

# Мессенджер и ВКС

## Инструкция по настройке интеграции с SIEM-системой

|   |    |
|---|----|
| Назначение документа  | 3  |
| Дополнительная документация                                   | 3  |
| Отправка логов в SIEM-систему                                 | 4  |
| Логируемые события и формат логов                             | 4  |
| Отправка текстового сообщения                                 | 6  |
| Отправка файла  | 6  |
| Аудио или видеовывод  | 6  |
| Вход в систему  | 7  |
| Скачивание/автоскачивание файла                               | 7  |
| Настройка отправки лог-файлов в SIEM-систему                  | 9  |
| Настройка отправки логов о скачивании и автоскачивании файлов | 10 |

# Назначение документа

---

В данном документе представлено описание логируемых событий и формат лог-файлов, а также настройка отправки лог-файлов в SIEM-систему.

Документ предназначен для использования системными администраторами.

# Дополнительная документация

---

[Логи Мессенджер и ВКС](#) — в документе представлена информация об инструментах сбора логов, расположении логов и приведены примеры запросов и ответов.

# Отправка логов в SIEM-систему

Для интеграции с SIEM-системой используется мультиплатформенный инструмент сбора и централизации журналов NXlog.

По умолчанию отправка лог-файлов в SIEM-систему осуществляется через syslog, однако используемый продукт поддерживает множество различных транспортов. Подробнее — в документации на продукт <https://nxlog.co/products/nxlog-community-edition>.

## Логируемые события и формат логов

Вы можете настроить отправку в SIEM-систему логов следующих событий

- Отправка текстового сообщения (IM).
- Отправка файла (FILE).
- Аудио или видеовызов (CALL).
- Логин (LOGIN).
- Удаление сообщения (DEL\_MSG).
- Удаление истории (DEL\_HISTORY).
- Скачивание/автоскачивание файла из чата/группы (получение клиентским приложением файла с сервера). В SIEM-систему передается информация, какой пользователь скачал, название, тип, размер и расширение файла. Автоскачивание файла — автоматическое скачивание файлов небольшого размера без явного действия со стороны пользователя, например, при прокрутке чата и отображении вложений. При скачивании/автоскачивании файла сервис пишет логи в файл по пути, указанному в конфиге (files.log).

Все записи в логе соответствуют следующему формату:

Дата время|IP пользователя А|ID пользователя А|ID пользователя Б|User-Agent пользователя А|Тип события|Специфические для события данные|Аутентификационный токен

Описание полей представлено в таблице ниже:

| Поле              | Описание      | Формат          |
|-------------------|---------------|-----------------|
| Дата              | Дата события  | YYYY-MM-DD      |
| Время             | Время события | hh:mm:ss        |
| IP пользователя А |               | XXX.XXX.XXX.XXX |

| Поле                             | Описание  | Формат   |
|----------------------------------|---|--|
|                                  | IP адрес пользователя, совершившего событие   |  |
| ID пользователя А                | Идентификатор пользователя, совершившего событие  | email  |
| ID пользователя Б                | Идентификатор пользователя получателя события   | email или ID группы или «-», если не применимо к событию |
| User-Agent пользователя А        | User-Agent пользователя А, по заголовку User-Agent в HTTP-запросах  | Описание формата представлено ниже                       |
| Тип события                      | Тип события: звонок, отправка сообщения и т.д.  | CALL, IM, FILE, LOGIN, DEL_MSG, DEL_HISTORY              |
| Специфические для события данные | Флаги и опции, специфичные для события  | Зависит от события                                       |
| Аутентификационный токен         | Хэш от сессионного токена пользователя. Может отсутствовать. Например, при логине, так как сессия пользователя еще не создана. Хэш от токена можно использовать, чтобы отличить различные сессии одного пользователя. Получить аутентификационный токен из хэша нельзя. | d9ce1e74d5   |

#### Формат User-Agent:

- Для Android, iOS и Desktop:

```
VKTeams {Android, iOS, Desktop} <user email> <Application ID> <build version A.B.C(D)> <OS Version> <Device>
```

- Для веб-клиента User-Agent зависит от браузера и может выглядеть так:

```
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.185 YaBrowser/20.11.3.0 (beta) Yowser/2.5 Safari/537.36
```

#### Пути к лог-файлам

**/oap/icq/logs/\*.on-premise.log** — для данной группы файлов все строки логов являются источником информации для SIEM-системы.

