# ??????? ????????? ? ????????? ??????????? EDR (KATA) ?? ???? KES Linux

## ? ???????? ???????????

**Версия решения:** KESL 11.4+; KEDR (KATA) 4.0>7.1;

**ВАЖНО:**
В этой инструкции рассмотрим только настройку через KSC Web Console. MMC консоль больше не поддерживается, поэтому рекомендуется использовать веб-консоль.

**Примечание:**
В отличие от версии KES Windows, KES Linux не требует установки и включения компонента EDR, так как он уже входит в состав установленного решения и для его активации необходимо включить использование его в политике и настроить интеграцию.

Начиная с версии **Kaspersky Endpoint Security 12.4 для Linux** компонент Endpoint Detection and Response (KATA) переименован в Endpoint Detection and Response Expert (on-premise). Теперь этот компонент обеспечивает интеграцию не только с Kaspersky Endpoint Detection and Response (KATA), компонентом Kaspersky Anti Targeted Attack Platform, но и с решением Kaspersky Endpoint Detection and Response Expert (on-premise).

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (О режимах использования приложения Kaspersky Endpoint Security, Просмотр в командной строке информации об использовании приложения в режиме Легкого агента), активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионных ключей на SVM.

> Для полноценной интеграции приложения Kaspersky Endpoint Security с Kaspersky Anti Targeted Attack Platform требуется включить компонент**Анализ поведения**. Если Анализ поведения выключен, необходимые данные телеметрии не передаются (кроме запросов на синхронизацию и данных об обнаружении угроз от других компонентов защиты).

---

**1. Подготовка**

# 1.1. ?????????????? ??????

| Компонент | Минимальная версия |
|---|---|
| KATA / KEDR | 4.0>7.1 |
| KSC | 13.2+ |
| KES для Linux | 11.4+ |

# 1.2. ?????????? ?????????? (?? ???????)

- **CPU**: ≥1 ГГц, поддержка **SSE2**
- **RAM**: ≥2 ГБ (x64)
- **HDD**: ≥2 ГБ свободного места

# 1.3. ?????????? ????????

- Лицензия **KESL+EDR**

---

**2. Чистая установка KESL 11.4+ с EDR через KSC Web Console**

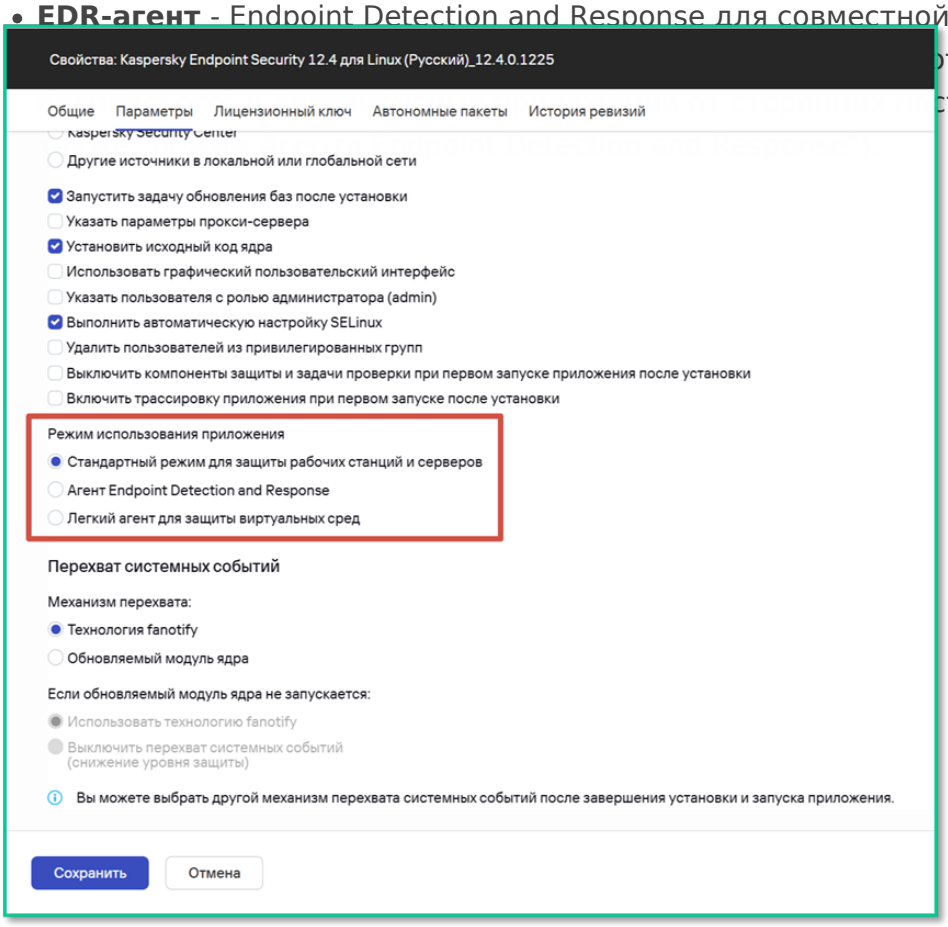
# 2.1. ????????? ???????????????? ??????

