??????? ????????? ? ????????? ??????????? Sandbox (OSMP) ?? ???? KES Windows

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

Версия решения: KES 12.7+; KEDR 8.0+ (OSMP);
Тип развёртывания:

- Чистая установка с компонентом Sandbox
- Активация компонента Sandbox на уже установленном KES

> □□ **Рекомендация**:
> Используйте **чистую установку**, если вы разворачиваете решение впервые.
> Используйте **активацию через задачу**, если KES уже развёрнут и обновлён до 12.7+.

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

Начиная с версии Kaspersky Endpoint Security для Windows 12.11 компонент EDR (KATA) переименован в Endpoint Detection and Response Expert (версия 8.0 и выше). В этой версии приложения компонент совместим с Kaspersky Anti Targeted Attack Platform версии 7.1 и ниже и Kaspersky Endpoint Detection and Response Expert (on-premise).

Компоненты EDR Optimum, EDR Expert и EDR (KATA) несовместимы между собой.

---

1. Подготовка

1.1. ?????????????? ??????

Компонент	Минимальная версия
KEDR	8.0+
KSC	13.2+
KES для Windows	12.7+

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

- **ОС**: Windows 10/11, Windows Server 2016–2022
- **RAM**: ≥2 ГБ (x64)
- **HDD**: ≥2 ГБ свободного места
- **CPU**: ≥1 ГГц, поддержка **SSE2**

1.3. ??????????? ????????

- Лицензия **KES**
- Для работы KATA Sandbox должно быть развернуто решение Kaspersky Anti Targeted Attack Platform версии 7.0 или выше.

---

2. Чистая установка KES 12.7+ с Sandbox через KSC Web Console

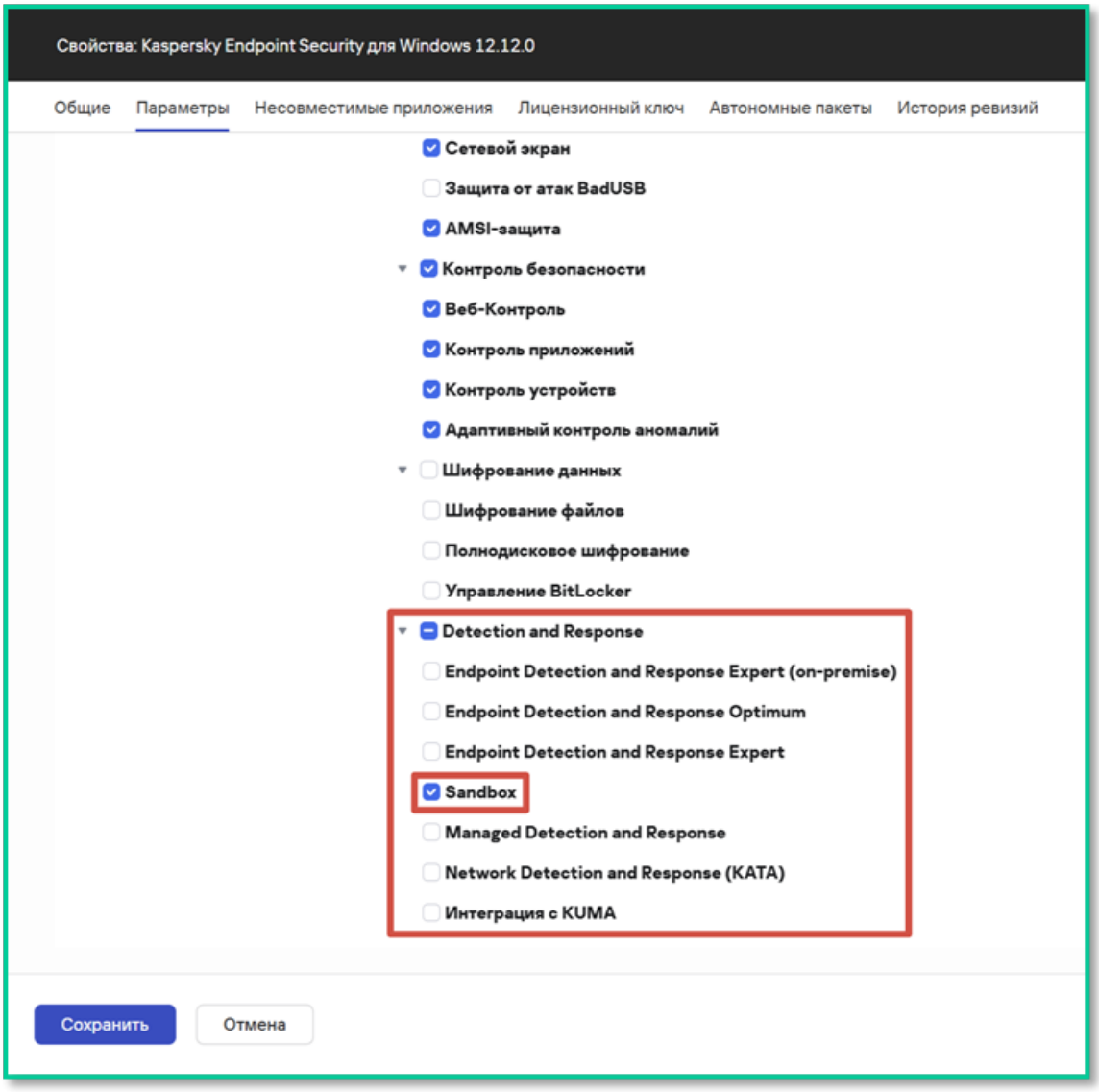
2.1. ????????? ???????????????? ??????

