kaspersky

# Kaspersky Linux Management Console

Руководство администратора

Версия программы: 1.0

kaspersky

Уважаемый пользователь!

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



Дата редакции документа: 09.04.2020



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

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

kaspersky

# Содержание

kaspersky

# Об этом руководстве

Руководство администратора Kaspersky Linux Management Console 1.0 (далее также "Kaspersky LMC") адресовано техническим специалистам которые осуществляют установку и администрирование Kaspersky LMC, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky LMC.

Руководство адресовано техническим специалистам, которые имеют опыт работы с операционной системой Linux®.

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

- подготовка к установке, установка и активация Kaspersky LMC;
- настройка и использование Kaspersky LMC.

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

kaspersky

# Условные обозначения

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

*Таблица 1. Условные обозначения*

| Пример текста | Описание условного обозначения |
|---|---|
| Обратите внимание на то, что... | Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия. |
| Рекомендуется использовать... | Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию. |
| **Пример:**<br>… | Примеры приведены в блоках на голубом фоне под заголовком "Пример". |
| *Обновление* – это...<br>Возникает событие *Базы устарели*. | Курсивом выделены следующие элементы текста:<br>• новые термины;<br>• названия статусов и событий программы. |
| Нажмите на клавишу **ENTER**.<br>Нажмите комбинацию клавиш **ALT**+**F4**. | Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами.<br>Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно. |
| Нажмите на кнопку **Включить**. | Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом. |
| ► *Чтобы настроить расписание задачи, выполните следующие действия:* | Вводные фразы инструкций выделены курсивом и значком "стрелка". |
| В командной строке введите текст `help`<br>Появится следующее сообщение:<br>`Укажите дату в формате ДД:ММ:ГГ.` | Специальным стилем выделены следующие типы текста:<br>• текст командной строки;<br>• текст сообщений, выводимых программой на экран;<br>• данные, которые требуется ввести с клавиатуры. |
| <Имя пользователя> | Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки. |

kaspersky

# Источники информации о программе

Этот раздел содержит описание источников информации о программе.

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

## В этом разделе



# Источники для самостоятельного поиска информации

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

- страница Kaspersky LMC на веб-сайте Службы технической поддержки (База знаний);
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 92).

Для использования Базы знаний требуется подключение к интернету.

**Страница Kaspersky LMC в Базе знаний**

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

На странице Kaspersky LMC в Базе знаний (https://support.kaspersky.ru/klmc1) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

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

**Документация**

В руководстве администратора вы можете найти информацию для выполнения следующих задач:

- подготовка к установке, установка и активация Kaspersky LMC;
- настройка и использование Kaspersky LMC.

# Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе (https://community.kaspersky.com).

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

kaspersky

# О Kaspersky Linux Management Console 1.0

Программа Kaspersky LMC предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты инфраструктуры организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности инфраструктуры организации и позволяет настраивать параметры защиты, построенной на основе программ "Лаборатории Касперского".

Kaspersky LMC версии 1.0 поддерживает управление программой Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux. Управление другими программами в этой версии не поддерживается.

Kaspersky LMC позволяет выполнять следующие действия:

- объединять устройства с установленными программами "Лаборатории Касперского" в группы администрирования для централизованного управления работой программ (см. раздел "Управление устройствами и группами администрирования" на стр. 30);
- с помощью политик централизовано управлять параметрами защиты устройств с установленными программами (см. раздел "Управление защитой с помощью политик" на стр. 44) "Лаборатории Касперского";
- с помощью задач удаленно управлять параметрами работы программ "Лаборатории Касперского", установленных в инфраструктуре организации (см. раздел "Управление защитой с помощью задач" на стр. 62);
- загружать обновления баз и модулей программ "Лаборатории Касперского" на Сервер Kaspersky LMC и ретранслировать на управляемые устройства (см. раздел "Обновление баз и модулей управляемых программ" на стр. 72);
- получать информацию о состоянии защиты инфраструктуры организации в виде событий от управляемых программ (см. раздел "События" на стр. 77) и отчетов о работе программ и устройств (см. раздел "Отчеты" на стр. 82);
- получать информацию о событиях в работе Сервера Kaspersky LMC;
- настраивать уведомления о событиях (см. раздел "Настройка уведомлений о событиях" на стр. 80);
- настраивать использование Локального KSN в работе управляемых программ (см. раздел "Участие в Kaspersky Security Network" на стр. 74).

## В этом разделе

kaspersky

# Комплект поставки

В комплект поставки входят файлы, необходимые для установки компонентов программы, в том числе:

- пакеты для установки компонентов программы Kaspersky LMC;
- архив с файлом для установки коннектора управляемой программы Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux;
- файл с текстом Положения о Kaspersky Security Network для Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux;
- файл с текстом Лицензионного соглашения, в котором указано, на каких условиях вы можете пользоваться программой, и Политики конфиденциальности, которая описывает обработку и передачу данных.

Состав комплекта поставки может быть различным в зависимости от региона, в котором распространяется программа.

# Аппаратные и программные требования

**Требования компонента Сервер Kaspersky LMC**

Для установки и работы Сервера Kaspersky LMC компьютер должен удовлетворять следующим программным требованиям:

- Операционная система Astra Linux SE 1.6 (Smolensk).
- Интерпретатор Python3.
- СУБД PostgreSQL 9.6.
- Сервер RabbitMQ™ 3.6.
- Веб-сервер Apache2.
- Библиотека ia32-libs.

Программа Kaspersky LMC сохраняет конфиденциальные данные (например, пароль прокси-сервера, который задается в политике) в зашифрованном виде. Для шифрования используется системная библиотека OpenSSL. Рекомендуется своевременно обновлять операционную систему для обеспечения защиты конфиденциальных данных.

Для установки и работы Сервера Kaspersky LMC компьютер должен удовлетворять следующим минимальным аппаратным требованиям:

- Процессор с частотой 2 ГГц или выше.
- Объем оперативной памяти: 4 ГБ.
- Объем свободного места на диске: 10 ГБ.

**Требования компонента Агент Kaspersky LMC**

Для установки и работы Агента Kaspersky LMC на компьютере должна быть установлена одна из следующих операционных систем:

- Astra Linux SE 1.6 (Smolensk).
- Astra Linux 1.5.

Для установки и работы Агента Kaspersky LMC компьютер должен удовлетворять следующим минимальным аппаратным требованиям:

- Процессор с частотой 1 ГГц или выше.
- Объем оперативной памяти: 1 ГБ.
- Объем свободного места на диске: 5 ГБ.

kaspersky

# Архитектура программы

В состав Kaspersky LMC входят следующие компоненты:

- Сервер Kaspersky Linux Management Console (далее – "Сервер Kaspersky LMC"). Обеспечивает централизованное управление программами "Лаборатории Касперского", которые осуществляют антивирусную защиту (далее – "управляемые программы"), а также централизованное хранение информации о работе управляемых программ и защите инфраструктуры организации. Устанавливается на рабочем месте администратора Kaspersky LMC.
- Агент Kaspersky Linux Management Console (далее – "Агент Kaspersky LMC"). Обеспечивает взаимодействие между Сервером Kaspersky LMC и управляемыми программами. Устанавливается на компьютере или другом устройстве, где установлена управляемая программа.

Взаимодействие между Агентом Kaspersky LMC и Сервером Kaspersky LMC обеспечивает сервер сообщений RabbitMQ.

Для хранения данных программы используется СУБД PostgreSQL.

Для загрузки обновлений баз и модулей управляемых программ на Сервер Kaspersky LMC используется утилита Update Utility. Утилита входит в комплект поставки программы Kaspersky LMC и устанавливается автоматически на рабочем месте администратора Kaspersky LMC.

## В этом разделе



# Концепция управления программой

Работа с программой осуществляется через интерфейс командной строки.

Установка, настройка и управление работой программы выполняется с помощью утилит командной строки:

- Утилита easy-install позволяет выполнять первоначальную настройку Сервера Kaspersky LMC.
- Утилита lmcadmin позволяет настраивать параметры Сервера Kaspersky LMC.
- Утилита lmc предоставляет интерфейс к основной функциональности программы Kaspersky LMC.

Для получения краткой информации обо всех доступных командах утилит lmcadmin и lmc вы можете использовать следующие команды:

- `<утилита> -h` – отобразить список доступных команд утилиты;
- `<утилита> <команда> -h` – отобразить информацию о параметрах команды.

Для просмотра информации о параметрах и состоянии Сервера Kaspersky LMC вы можете использовать следующие команды:

- `lmcadmin get` – отобразить параметры взаимодействия Сервера Kaspersky LMC с сервером RabbitMQ и СУБД PostgreSQL.
- `lmcadmin status` – отобразить подробную информацию о состоянии Сервера Kaspersky LMC.

Настройку Сервера Kaspersky LMC рекомендуется выполнять с помощью утилиты easy-install.

Для управления программой вы также можете использовать следующие команды:

- Для Сервера Kaspersky LMC:
  - `systemctl start lmc-server.service` – запустить Сервер Kaspersky LMC. После установки Сервер Kaspersky LMC запускается автоматически.
  - `systemctl stop lmc-server.service` – остановить Сервер Kaspersky LMC.
  - `systemctl restart lmc-server.service` – перезапустить Сервер Kaspersky LMC.
  - `systemctl status lmc-server.service` – посмотреть состояние Сервера Kaspersky LMC.
- Для Агента Kaspersky LMC:
  - `systemctl start lmc-agent.service` – запустить Агент Kaspersky LMC. После установки Агент Kaspersky LMC запускается автоматически.
  - `systemctl stop lmc-agent.service` – остановить Агент Kaspersky LMC.
  - `systemctl restart lmc-agent.service` – перезапустить Агент Kaspersky LMC.
  - `systemctl status lmc-agent.service` – посмотреть состояние Агента Kaspersky LMC.

**Особенности использования команд Kaspersky LMC**

Во всех командах, которые выводят какие-либо данные, вы можете использовать необязательный параметр `[--json | --yaml]`, чтобы указать формат вывода данных: JSON или YAML. По умолчанию данные выводятся в табличном виде.

По умолчанию в ходе выполнения команд создания и изменения параметров в программе Kaspersky LMC автоматически запускается текстовый редактор. Программа Kaspersky LMC использует редактор, установленный по умолчанию в вашей системе (определяется переменной окружения EDITOR).

Если вы хотите отменить запуск редактора после выполнения команды создания группы администрирования, политики или задачи, вам нужно выполнить команду с параметром `[--no-edit]`. В результате группа администрирования, политика или задача будет создана с параметрами по умолчанию.

Во время проведения работ по диагностике специалистам Службы технической поддержки может понадобиться дополнительная информация об ошибках, которые происходят во время выполнения команд утилиты lmc. Чтобы получить дополнительную информацию об ошибке, вы можете запустить команду с параметром `[--debug]`. В результате будет выведено сообщение об ошибке вместе со стеком вызовов, который привел к этой ошибке.

# Об обработке данных

Во время работы компоненты программы Kaspersky LMC могут сохранять и передавать другим компонентам программы информацию, которая может содержать персональные и конфиденциальные данные.

Сервер Kaspersky LMC принимает, хранит и обрабатывает следующие данные:

- Сведения об управляемых устройствах и о программах "Лаборатории Касперского", установленных на устройствах.

- События, полученные от управляемой программы, и события, произошедшие в процессе работы Сервера Kaspersky LMC.
- Значения параметров работы управляемых программ, представленные в виде политик.

  Программа Kaspersky LMC сохраняет конфиденциальные данные (например, пароль прокси-сервера, который задается в политике) в зашифрованном виде. Для шифрования используется системная библиотека OpenSSL. Рекомендуется своевременно обновлять операционную систему для обеспечения защиты конфиденциальных данных.
- Данные о лицензировании и активации управляемых программ.
- Данные об обновлениях баз управляемых программ.
- Сертификат безопасности сервера RabbitMQ, к которому подключается Сервер Kaspersky LMC для получения сообщений от Агентов Kaspersky LMC.
- Имена и пароли учетных записей для подключения к серверу RabbitMQ и СУБД PostgreSQL. Параметры учетных записей хранятся в открытом виде, защищены через ACL.
- Ключ шифрования, используемый для защиты персональных данных в политиках Kaspersky LMC.

Агент Kaspersky LMC хранит имя и пароль учетной записи для подключения к серверу RabbitMQ и СУБД PostgreSQL. Параметры учетной записи хранятся в открытом виде, защищены через ACL.

Все перечисленные данные хранятся и обрабатываются локально и не передаются в "Лабораторию Касперского".

Данные могут попадать в файлы трассировки Сервера Kaspersky LMC. Данные хранятся в открытом виде. Для доступа к данным необходимы полномочия учетной записи root.

Рекомендуется обеспечить защиту данных от несанкционированного доступа.

kaspersky

# Подготовка к установке программы

Перед началом установки Kaspersky LMC вам нужно выполнить следующие действия:

- Убедиться, что аппаратное и программное обеспечение компьютеров, на которых будут установлены компоненты программы, соответствует требованиям программы Kaspersky LMC (см. раздел "Аппаратные и программные требования" на стр. 11).
- Загрузить файлы, необходимые для установки программы (см. раздел "Комплект поставки" на стр. 11).
- Убедиться, что на компьютере, на котором будет установлен Агент Kaspersky LMC, не установлен Агент администрирования Kaspersky Security Center.

  Совместная работа Агента Kaspersky LMC и Агента администрирования Kaspersky Security Center не поддерживается.

- Убедиться в том, что в настройках сетевого оборудования или программного обеспечения, обеспечивающего контроль трафика в сети организации, разрешено прохождение сетевого трафика через порты, используемые при установке и работе программы:
  - порт 80 на Сервере Kaspersky LMC – для загрузки обновлений баз и модулей управляемых программ с Сервера Kaspersky LMC на управляемые устройства;
  - порт 5671 на сервере RabbitMQ – для подключения управляемых устройств и Сервера Kaspersky LMC.

kaspersky

# Установка и первоначальная настройка программы

Установку и первоначальную настройку программы Kaspersky LMC следует выполнять под учетной записью root.

Установка и первоначальная настройка программы Kaspersky LMC состоит из следующих этапов:

1. Установка и настройка компонента Сервер Kaspersky LMC на рабочем месте администратора Kaspersky LMC.

   Чтобы установить и подготовить к работе Сервер Kaspersky LMC, вам нужно выполнить следующие действия:

   a. Установить пакет Сервера Kaspersky LMC (см. раздел "Установка пакета Сервера Kaspersky LMC" на стр. 18). Вы можете выполнить установку в тихом или интерактивном режиме.

      Для установки Сервера Kaspersky LMC требуется принять условия Лицензионного соглашения и Политики конфиденциальности.

   b. Выполнить первоначальную настройку Сервера Kaspersky LMC (см. раздел "Первоначальная настройка Сервера Kaspersky LMC" на стр. 19). Настройка выполняется в автоматическом режиме с помощью скрипта первоначальной настройки easy-install.

2. Установка коннектора управляемой программы на компьютере или другом устройстве, где установлена управляемая программа (см. раздел "Установка коннектора управляемой программы Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux" на стр. 21).

3. Установка и настройка компонента Агент Kaspersky LMC на компьютере или другом устройстве, где установлена управляемая программа.

   Управляемую программу рекомендуется устанавливать перед началом установки Агента Kaspersky LMC. Если вы установили управляемую программу после Агента Kaspersky LMC, то после установки управляемой программы вам нужно перезапустить Агент Kaspersky LMC.

   Чтобы установить и подготовить к работе Агент Kaspersky LMC, вам нужно выполнить следующе действия:

   a. Установить пакет Агента Kaspersky LMC (см. раздел "Установка пакета Агента Kaspersky LMC" на стр. 21). Вы можете выполнить установку в тихом или интерактивном режиме.

      Для установки Агента Kaspersky LMC требуется принять условия Лицензионного соглашения.

   b. Подключить Агент Kaspersky LMC к Серверу Kaspersky LMC (см. раздел "Подключение Агента Kaspersky LMC к Серверу Kaspersky LMC" на стр. 22). Вы можете выполнить подключение в тихом или интерактивном режиме.

kaspersky

## В этом разделе



# Установка пакета Сервера Kaspersky LMC

► *Чтобы установить пакет Сервера Kaspersky LMC в интерактивном режиме, выполните следующие действия:*

1. Запустите скрипт установки:

   ```
   dpkg -i lmc-server-signed-<номер версии программы>_amd64.deb
   ```

2. Ознакомьтесь с текстом Лицензионного соглашения, которое заключается между вами и "Лабораторией Касперского", и Политики конфиденциальности, которая описывает обработку и передачу данных. Для этого нажмите на клавишу **ENTER**.

   Для завершения просмотра используйте клавишу **Q**.

   После выхода из режима просмотра введите `yes` (или `y`), если вы согласны с условиями Лицензионного соглашения и Политики конфиденциальности. Установив значение `yes`, вы подтверждаете следующее:

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

   > Согласие с условиями Лицензионного соглашения и Политикой конфиденциальности является необходимым условием для установки Сервера Kaspersky LMC.

► *Чтобы установить пакет Сервера Kaspersky LMC в тихом режиме, выполните команду:*

```
LMC_EULA_AGREED=yes LMC_PP_AGREED=yes dpkg -i lmc-server-signed-<номер версии программы>_amd64.deb
```

► *Чтобы убедиться, что Сервер Kaspersky LMC установлен и запущен, выполните команду:*

```
systemctl status lmc-server.service
```

kaspersky

# Первоначальная настройка Сервера Kaspersky LMC

Первоначальную настройку Сервера Kaspersky LMC рекомендуется выполнять с помощью утилиты первоначальной настройки easy-install.

Утилита первоначальной настройки выполняет следующие действия:

- Устанавливает сервер RabbitMQ, СУБД PostgreSQL и веб-сервера Apache, если они не установлены.

  Если СУБД PostgreSQL установлена средствами утилиты easy-install, доступ к СУБД с правами администратора осуществляется под системной учетной записью postgres. Для обеспечения защиты данных от несанкционированного доступа рекомендуется убедиться, что права на выполнение команд под учетной записью postgres предоставлены только уполномоченным пользователям (см. man sudo, man sudoers).

