kaspersky

Kaspersky Sandbox

Подготовительные процедуры и руководство по эксплуатации

kaspersky

Уважаемый пользователь!

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

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

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

Содержание

Kaspersky Sandbox

Решение Kaspersky Sandbox обнаруживает и автоматически блокирует сложные угрозы на клиентских устройствах (рабочих станциях, компьютерах, серверах, далее также "рабочих станциях").

Решение разработано для корпоративных пользователей.

Решение Kaspersky Sandbox состоит из:

- Программы Kaspersky Sandbox, отвечающей за серверную часть решения. Kaspersky Sandbox устанавливается на один или несколько серверов внутри сети вашей организации. Серверы

можно объединять в кластер. На серверах с Kaspersky Sandbox развернуты виртуальные образы операционных систем Microsoft Windows, в которых запускаются проверяемые объекты. Kaspersky Sandbox анализирует поведение объектов для выявления вредоносной активности и сложных угроз в IT-инфраструктуре организации.

- Программы защиты рабочих станций (Endpoint Protection Platform (далее также "EPP")) Kaspersky Endpoint Security для Windows версии 11.2. Kaspersky Endpoint Security устанавливается на рабочих станциях сети вашей организации и обеспечивает комплексную защиту рабочих станций от различного вида угроз, сетевых и мошеннических атак.

- Программы Kaspersky Endpoint Agent версии 3.7 (далее также "KEA"), устанавливающейся в составе EPP. Программа Kaspersky Endpoint Agent устанавливается на рабочих станциях и серверах сети вашей организации и обеспечивает коммуникацию EPP и Kaspersky Sandbox, а также выполнение действий по автоматическому реагированию на обнаруженные угрозы, настроенных в политиках Kaspersky Security Center.

Принцип работы решения Kaspersky Sandbox

Решение Kaspersky Sandbox работает по следующему принципу:

1. В момент обращения к объекту (запуска исполняемого файла или открытия документа, например, в формате DOCX или PDF) на рабочей станции программа защиты рабочих станций (EPP) принимает решение о необходимости дополнительной проверки объекта с помощью Kaspersky Sandbox.

2. Если программа EPP приняла решение о необходимости дополнительной проверки объекта с помощью Kaspersky Sandbox, она отправляет запрос на проверку объекта программе Kaspersky Endpoint Agent. До получения результата проверки от Kaspersky Endpoint Agent программа EPP блокирует доступ к объекту.

3. Kaspersky Endpoint Agent проверяет, был ли этот объект недавно проверен в Kaspersky Sandbox.

   > Время, по истечении которого объект считается проверенным давно, предустановлено на основании опыта антивирусных специалистов "Лаборатории Касперского".

   - Если объект проверялся недавно, Kaspersky Endpoint Agent отправляет результат проверки в EPP. Если объект представляет угрозу, выполняются действия над объектами, настроенные в EPP. Подробнее о настройке действий см. в документации используемой EPP.

     > В EPP может быть настроено действие **Удалять объект**.

   - Если объект не проверялся или проверялся давно, Kaspersky Endpoint Agent сообщает EPP об отсутствии данных об объекте и отправляет объект на проверку в Kaspersky Sandbox. EPP разрешает доступ к объекту.

4. Kaspersky Sandbox проверяет объект и передает результат проверки объекта в Kaspersky Endpoint Agent. Если объект представляет угрозу, Kaspersky Endpoint Agent выполняет действия по реагированию на угрозы, настроенные в политике Kaspersky Security Center.

Информация об обнаруженных угрозах хранится в Kaspersky Sandbox до обновления баз программы.

Комплект поставки

В комплект поставки программы Kaspersky Sandbox входят следующие файлы:

1. Образ диска (файл с расширением iso) с установочными файлами операционной системы CentOS 7.7 и программы Kaspersky Sandbox, а также файл с информацией о стороннем коде, используемом в Kaspersky Sandbox.

2. Образ диска (файл с расширением iso) 64-разрядной операционной системы Windows 7 с установленными программами, в которой Kaspersky Sandbox будет запускать файлы. Операционная система, а также программы уже активированы.

3. Установочный файл плагинов управления программами Kaspersky Sandbox и Kaspersky Endpoint Agent через Консоль администрирования Kaspersky Security Center.

Информацию о комплекте поставки программы Kaspersky Endpoint Agent в составе Kaspersky Endpoint Security для Windows см. в *Справке Kaspersky Endpoint Security для Windows*.

Аппаратные и программные требования

Для развертывания программы на виртуальной платформе должен быть установлен гипервизор VMware ESXi версии 6.7.0.

Конфигурация серверов Kaspersky Sandbox зависит от объема данных, обрабатываемых программой, а также от пропускной способности канала связи.

Аппаратные и программные требования к Kaspersky Sandbox

Решение Kaspersky Sandbox поддерживает следующие конфигурации:

- Один сервер Kaspersky Sandbox, рассчитанный на обработку объектов, получаемых от 1000 рабочих станций, или 305 объектов в час, получаемых по API.

- Один сервер Kaspersky Sandbox, рассчитанный на обработку объектов, получаемых от 5000 рабочих станций, или 910 объектов в час, получаемых по API.

- При установке на виртуальную машину VMware ESXi один сервер Kaspersky Sandbox может обрабатывать объекты, полученные от 250 рабочих станций, или 100 объектов в час, полученных по API.

Если вы хотите, чтобы Kaspersky Sandbox обрабатывал объекты от 10000 рабочих станций с программой Kaspersky Endpoint Agent, вы можете объединить 2 сервера, рассчитанных на обработку объектов, получаемых от 5000 рабочих станций, в кластер.

Для обработки объектов от 1000 рабочих станций вы можете установить Kaspersky Sandbox на сервер в одной из следующих конфигураций:

- Процессор: 16 ядер с поддержкой технологий Hyper-Threading, 2,2 ГГц.

  Объем оперативной памяти: 64 ГБ.

  Два жестких диска Hardware RAID 1:

  - объем: 600 ГБ каждый,
  - скорость вращения: 10000 оборотов/мин,
  - скорость передачи данных: 100 МБ/сек.

  Два сетевых адаптера со скоростью передачи данных 1 Гбит/с.

- Процессор: 14 ядер с поддержкой технологий Hyper-Threading, 2,6 ГГц.

  Объем оперативной памяти: 64 ГБ.

  Два жестких диска Hardware RAID 1:

  - объем: 600 ГБ каждый,
  - скорость вращения: 10000 оборотов/мин,
  - скорость передачи данных: 100 МБ/сек.

  Два сетевых адаптера со скоростью передачи данных 1 Гбит/с.

Для обработки объектов от 5000 рабочих станций вы можете установить Kaspersky Sandbox на сервер в следующей конфигурации:

- Два процессора: 18 ядер с поддержкой технологий Hyper-Threading, 2,2 ГГц каждый.

  Объем оперативной памяти: 196 ГБ.

  Два жестких диска Hardware RAID 1:

  - объем: 600 ГБ каждый,
  - скорость вращения: 10000 оборотов/мин,
  - скорость передачи данных: 100 МБ/сек.

  Два сетевых адаптера со скоростью передачи данных 1 Гбит/с.

При установке Kaspersky Sandbox на виртуальную машину VMware ESXi (два жестких диска Hardware RAID 1 по 600 Гб каждый) для обработки объектов от 250 рабочих станций настройте следующую конфигурацию:

- Процессор (CPU): 12 ядер (6 сокетов по 2 ядра).
- Объем оперативной памяти (Memory): 32 ГБ.
- Объем жесткого диска: 600 ГБ.

- Два сетевых адаптера со скоростью передачи данных 1 Гбит/с.

  На виртуальной машине:

  1. Разрешите вложенную виртуализацию.
  2. Установите параметр **High Latency Sensitivity**.
  3. Зарезервируйте всю оперативную память (32 ГБ).
  4. Зарезервируйте всю частоту процессора (26400 МГц).
  5. Установите параметр **Expose hardware assisted virtualization to the guest OS**.

Требования к браузеру для работы с программой Kaspersky Sandbox через веб-интерфейс

Для настройки и работы с программой Kaspersky Sandbox через веб-интерфейс рекомендуется использовать один из следующих браузеров:

- Google Chrome для Windows версии 77 или выше.
- Google Chrome для Linux версии 77 или выше.

Аппаратные и программные требования к программе Kaspersky Endpoint Agent

Вы можете установить Kaspersky Endpoint Agent 3.7 на рабочие станции под управлением следующих операционных систем:

- Windows 7 SP1 Enterprise x32 / x64.
- Windows 8.1.1 Enterprise x32 / x64.
- Windows 10, версия 1703 Enterprise x32 / x64 (RS3).
- Windows 10, версия 1803 Enterprise x32 / x64 (RS4).
- Windows 10, версия 1809 Enterprise x32 / x64 (RS5).
- Windows 10, версия 1903 Enterprise x32 / x64 (19H1).

Вы можете установить Kaspersky Endpoint Agent 3.7 на серверы под управлением следующих операционных систем:

- Windows Server 2008 R2 Enterprise x64.
- Windows Server 2012 Standard x64.
- Windows Server 2012 R2 Standard.
- Windows Server 2016 Standard / Datacenter.
- Windows Server 2019 Standard / Datacenter.

Требования к пропускной способности канала связи между рабочими станциями с программой Kaspersky Endpoint Agent и сервером Kaspersky Sandbox

Минимальные требования к каналу связи между рабочими станциями с программой Kaspersky Endpoint Agent и сервером с программой Kaspersky Sandbox приведены в таблице ниже.

Минимальные требования к каналу связи между сервером Kaspersky Sandbox и рабочими станциями с Kaspersky Endpoint Agent

Количество рабочих станций с программой Kaspersky Endpoint Agent	Требуемая пропускная способность канала связи, зарезервированная для Kaspersky Endpoint Agent (Мбит/с)
10	2
20	2
30	2
40	2
50	3
100	4
150	4
200	5
250	5
500	6
750	8
1000	9
1500	11
2000	13
2500	15
3000	18
3500	20
4000	22
4500	24
5000	27

Совместимость решения Kaspersky Sandbox версии 1.0 с другими программами

Kaspersky Sandbox версии 1.0 поддерживает интеграцию с Kaspersky Security Center версии 11.0.0.1131 патч B.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать решение Kaspersky Sandbox.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Sandbox.
- В веб-интерфейсе программы в меню  по ссылке **Лицензионное соглашение**.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

В Kaspersky Sandbox предусмотрены следующие типы лицензий:

- NFR (not for resale / не для перепродажи) – бесплатная лицензия на определенный период, предназначенная для ознакомления с программой и тестовых развертываний программы.
- Коммерческая – платная лицензия, предоставляемая при приобретении программы.

По истечении срока действия лицензии программа продолжает работу, но с ограниченной функциональностью. Чтобы использовать программу в режиме полной функциональности, вам нужно приобрести коммерческую лицензию или продлить срок действия коммерческой лицензии.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Чтобы добавить ключ в программу,

загрузите файл ключа.

Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы программы требуется добавить другой лицензионный ключ.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения программы или после заказа пробной версии программы.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа обратитесь к продавцу лицензии.

Просмотр информации о лицензии в веб-интерфейсе

Чтобы просмотреть информацию о лицензии и добавленных ключах,

в веб-интерфейсе программы выберите раздел **Параметры программы**.

Отобразится следующая информация о лицензии и добавленных ключах:

- серийный номер лицензии;
- описание лицензии;
- дата окончания срока действия лицензии;
- количество дней до окончания срока действия лицензии.

За 30 дней до окончания срока действия лицензии в разделе **Мониторинг** появляется уведомление о необходимости продлить лицензию.

Просмотр текста Лицензионного соглашения в веб-интерфейсе

Чтобы просмотреть текст Лицензионного соглашения в веб-интерфейсе Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса программы нажмите на кнопку  в левой нижней части окна.

   Откроется окно с информацией о программе.

2. По ссылке **Лицензионное соглашение** раскройте окно с текстом Лицензионного соглашения программы.

3. Просмотрите текст Лицензионного соглашения.

4. По окончании просмотра нажмите на кнопку ✕.

Просмотр текста Политики конфиденциальности в веб-интерфейсе

Чтобы просмотреть текст Политики конфиденциальности в веб-интерфейсе Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса программы нажмите на кнопку  в левой нижней части окна.

Откроется окно с информацией о программе.

2. По ссылке **Политика конфиденциальности** раскройте окно с текстом Политики конфиденциальности.

3. Просмотрите текст Политики конфиденциальности.

4. По окончании просмотра нажмите на кнопку ✕.

Добавление лицензионного ключа Kaspersky Sandbox через веб-интерфейс

Чтобы добавить лицензионный ключ, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Параметры**.

2. В блоке параметров **Лицензия** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

3. Выберите файл ключа, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Лицензионный ключ будет добавлен в программу.

Замена лицензионного ключа Kaspersky Sandbox через веб-интерфейс

Чтобы заменить активный лицензионный ключ программы другим лицензионным ключом, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Параметры**.

2. В блоке параметров **Лицензия** нажмите на кнопку **Заменить**.

   Откроется окно выбора файлов.

3. Выберите файл ключа, которым вы хотите заменить активный лицензионный ключ, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Загруженный лицензионный ключ заменит активный лицензионный ключ программы.

Удаление лицензионного ключа Kaspersky Sandbox через веб-интерфейс

Чтобы удалить лицензионный ключ, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Параметры**.
2. В блоке параметров **Лицензия** нажмите на кнопку **Отозвать**.

   Откроется окно подтверждения удаления ключа.
3. Нажмите на кнопку **Да**.

   Окно подтверждения удаления ключа закроется.

Лицензионный ключ будет удален.

Добавление лицензионного ключа Kaspersky Sandbox через KSC

Чтобы добавить лицензионный ключ Kaspersky Sandbox через KSC, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Выберите блок типов задач **Kaspersky Sandbox (KSB)** и тип задачи **Добавить ключ**.
5. Нажмите на кнопку **Далее**.

   Запустится мастер создания задачи.
6. Если вы хотите загрузить ключ с жесткого диска компьютера, на котором вы работаете, выполните следующие действия:

   a. Выберите вариант добавления ключа **Файл ключа** и нажмите на кнопку **Загрузить файл ключа**.

      Откроется окно выбора файлов.

   b. Выберите файл ключа, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

      Окно выбора файлов закроется.

   Ключ будет добавлен. Отобразится информация о лицензии Kaspersky Sandbox.
7. Если вы хотите загрузить ключ из хранилища ключей KSC, выполните следующие действия:

   a. Выберите вариант добавления ключа **Ключ в хранилище** и нажмите на кнопку **Выберите ключ в хранилище**.

      Откроется окно **Хранилище лицензионных ключей KSC**.

   b. Выберите в списке ключ, который вы хотите добавить и нажмите на кнопку **ОК**.

      Окно **Хранилище лицензионных ключей KSC** закроется.

   Ключ будет добавлен. Отобразится информация о лицензии Kaspersky Sandbox.

8. Нажмите на кнопку **Далее**.

9. В открывшемся окне выбора устройств выберите устройства, на которые вы хотите распространить лицензию, и нажмите на кнопку **Далее**.

   Например, вы можете выбрать вариант **Назначить задачу группе администрирования** и выбрать группу администрирования из списка.

10. В окне **Определение название задачи** в поле **Имя** введите название задачи добавления лицензионного ключа и нажмите на кнопку **Далее**.

11. Если вы хотите, чтобы задача запустилась сразу после создания, установите флажок **Запустить задачу после завершения работы мастера** и нажмите на кнопку **Готово**.

Лицензионный ключ Kaspersky Sandbox будет добавлен.

Замена лицензионного ключа Kaspersky Sandbox через KSC

Если вы хотите заменить лицензионный ключ Kaspersky Sandbox через KSC, вам нужно выполните действия по добавлению лицензионного ключа.

Загруженный лицензионный ключ заменит активный лицензионный ключ программы.

Режимы работы программы в соответствии с лицензией

В Kaspersky Sandbox предусмотрены различные режимы работы программы в зависимости от добавленных ключей.

Без лицензии

В этом режиме программа работает с момента установки программы и запуска веб-интерфейса до тех пор, пока вы не добавите ключ.

В режиме Без лицензии действуют следующие ограничения:

- Не обновляются базы программы.
- Ограничен прием и обработка данных от Kaspersky Endpoint Agent.

Коммерческая лицензия

В этом режиме программа обновляет базы, принимает и обрабатывает данные от Kaspersky Endpoint Agent.

По истечении срока годности ключа для коммерческой лицензии программа прекращает обновление баз, прием и обработку данных от Kaspersky Endpoint Agent.

Для возобновления работы программы необходимо заменить ключ или добавить новый ключ для коммерческой лицензии.

О предоставлении данных

Вы можете ознакомиться с перечнем данных и условиями их использования, а также дать согласие на обработку данных в следующих соглашениях между вашей организацией и "Лабораторией Касперского":

- В Лицензионных соглашениях программ Kaspersky Sandbox и Kaspersky Endpoint Agent (например, при установке программы).

  Для активации каждой из программ Kaspersky Sandbox и Kaspersky Endpoint Agent в составе решения Kaspersky Sandbox предусмотрены отдельные Лицензионные соглашения, входящие в комплекты поставки этих программ.

- В Положении о Kaspersky Security Network программы Kaspersky Endpoint Agent.

  При использовании Kaspersky Security Network (далее также "KSN") в "Лабораторию Касперского" автоматически передается информация, полученная в результате работы Kaspersky Endpoint Agent. Перечень передаваемых данных указан в Положении о Kaspersky Security Network. Пользователь Kaspersky Endpoint Agent самостоятельно принимает решение об участии в KSN.

  > Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского".

  > "Лаборатория Касперского" использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно.

Данные программы Kaspersky Sandbox

Программа Kaspersky Sandbox не отправляет данные в "Лабораторию Касперского". Использование Kaspersky Security Network на серверах программы Kaspersky Sandbox не предусмотрено.

На серверах Kaspersky Sandbox хранятся только файлы трассировки и системные журналы.

Данные в файлах трассировки и системных журналах могут содержать следующую информацию:

- Имена файлов, отправленных на проверку.
- IP-адреса и имена хостов, обратившихся к серверам Kaspersky Sandbox.
- IP-адреса и имена серверов Kaspersky Sandbox, входящих в один кластер.
- Имя учетной записи администратора сервера Kaspersky Sandbox.
- IP-адрес и имя прокси-сервера.

- IP-адрес и имя сервера Kaspersky Security Center.
- IP-адреса и имена серверов обновлений.

При работе с системным журналом Kaspersky Sandbox возможен следующий сценарий передачи данных Kaspersky Sandbox в "Лабораторию Касперского":

1. Администратор Kaspersky Sandbox загружает системный журнал Kaspersky Sandbox на жесткий диск компьютера, на котором он работает в веб-интерфейсе Kaspersky Sandbox.
2. Администратор Kaspersky Sandbox отправляет файл системного журнала в Службу технической поддержки "Лаборатории Касперского".

Администратор Kaspersky Sandbox самостоятельно принимает решение о безопасности передачи имен хостов рабочих станций с программой Kaspersky Endpoint Agent в Службу технической поддержки "Лаборатории Касперского".

Данные программы Kaspersky Endpoint Agent

Не используйте Kaspersky Endpoint Agent на тех хостах, передача данных с которых запрещена политикой вашей организации.

Для обеспечения основной функциональности, аудита и повышения скорости решения возникших проблем специалистами Службы технической поддержки "Лаборатории Касперского" Kaspersky Endpoint Agent хранит и обрабатывает данные локально.

На хостах с Kaspersky Endpoint Agent хранятся данные, подготовленные для отправки на серверы Kaspersky Sandbox и в Kaspersky Security Center в автоматическом режиме.

Файлы, подготовленные Kaspersky Endpoint Agent к отправке на проверку на серверы программы, хранятся на хостах с Kaspersky Endpoint Agent в открытом незашифрованном виде в той директории, которая по умолчанию используется для хранения файлов перед отправкой.

Администратору Kaspersky Sandbox необходимо обеспечить безопасность хостов с Kaspersky Endpoint Agent и серверов Kaspersky Sandbox с перечисленными выше данными самостоятельно. Администратор Kaspersky Sandbox несет ответственность за доступ к данной информации.

В этом разделе содержится следующая информация о данных пользователей, хранящихся на хостах с Kaspersky Endpoint Agent:

- состав хранимых данных;
- место хранения;
- срок хранения;

- доступ пользователей к данным.

Данные в полях событий Windows Event Log

Данные о событиях хранятся в файле %SystemRoot%\System32\Winevt\Logs\Kaspersky-Security-Soyuz%4Product.evtx в открытом незашифрованном виде. Данные хранятся до деинсталляции Kaspersky Endpoint Agent.

Эти данные могут передаваться в Kaspersky Security Center в автоматическом режиме и не передаются в Kaspersky Sandbox.

По умолчанию доступ на чтение к файлам имеют только пользователи с правами System и Administrator. Kaspersky Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Данные о событиях могут содержать следующую информацию:

- О пользовательских сессиях в операционной системе.
- Об учетных записях пользователей операционной системы.
- Об ошибках выполнения задач на проверку объектов.
- О задачах на проверку объектов.
- Об обнаружениях.
- Об IOC-файлах, сформированных при автоматическом реагировании.
- О результатах проверки объектов.
- О сертификатах серверов Kaspersky Sandbox.
- Об очереди объектов на проверку.
- Об изменении параметров Kaspersky Endpoint Agent.
- Об изменении политик KSC.
- Об изменении статуса задачи на проверку.
- О политиках KSC.
- Об объектах на карантине.
- О действиях по автоматическому реагированию на обнаруженные угрозы.
- Об ошибках взаимодействия с сервером программы, входящим в кластер.

