

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

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

Sandbox (KATA) ?? ??? KES Windows

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

Версия решения: KES 12.7+; KATA (NDR/KEDR) 7.0 > 8.0;

Тип развёртывания:

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

“ □ **Рекомендация:**

Используйте **чистую установку**, если вы разворачиваете решение впервые.

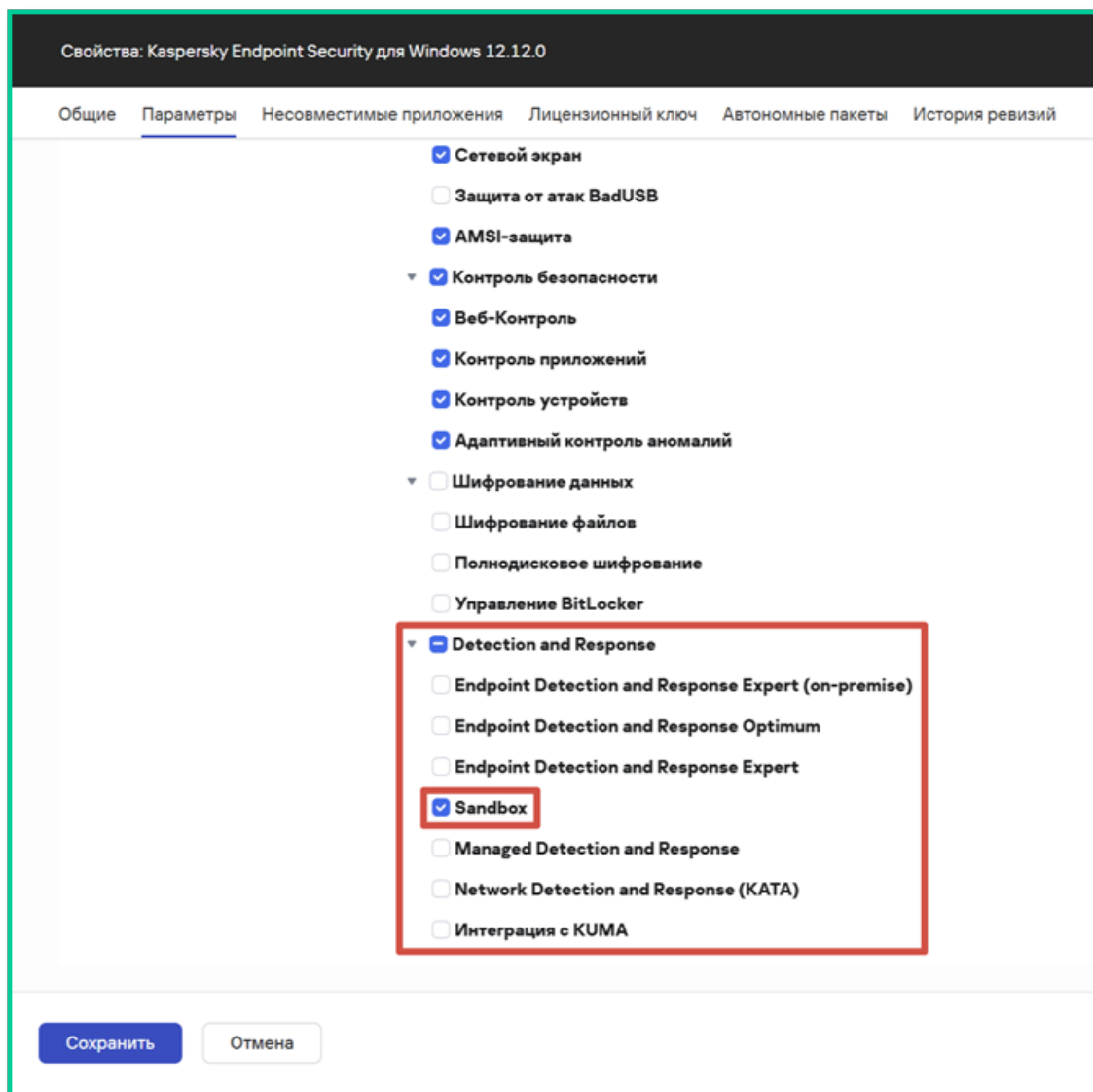
Используйте **активацию через задачу**, если KES уже развёрнут и обновлён до 12.7+.

