

Как включить EDR (KATA) в KES Mac

В этой инструкции мы рассмотрим, как включить EDR (KATA) в KES Mac.

Версия решения: KES for Mac 12+; KEDR (KATA) 6.0>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 и KES Linux, KES for Mac требует только чистую установку или переустановку для включения компонента EDR.

Начиная с версии **Kaspersky Endpoint Security 12.2.1 for Mac** 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).

1. Подготовка	
1.1. Проверка версии KES Mac	
Компонент	Минимальная версия

1.2. Требования к оборудованию (?? ????????)

- **CPU**: тип процессора: Intel, Apple;
- **RAM**: ≥4 ГБ
- **HDD**: ≥5 ГБ свободного места

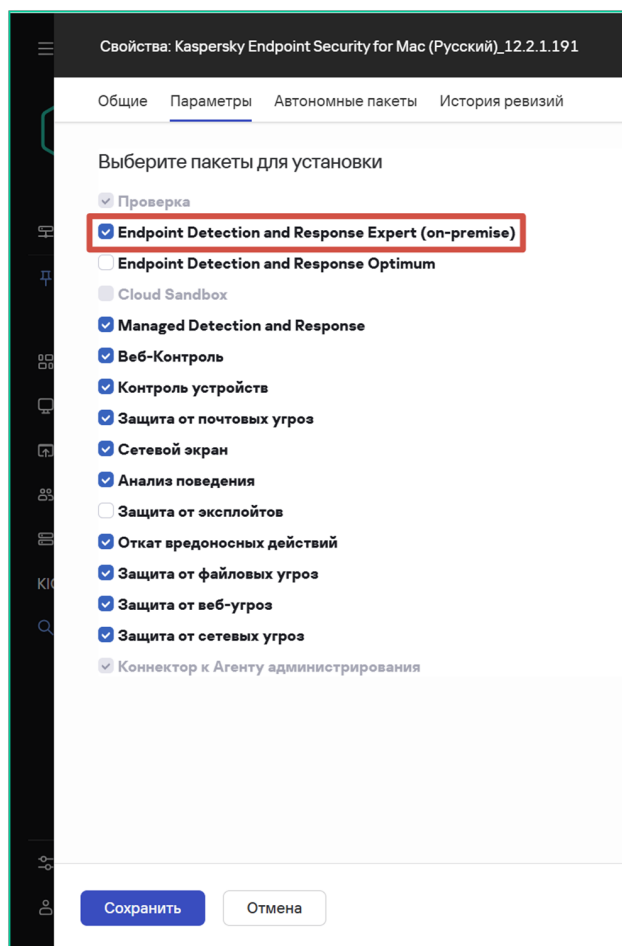
1.3. Требования к лицензиям

- Лицензия **KES**
- Лицензия **KEDR (KATA)**

2. Чистая установка KES for Mac 12+ с EDR через KSC Web Console

2.1. Требования к оборудованию и лицензиям

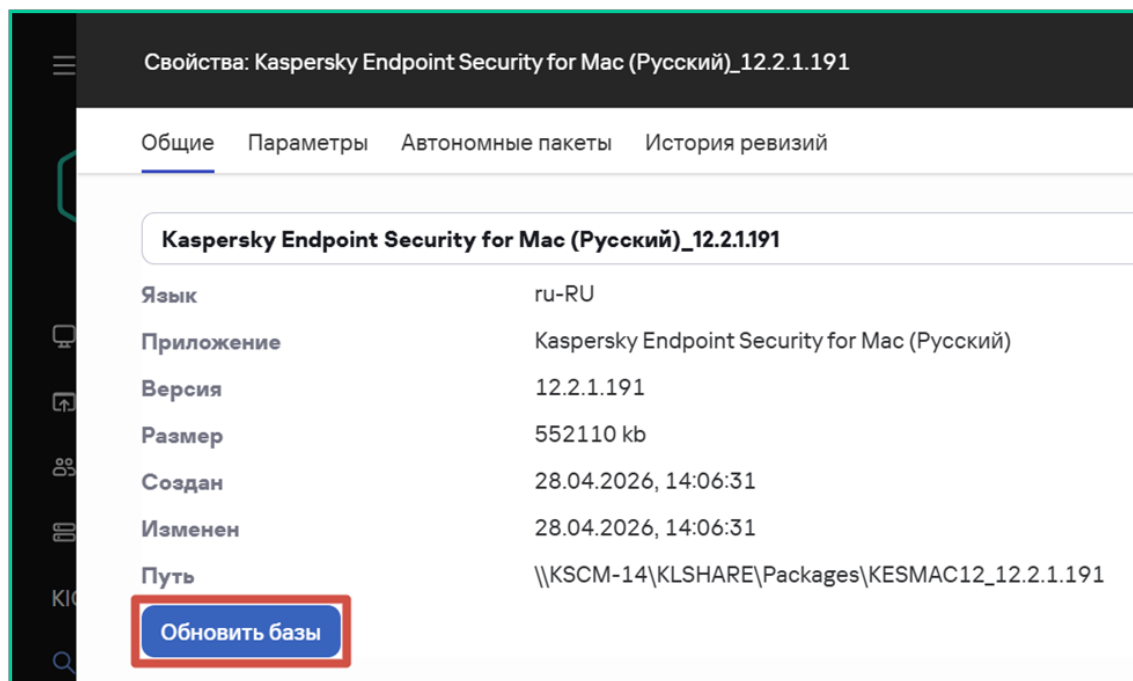
1. Откройте **KSC Web Console** → **Операции** → **Хранилища** → **Инсталляционные пакеты**
2. Найдите пакет **KES for Mac 12+**
3. Перейдите в **Параметры** и включите компонент **EDR**