Данные в запросах к Kaspersky Sandbox

При отправке запросов в Kaspersky Sandbox в полях запросов передаются следующие данные:

- MD5-хеш задачи на проверку.
- ID задачи на проверку.
- Проверяемый объект и все связанные с ним файлы.

Служебные данные

К служебным данным Kaspersky Endpoint Agent относятся:

- данные, попадающие в файлы конфигурации в результате настройки параметров администратором;
- данные, обрабатываемые при автоматическом реагировании на угрозы;
- данные, обрабатываемые при интеграции с Kaspersky Sandbox.

Служебные данные хранятся в файле %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<product version>. Данные в подкаталоге Settings зашифрованы с помощью Encrypting File System (EFS). Данные хранятся до деинсталляции Kaspersky Endpoint Agent.

Эти данные могут передаваться в Kaspersky Security Center в автоматическом режиме и не передаются в Kaspersky Sandbox.

По умолчанию доступ к файлам имеют только пользователи с правами System (полный доступ) и Administrator (чтение и исполнение). Папка %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<product version> и подпапка Restored также доступны пользователю с правами User (только чтение).

Kaspersky Endpoint Agent хранит следующие данные об автоматическом реагировании и интеграции с Kaspersky Sandbox:

1. Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров Kaspersky Endpoint Agent.
    - Пароль доступа к Kaspersky Endpoint Agent.
    - Файлы на карантине.
    - Параметры Kaspersky Endpoint Agent.
    - Учетные данные пользователей операционной системы для запуска задач с правами пользователя.
    - Учетные данные для авторизации на Сервере администрирования Kaspersky Security Center.
    - Учетные данные для авторизации на прокси-сервере.
    - Адреса пользовательских источников обновлений.
    - Открытый ключ сертификата для интеграции с Kaspersky Sandbox.
2. Кеш Kaspersky Endpoint Agent.

- Время записи результата проверки в кеш.
- MD5-хеш задачи на проверку.
- ID задачи на проверку.
- Результат проверки объекта.

3. Очередь запросов на проверку объекта.
   - ID объекта в очереди.
   - Время помещения объекта в очередь.
   - Статус обработки объекта в очереди.
   - ID пользовательской сессии в операционной системе, в которой создана задача на проверку.
   - SID пользователя операционной системы, под учетной записью которого создана задача на проверку.
   - MD5-хеш задачи на проверку.
4. Информация о задачах, для которых Kaspersky Endpoint Agent ожидает результат проверки от Kaspersky Sandbox.
   - Время получения задачи на проверку.
   - Статус обработки объекта.
   - ID пользовательской сессии в операционной системе, в которой создана задача на проверку.
   - ID задачи на проверку.
   - MD5-хеш задачи на проверку.
   - SID пользователя операционной системы, под учетной записью которого создана задача на проверку.
   - XML-схема автоматически созданного IOC.
   - MD5-, SHA256-хеш проверяемого объекта.
   - Ошибки обработки.
   - Имя/имена объектов, для которых создана задача на проверку.
   - Результат проверки объекта.

Данные в файлах трассировки и дампов

Kaspersky Endpoint Agent может выполнять запись отладочной информации в соответствии с заданными параметрами в файлы трассировки для оказания поддержки во время работы Kaspersky Endpoint Agent.

Файлы дампов Kaspersky Endpoint Agent формируются операционной системой при сбоях программы и перезаписываются при каждом сбое.

В файлы трассировки и дампов могут попасть любые персональные данные пользователя или конфиденциальные данные вашей организации.

> Не используйте Kaspersky Endpoint Agent на хостах, передача данных с которых запрещена политикой вашей организации.

По умолчанию Kaspersky Endpoint Agent не записывает отладочную информацию.

Автоматическая отправка файлов трассировки и дампов за пределы хоста, на котором они были сформированы, не производится. Содержимое файлов трассировки можно просмотреть с помощью стандартных средств просмотра текстовых файлов. Файлы трассировки и дампов хранятся бессрочно и не удаляются при деинсталляции Kaspersky Endpoint Agent.

Отладочная информация может понадобиться при обращении в Службу технической поддержки.

Специальных механизмов ограничения доступа к файлам трассировки и дампов не предусмотрено. Администратор может самостоятельно настроить запись этой информации в защищенную папку.

Путь к папке для записи файлов трассировки и дампов по умолчанию не задан. Администратору нужно указать папку для записи файлов трассировки и дампов самостоятельно.

Данные в файлах трассировки и дампов могут содержать следующую информацию:

- Действия, выполненные Kaspersky Endpoint Agent на хосте.
- Информация об объектах, обрабатываемых Kaspersky Endpoint Agent.
- Ошибки, возникшие в процессе работы Kaspersky Endpoint Agent.

Установка и первоначальная настройка решения

В этом разделе содержатся инструкции по установке и первоначальной настройке Kaspersky Sandbox.

Подготовка IT-инфраструктуры к установке Kaspersky Sandbox

Перед установкой программы подготовьте IT-инфраструктуру вашей организации:

1. Убедитесь, что серверы, а также компьютер, предназначенный для работы с веб-интерфейсом программы, и рабочие станции, на которых устанавливается EPP и Kaspersky Endpoint Agent, удовлетворяют аппаратным и программным требованиям.

2. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке Kaspersky Sandbox:

   a. Для обоих сетевых интерфейсов запретите доступ сервера Kaspersky Sandbox в локальную сеть организации для обеспечения безопасности сети от анализируемых объектов.

   b. Для первого сетевого интерфейса разрешите доступ сервера Kaspersky Sandbox в интернет для обновления баз и анализа поведения объектов.

   c. Для второго сетевого интерфейса:

      Разрешите входящее соединение сервера Kaspersky Sandbox на следующие порты:

      - TCP 22 для подключения к серверу по протоколу SSH.
      - TCP 80 и 8443 для использования веб-интерфейса программы.
      - TCP 443 для взаимодействия с внешними системами с помощью интерфейса REST API, для добавления серверов в кластер, для получения задач на обработку объектов от программы Kaspersky Endpoint Agent, для балансировки задач на обработку объектов между серверами кластера.
      - TCP 3301 для синхронизации данных об обработанных объектах между серверами кластера.
      - TCP 13299 для интеграции с Kaspersky Security Center.
      - UDP 15000 для взаимодействия с агентом администрирования (nagent) Kaspersky Security Center.

      Разрешите исходящее соединение сервера Kaspersky Sandbox на следующие порты:

      - TCP 443 и 80 для обновления баз.
      - TCP 13000 и 14000 для синхронизации данных с агентом администрирования (nagent) Kaspersky Security Center. Порты настраиваются на стороне Kaspersky Security Center. TCP 13000 и 14000 – значения по умолчанию, вы можете их изменить.

3. Разрешите входящее соединение рабочих станций, на которых устанавливается EPP и Kaspersky Endpoint Agent, и сервера Kaspersky Sandbox напрямую, без использования прокси-сервера.

4. Разрешите на сетевом оборудовании шифрованный канал связи между серверами Kaspersky Sandbox.

При необходимости вы можете назначить другие порты для работы Kaspersky Sandbox в меню администратора сервера Kaspersky Sandbox. При изменении портов в меню администратора вам нужно разрешить соединения на эти порты внутри IT-инфраструктуры вашей организации.

Порядок установки и настройки программ решения Kaspersky Sandbox

Выполняйте действия по установке и настройке программ решения в следующем порядке:

1. Установите образ диска с Kaspersky Sandbox
2. Выполните первоначальную настройку Kaspersky Sandbox через веб-интерфейс
3. Установите образ диска операционной системы Microsoft Windows 7 и программ для работы Kaspersky Sandbox
4. Настройте интеграцию Kaspersky Sandbox с Kaspersky Security Center
5. Установите EPP и программу Kaspersky Endpoint Agent на рабочих станциях, входящих в IT-инфраструктуру организации
6. Установите плагин управления Kaspersky Sandbox и Kaspersky Endpoint Agent в KSC
7. Настройте интеграцию Kaspersky Endpoint Agent с Kaspersky Sandbox
8. Настройте остальные параметры Kaspersky Sandbox
9. Настройте политики Kaspersky Endpoint Agent в KSC

Подготовка Kaspersky Sandbox к работе в виртуальной инфраструктуре

Для развертывания программы на виртуальной платформе должен быть установлен гипервизор VMware ESXi версии 6.7.0.

Kaspersky Sandbox, установленный на виртуальную машину, может обрабатывать объекты от 250 рабочих станций, или 100 объектов в час, полученных по API.

При установке Kaspersky Sandbox на виртуальную машину VMware ESXi настройте следующую конфигурацию:

- Процессор (CPU): 12 ядер (6 сокетов по 2 ядра).
- Объем оперативной памяти (Memory): 32 ГБ.
- Объем жесткого диска: 600 ГБ.
- Два сетевых адаптера со скоростью передачи данных 1 Гбит/с.

  На виртуальной машине:

  1. Разрешите вложенную виртуализацию.
  2. Установите параметр **High Latency Sensitivity**.
  3. Зарезервируйте всю оперативную память (32 ГБ).
  4. Зарезервируйте всю частоту процессора (26400 МГц).
- Установите параметр **Expose hardware assisted virtualization to the guest OS**.

Клонирование виртуальных машин не поддерживается.

Подробнее о работе с гипервизором VMware ESXi см. в *документации VMware ESXi*.

Установка программы Kaspersky Sandbox

Этот раздел представляет собой пошаговую инструкцию по установке программы Kaspersky Sandbox.

Шаг 1. Начало установки программы Kaspersky Sandbox и выбор языка для просмотра Лицензионных соглашений

Чтобы приступить к установке Kaspersky Sandbox и выбрать язык для просмотра лицензионных соглашений, выполните следующие действия:

1. Запустите образ диска Kaspersky Sandbox.

   Запустится мастер установки.

2. Выберите **Install - Kaspersky Sandbox**.

3. В открывшемся окне нажмите на кнопку **Ok**.

   Откроется окно выбора языка для просмотра Лицензионных соглашений.

4. Выберите язык.

   Например, если вы хотите просмотреть Лицензионные соглашения на английском языке, выберите **English**.

5. Нажмите на клавишу **ENTER**.

   Мастер установки перейдет к следующему шагу.

Шаг 2. Просмотр Лицензионного соглашения Kaspersky Sandbox и Политики конфиденциальности

Для продолжения установки вам нужно просмотреть Лицензионное соглашение Kaspersky Sandbox и Политику конфиденциальности и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

Чтобы принять условия Лицензионного соглашения Kaspersky Sandbox и Политики конфиденциальности, выполните следующие действия:

1. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности.

2. Если вы принимаете условия Лицензионного соглашения и Политики конфиденциальности, нажмите на кнопку **I accept the terms**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Просмотр Лицензионного соглашения Adobe

Для продолжения установки вам нужно просмотреть Лицензионное соглашение Adobe и принять его условия. Если условия Лицензионного соглашения не приняты, установка не выполняется.

Чтобы принять условия Лицензионного соглашения Adobe, выполните следующие действия:

1. Ознакомьтесь с Лицензионным соглашением.
2. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept the terms**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Просмотр Лицензионного соглашения Microsoft

Для продолжения установки вам нужно просмотреть Лицензионное соглашение Microsoft и принять его условия. Если условия Лицензионного соглашения не приняты, установка не выполняется.

Чтобы принять условия Лицензионного соглашения Microsoft, выполните следующие действия:

1. Ознакомьтесь с Лицензионным соглашением.
2. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept the terms**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Подтверждение конфигурации Kaspersky Sandbox

Чтобы подтвердить конфигурацию Kaspersky Sandbox,

Нажмите на кнопку **Ok**.

Расчет конфигурации производится в соответствии с Аппаратными и программными требованиями.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор диска для установки Kaspersky Sandbox

На этом шаге выберите физический диск для установки Kaspersky Sandbox.

Чтобы выбрать диск для установки Kaspersky Sandbox, выполните следующие действия:

1. В окне **Select device** в списке дисков выберите диск.
2. Нажмите на клавишу **ENTER**.

   Откроется окно подтверждения действия.
3. Нажмите на кнопку **Install**.

Архив с установочными файлами распакуется на диск. Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 7. Назначение имени хоста

Чтобы назначить имя хоста Kaspersky Sandbox для использования DNS-серверами, выполните следующие действия:

1. В поле **Hostname** введите полное доменное имя сервера.

   Указывайте имя сервера в формате FQDN (например, host.domain.com или host.domain.subdomain.com).

2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Выбор управляющего сетевого интерфейса в списке

Для работы Kaspersky Sandbox необходимо подключить минимум две сетевые карты и настроить следующие сетевые интерфейсы:

- Управляющий сетевой интерфейс. Этот интерфейс предназначен для управления программой Kaspersky Sandbox через веб-интерфейс. Также через этот интерфейс сервер Kaspersky Sandbox будет принимать объекты от EPP и программы Kaspersky Endpoint Agent.
- Сетевой интерфейс для доступа обрабатываемых объектов в интернет. Через этот интерфейс объекты, которые обрабатывает Kaspersky Sandbox, смогут предпринимать попытки действий в интернете, а Kaspersky Sandbox сможет анализировать их поведение. Если вы запретите доступ в интернет, Kaspersky Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

  > Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

На этом шаге выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.

Чтобы выбрать управляющий сетевой интерфейс, выполните следующие действия:

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.

2. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Назначение адреса, маски сети и шлюза управляющего интерфейса

Чтобы назначить IP-адрес, маску сети и шлюз управляющего сетевого интерфейса, выполните следующие действия:

1. В поле **Address** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
2. В поле **Netmask** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
3. В поле **Default gateway** введите IP-адрес шлюза по умолчанию.
4. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Создание учетной записи администратора Kaspersky Sandbox

На этом шаге создайте учетную запись администратора для работы в веб-интерфейсе программы и в консоли управления сервером Kaspersky Sandbox.

Чтобы создать учетную запись администратора Kaspersky Sandbox, выполните следующие действия:

1. В поле **Username** введите имя учетной записи администратора. По умолчанию используется учетная запись admin.
2. В поле **Password** введите пароль учетной записи администратора.

   Пароль должен удовлетворять следующим требованиям:

   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ;
   - не должен совпадать с именем пользователя.
3. В поле **Confirm password** введите пароль повторно.
4. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 11. Завершение установки Kaspersky Sandbox

На этом шаге отобразится URL-адрес сервера Kaspersky Sandbox, по которому вы можете войти в веб-интерфейс программы и выполнить настройку Kaspersky Sandbox.

Чтобы завершить установку Kaspersky Sandbox,

нажмите на кнопку **Ok**.

Сервер будет перезагружен. Перейдите к настройке Kaspersky Sandbox через веб-интерфейс.

Начало работы с программой Kaspersky Sandbox

Этот раздел содержит информацию о том, как начать работу с программой Kaspersky Sandbox в веб-интерфейсе и в режиме Technical Support Mode.

Управление параметрами программы Kaspersky Sandbox осуществляется через веб-интерфейс Kaspersky Sandbox и через Kaspersky Security Center.

При неполадках в работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить действия в меню администратора Kaspersky Sandbox или в режиме Technical Support Mode.

Например, вас могут попросить выполнить следующие действия:

- Активировать функциональность получения расширенной диагностической информации.
- Дополнительно настроить отдельные компоненты программы, недоступные для изменения стандартными средствами пользовательского интерфейса.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся информация, необходимая для выполнения перечисленных действий (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и т.д.), а также состав данных, собираемых в отладочных целях, будут озвучены вам специалистами Службы технической поддержки. Собранная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка собранных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в документации программы или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютеров, а также к нарушению доступности и целостности обрабатываемой информации.

Начало работы в веб-интерфейсе Kaspersky Sandbox

Веб-интерфейс Kaspersky Sandbox расположен на том сервере, на который вы установили программу.

Веб-интерфейс Kaspersky Sandbox защищен от *CSRF-атак* и работает только в том случае, если браузер пользователя веб-интерфейса программы предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Kaspersky Sandbox, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом Kaspersky Sandbox осуществляется через прокси-сервер вашей организации, убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

Чтобы начать работу в веб-интерфейсе Kaspersky Sandbox, выполните следующие действия:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Kaspersky Sandbox, введите IP-адрес сервера, отобразившийся на заключительном шаге установки программы.

   Откроется окно ввода учетных данных пользователя Kaspersky Sandbox.

2. Введите имя пользователя и пароль доступа к веб-интерфейсу программы, которые вы задали при установке программы.

Вы можете начать работу в веб-интерфейсе Kaspersky Sandbox.

Начало работы в меню администратора Kaspersky Sandbox

Вы можете работать с параметрами Kaspersky Sandbox в меню администратора в консоли управления каждого сервера, на котором установлена программа.

Чтобы начать работу в меню администратора Kaspersky Sandbox в консоли управления сервером Kaspersky Sandbox, выполните следующие действия:

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы (Установка и первоначальная настройка решения, Шаг 10. Создание учетной записи администратора Kaspersky Sandbox).

   Отобразится меню администратора программы.

Вы можете начать работу в меню администратора программы.

Начало работы с Kaspersky Sandbox в режиме Technical Support Mode

Не рекомендуется выполнять действия с Kaspersky Sandbox в режиме Technical Support Mode без консультации или указаний сотрудников Службы технической поддержки.

Режим Technical Support Mode предоставляет администратору Kaspersky Sandbox неограниченные права (root) доступа к программе и всем данным (в том числе персональным), которые в ней хранятся.

Работа с Kaspersky Sandbox из консоли управления в режиме Technical Support Mode с правами учетной записи суперпользователя позволяет выполнять следующие действия:

- Управлять параметрами работы программы с помощью конфигурационных файлов.

  При этом могут быть изменены параметры шифрования данных при передаче между серверами программы, параметры хранения и обработки объектов проверки.

  В этом случае данные передаются в открытом виде. Администратору Kaspersky Sandbox необходимо обеспечить безопасность серверов с этими данными самостоятельно. Администратор Kaspersky Sandbox несет ответственность за изменение конфигурационных файлов программы.

- Управлять параметрами журнала трассировки.

  Файлы трассировки могут содержать конфиденциальные данные пользователя.

Чтобы начать работу с программой в режиме Technical Support Mode, выполните следующие действия:

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы (Установка и первоначальная настройка решения, Шаг 10. Создание учетной записи администратора Kaspersky Sandbox).

   Отобразится меню администратора компонента программы.

3. В меню администратора программы выберите режим **Technical Support Mode**.

4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Если вы действительно хотите выполнять действия с программой в режиме Technical Support Mode, выберите **Yes** и нажмите на клавишу **ENTER**.

Управление Kaspersky Sandbox через веб-интерфейс

Веб-интерфейс Kaspersky Sandbox защищен от *CSRF-атак* и работает только в том случае, если браузер пользователя веб-интерфейса предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Sandbox, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом осуществляется через прокси-сервер вашей организации, проверьте параметры и убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

Чтобы начать работу в веб-интерфейсе Kaspersky Sandbox, выполните следующие действия:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Kaspersky Sandbox, введите IP-адрес сервера Kaspersky Sandbox.

   Откроется окно ввода учетных данных администратора Kaspersky Sandbox.

2. Введите имя пользователя и пароль администратора Kaspersky Sandbox, который вы задали при установке программы.

Вы можете начать работу в веб-интерфейсе программы.

Первоначальная настройка программы

Первоначальная настройка программы представляет собой последовательность шагов. Мастер первоначальной настройки программы запускается автоматически после первого входа в веб-интерфейс.

Вы можете пропустить шаги первоначальной настройки программы и выполнить настройку позднее.

Установка даты и времени

Чтобы установить дату и время Kaspersky Sandbox, выполните следующие действия:

1. В раскрывающемся списке **Страна** выберите нужную страну.
2. В раскрывающемся списке **Часовой пояс** выберите нужный часовой пояс.
3. Если вы хотите синхронизировать время с NTP-сервером, включите переключатель справа от названия параметра **Синхронизация с NTP-серверами**.
4. Если вы хотите установить дату и время вручную, не включайте переключатель справа от названия параметра **Синхронизация с NTP-серверами** и выполните следующие действия:
   a. В поле **Дата** введите текущую дату или нажмите на кнопку 🗓 и выберите дату в календаре.
   b. В поле **Время** введите текущее время.
5. Нажмите на кнопку **Далее** в нижней части окна.

Мастер первоначальной настройки перейдет к следующему шагу.

Добавление лицензионного ключа

Чтобы добавить лицензионный ключ, выполните следующие действия:

1. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

2. Выберите файл ключа, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

   Лицензионный ключ будет добавлен в программу. В окне мастера первоначальной настройки отобразится информация о лицензии.

3. Нажмите на кнопку **Далее** в нижней части окна.

Мастер первоначальной настройки перейдет к следующему шагу.

Вы можете пропустить этот шаг и добавить лицензионный ключ позднее одним из следующих способов: - Добавить ключ через веб-интерфейс Kaspersky Sandbox. - Создать задачу распространения лицензии на серверы Sandbox в Kaspersky Security Center.

Настройка параметров DNS

Чтобы настроить параметры DNS, выполните следующие действия:

1. Нажмите на кнопку **Добавить**.

   Добавится пустое поле ввода IP-адреса DNS-сервера.

2. Введите IPv4-адрес основного DNS-сервера.

3. Если вы хотите добавить дополнительный DNS-сервер, повторите действия 1-2.