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

2. Найдите пакет **KES 12.7+**

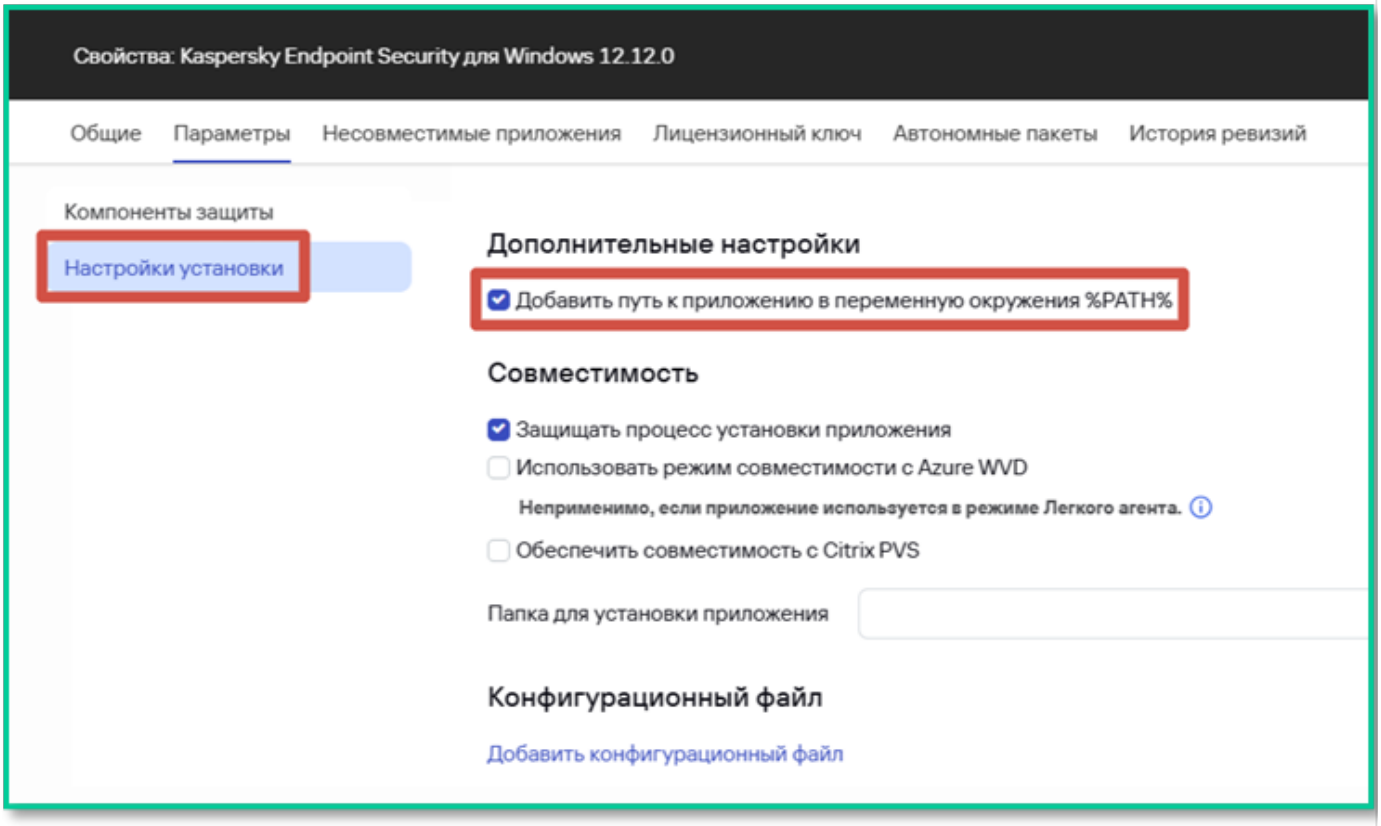
3. Перейдите в **Параметры → Detection and Response**

4. Включите: **Sandbox**



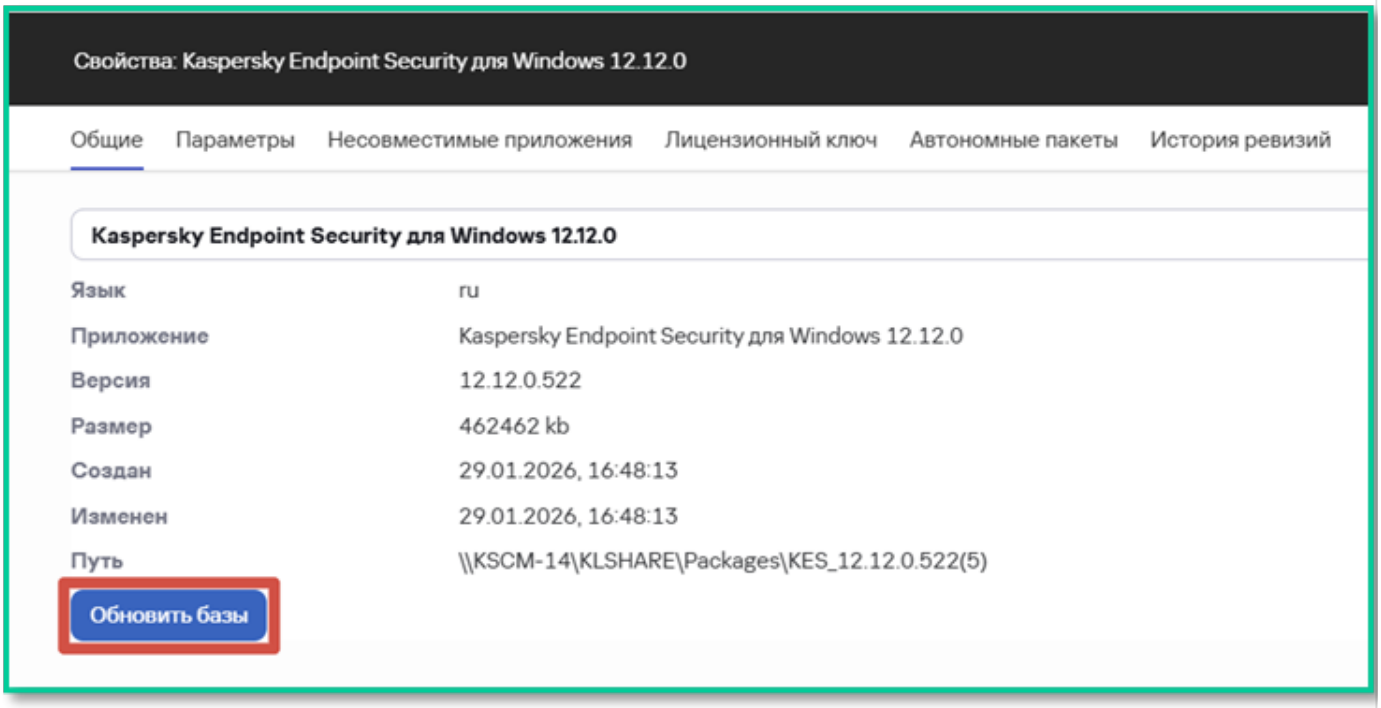
Скриншот 1: Выбор компонента Sandbox с KES 12.7

5. (Рекомендуется) Включите: **Настройки установки → Добавить путь к приложению в переменную окружения %PATH%**