1. Откройте **KSC Web Console → Операции → Хранилища → Инсталляционные пакеты**

2. Найдите пакет **KESL 11.4+**

3.Перейдите в **Параметры и выберите режим использования приложения:**

- **Стандартном режим** - Kaspersky Endpoint Security используется как автономное приложение для защиты рабочих станций и серверов под управлением операционных систем Linux.
- **Легкий агент** - Kaspersky Security для виртуальных в составе решения. Kaspersky Endpoint Security используется как компонент решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.
- **EDR-агент** - Endpoint Detection and Response для совместной работы на




**Скриншот 1:** Выбор

компонента Режима работы KESL 12.4+

4. Выполните дополнительные настройки в Консоли администрирования с детальным описанием можно ознакомиться в онлайн-документации

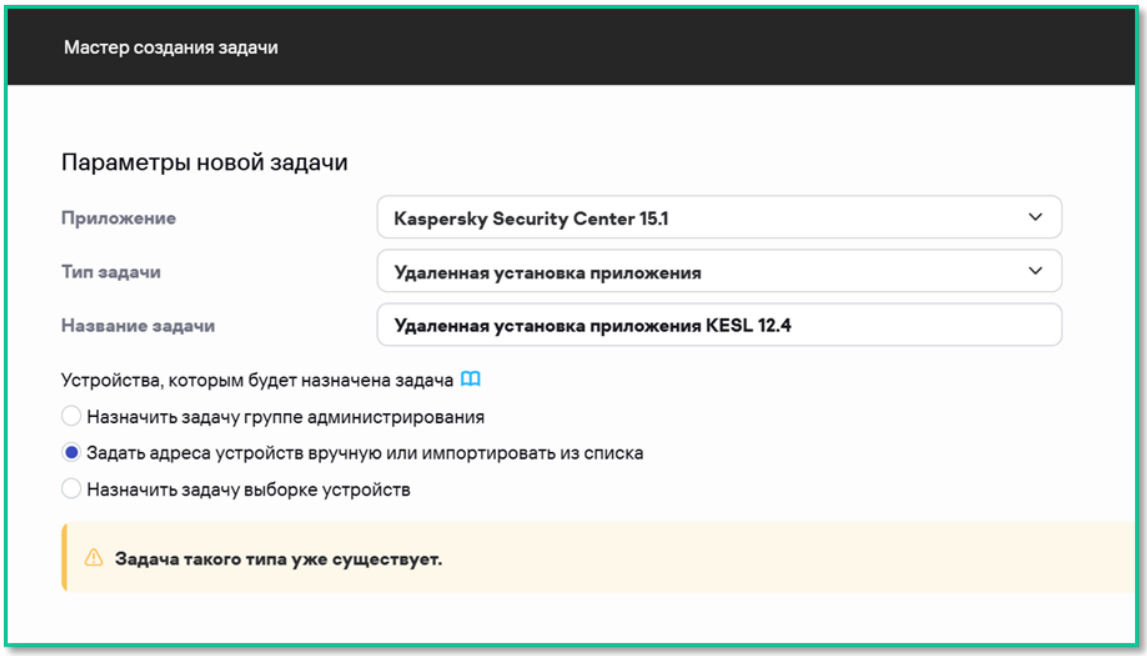
# 2.2. ???????? ?????? ????????? ?????????