4. Если вы хотите удалить добавленный DNS-сервер, нажмите на кнопку справа от строки с IP-адресом DNS-сервера.

5. Нажмите на кнопку **Далее** в нижней части окна.

Мастер первоначальной настройки перейдет к следующему шагу.

Вы можете пропустить этот шаг и добавить DNS-серверы позднее через веб-интерфейс Kaspersky Sandbox.

Настройка интеграции с Kaspersky Security Center

Чтобы настроить интеграцию с Kaspersky Security Center, выполните следующие действия:

1. В поле **Адрес сервера KSC** введите адрес и порт сервера Kaspersky Security Center.

2. Если вы хотите установить доверенное соединение с сервером Kaspersky Security Center, установите флажок **Использовать TLS-шифрование**.

3. Нажмите на кнопку **Далее** в нижней части окна.

   Мастер первоначальной настройки перейдет к следующему шагу.

Вы можете пропустить этот шаг и подключиться к Kaspersky Security Center позднее через веб-интерфейс Kaspersky Sandbox.

Вам также понадобится настроить интеграцию на стороне Kaspersky Security Center через консоль администрирования KSC.

Чтобы настроить интеграцию с Kaspersky Security Center на стороне Kaspersky Security Center, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Нераспределенные устройства**.

3. В списке нераспределенных устройств выберите сервер Kaspersky Sandbox и правой кнопкой мыши раскройте меню действий над устройствами.

4. Выберите пункт меню **Переместить в группу**.

5. В открывшемся окне выберите группу устройств Kaspersky Security Center, с которыми вы хотите работать в Kaspersky Sandbox и нажмите на кнопку **ОК**.

   Например, вы можете выбрать группу **Управляемые устройства**, создать новую группу в группе **Управляемые устройства** и поместить сервер Kaspersky Sandbox в созданную группу.

Kaspersky Security Center отображает устройства, с которыми настроена интеграция, в группах управляемых устройств. Статусы работоспособности этих устройств отображаются на панели мониторинга. Если в работе этих устройств возникают проблемы, Kaspersky Security Center отображает статусы **Критический** или **Предупреждение** для привлечения внимания администратора.

Поскольку сервер Kaspersky Sandbox не является стандартной рабочей станцией, управляемой через KSC, требуется отдельно настроить отображение статусов устройств Kaspersky Sandbox в KSC.

> Для корректного отображения статусов устройств Kaspersky Sandbox в KSC необходимо поместить серверы Kaspersky Sandbox в отдельную группу управляемых устройств.

Сервер Kaspersky Sandbox отобразится в списке устройств группы устройств дерева консоли KSC.

Интеграция Kaspersky Sandbox с Kaspersky Security Center будет настроена.

Загрузка ISO-образов операционных систем и программ для работы Kaspersky Sandbox и настройка сетевого интерфейса для доступа обрабатываемых объектов в интернет

Объекты, которые обрабатывает Kaspersky Sandbox, могут предпринимать попытки действий в интернете через сетевой интерфейс для доступа обрабатываемых объектов в интернет. Kaspersky Sandbox может анализировать поведение этих объектов.

Если вы запретите доступ в интернет, Kaspersky Sandbox будет использовать эмуляцию доступа в интернет, чтобы компенсировать снижение уровня обнаружений, связанное с отсутствием доступа обрабатываемых объектов в интернет.

Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

Если в соответствии с политикой безопасности вашей организации с компьютеров пользователей локальной сети запрещен доступ в интернет, и вы настроили сетевой интерфейс Kaspersky Sandbox для доступа обрабатываемых объектов в интернет, есть риск возникновения следующего сценария:

Злоумышленник может прикрепить вредоносную программу к произвольному файлу и запустить Sandbox-проверку этого файла с компьютера пользователя локальной сети. Этот файл будет выведен за пределы локальной сети через сетевой интерфейс для доступа обрабатываемых объектов в интернет в процессе проверки файла программой Kaspersky Sandbox.

Если у виртуальных машин нет доступа в интернет, уровень обнаружений Kaspersky Sandbox может быть значительно снижен.

Чтобы загрузить ISO-образ операционной системы и программ, необходимых для работы Kaspersky Sandbox, а также настроить сетевой интерфейс для доступа обрабатываемых объектов в интернет, выполните следующие действия:

1. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

2. Выберите образ операционной системы, входящий в комплект поставки (файл формата ISO), который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

   В списке отобразится загруженный образ операционной системы и программ, необходимых для работы Kaspersky Sandbox. Извлечение файлов и установка виртуальной машины и программ будут выполнены автоматически.

3. В списке **Сетевой интерфейс** выберите сетевой интерфейс, который вы хотите использовать для доступа обрабатываемых объектов в интернет.

Управляющий сетевой интерфейс недоступен для выбора в этом списке сетевых интерфейсов.

4. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
5. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
6. В поле **Шлюз по умолчанию** введите адрес шлюза сети, в которой вы хотите использовать этот сетевой интерфейс.
7. Нажмите на кнопку **Далее** в нижней части окна.

   Мастер первоначальной настройки перейдет к следующему шагу.
8. Нажмите на кнопку **Завершить**.

Вы можете пропустить этот шаг и настроить интерфейс для доступа виртуальных машин в интернет позднее через веб-интерфейс Kaspersky Sandbox.

Первоначальная настройка программы будет завершена, вы перейдете в веб-интерфейс программы.

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы Kaspersky Sandbox в разделах **Мониторинг** и **Управление кластерами** веб-интерфейса Kaspersky Sandbox, а также в разделе **Сервер администрирования** на закладке **Мониторинг** программы Kaspersky Security Center.

Для быстрой оценки состояния работы программы используются цветовые индикаторы. Цель администратора заключается в том, чтобы поддерживать все индикаторы в состоянии "зеленый".

Если все индикаторы зеленого цвета, Kaspersky Sandbox работает в штатном режиме.

Если хотя бы один индикатор желтого цвета, Kaspersky Sandbox работает, но требует внимания администратора.

Если хотя бы один индикатор красного или серого цвета, Kaspersky Sandbox не принимает объекты на обработку от Kaspersky Endpoint Agent и требует внимания администратора.

В разделе **Мониторинг** окна веб-интерфейса Kaspersky Sandbox отображается следующая информация:

- **Самодиагностика**. Индикаторы и описание состояния самодиагностики программы.
- **Обновление баз**. Индикаторы и описание состояния обновления баз программы.

- **Лицензия**. Индикаторы и описание статуса активации программы и срока действия лицензии.
- **Обработанные объекты**. График, отображающий статус обработки объектов, поступающих от программы Kaspersky Endpoint Agent.

В разделе **Управление кластерами** веб-интерфейса Kaspersky Sandbox отображается следующая информация:

- **В сети**. Индикаторы и количество серверов кластера:
  - в сети;
  - не в сети.
- **Самодиагностика**. Индикаторы и количество серверов кластера:
  - работающих в штатном режиме;
  - требующих устранения проблем в работе.
- **Обновление баз**.Индикаторы и количество серверов:
  - с актуальной версией баз;
  - требующих обновления баз.
- **Лицензия**.Индикаторы и количество серверов:
  - с успешно активированной программой Kaspersky Sandbox;
  - требующих загрузки лицензионного ключа или активации программы.

Информация о самодиагностике программы в веб-интерфейсе Kaspersky Sandbox

Для быстрой оценки состояния самодиагностики Kaspersky Sandbox используются цветовые индикаторы зеленого, красного и серого цвета.

Индикатор **Самодиагностика** зеленого цвета отображается при выполнении следующих условий:

- Самодиагностика программы запускалась недавно и завершилась успешно.
- Kaspersky Sandbox работает без ошибок.
- Все системы работают без ошибок.

Индикатор **Самодиагностика** красного цвета отображается в следующих случаях:

- Последний запуск самодиагностики программы был более часа назад.
- Самодиагностика завершилась с ошибкой.

- Самодиагностика выявила проблемы в работе программы.
- Необходимо повторно активировать образ виртуальной машины.

Индикатор **Самодиагностика** серого цвета отображается в следующих случаях:

- Программа не активирована: на сервер не загружен лицензионный ключ или срок действия лицензии истек.
- Не удалось получить данные о самодиагностике от одного или нескольких серверов кластера Kaspersky Sandbox.

Информация о состоянии обновления баз в веб-интерфейсе Kaspersky Sandbox

Для быстрой оценки состояния обновления баз Kaspersky Sandbox используются цветовые индикаторы зеленого, желтого и серого цвета.

Индикатор **Обновление баз** зеленого цвета отображается при выполнении следующих условий:

- Базы актуальны.
- Последнее успешное обновление баз выполнялось менее 24 часов назад.
- Программа активирована.

Индикатор **Обновление баз** желтого цвета отображается, если последнее успешное обновление баз выполнялось более 24 часов назад.

Индикатор **Обновление баз** серого цвета отображается в следующих случаях:

- Программа не активирована: на сервер не загружен лицензионный ключ или истек срок действия лицензии.
- Не удалось получить данные о состоянии обновления баз от одного или нескольких серверов кластера Kaspersky Sandbox.

Информация о статусе активации программы и сроке действия лицензии в веб-интерфейсе Kaspersky Sandbox

Для быстрой оценки статуса активации программы и срока действия лицензии Kaspersky Sandbox в разделе **Мониторинг** веб-интерфейса Kaspersky Sandbox используются цветовые индикаторы зеленого, желтого, красного и серого цвета.

Индикатор **Лицензия** зеленого цвета отображается при выполнении следующих условий:

- Программа активирована.
- Сервер использует действующую лицензию.
- До окончания срока действия лицензии осталось более 30 дней.

Индикатор **Лицензия** желтого цвета отображается, если до окончания срока действия лицензии осталось менее 30 дней.

Индикатор **Лицензия** красного цвета отображается в следующих случаях:

- На сервер не загружен лицензионный ключ.
- Срок действия лицензии истек.

Индикатор **Лицензия** серого цвета отображается, если не удалось получить данные о статусе активации программы и сроке действия лицензии от одного или нескольких серверов кластера Kaspersky Sandbox.

По ссылке **Перейти к управлению лицензией** вы можете перейти в раздел **Параметры** веб-интерфейса программы, и в блоке параметров **Лицензия** заменить или загрузить новый лицензионный ключ.

Настройка периода отображения данных на графике в веб-интерфейсе Kaspersky Sandbox

Вы можете настроить отображение данных на графике **Обработанные объекты** за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

Чтобы настроить отображение данных за сутки (с 00:00 до 23:59), выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **День**.
3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите получить данные на графике.

Чтобы настроить отображение данных за неделю (с понедельника по воскресенье), выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите получить данные на графике.

Чтобы настроить отображение данных за месяц (календарный месяц), выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.

2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Месяц**.

3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите получить данные на графике.

Мониторинг обработки объектов, полученных от Kaspersky Endpoint Agent, в веб-интерфейсе Kaspersky Sandbox

В разделе **Мониторинг** веб-интерфейса Kaspersky Sandbox на графике **Обработанные объекты** отображается количество объектов, полученных от программы Kaspersky Endpoint Agent и обработанных программой Kaspersky Sandbox за выбранный период.

Обработанные объекты подсчитываются по следующим категориям:

- **PE-файлы** – (от Portable Executable) исполняемые файлы формата PE_EXE;
- **Документы** – документы поддерживаемых форматов.

На графике **Обработанные объекты** отображается общее количество обработанных объектов независимо от того, обнаружил ли Kaspersky Sandbox угрозу в этих объектах и на каком количестве рабочих станций с программой Kaspersky Endpoint Agent был обнаружен один и тот же объект.

Пример подсчета общего количества обработанных объектов:

Kaspersky Sandbox получил от Kaspersky Endpoint Agent и обработал:

Файл *example.exe* – 1 шт.

Документ *example.docx* – 1 шт.

Документ *example.pdf* – 1 шт.

При этом файл *example.docx* есть на 10 рабочих станциях с программой Kaspersky Endpoint Agent.

На графике **Обработанные объекты** отобразится следующее количество объектов:

PE-файлы – 1 шт.

Документы – 11 шт.

Вы можете настроить отображение количества объектов на графике так, что если один и тот же объект был обнаружен на нескольких рабочих станциях, Kaspersky Sandbox будет отображать его на графике только один раз в количестве 1 шт.

Чтобы настроить отображение количества только уникальных объектов, полученных от программы Kaspersky Endpoint Agent и обработанных программой Kaspersky Sandbox за выбранный период,

установите флажок **Только уникальные объекты** в нижней части графика.

Вместо графика **Обработанные объекты** отобразится график **Обработанные уникальные объекты**.

Пример отображения количества только уникальных обработанных объектов::

Kaspersky Sandbox получил от Kaspersky Endpoint Agent и обработал:

Файл *example.exe* – 1 шт.

Документ *example.docx* – 1 шт.

Документ *example.pdf* – 1 шт.

При этом файл *example.docx* есть на 10 рабочих станциях с программой Kaspersky Endpoint Agent

На графике **Обработанные уникальные объекты** отобразится следующее количество объектов:

PE-файлы – 1 шт.

Документы – 2 шт.

Мониторинг работоспособности Kaspersky Sandbox в KSC

Kaspersky Security Center отображает устройства, с которыми настроена интеграция, в группах управляемых устройств. Статусы работоспособности этих устройств отображаются на панели мониторинга. Если в работе этих устройств возникают проблемы, Kaspersky Security Center отображает статусы **Критический** или **Предупреждение** для привлечения внимания администратора.

Поскольку сервер Kaspersky Sandbox не является стандартной рабочей станцией, управляемой через KSC, требуется отдельно настроить отображение статусов устройств Kaspersky Sandbox в KSC.

Для корректного отображения статусов устройств Kaspersky Sandbox в KSC необходимо поместить серверы Kaspersky Sandbox в отдельную группу управляемых устройств.

Чтобы оценить работоспособность Kaspersky Sandbox в KSC, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Управляемые устройства**, подпапку с новой группой устройств, в которую вы поместили сервер Kaspersky Sandbox.

3. Выберите сервер Kaspersky Sandbox, работоспособность которого вы хотите оценить.

   В верхней части рабочей области отобразится фильтр статусов устройств и количество серверов, имеющих соответствующие статусы.

4. Установите флажки рядом с теми статусами, информацию по которым вы хотите просмотреть. Доступны следующие статусы работоспособности Kaspersky Sandbox:

   ☑ – Статус **Критический**. Отображается для следующих проблем:

   - **Статус устройства определен программой**. Статус устройства определяется управляемой программой. Серверы Kaspersky Sandbox, у которых возникает проблема с

самодиагностикой, будут иметь статус "**Критический**": "**Проблемы с сервером Kaspersky Sandbox. Сервер не принимает объекты на проверку**".

- **Срок действия лицензии истек**. Устройство видимо в сети, но срок действия лицензии истек.

☑ – Статус **Предупреждение**. Отображается для следующих проблем:

- **Срок действия лицензии скоро истечет**. Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.

- **Базы устарели**. Двойным щелчком мыши откройте окно с условиями этого статуса и установите значение 1. Серверы Kaspersky Sandbox, на которых более суток не было успешного запуска задачи обновления баз, будут иметь статус "**Предупреждение**".

✅ – Статус **ОК**. Отображается если у серверов Kaspersky Sandbox нет проблем с самодиагностикой, активацией программы и обновления баз.

В списке серверов Kaspersky Sandbox отобразятся серверы, удовлетворяющие вашим условиям фильтрации статусов.

5. Выберите сервер, информацию о статусе которого вы хотите просмотреть.

   В правой части рабочей области отобразится панель с описанием статуса устройства Kaspersky Sandbox.

Обновление баз

Базы Kaspersky Sandbox представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код и признаки подозрительного поведения объектов.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений автоматически или обновлять базы вручную.

Запуск обновления баз вручную

Чтобы запустить обновление баз вручную, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Обновление баз**.

   В блоке параметров **Последнее обновление** отобразятся время и статус последней попытки обновления баз.

2. Нажмите на кнопку **Запустить обновление**.

Выбор источника обновления баз

Чтобы выбрать источник обновления баз, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Обновление баз**.
2. В блоке параметров **Источник обновлений** выберите источник, из которого вы хотите получать пакет обновлений:
   - **Сервер обновлений "Лаборатории Касперского"**.
   - **Безопасный сервер обновлений "Лаборатории Касперского"**.
   - **Сервер KSC**.
   - **Другой сервер**.

     В качестве **Другой сервер** вы можете использовать только HTTP-сервер.
3. Если вы выбрали **Сервер KSC**, в поле под названием этого параметра укажите IP-адрес сервера KSC.
4. Если вы выбрали **Другой сервер**, в поле под названием этого параметра укажите URL-адрес пакета обновлений на вашем HTTP-сервере или укажите полный путь к директории с пакетом обновлений.
5. Нажмите на кнопку **Применить** в нижней части окна.

Включение и отключение использования прокси-сервера для обновления баз

Чтобы включить или отключить использование прокси-сервера для обновления баз Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Обновление баз**.
2. В рабочей области выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы хотите использовать прокси-сервер при обновлении баз программы.
   - Выключите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы не хотите использовать прокси-сервер при обновлении баз программы.

Настройка параметров соединения с прокси-сервером для обновления баз

Чтобы настроить параметры соединения с прокси-сервером для обновления баз Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Обновление баз**.
2. Включите переключатель рядом с названием блока параметров **Прокси-сервер**.
3. В поле **Адрес** введите адрес и порт прокси-сервера.
4. Выполните одно из следующих действий:
   - Установите флажок **Не использовать прокси-сервер для локальных адресов**, если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации.
   - Снимите флажок **Не использовать прокси-сервер для локальных адресов**, если вы хотите использовать прокси-сервер независимо от принадлежности адресов к вашей организации.
5. В поле **Имя пользователя** введите имя пользователя прокси-сервера.
6. В поле **Пароль** введите пароль подключения к прокси-серверу.
7. Нажмите на кнопку **Применить** в нижней части окна.

Настройка сетевых интерфейсов

В этом разделе содержится информация о настройке сетевых интерфейсов, необходимых для работы Kaspersky Sandbox.

Настройка параметров DNS

> Управление сертификатами Kaspersky Endpoint Agent и сетевыми интерфейсами недоступно после создания кластера.

Чтобы настроить параметры DNS, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Сетевые интерфейсы**.
2. В поле **Имя хоста** введите имя сервера Kaspersky Sandbox в формате FQDN (например, sandbox).
3. Нажмите на кнопку **Добавить** рядом с названием параметра **DNS-серверы**.

   Добавится пустое поле ввода IP-адреса DNS-сервера.
4. Введите IPv4-адрес основного DNS-сервера.
5. Нажмите на кнопку **Применить** в нижней части окна.

   DNS-сервер будет добавлен.
6. Если вы хотите добавить дополнительный DNS-сервер, повторите действия 3-5.

7. Если вы хотите удалить добавленный DNS-сервер, нажмите на кнопку справа от строки с IP-адресом DNS-сервера.

   Вы можете удалить только дополнительные DNS-серверы. Вы не можете удалить основной DNS-сервер. Если вы добавили 2 и более DNS-сервера, вы можете удалить любой из них, при этом оставшийся DNS-сервер будет использоваться в качестве основного.

Настройка управляющего сетевого интерфейса

Управление сертификатами Kaspersky Endpoint Agent и сетевыми интерфейсами недоступно после создания кластера.

Управляющий сетевой интерфейс предназначен для доступа к серверу Kaspersky Sandbox по протоколу SSH.

Вы можете настроить управляющий сетевой интерфейс во время установки программы.

Вы также можете настроить управляющий сетевой интерфейс в веб-интерфейсе программы.

Чтобы настроить управляющий сетевой интерфейс в веб-интерфейсе Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Управляющий интерфейс** в раскрывающемся списке **Сетевой интерфейс** выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу, если IP-адрес не назначен.
4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. В поле **Шлюз по умолчанию** введите адрес шлюза сети, в которой вы хотите использовать этот сетевой интерфейс.
6. Нажмите на кнопку **Применить** в нижней части окна.

Настройка сетевого интерфейса для доступа обрабатываемых объектов в интернет

Объекты, которые обрабатывает Kaspersky Sandbox, могут предпринимать попытки действий в интернете через сетевой интерфейс для доступа обрабатываемых объектов в интернет. Kaspersky Sandbox может анализировать поведение этих объектов.

Если вы запретите доступ в интернет, Kaspersky Sandbox будет использовать эмуляцию доступа в интернет, чтобы компенсировать снижение уровня обнаружений, связанное с отсутствием доступа обрабатываемых объектов в интернет.

Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

Если в соответствии с политикой безопасности вашей организации с компьютеров пользователей локальной сети запрещен доступ в интернет, и вы настроили сетевой интерфейс Kaspersky Sandbox для доступа обрабатываемых объектов в интернет, есть риск возникновения следующего сценария:

Злоумышленник может прикрепить вредоносную программу к произвольному файлу и запустить Sandbox-проверку этого файла с компьютера пользователя локальной сети. Этот файл будет выведен за пределы локальной сети через сетевой интерфейс для доступа обрабатываемых объектов в интернет в процессе проверки файла программой Kaspersky Sandbox.

Если у виртуальных машин нет доступа в интернет, уровень обнаружений Kaspersky Sandbox может быть значительно снижен.

Чтобы настроить сетевой интерфейс для доступа обрабатываемых объектов в интернет, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Виртуальные машины**.
2. В группе параметров **Интерфейс для доступа виртуальных машин в интернет** в списке **Сетевой интерфейс** выберите сетевой интерфейс, который вы хотите использовать для доступа обрабатываемых объектов в интернет.

