??????? ????????? ? ????????? ??????????? Sandbox (OSMP) ?? ???? KES Linux

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

Версия решения: KESL 12.2+; KEDR (KATA) 4.0>7.1;

> **ВАЖНО:**
> **В этой инструкции мы 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 Sandbox, так как он уже входит в состав установленного решения и для его активации необходимо включить использование его в политике и настроить интеграцию.

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	12.2+

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 12.2+ с EDR через KSC Web Console

2.1. ????????? ???????????????? ??????

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

2. Найдите пакет **KESL 12.2+**

3.Перейдите в **Параметры**

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

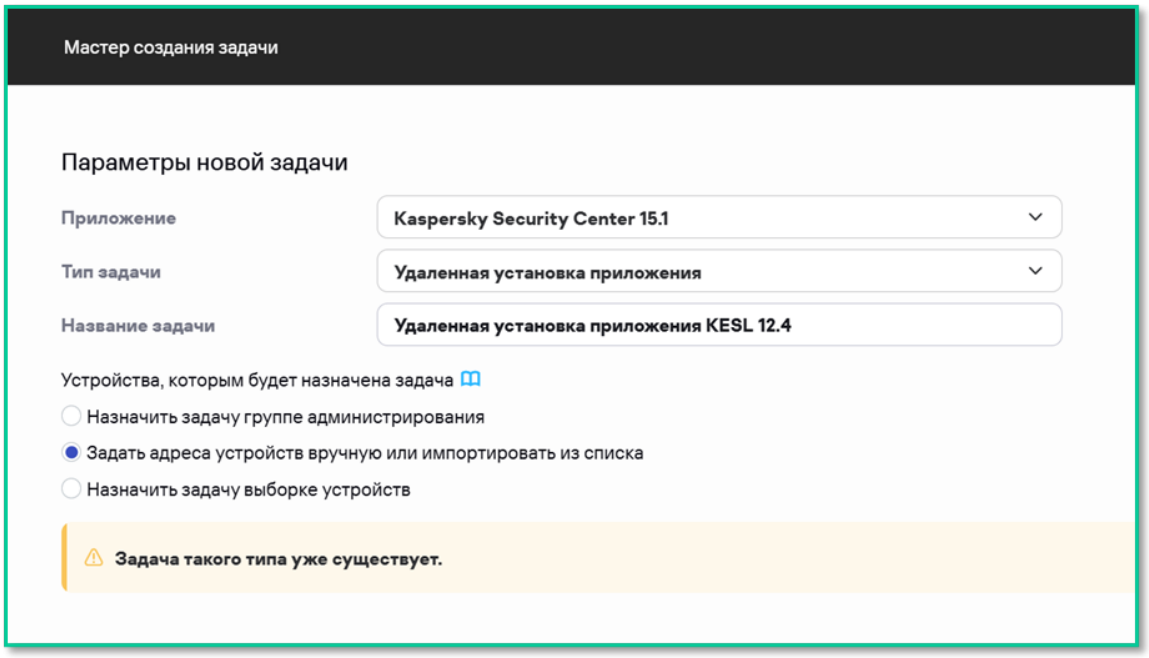
2.2. ???????? ?????? ????????? ?????????

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)

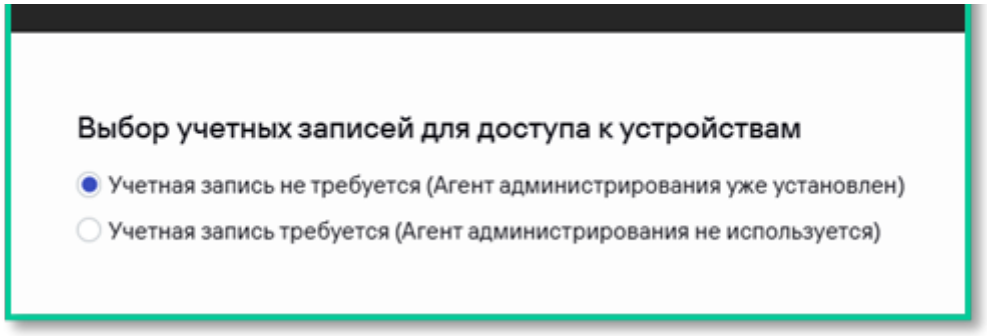


Скриншот 1: Удаленная установка программы

4. Выберите:

1. **Инсталляционный пакет**: `KESL 12.2+`
2. **Агент администрирования**: `KSC Agent`

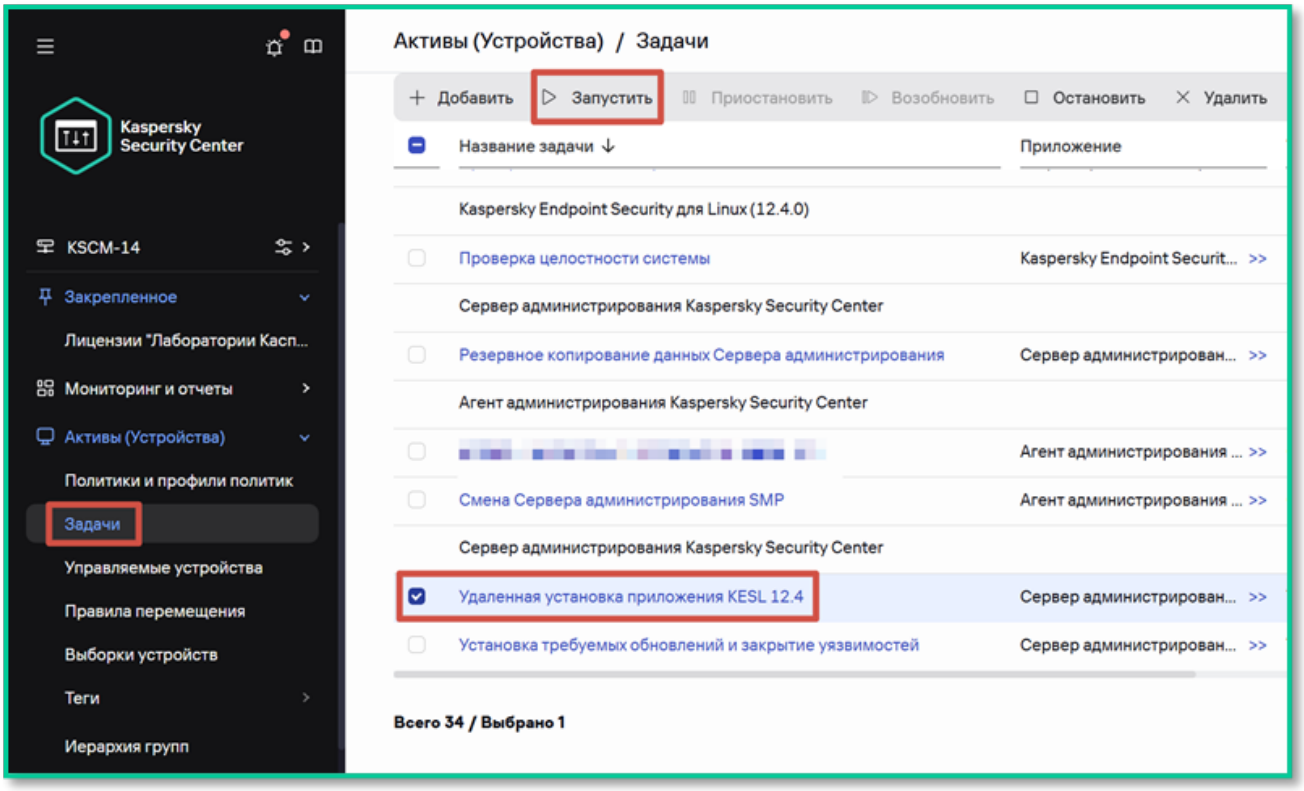
5. Если агент уже установлен — выберите: **«Учётная запись не требуется»**



Скриншот 2:

Учетная запись не требуется (Агент администрирования уже установлен)

6. Нажмите **«Готово» → «Запустить»**



Скриншот 3: После создания она автоматически переходит в состояние ожидания, поэтому её необходимо запустить вручную.

