Если вы хотите использовать доменную учетную запись для подключения Сервера интеграции к гипервизору, требуется убедиться, что выполняются следующие условия:
  - Сервер интеграции имеет возможность определять адрес гипервизора с помощью службы доменных имен (DNS) того домена, в котором находится гипервизор, на котором развертывается SVM.
  - DNS-сервер имеет прямую и обратную записи для Сервера интеграции.
  - Зоны, содержащие записи о Сервере интеграции и гипервизоре, на котором развернута SVM, интегрированы с Active Directory.
  - Устройство, с которого выполняется развертывание SVM, имеет возможность разрешать имена гипервизоров, на которых развертывается SVM.
- Если вы хотите, чтобы имя пользователя и пароль учетной записи для подключения к гипервизору, указываемые во время развертывания SVM, передавались в зашифрованном виде, вы можете настроить защищенное соединение с использованием SSL-сертификата между гипервизором, на котором будет развернута SVM, и устройством, где установлена Консоль администрирования Kaspersky Security Center.

Дополнительные действия для платформы VMware vSphere

В виртуальной инфраструктуре на платформе VMware vSphere вам нужно также выполнить следующие

действия перед началом установки решения Kaspersky Security:

- Убедиться в том, что на виртуальных машинах, которые вы хотите защищать, установлен пакет VMware Tools.
- Если при подключении устройства, на котором установлена Консоль администрирования Kaspersky Security Center, к серверу VMware vCenter Server используется прокси-сервер, требуется убедиться в том, что виртуальные машины доступны через прокси-сервер.

Дополнительные действия для платформы XenServer

В виртуальной инфраструктуре на платформе XenServer перед началом установки решения Kaspersky Security вам нужно убедиться, что на виртуальных машинах, которые вы хотите защищать, установлен пакет XenTools.

Дополнительные действия для платформы Proxmox VE

В виртуальной инфраструктуре на платформе Proxmox VE перед началом установки решения Kaspersky Security вам нужно убедиться, что в директории /var/tmp имеется не менее 30 ГБ свободного места.

Дополнительные действия для платформы HUAWEI FusionSphere

В виртуальной инфраструктуре на платформе HUAWEI FusionSphere перед началом установки решения Kaspersky Security вам нужно убедиться, что на виртуальных машинах, которые вы хотите защищать, установлен пакет HUAWEI Tools.

Во время развертывания SVM в виртуальной инфраструктуре на платформе HUAWEI FusionSphere мастер управления SVM устанавливает на SVM пакет HUAWEI Tools. Для получения пакета мастер обращается к гипервизору HUAWEI FusionCompute. Пакет HUAWEI Tools не входит в комплект поставки решения Kaspersky Security. Рекомендуется убедиться, что пакет HUAWEI Tools доступен на гипервизоре HUAWEI FusionCompute.

Дополнительные действия для платформы Astra Linux

В виртуальной инфраструктуре на платформе Astra Linux перед началом установки решения вам нужно настроить конфигурацию учетной записи (см. раздел "Учетные записи для установки и работы решения" на стр. 42), которая будет использоваться для развертывания, удаления и изменения конфигурации SVM, следующим образом:

1. Выполните команду:

   ```
   $ sudo usermod -a -G kvm,libvirt,libvirt-qemu,libvirt-admin <имя_пользователя>
   ```

2. Откройте конфигурационный файл sudoers с помощью команды:

   ```
   sudo visudo
   ```

3. Укажите в файле:

   ```
   <имя пользователя> ALL = (ALL) NOPASSWD: ALL
   ```

   где <имя пользователя> – имя учетной записи, которая будет использоваться для подключения к виртуальной инфраструктуре во время развертывания, удаления и изменения конфигурации SVM.

4. Сохраните и закройте файл sudoers.

kaspersky

В этом разделе

Файлы, необходимые для установки решения

Этот раздел содержит перечень файлов, которые необходимы для установки компонентов решения Kaspersky Security.

Мастер установки компонентов Kaspersky Security и Сервер интеграции на базе Windows

Мастер установки компонентов Kaspersky Security требуется для установки, обновления и удаления Сервера интеграции на базе Windows и Консоли Сервера интеграции.

Для запуска мастера установки компонентов Kaspersky Security требуется файл ksvla-components_<номер версии решения>_mlg.exe. Этот файл входит в комплект поставки решения.

Сервер интеграции на базе Linux

Для установки требуется пакет ksvla-viis_<номер версии>-<номер сборки>_amd64.deb. тот файл входит в комплект поставки решения.

Сервер защиты

Для создания SVM с установленным Сервером защиты (см. раздел "Установка Сервера защиты" на стр. 61) требуется дистрибутив сертифицированной ФСТЭК операционной системы AstraLinux Special Edition 1.7, а также следующие дистрибутивы:

- kl-lightagent-scanserver-6.2.2-305.amd64.deb – дистрибутив Сервера защиты.
- klnagent64_15.1.0-20748_amd64.deb – дистрибутив Агента администрирования Kaspersky Security Center.

Дистрибутивы Сервера защиты и Агента администрирования входят в комплект поставки решения. Дистрибутив операционной системы AstraLinux Special Edition вам нужно приобрести у производителя операционной системы.

Легкий агент для Linux

В качестве Легкого агента для Linux в составе решения Kaspersky Security используется приложение Kaspersky Endpoint Security для Linux. О файлах, необходимых для установки и использования Kaspersky Endpoint Security для Linux в режиме Легкого агента, см. в справке Kaspersky Endpoint Security для Linux.

Легкий агент для Windows

В качестве Легкого агента для Windows в составе решения Kaspersky Security используется приложение Kaspersky Endpoint Security для Windows. О файлах, необходимых для установки и использования

Kaspersky Endpoint Security для Windows в режиме Легкого агента, см. в справке Kaspersky Endpoint Security для Windows.

Kaspersky Security Center и Агент администрирования Kaspersky Security Center

Для установки и управления работой решения Kaspersky Security вам нужно установить Kaspersky Security Center.

Для взаимодействия компонентов Легкий агент, установленных на виртуальных машинах, с Kaspersky Security Center вам требуется установить Агент администрирования (см. раздел "Об установке Агента администрирования Kaspersky Security Center на виртуальные машины" на стр. 89) на виртуальные машины, где будет установлен Легкий агент.

Файлы, необходимые для установки Kaspersky Security Center и Агента администрирования, входят в комплект поставки Kaspersky Security Center.

MMC-плагины управления

Для управления компонентами решения через Консоль администрирования Kaspersky Security Center вам нужно установить MMC-плагины управления (см. раздел "О плагинах управления Kaspersky Security" на стр. 105) на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

Файлы klcfginst.msi, необходимые для установки MMC-плагинов, входят в комплект поставки решения.

Веб-плагины управления

Для управления компонентами решения через Kaspersky Security Center Web Console вам нужно установить веб-плагины управления (см. раздел "О плагинах управления Kaspersky Security" на стр. 105) на устройстве, где установлено приложение Kaspersky Security Center Web Console. Архивы, необходимые для установки веб-плагинов, входят в комплект поставки решения:

- Архив ksvla-web_plugin_svm_<номер версии>_mlg.zip используется для установки веб-плагина Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты.
- Архив ksvla-web_plugin_viis_<номер версии>_mlg.zip используется для установки веб-плагина Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер интеграции.
- Архивы для установки веб-плагина Kaspersky Endpoint Security для Linux и веб-плагина Kaspersky Endpoint Security для Windows.

Настройка используемых портов

Для установки и работы компонентов решения в настройках сетевого оборудования или программного обеспечения, используемого для контроля трафика между виртуальными машинами, требуется открыть порты, описанные в таблице ниже.

Таблица 1. Порты, используемые компонентами решения

Порт и протокол	Направление	Назначение и описание
Все платформы		
7271 TCP	От мастера управления SVM к Серверу интеграции.	Для передачи на Сервер интеграции параметров подключения к виртуальной инфраструктуре.

Порт и протокол	Направление	Назначение и описание
7271 TCP	От устройства, с которого выполняются запросы к REST API Сервера интеграции, к Серверу интеграции.	Для автоматизации процедур развертывания и использования решения в режиме мультитенантности (см. раздел "Использование Kaspersky Security для виртуальных сред 6.2 Легкий агент в режиме мультитенантности" на стр. 191) средствами REST API Сервера интеграции.
22 TCP	От мастера управления SVM к SVM.	Для изменения конфигурации SVM.
7271 TCP	От SVM к Серверу интеграции.	Для взаимодействия Сервера защиты и Сервера интеграции.
7271 TCP	От Легкого агента к Серверу интеграции.	Для взаимодействия Легкого агента и Сервера интеграции.
8000 UDP	От SVM к Легкому агенту.	Для передачи Легким агентам информации о доступных SVM с использованием списка адресов SVM.
8000 UDP	От Легкого агента к SVM.	Для получения Легким агентом информации о состоянии SVM.
11111 TCP	От Легкого агента к SVM.	Для передачи служебных запросов (например, на получение информации о лицензии) от Легкого агента Серверу защиты при незащищенном соединении.
11112 TCP	От Легкого агента к SVM.	Для передачи служебных запросов (например, на получение информации о лицензии) от Легкого агента Серверу защиты при защищенном соединении.
9876 TCP	От Легкого агента к SVM.	Для передачи запросов на проверку файлов от Легкого агента Серверу защиты при незащищенном соединении.
9877 TCP	От Легкого агента к SVM.	Для передачи запросов на проверку файлов от Легкого агента Серверу защиты при защищенном соединении.
80 TCP	От Легкого агента к SVM.	Для обновления баз и программных модулей решения на Легком агенте.
15000 UDP	От Kaspersky Security Center к SVM.	Для управления Сервером защиты через Kaspersky Security Center.
13000 TCP	От SVM к Kaspersky Security Center.	Для управления Сервером защиты через Kaspersky Security Center при защищенном соединении.

Порт и протокол	Направление	Назначение и описание
14000 TCP	От SVM к Kaspersky Security Center.	Для управления Сервером защиты через Kaspersky Security Center при незащищенном соединении.
15000 UDP	От Kaspersky Security Center к Легким агентам.	Для управления Легким агентом через Kaspersky Security Center.
13000 TCP	От Легкого агента к Kaspersky Security Center.	Для управления Легким агентом через Kaspersky Security Center при защищенном соединении.
14000 TCP	От Легкого агента к Kaspersky Security Center.	Для управления Легким агентом через Kaspersky Security Center при незащищенном соединении.
13111 TCP	От SVM к Серверу администрирования Kaspersky Security Center.	Для взаимодействия Сервера защиты с прокси-сервером KSN.
17000 TCP	От SVM к Серверу администрирования Kaspersky Security Center.	Для взаимодействия Сервера защиты с серверами активации "Лаборатории Касперского".
Платформа VMware vSphere		
80 TCP 443 TCP	От мастера управления SVM к VMware vCenter Server.	Для развертывания SVM на гипервизоре VMware ESXi с помощью VMware vCenter Server.
443 TCP	От мастера управления SVM к гипервизору ESXi.	Для развертывания SVM на гипервизоре VMware ESXi с помощью VMware vCenter Server.
80 TCP 443 TCP	От Сервера интеграции к VMware vCenter Server.	Для взаимодействия Сервера интеграции с гипервизором VMware ESXi с помощью VMware vCenter Server.
Платформа Microsoft Hyper-V		
135 TCP / UDP 445 TCP / UDP	От мастера управления SVM к гипервизору Microsoft Windows Server (Hyper-V).	Для развертывания SVM на гипервизоре Microsoft Windows Server (Hyper-V).
135 TCP / UDP 445 TCP / UDP 5985 TCP 5986 TCP	От Сервера интеграции к гипервизору Microsoft Windows Server (Hyper-V).	Для взаимодействия Сервера интеграции с гипервизором Microsoft Windows Server (Hyper-V).
Платформа XenServer		
80 TCP 443 TCP	От мастера управления SVM к гипервизору Citrix Hypervisor.	Для развертывания SVM на гипервизоре Citrix Hypervisor.
80 TCP 443 TCP	От Сервера интеграции к гипервизору Citrix Hypervisor.	Для взаимодействия Сервера интеграции с гипервизором Citrix Hypervisor.

Порт и протокол	Направление	Назначение и описание
Платформа KVM		
22 TCP	От мастера управления SVM к гипервизору KVM.	Для развертывания SVM на гипервизоре KVM.
22 TCP	От Сервера интеграции к гипервизору KVM.	Для взаимодействия Сервера интеграции с гипервизором KVM.
Платформа Proxmox VE		
22 TCP 8006 TCP	От мастера управления SVM к гипервизору Proxmox VE.	Для развертывания SVM на гипервизоре Proxmox VE.
8006 TCP	От Сервера интеграции к гипервизору Proxmox VE.	Для взаимодействия Сервера интеграции с гипервизором Proxmox VE.
Платформа Базис		
443 TCP	От мастера управления SVM к Базис.vControl.	Для развертывания SVM на гипервизоре Р-Виртуализация с помощью Базис.vControl.
22 TCP	От мастера управления SVM к гипервизору Р-Виртуализация.	Для развертывания SVM на гипервизоре Р-Виртуализация с помощью Базис.vControl.
22 TCP	От мастера управления SVM к Базис.vControl.	Для развертывания SVM на гипервизоре Р-Виртуализация с помощью Базис.vControl.
443 TCP	От Сервера интеграции к Базис.vControl.	Для взаимодействия Сервера интеграции с гипервизором Р-Виртуализация с помощью Базис.vControl
Платформа Скала-Р		
443 TCP	От мастера управления SVM к Скала-Р Управление.	Для развертывания SVM на гипервизоре Р-Виртуализация с помощью Скала-Р Управление.
22 TCP	От мастера управления SVM к гипервизору Р-Виртуализация.	Для развертывания SVM на гипервизоре Р-Виртуализация с помощью Скала-Р Управление.
22 TCP	От мастера управления SVM к Скала-Р Управление.	Для развертывания SVM на гипервизоре Р-Виртуализация с помощью Скала-Р Управление.
443 TCP	От Сервера интеграции к Скала-Р Управление.	Для взаимодействия Сервера интеграции с гипервизором Р-Виртуализация с помощью Скала-Р Управление.
Платформа HUAWEI FusionSphere		

Порт и протокол	Направление	Назначение и описание
7443 TCP	От мастера управления SVM к HUAWEI FusionCompute VRM.	Для развертывания SVM на гипервизоре HUAWEI FusionCompute CNA с помощью HUAWEI FusionCompute VRM.
8779 TCP	От мастера управления SVM к гипервизору HUAWEI FusionCompute CNA.	Для развертывания SVM на гипервизоре HUAWEI FusionCompute CNA с помощью HUAWEI FusionCompute VRM.
7443 TCP	От Сервера интеграции к HUAWEI FusionCompute VRM.	Для взаимодействия Сервера интеграции с гипервизором HUAWEI FusionCompute CNA с помощью HUAWEI FusionCompute VRM.
Платформа Nutanix Acropolis		
9440 TCP	От мастера управления SVM к Nutanix Prism Central.	Для развертывания SVM на гипервизоре Nutanix AHV в инфраструктуре под управлением Nutanix Prism Central.
9440 TCP	От мастера управления SVM к Nutanix Prism Element.	Для развертывания SVM на гипервизоре Nutanix AHV в инфраструктуре под управлением Nutanix Prism Element.
9440 TCP	От Сервера интеграции к Nutanix Prism Central.	Для взаимодействия Сервера интеграции с гипервизором Nutanix AHV в инфраструктуре под управлением Nutanix Prism Central.
9440 TCP	От Сервера интеграции к Nutanix Prism Element.	Для взаимодействия Сервера интеграции с гипервизором Nutanix AHV в инфраструктуре под управлением Nutanix Prism Element.
Облачная платформа ТИОНИКС		
5000 TCP	От мастера управления SVM к микросервису Keystone (Облачная платформа ТИОНИКС).	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы ТИОНИКС.
8774 TCP	От мастера управления SVM к микросервису Compute (Nova) (Облачная платформа ТИОНИКС).	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы ТИОНИКС.
8776 TCP	От мастера управления SVM к микросервису Cinder (Облачная платформа ТИОНИКС).	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы ТИОНИКС.
9292 TCP	От мастера управления SVM к микросервису Glance (Облачная платформа ТИОНИКС).	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы ТИОНИКС.
9696 TCP	От мастера управления SVM к микросервису Neutron (Облачная платформа ТИОНИКС).	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы ТИОНИКС.

Порт и протокол	Направление	Назначение и описание
5000 TCP	От Сервера интеграции к микросервису Keystone (Облачная платформа ТИОНИКС).	Для взаимодействия Сервера интеграции с Облачной платформой ТИОНИКС.
8774 TCP	От Сервера интеграции к микросервису Compute (Nova) (Облачная платформа ТИОНИКС).	Для взаимодействия Сервера интеграции с Облачной платформой ТИОНИКС.
Облачная платформа VK Cloud		
5000 TCP	От мастера управления SVM к микросервису Keystone.	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы VK Cloud.
8774 TCP	От мастера управления SVM к микросервису Compute (Nova).	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы VK Cloud.
8776 TCP	От мастера управления SVM к микросервису Cinder.	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы VK Cloud.
9292 TCP	От мастера управления SVM к микросервису Glance.	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы VK Cloud.
9696 TCP	От мастера управления SVM к микросервису Neutron.	Для развертывания SVM на гипервизоре KVM под управлением Облачной платформы VK Cloud.
5000 TCP	От Сервера интеграции к микросервису Keystone.	Для взаимодействия Сервера интеграции с Облачной платформой VK Cloud.
8774 TCP	От Сервера интеграции к микросервису Compute (Nova).	Для взаимодействия Сервера интеграции с Облачной платформой VK Cloud.
Платформа OpenStack		
5000 TCP	От мастера управления SVM к микросервису Keystone (платформа OpenStack).	Для развертывания SVM на гипервизоре KVM под управлением платформы OpenStack.
8774 TCP	От мастера управления SVM к микросервису Compute (Nova) (платформа OpenStack).	Для развертывания SVM на гипервизоре KVM под управлением платформы OpenStack.
8776 TCP	От мастера управления SVM к микросервису Cinder (платформа OpenStack).	Для развертывания SVM на гипервизоре KVM под управлением платформы OpenStack.
9292 TCP	От мастера управления SVM к микросервису Glance (платформа OpenStack).	Для развертывания SVM на гипервизоре KVM под управлением платформы OpenStack.

Порт и протокол	Направление	Назначение и описание
9696 TCP	От мастера управления SVM к микросервису Neutron (платформа OpenStack).	Для развертывания SVM на гипервизоре KVM под управлением платформы OpenStack.
5000 TCP	От Сервера интеграции к микросервису Keystone (платформа OpenStack).	Для взаимодействия Сервера интеграции с платформой OpenStack.
8774 TCP	От Сервера интеграции к микросервису Compute (Nova) (платформа OpenStack).	Для взаимодействия Сервера интеграции с платформой OpenStack.
Платформа Альт Сервер Виртуализации		
22 TCP	От мастера управления SVM к гипервизору.	Для развертывания SVM на базовом гипервизоре платформы Альт Сервер Виртуализации.
22 TCP	От Сервера интеграции к гипервизору.	Для взаимодействия Сервера интеграции с базовым гипервизором платформы Альт Сервер Виртуализации.
Платформа Astra Linux		
22 TCP	От мастера управления SVM к гипервизору.	Для развертывания SVM на гипервизоре KVM на платформе Astra Linux.
22 TCP	От Сервера интеграции к гипервизору.	Для взаимодействия Сервера интеграции с гипервизором KVM на платформе Astra Linux.
Платформа Numa vServer		
80 TCP 443 TCP	От мастера управления SVM к гипервизору Numa vServer.	Для развертывания SVM на гипервизоре Numa vServer.
80 TCP 443 TCP	От Сервера интеграции к гипервизору Numa vServer.	Для взаимодействия Сервера интеграции с гипервизором Numa vServer.

Развертывание, изменение конфигурации и удаление SVM с помощью мастера управления SVM не поддерживается в сертифицированной версии решения Kaspersky Security.

Если вы используете гипервизор XenServer или VMware ESXi и на сетевом адаптере гостевой операционной системы виртуальной машины включен беспорядочный режим (promiscuous mode), гостевая операционная система получает все Ethernet-фреймы, проходящие через виртуальный коммутатор, если это разрешено политикой VLAN. Этот режим может использоваться для мониторинга и анализа трафика в сегменте сети, в котором работают SVM и защищенные виртуальные машины. Если вы не настроили защиту соединения между SVM и защищенными виртуальными машинами (см. раздел "Защита соединения между Легким агентом и Сервером защиты" на стр. 144), трафик между SVM и защищенными виртуальными машинами не зашифрован и передается в открытом виде. В целях безопасности не рекомендуется использовать беспорядочный режим в сетевых сегментах с работающей SVM. Если такой режим необходим вам, например, для мониторинга трафика сторонними виртуальными машинами с целью выявления попыток несанкционированного доступа к сети и устранения сетевых неполадок, вам нужно настроить соответствующие ограничения, чтобы защитить трафик между SVM и защищенными виртуальными машинами от несанкционированного доступа.

Учетные записи для установки и работы решения

Общие требования к учетным записям

Для установки MMC-плагинов управления Kaspersky Security и Сервера интеграции требуется учетная запись, которая входит в группу локальных администраторов на устройстве, где выполняется установка.

Для запуска Консоли Сервера интеграции вы можете использовать следующие учетные записи:

- Если для управления решением Kaspersky Security вы планируете использовать Консоль администрирования Kaspersky Security Center и устройство, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен Microsoft Windows, для запуска Консоли Сервера интеграции вы можете использовать учетную запись, которая входит в локальную или доменную группу KLAdmins, или учетную запись, которая входит в группу локальных администраторов. Также вы можете использовать учетную запись администратора Сервера интеграции, созданную при установке Сервера интеграции (см. раздел "Установка Сервера интеграции и Консоли Сервера интеграции с помощью мастера" на стр. 53).
- Если для управления решением Kaspersky Security вы планируете использовать Kaspersky Security Center Web Console, или устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен Microsoft Windows, или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, для запуска Консоли Сервера интеграции вы можете использовать только учетную запись администратора Сервера интеграции, созданную при установке Сервера интеграции.

Платформа VMware vSphere

Для установки и работы решения в инфраструктуре VMware vSphere требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись администратора со следующими правами:
  - Datastore.Allocate space
  - Datastore.Low level file operations
  - Datastore.Remove file
  - Global.Cancel task

  - Global.Licenses
  - Host.Config.Virtual machine autostart configuration
  - Host.Inventory.Modify cluster
  - Network.Assign network
  - Tasks.Create task
  - vApp.Import
  - Virtual machine.Change configuration.Add new disk (только для VMware vCenter Server 7.0)
  - Virtual machine.Interaction.Power Off
  - Virtual machine.Interaction.Power On
- Для подключения Сервера интеграции к VMware vCenter Server рекомендуется использовать учетную запись, которой назначена предустановленная системная роль ReadOnly.
- Для подключения Сервера интеграции к VMware NSX Manager требуется учетная запись VMware NSX Manager, которой назначена роль Enterprise Administrator.

Права должны быть назначены учетным записям на верхнем уровне иерархии объектов управления VMware – на уровне VMware vCenter Server.

Платформа Microsoft Hyper-V

Для развертывания, удаления и изменения конфигурации SVM в инфраструктуре Microsoft Hyper-V требуется встроенная учетная запись локального администратора или доменная учетная запись, входящая в группу Администраторы Hyper-V. В случае доменной учетной записи вам также требуется выдать права на удаленное подключение и использование следующих пространств имен WMI:

- root\cimv2;
- root\MSCluster;
- root\virtualization;
- root\virtualization\v2 (для версий операционных систем Microsoft Windows для серверов, начиная с версии Windows Server 2012 R2).

Для подключения Сервера интеграции к гипервизору Microsoft Windows Server (Hyper-V) также используется встроенная учетная запись локального администратора или доменная учетная запись, входящая в группу Администраторы Hyper-V, которой предоставлены указанные выше права.

Платформа XenServer

Для установки и работы решения в инфраструктуре XenServer требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись с правами Pool Admin.
- Для подключения Сервера интеграции к гипервизору XenServer рекомендуется использовать учетную запись с ролью Read Only.

Платформа KVM

Для установки и работы решения в инфраструктуре KVM требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись `root` или учетная запись, которая имеет право выполнять действия от имени учетной записи `root`.
- Для подключения Сервера интеграции к гипервизору KVM рекомендуется использовать учетную запись непривилегированного пользователя, которой разрешен доступ к Unix-сокету "только для чтения" (libvirt-sock-ro) службы libvirtd (libvirtd daemon).

Платформа Proxmox VE

Для установки и работы решения в инфраструктуре Proxmox VE требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись `root`.
- Для подключения Сервера интеграции к гипервизору Proxmox VE рекомендуется использовать учетную запись, которой предоставлен доступ с ролью PVEAuditor к корневой директории (/) и всем дочерним директориям.

Платформа Базис, платформа Скала-Р

Для установки и работы решения в инфраструктурах Базис и Скала-Р требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись с ролью "Главный администратор".
- Для подключения Сервера интеграции к серверу управления виртуальной инфраструктурой (Базис.vControl / Скала-Р Управление) рекомендуется использовать учетную запись с ролью "Мониторинг инфраструктуры".

Платформа HUAWEI FusionSphere

Для установки и работы решения в инфраструктуре HUAWEI FusionSphere требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись с ролью VMManager.
- Для подключения Сервера интеграции к HUAWEI FusionCompute VRM рекомендуется использовать учетную запись с ролью Auditor.

Платформа Nutanix Acropolis

Для установки и работы решения в инфраструктуре Nutanix Acropolis требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись с ролью Cluster Admin.
- Для подключения Сервера интеграции к серверу управления виртуальной инфраструктурой Nutanix Prism рекомендуется использовать учетную запись с ролью Viewer. В инфраструктуре под управлением Nutanix Prism Central учетная запись с ролью Viewer требуется на сервере Nutanix Prism Central и на серверах Nutanix Prism Element.

Платформа OpenStack, Облачная платформа VK Cloud и Облачная платформа ТИОНИКС

Для установки и работы решения в инфраструктуре под управлением платформы OpenStack, Облачной

платформы VK Cloud или Облачной платформы ТИОНИКС требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись со следующими правами:

Права на действия с объектами инфраструктуры	Права на выполнение запросов к API микросервисов OpenStack
Keystone	
Аутентификация. Запрос состояния токена аутентификации текущего пользователя.	auth/tokens (POST/GET)
Получение списка всех доменов OpenStack.	domains (GET)
Получение списка проектов OpenStack, доступных для текущего пользователя.	auth/projects (GET)
Compute (Nova)	
Получение списка виртуальных машин.	servers/detail (GET)
Получение информации о виртуальной машине.	servers/{server_id} (GET)
Получение списка типов виртуальных машин (типов инстанса).	flavors/detail (GET)
Получение информации о доступных ресурсах проекта OpenStack.	limits (GET)
Получение списка Групп серверов.	os-server-groups (GET)
Получение списка Зон доступности.	os-availability-zone (GET)
Получение списка сетевых интерфейсов виртуальной машины.	servers/{server_id}/os-interface (GET)
Создание сетевого интерфейса для виртуальной машины.	servers/{server_id}/os-interface (POST)
Создание виртуальной машины.	servers (POST)
Остановка/запуск виртуальной машины.	servers/{server_id}/action (POST)
Удаление сетевого интерфейса виртуальной машины.	servers/{server_id}/os-interface/{port_id} (DELETE)
Удаление виртуальной машины.	servers/{server_id} (DELETE)
Cinder	
Получение списка типов диска.	{project_id}/types (GET)
Получение информации о диске.	{project_id}/volumes/{volume_id} (GET)
Создание диска.	{project_id}/volumes (POST)
Удаление диска, созданного текущим пользователем.	{project_id}/volumes/{volume_id} (DELETE)
Glance	
Получение информации об образе.	images/{image_id} (GET)

Создание образа.	images (POST)
Загрузка образа.	images/{image_id}/file (PUT)
Удаление образа, созданного текущим пользователем.	images/{image_id} (DELETE)
Neutron	
Получение списка сетей.	networks (GET)
Получение списка Групп безопасности.	security-groups (GET)
Создание сетевого порта	ports (POST)
Удаление сетевого порта	ports/{port_id} (DELETE)
Получение ID сетевого порта	ports/{port_id} (GET)

- Для подключения Сервера интеграции к виртуальной инфраструктуре требуется учетная запись со следующими правами:

Права на действия с объектами инфраструктуры	**Права на выполнение запросов к API микросервисов OpenStack**
Keystone	
Аутентификация. Запрос состояния токена аутентификации текущего пользователя.	auth/tokens (POST/GET)
Получение списка проектов OpenStack, доступных для текущего пользователя.	auth/projects (GET)
Compute (Nova)	
Получение списка виртуальных машин.	servers/detail (GET)
Получение информации о виртуальной машине.	servers/{server_id} (GET)
Получение списка Групп серверов.	os-server-groups (GET)
Получение списка Зон доступности.	os-availability-zone (GET)
Получение списка гипервизоров. Это право требуется, только если вы планируете использовать схему лицензирования (см. раздел "О лицензии" на стр. 79) по количеству процессоров или по количеству ядер процессоров на гипервизорах, на которых работают защищенные виртуальные машины.	/os-hypervisors/detail (GET)

Платформа Альт Сервер Виртуализации

Для установки и работы решения в инфраструктуре Альт Сервер Виртуализации требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись `root` или учетная запись, которая имеет право выполнять действия от имени учетной записи `root`.

- Для подключения Сервера интеграции к базовому гипервизору платформы Альт Сервер Виртуализации рекомендуется использовать учетную запись непривилегированного пользователя, которой разрешен доступ к Unix-сокету "только для чтения" (libvirt-sock-ro) службы libvirtd (libvirtd daemon).

Платформа Astra Linux

Для установки и работы решения на гипервизоре KVM на платформе Astra Linux требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись `root` или учетная запись, которая имеет право выполнять действия от имени учетной записи `root`.

  Перед началом установки решения вам нужно настроить конфигурацию учетной записи, которая будет использоваться для развертывания, удаления и изменения конфигурации SVM.

- Для подключения Сервера интеграции к гипервизору KVM на платформе Astra Linux рекомендуется использовать учетную запись непривилегированного пользователя, которой разрешен доступ к Unix-сокету "только для чтения" (libvirt-sock-ro) службы libvirtd (libvirtd daemon).

Платформа Numa vServer

Для установки и работы решения в инфраструктуре Numa vServer требуются следующие учетные записи:

- Для развертывания, удаления и изменения конфигурации SVM требуется учетная запись с правами Pool Admin.
- Для подключения Сервера интеграции к гипервизору Numa vServer рекомендуется использовать учетную запись с ролью Read Only.

Настройка использования безопасных криптографических алгоритмов, шифров и протоколов

Если вы используете Сервер интеграции на базе Windows, для обеспечения безопасности сетевых соединений между Сервером интеграции и виртуальной инфраструктурой рекомендуется настроить использование криптографических алгоритмов, шифров и протоколов, перечисленных в этом разделе. Если вы используете Сервер интеграции на базе Linux, настройка безопасности сетевых соединений не требуется.

На устройствах, где установлены Сервер интеграции и объекты виртуальной инфраструктуры, к которым подключается Сервер интеграции, рекомендуется использовать следующие криптографические алгоритмы, наборы шифров и протоколы:

- Алгоритмы шифрования: AES 256.
- Алгоритмы хеширования:
  - SHA256.
  - SHA384.
  - SHA512.

- Алгоритмы обмена ключами:
  - Diffie-Hellman (ServerMinKeyBitLength=2048, ClientMinKeyBitLength=2048).
  - ECDH (длина ключа не ниже 256, рекомендуемые эллиптические кривые: prime256v1, secp384r1, secp521r1, x25519).
- Протоколы:
  - TLS 1.2.
  - TLS 1.3.
- Наборы шифров:
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256.
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256.
  - TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256.
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384.
  - TLS_AES_128_GCM_SHA256.
  - TLS_AES_256_GCM_SHA384.
  - TLS_CHACHA20_POLY1305_SHA256.
  - TLS_AES_128_CCM_SHA256.

Если у вас установлены не последние версии операционных систем и гипервизоров, могут возникать проблемы в работе Сервера интеграции с виртуальной инфраструктурой по причине несовместимости используемых наборов шифров. В этом случае рекомендуется обратиться в Службу технической поддержки.

Настройка правил перемещения виртуальных машин в группы администрирования

Чтобы управлять через Kaspersky Security Center работой компонентов решения Kaspersky Security, вам требуется поместить устройства с установленными компонентами Kaspersky Security (SVM и защищенные виртуальные машины) в группы администрирования.

Группа администрирования – это набор управляемых устройств, объединенных по какому-либо признаку с целью управления устройствами группы как единым целым.

Перед началом установки решения Kaspersky Security вы можете создать в Kaspersky Security Center группы администрирования, в которые вы хотите поместить SVM и виртуальные машины с Легкими агентами, и настроить правила автоматического перемещения управляемых устройств в группы администрирования.

Если правила перемещения устройств в группы администрирования не настроены, после установки компонентов решения Kaspersky Security Center помещает устройства с установленными компонентами Kaspersky Security, обнаруженные в сети, в список **Нераспределенные устройства**. В этом случае вам требуется вручную переместить SVM и виртуальные машины с Легкими агентами в группы администрирования.

Вы можете настраивать правила перемещения устройств в группы администрирования с помощью Консоли администрирования Kaspersky Security Center или с помощью Kaspersky Security Center Web Console (см. подробнее в справке Kaspersky Security Center).

При создании правил перемещения SVM и виртуальных машин с Легкими агентами в группы администрирования вы можете использовать теги (см. раздел "Отображение виртуальных машин и SVM в Kaspersky Security Center" на стр. 96). SVM и защищенные виртуальные машины с установленным Агентом администрирования Kaspersky Security Center автоматически передают информацию о тегах в Kaspersky Security Center.

kaspersky

Установка решения

Установка решения Kaspersky Security для виртуальных сред 6.2 Легкий агент в виртуальной инфраструктуре состоит из следующих этапов:

1. **Установка Сервера интеграции**

   В зависимости от вашей инфраструктуры вам нужно установить Сервер интеграции на базе Windows (см. раздел "Установка Сервера интеграции на базе Windows" на стр. 52) или Сервер интеграции на базе Linux (см. раздел "Установка Сервера интеграции на базе Linux" на стр. 58).

   > Для Сервера интеграции на базе Linux не поддерживается подключение к виртуальной инфраструктуре на платформе Microsoft Hyper-V. Для установки и работы решения Kaspersky Security в инфраструктуре на платформе Microsoft Hyper-V используйте Сервер интеграции на базе Windows.

   Если для управления Сервером интеграции на базе Windows вы хотите использовать Консоль Сервера интеграции, вам также нужно установить Консоль Сервера интеграции на устройство, где установлена Консоль администрирования Kaspersky Security Center, или на другое устройство с операционной системой Windows.

   Если для управления Сервером интеграции вы хотите использовать Веб-консоль Сервера интеграции, вам нужно установить веб-плагин Сервера интеграции (см. раздел "Установка веб-плагинов Kaspersky Security" на стр. 59). После его установки в Kaspersky Security Center Web Console будет доступна Веб-консоль Сервера интеграции.

2. **Установка плагинов управления Kaspersky Security**

   Если вы хотите управлять компонентами решения Kaspersky Security с помощью Kaspersky Security Center Web Console, а также использовать Веб-консоль Сервера интеграции, вам нужно установить веб-плагины управления (см. раздел "Установка веб-плагинов Kaspersky Security" на стр. 59) на устройстве, где установлено приложение Kaspersky Security Center Web Console.

   Если вы хотите управлять компонентами решения Kaspersky Security с помощью Консоли администрирования Kaspersky Security Center вам нужно установить MMC-плагины управления (см. раздел "Установка MMC-плагинов Kaspersky Security" на стр. 60) на устройстве, где установлена Консоль администрирования.

   > Если вы используете Kaspersky Security Center Linux, вам необходимо установить веб-плагины управления. Консоль администрирования Kaspersky Security Center и MMC-плагины управления не поддерживаются.

   > После установки плагина управления Сервера защиты рекомендуется запустить в Kaspersky Security Center задачу *Загрузка обновлений в хранилище Сервера администрирования* и убедиться, что задача выполнена успешно. Подробнее см. в справке Kaspersky Security Center.

   После установки плагинов управления вы можете создать для Сервера защиты политику по умолчанию и задачу *Обновление баз и модулей решения* с помощью мастера первоначальной настройки Kaspersky Security Center.

3. **Установка Серверов защиты Kaspersky Security**

   Сервер защиты устанавливается в результате создания SVM на гипервизоре в виртуальной инфраструктуре (см. раздел "Установка Сервера защиты" на стр. 61).

4. **Подключение Сервера интеграции к виртуальной инфраструктуре**

   Для получения информации от виртуальной инфраструктуры Сервер интеграции подключается к объектам инфраструктуры. В зависимости от вида виртуальной инфраструктуры Сервер интеграции может подключаться к гипервизорам, серверам управления виртуальной инфраструктурой или микросервисам облачной инфраструктуры.

   Чтобы подключить Сервер интеграции к виртуальной инфраструктуре, вам нужно:

   1. Подключиться к Серверу интеграции через Веб-консоль Сервера интеграции или через Консоль Сервера интеграции (см. раздел "Подключение к Серверу интеграции" на стр. 64).
   2. Настроить параметры подключения Сервера интеграции к инфраструктуре в Веб-консоли Сервера интеграции или в Консоли Сервера интеграции (см. раздел "Подключение Сервера интеграции к виртуальной инфраструктуре" на стр. 68).

   В инфраструктуре под управлением VMware vCenter Server и VMware NSX Manager, если вы используете Консоль Сервера интеграции для подключения к Серверу интеграции, то вам нужно отдельно настроить подключение Сервера интеграции к VMware NSX Manager. Вы можете настроить подключение с помощью процедуры изменения параметров подключения Сервера интеграции к виртуальной инфраструктуре (см. раздел "Изменение параметров подключения к виртуальной инфраструктуре в Консоли Сервера интеграции" на стр. 178).

5. **Подготовка Серверов защиты к работе**

   Вам нужно выполнить действия (см. раздел "Подготовка Сервера защиты к работе" на стр. 77), необходимые для подготовки к работе развернутых SVM и Серверов защиты.

6. **Установка Легких агентов и Агента администрирования Kaspersky Security Center**

   На каждой виртуальной машине, которую требуется защищать с помощью решения Kaspersky Security, вам нужно установить:

   - На виртуальной машине с операционной системой Linux:
     - Легкий агент для Linux (см. раздел "Об установке Легкого агента для Linux" на стр. 89) (приложение Kaspersky Endpoint Security для Linux, которое работает в режиме Легкого агента).
     - Агент администрирования Kaspersky Security Center для Linux (см. раздел "Об установке Агента администрирования Kaspersky Security Center на виртуальные машины" на стр. 89).
   - На виртуальной машине с операционной системой Windows:
     - Легкий агент для Windows (см. раздел "Об установке Легкого агента для Windows" на стр. 90) (приложение Kaspersky Endpoint Security для Windows, которое работает в режиме Легкого агента).
     - Агент администрирования Kaspersky Security Center для Windows (см. раздел "Об установке Агента администрирования Kaspersky Security Center на виртуальные машины" на стр. 89).

   Для защиты инфраструктуры VDI вам нужно установить Легкий агент и Агент администрирования на шаблоны виртуальных машин (см. раздел "Установка Легкого агента на шаблон для временных виртуальных машин" на стр. 91).

7. **Подготовка Легких агентов к работе**

   Вам нужно выполнить действия (см. раздел "Подготовка Легких агентов к работе" на стр. 95), необходимые для подготовки к работе установленных Легких агентов.

В этом разделе

Установка Сервера интеграции на базе Windows

Процедура установки Сервера интеграции на базе Windows зависит от того, какую версию Kaspersky Security Center вы планируете использовать для управления решением Kaspersky Security:

- Если для управления решением Kaspersky Security вы планируете использовать Kaspersky Security Center Windows, вы можете использовать мастер установки компонентов Kaspersky Security (см. раздел "Установка Сервера интеграции и Консоли Сервера интеграции с помощью мастера" на стр. 53). Мастер позволяет установить Сервер интеграции на базе Windows и Консоль Сервера интеграции.

  Сервер интеграции нужно установить на том устройстве, где установлен Сервер администрирования Kaspersky Security Center. Консоль Сервера интеграции нужно установить на том устройстве, где установлена Консоль администрирования Kaspersky Security Center.

- Если для управления решением Kaspersky Security вы планируете использовать Kaspersky Security Center Linux, мастер установки компонентов Kaspersky Security не используется. Сервер интеграции на базе Windows нужно установить на устройство с операционной системой Windows, независимо от расположения компонентов Kaspersky Security Center. Вы также можете установить Консоль Сервера интеграции на устройство с операционной системой Windows. Установка выполняется вручную (см. раздел "Установка вручную" на стр. 57).

kaspersky

Установку Сервера интеграции и Консоли Сервера интеграции следует выполнять под учетной записью, которая входит в группу локальных администраторов.

Для установки требуется не менее 4 ГБ свободного места на диске, который содержит папку %ProgramData%.

Для успешной установки Сервера интеграции нужно в настройках сетевого оборудования или программного обеспечения, используемого для контроля трафика, разрешить соединения на порт, который SVM и Легкие агенты будут использовать для подключения к Серверу интеграции. По умолчанию используется порт 7271 по протоколу TCP.

В этом разделе

Установка Сервера интеграции и Консоли Сервера интеграции с помощью мастера

Вы можете выполнить установку Сервера интеграции и Консоли Сервера интеграции с помощью мастера установки компонентов Kaspersky Security в интерактивном режиме (см. раздел "Установка в интерактивном режиме с помощью мастера" на стр. 54) или в тихом режиме (см. раздел "Установка в тихом режиме с помощью мастера" на стр. 55).

Для работы мастера установки компонентов Kaspersky Security требуется платформа Microsoft .NET Framework версии 4.6.2, 4.7 или 4.8. Вы можете установить платформу Microsoft .NET Framework предварительно, или мастер установки компонентов Kaspersky Security предложит ее установить в ходе установки компонентов решения Kaspersky Security. Для установки Microsoft .NET Framework требуется доступ в интернет. В случае проблем с установкой Microsoft .NET Framework убедитесь, что на устройстве установлены обновления Windows KB2919442 и KB2919355.

В зависимости от наличия установленных на устройстве компонентов Kaspersky Security Center после запуска установки выполняются следующие действия:

- Если на устройстве установлена только Консоль администрирования Kaspersky Security Center, устанавливается Консоль Сервера интеграции.
- Если на устройстве установлены Сервер администрирования Kaspersky Security Center и Консоль администрирования Kaspersky Security Center, устанавливаются Сервер интеграции и Консоль Сервера интеграции.

При установке Сервера интеграции могут использоваться данные, сохраненные во время удаления Сервера интеграции предыдущей версии.

После установки Консоли Сервера интеграции в Консоли администрирования Kaspersky Security Center в рабочей области узла **Сервер администрирования <имя сервера>** на вкладке **Мониторинг** в блоке **Развертывание** отображается ссылка для запуска Консоли Сервера интеграции: **Управление Kaspersky Security для виртуальных сред <номер версии> Легкий агент**, где <номер версии> – номер установленной версии решения Kaspersky Security.

kaspersky

Процедура установки Сервера интеграции в рамках обновления решения Kaspersky Security отличается от процедуры "чистой" установки, описанной в этом разделе.

В этом разделе

Установка в интерактивном режиме с помощью мастера

► *Чтобы установить Сервер интеграции и Консоль Сервера интеграции в интерактивном режиме с помощью мастера:*

1. На устройстве, где установлены Консоль администрирования и Сервер администрирования Kaspersky Security Center, запустите файл ksvla-components_<номер версии решения>_mlg.exe. Этот файл входит в комплект поставки (см. раздел "Файлы, необходимые для установки решения" на стр. 34).

   Запустится мастер установки компонентов Kaspersky Security.

2. Выберите язык локализации мастера и компонентов Kaspersky Security и перейдите к следующему шагу мастера.

   По умолчанию используется язык локализации операционной системы, установленной на устройстве, где запущен мастер.

3. Убедитесь, что выбрано действие **Установить компоненты управления** и перейдите к следующему шагу мастера.

   Мастер проверяет объем свободного места на диске, который содержит папку %ProgramData%. Если на диске менее 4 ГБ свободного места, мастер выдает сообщение об ошибке, переход к следующему шагу невозможен. В этом случае завершите работу мастера, освободите место на диске и запустите мастер установки компонентов Kaspersky Security повторно.

4. На следующем шаге ознакомьтесь с Лицензионным соглашением решения Kaspersky Security, которое заключается между вами и "Лабораторией Касперского", и с Политикой конфиденциальности, которая описывает обработку и передачу данных.

   Для продолжения установки требуется подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности. Для подтверждения установите оба флажка в окне мастера.

   Перейдите к следующему шагу мастера.

5. Создайте пароль учетной записи администратора Сервера интеграции (`admin`). Учетная запись `admin` используется:

   - для подключения Консоли Сервера интеграции к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65), если устройство, на котором установлена Консоль Сервера интеграции, не входит в домен Microsoft Windows;

- для подключения Веб-консоли Сервера интеграции к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Веб-консоль Сервера интеграции" на стр. 64).

Введите пароль в полях **Пароль** и **Подтверждение пароля**. Имя учетной записи недоступно для изменения.

> Пароль должен содержать не более 60 символов. Вы можете использовать только символы латинского алфавита (прописные и строчные буквы), цифры, а также следующие специальные символы: `! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~`. В целях безопасности рекомендуется задавать пароль длиной не менее 8 символов и использовать хотя бы три из четырех категорий символов: строчные буквы, прописные буквы, цифры и специальные символы.

Перейдите к следующему шагу мастера.

6. Если на устройстве, на котором запущен мастер, занят порт 7271, используемый по умолчанию для подключения к Серверу интеграции, мастер предложит указать номер порта для подключения к Серверу интеграции.

   В поле **Порт** укажите номер порта из диапазона 1025–65535 и перейдите к следующему шагу мастера.

7. Просмотрите информацию о действиях, которые выполнит мастер, и нажмите на кнопку **Установить**, чтобы начать выполнение перечисленных действий.
8. Дождитесь завершения работы мастера.

   Если в ходе работы мастера возникает ошибка, мастер выполняет откат внесенных изменений.

9. Нажмите на кнопку **Завершить**, чтобы закрыть окно мастера.

Информация о работе мастера записывается в файлы трассировки мастера установки компонентов Kaspersky Security (на стр. 229). Если работа мастера завершилась с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Установка в тихом режиме с помощью мастера

> Перед началом установки Сервера интеграции и Консоли Сервера интеграции рекомендуется закрыть Консоль администрирования Kaspersky Security Center.

► *Чтобы установить Сервер интеграции и Консоль Сервера интеграции в тихом режиме с помощью мастера, выполните команду:*

```
ksvla-components_<номер версии решения>_mlg.exe -q --lang=<идентификатор языка> --accept-EulaAndPrivacyPolicy=yes --viisPass=<пароль> [--log-path=<путь к файлу>] [--viisPort=<номер порта>]
```

где:

- `<номер версии решения>` – номер версии решения в формате X.X.X.X.
- `-q` – параметр, определяющий, что установка выполняется в тихом режиме. Если вы хотите запустить установку из командной строки в интерактивном режиме, не указывайте этот параметр.

- `--lang=<идентификатор языка>` – идентификатор языка устанавливаемых компонентов.

  Идентификатор языка требуется указывать в следующем формате: ru, en, de, fr, zh-Hans, zh-Hant, ja. Регистр символов учитывается.

- `--accept-EulaAndPrivacyPolicy=yes` означает, что вы принимаете условия Лицензионного соглашения решения Kaspersky Security, которое заключается между вами и "Лабораторией Касперского", и Политики конфиденциальности, которая описывает обработку и передачу данных. Установив значение `yes`, вы подтверждаете следующее:

  - вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения решения Kaspersky Security;
  - вы полностью прочитали и понимаете Политику конфиденциальности, вы понимаете и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности.

  Текст Лицензионного соглашения и Политики конфиденциальности входит в комплект поставки решения. Согласие с условиями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки Сервера интеграции и Консоли Сервера интеграции.

  Вы можете ознакомиться с текстом Лицензионного соглашения и Политики конфиденциальности, выполнив следующую команду:

  ```
  ksvla-components_<номер версии решения>_mlg.exe --lang=<идентификатор языка> --show-EulaAndPrivacyPolicy
  ```

  Текст Лицензионного соглашения и Политики конфиденциальности выводится в файл license_<идентификатор языка>.txt в папке tmp.

- `--viisPass=<пароль>` – пароль учетной записи администратора Сервера интеграции `admin`. Учетная запись `admin` используется:

  - для подключения Консоли Сервера интеграции к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65), если устройство, на котором установлена Консоль Сервера интеграции, не входит в домен Microsoft Windows;
  - для подключения Веб-консоли Сервера интеграции к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Веб-консоль Сервера интеграции" на стр. 64).

  Пароль должен содержать не более 60 символов. Вы можете использовать только символы латинского алфавита (прописные и строчные буквы), цифры, а также следующие специальные символы: `! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~`. В целях безопасности рекомендуется задавать пароль длиной не менее 8 символов и использовать хотя бы три из четырех категорий символов: строчные буквы, прописные буквы, цифры и специальные символы.

- `--log-path=<путь к файлу>` – путь к файлу, в котором сохраняется информация о результате установки.

  Необязательный параметр. Если не указан, информация о результате установки записывается в файлы трассировки, которые сохраняются в архиве

%temp%\Kaspersky_Security_for_Virtualization_<номер версии>_Light_Agent_BundleInitialInstall_logs_<дата и время>.zip, где:

- <номер версии> – номер установленной версии решения Kaspersky Security;
- <дата и время> – дата и время завершения установки, указанные в формате dd_MM_yyyy_HH_mm_ss.

- `--viisPort=<номер порта>` – порт для подключения к Серверу интеграции.

  Необязательный параметр. По умолчанию для подключения к Серверу интеграции используется порт 7271. Укажите этот параметр, если для подключения к Серверу интеграции вы хотите использовать другой порт.

Чтобы посмотреть описание всех параметров установки и обновления компонентов Kaspersky Security из командной строки, используйте параметр `--help`.

