

# Network

Подключение сетевых источников событий: маршрутизаторы, коммутаторы, FW, NGFW и т.п.

- [Usergate](#)
- [ViPNet Coordinator](#)
- [Ideco UTM](#)
- [Cisco IOS](#)
- [Настройка отправки событий с FortiGate \(CEF\)](#)
- [Континент версия 4](#)

# Usergate

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

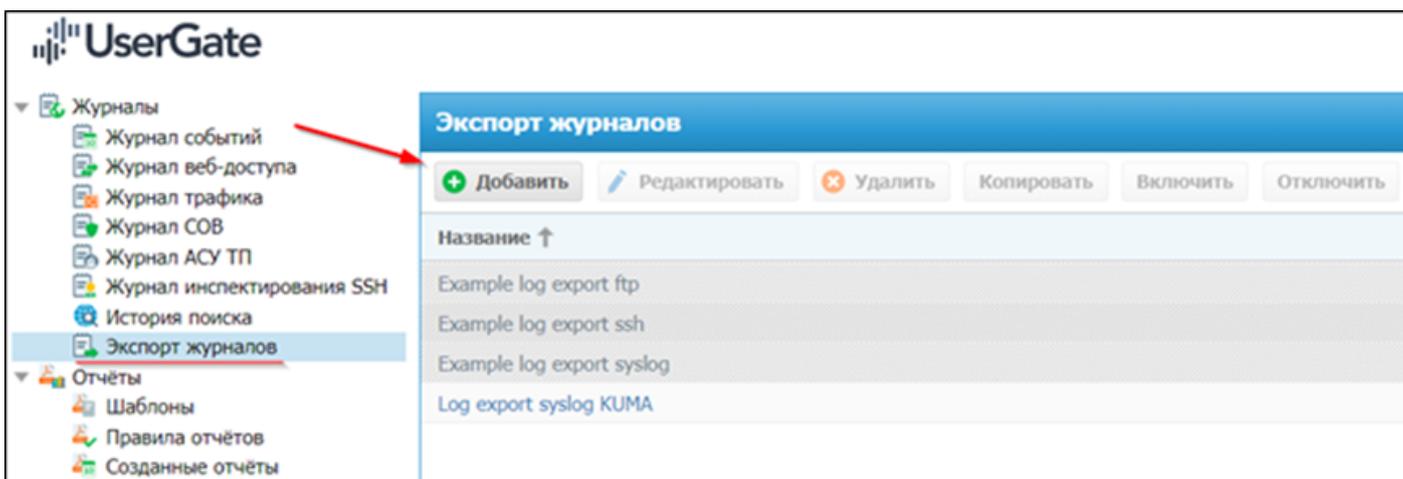
## Настройка Usergate

Для настройки отправки событий с Usergate в KUMA выполните следующие действия:

1. В веб-интерфейсе Usergate перейдите на вкладку **Журналы и отчёты**.

[Дашборд](#) | [Диагностика и мониторинг](#) | [Журналы и отчёты](#) | [Настройки](#) | [Гостевой портал](#) | [Помощь](#) ▾ | [Русский](#) ▾ | [Admin](#) ▾

2. Выберите **Экспорт журналов** и нажмите кнопку **Добавить**.



3. На вкладке **Общие** поставьте галочку напротив параметра **Включено** и задайте имя правилу экспорта журналов.

The screenshot shows a dialog box titled "Свойства правила экспорта журналов" (Properties of the log export rule). It has a blue header bar with a close button (X) on the right. Below the header is a tabbed interface with five tabs: "Общие" (General), "Удалённый сервер" (Remote server), "Журналы для экспорта" (Logs for export), "Расписание" (Schedule), and "Управление журналами" (Log management). The "Удалённый сервер" tab is selected. The main area contains the following fields:

- "Включено:" (Enabled): A checked checkbox.
- "Название:" (Name): A text input field containing "Log export syslog KUMA".
- "Описание:" (Description): An empty text area.

At the bottom of the dialog, there are three buttons: "Проверить соединение" (Check connection), "Сохранить" (Save), and "Отмена" (Cancel).

