

Table of Contents

Table of Contents	1
Интерфейс командной строки (CLI)	2
Общие положения	3
Общие положения (описание)	4
Команды, доступные до первичной инициализации узла	5
Команды, доступные до первичной инициализации узла (описание)	6
Первоначальная инициализация	7
Первоначальная инициализация (описание)	8
Режим конфигурации	9
Режим конфигурации (описание)	10
Настройка устройства	13
Настройка устройства (описание)	14
Настройка управления доступом к консоли устройства	17
Настройка сертификатов	20
Настройка серверов аутентификации	21
Настройка профилей аутентификации	24
Роли пользователей	25
Каталоги пользователей	26
Настройка сети	27
Зоны	28
Интерфейсы	30
Шлюзы	35
Настройка маршрутизации	36
DNS-настройки	37
Настройка библиотек	38
Настройка библиотек (Описание)	39
Настройка раздела пользователи и устройства	46
Настройка UserID агента	47
Настройка профиля редистрибуции UserID	49
Настройка сенсоров	50
Настройка сенсоров (описание)	51
Настройка мониторинга	54
Настройка параметров мониторинга устройства	55
Настройка инцидентов	57
Настройка инцидентов (описание)	58
Настройка аналитики	59
Настройка аналитики (описание)	60

Общие положения (описание)

Documentation: 
Product: SIEM
Version: 7.1.x

В UserGate SIEM имеется возможность производить настройку устройства с помощью интерфейса командной строки CLI (Command Line Interface).

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 через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании SIEM), через последовательный порт или с помощью 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 с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к устройству	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB.
Шаг 2. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами корневого администратора (по умолчанию Admin).

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к устройству	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к устройству.
Шаг 2. Запустить терминал	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.
Шаг 3. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами корневого администратора (по умолчанию Admin).

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200.
Шаг 2. Запустить SSH-терминал	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес устройства SIEM, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами корневого администратора (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так: <code>ssh Admin@IPSIEM -p 2200</code>
Шаг 3. Войти в CLI	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге.

После успешной аутентификации в CLI появится строка ожидающая ввода команды (режим диагностики). Для просмотра текущих возможных значений или автодополнения необходимо использовать клавишу **Tab**. Доступны:

- **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.

Данные команды доступны в режиме конфигурации; подробнее читайте в разделе [Команды execute](#).

Для отмены ввода текущей команды используется сочетание **Ctrl + C**; для просмотра истории команд — ↑, ↓.

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>.

Команды, доступные до первичной инициализации узла

Команды, доступные до первичной инициализации узла (описание)

Documentation: 

Product: SIEM

Version: 7.1.x

Если устройство не прошло первоначальную инициализацию, то в CLI доступны команды диагностики и мониторинга, а в режиме конфигурации — только команды настройки сети, т.е. настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, а также включение/отключение удалённого доступа к серверу `admin-emergency`.

Первоначальная инициализация

Первоначальная инициализация (описание)

Documentation: 
Product: SIEM
Version: 7.1.x

Первоначальная инициализация устройства с использованием интерфейса командной строки.

Для настройки устройства используется команда:

Admin@nodename# execute install master

Необходимо указать параметры:

Параметр	Описание
login	Задать логин администратора.
password	Задать пароль учётной записи администратора. Указание пароля также доступно при нажатии Enter после указания логина администратора; необходимо дважды ввести пароль учётной записи.

Режим конфигурации (описание)

Documentation: 
Product: SIEM
Version: 7.1.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  Configure DoS protection per IP for ICMP packets
> dos-protection-syn   Configure DoS protection per IP for SYN packets
> dos-protection-udp   Configure 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-интерфейса LogAp.
- <filter> — идентификатор объекта, к которому происходит обращение.
- <configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Наименование	Описание

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • execute — выполнение команд, которые не относятся к конфигурации UserGate (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации (<level>). • set — редактирование всех объектов, а также включение различных параметров, например, gadmin. • end — переход на один уровень выше. • show — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня. • edit — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой. • top — возврат на самый верхний уровень конфигурации. • exit — выход из режима конфигурации. • export — экспорт конфигурации. • import — импорт конфигурации. • create — создание новых объектов. • delete — удаление объекта или параметра из списка параметров. Например, для просмотра информации о всех интерфейсах необходимо выполнить команду: <pre>Admin@nodename# show network interface</pre> С использованием следующей команды производится переход на уровень network interface. Текущий уровень будет отображён под командной строкой: <pre>Admin@nodename# edit network interface Admin@nodename# Level: network interface</pre> После перехода на уровень network interface для отображения всех интерфейсов используется команда show без указания уровня: <pre>Admin@nodename# show 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> Для возвращения с уровня network interface обратно на общий уровень режима конфигурации необходимо набрать команду end: <pre>Admin@nodename# end Level: network interface Admin@nodename# end Level: network Admin@nodename#</pre>
<level>	Уровни в командной строке повторяют веб-интерфейс системной консоли LogAn: • network — соответствует разделу веб-интерфейса Сеть. • settings — соответствует разделу веб-интерфейса UserGate. • users — соответствует разделу веб-интерфейса Пользователи и устройства. • libraries — соответствует разделу веб-интерфейса Библиотеки. • monitoring — соответствует разделу веб-интерфейса Диагностика и мониторинг. • sensors — соответствует разделу веб-интерфейса Сенсоры. • analytics — соответствует разделу веб-интерфейса Аналитика. • incident — соответствует разделу веб-интерфейса Инциденты.
<filter>	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 <configuration_info>. В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках.
<configuration_info>	Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. Например, необходимо создать профиль аутентификации с именем New profile: <pre>Admin@nodename# create users auth-profile name "New profile"</pre> Множественные аргументы используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами. 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: <pre>Admin@nodename# create libraries ip-list name testlist ips [10.10.0.1 10.10.0.2]</pre> Важно! Квадратные скобки должны быть отделены пробелами с обеих сторон.

Команды execute

Команды имеет следующую структуру:

Admin@nodename# execute <command-name>

Доступны следующие команды:

Параметр	Описание

Параметр	Описание
tracert	Трассировка соединения до определённого хоста. Доступны параметры: • hostname <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка. • interface <iface-name> — интерфейс, с которого будут отправляться пакеты. • not-map-ip — не искать hostname для IP-адреса при отображении. • use-icmp-echo — использовать ICMP echo. • port — указать порт вместо порта по умолчанию (1 — 65535). • min-interval — минимальный интервал между пакетами. Admin@nodename# execute tracert hostname <hostname>
termination	Закрывание сессий администраторов. Подробнее читайте в разделе Управление сессиями администраторов .
ping	Выполнение ping определенного хоста. Можно задать следующие параметры: • hostname — IP-адрес или доменное имя хоста. • count — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C). • numeric — не резолвить имена. • timestamp — отображение временных меток. • interval — интервал времени, через который будет производиться отправка пакетов; указывается в секундах. • ttl — время жизни пакета. • interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • mtu — размер mtu отправляемых пакетов. • virtual-router — имя виртуального маршрутизатора. Admin@nodename# execute ping hostname <hostname> count <number>
reboot	Перезагрузка устройства.
date	Просмотр текущих даты и времени на сервере.
shutdown	Выключение устройства.
netcheck	Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры: • address — доменное имя хоста для проверки доступности по TCP или URL для HTTP. • dns-ip — IP-адрес сервера DNS. • dns-tcp — использование TCP вместо UDP для DNS-запроса. • check-cert — проверка SSL-сертификата • type — проверка доступности по: ◦ http. ◦ tcp (если порт не указан, то используется порт 80). • data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки. • timeout — максимальный таймаут ожидания ответа от веб-сервера. • user-agent — параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. Admin@nodename# execute netcheck type tcp address <host-domain-name> data on Admin@nodename# execute netcheck address <host-domain-name>
dig	Проверка записи DNS домена. • hostname — доменное имя хоста или IP-адрес для реверсивного поиска. • reverse-lookup — получение хоста по IP-адресу. • dns — указание IP-адреса DNS-сервера. • tcp — использование протокола TCP вместо UDP. Admin@nodename# execute dig hostname <host-domain-name> Admin@nodename# execute dig hostname <IP-address> reverse-lookup on
license	Команда регистрации продукта имеет следующую структуру: Admin@nodename# execute license activate <pin-code> Укажите код активации продукта вместо <pin-code>.

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

Admin@nodename> <command-name>

Documentation: 
Version: 7.1.x
Product: SIEM

Общие настройки устройства

Общие настройки устройства задаются на уровне **settings general**. Структура команды для настройки одного из разделов (<settings-module>):

Admin@nodename# set settings general <settings-module>

Доступна настройка следующих разделов:

Параметр	Описание
admin-console	Настройки интерфейса (уровень settings general admin-console): timezone: часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п. language: язык интерфейса: ru — русский. en — английский. api-session-lifetime: время ожидания сеанса администратора в секундах.
server-time	Настройка параметров установки точного времени (уровень settings general server-time): ntp-enabled: включение/отключение использования NTP-серверов: on. off. primary-ntp-server: указание основного ntp-сервера. second-ntp-server: указание запасного ntp-сервера. time: установка времени на сервере; время указывается в часовом поясе UTC в формате yyyy-mm-ddThh:mm:ss (например, 2022-02-15T12:00:00)
change-tracker	Настройка учёта изменений (уровень settings general change-tracker): enabled: включение/отключение учёта изменений. on. off. event-tracker-types: типы изменений задаются администратором. Для удаления типа изменения используется команда: Admin/system@nodename# delete settings general change-tracker event-tracker-types [type1 ...]
management-center	Настройка агента UserGate Management Center (уровень settings general management-center): enabled: включение/отключение агента UserGate Management Center. on. off. mc-address: адрес сервера UserGate Management Center. device-code: уникальный код устройства для подключения устройства к UserGate Management Center.
updates-schedule	Настройка расписания скачивания обновлений программного обеспечения и библиотек (уровень settings general updates-schedule). Для расписания обновления программного обеспечения UserGate: Admin/system@nodename# set settings general updates-schedule software schedule <schedule/disabled> Расписание скачивания обновлений библиотек может быть единым: Admin/system@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled> или может быть настроено отдельно для каждого элемента: Admin/system@nodename# set settings general updates-schedule libraries [lib-module ...] schedule <schedule/disabled> Время задаётся в crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""*/2" в поле "часы" будет означать "каждые два часа". Команда для просмотра расписания обновлений: Admin/system@nodename# show settings general updates-schedule

Настройка управления устройством

Настройка Radmin-emergency

Для активации удаленного помощника при возникновении проблемы с программным ядром устройства администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации узла. Обычно это учетная запись Admin, хотя может быть и другой. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора. Команда включения/отключения удалённого доступа к серверу для технической поддержки в таких случаях:

Adminm@emergency@LogAn# set radmin-emergency enabled <on | off>

Параметр	Описание

Параметр	Описание
interface	Название интерфейса.
ip-addr	IP-адрес и маска интерфейса.
gateway-address	IP-адрес шлюза.