Установка Сервера интеграции и Консоли Сервера интеграции занимает некоторое время. Информация о работе мастера записывается в файлы трассировки мастера установки компонентов Kaspersky Security (на стр. 229). Если работа мастера завершилась с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Установка вручную

► *Чтобы установить Сервер интеграции и Консоль Сервера интеграции вручную:*

1. Разместите на устройстве с операционной системой Windows файл ksvla-components_<номер версии решения>_mlg.exe, где <номер версии> – номер версии решения в формате X.X.X.X. Этот файл входит в комплект поставки (см. раздел "Файлы, необходимые для установки решения" на стр. 34).
2. Извлеките файлы, необходимые для установки Сервера интеграции и Консоли Сервера интеграции, выполнив команду:

   ```
   ksvla-components_<номер версии>_mlg.exe -layout <папка> --accept-EulaAndPrivacyPolicy=yes
   ```

   где:

   - `<номер версии>` – номер версии решения в формате X.X.X.X.
   - `<папка>` – путь к папке, в которую будут извлечены файлы, необходимые для установки Сервера интеграции с Консоли Сервера интеграции. Если вы не указали путь к папке, файлы будут извлечены во вложенную папку data в папке с файлом ksvla-components_<номер версии решения>_mlg.exe.
   - `accept-EulaAndPrivacyPolicy=yes` означает, что вы принимаете условия Лицензионного соглашения решения Kaspersky Security, которое заключается между вами и "Лабораторией Касперского", и Политики конфиденциальности, которая описывает обработку и передачу данных. Установив значение `yes`, вы подтверждаете следующее:
     - вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения решения Kaspersky Security;
     - вы полностью прочитали и понимаете Политику конфиденциальности, вы понимаете и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности.

Согласие с условиями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки Сервера интеграции и Консоли Сервера интеграции. Вы можете ознакомиться с текстом Лицензионного соглашения и Политики конфиденциальности, выполнив следующую команду:

```
ksvla-components_<номер версии>_mlg.exe --lang=<идентификатор языка> --show-EulaAndPrivacyPolicy
```

Текст Лицензионного соглашения и Политики конфиденциальности выводится в файл license_<идентификатор языка>.txt в папке tmp.

В результате выполнения команды в указанной папке создаются две вложенные папки с файлами. Во вложенной папке AttachedContainer среди прочих файлов находятся файлы:

- viis_service.msi – файл, необходимый для установки Сервера интеграции;
- viis_console.msi – файл, необходимый для установки Консоли Сервера интеграции.

3. Запустите установку Сервера интеграции, выполнив команду:

   ```
   viis_service.msi ADMIN_VIIS_PASSWORD=<пароль>
   ```

   где:

   - <пароль> – пароль учетной записи администратора Сервера интеграции admin. Учетная запись admin используется для подключения Консоли Сервера интеграции к Серверу интеграции.

     Пароль должен содержать не более 60 символов. Вы можете использовать только символы латинского алфавита (прописные и строчные буквы), цифры, а также следующие специальные символы: ! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~. В целях безопасности рекомендуется задавать пароль длиной не менее 8 символов и использовать хотя бы три из четырех категорий символов: строчные буквы, прописные буквы, цифры и специальные символы.

4. Запустите установку Консоли Сервера интеграции, выполнив команду:

   ```
   viis_console.msi
   ```

После завершения установки вы можете запускать Консоль Сервера интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65) с помощью исполняемого файла, расположенного в папке установки Консоли Сервера интеграции.

Установка Сервера интеграции на базе Linux

Чтобы установить Сервер интеграции на базе Linux, вам нужно установить пакет Сервера интеграции на устройстве с операционной системой Linux и выполнить первоначальную настройку Сервера интеграции.

► *Чтобы установить пакет Сервера интеграции на базе Linux, выполните команду:*

```
sudo apt-get install ./ksvla-viis_<номер версии>-<номер сборки>_amd64.deb
```

Если на устройстве отсутствуют необходимые пакеты (см. раздел "Требования для установки Сервера интеграции на базе Linux" на стр. 21), они могут быть установлены автоматически в ходе установки Сервера интеграции, или будет выведено предупреждение о необходимости их установки.

После завершения установки Сервера интеграции требуется выполнить первоначальную настройку Сервера интеграции.

► *Чтобы выполнить первоначальную настройку Сервера интеграции:*

1. Выполните команду:

   ```
   sudo /opt/kaspersky/viis/bin/viis-setup.sh
   ```

   Запустится скрипт первоначальной настройки.

2. По запросу скрипта выполните следующие действия:

   a. Выберите языковой стандарт, который будет использоваться для отображения Лицензионного соглашения и Политики конфиденциальности.

   b. Ознакомьтесь с текстом Лицензионного соглашения, которое заключается между вами и "Лабораторией Касперского" и Политики конфиденциальности, которая описывает обработку и передачу данных. Для продолжения установки требуется подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности.

   > Файлы с текстом Лицензионного соглашения и Политики конфиденциальности расположены в директории /opt/kaspersky/viis/doc/EULA/<идентификатор языка>/license.txt.

   c. Укажите номер порта для подключения к Серверу интеграции.

   d. Создайте пароль учетной записи администратора Сервера интеграции (`admin`).

Завершение работы скрипта и освобождение консоли означает, что процесс первоначальной настройки завершен. По завершении первоначальной настройки Сервер интеграции запущен и готов к работе.

Для управления Сервером интеграции на базе Linux используется Веб-консоль Сервера интеграции. Веб-консоль Сервера интеграции доступна в Kaspersky Security Center Web Console после установки веб-плагина Сервера интеграции (см. раздел "Установка веб-плагинов Kaspersky Security" на стр. 59).

Вы можете посмотреть информацию о результате установки и об установленной версии Сервера интеграции на базе Linux, выполнив команду:

```
# apt show ksvla-viis
```

Установка веб-плагинов Kaspersky Security

Для управления компонентами решения Kaspersky Security через Kaspersky Security Center Web Console вам нужно установить:

- Веб-плагин управления Сервера защиты (**Kaspersky Security для виртуальных сред <номер версии> Легкий агент – Сервер защиты**).
- Веб-плагин управления Легкого агента для Linux (приложения Kaspersky Endpoint Security для Linux, которое работает в режиме Легкого агента) и/или веб-плагин управления Легкого агента для Windows (приложения Kaspersky Endpoint Security для Windows, которое работает в режиме Легкого агента).
- Веб-плагин управления Сервера интеграции (**Kaspersky Security для виртуальных сред <номер версии> Легкий агент – Сервер интеграции**), если вы хотите использовать Веб-консоль Сервера интеграции для управления Сервером интеграции.

► *Чтобы установить веб-плагин:*

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры** → **Веб-плагины**.

   Откроется список установленных веб-плагинов.

2. Запустите установку веб-плагинов Kaspersky Security одним из следующих способов:

   - Установка из списка веб-плагинов "Лаборатории Касперского":

     a. Нажмите на кнопку **Добавить**.

        Откроется список всех доступных веб-плагинов "Лаборатории Касперского". Список обновляется автоматически после выпуска новых версий веб-плагинов.

     b. Найдите в списке нужный веб-плагин и нажмите на его название.

     c. В открывшемся окне с описанием веб-плагина нажмите на кнопку **Установить плагин**.

     d. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

   - Установка веб-плагина из стороннего источника. В комплект поставки решения (см. раздел "Файлы, необходимые для установки решения" на стр. 34) входят архивы, необходимые для установки веб-плагинов.

     a. Нажмите на кнопку **Добавить из файла**.

     b. В открывшемся окне загрузите ZIP-архив с дистрибутивом веб-плагина и файл с подписью в формате TXT. ZIP-архивы с дистрибутивами веб-плагинов и файлы с подписью находятся в архивах с веб-плагинами, которые входят в комплект поставки решения.

     c. Нажмите на кнопку **Добавить**.

     d. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новые плагины отображаются в списке установленных веб-плагинов.

Установка MMC-плагинов Kaspersky Security

Для управления компонентами решения Kaspersky Security через Консоль администрирования Kaspersky Security Center вам нужно установить:

- MMC-плагин управления Сервера защиты (**Kaspersky Security для виртуальных сред <номер версии> Легкий агент – Сервер защиты**);
- MMC-плагин управления Легкого агента для Linux (приложения Kaspersky Endpoint Security для Linux, которое работает в режиме Легкого агента) и/или MMC-плагин управления Легкого агента для Windows (приложения Kaspersky Endpoint Security для Windows, которое работает в режиме Легкого агента).

Перед началом установки MMC-плагинов рекомендуется закрыть Консоль администрирования Kaspersky Security Center.

► *Чтобы установить MMC-плагин,*

на устройстве, где установлена Консоль администрирования Kaspersky Security Center, запустите исполняемый файл klcfginst.msi.

Файлы, необходимые для установки MMC-плагинов, входят в комплект поставки решения Kaspersky Security (см. раздел "Файлы, необходимые для установки решения" на стр. 34).

После установки MMC-плагины управления отображаются в списке установленных MMC-плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

► *Чтобы посмотреть список установленных MMC-плагинов управления:*

1. В дереве Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования <имя сервера>** и откройте окно свойств Сервера администрирования одним из следующих способов:
   - с помощью пункта **Свойства** контекстного меню узла **Сервер администрирования <имя сервера>**;
   - по ссылке **Свойства сервера администрирования**, расположенной в рабочей области узла **Сервер администрирования <имя сервера>** в блоке **Сервер администрирования**.
2. В списке слева в разделе **Дополнительно** выберите раздел **Информация об установленных плагинах управления программами**.

Установка Сервера защиты

Установка Сервера защиты выполняется путем создания SVM в виртуальной инфраструктуре. SVM создается на базе сертифицированной ФСТЭК операционной системы AstraLinux Special Edition 1.7.

► *Чтобы создать SVM с установленным компонентом Сервер защиты:*

1. Создайте виртуальную машину, соответствующую следующим минимальным требованиям:
   - Двухъядерный виртуальный процессор.
   - Объем оперативной памяти – 2 ГБ.
   - Объем свободного места на диске – 30 ГБ.
2. Установите на виртуальную машину операционную систему Astra Linux Special Edition 1.7 в соответствии со следующей конфигурацией:
   - Разметка дисков:
     - Авто (использовать весь диск).
     - Все файлы в одном разделе.
   - Ядро для установки: linux-5.15-hardened.
   - Выбор программного обеспечения:
     - Комплект “Консольные утилиты”.
     - Комплект “Средства удаленного подключения SSH”.

     Остальные комплекты программного обеспечения следует отключить.
   - Уровень защищенности: усиленный уровень защищенности “Воронеж”.

     Следующие функции безопасности должны быть включены:
     - Запрос пароля для команды sudo.

- Запрет консоли.
- Запрет автонастройки сети.
- Запрет вывода загрузчика.

Другие функции безопасности необходимо отключить для корректной работы решения Kaspersky Security

3. Удалите следующее программное обеспечение:
   - ufw.
   - ntp.
4. Установите из основного репозитория следующее программное обеспечение:
   - Защищенный WEB сервер (Fly-web): apache2.
   - snmpd.
   - sysstat.
   - Iptables (если было удалено на предыдущем шаге вместе с удалением ufw).
5. Выполните первоначальную настройку сети посредством конфигурационных файлов /etc/network/interfaces.d/.

   Менеджеры сети, например NetworkManager, не совместимы с решением Kaspersky Security.

   Полное описание синтаксиса файла настроек интерфейсов /etc/network/interfaces доступно по команде man interfaces.
6. Установите и запустите инструменты для гостевых операционных систем, соответствующие платформе виртуализации, в которой развернута виртуальная машина:
   - VMware: open-vm-tools.
   - Huawei: Huawei guest tools (vm-agent).
   - Nutanix: cloud-init.
   - Citrix Xen Server: xs-tools.
   - Virtuozzo: vz-guest-tools.
7. Скопируйте на виртуальную машину дистрибутивы Агента администрирования Kaspersky Security Center и Сервера защиты, входящие в комплект поставки:
   - kl-lightagent-scanserver-6.2.2-305.amd64.deb;
   - klnagent64_15.1.0-20748_amd64.deb.
8. Выполните установку дистрибутива Агента администрирования Kaspersky Security Center в соответствии с документацией Kaspersky Security Center.
9. Выполните установку дистрибутива Сервера защиты с помощью команды:

   ```
   dpkg -I ./kl-lightagent-scanserver-6.2.2-305.amd64.deb
   ```
10. Измените пароль учетной записи klconfig:

    ```
    passwd klconfig
    ```

> Пароль должен содержать не более 60 символов. Вы можете использовать только символы латинского алфавита (прописные и строчные буквы), цифры, а также следующие специальные символы: `! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~`. В целях безопасности рекомендуется задавать пароль длиной не менее 8 символов и использовать хотя бы три из четырех категорий символов: строчные буквы, прописные буквы, цифры и специальные символы.

11. Настройте сеть средствами Kaspersky Security. Для этого выполните команды:
    - при использовании DHCP:

      ```
      ssh klconfig@localhost dhcp <InterfaceName> yes
      ```

    - при использовании статических параметров:

      ```
      [root@localhost ~]# ssh klconfig@localhost network <InterfaceName> <IP>
      <NetMask> <Broadcast> <Gateway>
      ```

    - для настройки DNS-сервера:

      ```
      ssh klconfig@localhost dns <dns server 1> <dns server 2> <dns server 3>
      ```

    - для настройки до трех DNS-серверов:

      ```
      [root@localhost ~]# ssh klconfig@localhost dns <server 1> <server 2> <server
      3>
      ```

12. Перезапустите сетевую службу.

    ```
    ssh klconfig@<IP> manageservices restart network
    ```

13. Настройте язык коннектора:

    ```
    ssh klconfig@<IP> connectorlang <lang>
    ```

14. Задайте имя SVM:

    ```
    ssh klconfig@<IP> hostname testsvm.contoso.com <IP>
    ```

15. Настройте параметры подключения Агента администрирования:

    ```
    ssh klconfig@<IP> nagent <IP or fqdn_of_KSC> 13000 14000
    ```

16. Перезапустите Агент администрирования:

    ```
    ssh klconfig@<IP> manageservices restart klnagent
    ```

17. Запустите установку Сервера защиты:

    ```
    ssh klconfig@<IP> productinstall
    ```

18. Чтобы продолжить развертывание Сервера защиты и обеспечить его работоспособность, необходимо подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности:

    ```
    ssh klconfig@<IP> accept_eula_and_privacypolicy yes
    ```

    Установив значение yes, вы подтверждаете следующее:

    - вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения решения Kaspersky Security;
    - вы полностью прочитали и понимаете Политику конфиденциальности, вы понимаете и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности.

Текст Лицензионного соглашения и Политики конфиденциальности входит в комплект поставки решения.

19. Запустите Сервер защиты:

    ```
    ssh klconfig@<IP> manageservices start scanserver
    ```

20. Убедитесь, что в списке служб systemd присутствует служба *la-scanserver.service* и эта служба запущена.

SVM станет доступна для управления через Kaspersky Security Center.

SVM является служебной ВМ, взаимодействие с которой должно происходить посредством klconfig только в целях SVM. Использование SVM в иных целях запрещено и может приводить к рискам безопасности и компрометации SVM.

Подключение к Серверу интеграции

Вы можете подключиться к Серверу интеграции с помощью Веб-консоли Сервера интеграции или с помощью Консоли Сервера интеграции.

Подключение к Серверу интеграции через Веб-консоль Сервера интеграции

► *Чтобы подключиться к Серверу интеграции через Веб-консоль Сервера интеграции:*

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры→ Kaspersky Security для виртуальных сред <номер версии> Легкий агент – Сервер интеграции**.

   Откроется главная страница Веб-консоли Сервера интеграции и окно **Параметры подключения** для ввода параметров подключения к Серверу интеграции.

   Если окно подключения не открылось автоматически, нажмите на кнопку **Подключиться**, расположенную на главной странице Веб-консоли Сервера интеграции.

2. В окне **Параметры подключения** укажите следующие параметры:

   - **Адрес**

     IP-адрес в формате IPv4 или полное доменное имя Сервера интеграции.

     Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

   - **Порт**

     Номер порта для подключения к Серверу интеграции.

   - **Пароль**

     Пароль учетной записи администратора Сервера интеграции (admin).

     Использование доменной учетной записи не поддерживается при подключении к Серверу интеграции через Веб-консоль Сервера интеграции.

> Использование доменной учетной записи не поддерживается при подключении к Серверу интеграции через Веб-консоль Сервера интеграции.

Нажмите на кнопку **Подключиться**.

3. Веб-плагин Сервера интеграции проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат не является доверенным или не соответствует ранее установленному сертификату, открывается окно **Проверка сертификата** с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

   Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Подтвердить и продолжить** в окне **Проверка сертификата**. Полученный сертификат будет установлен в качестве доверенного.

На главной странице Веб-консоли Сервера интеграции отображается адрес и порт Сервера интеграции, к которому выполнено подключение, и версия Сервера интеграции.

Если требуется, вы можете открыть окно ввода параметров подключения к Серверу интеграции с помощью кнопки **Изменить параметры подключения**.

При перезагрузке Сервера интеграции подключение к Серверу интеграции прерывается. После перезагрузки требуется повторная авторизация.

Если вы не выполняете никаких действий в Веб-консоли Сервера интеграции в течение 25 минут, сессия подключения к Серверу интеграции автоматически завершается. После завершения сессии требуется повторная авторизация.

Вы также можете отключиться от Сервера интеграции вручную.

► *Чтобы отключиться от Сервера интеграции:*

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры** → **Kaspersky Security для виртуальных сред <номер версии> Легкий агент – Сервер интеграции**.
2. На главной странице Веб-консоли Сервера интеграции нажмите на кнопку **Отключиться**.

Сессия подключения к Серверу интеграции завершается. На главной странице Веб-консоли Сервера интеграции отображается информация об отсутствии подключения.

Вы также можете завершить сессию подключения к Серверу интеграции, закрыв Kaspersky Security Center Web Console.

Подключение к Серверу интеграции через Консоль Сервера интеграции

Если Консоль Сервера интеграции установлена на том устройстве, где установлена Консоль администрирования Kaspersky Security Center, вы можете открывать Консоль Сервера интеграции из Консоли администрирования Kaspersky Security Center.

Если Консоль Сервера интеграции установлена на отдельном устройстве независимо от компонентов Kaspersky Security Center (например, в случае использования Kaspersky Security Center Linux), вы можете открывать Консоль Сервера интеграции с помощью исполняемого файла, расположенного в папке установки Консоли Сервера интеграции.

kaspersky

Как открыть Консоль Сервера интеграции из Консоли администрирования Kaspersky Security Center и подключиться к Серверу интеграции

Перед запуском Консоли Сервера интеграции, если устройство, на котором установлена Консоль Сервера интеграции, входит в домен Microsoft Windows, убедитесь в том, что ваша доменная учетная запись входит в доменную или локальную группу KLAdmins или в группу локальных администраторов на устройстве, где установлен Сервер интеграции.

► *Чтобы открыть Консоль Сервера интеграции и подключиться к Серверу интеграции:*

1. В дереве Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования <имя сервера>**.
2. В рабочей области узла на вкладке **Мониторинг** в блоке **Развертывание** перейдите по ссылке **Управление Kaspersky Security для виртуальных сред <номер версии> Легкий агент**, где <номер версии> – номер установленной версии решения Kaspersky Security.
3. Если выполняется одно из следующих условий, откроется окно для ввода параметров подключения к Серверу интеграции:
   - если устройство, на котором установлена Консоль Сервера интеграции, не входит в домен Microsoft Windows;
   - если устройство, на котором установлена Консоль Сервера интеграции, входит в домен, но ваша доменная учетная запись не входит в доменную или локальную группу KLAdmins или в группу локальных администраторов на устройстве, где установлен Сервер интеграции;
   - если устройство, на котором установлена Консоль Сервера интеграции, входит в домен, но не удалось подключиться к Серверу интеграции, используя заданные в параметрах Сервера интеграции адрес и порт подключения.

   Укажите следующие параметры подключения:

   - **Адрес Сервера интеграции**

     IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

     Если Консоль Сервера интеграции установлена на том же устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, то по умолчанию для подключения к Серверу интеграции используется адрес, заданный в параметрах Сервера администрирования Kaspersky Security Center. Вы можете изменить этот адрес в окне свойств папки **Инсталляционные пакеты** в дереве консоли (**Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**, окно открывается с помощью пункта **Свойства** контекстного меню).

     Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

   - **Порт**

     Номер порта для подключения к Серверу интеграции.

   - **Имя учетной записи**

     Имя учетной записи, под которой выполняется подключение к Серверу интеграции.

Если устройство, на котором установлена Консоль Сервера интеграции, входит в домен и ваша учетная запись входит в доменную или локальную группу KLAdmins или в группу локальных администраторов, вы можете использовать вашу учетную запись. Для этого вам нужно установить флажок **Использовать доменную учетную запись**.

Если устройство, на котором установлена Консоль Сервера интеграции, не входит в домен или устройство входит в домен, но ваша доменная учетная запись не входит в доменную или локальную группу KLAdmins или в группу локальных администраторов, вы можете использовать только учетную запись администратора Сервера интеграции.

- **Пароль**

  Пароль учетной записи, под которой выполняется подключение к Серверу интеграции.

- **Использовать доменную учетную запись**

  Использование доменной учетной записи текущего пользователя при подключении Консоли Сервера интеграции к Серверу интеграции.

  Если флажок установлен, для подключения к Серверу интеграции используется доменная учетная запись. Убедитесь, что ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции.

  Если флажок снят, для подключения к Серверу интеграции используется учетная запись администратора Сервера интеграции (admin).

  По умолчанию флажок снят.

Нажмите на кнопку **Подключить**.

4. Консоль проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат не является доверенным или не соответствует ранее установленному сертификату, открывается окно **Проверка сертификата** с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

   Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Считать сертификат доверенным** в окне **Проверка сертификата**. Полученный сертификат будет установлен в качестве доверенного. Сертификат сохраняется в реестре операционной системы на устройстве, где установлена Консоль Сервера интеграции.

Откроется Консоль Сервера интеграции. В разделе **Параметры Сервера интеграции** Консоли Сервера интеграции отображается адрес и порт Сервера интеграции, к которому выполнено подключение, и версия Сервера интеграции.

Как открыть Консоль Сервера интеграции с помощью исполняемого файла и подключиться к Серверу интеграции

► *Чтобы открыть Консоль Сервера интеграции и подключиться к Серверу интеграции:*

1. Выполните команду:

   ```
   Kaspersky.VIISConsole.UI.exe /lang:<идентификатор языка>
   ```

   где:

- Kaspersky.VIISConsole.UI.exe – файл, расположенный в папке %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA Console\ на устройстве, где вы установили Сервер интеграции и Консоль Сервера интеграции.
- <идентификатор языка> – идентификатор языка Консоли Сервера интеграции в следующем формате: ru, en, de, fr, zh-Hans, zh-Hant, ja. Регистр символов учитывается.

2. Укажите следующие параметры подключения:
   - Адрес и порт Сервера интеграции, к которому выполняется подключение.

     В качестве адреса вы можете указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

     > Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

   - Пароль администратора Сервера интеграции, который вы задали при установке Сервера интеграции.
3. Консоль проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат не является доверенным или не соответствует ранее установленному сертификату, открывается окно **Проверка сертификата** с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

   Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Считать сертификат доверенным** в окне **Проверка сертификата**. Полученный сертификат будет установлен в качестве доверенного. Сертификат сохраняется в реестре операционной системы на устройстве, где установлена Консоль Сервера интеграции.

Откроется Консоль Сервера интеграции. В разделе **Параметры Сервера интеграции** Консоли Сервера интеграции отображается адрес и порт Сервера интеграции, к которому выполнено подключение, и версия Сервера интеграции.

Подключение Сервера интеграции к виртуальной инфраструктуре

Вы можете настроить подключение Сервера интеграции к виртуальной инфраструктуре с помощью Веб-консоли Сервера интеграции или с помощью Консоли Сервера интеграции.

В этом разделе

kaspersky

Подключение к виртуальной инфраструктуре в Веб-консоли Сервера интеграции

► *Чтобы настроить подключение Сервера интеграции к виртуальной инфраструктуре:*

1. Откройте Веб-консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Веб-консоль Сервера интеграции" на стр. 64).
2. Перейдите в раздел **Список виртуальных инфраструктур**.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне **Добавление виртуальной инфраструктуры** укажите следующие обязательные параметры:

   - **Тип объекта инфраструктуры**

     Тип объекта виртуальной инфраструктуры, к которому подключается Сервер интеграции.

     В зависимости от вида виртуальной инфраструктуры выберите гипервизор, сервер управления виртуальной инфраструктурой или микросервис Keystone.

   - **Протокол**

     Протокол, который используется для подключения Сервера интеграции к виртуальной инфраструктуре. По умолчанию используется протокол HTTPS.

     Поле **Протокол** отображается, если вы настраиваете подключение к виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС.

   - **Адрес объекта инфраструктуры**

     Адрес объекта виртуальной инфраструктуры, к которому подключается Сервер интеграции. В зависимости от вида виртуальной инфраструктуры вам нужно указать адрес гипервизора или адрес сервера управления виртуальной инфраструктурой. Для подключения к инфраструктуре на базе OpenStack вам нужно указать адрес микросервиса Keystone.

     В качестве адреса вы можете указывать IP-адрес в формате IPv4 или полное доменное имя (FQDN).

     В этом поле вы можете также указать порт для подключения к объекту виртуальной инфраструктуры в формате <IP-адрес>:<порт>.

     Если вы настраиваете подключение к гипервизорам Microsoft Windows Server (Hyper-V), входящим в состав кластера гипервизоров под управлением службы Windows Failover Clustering, вы можете указать адрес кластера. Все гипервизоры, входящие в состав кластера, будут добавлены в список.

     Если вы используете Сервер интеграции на базе Linux, не поддерживается развертывание SVM в виртуальной инфраструктуре на платформе Microsoft Hyper-V.

     Если вы настраиваете подключение к гипервизорам VMware ESXi под управлением серверов VMware vCenter Server, которые работают в режиме Linked mode, вы можете указать адрес любого из этих серверов VMware vCenter Server. Все

гипервизоры, которые работают под управлением серверов VMware vCenter Server в режиме Linked mode, будут добавлены в список.

Если вы настраиваете подключение к инфраструктуре под управлением Nutanix Prism Element, вам нужно указать адрес Nutanix Prism Element. Если инфраструктура находится под управлением Nutanix Prism Central, вам нужно указать адрес Nutanix Prism Central. Все серверы Nutanix Prism Element, находящиеся под управлением Nutanix Prism Central, будут добавлены в список.

- Параметры учетной записи для подключения к инфраструктуре с правами администратора:
  - **Домен OpenStack**

    Имя домена OpenStack, к которому принадлежит учетная запись, которая используется для подключения Сервера интеграции к виртуальной инфраструктуре.

    Поле **Домен OpenStack** отображается, если вы настраиваете подключение к виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС.

  - **Имя пользователя**

    Имя учетной записи, которую Сервер интеграции использует для подключения к виртуальной инфраструктуре во время развертывания, удаления и изменения конфигурации SVM. Эта учетная запись должна обладать правами, достаточными для развертывания, удаления и изменения конфигурации SVM (см. раздел "Учетные записи для установки и работы решения" на стр. 42).

  - **Пароль**

    Пароль учетной записи, которую Сервер интеграции использует для подключения к виртуальной инфраструктуре во время развертывания, удаления и изменения конфигурации SVM.

5. В виртуальной инфраструктуре на платформе XenServer, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, OpenStack, Альт Сервер Виртуализации, Astra Linux, Numa vServer, на Облачной платформе VK Cloud или на Облачной платформе ТИОНИКС рекомендуется также указать учетную запись, которая обладает ограниченными правами (см. раздел "Учетные записи для установки и работы решения" на стр. 42) на действия в виртуальной инфраструктуре. Под этой учетной записью Сервер интеграции будет подключаться к виртуальной инфраструктуре во время работы Kaspersky Security: для получения информации о доступных для подключения SVM и распределения Легких агентов между SVM.

   Чтобы задать учетную запись с ограниченными правами:

   a. Нажмите на кнопку **Добавить учетную запись с ограниченными правами** в блоке **Учетная запись с ограниченными правами**.

   b. В открывшемся окне укажите имя и пароль учетной записи.

   c. Нажмите на кнопку **Сохранить**.

   Если учетная запись с ограниченными правами не задана, во время работы Kaspersky Security Сервер интеграции подключается к виртуальной инфраструктуре под той же учетной записью, которая используется для развертывания, удаления и изменения конфигурации SVM.

> В виртуальной инфраструктуре на платформе Microsoft Hyper-V для подключения к виртуальной инфраструктуре во время работы Kaspersky Security может использоваться только та же учетная запись, которая используется для развертывания, удаления и изменения конфигурации SVM.

6. В виртуальной инфраструктуре на платформе VMware vSphere вы можете настроить использование VMware NSX Manager в работе решения Kaspersky Security:
   a. Нажмите на кнопку **Указать параметры подключения к VMware NSX Manager** в блоке **VMware NSX Manager**.
   b. В открывшемся окне укажите следующие параметры:
      - **Адрес**

        IP-адрес в формате IPv4 или полное доменное имя (FQDN) VMware NSX Manager.

        Если в вашей виртуальной инфраструктуре VMware NSX Manager объединены в кластер, укажите виртуальный IP-адрес кластера. Предварительно вам нужно назначить кластеру виртуальный IP-адрес и сертификат (подробнее о настройке кластера VMware NSX Manager см. в документации VMware).
      - **Имя пользователя**

        Имя учетной записи, которую Сервер интеграции использует для подключения к VMware NSX Manager. Требуется учетная запись VMware NSX Manager, которой назначена роль Enterprise Administrator.
      - **Пароль**

        Пароль учетной записи, которую Сервер интеграции использует для подключения к VMware NSX Manager.
   c. Нажмите на кнопку **Сохранить** в окне **Параметры VMware NSX Manager**.
7. Нажмите на кнопку **Сохранить** в окне **Добавление виртуальной инфраструктуры**.

   Сервер интеграции добавляет выбранные объекты виртуальной инфраструктуры в список и пытается установить подключение.

   При этом Сервер интеграции проверяет подлинность всех объектов виртуальной инфраструктуры, к которым выполняется подключение.

   > Для гипервизора Microsoft Windows Server (Hyper-V) проверка подлинности не выполняется. Для микросервисов Keystone проверка подлинности выполняется, только если для подключения Сервера интеграции к виртуальной инфраструктуре используется протокол HTTPS.

   Для проверки подлинности Сервер интеграции получает от каждого объекта виртуальной инфраструктуры SSL-сертификат или отпечаток открытого ключа и проверяет их.

   Если не удалось установить подлинность одного или нескольких полученных сертификатов, открывается окно **Проверка сертификата** с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. Если сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и продолжить подключение к объекту виртуальной инфраструктуры. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлен Сервер интеграции. Если вы не считаете этот

сертификат подлинным, нажмите на кнопку **Отменить подключение** в окне **Проверка сертификата**, чтобы прервать подключение, и замените сертификат на новый.

Если не удалось установить подлинность открытого ключа, открывается окно **Проверка отпечатка открытого ключа** с сообщением об этом. Вы можете подтвердить подлинность открытого ключа и продолжить подключение. Отпечаток открытого ключа будет сохранен на устройстве, где установлен Сервер интеграции. Если вы не считаете этот открытый ключ подлинным, нажмите на кнопку **Отменить подключение** в окне **Проверка отпечатка открытого ключа**, чтобы прервать подключение.

Если подключение к объекту виртуальной инфраструктуры не удалось установить, информация об ошибках подключения отображается в списке инфраструктур в столбце **Статус**.

С помощью кнопок, расположенных над таблицей, вы можете:

- обновить список виртуальных инфраструктур;
- выполнить сортировку и поиск по списку;
- изменить (см. раздел "Изменение параметров подключения к виртуальной инфраструктуре в Веб-консоли Сервера интеграции" на стр. 175) параметры подключения Сервера интеграции к виртуальным инфраструктурам;
- удалить (см. раздел "Удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 182) параметры подключения к виртуальным инфраструктурам;
- экспортировать список в формате CSV.

Подключение к виртуальной инфраструктуре в Консоли Сервера интеграции

► *Чтобы настроить подключение Сервера интеграции к виртуальной инфраструктуре:*

1. Откройте Консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65).
2. В разделе **Управление SVM** нажмите на кнопку **Управление SVM**, чтобы запустить мастер управления SVM.
3. На первом шаге мастера выберите вариант **Развертывание SVM**.

   Перейдите к следующему шагу мастера.
4. Нажмите на кнопку **Добавить**.
5. В открывшемся окне **Параметры подключения к виртуальной инфраструктуре** укажите следующие параметры:

   - **Тип**

     Тип объекта виртуальной инфраструктуры, к которому подключается мастер управления SVM.

     В зависимости от вида виртуальной инфраструктуры выберите гипервизор, сервер управления виртуальной инфраструктурой или микросервис Keystone.

   - **Протокол**

     Протокол, который используется для подключения мастера управления SVM к виртуальной инфраструктуре. По умолчанию используется протокол HTTPS.

Поле **Протокол** отображается, если вы настраиваете подключение к виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС.

- **Адреса**

  Адреса объектов виртуальной инфраструктуры, к которым подключается мастер управления SVM.

  В зависимости от вида виртуальной инфраструктуры вам нужно указать адрес гипервизора или адрес сервера управления виртуальной инфраструктурой. Для подключения к инфраструктуре на базе OpenStack вам нужно указать адрес микросервиса Keystone.

  В качестве адреса вы можете указывать IP-адрес в формате IPv4 или полное доменное имя (FQDN).

  Вы можете указать несколько адресов через точку с запятой, через пробел или с новой строки. Количество правильно распознанных адресов отображается под списком адресов.

  В этом поле вы можете также указать порт для подключения к объекту виртуальной инфраструктуры в формате <IP-адрес>:<порт>.

  Если вы настраиваете подключение к гипервизорам Microsoft Windows Server (Hyper-V), входящим в состав кластера гипервизоров под управлением службы Windows Failover Clustering, вы можете указать адрес кластера. Все гипервизоры, входящие в состав кластера, будут добавлены в список.

  Если вы настраиваете подключение к гипервизорам VMware ESXi под управлением серверов VMware vCenter Server, которые работают в режиме Linked mode, вы можете указать адрес любого из этих серверов VMware vCenter Server. Все гипервизоры, которые работают под управлением серверов VMware vCenter Server в режиме Linked mode, будут добавлены в список.

  Если вы настраиваете подключение к гипервизорам, которые находятся под управлением Microsoft SCVMM, вы можете указать параметры подключения к Microsoft SCVMM. Все гипервизоры, которые находятся под управлением Microsoft SCVMM, будут добавлены в список.

  Если вы настраиваете подключение к инфраструктуре под управлением Nutanix Prism Element, вам нужно указать адрес Nutanix Prism Element. Если инфраструктура находится под управлением Nutanix Prism Central, вам нужно указать адрес Nutanix Prism Central. Все серверы Nutanix Prism Element, находящиеся под управлением Nutanix Prism Central, будут добавлены в список.

- **Домен OpenStack**

  Имя *домена OpenStack*, к которому принадлежит учетная запись, которая используется для подключения мастера управления SVM к объекту виртуальной инфраструктуры.

Поле **Домен OpenStack** отображается, если вы настраиваете подключение к виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС.

- **Имя пользователя**

  Имя учетной записи, которую мастер управления SVM использует для подключения к виртуальной инфраструктуре во время развертывания, удаления и изменения конфигурации SVM. Эта учетная запись должна обладать правами, достаточными для развертывания, удаления и изменения конфигурации SVM (см. раздел "Учетные записи для установки и работы решения" на стр. 42).

  Если вы используете доменную учетную запись для подключения к объекту виртуальной инфраструктуры, вы можете указывать имя учетной записи в формате <домен>\<имя пользователя> или <имя пользователя>@<домен>.

- **Пароль**

  Пароль учетной записи, которую мастер управления SVM использует для подключения к виртуальной инфраструктуре во время развертывания, удаления и изменения конфигурации SVM.

6. Если вы развертываете SVM в виртуальной инфраструктуре на платформе XenServer, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, OpenStack, Альт Сервер Виртуализации, Astra Linux, Numa vServer, на Облачной платформе VK Cloud или на Облачной платформе ТИОНИКС, для подключения Сервера интеграции к виртуальной инфраструктуре во время работы Kaspersky Security рекомендуется использовать учетную запись, которая обладает ограниченными правами (см. раздел "Учетные записи для установки и работы решения" на стр. 42) на действия в виртуальной инфраструктуре. Установите флажок **Учетная запись с ограниченными правами** и укажите параметры учетной записи, которую будет использовать Сервер интеграции для подключения к виртуальной инфраструктуре во время работы Kaspersky Security.

   Если флажок не установлен, во время работы Kaspersky Security Сервер интеграции будет подключаться к виртуальной инфраструктуре под той же учетную записью, которая используется для развертывания, удаления и изменения конфигурации SVM.

   > В виртуальной инфраструктуре на платформе Microsoft Hyper-V для подключения к виртуальной инфраструктуре во время работы Kaspersky Security может использоваться только та же учетная запись, которая используется для развертывания, удаления и изменения конфигурации SVM.

7. Нажмите на кнопку **Подключиться** в окне **Параметры подключения к виртуальной инфраструктуре**.

   Окно закроется. Мастер добавляет выбранные объекты виртуальной инфраструктуры в список и пытается установить подключение.

   При этом мастер проверяет подлинность всех объектов виртуальной инфраструктуры, к которым выполняется подключение.

   > Для гипервизора Microsoft Windows Server (Hyper-V) проверка подлинности не выполняется. Для микросервисов Keystone проверка подлинности выполняется, только если для подключения мастера управления SVM к виртуальной инфраструктуре используется протокол HTTPS.

   Для проверки подлинности мастер получает от каждого объекта виртуальной инфраструктуры SSL-сертификат или отпечаток открытого ключа и проверяет их.

Если не удалось установить подлинность одного или нескольких полученных сертификатов, открывается окно **Проверка сертификата** с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. Если сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и продолжить подключение к объекту виртуальной инфраструктуры. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center. Если вы не считаете этот сертификат подлинным, нажмите на кнопку **Отмена** в окне **Проверка сертификата**, чтобы прервать подключение, и замените сертификат на новый.

Если не удалось установить подлинность открытого ключа, открывается окно **Проверка отпечатка открытого ключа** с сообщением об этом. Вы можете подтвердить подлинность открытого ключа и продолжить подключение. Отпечаток открытого ключа будет сохранен на устройстве, где установлена Консоль администрирования Kaspersky Security Center. Если вы не считаете этот открытый ключ подлинным, нажмите на кнопку **Отмена** в окне **Проверка отпечатка открытого ключа**, чтобы прервать подключение.

Если подключение к объекту виртуальной инфраструктуры не удалось установить, информация об ошибках подключения отображается в таблице.

8. Завершите работу мастера.

Развертывание SVM с помощью мастера управления SVM не поддерживается в сертифицированной версии решения Kaspersky Security.

Вы можете изменять параметры подключения Сервера интеграции к виртуальной инфраструктуре (см. раздел "Изменение параметров подключения к виртуальной инфраструктуре в Консоли Сервера интеграции" на стр. 178) в Консоли Сервера интеграции в разделе **Параметры подключения к инфраструктуре**.

Автоматическое создание задач и политики по умолчанию для Сервера защиты

Мастер первоначальной настройки Kaspersky Security Center позволяет автоматически создать политику по умолчанию для Сервера защиты и задачу для Сервера защиты *Обновление баз и модулей решения*. Мастер первоначальной настройки доступен в Консоли администрирования Kaspersky Security Center и в Kaspersky Security Center Web Console.

Если вы используете Kaspersky Security Center Web Console, мастер первоначальной настройки запускается при первом запуске Kaspersky Security Center Web Console.

Вы можете также запустить мастер первоначальной настройки вручную.

Как запустить мастер первоначальной настройки в Kaspersky Security Center Web Console

► *Чтобы запустить мастер первоначальной настройки,*

в главном окне Kaspersky Security Center Web Console выберите **Обнаружение устройств и развертывание → Развертывание и назначение → Мастер первоначальной настройки**.

После установки веб-плагина Сервера защиты мастер предложит создать политику по умолчанию для Сервера защиты и задачу для Сервера защиты *Обновление баз и модулей решения*.

Если вы используете Консоль администрирования Kaspersky Security Center, мастер первоначальной настройки запускается автоматически при первом запуске Консоли администрирования после установки MMC-плагина управления Сервера защиты.

Если мастер первоначальной настройки управляемой программы не запустился автоматически, вы можете запустить его вручную.

Как запустить мастер первоначальной настройки в Консоли администрирования Kaspersky Security Center

► *Чтобы запустить мастер первоначальной настройки:*

1. В дереве Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования <имя сервера>**, откройте контекстное меню узла и выберите пункт **Все задачи → Мастер первоначальной настройки управляемых программ**.
2. В окне приветствия нажмите на кнопку **Далее** и на следующем шаге выберите в качестве управляемой программы **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты**.

Следуйте указаниям мастера первоначальной настройки.

Создание задачи для Сервера защиты *Обновление баз и модулей решения*

Задача *Обновление баз и модулей решения* создается для группы администрирования **Управляемые устройства** и позволяет загружать пакет обновлений баз и программных модулей решения Kaspersky Security на все SVM, которые будут помещены в группу администрирования **Управляемые устройства** или в любую вложенную группу администрирования. Задача запускается при каждой загрузке пакета обновлений в хранилище Сервера администрирования Kaspersky Security Center.

Создание политики по умолчанию для Сервера защиты

Политика по умолчанию для Сервера защиты создается для группы администрирования **Управляемые устройства** с именем **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты** и применяется на всех SVM, которые будут помещены в группу администрирования **Управляемые устройства** или в любую вложенную группу администрирования.

При создании политики по умолчанию для Сервера защиты мастер предлагает вам настроить следующие параметры:

1. Принять решение об использовании Kaspersky Security Network в работе Сервера защиты.

   Использование инфраструктурного решения Kaspersky Security Network приводит к выходу решения Kaspersky Security из безопасного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN.

2. Настроить параметры подключения SVM к Серверу интеграции (см. раздел "Настройка параметров подключения SVM к Серверу интеграции" на стр. 136).

Остальные параметры политики принимают значения по умолчанию.

Значения параметров политики, установленные по умолчанию, соответствуют рекомендациям специалистов "Лаборатории Касперского" и достаточны для первоначальной настройки решения. Во время работы с решением вы можете выполнить более тонкую настройку параметров политики для Сервера защиты (см. раздел "Политика для Сервера защиты" на стр. 108).

Если вы не настроили параметры подключения SVM к Серверу интеграции или подключиться с указанными параметрами не удалось, политика создается в состоянии **Неактивная политика**. Позже вы можете настроить параметры этой политики и активировать ее.

Подготовка Сервера защиты к работе

После завершения процедуры развертывания SVM рекомендуется проверить системную дату на SVM средствами виртуальной инфраструктуры. Несоответствие системной даты на Сервере администрирования Kaspersky Security Center и системной даты на SVM может привести к ошибке подключения SVM к Kaspersky Security Center и неверной работе компонентов решения Kaspersky Security.

После развертывания SVM на гипервизоре вы можете изменить выделенные под SVM ресурсы, например, в соответствии с рекомендациями специалистов "Лаборатории Касперского" (см. раздел "Требования к ресурсам SVM" на стр. 28). Производительность SVM вы можете регулировать с помощью ресурсов, выделенных для нее.

Для подготовки Сервера защиты к работе требуется выполнить следующие действия:

1. Убедиться в том, что новые SVM подключены к Серверу интеграции. Вы можете посмотреть список подключенных SVM (см. раздел "Просмотр списка SVM, подключенных к Серверу интеграции" на стр. 97) в Консоли Сервера интеграции или в Веб-консоли Сервера интеграции.
2. Активировать решение на всех новых SVM (см. раздел "Об активации решения" на стр. 78).

   Чтобы активировать решение на SVM, требуется добавить лицензионный ключ на SVM с помощью задачи активации (см. раздел "Процедура активации решения" на стр. 82). После установки компонента Легкий агент на виртуальных машинах и подключения Легких агентов к SVM компонент Сервер защиты передаст информацию о лицензии Легким агентам.
3. Обновить базы решения на всех новых SVM (см. раздел "Процедура обновления баз решения на SVM" на стр. 88).

В этом разделе

kaspersky

Об активации решения

Активация решения – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии решения в течение срока действия лицензии (см. раздел "О лицензии" на стр. 79).

Для активации решения Kaspersky Security для виртуальных сред 6.2 Легкий агент требуется добавить основной лицензионный ключ решения на все SVM. Добавление ключа на SVM позволяет активировать все компоненты решения, вам не нужно отдельно активировать приложения, которые используются в составе решения в качестве Легких агентов.

Если ваша основная лицензия не включает нужную вам дополнительную функциональность Легких агентов (например, функциональность интеграции с решениями Detection and Response от "Лаборатории Касперского"), чтобы использовать эту функциональность, вам нужно после добавления основного лицензионного ключа решения добавить на SVM отдельный лицензионный ключ для активации нужной дополнительной функциональности.

Для добавления лицензионных ключей на SVM используется задача для Сервера защиты *Активация решения*. Задача активации позволяет добавить на SVM ключ, который помещен в хранилище ключей Kaspersky Security Center.

Автоматическое распространение лицензионных ключей не поддерживается.

Рекомендуется добавлять ключ в хранилище ключей Kaspersky Security Center с помощью файла ключа. *Файл ключа* – это файл с расширением key, который вам предоставляет "Лаборатория Касперского".

Ключ также может быть добавлен с помощью кода активации. Код активации – это уникальная последовательность из двадцати латинских букв и цифр.

Использование кода активации для добавления ключа в хранилище ключей Kaspersky Security Center приводит к выходу решения Kaspersky Security из безопасного состояния.

После активации решения на SVM компонент Сервер защиты, установленный на этой SVM, передает информацию о лицензии Легким агентам, подключенным к SVM. Если статус ключа изменяется, Сервер защиты также передает информацию об этом Легким агентам.

Если информация о лицензии не передана, Легкий агент для Linux прекращает выполнять все свои функции.

Чтобы продлить срок действия основной лицензии решения, вы можете добавить резервный ключ для основной функциональности. Если вы активировали дополнительную функциональность по отдельной лицензии, вы можете также добавить резервный ключ для дополнительной функциональности.

Активный и резервный ключи должны быть одного типа (по типу лицензионного ограничения) и должны соответствовать одному виду лицензии (лицензия Standard / лицензия Enterprise).

Информацию о лицензионных ключах, которые использует решение Kaspersky Security, вы можете

посмотреть в Консоли администрирования Kaspersky Security Center или в Web Console:

- В хранилище лицензионных ключей Kaspersky Security Center. В хранилище отображаются сведения обо всех ключах, добавленных на Сервер администрирования Kaspersky Security Center.
- В свойствах задачи активации. В свойствах задачи для Сервера защиты Активация решения отображаются сведения о ключе, который добавляется на SVM в результате выполнения этой задачи.
- В свойствах приложения "Лаборатории Касперского", установленного на клиентском устройстве. В свойствах Сервера защиты на SVM отображаются сведения о ключах, добавленных на эту SVM. В свойствах Легкого агента на виртуальной машине отображается информация о лицензии, переданная с SVM.
- В отчете об использовании лицензионных ключей.

Информацию о лицензии, которую использует Легкий агент, вы можете посмотреть на виртуальной машине с установленным Легким агентом:

- На виртуальной машине с Легким агентом для Linux: с помощью команды `kesl-control -L --query`. Подробнее см. в справке приложения Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.1.0/ru-RU/264009.htm).
- На виртуальной машине с Легким агентом для Windows: в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows. Подробнее см. в справке приложения Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

О лицензии

Лицензия – это ограниченное по времени право на использование приложения "Лаборатории Касперского", предоставляемое вам на условиях заключенного Лицензионного соглашения.

Список доступных функций и срок использования приложения "Лаборатории Касперского" зависят от лицензии, по которой используется приложение.

Для приложений "Лаборатории Касперского" предусмотрены следующие *типы лицензий*:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с приложениями "Лаборатории Касперского".

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии приложения "Лаборатории Касперского" прекращают выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать приложение "Лаборатории Касперского" по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая* – платная лицензия.

  По истечении срока действия коммерческой лицензии приложения "Лаборатории Касперского" прекращают выполнять свои основные функции.

Решение Kaspersky Security для виртуальных сред 6.2 Легкий агент по истечении срока действия коммерческой лицензии прекращает обновлять базы решения и использовать Kaspersky Security Network. Вы по-прежнему можете защищать виртуальные машины и выполнять их проверку, но только на основе баз решения, установленных до истечения срока действия лицензии. Чтобы продолжить использование Kaspersky Security в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту виртуальных машин от угроз компьютерной безопасности.

Для решения Kaspersky Security для виртуальных сред 6.2 Легкий агент предусмотрены основные лицензии двух *видов*:

- лицензия Standard;
- лицензия Enterprise.

Основная лицензия требуется для активации решения. Вид основной лицензии определяет объем доступной функциональности решения.

Основная лицензия решения может включать или не включать дополнительную функциональность Легких агентов (например, функциональность интеграции с решениями Detection and Response от "Лаборатории Касперского"). Для активации дополнительной функциональности Легких агентов могут использоваться отдельные лицензии, например, лицензия для активации функциональности Kaspersky Endpoint Detection and Response Optimum. Если основная лицензия, по которой вы используете решение, не включает нужную вам дополнительную функциональность, вам нужно приобрести отдельную лицензию для активации дополнительной функциональности.

Объем функциональности, включенный в основную лицензию и в лицензию для дополнительной функциональности, уточняйте у партнера "Лаборатории Касперского", у которого вы приобретаете лицензию.

Рекомендуется учитывать, что объем доступной на Легком агенте функциональности зависит от лицензии, по которой решение активировано на SVM:

- Если вы хотите использовать функциональность Легких агентов, включенную в лицензию Enterprise, вам нужно подключить Легкий агент к SVM, на которой решение активировано по лицензии Enterprise. При подключении к SVM, на которой решение активировано по лицензии Standard, объем доступной на Легком агенте функциональности уменьшается.
- Если вы хотите использовать дополнительную функциональность Легких агентов (например, интеграцию с решениями Detection and Response от "Лаборатории Касперского" или интеграцию с Kaspersky Unified Monitoring and Analysis Platform), вам нужно подключить Легкий агент к SVM, на которой решение активировано по лицензии, включающей эту дополнительную функциональность, или к SVM, на которую добавлен отдельный лицензионный ключ для активации нужной дополнительной функциональности. При отключении Легкого агента от текущей SVM и подключении к SVM, на которой не активирована дополнительная функциональность, на Легком агенте эта функциональность становится недоступна.

Чтобы предотвратить переключение Легких агентов между SVM с разными видами лицензий, вы можете ограничить для Легкого агента количество доступных SVM с помощью тегов для подключения (см. раздел "Настройка использования тегов для подключения" на стр. 142) или списка SVM для подключения (см. раздел "Настройка параметров обнаружения SVM" на стр. 140).

Для решения Kaspersky Security для виртуальных сред 6.2 Легкий агент предусмотрены следующие *схемы лицензирования:*

- Лицензирование по количеству виртуальных машин, защищаемых с помощью решения. В этой схеме лицензирования используются ключи для виртуальных машин независимо от типа операционной системы, а также ключи для серверов и ключи для рабочих станций (в зависимости от типа операционной системы виртуальных машин). В соответствии с лицензионным ограничением решение используется для защиты определенного количества виртуальных машин.