4. На вкладке **Удаленный сервер** задайте следующие настройки:

- **Тип сервера** - **Syslog**
- **Адрес** - коллектора KUMA
- **Порт** - порт коллектора KUMA
- **Транспорт** - **UDP** или **TCP** (настройка должна совпадать с настройками коллектора KUMA).
- **Протокол** - **Syslog (RFC 5424)**.
- **Критичность** и **Объект** выберите в соответствии с потребностями в логировании.

В поле **Имя хоста** по умолчанию указано имя хоста Usergate с символом @. Замените символ «@» на символ «.» для корректной нормализации событий Usergate на стороне KUMA.

Свойства правила экспорта журналов

Общие Удалённый сервер **Журналы для экспорта** Расписание Управление журналами

Тип сервера: Syslog

Адрес сервера: 10.68.85.125

Порт: 5155

Транспорт: UDP

Протокол: Syslog (RFC 5424)

Критичность: Информативная

Объект: Сообщения пользовательские

Имя хоста: utmcore.icastasinpe

Название приложения: utm-loganalyzer

Проверить соединение Сохранить Отмена

5. На вкладке **Журналы для экспорта** поставьте галочки напротив **Журналов**, которые необходимо экспортировать в KUMA. Для каждого экспортируемого журнала выберите **Формат CEF**.

6. Сохраните внесенные изменения.

## Настройка KUMA

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

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне Usergate.
2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] Syslog-CEF**.
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

Экспорт журналов (документация UserGate): [https://docs.usergate.com/eksport-zhurnalov\\_178.html](https://docs.usergate.com/eksport-zhurnalov_178.html)

# VIPNet Coordinator

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

## Настройка VIPNet Coordinator

Для отправки событий VIPNet Coordinator в KUMA выполните следующее:

1. Подключитесь к консоли VIPNet Coordinator локально или через ssh.
2. Перейдите режим в Администратора с помощью следующей команды:

```
enable
```

3. Из командной строки в режиме Администратора выполните команду:

```
machine set loghost <ip-адрес коллектора KUMA>
```

После выполненных настроек VIPNet Coordinator будет отправлять системный журнал на адрес коллектора KUMA по протоколу UDP и 514-му порту.

В случае если коллектор KUMA является открытым узлом по отношению к VIPNet Coordinator, то также необходимо создать фильтр открытой сети, разрешающий исходящий трафик по протоколу UDP на 514-й порт коллектора KUMA.

## Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий VIPNet Coordinator.

1. На шаге **Транспорт** укажите тип UDP и порт 514.
2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] VipNet Coordinator syslog**.
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.

---

## Дополнительная настройка коллектора

После установки коллектора, необходимо внести изменения в файл сервиса коллектора для того, чтобы коллектор мог слушать входящие соединения на порту 514.

Для этого выполните следующие действия:

1. Остановите выполнение сервиса коллектора командой

```
systemctl stop kuma-collector-<id>
```

2. Откройте на редактирование файл коллектора `/usr/lib/systemd/system/kuma-collector-<id>.service`

3. В разделе **[Service]** добавьте следующую строку

```
AmbientCapabilities=CAP_NET_BIND_SERVICE
```

4. Сохраните полученный файл
5. Обновите параметры сервисов следующей командой

```
systemctl daemon-reload
```

6. Запустите службу коллектора следующей командой

```
systemctl start kuma-collector-<id>
```

# Ideco UTM

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

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/help/KUMA/2.1/ru-RU/255211.htm>

## Настройка Ideco UTM

Для передачи событий из Ideco UTM в KUMA выполните следующие действия:

1. Подключитесь к веб-интерфейсу Ideco UTM под учётной записью, обладающей административными привилегиями.
2. В меню **Пересылка системных сообщений** переведите переключатель **Syslog** в положение включено.
3. В параметре **IP-адрес** укажите IP-адрес коллектора KUMA.
4. В параметре **Порт** введите порт, который прослушивает коллектор KUMA.
5. Нажмите **Сохранить** для применения внесённых изменений.

**Syslog** ?  
Работает

Системные логи будут передаваться на указанный удалённый сервер.

IP-адрес

Порт

**Сохранить**

# Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Ideco UTM.

