

Table of Contents

Table of Contents	1
Настройка устройства	2
Базовые настройки	3
Настройка управления доступом к веб-консоли UserGate WAF	10
Настройка сертификатов	15
Настройка профилей клиентских сертификатов	17
Настройка кластеров	18

Product: WAF
Version: 7.7.x

Настройка параметров работы CLI

На уровне settings cli настраиваются следующие параметры работы интерфейса командной строки:

- вид системного приглашения (prompt) консоли CLI;
- уровень детализации диагностики.

Для настройки системного приглашения консоли CLI используется команда:

```
Admin@nodename# set settings cli custom-prompt <new-custom-prompt>
```

Вы можете поменять системное приглашение в консоли CLI с установленного по умолчанию (вида: Admin@nodename#) на удобное вам.

Например, чтобы поменять вид системного приглашения на NodeAABBCC, выполните следующую команду:

```
Admin@nodename# set settings cli custom-prompt NodeAABBCC  
NodeAABBCC#
```

Вернуть системное приглашение в первоначальное состояние можно с помощью команды:

```
Admin@nodename# set settings cli custom-prompt default
```

Пример использования команды:

```
NodeAABBCC#  
NodeAABBCC# set settings cli custom-prompt default  
Admin@nodename#
```

Чтобы задать уровень детализации диагностики используется следующая команда:

```
Admin@nodename# set settings cli log-level <off | error | debug | warning | info>
```

Вы можете установить следующие уровни детализации:

- off — отключить журналирование;
- error — только ошибки;
- warning — ошибки и предупреждения;
- info — ошибки, предупреждения и дополнительная информация;
- debug — максимальная детализация.

Посмотреть текущие значения параметров работы интерфейса командной строки можно с помощью команды:

```
Admin@nodename# show settings cli
```

Настройка базовых параметров устройства

Настройка базовых параметров UserGate WAF выполняется на уровне settings general.

Структура команд для настройки базовых параметров устройства:

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

Базовые параметры устройства сгруппированы в разделы.

Раздел	Описание

Раздел	Описание
admin-console	Параметры консоли управления: • <code>timezone</code> — 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. • <code>language</code> — язык интерфейса: ◦ <code>ru</code> — русский; ◦ <code>en</code> — английский. • <code>webaccess</code> — режим аутентификации веб-консоли: ◦ <code>password</code> — аутентификация по имени и паролю. ◦ <code>cert</code> — аутентификация по X.509-сертификату. • <code>web-ssl-profile</code> — выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL — в разделе «Настройка профилей SSL». • <code>api-session-lifetime</code> — время ожидания сеанса администратора в секундах • <code>http-connection-timeout</code> — время ожидания установления HTTP-соединения в секундах. Значение по умолчанию — 20 секунд. (Доступно в версии ПО 7.5.0 и выше). • <code>http-loading-timeout</code> — время, выделенное на загрузку HTTP-контента в секундах. Значение по умолчанию — 60 секунд. (Доступно в версии ПО 7.5.0 и выше)
server-time	Параметры установки точного времени: • <code>ntp-enabled</code> — включение или отключение использования NTP-серверов. • <code>primary-ntp-server</code> — адрес основного NTP-сервера. • <code>second-ntp-server</code> — адрес запасного NTP-сервера. • <code>time</code> — установка времени на устройстве. Время указывается в часовом поясе UTC в формате <code>yyyy-mm-ddThh:mm:ss</code> (например, 2022-02-15T12:00:00)
modules	Настройка модулей устройства: • <code>lldp</code> — настройка использования протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети, оповещать устройства о своем существовании, передавать им свои характеристики, а также получать от них аналогичную информацию. При настройке необходимо задать значения: ◦ <code>transmit-delay</code> — задержка передачи, указывается время ожидания устройства перед отправкой объявлений соседям после изменения TLV в протоколе LLDP или состояния локальной системы, например, изменение имени узла или адреса управления. Может принимать значения от 1 до 3600. Указывается в секундах. ◦ <code>transmit-hold</code> — значение мультипликатора удержания. Может принимать значения от 1 до 100. Произведение значений <code>transmit delay</code> и <code>transmit hold</code> определяет время жизни (TTL) пакетов LLDP
cache	Параметры кэширования прокси-сервера: • <code>caching-mode</code> — включение или отключение режима кэширования. • <code>exclusions</code> — список URL, которые не будут кэшироваться. Для удаления исключений используйте команду: <code>Admin@nodename# delete settings general cache exclusions [<URL>]</code> • <code>max-cacheable-size</code> — максимальный размер объектов, которые будут кэшироваться (МБ). • <code>ram-size</code> — размер оперативной памяти, отведенный под кэширование (МБ)
log-analyzer	Параметры модуля сбора статистики: • <code>use-local-stat-server</code> — использование локальной службы журналирования