Вы имеете право использовать решение Kaspersky Security по лицензии с ограничением по количеству рабочих станций только для защиты виртуальных машин с операционной системой для рабочих станций или для защиты устройств, которые используются в роли рабочих станций, в том числе в VDI-инфраструктурах.

- Лицензирование по количеству ядер, используемых в физических процессорах на гипервизорах, на которых работают защищенные виртуальные машины. В этой схеме лицензирования используются ключи с ограничением по ядрам. В соответствии с лицензионным ограничением решение используется для защиты всех виртуальных машин с компонентом Легкий агент, работающих на гипервизорах, в которых используется определенное количество ядер физических процессоров.
- Лицензирование по количеству процессоров, используемых на гипервизорах, на которых работают защищенные виртуальные машины. В этой схеме лицензирования используются ключи с ограничением по процессорам. В соответствии с лицензионным ограничением решение используется для защиты всех виртуальных машин с компонентом Легкий агент, работающих на гипервизорах, в которых используется определенное количество процессоров.

Особенности добавления ключей

При добавлении ключей следует учитывать следующие особенности:

- На одну SVM невозможно добавить несколько активных лицензионных ключей для основной функциональности одного типа (например, несколько ключей для серверов или несколько ключей с ограничением по процессорам). Если на SVM уже добавлен лицензионный ключ, и вы добавляете новый ключ того же типа, то новый ключ заменяет ранее добавленный ключ.
- Если вы используете схему лицензирования (см. раздел "О лицензии" на стр. 79) по количеству защищаемых виртуальных машин, в которой предусмотрены отдельные ключи для серверов и для рабочих станций, вам нужно добавить на SVM ключ, соответствующий типу гостевой операционной системы защищаемых виртуальных машин:
  - если SVM защищает только виртуальные машины с операционными системами для серверов, вам нужно добавить на SVM ключ для серверов;
  - если SVM защищает только виртуальные машины с операционными системами для рабочих станций, вам нужно добавить на SVM ключ для рабочих станций;
  - если SVM защищает виртуальные машины с операционными системами для серверов и с операционными системами для рабочих станций, вам нужно добавить на SVM два ключа: ключ для серверов и ключ для рабочих станций.

  Если вы используете схему лицензирования по количеству защищаемых виртуальных машин независимо от типа операционной системы, схему лицензирования по количеству ядер процессоров или схему лицензирования по количеству процессоров, вам требуется один ключ (с соответствующим лицензионным ограничением) независимо от операционной системы защищаемых виртуальных машин.
- Не поддерживается одновременное использование на SVM ключей для основной функциональности, которые соответствуют разным схемам лицензирования (см. раздел "О лицензии" на стр. 79). Если на SVM уже добавлен лицензионный ключ для основной функциональности, и вы добавляете новый ключ, соответствующий другой схеме лицензирования, то новый ключ заменяет ранее добавленный ключ. Например, на SVM добавлен ключ для рабочих станций и ключ для серверов (схема лицензирования по количеству виртуальных машин), и вы добавляете ключ с ограничением по ядрам (схема лицензирования по количеству ядер). В

результате выполнения задачи активный и (при наличии) резервный ключи для рабочих станций и ключи для серверов удаляются. Вместо них добавляется в качестве активного ключ с ограничением по ядрам.

Ключ для рабочих станций и ключ для серверов можно одновременно использовать на SVM, эти ключи соответствуют одной схеме лицензирования (по количеству виртуальных машин).

- Ключ, удаленный с SVM, вы можете добавить на другую SVM, если не истек срок действия лицензии, связанной с ключом.
- Не поддерживается одновременное использование на SVM коммерческих ключей и ключей по подписке. Например, если вы добавляете коммерческий ключ, а ранее на SVM был добавлен ключ по подписке, то ключ по подписке удаляется с SVM. Вместо него добавляется коммерческий ключ.
- Резервный ключ может быть добавлен только после добавления активного ключа. Активный и резервный ключи должны быть одного типа (по типу лицензионного ограничения) и должны соответствовать одному виду лицензии (лицензия Standard / лицензия Enterprise).
- Ключ для дополнительной функциональности можно добавлять на SVM независимо от типа основного лицензионного ключа, добавленного на эту SVM.
- Ключ для дополнительной функциональности может быть добавлен только после добавления основного лицензионного ключа решения.
- На одну SVM невозможно добавить несколько активных лицензионных ключей для активации одной и то же дополнительной функциональности Легких агентов (например, несколько ключей для активации функциональности Kaspersky Endpoint Detection and Response Optimum). Если на SVM уже активирована какая-либо дополнительная функциональность, и вы добавляете новый ключ для активации той же дополнительной функциональности, то новый ключ заменяет ранее добавленный ключ.

Процедура активации решения

► *Чтобы активировать решение:*

1. Создайте задачу для Сервера защиты *Активация решения*. В области действия задачи должны находиться SVM, на которых вы хотите активировать решение.

   При создании задачи используйте основной лицензионный ключ решения, добавленный в хранилище ключей Kaspersky Security Center. Вы можете добавить лицензионный ключ в хранилище ключей Kaspersky Security Center предварительно или во время создания задачи активации.

2. Запустите задачу активации решения и убедитесь, что задача выполнена успешно.

   Если вы добавляете активный ключ, задача активирует решение на тех SVM, где отсутствовал активный ключ, и заменит старый ключ на новый на тех SVM, где решение уже активировано (см. раздел "Особенности добавления ключей" на стр. 81).

   Если количество единиц лицензирования, для которых используется ключ, превышает количество, указанное в Лицензионном сертификате, Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center событие с информацией о нарушении лицензионных ограничений (подробнее см. в справке Kaspersky Security Center).

3. Если основная лицензия, по которой вы активировали решение, не включает нужную вам дополнительную функциональность Легких агентов, вам нужно создать и выполнить еще одну задачу активации. При создании этой задачи используйте лицензионный ключ для дополнительной функциональности. Добавление ключа для дополнительной функциональности ничем не отличается от добавления основного лицензионного ключа решения.

4. Убедитесь, что Легкие агенты подключены к SVM, на которые вы добавили лицензионный ключ (см. раздел "Подключение Легких агентов к SVM" на стр. 140).

Активация решения должна быть выполнена на SVM с актуальными системными датой и временем. Если вы изменили системные дату и время после активации решения, ключ становится неработоспособным. Решение переходит к режиму работы без обновления баз, и Kaspersky Security Network недоступен. В этом случае вам нужно развернуть SVM заново и выполнить активацию решения на SVM.

Если вы используете схему лицензирования по количеству защищаемых виртуальных машин, в которой предусмотрены отдельные ключи для серверов и для рабочих станций, для защиты виртуальных машин с операционными системами для серверов и с операционными системами для рабочих станций вам нужно создать две задачи активации: для добавления на SVM ключа для серверов и для добавления на SVM ключа для рабочих станций.

Вы можете создавать задачи активации решения с помощью Web Console, а также с помощью Консоли администрирования.

Как создать задачу активации в Kaspersky Security Center Web Console

► *Чтобы создать задачу активации:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. На первом шаге мастера выполните следующие действия:

   a. В раскрывающемся списке **Программа** выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты**.

   b. В раскрывающемся списке **Тип задачи** выберите тип задачи: **Активация решения**.

   c. В поле **Название задачи** введите название новой задачи.

   d. В блоке **Выбор устройств, которым будет назначена задача** выберите способ определения области действия задачи. Область действия задачи – это набор SVM, на которых будет выполняться задача.

      - Выберите вариант **Назначить задачу группе администрирования**, если задача должна выполняться на всех SVM, входящих в определенную группу администрирования.
      - Выберите вариант **Задать адреса устройств вручную или импортировать из списка**, если задача должна выполняться на указанных SVM.
      - Выберите вариант **Назначить задачу выборке устройств**, если задача должна выполняться на SVM, входящих в выборку устройств по предопределенному критерию. О создании выборки устройств см. в справке Kaspersky Security Center.

   Перейдите к следующему шагу мастера.

4. В зависимости от выбранного способа определения области действия задачи выполните одно из следующих действий:

- В дереве групп администрирования установите флажки рядом с нужными группами администрирования.
- В списке устройств установите флажки рядом с нужными SVM. Если нужные SVM отсутствуют в списке, вы можете добавить их следующими способами:
  - С помощью кнопки **Добавить устройства**. Вы можете добавить устройства по имени или IP-адресу, добавить устройства из указанного IP-диапазона или выбрать устройства из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.
  - С помощью кнопки **Импортировать устройства из файла**. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

  Если вы импортируете список адресов SVM из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.
- В списке выберите название выборки, содержащей нужные SVM.

Перейдите к следующему шагу мастера.

5. Нажмите на кнопку **Выбрать ключ**. Откроется окно **Хранилище ключей Kaspersky Security Center**. Если вы добавили ключ в хранилище ключей Kaspersky Security Center предварительно, выберите ключ и нажмите на кнопку **OK**.

   Если нужный ключ в хранилище ключей отсутствует, вы можете добавить его, не прерывая работу мастера создания задачи. Для этого нажмите на кнопку **Добавить новый ключ в хранилище**, расположенную в нижней части окна **Хранилище ключей Kaspersky Security Center**. Запустится мастер добавления ключа в хранилище ключей Kaspersky Security Center. Следуйте указаниям мастера.

   После того как вы выбрали ключ, в нижней части окна отобразится следующая информация:

   - **Лицензионный ключ** – уникальная буквенно-цифровая последовательность.
   - **Тип лицензии** – пробная, коммерческая или коммерческая (подписка).
   - **Срок действия лицензии** – количество дней, в течение которых возможно использование решения, активированного путем добавления этого ключа. Например, 365 дней. Поле не отображается, если вы используете решение по подписке.
   - **Льготный период** – количество дней после приостановки подписки, в течение которых решение продолжает выполнять все свои функции. Поле отображается, если вы используете решение по подписке, и поставщик услуг, у которого вы зарегистрировали подписку, предоставляет льготный период для продления подписки. Если вы используете решение по неограниченной подписке, в поле отображается **Недоступно**.
   - **Действует до** – дата и время окончания срока использования решения, активированного путем добавления этого ключа. Если вы используете решение по неограниченной подписке, в поле отображается **Неограниченно**.
   - **Ограничение** – в зависимости от типа ключа:
     - максимальное количество виртуальных машин, которые вы можете защищать;

- максимальное количество используемых ядер физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать;
- максимальное количество используемых физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.

- **Доступная функциональность** – по ссылке вы можете посмотреть информацию о функциональности решения, доступной в зависимости от вида лицензии.

6. Если вы хотите использовать выбранный ключ как резервный, установите флажок **Использовать лицензионный ключ в качестве резервного**.

   Флажок недоступен, если вы добавляете ключ для пробной лицензии или ключ по подписке. Ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного ключа.

   Перейдите к следующему шагу мастера.

7. Если вы хотите настроить расписание запуска задачи активации, установите флажок **Открыть окно свойств задачи после ее создания**. Подробнее о расписании задач см. в справке Kaspersky Security Center.
8. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Как создать задачу активации в Консоли администрирования Kaspersky Security Center

► *Чтобы создать задачу активации:*

1. В Консоли администрирования Kaspersky Security Center выполните одно из следующих действий:
   - Если вы хотите создать задачу, которая будет выполняться на SVM, входящих в выбранную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи** и нажмите на кнопку **Новая задача** в рабочей области.

     Запустится мастер создания задачи для устройств выбранной группы администрирования.
   - Если вы хотите создать задачу, которая будет выполняться на одной или нескольких SVM (задачу для набора устройств):
     - в дереве консоли выберите папку **Задачи** и нажмите на кнопку **Новая задача** в рабочей области.
     - в дереве консоли выберите папку **Лицензии "Лаборатории Касперского"** и нажмите на кнопку **Автоматически распространять лицензионный ключ на управляемые устройства** в рабочей области.

     Запустится мастер создания задачи для набора устройств.
2. На первом шаге мастера выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты** и тип задачи: **Активация решения**. Если вы запустили мастер создания задачи из папки **Лицензии "Лаборатории Касперского"**, тип задачи выбирать не требуется.

   Перейдите к следующему шагу мастера.
3. Нажмите на кнопку **Добавить**. Откроется окно **Хранилище ключей Kaspersky Security Center**. Если вы добавили ключ в хранилище ключей Kaspersky Security Center предварительно, выберите ключ и нажмите на кнопку **OK**.

Если нужный ключ в хранилище ключей отсутствует, вы можете добавить его, не прерывая работу мастера создания задачи. Для этого нажмите на кнопку **Добавить**, расположенную в нижней части окна **Хранилище ключей Kaspersky Security Center**. Запустится мастер добавления ключа в хранилище ключей Kaspersky Security Center. Следуйте указаниям мастера.

После того как вы выбрали ключ, в нижней части окна отобразится следующая информация:

- **Лицензионный ключ** – уникальная буквенно-цифровая последовательность.
- **Тип лицензии** – пробная, коммерческая или коммерческая (подписка).
- **Срок действия лицензии** – количество дней, в течение которых возможно использование решения, активированного путем добавления этого ключа. Например, 365 дней. Поле не отображается, если вы используете решение по подписке.
- **Льготный период** – количество дней после приостановки подписки, в течение которых решение продолжает выполнять все свои функции. Поле отображается, если вы используете решение по подписке, и поставщик услуг, у которого вы зарегистрировали подписку, предоставляет льготный период для продления подписки. Если вы используете решение по неограниченной подписке, в поле отображается **Недоступно**.
- **Действует до** – дата и время окончания срока использования решения, активированного путем добавления этого ключа. Если вы используете решение по неограниченной подписке, в поле отображается **Неограниченно**.
- **Ограничение** – в зависимости от типа ключа:
  - максимальное количество виртуальных машин, которые вы можете защищать;
  - максимальное количество используемых ядер физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать;
  - максимальное количество используемых физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.
- **Доступная функциональность** – по ссылке вы можете посмотреть информацию о функциональности решения, доступной в зависимости от вида лицензии.

4. Если вы хотите использовать выбранный ключ как резервный, установите флажок **Использовать лицензионный ключ в качестве резервного**.

   Флажок недоступен, если вы добавляете ключ для пробной лицензии или ключ по подписке. Ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного ключа.

   Перейдите к следующему шагу мастера.

5. Если вы создаете задачу для набора устройств, мастер предложит определить область действия задачи. Область действия задачи – это набор SVM, на которых будет выполняться задача.

   a. Укажите способ определения области действия задачи: выбрать SVM из списка устройств, обнаруженных Сервером администрирования, задать адреса SVM вручную, импортировать список SVM из файла или указать ранее настроенную выборку устройств (см. подробнее в справке Kaspersky Security Center).

   b. В зависимости от указанного вами способа определения области действия в открывшемся окне выполните одно из следующих действий:

      - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от названия устройства.

- Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM вручную.
- Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM.
- Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.

Перейдите к следующему шагу мастера.

6. Настройте параметры расписания запуска задачи:

- **Запуск по расписанию**

  В раскрывающемся списке выберите режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Запускать пропущенные задачи**

  Если требуется, чтобы решение запускало пропущенную задачу сразу после появления SVM в сети, установите этот флажок.

  Если флажок снят, для режима **Вручную** запуск задачи производится только на видимых в сети SVM.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  По умолчанию запуск задачи на SVM распределяется в течение определенного периода времени. Этот период рассчитывается автоматически, в зависимости от количества SVM, на которые распространяется задача:

  - 0–200 SVM – запуск задачи не распределяется;
  - 200–500 SVM – запуск задачи распределяется в течение 5 минут;
  - 500–1000 SVM – запуск задачи распределяется в течение 10 минут;
  - 1000–2000 SVM – запуск задачи распределяется в течение 15 минут;
  - 2000–5000 SVM – запуск задачи распределяется в течение 20 минут;
  - 5000–10000 SVM – запуск задачи распределяется в течение 30 минут;
  - 10000–20000 SVM – запуск задачи распределяется в течение 1 часа;
  - 20000–50000 SVM – запуск задачи распределяется в течение 2 часов;
  - более 50000 SVM – запуск задачи распределяется в течение 3 часов.

  Если не требуется распределять запуск задачи в течение автоматически рассчитываемого периода, снимите флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

  По умолчанию флажок установлен.

- **Использовать случайную задержку запуска задачи в интервале (мин.)**

  Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента запуска вручную, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае после запуска вручную задача запустится в случайное время в рамках указанного периода.

  Флажок доступен для изменения, если не установлен флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

Подробнее о параметрах расписания запуска задачи см. в справке Kaspersky Security Center.

Перейдите к следующему шагу мастера.

7. В поле **Имя** введите название новой задачи и перейдите к следующему шагу мастера.
8. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера, на последнем шаге установите флажок **Запустить задачу после завершения работы мастера**.
9. Завершите работу мастера.

Если вы задали расписание запуска задачи, то задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу (см. раздел "Запуск и остановка задач для Сервера защиты" на стр. 125) активации решения вручную.

Вы можете просматривать информацию о результатах выполнения задачи в Kaspersky Security Center (см. раздел "Просмотр информации о ходе и результатах выполнения задач" на стр. 126).

Процедура обновления баз решения на SVM

► *Чтобы обновить базы решения на SVM, выполните следующие действия:*

1. Убедитесь в том, что в Kaspersky Security Center создана задача *Загрузка обновлений в хранилище Сервера администрирования.* Если задача загрузки обновлений в хранилище отсутствует, создайте ее (см. в справке Kaspersky Security Center).
2. Дождитесь запуска по расписанию задачи загрузки обновлений в хранилище или запустите задачу вручную.
3. Убедитесь в том, что задача загрузки обновлений в хранилище выполнена успешно (см. подробнее в справке Kaspersky Security Center).
4. Убедитесь в том, что в Kaspersky Security Center создана задача баз на Сервере защиты – *Обновление баз и модулей решения*. Если задача отсутствует, запустите вручную мастер первоначальной настройки, чтобы создать ее (см. раздел "Автоматическое создание задач и политики по умолчанию для Сервера защиты" на стр. 75).

   По умолчанию на SVM загружаются обновления баз, необходимых для работы Сервера защиты, Легкого агента для Linux и Легкого агента для Windows. В политике для Сервера защиты вы можете указать версии Легких агентов, для которых Сервер защиты должен получать обновления (см. раздел "Настройка параметров загрузки обновлений на SVM" на стр. 157).
5. Дождитесь запуска задачи обновления баз на Сервере защиты по расписанию или запустите задачу вручную.
6. Убедитесь в том, что задача выполнена успешно. Вы можете просматривать информацию о результатах выполнения задачи в Kaspersky Security Center (см. раздел "Просмотр информации о ходе и результатах выполнения задач" на стр. 126).

В результате выполнения задачи компонент Сервер защиты загружает пакет обновлений из хранилища Сервера администрирования в папку на SVM и автоматически устанавливает на SVM обновления баз, необходимых для работы Сервера защиты.

При наличии пакета обновлений в папке на SVM Легкий агент устанавливает на защищенной виртуальной машине обновления баз, необходимых для работы Легкого агента (см. раздел "Подготовка Легких агентов к работе" на стр. 95).

kaspersky

Установка Легких агентов и Агента администрирования

На каждой виртуальной машине, которую требуется защищать с помощью решения Kaspersky Security, вам нужно установить Легкий агент и Агент администрирования Kaspersky Security Center.

Агент администрирования Kaspersky Security Center, установленный на защищенной виртуальной машине, обеспечивает взаимодействие между Легким агентом, установленным на этой виртуальной машине, и Сервером администрирования Kaspersky Security Center и позволяет управлять работой Легкого агента с помощью Kaspersky Security Center.

Вы можете устанавливать Легкий агент на шаблон виртуальных машин, из которого будут создаваться постоянные или временные виртуальные машины. В случае установки на шаблон для временных виртуальных машин рекомендуется настроить дополнительные параметры установки (см. раздел "Установка Легкого агента на шаблон для временных виртуальных машин" на стр. 91) Легких агентов и Агента администрирования.

Вы можете устанавливать Легкий агент на виртуальные машины в составе инфраструктуры, в которой используются решения для создания виртуальных рабочих мест на основе технологии VDI. Для поддержки совместимости Легкого агента для Windows с некоторыми решениями для виртуализации требуются дополнительные действия во время установки (см. раздел "Поддержка совместимости Легкого агента для Windows с решениями для виртуализации" на стр. 93).

В этом разделе

Об установке Агента администрирования Kaspersky Security Center на виртуальные машины

Перед началом или во время установки приложения Kaspersky Endpoint Security для Linux в режиме Легкого агента вам нужно установить на каждой виртуальной машине Агент администрирования для Linux.

Перед началом или во время установки приложения Kaspersky Endpoint Security для Windows в режиме Легкого агента вам нужно установить на каждой виртуальной машине Агент администрирования для Windows.

Файлы (см. раздел "Файлы, необходимые для установки решения" на стр. 34), необходимые для установки Агента администрирования, входят в комплект поставки Kaspersky Security Center. Подробнее об установке Агента администрирования см. в справке Kaspersky Security Center.

Об установке Легкого агента для Linux

Установка приложения Kaspersky Endpoint Security для Linux в режиме Легкого агента для защиты

виртуальных сред выполняется одним из следующих способов:

- Удаленно с рабочего места администратора с помощью Kaspersky Security Center.

  Чтобы использовать Kaspersky Endpoint Security для Linux в качестве Легкого агента для Linux, вам нужно выбрать режим Легкого агента одним из следующих способов:

  - в свойствах инсталляционного пакета приложения Kaspersky Endpoint Security для Linux на вкладке **Параметры**;
  - с помощью конфигурационного файла autoinstall.ini, который включен в инсталляционный пакет приложения (параметр `KSVLA_MODE=yes`).

- С помощью командной строки.

  Чтобы использовать Kaspersky Endpoint Security для Linux в качестве Легкого агента для Linux, после завершения установки вам нужно запустить первоначальную настройку приложения и выбрать режим Легкого агента одним из следующих способов:

  - Ввести `yes` на шаге `Specifying the application usage` скрипта первоначальной настройки.
  - Задать в конфигурационном файле первоначальной настройки параметр `KSVLA_MODE=yes`.

В случае установки на шаблон для временных виртуальных машин рекомендуется настроить дополнительные параметры установки (см. раздел "Установка Легкого агента на шаблон для временных виртуальных машин" на стр. 91) Легкого агента и Агента администрирования.

Подробнее об установке приложения Kaspersky Endpoint Security для Linux в режиме Легкого агента см. в справке приложения (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).

Об установке Легкого агента для Windows

Установка приложения Kaspersky Endpoint Security для Windows в режиме Легкого агента для защиты виртуальных сред, выполняется одним из следующих способов:

- Удаленно с рабочего места администратора с помощью Kaspersky Security Center.

  Чтобы использовать Kaspersky Endpoint Security для Windows в качестве Легкого агента для Windows, вам нужно выбрать конфигурацию **Легкий агент** в свойствах инсталляционного пакета приложения Kaspersky Endpoint Security для Windows на вкладке **Параметры**.

- Локально на виртуальной машине с помощью мастера установки.

  Чтобы использовать Kaspersky Endpoint Security для Windows в качестве Легкого агента для Windows, вам нужно выбрать конфигурацию **Легкий агент для защиты виртуальных сред** на шаге выбора конфигурации.

- С помощью командной строки.

  Чтобы использовать Kaspersky Endpoint Security для Windows в качестве Легкого агента для Windows, вам нужно выбрать режим Легкого агента одним из следующих способов:

  - Выполнить команду установки с параметром `LIGHTAGENTMODE=1`.
  - Выполнить установку в тихом режиме с использованием файла setup.ini, в котором задан параметр `KSVLAMode=1`.

Для оптимизации работы приложения Kaspersky Endpoint Security для Windows в режиме Легкого агента рекомендуется использовать предустановленные группы исключений и доверенных приложений для

различных решений виртуализации. Вы можете включить в доверенную зону рекомендуемые исключения из проверки и доверенные приложения во время локальной установки с помощью мастера или при создании инсталляционного пакета в интерактивном режиме.

В случае установки на шаблон для временных виртуальных машин рекомендуется настроить дополнительные параметры установки (см. раздел "Установка Легкого агента на шаблон для временных виртуальных машин" на стр. 91) Легкого агента и Агента администрирования.

Подробнее об установке приложения Kaspersky Endpoint Security для Windows в режиме Легкого агента см. в справке приложения (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Установка Легкого агента на шаблон для временных виртуальных машин

В случае установки на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины, рекомендуется настроить параметры, которые позволяют оптимизировать работу Легкого агента на временных виртуальных машинах.

Если эти параметры настроены, работа временных виртуальных машин, созданных из шаблона, будет оптимизирована следующим образом:

- Будет выключена функциональность Kaspersky Security Center, которая не требуется для временных виртуальных машин: получение информации о программном и аппаратном обеспечении, о наличии уязвимостей и о необходимых обновлениях.
- Обновления, требующие перезагрузки, не будут устанавливаться на виртуальных машинах, созданных из этого шаблона. При получении обновлений, требующих перезагрузки, Легкий агент, установленный на виртуальной машине, будет отправлять в Kaspersky Security Center сообщение о необходимости обновить шаблон виртуальных машин.
- На временных виртуальных машинах с операционными системами Windows не будет применяться технология лечения активного заражения независимо от настроенных параметров Легкого агента для Windows. Если потребуется выполнить процедуру лечения активного заражения, Легкий агент, установленный на виртуальной машине, будет отправлять в Kaspersky Security Center сообщение о необходимости выполнить эту процедуру на шаблон виртуальных машин.

Параметры Агента администрирования Kaspersky Security Center

Если вы устанавливаете Агент администрирования с помощью Kaspersky Security Center, в окне свойств инсталляционного пакета Агента администрирования в разделе **Дополнительно** вам нужно задать следующие параметры:

- **Включить динамический режим для VDI**.
- **Оптимизировать параметры для VDI**.

Если вы устанавливаете Агент администрирования с помощью командной строки, вам нужно использовать файл ответов (в формате TXT), в котором заданы следующие параметры:

- `KLNAGENT_VM_VDI=1`
- `KLNAGENT_VM_OPTIMIZE=1`

Подробнее об установке Агента администрирования см. в справке Kaspersky Security Center.

Параметры Легкого агента для Linux

Если вы устанавливаете Kaspersky Endpoint Security для Linux в режиме Легкого агента с помощью

Kaspersky Security Center, вам нужно включить в инсталляционный пакет приложения конфигурационный файл autoinstall.ini, в котором заданы следующие параметры:

- `KSVLA_MODE=yes`
- `VDI_MODE=yes`

Если вы создаете инсталляционный пакет в Kaspersky Security Center Web Console, вы можете задать эти параметры с помощью флажков в свойствах инсталляционного пакета на вкладке **Параметры**:

- Использовать приложение в режиме Легкого агента;
- Включить режим защиты инфраструктуры VDI.

Если вы устанавливаете Kaspersky Endpoint Security для Linux в режиме Легкого агента с помощью командной строки, после завершения установки вам нужно задать параметры следующим образом, в зависимости от режима первоначальной настройки:

- Запустить скрипт первоначальной настройки и ввести `yes` на шагах `Specifying the application usage mode` и `Enabling VDI protection mode`.
- Запустить первоначальную настройку в автоматическом режиме, задав в конфигурационном файле первоначальной настройки следующие параметры:
  - `KSVLA_MODE=yes`
  - `VDI_MODE=yes`

Подробнее об установке приложения Kaspersky Endpoint Security для Linux в режиме Легкого агента см. в справке приложения (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).

Параметры Легкого агента для Windows

Если вы устанавливаете Kaspersky Endpoint Security для Windows в режиме Легкого агента с помощью Kaspersky Security Center, вам нужно настроить следующие параметры в свойствах инсталляционного пакета приложения Kaspersky Endpoint Security для Windows на вкладке **Параметры**:

- выбрать конфигурацию **Легкий агент**;
- установить флажок **Защищать инфраструктуру VDI**.

Если вы устанавливаете Kaspersky Endpoint Security для Windows в режиме Легкого агента с помощью мастера установки, вам нужно настроить следующие параметры на шаге выбора конфигурации:

- выбрать конфигурацию **Легкий агент для защиты виртуальных сред**;
- установить флажок **Защищать инфраструктуру VDI**.

Если вы устанавливаете Kaspersky Endpoint Security для Windows в режиме Легкого агента с помощью командной строки, вам нужно выполнить одно из следующих действий:

- выполнить команду установки с параметрами `LIGHTAGENTMODE=1` и `VDI=1`;
- выполнить установку в тихом режиме с использованием файла setup.ini, в котором заданы параметры `KSVLAMode=1` и `InstallOnVDI=1`.

Подробнее об установке приложения Kaspersky Endpoint Security для Windows в режиме Легкого агента см. в справке приложения (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

kaspersky

Поддержка совместимости Легкого агента для Windows с решениями для виртуализации

Вам нужно выполнить дополнительные действия в случае установки Легкого агента для Windows в виртуальных инфраструктурах, в которых используются следующие решения для виртуализации:

- Citrix App Layering.
- Citrix Provisioning (Citrix Provisioning Services).
- VMware App Volumes.

Совместимость с технологией Citrix App Layering

Если для сохранения состояния временных виртуальных машин вы планируете использовать полный пользовательский слой (Full User Layer), перед установкой Легкого агента на шаблоне виртуальных машин вам нужно выполнить следующие действия:

1. Создать файл C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt и добавить в него следующие исключения:
   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`
2. Внести в реестр операционной системы следующие изменения:
   a. В разделе реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr создать новый ключ типа DWORD с именем MiniFilterBypass и значением 1.
   b. В разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd создать новый ключ типа MULTI_SZ с именем ExcludeKey и значением \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.
3. Перезагрузить виртуальную машину.

Для установки на виртуальных машинах в инфраструктуре, в которой используется технология Citrix App Layering, вам нужно выполнить следующие действия:

1. Установить Агент администрирования Kaspersky Security Center и Легкий агент для Windows на шаблоне виртуальных машин на слой приложений (Application Layer).
2. Создать образ виртуальной машины, состоящий из нескольких слоев.
3. Развернуть созданный образ на гипервизорах, которые поддерживают решение Citrix App Layering.
4. Настроить создание временных виртуальных машин из созданного образа.

Подробнее об установке антивирусного ПО совместно с Citrix App Layering см. в документации Citrix App Layering (https://docs.citrix.com/en-us/citrix-app-layering/4.html).

Совместимость с технологией Citrix Provisioning (Citrix Provisioning Services)

Чтобы обеспечить совместимость Легкого агента для Windows с технологией Citrix Provisioning (Citrix Provisioning Services), требуется выполнить следующие действия:

1. Если на виртуальной машине установлено программное обеспечение Citrix Provisioning Target Device, его требуется удалить перед началом установки Легкого агента. После завершения установки Легкого агента вам нужно установить Citrix Provisioning Target Device.
2. Установку Легкого агента для Windows требуется выполнить одним из следующих способов:

- С помощью мастера установки. Установите флажок **Обеспечить совместимость с Citrix PVS** на шаге **Дополнительные параметры**.
- Удаленно через Kaspersky Security Center. Установите флажок **Обеспечить совместимость с Citrix PVS** в параметрах инсталляционного пакета.

Совместимость с технологией VMware App Volumes

Перед установкой на шаблоне виртуальных машин вам нужно создать файл %SVAgent%\Config\Custom\snapvol.cfg и добавить в него следующие исключения:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Подробнее см. в документации VMware (https://docs.vmware.com/en/VMware-App-Volumes/2103/app-volumes-admin-guide/GUID-0B588F2C-4054-4C5B-B491-F55BDA33A028.html).

Об обновлении Легкого агента для Windows версии 5.2

Если вы использовали компонент Легкий агент для Windows, входящий в состав приложения Kaspersky Security для виртуальных сред 5.2 Легкий агент, для перехода к использованию Легкого агента для Windows версии 6.2 вам нужно выполнить следующие действия:

1. Удалить на виртуальных машинах и шаблонах виртуальных машин Легкий агент для Windows версии 5.2 (см. подробнее в справке Kaspersky Security для виртуальных сред 5.2 Легкий агент).

2. Установить (см. раздел "Об установке Легкого агента для Windows" на стр. 90) на виртуальных машинах и шаблонах виртуальных машин приложение Kaspersky Endpoint Security для Windows, которое работает в режиме Легкого агента, и Агент администрирования.
3. Если для управления компонентами решения вы используете Консоль администрирования Kaspersky Security Center, вы можете сконвертировать политики и задачи поиска вирусов, настроенные для Легкого агента для Windows версии 5.2. Конвертация выполняется с помощью мастера массовой конвертации политик и задач Kaspersky Security Center (см. подробнее в справке Kaspersky Security Center).

   Сконвертированные политики и задачи используют параметры политик и задач Легкого агента для Windows версии 5.2. Параметры, которые отсутствовали в политиках и задачах версии 5.2, в сконвертированных политиках и задачах принимают значения по умолчанию. Сконвертированные политики и задачи имеют название "<Название исходной политики или задачи> (конвертированная)".

   > Чтобы использовать сконвертированную политику, измените ее статус на **Активная**.

4. Удалить политики для Сервера защиты и для Легкого агента для Windows версии 5.2 и оставшиеся компоненты приложения Kaspersky Security для виртуальных сред 5.2 Легкий агент:
   - компоненты управления Kaspersky Security для виртуальных сред 5.2 Легкий агент;
   - SVM, входящие в состав приложения Kaspersky Security версии 5.2.

   Об удалении компонентов версии 5.2 см. подробнее в справке Kaspersky Security для виртуальных сред 5.2 Легкий агент.

Подготовка Легких агентов к работе

Для подготовки Легких агентов к работе требуется выполнить следующие действия:

1. Настроить параметры, необходимые для обнаружения SVM и подключения Легких агентов к SVM (см. раздел "О подключении Легкого агента к SVM" на стр. 13).

   Чтобы настроить параметры для Легкого агента для Linux, вам нужно создать политику для приложения Kaspersky Endpoint Security для Linux, работающего в режиме Легкого агента.

   Чтобы настроить параметры для Легкого агента для Windows, вам нужно создать политику для приложения Kaspersky Endpoint Security для Windows, работающего в режиме Легкого агента.

   Следуя указаниям мастера создания политики, вам нужно выбрать способ обнаружения SVM (см. раздел "Настройка параметров обнаружения SVM" на стр. 140) и в зависимости от выбранного способа настроить параметры подключения к Серверу интеграции или задать список адресов SVM.
2. Убедиться в том, что установлено подключение Легких агентов к SVM (см. раздел "О подключении Легкого агента к SVM" на стр. 13) и к Серверу интеграции (см. раздел "Настройка параметров подключения Легких агентов к Серверу интеграции" на стр. 138).
3. Убедиться в том, что Легкие агенты получили информацию о лицензии, по которой активировано решение Kaspersky Security для виртуальных сред Легкий агент (см. раздел "Об активации решения" на стр. 78).

   После активации решения на SVM и подключения Легких агентов к SVM компонент Сервер защиты передает информацию о лицензии Легким агентам. Вы можете посмотреть информацию о

лицензии, которую использует Легкий агент, на виртуальной машине с установленным Легким агентом.

4. Убедиться в том, что на защищенных виртуальных машинах установлены обновления баз, необходимых для работы Легкого агента.

   Обновление баз на защищенных виртуальных машинах выполняется с помощью специальной задачи *Обновление*, в которой в качестве источника обновлений указана папка на SVM. Задача обновления запускается автоматически.

   Вы можете проверить актуальность баз на защищенной виртуальной машине с Легким агентом:

   - Для Легкого агента для Linux: с помощью команды `kesl-control --app-info`.
   - Для Легкого агента для Windows: в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows.

Подробнее о настройке параметров приложений, работающих в режиме Легкого агента, см. в справке соответствующего приложения: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Отображение виртуальных машин и SVM в Kaspersky Security Center

После установки Kaspersky Security в виртуальной инфраструктуре SVM и защищенные виртуальные машины с установленным Агентом администрирования передают информацию о себе в Kaspersky Security Center. По умолчанию Kaspersky Security Center добавляет устройства с установленными компонентами Kaspersky Security в папку **Нераспределенные устройства**.

В Консоли администрирования Kaspersky Security Center SVM отображается под именем, которое вы указали во время развертывания этой SVM. Имя защищенной виртуальной машины совпадает с сетевым именем виртуальной машины (hostname). Если на Сервере администрирования Kaspersky Security Center уже зарегистрирована виртуальная машина с таким именем, то к имени новой виртуальной машины добавляется окончание с порядковым номером, например: <Имя>~1, <Имя>~2.

Если перед установкой решения вы настроили правила перемещения виртуальных машин в группы администрирования (см. раздел "Настройка правил перемещения виртуальных машин в группы администрирования" на стр. 48), Kaspersky Security Center перемещает устройства с установленными компонентами Kaspersky Security в указанные группы администрирования в соответствии с настроенными правилами перемещения устройств.

После установки компонентов решения SVM и защищенные виртуальные машины передают в Kaspersky Security Center теги. Вы можете использовать эти теги при создании правил перемещения SVM и защищенных виртуальных машин в группы администрирования.

SVM передает в Kaspersky Security Center следующий тег:

%VmType%=SVM – признак, определяющий, что эта виртуальная машина является SVM.

Защищенная виртуальная машина с установленным Агентом администрирования Kaspersky Security Center передает в Kaspersky Security Center следующие теги:

- %VmType%=<Persistent / Nonpersistent> – признак, определяющий, является ли эта виртуальная машина временной или постоянной виртуальной машиной:
  - %VmType%=Persistent – постоянная виртуальная машина;

- %VmType%=Nonpersistent – временная виртуальная машина.

- %KsvlaMode%=<Yes / No> – признак, определяющий режим работы приложения Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows на виртуальной машине:
  - %KsvlaMode%=Yes – приложение используется в режиме Легкого агента для защиты виртуальных сред;
  - %KsvlaMode%=No – приложение используется в стандартном режиме.

Вы можете вручную перемещать SVM и виртуальные машины в группу администрирования **Управляемые устройства** или во вложенные группы администрирования (подробнее о перемещении устройств в группы администрирования см. в справке Kaspersky Security Center).

Просмотр списка SVM, подключенных к Серверу интеграции

Вы можете посмотреть список всех SVM, которые подключены к Серверу интеграции, в Веб-консоли Сервера интеграции или в Консоли Сервера интеграции.

Как посмотреть информацию об SVM, подключенных к Серверу интеграции, в Веб-консоли Сервера интеграции

► *Чтобы посмотреть информацию об SVM, подключенных к Серверу интеграции:*

1. Откройте Веб-консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Веб-консоль Сервера интеграции" на стр. 64).
2. Перейдите в раздел **Список подключенных SVM**.

   В открывшемся окне отображается список SVM, подключенных к Серверу интеграции, в виде таблицы. В таблице содержится следующая информация о каждой SVM:

   - IP-адрес SVM.
   - Расположение SVM. В зависимости от вида защищаемой виртуальной инфраструктуры:
     - IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором развернута SVM.
     - IP-адрес в формате IPv4 или полное доменное имя (FQDN) микросервиса Keystone, управляющего проектом OpenStack, в рамках которого развернута SVM.

   Вы можете сортировать список по столбцу **IP-адрес SVM**, выполнять поиск по списку, а также экспортировать список в формате CSV с помощью кнопки, расположенной над таблицей.
3. Чтобы посмотреть подробную информацию об SVM, нажмите на IP-адрес выбранной SVM в списке.

   Откроется окно, содержащее следующую информацию о выбранной SVM:

   - Идентификатор SVM.
   - IP-адрес SVM.
   - Расположение SVM. В зависимости от вида защищаемой виртуальной инфраструктуры:
     - IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором развернута SVM.

- IP-адрес в формате IPv4 или полное доменное имя (FQDN) микросервиса Keystone, управляющего проектом OpenStack, в рамках которого развернута SVM.

- Информация о том, шифруется ли канал передачи данных от Легких агентов.
- Порт на SVM для передачи запросов на проверку Серверу защиты от Легких агентов при защищенном соединении.
- Порт на SVM для передачи запросов на проверку Серверу защиты от Легких агентов при незащищенном соединении.
- Порт на SVM для передачи служебных запросов Серверу защиты от Легких агентов при защищенном соединении.
- Порт на SVM для передачи служебных запросов Серверу защиты от Легких агентов при незащищенном соединении.

Как посмотреть информацию об SVM, подключенных к Серверу интеграции, в Консоли Сервера интеграции

► *Чтобы посмотреть информацию об SVM, подключенных к Серверу интеграции:*

1. Откройте Консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Список подключенных SVM**.

   В правой части окна в таблице отображается следующая информация обо всех SVM, подключенных к Серверу интеграции:

   - IP-адрес SVM.
   - Расположение SVM. В зависимости от вида защищаемой виртуальной инфраструктуры:
     - IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором развернута SVM.
     - IP-адрес в формате IPv4 или полное доменное имя (FQDN) микросервиса Keystone, управляющего проектом OpenStack, в рамках которого развернута SVM.
3. Чтобы посмотреть подробную информацию, выберите SVM в таблице и откройте окно **Информация об SVM** двойным щелчком мыши или по ссылке **Детальная информация**, расположенной над таблицей.

   В окне отображается следующая информация о выбранной SVM:

   - Уникальный идентификатор SVM.
   - IP-адрес SVM.
   - Расположение SVM. В зависимости от вида защищаемой виртуальной инфраструктуры:
     - IP-адрес в формате IPv4 или полное доменное имя (FQDN) гипервизора, на котором развернута SVM.
     - IP-адрес в формате IPv4 или полное доменное имя (FQDN) микросервиса Keystone, управляющего проектом OpenStack, в рамках которого развернута SVM.
   - Порт на SVM для передачи запросов на проверку Серверу защиты от Легких агентов при защищенном соединении.
   - Порт на SVM для передачи запросов на проверку Серверу защиты от Легких агентов при незащищенном соединении.

- Порт на SVM для передачи служебных запросов Серверу защиты от Легких агентов при защищенном соединении.
- Порт на SVM для передачи служебных запросов Серверу защиты от Легких агентов при незащищенном соединении.
- Информация о том, шифруется ли канал передачи данных от Легких агентов.

kaspersky

Процедура приемки

Перед вводом приложения в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

► *Чтобы убедиться, что установка решения завершилась успешно, выполните следующие действия:*

1. Если вы используете Сервер интеграции на базе Windows:
   a. Убедитесь, что на устройстве, где установлен Сервер интеграции, в списке установленных приложений операционной системы отображается **Kaspersky Security для виртуальных сред 6.2 Легкий агент – компоненты управления**.
   b. Убедитесь, что на устройстве, где установлен Сервер интеграции, в списке служб операционной системы присутствует служба **Сервер интеграции Kaspersky Security для виртуальных сред Легкий агент** и эта служба запущена.
2. Если вы используете Сервер интеграции на базе Linux: убедитесь, что на устройстве, где установлен Сервер интеграции, в списке служб systemd присутствует служба *viis.service* и эта служба запущена.
3. Откройте список установленных плагинов управления в Kaspersky Security Center Web Console или в Консоли администрирования (в зависимости от используемой консоли управления Kaspersky Security Center) и убедитесь, что в списке присутствуют веб-плагины управления Сервера защиты, Сервера интеграции, Легкого агента для Linux и Легкого агента для Windows (см. раздел "Установка веб-плагинов Kaspersky Security" на стр. 59) или MMC-плагины управления Сервера защиты, Легкого агента для Linux и Легкого агента для Windows (см. раздел "Установка MMC-плагинов Kaspersky Security" на стр. 60).
4. Откройте папку **Управляемые устройства** в Kaspersky Security Center Web Console или в Консоли администрирования и убедитесь, что в папке присутствуют группы администрирования, которые вы настроили (см. раздел "Настройка правил перемещения виртуальных машин в группы администрирования" на стр. 48). Проверьте, что все виртуальные машины с компонентами решения помещены в эти группы администрирования.
5. Откройте группу администрирования, в которую входят SVM, и убедитесь, что на закладке **Устройства** все SVM имеют статус **ОК** (зеленый).
6. Откройте группу администрирования, в которую входят виртуальные машины с компонентом Легкий агент, и убедитесь, что на закладке **Устройства** все виртуальные машины имеют статус **ОК** (зеленый) и состояние защиты **Выполняется**.

В этом разделе

Безопасное состояние решения

Решение находится в безопасном состоянии (сертифицированной конфигурации), если выполняются

следующие условия:

- Решение активировано на всех SVM (см. раздел "Процедура активации решения" на стр. 82), сведения о лицензии переданы на защищенные виртуальные машины (см. раздел "Об активации решения" на стр. 78).
- Базы решения обновлены на всех SVM (см. раздел "Процедура обновления баз решения на SVM" на стр. 88) и на всех защищенных виртуальных машинах (см. раздел "Подготовка Легких агентов к работе" на стр. 95).
- Настроена активная политика для Сервера защиты (см. раздел "Автоматическое создание задач и политики по умолчанию для Сервера защиты" на стр. 75).
- Настроена активная политика для Легких агентов (см. раздел "Подготовка Легких агентов к работе" на стр. 95).
- Параметры решения находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 240).
- На защищенной виртуальной машине приложение Kaspersky Endpoint Security для Linux или приложение Kaspersky Endpoint Security для Windows, используемое в режиме Легкого агента, запущено и находится в безопасном состоянии. См. подробнее в разделе "Безопасное состояние приложения" в руководстве соответствующего приложения.

Проверка работоспособности решения

Чтобы проверить работоспособность решения, выполните процедуру, описанную в разделе "Проверка работоспособности. Тестовый файл EICAR" руководств Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Windows.

Разделение доступа к функциям решения по пользовательским ролям

О разделении доступа к функциям Легкого агента для Linux по пользовательским ролям см. в руководстве Kaspersky Endpoint Security для Linux в разделе "Разделение доступа к функциям приложения по пользовательским ролям".

О разделении доступа к функциям Легкого агента для Windows по пользовательским ролям см. в руководстве Kaspersky Endpoint Security для Windows в разделах "Защита паролем" и "Разделение доступа к функциям приложения по пользовательским ролям".

kaspersky

Концепция управления решением

Вы можете управлять работой компонентов решения следующими средствами:

- Для управления компонентом Сервер защиты вы можете использовать Консоль администрирования Kaspersky Security Center или Kaspersky Security Center Web Console (см. раздел "Об управлении решением через Kaspersky Security Center" на стр. 104).
- Для управления компонентом Сервер интеграции вы можете использовать:
  - Веб-консоль Сервера интеграции (см. раздел "О Веб-консоли Сервера интеграции" на стр. 130);
  - Консоль Сервера интеграции (только для Сервера интеграции на базе Windows).
- Для управления компонентом Легкий агент для Linux вы можете использовать:
  - Kaspersky Security Center Web Console или Консоль администрирования Kaspersky Security Center;
  - команды управления и задачи командной строки Kaspersky Endpoint Security для Linux.

  Подробнее об управлении приложением Kaspersky Endpoint Security для Linux см. в справке приложения (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).
- Для управления компонентом Легкий агент для Windows вы можете использовать:
  - Kaspersky Security Center Web Console или Консоль администрирования Kaspersky Security Center;
  - локальный интерфейс приложения Kaspersky Endpoint Security для Windows.
  - команды управления приложением Kaspersky Endpoint Security для Windows из командной строки.

  Подробнее об управлении приложением Kaspersky Endpoint Security для Windows см. в справке приложения (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

В этом разделе

kaspersky

Об управлении решением через Kaspersky Security Center

Kaspersky Security Center позволяет вам удаленно управлять работой компонентов решения Kaspersky Security, установленных на клиентских устройствах. В случае решения Kaspersky Security клиентскими устройствами Kaspersky Security Center являются SVM с Серверами защиты, и виртуальные машины, на которых установлены Легкие агенты.

Используя возможности Kaspersky Security Center, вы можете:

- устанавливать и удалять компоненты решения в виртуальной инфраструктуре;
- запускать и останавливать работу Легких агентов на защищенных виртуальных машинах;
- централизованно управлять защитой виртуальных машин с помощью политик и задач;
- управлять лицензионными ключами для решения;
- обновлять базы и программные модули решения;
- формировать отчеты о событиях, которые произошли во время работы компонентов решения.

Для управления решением Kaspersky Security через Kaspersky Security Center вы можете использовать следующие консоли управления Kaspersky Security Center:

- Kaspersky Security Center Web Console (далее также "Web Console"). Представляет собой веб-интерфейс для управления системой защиты, построенной на основе приложений "Лаборатории Касперского". Вы можете работать в Kaspersky Security Center Web Console через браузер на любом устройстве, которое имеет доступ к Серверу администрирования.

  Интерфейс для управления решением Kaspersky Security через Kaspersky Security Center Web Console обеспечивают веб-плагины (см. раздел "О плагинах управления Kaspersky Security" на стр. 105) управления (далее также "веб-плагины").

- Консоль администрирования Kaspersky Security Center (далее также "Консоль администрирования"). Представляет собой оснастку к Microsoft Management Console (MMC), которая устанавливается на рабочее место администратора и предоставляет пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

  Интерфейс для управления решением Kaspersky Security через Консоль администрирования Kaspersky Security Center обеспечивают MMC-плагины (см. раздел "О плагинах управления Kaspersky Security" на стр. 105) управления для Консоли администрирования на основе MMC (далее также "MMC-плагины").

Консоль Сервера интеграции не запускается через Kaspersky Security Center Web Console. Если вы используете Web Console, вы можете запускать Консоль Сервера интеграции с помощью исполняемого файла (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65) или установить веб-плагин Сервера интеграции и использовать Веб-консоль Сервера интеграции (см. раздел "О Веб-консоли Сервера интеграции" на стр. 130).

В зависимости от используемой консоли управления Kaspersky Security Center может меняться набор доступных функций приложений, работающих в режиме Легкого агента. См. подробнее в справке соответствующего приложения: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Управление работой решения Kaspersky Security через Kaspersky Security Center, независимо от используемой консоли управления, осуществляется с помощью политик и задач:

- *Политики* (см. раздел "*Управление решением с помощью политик Kaspersky Security Center*" на стр. 106) определяют параметры работы Легких агентов и Серверов защиты.
- *Задачи (см. раздел "Управление решением с помощью задач" на стр.* 121*)* реализуют такие функции, как активация решения, проверка виртуальных машин, обновление баз и программных модулей решения.

С помощью политик и задач вы можете устанавливать одинаковые параметры работы Легких агентов или Серверов защиты, установленных на клиентских устройствах группы администрирования.

Подробную информацию о политиках и задачах см. в справке Kaspersky Security Center.

О плагинах управления Kaspersky Security

Для управления компонентами решения Kaspersky Security с помощью Kaspersky Security Center Web Console используются следующие веб-плагины управления:

- Веб-плагин управления Сервера защиты (Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты).
- Веб-плагин управления Сервера интеграции (Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер интеграции). После установки этого плагина в Kaspersky Security Center Web Console становится доступна Веб-консоль Сервера интеграции (см. раздел "О Веб-консоли Сервера интеграции" на стр. 130).
- Веб-плагин управления Легкого агента для Linux (приложения Kaspersky Endpoint Security для Linux).
- Веб-плагин управления Легкого агента для Windows (приложения Kaspersky Endpoint Security для Windows).