   Управляющий сетевой интерфейс недоступен для выбора в этом списке сетевых интерфейсов.

3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. В поле **Шлюз по умолчанию** введите адрес шлюза сети, в которой вы хотите использовать этот сетевой интерфейс.
6. Нажмите на кнопку **Применить**.

Добавление, изменение и удаление статических сетевых маршрутов

Управление сертификатами Kaspersky Endpoint Agent и сетевыми интерфейсами недоступно после создания кластера.

Чтобы добавить статический сетевой маршрут, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** нажмите на кнопку **Добавить**.

   В списке статических сетевых маршрутов добавится строка с пустыми полями.
3. В поле **IP** введите префикс подсети.
4. В поле **Маска** введите маску подсети.
5. В поле **Шлюз** введите IP-адрес шлюза.
6. В списке **Сетевой интерфейс** выберите сетевой интерфейс, для которого вы хотите добавить статический сетевой маршрут.
7. Нажмите на кнопку ✓.
8. Нажмите на кнопку **Применить** в нижней части окна.

Чтобы удалить статический сетевой маршрут, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите удалить, нажмите на кнопку 🗑.
3. Нажмите на кнопку **Применить** в нижней части окна.

Чтобы изменить статический сетевой маршрут, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите изменить, нажмите на кнопку ✎.

   Строка статического сетевого маршрута станет доступна для редактирования.
3. Внесите необходимые изменения.
4. Нажмите на кнопку ✓.

5. Нажмите на кнопку **Применить** в нижней части окна.

Настройка интеграции с Kaspersky Security Center

Вам понадобится настроить интеграцию и на стороне Kaspersky Sandbox через веб-интерфейс Kaspersky Sandbox, и на стороне Kaspersky Security Center через консоль администрирования KSC.

Чтобы настроить интеграцию с Kaspersky Security Center на стороне Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Подключение к KSC**.
2. В поле **Адрес сервера KSC** введите адрес и порт сервера Kaspersky Security Center.
3. Если вы хотите установить доверенное соединение с сервером Kaspersky Security Center, установите флажок **Использовать TLS-шифрование**.
4. Нажмите на кнопку **Подключиться** в нижней части окна.

Чтобы настроить интеграцию с Kaspersky Security Center на стороне Kaspersky Security Center, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Нераспределенные устройства**.
3. В списке нераспределенных устройств выберите сервер Kaspersky Sandbox и правой кнопкой мыши раскройте меню действий над устройствами.
4. Выберите пункт меню **Переместить в группу**.
5. В открывшемся окне выберите группу устройств Kaspersky Security Center, с которыми вы хотите работать в Kaspersky Sandbox и нажмите на кнопку **ОК**.

   Например, вы можете выбрать группу **Управляемые устройства**, создать новую группу в группе **Управляемые устройства** и поместить сервер Kaspersky Sandbox в созданную группу.

Kaspersky Security Center отображает устройства, с которыми настроена интеграция, в группах управляемых устройств. Статусы работоспособности этих устройств отображаются на панели мониторинга. Если в работе этих устройств возникают проблемы, Kaspersky Security Center отображает статусы **Критический** или **Предупреждение** для привлечения внимания администратора.

Поскольку сервер Kaspersky Sandbox не является стандартной рабочей станцией, управляемой через KSC, требуется отдельно настроить отображение статусов устройств Kaspersky Sandbox в KSC.

> Для корректного отображения статусов устройств Kaspersky Sandbox в KSC необходимо поместить серверы Kaspersky Sandbox в отдельную группу управляемых устройств.

Сервер Kaspersky Sandbox отобразится в списке устройств группы устройств дерева консоли KSC.

Интеграция Kaspersky Sandbox с Kaspersky Security Center будет настроена.

Создание TLS-сертификата веб-интерфейса Kaspersky Sandbox

Для безопасного использования веб-интерфейса Kaspersky Sandbox вам нужно сгенерировать или загрузить TLS-сертификат веб-интерфейса.

Генерация TLS-сертификата веб-интерфейса Kaspersky Sandbox

Чтобы сгенерировать TLS-сертификат веб-интерфейса Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В блоке **TLS-сертификат веб-интерфейса Kaspersky Sandbox** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.
3. Нажмите на кнопку **Да**.

Kaspersky Sandbox сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Загрузка TLS-сертификата веб-интерфейса Kaspersky Sandbox

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Sandbox.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Чтобы загрузить TLS-сертификат через веб-интерфейс Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В блоке **TLS-сертификат веб-интерфейса Kaspersky Sandbox** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

3. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Sandbox.

Настройка доверенного соединения Kaspersky Sandbox с Kaspersky Endpoint Agent

Вы можете настроить доверенное соединение Kaspersky Sandbox с Kaspersky Endpoint Agent в веб-интерфейсе сервера Kaspersky Sandbox, не входящего в кластер.

> Если вы уже объединили серверы в кластер, вам нужно удалить сервер из кластера, затем создать новый кластер на базе этого сервера и добавить в новый кластер все серверы, предназначенные для работы решения Kaspersky Sandbox.

> Если нужные вам серверы входят в другой кластер, вам нужно последовательно удалить их из кластера, в который они входят в настоящий момент, а затем добавить в новый кластер.

Установка и настройка доверенного соединения Kaspersky Sandbox с Kaspersky Endpoint Agent состоит из следующих этапов:

1. Удаление сервера из кластера (если сервер входит в кластер в настоящий момент)
2. Генерация или загрузка TLS-сертификата соединения с Kaspersky Endpoint Agent на этот сервер
3. Создание нового кластера на базе этого сервера
4. Удаление всех серверов, которые вы хотите добавить в этот кластер, из кластеров, в которые они входят в настоящий момент
5. Добавление всех нужных серверов в новый кластер
6. Добавление всех серверов нового кластера Kaspersky Sandbox в список Kaspersky Endpoint Agent
7. Настройка доверенного соединения с Kaspersky Sandbox на стороне Kaspersky Endpoint Agent

Генерация TLS-сертификата соединения с Kaspersky Endpoint Agent

Чтобы сгенерировать TLS-сертификат соединения Kaspersky Sandbox с Kaspersky Endpoint Agent, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.

2. В блоке **TLS-сертификат для соединения с Kaspersky Endpoint Agent** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.

3. Нажмите на кнопку **Да**.

Kaspersky Sandbox сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Загрузка TLS-сертификата соединения с Kaspersky Endpoint Agent

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Sandbox.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Чтобы загрузить TLS-сертификат через веб-интерфейс Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В блоке **TLS-сертификат для соединения с Kaspersky Endpoint Agent** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

3. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Sandbox.

Сохранение файла TLS-сертификата соединения с Kaspersky Endpoint Agent на компьютере

Чтобы сохранить файл TLS-сертификата соединения с Kaspersky Endpoint Agent на компьютере, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В блоке **TLS-сертификат для соединения с Kaspersky Endpoint Agent** нажмите на кнопку **Скачать**.

Файл TLS-сертификата будет сохранен в папке загрузки браузера.

Замена TLS-сертификата соединения с Kaspersky Endpoint Agent

Вы можете заменить TLS-сертификат соединения с Kaspersky Endpoint Agent.

Замена TLS-сертификата соединения с Kaspersky Endpoint Agent состоит из следующих этапов:

1. Удаление сервера, на котором вы хотите заменить TLS-сертификат, из кластера
2. Генерация или загрузка TLS-сертификата соединения с Kaspersky Endpoint Agent на этот сервер

   Добавленный сертификат заменит имевшийся ранее сертификат. Использование нескольких сертификатов одновременно не предусмотрено.
3. Создание нового кластера на базе этого сервера
4. Удаление всех серверов, которые вы хотите добавить в новый кластер, из кластеров, в которые они входят в настоящий момент
5. Добавление всех нужных серверов в новый кластер
6. Добавление всех серверов нового кластера Kaspersky Sandbox в список Kaspersky Endpoint Agent
7. Обновление данных TLS-сертификата Kaspersky Sandbox в Kaspersky Endpoint Agent

Установка даты и времени

Чтобы установить дату и время Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Дата и время**.
2. В раскрывающемся списке **Страна** выберите нужную страну.
3. В раскрывающемся списке **Часовой пояс** выберите нужный часовой пояс.
4. Если вы хотите синхронизировать время с NTP-сервером, включите переключатель справа от названия параметра **Синхронизация с NTP-серверами**.
5. Если вы хотите установить дату и время вручную, не включайте переключатель справа от названия параметра **Синхронизация с NTP-серверами** и выполните следующие действия:
   a. В поле **Дата** введите текущую дату или нажмите на кнопку 🗓 и выберите дату в календаре.
   b. В поле **Время** введите текущее время.
6. Нажмите на кнопку **Применить** в нижней части окна.

Установка и настройка образов операционных систем и программ для работы Kaspersky Sandbox

В комплекте поставки Kaspersky Sandbox вы получаете образ операционной системы Windows 7 x64 и программ, необходимых для работы Kaspersky Sandbox. Вам не требуется активировать эти операционные системы и программы. В поставляемых образах уже добавлены лицензионные ключи.

Kaspersky Sandbox будет запускать объекты в этой операционной системе и анализировать поведение объектов для выявления вредоносной активности, признаков целевых атак и вторжений в IT-инфраструктуру организации.

При возникновении проблем с активацией операционной системы или программ в веб-интерфейсе Kaspersky Sandbox отобразится сообщение об ошибке. В этом случае рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Работа программы с другими образами операционных систем не предусмотрена.

Загрузка ISO-образа операционной системы и программ для работы Kaspersky Sandbox

Чтобы загрузить ISO-образ операционной системы и программ, необходимых для работы Kaspersky Sandbox, выполните следующие действия для каждого ISO-образа:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Виртуальные машины**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно выбора файлов.
3. Выберите файл формата ISO, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

В разделе **Виртуальные машины** отобразится загруженный образ операционной системы и программ, необходимых для работы Kaspersky Sandbox.

Установка виртуальных машин с образом операционной системы и программ для работы Kaspersky Sandbox

Чтобы установить виртуальную машину с образом операционной системы и программ, необходимых для работы Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Виртуальные машины**.

2. В списке виртуальных машин нажмите на кнопку **Установить** в строке с виртуальной машиной, которую вы хотите установить.

   Начнется процесс распаковки архива и установки виртуальной машины.

После завершения установки виртуальная машина отобразится в разделе **Виртуальные машины** со статусом **Установлена**.

Удаление виртуальных машин

Чтобы удалить виртуальную машину, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Виртуальные машины**.

2. В списке виртуальных машин нажмите на кнопку **Удалить** в строке с той виртуальной машиной, которую вы хотите удалить

   Выбранная виртуальная машина будет удалена.

Управление кластером

Если вы используете несколько серверов Kaspersky Sandbox, вы можете объединить их в кластер. Вы можете добавлять серверы в кластер и удалять серверы из кластера.

> В один кластер допустимо объединить не более 32 серверов.

Все серверы в кластере равноправны независимо от того, на базе какого сервера был создан кластер. Результат обработки одного и того же объекта будет одинаковым на всех серверах кластера.

Программа Kaspersky Sandbox балансирует нагрузку между серверами. Объекты, поступающие на обработку в Kaspersky Sandbox от Kaspersky Endpoint Agent, обрабатываются на наименее загруженном сервере.

> Чтобы кластер Kaspersky Sandbox обрабатывал объекты от Kaspersky Endpoint Agent, необходимо добавить в Kaspersky Endpoint Agent хотя бы один сервер, входящий в кластер при интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox.

В списке серверов Kaspersky Sandbox программы Kaspersky Endpoint Agent отображаются только те серверы, которые вы добавили в этот список. При этом объекты могут обрабатываться любым сервером кластера с учетом балансировки нагрузки. Актуальный список серверов кластера можно просмотреть в веб-интерфейсе Kaspersky Sandbox.

> Рекомендуется добавить в Kaspersky Endpoint Agent все серверы кластера.

Kaspersky Endpoint Agent может подключиться к другому серверу Kaspersky Sandbox из списка при возникновении одной из следующих ошибок:

- Истекло время ожидания ответа от Kaspersky Sandbox (connection timeout).
- Kaspersky Sandbox недоступен (код ошибки 503 или 504).
- Проблема самодиагностики, за исключением проблем с лицензией (код ошибки 500).

При удалении сервера из кластера возможны следующие сценарии обработки объектов:

- Если в списке серверов Kaspersky Sandbox программы Kaspersky Endpoint Agent остается хотя бы один сервер этого кластера с актуальным IP-адресом или FQDN, Kaspersky Sandbox продолжит обрабатывать объекты от Kaspersky Endpoint Agent.
- Если в списке серверов Kaspersky Sandbox программы Kaspersky Endpoint Agent не остается ни одного сервера, входящего в этот кластер, или IP-адреса или FQDN серверов кластера неактуальны, Kaspersky Sandbox не сможет получать и обрабатывать объекты от Kaspersky Endpoint Agent.

  Для корректной обработки объектов необходимо добавить в Kaspersky Endpoint Agent хотя бы один сервер, входящий в кластер Kaspersky Sandbox.

После создания кластера в разделе **Управление кластерами** окна веб-интерфейса Kaspersky Sandbox отображается таблица серверов кластера и данные мониторинга состояния серверов кластера.

Управление сертификатами Kaspersky Endpoint Agent и сетевыми интерфейсами недоступно после создания кластера.

Создание нового кластера

Чтобы создать новый кластер, выполните следующие действия:

1. В разделе **Управление кластерами** веб-интерфейса любого сервера, который вы планируете включить в кластер, нажмите на кнопку **Создать новый кластер**.
2. В окне подтверждения нажмите на кнопку **Да**.

   Кластер будет создан. Страница браузера обновится. Отобразится таблица серверов, входящих в кластер, с информацией о сервере, на котором был создан кластер, а также информация о состоянии серверов, входящих в кластер.

После создания кластера вы можете добавлять другие серверы в этот кластер.

Управление сертификатами Kaspersky Endpoint Agent и сетевыми интерфейсами недоступно после создания кластера.

Просмотр таблицы серверов кластера

Таблица серверов кластера отображается в разделе **Управление кластерами** окна веб-интерфейса программы после создания кластера.

В таблице серверов кластера содержится следующая информация:

1. **Адрес сервера** – IP-адрес сервера.
2. **Состояние** – одно из следующих состояний подключения сервера к кластеру:
   - Подключен.
   - Подключение.
   - Ожидает соединения.
   - Отмена подключения.
   - Сбой.
   - Не в сети.
3. **Состояние** – информация о работоспособности сервера и о проблемах с этим сервером. Может иметь, например, следующие статусы:
   - ОК.
   - Проблема с лицензией.
   - Все попытки обновления за последние 24 часа завершались с ошибкой.
   - Самодиагностика завершилась с ошибкой.
   - Самодиагностика долго не запускалась.
   - Данные о состоянии серверов устарели.
   - Образ VM требует повторной активации.
   - Версии баз не совпадают.
   - Конфигурации виртуальных машин не совпадают.
   - Проблемы с системной службой сервера.
   - Образы виртуальных машин не установлены.
   - Не синхронизировано время на серверах.

По ссылке с IP-адресом сервера вы можете перейти в веб-интерфейс этого сервера.

Мониторинг состояния серверов кластера

Для быстрой оценки состояния серверов кластера используются цветовые индикаторы зеленого, желтого и красного цвета. Цель администратора заключается в том, чтобы поддерживать все индикаторы в состоянии "зеленый".

Если все индикаторы зеленого цвета, Kaspersky Sandbox работает в штатном режиме.

Если хотя бы один индикатор желтого цвета, Kaspersky Sandbox работает, но требует внимания администратора.

Если хотя бы один индикатор красного цвета, Kaspersky Sandbox не принимает объекты на обработку от Kaspersky Endpoint Agent и требует внимания администратора.

В разделе **Управление кластерами** веб-интерфейса Kaspersky Sandbox отображается следующая информация о состоянии серверов кластера:

- **В сети**. Индикаторы и количество серверов кластера:
  - в сети;
  - не в сети.
- **Самодиагностика**. Индикаторы и количество серверов кластера:
  - работающих в штатном режиме;
  - требующих устранения проблем в работе.
- **Обновление баз**.Индикаторы и количество серверов:
  - с актуальной версией баз;
  - требующих обновления баз.
- **Лицензия**.Индикаторы и количество серверов:
  - с успешно активированной программой Kaspersky Sandbox;
  - требующих загрузки лицензионного ключа или активации программы.

Индикаторы Самодиагностика, Обновление баз и Лицензия работают по принципу мониторинга работы программы в разделе **Мониторинг** веб-интерфейса Kaspersky Sandbox.

Добавление сервера в кластер

Чтобы добавить сервер в кластер, выполните следующие действия:

1. В разделе **Управление кластерами** веб-интерфейса сервера, входящего в кластер, нажмите на кнопку **Добавить сервер**.

   Откроется окно **Токен для добавления нового сервера в этот кластер**, содержащее уникальный токен. Вы можете использовать этот токен только для добавления одного сервера в кластер. Токен действителен в течение 30 минут после создания.

2. Нажмите на кнопку **Копировать**.

3. В разделе **Управление кластерами** веб-интерфейса сервера, который вы хотите добавить в кластер, нажмите на кнопку **Добавить сервер в существующий кластер**.

4. Вставьте токен, полученный на шаге 2, в поле **Токен кластера**.

5. Нажмите на кнопку **Подключиться**.

   Запустится подключение сервера к кластеру.

6. Если не удалось добавить сервер в кластер, нажмите на кнопку **Отменить** в веб-интерфейсе сервера, который вы хотите добавить в кластер, и повторите действия по добавлению сервера в кластер.

Сервер будет добавлен в кластер и отобразится в таблице серверов кластера в разделе **Управление кластерами** веб-интерфейса каждого из серверов, входящих в кластер.

Управление сертификатами Kaspersky Endpoint Agent и сетевыми интерфейсами недоступно после создания кластера.

Если вы хотите, чтобы добавленный сервер обрабатывал объекты от Kaspersky Endpoint Agent, вам нужно добавить этот сервер в список Kaspersky Endpoint Agent.

Удаление сервера из кластера

Чтобы удалить сервер из кластера, выполните следующие действия:

1. В разделе **Управление кластерами** веб-интерфейса сервера, входящего в кластер, нажмите на кнопку **Удалить** в строке с информацией о том сервере, который вы хотите удалить из кластера.

   Откроется окно подтверждения удаления сервера из кластера.

2. Нажмите на кнопку **Да**.

Сервер будет удален из кластера. Информация о сервере не будет отображаться в таблице серверов кластера. Удаленный сервер продолжит работу без подключения к кластеру. Управление сертификатами Kaspersky Endpoint Agent и сетевыми интерфейсами станет доступно. Остальные серверы кластера продолжат работу в кластере.

Удаление кластера

Если в кластер входит только один сервер, вы можете удалить кластер. Сервер продолжит работу без подключения к кластеру.

Чтобы удалить кластер, выполните следующие действия:

1. В разделе **Управление кластерами** веб-интерфейса единственного сервера, входящего в кластер, нажмите на кнопку **Удалить** в строке с информацией об этом сервере.

   Откроется окно подтверждения удаления кластера.

2. Нажмите на кнопку **Да**.

Кластер будет удален. Сервер продолжит работу без подключения к кластеру. Управление сертификатами Kaspersky Endpoint Agent и сетевыми интерфейсами станет доступно.

Изменение IP-адреса сервера, входящего в кластер

Если сервер входит в кластер, изменение IP-адреса этого сервера состоит из следующих этапов:

1. Удаление сервера из кластера
2. Изменение IP-адреса сервера
3. Добавление сервера в кластер

Загрузка системного журнала Kaspersky Sandbox на жесткий диск

Данные в системном журнале Kaspersky Sandbox хранятся в открытом незашифрованном виде. Данные хранятся за последние 30 дней.

При работе с системным журналом Kaspersky Sandbox возможен следующий сценарий передачи данных Kaspersky Sandbox в "Лабораторию Касперского":

1. Администратор Kaspersky Sandbox загружает системный журнал Kaspersky Sandbox на жесткий диск компьютера, на котором он работает в веб-интерфейсе Kaspersky Sandbox.

2. Администратор Kaspersky Sandbox отправляет файл системного журнала в Службу технической поддержки "Лаборатории Касперского".

Администратор Kaspersky Sandbox самостоятельно принимает решение о безопасности передачи имен хостов рабочих станций с программой Kaspersky Endpoint Agent в Службу технической поддержки "Лаборатории Касперского".

Чтобы загрузить системный журнал Kaspersky Sandbox на жесткий диск, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Параметры**.

2. В группе параметров **Системный журнал** нажмите на кнопку **Скачать**.

   Системный журнал Kaspersky Sandbox загрузится на жесткий диск вашего компьютера в директорию загрузки браузера.

Перезагрузка сервера Kaspersky Sandbox

Чтобы перезагрузить сервер Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Параметры**.
2. В группе параметров **Питание** нажмите на кнопку **Перезагрузить**.

   Откроется окно подтверждения перезагрузки сервера Kaspersky Sandbox.
3. Нажмите на кнопку **Да**.

Сервер Kaspersky Sandbox перезагрузится. Через несколько минут вы сможете войти в систему.

Выключение сервера Kaspersky Sandbox

Чтобы выключить сервер Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **Параметры**.
2. В группе параметров **Питание** нажмите на кнопку **Выключить**.

   Откроется окно подтверждения выключения сервера Kaspersky Sandbox.
3. Нажмите на кнопку **Да**.

Сервер Kaspersky Sandbox выключится.