- Производит настройку сервера RabbitMQ и СУБД PostgreSQL для работы с программой Kaspersky LMC:
  - Создает учетные записи для подключения Сервера Kaspersky LMC к серверу RabbitMQ и к СУБД PostgreSQL.
  - Настраивает параметры подключения Сервера Kaspersky LMC к серверу RabbitMQ и к СУБД PostgreSQL.
  - Создает базу данных для работы программы Kaspersky LMC.
  - Создает SSL-сертификат сервера RabbitMQ, необходимый для подключения Агентов Kaspersky LMC к Серверу Kaspersky LMC, и настраивает конфигурационный файл сервера RabbitMQ на использование этого сертификата.

    Если на момент установки Сервера Kaspersky LMC конфигурационный файл сервера RabbitMQ /etc/rabbitmq/rabbitmq.config уже существует, рекомендуется убедиться, что сервер RabbitMQ настроен на работу с использованием SSL-сертификата, и при необходимости настроить работу только по защищенному каналу SSL (подробнее см. в документации сервера RabbitMQ).

  - Создает и настраивает учетную запись сервера RabbitMQ для подключения Агентов Kaspersky LMC к Серверу Kaspersky LMC, и настраивает для этой учетной записи права, необходимые для авторизации Агентов.
- Позволяет настроить загрузку обновлений баз и модулей управляемых программ на Сервер Kaspersky LMC:
  - Производит настройку Update Utility и веб-сервера Apache для загрузки и ретрансляции обновлений для управляемых программ.
  - Настраивает расписание загрузки обновлений в системном планировщике Cron. По умолчанию загрузка запускается на пятнадцатой минуте каждого часа.
  - Позволяет задать источник обновлений и загрузить базы.

Вы также можете выполнить первоначальную настройку Сервера Kaspersky LMC вручную. За информацией обращайтесь в Службу Технической поддержки.

► *Чтобы выполнить первоначальную настройку Сервера Kaspersky LMC с помощью утилиты easy-install, выполните следующие действия:*

1. Запустите утилиту первоначальной настройки на компьютере, где установлен Сервер Kaspersky LMC:

   `/opt/kaspersky/lmc-server/install/easy-install`

2. Утилита создает сертификат сервера RabbitMQ, необходимый для подключения Агентов Kaspersky LMC к Серверу Kaspersky LMC. По запросу утилиты укажите следующие данные для сертификата:
   - название организации, на которую выпускается сертификат;
   - полное доменное имя (FQDN) сервера Kaspersky LMC.
3. По запросу утилиты введите пароль и подтверждение пароля для учетной записи lmc_agent_admin, которая создается автоматически и используется при подключении Агентов к Серверу Kaspersky LMC (см. раздел "Подключение Агента Kaspersky LMC к Серверу Kaspersky LMC" на стр. 22).
4. Если вы хотите настроить загрузку обновлений баз и модулей управляемых программ (см. раздел "Обновление баз и модулей управляемых программ" на стр. 72) на Сервер Kaspersky LMC, выполните следующие действия:
   a. Подтвердите необходимость настройки по запросу утилиты.
   b. Укажите путь к источнику обновлений баз. Возможные варианты:
      - `KLServers` – в качестве источника обновлений используются серверы "Лаборатории Касперского". Этот вариант используется по умолчанию.
      - `<путь к источнику обновлений>` – путь к локальной или сетевой директории, которая содержит последние обновления.
   c. Если в инфраструктуре используется прокси-сервер для доступа в интернет, укажите параметры прокси-сервера в одном из следующих форматов:
      - `<IP-адрес>:<порт>`, если при подключении к прокси-серверу не требуется аутентификация
      - `<имя пользователя>:<пароль>@<IP-адрес>:<порт>`, если при подключении к прокси-серверу требуется аутентификация.
   d. Если прокси-сервер не используется, введите `no`.
   e. Если требуется, подтвердите загрузку обновлений баз сразу после применения параметров.

      Базы будут помещены в директорию /var/opt/kaspersky/lmc-uu/Bases/.

      Вы можете выполнить загрузку обновлений позже вручную (см. раздел "Обновление баз и модулей управляемых программ" на стр. 72).

► *Чтобы проверить, что первоначальная настройка Сервера Kaspersky LMC завершена успешно, выполните команду:*

```
lmcadmin status
```

В результате выполнения команды отображается статус подключения к серверу RabbitMQ и СУБД PostgreSQL:

```
RabbitMQ: connected
PostgreSQL: connected
```

# Установка коннектора управляемой программы Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux

Коннектор управляемой программы для Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Linux нужно установить на компьютере перед установкой Агента Kaspersky LMC. Коннектор входит в комплект поставки Kaspersky LMC.

Чтобы установить коннектор управляемой программы, вам нужно распаковать архив коннектора в корневую директорию.

► *Чтобы распаковать архив коннектора управляемой программы, выполните команду:*

```
tar xvf lmc-kesl-connector-*.tar.gz -C / --no-overwrite-dir
```

В результате создается директория /opt/kaspersky/lmc-kesl-connector и конфигурационный файл /etc/opt/kaspersky/lmc-connectors/LmcConnector64.conf.

# Установка пакета Агента Kaspersky LMC

► *Чтобы установить Агент Kaspersky LMC в интерактивном режиме, выполните следующие действия:*

1. Запустите скрипт установки, выполнив следующую команду:

   ```
   dpkg -i lmc-agent-signed-<номер версии программы>_amd64.deb
   ```

2. Ознакомьтесь с текстом Лицензионного соглашения, которое заключается между вами и "Лабораторией Касперского". Для этого нажмите на клавишу **ENTER**. Для завершения просмотра используйте клавишу **Q**.

   После выхода из режима просмотра введите `yes` (или `y`), если вы согласны с условиями Лицензионного соглашения. Установив значение `yes`, вы подтверждаете, что вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения.

   > Согласие с условиями Лицензионного соглашения является необходимым условием для установки Агента Kaspersky LMC.

► *Чтобы установить пакет Агента Kaspersky LMC в тихом режиме, выполните команду:*

```
LMC_EULA_AGREED=yes dpkg -i lmc-agent-signed-<номер версии
программы>_amd64.deb
```

► *Чтобы убедиться, что Агент успешно установлен, выполните команду:*

```
systemctl status lmc-agent.service
```

# Подключение Агента Kaspersky LMC к Серверу Kaspersky LMC

► *Чтобы подключить Агент Kaspersky LMC в интерактивном режиме, выполните следующие действия:*

1. На компьютере, где установлен Агент Kaspersky LMC, выполните команду:

   ```
   lmcagent
   ```

2. По запросу последовательно введите следующие параметры:
   - Произвольное описание компьютера (device description). По умолчанию указано `<none>`.
   - Адрес сервера RabbitMQ, к которому подключен Сервер Kaspersky LMC. Вы можете указать IP-адрес или доменное имя компьютера, на котором установлен сервер RabbitMQ.
   - Порт для подключения к серверу RabbitMQ, к которому подключен Сервер Kaspersky LMC. По умолчанию используется порт `5671`.
   - Имя учетной записи для подключения Агентов Kaspersky LMC к Серверу Kaspersky LMC (lmc_agent_admin).
   - Пароль учетной записи для подключения Агентов Kaspersky LMC к Серверу Kaspersky LMC.
3. Посмотрите информацию об SSL-сертификате, полученном от сервера RabbitMQ. Для этого нажмите на клавишу **ENTER**. Для завершения просмотра используйте клавишу **Q**.

   Если сертификат соответствует сертификату, указанному в конфигурационном файле сервера RabbitMQ /etc/rabbitmq/rabbitmq.config, подтвердите подлинность сертификата, чтобы продолжить подключение к серверу RabbitMQ. Для этого после выхода из режима просмотра введите `yes` (или `y`).

   Если вы не считаете этот сертификат подлинным, введите `no` (или `n`), чтобы прервать подключение. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

► *Чтобы подключить Агент Kaspersky LMC в тихом режиме, выполните следующие действия:*

1. Создайте файл autoinstall.ini и укажите в этом файле следующие параметры подключения:

   ```
   [DEVICE]

   DESCRIPTION = <произвольное описание компьютера, на котором установлен Агент Kaspersky LMC>

   [SERVER]

   HOSTNAME = <IP-адрес или доменное имя сервера RabbitMQ, к которому подключен Сервер Kaspersky LMC>

   PORT = <порт для подключения к серверу RabbitMQ, к которому подключен Сервер
   ```

```
Kaspersky LMC>
FINGERPRINT = <отпечаток SHA-1 сертификата сервера RabbitMQ>
[ADMIN]
LOGIN = lmc_agent_admin
PASSWORD = <пароль учетной записи для подключения Агентов Kaspersky LMC к Серверу Kaspersky LMC>
```

(имя учетной записи для подключения Агентов Kaspersky LMC к Серверу Kaspersky LMC)

2. Выполните команду:

```
lmcagent --autoinstall <путь к файлу autoinstall.ini>
```

После подключения компьютера с установленным Агентом Kaspersky LMC к Серверу Kaspersky LMC, компьютер попадает в группу администрирования по умолчанию (default). Вы можете посмотреть информацию о компьютерах в этой группе с помощью команды:

```
lmc device list -g 1
```

где `1` – идентификатор группы администрирования по умолчанию (default).

kaspersky

# Изменения в системе после установки программы

В результате установки программы Kaspersky LMC в вашей инфраструктуре происходят следующие изменения:

- На сервере RabbitMQ создается учетная запись для подключения Агентов Kaspersky LMC к Серверу Kaspersky LMC.
- На сервере RabbitMQ и в СУБД PostgreSQL создаются учетные записи для подключения Сервера Kaspersky LMC.
- В СУБД PostgreSQL создается база данных для программы Kaspersky LMC.
- На компьютере, где установлен Сервер Kaspersky LMC, устанавливается утилита Update Utility, обеспечивающая загрузку обновлений баз и модулей управляемых программ.
- На компьютере, где установлен Сервер Kaspersky LMC, создается директория для размещения загруженных обновлений баз управляемых программ. К директории предоставляется доступ для устройств с установленным Агентом Kaspersky LMC.
- В системном планировщике Cron задается расписание загрузки обновлений баз и модулей управляемых программ. По умолчанию загрузка запускается на пятнадцатой минуте каждого часа.

kaspersky

# Удаление программы

Удаление компонентов программы следует выполнять под учетной записью root.

► *Чтобы удалить Сервер Kaspersky LMC, выполните следующие действия на рабочем месте администратора Kaspersky LMC:*

1. Остановите Сервер Kaspersky LMC:

   ```
   systemctl stop lmc-server.service
   ```

2. Удалите Сервер Kaspersky LMC:

   ```
   dpkg --purge lmc-server-signed
   ```

   В результате выполнения команды также удаляются:

   - утилита Update Utility;
   - директория /var/opt/kaspersky/lmc-server;
   - очереди сообщений от Сервера Kaspersky LMC на сервере RabbitMQ;
   - конфигурационные файлы и файлы трассировки Сервера Kaspersky LMC;
   - директория /var/opt/kaspersky/lmc-uu/Bases/ и загруженные в нее обновления баз управляемых программ;
   - утилита проверки целостности программы на Сервере Kaspersky LMC и файл манифеста Сервера Kaspersky LMC (см. раздел "Проверка целостности компонентов программы" на стр. 91);
   - база данных, созданная в СУБД PostgreSQL для работы Kaspersky LMC;
   - учетные записи для подключения Сервера Kaspersky LMC и Агентов Kaspersky LMC к серверу RabbitMQ.

► *Чтобы удалить Агент Kaspersky LMC, выполните следующие действия на управляемом устройстве:*

1. Остановите Агент Kaspersky LMC:

   ```
   systemctl stop lmc-agent.service
   ```

2. Удалите Агент Kaspersky LMC:

   ```
   dpkg --purge lmc-agent-signed
   ```

   В результате выполнения команды также удаляются:

   - конфигурационные файлы и файлы трассировки Агента Kaspersky LMC;
   - директория /var/opt/kaspersky/lmc-agent;
   - очереди сообщений от Агента Kaspersky LMC на сервере RabbitMQ;
   - утилита проверки целостности программы на управляемом устройстве и файл манифеста Агента Kaspersky LMC.

3. Удалите коннектор управляемой программы:

```
rm -rf /etc/opt/kaspersky/lmc-connectors
rm -rf /opt/kaspersky/lmc-kesl-connector
```

# Запуск и остановка программы

По умолчанию компоненты программы Kaspersky LMC запускаются автоматически при запуске операционной системы на компьютере, где они установлены.

Вы можете запускать, останавливать и перезапускать компоненты Kaspersky LMC вручную.

Для Сервера Kaspersky LMC используйте следующие команды:

- `systemctl start lmc-server.service` – запустить Сервер Kaspersky LMC. После установки Сервер Kaspersky LMC запускается автоматически.
- `systemctl stop lmc-server.service` – остановить Сервер Kaspersky LMC.
- `systemctl restart lmc-server.service` – перезапустить Сервер Kaspersky LMC.

Для Агента Kaspersky LMC используйте следующие команды:

- `systemctl start lmc-agent.service` – запустить Агент Kaspersky LMC. После установки Агент Kaspersky LMC запускается автоматически.
- `systemctl stop lmc-agent.service` – остановить Агент Kaspersky LMC.
- `systemctl restart lmc-agent.service` – перезапустить Агент Kaspersky LMC.

kaspersky

# Лицензирование программы

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

## В этом разделе



## О Лицензионном соглашении

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

Рекомендуется внимательно ознакомиться с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки программы.
- Прочитав license.txt. Этот документ включен в комплект поставки программы.

После установки программы вы можете ознакомиться с текстом Лицензионного соглашения в следующих файлах:

- /opt/kaspersky/lmc-server/doc/eula.ru. Файл расположен на компьютере, где установлен Сервер администрирования Kaspersky LMC. Файл также содержит текст Политики конфиденциальности, которая описывает обработку и передачу данных.
- /opt/kaspersky/lmc-agent/doc/eula.ru. Файл расположен на компьютере, где установлен Агент администрирования Kaspersky LMC.

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 основании 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 указан в Лицензионном соглашении.

Программа Kaspersky LMC готова к использованию сразу после установки и первоначальной настройки, активация программы не требуется.

# О предоставлении данных

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в «Лабораторию Касперского» в автоматическом режиме следующую информацию:

- идентификатор сессии обновления баз программ "Лаборатории Касперского";
- тип и версию управляемой программы;
- тип и версию операционной системы, на которой установлен Сервер Kaspersky LMC.

Информация передается при загрузке обновлений баз программ "Лаборатории Касперского" с помощью Update Utility.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Более подробную информацию об обработке, хранении и уничтожении информации, полученной во время использования программы и переданной в «Лабораторию Касперского», вы можете получить, ознакомившись с Политикой конфиденциальности на веб-сайте «Лаборатории Касперского» (https://www.kaspersky.ru/products-and-services-privacy-policy).

kaspersky

# Управление устройствами и группами администрирования

*Управляемое устройство* – это компьютер или другое устройство, на котором установлен Агент Kaspersky LMC и программа "Лаборатории Касперского", обеспечивающая антивирусную защиту (управляемая программа).

Программа Kaspersky LMC позволяет объединять управляемые устройства в *группы администрирования* с целью централизованного управления параметрами защиты устройств, входящих в группу.

Для всех управляемых устройств в группе вы можете назначить единые параметры работы управляемых программ с помощью групповых политик (см. раздел "Управление защитой с помощью политик" на стр. 44) и групповых задач (см. раздел "Управление защитой с помощью задач" на стр. 62).

При добавлении устройства в группу администрирования к управляемой программе, установленной на этом устройстве, применяется политика, назначенная группе администрирования, и групповые задачи, созданные для группы администрирования.

Управляемое устройство может входить в состав только одной группы администрирования.

После установки программы создается одна группа администрирования по умолчанию. В нее автоматически помещаются устройства с установленным Агентом Kaspersky LMC. Вы можете создавать другие группы администрирования и перемещать в них управляемые устройства.

Вы можете автоматизировать размещение устройств в группах администрирования при помощи правил перемещения устройств (см. раздел "Использование правил перемещения устройств" на стр. 36).

Программа Kaspersky LMC присваивает управляемым устройствам *статусы*, которые могут указывать на проблемы в защите устройств и работе управляемых программ. Устройству может быть присвоен один из следующих статусов:

- *OK* – проблемы в состоянии защиты устройства не обнаружены.
- *Warning* – предупреждение, уровень защиты устройства снижен.
- *Critical* – критический, уровень защиты устройства значительно снижен.

Программа Kaspersky LMC изменяет статус устройства на *Warning* или *Critical* на основе критериев, которые заданы в параметрах группы администрирования (см. раздел "Настройка условий изменения статусов устройств" на стр. 41).

Статус устройства отображается в списке устройств и в информации об устройстве (см. раздел "Просмотр информации об управляемых устройствах" на стр. 31).

В параметрах группы администрирования вы также можете настраивать условие автоматического удаления неактивных устройств из состава управляемой инфраструктуры (см. раздел "Удаление устройств из состава управляемой инфраструктуры" на стр. 42).

Вы можете посмотреть список всех доступных команд для управления устройствами и группами администрирования с помощью следующих команд:

```
lmc device -h
```

```
lmc group -h
```

kaspersky

## В этом разделе



# Просмотр информации об управляемых устройствах

Вы можете просматривать список управляемых устройств и подробную информацию о каждом устройстве.

**Просмотр списка управляемых устройств**

При просмотре списка управляемых устройств вам доступны следующие возможности:

- просмотр списка всех устройств, которые находятся под управлением Kaspersky LMC;
- просмотр списка устройств в составе указанной группы администрирования.

► *Чтобы посмотреть список управляемых устройств, выполните команду:*

```
lmc device list [-g <идентификатор группы>]
```

где: `[-g <идентификатор группы>]` – отображать только устройства в составе указанной группы администрирования.

Информация в списке управляемых устройств автоматически отсортирована по идентификатору устройства.

Список управляемых устройств содержит следующие сведения о каждом устройстве:

- **DeviceID** – идентификатор устройства в базе Kaspersky LMC.
- **GroupID** – идентификатор группы администрирования, в которую входит устройство.
- **GroupName** – название группы администрирования, в которую входит устройство.
- **HostName** – доменное имя устройства.
- **IPAddress** – IP-адрес устройства.
- **DeviceStatus** – статус устройства. Возможные значения: `OK`, `Critical`, `Warning`.
- **SinceLastConnectionToServer** – время с момента последнего соединения Агента Kaspersky LMC, установленного на устройстве, с Сервером Kaspersky LMC.

- **MachineID** – уникальный идентификатор (UID) устройства.

