?????????? ?? ????????? ? ????????? ????????? Sensor ? ????/NDR 8.0

> **Информация:** Приведенная на данной странице информация, является разработкой команды **pre-sales** и/или **AntiAPT Community** и **НЕ является** официальной рекомендацией вендора.

Версия платформы: KATA / NDR 8.0

Источник: Установка компонента Sensor

Официальная документация: Справка Kaspersky Anti Targeted Attack Platform 8.0

? Введение

Компонент **Sensor** в платформе **Kaspersky Anti Targeted Attack (KATA)/NDR 8.0** предназначен для сбора, фильтрации и анализа сетевого трафика в распределённых и высоконагруженных инфраструктурах. Он выступает в роли выделенного сервера, обеспечивающего эффективное обнаружение целевых атак, скрытых угроз и подозрительной активности в сети.

Установка Sensor требуется в следующих сценариях:

- Обработка SPAN-трафика объёмом **свыше 1 Гбит/с**, когда центральный узел (Central Node) не справляется с нагрузкой.
- Подключение **удалённых филиалов или изолированных сегментов сети**, где важно локально анализировать трафик и минимизировать нагрузку на каналы связи.
- Использование в качестве **прокси-сервера** для Endpoint Agent, что позволяет централизованно управлять соединениями и обеспечивать безопасность.

? Назначение компонента Sensor

Компонент **Sensor** выполняет ключевую функцию по анализу сетевых потоков и передаче данных на **Central Node** для дальнейшего корреляционного анализа и формирования инцидентов. Он не имеет веб-интерфейса — вся настройка осуществляется через SSH в псевдо-веб интерфейсе.

Основные режимы работы:

- **Мониторинг SPAN/TAP-трафика** — позволяет анализировать копии сетевого трафика в реальном времени.
- **Локальный анализ в филиалах** — снижает объём передаваемых данных и повышает скорость реагирования.
- **Прокси для Endpoint Agent** — обеспечивает безопасное и контролируемое подключение агентов к платформе.

Установка и подключение компонента Sensor в KATA/NDR 8.0

В данной статье подробно описаны все этапы установки и подключения компонента **Sensor** — от подготовки виртуальной машины до интеграции с **Central Node**.

Подробнее о работе компонента Sensor

> ⚠ **Перед началом** обязательно ознакомьтесь с официальными требованиями к оборудованию, сетевой конфигурации и режиму загрузки (UEFI).

Подготовка к установке

Подготовка к установке

Требования к оборудованию:

Компонент	Требование
Режим загрузки	Обязательно **UEFI**
Процессор	Поддержка **BMI2, AVX, AVX2**
Жёсткие диски	Только **SAS HDD 10K rpm и выше**
RAID	Только **аппаратный RAID**. Программный RAID не поддерживается

1.3. Платформы виртуализации

Поддерживаются следующие платформы:

- **VMware ESXi 6.7.0 или 7.0**

- **KVM**
- **ПК СВ "Брест" 3.3**
- **"РЕД Виртуализация" 7.3**
- **zVirt Node 4.2**

Решение **не поддерживает** **Microsoft Hyper-V**.

> ◻◻ **Примечание по KVM:**
>
> - ОС: **Debian GNU/Linux 12**
>
> ```
> cat /proc/cpuinfo | grep flags
> ```

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

Платформа	**Особенности**
VMware ESXi	Виртуальная машина требует на **10% больше CPU**, чем физический сервер. Тип виртуального диска: **Thick Provision**
ПК СВ "Брест" / "РЕД Виртуализация"	При использовании **KEDR** или **KATA+KEDR** увеличьте минимальное количество логических ядер на **20%**

> ◻◻**Примечание:**
> Если вы хотите устранить уязвимости типа **Spectre** и **Meltdown** на уровне гипервизора, необходимо дополнительно увеличить количество логических ядер в **1,5 раза** относительно уже увеличенного значения.

1.5. Требования к процессору

Центральный процессор должен поддерживать следующие наборы инструкций:

- **BMI2**
- **AVX**
- **AVX2**

> ◻◻ **Проверка поддержки:**

- Выполните в терминале команду: **cat /proc/cpuinfo | grep flags**
- Убедитесь, что в выводе присутствуют: **avx avx2 bmi2**
- Либо выполните следующую команду:

```
grep -E 'avx|avx2|bmi2' /proc/cpuinfo
```

 Если хотя бы один из этих флагов отсутствует, установка компонентов **не будет поддерживаться**.

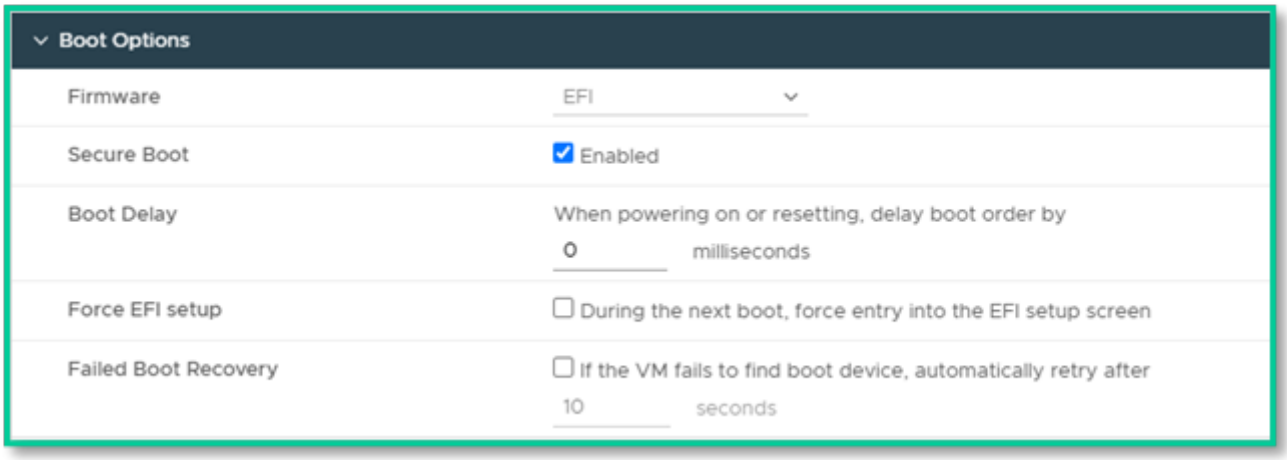
⚠ **Ограничения Sensor**

- Для компонента **Sensor** действуют следующие ограничения:
  - **Для захвата сетевого трафика на максимальной скорости 10 Гбит/с** могут использоваться только компоненты Sensor, установленные на **отдельных физических серверах**. Виртуальные машины не рекомендуются для таких нагрузок.
  - **При захвате FTP-трафика на скорости до 10 Гбит/с** возможен **высокий уровень потерь пакетов** из-за особенностей обработки протокола. Рекомендуется мониторинг и тестирование в реальных условиях.
  - **Настройка параметров проверки ICAP-трафика в режиме реального времени** на серверах с компонентом Sensor **возможна только в режиме Technical Support Mode** через CLI. Прямой доступ через веб-интерфейс отсутствует.

????????? ??????????? ?????? (???? ?????????)

Если используется VMware:

1. Откройте настройки ВМ.
2. Перейдите: **Options → Boot Options → Firmware**.
3. Выберите **UEFI**.



Скриншот: Настройки виртуальной машины с выделенным пунктом UEFI.

⚙ Установка компонента Sensor (пошагово)

Установка запускается автоматически после загрузки с образа.

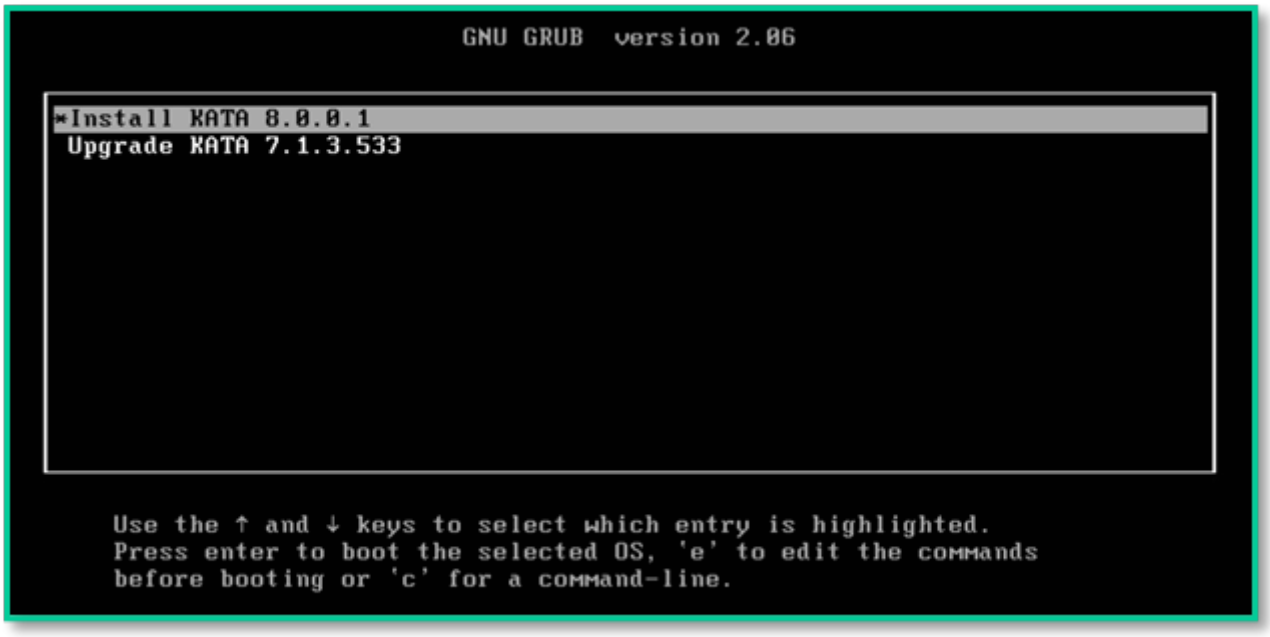
Шаг 1: Загрузка образа

Скачайте образ

- **Физический сервер:** запишите на USB/DVD и загрузитесь.
- **Виртуальный сервер:** подключите ISO к ВМ.

