KICS 3.1 и ниже

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

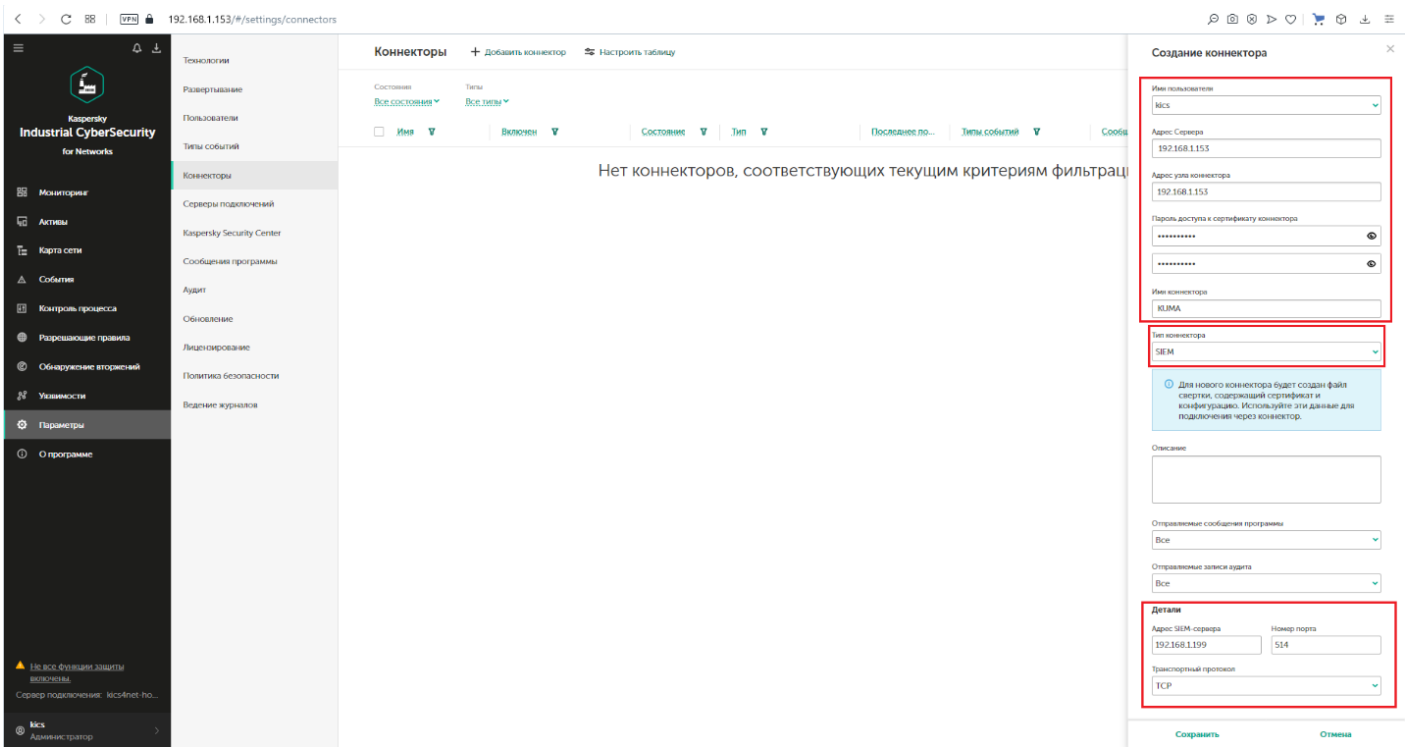
> Данная инструкция предназначена строго для версии KICS for Networks **3.1 или ниже**. Инструкция для версии 4.0 и выше находится в соответствующем разделе базы знаний.