**Просмотр подробной информации об отдельном управляемом устройстве**

► *Чтобы посмотреть информацию об управляемом устройстве, выполните команду:*

```
lmc device details -d <идентификатор устройства>
```

Команда выводит следующую информацию об указанном управляемом устройстве:

- **InGroup** – идентификатор группы администрирования, в которую входит устройство.
- **MachineID** – уникальный идентификатор (UID) устройства.
- **HostName** – доменное имя устройства.
- **Description** – описание устройства.
- **OS** – название и версия операционной системы, версия ядра на устройстве.
- **IPAddress** – IP-адрес устройства.
- **Online** – информация о нахождении устройства в сети или дата и время последнего нахождения в сети.
- **Synched** – информация о том, что данные на устройстве синхронизированы с Сервером Kaspersky LMC, или дата и время последней синхронизации.
- **SinceLastConnectionToServer** – время с момента последнего соединения Агента Kaspersky LMC с Сервером Kaspersky LMC.
- **NetworkAgentVersion** – версия Агента Kaspersky LMC на устройстве.
- **DeviceStatus** – статус устройства. Возможные значения: `Unknown`, `OK`, `Critical`, `Warning`.
- **DeviceStatusReason** – причина присвоения статуса устройства (только для статусов `Critical` и `Warning`).
- **Product** – информация об управляемой программе:
  - **Name** – название программы.
  - **Version** – версия программы.
  - **State** – состояние программы (запущена или остановлена).
  - **RestartRequired** – информация о том, требуется ли перезапуск управляемой программы на устройстве.
  - **RebootRequired** – информация о том, требуется ли перезагрузка операционной системы на устройстве.
- **Bases** – информация о базах программы на устройстве:
  - **State** – состояние баз. Возможные значения:
    - `UpToDate` – актуальные;
    - `NotLoaded` – не загружены;
    - `Outdated` – устарели;
    - `TotallyOutdated` – сильно устарели.

- **UpdateTime** – дата и время последнего успешного обновления баз. Если обновление не выполнялось, отображается `None`.
- **ReleaseTime** – дата и время выпуска баз.

- **License** – информация о лицензии, по которой используется управляемая программа на устройстве, и лицензионных ключах, добавленных в программу:
  - **Status** – статус активного лицензионного ключа.

    Если активный ключ не добавлен, то в поле **Status** отображается `NoLicense`. При этом остальные поля, касающиеся информации о лицензии и ключах, не отображаются.
  - **ActiveType** – тип лицензии, связанной с активным ключом (коммерческая или пробная).
  - **ActiveKey** – активный ключ.
  - **ActiveExpiresAt** – дата окончания срока использования программы с активным ключом.
  - **ActiveInstalledAt** – дата добавления активного ключа.
  - **ReserveType** – тип лицензии, связанной с резервным ключом.
  - **ReserveKey** – резервный ключ.
  - **ReserveExpiresAt** – дата окончания срока использования программы с резервным ключом.
  - **ReserveInstalledAt** – дата добавления резервного ключа.

    > Если резервный ключ не добавлен, то информация по нему не отображается.

  - **SubscriptionStatus** – состояние подписки, если программа используется по подписке.

# Просмотр информации о группах администрирования

Вы можете просматривать список групп администрирования и информацию о каждой группе.

**Просмотр списка групп администрирования**

► *Чтобы посмотреть список всех групп администрирования, выполните команду:*

```
lmc group list
```

Список групп содержит следующие сведения о каждой группе:

- **ID** – идентификатор группы администрирования.
- **Name** – название группы администрирования.
- **Devices** – количество устройств в группе.
- **Tasks** – количество задач, созданных для группы.
- **PolicyId** – идентификатор политики, назначенной группе администрирования.
- **Policy** – название политики, назначенной группе администрирования.
- **Rules** – количество правил перемещения устройств, в соответствии с которыми устройства перемещаются в эту группу.

**Просмотр подробной информации об отдельной группе администрирования**

► *Чтобы посмотреть информацию о группе администрирования, выполните команду:*

```
lmc group details -g <идентификатор группы администрирования>
```

Команда выводит следующие сведения об указанной группе администрирования:

- **Devices** – количество устройств в группе.
- **Group policy** – если группе администрирования назначена политика, название и идентификатор политики.
- **Global policy** – если для группы применяется глобальная политика, идентификатор и название глобальной политики.
- **PolicyEditedAt** – дата и время последнего изменения политики.
- **DevicesWithPolicyApplied** – количество устройств, на которые распространяется действие политики.
- **CreatedAt** – дата и время создания группы.
- **ModifiedAt** – дата и время последнего изменения параметров группы.
- **CleanupSettings** – группа параметров, определяющих условия автоматического удаления неактивных устройств из группы. Параметр **DeleteInactiveDeviceAfterDays** определяет количество дней, по истечении которых устройство, не подключавшееся к Серверу Kaspersky LMC, будет считаться неактивным и удаляться из состава управляемой инфраструктуры (см. раздел "Удаление устройств из состава управляемой инфраструктуры" на стр. 42).
- **DeviceStatusSettings** – группа параметров, которые определяют условия присвоения статусов *OK*, *Warning* и *Critical* устройствам, входящим в группу (см. раздел "Настройка условий изменения статусов устройств" на стр. 41).

# Создание группы администрирования

► *Чтобы создать группу администрирования, выполните команду:*

```
lmc group create -n <название группы>
```

Группа создается с параметрами по умолчанию, которые вы можете изменить позже (см. раздел "Настройка параметров группы администрирования" на стр. 34).

# Настройка параметров группы администрирования

► *Чтобы настроить параметры группы администрирования, выполните следующие действия:*

1. Выполните команду:

   ```
   lmc group edit -g <идентификатор группы администрирования>
   ```

   Запускается текстовый редактор.

2. Внесите необходимые изменения. Вы можете изменять следующие параметры группы администрирования:
   - **CleanupSettings** – группа параметров, определяющих условия автоматического удаления неактивных устройств из группы. Параметр **DeleteInactiveDeviceAfterDays** определяет количество дней, по истечении которых устройство, не подключавшееся к Серверу Kaspersky LMC, будет считаться неактивным и удаляться из состава управляемой инфраструктуры (см. раздел "Удаление устройств из состава управляемой инфраструктуры" на стр. 42).
   - **DeviceStatusSettings** – группа параметров, которые определяют условия присвоения статусов *OK*, *Warning* и *Critical* устройствам, входящим в группу (см. раздел "Настройка условий изменения статусов устройств" на стр. 41).
3. Сохраните изменения и закройте редактор.

# Экспорт и импорт параметров группы администрирования

С помощью процедур экспорта и импорта параметров группы администрирования вы можете выполнять следующие действия:

- сохранять настроенные параметры указанной группы администрирования в файл;
- применять на указанную группу администрирования параметры из файла.

► *Чтобы экспортировать параметры группы администрирования, выполните команду:*

```
lmc group export -g <идентификатор группы> -f <путь к файлу>
```

где:

- `-g <идентификатор группы>` – идентификатор группы администрирования, параметры которой нужно экспортировать.
- `-f <путь к файлу>` – путь к файлу, в котором нужно сохранить параметры.

► *Чтобы импортировать параметры группы администрирования, выполните команду:*

```
lmc group import -g <идентификатор группы> -f <путь к файлу>
```

где:

- `-g <идентификатор группы>` – идентификатор группы администрирования, на которую нужно применить ранее экспортированные параметры другой группы.
- `-f <путь к файлу>` – путь к файлу, из которого нужно импортировать параметры.

# Удаление группы администрирования

► *Чтобы удалить группу администрирования, выполните команду:*

```
lmc group delete -g <идентификатор группы> [--force]
```

где:

`[--force]` – удалить группу принудительно. Используйте этот параметр, если вы хотите удалить группу администрирования, для которой выполняется хотя бы одно из следующих условий:

- в группе есть управляемые устройства;
- для группы созданы правила перемещения устройств, в соответствии с которыми устройства перемещаются в эту группу;
- для группы созданы задачи.

Если для группы выполняется хотя бы одно из указанных условий и вы не указали параметр `[--force]` при удалении группы, команда удаления возвращает ошибку.

В результате удаления группы с параметром `[--force]` выполняются следующие действия:

- управляемые устройства из группы перемещаются в группу администрирования по умолчанию.
- удаляются правила перемещения устройств, в соответствии с которыми устройства перемещаются в группу;
- удаляются задачи, которые были созданы для группы.

# Использование правил перемещения устройств

Вы можете автоматизировать размещение устройств в группах администрирования при помощи правил перемещения устройств. Правило перемещения определяет условия, при обнаружении которых Kaspersky LMC перемещает устройство в целевую группу администрирования. В качестве условий могут использоваться различные атрибуты устройства, например, IP-адрес или версия управляемой программы на устройстве. Kaspersky LMC перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила могут применяться автоматически или вручную в зависимости от настроенных параметров правила. Если правило имеет признак "активное", то оно применяется автоматически и действует только для устройств, которые впервые подключаются к Серверу Kaspersky LMC. Если признак "активное" для правила не установлен, такое правило применяется только вручную и действует на все устройства, атрибуты которых удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Kaspersky LMC проверяет атрибуты устройства на соответствие условию выполнения каждого правила в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет.

Вы можете посмотреть список доступных команд для управления правилами перемещения устройств, выполнив команду: `lmc rule -h`.

kaspersky

## В этом разделе



# Просмотр списка правил перемещения устройств

► *Чтобы открыть для просмотра список правил автоматического перемещения устройств, выполните команду:*

```
lmc rule list
```

Список правил содержит следующие сведения о каждом правиле:

- **ID** – идентификатор правила.
- **Name** – название правила.
- **Group** – группа администрирования, в которую перемещаются устройства при применении этого правила.
- **Priority** – приоритет применения правила.
- **Autorun** – признак, определяющий, применяется ли правило автоматически. Возможные значения:
  - `True` – правило применяется к устройству автоматически при первом получении информации от Агента Kaspersky LMC на устройстве;
  - `False` – правило может быть применено только вручную.

# Создание правила перемещения устройств

► *Чтобы создать правило перемещения устройств, выполните следующие действия:*

1. Выполните команду:

   ```
   lmc rule create -n <название правила> [--no-edit]
   ```

   где:

   - `-n <название правила>` – уникальное название правила перемещения устройств.
   - `[--no-edit]` – после создания правила не запускать редактор для настройки параметров.

   Если вы выполнили команду с параметром `[--no-edit]`, создается правило перемещения устройств с параметрами по умолчанию.

2. Если вы не указали параметр `[--no-edit]`, в результате выполнения команды запускается текстовый редактор. Проверьте установленные по умолчанию параметры правила, внесите необходимые изменения.

   Вы можете настраивать следующие параметры и условия применения правила перемещения устройств:

   - **Priority** – число обозначающее приоритет применения правила.
   - **Autorun** – признак, определяющий, применяется ли правило автоматически. Возможные значения:
     - `True` – правило применяется автоматически при первом получении информации от Агента Kaspersky LMC на этом устройстве;
     - `False` – правило может быть применено только вручную.

     Значение по умолчанию: `True`.
   - **Description** – описание правила.
   - **Condition** – условия применения правила.

     Возможные условия:

     - `$address_ipv4` – адрес устройства в формате ipv4;
     - `$domain_name` – доменное имя устройства;
     - `$application_name` – имя управляемой программы, установленной на устройстве;
     - `$major_data_version` – версия управляемой программы;
     - `$description` – описание устройства, указанное на стороне Агента.

     Задавая условия, вы можете использовать следующие операторы сравнения: match, eq, contains, regex. Значения указываются в фигурных скобках, например:

     ```
     Condition: {
      $address_ipv4: {
        match: '10.10.*.*'
      }
     },
     ```

   - **Action: GroupName** – название группы администрирования, в которую перемещаются устройства при применении правила.

     Если группа с указанным в правиле названием отсутствует, она будет создана автоматически.
3. Сохраните изменения и закройте редактор.

## Изменение правила перемещения устройств

► *Чтобы изменить правило перемещения устройств, выполните следующие действия:*

1. Выполните команду:

```
lmc rule edit -r <идентификатор правила>
```

Запускается текстовый редактор.

2. Измените параметры правила перемещения устройств (см. раздел "Просмотр списка правил перемещения устройств" на стр. 37).
3. Сохраните изменения и закройте редактор.

## Проверка правила перемещения устройств

Вы можете проверить, как будет действовать правило, перед его применением.

► *Чтобы проверить действие правила перемещения устройств, выполните команду:*

```
lmc rule check -r <идентификатор правила> [-g <идентификатор группы>]
```

где `[-g <идентификатор группы>]` – проверить действие правила для устройств указанной группы администрирования. Если этот параметр не указан, действие правила проверяется для всех управляемых устройств.

В результате выполнения команды отображаются следующие сведения:

- **DeviceId** – идентификатор управляемого устройства, которое будет перемещено в результате применения правила.
- **DeviceName** – доменное имя управляемого устройства, которое будет перемещено в результате применения правила.
- **OldGroupID** – идентификатор группы администрирования, в которую входит перемещаемое устройство до применения правила.
- **OldGroupName** – название группы администрирования, в которую входит перемещаемое устройство до применения правила.
- **NewGroupID** – идентификатор группы администрирования, в которую будет перемещено устройство после применения правила.
- **NewGroupName** – название группы администрирования, в которую будет перемещено устройство после применения правила.

## Применение вручную правила перемещения устройств

► *Чтобы применить вручную правило перемещения устройств, выполните команду:*

```
lmc rule exec -r <идентификатор правила> [-g <идентификатор группы>]
```

где `[-g <идентификатор группы>]` – применить правило только для устройств указанной группы администрирования.

В результате выполнения команды все устройства, соответствующие условиям применения правила, перемещаются в группу администрирования, которая задана в параметрах правила.

## Экспорт и импорт параметров правила перемещения устройств

С помощью процедур экспорта и импорта параметров правила перемещения устройств вы можете выполнять следующие действия:

- сохранять настроенные параметры указанного правила перемещения устройств в файл;
- копировать ранее настроенные параметры и условия какого-либо правила в указанное правило.

► *Чтобы экспортировать параметры правила перемещения устройств, выполните команду:*

```
lmc rule export -r <идентификатор правила> -f <путь к файлу>
```

где:

- `-r <идентификатор правила>` – идентификатор правила перемещения устройств, параметры которого нужно экспортировать.
- `-f <путь к файлу>` – путь к файлу, в котором нужно сохранить параметры.

► *Чтобы импортировать параметры правила перемещения устройств, выполните команду:*

```
lmc rule import -r <идентификатор правила> -f <путь к файлу>
```

где:

- `-r <идентификатор правила>` – идентификатор правила перемещения устройств, на которое нужно применить ранее экспортированные параметры другого правила.
- `-f <путь к файлу>` – путь к файлу, из которого нужно импортировать параметры.

## Удаление правила перемещения устройств

► *Чтобы удалить правило перемещения устройств, выполните команду:*

```
lmc rule delete -r <идентификатор правила>
```

# Перемещение устройства вручную

► *Чтобы переместить устройство из одной группы администрирования в другую, выполните команду:*

```
lmc device move -d <идентификатор устройства> -g <идентификатор группы>
```

где:

- `-d <идентификатор устройства>` – устройство, которое нужно переместить.
- `-g <идентификатор группы>` – группа администрирования, в которую перемещается устройство.

kaspersky

# Настройка условий изменения статусов устройств

В параметрах группы администрирования вы можете настраивать условия изменения статусов устройств, которые входят в состав этой группы. В соответствии с этими условиями программа Kaspersky LMC присваивает управляемым устройствам статусы, которые могут указывать на проблемы в защите устройств и работе управляемых программ.

► *Чтобы настроить условия изменения статусов устройств, выполните следующие действия:*

1. Откройте для изменения параметры группы администрирования:

   `lmc group edit -g <идентификатор группы администрирования>`

   Запускается текстовый редактор.
2. В секции **DeviceStatusSettings** измените значения следующих параметров:
   - **AffectedByApplication** – статус устройства определяется управляемой программой.

     Возможные значения: `true`, `false`. Значение по умолчанию: `false` (сервер Kaspersky LMC не учитывает полученный от продукта HSDP статус при определении общего статуса устройства).
   - **ApplicationNotStarted** – статус устройства, на котором не запущена программа, обеспечивающая антивирусную защиту.

     Возможные значения: `Ok`, `Warning`, `Critical`. Значение по умолчанию: `Critical`.
   - **ApplicationRestartRequired** – статус устройства, на котором требуется перезапуск управляемой программы.

     Возможные значения: `Ok`, `Warning`, `Critical`. Значение по умолчанию: `Warning`.
   - **BasesNotLoaded** – статус устройства, на котором не удалось загрузить базы.

     Возможные значения: `Ok`, `Warning`, `Critical`. Значение по умолчанию: `Critical`.
   - **BasesOutdated** – статус устройства, на котором базы устарели (срок, после которого базы считаются устаревшими, определяет управляемая программа).

     Возможные значения: `Ok`, `Warning`, `Critical`. Значение по умолчанию: `Warning`.
   - **BasesTotallyOutdated** – статус устройства, на котором *базы* сильно устарели (срок, после которого базы считаются сильно устаревшими, определяет управляемая программа).

     Возможные значения: `Ok`, `Warning`, `Critical`. Значение по умолчанию: `Critical`.
   - **DeviceInactiveCriticalAfterDays** – количество дней, по истечении которых устройству будет присвоен статус *Critical*, если устройство за это время не подключалось к Серверу Kaspersky LMC.

     Возможные значения:`0 – 9999` (где `0` – не учитывать это условие). Значение по умолчанию: `60`.
   - **DeviceInactiveWarningAfterDays** – количество дней, по истечении которых устройству будет присвоен статус *Warning*, если устройство за это время не подключалось к Серверу Kaspersky LMC.

     Возможные значения: `0 – 9999` (где `0` – не учитывать это условие). Значение по умолчанию: `50`.
   - **DeviceRebootRequired** – статус устройства, на котором требуется перезагрузка ОС.

     Возможные значения: `Ok`, `Warning`, `Critical`. Значение по умолчанию: `Warning`.

- **FullScanOutdatedCriticalAfterDays** – количество дней, по истечении которых устройству будет присвоен статус *Critical*, если на устройстве за это время не запускалась задача полной проверки.

  Возможные значения: `0 – 9999` (где `0` – не учитывать это условие). Значение по умолчанию: `14`.

- **FullScanOutdatedWarningAfterDays** – количество дней, по истечении которых устройству будет присвоен статус *Warning*, если на устройстве за это время не запускалась задача полной проверки.