**/data/tarantool/logs/nomail-\*.log** — для данной группы файлов источником для SIEM-системы являются строки логов, попадающие под регулярное выражение `^.*?fss:.***`

## Отправка текстового сообщения

**Пример:** Пользователь i.ivanov@domain.ru отправил тестовое сообщение пользователю v.petrov@domain.ru. IP адрес и User-Agent пользователя i.ivanov@domain.ru - 109.195.135.94 и Myteam Desktop 155576093 ic1nmMjqg7Yu-0hL 10.0.0(42540) Windows\_10 PC соответственно.

**Запись в лог:**

```
2020-11-30 10:06:38|109.195.135.94|i.ivanov@domain.ru|v.petrov@domain.ru|Myteam Desktop  
i.ivanov@domain.ru ic1nmMjqg7Yu-0hL 10.0.0(42540) Windows_10 PC|IM|-|d9ce1e74d5
```

## Отправка файла

| Параметр | Описание  |
|----------|---|
| file_id  | Хэш от идентификатора файла. Можно использовать для сопоставления с другими записями в этом же логге. Нельзя использовать для получения контента файла. |

**Пример:** Пользователь d.sidorov@domain.ru отправил файл в группу 683673651@chat.agent.

**Запись в лог:**

```
2020-11-30 10:25:05|95.57.100.171|d.sidorov@domain.ru|683673651@chat.agent|Myteam Android  
d.sidorov@domain.ru ao1mAegmj4_7xQ0y 9.16.1(824729) Android_7.1.1_25 SM-J510FN|FILE|  
file_id=5191ceb402|ac6208d080
```

## Аудио или видеовывоз

**Пример:** Пользователь a.smirnov@domain.ru вызвал пользователя d.kulikov@domain.ru. 2020-11-30 09:36:36 - дата и время начала звонка.

**Запись в лог:**

```
2020-11-30 09:36:36|176.59.142.53|a.smirnov@domain.ru|d.kulikov@domain.ru|Myteam Android  
a.smirnov@domain.ru ao1mAegmj4_7xQ0y 7.7.2(823881) Android_5.1.1_22 SM-J320F|CALL|-|5daaefde7f
```

# Вход в систему

| Параметр | Описание   |
|----------|--|
| type     | Тип логина. Сейчас доступен только OTP.  |
| result   | <ul style="list-style-type: none"><li>- sent — OTP отправлен на почту пользователю;</li><li>- invalid — введен неверный OTP, или срок его жизни истёк;</li><li>- success — успешный логин.</li></ul> |

## Запрос OTP:

```
2020-11-30 01:21:21|172.11.11.67|d.sidorov@domain.ru|-|Myteam Android d.sidorov@domain.ru
ao1mAegmj4_7xQ0y 7.7.2(823881) Android_5.1.1_22 SM-J320F|логIN|type=otp,result=sent|-
```

## Неуспешная попытка логина пользователя d.kulikov@domain.ru по OTP:

```
2020-11-30 01:21:21|172.11.11.67|d.kulikov@domain.ru|-|Myteam Android d.kulikov@domain.ru
ao1mAegmj4_7xQ0y 7.7.2(823881) Android_5.1.1_22 SM-J320F|LOGIN|type=otp,result=invalid|-
```

## Успешная попытка логина пользователя d.kulikov@domain.ru по OTP:

```
2020-11-30 01:21:21|172.11.11.67|d.kulikov@domain.ru|-|Myteam Android d.kulikov@domain.ru
ao1mAegmj4_7xQ0y 7.7.2(823881) Android_5.1.1_22 SM-J320F|LOGIN|type=otp,result=success|-
```