Настройка KICS for Networks

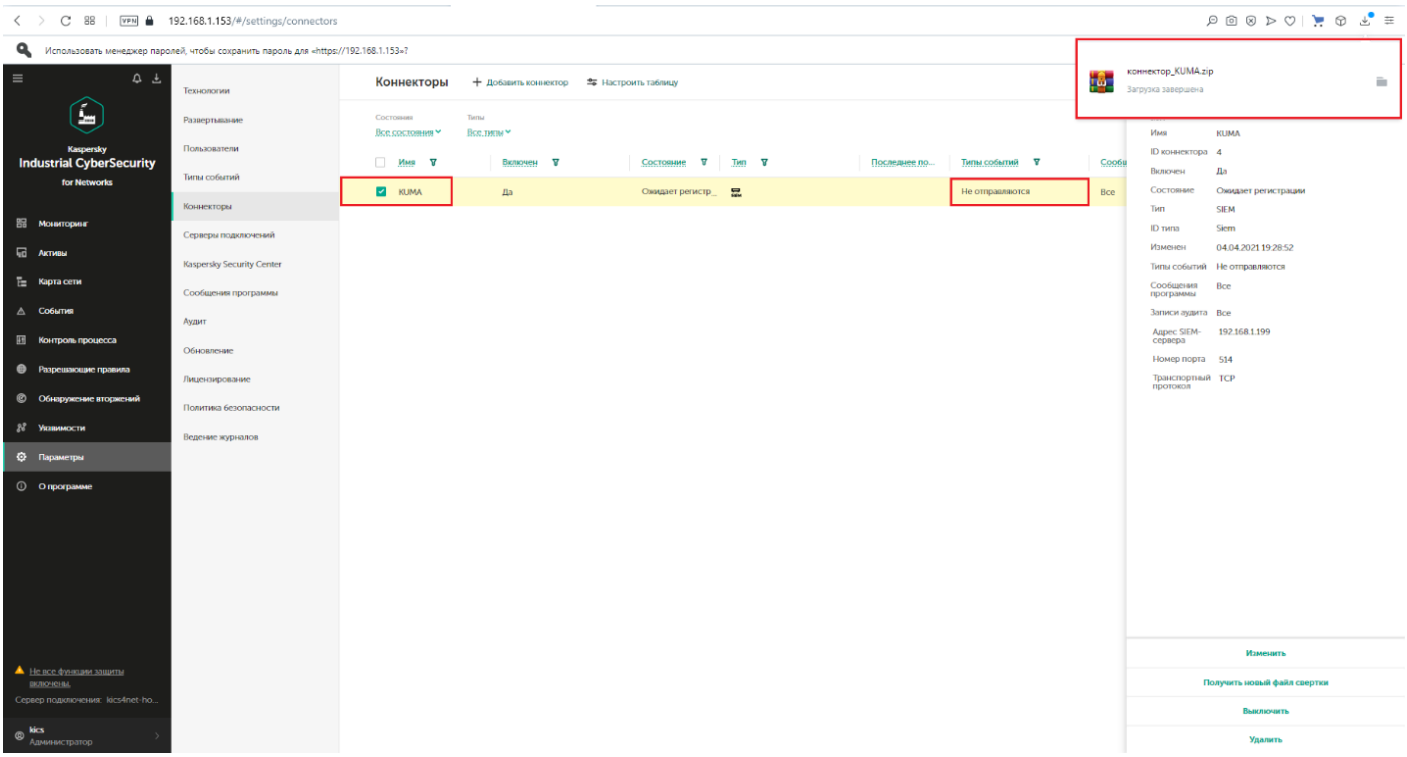
Для настройки пересылки событий из KICS4Net в SIEM KUMA необходимо выполнить следующие действия:

1. Перейти в веб-консоль KICS for Networks из-под учетной записи Администратора

2. Перейти в раздел **Параметры** – **Коннекторы** и настроить параметры отправки событий в KUMA SIEM:
Тип коннектора: SIEM;
Имя коннектора: произвольное название, например, *KUMA;*
Адрес сервера: IP-адрес MGMT интерфейса сервера KICS for Networks;
Адрес узла коннектора: IP-адрес узла, на котором Вы устанавливаете коннектор (Если используется коннектор, располагаемый на сервере KICS for Networks, то указывается IP адрес MGMT интерфейса сервера. Если пакет с коннектором будет установлен на другом узле, то необходимо указать IP адрес этого узла);
Пароль для доступа к сертификату коннектора: пароль для архива с сертификатом сервера KICS for Networks, который будет сформирован после применения настроек коннектора;
Адрес SIEM сервера: IP-адрес сервера коллектора KUMA;
Номер порта: порт коллектора KUMA;
Транспортный протокол: TCP или UDP.



