??????? ????????? ? ????????? ??????????? NDR (KATA) ?? ???? KES Linux

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

Версия решения: KESL 12.2+; NDR (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 NDR, так как он уже входит в состав установленного решения и для его активации необходимо включить использование его в политике и настроить интеграцию.

---

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+NDR**

---

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

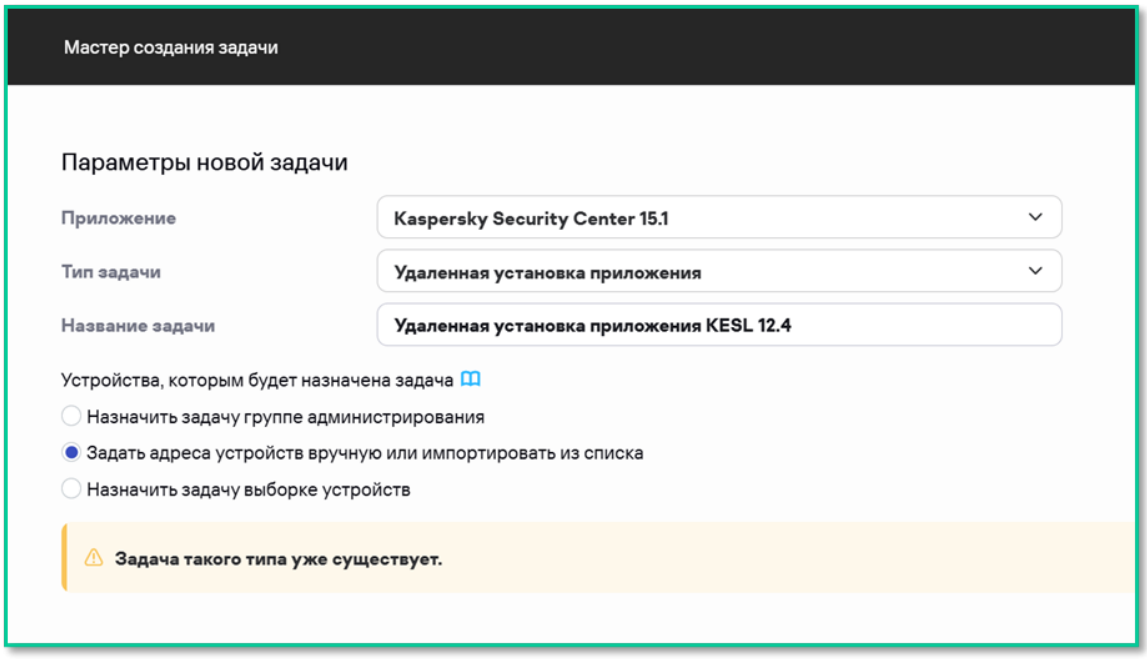
2.2. ???????? ?????? ????????? ?????????

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)

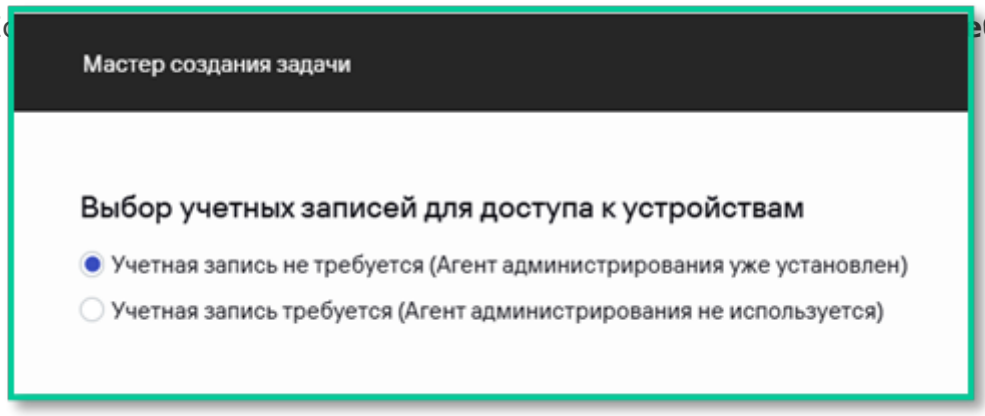


Скриншот 1: Удаленная установка программы

4. Выберите:

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

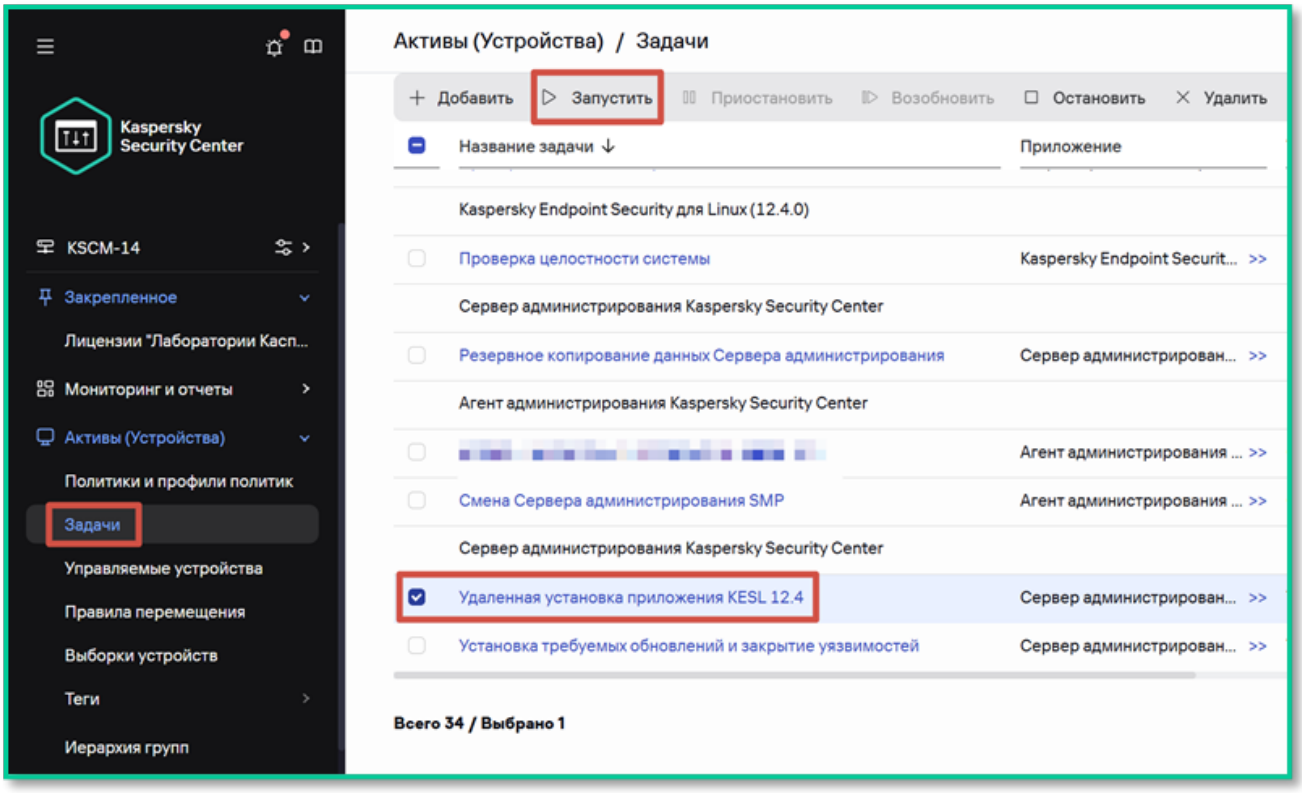
5. Ес **ебуется»**



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.

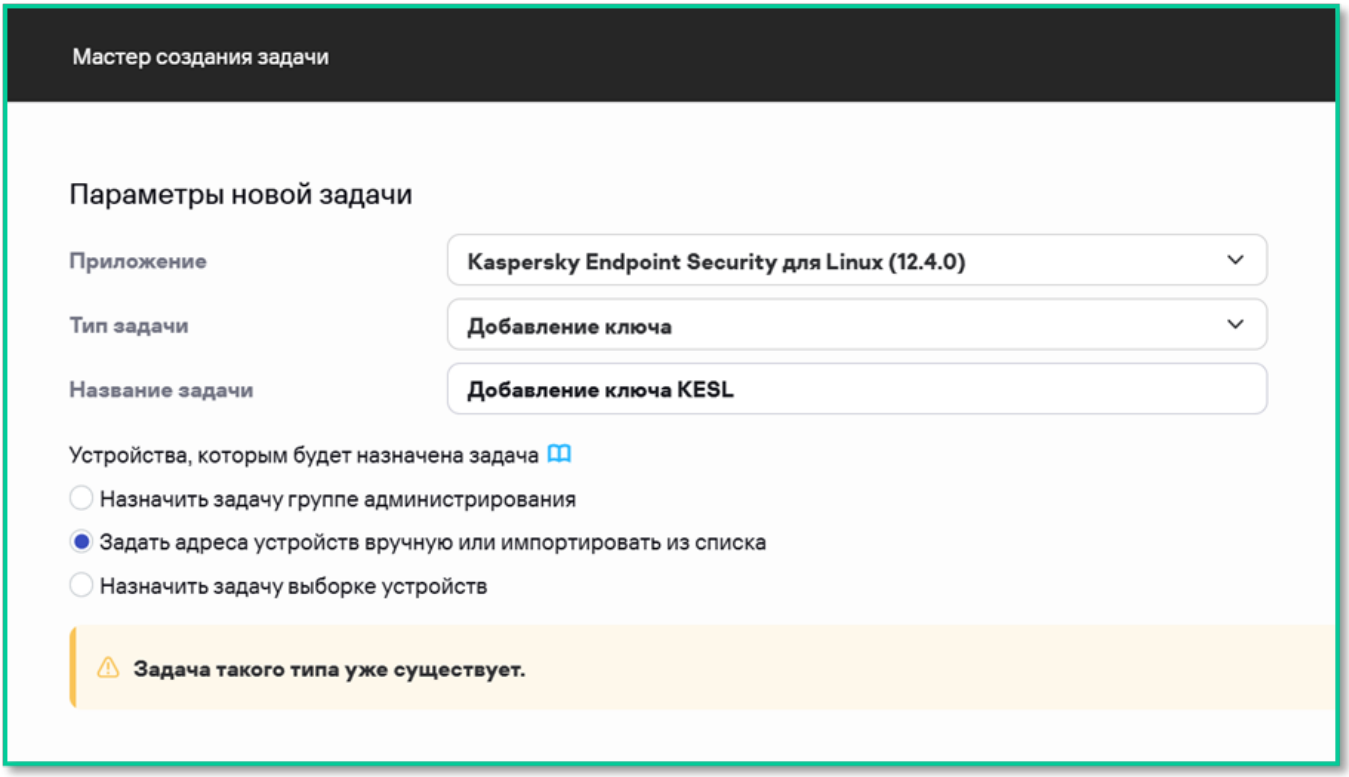
2.3. ?????????? ????????

