

????????? ?????????? ? ????????????? ?????????????? 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. Требования к оборудованию (к серверу)

- **CPU:** ≥1 ГГц, поддержка **SSE2**
- **RAM:** ≥2 ГБ (x64)
- **HDD:** ≥2 ГБ свободного места

1.3. Требования к лицензиям

- Лицензия **KESL+NDR**

2. Чистая установка KESL 12.2+ с EDR через KSC Web Console

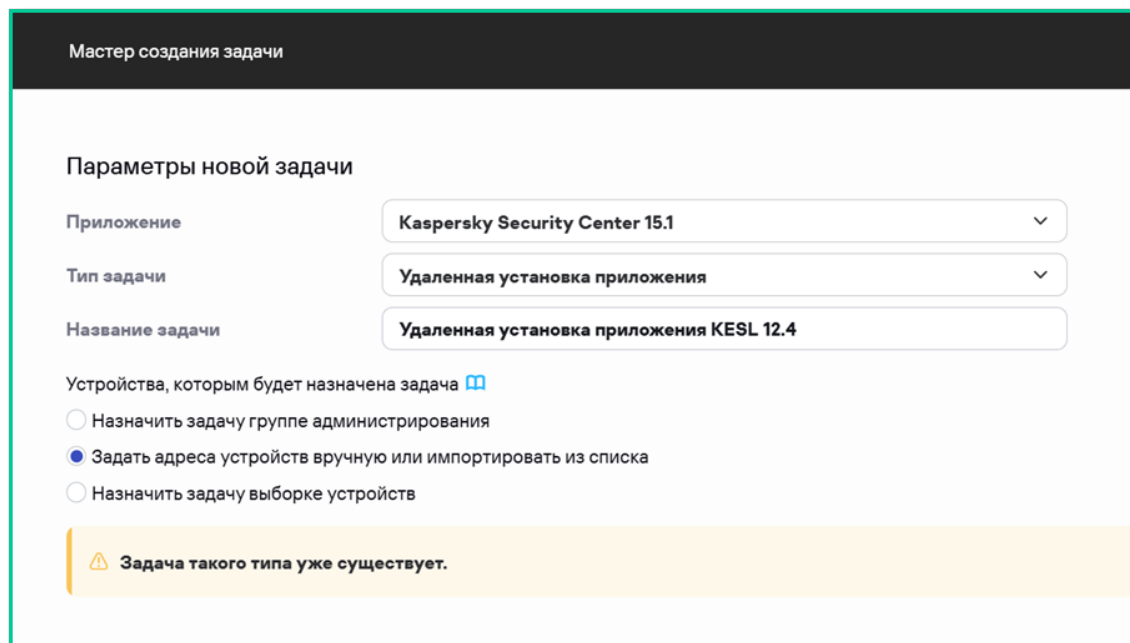
2.1. Подготовка сервера к установке

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. Установка KESL 12.2+ на сервер

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)



Мастер создания задачи

Параметры новой задачи

Приложение: Kaspersky Security Center 15.1

Тип задачи: Удаленная установка приложения

Название задачи: Удаленная установка приложения KESL 12.4

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

☐ Назначить задачу группе администрирования

☒ Задать адреса устройств вручную или импортировать из списка

☐ Назначить задачу выборке устройств

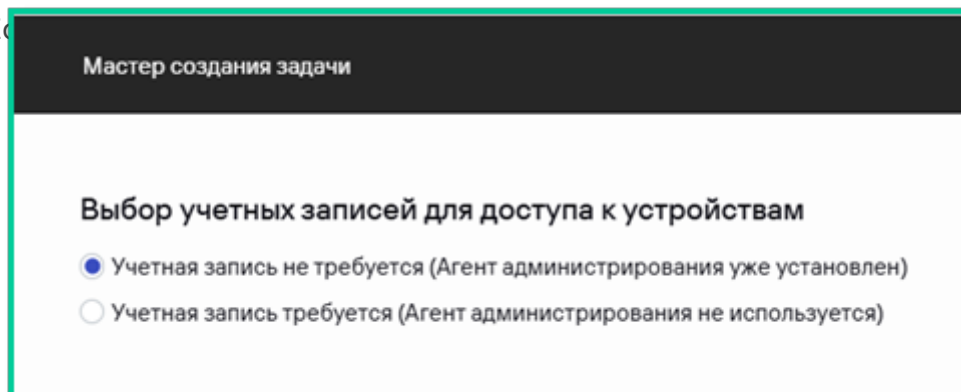
⚠ Задача такого типа уже существует.

