?????????? Kaspersky Endpoint Security ??? Linux (12.2) ? ???????? ?????? EDR (7.1)

????????

Приложение Kaspersky Endpoint Security for Linux совместимо с решением Kaspersky Anti Targeted Attack Platform, которое предназначено для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки нулевого дня, целевые атаки и сложные целевые атаки.

Приложение Kaspersky Endpoint Security может интегрироваться со следующими компонентами, входящими в состав решения Kaspersky Anti Targeted Attack Platform

- Kaspersky Endpoint Detection and Response (KATA) обеспечивает защиту устройств в локальной сети организации. При взаимодействии с Kaspersky Endpoint Detection and Response (KATA) приложение Kaspersky Endpoint Security может выполнять следующие функции
  - Отправлять данные о событиях на устройствах (телеметрию) на сервер Kaspersky Anti Targeted Attack Platform с компонентом Central Node (далее также сервер KATA). Приложение Kaspersky Endpoint Security передает на сервер KATA данные наблюдения за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.
  - Выполнять ответные действия, направленные на обеспечение функций безопасности, по командам, полученным от Kaspersky Anti Targeted Attack Platform.

?????????? ?????????? Kaspersky Endpoint Security Linux 12.2

Минимальные аппаратные требования

- процессор Core 2 Duo 1.86 ГГц или выше;
- раздел подкачки не менее 1 ГБ;
- 1 ГБ оперативной памяти для 32-битных операционных систем, 2 ГБ оперативной памяти для 64-битных операционных систем;
- 4 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов;
- при использовании графического пользовательского интерфейса монитор должен обеспечивать отображение окон шириной 1000 пикселей и высотой 600 пикселей (если применяется масштабирование экрана, то эти размеры также масштабируются);
- если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

Минимальные аппаратные требования для архитектуры Arm

- процессор Armv8.2-A Kunpeng 920 или Armv8-A Baikal-M (BE-M1000) или платформа m-TrusT Терминал;
- раздел подкачки не менее 1 ГБ;
- 2 ГБ оперативной памяти;
- 3 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов;
- при использовании графического пользовательского интерфейса монитор должен обеспечивать отображение окон шириной 1000 пикселей и высотой 600 пикселей (если применяется масштабирование экрана, то эти размеры также масштабируются).

?????????? ?????????? Kaspersky Endpoint Security Linux 12.2

Для установки Kaspersky Endpoint Security на устройстве должна быть установлена одна из следующих операционных систем

32-битные операционные системы

- Debian GNULinux 11.0 и выше.
- Debian GNULinux 12.0 и выше.
- Альт 8 СП Рабочая Станция (8.4).
- Альт 8 СП Сервер (8.4).

64-битные операционные системы

- AlmaLinux OS 8.0 и выше.
- AlmaLinux OS 9.0 и выше.
- AlterOS 7.5.
- Amazon Linux 2.
- Astra Linux Common Edition 2.12.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).
- Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6).
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3).
- Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7).
- CentOS 7.2 и выше.
- CentOS Stream 8.
- CentOS Stream 9.
- Debian GNULinux 11.0 и выше.
- Debian GNULinux 12.0 и выше.
- EMIAS 1.0 и выше.
- EulerOS 2.0 SP10.
- Fedora Linux 41.
- Kylin 10.
- Linux Mint 21.1 и выше.
- Linux Mint 22.0 и выше.
- Mostech 12.
- openSUSE Leap 15.0 и выше.
- Oracle Linux 7.3 и выше.
- Oracle Linux 8.0 и выше.
- Oracle Linux 9.0 и выше.
- Red Hat Enterprise Linux 7.2 и выше.
- Red Hat Enterprise Linux 8.0 и выше.
- Red Hat Enterprise Linux 9.0 и выше.
- Rocky Linux 8.5 и выше.
- Rocky Linux 9.0 и выше.
- SberLinux 9.0.1.
- SberOS 3.3.3.
- SUSE Linux Enterprise Server 12.5 и выше.
- SUSE Linux Enterprise Server 15 и выше.
- Ubuntu 22.04 LTS.
- Ubuntu 24.04 LTS.
- Альт 8 СП Рабочая станция (8.4).
- Альт 8 СП Сервер (8.4).
- Альт Образование 10.1.
- Альт СП Рабочая Станция релиз 10.
- Альт СП Рабочая Станция релиз 10.1.
- Альт СП Сервер релиз 10.

