

**Table of Contents**

|                               |   |
|-------------------------------|---|
| Table of Contents             | 1 |
| Режим конфигурации            | 2 |
| Режим конфигурации (описание) | 3 |



Режим конфигурации (описание)

Documentation: ☒  
Product: SIEM  
Version: 7.x

Для перехода в режим конфигурации используется команда:

Admin@nodename> configure

После перехода в режим конфигурации командная строка будет выглядеть следующим образом:

Admin@nodename#

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

- \* — обязательное поле в командах create и ряде других команд;
- + — необязательное/вариативное поле;
- > — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Например:

```
Admin/system@nodename# set network zone Trusted
* name          Name
+ antispoof-enable  Enable/Disable IP spoofing protection
+ antispoof-negate  Enable/Disable Negate ip-spoof addresses
+ description      Description
+ enabled-services  Services list to enable
+ geoip            IP spoofing protection by geo IP code
+ ip-list           IP spoofing protection by IP list
> dos-protection-icmp  Confugure DoS protection per IP for ICMP packets
> dos-protection-syn   Confugure DoS protection per IP for SYN packets
> dos-protection-udp   Confugure DoS protection per IP for UDP packets
> service-addresses   Access control service addresses
```

Общая структура команд в режиме конфигурации

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-консоли UserGate SIEM.
- <filter> — идентификатор объекта, к которому происходит обращение.
- <configuration\_info> — значение параметров, которые необходимо применить к объекту <filter>.

| Наименование | Описание |
|--------------|----------|
|              |          |

| Наименование | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <action>     | <p>В режиме конфигурации доступны следующие действия:</p> <ul style="list-style-type: none"> <li>• <b>execute</b> — выполнение команд, которые не относятся к конфигурации UserGate (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации (&lt;level&gt;).</li> <li>• <b>set</b> — редактирование всех объектов, а также включение различных параметров, например, radmin.</li> <li>• <b>end</b> — переход на один уровень выше.</li> <li>• <b>show</b> — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня.</li> <li>• <b>edit</b> — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой.</li> <li>• <b>top</b> — возврат на самый верхний уровень конфигурации.</li> <li>• <b>exit</b> — выход из режима конфигурации.</li> <li>• <b>export</b> — экспорт конфигурации.</li> <li>• <b>import</b> — импорт конфигурации.</li> <li>• <b>create</b> — создание новых объектов.</li> <li>• <b>delete</b> — удаление объекта или параметра из списка параметров.</li> </ul> <p>Например, для просмотра информации о всех интерфейсах необходимо выполнить команду:</p> <pre>Admin@nodename# show network interface</pre> <p>С использованием следующей команды производится переход на уровень <b>network interface</b>. Текущий уровень будет отображён под командной строкой:</p> <pre>Admin@nodename# edit network interface Admin@nodename# Level: network interface</pre> <p>После перехода на уровень <b>network interface</b> для отображения всех интерфейсов используется команда show без указания уровня:</p> <pre>Admin@nodename# show</pre> <pre>adapter: port0   type          : adapter   interface-name : port0   node-name      : node   zone           : Management   enabled        : on   ip-addresses   : 192.168.56.3/24   iface-mode     : dhcp ... ... ... Level: network interface</pre> <p>Для возвращения с уровня <b>network interface</b> обратно на общий уровень режима конфигурации необходимо набрать команду <b>end</b>:</p> <pre>Admin@nodename# end Level: network interface Admin@nodename# end Level: network Admin@nodename#</pre> |

| Наименование         | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <level>              | <p>Уровни в командной строке повторяют веб-интерфейс системной консоли UserGate SIEM:</p> <ul style="list-style-type: none"> <li>• <b>network</b> — соответствует разделу веб-интерфейса <b>Сеть</b>.</li> <li>• <b>settings</b> — соответствует разделу веб-интерфейса <b>UserGate</b>.</li> <li>• <b>users</b> — соответствует разделу веб-интерфейса <b>Пользователи и устройства</b>.</li> <li>• <b>libraries</b> — соответствует разделу веб-интерфейса <b>Библиотеки</b>.</li> <li>• <b>monitoring</b> — соответствует разделу веб-интерфейса <b>Диагностика и мониторинг</b>.</li> <li>• <b>sensors</b> — соответствует разделу веб-интерфейса <b>Сенсоры</b>.</li> <li>• <b>analytics</b> — соответствует разделу веб-интерфейса <b>Аналитика</b>.</li> <li>• <b>incident</b> — соответствует разделу веб-интерфейса <b>Инциденты</b>.</li> </ul>                                                                                           |
| <filter>             | <p>Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать &lt;configuration_info&gt;. В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <configuration_info> | <p>Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным.</p> <p><b>Одиночный аргумент</b> — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки.</p> <p>Например, необходимо создать профиль аутентификации с именем New profile:</p> <pre>Admin@nodename# create users auth-profile name "New profile"</pre> <p><b>Множественные аргументы</b> используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами.</p> <p>Например, необходимо создать список IP-адресов в библиотеке элементов и добавить в него два IP-адреса 10.10.0.1 и 10.10.0.2:</p> <pre>Admin@nodename# create libraries ip-list name testlist ips [ 10.10.0.1 10.10.0.2 ]</pre> <p><b>Важно!</b> Квадратные скобки должны быть отделены пробелами с обеих сторон.</p> |