□ □ Скриншот 1: Удаленная установка программы

4. Выберите:

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

5. Если требуется, выберите учетную запись администратора. Если не требуется, нажмите «Далее»



Мастер создания задачи

Выбор учетных записей для доступа к устройствам

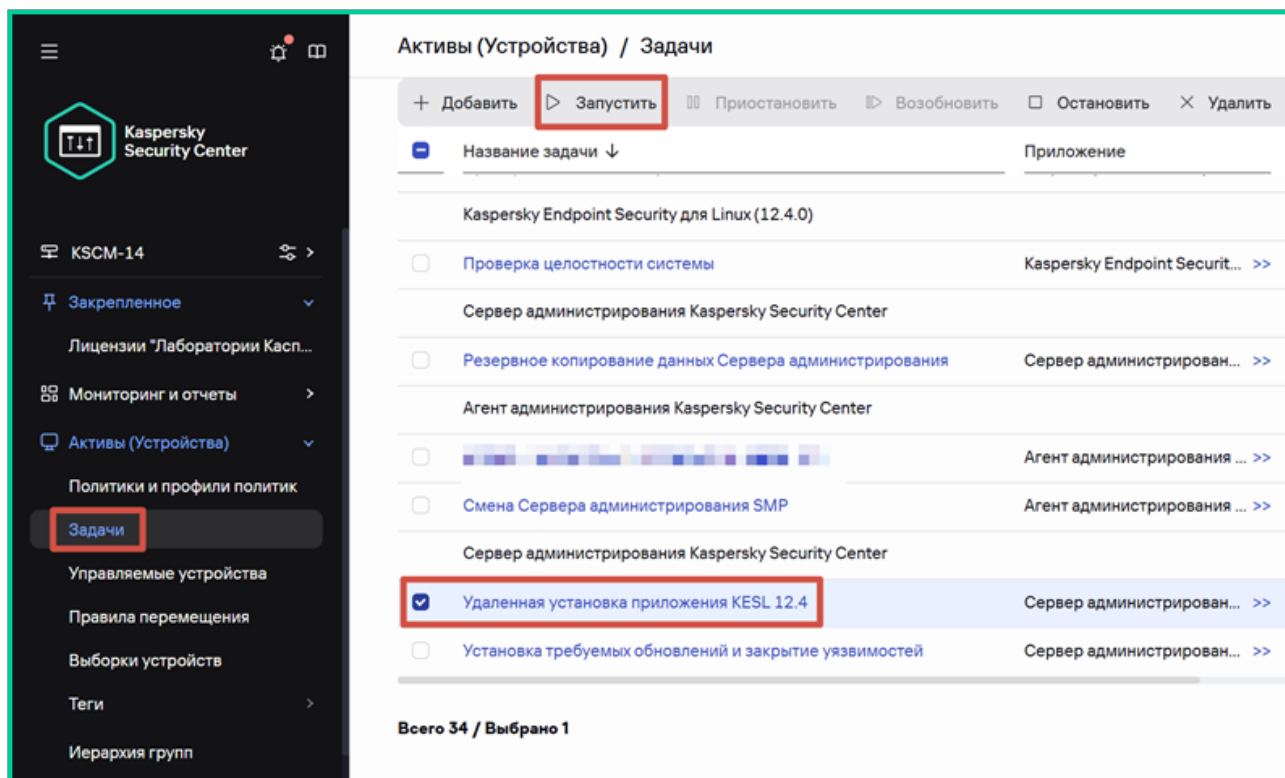
☒ Учетная запись не требуется (Агент администрирования уже установлен)

☐ Учетная запись требуется (Агент администрирования не используется)

