

# KICS 4.0 и выше

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.

## Настройка 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;

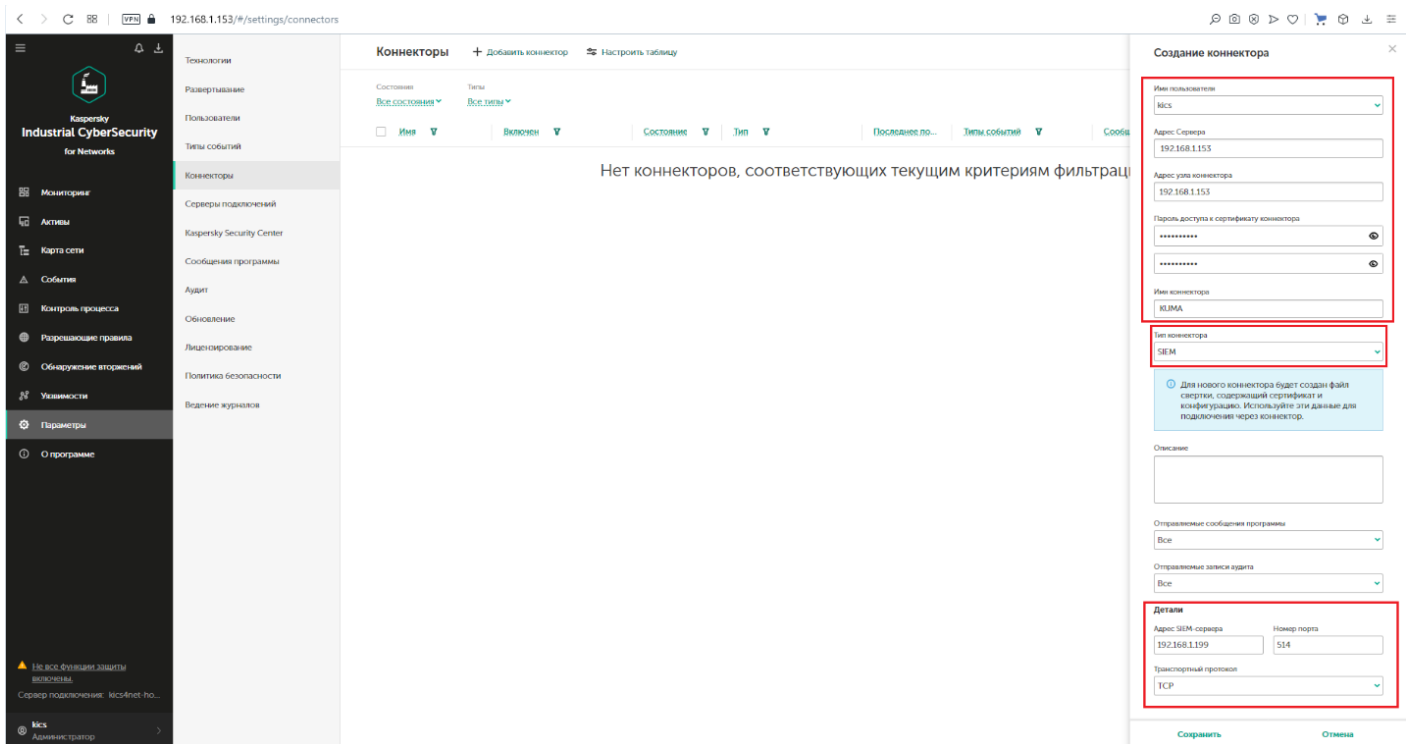
**Адрес узла коннектора:** IP-адрес узла, на котором Вы устанавливаете коннектор (Если используется коннектор, располагаемый на сервере KICS for Networks, то указывается IP адрес MGMT интерфейса сервера. Если пакет с коннектором будет установлен на другом узле, то необходимо указать IP адрес этого узла);