Скриншот 2: Добавить путь к приложению в переменную окружения **%PATH%**

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



Скриншот 3: Обновить базы

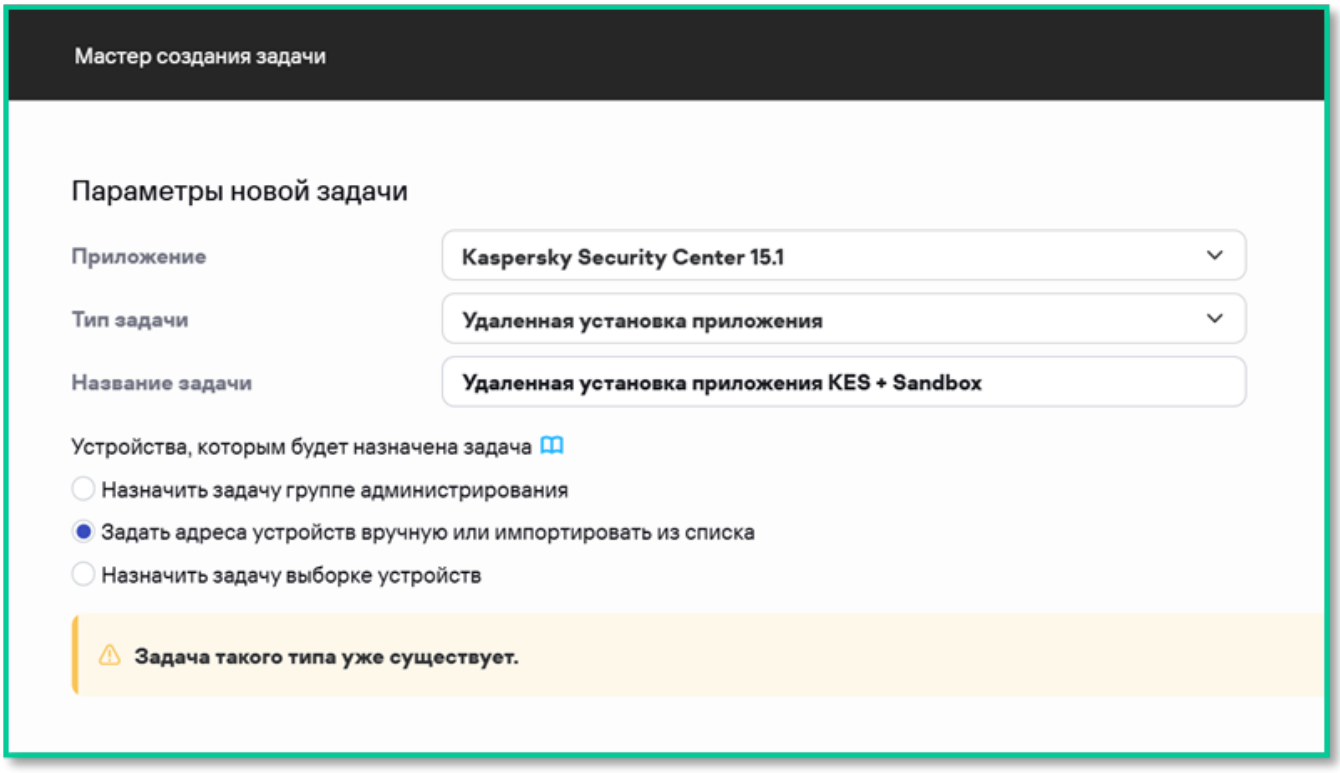
2.2. ???????? ?????? ????????? ?????????

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)

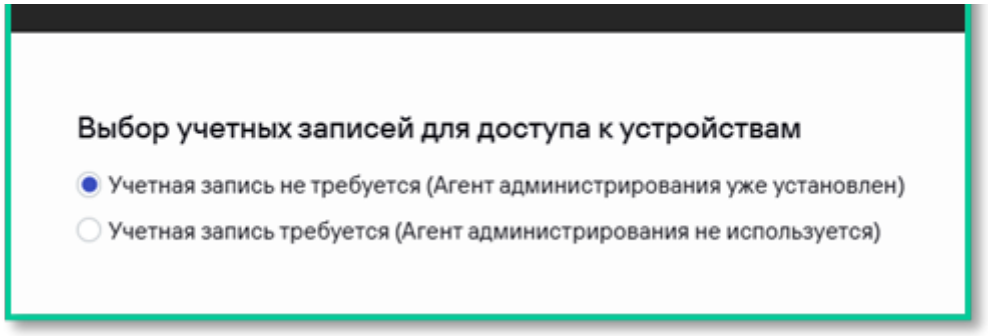


Скриншот 4: Удаленная установка программы

4. Выберите:

1. **Инсталляционный пакет**: `KES 12.7+`
2. **Агент администрирования**: `KSC Agent`

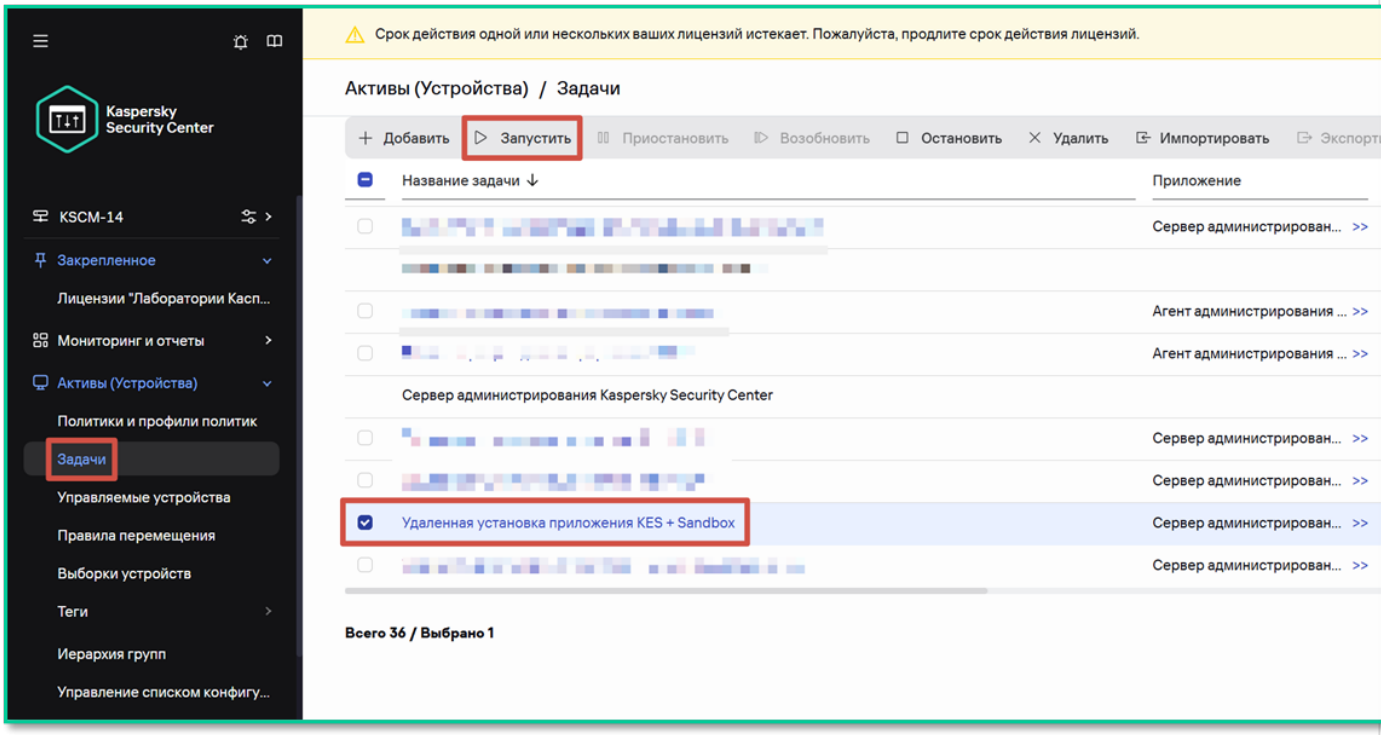
5. Если агент уже установлен — выберите: **«Учётная запись не требуется»**