Если вы хотите использовать Kaspersky Security Center Web Console для управления компонентами решения Kaspersky Security, вам нужно установить веб-плагины (см. раздел "Установка веб-плагинов Kaspersky Security" на стр. 59) на том устройстве, на котором установлено приложение Kaspersky Security Center Web Console.

Управление компонентами Kaspersky Security с помощью веб-плагинов доступно всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console через браузер.

Для управления компонентами решения Kaspersky Security с помощью Консоли администрирования

Kaspersky Security Center используются следующие MMC-плагины управления:

- MMC-плагин управления Сервера защиты (Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты).
- MMC-плагин управления Легкого агента для Linux (приложения Kaspersky Endpoint Security для Linux).
- MMC-плагин управления Легкого агента для Windows (приложения Kaspersky Endpoint Security для Windows).

Вам нужно установить MMC-плагины (см. раздел "Установка MMC-плагинов Kaspersky Security" на стр. 60) на том устройстве, на котором установлена Консоль администрирования Kaspersky Security Center.

Управление решением с помощью политик Kaspersky Security Center

Для работы с политиками вы можете использовать Консоль администрирования Kaspersky Security Center или Kaspersky Security Center Web Console.

Вы можете выполнять следующие действия над политиками:

- создавать политику;
- изменять параметры политики;
- удалять политику;
- изменять состояние политики;
- копировать и перемещать политику;
- экспортировать и импортировать политику.

Параметры и блоки параметров политик имеют *атрибут "замок"*, который показывает, наложен ли запрет на изменение параметра или блока параметров в параметрах задач и в политиках вложенного уровня иерархии (для вложенных групп администрирования, виртуальных и подчиненных Серверов администрирования).

Для управления параметрами решения Kaspersky Security используются следующие политики Kaspersky Security Center:

- **Политика для Сервера защиты** (на стр. 108) (политика *Kaspersky Security <номер версии> Легкий агент – Сервер защиты*) применяется на SVM. Политика определяет параметры работы Серверов защиты на всех SVM, входящих в группу администрирования, для которой настроена политика.

  Мастер первоначальной настройки Kaspersky Security Center позволяет автоматически создать политику по умолчанию для Сервера защиты. Политика по умолчанию создается для группы администрирования **Управляемые устройства** под именем **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты** и применяется на всех SVM, которые помещаются в группу администрирования **Управляемые устройства** или в любую вложенную группу администрирования.

  Вы можете изменить значения параметров этой политики, настроенные по умолчанию.

- **Политика для Легкого агента для Linux** (политика *Kaspersky Endpoint Security для Linux <номер версии>*) применяется на виртуальных машинах с гостевыми операционными системами Linux и определяет параметры работы приложения Kaspersky Endpoint Security для Linux, которое

используется в режиме Легкого агента. Политика применяется на всех защищенных виртуальных машинах, входящих в группу администрирования, для которой настроена политика.

С помощью политики для Легкого агента для Linux вы можете настраивать:

- параметры работы приложения Kaspersky Endpoint Security для Linux;
- параметры подключения Легкого агента для Linux к SVM и к Серверу интеграции, необходимые для работы приложения Kaspersky Endpoint Security для Linux в режиме Легкого агента для защиты виртуальной инфраструктуры.

Подробную информацию о параметрах политики Kaspersky Endpoint Security для Linux см. в справке приложения Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).

- **Политика для Легкого агента для Windows** (политика *Kaspersky Endpoint Security для Windows <номер версии>*) применяется на виртуальных машинах с гостевыми операционными системами Windows и определяет параметры работы приложения Kaspersky Endpoint Security для Windows, которое используется в режиме Легкого агента. Политика применяется на всех защищенных виртуальных машинах, входящих в группу администрирования, для которой настроена политика.

  С помощью политики для Легкого агента для Windows вы можете настраивать:

  - параметры работы приложения Kaspersky Endpoint Security для Windows;
  - параметры подключения Легкого агента для Windows к SVM и к Серверу интеграции, необходимые для работы приложения Kaspersky Endpoint Security для Windows в режиме Легкого агента для защиты виртуальной инфраструктуры.

  Подробную информацию о параметрах политики Kaspersky Endpoint Security для Windows см. в справке приложения Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

В политике для Легкого агента для Windows и в политике для Легкого агента для Linux вы можете создавать *профили политик*. Использование профилей политик позволяет более гибко настроить параметры работы Легких агентов на разных виртуальных машинах. Профиль политики может содержать параметры, которые отличаются от параметров "базовой" политики и применяются на защищенных виртуальных машинах при выполнении настроенных вами условий (правил активации).

Вы можете создавать и настраивать профили политики в свойствах политик для Легкого агента в разделе **Профили политик**.

Подробнее о работе с политиками и профилями политик см. в справке Kaspersky Security Center.

В этом разделе

kaspersky

Политика для Сервера защиты

С помощью политики для Сервера защиты вы можете настраивать следующие параметры работы решения:

- Параметры использования Kaspersky Security Network (KSN) в работе Сервера защиты (см. раздел "Использование Kaspersky Security Network" на стр. 166).
- Параметры загрузки обновлений баз и программных модулей решения на SVM (см. раздел "Настройка параметров загрузки обновлений на SVM" на стр. 157) .
- Параметры SNMP-мониторинга состояния SVM.
- Параметры подключения SVM к Серверу интеграции (см. раздел "Настройка параметров подключения SVM к Серверу интеграции" на стр. 136).
- Параметры подключения Легких агентов к SVM:
  - теги для подключения Легких агентов (см. раздел "Настройка использования тегов для подключения" на стр. 142);
  - параметры защиты соединения между Легкими агентами и Сервером защиты (см. раздел "Защита соединения между Легким агентом и Сервером защиты" на стр. 144).
- Режим защиты больших инфраструктур (см. раздел "Защита больших инфраструктур" на стр. 153).
- Дополнительные параметры работы Сервера защиты (см. раздел "Настройка дополнительных параметров Сервера защиты" на стр. 117).

> Если вы хотите настраивать дополнительные параметры работы Сервера защиты, вам нужно включить отображение дополнительных параметров в политике (см. раздел "Настройка отображения дополнительных параметров Сервера защиты" на стр. 116).

Изменение некоторых параметров политики может привести к выходу решения из безопасного состояния. Описание параметров, влияющих на безопасное состояние решения, и значений параметров в безопасном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 240).

> Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование решения.

О настройке общих параметров политики и параметрах событий см. в справке Kaspersky Security Center.

Вы можете создавать политику для Сервера защиты с помощью Консоли администрирования Kaspersky

Security Center или с помощью Kaspersky Security Center Web Console.

Создание политики для Сервера защиты в Kaspersky Security Center Web Console

► *Чтобы создать политику для Сервера защиты в Kaspersky Security Center Web Console:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик и профилей политик.

2. Выберите группу администрирования, содержащую SVM, на которых должна применяться политика. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите в открывшемся окне группу администрирования. Новая политика будет определять параметры работы Серверов защиты, установленных на SVM из выбранной группы администрирования.

3. Нажмите на кнопку **Добавить**, расположенную над списком политик и профилей.

   Запустится мастер создания политики.

4. На первом шаге мастера в списке выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты**.

   Перейдите к следующему шагу мастера.

5. Примите решение об использовании Kaspersky Security Network (KSN) в работе Сервера защиты (см. раздел "Использование Kaspersky Security Network" на стр. 166). Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выберите один из следующих вариантов:

   - **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**

     Если выбран этот вариант, вы соглашаетесь с условиями, изложенными в Положении о Kaspersky Security Network. Если в свойствах Сервера администрирования Kaspersky Security Center включена служба прокси-сервера KSN, использование KSN в работе Сервера защиты будет включено. Службы KSN используются во время защиты виртуальных машин и при выполнении задач проверки виртуальных машин.

     Выбор типа инфраструктуры KSN (KSN или KPSN) и настройка использования KPSN выполняется в свойствах Сервера администрирования Kaspersky Security Center. См. подробнее в справке Kaspersky Security Center.

     KSN по умолчанию используется в расширенном режиме. Если требуется, вы можете выключить использование расширенного KSN в свойствах политики для Сервера защиты.

   - **Я не принимаю условия Положения о Kaspersky Security Network**

     Если выбран этот вариант, вы отказываетесь от использования Kaspersky Security Network.

     Службы KSN не будут использоваться в работе Сервера защиты.

   При необходимости позже вы сможете изменить решение об использовании KSN и настроить режим KSN в свойствах политики для Сервера защиты (см. раздел "Настройка использования KSN в работе Сервера защиты" на стр. 169).

Использование инфраструктурного решения Kaspersky Security Network приводит к выходу решения Kaspersky Security из безопасного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN.

Если вы хотите использовать KSN в работе Сервера защиты, убедитесь в том, что параметры KSN настроены в свойствах Сервера администрирования Kaspersky Security Center (в разделе **Прокси-сервер KSN**). В свойствах Сервера администрирования определяется тип инфраструктуры KSN (KSN или KPSN), параметры прокси-сервера KSN и параметры KPSN. См. подробнее в справке Kaspersky Security Center.

Параметры KSN, настроенные для Сервера защиты, не влияют на использование KSN в работе Легкого агента. О настройке параметров KSN для Легких агентов см. в справках приложений, которые используются в режиме Легкого агента: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm). Рекомендуется задавать одинаковые параметры использования KSN для Сервера защиты и для Легкого агента, который взаимодействует с этим Сервером защиты.

Перейдите к следующему шагу мастера.

6. Настройте подключение SVM к Серверу интеграции:
   a. Нажмите на кнопку **Настройка**.
   b. В открывшемся окне **Подключение к Серверу интеграции** введите параметры:
      - **Адрес**

        IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

        Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

      - **Порт**

        Порт для подключения к Серверу интеграции.

        По умолчанию указан порт 7271.

   c. Нажмите на кнопку **Проверить**.

      Мастер создания политики проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибки или не является доверенным, в окне **Подключение к Серверу интеграции** отображается сообщение об этом. Нажав на строку **Посмотреть полученный сертификат**, вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

   d. Чтобы сохранить полученный сертификат и продолжить подключение к Серверу интеграции, в блоке **Выбор действия** выберите вариант **Игнорировать**.

e. Укажите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **Проверить**.

Мастер создания политики выполняет подключение к Серверу интеграции. Если установить подключение не удалось, в окне отображается сообщение об ошибке. Если подключение установлено, окно **Подключение к Серверу интеграции** закрывается, в окне мастера создания политики в поле **Подключение к Серверу интеграции** отображается статус **Установлено**.

Перейдите к следующему шагу мастера.

7. На закладке **Общие** укажите название новой политики, определите ее статус (**Активна** или **Неактивна**) и настройте параметры наследования. Подробнее см. в справке Kaspersky Security Center.
8. Если требуется, перейдите на закладку **Параметры программы** и измените настроенные по умолчанию параметры политики:
   - Список версий Легких агентов, для которых Сервер защиты будет получать обновления (см. раздел "Настройка параметров загрузки обновлений на SVM" на стр. 157).
   - Параметры подключения Легких агентов к SVM:
     - теги для подключения Легких агентов (см. раздел "Настройка использования тегов для подключения" на стр. 142);
     - параметры защиты соединения между Легкими агентами и Сервером защиты (см. раздел "Защита соединения между Легким агентом и Сервером защиты" на стр. 144).
   - Режим защиты больших инфраструктур (см. раздел "Защита больших инфраструктур" на стр. 153).
   - Дополнительные параметры работы Сервера защиты (см. раздел "Настройка дополнительных параметров Сервера защиты" на стр. 117).

   Включение автоматического обновления модулей решения и включение SNMP-мониторинга состояния SVM приводит к выходу решения Kaspersky Security из безопасного состояния.
9. Нажмите на кнопку **Сохранить**, чтобы завершить создание политики.

Созданная политика отобразится в списке политик на закладке **Политики и профили политик**.

Политика распространится на SVM и начнет применяться в работе Сервера защиты на этой SVM после того, как Сервер администрирования Kaspersky Security Center передаст информацию Серверу защиты при следующем подключении SVM.

Если на SVM не запущен Агент администрирования, созданная политика не применяется на этой SVM.

Если на закладке **Общие** вы указали состояние политики **Неактивна**, созданная политика не применяется на SVM.

kaspersky

Создание политики для Сервера защиты в Консоли администрирования Kaspersky Security Center

► *Чтобы создать политику для Сервера защиты в Консоли администрирования Kaspersky Security Center:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую SVM, на которых должна применяться политика. Политика будет определять параметры работы Серверов защиты, установленных на этих SVM.

   На закладке **Устройства** папки с названием группы администрирования вы можете просмотреть список SVM, которые входят в состав этой группы администрирования.

2. В рабочей области выберите закладку **Политики**.

3. Нажмите на кнопку **Новая политика**, чтобы запустить мастер создания политики.

   Вы также можете запустить мастер с помощью пункта **Создать → Политику** контекстного меню в списке политик.

4. На первом шаге мастера в списке выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты**.

   Перейдите к следующему шагу мастера.

5. Введите название новой политики.

6. Если вы хотите перенести в создаваемую политику параметры из политики для Сервера защиты предыдущей версии Kaspersky Security, установите флажок **Использовать параметры политики для предыдущей версии программы**.

   Перейдите к следующему шагу мастера.

7. Примите решение об использовании Kaspersky Security Network (KSN) в работе Сервера защиты (см. раздел "Использование Kaspersky Security Network" на стр. 166). Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выберите один из следующих вариантов:

   - **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**

     Если выбран этот вариант, вы соглашаетесь с условиями, изложенными в Положении о Kaspersky Security Network. Если в свойствах Сервера администрирования Kaspersky Security Center включена служба прокси-сервера KSN, использование KSN в работе Сервера защиты будет включено. Службы KSN используются во время защиты виртуальных машин и при выполнении задач проверки виртуальных машин.

     Выбор типа инфраструктуры KSN (KSN или KPSN) и настройка использования KPSN выполняется в свойствах Сервера администрирования Kaspersky Security Center. См. подробнее в справке Kaspersky Security Center.

     KSN по умолчанию используется в расширенном режиме. Если требуется, вы можете выключить использование расширенного KSN в свойствах политики для Сервера защиты.

   - **Я не принимаю условия Положения о Kaspersky Security Network**

     Если выбран этот вариант, вы отказываетесь от использования Kaspersky Security Network.

     Службы KSN не будут использоваться в работе Сервера защиты.

При необходимости позже вы сможете изменить решение об использовании KSN и настроить режим KSN в свойствах политики для Сервера защиты (см. раздел "Настройка использования KSN в работе Сервера защиты" на стр. 169).

Использование инфраструктурного решения Kaspersky Security Network приводит к выходу решения Kaspersky Security из безопасного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN.

Если вы хотите использовать KSN в работе Сервера защиты, убедитесь в том, что параметры KSN настроены в свойствах Сервера администрирования Kaspersky Security Center (в разделе **Прокси-сервер KSN**). В свойствах Сервера администрирования определяется тип инфраструктуры KSN (KSN или KPSN), параметры прокси-сервера KSN и параметры KPSN. См. подробнее в справке Kaspersky Security Center.

Параметры KSN, настроенные для Сервера защиты, не влияют на использование KSN в работе Легкого агента. О настройке параметров KSN для Легких агентов см. в справках приложений, которые используются в режиме Легкого агента: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm). Рекомендуется задавать одинаковые параметры использования KSN для Сервера защиты и для Легкого агента, который взаимодействует с этим Сервером защиты.

Перейдите к следующему шагу мастера.

8. На этом шаге вам предлагается настроить автоматическое получение обновлений программных модулей решения вместе с пакетом обновлений баз решения и настроить список версий Легких агентов, для которых Сервер защиты будет получать обновления.

   Включение автоматического обновления модулей решения приводит к выходу решения из безопасного состояния. Допускается устанавливать только обновления программных модулей, прошедшие сертификационные испытания.

   По умолчанию обновления программных модулей решения не включаются в пакет обновлений.

   Если требуется, с помощью флажков настройте список версий Легких агентов, для которых Сервер защиты будет получать обновления. Должна быть выбрана хотя бы одна версия. Список содержит поддерживаемые версии Легких агентов. Если в списке отсутствует версия Легкого агента, для которой требуется получать обновления, нажмите на кнопку **Обновить**.

   Перейдите к следующему шагу мастера.

9. На этом шаге вам предлагается включить SNMP-мониторинг состояния SVM с помощью системы сетевого управления, использующей протокол SNMP.

   Включение SNMP-мониторинга состояния SVM приводит к выходу решения Kaspersky Security из безопасного состояния.

   По умолчанию SNMP-мониторинг состояния SVM выключен.

Перейдите к следующему шагу мастера.

10. Если вы включили отображение дополнительных параметров политики для Сервера защиты (см. раздел "Настройка отображения дополнительных параметров Сервера защиты" на стр. 116), настройте дополнительные параметры работы Сервера защиты (см. раздел "Настройка дополнительных параметров Сервера защиты" на стр. 117):

    Перейдите к следующему шагу мастера.

11. Настройте подключение SVM к Серверу интеграции.

    - **Адрес**

        IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

        Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен, в поле по умолчанию указано доменное имя этого устройства.

        Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или Сервер интеграции установлен на другом устройстве, поле требуется заполнить вручную.

        Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

    - **Порт**

        Порт для подключения к Серверу интеграции.

        По умолчанию указан порт 7271.

    Перейдите к следующему шагу мастера.

    Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, в открывшемся окне **Подключение к Серверу интеграции** укажите пароль администратора Сервера интеграции (пароль учетной записи `admin`).

    Мастер создания политики проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. Вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

12. Если требуется, включите защиту соединения между Легкими агентами и Серверами защиты с помощью шифрования (см. раздел "Защита соединения между Легким агентом и Сервером защиты" на стр. 144):

    - **Шифровать канал передачи данных между Легким агентом и Сервером защиты**

        Защитить соединение между Легкими агентами и Серверами защиты с помощью шифрования.

        Если флажок установлен, между Легким агентом и Сервером защиты, находящимся под управлением политики, устанавливается защищенное соединение после подключения Легкого агента к SVM с этим Сервером защиты. Легкий агент может

подключиться к SVM, на которой включена защита соединения, только если на Легком агенте также включена защита соединения или на SVM разрешено незащищенное соединение.

Если флажок снят, между Легким агентом и Сервером защиты устанавливается незащищенное соединение после подключения Легкого агента к SVM с этим Сервером защиты.

По умолчанию флажок снят.

- **Разрешить незащищенное соединение, если не удалось установить защищенное соединение**

  Разрешать незащищенное соединение между Легкими агентами и Серверами защиты.

  Если флажок установлен, между Легкими агентами и Серверами защиты, находящимися под управлением политики, может быть установлено незащищенное соединение, если не удалось установить защищенное соединение.

  Если флажок снят, между Легкими агентами и Серверами защиты, находящимися под управлением политики, может быть установлено только защищенное соединение. Легкий агент не сможет подключиться к SVM, если не удалось установить защищенное соединение с Сервером защиты на этой SVM.

  По умолчанию флажок снят.

Перейдите к следующему шагу мастера.

13. Если вы хотите регулировать подключение Легких агентов к SVM с помощью тегов для подключения, настройте параметры использования тегов для подключения (см. раздел "Настройка использования тегов для подключения" на стр. 142):

    - **Разрешить подключение Легких агентов с указанными тегами**

      Разрешать подключение к SVM только Легким агентам, которым назначены теги, указанные в поле ниже.

      Если флажок установлен, к SVM могут подключаться только Легкие агенты с указанными тегами.

      Если флажок снят, к SVM могут подключаться только Легкие агенты, которым не назначены теги.

      Флажок по умолчанию снят.

    - Список тегов

      К SVM могут подключаться только Легкие агенты, которым назначены теги, указанные в этом поле.

      Вы можете указать один или несколько тегов через точку с запятой.

14. Если требуется, включите оптимизацию для защиты больших инфраструктур (см. раздел "Защита больших инфраструктур" на стр. 153).

    Перейдите к следующему шагу мастера.

15. Завершите работу мастера создания политики.

Созданная политика отобразится в списке политик группы администрирования на закладке **Политики** и в папке **Политики** дерева консоли.

Политика распространится на SVM после того, как Сервер администрирования Kaspersky Security Center передаст информацию программе Kaspersky Security при следующем подключении SVM. Kaspersky Security начнет защищать виртуальные машины на гипервизоре в соответствии с параметрами политики.

Если на SVM не запущен Агент администрирования, созданная политика не применяется на этой SVM.

Если на последнем шаге мастера создания политики вы выбрали вариант **Неактивная политика**, созданная политика не применяется на SVM.

Настройка отображения дополнительных параметров Сервера защиты

Если вы хотите настраивать дополнительные параметры Сервера защиты с помощью Консоли администрирования Kaspersky Security Center, вам нужно создать ключ `AdvancedUI` типа REG_DWORD и установить значение `1` для этого ключа в следующей ветке реестра операционной системы на устройстве, где установлена Консоль администрирования Kaspersky Security Center:

- HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Products\SVM\<номер версии>\Settings\ – для 32-разрядных операционных систем;
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\Components\34\Products\SVM\<номер версии>\Settings\ – для 64-разрядных операционных систем;

  где <номер версии> – номер установленной версии решения Kaspersky Security в формате X.X.X.X.

Если вы хотите настраивать дополнительные параметры работы SVM с помощью Web Console, вам нужно создать файл AdvancedPluginSettings.json в следующей папке:

- %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\svm_<номер версии> – для устройств с операционными системами Windows;
- /var/opt/kaspersky/ksc-web-console/server/plugins/svm_<номер версии> – для устройств с операционными системами Linux;

  где <номер версии> – номер установленной версии решения Kaspersky Security в формате X_X_X_X.

Структуру и параметры файла AdvancedPluginSettings.json вы можете посмотреть в шаблоне файла с названием ~AdvancedPluginSettings.json, расположенном в той же папке.

Файл AdvancedPluginSettings.json должен содержать параметр `AdvancedUI` со значением `1`:

```
{

"AdvancedUI" : 1

}
```

После создания или сохранения файла требуется заново открыть в Web Console политику для Сервера защиты.

kaspersky

Настройка дополнительных параметров Сервера защиты

Вы можете настраивать дополнительные параметры Сервера защиты в политике для Сервера защиты с помощью Консоли администрирования Kaspersky Security Center или Kaspersky Security Center Web Console. Предварительно вам нужно включить отображение дополнительных параметров (см. раздел "Настройка отображения дополнительных параметров Сервера защиты" на стр. 116) в политике.

Как настроить дополнительные параметры Сервера защиты в Консоли администрирования Kaspersky Security Center

► *Чтобы настроить дополнительные параметры Сервера защиты:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
4. В окне свойств политики в списке слева выберите раздел **Дополнительные параметры**.
5. В правой части окна настройте параметры:

   - **Максимальное количество одновременных запросов на проверку**

     Максимальное количество запросов на проверку от Легких агентов, которые одновременно обрабатывает Сервер защиты. Легкие агенты формируют запросы на проверку в ходе защиты виртуальных машин и в ходе выполнения задач проверки.

     По умолчанию Сервер защиты одновременно обрабатывает 75 запросов на проверку.

   - **Максимальное количество задач проверки, запущенных по расписанию**

     Максимальное количество одновременно выполняемых на Сервере защиты задач проверки, которые запущены по расписанию на Легком агенте. Для Сервера защиты такие задачи проверки являются низкоприоритетными.

     По умолчанию одновременно выполняется пять низкоприоритетных задач проверки.

   - **Максимальное количество задач проверки, запущенных вручную**

     Максимальное количество одновременно выполняемых на Сервере защиты задач проверки, которые вы запустили вручную. Для Сервера защиты такие задачи проверки являются высокоприоритетными.

     По умолчанию одновременно выполняется пять высокоприоритетных задач проверки.

   - **Уровень трассировки**

     Раскрывающийся список, в котором можно выбрать уровень трассировки работы Сервера защиты (службы `scanserver` на SVM). Уровни трассировки упорядочены таким образом, что каждый из них включает в себя все нижестоящие уровни.

     Доступны следующие элементы раскрывающегося списка:

- **Значение по умолчанию**. Значение, установленное по умолчанию.
- **Трассировка выключена (0)**. Создание файлов трассировки выключено.
- **Запуск и остановка компонентов (100)**. Информационные сообщения о запуске и остановке Сервера защиты.
- **Критические ошибки (200)**. Сообщения о критических ошибках в работе Сервера защиты.
- **Ошибки (300)**. Сообщения об ошибках и критических ошибках в работе Сервера защиты.
- **Критические предупреждения (400)**. Критические предупреждения и сообщения об обычных и критических ошибках.
- **Предупреждения (500)**. Все предупреждения и сообщения об обычных и критических ошибках.
- **Важные сообщения (600)**. Важные сообщения, все предупреждения и сообщения об обычных и критических ошибках.
- **Информационные сообщения (700)**. Информационные сообщения, важные сообщения и все предупреждения и сообщения об обычных и критических ошибках.
- **Отладочные сообщения (800)**. Отладочные сообщения и все информационные и важные сообщения, а также все предупреждения и сообщения об обычных и критических ошибках.
- **Детальные отладочные сообщения (900)**. Отладочные сообщения с более подробной информацией и все информационные и важные сообщения, а также все предупреждения и сообщения об обычных и критических ошибках.
- **Все сообщения (1000)**. Все возможные сообщения и предупреждения.

- **Восстановить значения по умолчанию**

  Восстанавливает значения параметров, заданные по умолчанию.

6. Нажмите на кнопку **Применить**.

Как настроить дополнительные параметры Сервера защиты в Kaspersky Security Center Web Console

► *Чтобы настроить дополнительные параметры Сервера защиты:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.
4. В открывшемся окне свойств политики выберите вкладку **Параметры приложения** и перейдите в раздел **Дополнительные параметры**.
5. В правой части окна настройте параметры:

   - **Максимальное количество одновременных запросов на проверку**

     Максимальное количество запросов на проверку от Легких агентов, которые одновременно обрабатывает Сервер защиты. Легкие агенты формируют запросы на проверку в ходе защиты виртуальных машин и в ходе выполнения задач

проверки.

По умолчанию Сервер защиты одновременно обрабатывает 75 запросов на проверку.

- **Максимальное количество задач проверки, запущенных по расписанию**

  Максимальное количество одновременно выполняемых на Сервере защиты задач проверки, которые запущены по расписанию на Легком агенте. Для Сервера защиты такие задачи проверки являются низкоприоритетными.

  По умолчанию одновременно выполняется пять низкоприоритетных задач проверки.

- **Максимальное количество задач проверки, запущенных вручную**

  Максимальное количество одновременно выполняемых на Сервере защиты задач проверки, которые вы запустили вручную. Для Сервера защиты такие задачи проверки являются высокоприоритетными.

  По умолчанию одновременно выполняется пять высокоприоритетных задач проверки.

- **Уровень трассировки**

  Раскрывающийся список, в котором можно выбрать уровень трассировки работы Сервера защиты (службы `scanserver` на SVM). Уровни трассировки упорядочены таким образом, что каждый из них включает в себя все нижестоящие уровни.

  Доступны следующие элементы раскрывающегося списка:

  - **Значение по умолчанию**. Значение, установленное по умолчанию.
  - **Трассировка выключена (0)**. Создание файлов трассировки выключено.
  - **Запуск и остановка компонентов (100)**. Информационные сообщения о запуске и остановке Сервера защиты.
  - **Критические ошибки (200)**. Сообщения о критических ошибках в работе Сервера защиты.
  - **Ошибки (300)**. Сообщения об ошибках и критических ошибках в работе Сервера защиты.
  - **Критические предупреждения (400)**. Критические предупреждения и сообщения об обычных и критических ошибках.
  - **Предупреждения (500)**. Все предупреждения и сообщения об обычных и критических ошибках.
  - **Важные сообщения (600)**. Важные сообщения, все предупреждения и сообщения об обычных и критических ошибках.
  - **Информационные сообщения (700)**. Информационные сообщения, важные сообщения и все предупреждения и сообщения об обычных и критических ошибках.
  - **Отладочные сообщения (800)**. Отладочные сообщения и все информационные и важные сообщения, а также все предупреждения и сообщения об обычных и критических ошибках.
  - **Детальные отладочные сообщения (900)**. Отладочные сообщения с более подробной информацией и все информационные и важные сообщения, а также все предупреждения и сообщения об обычных и критических ошибках.
  - **Все сообщения (1000)**. Все возможные сообщения и предупреждения.

- **Восстановить значения по умолчанию**

  Восстанавливает значения параметров, заданные по умолчанию.

6. Нажмите на кнопку **Применить**.

Изменение параметров политики для Сервера защиты

Вы можете изменять параметры политики для Сервера защиты с помощью Web Console, а также с помощью Консоли администрирования.

Как изменить параметры политики для Сервера защиты в Kaspersky Security Center Web Console

► *Чтобы изменить параметры политики для Сервера защиты:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую SVM, на которых применяется политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне группу администрирования.

   В списке отобразятся политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.

   Откроется окно свойств политики.

4. Измените параметры политики (см. раздел "Политика для Сервера защиты" на стр. 108) на вкладке **Параметры приложения**.

   Если вы хотите настроить дополнительные параметры работы SVM, вам нужно включить отображение дополнительных параметров политики для Сервера защиты в реестре операционной системы (см. раздел "Настройка отображения дополнительных параметров Сервера защиты" на стр. 116).

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Как изменить параметры политики для Сервера защиты в Консоли администрирования Kaspersky Security Center

► *Чтобы изменить параметры политики для Сервера защиты:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные SVM.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

   Вы также можете открыть окно свойств политики с помощью пункта **Свойства** контекстного меню политики или по ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

4. Измените параметры политики (см. раздел "Политика для Сервера защиты" на стр. 108).

   Если вы хотите настроить дополнительные параметры работы SVM, вам нужно включить отображение дополнительных параметров политики для Сервера защиты в реестре операционной системы (см. раздел "Настройка отображения дополнительных параметров Сервера защиты" на стр. 116).

Разделы **Общие** и **Оповещение о событиях** окна **Свойства: <Название политики>** стандартны для Kaspersky Security Center. Описание стандартных разделов см. в справке Kaspersky Security Center.

5. Нажмите на кнопку **OK** в окне **Свойства: <Название политики>**.

Управление решением с помощью задач

Вы можете управлять работой решения Kaspersky Security для виртуальных сред 6.2 Легкий агент с помощью задач для Сервера защиты и задач для Легкого агента.

Задача для Сервера защиты – это задача, которая выполняется на SVM и определяет параметры работы Сервера защиты на этой SVM. Для работы с задачами для Сервера защиты вы можете использовать Консоль администрирования Kaspersky Security Center или Kaspersky Security Center Web Console.

Задача для Легкого агента – это задача, которая выполняется на защищенной виртуальной машине с установленным компонентом Легкий агент и реализует функции Легкого агента. Управлять задачами для Легкого агента вы можете как централизованно через Kaspersky Security Center, так и локально на защищенных виртуальных машинах. Подробнее см. в справке приложения, которое используется в режиме Легкого агента: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Вы можете использовать задачи следующих типов в Kaspersky Security Center:

- *Групповая задача* – задача, которая выполняется на клиентских устройствах выбранной группы администрирования. Применительно к решению Kaspersky Security групповые задачи выполняются на SVM или на защищенных виртуальных машинах, входящих в группы администрирования.
- *Задача для наборов устройств* – задача, которая выполняется на одной или нескольких SVM или защищенных виртуальных машинах, независимо от их вхождения в группы администрирования.

Вы можете управлять работой решения Kaspersky Security для виртуальных сред 6.2 Легкий агент с помощью следующих задач для Сервера защиты:

- **Активация решения**. Задача позволяет добавить на SVM лицензионный ключ для активации решения или для продления срока действия лицензии.
- **Обновление баз** (см. раздел "**Создание задачи Обновление баз**" на стр. 158). В результате выполнения задачи Сервер защиты загружает пакет обновлений баз, необходимых для работы решения, и устанавливает обновления баз на SVM.
- **Обновление модулей решения на SVM**. В результате выполнения задачи Сервер защиты устанавливает обновления программных модулей решения на SVM.
- **Откат обновления баз** (см. раздел "**Создание задачи Откат обновления баз**" на стр. 162). В результате выполнения задачи Сервер защиты откатывает последнее обновление баз решения на SVM.

Вы можете выполнять следующие действия над задачами для Сервера защиты в Kaspersky Security Center:

- создавать (см. раздел "Создание задач для Сервера защиты" на стр. 122) и удалять задачи;
- изменять параметры (см. раздел "Изменение параметров задач для Сервера защиты" на стр. 124) задач;
- запускать и останавливать (см. раздел "Запуск и остановка задач для Сервера защиты" на стр. 125) задачи;

- просматривать результаты выполнения (см. раздел "Просмотр информации о ходе и результатах выполнения задач" на стр. 126) задач.

Сервер защиты отправляет на Сервер администрирования Kaspersky Security Center информацию обо всех событиях, произошедших во время выполнения задач. Подробнее о работе с задачами см. в справке Kaspersky Security Center.

В этом разделе

Создание задач для Сервера защиты

Вы можете создавать задачи для Сервера защиты с помощью Web Console, а также с помощью Консоли администрирования.

Как создать задачу для Сервера защиты в Kaspersky Security Center Web Console

► *Чтобы создать задачу для Сервера защиты:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. На первом шаге мастера выполните следующие действия:

   a. В раскрывающемся списке **Программа** выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты**.

   b. В раскрывающемся списке **Тип задачи** выберите тип задачи, которую вы хотите создать.

   c. В поле **Название задачи** введите название новой задачи.

   d. В блоке **Выбор устройств, которым будет назначена задача** выберите способ определения области действия задачи. Область действия задачи – это набор SVM, на которых будет выполняться задача.

      - Выберите вариант **Назначить задачу группе администрирования**, если задача должна выполняться на всех SVM, входящих в определенную группу администрирования.
      - Выберите вариант **Задать адреса устройств вручную или импортировать из списка**, если задача должна выполняться на указанных SVM.
      - Выберите вариант **Назначить задачу выборке устройств**, если задача должна выполняться на SVM, входящих в выборку устройств по предопределенному критерию. О создании выборки устройств см. в справке Kaspersky Security Center.

   Перейдите к следующему шагу мастера.

4. В зависимости от выбранного способа определения области действия задачи выполните одно из следующих действий:

   - В дереве групп администрирования установите флажки рядом с нужными группами администрирования.
   - В списке устройств установите флажки рядом с нужными SVM. Если нужные SVM отсутствуют в списке, вы можете добавить их следующими способами:
     - С помощью кнопки **Добавить устройства**. Вы можете добавить устройства по имени или IP-адресу, добавить устройства из указанного IP-диапазона или выбрать устройства из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.
     - С помощью кнопки **Импортировать устройства из файла**. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

     Если вы импортируете список адресов SVM из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

   - В списке выберите название выборки, содержащей нужные SVM.

   Перейдите к следующему шагу мастера.
5. Настройте доступные параметры задачи, следуя указаниям мастера. Наличие доступных параметров зависит от типа создаваемой задачи.
6. Если вы хотите настроить расписание запуска или другие параметры задачи, не доступные в мастере создания задачи, на последнем шаге мастера установите флажок **Открыть окно свойств задачи после ее создания**.
7. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Как создать задачу для Сервера защиты в Консоли администрирования Kaspersky Security Center

► *Чтобы создать задачу для Сервера защиты:*

1. В Консоли администрирования Kaspersky Security Center выполните одно из следующих действий:

   - Если вы хотите создать задачу, которая будет выполняться на SVM, входящих в выбранную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи** и нажмите на кнопку **Новая задача**.

     Запустится мастер создания задачи для устройств выбранной группы администрирования.
   - Если вы хотите создать задачу, которая будет выполняться на одной или нескольких SVM (задачу для набора устройств), в дереве консоли выберите папку **Задачи** и нажмите на кнопку **Новая задача** в рабочей области.

     Запустится мастер создания задачи для набора устройств.
2. На первом шаге мастера выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты** и тип задачи.

   Перейдите к следующему шагу мастера.

3. Если вы создаете задачу для набора устройств, мастер предложит определить область действия задачи. Область действия задачи – это набор SVM, на которых будет выполняться задача.

   a. Укажите способ определения области действия задачи: выбрать SVM из списка устройств, обнаруженных Сервером администрирования, задать адреса SVM вручную, импортировать список SVM из файла или указать ранее настроенную выборку устройств (см. подробнее в справке Kaspersky Security Center).

   b. В зависимости от указанного вами способа определения области действия в открывшемся окне выполните одно из следующих действий:

      - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от названия устройства.
      - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM вручную.
      - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM.
      - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.

   Перейдите к следующему шагу мастера.

4. Настройте доступные параметры задачи, следуя указаниям мастера.
5. Введите название новой задачи и перейдите к следующему шагу мастера.
6. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера, на последнем шаге установите флажок **Запустить задачу после завершения работы мастера**.
7. Завершите работу мастера.

Изменение параметров задач для Сервера защиты

Вы можете изменять параметры задач для Сервера защиты с помощью Web Console, а также с помощью Консоли администрирования.

Как изменить параметры задачи для Сервера защиты в Kaspersky Security Center Web Console

► *Чтобы изменить параметры задачи для Сервера защиты:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Выполните одно из следующих действий:

   - Если вы хотите изменить параметры задачи, которая выполняется на всех SVM, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне группу администрирования.

     В списке отобразятся только задачи, настроенные для выбранной группы администрирования.

   - Если вы хотите изменить параметры задачи, которая выполняется на одной или нескольких SVM (задачи для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне верхний узел с именем Сервера администрирования.

     В списке отобразятся все задачи, созданные на Сервере администрирования.

3. В списке задач выберите нужную задачу и откройте окно свойств задачи по ссылке в названии задачи.
4. Настройте параметры задачи:
   - На вкладке **Общие** вы можете изменить название задачи.
   - На вкладке **Параметры программы** вы можете настроить специфические параметры задачи. Наличие настраиваемых параметров зависит от типа задачи.
   - На вкладке **Расписание** вы можете настроить расписание запуска задачи и дополнительные параметры запуска и остановки задачи.

   Вкладки **Общие**, **Результаты**, **Параметры**, **Расписание** и **История ревизий** окна свойств задачи стандартны для Kaspersky Security Center, см. подробнее в справке Kaspersky Security Center.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Как изменить параметры задачи для Сервера защиты в Консоли администрирования Kaspersky Security Center

► *Чтобы изменить параметры задачи для Сервера защиты:*

1. В Консоли администрирования Kaspersky Security Center выполните одно из следующих действий:
   - Если вы хотите изменить параметры задачи, которая выполняется на SVM, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи**.
   - Если вы хотите изменить параметры задачи, которая выполняется на одной или нескольких SVM (задачи для набора устройств), в дереве консоли выберите папку **Задачи**.
2. В списке задач выберите нужную задачу и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.

   Вы также можете открыть окно свойств задачи с помощью пункта **Свойства** контекстного меню задачи.
3. Измените параметры задачи.
4. Нажмите на кнопку **Применить** или на кнопку **ОК** в окне **Свойства: <Название задачи>**, чтобы сохранить внесенные изменения.

Запуск и остановка задач для Сервера защиты

Вы можете запускать и останавливать задачи для Сервера защиты с помощью Web Console, а также с помощью Консоли администрирования. Вы можете запускать или останавливать задачу в любой момент независимо от выбранного режима запуска задачи.

Как запустить или остановить задачу для Сервера защиты в Kaspersky Security Center Web Console

► *Чтобы запустить или остановить задачу для Сервера защиты:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.
2. Выполните одно из следующих действий:

- Если вы хотите запустить или остановить задачу, которая выполняется на всех SVM, выходящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне группу администрирования.

  В списке отобразятся только задачи, созданные для выбранной группы администрирования.

- Если вы хотите запустить или остановить задачу, которая выполняется на одной или нескольких SVM (задачу для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне верхний узел с именем Сервера администрирования.

  В списке отобразятся все задачи, созданные на Сервере администрирования.

3. В списке задач установите флажок слева от задачи, которую вы хотите запустить или остановить.
4. Выполните одно из следующих действий:
   - Если вы хотите запустить задачу, нажмите на кнопку **Запустить**.
   - Если вы хотите остановить выполнение задачи, нажмите на кнопку **Остановить**.

Как запустить или остановить задачу для Сервера защиты в Консоли администрирования Kaspersky Security Center

► *Чтобы запустить или остановить задачу для Сервера защиты:*

1. В Консоли администрирования Kaspersky Security Center выполните одно из следующих действий:
   - Если вы хотите запустить или остановить задачу, которая выполняется на SVM, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи**.
   - Если вы хотите запустить или остановить задачу, которая выполняется на одной или нескольких SVM (задачу для набора устройств), в дереве консоли выберите папку **Задачи**.
2. В списке задач выберите нужную задачу, откройте контекстное меню задачи и выберите действие, которое вы хотите выполнить.

Просмотр информации о ходе и результатах выполнения задач

Вы можете просматривать информацию о ходе и результатах выполнения задач для Сервера защиты с помощью Web Console, а также с помощью Консоли администрирования.

Как просмотреть информацию о выполнении задачи для Сервера защиты в Kaspersky Security Center Web Console

► *Чтобы просмотреть информацию о выполнении задачи для Сервера защиты:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Выполните одно из следующих действий:
   - Если вы хотите посмотреть информацию о задаче, которая выполняется на всех SVM, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне группу администрирования.

     В списке отобразятся только задачи, настроенные для выбранной группы администрирования.

- Если вы хотите изменить параметры задачи, которая выполняется на одной или нескольких SVM (задачи для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне верхний узел с именем Сервера администрирования.

  В списке отобразятся все задачи, созданные на Сервере администрирования.

Краткая информация о выполнении задачи отображается в столбце **Статус** в списке задач.

3. Чтобы посмотреть более подробную информацию о задаче, выполните одно из следующих действий:

   - Откройте окно свойств задачи по ссылке в названии задачи и перейдите на вкладку **Результаты**.

     В таблице на вкладке **Результаты** отображается информация о выполнении задачи на устройствах.

   - Установите флажок рядом с названием нужной задачи в списке задач и нажмите на кнопку **Результат выполнения**, расположенную над списком.

     В открывшемся окне **Состояние задачи** отображается диаграмма с информацией о выполнении задачи на устройствах. С помощью кнопки **Посмотреть результаты** вы можете открыть вкладку **Результаты** в окне свойств задачи.

Как просмотреть информацию о выполнении задачи для Сервера защиты в Консоли администрирования Kaspersky Security Center

Вы можете посмотреть информацию о ходе и результатах выполнения задач в Консоли администрирования Kaspersky Security Center одним из следующих способов:

- В окне **Результаты выполнения задачи**. Окно открывается с помощью пункта **Результаты** контекстного меню задачи.
- В списке событий, которые решение Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center. Списки событий вы можете просматривать на вкладке **События** в рабочей области узла **Сервер администрирования <имя сервера>**. Информация на вкладке **События** представлена в виде выборок событий. Каждая выборка включает в себя только события определенного типа. В списке отображаются события из выборки, которая в настоящий момент указана в раскрывающемся списке **Выборки событий**. Чтобы отобразить список событий выборки, используйте кнопку **Запустить выборку**. Чтобы обновить список, используйте ссылку **Обновить**.

О правах доступа к параметрам политик и задач в Kaspersky Security Center

Kaspersky Security Center предоставляет доступ на основе ролей к функциям управляемых приложений "Лаборатории Касперского". Права на доступ к параметрам политик и задач (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center. Вы можете назначать учетным записям пользователей права на выполнение определенных действий в функциональных областях решения Kaspersky Security.

Для решения Kaspersky Security выделена одна функциональная область: **Базовая функциональность**. В эту функциональную область входят следующие параметры и функции:

- Параметры подключения SVM к Серверу интеграции.
- Параметры подключения Легких агентов к SVM.
- Параметры SNMP-мониторинга.

- Параметры использования KSN в работе Сервера защиты.
- Дополнительные параметры работы Сервера защиты.
- Задача активации решения Kaspersky Security.
- Задача обновления баз решения и задача отката последнего обновления баз.
- Задача обновления программных модулей решения на SVM.

Следующие действия доступны пользователю независимо от прав учетной записи в функциональных областях решения Kaspersky Security:

- Просмотр параметров политик.
- Создание политики.

  При создании политики пользователь может настроить только параметры, относящиеся к функциональным областям, в которых учетная запись пользователя обладает правами на изменение.

Для выполнения следующих действий с политиками и задачами учетная запись пользователя должна обладать правами в функциональных областях решения Kaspersky Security:

- Для изменения параметров ранее сохраненной политики требуются права на чтение и на изменение в функциональных областях, к которым относятся эти параметры.
- Для изменения состояния политики (активная / неактивная) и удаления политики требуются права на чтение и на изменение в функциональных областях, к которым относятся параметры политики, закрытые "замком". Если в политике есть параметры, закрытые "замком" (то есть, параметры, для которых установлен запрет на изменение параметра в дочерних политиках), и у пользователя нет прав на чтение и на изменение в функциональных областях, к которым относятся эти параметры, то удалить или изменить состояние политики невозможно. Если в политике нет параметров, для которых установлен запрет на изменение параметра в дочерних политиках, то удаление или изменение состояния политики доступны пользователю независимо от прав учетной записи в функциональных областях решения.
- Для создания, удаления и настройки параметров задач требуются права на чтение и на изменение в функциональной области, к которой относится задача.
- Для просмотра параметров задачи требуются права на чтение в функциональной области, к которой относится задача.
- Для запуска задачи требуются права на выполнение в функциональной области, к которой относится задача.

Подробнее о правах доступа к объектам Kaspersky Security Center и о настройке прав доступа к функциональным областям Kaspersky Security см. в справке Kaspersky Security Center (https://support.kaspersky.com/KSC/14.2/ru-RU/index.htm).

О Консоли Сервера интеграции

Консоль Сервера интеграции устанавливается на устройстве с операционной системой Windows и запускается (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65) с помощью исполняемого файла или по ссылке из Консоли администрирования Kaspersky Security Center (в случае установки на том же устройстве).

Не рекомендуется использовать Консоль Сервера интеграции для управления Сервером интеграции на базе Linux.

Консоль Сервера интеграции и содержит следующие разделы:

- **Параметры Сервера интеграции**

  В этом разделе отображается следующая информация:

  - версия Сервера интеграции, к которому выполнено подключение;
  - имя учетной записи, под которой выполнено подключение к Серверу интеграции;
  - тип аутентификации, который использовался при подключении к Серверу интеграции;
  - IP-адрес в формате IPv4 или полное доменное имя (FQDN) и порт Сервера интеграции.

- **Учетные записи Сервера интеграции**

  В этом разделе вы можете изменить пароли внутренних учетных записей Сервера интеграции (см. раздел "Изменение паролей учетных записей Сервера интеграции" на стр. 174), которые используются для подключения консолей управления, SVM и Легких агентов к Серверу интеграции.

- **Список подключенных SVM**

  В этом разделе вы можете посмотреть информацию об SVM, которые подключены к Серверу интеграции (см. раздел "Просмотр списка SVM, подключенных к Серверу интеграции" на стр. 97).

- **Управление SVM**

  Этот раздел открывается по умолчанию после запуска Консоли Сервера интеграции. В этом разделе вы можете запустить мастер управления SVM, который позволяет выполнить следующие действия:

  - развернуть SVM с компонентом Сервер защиты из образа в виртуальной инфраструктуре;
  - изменить конфигурацию ранее развернутых SVM;
  - удалить SVM.

  Развертывание, изменение конфигурации и удаление SVM с помощью мастера управления SVM не поддерживается в сертифицированной версии решения Kaspersky Security.

- **Параметры подключения к инфраструктуре**

  В этом разделе вы можете выполнить следующие действия:

  - посмотреть статус подключения Сервера интеграции к виртуальной инфраструктуре;
  - изменить параметры подключения (см. раздел "Изменение параметров подключения к виртуальной инфраструктуре в Консоли Сервера интеграции" на стр. 178) Сервера интеграции к виртуальной инфраструктуре;
  - если решение Kaspersky Security установлено в инфраструктуре VMware, настроить использование VMware NSX Manager (см. раздел "Изменение параметров подключения к виртуальной инфраструктуре в Консоли Сервера интеграции" на стр. 178) в работе решения;

- удалить виртуальную инфраструктуру из списка инфраструктур, к которым подключается Сервер интеграции (см. раздел "Удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 182).

- **Список тенантов**

  Если вы используете решение Kaspersky Security в режиме мультитенантности (см. раздел "Использование Kaspersky Security для виртуальных сред 6.2 Легкий агент в режиме мультитенантности" на стр. 191), в этом разделе вы можете посмотреть список всех тенантов (см. раздел "Получение информации о тенантах" на стр. 203), зарегистрированных в базе данных Сервера интеграции.

- **Параметры подключения к Kaspersky Security Center**

  Если вы используете решение Kaspersky Security в режиме мультитенантности (см. раздел "Использование Kaspersky Security для виртуальных сред 6.2 Легкий агент в режиме мультитенантности" на стр. 191) и вы развернули структуру защиты тенантов средствами REST API Сервера интеграции, в этом разделе вы можете настроить параметры подключения (см. раздел "Настройка параметров подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center" на стр. 194), необходимые для взаимодействия REST API Сервера интеграции с Сервером администрирования Kaspersky Security Center.

О Веб-консоли Сервера интеграции

Если вы используете Kaspersky Security Center Web Console, вы можете управлять Сервером интеграции через Веб-консоль Сервера интеграции. Веб-консоль Сервера интеграции доступна в Kaspersky Security Center Web Console в разделе **Параметры → Kaspersky Security для виртуальных сред <номер версии> Легкий агент – Сервер интеграции** после установки веб-плагина Сервера интеграции (см. раздел "Установка веб-плагинов Kaspersky Security" на стр. 59).

На главной странице Веб-консоли Сервера интеграции отображается информация о подключении к Серверу интеграции. Если подключение установлено, отображается адрес и порт подключения и версия Сервера интеграции.

Веб-консоль Сервера интеграции содержит следующие разделы:

- **Учетные записи Сервера интеграции**

  В этом разделе вы можете изменять пароли внутренних учетных записей Сервера интеграции (см. раздел "Изменение паролей учетных записей Сервера интеграции" на стр. 174), которые используются для подключения консолей управления, SVM и Легких агентов к Серверу интеграции.

- **Список подключенных SVM**

  В этом разделе вы можете посматривать информацию об SVM, которые подключены к Серверу интеграции (см. раздел "Просмотр списка SVM, подключенных к Серверу интеграции" на стр. 97).

- **Управление SVM**

  Этот раздел позволяет создавать следующие задания для Сервера интеграции:

  - задания на развертывание SVM;
  - задания на изменение конфигурации SVM;
  - задания на удаление SVM.

Развертывание, изменение конфигурации и удаление SVM с помощью Веб-консоли Сервера интеграции не поддерживается в сертифицированной версии решения Kaspersky Security.