ВАЖНО:

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

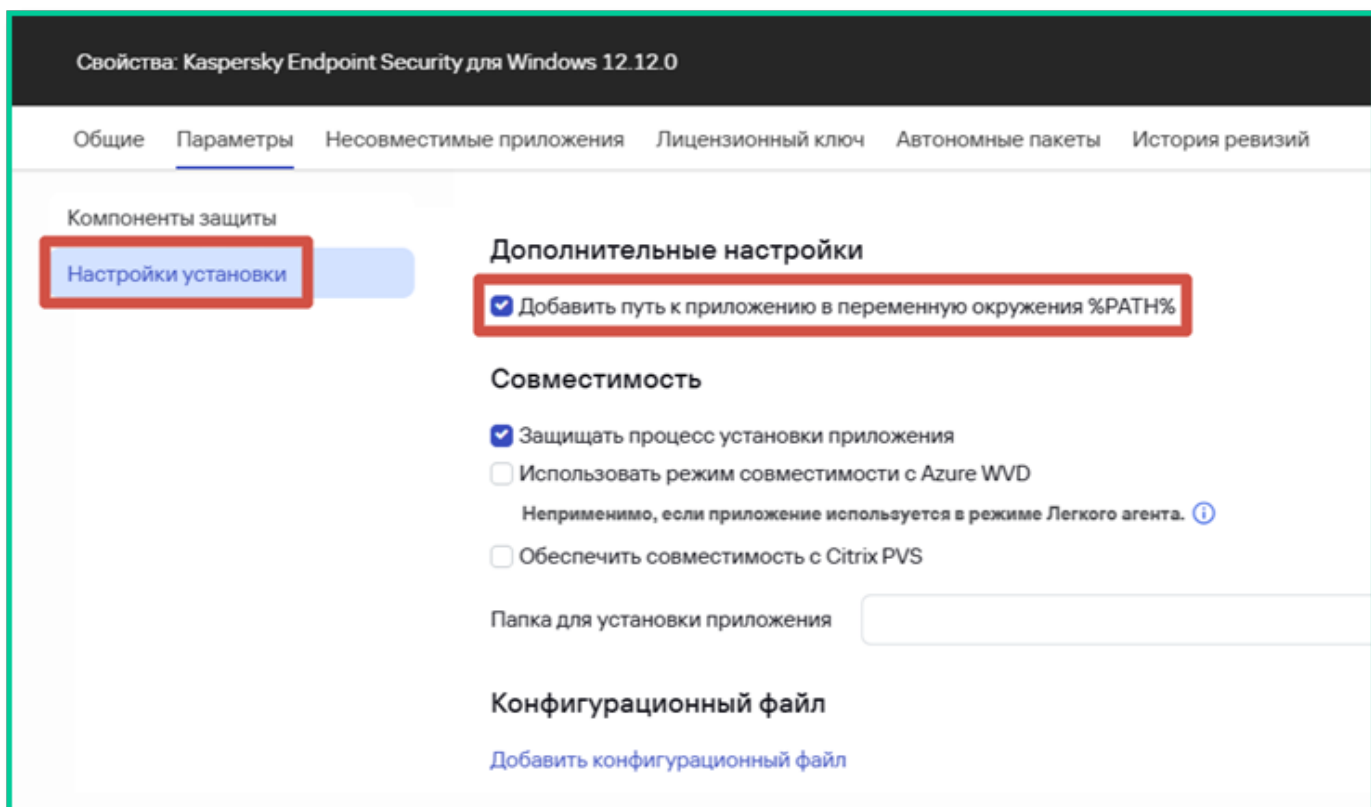
1. Подготовка

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