  Возможные значения: `0 – 9999` (где `0` – не учитывать это условие). Значение по умолчанию: `7`.

- **LicenseExpirationWarningBeforeDays** – присвоить устройству статус *Warning*, если на устройстве срок действия лицензии скоро истечет (количество оставшихся дней до окончания срока действия лицензии меньше или равно указанному значению).

  Возможные значения: `0 – 9999` (где `0` – не учитывать это условие). Значение по умолчанию: `7`.

- **LicenseExpired** – статус устройства, на котором истек срок действия лицензии (дата окончания срока действия лицензии меньше текущей даты).

  Возможные значения: `Ok`, `Warning`, `Critical`. Значение по умолчанию: `Critical`.

- **NoInstalledApplications** – статус устройства, на котором отсутствует программа, обеспечивающая антивирусную защиту.

  Возможные значения: `Ok`, `Warning`, `Critical`. Значение по умолчанию: `Critical`.

- **ProtectionDisabled** – статус устройства, на котором не включена постоянная защита.

  Возможные значения: `Ok`, `Warning`, `Critical`. Значение по умолчанию: `Critical`.

3. Сохраните изменения и закройте редактор.

# Удаление устройств из состава управляемой инфраструктуры

Устройство может быть удалено из состава управляемой инфраструктуры следующими способами:

- Вы можете удалить устройство вручную с помощью команды Kaspersky LMC.

  После удаления управляемого устройства этим способом все события, связанные с этим устройством, сохраняются на Сервере Kaspersky LMC.

- Kaspersky LMC автоматически удаляет неактивные устройств из состава управляемой инфраструктуры. Неактивными считаются устройства с установленным Агентом Kaspersky LMC, которые не подключались к Серверу Kaspersky LMC в течение установленного срока. По умолчанию устройство признается неактивным по истечении 70 дней с момента последнего подключения.

  Вы можете настроить срок, по истечении которого устройство автоматически удаляется из состава управляемой инфраструктуры, в параметрах группы администрирования.

  После автоматического удаления устройства на Сервере Kaspersky LMC формируется событие *InactiveHostsRemoved*.

  В результате автоматического удаления устройства вся информация об устройстве, включая события, относящиеся к устройству, также удаляется с Сервера Kaspersky LMC.

► *Чтобы удалить устройство из состава управляемой инфраструктуры вручную, выполните команду:*

```
lmc device delete -d <идентификатор устройства>
```

► *Чтобы настроить автоматическое удаление неактивных устройств, выполните следующие действия:*

1. Откройте для изменения параметры группы администрирования:

   ```
   lmc group edit -g <идентификатор группы администрирования>
   ```

   Запускается текстовый редактор.

2. Измените значение параметра **DeleteInactiveDeviceAfterDays**: укажите количество дней, по истечении которых устройство, не подключавшееся к Серверу Kaspersky LMC, будет считаться неактивным и удаляться из состава управляемой инфраструктуры. Возможные значения: `0` – `9999`.

   Если вы хотите выключить автоматическое удаление устройств в этой группе администрирования, укажите значение `0`. Kaspersky LMC не будет проверять количество дней, прошедшее с момента последнего соединения устройства с Сервером Kaspersky LMC.

3. Сохраните изменения и закройте редактор.

kaspersky

# Управление защитой с помощью политик

Политика – это набор параметров работы управляемой программы. С помощью политики вы можете централизовано управлять работой программы, установленной на нескольких управляемых устройствах.

Вы можете создавать политики и назначать их группам администрирования. Политика, назначенная группе администрирования, определяет работу управляемой программы на всех устройствах, которые входят в эту группу.

Группе администрирования может быть назначена только одна политика.

Одна из политик, настроенных для управляемой программы, применяется как глобальная. Глобальная политика автоматически назначается всем новым группам администрирования, а также группам администрирования, политика которых была удалена.

Для управляемой программы автоматически создается политика по умолчанию, которая применяется как глобальная. Вы можете сделать глобальной любую другую политику, настроенную для управляемой программы.

Политику, которая применяется как глобальная, нельзя удалить, но вы можете изменять ее параметры.

Вы можете посмотреть список доступных команд для управления политиками, выполнив команду: `lmc policy -h`.

## В этом разделе



# Просмотр информации о политиках

Вы можете просматривать список всех политик и подробную информацию о каждой политике.

**Просмотр списка политик**

► *Чтобы посмотреть список политик, выполните команду:*

```
lmc policy list
```

Список политик содержит следующие сведения о каждой политике:

- **ID** – идентификатор политики.
- **Name** – название политики.
- **AssignedGroups** – количество групп, которым назначена политика.
- **Global** – признак, определяющий, как применяется политика. Возможные значения:
  - `True` – политика применяется как глобальная;
  - `False` – политика назначена одной или нескольким группам администрирования.

**Просмотр подробной информации о политике**

► *Чтобы посмотреть информацию о политике, выполните команду:*

```
lmc policy details -p <идентификатор политики>
```

Команда выводит следующие сведения о политике:

- Общие параметры политики для всех управляемых программ:
  - **ID** – идентификатор политики.
  - **Name** – название политики.
  - **IsGlobal** – признак, определяющий, как применяется политика. Возможные значения:
    - `True` – политика применяется как глобальная;
    - `False` – политика назначена одной или нескольким группам администрирования.
  - **AssignedTo** – идентификаторы и названия групп администрирования, которым назначена политика.
- Параметры, специфичные для управляемой программы. В зависимости от управляемой программы, для которой создана политика, могут отображаться разные параметры.

# Создание политики

► *Чтобы создать политику, выполните следующие действия:*

1. Выполните команду:

   ```
   lmc policy create -n <название политики> [--no-edit]
   ```

   где:

   - `-n <название политики>` – уникальное название политики.
   - `[--no-edit]` – после создания политики не запускать редактор для настройки параметров. Используйте этот параметр, если вы хотите создать политику с параметрами по умолчанию.

   Если вы выполнили команду с параметром `[--no-edit]`, создается политика с параметрами по умолчанию.

2. Если вы не указали параметр `[--no-edit]`, в результате выполнения команды запускается текстовый редактор. Проверьте установленные по умолчанию параметры политики и внесите

необходимые изменения.

Набор параметров, доступных для настройки, зависит от управляемой программы, для которой создана политика (см. раздел "Параметры политики для Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Linux" на стр. 47).

> Чтобы значение параметра политики применялось к управляемой программе, для параметра должен быть установлен значок `(+)`. Если для параметра установлен значок `(-)`, значение этого параметра определяется не политикой, а локальными параметрами программы на устройстве.

3. Сохраните изменения и закройте редактор.
4. Если вы включили использование KSN в параметрах политики, на экране отображается запрос об участии в KSN. Вы можете прочитать текст Положения о Kaspersky Security Network в файле /opt/kaspersky/lmc-server/scripts/plugins/kesl_10/ksn_agreement.txt.

   Если вы согласны со всеми условиями Положения о Kaspersky Security Network, введите `yes` (или `y`). Использование KSN в работе управляемой программы будет включено, параметры политики будут сохранены.

   Если вы не согласны с условиями Положения о Kaspersky Security Network, введите `no` (или `n`). Использование KSN в работе управляемой программы будет выключено, параметры политики будут сохранены.

# Изменение параметров политики

► *Чтобы изменить параметры политики, выполните следующие действия:*

1. Выполните команду:

   ```
   lmc policy edit -p <идентификатор политики>
   ```

   Запускается текстовый редактор.
2. Измените параметры политики.

   Набор параметров, доступных для настройки, зависит от управляемой программы, для которой создана политика (см. раздел "Параметры политики для Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Linux" на стр. 47).

   > Чтобы значение параметра политики применялось к управляемой программе, для параметра должен быть установлен значок `(+)`. Если для параметра установлен значок `(-)`, значение этого параметра определяется не политикой, а локальными параметрами программы на устройстве.

3. Сохраните изменения и закройте редактор.
4. Если вы включили использование KSN в параметрах политики, на экране отображается запрос об участии в KSN.

   Вы можете прочитать текст Положения о Kaspersky Security Network в файле /opt/kaspersky/lmc-server/scripts/plugins/kesl_10/ksn_agreement.txt.

   Если вы согласны со всеми условиями Положения о Kaspersky Security Network, введите `yes` (или `y`).

Использование KSN в работе управляемой программы будет включено, параметры политики будут сохранены.

Если вы не согласны с условиями Положения о Kaspersky Security Network, введите `no` (или `n`). Использование KSN в работе управляемой программы будет выключено, параметры политики будут сохранены.

# Параметры политики для Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Linux

**InformAboutTif**

Включение / выключение отправки на Сервер Kaspersky LMC информации о необработанных файлах.

Возможные значения:

- `true` – отправлять информацию о необработанных файлах.
- `false` – не отправлять информацию о необработанных файлах.

Значение по умолчанию: `true`.

**InformAboutBackup**

Включение / выключение отправки на Сервер Kaspersky LMC информации о файлах, помещенных в резервное хранилище.

Возможные значения:

- `true` – отправлять информацию о файлах, помещенных в резервное хранилище.
- `false` – не отправлять информацию о файлах, помещенных в резервное хранилище.

Значение по умолчанию: `true`.

**DetectOtherObjects**

Включение / выключение обнаружения легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Возможные значения:

- `true` – обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда, включено.
- `false` – обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда, выключено.

Значение по умолчанию: `false`.

**AllowUserManageLocalTasks**

Возможность управления локальными задачами из интерфейса управляемой программы.

Возможные значения:

- `true` – пользователь может выполнять все доступные действия с локальными задачами из интерфейса управляемой программы.

- `false` – пользователь не может управлять локальными задачами из интерфейса управляемой программы.

Значение по умолчанию: `true`.

**AllowUserManageGroupTasks**

Возможность запуска и остановки групповых задач из интерфейса управляемой программы.

Возможные значения:

- `true` – пользователь может запускать и останавливать групповые задачи из интерфейса управляемой программы.
- `false` – пользователь не может запускать и останавливать групповые задачи из интерфейса управляемой программы.

Значение по умолчанию: `true`.

**OasEnabled**

Включение / выключение защиты от файловых угроз.

Возможные значения:

- `true` – защита от файловых угроз включена.
- `false` – защита от файловых угроз выключена.

Значение по умолчанию: `true`.

**Раздел OASSettings**

Раздел содержит параметры защиты от файловых угроз.

**ScanArchived**

Включение / выключение проверки архивов. Программа обнаруживает угрозы в архивах, но не лечит их. Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj, SFX.

Возможные значения:

- `true` – проверять архивы.
- `false` – не проверять архивы.

Значение по умолчанию: `false`.

**ScanSfxArchived**

Проверять самораспаковывающиеся архивы SFX (архивы, имеющие в своем составе исполняемый модуль-распаковщик, self-extracting archives). Программа может проверять самораспаковывающиеся архивы, только если параметр **ScanArchived** имеет значение `true`.

Возможные значения:

- `true` – проверять самораспаковывающиеся архивы.
- `false` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `false`.

**ScanMailBases**

Включение / выключение проверки почтовых баз приложений Microsoft® Outlook®, Outlook Express, The Bat! и других.

Возможные значения:

- `true` – проверять файлы почтовых баз.
- `false` – не проверять файлы почтовых баз.

Значение по умолчанию: `false`.

**ScanPlainMail**

Включение / выключение проверки сообщений электронной почты в текстовом формате (plain text).

Возможные значения:

- `true` – проверять сообщения электронной почты в текстовом формате.
- `false` – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: `false`.

**TimeLimit**

Максимальная продолжительность проверки объекта (в секундах). Программа прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.

Возможные значения: `0 – 9999`. Если указано значение `0` – продолжительность проверки объектов не ограничена.

Значение по умолчанию: `60`.

**SizeLimit**

Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, программа пропускает объект.

Возможные значения: `0 – 999999`. Если указано значение `0` – программа проверяет объекты любого размера.

Значение по умолчанию: `0`.

**FirstAction, SecondAction**

Первое и второе действия, которые выполняет программа над зараженными объектами. Программа выполняет второе действие, если не удалось выполнить первое действие. Если в качестве первого действия выбрано `Block (блокировать)` или `Remove (удалять)`, то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия.

Перед тем как выполнить над объектом выбранное вами действие, программа блокирует доступ к этому объекту для программ, которые к нему обращаются.

Возможные значения:

- `Cure (лечить)` – программа пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа оставляет объект неизменным.
- `Remove (удалять)` – программа удаляет зараженный объект, предварительно создав его резервную копию.

- `Recommended (выполнять рекомендуемое действие)` – программа автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, программа сразу удаляет троянские программы, так как они не заражают другие файлы и поэтому не предполагают лечения.
- `Block (блокировать)` – программа блокирует доступ к зараженному объекту. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию для **FirstAction**: `Recommended`.

Значение по умолчанию для **SecondAction**: `Block`.

#### UseExcludeMasks

Исключение из проверки объектов, указанных параметром **ExcludeMasks**.

Возможные значения:

- `true` – исключать объекты, указанные параметром **ExcludeMasks**.
- `false` – не исключать объекты, указанные параметром **ExcludeMasks**.

Значение по умолчанию: `false`.

#### ExcludeMasks

Имена или маски объектов, которые нужно исключать из проверки. Вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки. Подробнее см. в документации управляемой программы.

Значение по умолчанию не задано.

#### UseExcludeThreats

Исключение из проверки объектов с угрозами, указанными в параметре **ExcludeThreats**.

Возможные значения:

- `true` – исключать из проверки объекты, которые содержат угрозы, указанные в параметре **ExcludeThreats**.
- `false` – не исключать из проверки объекты, которые содержат угрозы, указанные в параметре **ExcludeThreats**.

Значение по умолчанию: `false`.

#### ExcludeThreats

Название угрозы, обнаруженной в объекте, который нужно исключать из проверки. Чтобы исключить из проверки объект, укажите полное название угрозы, обнаруженной в этом объекте (строку-заключение программы о том, что объект является зараженным). Например, вы используете одну из утилит для получения информации о сети. Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале управляемой программы. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии. Значение параметра чувствительно к регистру. Подробнее см. в документации управляемой программы.

Значение по умолчанию не задано.

**ReportCleanObjects, ReportPackedObjects**

Включение / выключение записи в журнал информации о проверенных объектах:

- **ReportCleanObjects** – о проверенных объектах, которые управляемая программа признала незараженными.
- **ReportPackedObjects** – о проверенных объектах, которые являются частью составных объектов.

Включение записи позволяет убедиться, что какой-либо объект был проверен программой.

Возможные значения:

- `true` – записывать в журнал информацию об объектах.
- `false` – не записывать в журнал информацию об объектах.

Значение по умолчанию: `false`.

**ReportUnprocessedObjects**

Включение / выключение записи в журнал информации о непроверенных объектах.

Возможные значения:

- `true` – записывать в журнал информацию о непроверенных объектах.
- `false` – не записывать в журнал информацию о непроверенных объектах.

Значение по умолчанию: `false`.

**UseAnalyzer**

Включение / выключение эвристического анализатора. Эвристический анализ позволяет программе распознавать новые угрозы еще до того, как они станут известны вирусным аналитикам.

Возможные значения:

- `true` – использовать эвристический анализатор.
- `false` – не использовать эвристический анализатор.

Значение по умолчанию: `true`.

**HeuristicLevel**

Уровень эвристического анализа.

Возможные значения:

- `Light` – наименее тщательная проверка, минимальная загрузка процессора.
- `Medium` – средний уровень эвристического анализа, сбалансированная загрузка процессора.
- `Deep` – наиболее тщательная проверка, максимальная загрузка процессора.
- `Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`.

**UseIChecker**

Включение / выключение технологии iChecker. Технология iChecker позволяет увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму,

учитывающему дату выпуска баз программы, дату предыдущей проверки файла, а также изменение параметров проверки.

Возможные значения:

- `true` – использовать технологию iChecker.
- `false` – не использовать технологию iChecker.

Значение по умолчанию: `true`.

**Раздел ScanScope**

Группа параметров, определяющих область проверки. Вы можете задавать несколько областей проверки путем добавления новой группы параметров.

- **AreaDesc**

  Произвольное описание области проверки. Максимальная длина строки: 4096 символов.

  Значение по умолчанию: `All objects`.

- **UseScanArea**

  Включение / выключение проверки указанной области. Необходимо включить проверку хотя бы одной области.

  Возможные значения:

  - `true` – проверять указанную область.
  - `false` – не проверять указанную область.

  Значение по умолчанию: `true`.

- **Path**

  Путь к объектам, которые нужно проверять.

  Возможные значения:

  - `<путь к локальной директории>` – проверять объекты в указанной директории.
  - `Shared:NFS` – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS.
  - `Shared:SMB` – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу SMB.
  - `AllRemoteMounted` – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS.
  - `AllShared` – проверять все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

  Значение по умолчанию не указано.

- **AreaMask**

  Маски файлов в формате командной оболочки, которые нужно проверять. Если значение параметра не указано, программа проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра. Подробнее см. в документации управляемой программы.

  Значение по умолчанию: `*` (проверять все объекты).

### Раздел ExcludedFromScanScope

Группа параметров, определяющих область, исключаемую из проверки. Вы можете задавать несколько областей путем добавления новой группы параметров. Для задания области, исключаемой из проверки, используются такие же параметры, как в разделе **ScanScope**.

По умолчанию области, исключаемые из проверки, не заданы.

### ScanByAccessType

Проверять файлы в зависимости от действия, выполняемого с файлом.

Возможные значения:

- `SmartCheck` – проверять файл при попытке открытия, и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом.
- `OpenAndModify` – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.
- `Open` – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.

Значение по умолчанию: `SmartCheck`.

### OafimEnabled

Включение / выключение мониторинга файловых операций в режиме реального времени.

Возможные значения:

- `true` – мониторинг файловых операций включен.
- `false` – мониторинг файловых операций выключен.

Значение по умолчанию: `true`.

### Раздел OAFIMSettings

Раздел содержит параметры мониторинга файловых операций.

### UseExcludeMasks

Исключение из области мониторинга объектов, указанных параметром **ExcludeMasks**.

Возможные значения:

- `true` – исключать объекты, указанные в параметре **ExcludeMasks**, из области мониторинга.
- `false` – не исключать объекты, указанные в параметре **ExcludeMasks**, из области мониторинга.

Значение по умолчанию: `false`.

### ExcludeMasks

Маски в формате командной оболочки, которые определяют объекты, исключаемые из области мониторинга. Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (ExcludeMasks.item_0000, ExcludeMasks.item_0001).