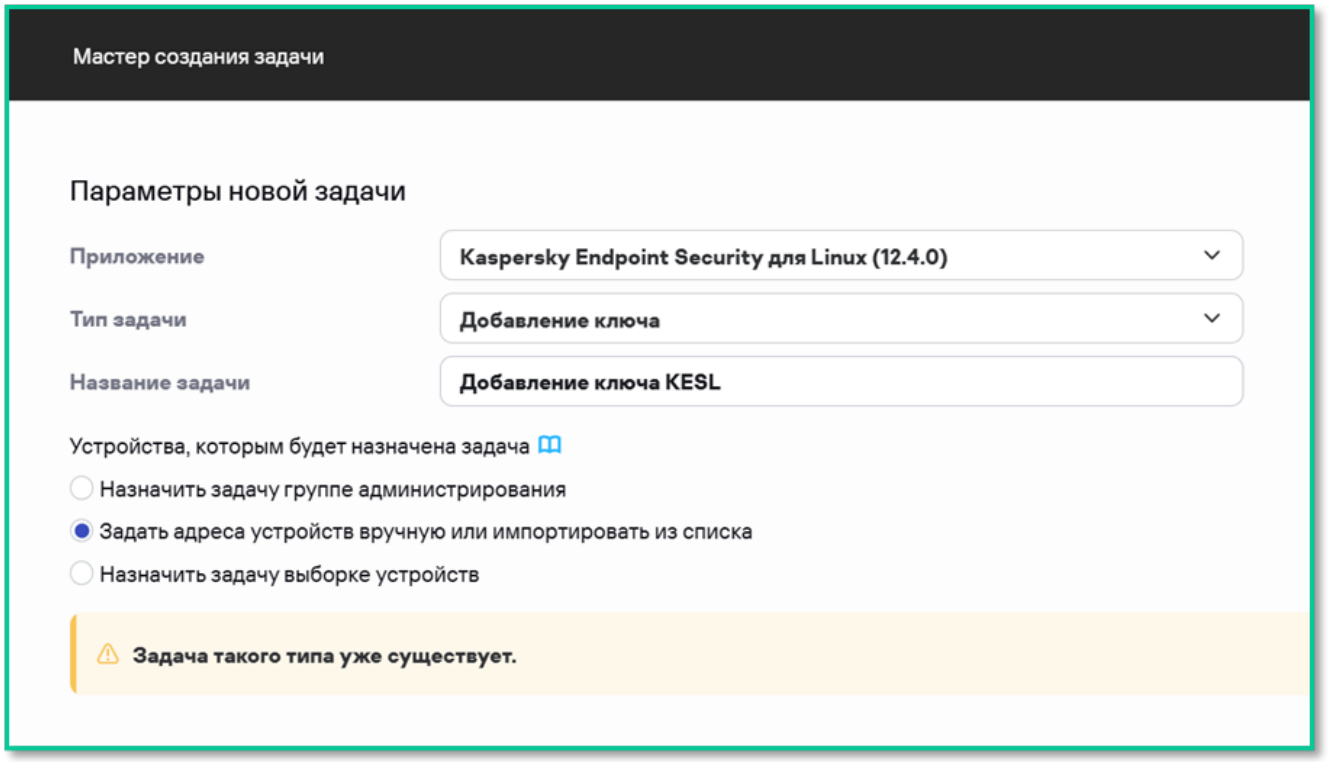
2.3. ?????????? ????????