- **Список виртуальных инфраструктур**

  В этом разделе отображается список виртуальных инфраструктур, к которым подключается Сервер интеграции.

  В этом разделе вы можете:

  - Настраивать (см. раздел "Подключение к виртуальной инфраструктуре в Веб-консоли Сервера интеграции" на стр. 69) подключение Сервера интеграции к виртуальной инфраструктуре. Для каждой инфраструктуры, в которой будет развернуто решение, вам нужно указать параметры подключения Сервера интеграции к объекту инфраструктуры, с которым должен взаимодействовать Сервер интеграции. В инфраструктуре на платформе VMware vSphere вы можете дополнительно настроить подключение к VMware NSX Manager.
  - Изменять параметры подключения (см. раздел "Изменение параметров подключения к виртуальной инфраструктуре в Веб-консоли Сервера интеграции" на стр. 175) Сервера интеграции к виртуальной инфраструктуре.
  - Просматривать статус подключения Сервера интеграции к виртуальной инфраструктуре.
  - Удалять виртуальные инфраструктуры (см. раздел "Удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 182) из списка инфраструктур, к которым подключается Сервер интеграции.

- **Режим мультитенантности**

  Если вы используете решение Kaspersky Security в режиме мультитенантности (см. раздел "Использование Kaspersky Security для виртуальных сред 6.2 Легкий агент в режиме мультитенантности" на стр. 191) и вы развернули структуру защиты тенантов средствами REST API Сервера интеграции, в этом разделе вы можете настраивать параметры подключения (см. раздел "Настройка параметров подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center" на стр. 194), необходимые для взаимодействия REST API Сервера интеграции с Сервером администрирования Kaspersky Security Center.

  Также в этом разделе вы можете посматривать список всех тенантов (см. раздел "Получение информации о тенантах" на стр. 203), зарегистрированных в базе данных Сервера интеграции, независимо от того, как вы развернули структуру защиты тенантов.

kaspersky

Запуск и остановка Kaspersky Security

Компонент Сервер защиты запускается автоматически при запуске операционной системы на SVM и останавливается при завершении работы операционной системы.

SVM, развернутая на гипервизоре VMware ESXi, автоматически запускается после включения гипервизора. Автоматическое включение SVM может не работать, если эта функция не активирована на уровне гипервизора или этот гипервизор находится в кластере VMware HA. См. подробнее в базе знаний VMware (https://kb.vmware.com/s/article/850).

Компонент Сервер интеграции запускается автоматически при запуске операционной системы на устройстве, где установлен Сервер интеграции, и останавливается при завершении работы операционной системы.

Компонент Легкий агент запускается автоматически при запуске операционной системы на защищенной виртуальной машине и останавливается при завершении работы операционной системы.

Защита виртуальных машин включается автоматически при запуске компонентов Легкий агент и Сервер защиты.

Если информация о лицензии не передана на защищенную виртуальную машину, Легкий агент работает в режиме ограниченной функциональности.

Задачи запускаются в соответствии со своим расписанием. Вы также можете запускать задачи вручную.

Останавливать и запускать Легкий агент для Linux вы можете стандартными средствами операционной системы Linux. См. подробнее в справке приложения Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm).

Останавливать и запускать Легкий агент для Windows вы можете удаленно с помощью Kaspersky Security Center или с помощью командной строки. См. подробнее в справке приложения Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

kaspersky

Состояние защиты виртуальной машины

Вы можете получать информацию о состоянии защиты виртуальных машин следующими способами:

- В Kaspersky Security Center с помощью статусов клиентских устройств (см. раздел "Статус клиентского устройства в Kaspersky Security Center" на стр. 133).
- В Kaspersky Security Center с помощью статусов функциональных компонентов Легкого агента (см. раздел "Статусы функциональных компонентов Легкого агента на виртуальных машинах" на стр. 134) на виртуальных машинах.
- На защищенной виртуальной машине:
  - Для Легкого агента для Linux: с помощью команды приложения Kaspersky Endpoint Security для Linux `kesl-control --app-info`. Команда выводит информацию о работе приложения и состоянии функциональных компонентов приложения. См. подробнее в справке приложения Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.1.0/ru-RU/264009.htm).
  - Для Легкого агента для Windows: с помощью виджета **Состояние защиты** в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows.
- В инфраструктуре на платформе VMware vSphere: с помощью тегов безопасности (Security Tags) (см. раздел "О тегах безопасности (Security Tags)" на стр. 134), которые решение Kaspersky Security может назначать защищенной виртуальной машине.

В этом разделе

Статус клиентского устройства в Kaspersky Security Center

Защищенная виртуальная машина (виртуальная машина, на которой установлен компонент Легкий агент) и SVM являются клиентскими устройствами для Kaspersky Security Center. Информация о состоянии клиентского устройства в Kaspersky Security Center отображается с помощью статуса клиентского устройства (*OK*, *Критический*, *Предупреждение*).

Статус клиентского устройства изменяется на *Критический* или *Предупреждение* по следующим причинам:

- В соответствии с правилами, определенными в Kaspersky Security Center. Например, статус изменяется, если на устройстве не установлено приложение защиты, давно не выполнялся поиск вирусов, устарели антивирусные базы или истек срок действия лицензии. Подробнее о причинах изменения статусов и настройке условий присвоения статусов см. в справке Kaspersky Security Center.

- Kaspersky Security Center получает статус устройства от управляемого приложения, то есть от компонентов решения Kaspersky Security.

  Получение статуса устройства от управляемого приложения должно быть включено в Kaspersky Security Center в списках условий назначения статусов *Критический* и *Предупреждение*. Условия назначения статусов устройства настраиваются в окне свойств группы администрирования.

  Статус SVM изменяется в следующих случаях:

  нет подключения к Серверу интеграции;

  нет подключения к виртуальной инфраструктуре.

  Статус защищенной виртуальной машины изменяется в следующих случаях:

  - нет подключения к Серверу интеграции;
  - нет подключения к SVM;
  - обнаружено изменение в файлах или реестре на виртуальной машине.

Подробнее о статусах клиентского устройства см. в справке Kaspersky Security Center.

Статусы функциональных компонентов Легкого агента на виртуальных машинах

В Консоли администрирования Kaspersky Security Center или в Kaspersky Security Center Web Console вы можете получать следующую информацию о функциональных компонентах Легкого агента:

- В свойствах приложения, работающего в режиме Легкого агента на виртуальной машине, отображается список функциональных компонентов Легкого агента. Для каждого компонента отображается его статус.
- В отчете Kaspersky Security Center *Отчет о статусе компонентов программы* отображается информация о функциональных компонентах Легкого агента, установленных и не установленных на виртуальных машинах. Для каждого из установленных компонентов в отчете отображается количество виртуальных машин, на которых установлен этот компонент, и количество групп администрирования, к которым относятся эти виртуальные машины.

  Отчет о статусе компонентов программы доступен в списке шаблонов отчета в Консоли администрирования Kaspersky Security Center (на вкладке **Отчеты** в рабочей области узла **Сервер администрирования <имя сервера>**), а также в Kaspersky Security Center Web Console (в разделе **Мониторинг и отчеты** → **Отчеты**).
- Вы можете строить выборки виртуальных машин, задавая в качестве условия выборки статус компонентов и / или номер версии приложения, работающего в режиме Легкого агента.

Подробнее о работе с отчетами и настройке выборки устройств см. в справке Kaspersky Security Center.

О тегах безопасности (Security Tags)

Если решение Kaspersky Security работает в виртуальной инфраструктуре на платформе VMware vSphere и

использует в своей работе VMware NSX Manager, решение Kaspersky Security может назначать защищенной виртуальной машине следующие теги безопасности (Security Tags):

- *ANTI_VIRUS.VirusFound.threat=high*. Тег назначается виртуальной машине, на которой обнаружены вирусы или другие вредоносные программы.
- *IDS_IPS.threat=high*. Тег назначается виртуальной машине, во входящем трафике которой обнаружена активность, характерная для сетевых атак.

Kaspersky Security может назначать теги безопасности, только если вы включили использование VMware NSX Manager и настроили параметры подключения Сервера интеграции к VMware NSX Manager в Веб-консоли Сервера интеграции (см. раздел "Подключение к виртуальной инфраструктуре в Веб-консоли Сервера интеграции" на стр. 69) или в Консоли Сервера интеграции (см. раздел "Изменение параметров подключения к виртуальной инфраструктуре в Консоли Сервера интеграции" на стр. 178).

Вы можете посматривать теги безопасности, назначенные виртуальной машине, в свойствах виртуальной машины:

- в консоли VMware vSphere Client в разделе **Hosts and Clusters** на вкладке **Summary**;
- в веб-консоли VMware NSX Manager в разделе **Inventory** → **Virtual Machines**.

Тег безопасности *ANTI_VIRUS.VirusFound.threat=high*, назначенный виртуальной машине решением Kaspersky Security, снимается автоматически, если в результате выполнения задачи полной проверки на виртуальной машине не обнаружены вирусы или другие вредоносные программы. Если тег безопасности *ANTI_VIRUS.VirusFound.threat=high* назначен виртуальной машине вручную средствами виртуальной инфраструктуры, его можно снять только вручную.

Тег безопасности *IDS_IPS.threat=high*, назначенный виртуальной машине решением Kaspersky Security или вручную средствами виртуальной инфраструктуры, можно снять только вручную.

После снятия тега вручную требуется перезапустить Легкий агент на виртуальной машине.

Подробнее о снятии и назначении тегов безопасности вручную см. в Базе знаний (https://support.kaspersky.ru/16005).

kaspersky

Подключение SVM и Легких агентов к Серверу интеграции

Для функционирования решения Kaspersky Security требуется постоянное взаимодействие между Сервером защиты и Сервером интеграции. Чтобы обеспечить это взаимодействие, вам нужно настроить подключение SVM с Сервером защиты к Серверу интеграции.

Если вы хотите, чтобы Легкие агенты получали информацию об SVM через Сервер интеграции (см. раздел "Настройка параметров обнаружения SVM" на стр. 140), или если вы хотите защищать соединение (см. раздел "Защита соединения между Легким агентом и Сервером защиты" на стр. 144) между Сервером защиты и Легким агентом, вам нужно настроить подключение Легких агентов к Серверу интеграции.

Информация о потере и восстановлении соединения Легкого агента и SVM с Сервером интеграции может сохраняться в виде событий в Kaspersky Security Center.

В этом разделе

Настройка параметров подключения SVM к Серверу интеграции

Вы можете настраивать параметры подключения SVM к Серверу интеграции с помощью Web Console или с помощью Консоли администрирования в политике для Сервера защиты, в том числе во время создания политики по умолчанию для Сервера защиты.

Как настроить параметры подключения SVM к Серверу интеграции в Kaspersky Security Center Web Console

► *Чтобы настроить параметры подключения SVM к Серверу интеграции:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.

4. В открывшемся окне свойств политики выберите вкладку **Параметры приложения** и перейдите в раздел **Параметры подключения SVM к Серверу интеграции**.

5. В правой части окна нажмите на кнопку **Изменить** и в открывшемся окне **Подключение к Серверу интеграции** укажите адрес и порт для подключения:

a. Укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

> Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

b. Если порт для подключения к Серверу интеграции отличается от используемого по умолчанию (7271), укажите номер порта в поле **Порт**.

6. Нажмите на кнопку **Проверить** в окне **Подключение к Серверу интеграции**.
7. Веб-плагин Kaspersky Security проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, в окне **Подключение к Серверу интеграции** отображается сообщение об этом. Вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, выберите вариант **Игнорировать**.
8. Укажите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **Проверить** в окне **Подключение к Серверу интеграции**.

   Выполняется проверка возможности подключения к Серверу интеграции. Если проверка подключения закончилась удачно и подключение к Серверу интеграции установлено, окно **Подключение к Серверу интеграции** закрывается. После подключения к Серверу интеграции с правами администратора в политику автоматически передается пароль учетной записи для подключения SVM к Серверу интеграции.

   Если проверка подключения закончилась неудачно или не удалось установить соединение с Сервером интеграции, в окне свойств политики отображается ошибка. Проверьте введенные параметры подключения.

   Информация об ошибках подключения к Серверу интеграции может записываться в файл трассировки Сервера интеграции (см. раздел "Файлы трассировки Сервера интеграции и Консоли Сервера интеграции" на стр. 230) (если вы включили запись информации в файл трассировки).
9. Нажмите на кнопку **Сохранить**.

Как настроить параметры подключения SVM к Серверу интеграции в Консоли администрирования Kaspersky Security Center

► *Чтобы настроить параметры подключения SVM к Серверу интеграции:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
4. В окне свойств политики в списке слева выберите раздел **Параметры подключения SVM к Серверу интеграции**.
5. В правой части окна укажите адрес и порт для подключения:

   a. По умолчанию в поле **Адрес** указывается доменное имя устройства, на котором установлена Консоль администрирования Kaspersky Security Center. Если это устройство не входит в домен или Сервер интеграции установлен на другом устройстве и в поле указан неверный адрес,

укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

> Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

b. Если порт для подключения к Серверу интеграции отличается от используемого по умолчанию (7271), укажите номер порта в поле **Порт**.

6. Нажмите на кнопку **Применить** в окне свойств политики.
7. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, откроется окно **Подключение к Серверу интеграции**. Укажите пароль администратора Сервера интеграции (пароль учетной записи `admin`). После подключения к Серверу интеграции с правами администратора в политику автоматически передается пароль учетной записи для подключения SVM к Серверу интеграции.

   Нажмите на кнопку **ОК** в окне **Подключение к Серверу интеграции**.

   MMC-плагин Kaspersky Security проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. Вы можете посмотреть информацию о полученном сертификате. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

   Выполняется проверка возможности подключения к Серверу интеграции. Если проверка подключения закончилась неудачно или не удалось установить соединение с Сервером интеграции, в окне свойств политики отображается ошибка. Проверьте введенные параметры подключения.

Информация об ошибках подключения к Серверу интеграции может записываться в файл трассировки Сервера интеграции (см. раздел "Файлы трассировки Сервера интеграции и Консоли Сервера интеграции" на стр. 230) (если вы включили запись информации в файл трассировки).

Настройка параметров подключения Легких агентов к Серверу интеграции

Вы можете настраивать параметры подключения Легких агентов к Серверу интеграции в политике для Легкого агента (в политике приложения, которое работает в режиме Легкого агента). Параметры обнаружения SVM для Легкого агента для Windows также доступны в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows.

Вам нужно настроить следующие параметры подключения к Серверу интеграции:

- IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции.

  > Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

- Порт для подключения к Серверу интеграции.

  По умолчанию указан порт 7271.

- Пароль администратора Сервера интеграции (пароль учетной записи `admin`).

Информация об ошибках подключения к Серверу интеграции может записываться в файл трассировки Сервера интеграции (см. раздел "Файлы трассировки Сервера интеграции и Консоли Сервера интеграции" на стр. 230) (если вы включили запись информации в файл трассировки).

Вы можете получать информацию о состоянии подключения Легкого агента к Серверу интеграции следующими способами:

- Для Легкого агента для Linux: с помощью команды приложения Kaspersky Endpoint Security для Linux `kesl-control --viis-info`.
- Для Легкого агента для Windows:
  - в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows;
  - с помощью команды приложения Kaspersky Endpoint Security для Windows `avp.com VIISINFO`.

Подробнее о настройке параметров приложений, работающих в режиме Легкого агента, см. в справке соответствующего приложения: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

kaspersky

Подключение Легких агентов к SVM

Для взаимодействия с Сервером защиты Легкий агент устанавливает и поддерживает подключение к SVM (см. раздел "О подключении Легкого агента к SVM" на стр. 13), на которой установлен этот Сервер защиты. Вы можете настраивать следующие параметры подключения Легкого агента к SVM:

- Способ обнаружения SVM (см. раздел "Настройка параметров обнаружения SVM" на стр. 140). Вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM.
- Теги для подключения (см. раздел "Настройка использования тегов для подключения" на стр. 142). Если вы используете теги для подключения, Легкий агент может подключаться только к тем SVM, на которых настроено использование этого тега для подключения.
- Защита соединения (см. раздел "Защита соединения между Легким агентом и Сервером защиты" на стр. 144) между Легким агентом и Сервером защиты. Вы можете защищать соединение между Легкими агентами и Серверами защиты с помощью шифрования.
- Алгоритм выбора SVM (см. раздел "Настройка алгоритма выбора SVM" на стр. 147) для подключения. Вы можете указать, какой алгоритм должны использовать Легкие агенты при выборе SVM для подключения.

В этом разделе

Настройка параметров обнаружения SVM

Вы можете настраивать параметры обнаружения SVM Легкими агентами в политике Легкого агента (в политике приложения, которое работает в режиме Легкого агента). Параметры обнаружения SVM для Легкого агента для Windows также доступны в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows.

Вы можете настроить следующие параметры обнаружения SVM (см. раздел "Об обнаружении SVM" на стр. 15) Легкими агентами:

- Способ, который Легкие агенты используют для обнаружения SVM:
  - **Использовать Сервер интеграции**

    Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них.

Если вы хотите использовать Сервер интеграции, вам нужно настроить параметры подключения Легких агентов к Серверу интеграции (см. раздел "Настройка параметров подключения Легких агентов к Серверу интеграции" на стр. 138).

- **Использовать список адресов SVM, заданный вручную**

  Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. раздел "Защита больших инфраструктур" на стр. 153), то подключение Легкого агента к этой SVM возможно, только если Легкий агент не учитывает расположение SVM. В разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Игнорировать**.

- Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную**, вам нужно сформировать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением политики. Вы можете добавить в список несколько IP-адресов или полных доменных имен SVM.

  В списке адресов SVM требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе решения.

Подробнее о настройке параметров приложений, работающих в режиме Легкого агента, см. в справке соответствующего приложения: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

В виртуальной инфраструктуре большого размера под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС, если вы выбрали вариант **Использовать Сервер интеграции**, вы можете настроить размер списка доступных SVM, который Сервер интеграции передает Легким агентам.

► *Чтобы настроить размер списка доступных SVM:*

1. Откройте на редактирование конфигурационный файл Сервера интеграции appsettings.json. В зависимости от версии Сервера интеграции файл расположен по следующему пути:
   - /var/opt/<KL_LOWCASE>/viis/common/ – файл Сервера интеграции на базе Linux.
   - %ProgramFiles(x86)%\<BRAND> Lab\<BRAND> VIISLA\ – файл Сервера интеграции на базе Windows.
2. Настройте значение параметра `OpenStackMaxSvmCountToReturn` в секции `HypervisorSpecificSettings:Openstack`:
   - Если вы хотите ограничить размер списка доступных SVM, который Сервер интеграции передает Легким агентам, в качестве значения укажите количество SVM, информация о которых должна содержаться в списке.

- Если вы хотите, чтобы Сервер интеграции передавал Легким агентам полный список доступных для подключения SVM, в качестве значения укажите `0`.

3. Сохраните файл appsettings.json.
4. Перезапустите Сервер интеграции.

Настройка использования тегов для подключения

Если вы хотите регулировать подключение Легких агентов к SVM с помощью тегов для подключения, вам нужно выполнить следующие действия:

- В параметрах Легкого агента (см. раздел "Назначение тегов для подключения Легким агентам" на стр. 144): включить использование тегов Легким агентом и назначить тег, который Легкий агент будет использовать для подключения.
- В параметрах Сервера защиты (см. раздел "Настройка использования тегов для подключения на SVM" на стр. 142): включить использование тегов на SVM и указать теги, с которыми разрешено подключаться к этой SVM. К SVM будут подключаться только Легкие агенты, которым назначены указанные теги. Если Легкому агенту назначен другой тег или тег не назначен, Легкий агент не сможет подключиться к этой SVM.

В этом разделе

Настройка использования тегов для подключения на SVM

Вы можете настраивать использование на SVM тегов для подключения в политике для Сервера защиты с помощью Web Console или с помощью Консоли администрирования.

Как настроить использование тегов на SVM в Kaspersky Security Center Web Console

► *Чтобы настроить использование тегов на SVM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.
4. В открывшемся окне свойств политики выберите вкладку **Параметры приложения** и перейдите в раздел **Теги для подключения**.
5. В правой части окна настройте параметры:

- **Разрешить подключение Легких агентов с указанными тегами**

  Разрешать подключение к SVM только Легким агентам, которым назначены теги, указанные в поле ниже.

  Если флажок установлен, к SVM могут подключаться только Легкие агенты с указанными тегами.

  Если флажок снят, к SVM могут подключаться только Легкие агенты, которым не назначены теги.

  Флажок по умолчанию снят.

- **Список тегов**

  К SVM могут подключаться только Легкие агенты, которым назначены теги, указанные в этом поле.

  Вы можете указать один или несколько тегов через точку с запятой.

К SVM с Сервером защиты, находящимся под управлением этой политики, будут подключаться только Легкие агенты, которым назначены указанные теги.

6. Нажмите на кнопку **Применить**.

Как настроить использование тегов на SVM в Консоли администрирования Kaspersky Security Center

► *Чтобы настроить использование тегов на SVM:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
4. В окне свойств политики в списке слева выберите раздел **Теги для подключения**.
5. В правой части окна настройте параметры:

   - **Разрешить подключение Легких агентов с указанными тегами**

     Разрешать подключение к SVM только Легким агентам, которым назначены теги, указанные в поле ниже.

     Если флажок установлен, к SVM могут подключаться только Легкие агенты с указанными тегами.

     Если флажок снят, к SVM могут подключаться только Легкие агенты, которым не назначены теги.

     Флажок по умолчанию снят.

   - **Список тегов**

     К SVM могут подключаться только Легкие агенты, которым назначены теги, указанные в этом поле.

     Вы можете указать один или несколько тегов через точку с запятой.

   К SVM с Сервером защиты, находящимся под управлением этой политики, будут подключаться только Легкие агенты, которым назначены указанные теги.

6. Нажмите на кнопку **Применить**.

Назначение тегов для подключения Легким агентам

Вы можете настраивать параметры использования тегов Легкими агентами в политике для Легкого агента (в политике приложения, которое работает в режиме Легкого агента). Параметры использования тегов для Легкого агента для Windows также доступны в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows.

Чтобы присвоить Легкому агенту тег для подключения к SVM, установите флажок **Использовать тег для подключения** и введите тег для подключения в поле **Тег**.

В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`.

Подробнее о настройке параметров приложений, работающих в режиме Легкого агента, см. в справке соответствующего приложения: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Легкие агенты, которым назначен тег, могут подключаться только к SVM, для которых разрешено (см. раздел "Настройка использования тегов для подключения на SVM" на стр. 142) подключение Легких агентов с этим тегом.

Защита соединения между Легким агентом и Сервером защиты

Вы можете настроить защиту соединения между Легкими агентами и Серверами защиты с помощью шифрования. Для этого вам требуется включить шифрование канала передачи данных между Легким агентом и Сервером защиты в параметрах Сервера защиты на SVM (см. раздел "Настройка защиты соединения на стороне Сервера защиты" на стр. 145) и в параметрах Легкого агента (см. раздел "Настройка защиты соединения на стороне Легкого агента" на стр. 147).

Легкий агент, для которого включена защита соединения, может подключаться только к тем SVM, на которых включено шифрование канала передачи данных между Легким агентом и Сервером защиты. Легкий агент, для которого выключена защита соединения, может подключаться только к тем SVM, на которых шифрование канала выключено или разрешено незащищенное соединение между Сервером защиты и Легким агентом.

Защита соединения с помощью шифрования может снижать производительность работы решения Kaspersky Security.

kaspersky

В этом разделе

Настройка защиты соединения на стороне Сервера защиты

Вы можете настраивать защиту соединения на стороне Сервера защиты в политике для Сервера защиты с помощью Web Console или с помощью Консоли администрирования.

Как настроить защиту соединения на стороне Сервера защиты в Kaspersky Security Center Web Console

► *Чтобы настроить защиту соединения на стороне Сервера защиты:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.
4. В открывшемся окне свойств политики выберите вкладку **Параметры приложения** и перейдите в раздел **Защита соединения**.
5. В правой части окна настройте параметры:

   - **Шифровать канал передачи данных между Легким агентом и Сервером защиты**

     Защитить соединение между Легкими агентами и Серверами защиты с помощью шифрования.

     Если флажок установлен, между Легким агентом и Сервером защиты, находящимся под управлением политики, устанавливается защищенное соединение после подключения Легкого агента к SVM с этим Сервером защиты. Легкий агент может подключиться к SVM, на которой включена защита соединения, только если на Легком агенте также включена защита соединения или на SVM разрешено незащищенное соединение.

     Если флажок снят, между Легким агентом и Сервером защиты устанавливается незащищенное соединение после подключения Легкого агента к SVM с этим Сервером защиты.

     По умолчанию флажок снят.

   - **Разрешить незащищенное соединение, если не удалось установить защищенное соединение**

     Разрешать незащищенное соединение между Легкими агентами и Серверами защиты.

Если флажок установлен, между Легкими агентами и Серверами защиты, находящимися под управлением политики, может быть установлено незащищенное соединение, если не удалось установить защищенное соединение.

Если флажок снят, между Легкими агентами и Серверами защиты, находящимися под управлением политики, может быть установлено только защищенное соединение. Легкий агент не сможет подключиться к SVM, если не удалось установить защищенное соединение с Сервером защиты на этой SVM.

По умолчанию флажок снят.

К SVM с Серверами защиты, находящимися под управлением этой политики, будут подключаться только Легкие агенты, для которых настроено защищенное соединение (см. раздел "Настройка защиты соединения на стороне Легкого агента" на стр. 147).

6. Нажмите на кнопку **Сохранить**.

Как настроить защиту соединения на стороне Сервера защиты в Консоли администрирования Kaspersky Security Center

► *Чтобы настроить защиту соединения на стороне Сервера защиты:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
4. В окне свойств политики в списке слева выберите раздел **Защита соединения**.
5. В правой части окна настройте параметры:
   - **Шифровать канал передачи данных между Легким агентом и Сервером защиты**

     Защитить соединение между Легкими агентами и Серверами защиты с помощью шифрования.

     Если флажок установлен, между Легким агентом и Сервером защиты, находящимся под управлением политики, устанавливается защищенное соединение после подключения Легкого агента к SVM с этим Сервером защиты. Легкий агент может подключиться к SVM, на которой включена защита соединения, только если на Легком агенте также включена защита соединения или на SVM разрешено незащищенное соединение.

     Если флажок снят, между Легким агентом и Сервером защиты устанавливается незащищенное соединение после подключения Легкого агента к SVM с этим Сервером защиты.

     По умолчанию флажок снят.

   - **Разрешить незащищенное соединение, если не удалось установить защищенное соединение**

     Разрешать незащищенное соединение между Легкими агентами и Серверами защиты.

     Если флажок установлен, между Легкими агентами и Серверами защиты, находящимися под управлением политики, может быть установлено незащищенное соединение, если не удалось установить защищенное соединение.

Если флажок снят, между Легкими агентами и Серверами защиты, находящимися под управлением политики, может быть установлено только защищенное соединение. Легкий агент не сможет подключиться к SVM, если не удалось установить защищенное соединение с Сервером защиты на этой SVM.

По умолчанию флажок снят.

К SVM с Сервером защиты, находящимся под управлением этой политики, будут подключаться только Легкие агенты, для которых настроено защищенное соединение (см. раздел "Настройка защиты соединения на стороне Легкого агента" на стр. 147).

6. Нажмите на кнопку **Применить**.

Настройка защиты соединения на стороне Легкого агента

Вы можете настраивать параметры защиты соединения на стороне Легкого агента в политике для Легкого агента (в политике приложения, которое работает в режиме Легкого агента). Параметры защиты соединения для Легкого агента для Windows также доступны в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows.

По умолчанию защита соединения между Легкими агентами и Сервером защиты выключена. Чтобы включить защиту соединения, установите флажок **Шифровать канал передачи данных между Легким агентом и Сервером защиты**.

Если флажок установлен, между Легким агентом, находящимся под управлением политики, и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается защищенное соединение. Легкий агент, для которого включена защита соединения, может подключиться только к SVM, на которой также включена защита соединения или разрешено незащищенное соединение с Сервером защиты.

Если флажок снят, между Легким агентом и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается незащищенное соединение.

Подробнее о настройке параметров приложений, работающих в режиме Легкого агента, см. в справке соответствующего приложения: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Настройка алгоритма выбора SVM

Вы можете указать, какой алгоритм выбора SVM (см. раздел "Об алгоритмах выбора SVM" на стр. 16) должны использовать Легкие агенты, и настроить параметры применения расширенного алгоритма выбора SVM в политике для Легкого агента (в политике приложения, которое работает в режиме Легкого агента). Для Легкого агента для Windows вы также можете выбрать алгоритм в локальном интерфейсе приложения Kaspersky Endpoint Security для Windows.

Вы можете выбрать один из следующих вариантов:

- **Использовать стандартный алгоритм выбора SVM**

  Если выбран этот вариант, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является локальной для Легкого агента.

  Локальность SVM относительно Легкого агента определяется в зависимости от вида виртуальной инфраструктуры:

- В виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer локальной для Легкого агента считается SVM, которая развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом.
- В виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС локальность SVM определяется в соответствии с параметром `StandardAlgorithmSvmLocality` в секции `HypervisorSpecificSettings:Openstack` в конфигурационном файле Сервера интеграции appsettings.json. В зависимости от версии Сервера интеграции файл расположен по следующему пути:
  - /var/opt/<KL_LOWCASE>/viis/common/ – файл Сервера интеграции на базе Linux.
  - %ProgramFiles(x86)%\<BRAND> Lab\<BRAND> VIISLA\ – файл Сервера интеграции на базе Windows.

  Если используется значение по умолчанию, локальной для Легкого агента считается SVM, которая находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом.

Если нет доступных для подключения локальных SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре.

Локальность SVM относительно Легкого агента не определяется, если для Сервера защиты на этой SVM включен режим защиты больших инфраструктур (см. раздел "Защита больших инфраструктур" на стр. 153). В этом случае рекомендуется использовать расширенный алгоритм выбора SVM и выбрать Сервер интеграции в качестве способа обнаружения SVM (см. раздел "Об обнаружении SVM" на стр. 15).

Этот вариант выбран по умолчанию.

- **Использовать расширенный алгоритм выбора SVM**

  Если выбран этот вариант, вы можете указать с помощью ползунка **Расположение SVM**, как расположение SVM в виртуальной инфраструктуре будет учитываться при определении локальности SVM относительно Легкого агента. Легкий агент сможет подключаться только к тем SVM, которые являются локальными (см. раздел "Об алгоритмах выбора SVM" на стр. 16).

  Также вы можете указать, что расположение SVM в виртуальной инфраструктуре не должно учитываться при выборе SVM для подключения.

  При выборе SVM Легкие агенты учитывают количество Легких агентов, подключенных к этой SVM, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM.

Если вы выбрали вариант **Использовать расширенный алгоритм выбора SVM** и в качестве способа обнаружения SVM Легкими агентами используется Сервер интеграции, вы можете указать, как учитывается расположение SVM в виртуальной инфраструктуре при выборе SVM для подключения, с помощью ползунка **Расположение SVM**.

Позволяет указать тип расположения SVM в виртуальной инфраструктуре, который учитывается при выборе SVM для подключения:

- **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):
    - SVM развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer).
    - SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС).

  Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
- **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):
    - SVM развернута в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer).
    - SVM развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС).

  Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
- **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):
    - SVM развернута в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux или Numa vServer).
    - SVM расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС).

  Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
- **Игнорировать**. Легкий агент не учитывает при выборе SVM ее расположение.

По умолчанию выбрано значение **Гипервизор**.

Параметр доступен, если выбран вариант **Использовать расширенный алгоритм выбора SVM**.

Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур (см. раздел "Защита больших инфраструктур" на стр. 153), то подключение Легкого агента к этой SVM возможно, только если Легкий агент не учитывает расположение SVM (для параметра **Расположение SVM** установлено значение **Игнорировать**).

Подробнее о настройке параметров приложений, работающих в режиме Легкого агента, см. в справке соответствующего приложения: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

В виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС, если вы выбрали вариант **Использовать стандартный алгоритм выбора SVM**, вы можете указать, как определяется локальность SVM относительно Легкого агента. Для этого нужно выполнить следующие действия:

1. Открыть на редактирование конфигурационный файл Сервера интеграции appsettings.json. В зависимости от версии Сервера интеграции файл расположен по следующему пути:
   - /var/opt/<KL_LOWCASE>/viis/common/ – файл Сервера интеграции на базе Linux.
   - %ProgramFiles(x86)%\<BRAND> Lab\<BRAND> VIISLA\ – файл Сервера интеграции на базе Windows.
2. Настроить значение параметра `StandardAlgorithmSvmLocality` в секции `HypervisorSpecificSettings:Openstack`. Параметр может принимать следующие значения:
   - `ServerGroup` – если установлено это значение, локальной для Легкого агента считается SVM, которая находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом. Это значение используется по умолчанию.
   - `Project` – если установлено это значение, локальной для Легкого агента считается SVM, которая развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом.
   - `AvailabilityZone` – если установлено это значение, локальной для Легкого агента считается SVM, которая расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом.
3. Сохранить файл appsettings.json.
4. Перезапустить Сервер интеграции.

Просмотр списка Легких агентов, подключенных к SVM

Информация о Легких агентах, подключенных к SVM, отображается в окне свойств Сервера защиты на этой SVM.

Вы можете открыть окно свойств Сервера защиты на SVM с помощью Web Console или с помощью Консоли администрирования.

Как посмотреть список Легких агентов, подключенных к SVM, в Kaspersky Security Center Web Console

► *Чтобы открыть список Легких агентов, подключенных к SVM:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужную SVM. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите нужную SVM и нажмите на имя SVM.
4. В открывшемся окне свойств SVM выберите вкладку **Программы**.
5. Нажмите на название **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты** в списке.

   Откроется окно свойств Сервера защиты на этой SVM.

6. Перейдите на вкладку **Параметры приложения**.

В окне отображается таблица, содержащая список Легких агентов, подключенных к SVM.

Как посмотреть список Легких агентов, подключенных к SVM, в Консоли администрирования Kaspersky Security Center

► *Чтобы открыть список Легких агентов, подключенных к SVM:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, в которую входит нужная SVM.
2. В рабочей области выберите вкладку **Устройства**.
3. В списке найдите нужную SVM и откройте окно **Свойства: <Имя SVM>** двойным щелчком мыши.
4. В открывшемся окне свойств SVM в списке слева выберите раздел **Программы**.
5. В правой части окна в списке выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты** и откройте окно свойств Сервера защиты на этой SVM двойным щелчком мыши или с помощью кнопки **Свойства** в нижней части окна.
6. В открывшемся окне в списке слева выберите раздел **Подключенные Легкие агенты**.

В правой части окна отображается таблица, содержащая список Легких агентов, подключенных к SVM. В поле над таблицей отображается время последнего запроса к SVM.

В списке Легких агентов отображается следующая информация:

- **Имя VM** – имя виртуальной машины, на которой установлен Легкий агент.
- **Адрес** – IP-адрес и порт, которые использует Легкий агент для подключения к SVM.
- **Операционная система** – версия операционной системы на виртуальной машине, на которой установлен Легкий агент.
- **Тип ОС** – тип операционной системы на виртуальной машине, на которой установлен Легкий агент: операционная система для серверов или операционная система для рабочих станций.

- **Идентификатор** – идентификатор виртуальной машины, на которой установлен Легкий агент.
- **Путь к VM** – путь в виртуальной инфраструктуре к виртуальной машине, на которой установлен Легкий агент.

Если вы хотите обновить информацию о Легких агентах, подключенных к SVM, нажмите на кнопку **Обновить**.

kaspersky

Защита больших инфраструктур

Если решение используется для защиты большой инфраструктуры (более 50 тысяч защищенных виртуальных машин), взаимодействие компонентов решения с виртуальной инфраструктурой в процессе предоставления информации об SVM Легким агентам может создавать повышенную нагрузку на виртуальную инфраструктуру.

Для оптимизации работы решения в больших инфраструктурах рекомендуется настроить параметры решения следующим образом:

- Включить для Сервера защиты режим защиты больших инфраструктур. Этот режим позволяет снизить нагрузку на виртуальную инфраструктуру.
- Использовать расширенный алгоритм выбора SVM (см. раздел "Об алгоритмах выбора SVM" на стр. 16).
- Выбрать Сервер интеграции в качестве способа обнаружения SVM (см. раздел "Об обнаружении SVM" на стр. 15) Легкими агентами.

Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур, то подключение Легкого агента к этой SVM возможно, только если Легкий агент не учитывает расположение SVM (см. раздел "Настройка алгоритма выбора SVM" на стр. 147).

Вы можете включать или выключать режим защиты больших инфраструктур во время создания или изменения политики для Сервера защиты с помощью Web Console или с помощью Консоли администрирования.

Как включить режим защиты больших инфраструктур в Kaspersky Security Center Web Console

► *Чтобы включить режим защиты больших инфраструктур:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.
4. В открывшемся окне свойств политики выберите вкладку **Параметры приложения** и перейдите в раздел **Параметры защиты больших инфраструктур**.
5. В правой части окна настройте параметр **Включить оптимизацию для защиты больших инфраструктур**.

   Включение / выключение режима защиты больших инфраструктур.

   Режим позволяет оптимизировать работу Сервера защиты для уменьшения нагрузки на виртуальную инфраструктуру.

Если режим включен, рекомендуется использовать расширенный алгоритм выбора SVM.

По умолчанию флажок снят.

6. Нажмите на кнопку **Сохранить**.

Как включить режим защиты больших инфраструктур в Консоли администрирования Kaspersky Security Center

► *Чтобы включить режим защиты больших инфраструктур:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
4. В окне свойств политики в списке слева выберите раздел **Параметры защиты больших инфраструктур**.
5. В правой части окна настройте параметр **Включить оптимизацию для защиты больших инфраструктур**.

   Включение / выключение режима защиты больших инфраструктур.

   Режим позволяет оптимизировать работу Сервера защиты для уменьшения нагрузки на виртуальную инфраструктуру.

   Если режим включен, рекомендуется использовать расширенный алгоритм выбора SVM.

   По умолчанию флажок снят.

6. Нажмите на кнопку **Применить**.

kaspersky

Обновление баз и программных модулей Kaspersky Security

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в решении на территории США.

Обновление баз и программных модулей решения Kaspersky Security обеспечивает актуальность защиты виртуальных машин. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Security. Базы Kaspersky Security содержат антивирусные базы и другие базы данных "Лаборатории Касперского", важные для безопасности защищаемой инфраструктуры. Обновление программных модулей Kaspersky Security позволяет своевременно получать важные обновления компонентов решения Kaspersky Security. Чтобы решение Kaspersky Security своевременно обнаруживало угрозы, вам нужно регулярно обновлять базы и программные модули решения.

Если базы Kaspersky Security давно не обновлялись, информация об этом появляется в Kaspersky Security Center в окне свойств SVM (в разделе **События**, если вы работаете через Консоль администрирования Kaspersky Security Center, на закладке **События**, если вы работаете через Kaspersky Security Center Web Console).

Обновления баз и программных модулей Kaspersky Security могут изменить некоторые параметры Kaspersky Security, например параметры эвристического анализа, повышающие эффективность защиты и проверки.

Для обновления баз и модулей Kaspersky Security требуется действующая лицензия на использование Kaspersky Security.

Обновление баз и программных модулей Kaspersky Security выполняется следующим образом:

1. Kaspersky Security Center загружает в хранилище Сервера администрирования пакет обновлений из источника обновлений для Kaspersky Security Center. *Источник обновлений* – это ресурс, содержащий обновления баз и программных модулей "Лаборатории Касперского". Источником обновлений для Kaspersky Security для виртуальных сред 6.2 Легкий агент является хранилище Сервера администрирования Kaspersky Security Center.

   Для загрузки обновлений в хранилище Сервера администрирования используется задача *Загрузка обновлений в хранилище Сервера администрирования*. Задача создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Если задача загрузки обновлений в хранилище отсутствует в списке задач для Сервера администрирования, вам нужно создать ее. Подробнее см. в справке Kaspersky Security Center.

2. Компонент Сервер защиты загружает пакет обновлений из хранилища Сервера администрирования в папку на SVM. Для загрузки пакетов обновлений на SVM используется задача для Сервера защита типа *Обновление баз*.

   Вы можете использовать задачу, которая создается автоматически после установки MMC-плагина или веб-плагина Сервера защиты в Kaspersky Security Center с названием *Обновление баз и модулей решения*. Задача создается для группы администрирования **Управляемые устройства** и позволяет загружать пакет обновлений на все SVM, которые входят в группу **Управляемые устройства** или в любую вложенную группу администрирования. Задача запускается при каждой загрузке пакета обновлений в хранилище Сервера администрирования Kaspersky Security Center.

   При необходимости вы можете изменить параметры автоматически созданной задачи обновления или удалить ее и создать (см. раздел "Создание задачи Обновление баз" на стр. 158) новую задачу для Сервера защиты *Обновление баз*.

   По умолчанию пакет обновлений содержит обновления баз, необходимых для работы Сервера защиты, Легкого агента для Linux и Легкого агента для Windows. Вы можете настроить параметры загрузки обновлений (см. раздел "Настройка параметров загрузки обновлений на SVM" на стр. 157), а также включить обновления программных модулей компонентов Kaspersky Security.

   > Допускается устанавливать только обновления модулей, прошедшие сертификационные испытания. Включение автоматического обновления программные модули компонентов Kaspersky Security приводит к выходу решения из безопасного состояния.

   Чтобы Сервер защиты успешно загрузил пакет обновлений из хранилища Сервера администрирования, SVM, на которой установлен Сервер защиты, должна иметь доступ к Серверу администрирования Kaspersky Security Center.

   > Если базы программы давно не обновлялись, то пакет обновлений может иметь значительный размер. Загрузка такого пакета обновлений может создать дополнительный сетевой трафик (до нескольких десятков мегабайт).

3. После загрузки пакета обновлений баз обновления устанавливаются из папки, расположенной на SVM:

   - Сервер защиты автоматически устанавливает на SVM обновления баз, необходимых для работы Сервера защиты.
   - Легкий агент проверяет наличие пакета обновлений в папке на той SVM, к которой он подключен.

     > Чтобы получать обновления баз, Легкий агент должен взаимодействовать с Сервером защиты по протоколу HTTP.

     При наличии пакета обновлений Легкий агент устанавливает на защищенной виртуальной машине обновления баз, необходимых для работы Легкого агента. Обновление баз для Легкого агента выполняется с помощью предустановленной локальной задачи *Обновление*. Эта задача создается автоматически в приложениях, работающих в режиме Легкого агента, и используется для обновления баз и программных модулей Легкого агента. В этой задаче в качестве источника обновлений указана папка на SVM. Задача запускается автоматически в следующих случаях:

     - при подключении Легкого агента к SVM, если на Легком агенте базы Kaspersky Security отсутствуют или не соответствуют базам, установленным на Сервере защиты;

- через 120 минут после предыдущего успешного обновления или через 20 минут, если обновление завершилось с ошибкой.

Вы также можете запускать задачу *Обновление* вручную. См. подробнее в справке приложения, работающего в режиме Легкого агента: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Для обеспечения актуальности защиты временных виртуальных машин рекомендуется регулярно обновлять базы и программные модули Легкого агента на шаблоне виртуальных машин, из которого созданы временные защищенные виртуальные машины.

Если при установке Легкого агента на шаблон виртуальных машин (см. раздел "Установка Легкого агента на шаблон для временных виртуальных машин" на стр. 91) вы включили поддержку VDI, то обновления, требующие перезагрузки защищенной виртуальной машины, не устанавливаются на временных виртуальных машинах. При получении обновлений, требующих перезагрузки защищенной виртуальной машины, Легкий агент, установленный на временной виртуальной машине, отправляет в Kaspersky Security Center сообщение о необходимости обновления шаблона защищенных виртуальных машин.

В этом разделе

Настройка параметров загрузки обновлений на SVM

Вы можете выбрать версии Легких агентов, для которых Сервер защиты будет получать обновления. По умолчанию пакет обновлений содержит обновления баз, необходимых для работы Сервера защиты, Легкого агента для Linux и Легкого агента для Windows.

Подключиться к SVM могут только те Легкие агенты, для которых на эту SVM загружаются обновления баз.

Вы можете настраивать параметры загрузки обновлений с помощью Web Console или с помощью Консоли администрирования в политике для Сервера защиты.

Как настроить параметры загрузки обновлений с помощью Web Console

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.
4. В открывшемся окне свойств политики выберите вкладку **Параметры приложения** и перейдите в раздел **Параметры обновления**.
5. В правой части окна отображается список версий Легких агентов, для которых Сервер защиты будет получать обновления. Если требуется, настройте список с помощью флажков. Должна быть выбрана хотя бы одна версия.

   Список содержит поддерживаемые версии Легкий агентов. Если в списке отсутствует версия Легкого агента, для которой требуется получать обновления, нажмите на кнопку **Обновить**.

   Включение автоматического обновления модулей решения приводит к выходу решения Kaspersky Security из безопасного состояния. Допускается устанавливать только обновления программных модулей, прошедшие сертификационные испытания.

6. Нажмите на кнопку **Сохранить**.

Как настроить параметры загрузки обновлений с помощью Консоли администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
4. В окне свойств политики в списке слева выберите раздел **Параметры обновления**.
5. В правой части окна отображается список версий Легких агентов, для которых Сервер защиты будет получать обновления. Если требуется, настройте список с помощью флажков. Должна быть выбрана хотя бы одна версия.

   Список содержит поддерживаемые версии Легкий агентов. Если в списке отсутствует версия Легкого агента, для которой требуется получать обновления, нажмите на кнопку **Обновить**.

   Включение автоматического обновления модулей решения приводит к выходу решения Kaspersky Security из безопасного состояния. Допускается устанавливать только обновления программных модулей, прошедшие сертификационные испытания.

6. Нажмите на кнопку **Применить**.

Создание задачи Обновление баз

Вы можете создавать задачи обновления баз на Сервере защиты с помощью Web Console или с помощью Консоли администрирования.

Как создать задачу Обновление баз в Kaspersky Security Center Web Console

► *Чтобы создать задачу Обновление баз:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. На первом шаге мастера выполните следующие действия:

   a. В раскрывающемся списке **Программа** выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты**.

   b. В раскрывающемся списке **Тип задачи** выберите тип задачи: **Обновление баз**.

   c. В поле **Название задачи** введите название новой задачи.

   d. В блоке **Выбор устройств, которым будет назначена задача** выберите способ определения области действия задачи. Область действия задачи – это набор SVM, на которых будет выполняться задача.

   - Выберите вариант **Назначить задачу группе администрирования**, если задача должна выполняться на всех SVM, входящих в определенную группу администрирования.
   - Выберите вариант **Задать адреса устройств вручную или импортировать из списка**, если задача должна выполняться на указанных SVM.
   - Выберите вариант **Назначить задачу выборке устройств**, если задача должна выполняться на SVM, входящих в выборку устройств по предопределенному критерию. О создании выборки устройств см. в справке Kaspersky Security Center.

   Перейдите к следующему шагу мастера.

4. В зависимости от выбранного способа определения области действия задачи выполните одно из следующих действий:

   - В дереве групп администрирования установите флажки рядом с нужными группами администрирования.
   - В списке устройств установите флажки рядом с нужными SVM. Если нужные SVM отсутствуют в списке, вы можете добавить их следующими способами:
     - С помощью кнопки **Добавить устройства**. Вы можете добавить устройства по имени или IP-адресу, добавить устройства из указанного IP-диапазона или выбрать устройства из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.
     - С помощью кнопки **Импортировать устройства из файла**. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

     Если вы импортируете список адресов SVM из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

- В списке выберите название выборки, содержащей нужные SVM.

Перейдите к следующему шагу мастера.

5. Установите флажок **Открыть окно свойств задачи после ее создания**, чтобы настроить расписание запуска задачи, и нажмите на кнопку **Готово**, чтобы завершить работу мастера.
6. В открывшемся окне свойств новой задачи перейдите на вкладку **Расписание** и в раскрывающемся списке **Запуск по расписанию** выберите **При загрузке обновлений в хранилище**.

   Если требуется, настройте остальные параметры расписания запуска задачи. Подробнее о расписании задач см. в справке Kaspersky Security Center.
7. Нажмите на кнопку **Сохранить** в окне свойств задачи.

Как создать задачу Обновление баз в Консоли администрирования Kaspersky Security Center

► *Чтобы создать задачу Обновление баз:*

1. В Консоли администрирования Kaspersky Security Center выполните одно из следующих действий:
   - Если вы хотите создать задачу, которая будет выполняться на SVM, входящих в выбранную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи** и нажмите на кнопку **Новая задача**.

     Запустится мастер создания задачи для устройств выбранной группы администрирования.
   - Если вы хотите создать задачу, которая будет выполняться на одной или нескольких SVM (задачу для набора устройств), в дереве консоли выберите папку **Задачи** и нажмите на кнопку **Новая задача** в рабочей области.

     Запустится мастер создания задачи для набора устройств.
2. На первом шаге мастера выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты** и тип задачи: **Обновление баз**.

   Перейдите к следующему шагу мастера.
3. Если вы создаете задачу для набора устройств, мастер предложит определить область действия задачи. Область действия задачи – это набор SVM, на которых будет выполняться задача.
   a. Укажите способ определения области действия задачи: выбрать SVM из списка устройств, обнаруженных Сервером администрирования, задать адреса SVM вручную, импортировать список SVM из файла или указать ранее настроенную выборку устройств (см. подробнее в справке Kaspersky Security Center).
   b. В зависимости от указанного вами способа определения области действия в открывшемся окне выполните одно из следующих действий:
      - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от названия устройства.
      - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM вручную.
      - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM.
      - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.

   Перейдите к следующему шагу мастера.

4. В раскрывающемся списке **Запуск по расписанию** выберите **При загрузке обновлений в хранилище**.
5. Если требуется, настройте остальные параметры расписания запуска задачи:
   - **Запускать пропущенные задачи**

     Если требуется, чтобы решение запускало пропущенную задачу сразу после появления SVM в сети, установите этот флажок.

     Если флажок снят, для режима **Вручную** запуск задачи производится только на видимых в сети SVM.

   - **Использовать автоматическое определение случайного интервала между запусками задачи**

     По умолчанию запуск задачи на SVM распределяется в течение определенного периода времени. Этот период рассчитывается автоматически, в зависимости от количества SVM, на которые распространяется задача:

     - 0–200 SVM – запуск задачи не распределяется;
     - 200–500 SVM – запуск задачи распределяется в течение 5 минут;
     - 500–1000 SVM – запуск задачи распределяется в течение 10 минут;
     - 1000–2000 SVM – запуск задачи распределяется в течение 15 минут;
     - 2000–5000 SVM – запуск задачи распределяется в течение 20 минут;
     - 5000–10000 SVM – запуск задачи распределяется в течение 30 минут;
     - 10000–20000 SVM – запуск задачи распределяется в течение 1 часа;
     - 20000–50000 SVM – запуск задачи распределяется в течение 2 часов;
     - более 50000 SVM – запуск задачи распределяется в течение 3 часов.