Раздел	Описание
management-center	Настройка агента UserGate Management Center. Команда для настройки: <pre>Admin@nodename# set settings general management-center <parameters></pre> Параметры: - enabled — включение или отключение агента UserGate Management Center; - 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. Для задания расписания обновления программного обеспечения: <pre>Admin@nodename# set settings general updates-schedule software schedule <schedule/disabled></pre> Расписание скачивания обновлений библиотек может быть единым: <pre>Admin@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled></pre> Также расписание может быть настроено отдельно для каждого элемента: <pre>Admin@nodename# set settings general updates-schedule libraries [lib-module ...] schedule <schedule/disabled></pre> Время задается в crontab-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. - Дефис (-) — для указания диапазона значений. - Запятая (,) — в качестве разделителя значений. - Косая черта (/) — для указания шага между значениями. Команда для просмотра расписания обновлений: <pre>Admin@nodename# show settings general updates-schedule</pre>

Настройка управления устройством

Настройка диагностики

В этом блоке вы можете управлять параметрами диагностики устройства, необходимыми службе технической поддержки для решения возможных проблем.

Параметры диагностики сервера, необходимые службе технической поддержки при решении проблем, задаются на уровне settings loglevel.

С помощью следующей команды вы можете установить необходимый уровень детализации журналирования событий:

```
Admin@nodename# set settings loglevel value <off | error | warning | info | debug>
```

- off — ведение журналов диагностики отключено;
- error — журналировать только ошибки в работе UserGate WAF;
- warning — журналировать только ошибки и предупреждения;
- info — журналировать только ошибки, предупреждения и дополнительную информацию;
- debug — журналировать все возможные события.

При журналировании с уровнями warning, info и debug может снижаться производительность устройства, поэтому рекомендуется устанавливать уровни error или off, если технической поддержкой UserGate не было предложено иное.

Для просмотра состояния уровня детализации диагностики используется команда:

```
Admin@nodename# show settings loglevel
```

Для включения или отключения удаленного помощника (Radmin) используется команда:

```
Admin@nodename# set settings radmin enabled <on | off>
```

Для просмотра состояния удаленного помощника используется команда:

Admin@nodename# show settings radmin

Настройка Radmin-emergency

Если произошли неполадки с ядром UserGate WAF, может пропасть возможность авторизации в CLI. Для активации удаленного помощника в таких случаях администратор может зайти в CLI в режиме emergency под учетной записью корневого администратора, которая была создана при инициализации UserGate WAF. Обычно это учетная запись Admin. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора.

Команда входа в режим emergency CLI выглядит следующим образом:

```
ssh Admin@emergency@<WAF_IP> -p 2200
```

Команда включения и отключения удаленного доступа к серверу для технической поддержки в режиме emergency:

```
Admin@emergency@WAF# set radmin-emergency enabled <on | off> <parameters>
```

В команде указываются следующие сетевые параметры:

- interface — название интерфейса;
- ip-addr — IP-адрес интерфейса;
- gateway-address — IP-адрес шлюза.

Настройка операций с сервером

В этом разделе вы можете установить канал получения обновлений для устройства (стабильные или бета-версии).

Канал обновлений устанавливается с помощью команды:

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

Для просмотра наличия обновлений и выбранного канала обновления используется команда:

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

Управление резервным копированием

Управление резервным копированием происходит на уровне setting 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>
```

Параметры правил резервного копирования.

Параметр	Описание
enabled	Включение или отключение правила создания резервной копии устройства
name	Название правила резервного копирования
description	Описание правила резервного копирования
type	Выбор типа удаленного сервера для экспорта файлов: • ssh; • ftp
address	IP-адрес удаленного сервера
port	Порт сервера
login	Учетная запись на удаленном сервере
password	Пароль учетной записи
path	Путь на сервере, куда будут выгружены файлы

Параметр	Описание
schedule	Расписание экспорта файлов резервных копий. Время задается в crontab-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. - Дефис (-) — для указания диапазона значений. - Запятая (,) — в качестве разделителя значений. - Косая черта (/) — для указания шага между значениями

Изменение существующего правила резервного копирования устройства UserGate производится с помощью 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>
```

Для команд изменения, удаления или отображения правил в качестве параметра **<filter>** можно использовать не только названия правила, но и другие заданные в правиле параметры (см. список параметров [в таблице выше](#)).

Экспорт настроек

Управление экспортом настроек происходит на уровне settings device-mgmt.

Правила экспорта настроек создаются с помощью команды :

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

Параметры экспорта настроек.