Изменение пароля учетной записи администратора Kaspersky Sandbox

Чтобы изменить пароль учетной записи администратора Kaspersky Sandbox, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы по ссылке с именем вашей учетной записи раскройте список действий.
2. Выберите действие **Изменение пароля**.
3. В поле **Текущий пароль** введите текущий пароль учетной записи администратора.
4. В поле **Новый пароль** введите новый пароль учетной записи администратора.
5. В поле **Подтвердить пароль** введите новый пароль учетной записи администратора повторно.

6. Нажмите на кнопку **Изменение пароля**.

Пароль учетной записи администратора Kaspersky Sandbox будет изменен.

Управление программой Kaspersky Sandbox через Kaspersky Security Center

Вы можете удаленно управлять параметрами программы из консоли администрирования Kaspersky Security Center (далее также "консоль KSC") с помощью плагина управления Kaspersky Sandbox.

Kaspersky Sandbox публикует обнаружения на сервере Kaspersky Security Center. Администратор Kaspersky Security Center может настроить сроки хранения обнаружений, а также действия над обнаружениями в свойствах каждого сервера Kaspersky Sandbox.

Установка плагина управления Kaspersky Sandbox

Для управления Kaspersky Sandbox из консоли KSC вам потребуется установить плагин управления Kaspersky Sandbox.

Плагин управления Kaspersky Sandbox устанавливается совместно с плагином управления Kaspersky Endpoint Agent.

Чтобы установить плагины управления Kaspersky Sandbox и Kaspersky Endpoint Agent,

скопируйте из дистрибутива решения установочный файл плагина Sandbox-and-Endpoint-Agent-plugins.exe и запустите его на компьютере с установленной консолью администрирования Kaspersky Security Center.

Настройка отображения статусов устройств Kaspersky Sandbox в KSC

Kaspersky Security Center отображает устройства, с которыми настроена интеграция, в группах управляемых устройств. Статусы работоспособности этих устройств отображаются на панели мониторинга. Если в работе этих устройств возникают проблемы, Kaspersky Security Center отображает статусы **Критический** или **Предупреждение** для привлечения внимания администратора.

Поскольку сервер Kaspersky Sandbox не является стандартной рабочей станцией, управляемой через KSC, требуется отдельно настроить отображение статусов устройств Kaspersky Sandbox в KSC.

Для корректного отображения статусов устройств Kaspersky Sandbox в KSC необходимо поместить серверы Kaspersky Sandbox в отдельную группу управляемых устройств.

Чтобы настроить отображение статусов устройств Kaspersky Sandbox в KSC, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Управляемые устройства**, подпапку с новой группой устройств, в которую вы поместили сервер Kaspersky Sandbox.

3. В правом верхнем углу рабочей области по ссылке **Свойства группы** откройте окно со свойствами группы устройств Kaspersky Sandbox.

4. Выберите раздел **Статус устройства**.

   Статус всех устройств группы устройств Kaspersky Sandbox, на которых нет проблем (**Статус устройства определен программой**, **Срок действия лицензии истек**, **Срок действия лицензии скоро истечет** и **Базы устарели**), изменится на **ОК/Видим в сети**.

5. В разделах **Установить статус "Критический", если** и **Установить статус "Предупреждение", если** снимите флажок **Наследовать** и снимите следующие флажки, установленные по умолчанию для стандартных рабочих станций, управляемых через KSC (подробнее о статусах устройств см. в *Справке Kaspersky Security Center*):

   - **Программа безопасности не установлена**. Агент администрирования установлен на устройстве, но не установлена программа безопасности.

   - **Найдено много вирусов**. В результате работы задач поиска вирусов, например, задачи **Поиск вирусов**, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.

   - **Уровень постоянной защиты отличается от уровня, установленного администратором**. Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.

   - **Давно не выполнялся поиск вирусов**. Устройство видимо в сети и на устройстве установлена программа безопасности, но задача поиска вирусов не выполнялась больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования 7 дней назад или ранее.

   - **Обнаружены активные угрозы**. Количество необработанных объектов в папке **Необработанные файлы** превышает указанное значение.

   - **Требуется перезагрузка**. Устройство видимо в сети, но программа требует перезагрузки устройства дольше указанного времени по одной из выбранных причин.

   - **Установлены несовместимые программы**. Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые программы.

   - **Обнаружены уязвимости в программах**. Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи **Поиск уязвимостей и требуемых обновлений**, на устройстве обнаружены уязвимости в программах с заданным уровнем критичности.

   - **Давно не выполнялась проверка обновлений Центра обновления Windows**. Не выполнялась задача **Поиск уязвимостей и требуемых обновлений** больше указанного времени.

   - **Определенное состояние шифрования данных**. Агент администрирования установлен на устройстве и результат шифрования устройства равен указанному значению.

- **Параметры мобильного устройства не соответствуют политике**. Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.

- **Есть необработанные инциденты**. На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором.

- **Защита выключена**. Устройство видимо в сети, но программа безопасности на устройстве отключена дольше указанного времени.

- **Программа безопасности не запущена**. Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена.

6. В разделе **Установить статус "Критический", если** установите следующие флажки:

   - **Статус устройства определен программой**. Статус устройства определяется управляемой программой. Серверы Kaspersky Sandbox, у которых возникает проблема с самодиагностикой, будут иметь статус "**Критический**": "**Проблемы с сервером Kaspersky Sandbox. Сервер не принимает объекты на проверку**".

   - **Срок действия лицензии истек**. Устройство видимо в сети, но срок действия лицензии истек.

7. В разделе **Установить статус "Предупреждение", если** установите следующие флажки:

   - **Срок действия лицензии скоро истечет**. Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.

   - **Базы устарели**. Двойным щелчком мыши откройте окно с условиями этого статуса и установите значение 1. Серверы Kaspersky Sandbox, на которых более суток не было успешного запуска задачи обновления баз, будут иметь статус "**Предупреждение**".

8. Нажмите на кнопки **Применить** и **ОК**.

Отображение статусов устройств Kaspersky Sandbox будет настроено.

Статус всех устройств группы устройств Kaspersky Sandbox, на которых нет проблем (**Статус устройства определен программой**, **Срок действия лицензии истек**, **Срок действия лицензии скоро истечет** и **Базы устарели**), изменится на **ОК/Видим в сети**.

Статус устройств, на которых есть проблемы (**Статус устройства определен программой**, **Срок действия лицензии истек**, **Срок действия лицензии скоро истечет** или **Базы устарели**), изменится согласно настроенным значениям параметров.

Начало работы с Kaspersky Sandbox в консоли администрирования KSC

Чтобы начать работу с Kaspersky Sandbox в консоли KSC, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Управляемые устройства**, подпапку с новой группой устройств, в которую вы поместили сервер **Kaspersky Sandbox**.

3. Выберите сервер Kaspersky Sandbox и откройте окно свойств сервера двойным щелчком мыши.

4. Выберите раздел **Программы**.

   В правой части окна отобразится список программ, установленных на сервере.

5. В списке программ выберите **Kaspersky Sandbox (KSB)** и нажмите на кнопку **Свойства**.

   Откроется окно с параметрами Kaspersky Sandbox.

Вы сможете управлять параметрами Kaspersky Sandbox.

Просмотр информации о Kaspersky Sandbox и состоянии обновления баз

Чтобы просмотреть информацию о Kaspersky Sandbox и состоянии обновления баз в консоли администрирования KSC, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Управляемые устройства**, подпапку с новой группой устройств, в которую вы поместили сервер **Kaspersky Sandbox**.

3. Выберите сервер Kaspersky Sandbox и откройте окно свойств сервера двойным щелчком мыши.

4. Выберите раздел **Программы**.

   В правой части окна отобразится список программ, установленных на сервере.

5. В списке программ выберите **Kaspersky Sandbox (KSB)** и нажмите на кнопку **Свойства**.

6. Выберите раздел **Общие**.

Отобразится версия Kaspersky Sandbox, даты установки программы и обновления баз, дата выпуска обновления, количество записей в антивирусных базах.

Переход в веб-интерфейс Kaspersky Sandbox

Вы можете управлять параметрами программы Kaspersky Sandbox через веб-интерфейс.

Чтобы перейти в веб-интерфейс Kaspersky Sandbox, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Управляемые устройства**, подпапку с новой группой устройств, в которую вы поместили сервер **Kaspersky Sandbox**.

3. Выберите сервер Kaspersky Sandbox и откройте окно свойств сервера двойным щелчком мыши.

4. Выберите раздел **Программы**.

   В правой части окна отобразится список программ, установленных на сервере.

5. В списке программ выберите **Kaspersky Sandbox (KSB)** и нажмите на кнопку **Свойства**.

6. Выберите раздел **KSB settings**.

7. Перейдите по ссылке **Веб-интерфейс Kaspersky Sandbox**.

Откроется окно веб-интерфейса программы Kaspersky Sandbox.

Просмотр информации о лицензии Kaspersky Sandbox

Чтобы просмотреть информацию о лицензии Kaspersky Sandbox и установленных ключах, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Управляемые устройства**, подпапку с новой группой устройств, в которую вы поместили сервер **Kaspersky Sandbox**.

3. Выберите сервер Kaspersky Sandbox и откройте окно свойств сервера двойным щелчком мыши.

4. Выберите раздел **Программы**.

   В правой части окна отобразится список программ, установленных на сервере.

5. В списке программ выберите **Kaspersky Sandbox (KSB)** и нажмите на кнопку **Свойства**.

6. Выберите раздел **Ключи**.

Отобразится информация о лицензионных ключах Kaspersky Sandbox. За 30 дней до окончания срока действия лицензии появляется уведомление о необходимости продлить лицензию.

Вы также можете просмотреть информацию об использовании лицензионных ключей на устройствах всех групп с помощью отчета об использовании ключей.

Чтобы просмотреть отчет об использовании лицензионных ключей, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли KSC выберите нужный Сервер администрирования.

3. Выберите закладку **Отчеты**.

   Откроется список доступных для просмотра отчетов.

4. Двойным щелчком мыши раскройте **Отчет об использовании ключей**.

   Откроется окно, содержащее отчет об использовании лицензионных ключей на устройствах всех групп.

Настройка событий Kaspersky Sandbox

Чтобы настроить события Kaspersky Sandbox, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. Выберите раздел **Настройка событий**.

   Откроется список событий, сгруппированных по степени важности событий. Список событий содержит названия событий и время их хранения на Сервере администрирования по умолчанию (в днях).
5. Выберите событие, которое вы хотите настроить.
6. В правом нижнем углу окна нажмите на кнопку **Свойства**.

   Откроется окно свойств выбранного события.
7. Вы можете настроить следующие параметры событий:

   a. В блоке **Регистрация событий** укажите количество дней хранения событий и выберите один или несколько из следующих типов хранения событий:

   - **Экспортировать в SIEM-систему по протоколу Syslog**.
   - **В журнале событий ОС на клиентском устройстве**.
   - **В журнале событий ОС на Сервере администрирования**.

   b. В блоке **Уведомления о событиях** выберите один или несколько способов уведомления о событии:

   - **Уведомлять по электронной почте**.
   - **Уведомлять по SMS**.
   - **Уведомлять запуском исполняемого файла или скрипта**.
   - **Уведомлять по SNMP**.

Просмотр информации о плагине управления Kaspersky Sandbox

Чтобы просмотреть информацию о плагине управления Kaspersky Sandbox, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Управляемые устройства**, подпапку с новой группой устройств, в которую вы поместили сервер **Kaspersky Sandbox**.

3. Выберите сервер Kaspersky Sandbox и откройте окно свойств сервера двойным щелчком мыши.

4. Выберите раздел **Программы**.

   В правой части окна отобразится список программ, установленных на сервере.

5. В списке программ выберите **Kaspersky Sandbox (KSB)** и нажмите на кнопку **Свойства**.

6. Выберите раздел **Дополнительно**.

Отобразится информация о плагине управления Kaspersky Sandbox.

Просмотр отчета об угрозах

Вы можете просматривать отчеты об угрозах из консоли KSC. Подробнее о создании и изменении шаблонов отчетов, настройке граф отчетов, сохранении и обновлении отчетов см. в *Справке Kaspersky Security Center*.

Чтобы просмотреть отчет об угрозах, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли KSC выберите нужный Сервер администрирования.

3. Выберите закладку **Отчеты**.

   Откроется список доступных для просмотра отчетов.

4. Двойным щелчком мыши раскройте **Отчет об угрозах**.

   Откроется окно, содержащее отчет об угрозах.

Просмотр статистики проверки объектов

Вы можете просматривать статистики обработки запросов и проверки объектов программой Kaspersky Sandbox.

Чтобы просмотреть статистику проверки объектов, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли KSC выберите нужный Сервер администрирования.

3. Выберите закладку **Статистика**.

4. Нажмите на кнопку **Настроить вид**.

   Откроется окно со списком страниц статистики.

5. В нижней части окна нажмите на кнопку **Добавить**.
6. В открывшемся окне в разделе **Общие** введите имя новой страницы статистики.
7. Выберите раздел **Информационные панели**.
8. В нижней части окна нажмите на кнопку **Добавить**.

   Откроется список информационных панелей, доступных для добавления.
9. В блоке списка **Kaspersky Sandbox (KSB)** выполните одно из следующих действий:

   - Если вы хотите просматривать статистику обработки всех запросов, выберите **Show all checked objects**.
   - Если вы хотите просматривать статистику проверки объектов на сервере Kaspersky Sandbox, выберите **Show unique checked objects**.
10. Нажмите на кнопку **ОК**.
11. В разделе **Период** задайте период, за который вы хотите просматривать статистику.
12. В разделе **Вид** выберите тип диаграммы для отображения статистики.
13. Нажмите на кнопку **ОК**.
14. В нижней части окна задайте количество граф информационных панелей.
15. Нажмите на кнопку **ОК**.
16. В окне свойств статистики нажмите на кнопку **Закрыть**.

Выбранная статистика будет отображаться на закладке добавленной страницы статистики. Статистика показывается по всем серверам Kaspersky Sandbox, подключенным к этому Серверу администрирования.

Добавление лицензионного ключа Kaspersky Sandbox через KSC

Чтобы добавить лицензионный ключ Kaspersky Sandbox через KSC, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Выберите блок типов задач **Kaspersky Sandbox (KSB)** и тип задачи **Добавить ключ**.

5. Нажмите на кнопку **Далее**.

   Запустится мастер создания задачи.

6. Если вы хотите загрузить ключ с жесткого диска компьютера, на котором вы работаете, выполните следующие действия:

   a. Выберите вариант добавления ключа **Файл ключа** и нажмите на кнопку **Загрузить файл ключа**.

      Откроется окно выбора файлов.

   b. Выберите файл ключа, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

      Окно выбора файлов закроется.

   Ключ будет добавлен. Отобразится информация о лицензии Kaspersky Sandbox.

7. Если вы хотите загрузить ключ из хранилища ключей KSC, выполните следующие действия:

   a. Выберите вариант добавления ключа **Ключ в хранилище** и нажмите на кнопку **Выберите ключ в хранилище**.

      Откроется окно **Хранилище лицензионных ключей KSC**.

   b. Выберите в списке ключ, который вы хотите добавить и нажмите на кнопку **ОК**.

      Окно **Хранилище лицензионных ключей KSC** закроется.

   Ключ будет добавлен. Отобразится информация о лицензии Kaspersky Sandbox.

8. Нажмите на кнопку **Далее**.

9. В открывшемся окне выбора устройств выберите устройства, на которые вы хотите распространить лицензию, и нажмите на кнопку **Далее**.

   Например, вы можете выбрать вариант **Назначить задачу группе администрирования** и выбрать группу администрирования из списка.

10. В окне **Определение название задачи** в поле **Имя** введите название задачи добавления лицензионного ключа и нажмите на кнопку **Далее**.

11. Если вы хотите, чтобы задача запустилась сразу после создания, установите флажок **Запустить задачу после завершения работы мастера** и нажмите на кнопку **Готово**.

Лицензионный ключ Kaspersky Sandbox будет добавлен.

Замена лицензионного ключа Kaspersky Sandbox через KSC

Если вы хотите заменить лицензионный ключ Kaspersky Sandbox через KSC, вам нужно выполните действия по добавлению лицензионного ключа.

Загруженный лицензионный ключ заменит активный лицензионный ключ программы.

Управление программой Kaspersky Endpoint Agent

Программа Kaspersky Endpoint Agent устанавливается в составе Endpoint Protection Platform (далее также "EPP").

В качестве EPP для Kaspersky Endpoint Agent версии 3.7 может использоваться программа Kaspersky Endpoint Security для Windows версии 11.2.

Kaspersky Endpoint Agent обеспечивает коммуникацию EPP и Kaspersky Sandbox, а также выполнение действий по автоматическому реагированию на угрозы, обнаруженные Kaspersky Sandbox.

Вы можете устанавливать и удалять программу, а также удаленно управлять параметрами программы из Консоли администрирования Kaspersky Security Center (далее также "консоль KSC") с помощью плагина управления Kaspersky Endpoint Agent через политики Kaspersky Endpoint Agent.

Подробную информацию о работе в консоли KSC см. в *Справке Kaspersky Security Center.*

Для оказания поддержки при неполадках в работе программы Kaspersky Endpoint Agent специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия:

- Активировать функциональность получения расширенной диагностической информации.
- Дополнительно настроить отдельные компоненты программы, недоступные для изменения стандартными средствами пользовательского интерфейса.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся информация, необходимая для выполнения перечисленных действий (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и т.д.), а также состав данных, собираемых в отладочных целях, будут озвучены вам специалистами Службы технической поддержки. Собранная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка собранных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в документации программы или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

Установка Kaspersky Endpoint Agent

Kaspersky Endpoint Agent устанавливается в составе EPP (Kaspersky Endpoint Security для Windows версии 11.2).

Инструкции по установке Kaspersky Endpoint Security для Windows приведены в *Справке Kaspersky Endpoint Security для Windows*.

Kaspersky Endpoint Security для Windows может быть установлена такими способами, как, например, локально с помощью мастера установки программы, локально из командной строки или удаленно через Kaspersky Security Center. В процессе установки, независимо от способа установки, вам потребуется выбрать компоненты Kaspersky Endpoint Security для Windows, которые вы хотите установить.

По умолчанию Kaspersky Endpoint Agent не выбран для установки в составе Kaspersky Endpoint Security для Windows. Вам нужно самостоятельно выбрать Kaspersky Endpoint Agent для установки в списке компонентов Kaspersky Endpoint Security для Windows.

Пример:

Если вы устанавливаете Kaspersky Endpoint Security для Windows удаленно через Kaspersky Security Center, вы можете выполнить следующие действия по выбору Kaspersky Endpoint Agent для установки в списке компонентов:

1. Откройте консоль KSC.
2. В дереве консоли в папке **Дополнительно**, вложенной папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В списке инсталляционных пакетов выберите пакет Kaspersky Endpoint Security для Windows и откройте его свойства двойным щелчком мыши.

   Если инсталляционный пакет программы Kaspersky Endpoint Security для Windows не создан, создайте его. Подробнее о создании инсталляционных пакетов в Kaspersky security Center см. в *Справке Kaspersky Security Center*.

4. Выберите раздел **Параметры**.

   В правой части окна отобразится список компонентов Kaspersky Endpoint Security для Windows.

5. Установите флажок рядом с названием программы Kaspersky Endpoint Agent.
6. Нажмите на кнопку **Применить**.
7. Нажмите на кнопку **ОК**.

   Kaspersky Endpoint Agent будет установлен в составе Kaspersky Endpoint Security для Windows.

Установка плагина управления Kaspersky Endpoint Agent

Для управления Kaspersky Endpoint Agent из консоли KSC вам потребуется установить плагин управления Kaspersky Endpoint Agent.

Если у вас установлен плагин управления Kaspersky Endpoint Agent версии Beta, удалите его перед установкой плагина управления Kaspersky Endpoint Agent версии 3.7.

Плагин управления Kaspersky Endpoint Agent устанавливается совместно с плагином управления Kaspersky Sandbox.

Создание политики Kaspersky Endpoint Agent

Чтобы создать политику Kaspersky Endpoint Agent в Kaspersky Security Center, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Нажмите на кнопку **Новая политика**.

   Запустится мастер создания политики.
4. Введите имя, под которым создаваемая политика будет отображаться в списке политик и нажмите на кнопку **Далее**.
5. Выберите один из следующих вариантов настройки параметров политики и нажмите на кнопку **Далее**:

   - **Создать новую политику и настроить параметры**

     Отобразится список блоков параметров программы, которые вы можете настроить на этапе создания политики.

     Настройка параметров программы в процессе создания политики состоит из следующих этапов:

     1. Настройка параметров безопасности Kaspersky Endpoint Agent
     2. Настройка параметров соединения с прокси-сервером
     3. Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox
     4. Настройка расширенных параметров: времени ожидания ответа от Kaspersky Sandbox и параметров очереди запросов
     5. Настройка действий Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox
     6. Настройка параметров карантина и восстановления объектов из карантина
     7. Настройка синхронизации данных с Сервером администрирования

     Вы также можете настроить все параметры программы позднее, после завершения создания политики.

- **Создать новую политику и использовать значения параметров по умолчанию**

  Отобразится окно настройки группы администрирования Kaspersky Security Center.

6. Если вы выбрали вариант **Создать новую политику и настроить параметры**, выполните одно из следующих действий:

   - Если вы хотите настроить параметры программы из какого-нибудь блока сейчас, нажмите на кнопку **Настроить** справа от названия выбранного блока.

     Откроется выбранный блок параметров программы. Вы можете настроить параметры программы.