Настройка операций с сервером

Следующая команда позволяет определить канал обновлений:

```
Admin@nodename# set settings device-mgmt updates-channel <stable | beta>
```

Для просмотра наличия обновлений и выбранного канал обновления используется команда:

```
Admin@nodename# show settings device-mgmt updates-channel
```

Для настройки активации лицензии и обновления ПО устройства через внешний прокси-сервер используется команда:

```
Admin@UGOS# set settings device-mgmt licensing-upstream-proxy <parameters>
```

В качестве дополнительных параметров указываются:

Параметр	Описание
enabled	Включение/выключение режима активации лицензии и обновления ПО через внешний прокси-сервер: - on — включено. - off — выключено.
ip	IP-адрес внешнего прокси-сервера.
port	Порт внешнего прокси-сервера.
auth	Аутентификация на внешнем прокси-сервере: - on — включена. - off — выключена.
name	Логин на внешнем прокси-сервере.
password	Пароль на внешнем прокси-сервере.

Для просмотра созданных настроек активации лицензии и обновления ПО устройства через внешний прокси-сервер используется команда:

```
Admin@UGOS# show settings device-mgmt licensing-upstream-proxy
```

Управление резервным копированием

Создание резервной копии устройства осуществляется на уровне **settings device-mgmt**. Для создания правила резервного копирования и выгрузки файлов на внешние серверы (FTP/SSH) используется следующая команда:

```
Admin@nodename# create settings device-mgmt settings-backup <parameters>
```

Для настройки доступны следующие параметры:

Параметр	Описание
enabled	Включение/отключение правила создания резервной копии устройства.
name	Название правила резервного копирования.
description	Описание правила резервного копирования.
type	Выбор удалённого сервера для экспорта файлов: - ssh. - ftp.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены файлы.

Параметр	Описание
schedule	Расписание экспорта файлов резервных копий. Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".

Редактирование существующего правила резервного копирования устройства производится с использованием следующей команды:

```
Admin@nodename# set settings device-mgmt settings-backup <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила резервного копирования:

```
Admin@nodename# delete settings device-mgmt settings-backup <rule-name>
```

Команда для отображения правила резервного копирования:

```
Admin@nodename# show settings device-mgmt settings-backup <rule-name>
```

Также, для команд редактирования, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Экспорт настроек

Создание и настройка правил экспорта настроек происходит на уровне **settings device-mgmt settings-export**.

Для создания правила экспорта настроек:

```
Admin@nodename# create settings device-mgmt settings-export ( <parameters> )
```

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение правила экспорта настроек сервера UserGate.
name	Название правила экспорта.
description	Описание правила экспорта.
type	Выбор удалённого сервера для экспорта настроек: - ssh. - ftp.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены настройки.
schedule	Расписание экспорта настроек. Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".

Обновление существующего правила экспорта настроек устройства производится с использованием следующей команды:

```
Admin@nodename# set settings device-mgmt settings-export <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила экспорта настроек:

```
Admin@nodename# delete settings device-mgmt settings-export <rule-name>
```

Команда для отображения правила экспорта настроек:

```
Admin@nodename# show settings device-mgmt settings-export <rule-name>
```

Также, для команд обновления, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Настройка управления доступом к консоли устройства

Version: 7.1.x
Product: SIEM
Documentation: 

Настройка данного раздела производится на уровне **settings administrators**. В разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Данный раздел позволяет настроить дополнительные параметры защиты учётных записей администраторов. Настройка производится на уровне **settings administrators general**.

Для изменения параметров используется следующая команда:

Admin@nodename# set settings administrators general

Параметры, доступные для редактирования:

Параметр	Описание
password	Изменить пароля текущего администратора.
unblock	Разблокировать администратора.
strong-password	Использовать сложный пароль: - on. - off.
num-auth-attempts	Установить максимальное количество неверных попыток аутентификации.
block-time	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд).
min-length	Определить минимальную длину пароля (максимальное значение: 100 символов).
min-uppercase	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов).
min-lowercase	Определить минимальное количество символов в нижнем регистре (максимальное значение: 100 символов).
min-digits	Определить минимальное количество цифр (максимальное значение: 100 символов).
spec-characters	Определить минимальное количество специальных символов (максимальное значение: 100 символов).
char-repetition	Указать максимальную длину блока из одного и того же символа (максимальное значение: 100 символов).

Пример редактирования параметров учетных записей:

Admin@nodename# set settings administrators general block-time 400

Для просмотра текущих параметров защиты учётных записей администраторов используется следующая команда:

Admin@nodename# show settings administrators general

strong-password : off
block-time : 400
min-length : 7
min-uppercase : 1
min-lowercase : 1
min-digits : 1
spec-characters : 1
char-repetition : 2
num-auth-attempts : 10

Настройка учётных записей администраторов

Настройка учётных записей администраторов производится на уровне **settings administrators administrators**.

Для создания учётной записи администратора используется следующая команда:

Admin@nodename# create settings administrators administrators

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации) и установить соответствующие параметры:

Параметр	Описание
local	Добавить локального администратора: - enabled: включение/отключение учётной записи администратора: - on. - off. - login: логин администратора. - display-name: отображаемое имя администратора. - description: описание учётной записи администратора. - admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. - password: пароль администратора.

Параметр	Описание
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • enabled: включение/отключение учётной записи администратора: ◦ on. ◦ off. • login: логин администратора в формате domain\user. Структура команды при указании данного параметра: • display-name: отображаемое имя администратора. • connector: название сконфигурированного ранее LDAP-коннектора. • description: описание учётной записи администратора. • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. <pre>Admin@nodename# create settings administrators administrators ldap-user admin-profile "test profile 1" connector "LDAP connector" description "Admin as domain user" login testd.local/user1 enabled on</pre>
ldap-group	Добавить группу пользователей из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • enabled: включение/отключение учётной записи администратора: ◦ on. ◦ off. • login: логин администратора • display-name: отображаемое имя администратора. • connector: название используемого LDAP-коннектора. • description: описание учётной записи администратора. • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. <pre>Admin@nodename# create settings administrators administrators ldap-group admin-profile "test profile 1" connector "LDAP connector" description "Domain admin group" login testd.local/users enabled on</pre>
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимо корректно настроенные серверы аутентификации; подробнее читайте в разделе Настройка серверов аутентификации): • enabled: включение/отключение учётной записи администратора: ◦ on. ◦ off. • login: логин администратора. • display-name: отображаемое имя администратора. • description: описание учётной записи администратора. • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. • auth-profile: выбор профиля аутентификации из созданных ранее; подробнее о профилях аутентификации читайте в разделе Настройка профилей аутентификации.

Для редактирования параметров профиля используется команда:

```
Admin@nodename# set settings administrators administrators <admin-type> <admin-login>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для отображения информации о всех учётных записях администраторов:

```
Admin@nodename# show settings administrators administrators
```

Для отображения информации об определённой учётной записи администратора:

```
Admin@nodename# show settings administrators administrators <admin-type> <admin-login>
```

Пример выполнения команды:

```
Admin@nodename# show settings administrators administrators ldap-user testd.local/user1
```

```
login      : testd.local/user1
enabled    : on
type       : ldap_user
locked     : off
admin-profile : test profile 1
```

Для удаления учётной записи используется команда:

```
Admin@nodename# delete settings administrators administrators <admin-type> <admin-login>
```

Пример команды:

```
Admin@nodename# delete settings administrators administrators ldap-user testd.local/user1
```

Настройка прав доступа профилей администраторов

Настройка прав доступа профилей администраторов производится на уровне **settings administrators profiles**.

Для создания профиля администратора используется следующая команда:

```
Admin@nodename# create settings administrators profiles
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора.
description	Описание профиля администратора.

Параметр	Описание
roles	Выбор роли для профиля администратора. Подробнее о ролях читайте в разделе Роли и ролевые разрешения пользователей .
permissions	Права доступа: • no-access: нет доступа. • read: только чтение. • write: чтение и запись.

Для редактирования профиля используется команда:

```
Admin@nodename# set settings administrators profiles <profile-name> <parameter>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

```
Admin@nodename# show settings administrators profiles
```

Для отображения информации об определённом профиле:

```
Admin@nodename# show settings administrators profiles <profile-name>
```

Чтобы удалить профиль администратора:

```
Admin@nodename# delete settings administrators profiles <profile-name>
```

Управление сессиями администраторов

С использованием следующих команд возможен просмотр активных сессий администраторов, прошедших аутентификацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators admin-sessions**).

Просмотр сессий администраторов устройства (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена аутентификация):

```
Admin@nodename# show settings administrators admin-sessions
```

Для отображения сессий доступно использование фильтра:

- **ip**: IP-адрес, с которого вошел администратор.
- **source**: где была произведена аутентификация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).
- **admin-login**: имя администратора.