**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;

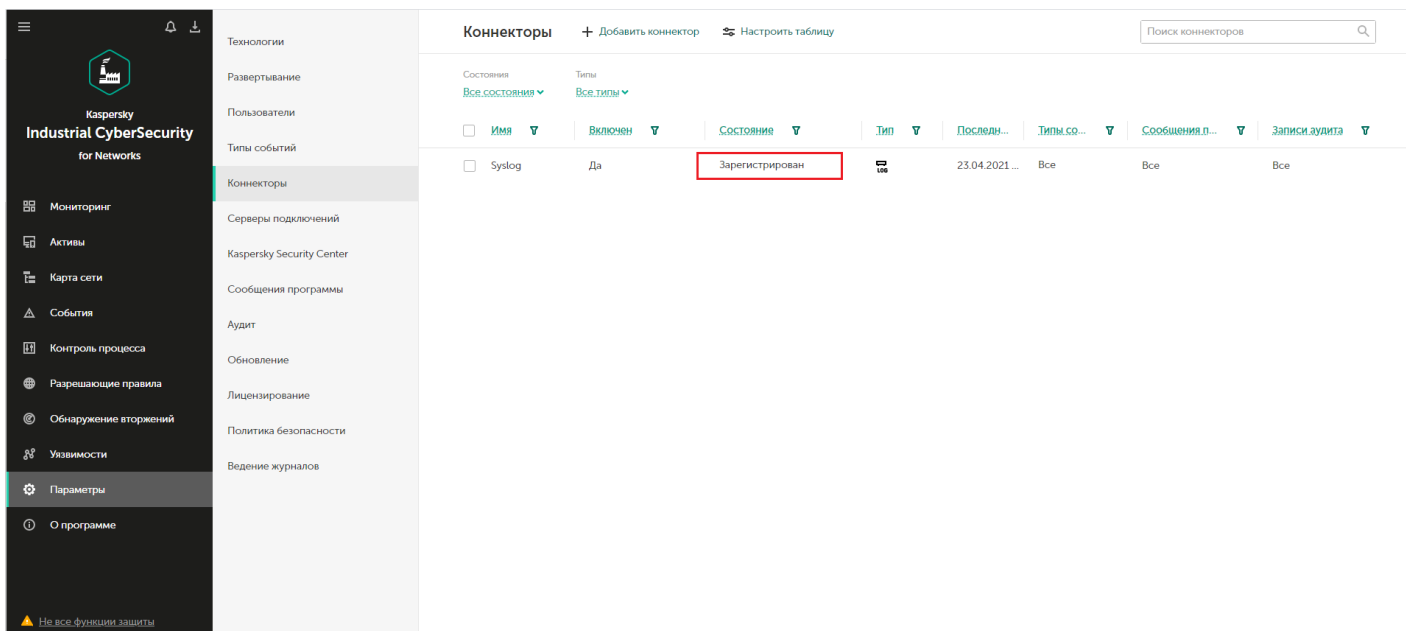
**Номер порта:** порт коллектора KUMA;