   - Если вы хотите настроить параметры программы из отображаемых блоков позднее, нажмите на кнопку **Далее**.

   Отобразится окно настройки группы администрирования Kaspersky Security Center.

7. Выполните следующие действия:

   a. Нажмите на кнопку **Обзор...**.

      Откроется окно выбора группы администрирования.

   b. Выберите группу администрирования в списке. Например, вы можете выбрать группу **Управляемые устройства**.

   c. Если вы хотите создать подгруппу устройств в группе **Управляемые устройства**, выполните следующие действия:

      1. Нажмите на кнопку **Новая группа**.
      2. В открывшемся окне введите имя подгруппы устройств.
      3. Нажмите на кнопку **ОК**.

   d. Нажмите на кнопку **Далее**

8. Выберите одно из следующих состояний политики:

   - **Активная политика**, если вы хотите, чтобы политика начала действовать сразу после создания.
   - **Неактивная политика**, если вы хотите активировать политику позднее.

9. Если вы хотите начать настройку политики сразу после создания политики, установите флажок **Открыть свойства политики сразу после создания**.

10. Нажмите на кнопку **Готово**.

Созданная политика отобразится в списке.

Включение параметров в политике Kaspersky Endpoint Agent

Когда вы настраиваете параметры политики Kaspersky Endpoint Agent, по умолчанию значения параметров сохраняются, но не применяются до тех пор, пока вы их не включите.

Включение параметров доступно для блоков, в которых находятся эти параметры.

Чтобы включить блок параметров в политике Kaspersky Endpoint Agent, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику Kaspersky Sandbox, в которой вы хотите включить параметры.
4. В открывшемся окне выберите раздел и блок параметров, к которым относятся нужные параметры.
5. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

Все параметры блока будут применяться в политике.

Настройка параметров безопасности Kaspersky Endpoint Agent

Для обеспечения максимального уровня безопасности IT-инфраструктуры организации вы можете настроить доступ пользователей и сторонних процессов к Kaspersky Endpoint Agent. Для этого предусмотрены следующие возможности:

- Ограничение прав пользователей на управление параметрами и службами программы.
- Защита действий в программе паролем.
- Механизм самозащиты программы.

Настройка прав пользователей

Вы можете предоставить доступ к Kaspersky Endpoint Agent для отдельных пользователей или групп пользователей. В результате только заданные пользователи смогут управлять параметрами или службами программы.

Чтобы настроить права пользователей, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.

5. В блоке параметров **Права пользователей** нажмите на кнопку **Настроить** рядом с названием нужного параметра.

   Откроется окно разрешений для группы "Kaspersky Endpoint Agent".

6. В верхнем блоке параметров групп или пользователей выберите группу или пользователя, которому вы хотите предоставить права.

7. В нижнем блоке параметров разрешений для групп или пользователей установите флажки в строках с требуемыми правами.

8. Нажмите на кнопку **ОК**.

9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

10. В окне свойств политики нажмите на кнопку **ОК**.

Права пользователей на управление параметрами и/или службами программы будут настроены.

Включение защиты паролем

Неограниченный доступ пользователей к программе и ее параметрам может привести к снижению уровня безопасности хоста в целом. Защита паролем позволяет ограничить доступ пользователей к программе.

Чтобы включить защиту паролем, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Политики**.

3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.

4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.

5. В блоке параметров **Защита паролем** установите флажок **Применить защиту паролем**.

6. Задайте пароль и подтвердите его.

7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

8. Нажмите на кнопку **ОК**.

Защита паролем будет включена. При попытке пользователя выполнить действие, защищенное паролем, программа предложит пользователю ввести пароль.

Включение и отключение механизма самозащиты

Для защиты от вредоносных программ, которые пытаются заблокировать работу Kaspersky Endpoint Agent или удалить программу, в программе реализован механизм самозащиты. Этот механизм предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.

Чтобы включить или отключить механизм самозащиты, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
5. В блоке параметров **Самозащита** выполните одно из следующих действий:
   - Установите флажок **Включить самозащиту модулей приложения в памяти**, если вы хотите включить механизм самозащиты.
   - Снимите флажок **Включить самозащиту модулей приложения в памяти**, если вы хотите отключить механизм самозащиты.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.
7. Нажмите на кнопку **ОК**.

Механизм самозащиты будет включен или отключен.

Настройка параметров соединения с прокси-сервером

Параметры соединения с прокси-сервером используются для обновления баз, активации программы и работы внешних служб.

Если вы используете NGINX в качестве прокси-сервера, настройте параметр `client_max_body_size:` значение параметра `client_max_body_size` должно быть равно максимальному размеру объекта, отправляемого программой Kaspersky Endpoint Agent на обработку в программу Kaspersky Sandbox. Иначе NGINX не будет пропускать объекты, превышающие установленное значение. Значение по умолчанию: 1 МБ.

Чтобы настроить параметры соединения с прокси-сервером , выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.

4. В разделе **Параметры программы** выберите подраздел **Другие параметры**.

5. Выберите один из следующих вариантов использования прокси-сервера:

   - **Не использовать прокси-сервер**.
   - **Использовать прокси-сервер и настроить параметры соединения**.

6. Если вы выбрали вариант **Использовать прокси-сервер и настроить параметры соединения**, в полях **Имя или IP-адрес сервера** и **Порт** введите адрес и порт прокси-сервера, соединение с которым вы хотите установить.

   По умолчанию используется порт 8080.

7. Если вы хотите использовать NTLM-аутентификацию при подключении к прокси-серверу, выполните следующие действия:

   a. Установите флажок **Использовать NTLM-аутентификацию по имени пользователя и паролю**.

   b. В поле **Имя пользователя** введите имя пользователя, под учетной записью которого вы хотите авторизоваться на прокси-сервере.

   c. В поле **Пароль** введите пароль подключения к прокси-серверу.

      Вы можете включить отображение символов пароля нажатием на кнопку **Показать** справа от поля **Пароль**.

8. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси-сервер для локальных адресов**.

9. Нажмите на кнопку **Применить**.

   Вы вернетесь в окно свойств политики.

10. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

11. Нажмите на кнопку **ОК**.

Параметры соединения с прокси-сервером будут настроены.

Настройка использования Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Agent использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

Kaspersky Security Network (далее также "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 Kaspersky Web Traffic Security на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, информация о которых еще не вошла в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы.

Во время участия в Kaspersky Security Network определенная статистика, полученная в результате работы Kaspersky Endpoint Agent, автоматически отправляется в "Лабораторию Касперского". Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Endpoint Agent передает в Kaspersky Security Network, вы можете прочитать в Положении о KSN.

Участие в Kaspersky Security Network добровольное. По умолчанию использование KSN отключено.

Чтобы включить использование KSN, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. Выберите раздел **Использование Kaspersky Security Network**.
5. Ознакомьтесь с Положением о KSN.
6. Если вы согласны с условиями Положения, установите флажок **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Положения о Kaspersky Security Network**.
7. Выберите вариант **Включить использование Kaspersky Security Network**.
8. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.
9. Нажмите на кнопку **ОК**.

Использование KSN будет включено.

Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с Kaspersky Sandbox. Вам понадобится настроить интеграцию и на стороне Kaspersky Endpoint Agent через консоль администрирования KSC, и на стороне Kaspersky Sandbox через веб-интерфейс.

Включение и отключение интеграции с Kaspersky Sandbox

Чтобы включить или отключить интеграцию с Kaspersky Sandbox, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры интеграции с Kaspersky Sandbox**.
5. В блоке параметров **Параметры интеграции с Kaspersky Sandbox** выполните одно из следующих действий:
   - Установите флажок **Включить интеграцию с Kaspersky Sandbox**, если вы хотите включить интеграцию с Kaspersky Sandbox.
   - Снимите флажок **Включить интеграцию с Kaspersky Sandbox**, если вы хотите отключить интеграцию с Kaspersky Sandbox.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.
7. Нажмите на кнопку **ОК**.

Интеграция с Kaspersky Sandbox будет включена или отключена.

Настройка доверенного соединения Kaspersky Sandbox с Kaspersky Endpoint Agent

Вы можете настроить доверенное соединение Kaspersky Sandbox с Kaspersky Endpoint Agent в веб-интерфейсе сервера Kaspersky Sandbox, не входящего в кластер.

Если вы уже объединили серверы в кластер, вам нужно удалить сервер из кластера, затем создать новый кластер на базе этого сервера и добавить в новый кластер все серверы, предназначенные для работы решения Kaspersky Sandbox.

Если нужные вам серверы входят в другой кластер, вам нужно последовательно удалить их из кластера, в который они входят в настоящий момент, а затем добавить в новый кластер.

Установка и настройка доверенного соединения Kaspersky Sandbox с Kaspersky Endpoint Agent состоит из следующих этапов:

1. Удаление сервера из кластера (если сервер входит в кластер в настоящий момент)
2. Генерация или загрузка TLS-сертификата соединения с Kaspersky Endpoint Agent на этот сервер
3. Создание нового кластера на базе этого сервера
4. Удаление всех серверов, которые вы хотите добавить в этот кластер, из кластеров, в которые они входят в настоящий момент
5. Добавление всех нужных серверов в новый кластер
6. Добавление всех серверов нового кластера Kaspersky Sandbox в список Kaspersky Endpoint Agent
7. Настройка доверенного соединения с Kaspersky Sandbox на стороне Kaspersky Endpoint Agent

Настройка доверенного соединения на стороне Kaspersky Sandbox

Для настройки доверенного соединения вам потребуется сгенерировать или загрузить TLS-сертификат на стороне Kaspersky Sandbox, а затем сохранить его на компьютере для загрузки в программу Kaspersky Endpoint Agent.

Чтобы сгенерировать TLS-сертификат соединения Kaspersky Sandbox с Kaspersky Endpoint Agent, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В блоке **TLS-сертификат для соединения с Kaspersky Endpoint Agent** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.
3. Нажмите на кнопку **Да**.

Kaspersky Sandbox сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Sandbox.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Чтобы загрузить TLS-сертификат через веб-интерфейс Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В блоке **TLS-сертификат для соединения с Kaspersky Endpoint Agent** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
3. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Sandbox.

Чтобы сохранить файл TLS-сертификата соединения с Kaspersky Endpoint Agent на компьютере, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В блоке **TLS-сертификат для соединения с Kaspersky Endpoint Agent** нажмите на кнопку **Скачать**.

Файл TLS-сертификата будет сохранен в папке загрузки браузера.

Настройка доверенного соединения на стороне Kaspersky Endpoint Agent

Чтобы настроить доверенное соединение Kaspersky Endpoint Agent, выполните следующие действия на стороне Kaspersky Endpoint Agent:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры интеграции с Kaspersky Sandbox**, блок параметров **Параметры интеграции с Kaspersky Sandbox**.
5. Установите флажок **Использовать доверенное соединение**.
6. Нажмите на кнопку **Добавить новый TLS-сертификат**.

   Откроется окно **Добавление TLS-сертификата**.
7. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Sandbox:

   - Добавьте файл сертификата. Для этого нажмите на кнопку **Обзор**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Open**.

- Скопируйте содержание файла сертификата в поле **Вставьте текстовые данные TLS-сертификата**.

В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера Kaspersky Sandbox. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.

8. Нажмите на кнопку **Добавить**.

   Информация о добавленном TLS-сертификате отобразится в блоке параметров **Параметры интеграции с Kaspersky Sandbox**.

9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

10. Нажмите на кнопку **ОК**.

Доверенное соединение с сервером Kaspersky Sandbox будет настроено.

Обновление данных TLS-сертификата Kaspersky Sandbox в Kaspersky Endpoint Agent

При замене TLS-сертификата сервера Kaspersky Sandbox, вам потребуется обновить данные TLS-сертификата Kaspersky Sandbox в Kaspersky Endpoint Agent и заново настроить доверенное соединение с Kaspersky Sandbox.

Чтобы обновить данные TLS-сертификата Kaspersky Sandbox в Kaspersky Endpoint Agent, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Политики**.

3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.

4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры интеграции с Kaspersky Sandbox**, блок параметров **Параметры интеграции с Kaspersky Sandbox**.

5. Установите флажок **Использовать доверенное соединение**.

6. Нажмите на кнопку **Добавить новый TLS-сертификат**.

   Откроется окно **Добавление TLS-сертификата**.

7. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Sandbox:

   - Добавьте файл сертификата. Для этого нажмите на кнопку **Обзор**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Open**.

- Скопируйте содержание файла сертификата в поле **Вставьте текстовые данные TLS-сертификата**.

В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера Kaspersky Sandbox. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.

8. Нажмите на кнопку **Добавить**.

   Информация о добавленном TLS-сертификате отобразится в блоке параметров **Параметры интеграции с Kaspersky Sandbox**.

9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

10. Нажмите на кнопку **ОК**.

Вы обновите данные TLS-сертификата сервера Kaspersky Sandbox и установите доверенное соединение с Kaspersky Sandbox.

Настройка времени ожидания ответа от Kaspersky Sandbox и параметров очереди запросов

Чтобы настроить время ожидания ответа от Kaspersky Sandbox и параметры очереди запросов на обработку объектов, поступающих от Kaspersky Endpoint Agent в Kaspersky Sandbox, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Политики**.

3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.

4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Расширенные параметры**.

5. В блоке параметров **Время ожидания** укажите максимальное время ожидания ответа сервера Kaspersky Sandbox.

6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

7. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Расширенные параметры**.

8. В блоке параметров **Очередь Kaspersky Sandbox** в поле **Папка очереди** укажите путь к папке, в которой будет храниться информация о запросах, отправляемых в Kaspersky Sandbox.

9. В поле **Максимальный размер очереди (МБ)** укажите максимально допустимый размер очереди запросов в мегабайтах.

10. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

11. Нажмите на кнопку **ОК**.

Добавление серверов Kaspersky Sandbox в список Kaspersky Endpoint Agent

Если вы включили интеграцию с Kaspersky Sandbox, вы можете добавить серверы Kaspersky Sandbox в список Kaspersky Endpoint Agent.

Вы можете добавить несколько серверов Kaspersky Sandbox.

В рамках одной политики добавляйте серверы, входящие в один кластер. Если серверы входят в разные кластеры, результат работы решения непредсказуем.

Все серверы в кластере равноправны независимо от того, на базе какого сервера был создан кластер. Результат обработки одного и того же объекта будет одинаковым на всех серверах кластера.

Программа Kaspersky Sandbox балансирует нагрузку между серверами. Объекты, поступающие на обработку в Kaspersky Sandbox от Kaspersky Endpoint Agent, обрабатываются на наименее загруженном сервере.

Чтобы кластер Kaspersky Sandbox обрабатывал объекты от Kaspersky Endpoint Agent, необходимо добавить в Kaspersky Endpoint Agent хотя бы один сервер, входящий в кластер при интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox.

В списке серверов Kaspersky Sandbox программы Kaspersky Endpoint Agent отображаются только те серверы, которые вы добавили в этот список. При этом объекты могут обрабатываться любым сервером кластера с учетом балансировки нагрузки. Актуальный список серверов кластера можно просмотреть в веб-интерфейсе Kaspersky Sandbox.

Рекомендуется добавить в Kaspersky Endpoint Agent все серверы кластера.

Kaspersky Endpoint Agent может подключиться к другому серверу Kaspersky Sandbox из списка при возникновении одной из следующих ошибок:

- Истекло время ожидания ответа от Kaspersky Sandbox (connection timeout).
- Kaspersky Sandbox недоступен (код ошибки 503 или 504).
- Проблема самодиагностики, за исключением проблем с лицензией (код ошибки 500).

При удалении сервера из кластера возможны следующие сценарии обработки объектов:

- Если в списке серверов Kaspersky Sandbox программы Kaspersky Endpoint Agent остается хотя бы один сервер этого кластера с актуальным IP-адресом или FQDN, Kaspersky Sandbox продолжит обрабатывать объекты от Kaspersky Endpoint Agent.

- Если в списке серверов Kaspersky Sandbox программы Kaspersky Endpoint Agent не остается ни одного сервера, входящего в этот кластер, или IP-адреса или FQDN серверов кластера неактуальны, Kaspersky Sandbox не сможет получать и обрабатывать объекты от Kaspersky Endpoint Agent.

  Для корректной обработки объектов необходимо добавить в Kaspersky Endpoint Agent хотя бы один сервер, входящий в кластер Kaspersky Sandbox.

Чтобы добавить серверы Kaspersky Sandbox в список Kaspersky Endpoint Agent, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры интеграции с Kaspersky Sandbox**.
5. Установите флажок **Включить интеграцию с Kaspersky Sandbox**, если он снят.
6. В блоке параметров **Список серверов Kaspersky Sandbox** нажмите на кнопку **Добавить**.

   Откроется окно **Свойства сервера**.
7. Введите IP-адрес или FQDN сервера Kaspersky Sandbox, а также порт подключения к серверу.
8. Нажмите на кнопку **Добавить**.

   Добавленный сервер отобразится в таблице серверов.
9. Повторите действия для добавления каждого сервера Kaspersky Sandbox в список.
10. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.
11. Нажмите на кнопку **ОК**.

Серверы Kaspersky Sandbox будут добавлены в список Kaspersky Endpoint Agent.

Настройка действий Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox

Kaspersky Endpoint Agent может выполнять действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox.

Вы можете настроить действия следующих типов:

- *Локальные* – действия, которые будут выполняться на каждой рабочей станции, на которой обнаружена угроза.

- *Групповые* – действия, которые будут выполняться на всех рабочих станциях группы администрирования, для которой вы настраиваете политику.

Локальные действия:

- **Поместить на карантин и удалить**.

  При обнаружении угрозы на рабочей станции копия объекта, содержащего угрозу, будет помещена на карантин, а объект будет удален с рабочей станции.

- **Уведомить пользователя рабочей станции**.

  При обнаружении угрозы на рабочей станции пользователю рабочей станции будет показано уведомление об обнаруженной угрозе.

  > Уведомление отображается, если рабочая станция включена под той учетной записью пользователя, под которой была обнаружена угроза.

  > Если рабочая станция выключена или выполнен вход под другой учетной записью, уведомление не отображается.

- **Дать команду Endpoint Protection Platform (EPP) на проверку критических областей**.

  При обнаружении угрозы на рабочей станции Kaspersky Endpoint Agent даст команду программе EPP на проверку критических областей этой рабочей станции. К критическим областям относятся память ядра, объекты, загружаемые при запуске операционной системы, и загрузочные секторы жесткого диска. Подробнее о настройке параметров проверки см. в документации используемой EPP.

Групповые действия:

- **Найти IOC по управляемой группе хостов**.

  При обнаружении угрозы на любой из рабочих станций группы администрирования, для которой вы настраиваете политику, Kaspersky Endpoint Agent проверит все рабочие станции этой группы администрирования на наличие объекта, содержащего обнаруженную угрозу.

- **Поместить на карантин и удалить, когда найден IOC**.

  При обнаружении угрозы на любой из рабочих станций группы администрирования, для которой вы настраиваете политику, Kaspersky Endpoint Agent проверит все рабочие станции этой группы администрирования на наличие объекта, содержащего обнаруженную угрозу. Если на каких-то рабочих станциях этой группы администрирования Kaspersky Endpoint Agent найдет объект, содержащий угрозу, копия этого объекта будет помещена на карантин, а объект будет удален с рабочих станций.

- **Дать команду Endpoint Protection Platform (EPP) на проверку критических областей, когда найден IOC**.

При обнаружении угрозы на любой из рабочих станций группы администрирования, для которой вы настраиваете политику, Kaspersky Endpoint Agent даст команду программе EPP на проверку критических областей на всех рабочих станциях этой группы администрирования, на которых Kaspersky Endpoint Agent найдет объект, содержащий угрозу. Подробнее о настройке параметров проверки см. в документации используемой EPP.

При настройке действий по реагированию на угрозы учитывайте, что в результате выполнения некоторых из настроенных действий объект, содержащий угрозу, может быть удален с рабочей станции, на которой он был обнаружен.

Включение и отключение выполнения действий по реагированию на угрозы

Чтобы включить или отключить выполнение программой Kaspersky Endpoint Agent действий по реагированию на угрозы, обнаруженные Kaspersky Sandbox, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
5. В блоке параметров **Действия**:
   - Установите флажок **Выполнять действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox**, если вы хотите включить выполнения действий по реагированию на угрозы.
   - Снимите флажок **Выполнять действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox**, если вы хотите отключить выполнения действий по реагированию на угрозы.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.
7. Нажмите на кнопки **Применить** и **ОК**.

Добавление действий по реагированию на угрозы в список действий текущей политики

Чтобы добавить действия по реагированию на угрозы в список действий текущей политики, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.

3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.

4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.

5. В блоке параметров **Действия** установите флажок **Выполнять действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox**, если он не установлен.

6. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите одно из следующих действий:

   - **Поместить на карантин и удалить**. Локальное действие. Будет выполняться на рабочей станции, на которой обнаружена угроза.
   - **Уведомить пользователя рабочей станции**. Локальное действие. Будет выполняться на рабочей станции, на которой обнаружена угроза.
   - **Дать команду Endpoint Protection Platform (EPP) на проверку критических областей**. Локальное действие. Будет выполняться на рабочей станции, на которой обнаружена угроза.
   - **Найти IOC по управляемой группе хостов**. Групповое действие. Будет выполняться на всех рабочих станциях группы администрирования.
   - **Поместить на карантин и удалить, когда найден IOC**. Групповое действие. Будет выполняться на всех рабочих станциях группы администрирования.
   - **Дать команду Endpoint Protection Platform (EPP) на проверку критических областей, когда найден IOC**. Групповое действие. Будет выполняться на всех рабочих станциях группы администрирования.