???????? KES:

1. Устройства → Задачи → Добавить → Добавление ключа

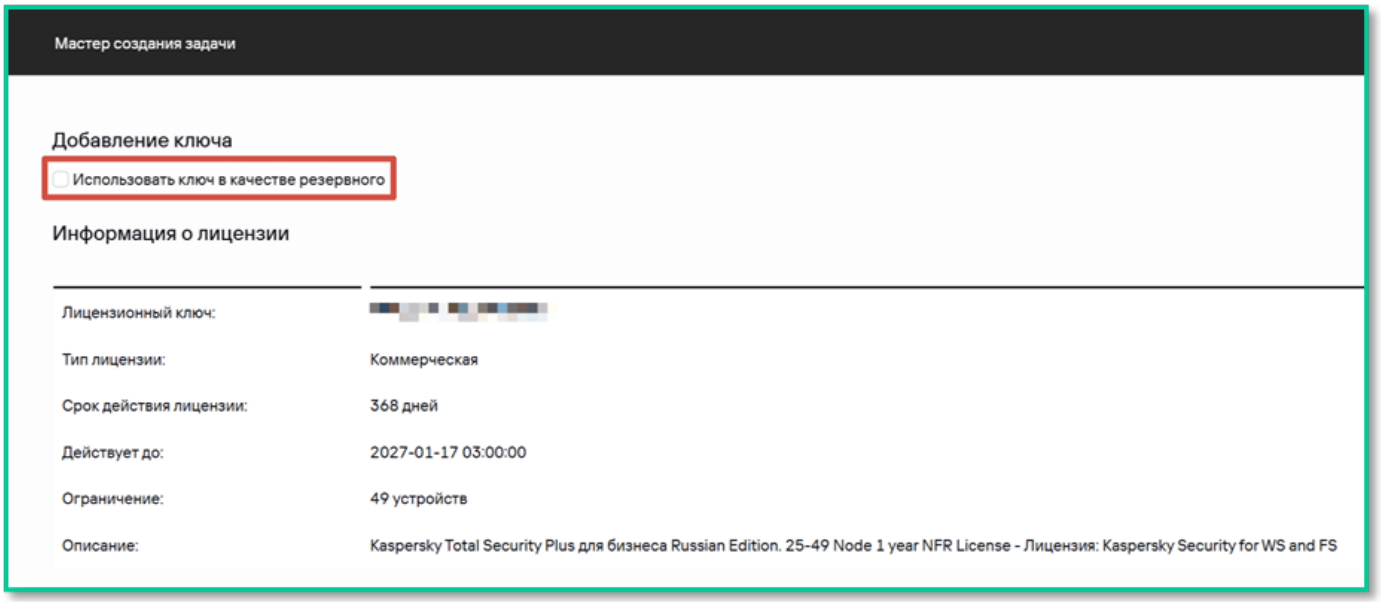
> Для интеграции с компонентами Kaspersky Anti Targeted Attack Platform вам нужно активировать решение Kaspersky Anti Targeted Attack Platform (см. подробнее в справке решения). Активировать компоненты приложения Kaspersky Endpoint Security, обеспечивающие интеграцию, не требуется, основные лицензии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



