

Table of Contents

Table of Contents	1
Настройка устройства	2
Настройка устройства (описание)	3
Настройка управления доступом к консоли устройства	6
Настройка сертификатов	9
Настройка серверов аутентификации	10
Настройка профилей аутентификации	13
Роли пользователей	14
Каталоги пользователей	15

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
interface	Название интерфейса.

Параметр	Описание
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**.

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. 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
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. 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
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы 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>
```

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>

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> ]
```

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.**