Параметр	Описание
enabled	Включение или отключение правила экспорта настроек устройства
name	Название правила экспорта
description	Описание правила экспорта
type	Тип удаленного сервера для экспорта настроек: - ssh; - ftp
address	IP-адрес удаленного сервера
port	Порт сервера
login	Учетная запись на удаленном сервере
password	Пароль учетной записи на удаленном сервере
path	Путь на сервере, куда будут выгружены настройки

Параметр	Описание
schedule	Расписание экспорта настроек. Время задается в crontab-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. - Дефис (-) — для указания диапазона значений. - Запятая (,) — в качестве разделителя значений. - Косая черта (/) — для указания шага между значениями

Изменение существующего правила экспорта настроек устройства выполняется с помощью 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>
```

Для команд изменения, удаления или отображения правил в качестве параметра <filter> можно использовать не только название правила, но и другие заданные в правиле параметры (см. список параметров [в таблице выше](#)).

Настройка защиты конфигурации от изменений

Для настройки параметров защиты конфигурации устройства от изменения используйте следующую команду:

```
Admin@nodename# set settings change-control config <off | log | block>
```

Проверка целостности конфигурации происходит каждые несколько минут после загрузки UserGate WAF.

- log — активация режима отслеживания изменений конфигурации. При обнаружении изменений UserGate WAF записывает информацию о факте изменения в журнал событий. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания.
- off — отключение режима отслеживания изменений конфигурации. Необходимо указать пароль, который был задан при активации режима отслеживания конфигурации.
- block — активация режима отслеживания изменений конфигурации. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate WAF записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик.

Перед активацией защиты конфигурации администратор производит настройку продукта в соответствии с требованиями организации, после чего защищает настройки от изменений (режим log или block). Любое изменение настроек через веб-интерфейс, CLI или другими способами будет приводить к журналированию и блокировке транзитного трафика, в зависимости от выбранного режима.

Для просмотра текущего режима защиты конфигурации от изменений используется команда:

```
Admin@nodename# show settings change-control config
```

Настройка защиты исполняемых файлов от изменения

Для настройки защиты исполняемого кода устройства от потенциального несанкционированного изменения используется команда:

```
Admin@nodename# set settings change-control code <off | log | block>
```

Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate WAF.

- log — активация режима отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate WAF записывает информацию о факте изменения в журнал событий. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания.
- off — отключение режима отслеживания несанкционированных изменений исполняемого кода. Необходимо указать пароль, который был задан при активации режима отслеживания исполняемого кода.
- block — активация режима отслеживания несанкционированных изменений исполняемого кода. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate WAF записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик. Чтобы отключить созданное правило межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.

Для просмотра текущего режима защиты исполняемых файлов используется команда:

```
Admin@nodename# show settings change-control code
```

Настройка режима ускоренной обработки сетевого трафика

Для включения или отключения режима ускоренной обработки трафика используется команда:

```
Admin@nodename# set settings fastpath enabled <on/off>
```

Для просмотра настройки режима ускоренной обработки трафика используется команда:

```
Admin@nodename# show settings fastpath
```

Product: WAF

Version: 7.7.x

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. description: описание учётной записи администратора. admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. password: пароль администратора
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее — 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: 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 — в разделе «Настройка LDAP-коннектора»): enabled: включение/отключение учётной записи администратора: on. off. login: логин 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>

Параметр	Описание
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы корректно настроенные серверы аутентификации; подробнее — в разделе «Настройка серверов аутентификации»): enabled: включение/отключение учётной записи администратора: on. off. login: логин 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 — 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
api-permissions	Права доступа к API: • no-access: нет доступа. • read: только чтение. • write: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@nodename# create settings administrators profiles ... api-permissions <permission> all или Admin@nodename# create settings administrators profiles ... api-permissions <permission> [object ...]
webui-permissions	Права доступа к веб-интерфейсу UserGate: • no-access: нет доступа. • read: только чтение. • write: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@nodename# create settings administrators profiles ... webui-permissions <permission> all или Admin@nodename# create settings administrators profiles ... webui-permissions <permission> [object ...]
cli-permissions	Права доступа к интерфейсу командной строки (CLI): • no-access: нет доступа. • read: только чтение. • write: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@nodename# create settings administrators profiles ... cli-permissions <permission> all или Admin@nodename# create settings administrators profiles ... cli-permissions <permission> [object ...]

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 авторизацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators admin-sessions**).

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

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

Для отображения сессий доступно использование фильтра:

- **ip**: IP-адрес, с которого авторизован администратор.
- **source**: где была произведена авторизация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).

- **admin-login**: имя администратора.
- **node**: узел кластера UserGate.