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

1. Устройства → Задачи → Добавить → Добавление ключа

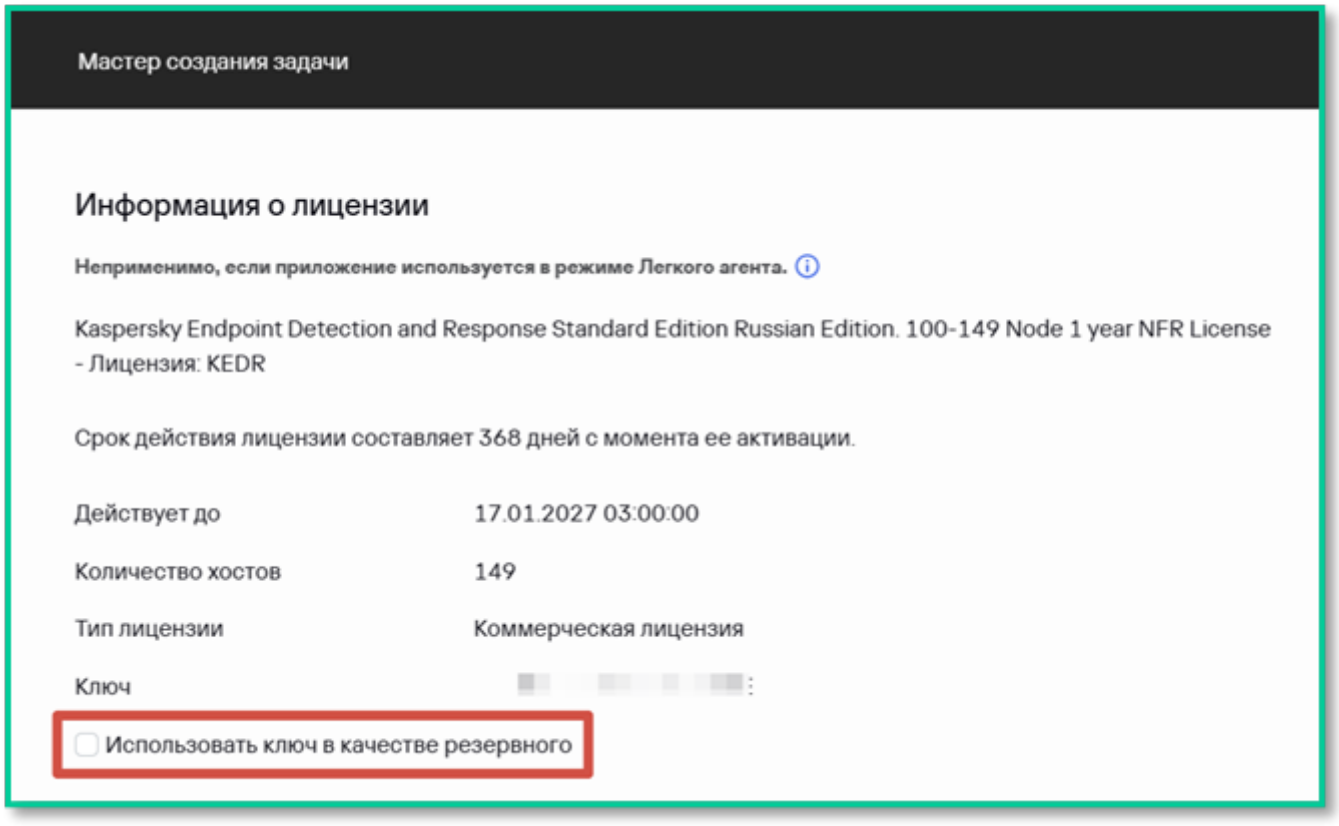
> Для интеграции с компонентами Kaspersky Anti Targeted Attack Platform вам нужно активировать решение Kaspersky Anti Targeted Attack Platform (см. подробнее в справке решения). Активировать компоненты приложения Kaspersky Endpoint Security, обеспечивающие интеграцию, не требуется, основные лицензии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

2. Выберите **KESL 12.2+**, укажите устройства



Скриншот 4: Добавление ключа KESL

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



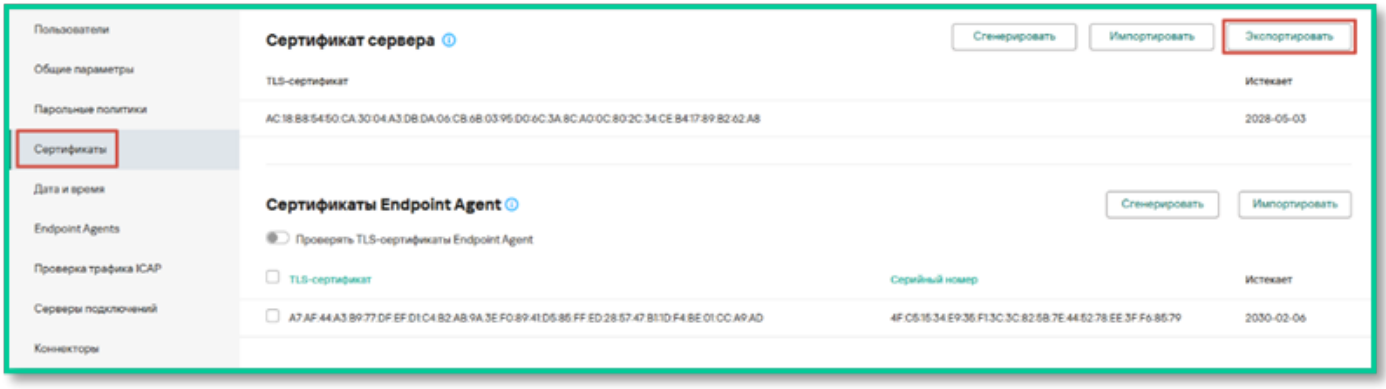
Скриншот 5: Использовать ключ в качестве резервного