Скриншот 5:

Учетная запись не требуется (Агент администрирования уже установлен)

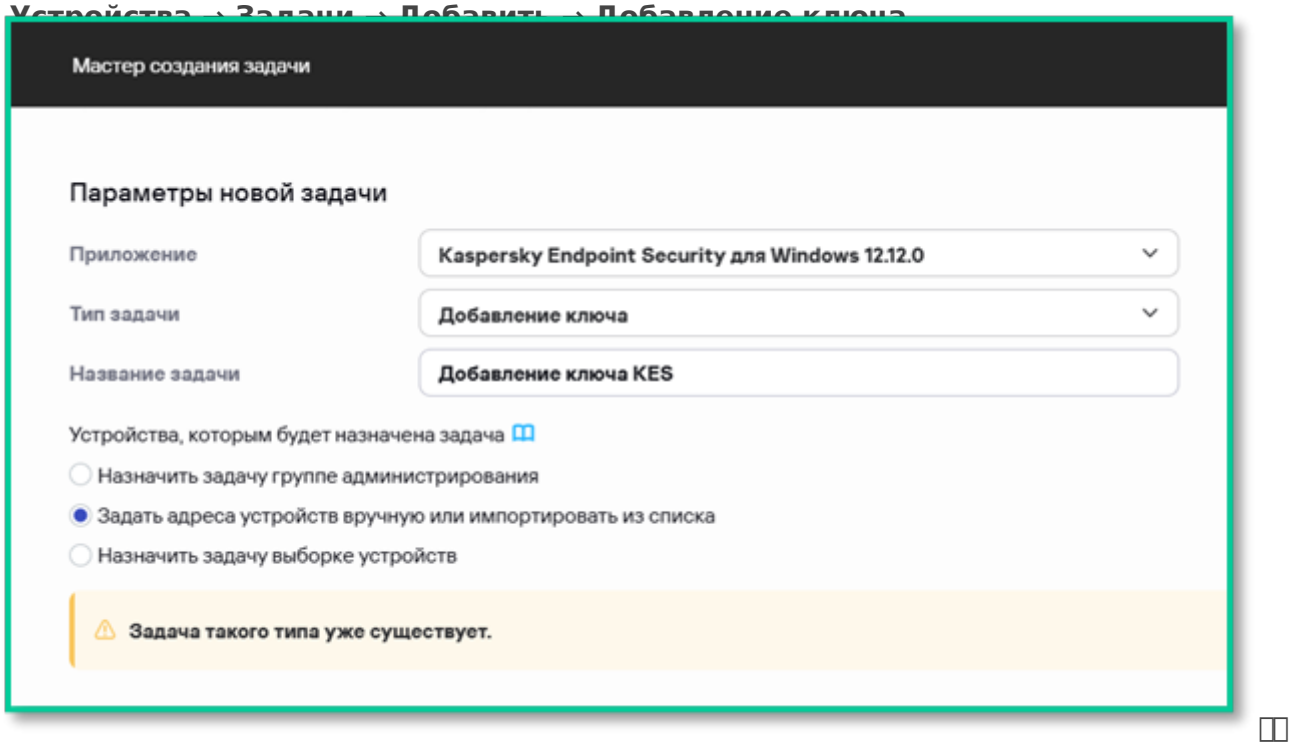
6. Нажмите **«Готово» → «Запустить»**



Скриншот 6: После создания она автоматически переходит в состояние ожидания, поэтому её необходимо запустить вручную.

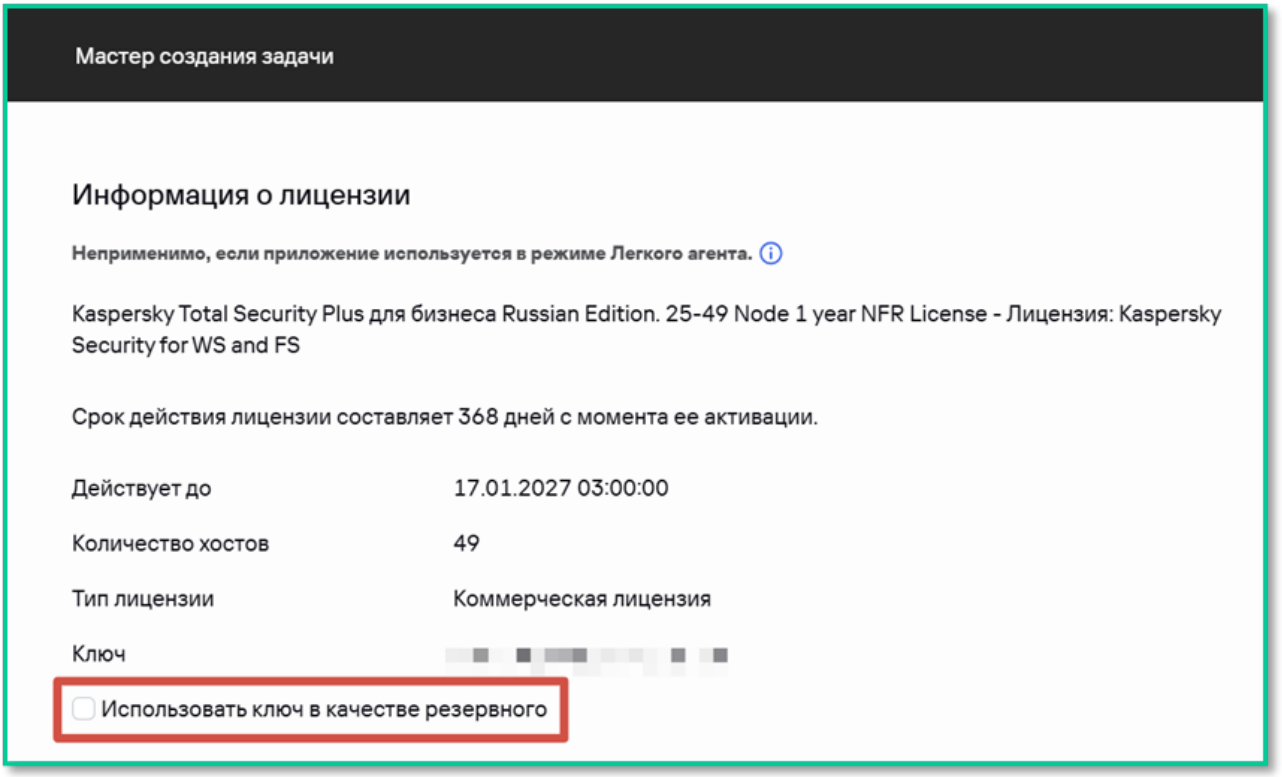
2.3. ?????????? ????????