1. На шаге **Транспорт** укажите тип **UDP** и порт в соответствии с настройками на стороне Ideco UTM.
2. На шаге **Парсинг** событий выберите нормализатор **[ООТВ] Ideco UTM syslog**.
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 получения событий Ideco UTM (онлайн-справка KUMA):

<https://support.kaspersky.com/help/KUMA/2.1/ru-RU/255211.htm>

Расшифровка передаваемых логов: <https://docs.ideco.dev/settings/monitor/syslog>

# Cisco IOS

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

## Настройка Cisco IOS

Войдите на источник Cisco IOS коммутатор или маршрутизатор.

Введите следующую команду для входа в маршрутизатор в привилегированный режим:

```
enable
```

Переключитесь в режим конфигурации (configure terminal):

```
conf t
```

Перед включением ведения журнала убедитесь, что ваш маршрутизатор правильно настроен для получения времени от сервера NTP, или настройте его вручную, чтобы получать время. Используйте команду `set clock` или `ntp server x.x.x.x` для синхронизации часов.

Включите журналирование:

```
logging on
```

Укажите IP-адрес коллектора и порт (можно использовать UDP или TCP транспорт):

```
logging host <IP-адрес коллектора> transport udp port <порт коллектора>
```

Укажите уровень важности событий (рекомендуется informational):

```
logging trap informational
```

Уровни критичности в CISCO:

Level Keyword	Level	Description	Syslog Definition
emergencies	0	Система нестабильна	LOG_EMERG
alerts	1	Требуются немедленные действия	LOG_ALERT

critical	2	Критические условия	LOG_CRIT
errors	3	Условия ошибки (по умолчанию)	LOG_ERR
warnings	4	Условия предупреждения	LOG_WARNING
notifications	5	Нормальное, но значимое состояние	LOG_NOTICE
informational	6	Только информационные сообщения	LOG_INFO
debugging	7	Отладка сообщений	LOG_DEBUG

Укажите интерфейса источника для отправки событий:

```
logging source-interface <Имя интерфейса>
```

<Имя интерфейса> - это имя интерфейса, например, *dmz*, *lan*, *ethernet0* или *ethernet1*.

Настройте средство для системного журнала:

```
logging facility syslog
```

Настройте идентификатор событий:

```
logging origin-id ip
```

Настройте временные метки событий и идентификаторы событий в логировании:

```
service timestamps log datetime year show-timezone  
service sequence numbers
```

Маршрутизатор по умолчанию не проверяет, авторизован ли пользователь в консольном порту или к нему подключено устройство; если ведение журнала консоли включено, на консольный порт всегда отправляются сообщения, которые могут вызвать нагрузку на процессор. Поэтому ниже включим логирование только необходимых событий. (вместо включения `logging console warning` )

Включите регистрацию событий входа пользователей:

```
logging userinfo  
login on-success log  
login on-failure log  
ip ssh logging events
```

Включите регистрацию событий выполнения конфигурационных команд:

```
archive
log config
logging enable
notify syslog contenttype plaintext
```

**Опционально.** Включите регистрацию событий VPN:

```
crypto logging ezvpn
crypto logging session
crypto logging ikev2
```

Выйдите из режима конфигурирования:

```
end
```

Сохраните изменения даже после перезагрузки:

на старых Cisco:

```
write memory
```

на новых Cisco (копирование рабочей конфигурации):

```
copy running-config startup-config
```

Чтобы отобразить состояние системного журнала (syslog) и содержимое стандартного буфера сообщений системного журнала, используйте команду из привилегированного режима:

```
show logging
```

# Настройка отправки событий с FortiGate (CEF)

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

## Настройка коллектора KUMA

### Создание коллектора KUMA

Для приема и обработки событий с FortiGate необходимо создать сервис коллектора в KUMA. Для этого в веб-интерфейсе перейдите на вкладку **Ресурсы** и нажмите на кнопку **Подключить источник**. В появившемся окне **Создание коллектора**:

- На шаге **Подключение источников** укажите **Имя коллектора** и **Тенант**, к которому будет принадлежать создаваемый коллектор

# Создание коллектора

## Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

## Подключение источников

Коллекторы используются для получения данных из источников событий, а также преобразования их в нормализованные события, понятные KUMA. С помощью коллектора можно также отсеивать ненужные события, объединять похожие события и обогащать события информацией из сторонних источников. Чтобы создать коллектор, следуйте шагам мастера. Подробнее см. [в онлайн-справке](#).