```
Admin@nodename# show settings administrators admin-sessions ( node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login> )
```

Команда для закрытия сессии администратора; необходимо из предложенного списка выбрать IP-адрес, с которого была произведена аутентификация:

```
Admin@nodename# execute termination admin-sessions <IP-address/connection type>
```

Пример выполнения команд:

```
Admin@nodename# show settings administrators admin-sessions
```

```
admin-login      : Admin
source           : ssh
session_start_date : 2023-08-10T11:33:47Z
ip               : 127.0.0.1
node             : <node-name>
```

```
admin-login      : Admin
source           : web
session_start_date : 2023-08-10T11:33:10Z
ip               : 10.0.2.2
node             : <node-name>
```

```
Admin@nodename# execute termination admin-sessions 10.0.2.2/web
```

```
Admin@nodename# show settings administrators admin-sessions
```

```
admin-login      : Admin
source           : ssh
session_start_date : 2023-08-10T11:33:47Z
ip               : 127.0.0.1
node             : <node-name>
```

При закрытии сессии администраторов возможно использование фильтра (**<filter>**). Параметры фильтрации аналогичны параметрам команды **show**.

```
Admin@nodename# execute termination admin-sessions ( node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login> )
```

Настройка сертификатов

Version: 7.1.x
Product: SIEM
Documentation: 

Раздел **Сертификаты** находится на уровне **settings certificates**.

Для импорта сертификатов предназначена команда:

```
Admin@nodename# import settings certificates
```

Далее необходимо указать параметры:

Параметр	Описание
name	Название сертификата, под которым он будет отображен в списке сертификатов.
description	Описание сертификата.
certificate-data	Данные сертификата в формате PEM.
private-key	Приватный ключ сертификата в формате PEM.
passphrase	Пароль для приватного ключа, если таковой требуется.
certificate-chain	Цепочка сертификатов вышестоящих центров сертификации, которые участвовали в создании сертификата, в формате PEM.

Для экспорта доступны сертификаты, вся цепочка сертификатов:

```
Admin@nodename# export settings certificates <certificate-name>
Admin@nodename# export settings certificates <certificate-name> with-chain on
```

С использованием командной строки возможно создание сертификата и CSR:

```
Admin@nodename# create settings certificates type <certificate | csr>
```

Далее необходимо указание следующих параметров:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
country	Страна, в которой выписывается сертификат.
state	Область/штат, в котором выписывается сертификат.
locality	Город, в котором выписывается сертификат.
organization	Название организации, для которой выписывается сертификат.
common-name	Имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.
email	Email компании.

Команда для управления сертификатом:

```
Admin@nodename# set settings certificates <certificate-name>
```

Доступны параметры:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
role	Тип сертификата: web-cert-chain: цепочка сертификатов веб-консоли. web-ssl: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. none.
certificate-chain	Цепочка сертификатов в формате PEM.

Для удаления сертификата:

```
Admin@nodename# delete settings certificates <certificate-name>
```

Команды для просмотра информации об определённом сертификате или о всех сертификатах:

```
Admin@nodename# show settings certificates
Admin@nodename# show settings certificates <certificate-name>
```

Настройка серверов аутентификации

Version: 7.1.x
Product: SIEM
Documentation: 

Раздел Серверы аутентификации позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+. Настройка серверов аутентификации производится на уровне **users auth-server** и будет рассмотрена далее в соответствующих разделах.

Настройка LDAP-коннектора

Настройка LDAP-коннектора производится на уровне **users auth-server ldap**.

Для создания LDAP-коннектора используется команда:

Admin@nodename# create users auth-server ldap <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: - on — использование SSL-соединения для подключения к LDAP-серверу. - off — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username @domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем LDAP-коннекторе используется команда:

Admin@nodename# set users auth-server ldap <ldap-server-name> <parameter>

Параметры, доступные для обновления, аналогичны параметрам создания LDAP-коннектора.

Команда для отображения информации о LDAP-коннекторе:

Admin@nodename# show users auth-server ldap <ldap-server-name>

Примеры команд создания и редактирования LDAP-коннектора:

Admin@nodename# create users auth-server ldap name "New LDAP connector" ssl on address 10.10.0.10 bind-dn ug@testd.local password 12345 domains [testd.local] search-roots [dc=testd,dc=local] enabled on
Admin@nodename# show users auth-server ldap "New LDAP connector"

```
name      : New LDAP connector
enabled   : on
ssl       : on
address   : 10.10.0.10
bind-dn   : ug@testd.local
domains   : testd.local
search-roots : dc=testd,dc=local
keytab_exists : off
Admin@nodename# set users auth-server ldap "New LDAP connector" description "New LDAP connector description"
Admin@nodename# show users auth-server ldap "New LDAP connector"
```

```
name      : New LDAP connector
description : New LDAP connector description
enabled   : on
ssl       : on
address   : 10.10.0.10
bind-dn   : ug@testd.local
domains   : testd.local
search-roots : dc=testd,dc=local
keytab_exists : off
```

Для удаления LDAP-коннектора используется команда:

Admin@nodename# delete users auth-server ldap <ldap-server-name> <parameter>

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- domains.
- search-roots.

Настройка RADIUS-сервера

Настройка RADIUS-сервера производится на уровне **users auth-server radius**.

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

Admin@nodename# create users auth-server radius <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
addresses	IP-адрес и UDP-порт, на котором сервер RADIUS слушает запросы (по умолчанию порт 1812); указывается в формате <ip:port>.

Команда для обновления информации о сервере RADIUS:

```
Admin@nodename# set users auth-server radius <radius-server-name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о RADIUS-сервере:

```
Admin@nodename# show users auth-server radius <radius-server-name>
```

Примеры команд создания и редактирования RADIUS-сервера:

```
Admin@nodename# create users auth-server radius name "New RADIUS server" addresses [ 10.10.0.9:1812 ] secret 12345 enabled on
Admin@nodename# show users auth-server radius "New RADIUS server"
```

```
name      : New RADIUS server
enabled   : on
addresses :
  host    : 10.10.0.9
  port    : 1812
Admin@nodename# set users auth-server radius "New RADIUS server" description "New RADIUS server description"
Admin@nodename# show users auth-server radius "New RADIUS server"
```

```
name      : New RADIUS server
description : New RADIUS server description
enabled   : on
addresses :
  host    : 10.10.0.9
  port    : 1812
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server radius <radius-server-name> <parameter>
```

Также возможно удаления отдельных параметров RADIUS-сервера. Для удаления доступны следующие параметры:

- **addresses.**

Настройка сервера TACACS+

Настройка сервера TACACS+ производится на уровне **users auth-server tacacs**.

Для создания сервера аутентификации TACACS+ используется команда со следующей структурой:

```
Admin@nodename# create users auth-server tacacs <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя сервера TACACS+.
enabled	Включение/отключение сервера.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом TACACS+ для аутентификации.
address	IP-адрес сервера TACACS+.
port	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
single-connection	Использовать одно TCP-соединение для работы с сервером TACACS+.
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Команда для редактирования информации о сервере TACACS+:

```
Admin@nodename# set users auth-server tacacs <tacacs-server-name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о сервере TACACS+:

```
Admin@nodename# show users auth-server tacacs <tacacs-server-name>
```

Примеры команд для создания и редактирования сервера TACACS+:

```
Admin@nodename# create users auth-server tacacs address 10.10.0.11 name "New TACACS+ server" port 1812 secret 12345 enabled on
Admin@nodename# show users auth-server tacacs "New TACACS+ server"
```

```
name      : New TACACS+ server
enabled   : on
address   : 10.10.0.11
port      : 1812
single-connection : off
timeout   : 4
```

```
Admin@nodename# set users auth-server tacacs "New TACACS+ server" description "New TACACS+ server description"
Admin@nodename# show users auth-server tacacs "New TACACS+ server"
```

```
name      : New TACACS+ server
description : New TACACS+ server description
enabled   : on
address   : 10.10.0.11
port      : 1812
single-connection : off
timeout   : 4
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server tacacs <tacacs-server-name>
```

Настройка профилей аутентификации

Technology: Identification and Authentication
Version: 7.1.x
Product: LogAn
Documentation: ☒

Настройка профилей аутентификации производится на уровне **users auth-profile**.

Для создания профиля аутентификации используется следующая команда:

Admi@nodename# create users auth-profile <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
idle-time	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user.
expiration-time	Время жизни аутентифицированного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user; необходима повторная аутентификация пользователя.
max-attempts	Число неудачных попыток аутентификации до блокировки учётной записи пользователя.
lockout-time	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток аутентификации; указывается в секундах.
auth-methods	Метод аутентификации: • ldap: аутентификация с использованием LDAP-коннектора. • radius: аутентификация с использованием RADIUS-сервера. • tacacs: аутентификация с использованием сервера TACACS+.

Команда для редактирования настроек профилей аутентификации:

Admin@nodename# set users auth-profile <auth-profile-name> <parameter>

Для обновления доступен список параметров, аналогичный списку параметров команды **create**.

Пример создания и редактирования профиля аутентификации пользователя:

Admin@nodename# create users auth-profile name "New LDAP auth profile" auth-methods ldap ["New LDAP connector"]
Admin@nodename# show users auth-profile "New LDAP auth profile"

name : New LDAP auth profile
max-attempts : 5
idle-time : 900
expiration-time : 86400
lockout-time : 300
mfa : none
auth-methods :
 http-basic : off
 local-user-auth : off
 policy-accept : off

Admin@nodename# set users auth-profile "New LDAP auth profile" description "New LDAP auth profile description"
Admin@nodename# show users auth-profile "New LDAP auth profile"

name : New LDAP auth profile
description : New LDAP auth profile description
max-attempts : 5
idle-time : 900
expiration-time : 86400
lockout-time : 300
mfa : none
auth-methods :
 http-basic : off
 local-user-auth : off
 policy-accept : off
 ldap : New LDAP connector

Через интерфейс командной строки возможно удаления всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

Admin@nodename# delete users auth-profile <auth-profile-name>

Для удаления методов аутентификации, заданных в профиле, необходимо указать метод аутентификации (доступные методы авторизации перечислены в таблице выше):

Admin@nodename# delete users auth-profile <auth-profile-name> auth-methods <auth-metod>

Роли пользователей

Version: 7.1.x

Product: SIEM

Documentation: 

Роль пользователя — это набор ролевых разрешений. Ролевое разрешение — это возможность администратору совершать определенные действия, например, добавлять или удалять вложение из созданного инцидента, создавать правило срабатывания, создать или закрыть инцидент и т.д. Роли назначаются профилям администраторов, которые присваиваются администраторам.