## Команды execute

Команды имеет следующую структуру:

```
Admin@nodename# execute <command-name>
```

Доступны следующие команды:

| Параметр    | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| traceroute  | <p>Трассировка соединения до определённого хоста. Доступны параметры:</p> <ul style="list-style-type: none"> <li>• <b>hostname &lt;ip-or-domain&gt;</b> — IP-адрес или имя домена, для которого производится трассировка.</li> <li>• <b>interface &lt;iface-name&gt;</b> — интерфейс, с которого будут отправляться пакеты.</li> <li>• <b>not-map-ip</b> — не искать hostname для IP-адреса при отображении.</li> <li>• <b>use-icmp-echo</b> — использовать ICMP echo.</li> <li>• <b>port</b> — указать порт вместо порта по умолчанию (1 — 65535).</li> <li>• <b>min-interval</b> — минимальный интервал между пакетами.</li> </ul> <pre>Admin@nodename# execute traceroute hostname &lt;hostname&gt;</pre> |
| termination | <p>Закрытие сессий администраторов. Подробнее читайте в разделе <a href="#">Управление сессиями администраторов</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Параметр | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ping     | <p>Выполнение ping определенного хоста. Можно задать следующие параметры:</p> <ul style="list-style-type: none"> <li>• <b>hostname</b> — IP-адрес или доменное имя хоста.</li> <li>• <b>count</b> — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C).</li> <li>• <b>numeric</b> — не резолвить имена.</li> <li>• <b>timestamp</b> — отображение временных меток.</li> <li>• <b>interval</b> — интервал времени, через который будет производиться отправка пакетов; указывается в секундах.</li> <li>• <b>ttl</b> — время жизни пакета.</li> <li>• <b>interface</b> — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping.</li> <li>• <b>mtu</b> — размер mtu отправляемых пакетов.</li> <li>• <b>virtual-router</b> — имя виртуального маршрутизатора.</li> </ul> <p>Admin@nodename# execute ping hostname &lt;hostname&gt; count &lt;number&gt;</p>                                                                                                                                                          |
| reboot   | Перезагрузка устройства.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| date     | Просмотр текущих даты и времени на сервере.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| shutdown | Выключение устройства.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| netcheck | <p>Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры:</p> <ul style="list-style-type: none"> <li>• <b>address</b> — доменное имя хоста для проверки доступности по TCP или URL для HTTP.</li> <li>• <b>dns-ip</b> — IP-адрес сервера DNS.</li> <li>• <b>dns-tcp</b> — использование TCP вместо UDP для DNS-запроса.</li> <li>• <b>check-cert</b> — проверка SSL-сертификата</li> <li>• <b>type</b> — проверка доступности по: <ul style="list-style-type: none"> <li>◦ <b>http</b>.</li> <li>◦ <b>tcp</b> (если порт не указан, то используется порт 80).</li> </ul> </li> <li>• <b>data</b> — запрос содержимого сайта. По умолчанию запрашиваются только заголовки.</li> <li>• <b>timeout</b> — максимальный таймаут ожидания ответа от веб-сервера.</li> <li>• <b>user-agent</b> — параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках.</li> </ul> <p>Admin@nodename# execute netcheck type tcp address &lt;host-domain-name&gt; data on<br/>Admin@nodename# execute netcheck address &lt;host-domain-name&gt;</p> |
| dig      | <p>Проверка записи DNS домена.</p> <ul style="list-style-type: none"> <li>• <b>hostname</b> — доменное имя хоста или IP-адрес для реверсивного поиска.</li> <li>• <b>reverse-lookup</b> — получение хоста по IP-адресу.</li> <li>• <b>dns</b> — указание IP-адреса DNS-сервера.</li> <li>• <b>tcp</b> — использование протокола TCP вместо UDP.</li> </ul> <p>Admin@nodename# execute dig hostname &lt;host-domain-name&gt;<br/>Admin@nodename# execute dig hostname &lt;IP-address&gt; reverse-lookup on</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| license  | <p>Команда регистрации продукта имеет следующую структуру:</p> <p>Admin@nodename# execute license activate &lt;pin-code&gt;</p> <p>Укажите код активации продукта вместо &lt;pin-code&gt;.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Часть представленных выше команд также доступны в режиме диагностики и мониторинга. Для их выполнения используется команда:

Admin@nodename> <command-name>