3. По завершении заполнения необходимых полей нажать кнопку **Сохранить**.
После сохранения настроек в списке коннекторов появится созданный коннектор. Для KICS for Networks 3.1 и ниже автоматически загрузится файл свертки с сертификатом сервера KICS for Networks, который необходимо перенести на узел, где установлен коннектор. Вновь созданный коннектор перейдет в режим **Ожидание регистрации** до того момента, как вы создадите службу на узле, где установлен коннектор.



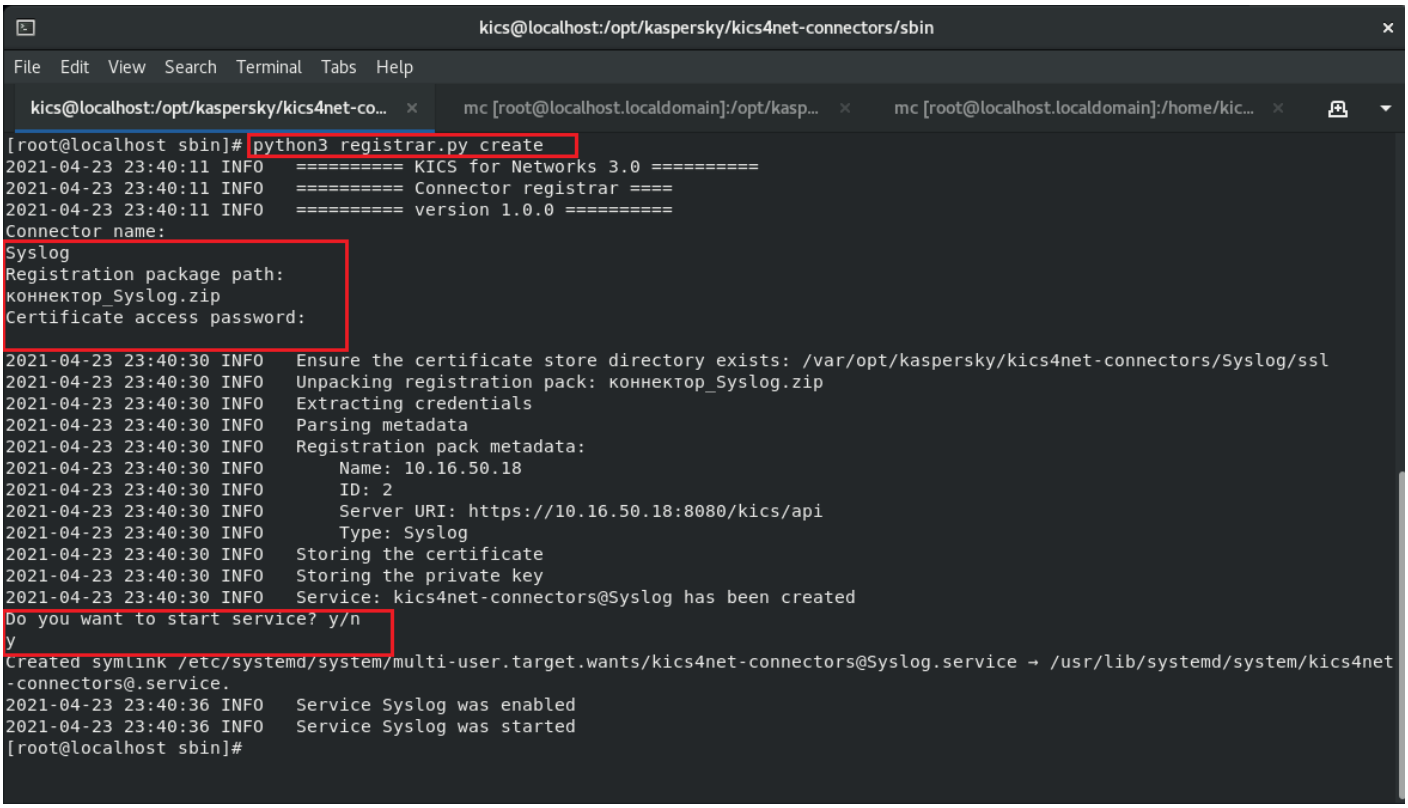
4. Для создании службы необходимо на узле, где установлен коннектор, перейти в раздел `/opt/kaspersky/kics4net-connectors/sbin`

```
cd /opt/kaspersky/kics4net-connectors/sbin
```