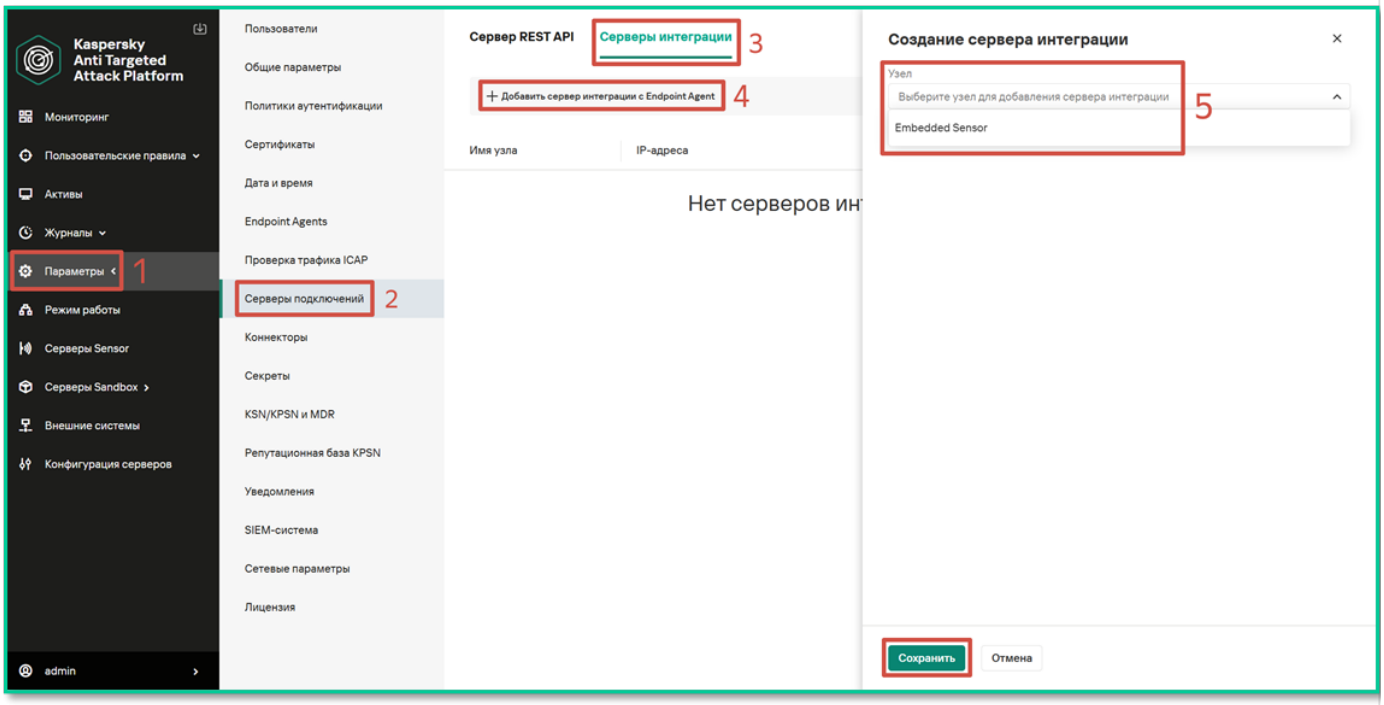
Скриншот 5: Использовать ключ в качестве резервного

3. Интеграция с Central Node KATA

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

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

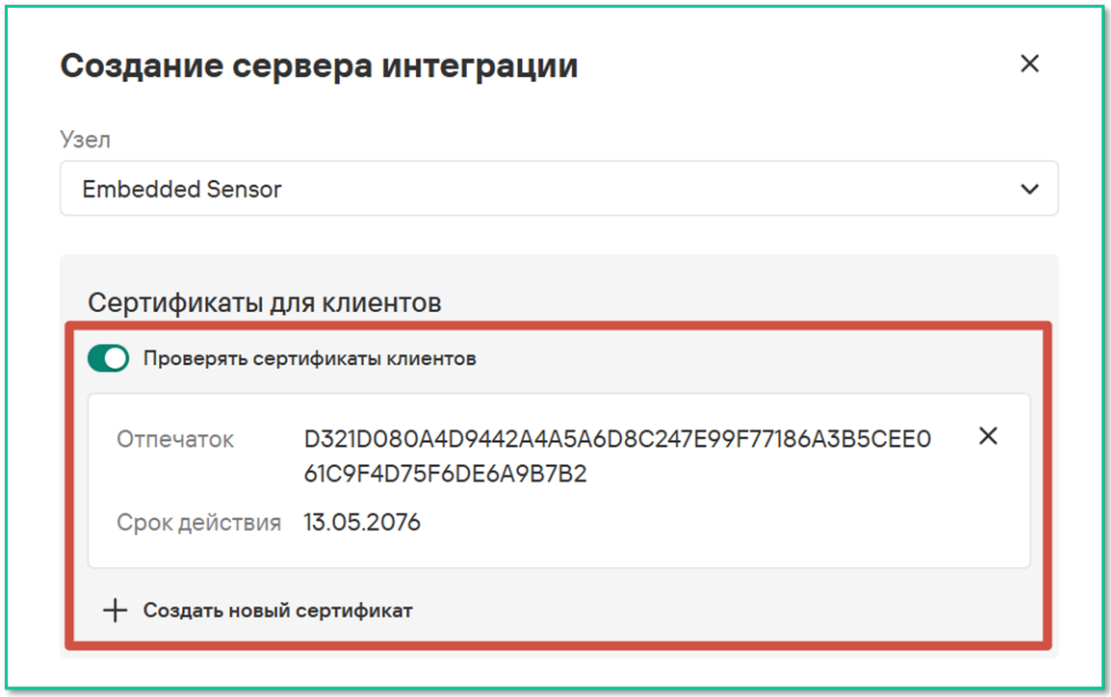
2. Перейдите: **Параметры → Серверы подключений → Серверы интеграции**