- Альт СП Сервер релиз 10.1.
- Атлант, сборка Alcyone, версия 2022.02.
- Гослинукс 7.17.
- Гослинукс 7.2.
- М ОС 12 Сервер.
- МОС ОС 15.4 Арбат.
- МСВСФЕРА АРМ 9.2 и выше.
- МСВСФЕРА СЕРВЕР 9.2 и выше.
- ОС МЭШ 12 Для всех пользователей (без телеметрии и без поддержки ДИТ).
- ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ).
- ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ).
- ОСнова 2.9 и выше.
- РЕД ОС 7.3.
- РЕД ОС 8.0.
- РОСА Кобальт 7.9.
- РОСА Хром 12.
- СинтезМ-Клиент 8.6.
- СинтезМ-Сервер 8.6.

64-битные операционные системы для архитектуры Arm

- Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
- CentOS Stream 9.
- EulerOS 2.0 SP10.
- SUSE Linux Enterprise Server 15.
- Ubuntu 22.04 LTS.
- Альт СП Рабочая Станция релиз 10.
- Альт СП Сервер релиз 10.
- РЕД ОС 7.3.
- РЕД ОС 8.0.

???????? ???????????????? ???????

В веб-консоли KSC перейти в раздел Операции Хранилища Инсталляционные пакеты и нажать Добавить

1.png

Выбираем «Создать инсталляционный пакет для приложения Лаборатории Касперского». При необходимости можно добавить инсталляционный пакет из файла, который был заранее скачан с сайта Лаборатории Касперского, для этого необходимо выбрать «Создать инсталляционный пакет из файла»

После этого отобразится окно со всеми доступными инсталляционными пакетами для скачивания, где для удобства поиска в верхнем правом углу можно настроить фильтры. В данном случае можно выставить фильтр на язык и операционные системы, затем нажать Применить

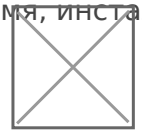
Выбираем инсталляционный пакет агента администрирования в соответствии с типом ОС Linux (в данном примере устанавливается DEB based версия) и нажимаем на него, затем выбираем **Загрузить и создать инсталляционный пакет**

Далее в этом же списке находим Kaspersky Endpoint Security для Linux. Аналогично нажать на него и выбирать **Загрузить и создать инсталляционный пакет**

После этого вернуться в раздел **Инсталляционные пакеты**. Для загружаемых инсталляционных пакетов необходимо принять лицензионное соглашение

Необходимо нажать на название каждого инсталляционного пакета, ознакомиться и затем принять лицензионное соглашение, как на скриншоте ниже

После этого, спустя некоторое время, инсталляционные пакеты будут полностью установлены и готовы к установке

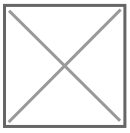


?????????? ? ?????????? ??????????

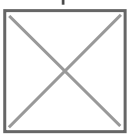
Перед тем как начать установку необходимо перенести обнаруженные Сервером администрирования устройства в раздел управляемые устройства. Для этого необходимо перейти в раздел **Обнаружение устройств и развертывание / Нераспределенные устройства** и выбрать необходимые для перемещения устройства, которые были обнаружены KSC, нажать **Переместить в группу** и выбрать необходимую группу для перемещения (по умолчанию создана корневая группа Управляемые устройства, в которую можно добавлять вложенные группы, формируя иерархию групп администрирования).

?????????? ??????
???????????????????