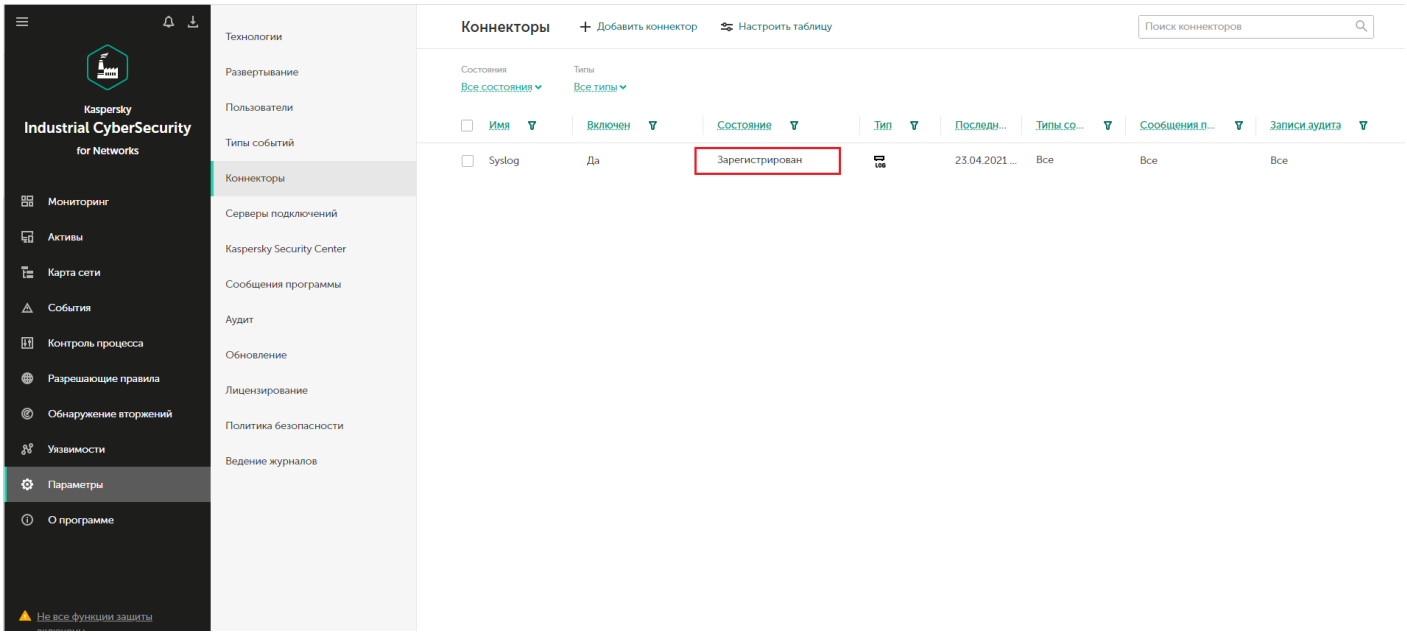
и запустить скрипт `registrar.py`

```
python3 registrar.py create
```

Далее потребуется указать имя коннектора, имя архива с файлом свертки и пароль к архиву файла свертки, подтвердить запуск службы после ее создания.



В результате в интерфейсе KICS for Networks созданный коннектор перейдет в состояние **Зарегистрирован**.