Создание и настройка ролей пользователей производится на уровне **users roles**.

Для создания ролей и назначения ролевых разрешений используется команда:

```
Admin@nodename# create users roles <role-name> description <role-description> permissions [ <permissions> ]
```

Подробнее о ролях и списке имеющихся ролевых разрешений читайте в разделе [Роли и ролевые разрешения пользователей](#) Руководства администратора SIEM.

Для редактирования созданных ранее ролей и ролевых ограничений используется команда:

```
Admin@nodename# set users roles <role-name> description <role-description> permissions [ <permissions> ]
```

Для удаления ранее созданных ролей или отдельных ролевых разрешений в ранее созданных ролях используется команда:

```
Admin@nodename# delete users roles <role-name> permissions [ <permissions> ]
```

Каталоги пользователей

Version: 7.1.x
Product: SIEM
Documentation: 

Для работы с каталогами пользователей необходим корректно настроенный LDAP-коннектор, который позволяет получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Пользователи и группы могут быть использованы при настройке политик, применяемых к управляемым устройствам.

Создание и настройка каталога пользователей производится на уровне **users catalogs ldap**.

Для создания каталога используется команда:

```
Admin@nodename# create users catalogs ldap <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: • on — использование SSL-соединения для подключения к LDAP-серверу. • off — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username@domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем каталоге используется команда:

```
Admin@nodename# set users catalogs ldap <ldap-server-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам создания каталога.

Команда для отображения информации о каталоге пользователей:

```
Admin@nodename# show users catalogs ldap <ldap-server-name>
```

Для удаления каталога используется команда:

```
Admin@nodename# delete users catalogs ldap <ldap-server-name> <parameter>
```

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains**.
- **search-roots**.

Зоны

Documentation: 
Product: SIEM
Version: 7.2.x

Данный раздел находится на уровне **network zone**. Команда для создания новой зоны:

Admin@nodename# create network zone

Далее необходимо указать параметры зоны:

Параметр	Описание
name	Название зоны.
description	Описание зоны.
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • enabled: включение/отключение защиты. ◦ on. ◦ off. • aggregate: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • enabled: включение/отключение защиты. ◦ on. ◦ off. • aggregate: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • enabled: включение/отключение защиты. ◦ on. ◦ off. • aggregate: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Параметры контроля доступа зоны: • "Any ICMP": разрешение использования команды ping адреса UserGate. • SNMP: доступ к UserGate по протоколу SNMP (UDP 161). • rpc: XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • VRRP: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • "CLI over SSH": доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • Cluster: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • "Admin Console": доступ к веб-консоли управления (TCP 8001).
service-addresses	Указание разрешённых IP-адресов для сервисов: • service: выбор сервисов (список соответствует enabled-services). • allowed-addresses: разрешённые IP-адреса: ◦ geoip — код GeoIP. ◦ ip-list — заранее созданный в библиотеке элементов список IP-адресов.

Параметр	Описание
antispoof-enable	Включение/отключение защиты от IP-спуфинга: • on. • off.
antispoof-negate	Возможные значения: • on. • off. При antispoof-negate on адреса источников, указанные в значении ip-spoofing-networks , будут являться адресами, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными IP-адресами источников.
sessions-limit-enabled	Включение ограничения количества одновременных сессий с одного IP-адреса: • on. • off.
sessions-limit-exclusions	Добавление списка IP-адресов, для которых ограничение на количество одновременных сессий не будет действовать.
sessions-limit-threshold	Максимально возможное количество одновременных сессий с одного IP-адреса.
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Пример создания новой зоны:

```
Admin@nodename# create network zone name Test_zone description "Test_zone description" antispoof-enable on enabled-services [ "Any ICMP" DNS ] dos-protection-icmp enabled on
```

Для редактирования параметров зоны:

```
Admin@nodename# set network zone <zone-name>
```

Пример редактирования параметров зоны:

```
Admin@nodename# set network zone Test_zone dos-protection-syn enabled on
```

Команда удаления зоны или её параметров:

```
Admin@nodename# delete network zone <zone-name>
```

Параметры, доступные для удаления:

Параметр	Описание
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Установленные ранее параметры контроля доступа в данной зоне
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Команда для просмотра настроек зоны:

```
Admin@nodename# show network zone <zone-name>
```

Documentation: 
Product: SIEM
Version: 7.1.x

Настройка интерфейсов производится на уровне **network interface**:

Настройка adapter

Сетевые адаптеры настраиваются на уровне **network interface adapter**.

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера используется команда:

Admin@nodename# set network interface adapter <adapter_name>

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: - on. - off.
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: - l3: интерфейс, работающий в режиме Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). - mirror: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: - dhcp: получение динамического IP-адреса по DHCP. - manual: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: - bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. - proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@nodename# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.

Команда удаления адаптера или его параметров:

Admin@nodename# delete network interface adapter <adapter-name>

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Команда для отображения информации о всех сетевых адаптерах:

Admin@nodename# show network interface adapter

Для отображения информации об адаптере:

Admin@nodename# show network interface adapter <adapter-name>

Настройка VLAN

Интерфейсы VLAN настраиваются на уровне **network interface vlan**.

Команда для добавления нового VLAN-интерфейса:

```
Admin@nodename# create network interface vlan
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: - on. - off.
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: - I3: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). - mirror: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: - dhcp: получение динамического IP-адреса по DHCP. - manual: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
tag	Tag VLAN. Допускается создание до 4094 интерфейсов.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: - bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. - proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@nodename# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: - enabled: включение/отключения релея: - on. - off. - utm-address: IP-адрес интерфейса UserGate, на который добавляется функция релея. - server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего VLAN:

```
Admin@nodename# set network interface vlan <vlan-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания VLAN, кроме **tag, node-name, interface** (изменение значений этих параметров недоступно).

Команда удаления VLAN-интерфейса или его параметров:

```
Admin@nodename# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления:

Параметр	Описание

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех интерфейсах VLAN:

Admin@nodename# show network interface vlan

или об определённом интерфейсе:

Admin@nodename# show network interface vlan <vlan-name>

Настройка bond-интерфейса

Настройка бонд-интерфейса производится на уровне **network interface bond**.

Команда для создания бонд-интерфейса:

Admin@nodename# create network interface bond

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение интерфейса: - on. - off.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1).
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Узел кластера, на котором будет создан бонд-интерфейс.
zone	Зона, которой будет принадлежать бонд.
link-info	Настройка параметров сетевого интерфейса: bc_forwarding: управление пересылкой пакетов directed broadcast, проходящих на указанный интерфейс. proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@nodename# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.

Параметр	Описание
bonding	Дополнительные параметры бонд-интерфейса: mode — режим работы бонда: round-robin: режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости). active-backup: режим Active backup (только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Данная политика применяется для обеспечения отказоустойчивости). xor: режим XOR (передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и обеспечения отказоустойчивости). broadcast: режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости). 802.3ad: режим IEEE 802.3ad (режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику). transmit: режим Adaptive transmit load balancing (исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты). load: режим Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. mii-monitoring: периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. down-delay: время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. up-delay: время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. lacp-rate: интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: slow: запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. fast: запрос партнера на передачу LACPDU-пакетов каждую секунду. failover-mac: определение способа назначения MAC-адресов на объединенные интерфейсы в режиме Active backup при переключении интерфейсов. Возможные значения: disabled: устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. active: MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. follow: MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном. xmit-hash: определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: I2: использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. I2-3: использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. I3-4: используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут прийти до получателя не в том порядке, так как отправляются через разные интерфейсы. interface: интерфейсы, которые будут объединены в бонд.
iface-mode	Режим назначения IP-адреса: dhcp: получение динамического IP-адреса по DHCP. manual: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
iface-type	Тип создаваемого интерфейса: I3 — Layer 3 интерфейс. mirror — интерфейс зеркалирования трафика.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размер MTU.

```
Обновление существующего бонд-интерфейса:

Admin@nodename# set network interface bond <bond-name>

Параметры, доступные для обновления, аналогичны параметрам создания бонд-интерфейс, кроме interface-name, node-name (изменение значений этих параметров недоступно).

Команда удаления бонд-интерфейса или его параметров:

Admin@nodename# delete network interface bond <bond-name>

Параметры, доступные для удаления:
```

Параметр	Описание
----------	----------

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.
bonding interface	Интерфейсы, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

```
Admin@nodename# show network interface bond
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface bond <bond-name>
```

Шлюзы

Documentation: 
Product: SIEM
Version: 7.1.x, 7.3.x

Данный раздел находится на уровне **network gateway**.

Для добавления нового шлюза используется команда:

Admin@nodename# create network gateway

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение шлюза: - on. - off.
name	Название шлюза.
description	Описание шлюза.
interface	Интерфейс, использующийся для выхода в Интернет: - Выбор конкретного порта (port0, port1, port2 итд.); auto — после выбора этого параметра порт определится автоматически. Данная опция доступна для узлов, прошедших инициализацию. Для узлов, не прошедших инициализацию, опция доступна начиная с релиза ПО 7.3.0.
ip	IP-адрес шлюза.
node-name	Выбор узла кластера, для которого настраивается шлюз.
weight	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз).
balancing	Режим балансировки - весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами: - on. - off.
default	Использование данного шлюза в качестве шлюза по умолчанию: - on. - off.

Обновление параметров шлюза:

Admin@nodename# set network gateway <gateway-name>

Список параметров, доступных для изменения, аналогичен списку, доступному при создании шлюза.

Команда для удаления шлюза:

Admin@nodename# delete network gateway <gateway-name>

Чтобы отобразить информацию о всех шлюзах:

Admin@nodename# show network gateway

или об определённом шлюзе:

Admin@nodename# show network gateway <gateway-name>

Настройка маршрутизации

Documentation: 
Product: SIEM
Version: 7.1.x
Technology: Routing

В данном разделе описана настройка маршрутизации с использованием интерфейса командной строки. Настройка производится на уровне **network routes**.

Для добавления нового статического маршрута используется команда:

```
Admin@nodename# create network routes <parameters>
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статического маршрута: • on. • off.
name	Имя маршрута.
description	Описание маршрута.
node-name	Выбор узла кластера для настройки маршрутизации.
type	Тип маршрута: • unicast — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз. • unreachable — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 1). • prohibit — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 13). • blackhole — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата.
destination-ip	IP-адрес подсети назначения; указывается в формате <ip/mask>.
gateway	IP-адрес шлюза, через который будет доступна указанная подсеть; этот IP-адрес должен быть доступен с устройства.
interface	Интерфейс, через который будет добавлен маршрут.
metric	Метрика маршрута. Если маршрутов в данную сеть несколько: чем меньше метрика, тем более приоритетен маршрут.