❏ Скриншот 1: Выбор компонента Режимы работы KES for Mac 12+

4. Выполните дополнительные настройки в Консоли администрирования с детальным описанием можно ознакомиться в [онлайн-документации](#)

5. Нажмите «**Обновить базы**» → «**Сохранить**»



❏ Скриншот 4: Обновить базы

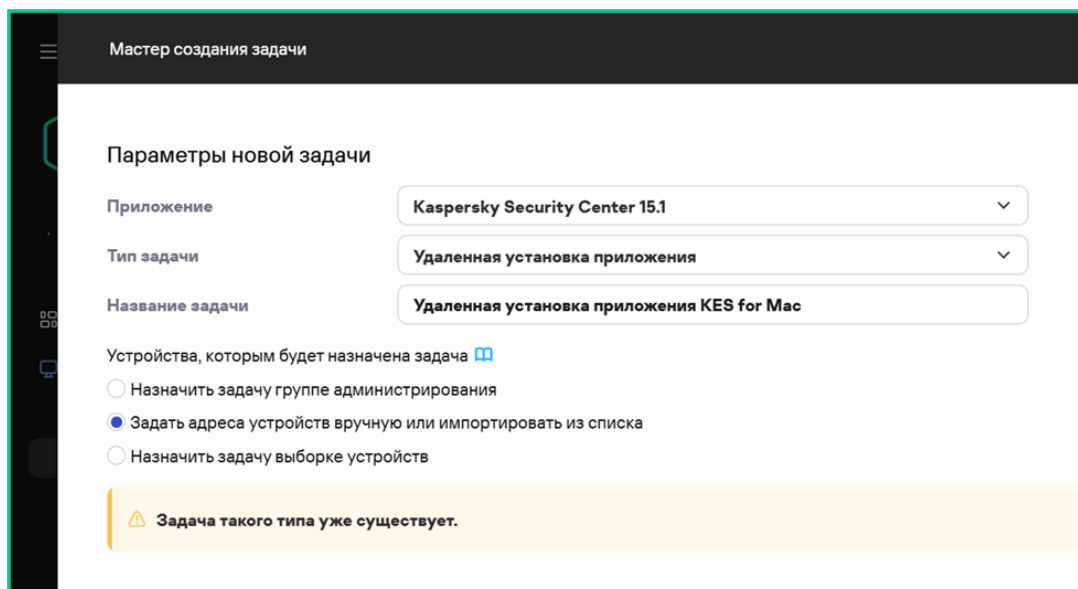
2.2. ?????????? ??????? ?????????????? ?????????????

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)

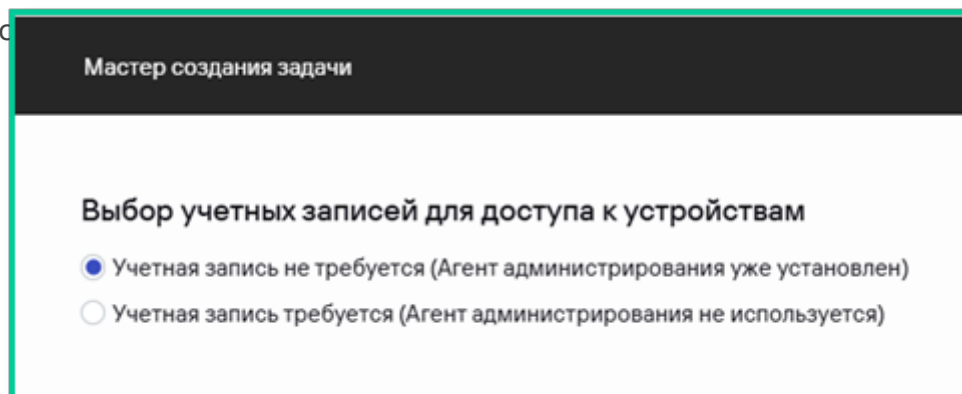


□□ Скриншот 2: Удаленная установка программы

4. Выберите:

1. **Инсталляционный пакет:** KES for MAC 12+
2. **Агент администрирования:** KSC_Agent

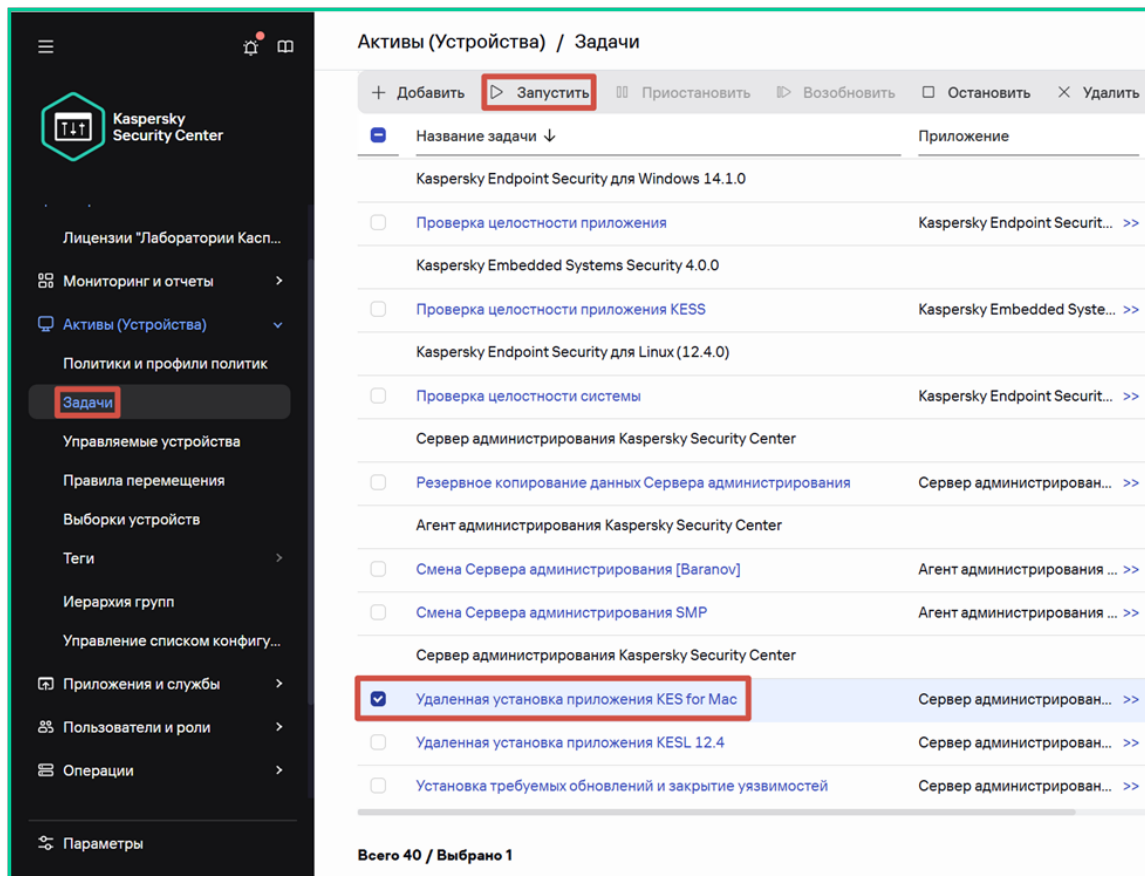
5. Если нажать «Далее» → «Готово» → «Запустить»



□□ 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. ?????????? ??????????