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

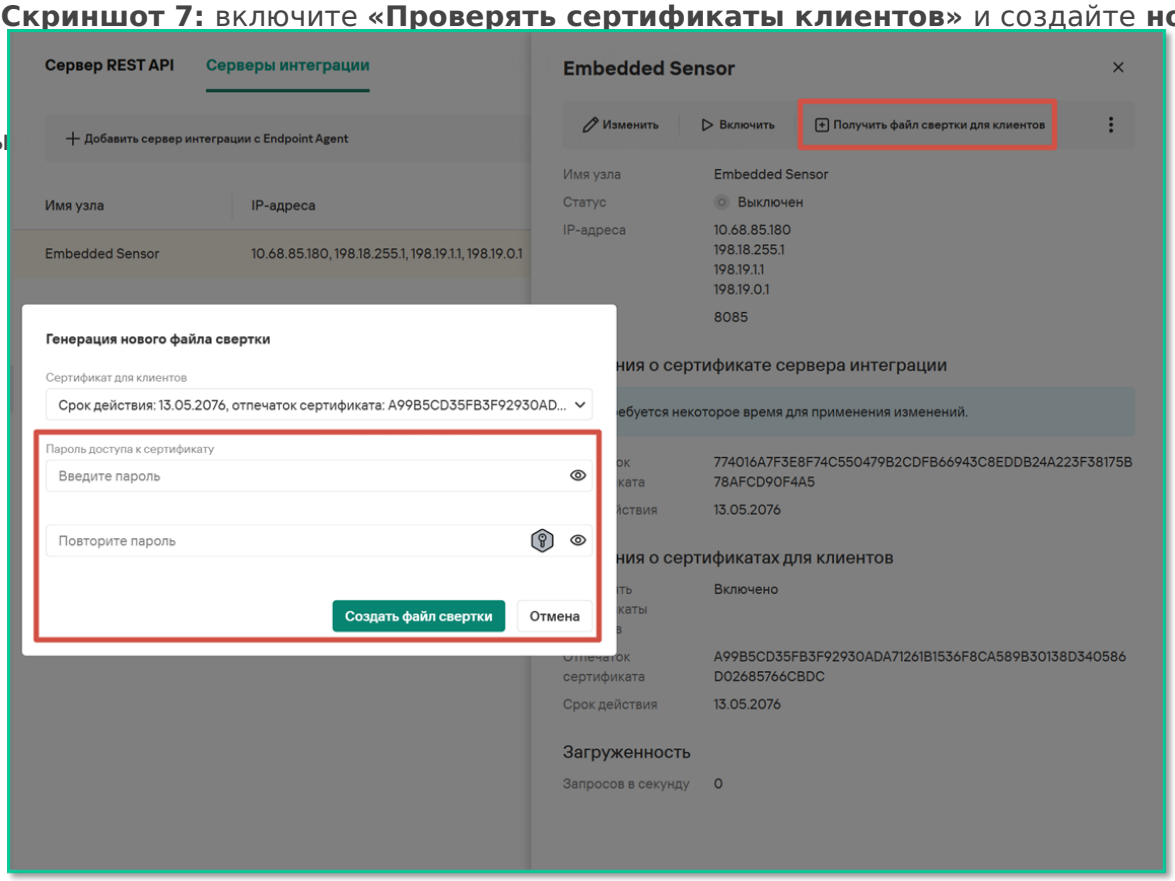
3. Нажмите **Добавить сервер интеграции с Endpoint Agent**

4. Выберите узел для добавления сервера интеграции. Это может быть как встроенный Embeded Sensor, так и внешний узел, установленный с ролью Sensor.



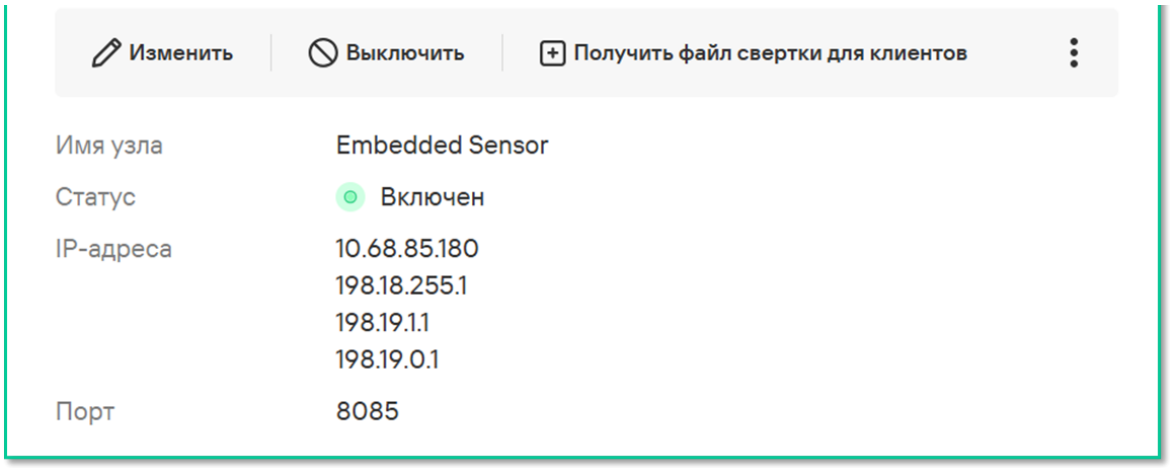
Скриншот 7: включите «**Проверять сертификаты клиентов**» и создайте **новый**

5. Вы



Скриншот 8: Будет выгружен архив с сертификатами**.**

6. Включить сервер интеграции.