> Для активации KATA Sandbox вам потребуется лицензионный ключ, который включает в себе функциональность KATA или KEDR. Подробнее о доступных функциональностях см. в справке Kaspersky Anti Targeted Attack Platform.

1. **Устройства → Задачи → Добавить → Добавление ключа**
2. 

Скриншот 7: Добавление ключа KES

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



Скриншот 8: Использовать ключ в качестве резервного

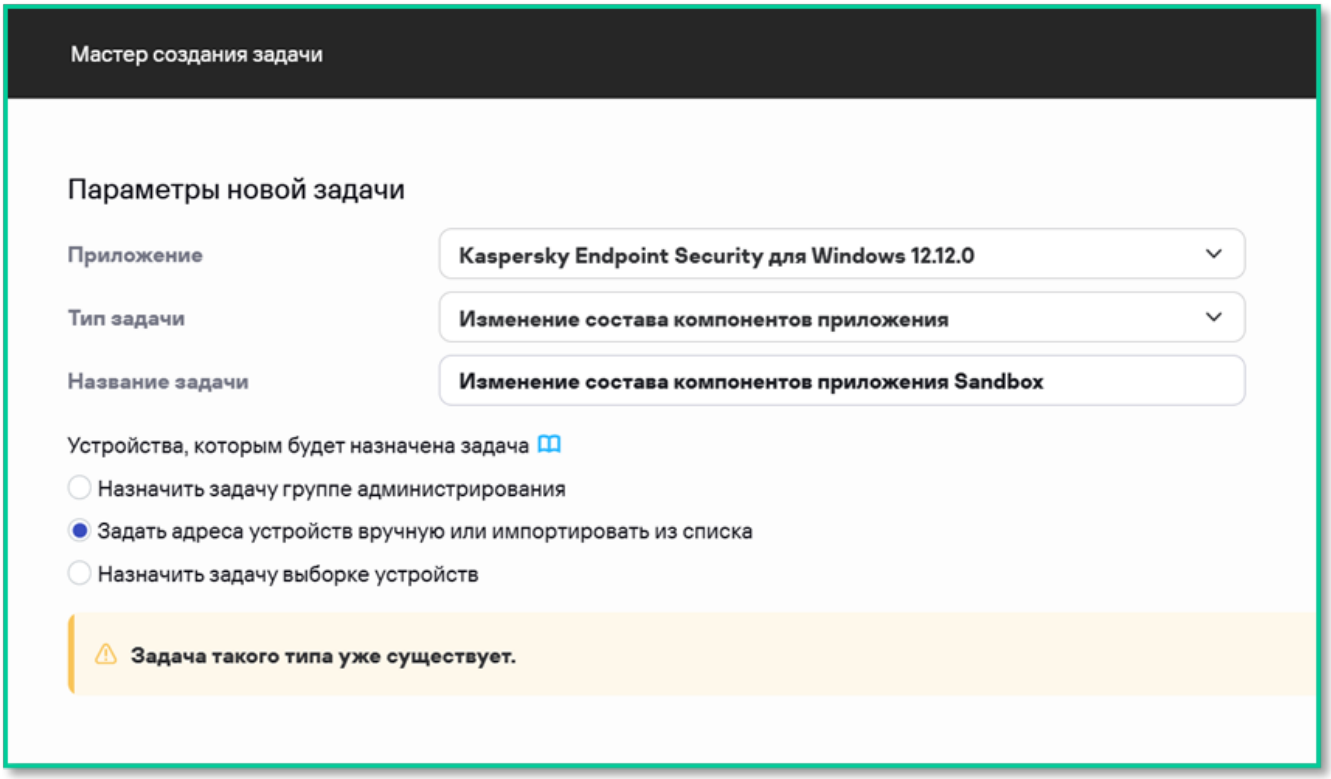
---

3. Активация Sandbox на уже установленном KES

3.1. ???????? ??????

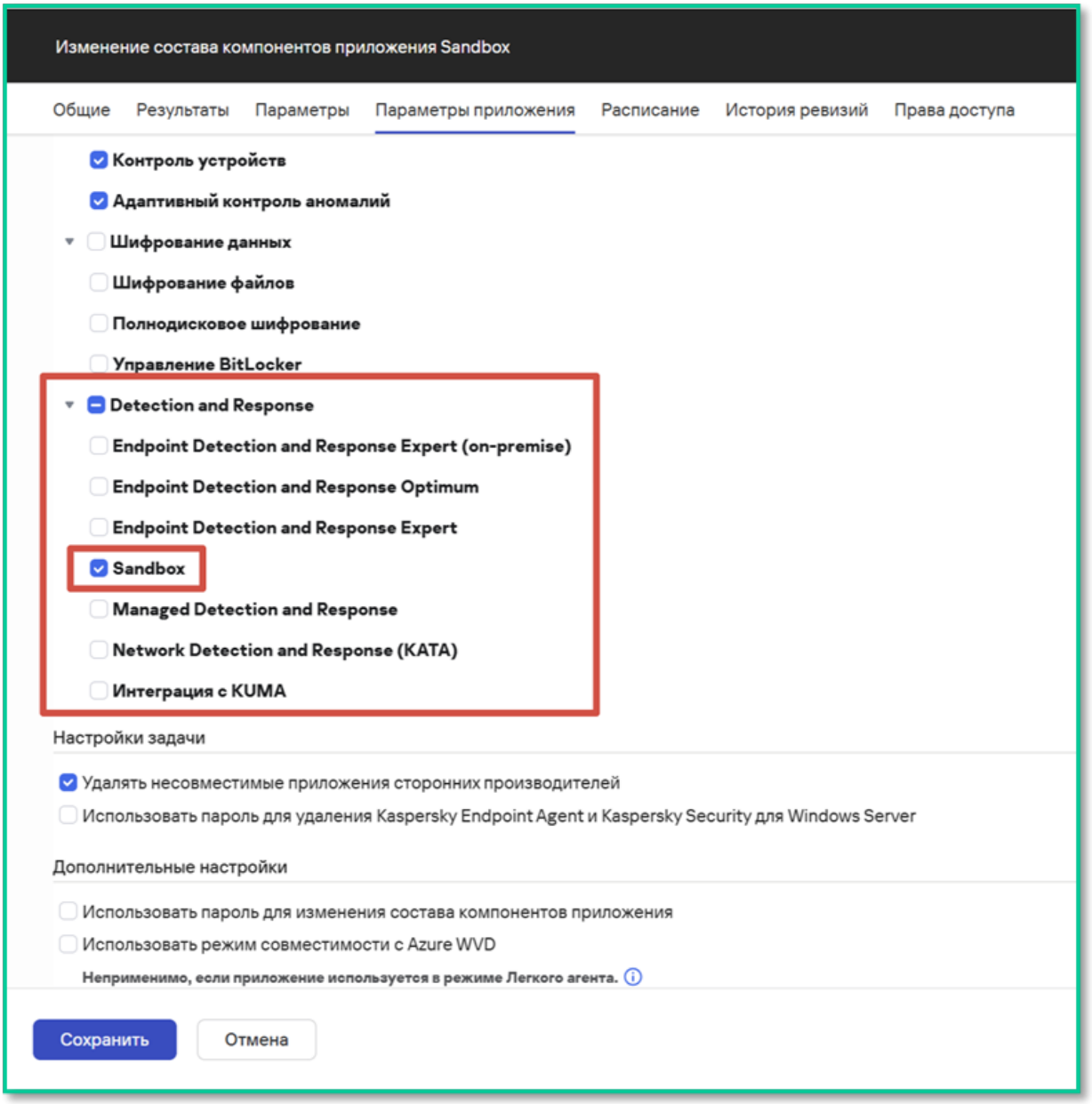
1. Устройства → Задачи → Добавить → Изменение состава компонентов