Первым делом на устройство необходимо установить агент администрирования, инсталляционный пакет которого был загружен ранее. Перед началом установки проверьте готовность устройства с операционной системой Linux

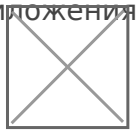
В разделе **Активы (Устройства)** / **Задачи** выбрать **Добавить** 

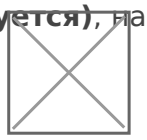
Выбрать задачу **Удаленная установка приложения** и задать ей удобное название.

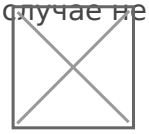


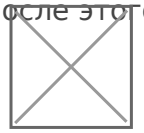
Выбрать группу администрирования на которую будет распространяться действие данной задачи 

Затем указать из выпадающего списка инсталляционный пакет **агента администрирования** и выбрать установку **Средствами операционной системы с помощью Сервера администрирования**. Остальные параметры можно оставить по умолчанию 

Далее выбрать действие, которое следует предпринять, если в ходе установки приложения потребуется перезагрузка операционной системы (можно оставить по умолчанию) 

На следующем шаге необходимо выбрать **Учетная запись требуется (Агент администрирования не используется)**, нажать **Добавить** и указать учётную запись пользователя или SSH сертификат 

Открывать окно свойств задачи после ее создания в данном случае не нужно, поэтому можно убрать эту галочку и сохранить задачу нажав **Готово** 

Затем выбрать созданную задачу и нажать **Запустить**. После этого необходимо дождаться, когда статус задачи изменится на **Завершена успешно** 

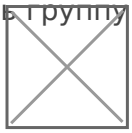
После установки Агента администрирования в разделе **Активы (Устройства) / Управляемые устройства** в столбце **Агент администрирования** запущен появится зеленая галочка. Статус останется критическим, т.к. еще не установлено приложение безопасности 

После успешной установки агента администрирования можно переходить к установке Kaspersky Endpoint Security for Linux (KESL)

????????? Kaspersky Endpoint Security for Linux

Удаленная установка KESL также производится через задачу удаленной установки. В разделе **Активы (Устройства) / Задачи выбрать Добавить** 

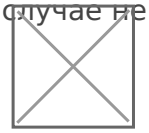
Выбрать задачу **Удаленная установка приложения** и задать ей удобное название.

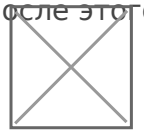
Выбрать группу администрирования на которую будет распространяться действие данной задачи 

Затем указать из выпадающего списка инсталляционный пакет **KESL** и выбрать установку **С помощью Агента администрирования**. Поле Выбор Агента администрирования оставить пустым, т.к. он уже был установлен на предыдущем шаге. Остальные параметры можно оставить по умолчанию 

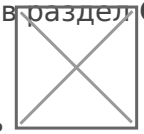
Далее выбрать действие, которое следует предпринять, если в ходе установки приложения потребуется перезагрузка операционной системы (можно оставить по умолчанию) 

Затем выбрать **Учетная запись не требуется**, т.к. Агент администрирования уже установлен и установка KESL, будет производиться от его имени 

Открывать окно свойств задачи после ее создания в данном случае не нужно, поэтому можно убрать эту галочку и сохранить задачу нажав **Готово** 

Затем выбрать созданную задачу и нажать **Запустить**. После этого необходимо дождаться, когда статус задачи изменится на **Завершена успешно** 

?????????? ????????? ? KSC

Для удобства и возможности постоянного доступа к лицензии, рекомендуется добавлять их в хранилище лицензий KSC. Необходимо перейти в раздел **Операции / Лицензии Лаборатории Касперского** и выбрать **Добавить** 

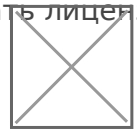
В появившемся разделе выбрать **Ввести код активации** и вписать активационный код и нажать **Отправить** (подходит, когда KSC и агенты имеют доступ в интернет). Если у KSC или агентов нет доступа в интернет (серверам активации ЛК), то необходимо выбрать **Добавить файл ключа** и подгрузить соответствующий файл и нажать **Отправить**. Затем нажать

Сохранить. Конвертировать активационный код в файл ключа можно на специализированном портале Лаборатории Касперского.