Скриншот 9: сервер включен**.**

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

1. Устройства → Политики → Добавить → KESL 12.2+

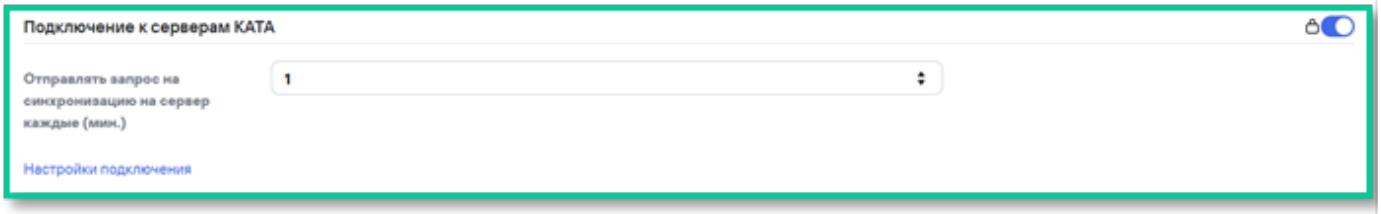
2. В мастере выберите **стандартный режим**

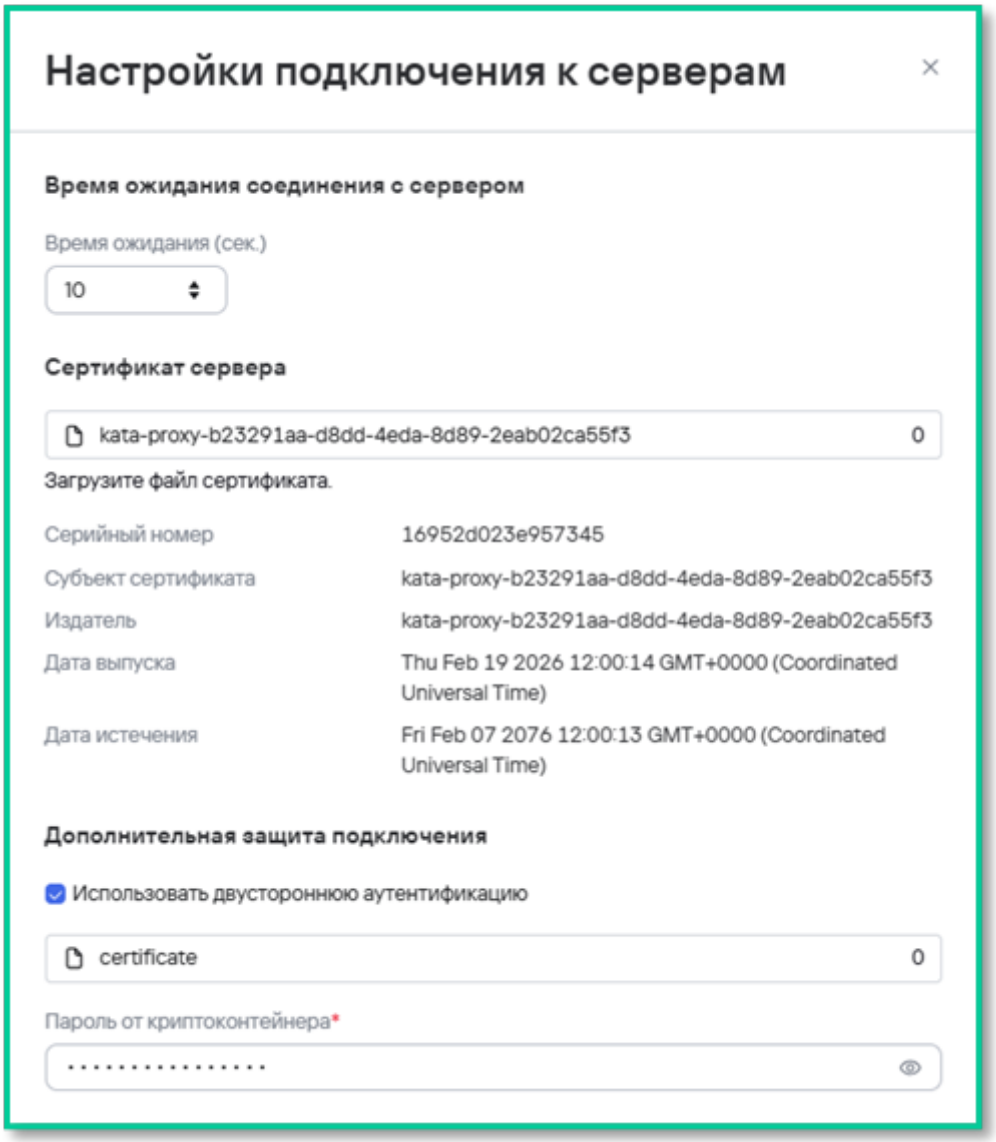
3. Перейдите: **Параметры приложения → Detection and Response → Network Detection and Response (KATA)**