“ **Важно:** Добавьте **обе лицензии отдельно!**

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

1. Устройства → Задачи → Добавить → Добавление ключа

2. Выберите **KES for Mac 12+**, укажите устройства

Мастер создания задачи

Параметры новой задачи

Приложение: Kaspersky Endpoint Security для Mac (12.2.1)

Тип задачи: Добавление ключа

Название задачи: Добавление ключа KES for Mac

Устройства, которым будет назначена задача

- ☐ Назначить задачу группе администрирования
- ☒ Задать адреса устройств вручную или импортировать из списка
- ☐ Назначить задачу выборке устройств

❏ Скриншот 8: Добавление ключа KES for Mac

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

Мастер создания задачи

Kaspersky Total Security Plus для бизнеса Russian Edition. 25-49 Node 1 year NFR License - Лицензия: Kaspersky Security for WS and FS

- ✓ Защита
- ✓ Шифрование данных
- ⊗ Endpoint Detection and Response Expert (on-premise)
- ✓ Endpoint Detection and Response Optimum
- ✓ Защита от почтовых угроз
- ✓ Сетевой экран
- ✓ Веб-Контроль
- ✓ Контроль устройств
- ✓ Анализ поведения
- ✓ Защита от эксплойтов
- ✓ Откат вредоносных действий
- ⊗ Managed Detection and Response

Лицензия действует 368 дней с момента активации, если активация произошла не позднее 16.01.2027, 03:00:00

Дата истечения: до 17.01.2027, 03:00:00

Срок действия: 368 дней

Количество компьютеров: 49

Тип лицензии: Коммерческая лицензия

🔗 [Ключ]