1. Перейдите: **Устройства → Задачи → Добавить**

2. Выберите:

1. **Приложение**: `Kaspersky Security Center`
2. **Тип задачи**: `Удалённая установка программы`

3. Укажите устройства (вручную или из списка)

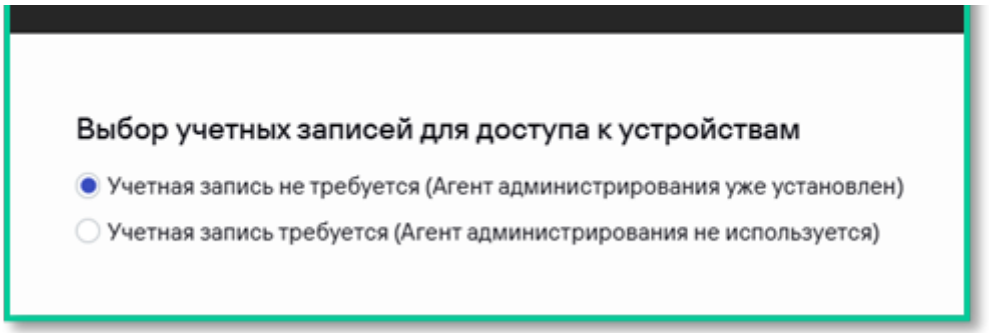



**Скриншот 2:** Удаленная установка программы

4. Выберите:

1. **Инсталляционный пакет**: `KESL 11.4+`
2. **Агент администрирования**: `KSC Agent`

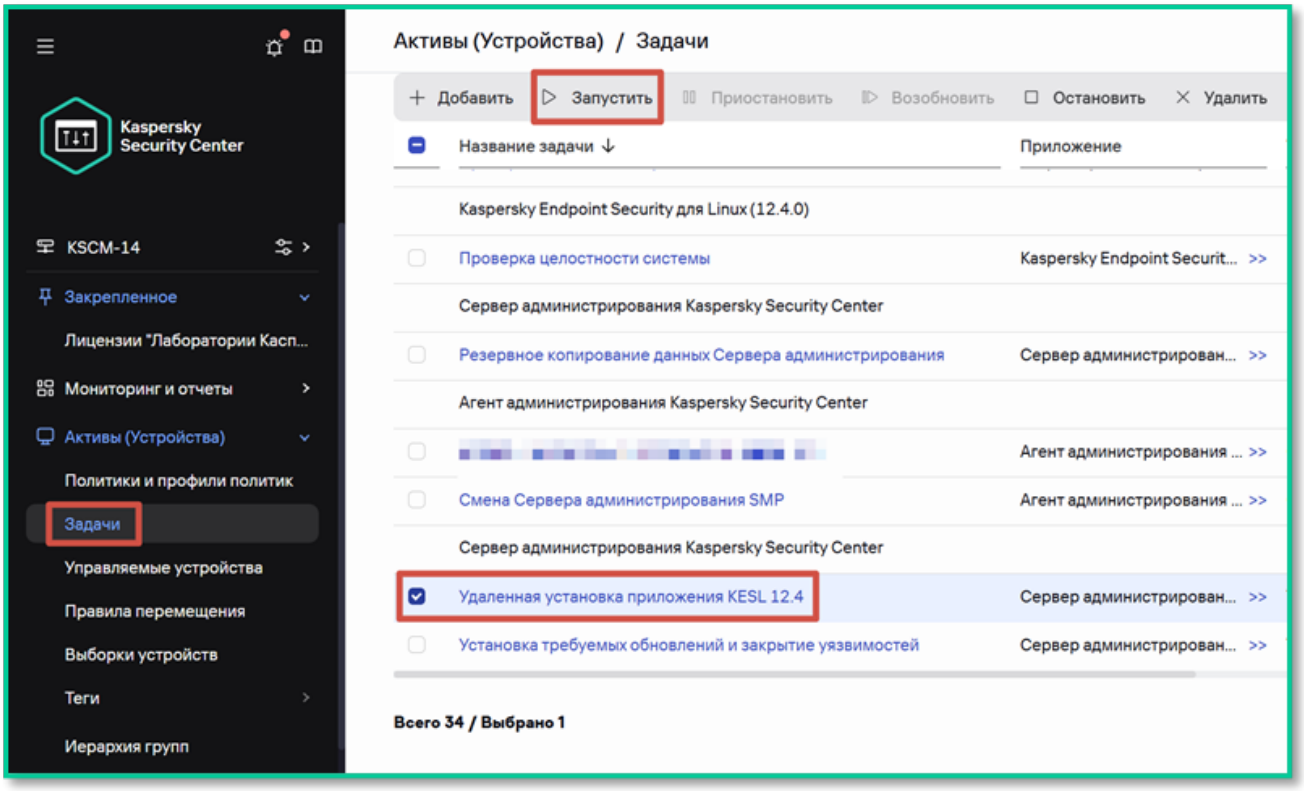
5. Если агент уже установлен — выберите: **«Учётная запись не требуется»**




**Скриншот 3:**

Учетная запись не требуется (Агент администрирования уже установлен)

6. Нажмите **«Готово» → «Запустить»**




**Скриншот 4:** После создания она автоматически переходит в состояние ожидания, поэтому её необходимо запустить вручную.