Значение по умолчанию не задано.

### Раздел ExcludedFromScanScope

Группа параметров, определяющих области, исключаемые из мониторинга. Вы можете задавать несколько областей путем добавления новой группы параметров. Для задания области, исключаемой из мониторинга, используются такие же параметры, как в разделе **ScanScope**.

По умолчанию области, исключаемые из мониторинга, не заданы.

### Раздел ScanScope

Группа параметров, определяющих область мониторинга. Вы можете задавать несколько областей мониторинга путем добавления новой группы параметров.

- **AreaDesc**

  Произвольное описание области мониторинга.

  Значение по умолчанию: `Kaspersky internal objects`.

- **UseScanArea**

  Включение / выключение мониторинга указанной области.

  Возможные значения:

  - `true` – контролировать указанную область.
  - `false`– не контролировать указанную область.

  Значение по умолчанию: `true`.

- **Path**

  Полный путь к объекту или директориям, которые нужно контролировать.

  Значение по умолчанию: `/opt/kaspersky/kesl/`.

- **AreaMask**

  Маска в формате командной оболочки, которая определяет объекты для мониторинга. Подробнее см. в документации управляемой программы.

  Значение по умолчанию: `*` (будут обработаны все объекты).

### AntiCryptorHostBlockerEnabled

Включение / выключение защиты от шифрования. Защита от шифрования позволяет защитить файлы в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования. Если программа расценивает действия удаленного компьютера, получающего доступ к общим сетевым ресурсам, как шифрование, она может добавить этот компьютер в список недоверенных компьютеров и запретить ему доступ к общим сетевым директориям.

Возможные значения:

- `true` – защита от шифрования включена.
- `false` – защита от шифрования выключена.

Значение по умолчанию: `true`.

### Раздел AntiCryptorHostBlockerSettings

Группа параметров: параметры защиты от шифрования.

**BlockTime**

Длительность блокирования доступа к сетевым файловым ресурсам в минутах. Изменение параметра не влияет на длительность блокировки ранее заблокированных скомпрометированных компьютеров. Длительность блокирования не является динамическим значением и рассчитывается на момент блокирования.

Возможные значения: целые числа от `1` до `4294967295`.

Значение по умолчанию: `30`.

**UseExcludeMasks**

Исключение из области защиты объектов, указанных параметром **ExcludeMasks**.

Возможные значения:

- `true` – исключать объекты, указанные параметром **ExcludeMasks**.
- `false` – не исключать объекты, указанные параметром **ExcludeMasks**.

Значение по умолчанию: `false`.

**ExcludeMasks**

Имена или маски объектов, которые нужно исключать из защиты от шифрования. Вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки. Подробнее см. в документации управляемой программы.

Значение по умолчанию не задано.

**Раздел ExcludedFromScanScope**

Группа параметров, определяющих область, исключаемую из защиты от шифрования. Вы можете задавать несколько областей путем добавления новой группы параметров. Для задания области, исключаемой из защиты от шифрования, используются такие же параметры, как в разделе **ScanScope**.

По умолчанию области, исключаемые из защиты от шифрования, не заданы.

**Раздел ScanScope**

Группа параметров, определяющих область защиты от шифрования. Вы можете задавать несколько областей защиты от шифрования путем добавления новой группы параметров.

- **AreaDesc**

  Произвольное описание области защиты. Максимальная длина строки: 4096 символов.

  Значение по умолчанию: `All shared directories`.

- **UseScanArea**

  Включение / выключение защиты указанной области. Необходимо включить защиту хотя бы одной области.

  Возможные значения:

  - `true` – защищать указанную область.
  - `false` – не защищать указанную область.

  Значение по умолчанию: `true`.

- **Path**

  Путь к объектам, которые нужно защищать.

  Возможные значения:

  - Абсолютный путь, доступный через SMB / NFS (например, `Path=/tmp`).
  - `AllShared` – защищать все ресурсы, доступные через SMB / NFS.
  - `Shared:SMB <путь>` – защищать ресурсы, доступные через SMB.
  - `Shared:NFS <путь>` – защищать ресурсы, доступные через NFS.

  Значение по умолчанию: `AllShared`.

- **AreaMask**

  Маски файлов в формате командной оболочки, которые нужно защищать. Если значение параметра не указано, программа защищает все объекты в области проверки. Вы можете указать несколько значений этого параметра. Подробнее см. в документации управляемой программы.

  Значение по умолчанию: `*` (будут обработаны все объекты).

**UseHostBlocker**

Включение / выключение блокирования недоверенных компьютеров. Программа проверяет обращения удаленных компьютеров сети к файлам, расположенным в общих сетевых директориях защищаемого сервера. Если программа расценивает действия удаленного компьютера, получающего доступ к общим сетевым ресурсам, как шифрование, она добавляет этот компьютер в список недоверенных компьютеров и может запрещать ему доступ к общим сетевым директориям. Если блокирование недоверенных компьютеров выключено, программа все равно проверяет действия удаленных компьютеров с сетевыми файловыми ресурсами на наличие вредоносного шифрования, но атакующий компьютер не блокируется.

Возможные значения:

- `true` – блокирование недоверенных компьютеров включено.
- `false` – блокирование недоверенных компьютеров выключено.

Значение по умолчанию: `true`.

**FirewallEnabled**

Включение / выключение сетевого экрана.

Возможные значения:

- `true` – сетевой экран включен.
- `false` – сетевой экран выключен.

Значение по умолчанию: `true`.

**Раздел FirewallSettings**

Группа параметров: параметры сетевого экрана.

**DefaultIncomingAction**

Действие по умолчанию, применяемое к входящему соединению, если другие сетевые правила не применяются к этому виду соединения.

Возможные значения:

- `Allow` – разрешать входящие соединения.
- `Block` – запрещать входящие соединения.

Значение по умолчанию: `Allow`.

#### DefaultIncomingPacketAction

Действие по умолчанию, применяемое к входящему пакету, если другие сетевые пакетные правила не применяются к этому виду соединения.

Возможные значения:

- `Allow` – разрешать входящие пакеты.
- `Block` – запрещать входящие пакеты.

Значение по умолчанию: `Allow`.

#### NetworkZonesLocal, NetworkZonesPublic, NetworkZonesTrusted

Сетевые адреса, связанные с локальными сетями, публичными сетями и доверенными сетями. Вы можете указать несколько IP-адресов или IP-подсетей каждого вида в параметре **Address**.

Возможные значения:

- `d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255.
- `d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32.
- `x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff.
- `x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64.

#### PacketRules

Раздел содержит сетевые пакетные правила для сетевого экрана. Сетевое правило задается с помощью набора параметров. Вы можете задавать несколько сетевых правила путем добавления новой группы параметров. Подробнее о параметрах сетевых правил см. в документации к управляемой программе.

### Раздел KsnSettings

Раздел содержит параметры использования KSN.

#### UseKSN

Включение / выключение использования Глобального KSN в работе управляемой программы.

Возможные значения:

- `Basic` – Глобальный KSN используется без отправки статистики.
- `Extended` – Глобальный KSN используется с отправкой статистики.
- `Disabled` – Глобальный KSN не используется.

Значение по умолчанию: `Disabled`.

**UseKpsn**

Включение / выключение использования Локального KSN в работе управляемой программы.

Возможные значения:

- `true` – Локальный KSN используется.
- `false` – Локальный KSN не используется.

Значение по умолчанию: `false`.

**Раздел ProxySettings**

Раздел содержит параметры использования прокси-сервера.

**ProxyAuthPassword**

Пароль учетной записи для подключения к прокси-серверу.

Значение по умолчанию: `<пусто>`.

**ProxyAuthUser**

Имя учетной записи для подключения к прокси-серверу.

Значение по умолчанию: `<пусто>`.

**ProxyPort**

Порт для подключения к прокси-серверу.

Значение по умолчанию: `3128`.

**ProxyServer**

Параметры прокси-сервера в формате `<IP-адрес>:[<порт>]`.

Значение по умолчанию: `<пусто>`.

**UseProxy**

Включение / выключение использования прокси-сервера для подключения к Kaspersky Security Network, серверам активации и источникам обновлений.

Возможные значения:

- `true` – прокси-сервер используется.
- `false` – прокси-сервер не используется.

Значение по умолчанию: `false`.

**UseProxyAuth**

Включение / выключение использования аутентификации при подключении к прокси-серверу.

Возможные значения:

- `true` – аутентификация используется.
- `false` – аутентификация не используется.

Значение по умолчанию: `false`.

**SyslogSettings**

Типы событий, которые записываются в syslog.

Значение по умолчанию не задано.

**Раздел BackupSettings**

Раздел содержит параметры резервного хранилища.

**DaysToLive**

Время хранения объектов в резервном хранилище (в днях).

Возможные значения: `0 – 3653`. Если указано значение `0`, объекты хранятся бессрочно.

Значение по умолчанию: `90`.

**BackupSizeLimit**

Максимальный размер резервного хранилища (в МБ).

Возможные значения: `0 – 999999`. Если указано значение `0`, размер резервного хранилища не ограничен.

Значение по умолчанию: `0`.

**ExcludedMountPoint**

Точка монтирования, которую требуется исключить из области проверки во время защиты от файловых угроз и защиты от шифрования.

Возможные значения:

- `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS.
- `Mounted:NFS` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протокола NFS.
- `Mounted:SMB` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протокола NFS.
- `/Mnt` – исключать из проверки объекты, находящиеся в директории /mnt (включая вложенные директории), используемой в качестве временной точки монтирования съемных дисков.
- `<путь с применением маски /mnt/user* или /mnt/**/user_share>` – исключать из проверки объекты, находящиеся в директориях, имена которых содержат указанную маску.

Значение по умолчанию не задано.

# Назначение политики

С помощью процедуры назначения политики вы можете назначить политику указанной группе администрирования или назначить политику, которая будет применяться как глобальная.

► *Чтобы назначить политику группе администрирования, выполните команду:*

```
lmc policy assign -p <идентификатор политики> -g <идентификатор группы>
```

где `-g <идентификатор группы>` – идентификатор группы администрирования, которой вы хотите назначить политику.

► *Чтобы назначить политику, которая будет применяться как глобальная, выполните команду:*

```
lmc policy assign -p <идентификатор политики> --global
```

Указанная политика будет автоматически назначаться всем новым группам администрирования, а также группам администрирования, политика которых удалена. Политика, которая ранее применялась как глобальная, продолжает использоваться для групп, которым она была назначена.

# Экспорт и импорт параметров политики

С помощью процедур экспорта и импорта параметров политики вы можете выполнять следующие действия:

- сохранять настроенные параметры указанной политики в файл;
- переносить в указанную политику параметры из файла.

► *Чтобы экспортировать параметры политики, выполните команду:*

```
lmc policy export -p <идентификатор политики> -f <путь к файлу>
```

где:

- `-p <идентификатор политики>` – идентификатор политики, параметры которой нужно экспортировать.
- `-f <путь к файлу>` – путь к файлу, в котором нужно сохранить параметры.

► *Чтобы импортировать параметры политики, выполните команду:*

```
lmc policy import -p <идентификатор политики> -f <путь к файлу>
```

где:

- `-p <идентификатор политики>` – идентификатор политики, в которую нужно перенести ранее экспортированные параметры другой политики.
- `-f <путь к файлу>` – путь к файлу, из которого нужно импортировать параметры.

# Удаление политики

► *Чтобы удалить политику, выполните команду:*

```
lmc policy delete -p <идентификатор политики> [--force]
```

где:

`[--force]` – удалить политику принудительно. Используйте этот параметр, если вы хотите удалить политику, которая назначена группе администрирования. После удаления назначенной политики на эту группу распространяется политика, которая применяется как глобальная.

Если политика назначена какой-либо группе администрирования и при удалении политики вы не указали параметр `[--force]`, команда удаления возвращает ошибку.

Политика, которая применяется как глобальная, недоступна для удаления.

kaspersky

# Управление защитой с помощью задач

Вы можете управлять работой программ, установленных на устройствах, путем создания и запуска различных задач.

С помощью программы Kaspersky LMC вы можете создавать задачи следующих *видов*:

- Групповые задачи – это задачи, которые выполняются на устройствах выбранной группы администрирования.
- Локальные задачи – это задачи, которые выполняются на конкретном устройстве.

Для каждой управляемой программы вы можете создавать любое количество групповых и локальных задач. Вы также можете управлять локальными задачами, созданными в интерфейсе управляемой программы.

*Типы задач*, с которыми вы можете работать в программе Kaspersky LMC, зависят от управляемой программы.

Для управления программой Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Linux предусмотрены задачи следующих типов:

- Задача антивирусной проверки (ODS). В процессе выполнения задачи управляемая программа проверяет на вирусы и другие программы, представляющие угрозу, области управляемого устройства, указанные в параметрах задачи.
- Задача мониторинга файловых операций по требованию (ODFIM). В ходе выполнения этой задачи изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.
- Задача проверки загрузочных секторов (BootScan). В процессе выполнения задачи управляемая программа проверяет загрузочные секторыуправляемого устройства.
- Задача проверки памяти процессов (MemoryScan). В процессе выполнения задачи управляемая программа проверяет память процессов управляемого устройства.
- Задача обновления баз (Update). В процессе выполнения задачи управляемая программа обновляет антивирусные базы в соответствии с установленными параметрами обновления.
- Задача копирования обновлений (Retranslate). В процессе выполнения задачи управляемая программа скачивает антивирусные базы в указанную директорию, не устанавливая их.
- Задача отката обновлений (Rollback). В процессе выполнения задачи управляемая программа откатывает последнее обновление антивирусных баз.
- Задача добавления лицензионного ключа (License). В процессе выполнения задачи управляемая программа добавляет лицензионный ключ, в том числе резервный, чтобы активировать программу.

Запуск задач на устройстве выполняется только в том случае, если запущена программа, для которой созданы эти задачи. При остановке программы выполнение всех запущенных задач прекращается.

Вы можете посмотреть список доступных команд для управления задачами, выполнив команду: `lmc task -h`.

Результаты выполнения задач сохраняются как централизованно на Сервере Kaspersky LMC, так и локально на каждом устройстве.

kaspersky

## В этом разделе



# Просмотр информации о задачах

Вы можете просматривать список задач и подробную информацию о каждой задаче.

**Просмотр списка задач**

Вы можете посмотреть список задач, созданных для указанной группы администрирования, или список задач, созданных для указанного устройства.

► *Чтобы посмотреть список задач, выполните команду:*

```
lmc task list (-g <идентификатор группы> | -d <идентификатор устройства>)
```

где:

- `-g <идентификатор группы>` – отображать групповые задачи, созданные для указанной группы администрирования.
- `-d <идентификатор устройства>` – отображать локальные задачи, созданные для указанного управляемого устройства.

Если в списке отображаются групповые задачи, список содержит следующие сведения о каждой задаче:

- **ID** – идентификатор задачи.
- **Name** – название задачи.
- **Type** – тип задачи.
- **RunningOn** – количество управляемых устройств, на которых задача выполняется.
- **StoppedOn** – количество управляемых устройств, на которых задача остановлена.
- **SynchedOn** – количество управляемых устройств, на которых задача готова к выполнению.
- **SuspendedOn** – количество управляемых устройств, на которых задача приостановлена.

Если в списке отображаются локальные задачи, список содержит следующие сведения о каждой задаче:

- **ID** – идентификатор задачи.
- **Name** – название задачи.
- **Type** – тип задачи.
- **State** – состояние задачи. Возможные значения:

- **Started** – задача запущена;
- **Stopped** – задача остановлена;
- **Suspended** – задача приостановлена.

**Просмотр подробной информации о задаче**

► *Чтобы посмотреть информацию о задаче, выполните команду:*

```
lmc task details -t <идентификатор задачи>
```

Если вы указали идентификатор групповой задачи, команда выводит следующие сведения:

- **ID** – идентификатор задачи.
- **Name** – название задачи.
- **Type** – обозначение типа задачи.
- **Created** – дата и время создания задачи.
- **Edited** – дата и время последнего изменения задачи.

  **LastCommand** – последнее действие, выполненное с задачей, дата и время выполнения действия. Если задача никогда не запускалась, отображается `task is never used`.
- **State** – состояние задачи. Возможные значения:
  - **RunningOn** – количество управляемых устройств, на которых задача выполняется;
  - **StoppedOn** – количество управляемых устройств, на которых задача остановлена;
  - **SynchedOn** – количество управляемых устройств, на которых задача готова к выполнению;
  - **SuspendedOn** – количество управляемых устройств, на которых задача приостановлена;
  - **TotalDevices** – общее количество управляемых устройств.
- **Settings** – параметры задачи, если они есть, в зависимости от типа задачи.
- **Schedule** – расписание запуска задачи, если оно задано.

Если вы указали идентификатор локальной задачи, команда выводит следующие сведения:

- **ID** – идентификатор задачи.
- **Name** – название задачи.
- **Type** – обозначение типа задачи.
- **State** – состояние задачи. Возможные значения:
  - **Started** – задача запущена;
  - **Stopped** – задача остановлена;
  - **Suspended** – задача приостановлена.
- **Settings** – параметры задачи, если они есть, в зависимости от типа задачи.
- **Schedule** – расписание запуска задачи, если оно задано.

kaspersky

# Создание задачи

► *Чтобы создать задачу, выполните следующие действия:*

1. Выполните команду:

   ```
   lmc task create -n <название задачи> -t <тип задачи> (-g <идентификатор группы> | -d <идентификатор устройства>) [--no-edit]
   ```

   где:

   - `-n <название задачи>` – уникальное название задачи. Название должно быть уникальным в рамках одной группы администрирования или в рамках локальных задач для каждого устройства.
   - `-t <тип задачи>` – обозначение типа задачи.
   - `-g <идентификатор группы>` – название группы администрирования, для которой создается задача. Укажите этот параметр, если вы хотите создать групповую задачу. Не применимо вместе с параметром `-d <идентификатор устройства>`.
   - `-d <идентификатор устройства>` – идентификатор устройства, для которого создается задача. Укажите этот параметр, если вы хотите создать локальную задачу. Не применимо вместе с параметром `-g <идентификатор группы>`.
   - `[--no-edit]` – после создания задачи не запускать редактор для настройки параметров.

   Если вы выполнили команду с параметром `[--no-edit]`, создается задача с параметрами по умолчанию.

2. Если вы не указали параметр `[--no-edit]`, в результате выполнения команды запускается текстовый редактор. Проверьте установленные по умолчанию параметры задачи и внесите необходимые изменения.