     Если не требуется распределять запуск задачи в течение автоматически рассчитываемого периода, снимите флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

     По умолчанию флажок установлен.

   - **Использовать случайную задержку запуска задачи в интервале (мин.)**

     Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента запуска вручную, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае после запуска вручную задача запустится в случайное время в рамках указанного периода.

     Флажок доступен для изменения, если не установлен флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

   Подробнее о параметрах расписания запуска задачи см. в справке Kaspersky Security Center.

   Перейдите к следующему шагу мастера.
6. В поле **Имя** введите название новой задачи и перейдите к следующему шагу мастера создания задачи.
7. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.
8. Завершите работу мастера.

Задача будет запускаться каждый раз при загрузке пакета обновлений в хранилище Сервера администрирования. Также вы можете в любой момент запустить задачу (см. раздел "Запуск и остановка задач для Сервера защиты" на стр. 125) обновления баз на Сервере защиты вручную.

Откат последнего обновления баз Kaspersky Security

После первого обновления баз Kaspersky Security становится доступна функция отката к предыдущему набору баз.

Каждый раз, когда запускается обновление баз на Сервере защиты, Kaspersky Security создает резервную копию используемых баз и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущего набора баз при необходимости. Возможность отката последнего обновления полезна, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Security блокирует безопасное приложение.

Откат последнего обновления баз и программных модулей Kaspersky Security выполняется следующим образом:

1. Компонент Сервер защиты выполняет откат последнего обновления баз и программных модулей Kaspersky Security на SVM. Вы можете откатить последнее обновление баз и модулей на одной или на нескольких SVM. Откат последнего обновления баз на SVM выполняется с помощью задачи для Сервера защиты *Откат обновления баз*. Задача запускается из Kaspersky Security Center и выполняется на SVM.

   В результате отката последнего обновления баз на SVM Сервер защиты также откатывает обновления баз для Легких агентов, которые размещаются в папке на SVM. Сервер защиты отправляет Легким агентам событие о том, что требуется выполнить обновление.

2. После того, как на SVM выполнен откат обновления баз, на подключенных к этой SVM Легких агентах автоматически запускается специальная локальная задача Kaspersky Endpoint Security для Linux *Обновление*. В этой задаче в качестве источника обновлений указана папка на SVM.

   В результате выполнения задачи обновления Легкий агент переходит к использованию предыдущего набора баз Kaspersky Security.

Создание задачи Откат обновления баз

Вы можете создавать задачи Откат обновления баз с помощью Web Console или с помощью Консоли администрирования.

Как создать задачу Откат обновления баз в Kaspersky Security Center Web Console

► *Чтобы создать задачу Откат обновления баз:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. На первом шаге мастера выполните следующие действия:

a. В раскрывающемся списке **Программа** выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты**.

b. В раскрывающемся списке **Тип задачи** выберите тип задачи: **Откат обновления баз**.

c. В поле **Название задачи** введите название новой задачи.

d. В блоке **Выбор устройств, которым будет назначена задача** выберите способ определения области действия задачи. Область действия задачи – это набор SVM, на которых будет выполняться задача.

- Выберите вариант **Назначить задачу группе администрирования**, если задача должна выполняться на всех SVM, входящих в определенную группу администрирования.
- Выберите вариант **Задать адреса устройств вручную или импортировать из списка**, если задача должна выполняться на указанных SVM.
- Выберите вариант **Назначить задачу выборке устройств**, если задача должна выполняться на SVM, входящих в выборку устройств по предопределенному критерию. О создании выборки устройств см. в справке Kaspersky Security Center.

Перейдите к следующему шагу мастера.

4. В зависимости от выбранного способа определения области действия задачи выполните одно из следующих действий:

- В дереве групп администрирования установите флажки рядом с нужными группами администрирования.
- В списке устройств установите флажки рядом с нужными SVM. Если нужные SVM отсутствуют в списке, вы можете добавить их следующими способами:
  - С помощью кнопки **Добавить устройства**. Вы можете добавить устройства по имени или IP-адресу, добавить устройства из указанного IP-диапазона или выбрать устройства из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.
  - С помощью кнопки **Импортировать устройства из файла**. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

> Если вы импортируете список адресов SVM из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

- В списке выберите название выборки, содержащей нужные SVM.

Перейдите к следующему шагу мастера.

5. Установите флажок **Открыть окно свойств задачи после ее создания**, чтобы настроить расписание запуска задачи, и нажмите на кнопку **Готово**, чтобы завершить работу мастера.

6. В открывшемся окне свойств новой задачи перейдите на вкладку **Расписание** и в раскрывающемся списке **Запуск по расписанию** выберите **Вручную**.

   Если требуется, настройте остальные параметры расписания запуска задачи. Подробнее о расписании задач см. в справке Kaspersky Security Center.

7. Нажмите на кнопку **Сохранить** в окне свойств задачи.

Как создать задачу Откат обновления баз в Консоли администрирования Kaspersky Security Center

► *Чтобы создать задачу Откат обновления баз:*

1. В Консоли администрирования Kaspersky Security Center выполните одно из следующих действий:
   - Если вы хотите создать задачу, которая будет выполняться на SVM, входящих в выбранную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи** и нажмите на кнопку **Новая задача**.

     Запустится мастер создания задачи для устройств выбранной группы администрирования.
   - Если вы хотите создать задачу, которая будет выполняться на одной или нескольких SVM (задачу для набора устройств), в дереве консоли выберите папку **Задачи** и нажмите на кнопку **Новая задача** в рабочей области.

     Запустится мастер создания задачи для набора устройств.
2. На первом шаге мастера выберите **Kaspersky Security для виртуальных сред 6.2 Легкий агент – Сервер защиты** и тип задачи: **Откат обновления баз**.

   Перейдите к следующему шагу мастера.
3. Если вы создаете задачу для набора устройств, мастер предложит определить область действия задачи. Область действия задачи – это набор SVM, на которых будет выполняться задача.
   a. Укажите способ определения области действия задачи: выбрать SVM из списка устройств, обнаруженных Сервером администрирования, задать адреса SVM вручную, импортировать список SVM из файла или указать ранее настроенную выборку устройств (см. подробнее в справке Kaspersky Security Center).
   b. В зависимости от указанного вами способа определения области действия в открывшемся окне выполните одно из следующих действий:
      - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от названия устройства.
      - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM вручную.
      - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов SVM.
      - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.

   Перейдите к следующему шагу мастера.
4. В раскрывающемся списке **Запуск по расписанию** выберите **Вручную**.
5. Если требуется, настройте остальные параметры расписания запуска задачи:
   - **Запускать пропущенные задачи**

     Если требуется, чтобы решение запускало пропущенную задачу сразу после появления SVM в сети, установите этот флажок.

     Если флажок снят, для режима **Вручную** запуск задачи производится только на видимых в сети SVM.
   - **Использовать автоматическое определение случайного интервала между запусками задачи**

     По умолчанию запуск задачи на SVM распределяется в течение определенного периода времени. Этот период рассчитывается автоматически, в зависимости от

количества SVM, на которые распространяется задача:

- 0–200 SVM – запуск задачи не распределяется;
- 200–500 SVM – запуск задачи распределяется в течение 5 минут;
- 500–1000 SVM – запуск задачи распределяется в течение 10 минут;
- 1000–2000 SVM – запуск задачи распределяется в течение 15 минут;
- 2000–5000 SVM – запуск задачи распределяется в течение 20 минут;
- 5000–10000 SVM – запуск задачи распределяется в течение 30 минут;
- 10000–20000 SVM – запуск задачи распределяется в течение 1 часа;
- 20000–50000 SVM – запуск задачи распределяется в течение 2 часов;
- более 50000 SVM – запуск задачи распределяется в течение 3 часов.

Если не требуется распределять запуск задачи в течение автоматически рассчитываемого периода, снимите флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию флажок установлен.

- **Использовать случайную задержку запуска задачи в интервале (мин.)**

  Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента запуска вручную, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае после запуска вручную задача запустится в случайное время в рамках указанного периода.

  Флажок доступен для изменения, если не установлен флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

Подробнее о параметрах расписания запуска задачи см. в справке Kaspersky Security Center.

Перейдите к следующему шагу мастера.

6. В поле **Имя** введите название новой задачи и перейдите к следующему шагу мастера создания задачи.
7. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.
8. Завершите работу мастера.

Вы можете в любой момент запустить задачу (см. раздел "Запуск и остановка задач для Сервера защиты" на стр. 125) отката обновления баз вручную.

kaspersky

Использование Kaspersky Security Network

Функциональность KSN может быть недоступна в решении на территории США.

Чтобы повысить эффективность защиты виртуальных машин, компоненты решения Kaspersky Security могут использовать данные, полученные от пользователей приложений "Лаборатории Касперского" во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции решения Kaspersky Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Kaspersky Security поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network* (KSN) – это решение, которое позволяет получать информацию от "Лаборатории Касперского", а также отправлять в "Лабораторию Касперского" данные об объектах, обнаруженных на устройствах пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.
- *Kaspersky Private Security Network* (KPSN) – это решение, которое позволяет получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского". KPSN разработан для корпоративных клиентов, не имеющих возможности использовать Kaspersky Security Network, например, по следующим причинам:
  - отсутствие подключения локальных рабочих мест к интернету;
  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Использование инфраструктурного решения Kaspersky Security Network приводит к выходу решения Kaspersky Security из безопасного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN.

Если вы используете Kaspersky Security Network, компоненты решения Kaspersky Security получают от служб KSN сведения о категории и репутации проверяемых файлов, а также сведения о репутации проверяемых веб-адресов.

Использование Kaspersky Security Network является добровольным. Вы можете начать или прекратить использование KSN в любой момент.

Параметры использования KSN в работе компонентов решения Kaspersky Security задаются отдельно для каждого компонента. О настройке параметров KSN для Легких агентов см. в справках приложений, которые используются в режиме Легкого агента: Kaspersky Endpoint Security для

Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Рекомендуется задавать одинаковые параметры использования KSN для Сервера защиты и Легкого агента, который взаимодействует с этим Сервером защиты.

Использование KSN в работе Сервера защиты

Включение и выключение использования KSN выполняется в свойствах политики для Сервера защиты (см. раздел "Настройка использования KSN в работе Сервера защиты" на стр. 169).

Если вы включили использование Kaspersky Security Network, по умолчанию Сервер защиты использует в своей работе KSN в расширенном режиме. Режим KSN влияет на объем данных, которые передаются в "Лабораторию Касперского" при использовании KSN (см. раздел "О предоставлении данных при использовании KSN в работе Сервера защиты" на стр. 168).

Взаимодействие Сервера защиты с инфраструктурой KSN обеспечивает служба прокси-сервера KSN. Для использования KSN в работе Kaspersky Security служба прокси-сервера KSN должна быть включена в Kaspersky Security Center. Подробнее о службе прокси-сервера KSN см. в справке Kaspersky Security Center.

Если служба прокси-сервера KSN выключена в Kaspersky Security Center, обмен данными между Сервером защиты и KSN не производится. Если при этом использование KSN включено в политике для Сервера защиты, возможно снижение производительности работы Kaspersky Security. Рекомендуется выключить использование KSN в политике для Сервера защиты, если служба прокси-сервера KSN выключена в Kaspersky Security Center.

Инфраструктурное решение KSN, которое использует в своей работе Сервер защиты (KSN или KPSN), определяется в свойствах Сервера администрирования Kaspersky Security Center (в Консоли администрирования в разделе **Прокси-сервер KSN** или в Web Console в разделе **Параметры прокси-сервера KSN**). В этом разделе вы также можете настроить параметры KPSN. См. подробнее в справке Kaspersky Security Center.

В этом разделе

kaspersky

О предоставлении данных при использовании KSN в работе Сервера защиты

Информацию о предоставлении данных при использовании KSN Легкими агентами см. в справках приложений, которые используются в режиме Легкого агента: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Если вы используете KSN в стандартном режиме, вы соглашаетесь автоматически передавать в "Лабораторию Касперского" следующие данные:

- Информацию, необходимую для проверки файлов: имя и идентификатор обнаруженной угрозы согласно классификации "Лаборатории Касперского", хеш проверяемого объекта и тип хеш-функции, идентификатор используемых антивирусных баз.
- Информацию, необходимую для получения репутации веб-адресов: проверяемый веб-адрес, тип протокола соединения, номер используемого порта и веб-адрес, с которого осуществлен переход на проверяемый веб-адрес.
- Общую информацию: тип и полную версию решения Kaspersky Security, информацию о компонентах решения и об обновлении программных модулей решения, информацию об операционной системе, установленной на SVM и защищенных виртуальных машинах.

Если вы используете KSN в расширенном режиме, вы соглашаетесь автоматически передавать в "Лабораторию Касперского" все данные, перечисленные в Положении о Kaspersky Security Network. В том числе в "Лабораторию Касперского" для проверки могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда виртуальной машине или хранящимся в ее операционной системе данным. Расширенный KSN используется по умолчанию. Вы можете выключить использование расширенного KSN в свойствах политики для Сервера защиты.

Текст Положения о Kaspersky Security Network вы можете посмотреть (см. раздел "Просмотр Положения о Kaspersky Security Network" на стр. 168) в свойствах политики для Сервера защиты в разделе **Параметры Kaspersky Security Network**.

Информацию о хранении, защите и уничтожении статистической информации, полученной во время использования KSN и переданной в "Лабораторию Касперского", вы можете получить, ознакомившись с Политикой конфиденциальности на веб-сайте "Лаборатории Касперского" (https://www.kaspersky.ru/products-and-services-privacy-policy).

Если вы не участвуете в Kaspersky Security Network, то данные, перечисленные в Положении о Kaspersky Security Network, не передаются в "Лабораторию Касперского".

Просмотр Положения о Kaspersky Security Network

Вы можете ознакомиться с Положением о Kaspersky Security Network в свойствах политики для Сервера защиты.

Как просмотреть Положение о Kaspersky Security Network в Kaspersky Security Center Web Console

► *Чтобы посмотреть Положение о Kaspersky Security Network:*

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую SVM с Серверами защиты. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.
4. В открывшемся окне свойств политики выберите вкладку **Параметры приложения** и перейдите в раздел **Параметры Kaspersky Security Network**.
5. Перейдите по ссылке **Положение о Kaspersky Security Network**.

Откроется окно с текстом Положения о Kaspersky Security Network.

Как просмотреть Положение о Kaspersky Security Network в Консоли администрирования Kaspersky Security Center

► *Чтобы посмотреть Положение о Kaspersky Security Network:*

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую SVM с Серверами защиты.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
4. В окне свойств политики в списке слева выберите раздел **Параметры Kaspersky Security Network**.
5. В правой части перейдите по ссылке **Положение о Kaspersky Security Network**.

Откроется окно с текстом Положения о Kaspersky Security Network.

Настройка использования KSN в работе Сервера защиты

Службы KSN используются в работе Сервера защиты, если использование KSN включено в активной политике для Сервера защиты. Если политика, в которой использование KSN включено, не активна, KSN не используется в работе Сервера защиты.

Если вы хотите использовать KSN в работе Сервера защиты, убедитесь в том, что параметры KSN настроены в свойствах Сервера администрирования Kaspersky Security Center (в Консоли администрирования в разделе **Прокси-сервер KSN**, в Web Console в разделе **Параметры прокси-сервера KSN**). В свойствах Сервера администрирования определяется тип инфраструктуры KSN (KSN или KPSN), параметры прокси-сервера KSN и параметры KPSN. См. подробнее в справке Kaspersky Security Center.

Вы можете настроить параметры использования KSN в работе Сервера защиты с помощью Kaspersky Security Center Web Console или с помощью Консоли администрирования Kaspersky Security Center.

Как настроить использование KSN в Kaspersky Security Center Web Console

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

   Откроется список политик.

2. Выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите в открывшемся окне группу администрирования.

   В списке отобразятся только политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.
4. В открывшемся окне свойств политики выберите вкладку **Параметры приложения** и перейдите в раздел **Параметры Kaspersky Security Network**.
5. Если вы хотите включить использование KSN, в правой части окна выполните следующие действия:
   a. Установите флажок **Использовать KSN**.
   b. В открывшемся окне ознакомьтесь с Положением о Kaspersky Security Network.
   c. Если вы согласны со всеми пунктами Положения, выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network** и нажмите на кнопку **OK**.
   d. По умолчанию KSN используется в расширенном режиме. Режим KSN влияет на объем данных, которые автоматически передаются в "Лабораторию Касперского" (см. раздел "О предоставлении данных при использовании KSN в работе Сервера защиты" на стр. 168) при использовании KSN. Если вы хотите выключить использование расширенного KSN, снимите флажок **Расширенный режим KSN**.

   Использование инфраструктурного решения Kaspersky Security Network приводит к выходу решения Kaspersky Security из безопасного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN.

6. Если вы хотите выключить использование KSN, снимите флажок **Использовать KSN**.
7. Нажмите на кнопку **Сохранить**.

Как настроить использование KSN в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую SVM с Сервером защиты, параметры которого вы хотите настроить.

2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите политику для Сервера защиты и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
4. В окне свойств политики в списке слева выберите раздел **Параметры Kaspersky Security Network**.
5. Если вы хотите включить использование KSN, в правой части окна выполните следующие действия:
   a. Установите флажок **Использовать KSN**.
   b. В открывшемся окне ознакомьтесь с Положением о Kaspersky Security Network.
   c. Если вы согласны со всеми пунктами Положения, выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network** и нажмите на кнопку **OK**.
   d. По умолчанию KSN используется в расширенном режиме. Режим KSN влияет на объем данных, которые автоматически передаются в "Лабораторию Касперского" (см. раздел "О предоставлении данных при использовании KSN в работе Сервера защиты" на стр. 168) при использовании KSN. Если вы хотите выключить использование расширенного KSN, снимите флажок **Расширенный режим KSN**.

   Использование инфраструктурного решения Kaspersky Security Network приводит к выходу решения Kaspersky Security из безопасного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN.

6. Если вы хотите выключить использование KSN, снимите флажок **Использовать KSN**.
7. Нажмите на кнопку **Применить**.

kaspersky

Отчеты и уведомления

В процессе работы компонентов решения Kaspersky Security возникают различного рода *события*. Они могут иметь информационный характер или нести важную информацию. Например, с помощью события компонент решения может уведомлять об успешно выполненном обновлении баз и программных модулей решения или может фиксировать ошибку в работе компонента, которую требуется устранить.

Список всех событий в работе компонентов решения отображается в Консоли администрирования Kaspersky Security Center и в Kaspersky Security Center Web Console. Вы можете настроить уведомления о событиях. *Уведомление* – это сообщение с информацией о событии, которое произошло на SVM или на защищенной виртуальной машине. С помощью уведомлений вы можете своевременно получать информацию о событиях в работе решения.

На основе событий, происходящих во время работы компонентов решения Kaspersky Security, можно формировать различные отчеты.

С помощью отчетов Kaspersky Security Center вы можете, например, получить сведения о зараженных файлах, изменении параметров защиты, использовании ключей и баз решения. Вы можете формировать и просматривать отчеты Kaspersky Security Center в Консоли администрирования и в Web Console. Подробную информацию о событиях и о работе с отчетами Kaspersky Security Center см. в справке Kaspersky Security Center.

kaspersky

Настройка параметров Сервера интеграции

Вы можете выполнять следующие действия для настройки параметров Сервера интеграции:

- Изменять пароли внутренних учетных записей Сервера интеграции (см. раздел "Изменение паролей учетных записей Сервера интеграции" на стр. 174). Предусмотрены следующие учетные записи:
  - `admin` – учетная запись администратора Сервера интеграции, используется:
    - для подключения к Серверу интеграции в политике для Сервера защиты и в политике для Легкого агента;
    - для подключения консолей управления к Серверу интеграции.

    Пароль учетной записи `admin` задается при установке Сервер интеграции.
  - `svm` – используется для подключения SVM к Серверу интеграции.
  - `agent` – используется для подключения Легких агентов к Серверу интеграции.
  - `multitenancy` – используется для взаимодействия с REST API Сервера интеграции в сценариях мультитенантности.

  Имена учетных записей недоступны для изменения.

- Изменять параметры, которые использует Сервер интеграции для подключения к виртуальной инфраструктуре.

  Сервер интеграции подключается к каждой защищаемой виртуальной инфраструктуре и получает информацию, необходимую для работы решения. В зависимости от вида защищаемой инфраструктуры Сервер интеграции подключается к одному из следующих объектов виртуальной инфраструктуры:
  - к гипервизору;
  - к серверу управления виртуальной инфраструктурой;
  - к микросервису Keystone.

  Если вы использовали Консоль Сервера интеграции для развертывания SVM, Сервер интеграции подключается к виртуальной инфраструктуре с параметрами, которые вы указали в ходе работы мастера управления SVM.

  Если вы использовали Веб-консоль Сервера интеграции для развертывания SVM, Сервер интеграции подключается к виртуальной инфраструктуре с параметрами, которые вы указали в Веб-консоли перед началом развертывания SVM (см. раздел "Подключение к виртуальной инфраструктуре в Веб-консоли Сервера интеграции" на стр. 69).

  Вы можете изменять параметры подключения Сервера интеграции к виртуальной инфраструктуре (кроме адреса инфраструктуры).

  В инфраструктуре VMware vSphere вы также можете включать или выключать использование VMware NSX Manager в работе Kaspersky Security, а также изменять параметры подключения Сервера интеграции к VMware NSX Manager.

- Удалять параметры подключения Сервера интеграции к виртуальной инфраструктуре (см. раздел "Удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре" на стр. 182).

Вы можете настраивать параметры Сервера интеграции в Консоли Сервера интеграции или в Веб-консоли Сервера интеграции.

В этом разделе

Изменение паролей учетных записей Сервера интеграции

Вы можете изменять пароли учетных записей Сервера интеграции в Веб-консоли Сервера интеграции или в Консоли Сервера интеграции.

Как изменить пароли учетных записей Сервера интеграции в Веб-консоли Сервера интеграции

► *Чтобы изменить пароли учетных записей Сервера интеграции:*

1. Откройте Веб-консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Веб-консоль Сервера интеграции" на стр. 64).
2. Перейдите в раздел **Учетные записи Сервера интеграции**.
3. В открывшемся окне выберите имя учетной записи, пароль которой вы хотите изменить.

   Откроется окно **Изменение пароля**. В поле **Имя учетной записи** отображается имя выбранной учетной записи.
4. Укажите новый пароль в полях **Новый пароль** и **Подтверждение пароля**.

   Пароли должны содержать не более 60 символов. Вы можете использовать только символы латинского алфавита (прописные и строчные буквы), цифры, а также следующие специальные символы: `! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~`. В целях безопасности рекомендуется задавать пароли длиной не менее 8 символов и использовать хотя бы три из четырех категорий символов: строчные буквы, прописные буквы, цифры и специальные символы.
5. Нажмите на кнопку **Сохранить** в окне **Изменение пароля**.

Как изменить пароли учетных записей Сервера интеграции в Консоли Сервера интеграции

► *Чтобы изменить пароли учетных записей Сервера интеграции:*

1. Откройте Консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Учетные записи Сервера интеграции**.
3. В таблице справа выберите имя учетной записи, пароль которой вы хотите изменить.
4. По ссылке **Изменить пароль учетной записи**, расположенной над таблицей, откройте окно **Пароль учетной записи** и введите новый пароль в полях **Пароль** и **Подтверждение пароля**.

   Пароли должны содержать не более 60 символов. Вы можете использовать только символы латинского алфавита (прописные и строчные буквы), цифры, а также следующие специальные символы: ! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~. В целях безопасности рекомендуется задавать пароли длиной не менее 8 символов и использовать хотя бы три из четырех категорий символов: строчные буквы, прописные буквы, цифры и специальные символы.

5. Нажмите на кнопку **OK** в окне **Пароль учетной записи**.

Если вы изменили пароль учетной записи для подключения SVM к Серверу интеграции, вам нужно повторно настроить подключение SVM к Серверу интеграции (см. раздел "Настройка параметров подключения SVM к Серверу интеграции" на стр. 136).

Если в политике для Легкого агента настроено подключение Легких агентов к Серверу интеграции и вы изменили пароль учетной записи для подключения Легких агентов, вам нужно повторно настроить подключение Легких агентов к Серверу интеграции (см. раздел "Настройка параметров подключения Легких агентов к Серверу интеграции" на стр. 138).

Изменение параметров подключения к виртуальной инфраструктуре в Веб-консоли Сервера интеграции

1. Откройте Веб-консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Веб-консоль Сервера интеграции" на стр. 64).
2. В рабочей области выберите раздел **Список виртуальных инфраструктур**.

   В открывшемся окне отображается список виртуальных инфраструктур, к которым подключается Сервер интеграции, в виде таблицы. В каждой строке таблицы отображается следующая информация о виртуальной инфраструктуре:

   - **Адрес объекта инфраструктуры**

     Столбец содержит IP-адреса или полные доменные имена (FQDN) объектов виртуальной инфраструктуры, к которым подключается Сервер интеграции, и имена SVM, развернутых на гипервизорах.

     В зависимости от вида виртуальной инфраструктуры в столбце может отображаться:

     - IP-адрес или полное доменное имя (FQDN) сервера управления виртуальной

инфраструктурой;
- IP-адрес или полное доменное имя гипервизора;
- IP-адрес или полное доменное имя микросервиса Keystone;
- имя проекта и домена OpenStack.

- **Тип объекта инфраструктуры**

  Столбец содержит тип объекта виртуальной инфраструктуры, к которому подключается Сервер интеграции.

- **Статус**

  Столбец содержит информацию о статусе подключения Сервера интеграции к виртуальной инфраструктуре, о состоянии объектов инфраструктуры, к которым выполняется подключение, и о состоянии SVM, развернутых в инфраструктуре.

  Если подключение Сервера интеграции к объекту виртуальной инфраструктуры не установлено, в столбце отображается сообщение об ошибке.

- **VMware NSX Manager**

  Для инфраструктуры под управлением VMware vCenter Server: если включено использование VMware NSX Manager в работе Kaspersky Security, столбец содержит IP-адрес в формате IPv4 или полное доменное имя (FQDN) VMware NSX Manager.

С помощью кнопок, расположенных над таблицей, вы можете:

- изменить учетную запись с правами администратора, которую Сервер интеграции использует для подключения к виртуальной инфраструктуре;
- изменить учетную запись с ограниченными правами (см. раздел "Учетные записи для установки и работы решения" на стр. 42) на действия в виртуальной инфраструктуре, которую Сервер интеграции использует во время работы Kaspersky Security: для получения информации о доступных для подключения SVM и распределения Легких агентов между SVM;
- изменить параметры подключения Сервера интеграции к VMware NSX Manager (в виртуальной инфраструктуре на платформе VMware vSphere);
- подтвердить подлинность сертификата или отпечатка открытого ключа, полученных от виртуальной инфраструктуры, в случае, если не удалось установить их подлинность.

Как изменить учетную запись с правами администратора

1. В разделе **Список виртуальных инфраструктур** выберите виртуальную инфраструктуру, для которой вы хотите изменить параметры подключения, нажмите на кнопку **Изменить**, расположенную над таблицей. и выберите пункт **Параметры учетной записи администратора**.
2. В открывшемся окне укажите параметры учетной записи:

   - **Домен OpenStack**

     Имя домена OpenStack, к которому принадлежит учетная запись, которая используется для подключения Сервера интеграции к виртуальной инфраструктуре.

     Поле **Домен OpenStack** отображается, если вы настраиваете подключение к виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС.

   - **Имя пользователя**

Имя учетной записи, которую Сервер интеграции использует для подключения к виртуальной инфраструктуре во время развертывания, удаления и изменения конфигурации SVM. Эта учетная запись должна обладать правами, достаточными для развертывания, удаления и изменения конфигурации SVM (см. раздел "Учетные записи для установки и работы решения" на стр. 42).

- **Пароль**

  Пароль учетной записи, которую Сервер интеграции использует для подключения к виртуальной инфраструктуре во время развертывания, удаления и изменения конфигурации SVM.

3. Нажмите на кнопку **Сохранить**.

Как изменить учетную запись с ограниченными правами

1. В разделе **Список виртуальных инфраструктур** выберите виртуальную инфраструктуру, для которой вы хотите изменить параметры подключения, нажмите на кнопку **Изменить**, расположенную над таблицей. и выберите пункт **Параметры учетной записи с ограниченными правами**.
2. В открывшемся окне укажите параметры учетной записи:

   - **Домен OpenStack**

     Имя домена OpenStack, к которому принадлежит учетная запись, которая используется для подключения Сервера интеграции к виртуальной инфраструктуре.

     Поле **Домен OpenStack** отображается, если вы настраиваете подключение к виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС.

   - **Имя пользователя**

     Имя учетной записи, которую Сервер интеграции использует для подключения к виртуальной инфраструктуре во время работы Kaspersky Security: для получения информации о доступных для подключения SVM и распределения Легких агентов между SVM.

     Для подключения к виртуальной инфраструктуре на платформе Citrix Hypervisor, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, OpenStack, Альт Сервер Виртуализации, Astra Linux, на Облачной платформе VK Cloud или на Облачной платформе ТИОНИКС рекомендуется использовать учетную запись, которая обладает ограниченными правами (см. раздел "Учетные записи для установки и работы решения" на стр. 42) на действия в виртуальной инфраструктуре.

     Для подключения к виртуальной инфраструктуре на платформе Microsoft Hyper-V во время работы Kaspersky Security может использоваться только та же учетная запись, под которой выполняется развертывание, удаление и изменение конфигурации SVM.

   - **Пароль**

     Пароль учетной записи, которую Сервер интеграции использует для подключения к виртуальной инфраструктуре во время работы Kaspersky Security.

3. Нажмите на кнопку **Сохранить**.

Как изменить параметры подключения к VMware NSX Manager

1. В разделе **Список виртуальных инфраструктур** выберите виртуальную инфраструктуру, для которой вы хотите изменить параметры подключения, нажмите на кнопку **Изменить**, расположенную над таблицей. и выберите пункт **Параметры VMware NSX Manager**.
2. В открывшемся окне укажите параметры учетной записи:
   - **Адрес**

     IP-адрес в формате IPv4 или полное доменное имя (FQDN) VMware NSX Manager.

     Если в вашей виртуальной инфраструктуре VMware NSX Manager объединены в кластер, укажите виртуальный IP-адрес кластера. Предварительно вам нужно назначить кластеру виртуальный IP-адрес и сертификат (подробнее о настройке кластера VMware NSX Manager см. в документации VMware).
   - **Имя пользователя**

     Имя учетной записи, которую Сервер интеграции использует для подключения к VMware NSX Manager. Требуется учетная запись VMware NSX Manager, которой назначена роль Enterprise Administrator.
   - **Пароль**

     Пароль учетной записи, которую Сервер интеграции использует для подключения к VMware NSX Manager.
3. Нажмите на кнопку **Сохранить**.

Как подтвердить сертификат или отпечаток открытого ключа

1. В разделе **Список виртуальных инфраструктур** выберите виртуальную инфраструктуру, для которой вы хотите подтвердить подлинность сертификата или открытого ключа, и нажмите на кнопку **Подтвердить сертификат**.

   Откроется окно **Проверка сертификата** или **Проверка отпечатка открытого ключа** (в зависимости от типа объекта виртуальной инфраструктуры).

   По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате или отпечаток ключа.
2. Если сертификат соответствует политике безопасности вашей организации, нажмите на кнопку **Подтвердить и продолжить**.

   Полученный сертификат или отпечаток открытого ключа будет сохранен на устройстве, где установлен Сервер интеграции.

   Если вы не считаете сертификат или открытый ключ подлинными, нажмите на кнопку **Отменить подключение**, чтобы прервать подключение.

Изменение параметров подключения к виртуальной инфраструктуре в Консоли Сервера интеграции

► *Чтобы открыть список виртуальных инфраструктур, к которым подключается Сервер интеграции:*

1. Откройте Консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65).

2. В списке слева выберите раздел **Параметры подключения к инфраструктуре**.

   Откроется список виртуальных инфраструктур, к которым подключается Сервер интеграции, в виде таблицы.

Каждая строка таблицы содержит следующие сведения:

- **Инфраструктура**

  Тип виртуальной инфраструктуры и IP-адрес в формате IPv4 или полное доменное имя (FQDN) объекта виртуальной инфраструктуры, к которому подключается Сервер интеграции для взаимодействия с виртуальной инфраструктурой.

  Для инфраструктуры под управлением VMware vCenter Server, если включено использование VMware NSX Manager в работе Kaspersky Security, в этом столбце также отображается IP-адрес в формате IPv4 или полное доменное имя (FQDN) VMware NSX Manager.

- **Состояние**

  Статус подключения Сервера интеграции к виртуальной инфраструктуре.

Если подключение Сервера интеграции к объекту виртуальной инфраструктуры не установлено, в таблице отображается сообщение об ошибке.

Сервер интеграции проверяет подлинность всех объектов виртуальной инфраструктуры, к которым выполняется подключение, кроме гипервизора Microsoft Windows Server (Hyper-V).

Для гипервизора Microsoft Windows Server (Hyper-V) проверка подлинности не выполняется. Проверка подлинности для микросервисов платформы OpenStack, Облачной платформы VK Cloud и Облачной платформы ТИОНИКС выполняется, только если для подключения Сервера интеграции к виртуальной инфраструктуре используется протокол HTTPS.

Для проверки подлинности Сервер интеграции получает от каждого объекта виртуальной инфраструктуры SSL-сертификат или отпечаток открытого ключа и проверяет их.

Если не удалось установить подлинность сертификата или открытого ключа, полученного от объекта виртуальной инфраструктуры, Сервер интеграции разрывает соединение с виртуальной инфраструктурой. В таблице отображается сообщение об ошибке. Вы можете устранить эту ошибку.

Чтобы устранить ошибку проверки SSL-сертификата или открытого ключа, полученных от объекта виртуальной инфраструктуры, выполните одно из следующих действий:

- Подтвердите подлинность сертификата или открытого ключа, полученного от объекта виртуальной инфраструктуры. Для этого вам нужно запустить мастер управления SVM (в разделе Консоли Сервера интеграции **Управление SVM**) и открыть список виртуальных инфраструктур, к которым настроено подключение мастера управления SVM (см., например, шаг "Выбор инфраструктуры для развертывания SVM" в процедуре установки Сервера защиты). Мастер предложит подтвердить подлинность сертификата или открытого ключа в окне **Проверка сертификата** или **Проверка отпечатка открытого ключа** (в зависимости от типа объекта виртуальной инфраструктуры).
- Замените сертификат на новый, если вы не считаете сертификат подлинным.

Если включено использование VMware NSX Manager в работе Kaspersky Security, Сервер интеграции также проверяет сертификат VMware NSX Manager. Если сертификат не является доверенным для Сервера интеграции или не соответствует ранее установленному сертификату, в таблице отображается сообщение об ошибке. Вы можете устранить эту ошибку.

Чтобы устранить ошибку проверки SSL-сертификата VMware NSX Manager, выполните одно из следующих действий:

- Подтвердите подлинность сертификата. Чтобы посмотреть информацию о полученном сертификате, вам нужно перейти по ссылке **Подтверждение подлинности сертификата VMware NSX Manager**, которая отображается в сообщении об ошибке. Если сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и продолжить подключение к VMware NSX Manager. Для этого нажмите на кнопку **Считать сертификат подлинным** в окне **Проверка сертификата**. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center.
- Если вы не считаете сертификат подлинным, вы можете прервать подключение, нажав на кнопку **Отмена**, и заменить сертификат на новый.

Как изменить параметры подключения к виртуальной инфраструктуре

1. Откройте Консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Параметры подключения к инфраструктуре**.

   Откроется список всех виртуальных инфраструктур, к которым подключается Сервер интеграции.
3. В таблице выберите виртуальную инфраструктуру, параметры подключения к которой вы хотите изменить, и перейдите по ссылке **Изменить**, расположенной над таблицей.

   Откроется окно **Изменение параметров подключения к виртуальной инфраструктуре**.

   В поле **Адрес** отображается IP-адрес в формате IPv4 или полное доменное имя (FQDN) объекта виртуальной инфраструктуры, к которому подключается Сервер интеграции для взаимодействия с защищаемой виртуальной инфраструктурой. Поле **Адрес** недоступно для изменения.
4. Внесите необходимые изменения. Для изменения доступны следующие параметры подключения Сервера интеграции к виртуальной инфраструктуре:

   - **Протокол**

     Протокол, который используется для подключения Сервера интеграции к виртуальной инфраструктуре. По умолчанию используется протокол HTTPS.

     Поле **Протокол** отображается, если вы настраиваете подключение к виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС.

   - **Домен OpenStack**

     Имя домена OpenStack, к которому принадлежит учетная запись, которая используется для подключения Сервера интеграции к виртуальной инфраструктуре.

     Поле **Домен OpenStack** отображается, если вы настраиваете подключение к виртуальной инфраструктуре под управлением платформы OpenStack, Облачной платформы VK Cloud или Облачной платформы ТИОНИКС.

   - **Имя пользователя**

     Имя учетной записи, которую Сервер интеграции использует для подключения к виртуальной инфраструктуре во время работы Kaspersky Security.

Для подключения к виртуальной инфраструктуре на платформе XenServer, VMware vSphere, KVM, Proxmox VE, Базис, Скала-Р, HUAWEI FusionSphere, Nutanix Acropolis, OpenStack, Альт Сервер Виртуализации, Astra Linux, Numa vServer, на Облачной платформе VK Cloud или на Облачной платформе ТИОНИКС рекомендуется использовать учетную запись, которая обладает ограниченными правами (см. раздел "Учетные записи для установки и работы решения" на стр. 42) на действия в виртуальной инфраструктуре.

Для подключения к виртуальной инфраструктуре на платформе Microsoft Hyper-V во время работы Kaspersky Security может использоваться только та же учетная запись, под которой выполняется развертывание, удаление и изменение конфигурации SVM.

- **Пароль**

  Пароль учетной записи, которую Сервер интеграции использует для подключения к виртуальной инфраструктуре во время работы Kaspersky Security.

5. Нажмите на кнопку **OK** в окне **Изменение параметров подключения к виртуальной инфраструктуре**.

Как настроить использование VMware NSX Manager в работе решения Kaspersky Security

1. Откройте Консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Параметры подключения к инфраструктуре**.

   Откроется список всех виртуальных инфраструктур, к которым подключается Сервер интеграции.
3. В таблице выберите виртуальную инфраструктуру под управлением VMware vCenter Server и перейдите по ссылке **Изменить**, расположенной над таблицей.

   Откроется окно **Изменение параметров подключения к виртуальной инфраструктуре**.
4. Настройте параметры подключения Сервера интеграции к VMware NSX Manager:

   - **Использовать VMware NSX Manager**

     Включает и выключает использование VMware NSX Manager в работе решения Kaspersky Security.

     Если VMware NSX Manager используется в работе решения, Kaspersky Security может назначать защищенной виртуальной машине теги безопасности (Security Tags) (см. раздел "О тегах безопасности (Security Tags)" на стр. 134).

   - **Адрес**

     IP-адрес в формате IPv4 или полное доменное имя (FQDN) VMware NSX Manager.

     Если в вашей виртуальной инфраструктуре VMware NSX Manager объединены в кластер, укажите виртуальный IP-адрес кластера. Предварительно вам нужно назначить кластеру виртуальный IP-адрес и сертификат (подробнее о настройке кластера VMware NSX Manager см. в документации VMware).

   - **Имя пользователя**

     Имя учетной записи, которую Сервер интеграции использует для подключения к VMware NSX Manager. Требуется учетная запись VMware NSX Manager, которой назначена роль Enterprise Administrator.

   - **Пароль**

     Пароль учетной записи, которую Сервер интеграции использует для подключения к

VMware NSX Manager.

Если вы изменили пароль учетной записи для подключения к VMware NSX Manager, то Сервер интеграции сможет подключиться к VMware NSX Manager не ранее, чем через 15 минут после сохранения новых параметров подключения.

5. Нажмите на кнопку **OK** в окне **Изменение параметров подключения к виртуальной инфраструктуре**.

Удаление параметров подключения Сервера интеграции к виртуальной инфраструктуре

Если вы хотите, чтобы Сервер интеграции перестал получать информацию от виртуальной инфраструктуры, вы можете удалить эту виртуальную инфраструктуру из списка инфраструктур, к которым подключается Сервер интеграции.

Рекомендуется удалять из списка виртуальную инфраструктуру, только если в этой инфраструктуре не установлены компоненты решения Kaspersky Security.

Как удалить виртуальную инфраструктуру в Веб-консоли Сервера интеграции

► *Чтобы удалить виртуальную инфраструктуру:*

1. Откройте Веб-консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Веб-консоль Сервера интеграции" на стр. 64).
2. Перейдите в раздел **Список виртуальных инфраструктур**.
3. В таблице выберите виртуальную инфраструктуру, которую вы хотите удалить, и нажмите на кнопку **Удалить**, расположенную над таблицей.
4. Подтвердите удаление в открывшемся окне.

Как удалить виртуальную инфраструктуру в Консоли Сервера интеграции

► *Чтобы удалить виртуальную инфраструктуру:*

1. Откройте Консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Параметры подключения к инфраструктуре**.
3. В правой части окна в таблице выберите виртуальную инфраструктуру, которую вы хотите удалить, и перейдите по ссылке **Удалить**, расположенной над таблицей.
4. Подтвердите удаление в открывшемся окне.

Если вы удалили виртуальную инфраструктуру из этого списка, рекомендуется также удалить эту виртуальную инфраструктуру из списка виртуальных инфраструктур, к которым настроено подключение для мастера управления SVM (см., например, шаг "Выбор SVM для удаления" в процедуре удаления Сервера защиты).

kaspersky

Замена сертификатов Сервера интеграции и SVM

В комплект поставки решения Kaspersky Security входит *утилита управления сертификатами* Сервера интеграции и SVM. SSL-сертификат Сервера интеграции используется при установке защищенного соединения с Сервером интеграции и для шифрования канала связи между Сервером защиты и Легким агентом. SSL-сертификат SVM используется для шифрования канала связи между Легким агентом и Сервером защиты.

Утилита управления сертификатами позволяет:

- Создать сертификат Сервера интеграции.
- Заменить самоподписанный сертификат Сервера интеграции, установленный в ходе развертывания решения.

  При замене сертификата Сервера интеграции автоматически заменяется сертификат SVM. Новый сертификат SVM создается на основе сертификата Сервера интеграции.

Замена сертификатов может потребоваться в следующих случаях:

- В ходе обновления решения для замены ранее установленного сертификата на более безопасный.
- Если срок действия используемого сертификата истек или сертификат скомпрометирован.
- Если изменился IP-адрес или доменное имя устройства, на котором установлен Сервер интеграции.

Вы можете заменить сертификат Сервера интеграции на новый сертификат, созданный с помощью утилиты или с помощью сторонних инструментов. Если вы хотите использовать сертификат Сервера интеграции, созданный с помощью сторонних инструментов, убедитесь, что новый сертификат удовлетворяет требованиям утилиты к сертификатам.

Сертификат Сервера интеграции должен удовлетворять следующим требованиям:

- Формат PFX.
- Сертификат содержит закрытый ключ.
- Сертификат защищен паролем.
- Поле Subject alternative name содержит значения:
  - IP Address – внешний и локальный IP-адреса Сервера интеграции;
  - DNS Name – внешний и локальный IP-адреса, а также доменное имя (FQDN) Сервера интеграции.
- Key Usage:
  - KeyEncipherment;
  - DigitalSignature;
  - DataEncipherment;
  - KeyCertSign.
- Enhanced Key Usage:
  - Server Authentication (1.3.6.1.5.5.7.3.1);
  - Client Authentication (1.3.6.1.5.5.7.3.2).

- Дата окончания срока действия сертификата больше текущей даты.
- Алгоритм ключа: RSA (1.2.840.113549.1.1.1).
- Размер ключа: 4096 бит.
- Разрешенные алгоритмы подписи:
  - Sha256WithRSA (1.2.840.113549.1.1.11);
  - Sha384WithRSA (1.2.840.113549.1.1.12);
  - Sha512WithRSA (1.2.840.113549.1.1.13).

Утилита управления сертификатами может работать с Сервером интеграции на базе Linux и с Сервером интеграции на базе Windows. Утилита расположена на устройстве, где установлен Сервер интеграции. В зависимости от операционной системы устройства утилита расположена по следующему пути:

- /opt/kaspersky/viis/bin/certificate_manager.sh – на устройствах с операционными системами Linux;
- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\certificate_manager.exe – на устройствах с операционными системами Windows.

Для использования утилиты в операционной системе Linux учетная запись пользователя должна находиться в группе sudoers. Для использования утилиты в операционной системе Windows требуются права Администратора в операционной системе.

Как создать сертификат Сервера интеграции на базе Linux с помощью утилиты

На устройстве, где установлен Сервер интеграции, выполните команду:

```
sudo /opt/kaspersky/viis/bin/certificate_manager.sh create-self-signed-certs --outputFolder <путь к директории с сертификатом> [--keySize <2048 или 4096>] [--quiet]
```

где:

- `<путь к директории с сертификатом>` – путь к директории, в которую будет помещен созданный сертификат. Директория должна находиться на устройстве, где установлен Сервер интеграции.
- `--keySize <2048 или 4096>` – длина ключа сертификата. Необязательный параметр. Если параметр не указан, используется значение по умолчанию 4096.
- `--quiet` – необязательный параметр. Если параметр указан, то утилита будет работать в тихом режиме, в консоль ничего не будет выводиться.

В результате выполнения команды утилита создает сертификат Сервера интеграции (файл viis.pfx) и помещает его в указанную директорию.

Рекомендуется обеспечить защиту сертификата от несанкционированного доступа. Например, вы можете использовать для размещения сертификата защищенную директорию.

Как создать сертификат Сервера интеграции на базе Windows с помощью утилиты

На устройстве, где установлен Сервер интеграции, выполните команду:

```
%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\certificate_manager.exe create-self-signed-certs --outputFolder <путь к папке с сертификатом> [--keySize <2048 или 4096>] [--quiet]
```

где:

- `<путь к папке с сертификатом>` – путь к папке, в которую будет помещен созданный сертификат. Папка должна находиться на устройстве, где установлен Сервер интеграции.
- `--keySize <2048 или 4096>` – длина ключа сертификата. Необязательный параметр. Если параметр не указан, используется значение по умолчанию 4096.
- `--quiet` – необязательный параметр. Если параметр указан, то после выполнения команды окно консоли ввода закрывается, в противном случае окно консоли остается открытым.

В результате выполнения команды утилита создает сертификат Сервера интеграции (файл viis.pfx) и помещает его в указанную папку.

Рекомендуется обеспечить защиту сертификата от несанкционированного доступа. Например, вы можете использовать для размещения сертификата защищенную папку.

Как заменить сертификаты Сервера интеграции на базе Linux и SVM

На устройстве, где установлен Сервер интеграции, выполните команду:

```
sudo /opt/kaspersky/viis/bin/certificate_manager.sh replace --certificatePath <путь к сертификату> [--quiet]
```

где:

- `<путь к сертификату>` – путь к сертификату Сервера интеграции (файлу viis.pfx).
- `--quiet` – необязательный параметр. Если параметр указан, то утилита будет работать в тихом режиме, в консоль ничего не будет выводиться.

В результате выполнения команды утилита выполняет следующие действия:

- Создает сертификат SVM на основе сертификата, размещенного в указанной папке.
- Заменяет ранее установленные сертификат Сервера интеграции и сертификат SVM на новые.
- Перезапускает службу Сервера интеграции.

Как заменить сертификаты Сервера интеграции на базе Windows и SVM

На устройстве, где установлен Сервер интеграции, выполните команду:

```
%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\certificate_manager.exe replace --certificatePath <путь к сертификату>
```

где `<путь к сертификату>` – путь к сертификату Сервера интеграции (файлу viis.pfx).

В результате выполнения команды утилита выполняет следующие действия:

- Создает сертификат SVM на основе сертификата, размещенного в указанной папке.
- Заменяет ранее установленные сертификат Сервера интеграции и сертификат SVM на новые.
- Перезапускает службу Сервера интеграции.

После замены сертификатов Сервера интеграции и SVM вам нужно обновить все политики для Легкого агента и политики для Сервера защиты, чтобы передать в политики открытый ключ нового сертификата.

Во время работы утилиты управления сертификатами могут создаваться файлы трассировки (см. раздел "Файлы трассировки утилиты управления сертификатами Сервера интеграции и SVM" на стр. 234).

kaspersky

Проверка целостности компонентов решения

Компоненты решения Kaspersky Security содержат множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленник может подменить один или несколько модулей или файлов решения модулями или файлами, содержащими вредоносный код. Чтобы избежать подмены модулей и файлов решения, в Kaspersky Security предусмотрена проверка целостности файлов и модулей. Во время проверки выявляется наличие неавторизованных изменений или повреждений в файлах и модулях компонентов решения. Если файл или модуль решения имеет некорректную контрольную сумму, то он считается поврежденным.

Проверка целостности компонентов решения Kaspersky Security выполняется с помощью *утилиты проверки целостности*. Для проверки целостности используются специальные списки, которые называются *файлы манифеста*. Файл манифеста компонента решения содержит список файлов и модулей, целостность которых важна для корректной работы этого компонента. Файлы манифеста подписаны цифровой подписью, их целостность также проверяется.

С помощью утилиты проверки целостности вы можете проверять целостность файлов и модулей следующих компонентов решения:

- Компонентов, установленных на SVM: Сервера защиты и Агента администрирования Kaspersky Security Center.
- Сервера интеграции на базе Windows и Сервера интеграции на базе Linux.
- Консоли Сервера интеграции.
- Веб-плагинов управления Сервера защиты и Сервера интеграции.
- MMC-плагина управления Сервера защиты.
- Легкого агента для Linux и плагинов управления Легкого агента для Linux (приложения Kaspersky Endpoint Security для Linux).

Для запуска утилиты проверки целостности на SVM и на виртуальной машине с установленным Легким агентом для Linux требуется учетная запись `root`. Для запуска утилиты проверки целостности остальных компонентов решения требуется учетная запись администратора.

Подробную информацию о проверке целостности Легкого агента для Linux и плагинов управления Легкого агента для Linux см. в справке приложения Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/98842.htm.

Информацию о проверке целостности Агента администрирования Kaspersky Security Center см. в справке Kaspersky Security Center.

Для Легкого агента для Windows (приложения Kaspersky Endpoint Security для Windows) предусмотрена процедура проверки целостности приложения с помощью специальной задачи (см. подробнее в справке приложения Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.8/ru-RU/201526.htm).