При запуске системы выберите:

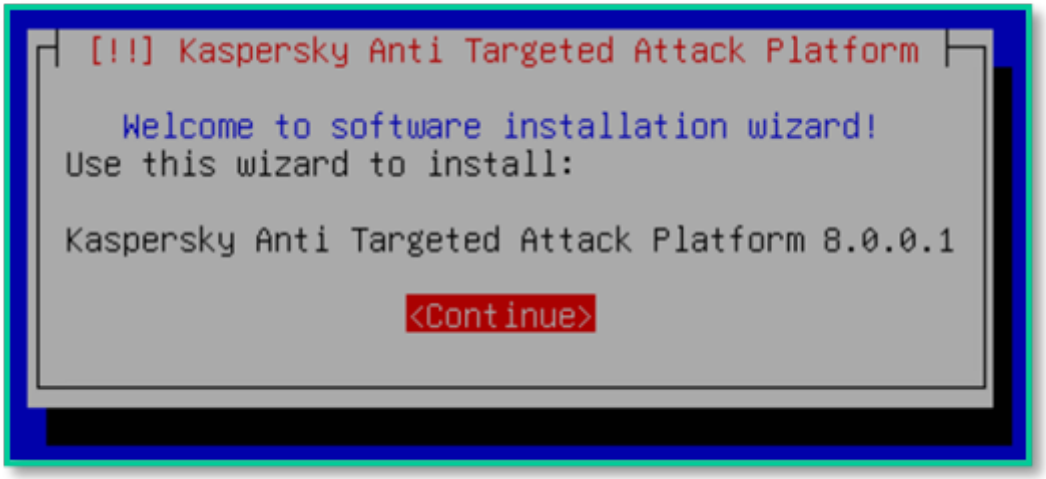
```
Install KATA 8.0.0.1
```



Скриншот 1: Экран загрузки с выделенным пунктом `Install KATA 8.0.0.1` в меню GRUB.

Шаг 2: Приветственное окно

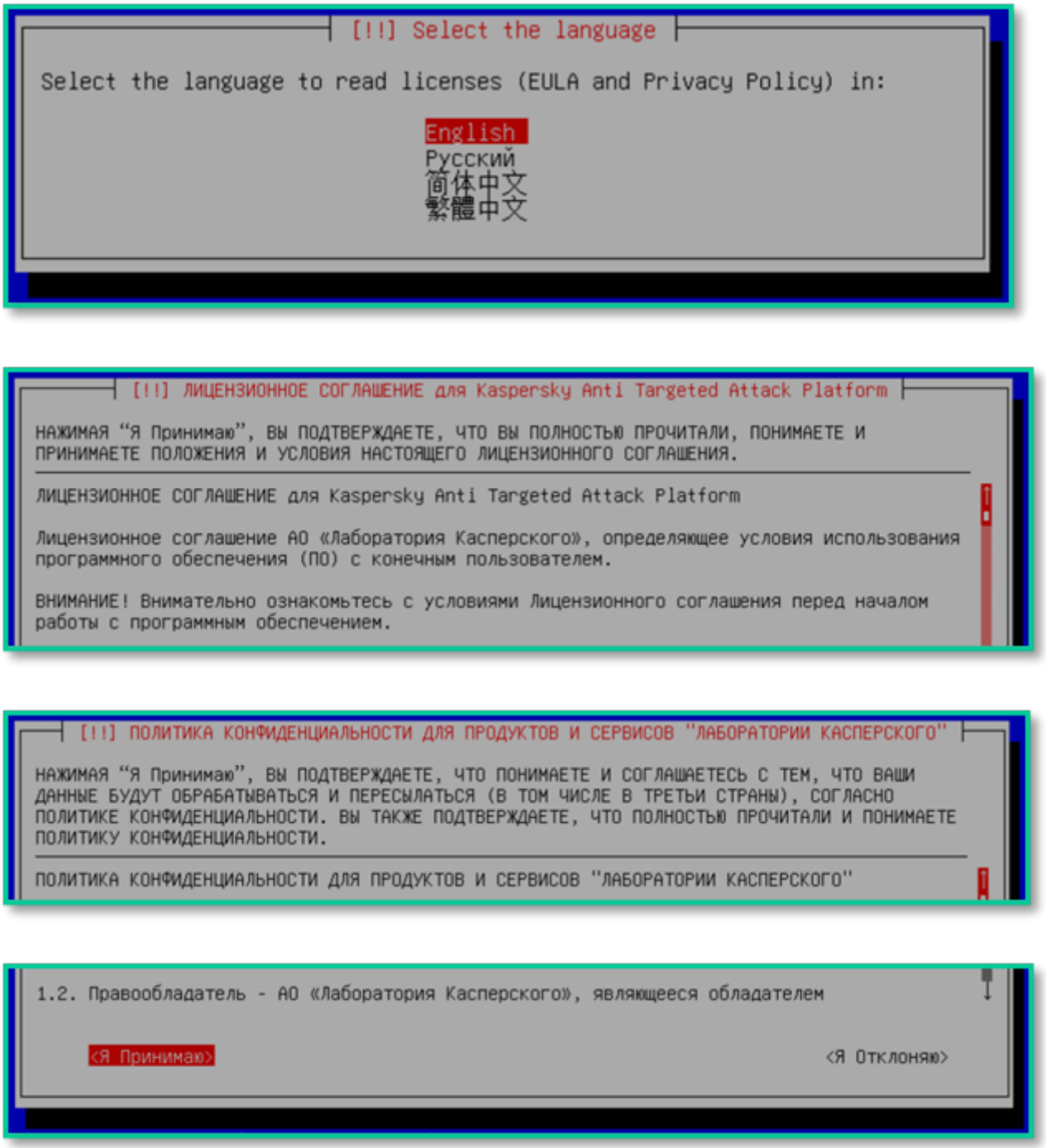
Нажмите: **Continue**



Скриншот 2: Приветственное окно установщика с кнопкой `Continue`.

Шаг 3: Лицензионное соглашение

1. Нажмите **TAB**, чтобы перейти к опции.
2. Выберите: **Я принимаю**
3. Нажмите **Enter**.



Скриншот 3: Окно лицензионного соглашения с активной кнопкой `Я принимаю`.

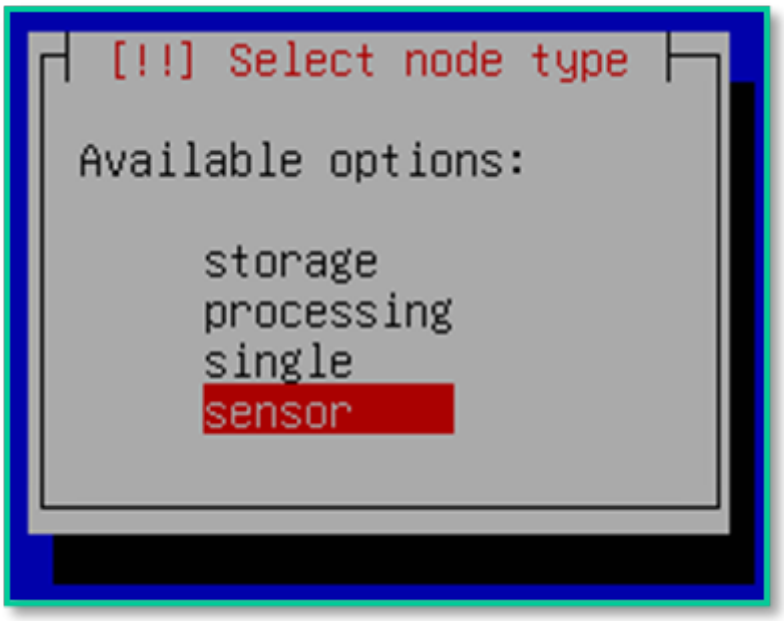
Шаг 4: Выбор роли сервера

При установке доступны следующие роли сервера:

Роль	Описание
single	Central Node + Sensor на одном сервере (подходит для тестовых и малых сред)

sensor	Только **Sensor** (выделенный сервер для обработки трафика)
storage	Сервер хранения данных в кластерной конфигурации
processing	Обрабатывающий сервер (включает функциональность Sensor)

Для установки **выделенного Sensor** выберите **sensor** и нажмите **Enter**.