Название коллектора\*

FortiGate UDP/5205 **1**

Тенант\*

Main **2**

Обработчики

0

Отладка



Описание

Создать

Отмена

- На шаге **Транспорт** укажите **Тип** и **Порт** (данные параметры должны соответствовать настройкам на стороне FortiGate: **set mode** и **set port** соответственно)

Для распределенной инсталляции укажите hostname:port сервера коллектора в поле **URL**

# Создание коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

## Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор	Создать
Тип* 	udp 
URL* 	:5205 
Разделитель	

Создать

Отмена

- На шаге **Парсинг событий** укажите нормализатор. Рекомендуется использовать предустановленный нормализатор **[OOTB] Syslog-CEF** (<https://support.kaspersky.com/help/KUMA/3.0.3/ru-RU/255782.htm>).

Если планируете использовать правила корреляции для FortiGate из Community-Pack необходимо использовать нормализатор **[2024-04-22] FortiGate Syslog-CEF**, также доступный в Community-Pack

Схема нормализации

Обогащение

Нормализатор

Название\*

Метод парсинга\*

Сохранить исходное событие\*

Сохранить дополнительные поля\*

Ошибка коннектора. Невозможно скачать файл.

Примеры событий

## Сопоставление

Исходные данные	Поле KUMA	Подпись	Примеры
app	<input type="text" value="DeviceProcessName"/>		
facility	<input type="text" value="DeviceFacility"/>		

OK

Отмена

- Шаги мастера настройки с четвертого по шестой можно пропустить и вернуться к их настройке позднее.
- На седьмом шаге **Маршрутизация** задайте точки назначения. Для хранения событий добавьте точку назначения типа **Хранилище**. В случае если предполагается также корреляция по событиям добавьте точку назначения типа **Коррелятор**.

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

## Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см. [в онлайн-справке](#).

+ Добавить  Удалить

<input type="checkbox"/>	Название	Тип	URL
<input type="checkbox"/>	[OТВ] Storage <span>1</span>	storage	<a href="#">https://storage.svc.cluster.local:7230</a>
<input type="checkbox"/>	[OТВ] Correlator <span>2</span>	correlator	<a href="#">https://correlator.svc.cluster.local:7231</a>

Создать

Отмена

- На завершающем шаге **Проверка параметров** нажмите на кнопку **Сохранить и создать сервис**. После чего появится команда установки сервиса, которую необходимо скопировать для дальнейшей установки.

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

## Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты. Подробнее см. [в онлайн-справке](#).

## Сервисы, использующие этот коллектор

Тип	Название
collector	FortiGate UDP/5205

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

## Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://kuma-ai.kaspersky-lab:7210 --id 9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd --api.port 7249 --install
```



Сохранить

Отмена

Также после выполнения вышеуказанных действий на вкладке **Ресурсы > Активные сервисы** появится созданный сервис коллектора.

Ресурсы и сервисы / Сервисы

## Сервисы

+	Добавить сервис	↻	Обновить	↻	Обновить параметры	↻	Перезапустить	🗑	Сбросить сертификат	✕	Удалить	⋮	fortigate udp	🔍	⚙			
☐	Статус	▼	Тип	▼	Сервис	▼	Версия	▼	Тенант	▼	Полное доменное имя	▼	IP-адрес	▼	Порт API	▼	Время работы	Создан
☐	●		Коллектор		FortiGate UDP/5205				Main								01.04.2024 18:45:21	

## Установка коллектора KUMA

Выполните подключение к CLI KUMA (установка коллектора выполняется с правами root).

Перед установкой рекомендуется выполнить из командной строки команду, скопированную на прошлом шаге без ключа **--install**, чтобы убедиться в отсутствии ошибок.

```
[root@kuma-ai ~]# /opt/kaspersky/kuma/kuma collector --core https://kuma-ai.kaspersky-lab:7210 --id 9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd --api.port 7249
```

В случае отсутствия ошибок в выводе командной строки, прервите исполнение в командной строке, после чего можно переходить к установке.

Для установки сервиса коллектора в командной строке выполните команду, скопированную на прошлом шаге.