## Удаление сообщения

```
21-12-10 17:02:59|100.100.31.151|dev001@nsoldatov.v2.im-sandbox.devmail.ru|
dev002@nsoldatov.v2.im-sandbox.devmail.ru|<-|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36|DEL_MSG|-|
silent=0,msgid=7040073549926629644,
```

## Удаление истории

```
21-12-10 17:14:34|100.100.31.151|dev001@nsoldatov.v2.im-sandbox.devmail.ru|
dev002@nsoldatov.v2.im-sandbox.devmail.ru|<-|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36|DEL_HISTORY|-|
upTo=7040073549926629644,
```

# Скачивание/автоскачивание файла

**Пример:** пользователь d.kulikov@domain.ru загрузил файл на устройство.

## Запись в лог:

```
25-08-29 14:47:27|172.1.15.23|d.kulikov@domain.ru|Mozilla/5.0 (Macintosh; Intel Mac OS X
10.15; rv:102.0) Gecko/20100101 Firefox/102.0|DOWNLOAD|file_id=1d42f31c-
```

```
c36e-4ba6-9e7c-558768b4c184,size=5000,name=test_image,type=image,extension=,auto=false,author=test-user@dev.001.ru|-
```

Если произошло автоматическое скачивание файла, в логе будет признак `auto=true`



# Настройка отправки лог-файлов в SIEM-систему

Чтобы включить отправку в SIEM-систему логов следующих событий:

- Отправка текстового сообщения.
- Отправка файла.
- Аудио или видеовывод.
- >Login.
- Удаление сообщения.
- Удаление истории.

выполните шаги, описанные ниже:

1. В конфигурационном файле **/usr/local/etc/k8s/helmwave/projects/nxlog/values/nxlog.yml** в блоке **<Output siem\_system>**

указать IP-адрес и порт приемника SIEM:

```
<Output siem_system>
  Module  om_udp
  Host     <указать IP-адрес>
  Port     <указать порт>
  <Exec>
    $Severity = 'INFO';
    $SyslogFacility = 'AUDIT';
    $SourceName = 'logs';
    $Hostname = '${NODE_NAME}';
    to_syslog_bsd();
  </Exec>
</Output>
```

В данном блоке в качестве приемника используется Syslog-сервер. Если будет использоваться не Syslog-сервер, опишите настройки для другой системы (см. официальную документацию <https://docs.nxlog.co/integrate/index.html>).

2. В конфигурационном файле **/usr/local/etc/k8s/helmwave/projects.yml** удалить nxlog.
3. Для запуска nxlog выполните команды в зависимости от типа инсталляции.

Для инсталляций на одну виртуальную машину:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwbuid -t nxlog
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t nxlog
```

Для кластерной инсталляции:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwbuid -t nxlog  
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t nxlog
```

4. Посмотреть логи самого сервиса можно при помощи команды:

```
kubectl -n vkteams -l app=nxlog --tail -1
```

## Настройка отправки логов о скачивании и автоскачивании файлов

На каждой виртуальной машине, где необходимо включить логирование, выполните:

1. Перейдите в конфигурационный файл сервиса Go-files **/usr/local/go.files.icq.com/files.icq.com.config.yaml** и убедитесь, что указано корректное значение для параметра **path**. Убедитесь, что файл существует и установите для **enabled** значение true. Конфигурация должна выглядеть так:

```
fss:  
  enabled: true  
  path: "/oap/icq/logs/go.files.icq.com/siem/files.log"
```

где:

- enabled — включение/отключение отправки логов в SIEM-систему.
- path — путь до файла, где будут лежать SIEM-логи сервиса.

2. Перезапустите сервис Go-files командой:

```
sudo systemctl restart gofiles_httpd
```

Чтобы включить отставку логов в SIEM-систему, на каждой виртуальной машине, где необходимо включить отставку логов, создайте simlink:

```
ln -s /oap/icq/logs/go.files.icq.com/siem/files.log /oap/icq/logs/gofiles_httpd.on-premise.log
```

 Технический писатель: Белова Ирина

 26 ноября 2025 г.