3. Интеграция с Central Node KATA

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

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

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



Скриншот 6: разделе **«Сертификат сервера»** нажимаем **«Экспортировать».**

3. Будет экспортирован файл `kata.crt`

4.2. ????????? ????????

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

2. В мастере выберите необходимый **режим**

3. Перейдите: **Параметры приложения → Detection and Response → Sandbox (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

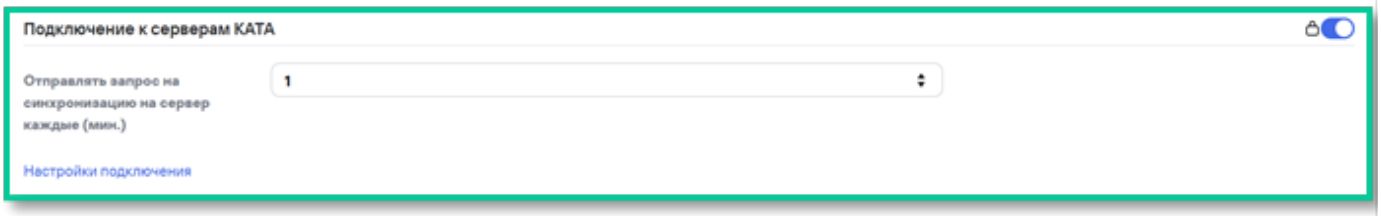
5. Выбираем Режим интеграции: **KATA Sandbox**

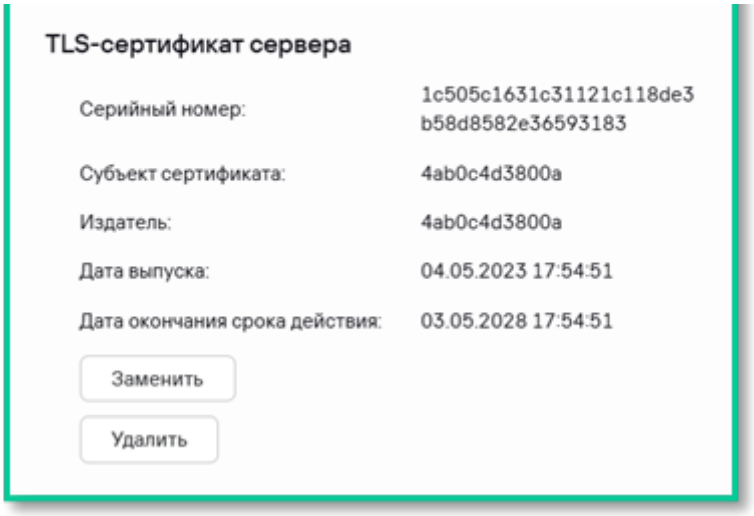
6. Выберите способ отправки файлов на проверку. Для версий KATA 7.0 и выше доступен только **ручной режим отправки**.

> Для работы KATA Sandbox в **ручном режиме** должно быть развернуто решение Kaspersky Anti Targeted Attack Platform версии 7.0 или выше. Для работы KATA Sandbox в **автоматическом режим** должно быть развернуто решение Kaspersky Anti Targeted Attack Platform версии 8.0 или выше.