□ □ 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

Мастер создания задачи

Параметры новой задачи

Приложение

Kaspersky Endpoint Security для Linux (12.4.0)

Тип задачи

Добавление ключа

Название задачи

Добавление ключа KESL

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 4: Добавление ключа KESL

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

Мастер создания задачи

Добавление ключа

☐ Использовать ключ в качестве резервного

Информация о лицензии

Лицензионный ключ:

Тип лицензии:

Коммерческая

Срок действия лицензии:

368 дней

Действует до:

2027-01-17 03:00:00

Ограничение:

49 устройств

Описание:

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

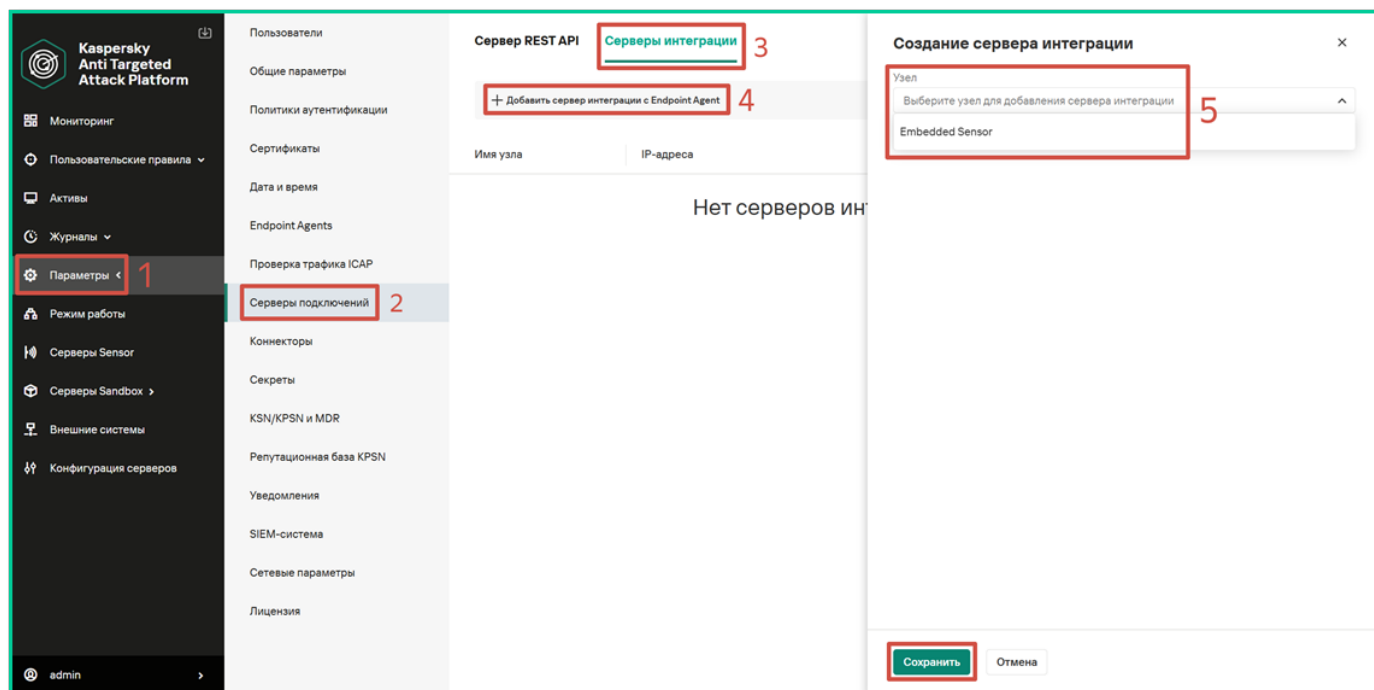
■ **Скриншот 5:** Использовать ключ в качестве резервного

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 Embedded Sensor, так и внешний узел, установленный с ролью Sensor.