---

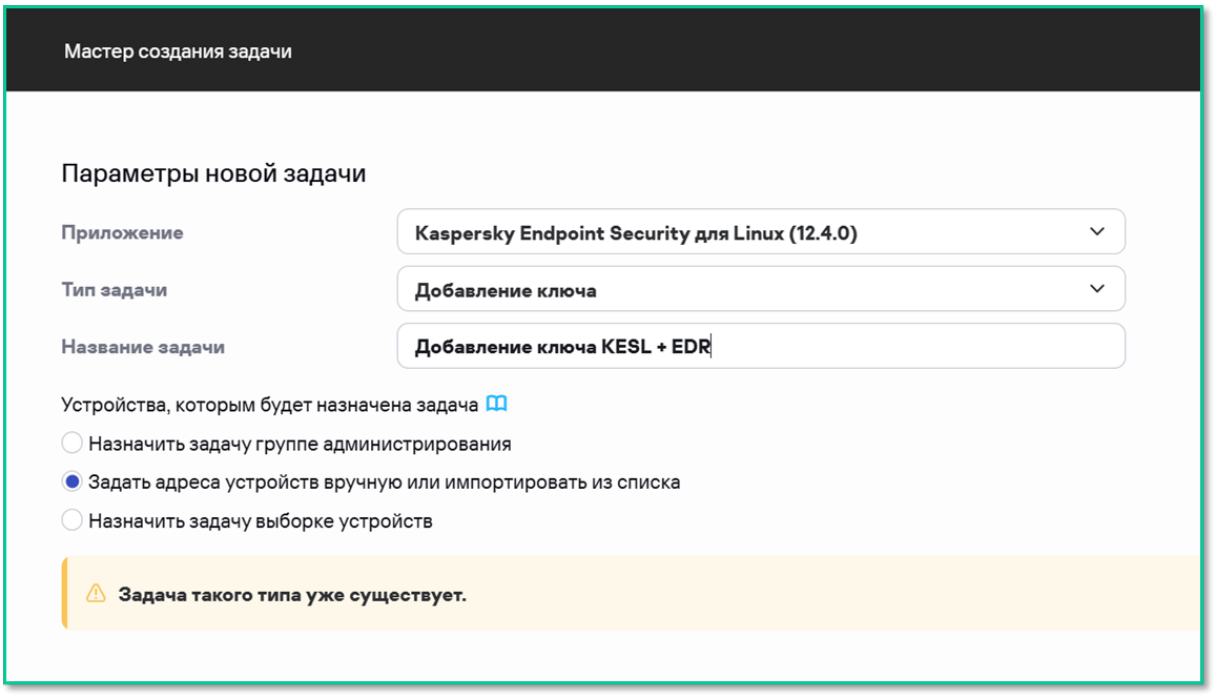
# 2.3. ?????????? ????????