2. Выберите KES 12.7+ → укажите устройства



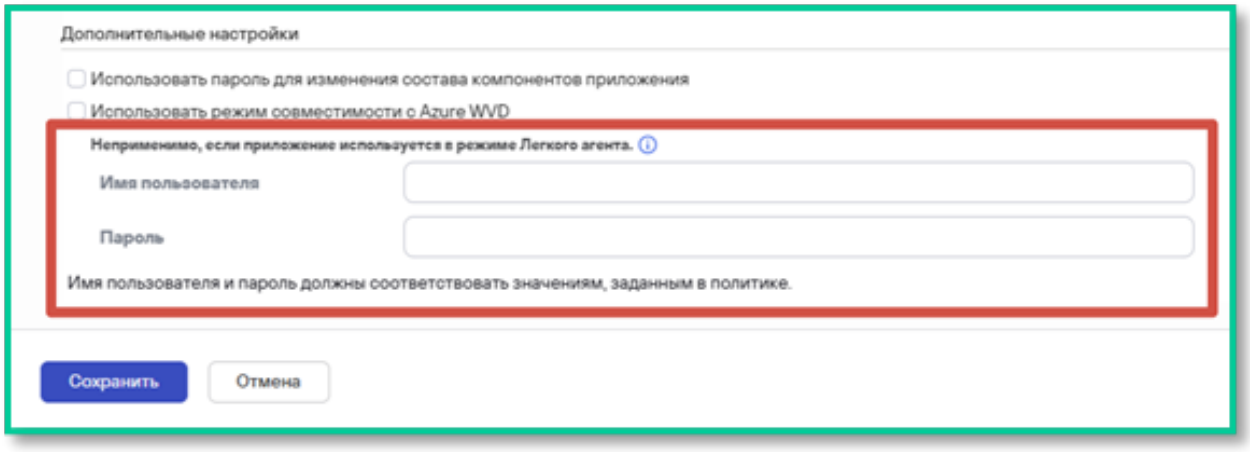
Скриншот 9: выбор на «**Изменение состава компонентов приложения**».

3. В параметрах задачи включите: **Detection and Response → Sandbox**



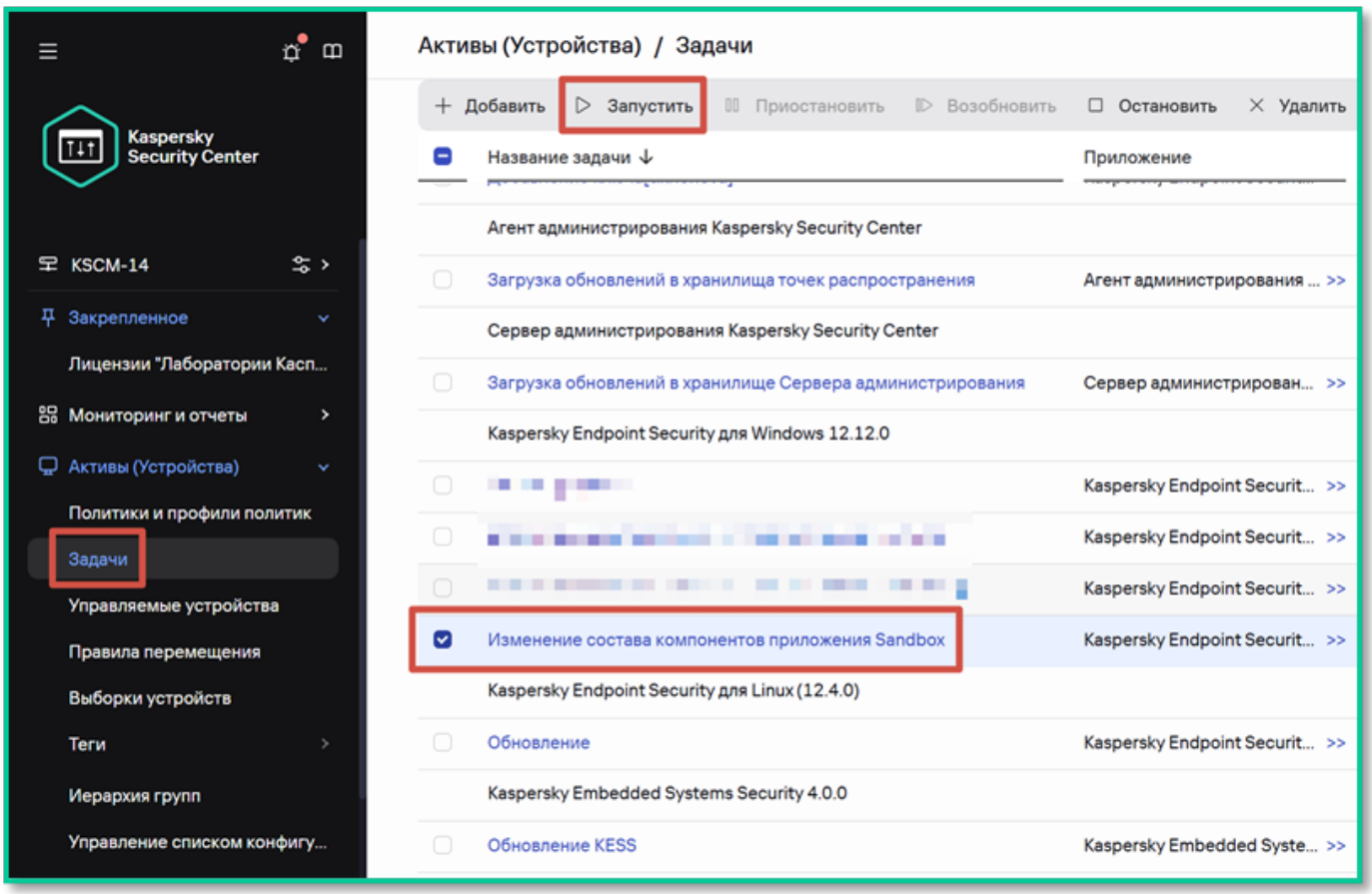
Скриншот 10: «**Параметры приложения**» и выберите компоненты «**Detection and Response**». Активируйте компонент «**Sandbox**»

4. Внесите изменения в задачу «**Изменение состава компонентов приложения**». Добавьте данные «**Имя пользователя**» и «**Пароль**» для её выполнения, чтобы избежать проблем в процессе.