```
[root@kuma-aio ~]# /opt/kaspersky/kuma/kuma_collector --core https://kuma-aio.sail.m:7218 --id 9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd --api.port 7249 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd.service → /usr/lib/systemd/system/kuma-collector-9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd.service.
[root@kuma-aio ~]#
```

При необходимости добавьте порт коллектора в исключения фаервола и обновите параметры службы.

```
firewall-cmd --add-port=<порт, выбранный для коллектора>/udp --permanent
firewall-cmd --reload
```

После успешной установки сервиса его в статус в веб-интерфейсе KUMA изменится на **зеленый**.

Ресурсы и сервисы / Сервисы

## Сервисы

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
<input checked="" type="checkbox"/>	Коллектор	FortiGate UDP/5205	5.2.0.17	Main	kuma-aio.sail.m	10.40.0.17	7249	38 секунд	01.04.2024 18:45:21

## Настройка FortiGate

Для настройки отправки событий в формате CEF с FortiGate в KUMA выполните следующие действия:

- Подключитесь к CLI FortiGate по SSH
- Перейдите в секцию настройки параметров Syslog:

```
config log syslogd setting
```

- Выполните настройку параметров Syslog:

```
set status enable # включить отправки событий на удаленный Syslog-сервер
set server <IP-адреса сервера-коллектора KUMA>
set mode udp # отправлять события по UDP
set port <порт, заданный в параметрах коллектора KUMA>
set source-ip <IP-адрес FortiGate> # IP-адрес, который будет использоваться в качестве Source IP при
```

взаимодействии с коллектором KUMA [опционально]

```
set format cef # отправлять события в формате CEF
```

```
set interface-select-method <auto|sdwan|specify> # если выбран specify указать вручную исходящий интерфейс для взаимодействия с коллектором KUMA с помощью команды set interface <наименование интерфейса> [опционально]
```