```
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 авторизация:

```
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             : utmcore@dineanoulwer
```

```
admin-login      : Admin
source           : web
session_start_date : 2023-08-10T11:33:10Z
ip               : 10.0.2.2
node             : utmcore@dineanoulwer
```

```
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             : utmcore@dineanoulwer
```

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

Product: WAF
Version: 7.7.x

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, которое будет отображено в списке
description	Описание сертификата
certificate-data	Сертификат в формате PEM
certificate-chain	Цепочка сертификатов в формате PEM
private-key	Приватный ключ в формате PEM
passphrase	Пароль для приватного ключа или контейнера PKCS12 (необязательное значение)
user	Локальный пользователь, которому будет назначен пользовательский сертификат
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • user: имя пользователя в формате domain\user. • connector: выбор LDAP-сервера
role	Тип сертификата: • web-cert-chain: цепочка сертификатов веб-консоли. • saml: сертификат, который будет использован в SAML-клиенте. • none

Для экспорта доступны сертификаты, вся цепочка сертификатов и CSR:

```
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

Параметр	Описание
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	Электронная почта 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. • user: пользовательский сертификат, который может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси. • captive-portal: сертификат, использующийся для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. • web-ssl: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. • saml: сертификат, который будет использован в SAML-клиенте. • none
user	Локальный пользователь, которому будет назначен пользовательский сертификат
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • user: имя пользователя в формате domain\user. • connector: выбор LDAP-сервера
certificate-data	Сертификат в формате PEM
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>
```

Чтобы удалить сертификат из кэша используется команда:

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

Настройка профилей клиентских сертификатов

Product: WAF

Version: 7.7.x

Раздел **Профили клиентских сертификатов** находится на уровне **settings certificate-profiles**.

Для создания профиля клиентского сертификата предназначена команда:

```
Admin@nodename# create settings certificate-profiles <parameters>
```

Далее могут использоваться следующие параметры:

Параметр	Описание
name	Название профиля клиентского сертификата
description	Описание профиля
username-field	Выбор поля в сертификате, по которому определяется имя пользователя, используемое при аутентификации: • common — доменное имя или имя хоста в поле Subject, для которых предназначен сертификат. • email — для определения имени пользователя используется параметр с префиксом email в расширении SAN (Subject Alternative Name). • principal — для определения имени пользователя используется параметр Universal Principal Name (UPN), содержащийся в поле otherName в расширении SAN. Если в полях расширения SAN сертификата указано несколько имен UPN или несколько адресов email, берется первый, указанный в сертификате
certificates	Сертификаты УЦ, назначаемые профилю
crl	В списках отзыва сертификатов (CRL) содержатся сертификаты, которые были отозваны и больше не могут использоваться. В этот список входят сертификаты, срок действия которых истек или они были скомпрометированы. Параметр для проверки состояния отзыва сертификатов: • off — не проверять ни один сертификат. • on — проверять все сертификаты в цепочке и требовать, чтобы они все были валидными. • peer — проверять только сертификат клиента. • best-effort — если проверить CRL не удалось по какой-то причине, то сертификат считается валидным (при этом он всё равно проверяется и может вернуть статус invalid, если сертификат есть в списке отозванных)
receive-timeout	Интервал времени, по истечению которого WAF перестает ожидать ответа от службы списков отзыва сертификатов

Для просмотра ранее созданных профилей клиентских сертификатов используются команды:

```
Admin@nodename# show settings certificate-profiles
```

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

Для редактирования ранее созданного профиля используется команда:

```
Admin@nodename# set settings certificate-profiles <certificate-profile-name> <parameters>
```

Параметры, доступные для редактирования профиля, аналогичны параметрам создания профиля, рассмотренным ранее.

Для удаления ранее созданного профиля используется команда:

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

Documentation: 
Product: WAF
Version: 7.7.x
Technology: Clustering and HA

Настройка кластера конфигурации

Данный раздел находится на уровне **settings device-mgmt configuration-cluster**.

Команда обновления существующего узла кластера:

Admin@nodename# set settings device-mgmt configuration-cluster <node-name>

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменить имя узла кластера
description	Обновить описание узла кластера
ip	Задать IP-адрес интерфейса, входящего в зону, выделенную для кластера

Команды для удаления и отображения настроек узла кластера:

Admin@nodename# delete settings device-mgmt configuration-cluster <node-name>
...
Admin@nodename# show settings device-mgmt configuration-cluster <node-name>

Команда для генерации секретного кода для добавления нового узла в кластер конфигурации:

Admin@nodename# execute configure-cluster generate-secret-key