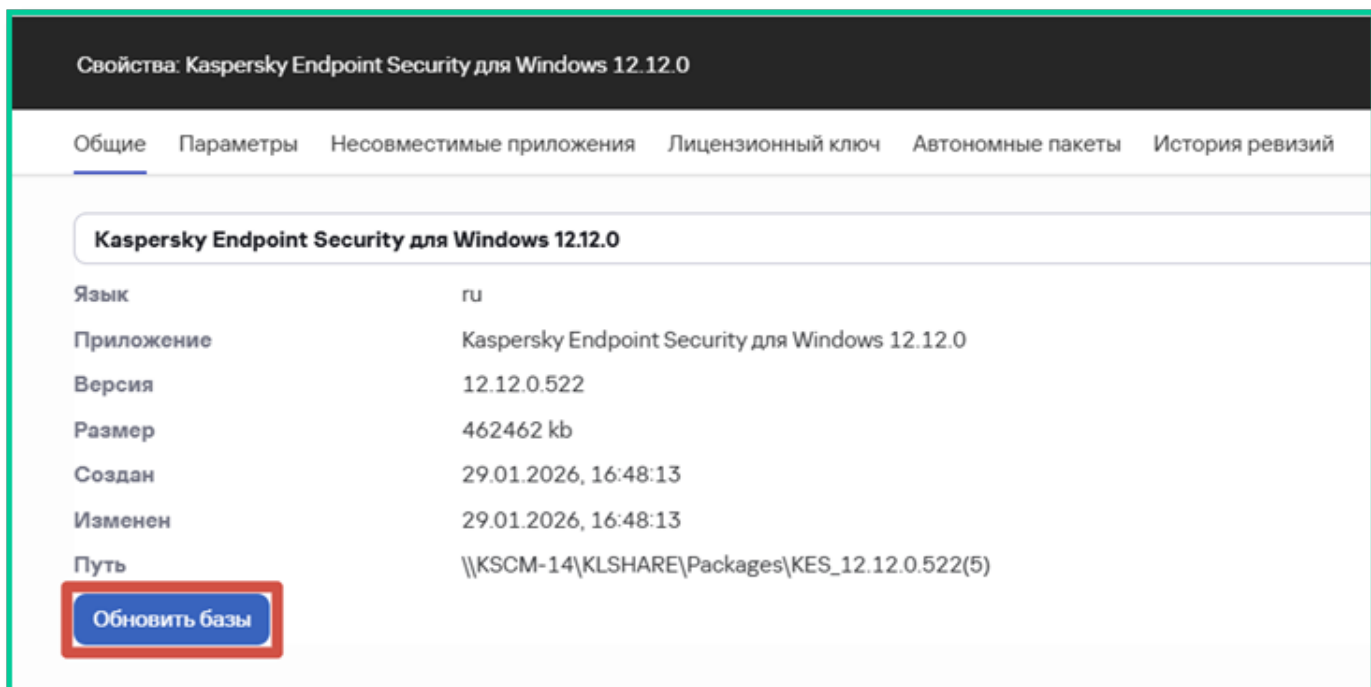
□ Скриншот 1: Выбор компонента Sandbox с KES 12.7

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**»