   Действие будет добавлено в список **Текущие действия**.

   При настройке действий по реагированию на угрозы учитывайте, что в результате выполнения некоторых из настроенных действий объект, содержащий угрозу, может быть удален с рабочей станции, на которой он был обнаружен.

7. Если вы хотите удалить действие, выберите его в таблице и нажмите на кнопку **Удалить**.

8. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

9. Нажмите на кнопки **Применить** и **ОК**.

Аутентификация на Сервере администрирования для групповых задач по реагированию на угрозы

Если вы хотите, чтобы программа Kaspersky Endpoint Agent создавала групповые задачи по реагированию на угрозы, вам нужно пройти аутентификацию на Сервере администрирования: ввести имя пользователя и пароль подключения к Kaspersky Security Center.

Вы можете пройти аутентификацию под учетной записью "внутреннего пользователя KSC", созданной в Kaspersky Security Center, или использовать механизм аутентификации "Windows authentication".

Подробнее о создании учетных записей Kaspersky Security Center и механизме аутентификации "Windows authentication" см. в *Справке Kaspersky Security Center*.

Имя учетной записи не должно совпадать с доменным именем пользователя и не может быть в формате `<имя домена>\<имя пользователя>`.

Чтобы пройти аутентификацию на Сервере администрирования, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
5. В блоке параметров **Аутентификация на Сервере администрирования** в поле **Имя пользователя Сервера администрирования** введите имя учетной записи пользователя Kaspersky Security Center.
6. В блоке параметров **Аутентификация на Сервере администрирования** в поле **Пароль для входа на Сервер администрирования** введите пароль доступа к Kaspersky Security Center.
7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.
8. Нажмите на кнопку **ОК**.

Защита рабочих станций от легальных программ, которые могут быть использованы злоумышленниками

Вы можете включить обнаружение легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда локальной сети вашей организации. Kaspersky Endpoint Agent будет считать такие программы угрозой и выполнять над ними действия по реагированию на угрозы.

Легальные программы – программы, разрешенные к установке и использованию на рабочих станциях и предназначенные для выполнения задач пользователя. Однако легальные программы некоторых типов при использовании злоумышленниками могут нанести вред рабочей станции или локальной сети организации. Если злоумышленники получат доступ к таким программам или внедрят их на рабочую станцию, они могут использовать некоторые функции таких программ для нарушения безопасности рабочей станции или локальной сети организации.

К таким программам относятся: IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Если вы хотите включить обнаружение таких программ, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
5. В блоке параметров **Дополнительные параметры** установите флажок **Включить обнаружение легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру**.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.
7. Нажмите на кнопки **Применить** и **ОК**.

Обнаружение легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда локальной сети вашей организации, будет включено.

Настройка запуска задач поиска IOC

Если Kaspersky Sandbox обнаружил угрозу, в Kaspersky Endpoint Agent автоматически создаются задачи поиска IOC (MD5-хешей объектов, в которых была обнаружена угроза) по всем рабочим станциям.

Чтобы просмотреть список задач на сервере Kaspersky Security Center, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.

Отобразится список задач.

Вы можете настроить запуск этих задач.

Чтобы настроить запуск задач поиска IOC, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
5. В блоке параметров **Дополнительные параметры** нажмите на кнопку **Настроить**.

   Откроется окно **Параметры поиска IOC**.

6. В блоке параметров **Области поиска** выберите одну из следующих областей, в которых Kaspersky Endpoint Agent будет выполнять поиск IOC:

   - **Файловые области, в которых расположены системные папки**.
   - **Критические файловые области**.

7. В блоке параметров **Начало поиска** выберите один из следующих вариантов запуска задач поиска IOC:

   - **Вручную**.

     Задачи поиска IOC будут создаваться автоматически, но не будут запускаться. Вы сможете запускать вручную каждую задачу или все задачи.

   - **Сразу после появления обнаружений Kaspersky Sandbox**.

     Задачи поиска IOC будут автоматически создаваться и запускаться.

   - **В заданный период**.

     Задачи поиска IOC будут создаваться автоматически, а запускаться будут в заданный период. Например, в нерабочее время с 20:00 до 7:00.

     Если вы выбрали вариант **В заданный период**, в полях **Начало периода (чч:мм)** и **Конец периода (чч:мм)** настройте начало и конец периода.

     Все задачи поиска IOC, автоматически созданные ДО указанного начала периода, запустятся в произвольное время В ПРЕДЕЛАХ указанного периода.

     Все задачи поиска IOC, автоматически созданные В ПРЕДЕЛАХ указанного периода, запустятся немедленно.

     Все задачи поиска IOC, автоматически созданные ПОСЛЕ указанного начала периода, запустятся на следующий день.

   Пример:

   Если вы настроили запуск задач в заданный период с 20:00 до 7:00:

   Задачи, автоматически созданные в 19:00, запустятся в произвольное время с 20:00 до 7:00.

   Задачи, автоматически созданные в 21:00, запустятся в 21:00.

   Задачи, автоматически созданные в 22:00, запустятся на следующий день с 20:00 до 7:00.

8. Нажмите на кнопку **ОК**.

Окно **Параметры поиска IOC** закроется.

9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

10. Нажмите на кнопки **Применить** и **ОК**.

Запуск задач поиска IOC будет настроен.

Настройка параметров карантина и восстановления объектов из карантина

Одним из действий Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox, является помещение объектов, содержащих угрозу, на карантин.

Карантин – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности рабочей станции.

Kaspersky Security Center формирует общий список объектов, помещенных на карантин на рабочих станциях с программой Kaspersky Endpoint Agent. Агенты администрирования рабочих станций передают информацию о файлах на карантине на Сервер администрирования. Через консоль KSC можно просматривать свойства объектов, находящихся на карантине на рабочих станциях, запускать проверку этих объектов, удалять объекты, находящиеся на карантине, а также восстанавливать объекты из карантина.

Kaspersky Security Center не копирует файлы из карантина на Сервер администрирования. Все объекты находятся на рабочих станциях с программой Kaspersky Endpoint Agent. Восстановление объектов из карантина также выполняется на рабочих станциях.

Карантин создается под той учетной записью пользователя рабочей станции, под которой был обнаружен объект, содержащий угрозу.

> Удаление объектов, помещенных на карантин, через командную строку доступно только под локальной учетной записью пользователя рабочей станции.

Чтобы настроить параметры карантина Kaspersky Endpoint Agent, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Политики**.

3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.

4. В разделе **Репозитории** выберите подраздел **Карантин**.

5. В блоке **Параметры карантина** настройте параметры карантина. Выполните следующие действия:

a. В поле **Папка карантина** введите путь, по которому вы хотите создать папку карантина на рабочих станциях или нажмите на кнопку **Обзор** и выберите путь.

   По умолчанию используется путь `%SOYUZAPPDATA%\Quarantine\`. Папка Quarantine будет создана на всех рабочих станциях с Kaspersky Endpoint Agent в директории `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

   Значения переменной `%ALLUSERSPROFILE%` зависят от операционной системы рабочей станции, на которой установлена программа Kaspersky Endpoint Agent.

   Пример:

   Если на рабочей станции установлена операционная система Windows 7 и программа Kaspersky Endpoint Agent установлена на диске C, путь к папке карантина будет следующим:

   `C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Quarantine`

b. Если вы хотите задать максимальный размер карантина, установите флажок **Максимальный размер карантина (МБ)** и введите или выберите в списке максимальный размер карантина в МБ.

   По достижении максимального размера карантина Kaspersky Endpoint Agent не сможет помещать на карантин новые объекты, пока вы не удалите часть старых объектов.

   Например, вы можете задать максимальный размер карантина 200 МБ.

c. Если вы хотите задать пороговое значение карантина (место в карантине, оставшееся до достижения максимального размера карантина), установите флажок **Пороговое значение места на диске (МБ)**.

   По достижении порогового значения карантина, Kaspersky Endpoint Agent перестанет помещать на карантин новые объекты, пока вы не удалите часть старых объектов.

   Например, вы можете задать пороговое значение карантина 50 МБ.

6. В блоке **Восстановление объектов из карантина** в поле **Папка назначения для восстановленных объектов** введите путь, по которому вы хотите создать папку для объектов, восстановленных из карантина.

   По умолчанию используется путь `%SOYUZAPPDATA%\Restored\`. Папка Restored будет создана на всех рабочих станциях с Kaspersky Endpoint Agent в директории `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

   Значения переменной `%ALLUSERSPROFILE%` зависят от операционной системы рабочей станции, на которой установлена программа Kaspersky Endpoint Agent.

   Пример:

   Если на рабочей станции установлена операционная система Windows 7 и программа Kaspersky Endpoint Agent установлена на диске C, путь к папке карантина будет следующим:

   `C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored`

7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

8. Нажмите на кнопки **Применить** и **ОК**.

Параметры карантина и восстановления объектов из карантина будут настроены.

Настройка синхронизации данных с Сервером администрирования

Вы можете настроить синхронизацию данных о работе программы Kaspersky Endpoint Agent на рабочих станциях с Сервером администрирования Kaspersky Security Center.

Чтобы настроить синхронизацию данных с Сервером администрирования, выполните следующие действия:

1. Откройте консоль KSC.

2. В дереве консоли откройте папку **Политики**.

3. Выберите нужную политику и откройте ее свойства двойным щелчком мыши.

4. В разделе **Репозитории** выберите подраздел **Синхронизация с Сервером администрирования**.

5. В блоке **Параметры** для параметра **Синхронизировать с Сервером администрирования** установите флажок **Данные об объектах, помещенных на карантин на управляемых хостах**.

6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.

7. Нажмите на кнопки **Применить** и **ОК**.

Синхронизация данных с Сервером администрирования будет настроена.

Работа с задачами Kaspersky Endpoint Agent

В этом разделе описана работа с задачами Kaspersky Endpoint Agent в KSC.

Просмотр списка задач

Чтобы просмотреть список задач на сервере Kaspersky Security Center, выполните следующие действия:

1. Откройте консоль KSC.

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

Отобразится список задач.

Удаление задач из списка

Чтобы удалить задачи из списка задач на сервере Kaspersky Security Center, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.
3. В списке задач выберите задачи, которые вы хотите удалить.

   Откроется окно со списком действий, которые вы можете выполнять над задачами.
4. Выберите действие **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные задачи будут удалены из списка.

Запуск задач вручную

Вы можете вручную запустить задачи обновления баз и поиска IOC.

Чтобы вручную запустить одну задачу, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите задачу в списке и правой кнопкой мыши раскройте меню действий над задачами.
4. Выберите действие **Запустить**.

Задача запустится.

Чтобы вручную запустить все задачи, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите любую задачу в списке и правой кнопкой мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Все задачи** и действие **Запустить**.

Все задачи запустятся.

Просмотр результатов выполнения задач

Вы можете просмотреть результат выполнения задач в течение срока хранения результатов выполнения задач.

Вы можете изменить срок хранения результатов выполнения задач.

Рекомендуется не сокращать срок хранения результатов выполнения задач поиска IOC.

Чтобы просмотреть результат выполнения задачи, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите задачу в списке и правой кнопкой мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Результаты**.

Откроется окно **Результат выполнения задачи**.

Изменение срока хранения результатов выполнения задач на Сервере администрирования

По умолчанию результаты выполнения задач хранятся на Сервере администрирования 7 дней.

Чтобы изменить срок хранения результатов выполнения задач на Сервере администрирования, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите задачу в списке и правой кнопкой мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел **Уведомление**.
6. В блоке **Сохранять информацию о результатах** убедитесь, что флажок **На Сервере администрирования в течение (сут)** установлен и укажите, сколько суток вы хотите хранить

результат выполнения задачи.

7. Нажмите на кнопки **Применить** и **ОК**.

Рекомендуется не сокращать срок хранения результатов выполнения задач поиска IOC.

Управление задачами обновления баз

Вы можете создавать и настраивать параметры задач обновления баз программы.

Создание задачи обновления баз

Чтобы создать задачу обновления баз Kaspersky Endpoint Agent в Kaspersky Security Center, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Выберите блок типов задач **Kaspersky Endpoint Agent 3.7** и тип задачи **Обновить базы**.
5. Нажмите на кнопку **Далее**.

   Запустится мастер создания задачи обновления баз.

Мастер создания задачи обновления баз состоит из следующих этапов:

1. Выбор источника обновления баз

   Выполните следующие действия:

   1. В блоке **Источник обновлений** выберите один из следующих источников обновления баз:
      - **Источник обновлений**.
      - **Серверы обновлений "Лаборатории Касперского"**.
      - **Другие HTTP-, FTP-серверы или сетевые ресурсы**.
   2. Если вы хотите включить параметр **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**, установите флажок слева от названия параметра.

3. Если вы выбрали источник обновления баз **Серверы обновлений "Лаборатории Касперского"** и хотите использовать прокси-сервер для обновления баз, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.

4. Если вы выбрали источник обновления баз **Другие HTTP-, FTP-серверы или сетевые ресурсы**, выполните следующие действия:

   a. По ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы** откройте окно **Серверы обновлений**.

   b. Добавьте серверы обновлений в список:

      1. Нажмите на кнопку **Серверы обновлений**.

      2. В добавленной строке введите IP-адрес сервера обновлений.

      3. Если вы хотите использовать этот сервер для обновления баз, установите флажок рядом с его IP-адресом. Вы также можете добавить в список серверы и снять флажки рядом с IP-адресами серверов, которые вы не хотите использовать сейчас, а планируете использовать в будущем.

         Выполняйте аналогичные действия по добавлению каждого сервера.

      4. Нажмите на кнопку **ОК**.

      5. Окно **Серверы обновлений** закроется.

   c. Если вы хотите использовать прокси-сервер для соединения с серверами обновлений, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами** и нажмите на кнопку **Далее**.

2. Настройка расписания обновления баз

Выполните следующие действия:

1. В блоке **Расписание запуска задач** установите флажок **Запускать по расписанию**.

2. В списке **Периодичность** выберите один из следующих вариантов запуска задачи по расписанию: **В назначенное время**, **Каждый час**, **Каждый день**, **Каждую неделю**, **При запуске программы** или **После обновления баз программы**.

3. Если вы выбрали запуск задачи обновления баз **В назначенное время**, в блоке **Запускать по расписанию** укажите время и дату запуска задачи.

4. Если вы выбрали запуск задачи обновления баз **Каждый час**, **Каждый день** или **Каждую неделю**, в блоке **Запускать по расписанию** настройте параметры запуска задачи:

a. В списке **Каждый:** выберите периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.

b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.

5. Если вы хотите выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и выполните следующие действия в окне **Дополнительно**:

a. Если вы хотите задать максимальное время ожидания выполнения задачи обновления баз, установите флажок **Завершать задачу через** и укажите, через сколько часов и минут задача будет автоматически завершаться.

b. Если вы хотите, чтобы расписание запуска задачи обновления баз действовало до определенной даты, установите флажок **Отключить расписание** и укажите дату окончания действия расписания.

c. Если вы хотите, чтобы программа при первой возможности запускала задачи обновления баз, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.

d. Если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Распределить время запуска в интервале** и задайте интервал запуска в минутах.

e. Нажмите на кнопку **ОК**.

6. Нажмите на кнопку **Далее**

3. Выбор устройств, на которые будет назначена задача

В открывшемся окне выбора устройств выберите устройства, на который вы хотите назначить задачу и нажмите на кнопку **Далее**.

Например, вы можете выбрать вариант **Назначить задачу группе администрирования** и выбрать группу администрирования из списка.

4. Выбор учетной записи пользователя Kaspersky Security Center, под которой вы хотите запускать задачу

В окне **Выбор учетной записи для запуска задачи** выполните одно из следующих действий:

- Выберите учетную запись по умолчанию и нажмите на кнопку **Далее**.
- Введите имя и пароль пользователя, под учетной записью которого вы хотите выполнять задачу и нажмите на кнопку **Далее**.

5. Назначение имени задачи

В окне **Определение название задачи** в поле **Имя** введите название задачи и нажмите на кнопку **Далее**.

6. Запуск задачи сразу после создания

   Если вы хотите, чтобы задача запустилась сразу после создания, установите флажок **Запустить задачу после завершения работы мастера**.и нажмите на кнопку **Готово**.

Настройка параметров задачи обновления баз

Вы можете настроить параметры задачи обновления баз после ее создания.

Чтобы изменить параметры задачи, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.

   Отобразится список задач.
3. В секции **Обновить базы** выберите задачу в списке и правой кнопкой мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел параметров, которые вы хотите настроить.
6. В правой части окна внесите необходимые изменения и нажмите на кнопки **Применить** и **ОК**.

Вы можете настроить следующие параметры задачи:

1. Имя задачи

   Выполните следующие действия:

   1. Выберите раздел **Общие**.
   2. Измените имя задачи в верхней строке.

2. Устройства, на которые будет назначена задача

   В правой части окна отображаются текущие устройства, на которые назначена задача. Если вы хотите добавить устройства, выполните следующие действия:

   1. Нажмите на кнопку **Добавить**.

Откроется окно со списком управляемых устройств.

2. Установите флажки рядом с теми устройствами, которые вы хотите добавить.

3. Если вы хотите добавить устройства, которых нет в списке, нажмите на кнопку **Добавить** в правой части окна и выполните действия по добавлению устройств.

   Например, вы можете задать адреса устройств вручную или импортировать их из списка

   Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым вы хотите назначить задачу.

Подробнее о работе с управляемыми устройствами см. в *Справке Kaspersky Security Center*.

3. Источник обновления баз

Выполните следующие действия:

1. В блоке **Источник обновлений** выберите один из следующих источников обновления баз:

   - **Источник обновлений**.
   - **Серверы обновлений "Лаборатории Касперского"**.
   - **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

2. Если вы хотите включить параметр **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**, установите флажок слева от названия параметра.

3. Если вы выбрали источник обновления баз **Серверы обновлений "Лаборатории Касперского"** и хотите использовать прокси-сервер для обновления баз, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.

4. Если вы выбрали источник обновления баз **Другие HTTP-, FTP-серверы или сетевые ресурсы**, выполните следующие действия:

   a. По ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы** откройте окно **Серверы обновлений**.

   b. Добавьте серверы обновлений в список:

      1. Нажмите на кнопку **Серверы обновлений**.

      2. В добавленной строке введите IP-адрес сервера обновлений.

      3. Если вы хотите использовать этот сервер для обновления баз, установите флажок рядом с его IP-адресом. Вы также можете добавить в список серверы

и снять флажки рядом с IP-адресами серверов, которые вы не хотите использовать сейчас, а планируете использовать в будущем.

Выполняйте аналогичные действия по добавлению каждого сервера.

4. Нажмите на кнопку **ОК**.

5. Окно **Серверы обновлений** закроется.

c. Если вы хотите использовать прокси-сервер для соединения с серверами обновлений, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

4. Расписание обновления баз

Выполните следующие действия:

1. В блоке **Расписание запуска задач** установите флажок **Запускать по расписанию**.

2. В списке **Периодичность** выберите один из следующих вариантов запуска задачи по расписанию: **В назначенное время**, **Каждый час**, **Каждый день**, **Каждую неделю**, **При запуске программы** или **После обновления баз программы**.

3. Если вы выбрали запуск задачи обновления баз **В назначенное время**, в блоке **Запускать по расписанию** укажите время и дату запуска задачи.

4. Если вы выбрали запуск задачи обновления баз **Каждый час**, **Каждый день** или **Каждую неделю**, в блоке **Запускать по расписанию** настройте параметры запуска задачи:

   a. В списке **Каждый:** выберите периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.

   b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.

5. Если вы хотите выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и выполните следующие действия в окне **Дополнительно**:

   a. Если вы хотите задать максимальное время ожидания выполнения задачи обновления баз, установите флажок **Завершать задачу через** и укажите, через сколько часов и минут задача будет автоматически завершаться.

   b. Если вы хотите, чтобы расписание запуска задачи обновления баз действовало до определенной даты, установите флажок **Отключить расписание** и укажите дату окончания действия расписания.

   c. Если вы хотите, чтобы программа при первой возможности запускала задачи обновления баз, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.

d. Если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Распределить время запуска в интервале** и задайте интервал запуска в минутах.

e. Нажмите на кнопку **ОК**.

5. Учетную запись пользователя Kaspersky Security Center, под которой вы хотите запускать задачу

   В окне **Выбор учетной записи для запуска задачи** выполните одно из следующих действий:

   - Выберите учетную запись по умолчанию и нажмите на кнопку **Далее**.
   - Введите имя и пароль пользователя, под учетной записью которого вы хотите выполнять задачу.

6. Срок хранения результатов выполнения задачи на Сервере администрирования

   Выполните следующие действия:

   1. Выберите раздел **Уведомление**.
   2. В блоке **Сохранять информацию о результатах** убедитесь, что флажок **На Сервере администрирования в течение (сут)** установлен и укажите, сколько суток вы хотите хранить результат выполнения задачи.

      По умолчанию результат выполнения задачи хранится на Сервере администрирования 7 дней.

Управление задачами поиска IOC

Вы можете настраивать параметры задач поиска IOC, а также параметры запуска задач поиска IOC.

Создание задач поиска IOC недоступно в текущей версии программы.

О задачах поиска IOC

Задачи поиска IOC создаются автоматически на сервере Kaspersky Security Center, если в политиках Kaspersky Endpoint Agent настроено действие по реагированию на угрозу **Найти IOC по управляемой группе хостов**.