☐ Добавить в качестве резервного ключа

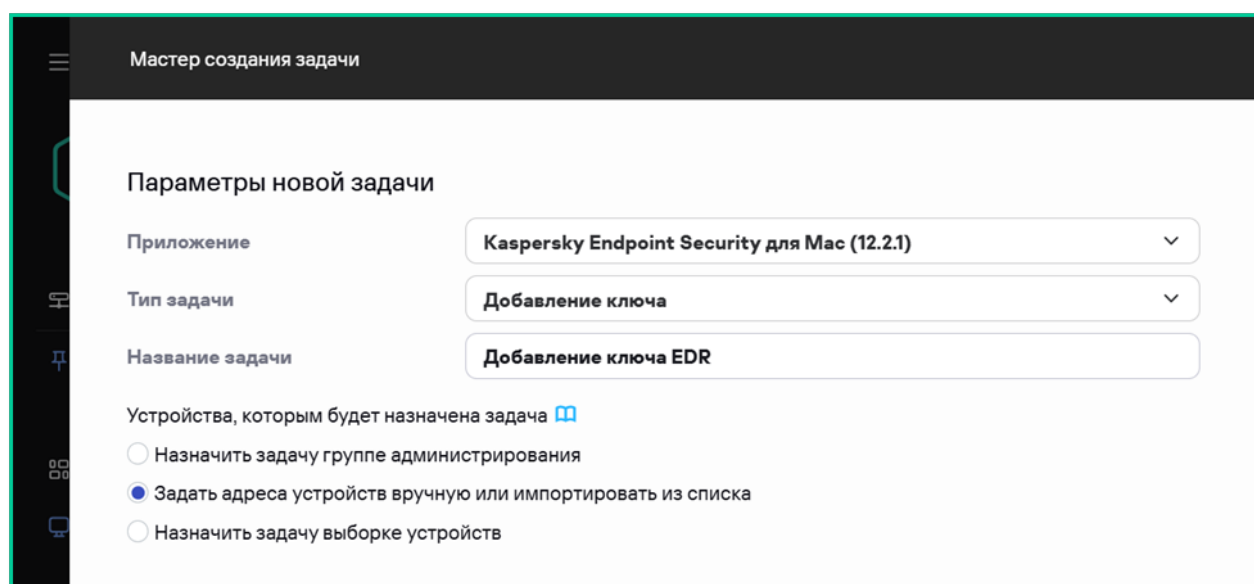
Выберите другой ключ

Назад Далее

❏ Скриншот 9: Использовать ключ в качестве резервного

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

1. Повторите шаги выше, но выберите **ключ KEDR**



Мастер создания задачи

Параметры новой задачи

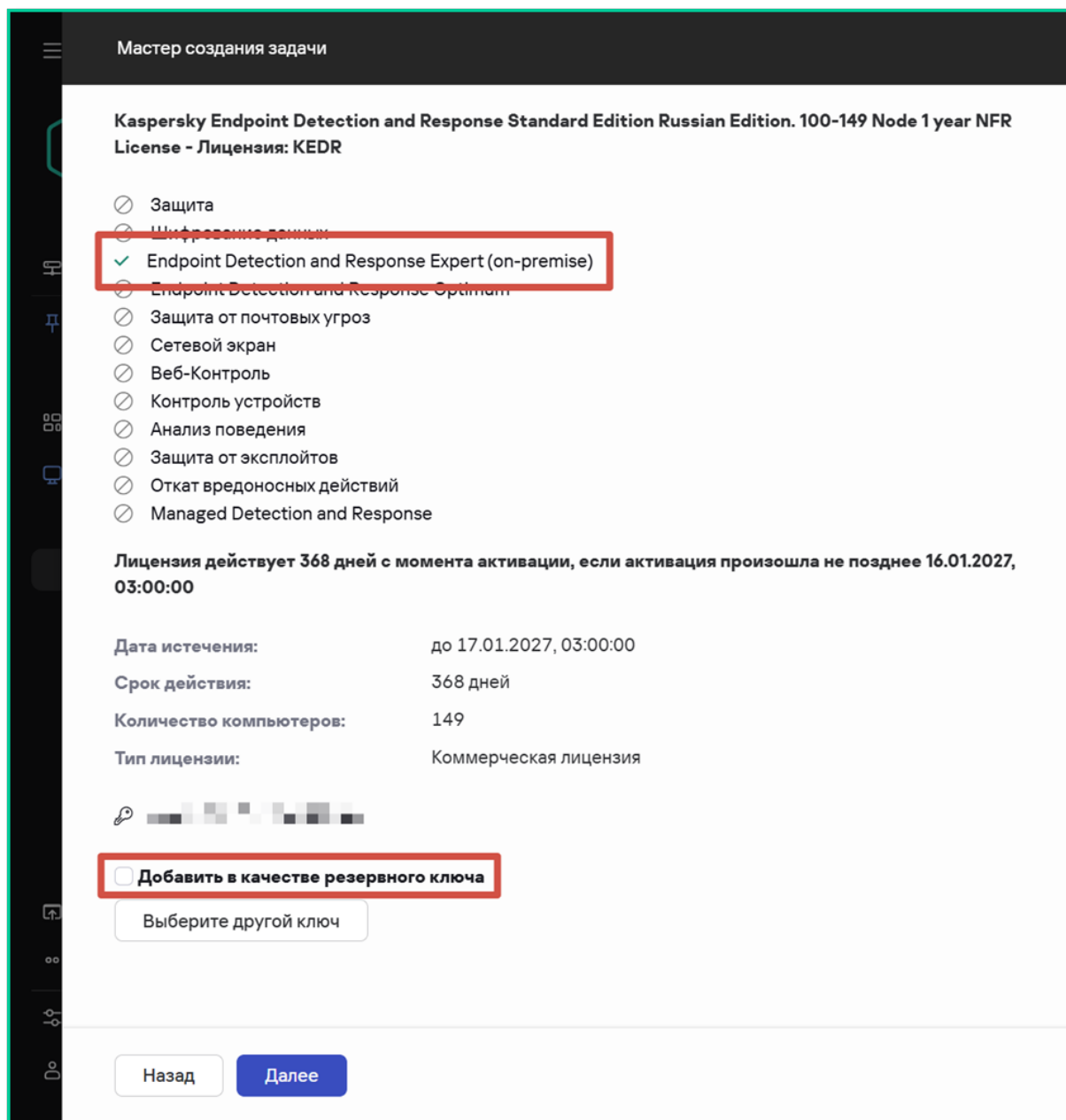
Приложение: Kaspersky Endpoint Security для Mac (12.2.1) ▼

Тип задачи: Добавление ключа ▼

Название задачи: Добавление ключа EDR

Устройства, которым будет назначена задача [?](#)

- ☐ Назначить задачу группе администрирования
- ☒ Задать адреса устройств вручную или импортировать из списка
- ☐ Назначить задачу выборке устройств



