

# KICS 4.0 ? ?????

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 **4.0 или ниже**. Инструкция для версии 3.1 и ниже находится в соответствующем разделе базы знаний.

## ?????????? KICS for Networks

Для настройки пересылки событий из KICS for Networks 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;

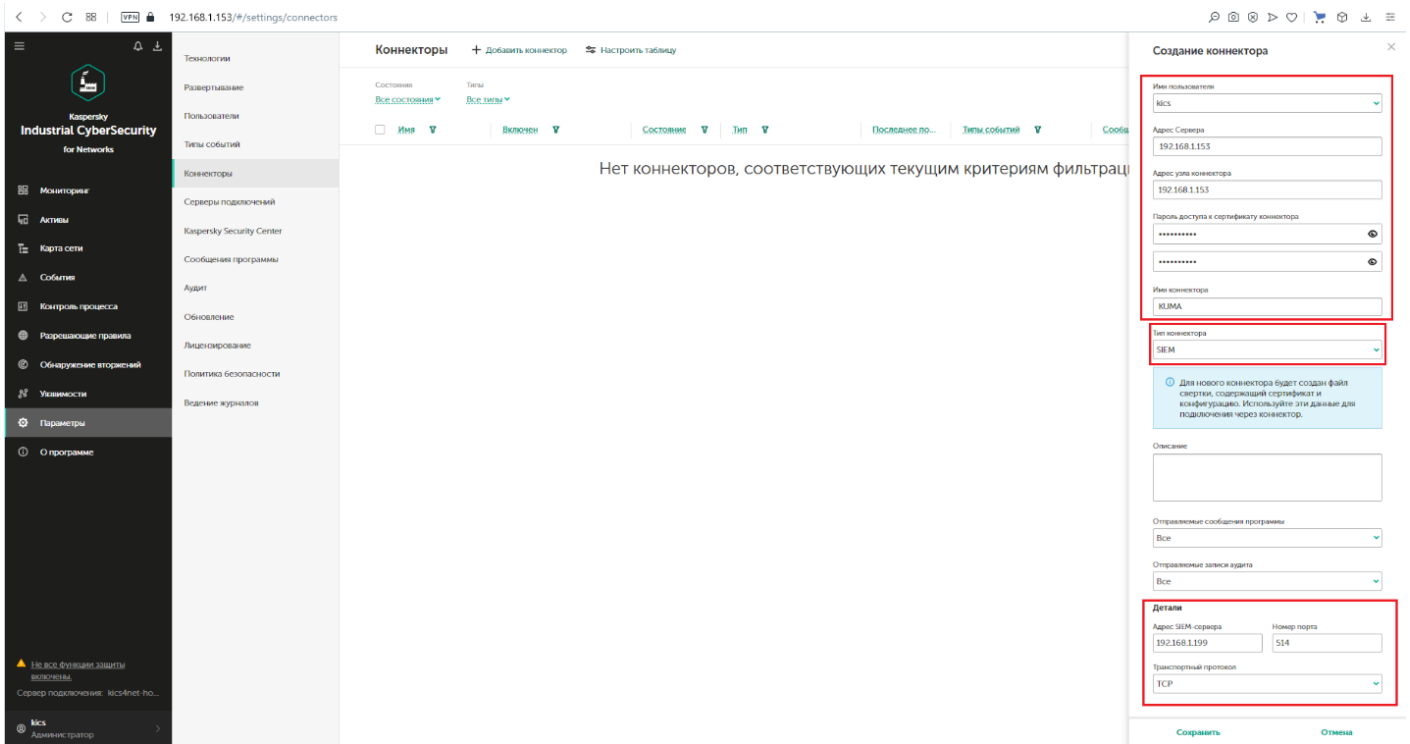
**Адрес узла коннектора:** IP-адрес узла, на котором Вы устанавливаете коннектор (Если используется коннектор, располагаемый на сервере KICS for Networks, то указывается IP адрес MGMT интерфейса сервера. Если пакет с коннектором будет установлен на другом узле, то необходимо указать IP адрес этого узла);