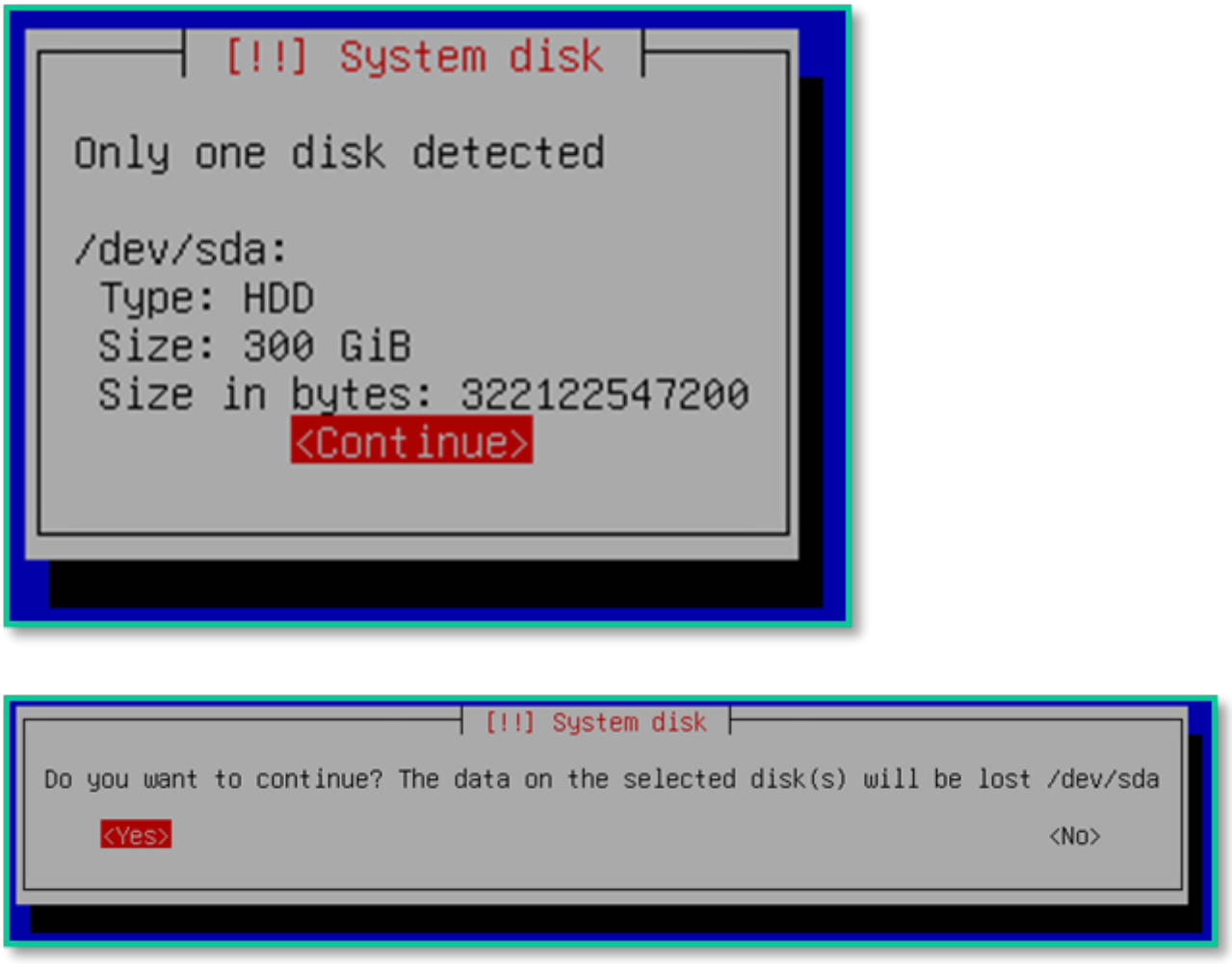


Скриншот 4: Меню выбора роли сервера с выделенным пунктом `sensor`.

Шаг 5: Подтверждение очистки диска

Система предупреждает об очистке дискового пространства.

Выберите: **Yes** и нажмите **Enter**.



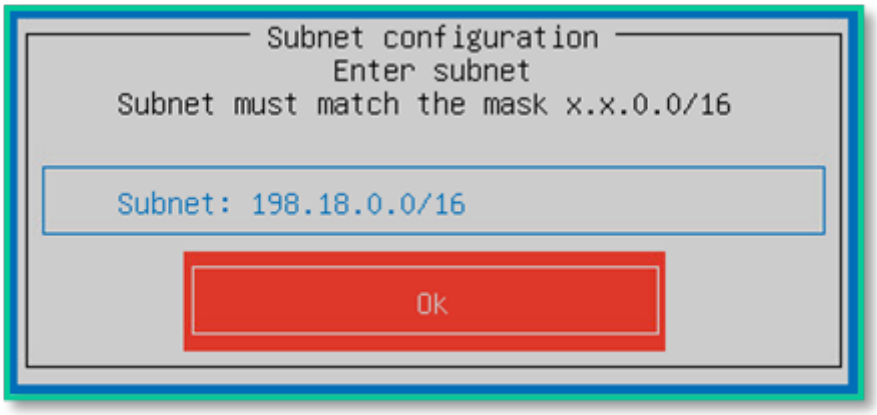
Скриншот 5: Окно предупреждения о необходимости очистки диска с кнопкой `**Yes**`.

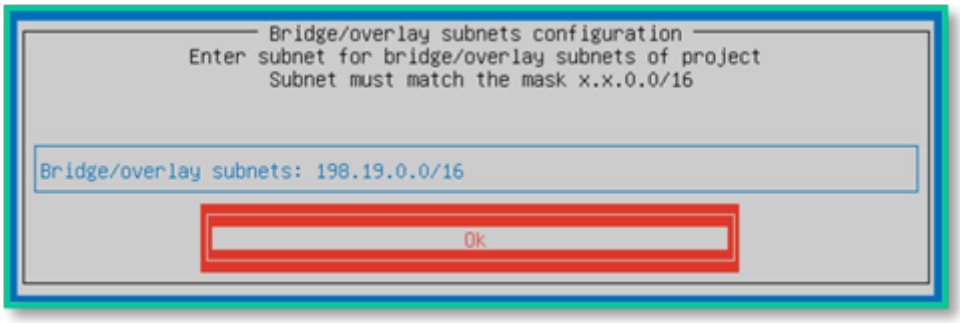
Шаг 6: Настройка кластерной подсети

Выбор маски сети для адресации серверов кластера.

> *“В данном пункте настройка производиться только при установке кластера “KATA”, если установка выполняется не для кластера, то выбираем пункт “1”.*

- Для выбора значения по умолчанию: 198.18.0.0/16 нажмите на клавишу **Enter**.
- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.
- Маска должна соответствовать шаблону x.x.0.0/16.

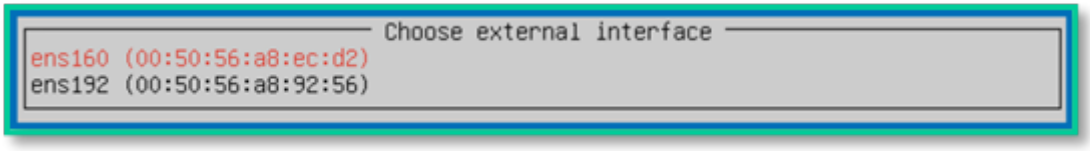




Скриншот 6: Экран настройки кластерной подсети.

Шаг 7: Выбор сетевого интерфейса (Management Interface)

Выберите один из доступных интерфейсов (например, `eth0`) и нажмите **Enter**.



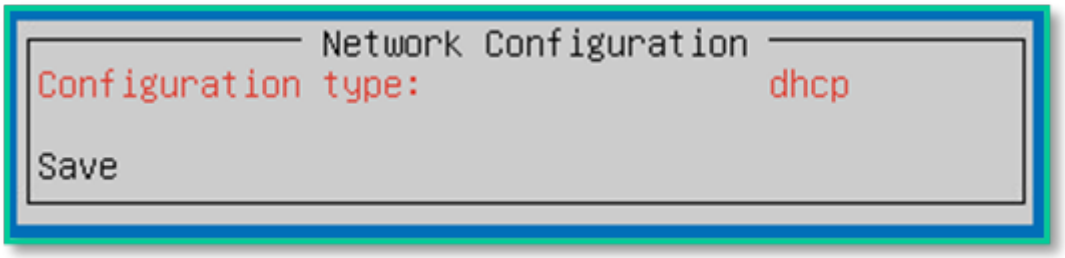
Скриншот 7: Список сетевых интерфейсов с подсказкой `**Выберите один из доступных сетевых интерфейсов**`.