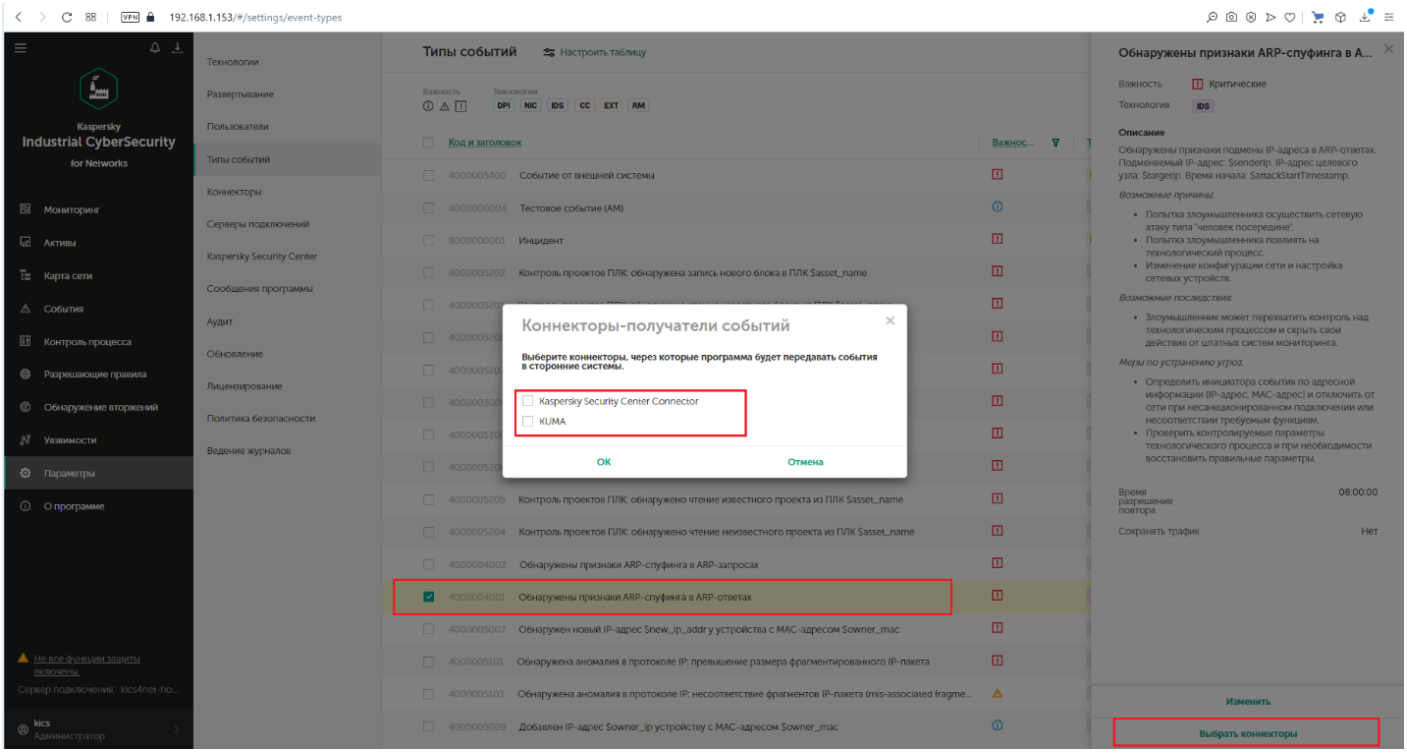


Настройка отправки событий

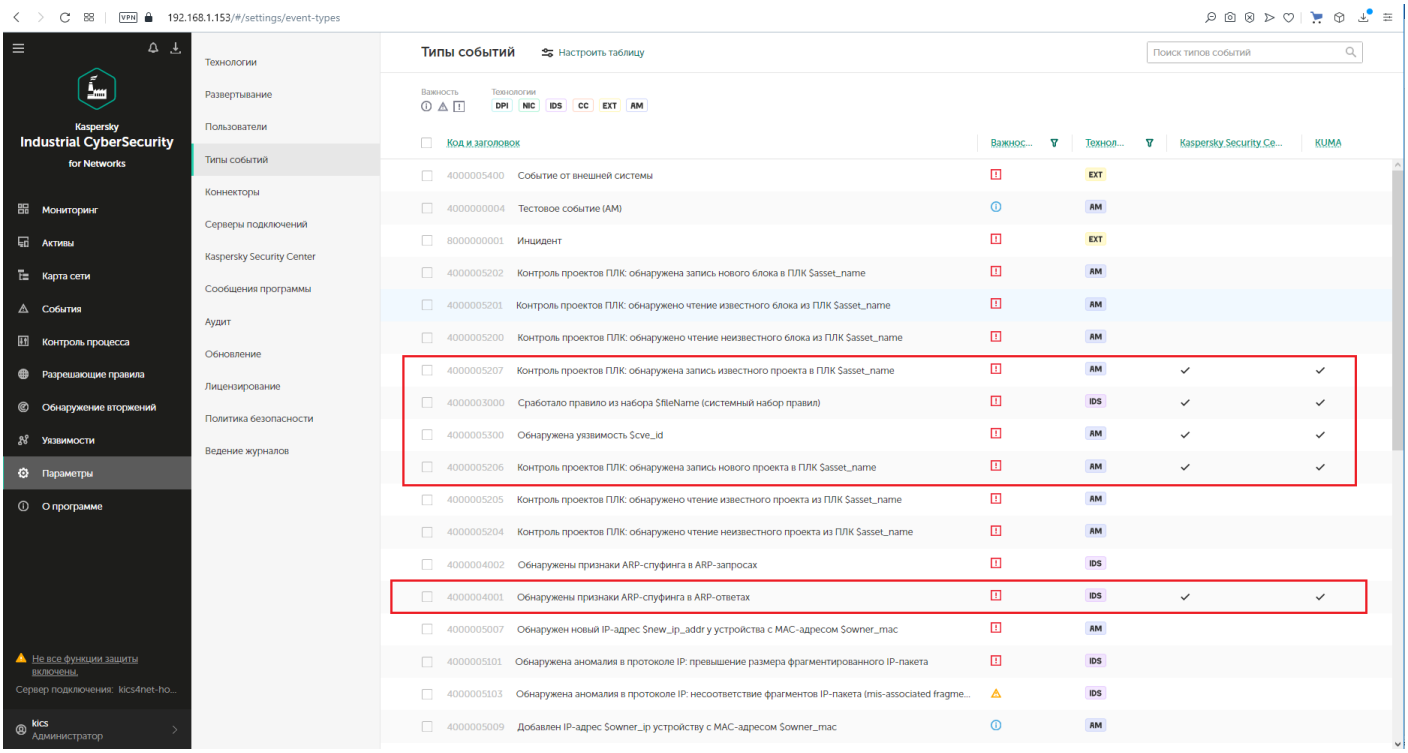
> По умолчанию события безопасности KICS for Networks не передаются ни в какие смежные системы, о чем свидетельствует колонка **Тип события** - **Не отправляются**. Поэтому, чтобы события безопасности передавать в другие системы необходимо определить перечень таких событий для каждой системы, для который мы настроили коннектор.

Для настройки отправки событий необходимо:

1. Перейти на вкладку **Параметры** – **Типы событий**
2. Выбрать один или несколько типов событий, которые необходимо передавать
3. Нажать на кнопку **Выбрать коннекторы**
4. Установить флаг напротив тех систем, в которые необходимо предавать выбранные события
5. Подтвердить выбор нажатием кнопки **OK**



После завершения настроек добавленные события будут отмечены флагом в колонке соответствующего коннектора



Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий KICS for Networks.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне KICS for Networks.

2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] KICS4Net v3.x**.

3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище**. Для отправки обработанных событий в хранилище.
- **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

Полезные ссылки

Настройка создания коннектора KICS for Networks (онлайн-справка KICS for Networks):

https://support.kaspersky.com/help/KICSforNetworks/3.1/ru-RU/136497.htm

---

Revision #4
Created 2023-09-18 13:06:08 UTC by Koala
Updated 2024-12-25 14:38:26 UTC by Koala