Скриншот 11: выбор на «**Изменение состава компонентов приложения**».

5. Запустите задачу



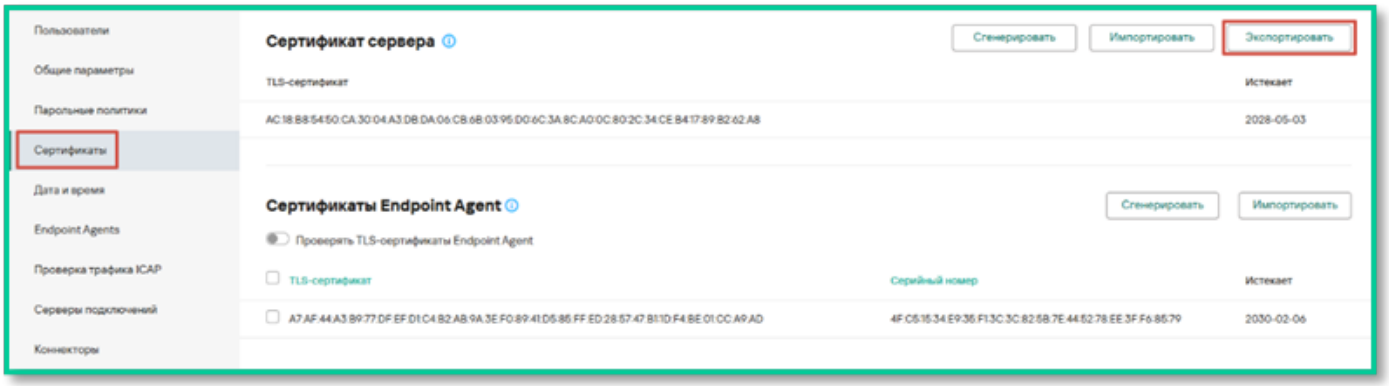
Скриншот 12: Запустите созданную задачу**.**

4. Интеграция с Central Node KATA

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

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

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



Скриншот 13: разделе **«Сертификат сервера»** нажимаем **«Экспортировать».**

3. Будет экспортирован файл `kata.crt`

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

1. Устройства → Политики → Добавить → KES 12.7+

2. В мастере выберите **стандартный режим**

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

4. Включите компонент

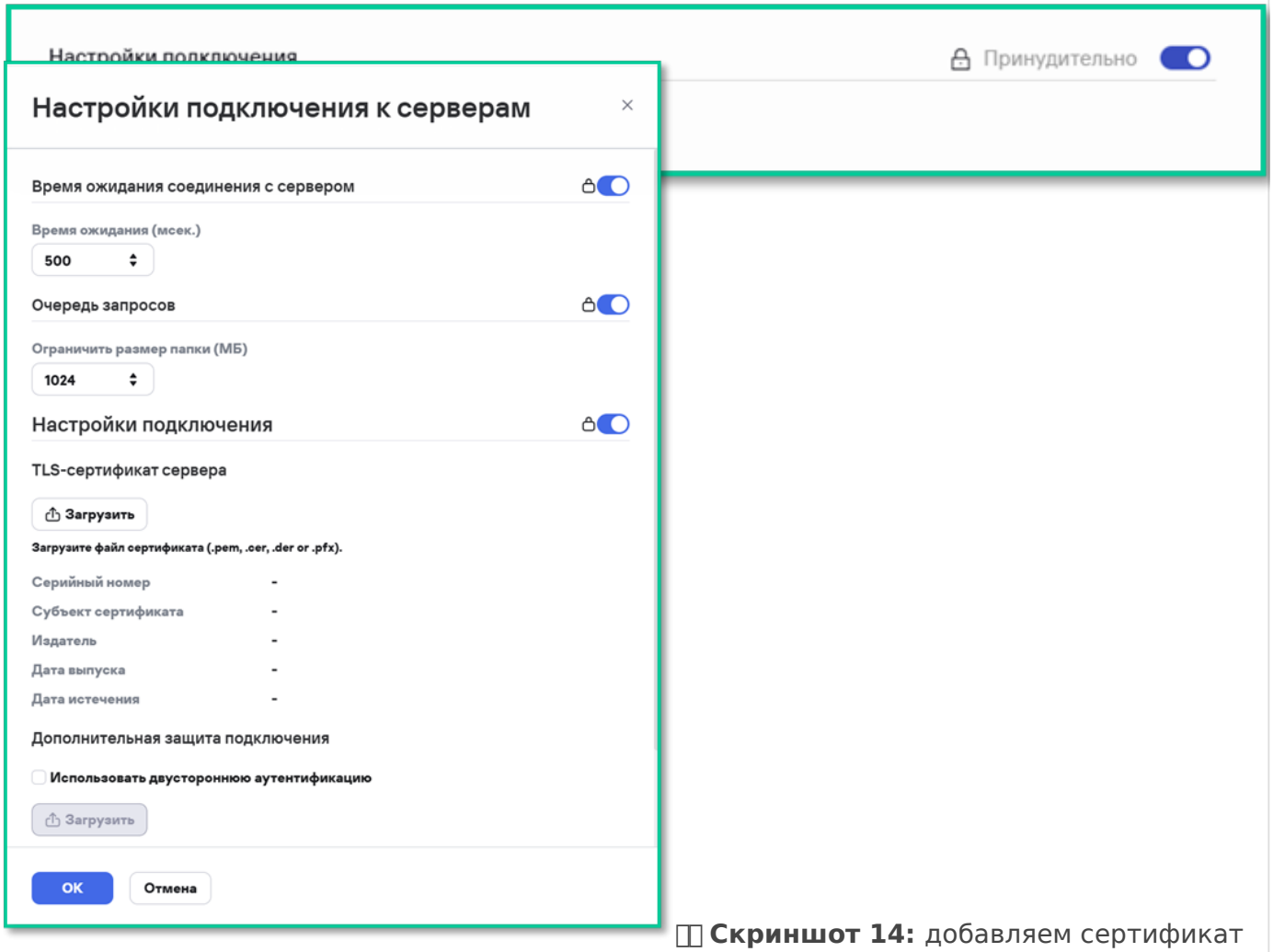
5. Выбираем Режим интеграции: **KATA Sandbox**

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 **«Подключение к серверам Sandbox»**