Создание задач поиска IOC вручную недоступно в текущей версии программы.

Вы можете просматривать список задач, удалять неиспользуемые задачи из списка, просматривать результаты выполнения задач, запускать задачи вручную, настраивать срок хранения результатов выполнения задач, а также настраивать параметры запуска задач поиска IOC.

Автоматически созданные задачи накапливаются на сервере Kaspersky Security Center. Администратору программы рекомендуется следить за тем, чтобы количество задач в списке не превышало 1000 задач и периодически вручную удалять задачи из списка.

Задачи поиска IOC по умолчанию хранятся на сервере Kaspersky Security Center 7 дней с момента последнего запуска.

Kaspersky Endpoint Agent удаляет автоматически созданные задачи поиска IOC в случае, если хотя бы на одной рабочей станции программа KEA работала без перерыва 7 или более дней и выполнено одно из следующих условий:

- Задача в последний раз запускалась 7 или более дней назад.
- Задача не запускалась ни разу, и с момента создания задачи прошло 7 или более дней.

Kaspersky Endpoint Agent удаляет задачу поиска IOC независимо от того, на какой рабочей станции впервые был обнаружен объект и было выполнено действие по реагированию на угрозы. Удаленная задача будет недоступна для всех рабочих станций, входящих в группу администрирования.

Удаление неиспользуемых задач поиска IOC происходит автоматически. Настройка параметров автоматического удаления задач поиска IOC не предусмотрена программой.

Если удаление задач поиска IOC выполняется некорректно или вы хотите изменить поведение программы, обратитесь в Службу технической поддержки "Лаборатории Касперского".

По умолчанию в задаче поиска IOC настроено хранение ВСЕХ типов событий, возникающих в ходе работы групповых задач. По умолчанию результаты выполнения задач поиска IOC хранятся 7 дней. Вы можете изменить срок хранения результатов выполнения задач.

Рекомендуется не изменять значения параметров хранения результатов выполнения задач, установленные по умолчанию, и не сокращать срок хранения результатов выполнения задач поиска IOC.

Настройка прав пользователей KSC для управления задачами поиска IOC

Необходимо настроить права пользователя KSC, под учетной записью которого вы хотите управлять задачами поиска IOC.

Чтобы настроить права пользователя KSC для управления задачами поиска IOC, выполните следующие действия:

1. Откройте консоль KSC.
2. Выберите **Сервер администрирования** и правой кнопкой мыши раскройте меню действий над Сервером администрирования.
3. Выберите пункт меню **Свойства**.

   Откроется окно свойств Сервера администрирования.
4. В левой части окна выберите раздел **Безопасность**.
5. Выберите пользователя KSC, под учетной записью которого вы хотите управлять задачами поиска IOC.

   В нижней части окна отобразится список прав выбранного пользователя, сгруппированных по программам, которыми пользователь может управлять через KSC.
6. В группе прав **Kaspersky Endpoint Agent** раскройте блок **Предотвращение вторжений**.
7. Для типов прав **Изменение**, **Выполнение** и **Выполнение действий над выборками устройств** установите флажки в колонке **Разрешить**.
8. Нажмите на кнопки **Применить** и **ОК**.

Настройка параметров задачи поиска IOC

Чтобы настроить параметры задачи поиска IOC, выполните следующие действия:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Задачи**.

   Отобразится список задач.
3. В блоке **Запустить поиск IOC** выберите задачу в списке и правой кнопкой мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел параметров, которые вы хотите изменить.
6. В правой части окна внесите необходимые изменения и нажмите на кнопки **Применить** и **ОК**.

Вы можете настроить следующие параметры задачи:

1. Имя задачи

   Выполните следующие действия:

1. Выберите раздел **Общие**.
2. Измените имя задачи в верхней строке.

2. Срок хранения результатов выполнения задачи на Сервере администрирования

   Выполните следующие действия:

   1. Выберите раздел **Уведомление**.
   2. В блоке **Сохранять информацию о результатах** убедитесь, что флажок **На Сервере администрирования в течение (сут)** установлен и укажите, сколько суток вы хотите хранить результат выполнения задачи.

      По умолчанию результат выполнения задачи хранится на Сервере администрирования 7 дней.

3. Параметры поиска IOC

   Выполните следующие действия:

   1. Если вы хотите, чтобы Kaspersky Endpoint Agent выполнял действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox, на всех рабочих станциях группы администрирования, в блоке **Действия** установите флажок **Выполнить действия по реагированию на угрозы, когда найден IOC**.
   2. Установите флажок **Поместить на карантин и удалить**.

      При обнаружении угрозы на любой из рабочих станций группы администрирования Kaspersky Endpoint Agent проверит все рабочие станции группы администрирования на наличие объекта, содержащего обнаруженную угрозу. Если на каких-то рабочих станциях группы администрирования Kaspersky Endpoint Agent найдет объект, содержащий угрозу, копия этого объекта будет помещена на карантин, а объект будет удален с рабочих станций.
   3. Установите флажок **Дать команду Endpoint Protection Platform (EPP) на проверку критических областей**.

      При обнаружении угрозы на любой из рабочих станций группы администрирования Kaspersky Endpoint Agent даст команду программе EPP на проверку критических областей на всех рабочих станциях группы администрирования, на которых Kaspersky Endpoint Agent найдет объект, содержащий угрозу. Подробнее о настройке параметров проверки см. в документации используемой EPP.

4. Экспорт базы поиска IOC

   Выполните следующие действия:

1. В блоке **База поиска IOC** нажмите на кнопку **Экспортировать базу поиска IOC**.

2. Выберите директорию, в которую вы хотите сохранить файл и нажмите на кнопку **Сохранить**.

Файл формата zip загрузится на жесткий диск вашего компьютера.

5. Расписание запуска задач поиска IOC

Выполните следующие действия:

1. В блоке **Расписание запуска задач** установите флажок **Запускать по расписанию**.

2. В списке **Периодичность** выберите один из следующих вариантов запуска задач поиска IOC: **В назначенное время**, **Каждый час**, **Каждый день**, **Каждую неделю** или **При запуске программы**.

3. Если вы выбрали запуск задачи **В назначенное время**, в блоке **Запускать по расписанию** укажите время и дату запуска задачи.

4. Если вы выбрали запуск задачи **Каждый час**, **Каждый день** или **Каждую неделю**, в блоке **Запускать по расписанию** настройте параметры запуска задачи:

   a. В списке **Каждый:** выберите периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.

   b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.

5. Если вы хотите выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и выполните следующие действия в окне **Дополнительно**:

   a. Если вы хотите задать максимальное время ожидания выполнения задачи, установите флажок **Завершать задачу через** и укажите, через сколько часов и минут задача будет автоматически завершаться.

   b. Если вы хотите, чтобы расписание запуска задачи действовало до определенной даты, установите флажок **Отключить расписание** и укажите дату окончания действия расписания.

   c. Если вы хотите, чтобы программа при первой возможности запускала задачи поиска IOC, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.

   d. Если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Распределить время запуска в интервале** и задайте интервал запуска в минутах.

   e. Нажмите на кнопку **ОК**.

6. Просмотр результатов выполнения задач поиска IOC

   В списке **Показать результаты выполнения задач на хосте** выберите, по каким рабочим станциям вы хотите просмотреть результаты выполнения задач поиска IOC.

   Отобразится таблица, содержащая следующую информацию о выполнении задач поиска IOC: **Уровень важности**, **Имя хоста**, **Время**, **Результаты**.

   Чтобы просмотреть подробную информацию об определенной задаче, раскройте ее двойным щелчком мыши.

7. Выбор учетной записи пользователя Kaspersky Security Center, под которой вы хотите запускать задачу

   В окне **Выбор учетной записи для запуска задачи** выполните одно из следующих действий:

   - Выберите учетную запись по умолчанию и нажмите на кнопку **Далее**.
   - Введите имя и пароль пользователя, под учетной записью которого вы хотите выполнять задачу.

8. Исключение групп хостов из области действия задачи

   Если вы хотите исключить группы хостов из области действия задачи, в разделе **Исключения из области действия задачи** выберите группы устройств, к которым не будет применяться задача.

   Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

Взаимодействие с внешними системами по API

Вы можете настроить интеграцию Kaspersky Sandbox с внешними системами для проверки хранящихся в них файлов, а также для предоставления внешним системам доступа к результатам этой проверки. Программа анализирует и оценивает поведение файлов в изолированной среде, но не устанавливает наличие в них вредоносных объектов. По результатам проверки пользователь внешней системы получает информацию, обнаружены ли признаки подозрительного поведения файла. Пользователю требуется самостоятельно принять решение о дальнейших действиях с файлом.

Взаимодействие внешних систем с Kaspersky Sandbox осуществляется с помощью интерфейса REST API.

Программа анализирует заголовок файла и определяет его формат, который может отличаться от расширения файла. Например, злоумышленник может отправить вирус или другую программу, представляющую угрозу, в исполняемом файле, переименованном в файл с расширением txt.

Список поддерживаемых форматов файлов

Поддерживается проверка файлов следующих форматов:

- PE_EXE.
- DOC.
- DOCX.
- DOTX.
- DOCM.
- DOTM.
- XLS.
- XLSX.
- XLTX.
- XLSM.
- XLTM.
- XLAM.
- XLSB.
- PPT.
- PPTX.
- POTX.
- PPTM.
- POTM.
- PPSX.
- PPSM.
- RTF.
- PDF.

Проверка объектов

Для проверки объектов используется метод `POST`.

Синтаксис

```
POST "sample=<путь к объекту> <URL-адрес сервера Sandbox>/sandbox/v1/tasks"
```

Пример

```
curl POST https://api.example.com/sandbox/v1/tasks -F "sample=@/path/to/file.ext"
```

Возвращаемое значение

Код возврата	Описание
`200`	Данный файл уже был проверен. Возможные значения: • `Not found` – не обнаружены признаки вредоносных объектов. • `Found` – обнаружены признаки вредоносных объектов.
`201`	Файл успешно отправлен на проверку. Задаче присвоен идентификатор `task_id`.
`400`	Некорректный запрос.
`500`	Не удалось отправить файл на проверку по одной из следующих причин: • Нет действующей лицензии. • Превышен максимально допустимый размер файла (60 МБ). • Не поддерживается формат файла. • Переполнена очередь запросов. • Неизвестная ошибка.
`503`	Сервер недоступен. Попробуйте обратиться к другому серверу или повторите попытку позже.
`504`	Истекло время ожидания сервера. Попробуйте обратиться к другому серверу или повторите попытку позже.

Просмотр результатов проверки

Для просмотра результатов проверки используется метод `GET`.

Синтаксис

```
GET "<URI-адрес сервера Sandbox>/sandbox/v1/tasks/<task_id>"
```

Пример

```
curl GET
"https://api.example.com/sandbox/v1/tasks/c0999b05aca8ffd5692d4a13ad16281b"
```

Параметры

Параметр	Тип	Описание
`task_id`	string	Уникальный идентификатор задачи, присвоенный во время отправки объекта на проверку.

Возвращаемое значение

Код возврата	Описание
`200`	Результат проверки получен. Возможны следующие значения: • `Processing` – проверка выполняется. • `Found` – обнаружены признаки вредоносных объектов. • `Not found` – не обнаружены признаки вредоносных объектов. • `Error` – ошибка проверки.
`400`	Некорректный запрос.
`404`	Не найдены результаты проверки по указанному идентификатору.
`500`	Ошибка получения результатов проверки. Возможны следующие причины: • Нет действующей лицензии. • Неизвестная ошибка.
`503`	Сервер недоступен. Попробуйте обратиться к

	другому серверу или повторите попытку позже.
504	Истекло время ожидания ответа сервера. Попробуйте обратиться к другому серверу или повторите попытку позже.

Глоссарий

End User License Agreement

Юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

IOC

Indicator of Compromise (индикатор компрометации). Набор данных о вредоносном объекте или действии.

IOC-файл

IOC-файл содержит набор индикаторов IOC.

Kaspersky Endpoint Agent

Программа в составе решения Kaspersky Sandbox. Устанавливается в составе Endpoint Protection Platform (EPP) на рабочих станциях и серверах сети вашей организации и обеспечивает коммуникацию EPP и программы Kaspersky Sandbox, а также выполнение действий по автоматическому реагированию на обнаруженные угрозы, настроенных в политиках Kaspersky Security Center.

Kaspersky Sandbox

Решение, обнаруживающее и автоматически блокирующее сложные угрозы на клиентских устройствах (рабочих станциях, компьютерах, серверах, далее также "рабочих станциях").

Также программа в составе решения Kaspersky Sandbox, отвечающая за серверную часть решения. Устанавливается на один или несколько серверов внутри сети вашей организации. Серверы можно объединять в кластер. На серверах Kaspersky Sandbox развернуты виртуальные образы операционных систем Microsoft Windows, в которых запускаются проверяемые объекты. Kaspersky Sandbox анализирует поведение объектов для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Open IOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий свыше 500 различных индикаторов компрометации.

Дамп

Содержимое рабочей памяти процесса или всей оперативной памяти системы в определенный момент времени.

Поиск IOC

Действие Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox. Настраивается в политиках Kaspersky Security Center.

При обнаружении угрозы на любой из рабочих станций группы администрирования, для которой вы настраиваете политику, Kaspersky Endpoint Agent проверяет все рабочие станции этой группы администрирования на наличие объекта, содержащего обнаруженную угрозу.

Политики Kaspersky Endpoint Agent

Набор параметров программы Kaspersky Endpoint Agent. Настраивается в Kaspersky Security Center для рабочих станций, входящих в группу администрирования.

Трассировка

Отладочное выполнение программы, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

Основные понятия Kaspersky Security Center, относящиеся к управлению решением через KSC

Этот раздел содержит определения основных понятий Kaspersky Security Center, относящихся к управлению программами Kaspersky Sandbox и Kaspersky Endpoint Agent через Kaspersky Security Center.

Сервер администрирования

Компоненты Kaspersky Security Center позволяют осуществлять удаленное управление программами "Лаборатории Касперского", установленными на клиентских устройствах (на рабочих станциях, компьютерах, серверах).

Устройства, на которых установлен компонент Kaspersky Security Center Сервер администрирования, называются *Серверами администрирования*. Серверы администрирования должны быть защищены от любого типа несанкционированного доступа, включая физическую защиту.

Сервер администрирования устанавливается на устройство в качестве службы со следующим набором атрибутов:

- под именем "Сервер администрирования Kaspersky Security Center";

- с автоматическим типом запуска, при старте операционной системы;
- с учетной записью Локальная система либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов программ;
- удаленная установка программ на клиентские устройства и удаление программ;
- обновление баз и модулей программ "Лаборатории Касперского";
- управление политиками и задачами на клиентских устройствах;
- хранение информации о событиях, произошедших на клиентских устройствах;
- формирование отчетов о работе программ "Лаборатории Касперского";
- распространение ключей на клиентские устройства, хранение информации о ключах;
- отправка уведомлений о ходе выполнения задач (например, об обнаружении вирусов на клиентском устройстве).

Агент администрирования

Взаимодействие между Сервером администрирования и устройствами обеспечивается *Агентом администрирования* – компонентом Kaspersky Security Center. Агент администрирования требуется установить на все устройства, на которых управление работой Kaspersky Endpoint Agent выполняется с помощью Kaspersky Security Center.

Агент администрирования устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- под именем "Kaspersky Security Center <версия Kaspersky Security Center> Network Agent" (например: "Kaspersky Security Center 12 Network Agent");
- с автоматическим типом запуска при старте операционной системы;
- с помощью учетной записи LocalSystem.

Устройство, на которое установлен Агент администрирования, называется *управляемым устройством*.

Агент администрирования для управления программой Kaspersky Endpoint Agent можно установить на устройство под управлением операционной системы Windows.

Нет необходимости устанавливать Агент администрирования на устройства, на которых установлен Сервер администрирования, поскольку северная версия Агента администрирования устанавливается автоматически совместно с Сервером администрирования.

Название процесса, который запускает Агент администрирования, – klnagent.exe.

Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (периодический сигнал) равным 15 минут на 10 000 управляемых устройств.

Консоль администрирования

Консоль администрирования (далее также "*консоль KSC*") – это компонент программы Kaspersky Security Center, предоставляющий пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

Группа администрирования

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

Для всех клиентских устройств в группе устанавливаются:

- Единые параметры работы программ – с помощью групповых политик.
- Единый режим работы всех программ – с помощью создания групповых задач с определенным набором параметров. Примеры групповых задач включают создание и установку общего инсталляционного пакета, обновление баз и модулей программы, проверку устройства по требованию и включение постоянной защиты.

Клиентское устройство может входить в состав только одной группы администрирования.

Для Серверов администрирования и групп администрирования можно создавать иерархии с любым уровнем вложенности. На одном уровне иерархии могут располагаться подчиненные и виртуальные Серверы администрирования, группы и клиентские устройства. Можно переводить устройства из одной группы в другую, не перемещая их физически. Например, если сотрудник предприятия перешел с позиции бухгалтера на позицию разработчика, вы можете перевести компьютер этого сотрудника из группы администрирования "Бухгалтеры" в группу администрирования "Разработчики". Таким образом, на компьютер будут автоматически переданы параметры работы программ, необходимые для позиции разработчика.

Управляемое устройство

Управляемое устройство – это устройство (рабочая станция, компьютер, сервер) под управлением Windows, на котором установлен Агент администрирования. Вы можете управлять такими устройствами с помощью задач и политик для программ "Лаборатории Касперского", установленных на устройствах. Вы также можете формировать отчеты для управляемых устройств.

Вы можете настроить управляемое устройство, чтобы оно выполняло функции точки распространения и шлюза соединений.

Устройство может находиться под управлением только одного Сервера администрирования. Один Сервер администрирования может обслуживать до 100 000 устройств.

Плагин управления

Управление программами "Лаборатории Касперского" через Консоль администрирования выполняется при помощи плагинов управления. В состав каждой программы "Лаборатории Касперского", которой можно управлять при помощи Kaspersky Security Center, входит плагин управления.

С помощью плагина управления программой в Консоли администрирования можно выполнять следующие действия:

- создавать и редактировать политики и параметры программы, а также параметры задач этой программы;
- получать информацию о задачах программы, событиях в ее работе, а также о статистике работы программы, получаемой с клиентских устройств.

Политики

Политика – это набор параметров работы программы, определенный для группы администрирования. Политика определяет не все параметры программы.

Для одной программы можно настроить несколько политик с различными значениями. Однако в каждый момент времени для программы может быть активна только одна политика в группе администрирования.

Вы можете активировать отключенную политику при возникновении определенного события. Это означает, например, что в период вирусных эпидемий можно включить параметры для более сильной антивирусной защиты.

Для разных групп администрирования параметры работы программы могут быть различными. В каждой группе может быть создана собственная политика для программы.

Параметры программы определяются параметрами политик и задач.

Вложенные группы и подчиненные Серверы администрирования наследуют задачи групп более высоких уровней иерархии.

Параметр **Наследовать параметры родительской политики** находится в окне свойств унаследованной политики, в блоке **Наследование параметров** раздела **Общие**. В любое время можно отключить наследование из родительской политики, если эта возможность не заблокирована в политике верхнего уровня.

В разделе **Параметры программы** вы можете заблокировать параметры, которые требуется оставить без изменений в дочерних политиках. Каждый параметр, представленный в политике, имеет атрибут замок:  или . Значок замка показывает, можно ли изменять параметры политики для вложенных групп и подчиненных Серверов администрирования.

Профиль политики

Может возникнуть необходимость создать несколько копий одной политики для разных групп администрирования; может также возникнуть необходимость централизованно изменить параметры этих политик. Эти копии могут различаться одним или двумя параметрами. Например, все бухгалтеры в организации работают под управлением одной и той же политики, но старшим бухгалтерам разрешено использовать флеш-накопители USB, а младшим бухгалтерам – не разрешено. В этом случае применение политик к устройствам только через иерархию групп администрирования может оказаться неудобным.

Чтобы избежать создания нескольких копий одной политики, Kaspersky Security Center позволяет создавать *профили политик*. Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики.

Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – условия активации профиля. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве. При активации профиля изменяются параметры "базовой" политики, которые исходно действовали на устройстве. Эти параметры принимают значения, указанные в профиле.

Задачи

Kaspersky Security Center управляет работой программ "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка программ, проверка файлов, обновление баз и модулей программ, другие действия с программами.

Вы можете создать задачу для программы, только если для этой программы установлен плагин управления.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных;
- синхронизация обновлений Windows Update;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

Локальные задачи могут быть изменены не только администратором средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе программы безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждой программы вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущена программа, для которой созданы эти задачи.

Результаты выполнения задач сохраняются в журналах событий Microsoft Windows и Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

Не используйте в параметрах задач конфиденциальные данные. Например, пароль доменного администратора.

Область действия задачи

Область задачи – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- *Локальная задача*. Область задачи – это само устройство.
- *Задача Сервера администрирования*. Область задачи – Сервер администрирования.
- *Групповая задача*. Область задачи – перечень устройств, входящих в группу.
- *Глобальная задача*. Область задачи можно задать с помощью различных методов, подробнее см. в *Справке Kaspersky Security Center*.

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского": https://www.kaspersky.ru

Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com

Информация о стороннем коде

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe – товарный знак или зарегистрированный в Соединенных Штатах Америки и/или в других странах товарный знак Adobe Systems Incorporated.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Android и Google Chrome – товарные знаки Google, Inc.

Microsoft, Windows и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS – товарный знак компании Red Hat, Inc.

VMware ESXi – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.