   Набор параметров задачи, которые вы можете настраивать, зависит от типа задачи и от управляемой программы, для которой создана задача. Подробнее о параметрах задач разных типов см. в документации управляемой программы.

3. Если требуется, в секции **Schedule** измените параметры расписания запуска задачи, настроенные по умолчанию. Расписание запуска предусмотрено для всех задач, кроме задачи добавления лицензионного ключа.

   - **RuleType** – режим запуска задачи. Возможные значения:
     - `Monthly` – задача запускается в каждый N день месяца;
     - `Weekly` – задача запускается в каждый N день недели;
     - `Daily` – задача запускается каждый N день;
     - `Hourly` – задача запускается каждые N часов;
     - `Minutely` – задача запускается каждые N минут;
     - `Once` – задача запускается только один раз в указанное время;
     - `OnStartUp` – задача запускается сразу после запуска программы;
     - `AfterUpdate` – задача запускается сразу после обновления баз программы;
     - `Manual` – задача запускается только вручную (см. раздел "Запуск и остановка задачи" на стр. 67).

В зависимости от выбранного режима запуска вы можете настроить следующие дополнительные параметры:

- **StartTime** – время и периодичность запуска:
  - для режимов `Monthly`, `Weekly`, `Daily`, `Minutely` время запуска указывается в формате `<hh:mm:ss>;<период>`, где:

    `<hh:mm:ss>` – время первого запуска задачи по расписанию;

    `<период>` – периодичность в днях или минутах, с которой запускается задача.
  - для режима `Hourly` время запуска указывается в формате `<YYYY/MM/DD hh:mm:ss>;<период>`, где:

    `<YYYY/MM/DD hh:mm:ss>` – дата и время первого запуска задачи по расписанию;

    `<период>` – периодичность в часах, с которой запускается задача.
  - для режима `Once` время запуска указывается в формате `<YYYY/MM/DD hh:mm:ss>`, где:

    `<YYYY/MM/DD hh:mm:ss>` – дата и время запуска задачи.
- **RandomInterval** – максимальное время задержки запуска задачи (в минутах), если несколько задач запущено одновременно.
- **ExecuteTimeLimit** – максимальное время выполнения задачи (в минутах).
- **RunMissedStartRules** – запускать пропущенные задачи. Возможные значения:
  - `true` – если во время запуска задачи по расписанию отсутствовало подключение Агента Kaspersky LMC на управляемом устройстве к Серверу Kaspersky LMC и запуск задачи по расписанию не состоялся, то задача будет запущена сразу после подключения Агента Kaspersky LMC к Серверу Kaspersky LMC.
  - `false` – запуск задачи производится только по расписанию, попытка запуска пропущенных задач не производится.

4. Сохраните изменения и закройте редактор.

# Изменение параметров задачи

► *Чтобы изменить параметры задачи, выполните следующие действия:*

1. Выполните команду:

   `lmc task edit -t <идентификатор задачи>`

   Запускается текстовый редактор.
2. Внесите необходимые изменения.

   Вы можете настраивать следующие параметры задач:
   - Различные параметры работы управляемой программы в зависимости от типа задачи и управляемой программы. Подробнее о параметрах задач разных типов см. в документации управляемой программы.
   - Параметры расписания запуска задачи (см. раздел "Создание задачи" на стр. 65).

3. Сохраните изменения и закройте редактор.

# Запуск и остановка задачи

Вы можете запускать и останавливать задачи, независимо от заданного режима запуска.

Запуск и остановке задач на управляемом устройстве выполняется, только если на устройстве запущена управляемая программа, для которой созданы эти задачи. Если управляемая программа остановлена, выполнение всех запущенных задач прекращается, управление запуском и остановкой задач невозможно.

► *Чтобы запустить задачу, выполните команду:*

```
lmc task start --task|-t <идентификатор задачи>
```

Перед запуском задачи рекомендуется убедиться, что управляемые устройства, на которых должна выполняться задача, синхронизированы с Сервером Kaspersky LMC. Сведения о синхронизации устройства с Сервером Kaspersky LMC вы можете посмотреть в подробной информации об устройстве, параметр **Synched** (см. раздел "**Просмотр информации об управляемых устройствах**" на стр. 31).

► *Чтобы остановить задачу, выполните команду:*

```
lmc task stop --task|-t <идентификатор задачи>
```

# Экспорт и импорт параметров задачи

С помощью процедур экспорта и импорта параметров задачи вы можете выполнять следующие действия:

- сохранять настроенные параметры указанной задачи в файл;
- переносить в указанную задачу параметры из файла;

► *Чтобы экспортировать параметры задачи, выполните команду:*

```
lmc task export -t <идентификатор задачи> -f <путь к файлу>
```

где:

- `-t <идентификатор задачи>` – идентификатор задачи, параметры которой нужно экспортировать.
- `-f <путь к файлу>` – путь к файлу, в котором нужно сохранить параметры.

► *Чтобы импортировать параметры задачи, выполните команду:*

```
lmc task import -t <идентификатор задачи> -f <путь к файлу>
```

где:

- `-t <идентификатор задачи>` – идентификатор задачи, в которую нужно перенести ранее экспортированные параметры другой задачи. Тип задачи, в которую переносятся параметры, должен соответствовать типу задачи, из которой параметры были экспортированы.
- `-f <путь к файлу>` – путь к файлу, из которого нужно импортировать параметры.

# Удаление задачи

► *Чтобы удалить задачу, выполните команду:*

```
lmc task delete -t <идентификатор задачи>
```

kaspersky

# Лицензирование и активация управляемых программ

Kaspersky LMC позволяет удаленно активировать управляемые программы, наблюдать за использованием лицензионных ключей и продлевать сроки действия лицензий.

Агенты Kaspersky LMC передают Серверу Kaspersky LMC сведения о лицензии, по которой активированы управляемые программы, и о добавленных в программы лицензионных ключах. Вы можете посмотреть эти сведения:

- в информации об устройстве, на котором установлена программа (см. раздел "Просмотр информации об управляемых устройствах" на стр. 31);
- в отчете об использовании лицензионных ключей (см. раздел "Отчеты" на стр. 82).

Если количество единиц лицензирования, для которых используется ключ, составляет более 110% от количества единиц лицензирования, для которых ключ может использоваться в соответствии с лицензионным ограничением, на Сервере Kaspersky LMC формируется событие о превышении лицензионных ограничений.

## В этом разделе



## Об активации управляемой программы

*Активация программы* – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии.

Чтобы активировать программу, требуется добавить лицензионный ключ в программу.

Лицензионный ключ может быть активным и резервным.

*Активный лицензионный ключ* – лицензионный ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного лицензионного ключа.

*Резервный лицензионный ключ* – лицензионный ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Резервный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Резервный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве резервного лицензионного ключа.

Вы можете добавить лицензионный ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе программы в виде

уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Независимо от выбранного вами способа активации программы для добавления ключа используется *задача добавления ключа*.

Для активации программы с помощью кода активации необходимо подключение к серверам активации "Лаборатории Касперского".

Подробнее об основных понятиях, связанных с лицензированием, и об особенностях активации программ "Лаборатории Касперского" см. в документации управляемых программ.

► *Чтобы добавить лицензионный ключ в программу, выполните следующие действия:*

1. Создайте задачу добавления лицензионного ключа (см. раздел "Создание задачи добавления лицензионного ключа" на стр. 70). Вы можете создать групповую задачу для добавления ключа в управляемую программу на всех устройствах указанной группы администрирования или локальную задачу для добавления ключа в управляемую программу на указанном устройстве.
2. Запустите задачу добавления лицензионного ключа вручную (см. раздел "Запуск и остановка задачи" на стр. 67).

# Создание задачи добавления лицензионного ключа

► *Чтобы создать задачу добавления ключа, выполните следующие действия:*

1. Выполните команду:

   ```
   lmc task create -t License -n <название задачи> (-g <идентификатор группы> | -d <идентификатор устройства>)
   ```

   где:

   - `-n <название задачи>` – уникальное название задачи. Название должно быть уникальным в рамках одной группы администрирования или в рамках локальных задач.
   - `-g <идентификатор группы>` – название группы администрирования, для которой создается задача. Используйте этот параметр, если вы хотите добавить лицензионный ключ на все устройства указанной группы администрирования. Не применимо вместе с параметром `-d <идентификатор устройства>`.
   - `-d <идентификатор устройства>` – идентификатор устройства, для которого создается задача. Используйте этот параметр, если вы хотите добавить лицензионный ключ на указанное устройство. Не применимо вместе с параметром `-g <идентификатор группы>`.

   В результате выполнения команды запускается текстовый редактор.
2. Укажите следующие параметры задачи:
   - **IsAdditional** – использовать лицензионный ключ в качестве резервного. Возможные значения:
     - `false` – лицензионный ключ будет добавлен в качестве активного ключа. Это значение установлено по умолчанию.
     - `true` – лицензионный ключ будет добавлен в качестве резервного ключа.

- **Type** – способ добавления ключа. Возможные значения:
  - `code` – лицензионный ключ будет добавлен с помощью кода активации. Это значение установлено по умолчанию.
  - `keyfile` – лицензионный ключ будет добавлен с помощью файла ключа.
- **KeyFile** – путь к файлу ключа. Если вы выбрали способ добавления ключа с помощью файла ключа, вы можете указать путь к файлу ключа в этом поле или указать данные файла ключа, закодированные методом Base64, в поле **KeyBody**.
- **KeyBody** – возможные значения в зависимости от выбранного способа добавления ключа:
  - `<код активации>`;
  - `<данные файла ключа, закодированные методом Base64>`.

3. Сохраните изменения и закройте редактор.

Задача запускается вручную (см. раздел "Запуск и остановка задачи" на стр. 67).

kaspersky

# Обновление баз и модулей управляемых программ

Базы программ "Лаборатории Касперского" содержат описания угроз компьютерной безопасности, которые позволяют обнаруживать в проверяемых объектах вредоносный код, описания известных в настоящее время видов сетевых атак и признаков вторжений, а также базы вредоносных и фишинговых веб-адресов.

Обновление баз и модулей программы обеспечивает актуальность защиты компьютеров.

Для обновления баз управляемой программы требуется действующая лицензия на использование программы.

Kaspersky LMC позволяет реализовать централизованное распространение обновлений на управляемые программы.

Чтобы настроить обновление баз и модулей управляемых программ с помощью Kaspersky LMC требуется выполнить следующие действия:

1. Настроить загрузку обновлений баз и модулей управляемых программ на Сервер Kaspersky LMC. Загрузка обновлений выполняется с помощью утилиты Update Utility. Подробнее об Update Utility см. в Базе знаний (https://support.kaspersky.ru/updater3/linux).

   По умолчанию загрузка запускается на пятнадцатой минуте каждого часа. Источником обновлений служат серверы обновлений "Лаборатории Касперского".

   Рекомендуется выполнять настройку загрузки обновлений во время первоначальной настройки Сервера с помощью скрипта easy-install (см. раздел "Первоначальная настройка Сервера Kaspersky LMC" на стр. 19).

   Вы также можете настроить параметры загрузки обновлений в следующих конфигурационных файлах:

   - /var/opt/kaspersky/lmc-uu/updater.ini;
   - /var/opt/kaspersky/lmc-uu/lmc_retrans.apache2.conf.

2. Загрузить обновления на Сервер Kaspersky LMC.

   Каждая управляемая программа "Лаборатории Касперского" запрашивает требуемые обновления с Сервера Kaspersky LMC. Сервер Kaspersky LMC объединяет эти запросы и загружает те обновления, которые запрашиваются программами, в директорию на Сервере Kaspersky LMC.

   Команда загрузки обновлений запускается по расписанию, которое задано в системном планировщике Cron, или вручную. Дождитесь загрузки по расписанию или выполните команду:

   ```
   lmc update bases
   ```

   Базы будут помещены в директорию /var/opt/kaspersky/lmc-uu/Bases/. В результате выполнения команды формируется событие *BasesUpdated*.

3. Для каждой управляемой программы настроить задачу обновления баз и модулей программы. Вы можете создать локальную или групповую задачу. В параметрах задачи нужно указать следующие параметры:

   - Источник обновлений – директория на Сервере Kaspersky LMC /var/opt/kaspersky/lmc-uu/Bases/.
   - Режим запуска задачи – рекомендуется выбрать режим в соответствии с настроенным расписанием загрузки обновлений баз и модулей управляемых программ на Сервер Kaspersky LMC.

Подробнее о настройке задачи обновления баз см. в документации управляемой программы.

После первого обновления баз программы доступен откат к предыдущему набору баз. Возможность отката последнего обновления используется, например, в том случае, если новая версия баз программы содержит некорректную сигнатуру, из-за которой программа "Лаборатории Касперского" блокирует безопасную программу.

Чтобы вернуться к использованию предыдущего набора баз программы, вам нужно создать и запустить задачу отката обновлений управляемой программы. Вы можете создать локальную или групповую задачу. Подробнее о задаче отката обновлений см. в документации управляемой программы.

kaspersky

# Участие в Kaspersky Security Network

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры KSN различают:

- Глобальный KSN – инфраструктура расположена на серверах "Лаборатории Касперского".
- Локальный KSN – инфраструктура расположена внутри корпоративной сети организации или на сторонних серверах поставщика услуг, например внутри сети интернет-провайдера. Локальный KSN предназначен для организаций, которые не могут использовать Глобальный Kaspersky Security Network по одной из следующих причин:
  - Устройства пользователей не подключены к интернету.
  - Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

В зависимости от управляемой программы при использовании KSN программа может автоматически отправлять в "Лабораторию Касперского" информацию об использовании KSN и другую статистическую информацию, полученную в результате работы программы. Также программа может отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые могут использовать злоумышленники для нанесения вреда компьютеру или данным.

Подробнее об особенностях использования Kaspersky Security Network в работе управляемой программы см. в документации управляемой программы.

Kaspersky LMC позволяет управлять параметрами использования KSN в работе управляемых программ. По умолчанию использование KSN выключено.

## В этом разделе



# Об использовании Глобального KSN

Если вы хотите использовать Глобальный KSN, вам нужно включить его в параметрах политики (см. раздел "Параметры политики для Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Linux" на стр. 47).

Чтобы включить использование KSN, вам нужно прочитать и принять условия Положения о Kaspersky Security Network (см. раздел "Изменение параметров политики" на стр. 46).

kaspersky

Вы можете прочитать текст Положения о Kaspersky Security Network в файле /opt/kaspersky/lmc-server/scripts/plugins/kesl_10/ksn_agreement.txt.

Также в политике вы можете указать параметры использования Глобального KSN, предусмотренные для управляемой программы, например, режим использования KSN с отправкой или без отправки статистики.

Вы можете настраивать параметры использования Глобального KSN в локальных параметрах управляемой программы, если это не запрещено политикой.

Подробнее о параметрах Глобального Kaspersky Security Network см. в документации управляемой программы.

# Настройка использования Локального KSN

Если вы хотите использовать Локальный KSN, вам нужно выполнить следующие действия:

- Включить использование Локального KSN в параметрах политики (см. раздел "Параметры политики для Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Linux" на стр. 47);
- Настроить параметры Локального KSN с помощью команды Kaspersky LMC.

► *Чтобы настроить параметры Локального KSN, выполните команду:*

```
lmc kpsn set --usekpsn true --filepkcs <путь к файлу *.pkcs7> --filepem <путь к файлу *.pem>
```

где:

- файл `*.pkcs7` – конфигурационный файл, который содержит параметры Локального KSN;
- файл `*.pem` – файл, который содержит сертификат для проверки подписи файла *.pkcs7.

В результате выполнения команды параметры Локального KSN передаются управляемой программе, если в политике для управляемой программы включено использование Локального KSN. В работе управляемой программы используется Локальный KSN.

► *Чтобы посмотреть настроенные параметры Локального KSN, выполните одну из следующих команд:*

- `lmc kpsn get`

  Команда выводит следующие сведения:

  - **ProviderName** – наименование провайдера услуг;
  - **ProviderContacts** – контакты провайдера услуг;
  - **ConfigCreatedAt** – дата и время создания конфигурационного файла *.pkcs7, содержащего параметры Локального KSN.

- `lmc kpsn details`

  Команда выводит параметры использования Локального KSN, перечисленные выше, и дополнительную информацию об использовании Локального KSN, если она предоставлена поставщиком услуг.

► *Чтобы отменить использование Локального KSN, выполните команду:*

```
lmc kpsn set --usekpsn false
```

kaspersky

# Получение информации о состоянии защиты инфраструктуры

Этот раздел описывает средства получения сведений о работе программы Kaspersky LMC, управляемых программ и состоянии защиты управляемых устройств.

## В этом разделе



## События

Информация о событиях, произошедших во время работы программы Kaspersky LMC и управляемых программ, сохраняется на Сервере Kaspersky LMC.

Все события подразделяются на четыре группы по уровню важности:

- *Критическое событие* (critical). Это событие указывает на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Ошибка* (error). Это событие указывает на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- *Предупреждение* (warning). Это событие не обязательно является серьезным, однако указывает на потенциально возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* (info). Это событие, информирует об успешном выполнении операции, корректной работе программы или завершении процедуры.

Вы можете просматривать список событий и информацию об отдельных событиях.

События хранятся на Сервере Kaspersky LMC в течение определенного срока. По умолчанию установлены следующие сроки хранения событий в зависимости от уровня важности события:

- критическое событие – 180 суток;
- ошибка – 180 суток;
- предупреждение – 90 суток;
- информационное сообщение – 30 суток.

Сервер Kaspersky LMC проверяет срок хранения событий раз в сутки. События, срок хранения которых истек, автоматически удаляются.

Вы можете выполнять следующие действия с событиями:

- Просматривать списки событий и подробную информацию о каждом событии (см. раздел "Просмотр событий" на стр. 78).
- Настраивать время хранения событий для каждого из уровней важности событий (см. раздел

"Настройка времени хранения событий" на стр. 80).

- Настраивать уведомления о событиях (см. раздел "Настройка уведомлений о событиях" на стр. 80).

Вы можете посмотреть список доступных команд для управления событиями, выполнив команду: `lmc event -h`.

### В этом разделе



## Просмотр событий

При просмотре списка событий вам доступны следующие возможности:

- Просмотр всех событий. По умолчанию в списке отображаются последние 100 событий.
- Просмотр указанного количества событий.
- Просмотр событий, связанных с указанным управляемым устройством.
- Просмотр событий, связанных с устройствами, входящими в указанную группу администрирования.
- Просмотр событий, связанных с указанной задачей.
- Просмотр событий, произошедших за указанный период.
- Просмотр списка событий указанного уровня важности.