## ???????? KES + EDR:

**1. Устройства → Задачи → Добавить → Добавление ключа**

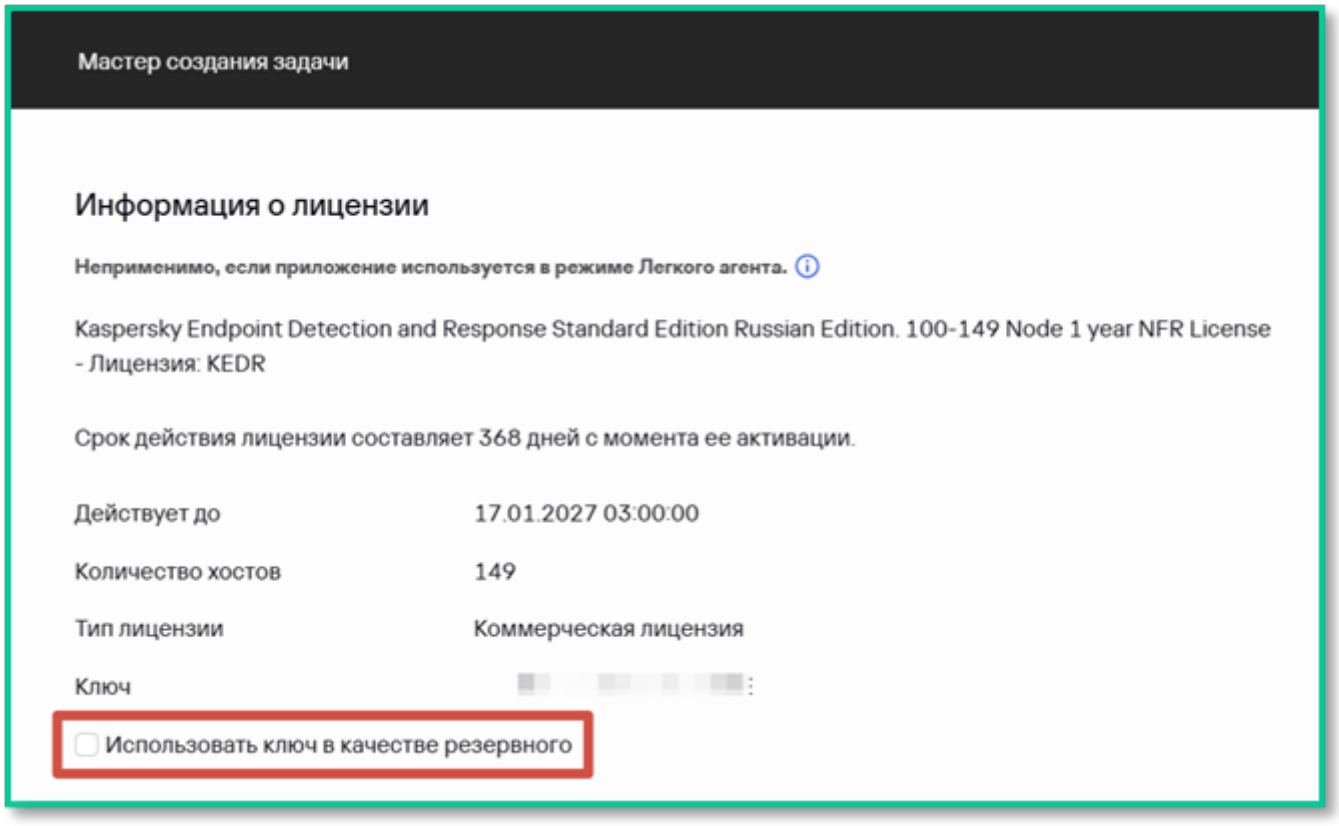
> Для интеграции с компонентами Kaspersky Anti Targeted Attack Platform вам нужно активировать решение Kaspersky Anti Targeted Attack Platform (см. подробнее в справке решения). Активировать компоненты приложения Kaspersky Endpoint Security, обеспечивающие интеграцию, не требуется, основные лицензии Kaspersky Endpoint Security включают в себя эту функциональность.