Пример добавления статического маршрута:

```
Admin@nodename# create network routes name test_route description "Test static route" destination-ip 192.168.200.0/2
4 gateway 192.168.100.100 interface port1 type unicast metric 1 enabled on
Admin@nodename#

Admin@nodename# show network routes test_route
```

```
name      : test_route
description : Test static route
enabled   : on
node-name  : testnode1
interface  : port1
type       : unicast
destination-ip : 192.168.200.0/24
gateway    : 192.168.100.100
metric     : 1
```

Чтобы изменить параметры созданного ранее статического маршрута, используйте команду:

```
Admin@nodename# set network routes <route-name>
```

Параметры, доступные для изменения, представлены в таблице выше.

Используйте следующую команду для удаления статического маршрута:

```
Admin@nodename# delete network routes <route-name>
```

Пример удаления статического маршрута:

```
Admin@nodename# delete network routes test_route
```

Для отображения статических маршрутов:

```
Admin@nodename# show network routes
```

DNS-настройки

Documentation: 

Product: SIEM

Version: 7.1.x

Настройка системных серверов DNS производится на уровне **network dns system-dns-servers**.

Для добавления новых DNS-серверов или обновления существующего списка используются следующие команды:

```
Admin@nodename# set network dns system-dns-servers ip [ <ip> <ip> ... ]
```

Для удаления всего списка адресов серверов DNS:

```
Admin@nodename# delete network dns system-dns-servers
```

Для удаления определённых серверов:

```
Admin@nodename# delete network dns system-dns-servers ip [ <ip> <ip> ... ]
```

Для отображения списка системных DNS-серверов используется команда:

```
Admin@nodename# show network dns
```


Настройка библиотек (Описание)

Documentation: 
Product: SIEM
Version: 7.1.x, 7.2.x

Настройка IP-адресов

Данный раздел находится на уровне **libraries ip-list**.
Для создания группы IP-адресов используется следующая команда:
Admin@nodename# create libraries ip-list <parameters>
Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: very-low — очень низкий уровень угрозы. low — низкий уровень угрозы. medium — средний уровень угрозы. high — высокий уровень угрозы. very-high — высокий уровень угрозы.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
lists	Выбор существующих IP-листов для добавления в создаваемый лист.
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: on; off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):
Admin@nodename# set libraries ip-list <ip-list-name> <parameters>
Чтобы добавить в список новые адреса:
Admin@nodename# set libraries ip-list <ip-list-name> [<ip1> <ip2> ...]
Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:
Admin@nodename# delete libraries ip-list <ip-list-name>
Admin@nodename# delete libraries ip-list <ip-list-name> ips [<ip1> <ip2>...]
Команда отображения информации о всех имеющихся списках:
Admin@nodename# show libraries ip-list
Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:
Admin@nodename# show libraries ip-list <ip-list-name>
Также доступен просмотр содержимого списка IP-адресов:
Admin@nodename# show libraries ip-list <ip-list-name> items

Настройка useragent браузеров

Данный раздел находится на уровне **libraries useragents**. (Доступно начиная с релиза ПО 7.2.0).
Для создания списка useragent браузеров используется следующая команда:
Admin@nodename# create libraries useragents <parameters>
Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка.
description	Описание списка.

Параметр	Описание
patterns	Строка описания useragent. Искерпывающий список строк aseragent представлен на этом ресурсе: http://www.useragentstring.com/pages/useragentstring.php .
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: • on; • off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

Admin@nodename# set libraries useragents <list-name> <parameters>

Следующие команды используются для удаления всего списка или отдельных useragent из списка по их паттернам:

Admin@nodename# delete libraries useragents <list-name>
Admin@nodename# delete libraries useragents <list-name> <patterns>

Команда отображения информации о всех имеющихся списках:

Admin@nodename# show libraries useragents

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка:

Admin@nodename# show libraries useragents <list-name>

Также доступен просмотр содержимого конкретного списка useragents:

Admin@nodename# show libraries useragents <list-name> patterns

Настройка типов контента

Данный раздел находится на уровне **libraries content-types**. (Доступно начиная с релиза ПО 7.2.0).

Для создания списка типов контента используется следующая команда:

Admin@nodename# create libraries content-types <parameters>

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка.
description	Описание списка.
mime	Данные в формате MIME. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml .
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: • on; • off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

Admin@nodename# set libraries content-types <list-name> <parameters>

Следующие команды используются для удаления всего списка или отдельных типов контента, содержащихся в нём:

Admin@nodename# delete libraries content-types <list-name>
Admin@nodename# delete libraries content-types <list-name> mime [<mime1> <mime2>...]

Команда отображения информации о всех имеющихся списках:

Admin@nodename# show libraries content-types

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка:

Admin@nodename# show libraries content-types <list-name>

Также доступен просмотр содержимого списка типов контента:

Настройка списков URL

Данный раздел находится на уровне **libraries url-list**. (Доступно начиная с релиза ПО 7.2.0).

Для создания списка URL-адресов используется следующая команда:

```
Admin@nodename# create libraries url-list <parameters>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка.
description	Описание списка.
case-sensitivity	Чувствительность к регистру в написании адреса URL: sensitive — чувствительно к регистру букв в адресе. insensitive — нечувствительно к регистру букв в адресе. domain — список адресов доменов.
urls	URL, которые необходимо добавить в список.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: on; off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin@nodename# set libraries url-list <list-name> <parameters>
```

Следующие команды используются для удаления всего списка или отдельных URL-адресов, содержащихся в нём:

```
Admin@nodename# delete libraries url-list <list-name>
Admin@nodename# delete libraries url-list <list-name> urls [ <url1> <url2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries url-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка:

```
Admin@nodename# show libraries url-list <list-name>
```

Также доступен просмотр содержимого списка URL-адресов:

```
Admin@nodename# show libraries url-list <list-name> urls
```

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

```
Admin@nodename#& create libraries email-list <parameter>
```

Далее указываются параметры:

Параметр	Описание
name	Название группы почтовых адресов.
description	Описание группы почтовых адресов.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".

Параметр	Описание
emails	Почтовые адреса, которые необходимо добавить в данную группу.

Команда, предназначенная для редактирования информации о группе почтовых адресов:

```
Admin@nodename# set libraries email-list <email-list-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Для удаления группы или почтовых адресов из неё используются следующие команды:

```
Admin@nodename# delete libraries email-list <email-list-name>
Admin@nodename# delete libraries email-list <email-list-name> emails [ <email> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах, об определённых группах или для просмотра почтовых адресов, входящих в группу:

```
Admin@nodename# show libraries email-list
Admin@nodename# show libraries email-list <email-list-name>
Admin@nodename# show libraries email-list <email-list-name> emails
```

Настройка номеров телефонов

Настройка раздела **Номера телефонов** производится на уровне **libraries phone-list**.

Для создания группы телефонных номеров:

```
Admin@nodename# create libraries phone-list <parameter>
```

Далее необходимо указать следующие данные:

Параметр	Описание
name	Название группы телефонных номеров.
description	Описание группы телефонных номеров.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для редактирования информации о группе телефонных номеров используется команда:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
Admin@nodename# delete libraries phone-list <phone-list-name> phones [ <phone> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах:

```
Admin@nodename# show libraries phone-list
```

или об определённых группах телефонных номеров:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

Для просмотра номеров, содержащихся в группе, используется команда:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Настройка команд

Данный раздел позволяет создавать группы команд, предназначенных для отправки на коннекторы.

Для создания списка команд используется команда:

```
Admin@nodename# create libraries commands-list name <command-list-name> type <local | updatable> commands new <command-string>
```

Для редактирования созданного ранее списка команд используется команда:

```
Admin@nodename# set libraries commands-list <command-list-name> commands <command-string>
```

Для просмотра созданного ранее списка команд используется команда:

```
Admin@nodename# show libraries commands-list <command-list-name>
```

Для удаления созданного ранее списка команд или отдельных команд из списка используется команда:

```
Admin@nodename# delete libraries commands-list <command-list-name>
```

```
Admin@nodename# delete libraries commands-list <command-list-name> commands <command-string>
```

Настройка профилей оповещений

Профили оповещений SMTP (по email) и SMPP (по SMS) настраиваются на уровне **libraries notification-profiles**.

Для добавления нового профиля оповещения SMTP:

```
Admin@nodename# create libraries notification-profiles smtp <parameter>
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
port	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 465. Уточните данное значение у администратора почтового сервера.
connection-security	Варианты безопасности отправки почты; возможны варианты: • none. • starttls. • ssl.
authentication	Включение/отключение авторизации при подключении к серверу SMTP: • on. • off.
login	Имя учётной записи для подключения к SMTP-серверу.
password	Пароль учётной записи для подключения к SMTP-серверу.