```
end
```

# Проверка поступления событий FortiGate в KUMA

Для проверки, что сбор событий с FortiGate успешно настроен перейдите в **Ресурсы** > **Активные сервисы** > выберите ранее созданный коллектор для FortiGate и нажмите **Перейти к событиям**.

Ресурсы и сервисы / Сервисы

## Сервисы

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	Время работы	Создан
1	Коллектор	FortiGate UDP/5205	3.11.1	Main	10.10.10.10:5205	38 секунд	01.04.2024 18:45:21

В открывшемся окне **События** убедитесь, что присутствуют события с FortiGate.


  
**Kaspersky**
  
**Unified Monitoring and Analysis Platform**

- Выбрано тенантов: 4
- Панель мониторинга
- Алерты
- Инциденты
- События**
- Активы
- Отчеты
- Ресурсы
- Диспетчер задач
- Параметры
- Состояние источников
- Метрики

bergov

## События

Не обновлять

## Информация о событии

SELECT \* FROM 'events' WHERE ServiceID = '9a9b81f9-58ae-4d8b-a833-d22ab08c7ecd' ORDER BY Timestamp DESC LIMIT

Timestamp ↓	TenantID	DeviceProduct	DeviceVendor	DestinationUserNa...	Dest
01.04.2024 18:51:13	Main	Fortigate	Fortinet	admin	
01.04.2024 18:50:16	Main	Fortigate	Fortinet		

TenantName	Main
Timestamp	01.04.2024 18:51:13.716
Name	eventssystem login success
EndTime	01.04.2024 18:51:22.000
Message	Administrator admin logged in successfully from ssh[...]
DeviceAction	login
DeviceAddress	[...]
DeviceAssetID	FortiGate-VM64
DeviceEventCategory	eventssystem
DeviceEventClassID	32001
DeviceExternalID	FGVMEVWMA2YKBF5A
DeviceFacility	23
DeviceHostName	FortiGate-VM64
DeviceProduct	Fortigate
DeviceReceiptTime	01.04.2024 18:51:22.000
DeviceTimeZone	+03:00
DeviceVendor	Fortinet
DeviceVersion	v6.4.15
SourceAddress	[...]
SourceAssetID	[...]
SourceProcessName	ssh([...])
DestinationAddress	[...]
DestinationAssetID	FortiGate-VM64

# Полезные ссылки

Отправка событий в формате CEF - <https://community.fortinet.com/t5/FortiGate/Technical-Note-FortiGate-Logs-can-be-sent-to-syslog-servers-in/ta-p/190617>

# Континент версия 4

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

## Настройки Континента

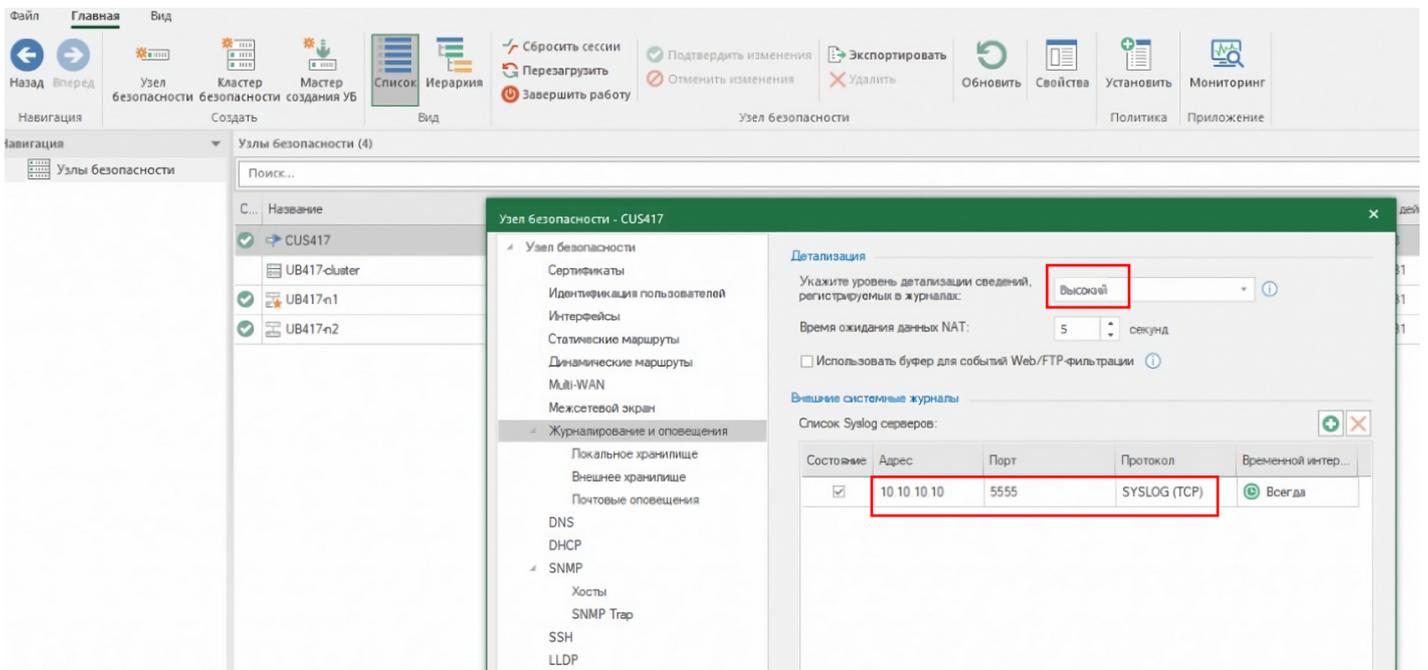
Откройте Менеджер конфигурации Континента.

В настройках узла безопасности раскройте пункт **Журналирование и оповещение**, затем нажмите **+** и пропишите IP адрес и порт коллектора KUMA, рекомендуется использовать протокол TCP.

Уровни детализации журнала в Континенте (Рекомендуемый уровень детализации **Высокий**):

Уровень детализации журнала	Уровень важности события
Отладочный	Отладка (DEBUG)
Минимальный	Информация (INFO)
Низкий	Ошибка (ERR)
Средний	Критическая ошибка (CRIT)
Высокий	Тревога (ALERT)
Предустановленный	Предупреждение (Warning)

Пример настройки ниже:



Нажмите **Применить** и **ОК**.

## Настройка KUMA

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

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне Континента.
2. На шаге **Парсинг** событий выберите нормализатор **[2024-05-03] Unix AuditD (REGEX)** из папки нормализаторов Community-Pack.
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

Справка по Континенту версия 4 - [тут](#)

Статья в HABR по интеграции Континента и KUMA -

<https://habr.com/ru/companies/tssolution/articles/792078/>