2. Выберите **KESL 11.4+**, укажите устройства




**Скриншот 5:** Добавление ключа KESL

3. Выберите файл ключа → **снимите галочку «Использовать как резервный»**



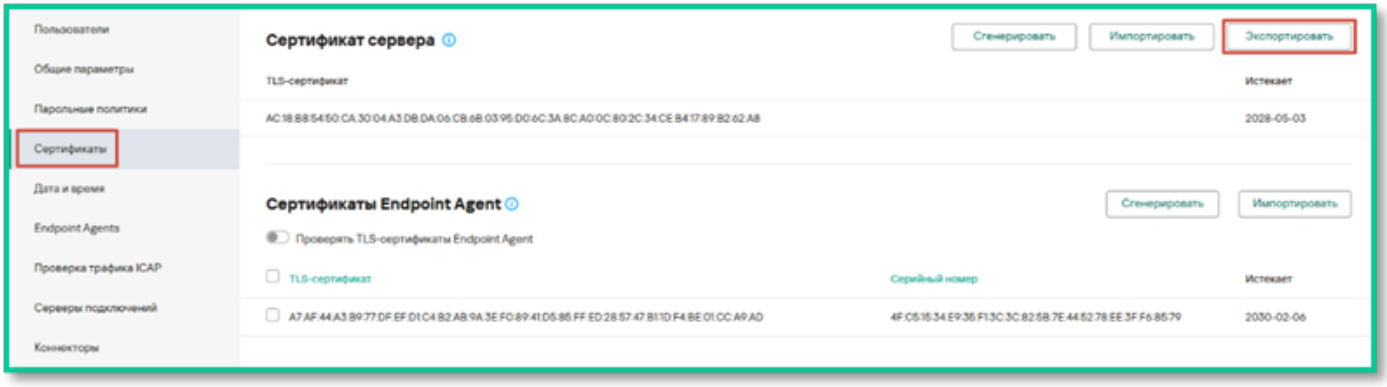

**Скриншот 6:** Использовать ключ в качестве резервного

### 3. Интеграция с Central Node KATA

# 4.1. ?????????? TLS-??????????? ?? KATA

1. Войдите в **KATA Web Console (администратор)**

2. Перейдите: **Активы → Endpoint Agents**



**Скриншот 7:** разделе **«Сертификат сервера»** нажимаем **«Экспортировать».**

3. Будет экспортирован файл `.crt`

---

# 4.2. ????????? ????????

**1. Устройства → Политики → Добавить → KESL 11.4+**

2. В мастере выберите необходимый **режим**

3. Перейдите: **Параметры приложения → Detection and Response → Endpoint Detection and Response (KATA)**

> **Начиная с версии Kaspersky Endpoint Security 12.4 для Linux компонент Endpoint Detection and Response (KATA) переименован в Endpoint Detection and Response Expert (on-premise). Теперь этот компонент обеспечивает интеграцию не только с Kaspersky Endpoint Detection and Response (KATA), компонентом Kaspersky Anti Targeted Attack Platform, но и с решением Kaspersky Endpoint Detection and Response Expert (on-premise).**

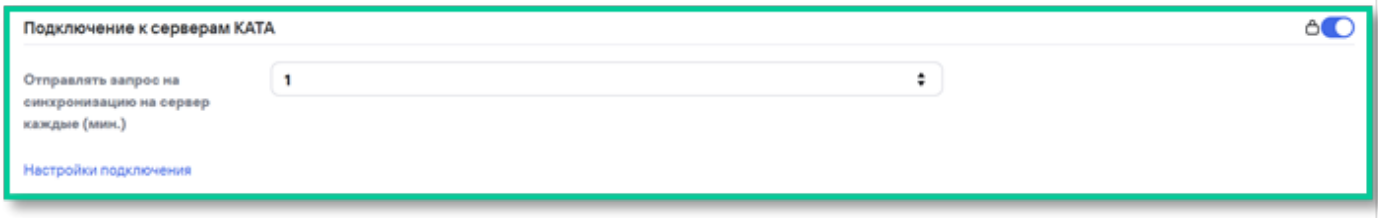
4. Включите компонент

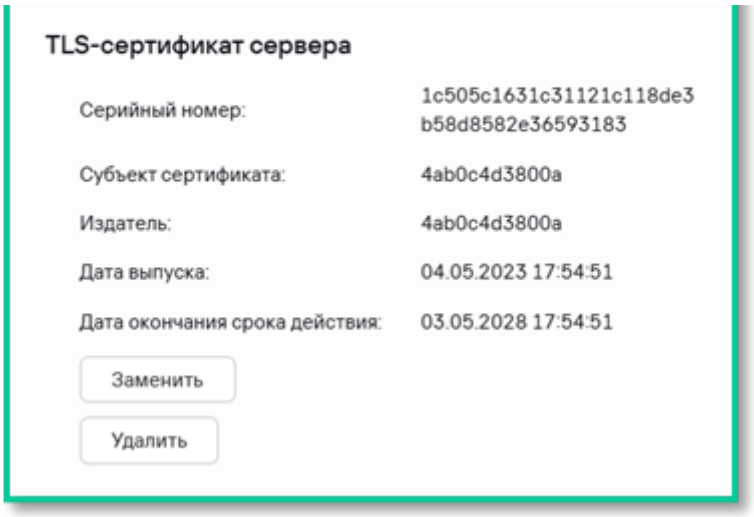
5. Включите **Запрет запуска**

6. Выбираем платформу для интеграции **Endpoint Detection and Response Expert (версия 7.1 и ниже)**