**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;

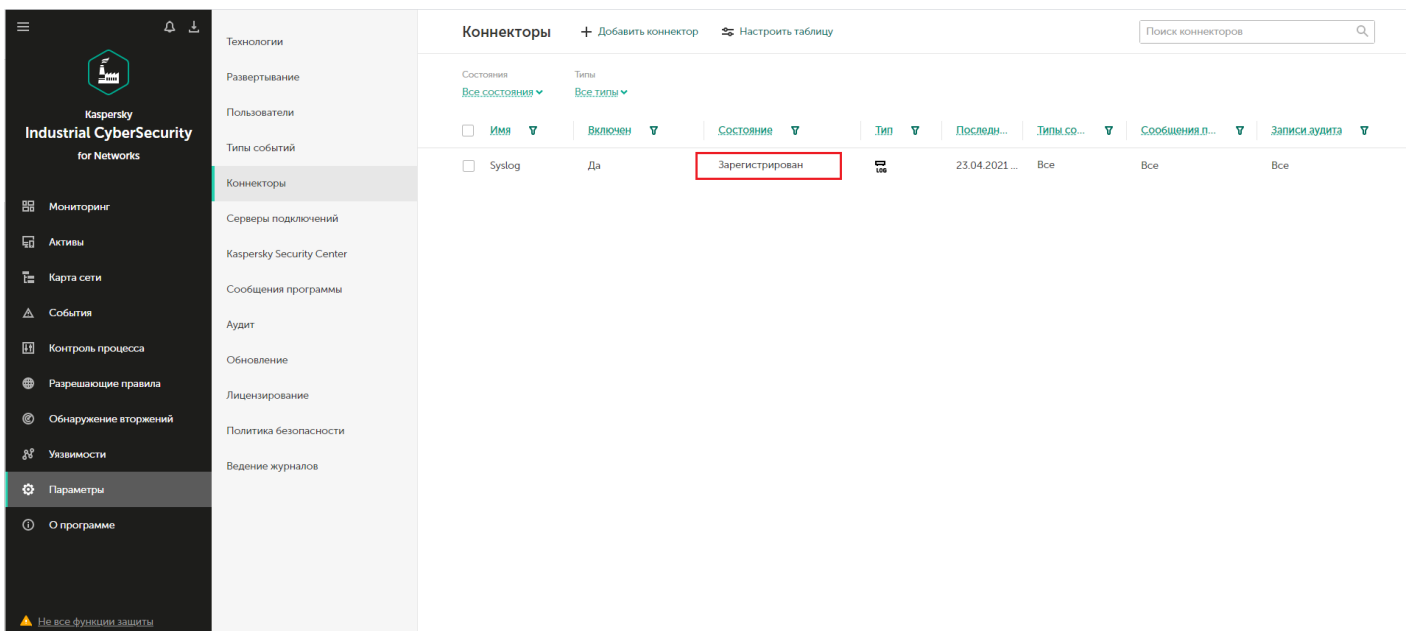
**Номер порта:** порт коллектора KUMA;

**Транспортный протокол:** TCP или UDP.

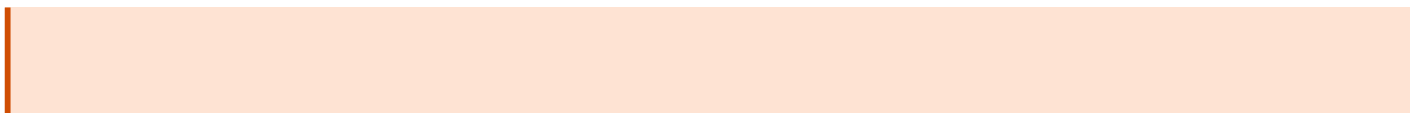


3. По завершении заполнения необходимых полей нажать кнопку **Сохранить**.  
Начиная с версии 4.0 коннектор автоматически осуществит регистрацию в продукте.