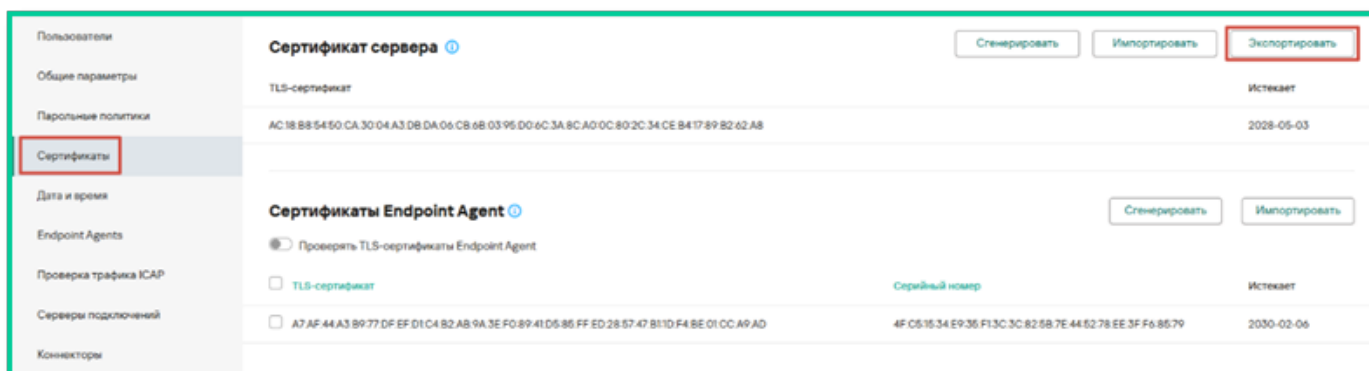
□ Скриншот 10: Добавление ключа EDR

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** → **KES for Mac 12+**

2. В мастере выберите необходимый **режим**

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

Начиная с версии Kaspersky Endpoint Security 12.2.1 for Mac 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).