7. Нажмите **«Настройки подключения»**

- Загрузите **TLS-сертификат**





Скриншот 7: добавляем

сертификат сервера TLS выгруженный из Central Node,

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

Скриншот 8: указываем адрес сервера KATA и порт

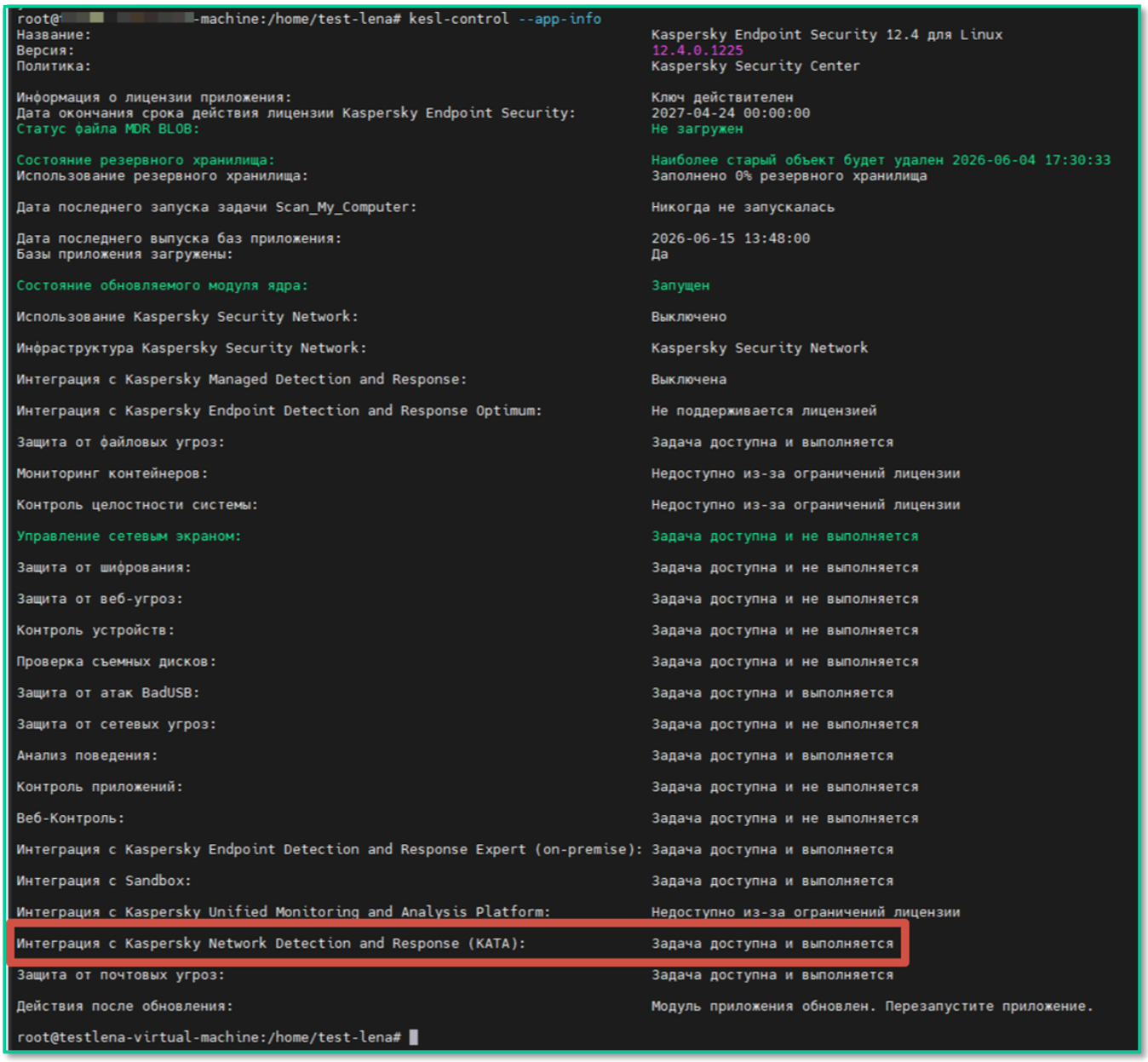
6. Нажмите **«Сохранить»**

---

5. Проверка интеграции

5.1. ?? ??????? ??????? (??????)

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



Скриншот 11: 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).

Полезные ссылки

- 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 #1
Created 15 June 2026 14:24:48 by Николай
Updated 15 June 2026 14:25:06 by Николай