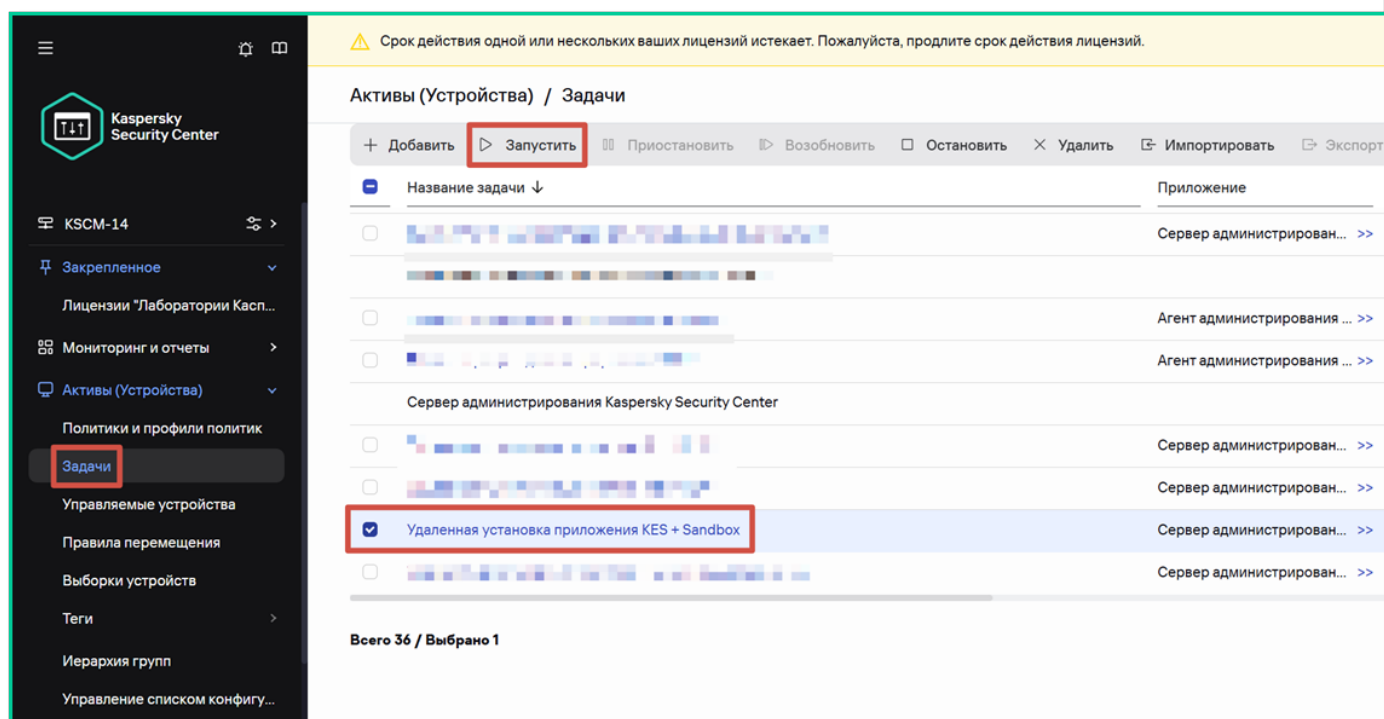
Выбор учетных записей для доступа к устройствам

- ☒ Учетная запись не требуется (Агент администрирования уже установлен)
- ☐ Учетная запись требуется (Агент администрирования не используется)

❏ 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»**

Параметры новой задачи

Приложение

Kaspersky Endpoint Security для Windows 12.12.0

Тип задачи

Изменение состава компонентов приложения

Название задачи

Изменение состава компонентов приложения Sandbox

Устройства, которым будет назначена задача 

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

 Задача такого типа уже существует.

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

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

Изменение состава компонентов приложения Sandbox

Общие Результаты Параметры Параметры приложения Расписание История ревизий Права доступа

- ☒ Контроль устройств
- ☒ Адаптивный контроль аномалий
- ☐ Шифрование данных
 - ☐ Шифрование файлов
 - ☐ Полнодисковое шифрование
 - ☐ Управление BitLocker
- ☒ Detection and Response
 - ☐ Endpoint Detection and Response Expert (on-premise)
 - ☐ Endpoint Detection and Response Optimum
 - ☐ Endpoint Detection and Response Expert
 - ☒ Sandbox
 - ☐ Managed Detection and Response
 - ☐ Network Detection and Response (KATA)
 - ☐ Интеграция с KUMA

Настройки задачи

- ☒ Удалять несовместимые приложения сторонних производителей
- ☐ Использовать пароль для удаления Kaspersky Endpoint Agent и Kaspersky Security для Windows Server

Дополнительные настройки

- ☐ Использовать пароль для изменения состава компонентов приложения
- ☐ Использовать режим совместимости с Azure WVD