Создание сервера интеграции

Узел
Embedded Sensor

Сертификаты для клиентов

☒ Проверять сертификаты клиентов

ОтпечатокD321D080A4D9442A4A5A6D8C247E99F77186A3B5CEE061C9F4D75F6DE6A9B7B2

Срок действия13.05.2076

+ Создать новый сертификат

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

5. Вы

Сервер REST APIСерверы интеграции

+ Добавить сервер интеграции с Endpoint Agent

Имя узла	IP-адреса
Embedded Sensor	10.68.85.180, 198.18.255.1, 198.19.11, 198.19.0.1

Генерация нового файла свертки

Сертификат для клиентов
Срок действия: 13.05.2076, отпечаток сертификата: A99B5CD35FB3F92930AD...

Пароль доступа к сертификату

Введите пароль

Повторите пароль

Создать файл сверткиОтмена

Embedded Sensor

Изменить

Включить

Получить файл свертки для клиентов

Имя узла	Embedded Sensor
Статус	Выключен
IP-адреса	10.68.85.180 198.18.255.1 198.19.11 198.19.0.1 8085

Информация о сертификате сервера интеграции

Требуется некоторое время для применения изменений.

Отпечаток сертификата	774016A7F3E8F74C550479B2CDFB66943C8EDDB24A223F38175B78AFCD90F4A5
Срок действия	13.05.2076

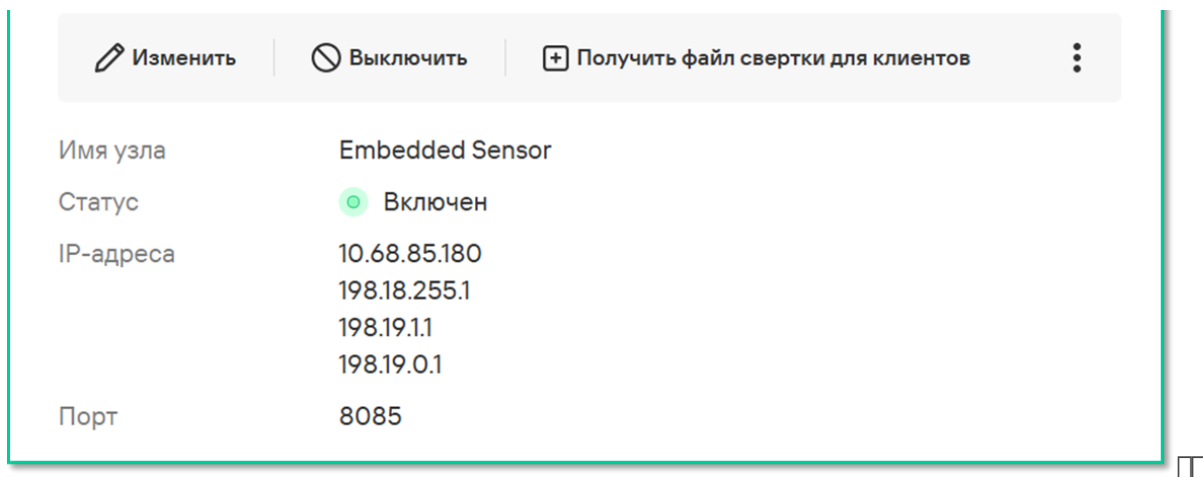
Информация о сертификатах для клиентов

Отпечаток сертификата	A99B5CD35FB3F92930ADA71261B1536F8CA589B30138D340586D02685766CBDC
Срок действия	13.05.2076

Загруженность
Запросов в секунду0

Скриншот 8: Будет выгружен архив с сертификатами.

6. Включить сервер интеграции.



Скриншот 9: сервер включен.

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

1. Устройства → Политики → Добавить → KESL 12.2+

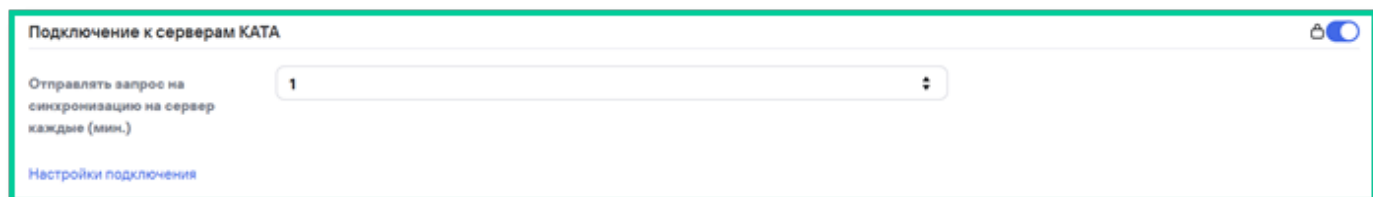
2. В мастере выберите **стандартный режим**