Файлы манифеста и утилиты проверки целостности для Сервера защиты, плагинов управления Сервера

защиты, Сервера интеграции и Консоли Сервера интеграции расположены по следующим путям:

- Для проверки Сервера защиты, установленного на SVM:
  - Файл манифеста: /opt/kaspersky/la/bin/integrity_check.xml.
  - Утилита проверки целостности: /opt/kaspersky/la/bin/integrity_checker.
- Для проверки Сервера интеграции на базе Linux:
  - Файл манифеста: /opt/kaspersky/viis/bin/integrity_check.xml.
  - Утилита проверки целостности: /opt/kaspersky/viis/bin/integrity_checker.
- Для проверки Сервера интеграции на базе Windows:
  - Файл манифеста: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\integrity_check.xml.
  - Утилита проверки целостности: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\integrity_checker.exe.
- Для проверки Консоли Сервера интеграции:
  - Файл манифеста: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA Console\integrity_check.xml.
  - Утилита проверки целостности: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA Console\integrity_checker.exe.
- Для проверки MMC-плагина управления Сервера защиты:
  - Файл манифеста: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\KSVLA<номер версии>.SVM.plg\integrity_check.xml.
  - Утилита проверки целостности: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\KSVLA<номер версии>.SVM.plg\integrity_checker.exe.
- Для проверки веб-плагинов управления Сервера защиты и Сервера интеграции:
  - Файл манифеста веб-плагина Сервера защиты:
    - /var/opt/kaspersky/ksc-web-console/server/plugins/svm_<номер версии>/integrity_check.xml – для веб-плагина Сервера защиты на устройствах с операционными системами Linux.
    - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\svm_<номер версии>\integrity_check.xml – для веб-плагина Сервера защиты на устройствах с операционными системами Windows.
  - Файл манифеста веб-плагина Сервера интеграции:
    - var/opt/kaspersky/ksc-web-console/server/plugins/VIISLA_<номер версии>/integrity_check.xml – для веб-плагина Сервера интеграции на устройствах с операционными системами Linux.
    - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\VIISLA_<номер версии>\integrity_check.xml – для веб-плагина Сервера интеграции на устройствах с операционными системами Windows.
  - Утилита проверки целостности:
    - /var/opt/kaspersky/ksc-web-console/integrity_checker – на устройствах с операционными системами Linux.
    - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\integrity_checker.exe – на устройствах с операционными системами Windows.

Чтобы проверить целостность компонента решения, вам нужно запустить утилиту из папки расположения утилиты для этого компонента.

► *Чтобы запустить утилиту проверки целостности, выполните одну из следующих команд:*

- для проверки целостности Сервера защиты:

  ```
  integrity_checker --signature-type kds-with-filename [<путь к файлу манифеста>]
  ```

- для проверки целостности MMC-плагина управления Сервера защиты, Сервера интеграции на базе Windows или Консоли Сервера интеграции:

  ```
  integrity_checker.exe --signature-type kds-with-filename [<путь к файлу манифеста>]
  ```

- для проверки целостности Сервера интеграции на базе Linux:

  ```
  integrity_checker --signature-type kds-with-filename [<путь к файлу манифеста>]
  ```

- для проверки целостности веб-плагинов управления на устройствах с операционными системами Linux:

  ```
  integrity_checker --signature-type kds-with-filename [<путь к файлу манифеста>]
  ```

- для проверки целостности веб-плагинов управления на устройствах с операционными системами Windows:

  ```
  integrity_checker.exe --signature-type kds-with-filename [<путь к файлу манифеста>]
  ```

где `<путь к файлу манифеста>` – полный путь к файлу манифеста для проверяемого компонента. По умолчанию используется путь к файлу манифеста, расположенному в той же директории, в которой расположена утилита проверки целостности.

Вы можете просмотреть описание всех доступных параметров утилиты проверки целостности в справке параметров утилиты. Для этого запустите утилиту с параметром `--help`.

Результат проверки целостности компонента решения отображается в следующем виде:

- `SUCCEEDED` – целостность файлов и модулей подтверждена (код возврата `0`).
- `FAILED` – целостность файлов и модулей не подтверждена (код возврата отличен от `0`).

kaspersky

Использование Kaspersky Security для виртуальных сред 6.2 Легкий агент в режиме мультитенантности

При использовании Kaspersky Security в режиме мультитенантности один экземпляр Kaspersky Security, установленный в инфраструктуре поставщика услуг защиты от киберугроз (далее также "поставщика услуг"), позволяет обеспечивать защиту изолированных виртуальных инфраструктур организаций-тенантов или изолированных подразделений одной организации (далее также "тенантов").

Процедуры развертывания и использования Kaspersky Security в режиме мультитенантности автоматизированы средствами REST API Сервера интеграции (см. раздел "Использование REST API Сервера интеграции в сценариях мультитенантности" на стр. 209).

Предусмотрены следующие сценарии использования Kaspersky Security в режиме мультитенантности:

- Развертывание структуры защиты тенантов (на стр. 191) средствами REST API Сервера интеграции с использованием виртуальных Серверов администрирования Kaspersky Security Center и получение отчетов о защите тенантов (на стр. 204).
- Получение отчетов о защите тенантов без развертывания структуры защиты тенантов средствами REST API Сервера интеграции.

  Если структура защиты тенантов уже развернута в вашей инфраструктуре без использования REST API Сервера интеграции, вы можете регистрировать существующих тенантов и их виртуальные машины (см. раздел "Регистрация существующих тенантов и их виртуальных машин" на стр. 201) и получать отчеты о защите тенантов.

В этом разделе

Развертывание структуры защиты тенантов

Структура защиты тенантов, созданная с помощью REST API Сервера интеграции, основана на использовании виртуальных Серверов администрирования Kaspersky Security Center. Каждому тенанту предоставляется виртуальный Сервер администрирования и учетная запись, под которой администратор тенанта будет подключаться к виртуальному Серверу администрирования.

Один Сервер администрирования Kaspersky Security Center может поддерживать до 500 виртуальных Серверов администрирования.

Виртуальные машины тенанта с установленными Легкими агентами размещаются на виртуальном Сервере администрирования тенанта.

Администратор тенанта может выполнять следующие действия на своем виртуальном Сервере администрирования:

- Централизованно управлять защитой своих виртуальных машин с помощью политик для Легкого агента и групповых задач.
- Получать информацию о состоянии защиты своей инфраструктуры с помощью уведомлений о событиях и отчетов, доступных на виртуальном Сервере администрирования.
- Работать с копиями файлов, помещенными в резервные хранилища на всех виртуальных машинах этого тенанта.

Подробнее о виртуальных Серверах администрирования см. в справке Kaspersky Security Center.

Администратор поставщика услуг выполняет установку решения в своей инфраструктуре и обеспечивает работу Легких агентов и других компонентов решения:

- Настраивает параметры подключения Легких агентов, установленных на виртуальных машинах тенанта, к SVM и к Серверу интеграции.
- Активирует решение и осуществляет контроль лицензионных ограничений.
- Выполняет обновление баз и программных модулей решения.
- Настраивает параметры работы Сервера защиты.

Также администратор поставщика услуг может настраивать общие параметры защиты виртуальных машин тенантов.

Во время работы между компонентами решения Kaspersky Security, установленными в инфраструктуре поставщика услуг и на виртуальных машинах тенанта, а также приложением Kaspersky Security Center осуществляется передача информации, которая может содержать персональные и конфиденциальные данные.

Перед тем, как создавать структуру защиты тенантов, вам нужно выполнить следующие действия:

1. Установить или обновить решение Kaspersky Security.

   В инфраструктуре поставщика услуг должны быть установлены следующие компоненты:

   - Сервер интеграции и Консоль Сервера интеграции.
   - Сервер защиты.
   - Плагины управления Kaspersky Security (см. раздел "О плагинах управления Kaspersky Security" на стр. 105).
2. Подготовить решение к работе:
   - Подготовить к работе Сервер защиты (см. раздел "Подготовка Сервера защиты к работе" на стр. 77).

- Изменить заданный по умолчанию пароль (см. раздел "Изменение паролей учетных записей Сервера интеграции" на стр. 174) учетной записи `multitenancy`. Учетная запись `multitenancy` создается автоматически в результате установки Сервера интеграции и требуется для взаимодействия с REST API Сервера интеграции.
- Настроить параметры подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center (см. раздел "Настройка параметров подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center" на стр. 194). Эти параметры требуются для авторизации на Сервере администрирования Kaspersky Security Center при выполнении запросов к REST API Сервера интеграции.

Развертывание структуры защиты тенанта состоит из следующих этапов:

1. Создание тенанта и виртуального Сервера администрирования Kaspersky Security Center для тенанта (см. раздел "Создание тенанта и виртуального Сервера администрирования" на стр. 196).
2. Настройка расположения SVM, которые будут защищать виртуальные машины тенантов, и настройка параметров работы Сервера защиты (см. раздел "Настройка расположения SVM и параметров Сервера защиты" на стр. 197).
3. Настройка параметров обнаружения SVM Легкими агентами, установленными на виртуальных машинах тенантов, и настройка общих параметров работы Легких агентов (см. раздел "Настройка параметров обнаружения SVM Легкими агентами и общих параметров защиты тенантов" на стр. 198).
4. Установка Агента администрирования Kaspersky Security Center и Легкого агента на виртуальные машины тенанта и перемещение виртуальных машин на виртуальный Сервер администрирования, настроенный для тенанта (см. раздел "Установка Легкого агента на виртуальные машины тенанта" на стр. 199).
5. Регистрация виртуальных машин тенанта в базе данных Сервера интеграции (см. раздел "Регистрация виртуальных машин тенанта" на стр. 200).
6. Активация тенанта (на стр. 200).
7. Передача администратору тенанта параметров для подключения к виртуальному Серверу администрирования Kaspersky Security Center:
   - адреса виртуального Сервера администрирования, настроенного для тенанта;
   - параметров учетной записи администратора виртуального Сервера администрирования.

   Администратору тенанта рекомендуется изменить пароль учетной записи, полученный от администратора поставщика услуг.

Этапы развертывания структуры защиты тенантов могут быть автоматизированы средствами REST API Сервера интеграции (см. раздел "Использование REST API Сервера интеграции в сценариях мультитенантности" на стр. 209) и OpenAPI™ Kaspersky Security Center (открыть описание методов OpenAPI Kaspersky Security Center - https://support.kaspersky.com/help/KSVLA/API/6.1/ru-RU/Examples_of_using_KSC_OpenAPI_in_KSV6.1LA.pdf).

В целях предотвращения несанкционированного доступа рекомендуется SVM и устройство, на котором установлены Сервер администрирования Kaspersky Security Center и Сервер интеграции, разместить в выделенной виртуальной сети и настроить маршрутизацию с трансляцией адресов (SNAT) из подсетей тенантов в эту подсеть.

kaspersky

В этом разделе

Настройка параметров подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center

Для взаимодействия REST API Сервера интеграции с Сервером администрирования Kaspersky Security Center во время выполнения запросов требуется учетная запись, которая обладает следующими правами в Kaspersky Security Center:

- Правами в функциональных областях Сервера администрирования:
  - Общий функционал → Базовая функциональность: Чтение, Изменение.
  - Общий функционал → Управление группами администрирования: Изменение.
  - Общий функционал → Права пользователей: Изменение списков управления доступом объектов.
  - Общий функционал → Виртуальные Серверы администрирования: Чтение, Изменение, Выполнение, Управление.
- Правами на чтение и на изменение в функциональных областях, к которым относятся параметры Легкого агента (см. раздел "О правах доступа к параметрам политик и задач в Kaspersky Security Center" на стр. 127).

Вы можете создать и настроить учетную запись для подключения Сервера интеграции к Kaspersky Security Center:

- В Консоли администрирования Kaspersky Security Center в разделе **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center.

  По умолчанию раздел **Безопасность** не отображается в окне свойств Сервера администрирования. Чтобы включить отображение раздела **Безопасность**, требуется установить флажок **Отображать разделы с параметрами безопасности** в окне **Настройка интерфейса** (меню **Вид** → **Настройка интерфейса**) и перезапустить Консоль администрирования Kaspersky Security Center.

- В Kaspersky Security Center Web Console в разделе **Пользователи и роли** → **Пользователи и группы** главного окна.

Подробнее о создании и настройке прав учетных записей в Kaspersky Security Center см. в справке Kaspersky Security Center.

Как настроить подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center в Веб-консоли Сервера интеграции

► *Чтобы настроить подключение Сервера интеграции к Серверу администрирования:*

1. Откройте Веб-консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Веб-консоль Сервера интеграции" на стр. 64).
2. Перейдите в раздел **Режим мультитенантности**.
3. Нажмите на кнопку **Подключиться**, расположенную в блоке **Параметры подключения к Kaspersky Security Center**.
4. В открывшемся окне укажите параметры подключения:
   - IP-адрес в формате IPv4 или полное доменное имя (FQDN) Сервера администрирования Kaspersky Security Center.
   - Имя и пароль учетной записи, которая будет использоваться для взаимодействия REST API Сервера интеграции с Сервером администрирования Kaspersky Security Center.
5. Нажмите на кнопку **Сохранить**.

Сервер интеграции выполняет попытку подключения, чтобы проверить указанные параметры подключения. Если SSL-сертификат, полученный от Сервера администрирования Kaspersky Security Center, не является доверенным для Сервера интеграции, открывается окно **Проверка сертификата** с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. Если сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и продолжить подключение к Серверу администрирования. Если вы не считаете этот сертификат подлинным, нажмите на кнопку **Отменить подключение**, чтобы прервать подключение.

После установки подключения Сервер интеграции сохраняет параметры подключения. Адрес Сервера администрирования Kaspersky Security Center, к которому выполнено подключение, отображается в окне **Режим мультитенантности** в блоке **Параметры подключения к Kaspersky Security Center**. С помощью кнопок справа от адреса Сервера администрирования вы можете:

- открыть окно **Параметры подключения к Kaspersky Security Center** для изменения параметров подключения;
- разорвать подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center и удалить настроенные параметры подключения.

Как настроить подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center в Консоли Сервера интеграции

► *Чтобы настроить подключение Сервера интеграции к Серверу администрирования:*

1. Откройте Консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Параметры подключения к Kaspersky Security Center**.
3. Укажите параметры подключения:
   - IP-адрес в формате IPv4 или полное доменное имя (FQDN) Сервера администрирования Kaspersky Security Center.

- Имя и пароль учетной записи, которая будет использоваться для взаимодействия REST API Сервера интеграции с Сервером администрирования Kaspersky Security Center.

4. Нажмите на кнопку **Сохранить**.

Сервер интеграции выполняет попытку подключения, чтобы проверить указанные параметры подключения. Если SSL-сертификат, полученный от Сервера администрирования Kaspersky Security Center, не является доверенным для Сервера интеграции, открывается окно с сообщением об этом. По ссылке в этом окне вы можете посмотреть информацию о полученном сертификате. Если полученный сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата, нажав на кнопку **Установить сертификат**. Полученный сертификат сохраняется в качестве доверенного для Сервера интеграции.

После установки подключения Сервер интеграции сохраняет параметры подключения. Если требуется, вы можете изменить параметры подключения в этом же разделе.

С помощью кнопки **Удалить** вы можете разорвать подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center и удалить настроенные параметры подключения.

Создание тенанта и виртуального Сервера администрирования

На этом этапе развертывания структуры защиты тенанта выполняется добавление информации о тенанте в базу данных Сервера интеграции и создание виртуального Сервера администрирования для тенанта. Процедуры автоматизированы средствами REST API Сервера интеграции (см. раздел "Создание тенанта" на стр. 212).

Действия, выполняемые в результате запроса к REST API, зависят от типа тенанта, который вы указываете при вызове метода REST API: развертывание структуры защиты тенантов доступно только для тенантов типа "полный".

В запросе к REST API нужно передать следующие сведения:

- Название тенанта.
- Тип тенанта: полный.
- Параметры учетной записи, которую будет использовать администратор тенанта для подключения к виртуальному Серверу администрирования, настроенному для тенанта. Во время выполнения процедуры автоматически будет создана учетная запись с правами главного администратора на виртуальном Сервере администрирования.

  Kaspersky Security Center проверяет уникальность имен учетных записей в пределах главного Сервера администрирования Kaspersky Security Center и всех его виртуальных Серверов администрирования. По умолчанию, если имя пользователя не уникально, создание учетной записи завершается с ошибкой. Если вы хотите использовать одинаковые имена учетных записей для виртуальных Серверов администрирования, вы можете отключить проверку уникальности имени внутреннего пользователя, см. подробнее в справке Kaspersky Security Center.

В результате выполнения процедуры выполняются следующие действия:

- В базе данных Сервера интеграции сохраняются данные о тенанте, тенанту присваивается уникальный идентификатор.
- Для каждого тенанта создается виртуальный Сервер администрирования Kaspersky Security Center и учетная запись, под которой администратор тенанта будет подключаться к виртуальному Серверу администрирования.
- При регистрации первого тенанта на главном Сервере администрирования в папке **Управляемые устройства** создается папка с названием по умолчанию **Multitenancy KSV LA**. Вы можете изменить это название, если требуется.
- В папке **Multitenancy KSV LA** для каждого тенанта создается структура папок и узлов следующего вида:

  папка **<Название тенанта>**

  - узел **Серверы администрирования**
    - узел **Сервер администрирования <Название тенанта>**
      - папки и группы администрирования, необходимые для управления защитой этого тенанта, аналогично структуре папок и групп главного Сервера администрирования Kaspersky Security Center.

Настройка расположения SVM и параметров Сервера защиты

На этом этапе развертывания структуры защиты тенанта вы можете выполнить следующие действия:

1. Настроить расположение SVM, которые будут защищать виртуальные машины тенантов, в иерархии групп администрирования Kaspersky Security Center.
2. Настроить параметры работы Сервера защиты, установленного на этих SVM, с помощью политики для Сервера защиты.
3. Настроить общие параметры работы Легких агентов, которые будут установлены на виртуальных машинах тенантов, с помощью политик для Легкого агента.

Вы можете размещать SVM, которые будут защищать виртуальные машины тенантов, в любых папках и группах администрирования на главном Сервере администрирования Kaspersky Security Center.

Не рекомендуется размещать SVM и политику для Сервера защиты в папках и группах администрирования, к которым администратор тенанта имеет доступ, то есть в папках и группах администрирования внутри узла **Сервер администрирования <Название тенанта>**.

Если вы хотите, чтобы SVM защищала виртуальные машины только одного или нескольких тенантов, вам нужно ограничить доступ Легких агентов к SVM одним из следующих способов:

- С помощью механизма тегов для подключения. Теги нужно указать в политике для Сервера защиты (см. раздел "Настройка использования тегов для подключения на SVM" на стр. 142) и в политике для Легкого агента (см. раздел "Назначение тегов для подключения Легким агентам" на стр. 144). Настроенные параметры рекомендуется закрыть "замком", чтобы запретить изменение этих параметров в политиках вложенного уровня иерархии.

- Запретив сетевые подключения из подсети тенанта в подсеть с SVM на TCP-порты 80, 9876, 9877, 11111, 11112 (см. раздел "Настройка используемых портов" на стр. 35).

Не рекомендуется настраивать теги для подключения в политиках для Легкого агента, расположенных в папках и группах администрирования, к которым администратор тенанта имеет доступ, то есть в папках и группах администрирования внутри узла **Сервер администрирования <Название тенанта>**.

В соответствии с порядком наследования политик Kaspersky Security Center на всех SVM в иерархии групп администрирования применяется политика по умолчанию для Сервера защиты, созданная в папке **Управляемые устройства** на главном Сервере администрирования. Если вы хотите настроить особые параметры работы для SVM, которые будут защищать виртуальные машины тенантов, вам нужно создать политику для Сервера защиты в папке расположения SVM, которая защищает виртуальные машины тенантов.

Если вы хотите централизованно включить использование Kaspersky Security Network для защиты виртуальных машин тенантов, вам нужно убедиться, что обеспечивается законность обработки персональных данных тенантов (см. раздел "О предоставлении данных при использовании KSN в работе Сервера защиты" на стр. 168).

Настройка параметров обнаружения SVM Легкими агентами и общих параметров защиты тенантов

На этом этапе развертывания структуры защиты тенанта вам нужно создать политику для Легкого агента в одной из следующих папок:

- В папке **Multitenancy KSV LA** → **<Название тенанта>**, если вы хотите настраивать общие параметры работы для всех Легких агентов, которые будут установлены на виртуальных машинах одного тенанта. Политику в папке **Multitenancy KSV LA** → **<Название тенанта>** нужно создать для каждого тенанта.
- В папке **Multitenancy KSV LA**, если вы хотите настраивать общие параметры работы для всех Легких агентов, которые будут установлены на виртуальных машинах всех тенантов.

В политике для Легкого агента вам нужно настроить параметры работы Легкого агента следующим образом:

- Параметры подключения Легких агентов к SVM (см. раздел "Подключение Легких агентов к SVM" на стр. 140):
  - Вам нужно включить использование Сервера интеграции для обнаружения SVM в политике для Легкого агента (см. раздел "Настройка параметров обнаружения SVM" на стр. 140). Легкие агенты, установленные на виртуальных машинах тенантов типа "полный", должны использовать Сервер интеграции для обнаружения SVM (см. раздел "Об обнаружении SVM" на стр. 15), доступных для подключения.
  - Если вы хотите ограничить доступ Легких агентов к SVM с помощью механизма тегов для подключения, вы можете назначить теги для подключения Легким агентам (см. раздел "Назначение тегов для подключения Легким агентам" на стр. 144).

Чтобы ограничить доступ Легких агентов к SVM, вы также можете запретить сетевые подключения из подсети тенанта в подсеть с SVM на TCP-порты 80, 9876, 9877, 11111, 11112 (см. раздел "Настройка используемых портов" на стр. 35).

Для остальных параметров подключения Легких агентов к SVM можно использовать значения по умолчанию.

Все параметры подключения Легких агентов к SVM рекомендуется закрыть "замком", чтобы запретить изменение этих параметров в политиках вложенного уровня иерархии.

- Если требуется, вы можете настроить общие параметры работы Легких агентов, которые будут установлены на виртуальных машинах тенантов.

  С помощью атрибута "замок" вы можете запретить или разрешить изменение параметров или блоков параметров в параметрах задач и в политиках вложенного уровня иерархии (для вложенных групп администрирования и подчиненных Серверов администрирования). Администраторы тенантов не могут настраивать параметры, которые закрыты "замком". Если "замки" открыты, то администратор тенанта сможет самостоятельно настраивать работу компонентов Легкого агента.

Не рекомендуется настраивать общие параметры работы Легких агентов в политиках, расположенных в папках и группах администрирования, к которым администратор тенанта имеет доступ, то есть в папках и группах администрирования внутри узла **Сервер администрирования <Название тенанта>**.

Установка Легкого агента на виртуальные машины тенанта

На этом этапе развертывания структуры защиты тенанта выполняются следующие действия:

- На виртуальные машины тенанта устанавливается Агент администрирования Kaspersky Security Center, настроенный на подключение к виртуальному Серверу администрирования тенанта.
- Виртуальные машины тенанта перемещаются в папку **Управляемые устройства** виртуального Сервера администрирования, настроенного для тенанта.
- На виртуальные машины тенанта устанавливается Легкий агент для Linux или Легкий агент для Windows.

Указанные действия могут быть выполнены как на стороне поставщика услуг, так и на стороне тенанта после предоставления администратору тенанта параметров подключения к виртуальному Серверу администрирования.

Если установка выполняется на стороне поставщика услуг

Вы можете использовать следующие способы установки:

- Средствами OpenAPI Kaspersky Security Center автоматизировать установку приложений на виртуальные машины тенантов и перемещение виртуальных машин в группы администрирования (открыть описание методов OpenAPI Kaspersky Security Center - https://support.kaspersky.com/help/KSVLA/API/6.1/ru-RU/Examples_of_using_KSC_OpenAPI_in_KSV6.1LA.pdf).

- Удаленно устанавливать приложения на виртуальные машины с помощью мастера или задачи удаленной установки Kaspersky Security Center.
- Развертывать виртуальные машины из шаблона виртуальных машин.

  Если вы хотите использовать OpenAPI Kaspersky Security Center или средства удаленной установки Kaspersky Security Center, вам нужно подготовить для каждого тенанта инсталляционные пакеты, необходимые для установки Легкого агента и Агента администрирования Kaspersky Security Center (см. раздел "Установка Легких агентов и Агента администрирования" на стр. 89). Вы можете распространять инсталляционные пакеты на выбранные виртуальные Серверы администрирования с помощью задачи Сервера администрирования или автоматизировать распространение пакетов средствами OpenAPI Kaspersky Security Center (открыть описание методов OpenAPI Kaspersky Security Center - https://support.kaspersky.com/help/KSVLA/API/6.1/ru-RU/Examples_of_using_KSC_OpenAPI_in_KSV6.1LA.pdf).

  В свойствах пакета или в свойствах задачи удаленной установки вы можете указать группу администрирования, в которую должна попасть виртуальная машина после установки на ней Агента администрирования. Подробнее о настройке инсталляционного пакета и описание процедур развертывания см. в справке Kaspersky Security Center.

  Если вы хотите развертывать виртуальные машины из шаблона виртуальных машин, вам нужно подготовить для каждого тенанта шаблон виртуальных машин (см. раздел "Установка Легкого агента на шаблон для временных виртуальных машин" на стр. 91), на котором установлен Агент администрирования, настроенный на подключение к виртуальному Серверу администрирования тенанта, и Легкий агент. Затем вы можете развернуть виртуальные машины для тенанта из этого шаблона.

  > В ходе установки Агента администрирования на шаблон виртуальных машин рекомендуется включить оптимизацию параметров Агента администрирования для VDI.

Если установка выполняется на стороне тенанта

При наличии подготовленных администратором поставщика услуг инсталляционных пакетов или шаблона виртуальных машин установку Агента администрирования и Легкого агента на виртуальные машины тенанта может выполнять администратор тенанта.

Регистрация виртуальных машин тенанта

На этом этапе развертывания структуры защиты тенанта выполняется регистрация виртуальных машин тенанта. Процедура автоматизирована средствами REST API Сервера интеграции (см. раздел "Регистрация виртуальных машин тенанта" на стр. 215).

В запросе к REST API вам нужно передать идентификатор (BIOS ID) виртуальной машины и идентификатор тенанта, которому принадлежит виртуальная машина.

В результате выполнения процедуры в базу данных Сервера интеграции добавляется информация о виртуальной машине и устанавливается связь между виртуальной машиной и тенантом.

Активация тенанта

На этом этапе развертывания структуры защиты тенанта выполняется процедура активации тенанта. тенанты регистрируются в базе данных Сервера интеграции со статусом "неактивный". Пока тенант имеет этот статус, Легкие агенты, установленные на виртуальных машинах тенанта, не получают информацию об

SVM, к которым доступно подключение, защита виртуальных машин тенанта выключена. Чтобы начать защищать виртуальные машины тенанта, вам нужно активировать тенанта.

Процедура активации тенанта автоматизирована средствами REST API Сервера интеграции (см. раздел "Активация тенанта" на стр. 214).

В результате выполнения процедуры выполняются следующие действия:

- Статус тенанта изменяется на "активный". Статус тенанта сохраняется в базе данных Сервера интеграции. Вы можете получать информацию о статусе тенанта средствами REST API Сервера интеграции или при просмотре списка тенантов в Консоли Сервера интеграции (см. раздел "Получение информации о тенантах" на стр. 203).
- Легкие агенты, установленные на виртуальных машинах тенанта, получают от Сервера интеграции информацию об SVM, доступных для подключения. Легкие агенты выбирают оптимальную для подключения SVM в соответствии с настроенными параметрами подключения к SVM, защита виртуальных машин тенанта включается.

Регистрация существующих тенантов и их виртуальных машин

Если структура защиты тенантов настроена без использования REST API Сервера интеграции, для получения отчетов о защите тенантов вам нужно добавить информацию о тенантах и их виртуальных машинах в базу данных Сервера интеграции.

Регистрация существующего тенанта и его виртуальных машин в базе данных Сервера интеграции состоит из следующих этапов:

1. Создание тенанта в базе данных Сервера интеграции.

   Процедура создания тенантов автоматизирована средствами REST API Сервера интеграции (см. раздел "Создание тенанта" на стр. 212).

   Действия, выполняемые в результате запроса к REST API, зависят от типа тенанта, который вы указываете при вызове метода REST API. Чтобы внести данные о тенанте в базу данных Сервера интеграции без создания структуры защиты тенанта, вам нужно указать тип тенанта "упрощенный".

   В запросе к REST API вам нужно передать следующие сведения:

   - Название тенанта.
   - Тип тенанта: упрощенный.

   В результате выполнения процедуры в базе данных Сервера интеграции сохраняются данные о тенанте; тенанту присваивается идентификатор.

2. Регистрация виртуальных машин тенанта в базе данных Сервера интеграции.

   Процедура регистрации виртуальных машин автоматизирована средствами REST API Сервера интеграции (см. раздел "Регистрация виртуальных машин тенанта" на стр. 215).

   В запросе к REST API нужно передать идентификатор (BIOS ID) каждой виртуальной машины и идентификатор тенанта, которому принадлежат виртуальные машины.

   В результате выполнения процедуры в базе данных Сервера интеграции сохраняются данные о виртуальных машинах тенанта.

3. Активация тенанта.

Процедура активации тенанта автоматизирована средствами REST API Сервера интеграции (см. раздел "Активация тенанта" на стр. 214).

После активации статус тенанта сохраняется в базе данных Сервера интеграции. Вы можете получать информацию о статусе тенанта средствами REST API Сервера интеграции или при просмотре списка тенантов в Консоли Сервера интеграции (см. раздел "Получение информации о тенантах" на стр. 203).

В случае тенанта типа "упрощенный" статус ("активный" или "неактивный") не влияет на состояние защиты виртуальных машин тенанта.

Включение и выключение защиты тенантов

Тенанты, зарегистрированные в базе данных Сервера интеграции, могут находиться в статусе "активный" или "неактивный". По умолчанию статус тенанта "неактивный".

Для тенантов типа "полный" статус тенанта определяет состояние защиты виртуальных машин тенанта:

- Если тенант имеет статус "активный", Сервер интеграции передает Легким агентам, установленным на виртуальных машинах тенанта, список SVM, доступных для подключения. Легкие агенты выбирают оптимальную для подключения SVM в соответствии с настроенными параметрами подключения к SVM, и подключаются к ней. Защита виртуальных машин тенанта включена.
- Если тенант имеет статус "неактивный", Сервер интеграции передает Легким агентам, установленным на виртуальных машинах тенанта, адрес несуществующей SVM. Это означает, что Легкие агенты не смогут подключиться ни к одной SVM. Защита виртуальных машин тенанта выключена.

Чтобы включить защиту виртуальных машин тенанта типа "полный", вам нужно активировать тенанта. Если вы хотите выключить защиту виртуальных машин тенанта типа "полный" (приостановить предоставление услуг защиты тенанту), вы можете деактивировать тенанта.

После деактивации тенанта на Сервере администрирования Kaspersky Security Center регистрируются события от Легких агентов, установленных на виртуальных машинах тенанта: однократно регистрируется событие об отсутствии доступных для подключения SVM и каждые 2 часа регистрируются события о том, что невозможно выполнить задачу обновления на защищенной виртуальной машине.

Чтобы избежать несанкционированного использования программы, после деактивации тенанта рекомендуется запретить сетевые подключения из подсети деактивированного тенанта в подсеть с SVM на TCP-порты 80, 9876, 9877, 11111, 11112 (см. раздел "Настройка используемых портов" на стр. 35).

Для тенанта типа "упрощенный" статус не влияет на состояние защиты виртуальных машин.

Процедуры активации (см. раздел "Активация тенанта" на стр. 214) и деактивации (см. раздел "Деактивация тенанта" на стр. 215) тенантов автоматизированы средствами REST API Сервера интеграции.

kaspersky

Получение информации о тенантах

В Kaspersky Security реализованы следующие способы получения информации о тенантах:

- просмотр списка тенантов в Веб-консоли Сервера интеграции или в Консоли Сервера интеграции;
- получение списка тенантов (см. раздел "Получение списка тенантов" на стр. 211), списка виртуальных машин тенанта (см. раздел "Получение списка виртуальных машин тенанта" на стр. 211) и информации о тенанте (см. раздел "Получение информации о тенанте" на стр. 210) средствами REST API Сервера интеграции.

Как посмотреть информацию о тенантах в Веб-консоли Сервера интеграции

► *Чтобы посмотреть информацию о тенантах:*

1. Откройте Веб-консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Веб-консоль Сервера интеграции" на стр. 64).
2. Перейдите в раздел **Режим мультитенантности**.

   В открывшемся окне в блоке **Список тенантов** в виде таблицы отображается список всех тенантов, зарегистрированных в базе данных Сервера интеграции.

   В таблице содержится следующая информация о каждом тенанте:

   - Статус тенанта в базе данных Сервера интеграции. Для тенантов типа "полный" статус определяет состояние защиты виртуальных машин тенанта:
     - если тенант имеет статус "активный", защита виртуальных машин тенанта включена;
     - если тенант имеет статус "неактивный", защита виртуальных машин тенанта выключена.

     Для тенантов типа "упрощенный" статус не влияет на состояние защиты виртуальных машин.
   - Название тенанта.
   - Тип тенанта: **Полный** или **Упрощенный**.
   - Идентификатор тенанта.
   - Идентификатор виртуального Сервера администрирования, настроенного для тенанта.
   - Имя учетной записи, под которой администратор тенанта подключается к виртуальному Серверу администрирования, настроенному для тенанта (только для тенанта типа "полный").

   Вы можете сортировать список по столбцам **Статус**, **Имя** и **Тип**, а также выполнять поиск по списку.
3. Чтобы посмотреть список виртуальных машин выбранного тенанта, нажмите на название тенанта в списке. В открывшемся окне отображается информация о тенанте, которая содержится в списке тенантов, а также список виртуальных машин тенанта в виде таблицы. В таблице содержится следующая информация о каждой виртуальной машине:
   - Идентификатор (BIOS ID) виртуальной машины.
   - Имя виртуальной машины.

Как посмотреть информацию о тенантах в Консоли Сервера интеграции

► *Чтобы посмотреть информацию о тенантах:*

1. Откройте Консоль Сервера интеграции и подключитесь к Серверу интеграции (см. раздел "Подключение к Серверу интеграции через Консоль Сервера интеграции" на стр. 65).
2. В списке слева выберите раздел **Список тенантов**.

   В правой части окна в виде таблицы отображается список всех тенантов, зарегистрированных в базе данных Сервера интеграции.

В списке отображается следующая информация о каждом тенанте:

- **Статус** – статус тенанта в базе данных Сервера интеграции. Статус обозначается значком:
  -  – тенант находится в статусе "активный".
  -  – тенант находится в статусе "неактивный".

  Для тенантов типа "полный" статус определяет состояние защиты виртуальных машин тенанта:
  - если тенант имеет статус "активный", защита виртуальных машин тенанта включена;
  - если тенант имеет статус "неактивный", защита виртуальных машин тенанта выключена.

  Для тенантов типа "упрощенный" статус не влияет на состояние защиты виртуальных машин.
- **Сведения о тенанте и его виртуальных машинах**:
  - название тенанта;
  - тип тенанта: **Полный** или **Упрощенный**;
  - идентификатор тенанта;
  - для тенанта типа "полный": идентификатор виртуального Сервера администрирования, настроенного для тенанта;
  - список идентификаторов (BIOS ID) или имен виртуальных машин тенанта.
- **Учетная запись администратора** – имя учетной записи, под которой администратор тенанта типа "полный" подключается к виртуальному Серверу администрирования, настроенному для тенанта. В списке отображается имя учетной записи, указанное при создании тенанта, даже если впоследствии имя было изменено.

Вы можете обновлять список тенантов с помощью ссылки **Обновить**, расположенной над таблицей.

Получение отчетов о защите тенантов

Виртуальная машина считается защищенной, когда установленный на ней Легкий агент подключен к SVM. Каждая SVM может собирать данные о периодах времени, когда Легкие агенты были подключены к SVM, и передавать эти данные в базу данных Сервера интеграции. На основе этой информации средствами REST API Сервера интеграции можно получать отчеты о защите виртуальных машин тенантов.

С помощью отчета о защите тенантов вы можете получать информацию обо всех защищаемых виртуальных машинах тенанта с указанием всех периодов времени, когда каждая виртуальная машина находилась под защитой Kaspersky Security. Также с помощью отчета вы можете получать информацию о защите всех виртуальных машин, которые подключались к SVM за указанный отчетный период, в том числе виртуальных машин, которые не принадлежат ни одному тенанту.

Получение отчетов о защите тенантов состоит из следующих этапов:

1. Включение функции передачи данных для отчетов (на стр. 205) в базу данных Сервера интеграции.
2. Формирование отчета (см. раздел "Формирование отчета о защите тенантов" на стр. 206). Отчет формируется в виде файла формата CSV во временной папке.
3. Выгрузка отчета (см. раздел "Выгрузка отчета о защите тенантов" на стр. 207). Сформированный отчет может быть выгружен целиком или по частям для интеграции в систему отчетов поставщика услуг.

В этом разделе

Включение функции передачи данных для отчетов

По умолчанию функция передачи данных для отчетов выключена на Сервере интеграции. Если вы хотите получать отчеты о защите тенантов, вам нужно включить функцию получения данных для отчетов в конфигурационном файле Сервера интеграции appsettings.json. В зависимости от версии Сервера интеграции файл расположен по следующему пути:

- /var/opt/kaspersky/viis/common/ – файл Сервера интеграции на базе Linux.
- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ – файл Сервера интеграции на базе Windows.

► *Чтобы включить функцию получения данных для отчетов:*

1. Откройте на редактирование конфигурационный файл appsettings.json.
2. В секции `Multitenancy` установите для параметра `EnableProtectionReports` значение `true` и сохраните файл.
3. Перезапустите Сервер интеграции.

Сервер интеграции будет получать от каждой SVM данные о периодах подключения Легких агентов к SVM.

Если функция получения данных включена, но подключение SVM к Серверу интеграции отсутствует, пакеты данных помещаются в очередь на отправку. После достижения максимального числа пакетов в очереди более старые пакеты данных удаляются. Параметры отправки данных задаются в конфигурационном файле /etc/opt/kaspersky/agents_monitor/agents_monitor.conf на SVM. Вы можете настраивать максимальный размер очереди пакетов на отправку с помощью параметра `max_queue_size`.

Полученные данные сохраняются в базе данных Сервера интеграции. Срок хранения данных для отчетов по умолчанию составляет 460 дней. Вы можете настраивать это значение с помощью параметра `ProtectionPeriodsRecordsLifetimeDays` в секции `Multitenancy` в конфигурационном файле Сервера интеграции appsettings.json.

Размер базы данных Сервера интеграции увеличивается пропорционально числу защищаемых виртуальных машин тенантов.

Формирование отчета о защите тенантов

Процедура формирования отчета автоматизирована средствами REST API Сервера интеграции (см. раздел "Формирование отчета" на стр. 218).

В запросе к REST API вы можете передавать следующие параметры формирования отчета:

- идентификатор тенанта, о защите которого вы хотите получить отчет;
- дата и время начала периода, за который вы хотите получить отчет;
- дата и время окончания периода, за который вы хотите получить отчет.

Если в запросе не указан идентификатор тенанта, отчет будет включать в себя данные обо всех виртуальных машинах, которые находились под защитой в указанный период. В том числе, о виртуальных машинах, которые не принадлежат тенантам.

Если в запросе не указан период формирования отчета, в отчет войдут данные с самой ранней из дат, зафиксированных в базе данных Сервера интеграции, и до текущего момента.

Для получения достоверной информации в отчетах при формировании отчетного периода рекомендуется следовать правилам:

- задавать отчетный период с точностью до дня;
- устанавливать окончание отчетного периода не менее чем через 60 минут от текущего момента.

В результате выполнения процедуры формирования отчета возвращается идентификатор отчета. В зависимости от версии Сервера интеграции отчет сохраняется по следующему пути:

- /var/opt/kaspersky/viis/common/reports – защищенная служебная директория Сервера интеграции на базе Linux.
- %ProgramData%\Kaspersky Lab\VIISLA\protectionPeriodsReports – защищенная служебная папка Сервера интеграции на базе Windows.

Отчет хранится по умолчанию 24 часа с момента формирования. Чтобы получить отчет, вам нужно использовать идентификатор отчета в запросе к REST API для выгрузки отчета (см. раздел "Выгрузка отчета о защите тенантов" на стр. 207).

Вы можете настроить срок хранения отчета с помощью параметра `ProtectionPeriodsRecordsLifetimeDays` в секции `Multitenancy` в конфигурационном файле Сервера интеграции appsettings.json. В зависимости от версии Сервера интеграции файл расположен по следующему пути:

- /var/opt/kaspersky/viis/common/ – файл Сервера интеграции на базе Linux.
- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ – файл Сервера интеграции на базе Windows.

Данные в отчете представлены построчно. В каждой строке содержится информация об одном периоде защиты виртуальной машины в следующем формате:

`{идентификатор тенанта};{название тенанта};{идентификатор виртуальной машины};{имя виртуальной машины};{дата и время включения защиты};{дата и время выключения защиты}`

где:

- `{идентификатор тенанта}` – идентификатор тенанта, которому принадлежит виртуальная машина. Если виртуальная машина не принадлежит ни одному тенанту, в поле ничего не указывается.
- `{название тенанта}` – название тенанта, заданное при создании тенанта. Если виртуальная машина не принадлежит ни одному тенанту, в поле ничего не указывается.
- `{идентификатор виртуальной машины}` – идентификатор виртуальной машины, которая находилась под защитой программы.
- `{имя виртуальной машины}` – имя виртуальной машины, которая находилась под защитой программы.
- `{дата и время включения защиты}` – дата и время начала периода защиты виртуальной машины.
- `{дата и время выключения защиты}` – дата и время окончания периода защиты виртуальной машины.

Если в течение отчетного периода виртуальная машина находилась под защитой программы несколько раз (защита включалась и выключалась), то в отчете отображается каждый период защиты виртуальной машины.

Выгрузка отчета о защите тенантов

Процедура выгрузки отчета автоматизирована средствами REST API Сервера интеграции (см. раздел "Выгрузка отчета" на стр. 219).

В запросе к REST API вам нужно передать идентификатор отчета, полученный на предыдущем этапе (см. раздел "Формирование отчета о защите тенантов" на стр. 206), и формат отображения данных: CSV.

> Другие форматы отображения данных не поддерживаются.

Вы можете выгружать данные отчета полностью или получить частичные данные.

Вы можете интегрировать данные, полученные в результате выполнения запроса, в вашу систему отчетов.

kaspersky

Удаление виртуальных машин из защищаемой инфраструктуры

Для удаления виртуальной машины из защищаемой инфраструктуры тенанта типа "полный" вам нужно выполнить следующие действия:

1. Отменить регистрацию виртуальной машины в базе данных Сервера интеграции. Процедура отмены регистрации автоматизирована средствами REST API Сервера интеграции (см. раздел "Отмена регистрации виртуальной машины" на стр. 216).

   В результате выполнения процедуры информация о виртуальной машине тенанта удаляется из базы данных Сервера интеграции.

2. Удалить на виртуальной машине Агент администрирования Kaspersky Security Center, Легкий агент для Linux или Легкий агент для Windows.

   Вы можете выполнить эти действия вручную в интерфейсе Kaspersky Security Center или автоматизировать удаление средствами OpenAPI Kaspersky Security Center (открыть описание методов OpenAPI Kaspersky Security Center - https://support.kaspersky.com/help/KSVLA/API/6.1/ru-RU/Examples_of_using_KSC_OpenAPI_in_KSV6.1LA.pdf).

3. Удалить виртуальную машину из списка управляемых устройств тенанта. Вы можете переместить виртуальную машину в папку **Нераспределенные устройства** главного Сервера администрирования Kaspersky Security Center или удалить виртуальную машину из Kaspersky Security Center.

   Вы можете выполнить эти действия вручную в интерфейсе Kaspersky Security Center или автоматизировать удаление виртуальных машин из списка управляемых устройств средствами OpenAPI Kaspersky Security Center (открыть описание методов OpenAPI Kaspersky Security Center - https://support.kaspersky.com/help/KSVLA/API/6.1/ru-RU/Examples_of_using_KSC_OpenAPI_in_KSV6.1LA.pdf).

Если виртуальная машина удалена из защищаемой инфраструктуры тенанта типа "упрощенный", вам нужно отменить регистрацию виртуальной машины в базе данных Сервера интеграции (см. раздел "Отмена регистрации виртуальной машины" на стр. 216).

Удаление тенантов

Если вы хотите прекратить предоставление услуг тенанту типа "полный", вам нужно удалить тенанта. Для этого нужно выполнить следующие действия:

1. Удалить на виртуальной машине Агент администрирования Kaspersky Security Center, Легкий агент для Linux или Легкий агент для Windows.

   Вы можете выполнить эти действия вручную в интерфейсе Kaspersky Security Center или автоматизировать удаление средствами OpenAPI Kaspersky Security Center (открыть описание методов OpenAPI Kaspersky Security Center - https://support.kaspersky.com/help/KSVLA/API/6.1/ru-RU/Examples_of_using_KSC_OpenAPI_in_KSV6.1LA.pdf).

2. Удалить тенанта из базы данных Сервера интеграции, а также удалить структуру защиты тенанта. Процедура удаления автоматизирована средствами REST API Сервера интеграции (см. раздел "Удаление тенанта" на стр. 217). При вызове метода REST API вам нужно указать параметр `removeTenantArtifacts=true`.

   В результате выполнения процедуры автоматически выполняются следующие действия:

- Удаляется информация о тенанте и виртуальных машинах тенанта из базы данных Сервера интеграции.
- Удаляется структура защиты тенанта в Kaspersky Security Center: виртуальный Сервер администрирования и учетная запись для подключения к нему, папка **Multitenancy KSV LA** → **<Название тенанта>** и ее содержимое (вложенные папки и группы администрирования, политики и задачи, инсталляционные пакеты).
- Если других тенантов нет, также удаляется папка **Multitenancy KSV LA**.

Если прекращено предоставление услуг защиты тенанту типа "упрощенный", вам нужно удалить тенанта из базы данных Сервера интеграции (см. раздел "Удаление тенанта" на стр. 217).

Использование REST API Сервера интеграции в сценариях мультитенантности

Взаимодействие с REST API Сервера интеграции основано на запросах и ответах и осуществляется по протоколу HTTPS под учетной записью `multitenancy`.

Параметры учетной записи передаются при вызове каждого метода в заголовке запроса Authorization в виде строки `{имя пользователя}:{пароль}`, закодированной методом Base64. Используется аутентификация типа Basic.

Адрес запроса к REST API Сервера интеграции состоит из следующих частей:

`https://{адрес Сервера интеграции}:{порт Сервера интеграции}/{метод}?{параметры}`

где:

- `{адрес Сервера интеграции}` – IP-адрес или полное доменное имя (FQDN) Сервера интеграции.
- `{порт Сервера интеграции}` – порт для подключения к Серверу интеграции (по умолчанию 7271).
- `{метод}` – метод, который нужно вызвать.
- `{параметры}` – параметры метода, если есть.

Для обработки запросов, которые требуют много времени и выполняются асинхронно, используются задачи (см. раздел "Методы для работы с задачами" на стр. 220) (*tasks*). Задача создается как промежуточный результат выполнения запроса.

В этом разделе

Методы для работы с тенантами

Средствами REST API Сервера интеграции вы можете выполнять следующие действия при работе с тенантами и виртуальными машинами тенантов:

- получать информацию о тенанте;
- получать список тенантов;
- получать список виртуальных машин тенантов;
- создавать нового тенанта и структуру защиты для него или регистрировать существующего тенанта;
- удалять тенанта;
- активировать и деактивировать тенанта;
- регистрировать виртуальные машины тенанта и отменять их регистрацию.

Набор действий, выполняемых в результате некоторых запросов к REST API, зависит от признака *тип тенанта*, который вы указываете при добавлении информации о тенанте в базу данных Сервера интеграции. Развертывание и удаление структуры защиты тенантов средствами REST API Сервера интеграции доступно для тенантов типа "полный". Для тенантов типа "упрощенный" автоматизируется только функция получения отчетов.

В этом разделе

Получение информации о тенанте

Позволяет получить информацию о тенанте из базы данных Сервера интеграции.

Метод:

```
GET /api/2.0/virtualization/tenants/{идентификатор тенанта}
```

где:

`{идентификатор тенанта}` – идентификатор тенанта в базе данных Сервера интеграции (обязательный параметр).

В случае успешного выполнения запроса REST API возвращает сведения о тенанте в следующем виде:

```
<tenant id="{идентификатор}" created="{дата и время}" updated="{дата и время}">
   <name>{название}</name>
   <description>{описание}</description>
   <userData><![CDATA[{дополнительные сведения}]]></userData>
   <!-- Информация в секции vKsc доступна только для тенанта типа "полный" -->
      <vKsc id="{идентификатор}">
         <user>
            <name>{администратор}</name>
```

```
          </user>
        </vKsc>
    <status>{статус}</status>
    <type>{тип тенанта}</type>
</tenant>
```

где:

- `tenant id="{идентификатор}"` – идентификатор тенанта в базе данных Сервера интеграции.
- `created="{дата и время}"` – дата и время регистрации тенанта в базе данных Сервера интеграции в формате YYYY-MM-DDThh:mm:ss.
- `updated="{дата и время}"` – дата и время обновления сведений о тенанте в базе данных в формате YYYY-MM-DDThh:mm:ss.
- `{название}` – название тенанта, указанное при создании тенанта.
- `{описание}` – описание тенанта.
- `{дополнительные сведения}` – дополнительная информация о тенанте, внесенная в базу данных Сервера интеграции.
- `vKsc id="{идентификатор}"` – идентификатор, назначенный виртуальному Серверу администрирования тенанта в Kaspersky Security Center.
- `{администратор}` – имя администратора виртуального Сервера администрирования тенанта.
- `{статус}` – текущий статус тенанта: "активный" (`Active`) или "неактивный" (`Inactive`).
- `{тип тенанта}` – тип тенанта: "полный" (`Complete`) или "упрощенный" (`Simple`).

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращаются сведения о тенанте.
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found) VIRMT_TenantWithSpecifiedIdNotFound` – тенант с указанным идентификатором не найден в базе данных Сервера интеграции.

Получение списка тенантов

Позволяет получить список всех тенантов, сведения о которых содержатся в базе данных Сервера интеграции, и сведения о каждом тенанте.

Метод:

```
GET /api/2.0/virtualization/tenants
```

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращаются в виде списка сведения (см. раздел "Получение информации о тенанте" на стр. 210) обо всех тенантах.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Получение списка виртуальных машин тенанта

Позволяет получить список всех зарегистрированных виртуальных машин тенанта.

Метод:

```
GET /api/2.0/virtualization/tenants/{идентификатор тенанта}/vms
```

где:

`{идентификатор тенанта}` – идентификатор тенанта в базе данных Сервера интеграции (обязательный параметр).