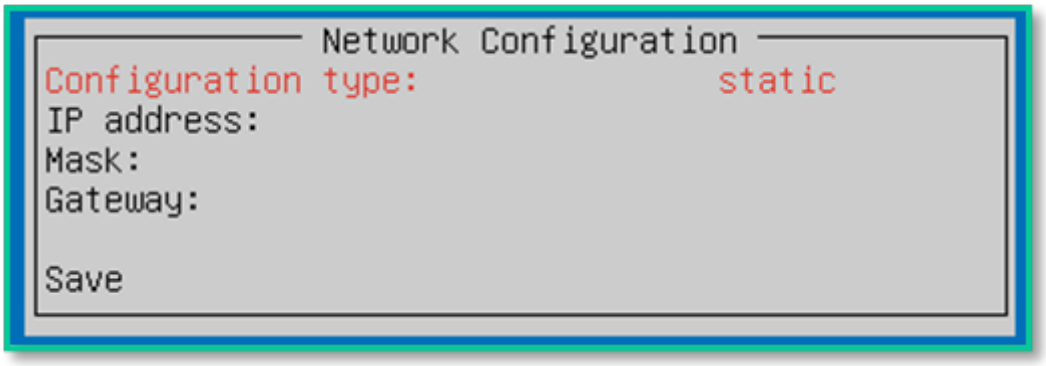
Шаг 8: Настройка IP-адреса

Выберите способ назначения IP:

- **DHCP** — автоматическое получение.
- **Static** — ручной ввод.

После настройки нажмите: **Save**

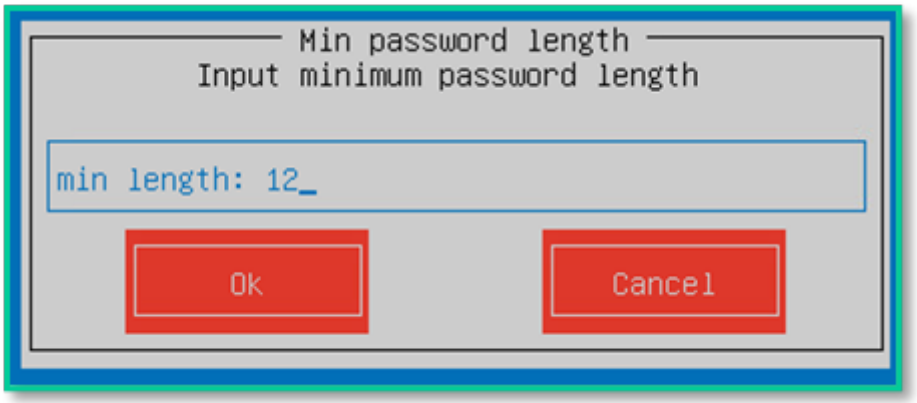


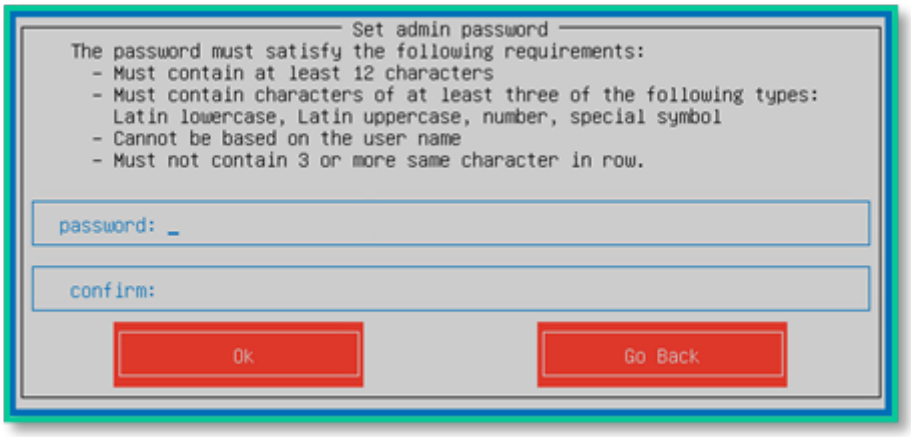


Скриншот 8: Меню настройки IP-адреса с опциями `**DHCP**` и `**Static**`, кнопка `**Save**`.

Шаг 9: Настройка учётной записи admin

1. Убедитесь, что длина пароля — **минимум 12 символов**.
2. Введите пароль.
3. Нажмите **OK**.





Скриншот 9: Окно настройки пароля администратора с подсказкой о минимальной длине — 12 символов.

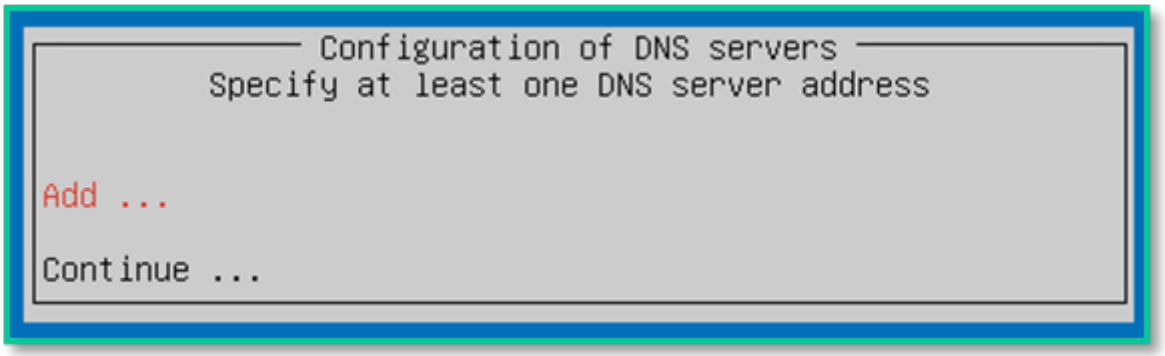
Шаг 10: Настройка DNS-серверов

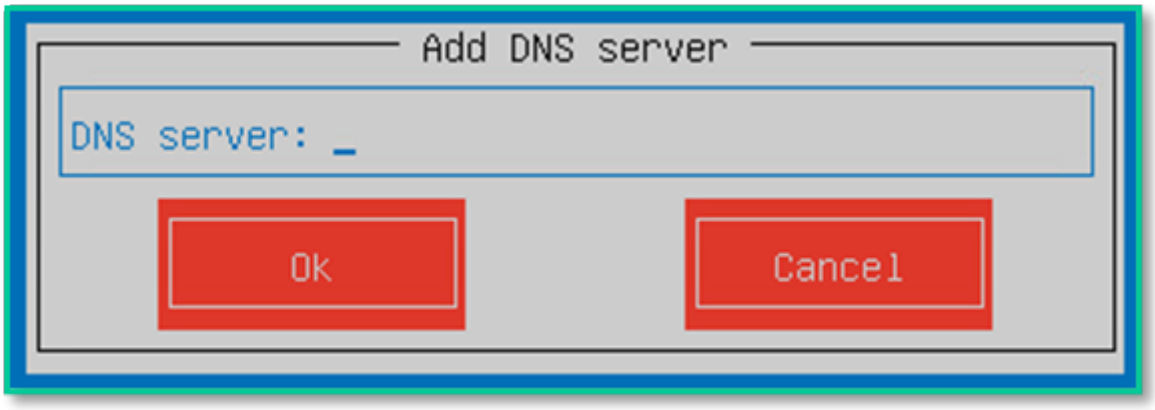
> ⚠ **ВАЖНО:** Указание DNS сервера обязательно, даже если платформа будет установлена в изолированной сети без доступа к внутреннему или внешнему DNS серверу. В такой конфигурации можно указать просто адрес, необязательно к существующему узлу, так как данный пункт конфигурации заложен в логику работы системы. Не указав адрес в данном пункте, может привести к ошибке в работе платформы и **загрузке ЦП на 100%.** Можно указать любой IP (например, `1.1.1.1`), чтобы избежать 100% загрузки CPU.

Введите:

- Основной DNS (IPv4)
- Дополнительный DNS (IPv4)

После ввода **дважды нажмите Enter**.





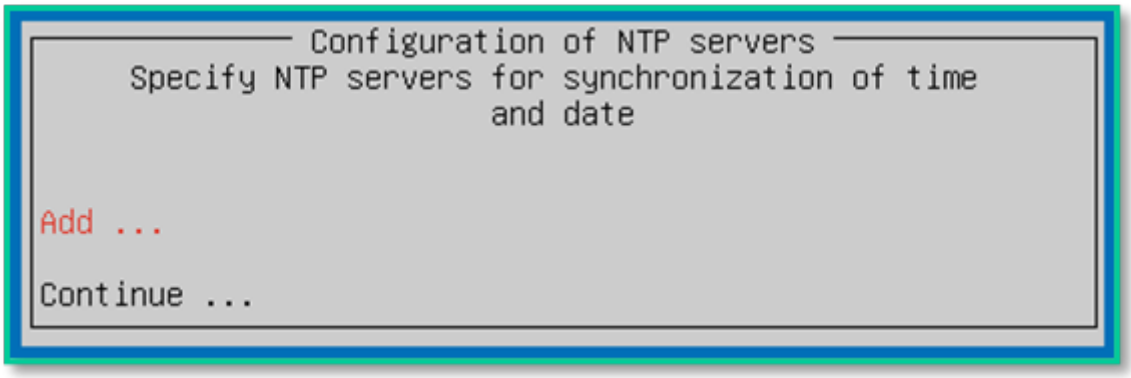
Скриншот 10: Поле ввода DNS-серверов с подсказкой: `**ВАЖНО: Указание DNS обязательно...**`.