5. Нажмите **«Настройки подключения»**

- Загрузите **TLS-сертификат**






**Скриншот 8:** добавляем

сертификат сервера TLS выгруженный из Central Node,

- Укажите **адрес Central Node** и **порт 443**


**Скриншот 9:** указываем адрес сервера KATA и порт

6. Нажмите **«Сохранить»**

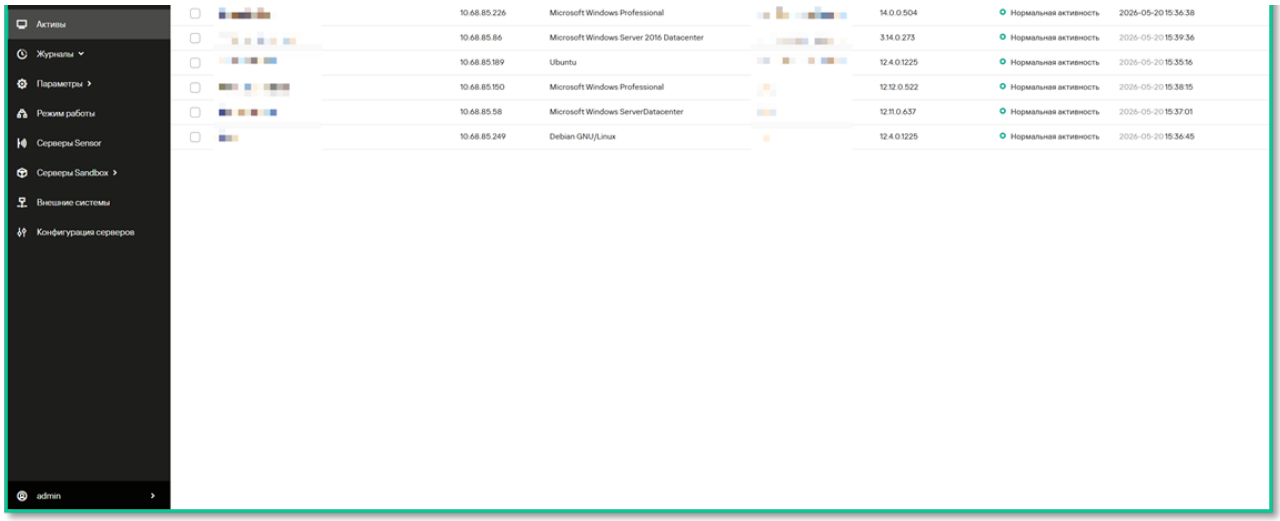
---

**5. Проверка интеграции**

# 5.1. ?????????????? ?? Central Node

1. Войдите в **KATA Web Console (администратор)**

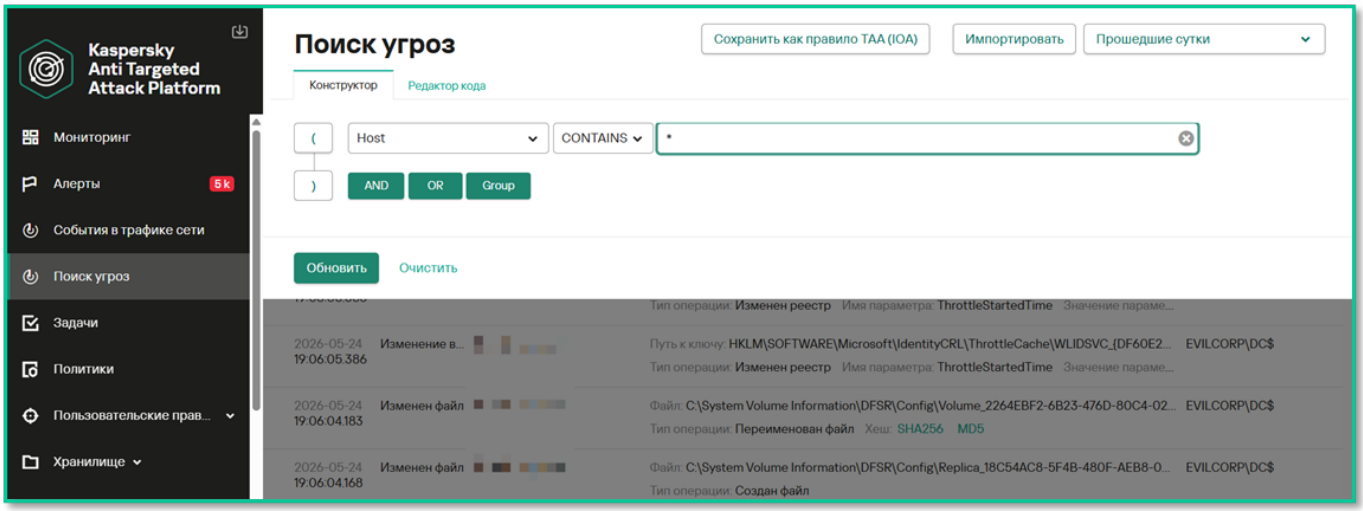
2. Перейдите: **Активы**




**Скриншот 10:** разделе **«Endpoint Agents»** начнут появляться **«Агенты»** со статусом **« Нормальная активность».**

3. Войдите в **KATA Web Console (Под аналитиком)**

4. Перейдите в раздел «**Поиск угроз**». В конструкторе выберите тип событий **Host** вместо **EventType**, укажите значение * и нажмите «**Найти**». Это выведет все события от всех устройств, подключенных к системе с EDR.




**Скриншот 11:** разделе **«Поиск угроз»** вывод собранной телеметрии с EDR агентов**.**

---

# 5.2. ?? ??????? ??????? (??????)

1. Откройте клиент и используйте команду **kesl-control --app-info**

```
root@[redacted]-machine:/home/test-lena# kesl-control --app-info
Название:                                                       Kaspersky Endpoint Security 12.4 для Linux
Версия:                                                         12.4.0.1225
Политика:                                                       Kaspersky Security Center

Информация о лицензии приложения:                               Ключ действителен
Дата окончания срока действия лицензии Kaspersky Endpoint Security:  2027-04-24 00:00:00
Статус файла MDR BLOB:                                          Не загружен

Состояние резервного хранилища:                                 Наиболее старый объект будет удален 2026-06-04 17:30:33
Использование резервного хранилища:                             Заполнено 0% резервного хранилища

Дата последнего запуска задачи Scan_My_Computer:                Никогда не запускалась

Дата последнего выпуска баз приложения:                         2026-06-15 13:48:00
Базы приложения загружены:                                      Да

Состояние обновляемого модуля ядра:                             Запущен

Использование Kaspersky Security Network:                       Выключено

Инфраструктура Kaspersky Security Network:                      Kaspersky Security Network

Интеграция с Kaspersky Managed Detection and Response:          Выключена

Интеграция с Kaspersky Endpoint Detection and Response Optimum: Не поддерживается лицензией