В случае успешного выполнения запроса REST API возвращает список виртуальных машин и сведения о каждой виртуальной машине тенанта в следующем виде:

```
<vm id="{идентификатор в базе}" biosId={идентификатор BIOS ID} created="{дата и время}" updated="{дата и время}">
   <name>{имя}</name>
   <userData><![CDATA[{дополнительные сведения}]]></userData>
</vm>
```

где:

- `{идентификатор в базе}` – идентификатор, назначенный виртуальной машине в базе данных Сервера интеграции.
- `{идентификатор BIOS ID}` – идентификатор виртуальной машины (BIOS ID) в формате UUID.
- `created="{дата и время}"` – дата и время регистрации виртуальной машины в базе данных Сервера интеграции в формате YYYY-MM-DDThh:mm:ss.
- `updated="{дата и время}"` – дата и время обновления сведений о виртуально машине в базе данных в формате YYYY-MM-DDThh:mm:ss.
- `{имя}` – имя виртуальной машины.
- `{дополнительные сведения}` – дополнительная информация о виртуальной машине, внесенная в базу данных Сервера интеграции.

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращается список виртуальных машин тенанта.
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found) VIRMT_TenantWithSpecifiedIdNotFound` – тенант с указанным идентификатором не найден в базе данных Сервера интеграции.

Создание тенанта

В зависимости от типа тенанта, который вы указываете при вызове метода REST API, позволяет выполнить следующие действия:

- Для тенанта типа "полный":
  - Добавить сведения о тенанте в базу данных Сервера интеграции.
  - Создать структуру защиты тенанта в Kaspersky Security Center (виртуальный Сервер администрирования, учетную запись для подключения к нему, структуру папок и групп администрирования).
  - Добавить сведения о виртуальном Сервере администрирования тенанта в базу данных Сервера интеграции.
- Для тенанта типа "упрощенный": добавить сведения о тенанте в базу данных Сервера интеграции.

Метод:

```
POST /api/2.0/virtualization/tenants
```

В теле запроса вам нужно указать следующие параметры:

```
<tenant>
   <name>{название}</name>
   <description>{описание}</description>
   <userData><![CDATA[{дополнительные сведения}]]></userData>
   <preferredViisAddress>{IP-адрес}</preferredViisAddress>
   <type>{тип тенанта}</type>
   <!-- Данные в секции vKsc указываются только для тенанта типа "полный" -->
      <vKsc>
         <user>
            <name>{имя администратора}</name>
            <password>{пароль администратора}</password>
         </user>
      </vKsc>
</tenant>
```

где:

- `{название}` – название тенанта (обязательный параметр).
- `{описание}` – описание тенанта (необязательный параметр).
- `{дополнительные сведения}` – дополнительная информация о тенанте (необязательный параметр).
- `{IP-адрес}` – IP-адрес Сервера интеграции, к которому должны подключаться Легкие агенты, установленные на виртуальных машинах тенанта (необязательный параметр). Указанный адрес используется по умолчанию при создании политики для Легкого агента. Если параметр не указан, в политике используется IP-адрес Сервера интеграции из запроса к REST API.
- `{тип тенанта}` – тип тенанта: "полный" (`Complete`) или "упрощенный" (`Simple`) (обязательный параметр).
- `{имя администратора}` – имя учетной записи администратора для подключения к виртуальному Серверу администрирования тенанта (обязательный параметр при создании тенанта типа "полный"). Учетная запись будет создана автоматически во время выполнения процедуры.
- `{пароль администратора}` – пароль учетной записи администратора, закодированный методом Base64 (обязательный параметр при создании тенанта типа "полный").

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **CreateTenant**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 220) вы можете следить за ходом выполнения процедуры создания тенанта. После завершения задачи в поле **result** содержится информация о тенанте, в том числе идентификатор созданного тенанта, или сведения об ошибке. В случае ошибки на любом из шагов выполнения процедуры выполняется откат всех внесенных изменений.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа **CreateTenant**.
- `400 (Bad request) VIRMT_MandatoryParameterIsNotSpecified` – в теле запроса не указан один из обязательных параметров, например название тенанта.

- `400 (Bad request) VIRMT_InvalidTenantType` – в теле запроса указан неверный тип тенанта, указанный тип не существует.
- `400 (Bad request) VIRMT_VKscCredentialsNotSpecified` – не указаны имя или пароль учетной записи администратора виртуального Сервера администрирования Kaspersky Security Center (при создании тенанта типа "полный").
- `400 (Bad request) VIRMT_InvalidViisAddressFormat` – неверный формат IP-адреса Сервера интеграции.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Возможные коды ошибок в задаче:

- `KSC_ServiceNotConfigured` – не заданы параметры подключения к Kaspersky Security Center.
- `VIRMT_TenantGroupAlreadyExists` – папка с названием, соответствующим указанному названию тенанта, уже существует в Kaspersky Security Center.
- `VIRMT_TenantWithSpecifiedNameAlreadyExists` – тенант с указанным названием уже существует в базе данных Сервера интеграции.
- `VIRMT_PasswordNotComplyPolicy` – не удалось создать учетную запись администратора виртуального Сервера администрирования Kaspersky Security Center: указанный пароль не удовлетворяет требованиям к паролям в Kaspersky Security Center.
- `VIRMT_UserWithSpecifiedNameAlreadyExists` – не удалось создать учетную запись администратора виртуального Сервера администрирования Kaspersky Security Center: пользователь с таким именем уже существует в Kaspersky Security Center.

Активация тенанта

Позволяет изменить статус тенанта на "активный".

Метод:

```
POST /api/2.0/virtualization/tenants/{идентификатор тенанта}/activate
```

где:

`{идентификатор тенанта}` – идентификатор тенанта в базе данных Сервера интеграции (обязательный параметр).

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **ChangeTenantActivation**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 220) вы можете следить за ходом выполнения процедуры изменения статуса тенанта. После завершения задачи в поле **result** содержится подтверждение изменения статуса тенанта (`true`) или сведения об ошибке.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа **ChangeTenantActivation**.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Коды ошибок в задаче:

- `VIRMT_TenantWithSpecifiedIdNotFound` – тенант с указанным идентификатором не найден в базе данных Сервера интеграции.

- `KSC_ServiceNotConfigured` – не заданы параметры подключения к Kaspersky Security Center.

Деактивация тенанта

Позволяет изменить статус тенанта на "неактивный".

Метод:

```
POST /api/2.0/virtualization/tenants/{идентификатор тенанта}/deactivate
```

где:

`{идентификатор тенанта}` – идентификатор тенанта в базе данных Сервера интеграции (обязательный параметр).

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **ChangeTenantActivation**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 220) вы можете следить за ходом выполнения процедуры изменения статуса тенанта. После завершения задачи в поле **result** содержится подтверждение изменения статуса тенанта (`true`) или сведения об ошибке.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа **ChangeTenantActivation**.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Коды ошибок в задаче:

- `VIRMT_TenantWithSpecifiedIdNotFound` – тенант с указанным идентификатором не найден в базе данных Сервера интеграции.
- `KSC_ServiceNotConfigured` – не заданы параметры подключения к Kaspersky Security Center.

Регистрация виртуальных машин тенанта

Позволяет добавить информацию о виртуальных машинах тенантов в базу данных Сервера интеграции.

Метод:

```
POST /api/2.0/virtualization/tenants/{идентификатор тенанта}/vms/register
```

где:

`{идентификатор тенанта}` – идентификатор тенанта в базе данных Сервера интеграции (обязательный параметр).

В теле запроса нужно указать следующие параметры:

```
<vm biosId="{идентификатор BIOS ID}">
   <name>{имя}</name>
   <userData><![CDATA[{дополнительные сведения}]]></userData>
</vm>
```

где:

- `{идентификатор BIOS ID}` – уникальный идентификатор (BIOS ID) виртуальной машины (обязательный параметр).
- `{имя}` – имя виртуальной машины (необязательный параметр).

- {дополнительные сведения} – дополнительная информация о виртуальной машине (необязательный параметр).

Коды возврата:

- 200 (OK) – запрос выполнен успешно (информация о виртуальной машине добавлена в базу данных Сервера интеграции).
- 403 (Forbidden) – доступ к ресурсу запрещен.
- 404 (Not Found) VIRMT_TenantWithSpecifiedIdNotFound – тенант с указанным идентификатором не найден в базе данных Сервера интеграции.
- 409 (Conflict) VIRMT_VmWithSpecifiedBiosIdAlreadyExists – виртуальная машина с указанным идентификатором уже зарегистрирована в базе данных Сервера интеграции.

Отмена регистрации виртуальной машины

Позволяет удалить информацию о виртуальной машине тенанта из базы данных Сервера интеграции.

> Отмена регистрации не приводит к выключению защиты на виртуальной машине тенанта. Вы можете выключить защиту на виртуальной машине тенанта типа "полный", выполнив все этапы процедуры удаления виртуальных машин из защищаемой инфраструктуры (см. раздел "Удаление виртуальных машин из защищаемой инфраструктуры" на стр. 208).

Метод:

```
POST /api/2.0/virtualization/tenants/{идентификатор тенанта}/vms/unregister?biosId={идентификатор}
```

или

```
POST /api/2.0/virtualization/tenants/{идентификатор тенанта}/vms/unregister?vmId={идентификатор}
```

где:

- {идентификатор тенанта} – идентификатор тенанта в базе данных Сервера интеграции (обязательный параметр).
- biosId={идентификатор} – идентификатор виртуальной машины (BIOS ID) в формате UUID (обязательный параметр).
- vmId={идентификатор} – идентификатор виртуальной машины в базе данных Сервера интеграции в формате UUID (обязательный параметр).

Коды возврата:

- 200 (OK) – запрос выполнен успешно (информация о виртуальной машине удалена из базы данных Сервера интеграции).
- 403 (Forbidden) – доступ к ресурсу запрещен.
- 404 (Not Found) VIRMT_TenantWithSpecifiedIdNotFound – тенант с указанным идентификатором не найден в базе данных Сервера интеграции.

- `404 (Not Found) VIRMT_VmWithSpecifiedIdNotFound` – виртуальная машина с указанным идентификатором не найдена в базе данных Сервера интеграции.

Удаление тенанта

В зависимости от типа тенанта и заданных параметров, позволяет выполнить следующие действия:

- Для тенанта типа "полный":
  - Удалить информацию о тенанте и виртуальных машинах тенанта из базы данных Сервера интеграции.
  - Удалить структуру защиты тенанта в Kaspersky Security Center (виртуальный Сервер администрирования, учетную запись для подключения к нему, структуру папок и групп администрирования, политики, задачи и инсталляционные пакеты). Если других тенантов нет, также удаляется папка **Multitenancy KSV LA**.
  - Удалить сведения о виртуальном Сервере администрирования тенанта из базы данных Сервера интеграции.

  > Вызов метода удаления тенанта не приводит к выключению защиты на виртуальных машинах тенанта. Чтобы выключить защиту, вам нужно выполнить все этапы процедуры удаления тенанта (см. раздел "Удаление тенантов" на стр. 208), в том числе удалить на виртуальных машинах Легкий агент для Windows, Легкий агент для Linux и Агент администрирования Kaspersky Security Center. Если вы хотите приостановить защиту виртуальных машин тенанта типа "полный", вы можете использовать метод деактивации тенанта (см. раздел "Деактивация тенанта" на стр. 215).

- Для тенанта типа "упрощенный": удалить тенанта из базы данных Сервера интеграции.

Метод:

```
DELETE /api/2.0/virtualization/tenants/{идентификатор тенанта}?removeTenantArtifacts={true|false}
```

где:

- `{идентификатор тенанта}` – идентификатор тенанта в базе данных Сервера интеграции (обязательный параметр).
- `removeTenantArtifacts={true|false}` – необязательный параметр, определяющий необходимость удаления структуры защиты тенанта при удалении тенанта из базы данных Сервера интеграции. Возможные значения:
  - `true` – при удалении тенанта будут также выполнены следующие действия:
    - удаление виртуального Сервера администрирования тенанта;
    - удаление учетной записи администратора виртуального Сервера администрирования тенанта;
    - удаление папки **Multitenancy KSV LA** → **<Название тенанта>** и ее содержимого;
    - если других тенантов нет, удаление папки **Multitenancy KSV LA**.
  - `false` – выполняется только удаление тенанта из базы данных Сервера интеграции, структура защиты тенанта не удаляется.

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **DeleteTenant**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 220) вы можете следить за ходом выполнения процедуры удаления тенанта. После завершения задачи в поле **result** содержится информация об удаленном тенанте или сведения об ошибке.

В случае ошибки на любом из шагов выполнения процедуры выполняется откат всех внесенных изменений.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа DeleteTenant.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Коды ошибок в задаче:

- `VIRMT_TenantWithSpecifiedIdNotFound` – тенант с указанным идентификатором не найден в базе данных Сервера интеграции.
- `KSC_ServiceNotConfigured` – не заданы параметры подключения к Kaspersky Security Center.

Методы для работы с отчетами

Средствами REST API Сервера интеграции вы можете выполнять следующие действия при работе с отчетами о защите тенантов:

- формировать отчет;
- выгружать отчет.

В этом разделе

Формирование отчета

Позволяет сформировать отчет на основе данных, переданных в базу данных Сервера интеграции, с учетом заданных параметров отчета. Вы можете указать тенанта, о защите которого нужно сформировать отчет, и период, данные за который вы хотите получить.

В заголовке запроса `Accept` нужно передать формат вывода данных в виде `Accept:application/csv`.

Метод:

```
POST /api/2.0/virtualization/reports/tenants?tenantId={идентификатор тенанта}&from={дата и время}&to={дата и время}
```

где:

- `tenantId={идентификатор тенанта}` – идентификатор тенанта в базе данных Сервера интеграции. Если тенант указан, в отчет попадают только сведения о периодах защиты виртуальных машин этого тенанта. Если тенант не указан, отчет будет включать в себя данные обо всех виртуальных машинах, которые находились под защитой в указанный период.

- `from={дата и время}` – дата и время начала отчетного периода в формате YYYY-MM-DDThh:mm:ss. Если не задано, то используется дата самой ранней записи в базе данных Сервера интеграции.
- `to={дата и время}` – дата и время окончания отчетного периода в формате YYYY-MM-DDThh:mm:ss. Если не задано, то используется текущая дата.

Запрос выполняется асинхронно, REST API возвращает идентификатор задачи с типом **CreateTenantReport**. С помощью задачи (см. раздел "Методы для работы с задачами" на стр. 220) вы можете следить за ходом выполнения процедуры формирования отчета. После завершения задачи в поле **result** содержится идентификатор отчета или сведения об ошибке.

Коды возврата:

- `202 (Accepted)` – запрос принят к исполнению. В ответе возвращается идентификатор задачи типа **CreateTenantReport**.
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found)` – тенант с указанным идентификатором не найден в базе данных Сервера интеграции.

Выгрузка отчета

Позволяет выгрузить отчет, сформированный ранее.

В заголовке запроса `Accept` нужно передать формат вывода данных в виде `Accept: application/csv`.

Поддерживается выгрузка отчета по частям. Вы можете указать диапазон данных в заголовке запроса `Range`, например:

```
Range: bytes=0-1023
```

В ответ на запрос с таким заголовком REST API возвращает результат `206 (Partial content)` и первый килобайт данных. В ответе присутствуют заголовки `Content-Range` и `Content-Length`.

Например:

```
Content-Range: bytes=0-1023/123456
Content-Length: 1024
```

Метод:

```
GET /api/2.0/virtualization/reports/tenants/{идентификатор отчета}
```

где:

`{идентификатор отчета}` – идентификатор отчета, полученный в результате успешного завершения задачи **CreateTenantReport** (обязательный параметр).

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращаются данные отчета в формате, указанном в заголовке `Accept`.
- `206 (Partial content)` – запрос выполнен успешно. В ответе возвращается часть отчета, заданная заголовком `Range`.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

- `404 (Not Found)` – отчет с указанным идентификатором не найден.
- `415 (Unsupported Media Type)` – неподдерживаемый формат запрашиваемых данных (в заголовке запроса `Accept` передан неверный формат).

Методы для работы с задачами

Задачи используются для обработки запросов, которые требуют много времени и выполняются асинхронно. С помощью состояний задачи вы можете следить за ходом выполнения действий, заданных в запросе.

Задача может находиться в одном из следующих состояний:

- **Created** – задача создана, но не запущена.
- **Starting** – задача находится в процессе запуска.
- **Running** – задача выполняется. Для задачи в этом состоянии указывается прогресс (**progress**) выполнения в процентах.
- **Completed** – задача успешно завершена. Для задачи в этом состоянии указывается результат выполнения (**result**). Результат содержит зависимые от задачи данные, например идентификатор нового тенанта после выполнения задачи **CreateTenant**.
- **Stopping** – задача подготавливается к завершению. Если вы прекратили выполнение задачи, она может находиться в этом состоянии, прежде чем перейти в состояние **Cancelled**.
- **Failed** – задача завершилась с ошибкой. Для задачи в этом состоянии указывается расширенная информация об ошибке (**error**).
- **Cancelled** – выполнение задачи прекращено пользователем или системой. Для задачи в этом состоянии указывается расширенная информация об ошибке (**error**).
- **Queued** – задача поставлена в очередь и ожидает начала выполнения.

Средствами REST API Сервера интеграции вы можете выполнять следующие действия с задачами:

- получать список задач;
- получать сведения об указанной задаче;
- отменять выполнение указанной задачи.

В этом разделе

Получение информации о задаче

Позволяет получить информацию о задаче по ее идентификатору.

Метод:

```
GET /api/2.0/virtualization/tasks/{идентификатор}
```

где:

{идентификатор} – идентификатор задачи (обязательный параметр).

В случае успешного выполнения запроса REST API возвращает сведения о задаче в следующем виде:

```
<task id="{идентификатор}" created="{дата и время}" stateChanged="{дата и время}"
changed="{дата и время}">
   <state>{состояние}</state>
   <type>{тип}</type>
   <stage>{этап}</stage>
   <progress>{процент выполнения}</progress>
   <result>{результат}</result>
   <!-- Если задача завершилась с ошибкой вместо результата отображается сообщение
   об ошибке. -->
   <error>{сообщение об ошибке}</error>
</task>
```

где:

- {идентификатор} – идентификатор задачи.
- created="{дата и время}" – время создания задачи в формате YYYY-MM-DDThh:mm:ss.
- stateChanged="{дата и время}" – время изменения состояния задачи в формате YYYY-MM-DDThh:mm:ss.
- changed="{дата и время}" – время изменения задачи в формате YYYY-MM-DDThh:mm:ss.
- {состояние} – состояние (см. раздел "Методы для работы с задачами" на стр. 220) задачи.
- {тип} – тип задачи. Например:
  - CreateTenant – задача, которая используется в процедуре создания тенанта (см. раздел "Создание тенанта" на стр. 212).
  - ChangeTenantActivation – задача, которая используется в процедурах активации (см. раздел "Активация тенанта" на стр. 214) и деактивации (см. раздел "Деактивация тенанта" на стр. 215) тенанта.
  - DeleteTenant – задача, которая используется в процедуре удаления тенанта (см. раздел "Удаление тенанта" на стр. 217).
  - CreateTenantReport – задача, которая используется в процедуре формирования отчета (см. раздел "Формирование отчета" на стр. 218) о защите тенантов.
- {название} – название задачи.
- {этап} – этап выполнения задачи.
- {процент выполнения} – ход выполнения задачи в процентах.
- {результат} – результат выполнения задачи, например, информация о созданном тенанте или идентификатор отчета.
- {сообщение об ошибке} – если в ходе выполнения задачи произошла ошибка, отображается сообщение об ошибке.

Коды возврата:

- 200 (OK) – запрос выполнен успешно.
- 403 (Forbidden) – доступ к ресурсу запрещен.

- `404 (Not Found)` – задача с указанным идентификатором не найдена в базе данных Сервера интеграции.

Получение списка задач

Позволяет получить список всех существующих задач и информацию о каждой задаче (см. раздел "Получение информации о задаче" на стр. 220) из списка.

Метод:

```
GET /api/2.0/virtualization/tasks?createdFrom={дата и
время}&state={статус}&type={тип}
```

где:

- `createdFrom={дата и время}` – дата и время в формате YYYY-MM-DDThh:mm:ss (необязательный параметр). Если параметр задан, в списке отображаются задачи, которые созданы не раньше указанных даты и времени.
- `state={состояние}` – состояние задачи (необязательный параметр). Если параметр задан, в списке отображаются только задачи в указанном состоянии (см. раздел "Методы для работы с задачами" на стр. 220).
- `type={тип}` – тип (см. раздел "Получение информации о задаче" на стр. 220) задачи (необязательный параметр). Если параметр задан, в списке отображаются только задачи указанного типа.

Коды возврата:

- `200 (OK)` – запрос выполнен успешно. В ответе возвращается список задач.
- `403 (Forbidden)` – доступ к ресурсу запрещен.

Отмена выполнения задачи

Позволяет прекращать выполнение запущенных задач. Некоторые задачи не могут быть завершены немедленно. В этом случае возвращается код `202 (Accepted)` и состояние задачи изменяется на **Stopping**.

Метод:

```
POST /api/2.0/virtualization/tasks/{идентификатор}/cancel
```

где:

`{идентификатор}` – идентификатор задачи (обязательный параметр).

Коды возврата:

- `200 (OK)` – запрос выполнен успешно (выполнение задачи отменено).
- `202 (Accepted)` – запрос принят к исполнению (состояние задачи изменяется на **Stopping**).
- `403 (Forbidden)` – доступ к ресурсу запрещен.
- `404 (Not Found)` – задача с указанным идентификатором не найдена.
- `405 (Method Not Allowed)` – для дочерних задач: отменить дочернюю задачу можно, только отменив родительскую задачу.

- `409 (Conflict)` – задача уже находится в одном из состояний: **Cancelled**, **Failed**, **Stopped**.

kaspersky

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления приложения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе приложения, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

Лицо, ответственное за эксплуатацию приложения, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в приложении, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях приложения следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability/report-a-vulnerability/12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

kaspersky

Действия после сбоя или неустранимой ошибки в работе программы

Компоненты решения Kaspersky Security автоматически восстанавливают свою работу после сбоев, участие пользователя не требуется. В случае, когда решение не может восстановить свою работу, вам требуется переустановить решение или его компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 226).

kaspersky

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в справке или в других источниках информации о решении Kaspersky Security, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании решения.

"Лаборатория Касперского" предоставляет поддержку решения в течение его жизненного цикла (см. страницу жизненного цикла приложений "Лаборатории Касперского" (https://support.kaspersky.com/corporate/lifecycle)). Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules/ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Посетить сайт Службы технической поддержки (http://support.kaspersky.ru/b2b).
- Отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Получение информации для Службы технической поддержки

Получение файлов данных

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас прислать следующие файлы:

- файлы системной статистики SVM;
- файлы дампа Сервера защиты и Легких агентов (см. раздел "Файлы дампа Сервера защиты и Легкого агента" на стр. 228);
- файлы трассировки мастера установки компонентов решения (см. раздел "Файлы трассировки мастера установки компонентов Kaspersky Security" на стр. 229);
- файлы трассировки Сервера интеграции и Консоли Сервера интеграции (на стр. 230);
- файлы трассировки SVM, Легкого агента и плагинов управления Kaspersky Security (см. раздел "Файлы трассировки SVM, Легких агентов и плагинов управления Kaspersky Security" на стр. 235).

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Security на момент создания файла дампа.

Файл трассировки позволяет отследить процесс пошагового выполнения команд компонентов решения и обнаружить, на каком этапе работы компонента возникает ошибка.

Изменение параметров компонентов решения

Специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на защищенной виртуальной машине, подробные отчеты о работе компонентов решения.

Во время проведения работ по диагностике специалисты Службы технической поддержки могут попросить вас в отладочных целях изменить параметры компонентов решения:

- активировать функциональность получения расширенной диагностической информации;

- запустить утилиты поддержки, входящие в комплект поставки решения;
- изменить параметры хранения диагностической информации;
- включить режим отладки для Сервера интеграции;
- настроить перехват сетевого трафика и сохранение сетевого трафика в файле;
- выполнить более тонкую настройку работы Легких агентов, Сервера защиты, Сервера интеграции, Консоли Сервера интеграции и плагинов управления, недоступную через описанные в этой справке средства управления работой решения.

Специалисты Службы технической поддержки сообщат вам всю необходимую для выполнения перечисленных действий информацию: описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты, а также состав отправляемых в отладочных целях данных.

Расширенная диагностическая информация сохраняется на вашей виртуальной машине. Автоматическая пересылка данных в "Лабораторию Касперского" не выполняется.

Настоятельно рекомендуется выполнять перечисленные выше действия только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы компонентов решения способами, не описанными в справке решения или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты виртуальной машины, а также к нарушению доступности и целостности обрабатываемой информации.

Получение информации об SVM, подключенных к Серверу интеграции

Специалисты Службы технической поддержки могут попросить вас предоставить информацию об SVM, которые подключены к Серверу интеграции. Вы можете просмотреть список всех SVM, подключенных к Серверу интеграции (см. раздел "Просмотр списка SVM, подключенных к Серверу интеграции" на стр. 97), в Консоли Сервера интеграции.

Диагностика работы решения

Для диагностики работы решения может потребоваться включить отладочный режим работы Сервера интеграции. Для включения отладочного режима работы используются специальные параметры конфигурационного файла. Более подробную информацию вы можете получить у специалистов Службы технической поддержки.

Файлы дампа Сервера защиты и Легкого агента

Файлы дампа содержат информацию о рабочей памяти процессов Kaspersky Security на момент создания файла.

Файлы дампа могут содержать персональные данные. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Автоматическая отправка файлов дампа в "Лабораторию Касперского" не выполняется.

По умолчанию файлы дампа не создаются. Вы можете включать и выключать запись дампов.

Файлы дампа Сервера защиты

► *Чтобы включить запись дампов Сервера защиты:*

1. На SVM создайте файл etc/opt/kaspersky/la/dumps_enabled.
2. Перезапустите службу scanserver, выполнив команду `systemctl restart la-scanserver`.

Все созданные файлы дампа по умолчанию располагаются на SVM в директории /var/opt/kaspersky/la/dumps. Имя каждого файла *.dmp содержит дату и время создания файла, идентификатор процесса (PID) и номер дампа в сессии.

Вы можете изменять параметры записи дампов в конфигурационном файле ScanServer.conf (раздел [dumps]).

Для доступа к файлам дампа требуется пароль учетной записи `root` на SVM, заданный при установке Сервера защиты. Если вы изменили директорию хранения файлов дампа по умолчанию, то Kaspersky Security не контролирует доступ к файлам дампов. Если файловая система, в которой расположена указанная директория, поддерживает соответствующее управление доступом, для доступа к файлам дампов требуются права учетной записи `root`.

Файлы дампа автоматически удаляются при удалении SVM.

► *Чтобы выключить запись дампов Сервера защиты:*

1. Удалите файл etc/opt/kaspersky/la/dumps_enabled.
2. Перезапустите службу scanserver, выполнив команду `systemctl restart la-scanserver`.

Файлы дампа Легких агентов

Вы можете включать и выключать запись дампов Легкого агента для Linux и Легкого агента для Windows на устройствах, где установлено приложение Kaspersky Endpoint Security для Linux или приложение Kaspersky Endpoint Security для Windows в режиме Легкого агента.

Подробнее см. в справке приложения, которое используется в режиме Легкого агента: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

Файлы трассировки мастера установки компонентов Kaspersky Security

Информация о ходе и результатах работы мастера установки компонентов Kaspersky Security записывается в файлы трассировки. Если установка, обновление или удаление Сервера интеграции и Консоли Сервера интеграции завершилось с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Файлы трассировки мастера установки компонентов Kaspersky Security представляют собой файлы в формате TXT. Они автоматически сохраняются на том устройстве, на котором был запущен мастер.

Если вы выполняли установку компонентов Kaspersky Security или загрузку образов SVM, файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_<номер версии>_Light_Agent_BundleInitialInstall_logs_<дата и время>.zip, где:

- <номер версии> – номер установленной версии Kaspersky Security;
- <дата и время> – дата и время завершения установки.

Если вы выполняли обновление компонентов Kaspersky Security, файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_<номер версии>_Light_Agent_BundleMajorUpgrade_logs_<дата и время>.zip, где:

- <номер версии> – номер установленной версии Kaspersky Security;
- <дата и время> – дата и время завершения обновления.

Если вы выполняли удаление компонентов Kaspersky Security, файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_<номер версии>_Light_Agent_BundleUninstall_logs_<дата и время>.zip, где:

- <номер версии> – номер установленной версии Kaspersky Security;
- <дата и время> – дата и время завершения удаления.

Файлы трассировки мастера установки компонентов Kaspersky Security содержат следующую информацию:

- диагностическую информацию о процессе установки, обновления, удаления компонентов Kaspersky Security;
- имя устройства, на котором запущена процедура установки, обновления или удаления компонентов Kaspersky Security, и имя пользователя, запустившего процедуру;
- информацию об ошибках, возникающих в процессе установки, обновления или удаления компонентов Kaspersky Security.

Файлы трассировки мастера установки компонентов Kaspersky Security хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Автоматическая отправка файлов трассировки мастера установки компонентов Kaspersky Security в "Лабораторию Касперского" не выполняется.

Файлы трассировки Сервера интеграции и Консоли Сервера интеграции

Файлы трассировки Сервера интеграции на базе Linux

Информация о работе Сервера интеграции на базе Linux может записываться в следующие файлы трассировки:

- /var/log/kaspersky/viis/service.log – файл трассировки Сервера интеграции.

- /var/log/kaspersky/viis/SvmManagement/sm_<дата создания файла>.log – файл трассировки процедур развертывания, изменения конфигурации и удаления SVM с помощью REST API Сервера интеграции на базе Linux.

По умолчанию запись информации в файлы трассировки выключена.

Вы можете включать и выключать запись информации в файлы трассировки Сервера интеграции на базе Linux с помощью конфигурационного файла /var/opt/kaspersky/viis/common/appsettings.logging.json.

Для изменения конфигурационного файла требуются права привилегированной учетной записи.

► *Чтобы включить запись информации в файлы трассировки Сервера интеграции на базе Linux:*

1. Откройте файл /var/opt/kaspersky/viis/common/appsettings.logging.json.
2. В разделе **LogLevel** укажите значение `Trace` для параметра `Default`. По умолчанию указано значение `None`.
3. В разделе **rules** в подразделах **Service** и **SvmManagement** укажите значение `Trace` для параметра `minlevel`. По умолчанию указано значение `None`.
4. Сохраните файл /var/opt/kaspersky/viis/common/appsettings.logging.json.

Новые значения параметров применяются без перезагрузки Сервера интеграции.

Файлы трассировки перемещаются в директорию архива (/var/log/kaspersky/viis/archives). Файлы трассировки Сервера интеграции помещаются в архив при достижении размера файла в 50 МБ. Файлы трассировки процедур развертывания, изменения конфигурации и удаления SVM помещаются в архив ежедневно. В архиве хранится до 20 файлов трассировки Сервера интеграции и до 10 файлов трассировки процедур развертывания, изменения конфигурации и удаления SVM. После достижения этого числа более старые файлы удаляются.

Доступ к директории, в которой сохраняются файлы трассировки, ограничивается с помощью ACL. Для доступа к директории требуются права администратора (root, sudoers).

Если вы изменили директорию хранения файлов трассировки по умолчанию, то Kaspersky Security не контролирует доступ к файлам трассировки. Рекомендуется обеспечить защиту информации от несанкционированного доступа.

Файлы трассировки Сервера интеграции на базе Windows и Консоли Сервера интеграции

Информация о работе Сервера интеграции на базе Windows и Консоли Сервера интеграции может записываться в следующие файлы трассировки:

- %ProgramData%\Kaspersky Lab\VIISLA\logs\viisla_service_loader.log – файл трассировки запуска Сервера интеграции на базе Windows. Файл не содержит персональные данные.
- %ProgramData%\Kaspersky Lab\VIISLA\logs\service.log – файл трассировки Сервера интеграции на базе Windows.
- %ProgramData%\Kaspersky Lab\VIISLA Console\logs\console.log – файл трассировки Консоли Сервера интеграции.

- %ProgramData%\Kaspersky Lab\VIISLA\logs\SvmManagement\sm_<дата создания файла>.log – файл трассировки процедур развертывания, изменения конфигурации и удаления SVM с помощью REST API Сервера интеграции на базе Windows.

Файлы трассировки создаются по умолчанию с уровнем детализации Error. Вы можете включать и выключать запись информации в файлы трассировки Сервера интеграции и Консоли Сервера интеграции, а также изменить уровень детализации информации в файлах трассировки с помощью следующих конфигурационных файлов:

- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\appsettings.logging.json – для файла трассировки Сервера интеграции и файла трассировки процедур развертывания, изменения конфигурации и удаления SVM.
- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA Console\NLog.config – для файла трассировки Консоли Сервера интеграции.

За подробной информацией вы можете обратиться к специалистам Службы технической поддержки.

Файлы трассировки перемещаются в папку архива (%ProgramData%\Kaspersky Lab\VIISLA\logs\archives). Файлы трассировки Сервера интеграции помещаются в архив при достижении размера файла в 50 МБ. Файлы трассировки процедур развертывания, изменения конфигурации и удаления SVM помещаются в архив ежедневно. В архиве хранится до 20 файлов трассировки Сервера интеграции и до 10 файлов трассировки процедур развертывания, изменения конфигурации и удаления SVM. После достижения этого числа более старые файлы удаляются.

Доступ к папке, в которой сохраняются файлы трассировки, ограничивается с помощью ACL. Для доступа к папке требуются права администратора.

Если вы изменили папку хранения файлов трассировки по умолчанию, то Kaspersky Security не контролирует доступ к файлам трассировки. Рекомендуется обеспечить защиту информации от несанкционированного доступа.

Содержимое файлов трассировки

В файле трассировки Сервера интеграции может сохраняться следующая информация:

- диагностическая информация о работе Сервера интеграции, его загруженности, о результатах проверки целостности данных;
- заголовки и содержимое http-запросов, которые отправляет и принимает Сервер интеграции в процессе своей работы;
- IP-адреса SVM и защищенных виртуальных машин, а также IP-адрес устройства, на котором установлена Консоль администрирования Kaspersky Security Center, если Консоль администрирования Kaspersky Security Center установлена отдельно от Сервера администрирования Kaspersky Security Center;
- трассировка запросов к Серверу интеграции;
- описание исключений и ошибок, возникающих при работе с внутренними подсистемами и внешними службами;
- имена внутренних учетных записей Сервера интеграции;
- имена учетных записей, которые используются для подключения Сервера интеграции к объектам виртуальной инфраструктуры;

- в зависимости от вида виртуальной инфраструктуры:
  - IP-адреса или полные доменные имена (FQDN) гипервизоров или серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции;
  - IP-адреса или полные доменные имена (FQDN) микросервиса Keystone и других микросервисов облачной инфраструктуры, к которым подключается Сервер интеграции;
- если Kaspersky Security используется в режиме мультитенантности:
  - названия и идентификаторы тенантов, зарегистрированных в базе данных Сервера интеграции;
  - имена учетных записей администраторов виртуальных Серверов администрирования Kaspersky Security Center;
  - идентификаторы и IP-адреса виртуальных машин тенантов.

В файле трассировки Консоли Сервера интеграции может сохраняться следующая информация:

- диагностическая информация о работе Консоли Сервера интеграции;
- трассировка параметров командной строки и результаты их проверки;
- заголовки и содержимое http-запросов, которые отправляет и принимает Консоль Сервера интеграции в процессе своей работы;
- информация о переходах по разделам Консоли Сервера интеграции и работе с элементами интерфейса;
- IP-адрес Сервера администрирования Kaspersky Security Center;
- номера портов для взаимодействия с Сервером администрирования Kaspersky Security Center через Агент администрирования Kaspersky Security Center;
- описание исключений и ошибок, возникающих при работе с внутренними подсистемами и внешними службами;
- имена внутренних учетных записей Сервера интеграции;
- имена учетных записей, которые используются для подключения Сервера интеграции к объектам виртуальной инфраструктуры;
- в зависимости от вида виртуальной инфраструктуры:
  - IP-адреса или полные доменные имена (FQDN) гипервизоров или серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции;
  - IP-адреса или полные доменные имена (FQDN) микросервиса Keystone и других микросервисов облачной инфраструктуры, к которым подключается Сервер интеграции;
- если Kaspersky Security используется в режиме мультитенантности, названия тенантов, зарегистрированных в базе данных Сервера интеграции.

Вы можете использовать файлы трассировки Сервера интеграции и Консоли Сервера интеграции при обращении в Службу технической поддержки. Информация, записанная в файлы трассировки, может потребоваться для анализа и выяснения причин возникновения ошибок в работе Сервера интеграции.

Автоматическая отправка файлов трассировки Сервера интеграции и Консоли Сервера интеграции в "Лабораторию Касперского" не выполняется.

kaspersky

Файлы трассировки утилиты управления сертификатами Сервера интеграции и SVM

Информация о работе утилиты управления сертификатами Сервера интеграции и SVM (см. раздел "Замена сертификатов Сервера интеграции и SVM" на стр. 184) может записываться в файлы трассировки. В зависимости от операционной системы устройства, на котором работает утилита, файлы расположены по следующему пути:

- /var/log/kaspersky/viis/ – на устройствах с операционными системами Linux;
- %ProgramData%\Kaspersky Lab\VIISLA\logs – на устройствах с операционными системами Windows.

По умолчанию запись информации в файлы трассировки выключена.

Вы можете включать и выключать запись информации в файлы трассировки утилиты управления сертификатами, а также настраивать параметры трассировки в конфигурационном файле утилиты управления сертификатами appsettings.certificate_manager.json. В зависимости от операционной системы устройства, на котором работает утилита, файл расположен по следующему пути:

- /var/opt/kaspersky/viis/common/ – на устройствах с операционными системами Linux;
- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ – на устройствах с операционными системами Windows.

Файлы трассировки утилиты управления сертификатами могут содержать следующую информацию:

- Строки вызова утилиты, включая аргументы и их значения, кроме паролей.
- Строки вывода утилиты, содержащие запросы к пользователю.
- Информацию о ходе выполнения команд, в том числе информацию об ошибках.

Файлы трассировки утилиты управления сертификатами не содержат персональные данные.

Файлы трассировки перемещаются в архив при достижении размера файла в 5 МБ. В архиве хранится до 10 файлов, после достижения этого числа более старые файлы удаляются. В зависимости от операционной системы устройства, на котором работает утилита, архив расположен по следующему пути:

- /var/log/kaspersky/viis/archives/ – на устройствах с операционными системами Linux;
- %ProgramData%\Kaspersky Lab\VIISLA\logs\archives – на устройствах с операционными системами Windows.

Доступ к папке хранения файлов трассировки ограничивается. В операционной системе Linux доступ к директории имеют только учетные записи, которые находятся в группе sudoers. В операционной системе Windows для доступа к папке требуются права администратора.

Если вы изменили папку хранения файлов трассировки по умолчанию, то Kaspersky Security не контролирует доступ к файлам трассировки. Рекомендуется обеспечить защиту информации от несанкционированного доступа.

Автоматическая отправка файлов трассировки в "Лабораторию Касперского" не выполняется.

kaspersky

Файлы трассировки SVM, Легких агентов и плагинов управления Kaspersky Security

Файлы трассировки SVM (см. раздел "Файлы трассировки SVM" на стр. 235), Легких агентов и плагинов управления (см. раздел "Файлы трассировки плагинов управления" на стр. 236) Kaspersky Security могут содержать следующие общие данные:

- время события;
- номер потока выполнения;
- название компонента Kaspersky Security, в результате работы которого произошло событие;
- степень важности события (информационное, предупреждение, критическое, ошибка);
- описание события выполнения команды, полученной от компонента Kaspersky Security, и результата выполнения этой команды.

Подробную информацию о файлах трассировки Легкого агента для Linux и Легкого агента для Windows см. в справке приложения, которое используется в режиме Легкого агента: Kaspersky Endpoint Security для Linux (https://support.kaspersky.com/KES4Linux/12.2.0/ru-RU/index.htm) или Kaspersky Endpoint Security для Windows (https://support.kaspersky.com/KESWin/12.8/ru-RU/index.htm).

В этом разделе

Файлы трассировки SVM

Во время работы на SVM могут создаваться следующие файлы трассировки:

- Файл трассировки Сервера защиты ScanServer.log. Имя файла содержит дату и время создания файла. Помимо общих данных (см. раздел "Файлы трассировки SVM, Легких агентов и плагинов управления Kaspersky Security" на стр. 235) этот файл может содержать следующую информацию:
  - персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам на защищенных виртуальных машинах;
  - имя учетной записи для входа в операционную систему, если имя учетной записи является частью имени файла;
  - адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта;
  - параметры подключения SVM к Серверу интеграции;
  - информацию о подключении Легких агентов к SVM: уникальный идентификатор SVM, уникальный идентификатор и сведения об операционной системе виртуальной машины, на которой установлен Легкий агент, периоды времени, в течение которых Легкий агент был подключен к SVM.
- Файл трассировки boot_config.log. В этот файл записываются результаты выполнения команд скрипта первого запуска SVM.

- Файл трассировки wdserver.log. В этот файл записывается информация о событиях, возникающих во время работы службы watchdog (wdserver). Файл содержит общие данные.
- Файл трассировки SnmpTool.log. В этот файл записывается информация о событиях, возникающих во время работы службы SNMP (SnmpTool). Файл содержит общие данные.
- Файл трассировки Агента администрирования Kaspersky Security Center. В этот файл записывается информация о событиях, возникающих при работе модуля связи с Kaspersky Security Center. Файл содержит общие данные.

Файлы трассировки boot_config.log и wdserver.log создаются автоматически.

Файлы трассировки ScanServer.log и SnmpTool.log вы можете создать с помощью конфигурационных файлов ScanServer.conf и SnmpTool.conf, которые расположены в директории /etc/opt/kaspersky/la/ на SVM. Для создания файла трассировки Агента администрирования используется специальный скрипт.

За подробной информацией о том, как создать и настроить файлы трассировки, вы можете обратиться к специалистам Службы технической поддержки.

Все созданные файлы трассировки SVM расположены в директории /var/log/kaspersky/la/.

Файл трассировки ScanServer.log вы также можете создать в политике для Сервера защиты. Для этого вам нужно:

1. Включить отображение дополнительных параметров (см. раздел "Настройка отображения дополнительных параметров Сервера защиты" на стр. 116) в политике для Сервера защиты. По умолчанию дополнительные параметры не отображаются.
2. Настроить уровень трассировки (см. раздел "Настройка дополнительных параметров Сервера защиты" на стр. 117) в разделе политики **Дополнительные параметры** и применить изменение.

   Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки.

Файлы трассировки SVM хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского"

Автоматическая отправка файлов трассировки SVM в "Лабораторию Касперского" не выполняется. Файлы трассировки автоматически удаляются при удалении Kaspersky Security.

Файлы трассировки плагинов управления

Файлы трассировки веб-плагинов

Если для управления компонентами решения Kaspersky Security вы используете Kaspersky Security Center Web Console, информация о событиях, возникающих во время работы веб-плагинов управления, может записываться в файлы трассировки веб-плагинов.

Файлы трассировки веб-плагинов создаются автоматически, если при установке Kaspersky Security Center Web Console была включена запись в *журнал активности* Kaspersky Security Center Web Console (см. подробнее в справке Kaspersky Security Center).

Файлы трассировки веб-плагинов сохраняются в папке установки Kaspersky Security Center Web Console во вложенной папке logs:

- /var/opt/kaspersky/ksc-web-console/logs – на устройствах с операционными системами Linux.
- %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\logs – на устройствах с операционными системами Windows.

В файле трассировки веб-плагина Сервера интеграции может сохраняться следующая информация:

- диагностическая информация о работе Веб-консоли Сервера интеграции;
- IP-адрес Сервера администрирования Kaspersky Security Center;
- номера портов для взаимодействия с Сервером администрирования Kaspersky Security Center через Агент администрирования Kaspersky Security Center;
- описание исключений и ошибок, возникающих при работе с внутренними подсистемами и внешними службами;
- имена внутренних учетных записей Сервера интеграции;
- IP-адреса или полные доменные имена (FQDN) гипервизоров или серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции;
- IP-адреса, версии и имена SVM, развернутых на гипервизорах.

В файле трассировки веб-плагина Сервера защиты может сохраняться следующая информация:

- диагностическая информация о работе веб-плагина Сервера защиты;
- описание исключений и ошибок, возникающих при работе с внутренними подсистемами и внешними службами.

Файлы трассировки MMC-плагинов

Если для управления компонентами решения Kaspersky Security вы используете Консоль администрирования Kaspersky Security Center, информация о событиях, возникающих во время работы на MMC-плагинов управления, может записываться в следующие файлы на устройстве, где установлен Сервер администрирования Kaspersky Security Center:

- Файл трассировки MMC-плагина управления Сервера защиты. Имя файла задается пользователем, к заданному имени добавляются имя пользователя и идентификатор процесса (PID). В этот файл записывается информация о событиях, возникающих во время работы плагина, в частности, о работе политики для Сервера защиты и задач.
- Файлы трассировки MMC-плагинов управления Легкого агента для Linux и Легкого агента для Windows (приложений, которые работают в режиме Легкого агента). Имена файлов содержат номер версии приложения, дату и время создания файла и идентификатор процесса (PID). В этот файл записывается информация о событиях, возникающих во время работы плагина, в частности, о работе политики для Легкого агента и задач.

Помимо общих данных (см. раздел "Файлы трассировки SVM, Легких агентов и плагинов управления Kaspersky Security" на стр. 235) файлы трассировки MMC-плагинов могут содержать следующую информацию:

- персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам;

- имя учетной записи для входа в операционную систему, если имя учетной записи является частью имени файла.

По умолчанию файлы трассировки MMC-плагинов Kaspersky Security не создаются. Вы можете создать все файлы трассировки MMC-плагинов с помощью ключей реестра. За подробной информацией о том, как создать файлы трассировки, вы можете обратиться к специалистам Службы технической поддержки.

Все созданные файлы трассировки MMC-плагинов расположены в папке %ProgramData%\Kaspersky Lab\Plugins\.

Файлы трассировки плагинов управления хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Автоматическая отправка файлов трассировки плагинов управления в "Лабораторию Касперского" не выполняется. Файлы трассировки автоматически удаляются при удалении решения Kaspersky Security.

Использование утилит и скриптов из комплекта поставки Kaspersky Security

Для анализа ошибок в работе Kaspersky Security специалисты Службы технической поддержки могут попросить вас использовать следующие утилиты, входящие в комплект поставки Kaspersky Security:

- ai_config – утилита, позволяющая преобразовать параметры SVM из формата базы данных конфигурации SVM в текстовый файл и обратно.
- cleanUpdateShare.sh – скрипт, предназначенный для удаления старых баз Легких агентов с SVM.
- configure.sh – скрипт, предназначенный для управления SVM, просмотра и изменения параметров конфигурации SVM; используется мастером управления SVM для изменения конфигурации SVM под учетной записью `klconfig`.
- dump_ods_scan_queue и dump_ods_scan_queue.sh – утилиты, позволяющие посмотреть текущую очередь задач проверки.
- eventlog_client и eventlog_client.sh – утилиты, позволяющие формировать события для отправки в Kaspersky Security Center.
- firewall.sh – скрипт, позволяющий открыть порты для подключения к Агенту администрирования.
- first_boot.sh – скрипт, позволяющий изменить параметры конфигурации SVM при первой загрузке SVM.
- get_used_mem.sh – скрипт, позволяющий посмотреть статистику использования памяти.
- kvp_read – утилита, позволяющая посмотреть общие данные гипервизора в хранилище Hyper-V KVP Exchange.
- la-kvm-guest – скрипт в формате init.d, предназначенный для управления службой KVM guest.
- la-scanserver – скрипт в формате init.d, предназначенный для управления службой scanserver.

- managenet.sh – скрипт, предназначенный для управления сетевыми интерфейсами.
- on_product_install.sh – скрипт, позволяющий применить временную конфигурацию SVM во время развертывания SVM.
- sfw – утилита, позволяющая управлять брандмауэром netfilter операционной системы Linux.
- show_inventory и show_inventory.sh – утилиты, позволяющие посмотреть информацию о дереве виртуальной инфраструктуры, полученную Сервером защиты от Сервера интеграции.
- show_virt_info и show_virt_info.sh – утилиты, позволяющие посмотреть информацию о виртуальной машине (например, версию BIOS, информацию о гипервизоре).
- snmp.sh – скрипт, предназначенный для включения и выключения SNMP-мониторинга на SVM.
- storage_util – утилита, предназначенная для управления хранилищем данных, которые используются при обновлении баз Kaspersky Security.
- patch_detector.pl – скрипт, позволяющий искать обновление модулей программы в указанной папке и запускать утилиту KSV Patch Installer для установки обновления.
- patch_installer.pl – скрипт, позволяющий установить обновление модулей Kaspersky Security из файла tar.gz.
- patch_list.pl – скрипт, позволяющий сформировать список установленных на SVM обновлений модулей Kaspersky Security в формате XML.
- patch_rollback.pl – скрипт, позволяющий откатить последнее установленное обновление модулей Kaspersky Security.

kaspersky

Приложение. Значения параметров программы в сертифицированном состоянии

Этот раздел содержит перечень параметров решения, влияющих на безопасное состояние решения, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированной конфигурации на другие значения выводит решение из безопасного состояния.

Таблица 2. Параметры и их безопасные значения для решения в сертифицированной конфигурации

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Политика для Сервера защиты – **Настройка событий**	**Регистрация событий**: **Хранить в базе данных Сервера администрирования в течение**	Флажок установлен, значение не ниже установленного по умолчанию.
Политика для Сервера защиты – **Параметры Kaspersky Security Network**	**Использовать KSN**	Флажок снят. Допускается устанавливать флажок только при использовании KPSN.
Политика для Сервера защиты – **Параметры обновления**	**Обновлять модули решения**	Флажок снят.
Политика для Сервера защиты – **Параметры SNMP-мониторинга**	**Включить SNMP-мониторинг состояния SVM**	Флажок снят.
Задача Обновление баз для Сервера защиты – **Уведомление**	**Сохранять все события**	Выбран этот вариант.
Задача Обновление баз для Сервера защиты – **Расписание**	**Запуск по расписанию**	**При загрузке обновлений в хранилище**
Задача Обновление баз для Сервера защиты – **Исключения из области действия задачи**	Таблица исключений.	Не заданы.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 3. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
решение	продукт, объект оценки, программное изделие
виртуальная инфраструктура	среда функционирования
файл виртуальной машины	объект воздействия
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы решения	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

kaspersky

Информация о стороннем коде

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

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apache является либо зарегистрированным товарным знаком, либо товарным знаком Apache Software Foundation.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Ubuntu, LTS являются зарегистрированными товарными знаками Canonical Ltd.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenApp, XenDesktop и XenServer являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

HUAWEI, FusionCompute и FusionSphere являются товарными знаками Huawei Technologies Co., Ltd.

Core является товарным знаком Intel Corporation или ее дочерних компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Excel, Hyper-V, PowerShell, Windows и Windows Server являются товарными знаками группы компаний Microsoft.

OpenStack – зарегистрированный товарный знак OpenStack Foundation в США и других странах.

Red Hat Enterprise Linux и CentOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

OpenAPI – товарный знак компании The Linux Foundation.