4. Включите компонент

5. Нажмите **«Настройки подключения»**

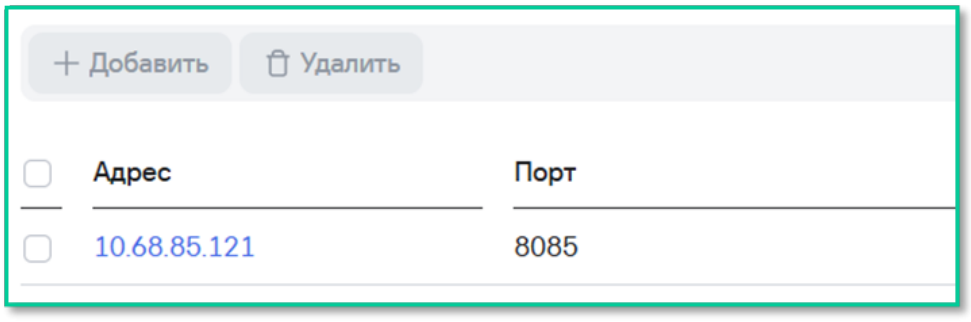
- Загрузите **TLS-сертификат**





Скриншот 10: добавляем сертификат сервера TLS выгруженный из Central Node,

- Укажите **адрес Central Node** и **порт 8085**



Скриншот 11: указываем адрес сервера KATA и порт

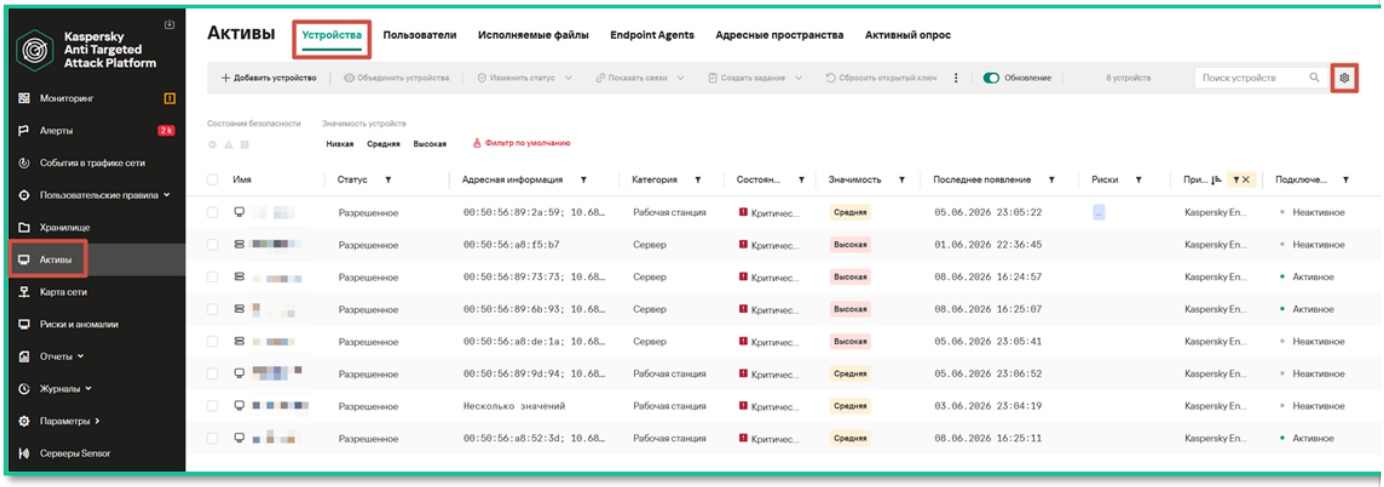
6. Нажмите **«Сохранить»**

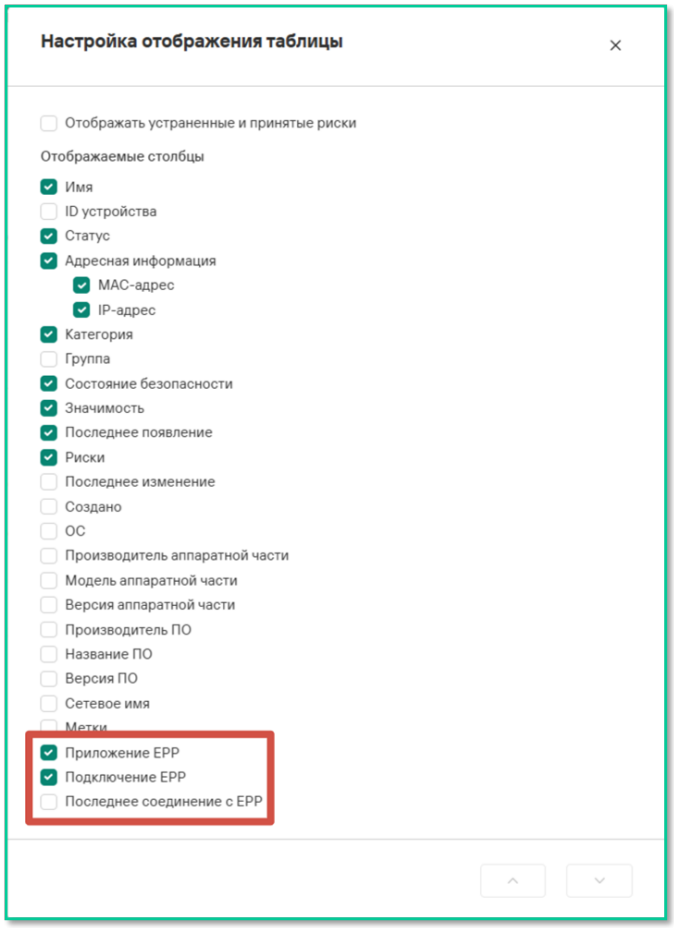
5. Проверка интеграции

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

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

2. Перейдите:

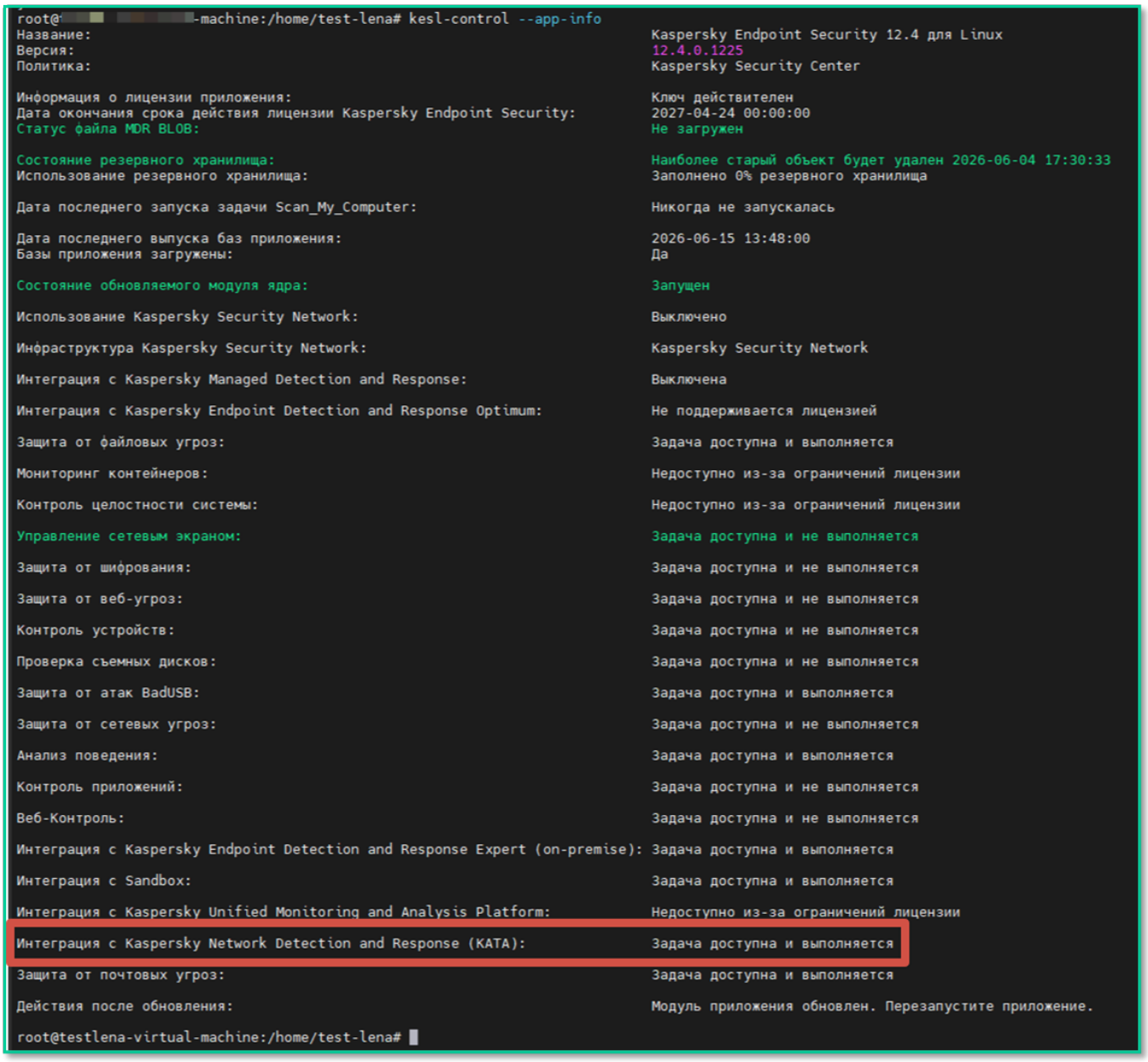




Скриншот 12: В разделе «**Активы → Устройства**» начнут появляться активы с установленными «**Агентами**», но для фильтрации и отображения только устройств с установленным агентом необходимо добавить дополнительные поля, перейдя в настройку в правом верхнем углу, нажав на шестеренку.

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

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



Скриншот 13: результаты вывода команды «**kesl-control**» со статусом подключения NDR 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 NDR завершено!

Теперь ваши конечные точки:

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

Revision #14
Created 13 June 2026 12:01:10 by Николай
Updated 29 June 2026 12:18:45 by Николай