События в списке сортируются от более поздних к более ранним по времени их возникновения на Сервере Kaspersky LMC или времени получения от Агента Kaspersky LMC.

► *Чтобы посмотреть список событий, выполните команду:*

```
lmc event list [-d <идентификатор устройства>] [--device-name <имя устройства>] [-t <идентификатор задачи>] [-g <идентификатор группы>] [-l <количество> | -i <период>] [-s <степень важности>]
```

где:

- `[-d <идентификатор устройства>]`, `[--device-name <имя устройства>]` – отображать только события, связанные с указанным управляемым устройством.
- `[-t <идентификатор задачи>]` – отображать только события, связанные с указанной задачей.
- `[-g <идентификатор группы>]` – отображать только события, связанные с устройствами, входящими в указанную группу администрирования.
- `[-l <количество>]` – отображать указанное количество событий. Не применимо вместе с параметром `[-i <период>]`.
- `[-i <период>]` – отображать события за указанный период, включая указанные даты начала и окончания периода. Период указывается в формате: `<дата и время начала периода>~<дата и время окончания периода>`. Не применимо вместе с параметром `[-l <количество>]`.

- `[-s <уровень важности>]` – отображать события с указанным уровнем важности. Возможные значения:
  - `CRT` – критическое;
  - `ERR` – ошибка;
  - `WRN` – предупреждение;
  - `INF` – информационное сообщение.

Список содержит следующие сведения о каждом событии:

- **ID** – идентификатор события.
- **Application** – название программы (для событий Сервера Kaspersky LMC отображается `LMC`).
- **DeviceId** – идентификатор управляемого устройства, на котором произошло событие (для событий Сервера Kaspersky LMC не отображается).
- **HostName** – доменное имя управляемого устройства, на котором произошло событие (для событий Сервера Kaspersky LMC не отображается).
- **Severity** – уровень важности.
- **Type** – тип события.
- **Description** – описание события.
- **Creation Time (UTC)** – дата и время формирования события на Сервере Kaspersky LMC.
- **Receive Time (UTC)** – дата и время помещения события в базу данных Kaspersky LMC.

► *Чтобы посмотреть подробную информацию о событии, выполните команду:*

```
lmc event details -e <идентификатор события>
```

Команда выводит следующие сведения о событии:

- **Description** – описание события.
- **Severity** – уровень важности события.
- **Creation time** – дата и время формирования события.
- **Send time** – дата и время отправки информации о событии на Сервер Kaspersky LMC (для событий Сервера Kaspersky LMC указывается дата и время формирования события).
- **Transport time** – дата и время получения информации о событии на сервере RabbitMQ.
- **Receive time** – дата и время помещения события в базу данных Kaspersky LMC.
- **Device** – информация об устройстве, на котором произошло событие:
  - **ID** – идентификатор управляемого устройства, на котором произошло событие.
  - **HostName** – доменное имя управляемого устройства, на котором произошло событие (для событий Сервера Kaspersky LMC не отображается).
  - **Application** – название программы, в работе которой произошло событие (для событий Сервера Kaspersky LMC отображается "LMC").
- **Group** – информация о группе администрирования, в которую входит устройство, на котором произошло событие (для событий Сервера Kaspersky LMC не отображается).

- **ID** – идентификатор группы администрирования, в которую входит устройство, на котором произошло событие (для событий Сервера Kaspersky LMC не отображается).
- **Name** – название группы администрирования, в которую входит устройство, на котором произошло событие (для событий Сервера Kaspersky LMC не отображается).

- **Parameters** – дополнительные параметры события.

## Настройка времени хранения событий

► *Чтобы настроить время хранения событий на Сервере Kaspersky LMC, выполните команду:*

```
lmc event timeout set -s <уровень важности> -d <срок хранения>
```

где:

- `-s <уровень важности>` – уровень важности событий, для которых нужно установить срок хранения. Возможные значения:
  - `CRT` – критическое;
  - `ERR` – ошибка;
  - `WRN` – предупреждение;
  - `INF` – информационное сообщение.
- `-d <срок хранения>` – срок хранения событий указанного уровня важности в днях. Событие будет удалено автоматически по прошествии указанного количества календарных дней со дня создания события

  Если вы хотите, чтобы события указанного уровня важности не сохранялись на Сервере Kaspersky LMC, в качестве срока хранения укажите `0`.

Вы можете посмотреть срок хранения, заданный для событий каждого уровня важности.

► *Чтобы посмотреть срок хранения событий, выполните команду:*

```
lmc event timeout get -s <уровень важности>
```

Команда выводит срок хранения событий указанного уровня важности в днях.

## Настройка уведомлений о событиях

Вы можете включить и настроить уведомления о событиях, которые происходят в работе программы Kaspersky LMC. По умолчанию уведомления о событиях выключены.

► *Чтобы включить и настроить уведомления о событиях, выполните следующие действия:*

1. Создайте исполняемый файл (например, bash-скрипт), который будет обрабатывать события и выполнять уведомления. Вы можете создать несколько исполняемых файлов, чтобы обрабатывать события разного уровня важности.

Исполняемые файлы будут запускаться под учетной записью root. Рекомендуется убедиться в безопасном поведении исполняемых файлов.

Информация о событиях передается через переменные окружения. Вы можете использовать следующие переменные окружения:

- `$LMC_EVENT_ID` – идентификатор события.
- `$LMC_EVENT_CODE` – тип события.
- `$LMC_EVENT_SEVERITY` – уровень важности события.
- `$LMC_EVENT_CREATED` – дата и время формирования события.
- `$LMC_EVENT_NAME` – название события.
- `$LMC_EVENT_DESCRIPTION` – описание события.
- `$LMC_DEVICE_ID` – идентификатор управляемого устройства, на котором возникло событие.
- `$LMC_DEVICE_HOSTNAME` – доменное имя управляемого устройства, на котором возникло событие.
- `$LMC_DEVICE_ADDRESS` – IP-адрес управляемого устройства, на котором возникло событие.
- `$LMC_DEVICE_APPLICATION` – название управляемой программы на устройстве, на котором возникло событие.

2. Разместите созданный исполняемый файл (или файлы) в директории /etc/opt/kaspersky/lmc-server/notifications. Убедитесь, что учетная запись root имеет право на запуск исполняемого файла.
3. Выполните команду:

   ```
   lmc event notification edit
   ```

4. Укажите значения следующих параметров:

   **IsEnabled** – `1`.

   **BySeverity** – одна или несколько строк в виде:

   ```
   <уровень важности>:<имя файла>
   ```

   где:

   - `<уровень важности>` – идентификатор уровня важности событий, по которым вы хотите получать уведомления. Возможные значения:
     - `CRT` – критическое;
     - `ERR` – ошибка;
     - `WRN` – предупреждение;
     - `INF` – информационное сообщение.
   - `<имя файла>` – имя исполняемого файла, который обрабатывает события указанного уровня важности.

► *Чтобы выключить уведомления о событиях, выполните следующие действия:*

1. Выполните команду:

   ```
   lmc event notification edit
   ```

2. Укажите для параметра **IsEnabled** значение `0`.

# Отчеты

Вы можете получать информацию о состоянии управляемых устройств и работе управляемых программ с помощью отчетов. Отчеты формируются на основании информации, хранящейся на Сервере Kaspersky LMC.

Вы можете формировать следующие отчеты:

- **Отчет о развертывании защиты**. Содержит сведения об устройствах, на которых установлены Агент Kaspersky LMC и программа, обеспечивающая антивирусную защиту, или только Агент Kaspersky LMC.
- **Отчет о версиях управляемых программ**. Содержит сведения о версиях программ "Лаборатории Касперского", установленных на управляемых устройствах.
- **Отчет об угрозах**. Содержит информацию о вирусах и других вредоносных программах, которые были обнаружены на управляемых устройствах за указанный период времени.
- **Отчет о состоянии защиты**. Содержит информацию о состоянии защиты управляемых устройств.
- **Отчет об используемых базах**. Содержит информацию о версиях антивирусных баз, используемых на управляемых устройствах.
- **Отчет об использовании лицензионных ключей**. Содержит информацию о лицензионных ключах, которые используются для активации управляемых программ.

Отчеты формируются по шаблонам, которые содержатся в Kaspersky LMC (см. раздел "Просмотр информации о шаблонах отчетов" на стр. 82).

## В этом разделе



# Просмотр информации о шаблонах отчетов

► *Чтобы посмотреть список шаблонов отчетов, которые доступны в Kaspersky LMC, выполните команду:*

```
lmc report list
```

Список содержит следующие сведения о каждом шаблоне отчета:

- **ReportName** – название шаблона отчета: Возможные значения:
  - `deployment` – шаблон для формирования отчета о развертывании защиты;

- `appversion` – шаблон для формирования отчета о версиях управляемых программ;
- `viruses` – шаблон для формирования отчета о вирусах;
- `protection` – шаблон для формирования отчета о состоянии защиты;
- `bases` – шаблон для формирования отчета об используемых базах;
- `keyusage` – шаблон для формирования отчета об использовании лицензионных ключей.

- **ApplicationName** – название программы, для которой можно сформировать отчет по этому шаблону.
- **Description** – название отчета, который формируется по этому шаблону.

► *Чтобы посмотреть подробную информацию о шаблоне отчета, выполните команду:*

```
lmc report details -r <название шаблона отчета>
```

Команда выводит следующие сведения:

- **Report name** – название шаблона отчета.
- **Product name** – название программы, для которой можно сформировать отчет по этому шаблону.
- **Help** – краткое описание отчета, который формируется по этому шаблону.
- **Description** – название отчета, который формируется по этому шаблону.
- **Report params** – информация о параметрах отчета.

## Формирование отчета

► *Чтобы сформировать отчет, выполните команду:*

```
lmc report create -r <тип отчета> [-g <идентификатор группы>] [--html]
```

где:

- `<тип отчета>` – обозначение типа отчета, который нужно сформировать:
  - `deployment` – отчет о развертывании защиты;
  - `appversion` – отчет о версиях управляемых программ;
  - `viruses` – отчет об угрозах;
  - `protection` – отчет о состоянии защиты;
  - `bases` – отчет об используемых базах;
  - `keyusage` – отчет об использовании лицензионных ключей.
- `[-g <идентификатор группы>]` – отчет содержит сведения только об устройствах, входящих в указанную группу администрирования. По умолчанию в отчете содержатся сведения обо всех управляемых устройствах, подключенных к Серверу Kaspersky LMC на момент формирования отчета.
- `[--html]` – сформировать отчет в виде html-страницы.

Все отчеты, кроме отчета об угрозах, содержат сведения на момент формирования отчета.

В отчете об угрозах по умолчанию отображается информация за последние 30 дней. При формировании

отчета об угрозах вы можете использовать дополнительные параметры, чтобы указать период, данные за который нужно включить в отчет:

- `[--date-from <дата начала отчетного периода>]` – включить в отчет данные, начиная с указанной даты.
- `[--date-to <дата окончания отчетного периода>]` – включить в отчет данные до указанной даты.

Даты задаются в формате `<YYYY-MM-DD>T<hh:mm:ss±hhmm>`, например, `2020-04-01T00:00:00+0300`.

## Просмотр отчетов

Каждый отчет состоит из следующих частей:

- Общая информация об отчете:
  - название программы, для которой сформирован отчет;
  - название отчета;
  - краткое описание отчета;
  - дата и время формирования отчета в формате UTC.

  Для отчета об угрозах также отображается период, данные за который включены в отчет.
- Таблица детальной информации.
- Таблица сводной информации.
- Графическая диаграмма с наиболее характерными данными отчета, если отчет сформирован в виде html-страницы.

### В этом разделе



### Отчет о развертывании защиты (Kaspersky protection deployment report)

Таблица детальной информации содержит следующие сведения:

- **GROUP_ID** – идентификатор группы администрирования, в которую входит управляемое устройство.
- **GROUP_NAME** – название группы администрирования, в которую входит управляемое устройство.
- **DEVICE_ID** – идентификатор управляемого устройства.

- **MACHINE_ID** – уникальный идентификатор (UID) устройства.
- **DEVICE_NAME** – доменное имя управляемого устройства.
- **IP_ADDRESS** – IP-адрес управляемого устройства.
- **APPLICATION_NAME** – название управляемой программы на устройстве.
- **APPLICATION_VERSION** – версия управляемой программы на устройстве.
- **LAST_CONNECTION** – дата и время последнего соединения Агента Kaspersky LMC, установленного на устройстве, с Сервером Kaspersky LMC.

Под таблицей детальной информации отображается общее количество управляемых устройств.

Таблица сводной информации содержит следующие сведения:

- **PROTECTION_COMPONENTS** – установленные программы и компоненты. Возможные значения:
  - `Only Agent Lmc` – установлен только Агент Kaspersky LMC;
  - `Agent Lmc And Applications` – установлен Агент Kaspersky LMC и программа, обеспечивающая антивирусную защиту.
- **TOTAL_DEVICES** – общее количество устройств, на которых установлены Агент Kaspersky LMC и программа, обеспечивающая антивирусную защиту, или только Агент Kaspersky LMC.

Если отчет сформирован в виде html-страницы, в отчете отображается круговая диаграмма, которая показывает количество устройств, на которых установлен только Агент Kaspersky LMC, и количество устройств, на которых установлен Агент Kaspersky LMC и антивирусная программа.

## Отчет о версиях управляемых программ (Kaspersky software version report)

Таблица детальной информации содержит следующие сведения:

- **PRODUCT_ID** – идентификатор установленной программы на устройстве.
- **GROUP_ID** – идентификатор группы администрирования, в которую входит управляемое устройство.
- **GROUP_NAME** – название группы администрирования, в которую входит управляемое устройство.
- **DEVICE_ID** – идентификатор управляемого устройства.
- **MACHINE_ID** – уникальный идентификатор (UID) устройства.
- **DEVICE_NAME** – доменное имя управляемого устройства.
- **IP_ADDRESS** – IP-адрес управляемого устройства.
- **APPLICATION_NAME** – название программы, установленной на устройстве.
- **APPLICATION_VERSION** – версия программы, установленной на устройстве.
- **LAST_CONNECTION** – дата и время последнего соединения Агента Kaspersky LMC, установленного на устройстве, с Сервером Kaspersky LMC.

Под таблицей детальной информации отображаются следующие сведения:

- **TOTAL_APPLICATIONS** – общее количество всех установленных программ.
- **TOTAL_INSTALLATIONS** – общее количество установок программ на всех устройствах.
- **TOTAL_DEVICES** – общее количество устройств, на которых установлены программы.
- **TOTAL_GROUPS** – общее количество групп, в которые входят устройства с установленными

программами.

Таблица сводной информации содержит следующие сведения:

- **APPLICATION_NAME** – название установленной программы на устройстве.
- **APPLICATION_VERSION** – версия установленной программы на устройстве.
- **TOTAL_DEVICES** – общее количество управляемых устройств, на которых установлена программа, указанная в графе **APPLICATION_NAME**.
- **TOTAL_GROUPS** – общее количество групп администрирования, в которые входят устройства с установленными управляемыми программами.

Если отчет сформирован в виде html-страницы, в отчете отображается диаграмма, которая содержит сведения об установленных программах и количестве устройств, на которых эти программы установлены.

## Отчет об угрозах (Kaspersky threats report)

Таблица детальной информации содержит следующие сведения:

- **GROUP_ID** – идентификатор группы администрирования, в которую входит управляемое устройство.
- **GROUP_NAME** – название группы администрирования, в которую входит управляемое устройство.
- **DEVICE_ID** – идентификатор управляемого устройства.
- **DEVICE_NAME** – доменное имя управляемого устройства.
- **IP_ADDRESS** – IP-адрес управляемого устройства.
- **APPLICATION_NAME** – название программы, установленной на устройстве.
- **APPLICATION_VERSION** – версия программы, установленной на устройстве.
- **OBJECT_ID** – идентификатор обнаруженного объекта на управляемом устройстве.
- **THREAT_NAME** – название обнаруженной угрозы.
- **OBJECT_PATH** – путь к обнаруженному объекту на управляемом устройстве.
- **OBJECT_ACTION** –результат действия, которое управляемая программа выполнила над обнаруженным объектом. Возможные значения: `Desinfected`, `Deleted`, `Blocked`, `Skipped` и комбинации этих значений.
- **THREAT_TYPE** – тип обнаруженной угрозы.
- **DETECT_TIME** – дата и время обнаружения угрозы на управляемом устройстве.

Под таблицей детальной информации отображаются следующие сведения:

- **TOTAL_OBJECTS** – общее количество различных объектов, которые были обнаружены на всех управляемых устройствах за отчетный период.
- **TOTAL_FILES** – общее количество различных файлов, содержащих все объекты, обнаруженные за отчетный период.
- **TOTAL_DEVICES** – общее количество управляемых устройств, на которых обнаружены объекты за отчетный период.
- **TOTAL_GROUPS** – общее количество групп, в которые входят устройства, на которых обнаружены объекты.

Таблица сводной информации содержит следующие сведения:

- **DETECT_NAME** – имя обнаруженного объекта.
- **THREAT_TYPE** – тип обнаруженной угрозы.
- **TOTAL_DETECT** – общее количество обнаружений объекта, указанного в графе **DETECT_NAME**, на всех устройствах.
- **DIFFERENT** – общее количество различных файлов, содержащих обнаруженный объект.
- **TOTAL_DEVICES** – общее количество устройств, на которых обнаружен объект, указанный в графе **DETECT_NAME**.
- **FIRST_DETECT_TIME** – дата и время первого обнаружения объекта.
- **LAST_DETECT_TIME** – дата и время последнего обнаружения объекта.

Если отчет сформирован в виде html-страницы, в отчете отображается столбчатая диаграмма, которая содержит сведения о действиях, выполненных над зараженным объектом, и о количестве обнаруженных угроз.