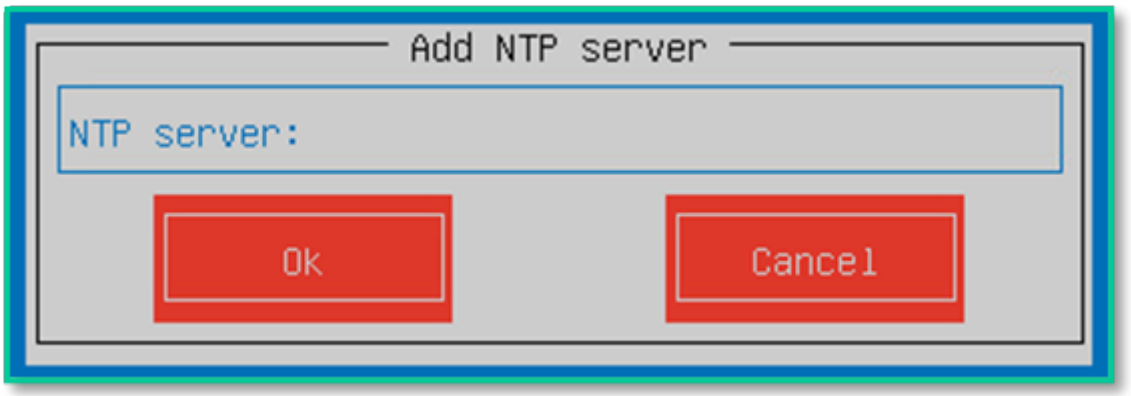
Шаг 11: Настройка NTP-сервера

Введите IP или доменное имя NTP-сервера (например, `ntp.kaspersky.com` или `10.10.0.100`).

При необходимости добавьте резервный сервер.

Завершите ввод **дважды нажав Enter**.



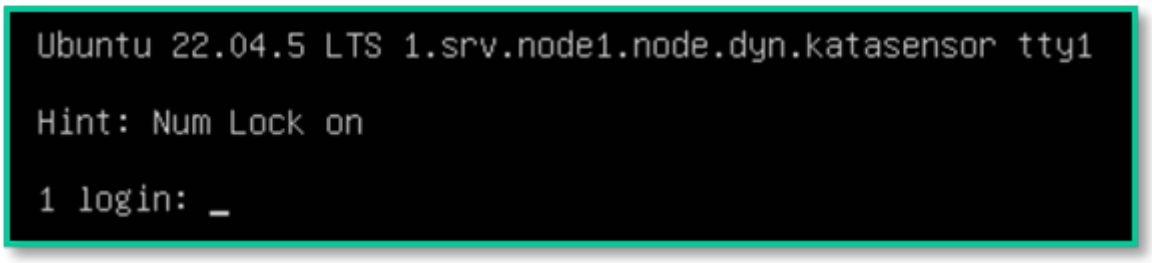


Скриншот 11: Окно настройки NTP-сервера с подсказкой: `Введите IP-адрес или имя NTP-сервера`.

Шаг 12: Завершение установки

Подождите завершения настройки. После окончания:

- Появится приглашение к вводу логина и пароля.
- **Sensor не имеет веб-интерфейса** — вся дальнейшая настройка через SSH.



Скриншот 12: Терминал с сообщением: `На данном этапе процесс установки завершен...`.

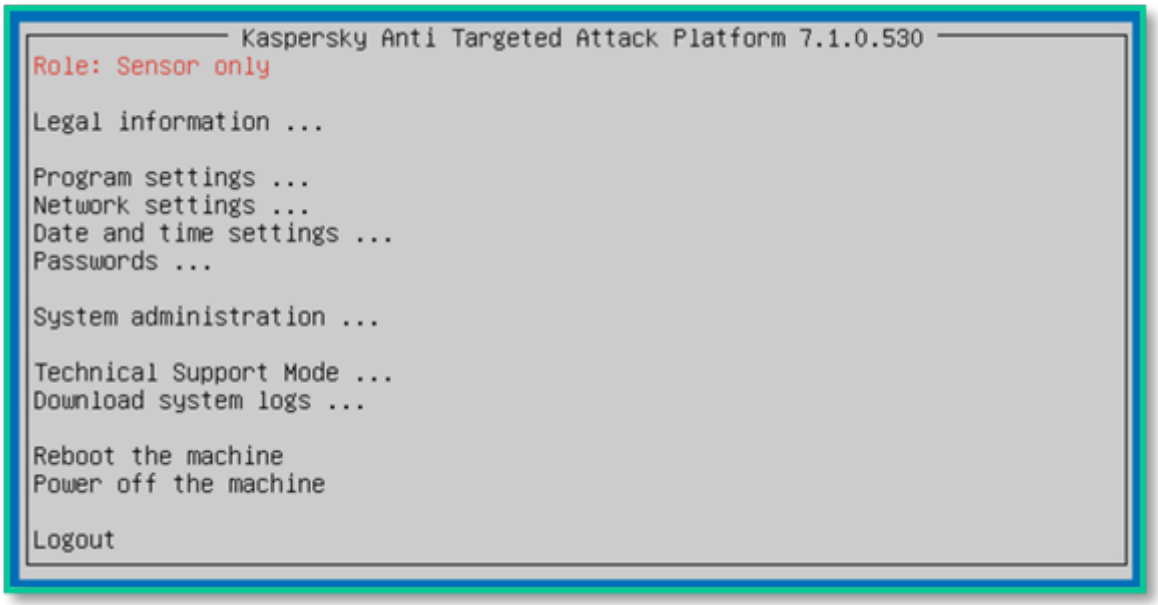
Получение IP-адреса (если использовался DHCP)

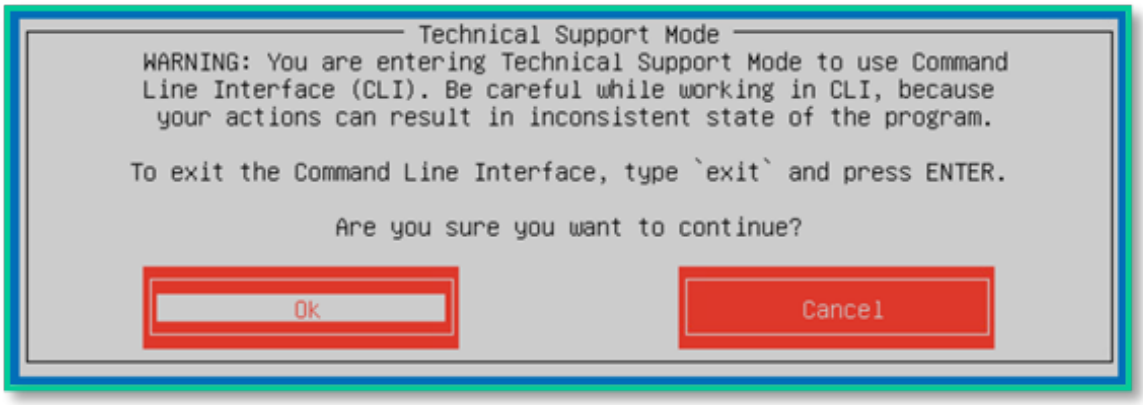
Если IP получен по DHCP, выполните:

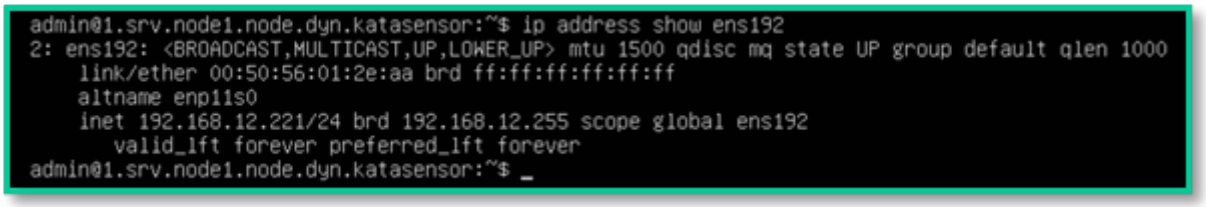
1. Подключитесь по SSH как `**admin**`.
2. Перейдите в **Technical Support Mode** → подтвердите переход в **CLI**.
3. Выполните команду:

```
ip address show eth0
```

(замените `eth0` на интерфейс, выбранный при установке)







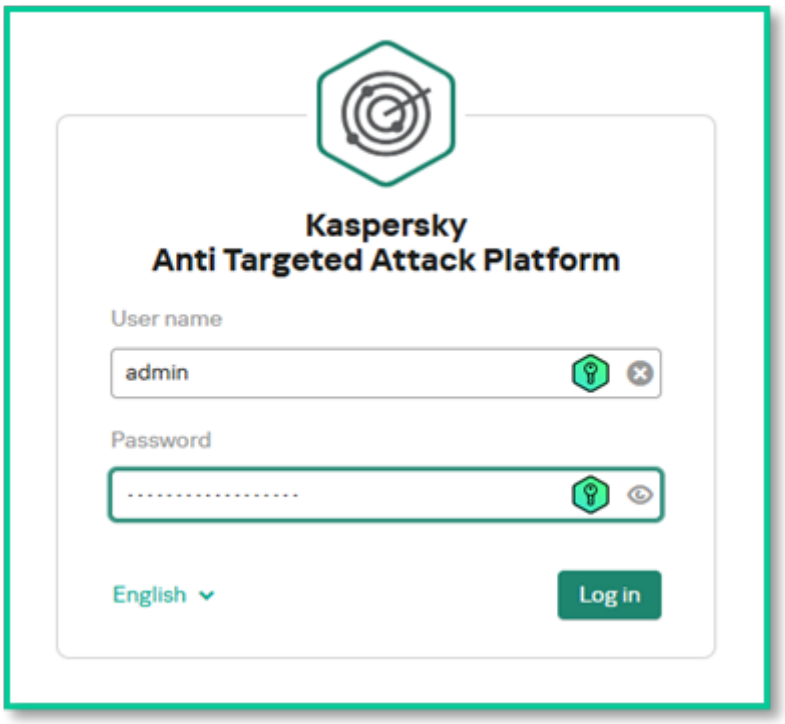
Скриншот 13: Терминал с выводом команды `ip address show`, где виден назначенный IP-адрес.