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



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



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 которой 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 **ОК**

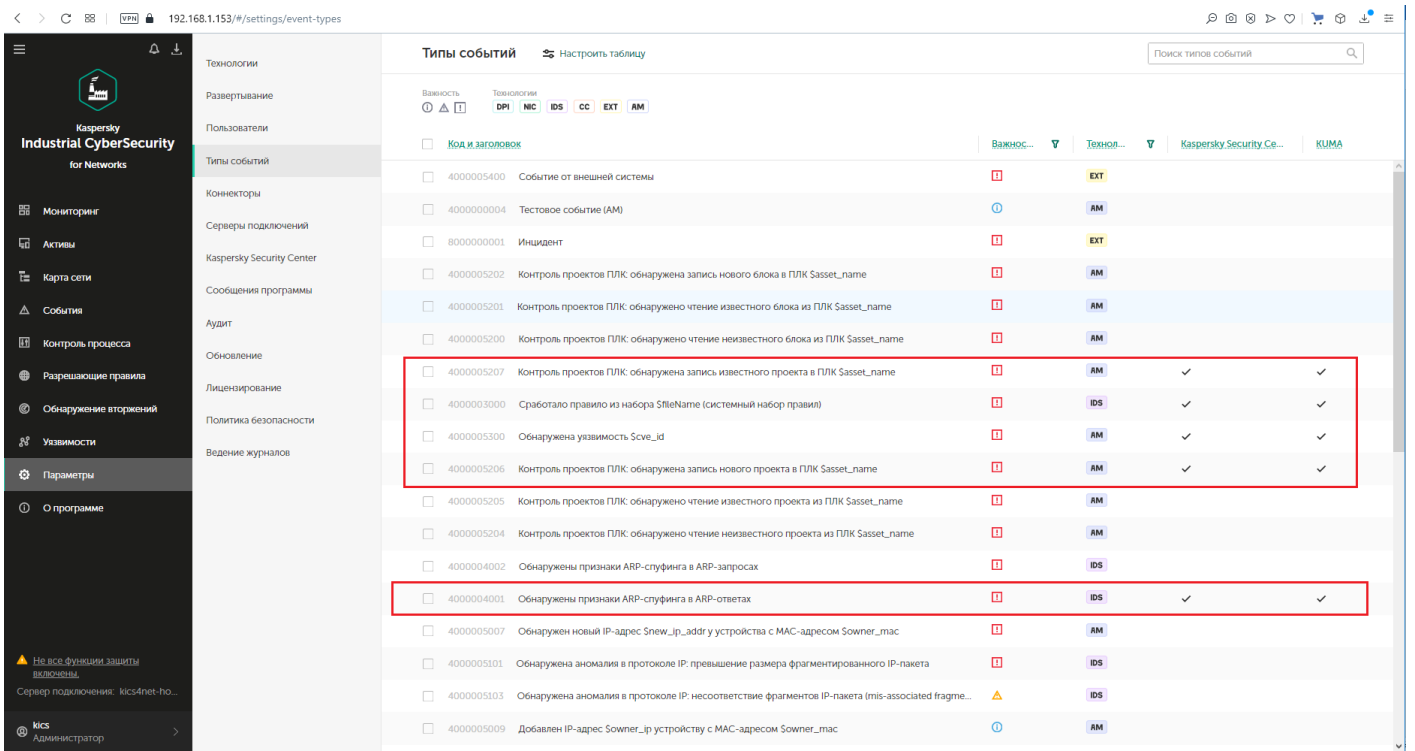
The screenshot displays the 'Типы событий' (Event Types) configuration page in the Kaspersky Industrial CyberSecurity for Networks interface. The page is divided into three main sections: a left sidebar with navigation options, a central table of event types, and a right sidebar with details for the selected event.

The central table lists various event types with columns for 'Важность' (Importance), 'Технология' (Technology), and 'Важность...' (Importance...). The event 'Обнаружены признаки ARP-спуфинга в ARP-ответах' (4000004001) is highlighted in green, indicating it is selected. A red box highlights the 'Выбрать коннекторы' (Select connectors) button at the bottom right of the dialog box.

The dialog box 'Коннекторы-получатели событий' (Event Receivers) is open, showing a list of connectors. The 'Kaspersky Security Center Connector' option is selected, and a red box highlights this selection. The 'KUMA' option is also visible but not selected.

The right sidebar shows details for the selected event, including its importance (Critical), technology (IDS), and a description of the event. It also includes a 'Время разрешения полтора' (Resolution time) of 08:00:00 and a 'Сохранять трафик' (Save traffic) option set to 'Нет' (No).

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



# ????????? 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 соответствующий нормализатор.
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.

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

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

<https://support.kaspersky.com/help/KICSforNetworks/4.0/ru-RU/136497.htm>

---

Revision #5

Created 2023-09-18 13:47:26 UTC by Koala

Updated 2024-12-25 14:38:26 UTC by Koala