## Отчет о состоянии защиты (Kaspersky protection status report)

Таблица детальной информации содержит следующие сведения:

- **GROUP_ID** – идентификатор группы администрирования, в которую входит управляемое устройство.
- **GROUP_NAME** – название группы администрирования, в которую входит управляемое устройство.
- **DEVICE_ID** – идентификатор управляемого устройства.
- **MACHINE_ID** – уникальный идентификатор (UID) устройства.
- **DEVICE_NAME** – доменное имя управляемого устройства.
- **IP_ADDRESS** – IP-адрес управляемого устройства.
- **APPLICATION_NAME** – название программы, установленной на устройстве.
- **APPLICATION_VERSION** – версия программы, установленной на устройстве.
- **DEVICE_STATUS** – статус управляемого устройства. Возможные значения: `Ok`, `Warning`, `Critical`.
- **DEVICE_STATUS_REASON** – причина присвоения статуса управляемому устройству.
- **BASES_RELEASE_TIME** – дата выпуска баз, используемых на управляемом устройстве.
- **LAST_ODS** – дата и время последнего запуска задачи проверки.
- **LAST_CONNECTION** – дата и время последнего соединения Агента Kaspersky LMC, установленного на устройстве, с Сервером Kaspersky LMC.

Под таблицей детальной информации отображается общее количество всех устройств со статусами, указанными в таблице.

Таблица сводной информации содержит следующие сведения:

- **DEVICE_STATUS** – статус управляемого устройства.
- **DEVICE_STATUS_REASON** – причина присвоения статуса управляемому устройству.
- **TOTAL_DEVICES** – общее количество устройств, которые имеют указанный статус и указанную причину присвоения статуса.

- **TOTAL_GROUPS** – общее количество групп, в которые входят устройства с указанным статусом и указанной причиной присвоения статуса.

Если отчет сформирован в виде html-страницы, в отчете отображается диаграмма, которая содержит сведения о причинах присвоения статуса и количестве устройств, которым присвоен этот статус.

## Отчет об используемых базах (Kaspersky databases report)

Таблица детальной информации содержит следующие сведения:

- **GROUP_ID** – идентификатор группы администрирования, в которую входит управляемое устройство.
- **GROUP_NAME** – название группы администрирования, в которую входит управляемое устройство.
- **DEVICE_ID** – идентификатор управляемого устройства.
- **MACHINE_ID** – уникальный идентификатор (UID) устройства.
- **DEVICE_NAME** – доменное имя управляемого устройства.
- **IP_ADDRESS** – IP-адрес управляемого устройства.
- **APPLICATION_NAME** – название программы, установленной на устройстве.
- **APPLICATION_VERSION** – версия программы, установленной на устройстве.
- **BASES_UPDATE_TIME** – дата и время последнего успешного обновления баз программы.
- **BASES_RELEASE_TIME** – дата и время выпуска используемых баз программы.
- **BASES_STATE** – статус баз программы. Возможные значения:
  - `UP_TO_DATE` – актуальные;
  - `NOT_LOADED` – не загружены;
  - `OUTDATED` – устарели;
  - `TOTALY_OUTDATED` – сильно устарели;
  - `UNKNOWN` – нет информации о статусе баз.
- **LAST_CONNECTION** – дата и время последнего соединения Агента Kaspersky LMC, установленного на устройстве, с Сервером Kaspersky LMC.

Под таблицей детальной информации по каждому статусу баз отображается количество устройств, на которых базы имеют этот статус.

Таблица сводной информации содержит следующие сведения:

- **BASES_RELEASE_TIME** – дата и время выпуска баз программы.
- **BASES_STATE** – статус баз программы. Возможные значения:
  - `UP_TO_DATE` – актуальные;
  - `NOT_LOADED` – не загружены;
  - `OUTDATED` – устарели;
  - `TOTALY_OUTDATED` – сильно устарели;
  - `UNKNOWN` – нет информации о статусе баз.

- **TOTAL_DEVICES** – количество управляемых устройств, на которых используются базы с указанной датой выпуска и указанным статусом.
- **TOTAL_GROUPS** – количество групп, в которые входят управляемые устройства с указанными базами.

Если отчет сформирован в виде html-страницы, в отчете отображается круговая диаграмма, которая содержит следующие сведения:

- количество устройств с актуальными базами;
- количество устройств с устаревшими базами;
- количество устройств с сильно устаревшими базами;
- количество устройств, на которых возникла ошибка при загрузке баз.

## Отчет об использовании лицензионных ключей (Kaspersky key usage report)

Таблица детальной информации содержит следующие сведения:

- **GROUP_ID** – идентификатор группы администрирования, в которую входит управляемое устройство.
- **GROUP_NAME** – название группы администрирования, в которую входит управляемое устройство.
- **DEVICE_ID** – идентификатор управляемого устройства.
- **DEVICE_NAME** – доменное имя управляемого устройства.
- **IP_ADDRESS** – IP-адрес управляемого устройства.
- **APPLICATION_NAME** – название управляемой программы на устройстве.
- **APPLICATION_VERSION** – версия управляемой программы на устройстве.
- **ACTIVE_KEY** – активный лицензионный ключ. Если активный ключ не добавлен, отображается `none`.
- **EXPIRATION_DATE** – дата окончания использования программы с этим ключом.
- **RESTRICTION_TYPE** – тип лицензионного ограничения. Возможные значения:
  - `Server` – ограничение по количеству защищаемых устройств с операционными системами для серверов;
  - `Desktop` – ограничение по количеству защищаемых устройств с операционными системами для рабочих станций;
  - `CPU` –ограничение по количеству процессоров на всех защищаемых устройствах;
  - `Core` – ограничение по количеству ядер процессоров на всех защищаемых устройствах.
- **USED_RESTRICTIONS** – количество единиц лицензирования, для которых лицензионный ключ уже используется в зависимости от типа ключа (количество устройств, количество ядер, количество процессоров).
- **RESERVE_KEY** – резервный лицензионный ключ. Если резервный ключ не добавлен, отображается `none`.
- **LAST_CONNECTION** – дата и время последнего соединения Агента Kaspersky LMC, установленного на устройстве, с Сервером Kaspersky LMC.

Под таблицей детальной информации отображаются следующие сведения:

- **KEYS** – общее количество используемых лицензионных ключей.
- **KEY_EXCEEDED** – общее количество лицензионных ключей, для которых превышено лицензионное ограничение.

Таблица сводной информации содержит следующие сведения:

- **KEY** – лицензионный ключ.
- **RESTRICTION_TYPE** – тип лицензионного ограничения. Возможные значения:
  - `Server` – ограничение по количеству защищаемых устройств с операционными системами для серверов;
  - `Desktop` – ограничение по количеству защищаемых устройств с операционными системами для рабочих станций;
  - `CPU` –ограничение по количеству процессоров на всех защищаемых устройствах;
  - `Core` – ограничение по количеству ядер процессоров на всех защищаемых устройствах.
- **USED_RESTRICTIONS** – количество единиц лицензирования, для которых лицензионный ключ уже используется в зависимости от типа ключа (количество устройств, количество ядер, количество процессоров).
- **MAX_RESTRICTIONS** – максимальное количество единиц лицензирования, для которых может использоваться ключ в соответствии с лицензионным ограничением.
- **USED_AS_RESERVE** – количество устройств, на которых лицензионный ключ добавлен в качестве резервного.

Если отчет сформирован в виде html-страницы, в отчете отображается диаграмма, которая содержит сведения о лицензионных ключах, количестве единиц лицензирования, для которых ключ уже используется, и количестве единиц лицензирования, на которое превышено лицензионное ограничение при использовании ключа.

kaspersky

# Проверка целостности компонентов программы

Чтобы избежать подмены модулей и файлов программы, в Kaspersky LMC предусмотрена проверка целостности компонентов программы. Для проверки целостности используется утилита integrity_check_tool, которая проверяет модули и файлы на наличие несанкционированных изменений и повреждений.

Утилита проверки целостности входит в комплект поставки программы и располагается по следующим путям:

- /opt/kaspersky/lmc-server/bin/integrity_check_tool – утилита проверки целостности компонента Сервер Kaspersky LMC;
- /opt/kaspersky/lmc-agent/bin/integrity_check_tool – утилита проверки целостности компонента Агент Kaspersky LMC.

Утилита проверяет целостность файлов, перечисленных в специальных списках, которые называются *файлы манифеста*. Файл манифеста компонента программы содержит файлы, целостность которых важна для корректной работы компонента программы. Если контрольная сумма модуля или файла программы является некорректной, он считается поврежденным.

Целостность самих файлов манифеста также проверяется.

Файлы манифеста для компонентов программы расположены по следующим путям:

- /opt/kaspersky/lmc-server/bin/integrity_check.xml – файл манифеста для Сервера Kaspersky LMC;
- /opt/kaspersky/lmc-agent/bin/integrity_check.xml – файл манифеста для Агента Kaspersky LMC.

► *Чтобы проверить целостность компонента программы, выполните следующую команду:*

```
integrity_check_tool -v | --verify -m | --manifest <путь>
```

где `<путь>` – полный путь к файлу манифеста.

Вы можете запустить утилиту со следующими необязательными параметрам:

- `-V, --verbose` – расширенный вывод выполняемых действий и результатов. Если вы не укажете этот параметр, будут выводиться только ошибки, объекты, не прошедшие проверку, и суммарная статистика проверки.
- `-L, --log-file <файл>`, где <файл> – имя файла для вывода событий, произошедших во время проверки. По умолчанию события выводится в стандартный поток stdout.
- `-l, --log-level <число>`, где `<число>` – уровень детализации вывода событий от 1 до 1000. По умолчанию используется уровень детализации 0.

Результат проверки каждого файла манифеста выводится рядом с названием файла манифеста в следующем виде:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата 0).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от 0).

Вы можете посмотреть список всех доступных команд для утилиты проверки целостности, выполнив команду: `integrity_check_tool -h`.

kaspersky

# Обращение в Службу технической поддержки

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

## В этом разделе



## Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе (см. раздел "Источники информации о программе" на стр. 8), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2c) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

## Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2c).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

kaspersky

# Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

# Использование файлов трассировки

По умолчанию информация о ходе и результатах работы программы Kaspersky LMC записывается в следующие файлы трассировки:

- /var/log/kaspersky/lmc-server/lmc-server.<PID>.<YYYY-MM-DD>T<hhmmss>.log – файл трассировки Сервера Kaspersky LMC;
- /var/log/kaspersky/lmc-agent/lmc-agent.<PID>.<YYYY-MM-DD>T<hhmmss>.log – файл трассировки Агента Kaspersky LMC;

  где:

  - <PID> – идентификатор процесса;
  - <YYYY-MM-DD>T<hhmmss> – дата и время создания файла.

Вы можете настраивать параметры создания файлов трассировки.

► *Чтобы настроить параметры создания файлов трассировки Сервера Kaspersky LMC, выполните следующие действия:*

1. Откройте файл /var/opt/kaspersky/lmc-server/lmc_server.ini.
2. Укажите нужные значения параметров в секции `[LOGGING]`:

   `TraceFolder=<путь к директории>` – путь к директории, в которой расположены файлы трассировки Сервера Kaspersky LMC. Значение по умолчанию: `/var/log/kaspersky/lmc-server`.

   `MaxFileCount=<число>` – максимальное количество файлов трассировки. Значение по умолчанию: `2`. Если указано значение `0`, создание файлов трассировки выключено.

   `MaxFileSize=<число>` – максимальный размер одного файла трассировки в МБ. Значение по умолчанию: `250`.

   `TraceLevel=<уровень>` – уровень детализации отладочной информации. Возможные значения: `non`, `err`, `wrn`, `inf`, `dbg`, `any`. Значение по умолчанию: `err`. Если указано значение `non`, создание файлов трассировки выключено.
3. Сохраните и закройте файл lmc_server.ini.
4. Перезапустите Сервер Kaspersky LMC с помощью команды:

   ```
   systemctl restart lmc-server.service
   ```

Файлы трассировки Сервера Kaspersky LMC могут содержать персональные данные. Данные хранятся в открытом виде. Для доступа к данным необходимы полномочия учетной записи root. Рекомендуется обеспечить защиту данных от несанкционированного доступа.

► *Чтобы настроить параметры создания файлов трассировки Агента Kaspersky LMC, выполните следующие действия:*

1. Откройте файл /var/opt/kaspersky/lmc-agent/lmc_agent.ini.
2. Укажите нужные значения параметров в секции `[LOGGING]`:

   `TraceFolder=<путь к директории>` – путь к директории, в которой расположены файлы трассировки Агента Kaspersky LMC. Значение по умолчанию: `/var/log/kaspersky/lmc-agent`.

   `MaxFileCount=<число>` – максимальное количество файлов трассировки. Значение по умолчанию: `2`. Если указано значение `0`, создание файлов трассировки выключено.

   `MaxFileSize=<число>` – максимальный размер одного файла трассировки в МБ. Значение по умолчанию: `250`.

   `TraceLevel=<уровень>` – уровень детализации отладочной информации. Возможные значения: `non`, `err`, `wrn`, `inf`, `dbg`, `any`. Значение по умолчанию: `err`. Если указано значение `non`, создание файлов трассировки выключено.
3. Сохраните и закройте файл lmc_agent.ini.
4. Перезапустите Агент Kaspersky LMC с помощью команды:

   ```
   systemctl restart lmc-agent.service
   ```

kaspersky

# Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

## В этом разделе



# Параметры конфигурационных файлов

Для управления работой программы Kaspersky LMC вы можете использовать следующие конфигурационные файлы:

- /var/opt/kaspersky/lmc-server/lmc_server.ini. Файл содержит параметры работы Сервера Kaspersky LMC.
- /var/opt/kaspersky/lmc-agent/lmc_agent.ini. Файл содержит параметры работы Агента Kaspersky LMC.
- /var/opt/kaspersky/lmc-uu/updater.ini и /var/opt/kaspersky/lmc-uu/lmc_retrans.apache2.conf. Файлы содержат параметры загрузки и распространения обновлений баз на управляемые программы.
- /opt/kaspersky/lmc-server/scripts/package_vars.ini и /opt/kaspersky/lmc-agent/scripts/package_vars.ini. Файлы содержат константы, используемые в работе программы.

**Файл /var/opt/kaspersky/lmc-server/lmc_server.ini**

Секция `[LOGGING]`. Содержит параметры создания файлов трассировки (см. раздел "Использование файлов трассировки" на стр. 93).

**Файл /var/opt/kaspersky/lmc-agent/lmc_agent.ini**

Секция `[LOGGING]`. Содержит параметры создания файлов трассировки (см. раздел "Использование файлов трассировки" на стр. 93).

Секция `[SERVER]`. Содержит параметры подключения Агента Kaspersky LMC к Серверу Kaspersky LMC:

`hostname` – адрес Сервера Kaspersky LMC;

`port` – порт для подключения к Серверу Kaspersky LMC;

`login` – имя учетной записи для подключения Агента Kaspersky LMC;

`password` – пароль учетной записи для подключения Агента Kaspersky LMC.

Секция `[DEVICE]`. Содержит параметр `description` – описание устройства.

**Файл /opt/kaspersky/lmc-server/scripts/package_vars.ini**

Секция `[GENERAL]`

```
socket=/var/run/lmc-control.socket
```

**Файл /opt/kaspersky/lmc-agent/scripts/package_vars.ini**

Секция `[GENERAL]`

```
AGENT_CONFIG=/var/opt/kaspersky/lmc-agent/lmc_agent.ini
AUTH_VHOST=lmc.auth_vhost
AUTH_EXCHANGE=auth_exchange
AUTH_ROUTING=auth_routing
CERT_FILENAME=/var/opt/kaspersky/lmc-agent/server.cert
```

# Коды возврата командной строки

**Коды возврата утилит lmc, lmcadmin, lmcagent**

- 0 – успешное выполнение команды;
- 1 – ошибка, не связанная с парсингом аргументов, указанных в команде);
- 2 – ошибка, связанная с парсингом аргументов, указанных в команде).

**Коды возврата утилиты первоначальной настройки Сервера Kaspersky LMC (easy-install)**

- 0 – успешное выполнение команды;
- 1 – ошибка.

kaspersky

# Глоссарий

## К

### Kaspersky CompanyAccount

Портал, предназначенный для отправки электронных запросов в "Лабораторию Касперского" и отслеживания их обработки специалистами "Лаборатории Касперского".

### 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.

## А

### Активация программы

Процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии.

### Активный ключ

Ключ, используемый в текущий момент для работы программы.

## Б

### Базы программы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска баз. Базы программы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

## И

### Источник обновлений

Ресурс, содержащий обновления антивирусных баз программы Kaspersky LMC. Источником обновлений антивирусных баз могут служить серверы обновлений "Лаборатории Касперского", а также HTTP-, FTP-сервер, локальная или сетевая папка.

## К

### Код активации

Код, который предоставляет вам "Лаборатория Касперского" при получении пробной лицензии или при приобретении коммерческой лицензии на использование Kaspersky LMC. Этот код требуется для активации программы.

Код активации представляет собой последовательность из двадцати латинских букв и цифр в формате XXXXX-XXXXX-XXXXX-XXXXX.

# Л

## Лицензионное соглашение

Юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

## Лицензионный ключ (ключ)

Уникальная буквенно-цифровая последовательность. Лицензионный ключ обеспечивает использование программы в соответствии с условиями Лицензионного соглашения (типом лицензии, сроком действия лицензии, лицензионными ограничениями). Вы можете использовать программу только при наличии в ней лицензионного ключа.

## Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

## Лицензия

Ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

# Р

## Резервный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

# Т

## Технология iChecker

Технология, позволяющая увеличить скорость антивирусной проверки за счет исключения тех объектов, которые не были изменены с момента предыдущей проверки, при условии, что настройки проверки (базы программы и настройки) не были изменены. Информация об этом хранится в специальной базе. Технология применяется как в режиме постоянной защиты, так и в режиме проверки по требованию.

Например, у вас есть файл архива, который был проверен программой "Лаборатории Касперского" и которому был присвоен статус *не заражен*. В следующий раз этот архив будет исключен из проверки, если он не был изменен и не менялись настройки проверки. Если вы изменили состав архива, добавив в него новый объект, изменили настройки проверки, обновили базы программы, архив будет проверен повторно.

Ограничения технологии iChecker:

- технология не работает с файлами больших размеров, так как в этом случае проверить весь файл быстрее, чем вычислять, был ли он изменен с момента последней проверки;
- технология поддерживает ограниченное число форматов.

kaspersky

# Ф

## Файл ключа

Файл вида xxxxxxxx.key, который предоставляет вам "Лаборатория Касперского" при получении пробной лицензии или при приобретении коммерческой лицензии на использование Kaspersky LMC. Файл ключа требуется для активации программы.

# Э

## Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

kaspersky

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft и Outlook – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Pivotal, RabbitMQ – товарные знаки и/или зарегистрированные в США и/или других странах товарные знаки Pivotal Software, Inc.