**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**.



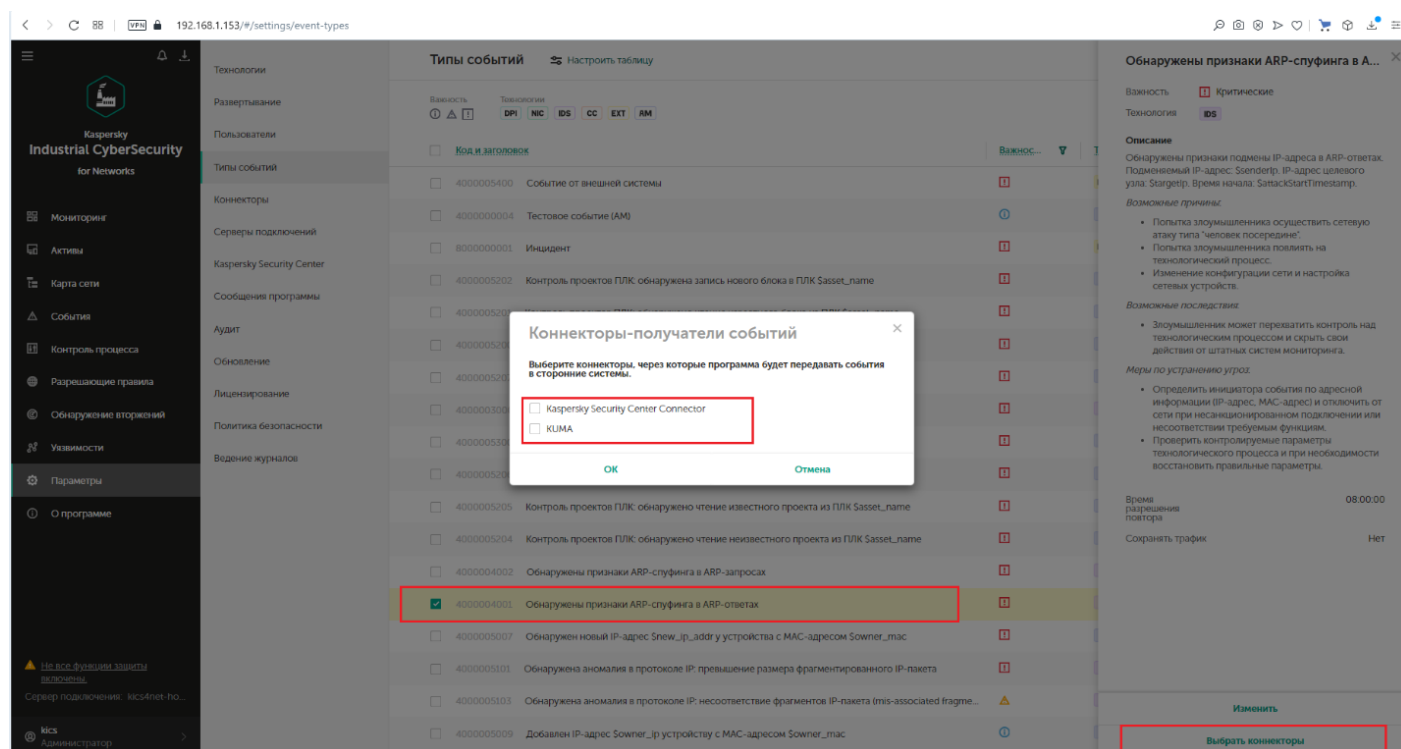
## Настройка отправки событий

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 **ОК**



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

192.168.1.153/#/settings/event-types

Касперский  
Industrial CyberSecurity  
for Networks

Мониторинг  
Активы  
Карта сети  
События  
Контроль процесса  
Разрешающие правила  
Обнаружение вторжений  
Уязвимости  
Параметры  
О программе

Технологии  
Развертывание  
Пользователи  
Типы событий  
Коннекторы  
Серверы подключений  
Kaspersky Security Center  
Сообщения программы  
Аудит  
Обновление  
Лицензирование  
Политика безопасности  
Ведение журналов

Типы событий

Важность: DPI, NIS, IDS, CC, EXT, AM

| Код и заголовок  | Важность | Технология | Kaspersky Security Ce... | KUMA |
|--|----------|------------|--------------------------|------|
| 4000005400 Событие от внешней системы  | PI       | EXT        |                          |      |
| 4000000004 Тестовое событие (AM)   | PI       | AM         |                          |      |
| 8000000001 Инцидент  | PI       | EXT        |                          |      |
| 4000005202 Контроль проектов ПЛК: обнаружена запись нового блока в ПЛК Sasset_name                           | PI       | AM         |                          |      |
| 4000005201 Контроль проектов ПЛК: обнаружено чтение известного блока из ПЛК Sasset_name                      | PI       | AM         |                          |      |
| 4000005200 Контроль проектов ПЛК: обнаружено чтение неизвестного блока из ПЛК Sasset_name                    | PI       | AM         |                          |      |
| 4000005207 Контроль проектов ПЛК: обнаружена запись известного проекта в ПЛК Sasset_name                     | PI       | AM         | ✓                        | ✓    |
| 4000003000 Сработало правило из набора SfileName (системный набор правил)                                    | PI       | IDS        | ✓                        | ✓    |
| 4000005300 Обнаружена уязвимость Scve_id   | PI       | AM         | ✓                        | ✓    |
| 4000005206 Контроль проектов ПЛК: обнаружена запись нового проекта в ПЛК Sasset_name                         | PI       | AM         | ✓                        | ✓    |
| 4000005205 Контроль проектов ПЛК: обнаружено чтение известного проекта из ПЛК Sasset_name                    | PI       | AM         |                          |      |
| 4000005204 Контроль проектов ПЛК: обнаружено чтение неизвестного проекта из ПЛК Sasset_name                  | PI       | AM         |                          |      |
| 4000004002 Обнаружены признаки ARP-спуфинга в ARP-запросах   | PI       | IDS        |                          |      |
| 4000004001 Обнаружены признаки ARP-спуфинга в ARP-ответах  | PI       | IDS        | ✓                        | ✓    |
| 4000005007 Обнаружен новый IP-адрес Snew_ip_addr у устройства с MAC-адресом Sowner_mac                       | PI       | AM         |                          |      |
| 4000005101 Обнаружена аномалия в протоколе IP: превышение размера фрагментированного IP-пакета               | PI       | IDS        |                          |      |
| 4000005103 Обнаружена аномалия в протоколе IP: несоответствие фрагментов IP-пакета (mis-associated fragme... | PI       | IDS        |                          |      |
| 4000005009 Добавлен IP-адрес Sowner_ip устройству с MAC-адресом Sowner_mac                                   | PI       | AM         |                          |      |

# 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 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.

## Полезные ссылки

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 18 September 2023 13:47:26 by Koala

Updated 7 July 2024 08:59:29 by Koala