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

4. Включите компонент

5. Нажмите «**Настройки подключения**»

- Загрузите **TLS-сертификат**



Настройки подключения к серверам

Время ожидания соединения с сервером

Время ожидания (сек.)

10

Сертификат сервера

kata-proxy-b23291aa-d8dd-4eda-8d89-2eab02ca55f3

0

Загрузите файл сертификата.

Серийный номер

16952d023e957345

Субъект сертификата

kata-proxy-b23291aa-d8dd-4eda-8d89-2eab02ca55f3

Издатель

kata-proxy-b23291aa-d8dd-4eda-8d89-2eab02ca55f3

Дата выпуска

Thu Feb 19 2026 12:00:14 GMT+0000 (Coordinated Universal Time)

Дата истечения

Fri Feb 07 2076 12:00:13 GMT+0000 (Coordinated Universal Time)

Дополнительная защита подключения

☒ Использовать двустороннюю аутентификацию

certificate

0

Пароль от криптоконтейнера*

.....

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

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

+ Добавить

Удалить

☐	Адрес	Порт
☐	10.68.85.121	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:

Мониторинг

Алерты

События в трафике сети

Пользовательские правила

Хранилище

Активы

Карта сети

Риски и аномалии

Отчеты

Журналы

Параметры

Серверы Sensor

АКТИВЫ

Устройства

Пользователи

Исполняемые файлы

Endpoint Agents

Адресные пространства

Активный опрос

+ Добавить устройство

Объединить устройства

Изменить статус

Показать связи

Создать задание

Сбросить открытый ключ

Обновление

8 устройств

Поиск устройств

Состояние безопасности

Значимость устройств

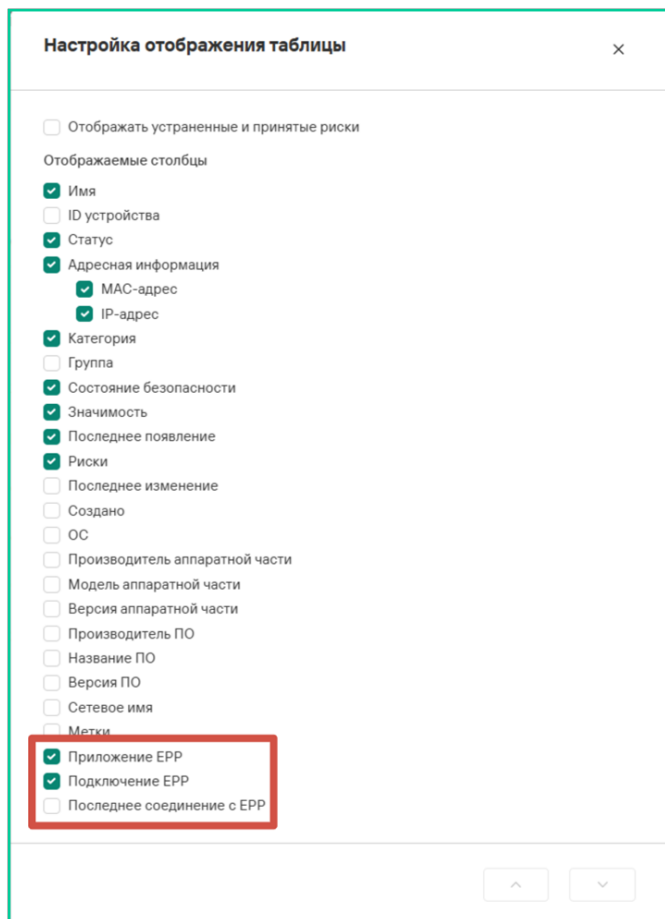
Низкая

Средняя

Высокая

Фильтр по умолчанию

Имя	Статус	Адресная информация	Категория	Состоян...	Значимость	Последнее появление	Риски	При...	Подключе...
	Разрешенное	00:50:56:89:2a:59; 10.68...	Рабочая станция	Критичес...	Средняя	05.06.2026 23:05:22		Kaspersky En...	Неактивное
	Разрешенное	00:50:56:a8:f5:b7	Сервер	Критичес...	Высокая	01.06.2026 22:36:45		Kaspersky En...	Неактивное
	Разрешенное	00:50:56:89:73:73; 10.68...	Сервер	Критичес...	Высокая	08.06.2026 16:24:57		Kaspersky En...	Активное
	Разрешенное	00:50:56:89:6b:93; 10.68...	Сервер	Критичес...	Высокая	08.06.2026 16:25:07		Kaspersky En...	Активное
	Разрешенное	00:50:56:a8:de:1a; 10.68...	Сервер	Критичес...	Высокая	05.06.2026 23:05:41		Kaspersky En...	Неактивное
	Разрешенное	00:50:56:89:9d:94; 10.68...	Рабочая станция	Критичес...	Средняя	05.06.2026 23:06:52		Kaspersky En...	Неактивное
	Разрешенное	Несколько значений	Рабочая станция	Критичес...	Средняя	03.06.2026 23:04:19		Kaspersky En...	Неактивное