Неприменимо, если приложение используется в режиме Легкого агента. ⓘ

Сохранить Отмена

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

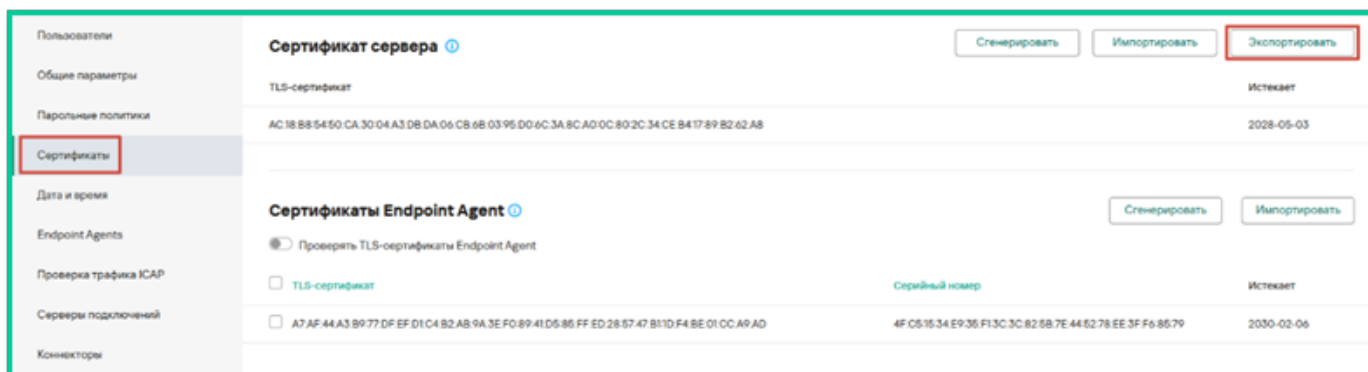
4. Внесите изменения в задачу «**Изменение состава компонентов приложения**». Добавьте данные «**Имя пользователя**» и «**Пароль**» для её выполнения, чтобы избежать проблем в процессе.

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

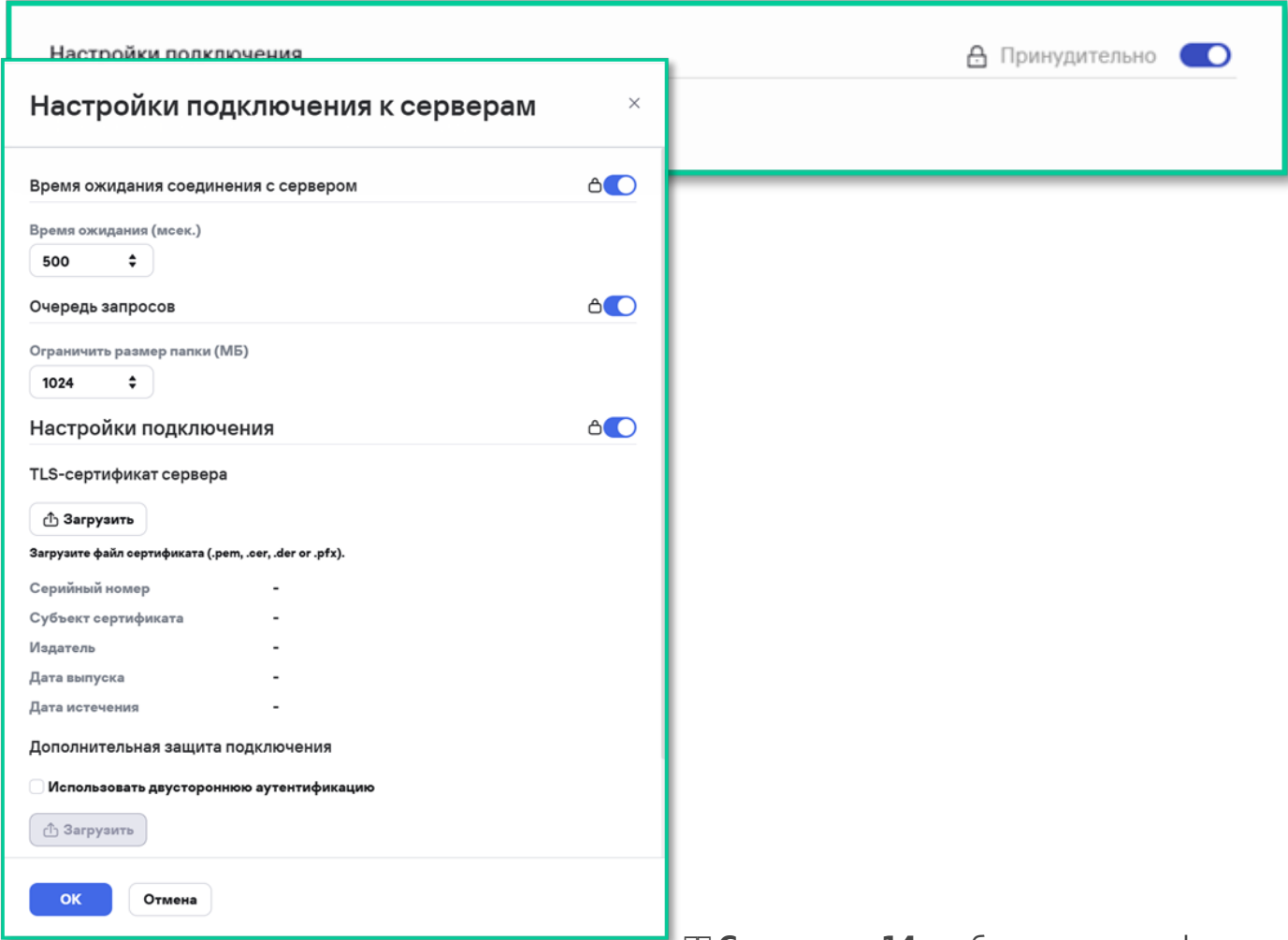
5. Выбираем Режим интеграции: **KATA Sandbox**

