

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>

?????????? 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

?????????? 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.

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

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>

Revision #5

Created 2023-08-11 12:38:47 UTC by Koala

Updated 2024-07-07 08:51:23 UTC by Koala