

Table of Contents

Table of Contents	1
Общие положения	2
Общие положения (описание)	3

Общие положения (описание)

Documentation: ☒

Product: SIEM

Version: 7.x

UserGate SIEM поддерживает интерфейс командной строки CLI (Command Line Interface), с помощью которого можно производить настройку устройства.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить с помощью протокола SSH по сети.

Примечание Если устройство не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — usergate.

Для подключения к CLI выполните следующие шаги:

1. В разделе **Настройки** → **Сеть** → **Зоны** для зоны, к которой вы собираетесь подключаться для управления с помощью CLI, разрешите доступ для протокола CLI по SSH. Будет открыт порт TCP 2200.
2. Запустите у себя на компьютере SSH-терминал, например SSH для Linux или Putty для Windows. Укажите адрес устройства UserGate SIEM, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами корневого администратора (по умолчанию Admin с паролем usergate). Для Linux команда на подключение должна выглядеть так:

```
ssh Admin@<IP-SIEM> -p 2200
```

После успешной аутентификации в CLI появится строка ожидания ввода команды (режим диагностики). Для просмотра текущих возможных значений или автодополнения команды используйте клавишу «Tab». В режиме диагностики доступны следующие команды:

- **configure** — переход в режим конфигурации.
- **date** — просмотр текущих даты и времени на устройстве.
- **dig** — проверка записи DNS-домена.
- **exit** — выход из командной строки.
- **netcheck** — проверка доступности стороннего HTTP/HTTPS-сервера.
- **show** — просмотр сетевых настроек, версии ПО, статистики активных сессий.
- **clear** — очистка данных статистики по активным сессиям и сетевым интерфейсам.
- **ping** — выполнение ping определённого хоста.
- **reboot** — перезагрузка устройства.
- **shutdown** — выключение устройства.
- **traceroute** — трассировка соединения до определённого хоста.

Эти команды доступны также в режиме конфигурации. Подробнее — в разделе [«Команды execute»](#).

Для отмены ввода текущей команды используйте сочетание клавиш «Ctrl + C»; для просмотра истории команд — клавиши клавиатуры «↑» и «↓».

Все команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

Где:

<action> — действие, которое необходимо выполнить.

<level> — уровень конфигурации; уровни соответствуют разделам веб-интерфейса NGFW.

<filter> — идентификатор объекта, к которому происходит обращение.

<configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