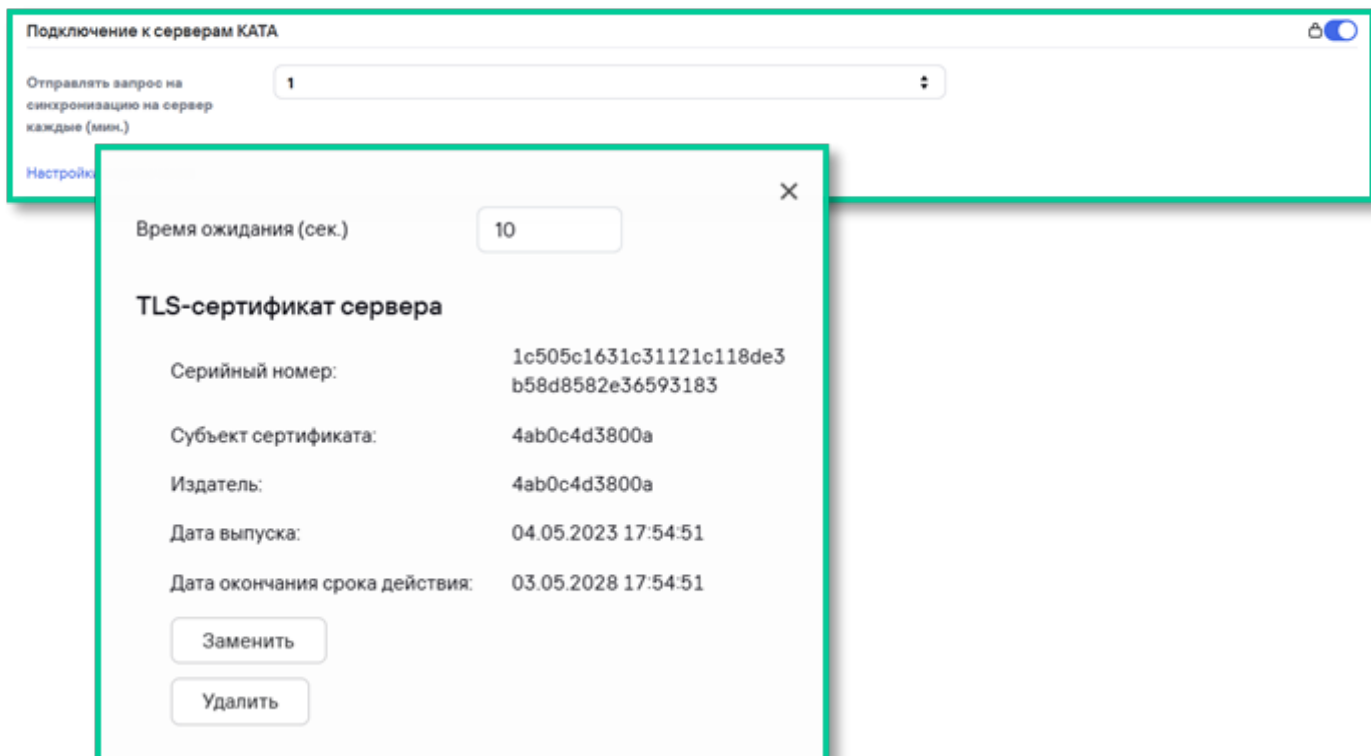
4. Включите компонент

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**



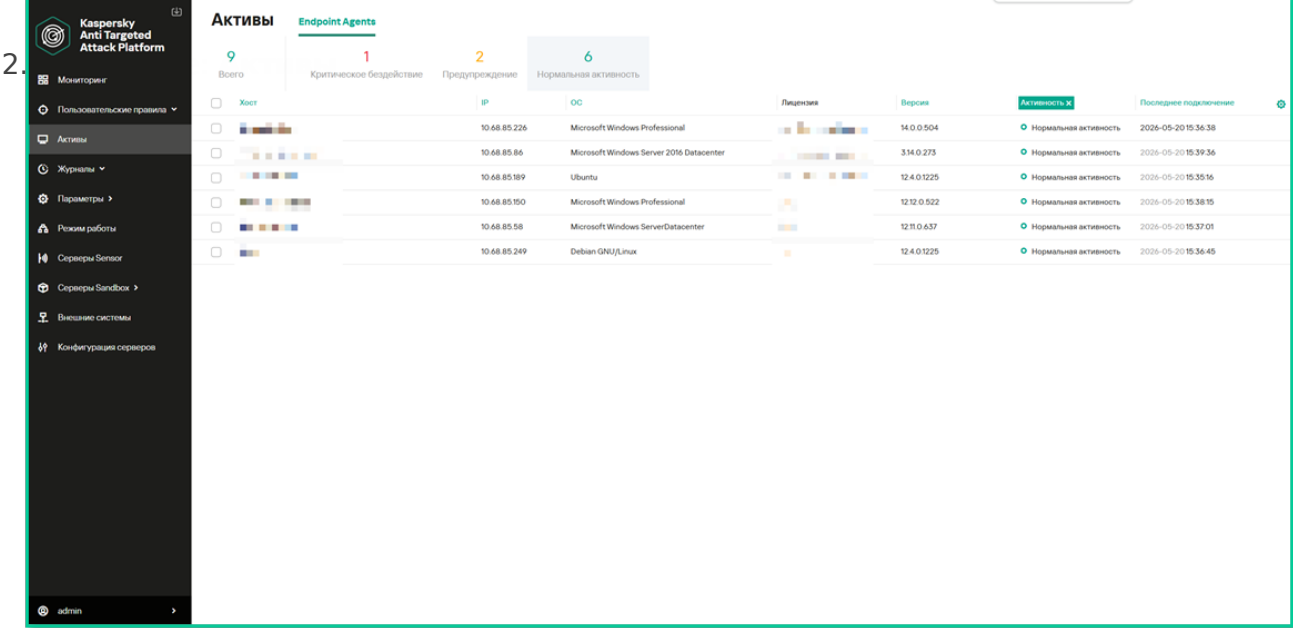
❑ Скриншот 9: указываем адрес сервера КАТА и порт

6. Нажмите «**Сохранить**»

5. Проверка интеграции

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

1. Войдите в KATA Web Console (администратор)

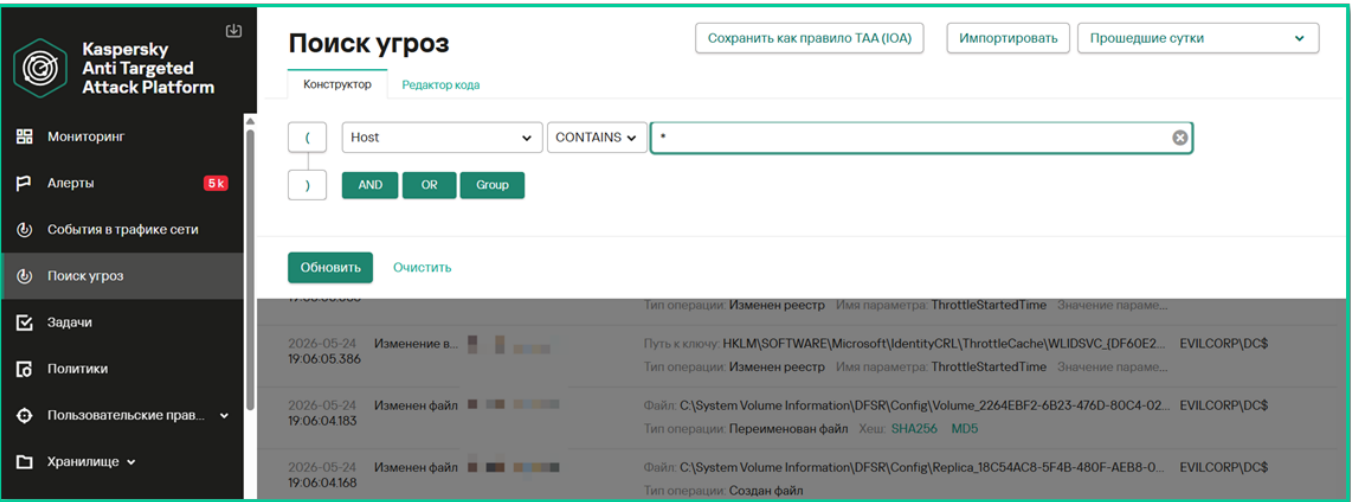


□□

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.