После добавления лицензия будет отображаться в разделе **Операции / Лицензии Лаборатории Касперского**

????????? KESL

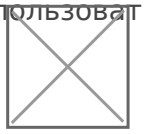
После успешной установки KESL, необходимо его необходимо активировать лицензией. Для активации в разделе **Активы (Устройства) / Задачи** выбрать **Добавить**



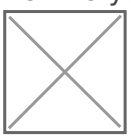
Указать задачу для Добавления ключа для приложения KESL и задать ей удобное название

Выбрать группу администрирования на которую будет распространяться действие данной задачи

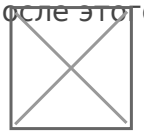
Затем выбрать доступную лицензию и убедиться, что она активирует функциональность KESL. Использовать ключ в качестве резервного **НЕ** нужно



Открывать окно свойств задачи после ее создания в данном случае не нужно, поэтому можно убрать эту галочку и сохранить задачу нажав **Готово**



Затем выбрать созданную задачу и нажать **Запустить**. После этого необходимо дождаться, когда статус задачи изменится на **Завершена успешно**



После этого KESL готов к настройке работы в качестве EDR-агента.

??????? ???????????? KATA (KEDR)

Для подключения KESL в режим EDR-агента используется сертификат платформы KATA. Необходимо зайти в веб-консоль платформы KATA под УЗ администратора

В разделе **Параметры / Сертификаты** сгенерировать сертификат сервера (не нужно, если выполнялось ранее) и затем нажать **экспортировать**. Будет скачан сертификат сервера KATA

???????? ???????? KESL

Данный шаг необходим, если у вас ещё нет политики KESL для Linux-устройств, которые планируется подключать в качестве EDR-агентов.

Для централизованного управления приложением Kaspersky Endpoint Security for Linux, в том числе и подключение к KEDR, используются политики. Для создания новой политики перейдите в раздел **Активы (Устройства) / Политики и профили политик** и нажмите **Добавить**

Выберите необходимую версию Kaspersky Endpoint Security for Linux, которая установлена на Linux-устройстве 

Укажите стандартный режим работы приложения 

Затем рекомендуется принять условия положения о KSN для его автоматического включения в политике 

Далее, если нет в этом необходимости, деактивировать переключатель Наследовать параметры родительской политики и сохранить политику. Она будет отображаться в разделе **Активы (Устройства) / Политики и профили политик** и сохранить политику

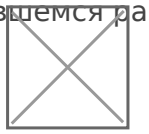
?????????? KESL ? ???????? EDR-??????

В разделе **Активы (Устройства) / Политики и профили политик** перейти в политику KESL

В политике перейти в раздел **Параметры приложения □□ Detection and Response □□**

Endpoint Detection and Response (KATA)

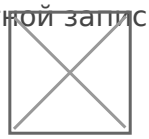
Перевести переключатель работы компонента в активный режим, затем в блоке **Параметры подключения к серверам** нажать **Настроить**. В появившемся разделе выбрать добавить и



указать ранее скачанный сертификат KATA и нажать **Ок**

В блоке **Серверы KATA** нажать **Добавить** и указать адрес подключения к центральному узлу KATA, затем нажать Ок. Адрес по умолчанию (127.0.0.1) удалить. Сохранить политику

Спустя некоторое время подключенные устройства отобразятся в веб-консоли KATA Platform. Необходимо зайти под учётной записью сотрудника безопасности и перейти в раздел



Активы / Endpoint Agents

На этом подключение KESL в качестве агента EDR окончено

Revision #7
Created 11 July 2025 12:05:48 by Сергей
Updated 6 February 2026 10:48:58 by Кирилл