Защита от файловых угроз:                                       Задача доступна и выполняется

Мониторинг контейнеров:                                         Недоступно из-за ограничений лицензии

Контроль целостности системы:                                   Недоступно из-за ограничений лицензии

Управление сетевым экраном:                                     Задача доступна и не выполняется

Защита от шифрования:                                           Задача доступна и не выполняется

Защита от веб-угроз:                                            Задача доступна и не выполняется

Контроль устройств:                                             Задача доступна и не выполняется

Проверка съемных дисков:                                        Задача доступна и не выполняется

Защита от атак BadUSB:                                          Задача доступна и выполняется

Защита от сетевых угроз:                                        Задача доступна и не выполняется

Анализ поведения:                                               Задача доступна и выполняется

Контроль приложений:                                            Задача доступна и не выполняется

Веб-Контроль:                                                   Задача доступна и не выполняется

Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise): Задача доступна и выполняется

Интеграция с Sandbox:                                           Задача доступна и выполняется

Интеграция с Kaspersky Unified Monitoring and Analysis Platform: Недоступно из-за ограничений лицензии

Интеграция с Kaspersky Network Detection and Response (KATA):   Задача доступна и выполняется

Защита от почтовых угроз:                                       Задача доступна и выполняется

Действия после обновления:                                      Модуль приложения обновлен. Перезапустите приложение.

root@testlena-virtual-machine:/home/test-lena#
```

**Скриншот 12:** результаты вывода команды «**kesl-control**» со статусом подключения EDR агента**.**

2. В свойствах устройства в Web Console (Активы (Устройства) → Управляемые устройства → ссылка <имя устройства> → Приложения → ссылка <название приложения Kaspersky Endpoint Security> → Общие → Компоненты).

---

## ? ???????? ??????

- Kaspersky Tech на YouTube

- Kaspersky на Rutube

**Развёртывание KESL 11.4+ с EDR завершено!**
Теперь ваши конечные точки:

- Передают телеметрию в KATA
- Участвуют в расследовании инцидентов
- Поддерживают автоматическую корреляцию с сетевыми событиями

---

Revision #18
Created 13 June 2026 12:00:16 by Николай
Updated 15 June 2026 15:42:29 by Николай