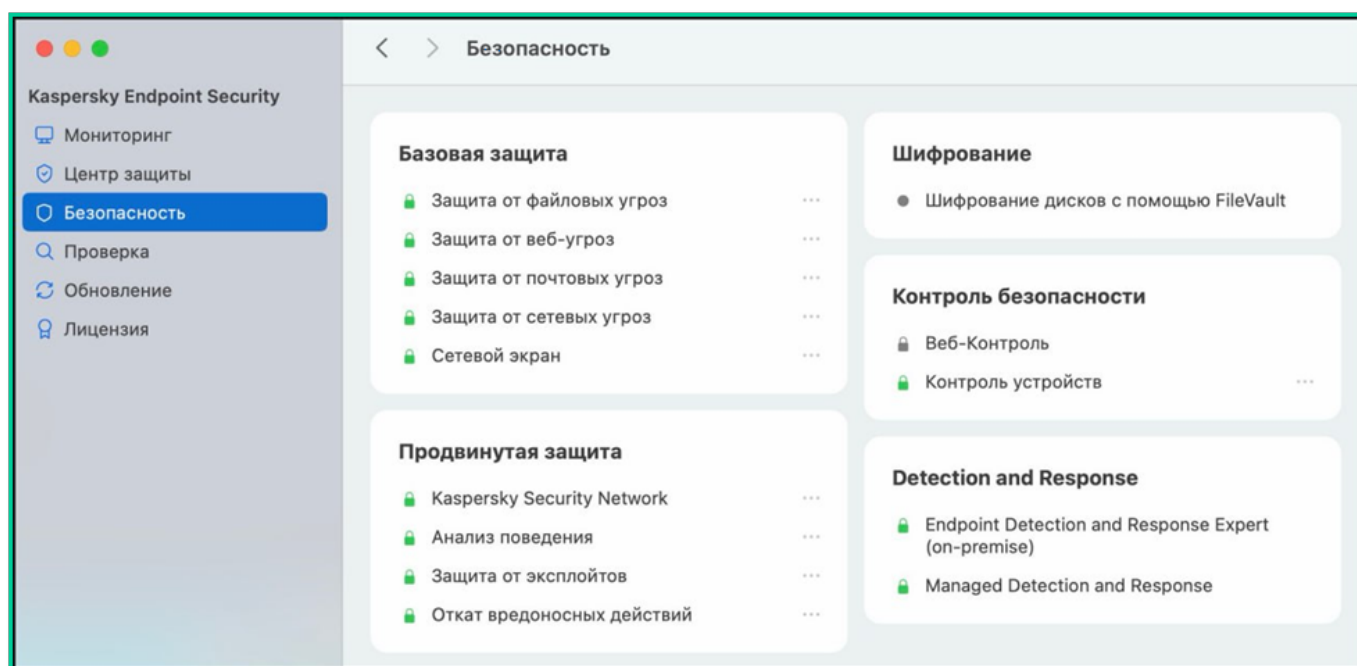


□□ **Скриншот 11:** разделе «Поиск угроз» вывод собранной телеметрии с EDR агентов.

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

1. Откройте клиент KES for Mac

2. Перейдите в раздел «**Безопасность**». Убедиться, что должен быть добавлен компонент **Endpoint Detection and Response Expert (on-premise)**. Он должен быть подсвечен зеленым цветом, что подтверждает его активацию и наличие лицензии.



❏ **Скриншот 12:** разделе «**Безопасность**» присутствует установленный компонент «**Endpoint Detection and Response Expert (on-premise)**».

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

- [Kaspersky Tech на YouTube](#)
- [Kaspersky на Rutube](#)

☐ **Развёртывание KES for Mac 12+ с EDR завершено!**

Теперь ваши конечные точки:

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

Revision #8

Created 1 October 2026 11:23:44 by Николай

Updated 1 October 2026 14:25:33 by Николай