Подключение Sensor к Central Node (метод: "Автоматически по сети")

> **Рекомендуемый способ.** Требует доступа к Central Node и Sensor.

Шаг 1: Откройте веб-интерфейс Central Node

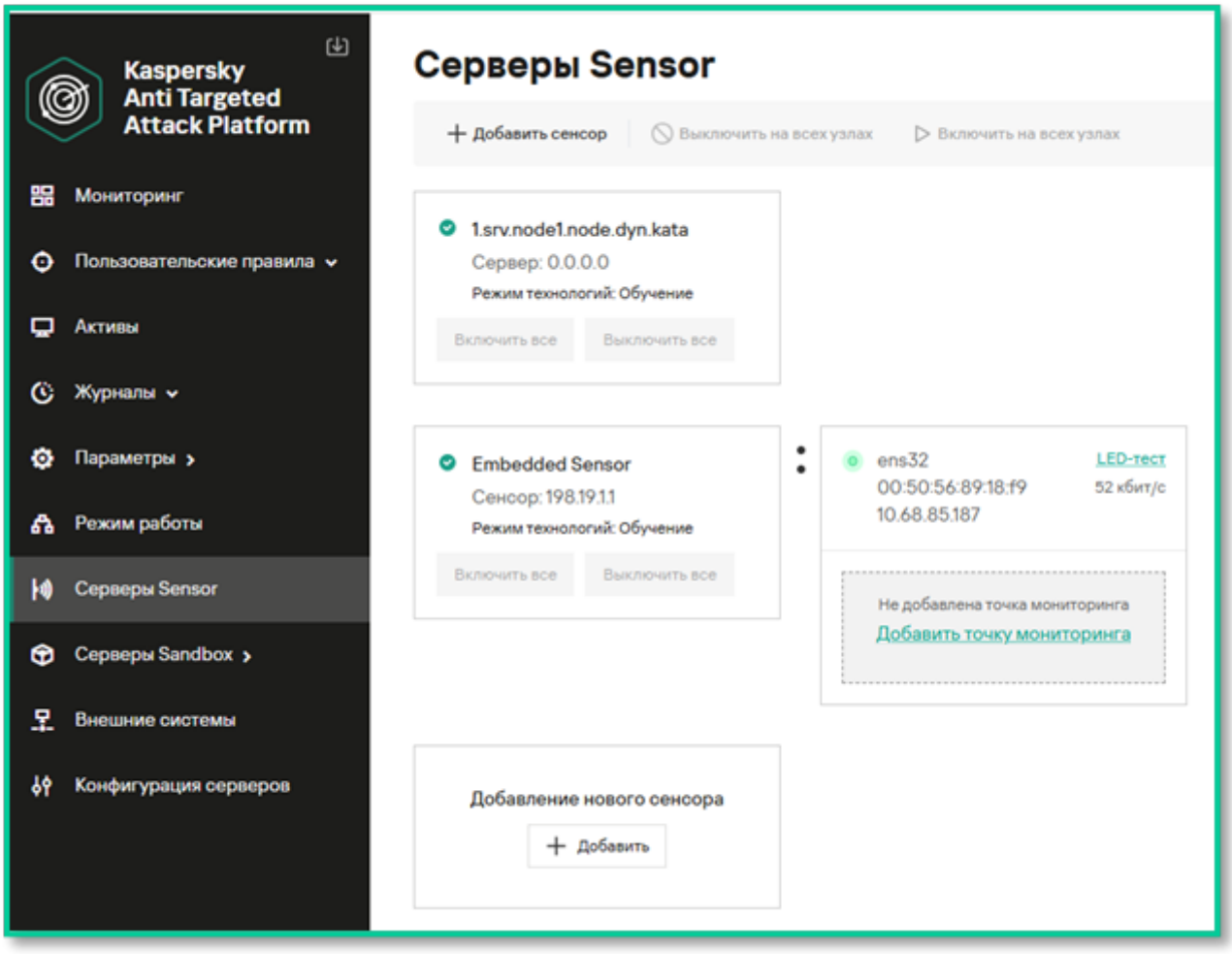
Перейдите по адресу: **https://<IP_Central_Node>:8443** и авторизуйтесь под учётной записью `**admin**`.

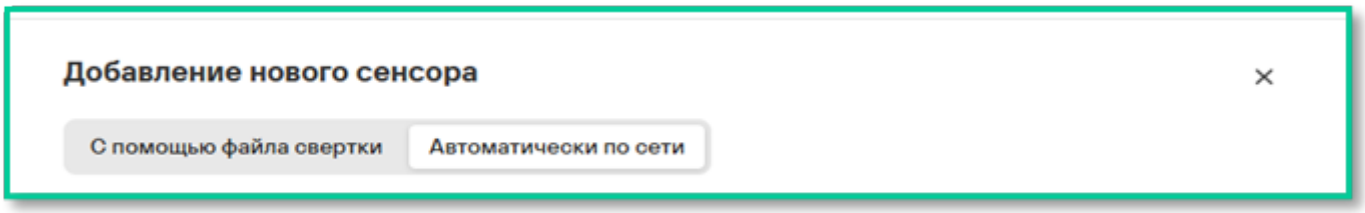


Скриншот 14: Страница входа в веб-интерфейс Central Node с полем ввода логина и пароля.

Шаг 2: Добавление нового Sensor

1. Перейдите в раздел: **Серверы Sensor**.
2. Нажмите: **Добавить сенсор**.
3. Выберите вкладку: **Автоматически по сети**.



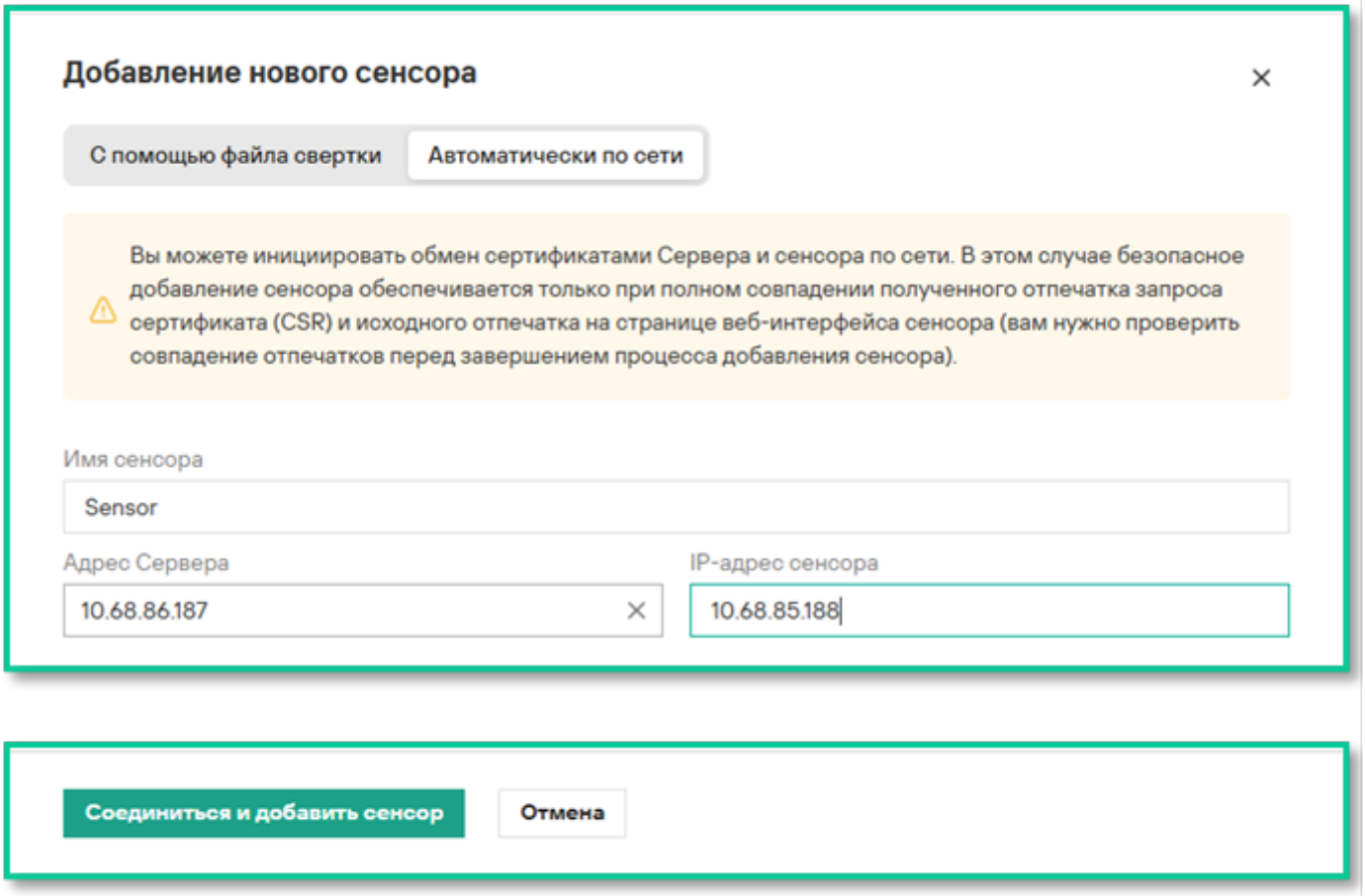


Скриншот 15: Окно "Добавление нового сенсора" с активной вкладкой "Автоматически по сети".