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 режиме** 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 выгружены ntral Node - [kata.crt](#),

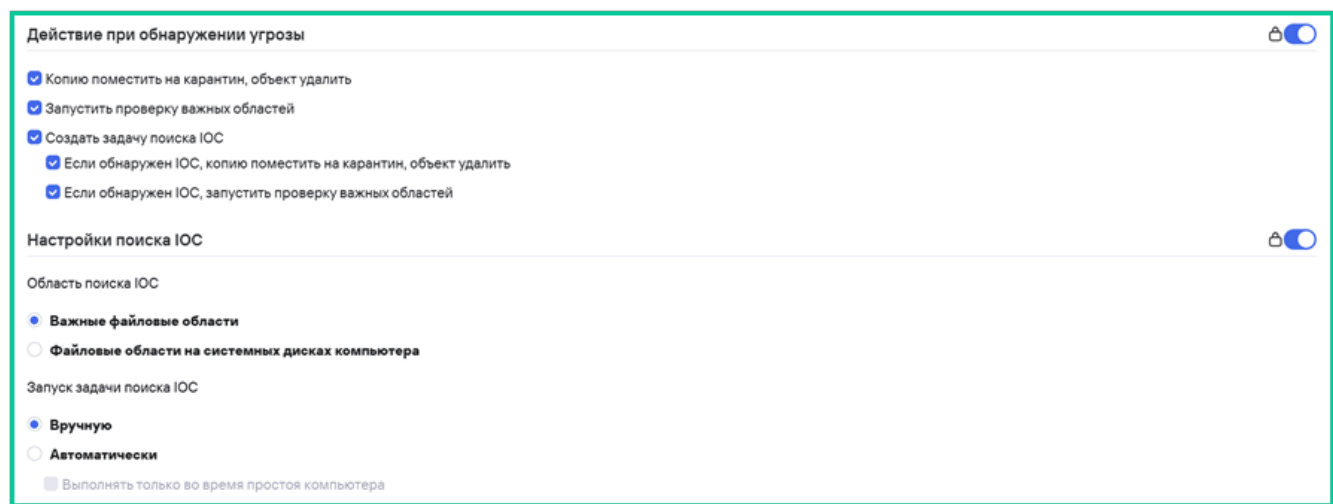
- Укажите **адрес Central Node** и **порт 443**



