

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

SIEM (Syslog)

- [Настройка отправки событий в Syslog](#)

Настройка отправки системных событий Printum во внешний Syslog-сервер (SIEM)

Системные события

Настройка

Настройка отправки системных событий Printum во внешний Syslog-сервер (SIEM).

Требования

- Syslog-сервер развёрнут и доступен из сети Printum
 - Известен адрес и порт Syslog-сервера
-

Параметры отправки

- Отправка происходит по указанному хосту и порту (например, `192.168.10.10:1514`).
 - Допустимые порты: `514`, `1514`, `1468`. Если порт не указан — используется `514`.
 - Авторизация по стандарту syslog не поддерживается — логин и пароль указывать не нужно.
 - Тело отчёта заполнять не нужно — отправляются все доступные параметры события.
-

Безопасность (TLS)

Для отправки по зашифрованному протоколу укажите CA-сертификат и сертификат клиента в формате `.pem`. Шифрование выполняется по протоколу TLS (выбирается максимально возможная версия для сервера). Если нежелательный протокол TLS активирован — запретите его непосредственно на сервере syslog.

Для настройки syslog-сервера обратитесь к его официальной документации.

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

Логи передаются в следующем формате:

```
2023-05-25T06:15:21.930828+00:00 local Обнаружено новое устройство event=2 user=0ne
additional_parameters={'foo': 0}
2023-05-25T06:32:44.487278+00:00 test.local Обнаружено новое устройство event=4 user=0ne
location="0фис в Иваново" additional_parameters={'foo': 0}
```

Поля:

- event — уникальный идентификатор события.
- user — логин пользователя.
- location — название локации (если есть).
- additional_parameters — дополнительные параметры события.

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

Для проверки прослушиваемого порта (TCP/UDP) на сервере syslog:

```
netstat -tulnp
```

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

События из Printum поступают в Syslog-сервер в заданном формате.

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

Перейдите по адресу https://<адрес_сервера>:8001/config/integrations/ и выберите раздел «Внешние интеграции». Нажмите «Добавить».

Заполните поля:

Параметр	Описание
Название конфигурации	Произвольное имя интеграции, например «Syslog SIEM»

Параметр	Описание
Хост	Адрес и порт сервера Syslog, например `192.168.10.10:1514`. Допустимые порты: 514, 1514, 1468. Если порт не указан — используется 514
Тип интеграции	Выбрать **Syslog**
Locations	Локации, события которых передаются. Если не выбрать — передаются все события
Интервал между обменами	Время в минутах (минимум 1 минута)
Включено	Активировать интеграцию после создания
CA сертификат	Для шифрования по TLS — CA-сертификат в формате .pem
Сертификат	Файл SSL-сертификата клиента (.pem, без кодовой фразы)

Важно: авторизация по стандарту Syslog не поддерживается — логин и пароль указывать не нужно.

????????? ?????????????????? ?????????? ??? Syslog

- После создания интеграции нажать **«Добавить»** рядом с разделом «Отчёты для отправки» (события или логи безопасности).
- Заполнить поля:
 - Внешняя интеграция** — выбрать созданную интеграцию.
 - Тело отчёта** — поля для включения в отчёт (оставить пустым — передаются все поля).

Для каждой интеграции допускается только один конструктор отчётов. Для передачи данных по нескольким пользователям необходимо создать несколько интеграций.

??????? ?????????? Syslog

Пример лога:

```
2023-05-25T06:15:21.930828+00:00 local Обнаружено новое устройство event=2 user=0ne
additional_parameters={'foo': 0}
2023-05-25T06:32:44.487278+00:00 test.local Обнаружено новое устройство event=4 user=0ne
```

```
location="Офис в Иваново" additional_parameters={'foo': 0}
```

Поля события:

Поле	Тип	Описание
event	число	Уникальный ID события
user	строка	Логин пользователя
location	строка	Название локации (если есть)
additional_parameters	JSON	Дополнительные параметры события

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

Поле	Тип	Описание
event_group	строка	Группа событий
event_name	строка	Название события
event_name_unique_id	число	ID события
timestamp	строка	Время в формате ISO (пример: "2005-08-09T18:31:42")
operation_subject	строка	Субъект операции
operation_object	строка	Объект операции
result	строка	Результат операции
event_level	строка	Уровень критичности
changed_params	JSON	Изменённые параметры

????????? TLS

Для передачи по зашифрованному каналу укажите CA-сертификат и сертификат клиента в формате .pem. Версия TLS выбирается максимально возможная для сервера Syslog. Если нужна конкретная версия TLS — запретите нежелательные протоколы на стороне сервера Syslog.

Для проверки порта Syslog на сервере:

```
netstat -tulnp
```

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

- [Настройка подключения к почтовому серверу](#)
- [Управление пользователями — обзор](#)