	Разрешенное	00:50:56:a8:52:3d; 10.68...	Рабочая станция	Критичес...	Средняя	08.06.2026 16:25:11		Kaspersky En...	Активное



❏ **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**

```

root@~ -machine:/home/test-lena# kesi-control --app-info
Название: Kaspersky Endpoint Security 12.4 для Linux
Версия: 12.4.0.1225
Политика: Kaspersky Security Center

Информация о лицензии приложения: Ключ действителен
Дата окончания срока действия лицензии Kaspersky Endpoint Security: 2027-04-24 00:00:00
Статус файла MDR Blob: Не загружен

Состояние резервного хранилища: Наиболее старый объект будет удален 2026-06-04 17:30:33
Использование резервного хранилища: Заполнено 0% резервного хранилища

Дата последнего запуска задачи Scan_My_Computer: Никогда не запускалась

Дата последнего выпуска баз приложения: 2026-06-15 13:48:00
Базы приложения загружены: Да

Состояние обновляемого модуля ядра: Запущен

Использование Kaspersky Security Network: Выключено

Инфраструктура Kaspersky Security Network: Kaspersky Security Network

Интеграция с Kaspersky Managed Detection and Response: Выключена

Интеграция с Kaspersky Endpoint Detection and Response Optimum: Не поддерживается лицензией

Защита от файловых угроз: Задача доступна и выполняется

Мониторинг контейнеров: Недоступно из-за ограничений лицензии

Контроль целостности системы: Недоступно из-за ограничений лицензии

Управление сетевым экраном: Задача доступна и не выполняется

Защита от шифрования: Задача доступна и не выполняется

Защита от веб-угроз: Задача доступна и не выполняется

Контроль устройств: Задача доступна и не выполняется

Проверка съемных дисков: Задача доступна и не выполняется

Защита от атак BadUSB: Задача доступна и выполняется

Защита от сетевых угроз: Задача доступна и не выполняется

Анализ поведения: Задача доступна и выполняется

Контроль приложений: Задача доступна и не выполняется

Веб-Контроль: Задача доступна и не выполняется

Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise): Задача доступна и выполняется

Интеграция с Sandbox: Задача доступна и выполняется

Интеграция с Kaspersky Unified Monitoring and Analysis Platform: Недоступно из-за ограничений лицензии
Интеграция с Kaspersky Network Detection and Response (KATA): Задача доступна и выполняется

Защита от почтовых угроз: Задача доступна и выполняется

Действия после обновления: Модуль приложения обновлен. Перезапустите приложение.

root@testlena-virtual-machine:/home/test-lena#

```

❏ **Скриншот 13:** результаты вывода команды «kesi-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