❏ Скриншот 15: указываем адрес сервера КАТА и порт

6. Нажмите «**Сохранить**»

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



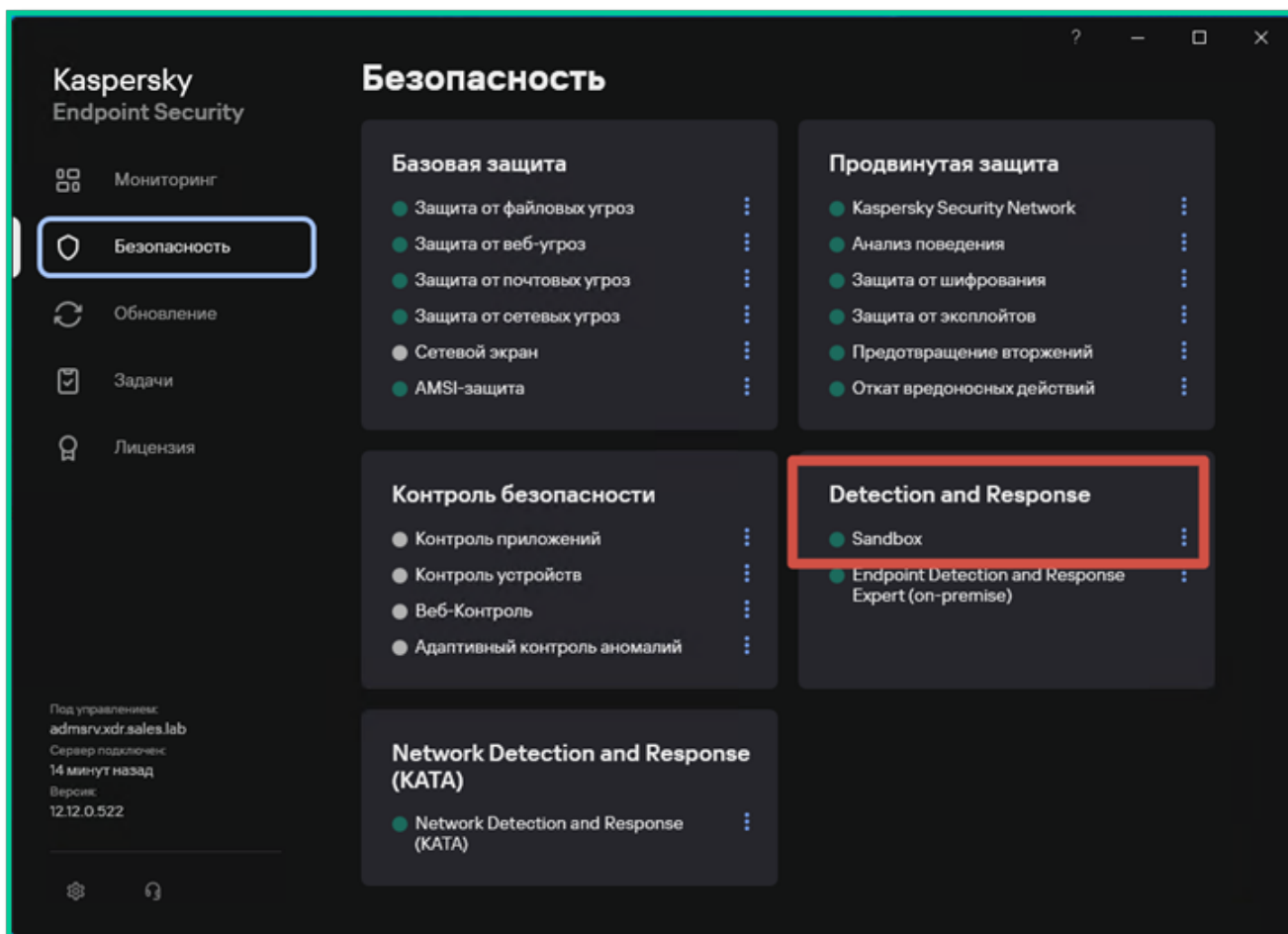
❏ Скриншот 16: указываем адрес сервера KATA и порт

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 **Sandbox**. Он должен быть подсвечен зеленым цветом, что подтверждает его активацию и наличие лицензии.