Шаг 3: Заполнение формы

Заполните поля:

Поле	Пример значения
Имя сенсора	`Sensor-Moscow`
Адрес сервера	`192.168.10.10` (IP Central Node)
IP-адрес сенсора	`192.168.20.15` (IP установленного Sensor)

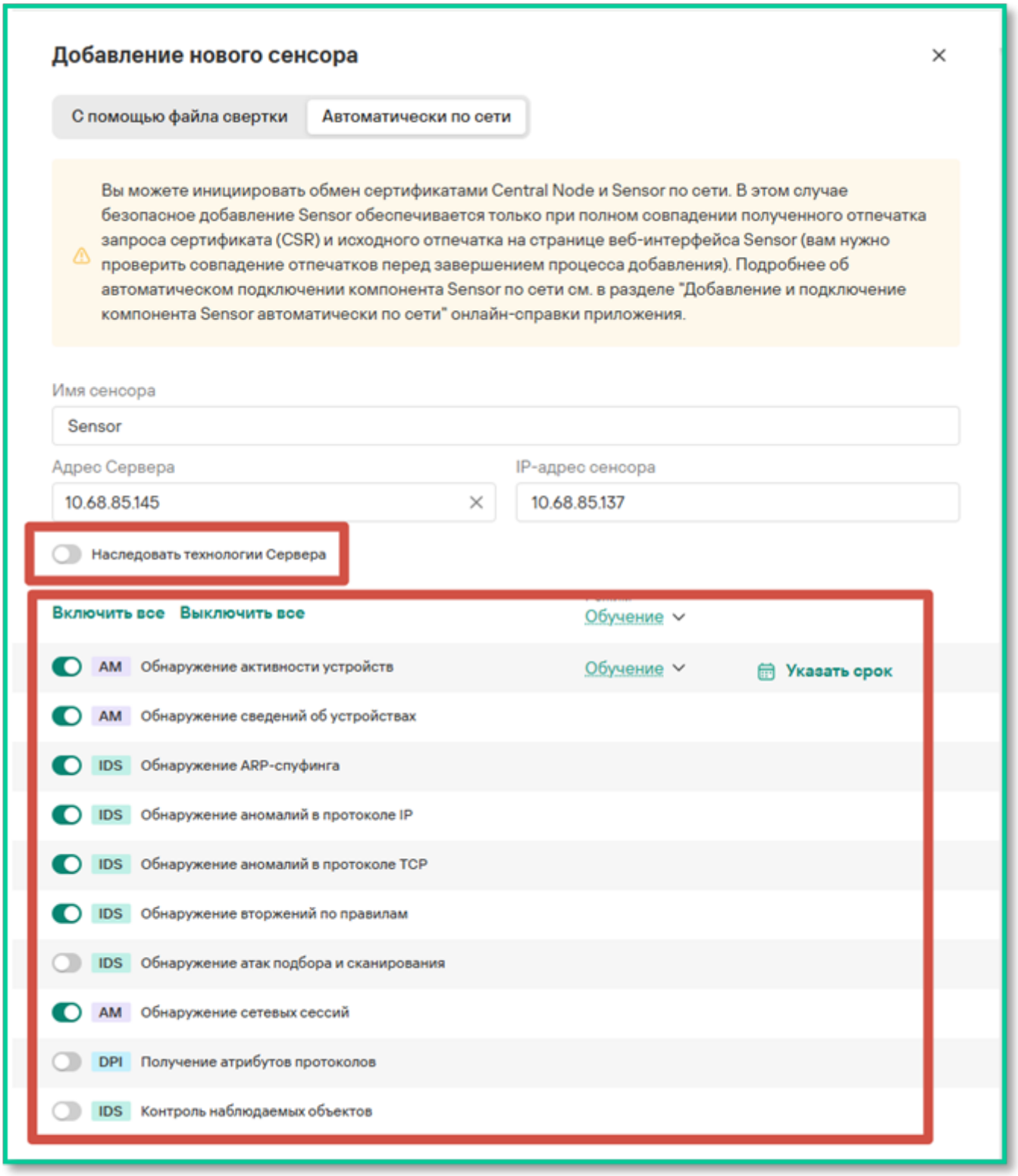


Скриншот 16: Форма с заполненными полями: имя, адрес сервера, IP-адрес сенсора.

Шаг 4: Наследование технологий Сервера

Если вы хотите, чтобы компонент Sensor или точка мониторинга автоматически получали параметры использования технологий, настроенные для родительского объекта, вы можете включить наследование технологий. При этом компонент Sensor получает параметры использования технологий, заданные для компонента Central Node, а точка мониторинга получает параметры, заданные для того компонента, на котором точка мониторинга была добавлена (Central Node или Sensor).

При необходимости вы можете выключить наследование технологий для компонента Sensor или точки мониторинга. Это позволит настроить на этом объекте специфические параметры использования технологий.



Скриншот 17: Форма с заполненными полями: имя, адрес сервера, IP-адрес сенсора.

Шаг 5: Создание SSH-туннеля

На ПК с доступом к Sensor выполните команду:

```
ssh -4 -L 9444:localhost:9444 admin@<IP_Sensor>
```

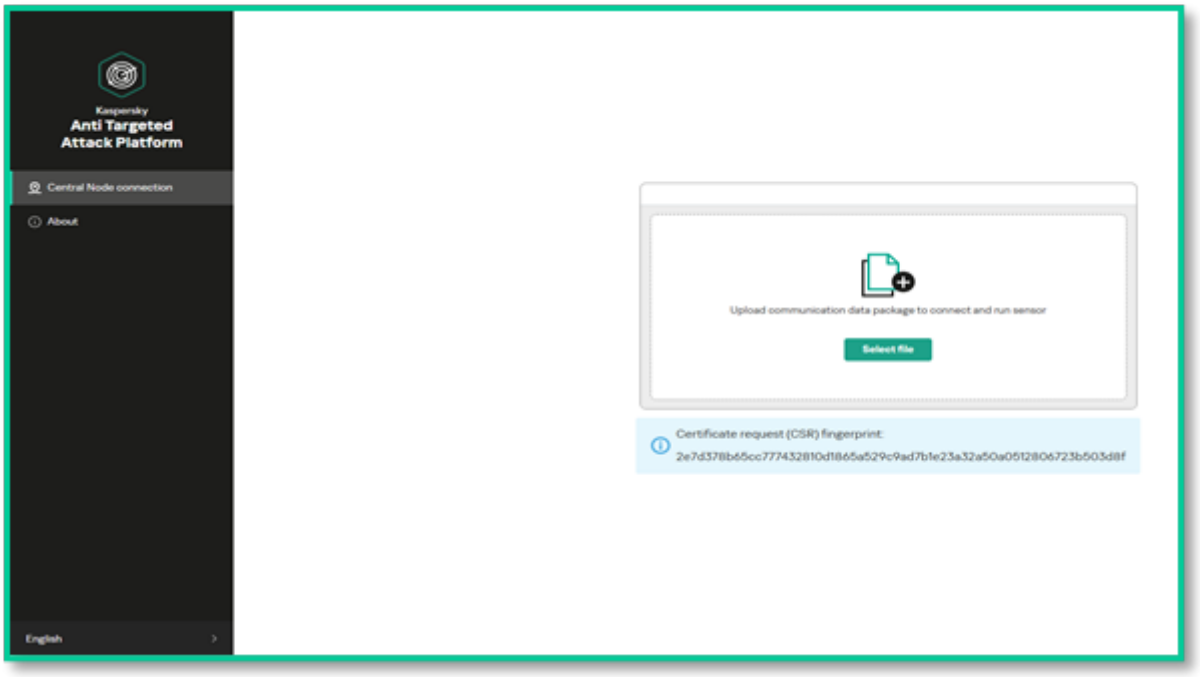
> ⚠ Если ошибка `**Corrupted MAC on input**`, используйте:

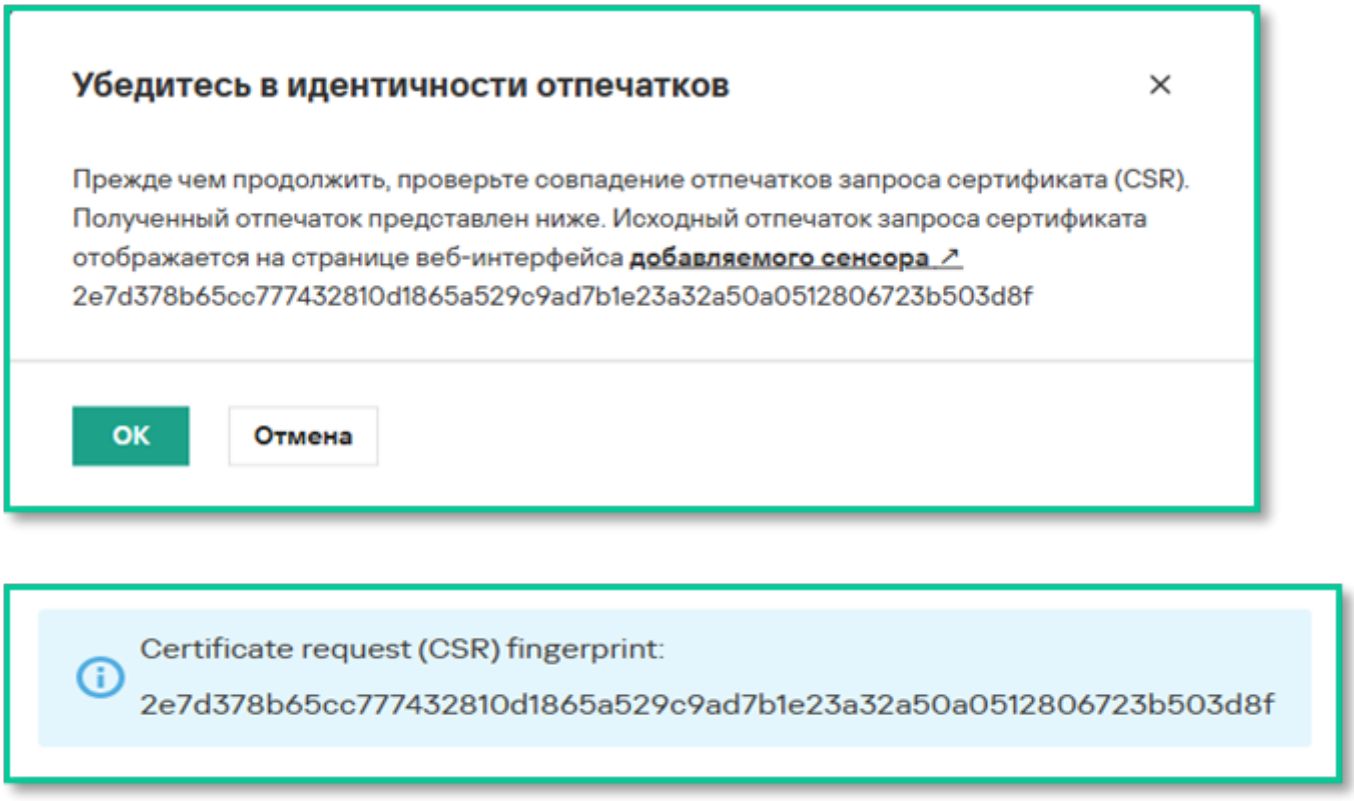
```
ssh -4 -L 9444:localhost:9444 admin@<IP_Sensor> -o "MACs hmac-sha2-256"
```

В браузере на этом же компьютере, на котором разрешен доступ к серверу **Sensor**, в адресной строке браузера введите: **https//localhost:9444**. (именно **localhost**)
В окне браузера откроется страница веб-интерфейса компонента **Sensor**. На странице веб-интерфейса отобразится сообщение, содержащее информацию об отпечатке запроса сертификата, который был отправлен компоненту **Central Node**.

Шаг 6: Проверка отпечатка сертификата

1. Откройте в браузере: **https://localhost:9444**
2. На странице отобразится **отпечаток сертификата (fingerprint)**.

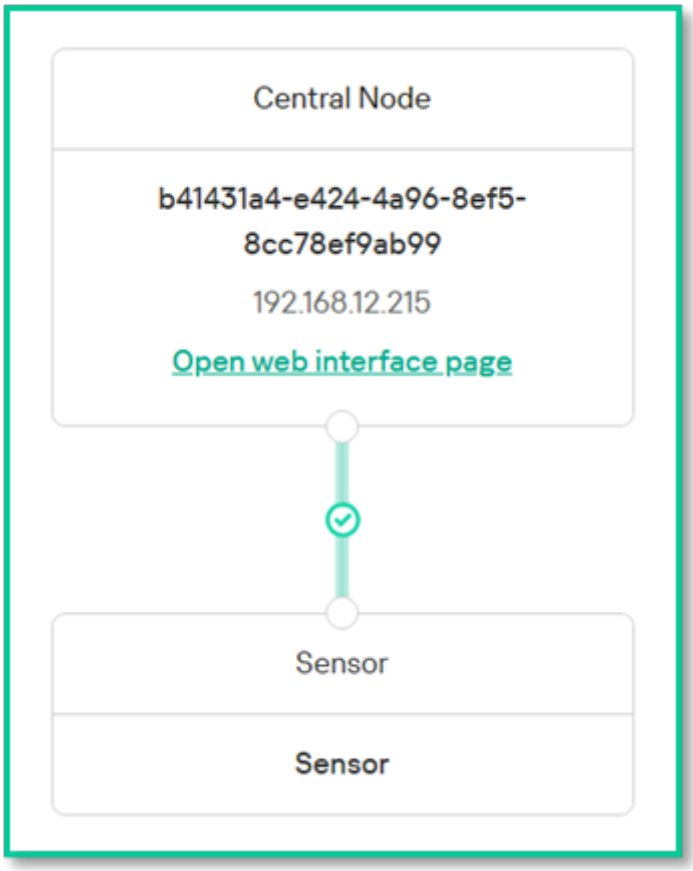




Скриншот 18: Страница https://localhost:9444 с отпечатком сертификата

Шаг 7: Подтверждение подключения

1. Сравните отпечаток на странице Sensor и в интерфейсе Central Node.
2. Если совпадают — нажмите **OK**.

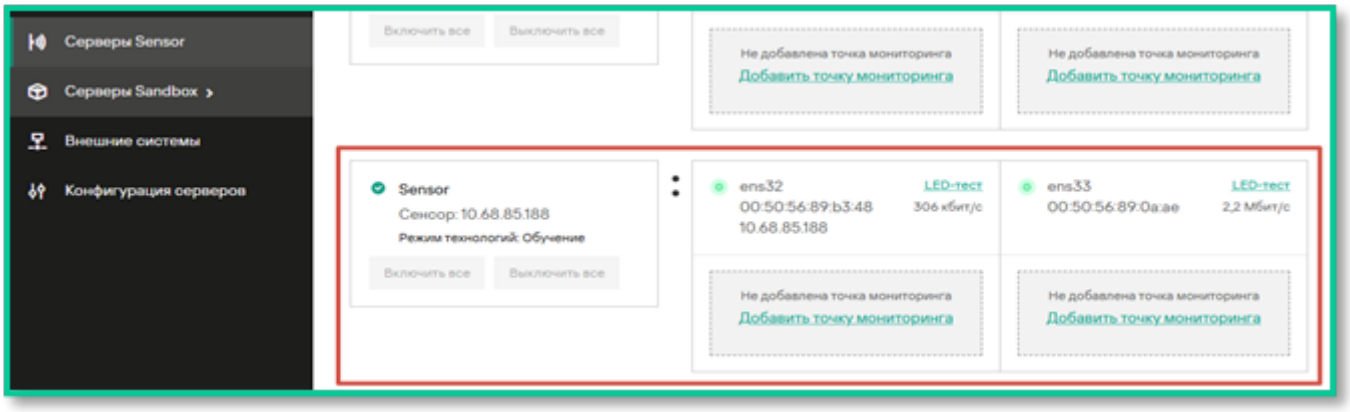


Скриншот 19: Интерфейс Central Node с запросом подтверждения отпечатка и кнопкой `OK`.

Шаг 8: Проверка подключения

После подтверждения:

- Sensor появится в списке.
- Статус: **Подключён**.
- Начнётся синхронизация.



Скриншот 20: Список Sensor в веб-интерфейсе Central Node с новым подключённым узлом. **Рекомендуемый способ.** Требует доступа к Central Node и Sensor.

? **Важно:** ??????????? ???????? ??????? ??????????? ??? ?????????? Sensor

Следуйте инструкции, если в процессе работы приложения наблюдаются потери сетевых пакетов или проблемы с производительностью при обработке сетевого трафика. Описание в онлайн-документации.

□ Заключение

Установка и подключение компонента **Sensor** завершены. Теперь он готов к:

- Приёму SPAN/TAP-трафика.
- Мониторингу сетевой активности.
- Работе в качестве прокси для Endpoint Agent.

? Следующий этап:

Настройка источников трафика — см. раздел Интеграции в руководстве.

□□ Полезные ссылки

- Официальная документация Kaspersky Anti Targeted Attack Platform
- Kaspersky на YouTube
- Kaspersky на Rutube

Revision #9
Created 1 April 2026 10:31:16 by Николай
Updated 17 April 2026 11:16:04 by Николай