- Загрузите **TLS-сертификат**



Скриншот 14: добавляем сертификат

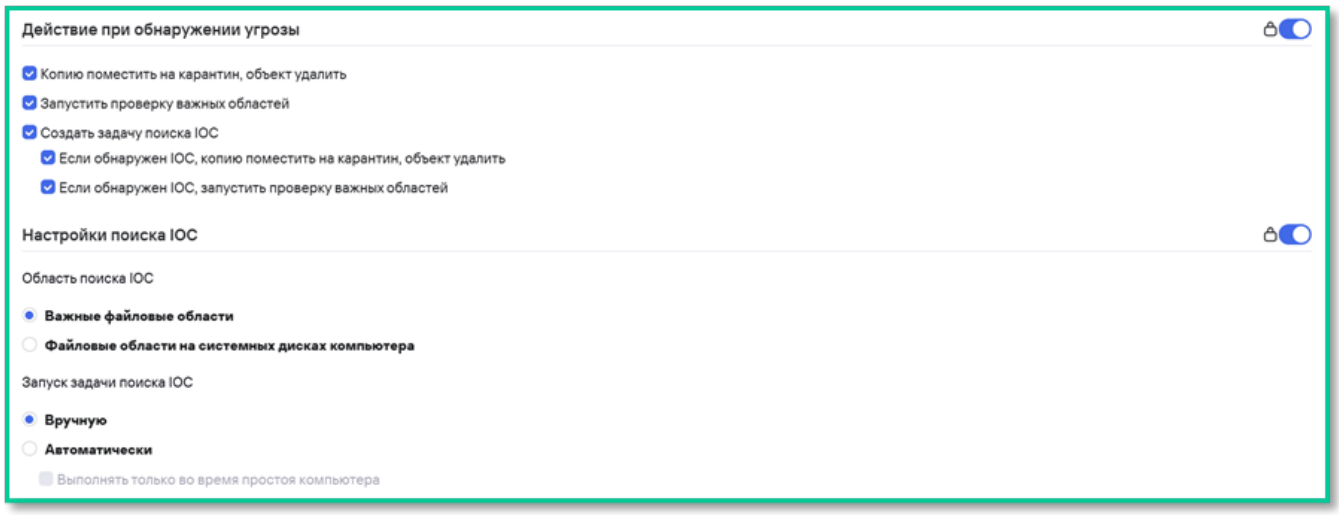
сервера TLS выгруженный из Central Node - `kata.crt`,

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

Скриншот 15: указываем адрес сервера KATA и порт

6. Нажмите **«Сохранить»**

7. Рекомендуется ознакомится и дополнительно настроить действий по реагированию на угрозы



Скриншот 16: указываем адрес сервера KATA и порт

8. Детально описание доступно в [онлайн-документации]

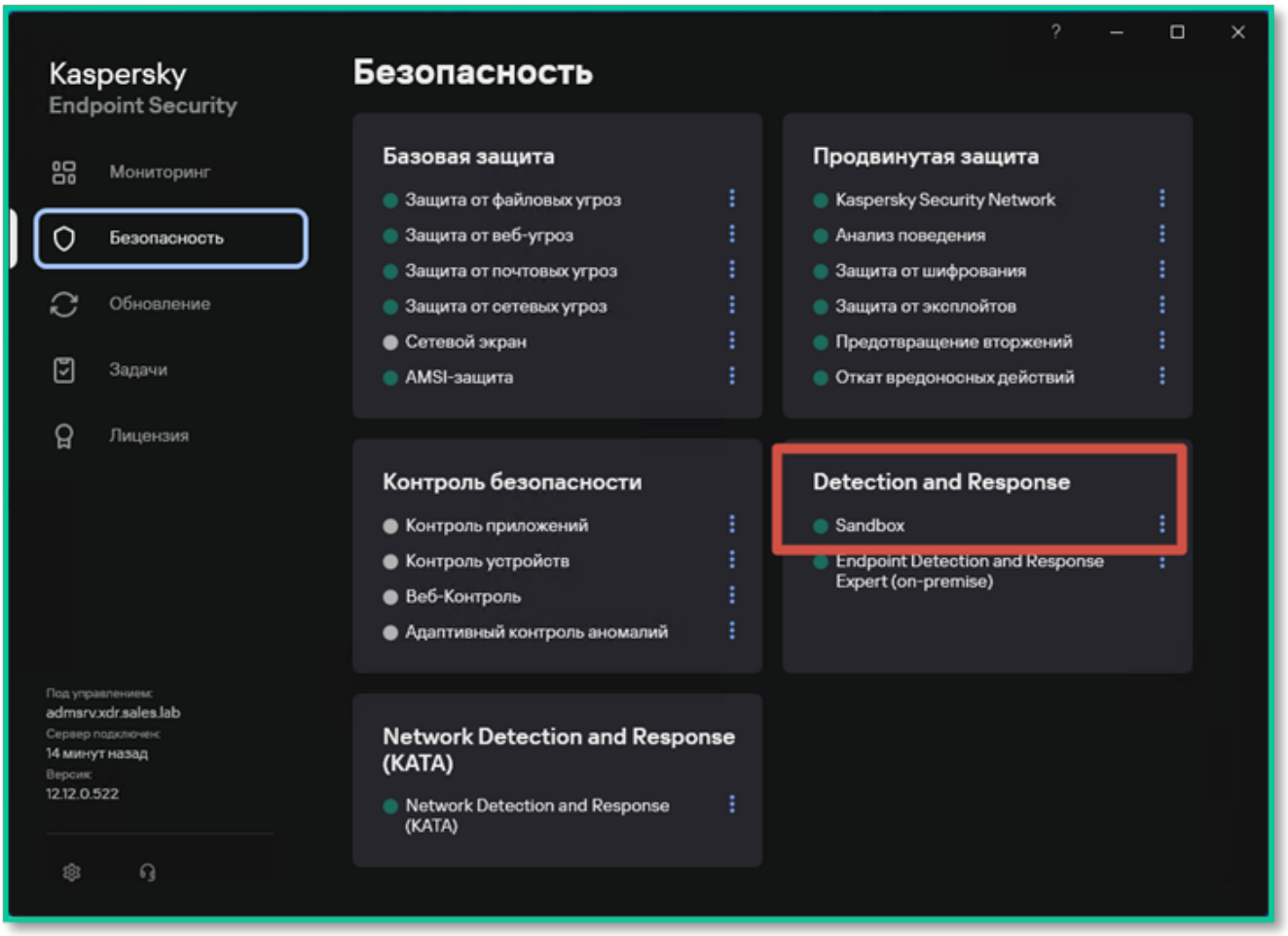
---

5. Проверка интеграции

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

1. Откройте клиент KES

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



Скриншот 20: разделе **«Безопастность»** присуствует установленный компонент **«Sandbox».**

3. Перейти в раздел **Мониторинг → Отчеты→ Network Detection and Response (KATA),** либо в том же разделе **Безопасность** кликнуть по значку троеточия и выпадающем меню выбрать **Открыть отчет**.

Полезные ссылки

- Kaspersky Tech на YouTube
- Kaspersky на Rutube

Развёртывание KES 12.7+ с EDR завершено!
Теперь ваши конечные точки:

- Передают телеметрию в KATA
- Участвуют в расследовании инцидентов

- Поддерживают автоматическую корреляцию с сетевыми событиями

Revision #9
Created 15 June 2026 14:21:41 by Николай
Updated 15 June 2026 15:45:08 by Николай