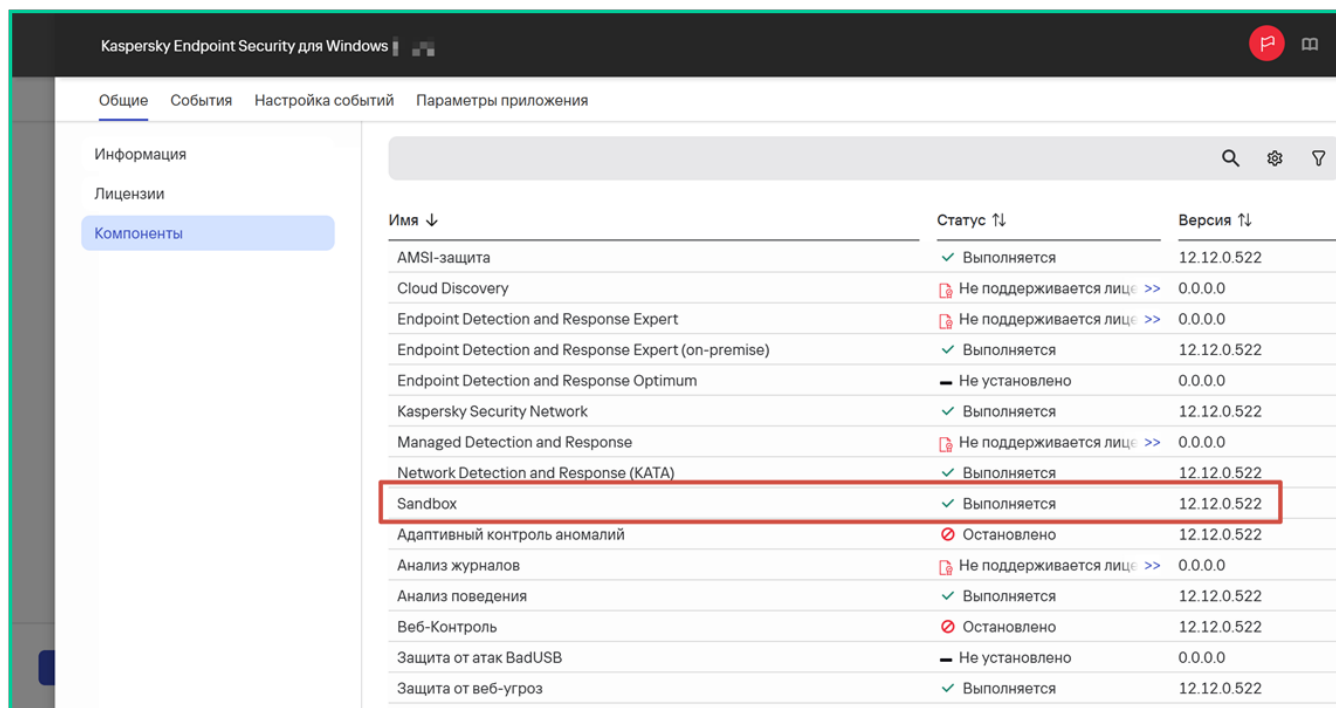


Скриншот 17: разделе «Безопасность» присутствует установленный компонент «Sandbox».

3. Перейти в раздел **Мониторинг** → **Отчеты** → **Sandbox**, либо в том же разделе **Безопасность** кликнуть по значку троеточия и выпадающем меню выбрать **Открыть отчет**.

5.2. ??? ?????? ???????? KSC Web Console

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



☐ **Скриншот 18:** разделе «Безопасность» присутствует установленный компонент «Sandbox».

☐ Полезные ссылки

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

☐ **Развёртывание KES 12.7+ с Sandbox завершено!**

Теперь ваши конечные точки:

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

Revision #13

Created 8 June 2026 14:52:16 by Николай

Updated 29 June 2026 12:05:38 by Николай