

## Table of Contents

|                                             |   |
|---------------------------------------------|---|
| Table of Contents                           | 1 |
| Настройка мониторинга                       | 2 |
| Настройка параметров мониторинга устройства | 3 |



Documentation: ☒  
Product: SIEM  
Version: 7.1.x

Настройка параметров мониторинга устройства в интерфейсе CLI производится в режиме конфигурации на уровне **monitoring**. Команды этого уровня позволяют управлять настройкой параметров SNMP устройства, правил мониторинга по SNMP, профилей безопасности для аутентификации SNMP-менеджеров, правилами оповещений. Подробнее о правилах мониторинга и оповещений читайте в разделе [Оповещения](#).

Настройка параметров SNMP устройства

Для настройки параметров SNMP устройства используются команды на уровне **monitoring snmp-parameter**:

Admin@nodename# edit monitoring snmp-parameter <parameters>

Для редактирования доступны следующие параметры:

| Параметр    | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| agent-name  | Название системы, используемое подсистемой управления SNMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| location    | Информация о физическом расположении SNMP-агента.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| description | Описание системы.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Engine ID   | <p>Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину (<b>length</b>), тип и значение идентификатора. Длина может быть определена как фиксированная (не более 8 байт) или динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа <b>text</b>.</p> <p>Engine ID может быть сформирован в формате:</p> <ul style="list-style-type: none"><li>• <b>ip4</b> — IPv4.</li><li>• <b>ipv6</b> — IPv6.</li><li>• <b>mac</b> — MAC-адрес.</li><li>• <b>text</b> — Текст.</li><li>• <b>octets</b> — Октеты.</li></ul> |

Подробнее о параметрах SNMP устройства UserGate читайте в разделе [SNMP](#).

Настройка правил мониторинга по SNMP

Для настройки правил мониторинга устройства по SNMP используются команды на уровне **monitoring snmp**:

Admin@nodename# edit monitoring snmp <parameters>

Для редактирования доступны следующие параметры:

| Параметр  | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| name      | Название правила.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| enabled   | Включение/отключение правила                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| community | SNMP community — строка для идентификации устройства UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| context   | <p>Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры.</p> <p>На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.</p> |

| Параметр                | Описание                                                                                                                                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>version</b>          | Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.                                                    |
| <b>query</b>            | При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.                                                                                           |
| <b>trap</b>             | При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.                                                                               |
| <b>trap-host</b>        | IP-адрес сервера для трапов. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.                                         |
| <b>trap-port</b>        | Порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений. |
| <b>security-profile</b> | Только для SNMP v3. Подробнее — в разделе <a href="#">Профили безопасности SNMP</a> .                                                                                    |
| <b>events</b>           | Выбор типов параметров, доступных для мониторинга по правилу.                                                                                                            |

Для работы SNMP-менеджера с устройством UserGate необходимо в свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, разрешить сервис **SNMP** в настройках контроля доступа. Подробнее о настройке зон в CLI читайте в разделе [Настройки сети](#).

## Настройка профилей безопасности SNMP

Для настройки профилей безопасности для аутентификации SNMP-менеджеров используются команды на уровне **monitoring snmp-security-profile**:

```
Admin@nodename# edit monitoring snmp-security-profile <parameters>
```

Для редактирования доступны следующие параметры:

| Параметр             | Описание                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>name</b>          | Название профиля безопасности SNMP                                                                                                                                                                                                                                                                                                                                |
| <b>description</b>   | Описание профиля безопасности SNMP                                                                                                                                                                                                                                                                                                                                |
| <b>username</b>      | Имя пользователя для аутентификации SNMP-менеджера.                                                                                                                                                                                                                                                                                                               |
| <b>auth-type</b>     | <p>Выбор режима аутентификации SNMP-менеджера. Возможны варианты:</p> <ul style="list-style-type: none"> <li><b>none</b> — без аутентификации, без шифрования.</li> <li><b>no-encrypt</b> — с аутентификацией, без шифрования.</li> <li><b>encrypt</b> — с аутентификацией, с шифрованием.</li> </ul> <p>Наиболее безопасным считается режим работы authPriv.</p> |
| <b>auth-alg</b>      | <p>Алгоритм, используемый для аутентификации. Возможно использовать:</p> <ul style="list-style-type: none"> <li><b>sha</b>;</li> <li><b>md5</b>;</li> <li><b>sha224</b>;</li> <li><b>sha256</b>;</li> <li><b>sha384</b>;</li> <li><b>sha512</b>.</li> </ul>                                                                                                       |
| <b>auth-password</b> | Пароль, используемый для аутентификации.                                                                                                                                                                                                                                                                                                                          |

| Параметр                | Описание                                                                |
|-------------------------|-------------------------------------------------------------------------|
| <b>encrypt-alg</b>      | Алгоритм, используемый для шифрования. Возможно использовать DES и AES. |
| <b>encrypt-password</b> | Пароль, используемый для шифрования.                                    |

## Настройка правил оповещений

Для настройки правил оповещений используются команды на уровне **monitoring alert-rules**:

Admin@nodename# edit monitoring alert-rules <parameters>

Для редактирования доступны следующие параметры:

| Параметр                    | Описание                                                                                                                                                                                                           |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>enabled</b>              | Включает/отключает данное правило.                                                                                                                                                                                 |
| <b>name</b>                 | Название правила.                                                                                                                                                                                                  |
| <b>description</b>          | Описание правила.                                                                                                                                                                                                  |
| <b>notification-profile</b> | Созданный ранее профиль оповещения.                                                                                                                                                                                |
| <b>sender</b>               | От кого будет приходить оповещение.                                                                                                                                                                                |
| <b>subject</b>              | Тема оповещения.                                                                                                                                                                                                   |
| <b>timeout</b>              | Тайм-аут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения. |
| <b>events</b>               | События, для которых необходимо получать оповещения.                                                                                                                                                               |
| <b>phones</b>               | Для SMPP-профиля. Группы номеров телефонов, куда отправлять SMS-оповещения.                                                                                                                                        |
| <b>emails</b>               | Для SMTP-профиля. Группы адресов email, на которые будут отправляться почтовые оповещения.                                                                                                                         |