Для создания профиля оповещения по SMS (SMPP):

Admin@nodename# create libraries notification-profiles smpp <parameter>

Далее необходимо указать значения следующих параметров:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS.
port	Порт TCP, который используется для подключения к серверу SMPP. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550.
ssl	Включение/отключение шифрования SSL: • on. • off.
login	Имя учётной записи для подключения к SMPP-серверу.
password	Пароль учётной записи для подключения к SMPP-серверу.
phone-translation-rules	Правила трансляции телефонных номеров. Правила используются для соответствия требованиям провайдера. Например, если необходимо заменить все номера, начинающиеся на +7, на 8: Admin@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [+7 8]
source-ton	Тип номера (Type of Number) для источника сообщения: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
dest-ton	Тип номера (Type of Number) для адресата: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).

Параметр	Описание
source-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника: 0 — Unknown. 1 — ISDN/telephone numbering plan (E.163/E.164). 3 — Data numbering plan (X.121). 4 — Telex numbering plan (F.69). 6 — Land Mobile (E.212). 8 — National numbering plan. 9 — Private numbering plan. 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). 13 — Internet (IP). 18 — WAP Client Id (to be defined by WAP Forum).
dest-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата: 0 — Unknown. 1 — ISDN/telephone numbering plan (E.163/E.164). 3 — Data numbering plan (X.121). 4 — Telex numbering plan (F.69). 6 — Land Mobile (E.212). 8 — National numbering plan. 9 — Private numbering plan. 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). 13 — Internet (IP). 18 — WAP Client Id (to be defined by WAP Forum).

Для редактирования профиля оповещения используется команда:

```
Admin@nodename# set libraries notification-profiles <smtp | smpp> <profile-name> <parameter>
```

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

```
Admin@nodename# delete libraries notification-profiles <smtp | smpp> <profile-name>
```

Также для профилей оповещений SMPP доступно удаления правил трансляции номеров:

```
Admin@nodename# delete libraries notification-profiles smpp <profile-name> phone-translation-rules [ phone1|phone2 ]
```

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

```
Admin@nodename# show libraries notification-profiles
```

о всех профилях одного типа:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp>
```

об определённом профиле оповещения:

```
Admin@nodename#show libraries notification-profiles <smtp | smpp> <profile-name>
```

Настройка категорий срабатывания

Элемент библиотеки **Категории срабатываний** позволяет создать категории, по которым можно группировать определенные срабатывания правил аналитики, применяемые к событиям. Более подробно о правилах аналитики смотрите в разделе [Аналитика](#). По умолчанию создаются категории:

- Availability** — правила аналитики, определяющие инциденты, приводящие к ухудшению доступности информационных систем.
- Performance** — правила аналитики, определяющие инциденты, приводящие к ухудшению производительности информационных систем.
- Security** — правила аналитики, определяющие инциденты, приводящие к ухудшению безопасности информационных систем.

Для создания категорий срабатывания используется команда:

```
Admin@nodename# create libraries alert-categories name <category-name> key <category-key>
```

Для редактирования категорий срабатывания используется команда:

```
Admin@nodename# set libraries alert-categories name <category-name> key <category-key>
```

Для просмотра созданных ранее категорий срабатывания используется команда:

```
Admin@nodename# show libraries alert-categories name <category-name>
```

Для удаления созданных ранее категорий срабатывания используется команда:

```
Admin@nodename# delete libraries alert-categories name <category-name>
```

Настройка внешних сервисов обогащений

В данном элементе библиотеки представлены ресурсы, с помощью которых происходит дополнительный сбор информации об угрозах. С данных источников приходят фиды — структурированные проанализированные данные об IP-адресах и доменах, с которых происходит распространение вредоносных файлов, их сэмплы и хэши; списки фишинговых сайтов, почтовые адреса отправителей фишинговых писем; адреса, с которых происходит сканирование сетей с целью обнаружения уязвимостей; IP-адреса, с которых проводятся атаки типа брутфорс; сигнатуры для обнаружения вредоносного программного обеспечения. Подробнее о доступных сервисах читайте в разделе [Внешние сервисы обогащений](#). Руководства администратора SIEM.

Чтобы использовать сервисы обогащения их необходимо включить. Для использования некоторых сервисов обогащения необходимо прохождение регистрации и предоставление ключа доступа.

Для редактирования сервисов обогащений используется команда:

```
Admin@nodename# set libraries enrichment-services <service-name>
```

Для просмотра сервисов обогащений используется команда:

```
Admin@nodename# show libraries enrichment-services <service-name>
```

Настройка syslog-фильтров

Создание и настройка syslog-фильтров производятся на уровне **libraries syslog-filters**.

Команда для создания syslog-фильтра:

Admin@nodename# create libraries syslog-filters <parameter>

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название фильтра.
description	Описание фильтра.
login-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
login-event	Строка для поиска события входа пользователя в syslog-сообщении.
login-username	Строка для поиска имени пользователя в syslog-сообщении.
logout-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
logout-event	Строка для поиска события выхода пользователя в syslog-сообщении.
logout-username	Строка для поиска имени пользователя в syslog-сообщении.

Следующая команда предназначена для редактирования информации о syslog-фильтре:

Admin@nodename# set libraries syslog-filters <filter-name> <parameter>

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании фильтра.

Чтобы отобразить информацию о syslog-фильтрах:

Admin@nodename# show libraries syslog-filters <filter-name>

Пользователь может удалить syslog-фильтр, используя следующую команду:

Admin@nodename# delete libraries syslog-filters <filter-name>

Настройка приложений syslog

Создание и настройка приложений syslog производятся на уровне **libraries syslog-application**.

Команда для создания приложений syslog:

Admin@nodename# create libraries syslog-application <parameter>

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название приложения.
description	Описание приложения.
app-name	Название приложения, отображаемое в журналах.

Настройка UserID агента

Documentation: ☒
Product: SIEM
Version: 7.1.x

UserID агент предназначен для осуществления прозрачной аутентификации на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Microsoft Active Directory (посредством протокола WMI) и Syslog (посредством стандартизированного протокола syslog [RFC 3164](#), [RFC 5424](#), [RFC 6587](#)). Подробнее о схеме работы UserID агента читайте в разделе [Пользователи и устройства](#). Руководства администратора LogAn.

Настройка UserID в CLI производится на уровне **users userid-agent**.

Настройка параметров UserID агента

Общие параметры UserID агента настраиваются с помощью команды:

Admin@nodename# set users userid-agent configurate-agent <parameters>

При настройке необходимо установить следующие параметры:

Параметр	Описание
polling-interval	Период опроса серверов Active Directory. Значение по умолчанию - 120 секунд.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).
syslog-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников.
ignore-network-list	Списки IP-адресов, события от которых будут проигнорированы агентом UserID. Запись об игнорировании источника появится в журнале Агент UserID . Список может быть создан в разделе библиотек (IP-адреса). Данная настройка является глобальной и относится ко всем источникам.
ignore-user-list	Имена пользователей, события от которых будут проигнорированы агентом UserID. Поиск производится по Common Name (CN) пользователя AD. Данная настройка является глобальной и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID. Важно! При задании имени допустимо использовать символ астериск (*), но только в конце строки.

Настройка источника событий

Microsoft Active Directory

Для добавления Microsoft Active Directory в качестве источника событий предназначена следующая команда:

Admin@nodename# create users userid-agent active-directory <parameters>

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника (опционально).
address	Адрес Microsoft Active Directory.
protocol	Протокол доступа к AD (WMI).
login	Имя пользователя для подключения к AD.
password	Пароль пользователя для подключения к AD.
sharing-profile	Профиль редистрибуции, который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел Профиль редистрибуции .

Syslog

Для добавления отправителя syslog в качестве источника событий предназначена следующая команда:

Admin@nodename# create users userid-agent syslog-sender <parameters>

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника.
address	Адрес хоста, с которого UserGate будет получать события по протоколу syslog.
default-domain	Название домена, который используется для поиска найденных в журналах syslog пользователей.
timezone	Часовой пояс, установленный на источнике.

Параметр	Описание
sharing-profile	Профиль редистрибуции который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел Профиль редистрибуции .
filters	Фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе Библиотеки → Syslog фильтры UserID агента . Подробнее читайте в разделе Syslog фильтры UserID агента .
users-catalogs	Предназначена для выбора LDAP коннектора, который используется для поиска информации о пользователях, найденных в журналах агентом UserID. Можно выбрать настроенный ранее каталог или добавить новый.

Настройка профиля редистрибуции UserID

Documentation: 
Product: SIEM
Version: 7.1.x

Профили редистрибуции UserID предназначены для определения круга устройств UserGate, на которые отправляется информация о найденных агентом UserID пользователях.

Настройка профилей редистрибуции UserID в CLI производится на уровне **users sharing-profile**.

Команда для настройки:

Admin@nodename# create users sharing-profile <parameters>

При настройке необходимо установить следующие параметры:

Параметр	Описание
name	Название профиля.
description	Описание профиля (опционально).
sensors	Выбор сенсоров UserGate, на которые будет отправлена информация о пользователях.

Documentation: 
Product: SIEM
Version: 7.1.x

Для сбора информации с различных устройств и последующего ее анализа LogAn использует сенсоры. Сенсор — это совместимое с LogAn устройство, которое может передавать определенные данные на сервер LogAn. Сенсорами могут выступать устройства UserGate NGFW, конечные устройства UserGate Client, а также любые другие сетевые устройства, способные передавать данные по протоколу SNMP.

Сенсоры UserGate

Сенсор UserGate подключает одно устройство типа межсетевого экрана UserGate к LogAn. Для подключения сенсора UserGate необходимо выполнить следующие шаги:

1. На **NGFW** разрешить сервисы **Log Analyzer** и **SNMP** в настройках требуемой зоны:

Admin@ngfw-nodename# set network zone <zone-name> enabled-services [SNMP "Log Analyzer"]

2. На **NGFW** получить токен устройства:

Admin@ngfw-nodename# show settings general log-analyzer

state : ready
logan-server : 127.0.0.1
logan-version : 7.1.0.
device-version : 7.1.0.
device-code : 9R4FCVET

3. На LogAn разрешить сервис **Log Analyzer** в свойствах требуемой зоны:

Admin@nodename# set network zone <zone-name> enabled-services ["Log Analyzer"]

4. Создать сенсор UserGate.

Для создания сенсора UserGate используется команда:

Admin@ndeformaledo# create sensors ug-sensors <parameters>

Необходимо добавить следующие параметры:

Параметр	Описание
enabled	Включает или выключает данный сенсор UserGate.
name	Название сенсора UserGate.
description	Опциональное описание сенсора UserGate.
address	IP-адрес узла UserGate, для которого создается данный сенсор.
logan-address	IP-адрес сервера LogAn, который будет использоваться на узле UserGate, в качестве назначения для отсылки журналов. Для выбора отображаются только те адреса, на интерфейсах зон которых разрешен сервис Log Analyzer.
device-code	Токен, полученный на узле UserGate.

После создания сенсора, узел UserGate начинает отсылать данные на LogAn.

Для просмотра сенсоров UserGate используется команда:

Admin@nodename# show sensors ug-sensors

Сенсоры SNMP

С помощью сенсора SNMP администратор может подключить SNMP-совместимое сетевое устройство к серверу LogAn для сбора и анализа его метрик. LogAn может отображать любые счетчики, полученные по SNMP с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB (Management Information Base) на управляемое устройство.

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

1. Загрузить базу того устройства, которое требуется добавить для мониторинга.

2. Создать сенсор SNMP:

Admin@nodename# create sensors snmp-sensors <parameters>

Далее указать следующие параметры.:

Наименование	Описание
enabled	Включает или выключает данный сенсор SNMP.
name	Название сенсора SNMP.
description	Опциональное описание сенсора SNMP.
ip	IP-адрес сенсора SNMP.
port	Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161.
version	Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2 (2) и SNMP v3 (3).
community	SNMP community - строка для идентификации сервера LogAn и сетевого устройства для версии SNMP v2. Используйте только латинские буквы и цифры.

Наименование	Описание
interval	Интервал в секундах, через который сервер LogAp будет инициировать получение данных с сетевого устройства.
username	Только для SNMP v3. Имя пользователя для аутентификации сетевом устройстве.
auth-type	Выбор режима аутентификации. Возможны варианты: - Без аутентификации, без шифрования (none). - С аутентификацией, без шифрования (no-encrypt). - С аутентификацией, с шифрованием (encrypt).
auth-alg	Алгоритм, используемый для аутентификации: - md5; - sha; - sha224; - sha256; - sha284; - sha512.
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	Пароль, используемый для шифрования.
counters	Укажите здесь все требуемые данные, которые LogAp будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство. Укажите в скобках [] SNMP OID счетчика.

Для просмотра сенсоров SNMP используется команда:

```
Admin@nodename# show sensors snmp-sensors
```

Сенсоры WMI

С помощью сенсора WMI администратор может подключить WMI-совместимое сетевое устройство (компьютер под управлением ОС Windows) к LogAp для сбора и анализа его метрик.

Для создания сенсора WMI используется команда:

```
Admin@nodename# create sensors wmi-sensors <parameters>
```

Далее указать следующие параметры::

Наименование	Описание
enabled	Включает или выключает данный сенсор.
name	Название сенсора.
description	Оptionальное описание сенсора.
ip	IP-адрес сенсора.
login	Имя пользователя для подключения к устройству.
password	Пароль пользователя для подключения к устройству.
namespace	Пространство имен идентификаторов.
polling-interval	Интервал опроса в секундах.
counters	Указать данные, которые LogAp будет мониторить на сетевом устройстве: name — название счетчика. type — тип счетчика (windows-event-logs). filter-query — WQL запрос (например, Logfile="Security").

Для просмотра сенсоров WMI используется команда:

```
Admin@nodename# show sensors wmi-sensors
```

Конечные устройства

Конечное устройство с установленным программным обеспечением UserGate Client будет отображено при выборе на UGMC данного устройства LogAp в качестве сервера для передачи информации о событиях, при этом LogAp должен быть предварительно зарегистрирован на UGMC (подробнее читайте в разделе [Управление устройствами LogAp](#)).

Для просмотра данных конечных устройств используется команда:

```
Admin@nodename# show sensors endpoint-devices
```

Коннекторы

Коннекторы используются для возможности подключения устройства SIEM к различным средствам защиты с целью сбора информации.

Для добавления коннектора предназначена команда:

Admin@nodename# create sensors connectors <parameters>

Необходимо указать следующие данные:

Параметр	Описание
name	Название коннектора.
description	Описание коннектора (опционально).
server-type	Выбор типа сервера: - SSH. - HTTP. - HTTPS (в текущей версии реализован только для интеграции с ГосСОПКА).
address-format	Тип: - ip. - fqdn.
ip	IP-адрес сервера; указывается в случае выбора адреса сервера типа IP.
port	Порт сервера; указывается в случае выбора адреса сервера типа IP.
fqdn	FQDN сервера; указывается в случае выбора адреса сервера типа FQDN.
url-path	Используется при управлении устройством по API.
login	Логин пользователя для авторизации на коннекторе.
password	Пароль учётной записи пользователя, необходимый для авторизации на коннекторе.
connamd-group	Указание группы команд доступно только для SSH-сервера, подробнее читайте в разделе Команды .
headers	Указание заголовков доступно только для серверов HTTP и HTTPS.

Для редактирования созданного ранее коннектора используется команда:

Admin@nodename# create sensors connectors <connector-name> <parameters>

Для просмотра параметров созданных ранее коннекторов используется команда:

Admin@nodename# show sensors connectors <connector-name>

Для удаления созданных ранее коннекторов используется команда:

Admin@nodename# delete sensors connectors <connector-name>

Настройка параметров мониторинга устройства

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	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 (length), 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 text . Engine ID может быть сформирован в формате: ip4 — IPv4. ipv6 — IPv6. mac — MAC-адрес. text — Текст. octets — Октеты.

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	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. 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.
version	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
query	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
trap	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
trap-host	IP-адрес сервера для трапов. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
trap-port	Порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
security-profile	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP .
events	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
----------	----------

Параметр	Описание
name	Название профиля безопасности SNMP
description	Описание профиля безопасности SNMP
username	Имя пользователя для аутентификации SNMP-менеджера.
auth-type	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • none — без аутентификации, без шифрования. • no-encrypt — с аутентификацией, без шифрования. • encrypt — с аутентификацией, с шифрованием. Наиболее безопасным считается режим работы authPriv.
auth-alg	Алгоритм, используемый для аутентификации. Возможно использовать: • sha; • md5; • sha224; • sha256; • sha384; • sha512.
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	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
enabled	Включает/отключает данное правило.
name	Название правила.
description	Описание правила.
notification-profile	Созданный ранее профиль оповещения.
sender	От кого будет приходить оповещение.
subject	Тема оповещения.
timeout	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.
events	События, для которых необходимо получать оповещения.
phones	Для SMPP-профиля. Группы номеров телефонов, куда отправлять SMS-оповещения.
emails	Для SMTP-профиля. Группы адресов email, на которые будут отправляться почтовые оповещения.

Настройка инцидентов (описание)

Documentation: 
Product: SIEM
Version: 7.1.x

Раздел **Инциденты** предоставляет функциональность встроенной в UserGate SIEM системы IRP — платформы управления процессами реагирования на инциденты информационной безопасности. Инцидентом считается событие или набор событий информационной безопасности, которые подлежат расследованию. UserGate SIEM позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании.

Подробнее о функциональности системы IRP читайте в разделе [Инциденты](#) в Руководстве пользователя SIEM.

Настройки инцидентов в интерфейсе CLI производятся на уровне **incident**.

Для создания собственной схемы расследования инцидентов необходимо:

- 1. Создать необходимые решения инцидентов.
- 2. Создать типы инцидентов.
- 3. Создать состояния инцидентов.
- 4. Создать схему инцидентов.
- 5. Активировать схему инцидентов.

Для создания решения инцидентов используется команда:

Admin@nodename# create incident resolutions name <incident-name> description <incident-description>

Для создания типов инцидентов используется команда:

Admin@nodename# create incident types name <incident-type-name> description <incident-type-description>

Для создания состояния инцидентов используется команда:

Admin@nodename# create incident states name <incident-state-name> description <incident-state-description> group <open|closed|progress>

Для создания схемы инцидентов используется команда:

Admin@nodename# create incident schema <parameters>

Для редактирования доступны следующие параметры схемы инцидентов:

Параметр	Описание
name	Название схемы.
description	Описание схемы
prefix	Префикс, который будет использован при назначении идентификаторов создаваемым инцидентам. Идентификатор будет иметь вид: префикс — порядковый номер, например INC-99.
initial-state	Начальное состояние, которое принимает инцидент при его создании.
workflow-states	Состояния рабочего процесса — описывает все состояния, которые может принимать инцидент в своем жизненном цикле.
incidents-resolutions	Решения инцидентов — указывает список возможных решений инцидентов.
incidents-types	Типы инцидентов, которые могут быть использованы в этой схеме.
transition	Все возможные переходы между состояниями.

Для всех этапов создания схемы инцидентов также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Настройка аналитики (описание)

Documentation: 
Product: SIEM
Version: 7.1.x

UserGate SIEM позволяет проводить анализ журналов событий безопасности, получаемых с настроенных сенсоров. Все данные хранятся в одной базе данных, что даёт возможность осуществлять сложный поиск, корреляцию повторяющихся событий, их агрегацию, создавая инциденты безопасности, и упростить процесс изучения особенностей инцидентов. Подробнее об архитектуре и принципах работы функциональности SIEM читайте в разделе [Аналитика](#) Руководства администратора SIEM.

В интерфейсе CLI возможно создавать и настраивать правила аналитики и действия реагирования. С помощью правил аналитики инженер безопасности может автоматизировать процесс корреляции событий и создание срабатываний, а также назначить определенные действия реагирования (реакцию) системы на создаваемые срабатывания. Все это позволяет облегчить процесс изучения регистрируемых событий и сократить время между обнаружением проблемы и ее решением.

Правила аналитики и действия реагирования в CLI создаются и настраиваются на уровне **analytics**.

Правила аналитики

С помощью правил аналитики происходит обработка событий журналов. Настройка правил аналитики позволяет производить сложный поиск среди событий информационной безопасности. Срабатывание правила происходит при выявлении корреляции событий с разных источников.

Для создания правила аналитики предназначена команда:

```
Admin@nodename# create analytics analytics-rules <parameters>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	on/off — Включение/отключение правила аналитики для работы в режиме реального времени.
name	Название правила аналитики.
description	Описание правила аналитики.
threat-level	Уровень угрозы, который будет отображаться при срабатывании правила. informational: события, сформировавшие срабатывание правила аналитики, представляют очень низкий уровень угрозы, и администратор может не предпринимать никаких действий. low: события, сформировавшие срабатывание правила аналитики, представляют низкий уровень угрозы, и администратор может не предпринимать никаких действий. medium: необходимо обратить внимание на события, попавшие под срабатывание правила аналитики. high: события, требующие исследования и принятия мер. critical: события, требующие исследования и срочного принятия мер.
priority	Показывает приоритет, установленный для срабатывания правила аналитики: low: срабатывания данных правил обладают низким приоритетом реагирования. normal: на срабатывания данных правил необходимо обратить внимание и, возможно, предпринять меры. important: на срабатывания данных правил необходимо обратить внимание и предпринять меры. critical: срабатывания данных правил требуют незамедлительного реагирования. При срабатывании правила установленный приоритет будет указывать на важность срабатывания правила аналитики.
alert-category	Отображает категорию, к которой относится срабатывание. По умолчанию для выбора доступны следующие категории: security: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем. availability: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем. performance: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем. Дополнительные категории срабатываний могут быть созданы в библиотеке Категории срабатывания . Подробнее читайте в разделе Настройка категорий срабатывания .
timezone	Указывает на часовой пояс, по времени которого будут работать правила аналитики, т.к. сервер может собирать данные с источников, находящихся в различных часовых поясах.
response-actions	Выбор действий реагирования, которые будут выполнены автоматически при срабатывании правила аналитики. Подробнее о создании действий реагирования и их настройке читайте в разделе Действия реагирования .
conditions	Указание условий срабатывания правила.

Условия срабатывания, которые указываются при создании правила аналитики, имеют следующие параметры настройки:

Параметр	Описание
name	Название условия правила аналитики.
description	Описание условия правила аналитики.
condition-time-enabled	Включить/отключить ограничение времени выполнения условия. При включении ограничения времени правило аналитики работает, только в том случае, когда за указанный отрезок времени условие выполнится заданное количество раз.
condition-time	Указывает на отрезок времени, за который условие должно выполниться заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах. Указание времени выполнения условия доступно при активированном параметре condition-time-enabled .
break-query-enabled	Включить/отключить использование запроса остановки в правиле аналитики.

Параметр	Описание
break-query	SQL-подобный поисковый запрос остановки выполняется вместе с запросом условия. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы (задаётся аналогично запросу фильтра). Если при выполнении анализа найдётся хотя бы одна запись, соответствующая заданному запросу остановки, до того, как будет найдено заданное количество событий, соответствующих условию правила аналитики, то правило аналитики не сработает, а счётчик количества записей, найденных до выполнения запроса остановки, будет обнулён.
filter-query	Отображает SQL-подобный поисковый запрос условия, который пишется по базе журналов. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы. Синтаксис написания запроса можно посмотреть в разделе Поиск и фильтрация данных . Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH. Подробнее о синтаксисе Google/RE2 в операторе MATCH: https://github.com/google/re2/wiki/Syntax .
group-by	Отображает список параметров, по которым могут быть сгруппированы правила в результате срабатывания. Поля будут отображены при просмотре карточки срабатывания. О параметрах, по которым возможна группировка, читайте в разделе Поиск . При указании категорий для группировки правило аналитики сработает только в том случае, если условие выполнится именно для выбранной категории заданное количество раз, указанное в поле параметра pattern-repeats .
pattern-repeats	Показывает количество выполнений условия, необходимое для срабатывания правила. Данный параметр может быть использован вместе с параметром condition-time-enabled или без него.

Для правил аналитики также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Действия реагирования

Действия реагирования позволяют определить методы реагирования при срабатывании правил аналитики информационной безопасности. UserGate SIEM позволяет гибко настраивать правила, используя переменные, относящиеся к категориям срабатывания правил аналитики.

Для создания действия реагирования предназначена команда:

Admin@nodename# create analytics response-actions <parameters>

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	on/off — Включение/отключение правила реагирования.
name	Название правила реагирования.
description	Описание правила реагирования.
action	Показывает действие, выбранное для исполнения в случае срабатывания правила аналитики. Действие реагирования выполнится, если оно указано в свойствах правила аналитики. Для выбора доступны следующие виды реагирования: send-email: отправка письма на выбранные почтовые адреса. Настройка действия Отправить email будет рассмотрена далее в разделе Действие типа send-email. send-message: отправка сообщения на указанные номера телефонов. Настройка действия Отправить сообщение будет рассмотрена далее в разделе Действие типа send-message. webhook: получение уведомления о срабатывании правила на веб-странице, адрес которой был указан при настройке действия. Настройка действия Webhook будет рассмотрена далее в разделе Действие типа webhook. create-incident: автоматическое создание инцидента в результате срабатывания правил аналитики. О настройке действия Создать инцидент читайте в разделе Настройки инцидентов. send-command-to-connector: отправка команды на выбранный коннектор. Настройка действия Послать команду на коннектор будет рассмотрена далее в разделе Действие типа послать send-command-to-connector. send-command-to-endpoint: отправка команды на конечное устройство с установленным ПО UserGate Client. Подробнее читайте в раздел Действие типа send-command-to-endpoint.
enable-logging	Включает/отключает журналирование данных о срабатывании действия реагирования. Данные записываются в журнал событий SIEM.
grouping	Для удобства при настройке действий реагирования возможно использование функции группировки срабатываний. Группировка возможна по следующим параметрам: never — никогда. period — при настройке группировки срабатываний правила аналитики за период времени действие реагирования выполнится, если в течение указанного времени произошло хотя бы одно срабатывание. number — при настройке группировки по количеству срабатываний правила аналитики действие реагирования выполнится только после указанного количества срабатываний.
time-period	Отображает период группировки в минутах. Задание параметра возможно только при выборе группировки похожих срабатываний за период времени.
alerts-number	Отображает заданное количество срабатываний. Задание параметра возможно только при выборе группировки похожих срабатываний по их количеству.

Для действий реагирования также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Действие типа send-email

Если в качестве действия реагирования была выбрана отправка email, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
notification-profile	Профиль оповещения SMTP, который будет использован для отправки email. Подробнее о настройке профилей SMTP читайте в главе Настройка профилей оповещений .

Наименование	Описание
sender	Имя отправителя письма.
subject	Тема письма.
emails	Список почтовых адресов получателей. Получатели должны быть добавлены в списки в библиотеке элементов. О добавлении почтовых адресов читайте в разделе Настройка почтовых адресов .
template	Шаблон письма уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд .

Действие типа send-message

Если в качестве действия реагирования была выбрана отправка сообщения, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
notification-profile	Профиль оповещения SMPP, который будет использован для отправки сообщения. Подробнее о настройке профилей SMPP читайте в главе Настройка профилей оповещений .
sender	Имя отправителя письма.
phones	Список номеров телефонов получателей. Получатели должны быть добавлены в библиотеке элементов. О добавлении телефонных номеров читайте в разделе Настройка номеров телефонов .
template	Шаблон сообщения с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд .

Действие типа webhook

Для настройки webhook в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
url	Адрес веб-сайта, на котором будут отображаться оповещения о срабатывании правила.
template	Шаблон уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд .

Для тестирования webhook можно воспользоваться сервисом <https://webhook.site>. Для этого необходимо перейти на сайт [Webhook.site](#) и скопировать сгенерированную ссылку. Далее её необходимо указать в свойствах правила реагирования в поле **url** параметра **action**.

Действие типа send-command-to-connector

В качестве одного из действий реагирования может быть настроена отправка команды на коннектор.

Если в качестве действия реагирования настроена передача команды для исполнения на коннекторе, то необходимо указать следующие параметры:

Наименование	Описание
connectors	Выбор устройств, на которые необходимо отправить команду в случае срабатывания правила аналитики. Коннектор должен быть заранее добавлен и настроен. Подробнее читайте в разделе Коннекторы . Важно! Могут выбраны только коннекторы с одинаковой группой команд.
command	Определение команды, которая будет передана на коннектор для выполнения; представлены команды группы, указанной для выбранных коннекторов. В случае наличия в команде переменных, будут отображены дополнительные поля для указания их значений. Подробнее о командах читайте в разделе Настройка команд .

Действие типа send-command-to-endpoint

В качестве одного из действий реагирования может быть настроена отправка команды на конечное устройство с установленным ПО UserGate Client. Доступны следующие команды:

- block** — блокировка доступа к сети Интернет.
- kill** — завершение указанного в запросе фильтра процесса.

Шаблон уведомлений

В параметре **template** необходимо указать текст уведомления. Можно передавать не только фиксированный текст, но и данные, относящиеся к срабатыванию или его записям в журнале.

Чтобы передать данные, относящиеся к срабатыванию, необходимо в поле **template** ввести название одного из параметров, представленных в таблице. Например, если ввести **{ANALYTICS_RULE_NAME}**, то в тексте уведомления, настроенном как отправка email, SMS или webhook, будет отражено название правила аналитики, которое сработало. Если заполнить шаблон при настройке действия **create incident**, то текст будет отображён в описании инцидента.

