Table of Contents

Table of Contents 1
Настройка устройства 2
- Настройка устройства (Описание) 3
- Настройка кластеров 10
- Настройка управления доступом к консоли UserGate DCFW 13
- Настройка сертификатов 17
- Настройка параметров устройства 19
- Настройка параметров мониторинга устройства 21
- Настройка профилей клиентских сертификатов 24

Настройка устройства

Product: DCFW
Version: 8.x

Настройка CLI

Настройка интерфейса командной строки производится на уровне **settings cli**. Чтобы задать уровень детализации диагностики используется следующая команда:

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

Уровни детализации:

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

Для отображения настроек CLI:

Admin@nodename# show settings cli

Для настройки системного приглашения (prompt) консоли CLI используется команда:

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

Для возвращения системного приглашения в первоначальное состояние используется команда:

Admin@nodename# set settings cli custom-prompt default

Общие настройки UserGate

Общие настройки сервера UserGate 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. • **uc-profile**: выбор профиля пользовательских сертификатов. • **web-ssl-profile**: выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL смотрите в разделе Настройка профилей SSL. • **response-pages-ssl-profile**: выбор профиля SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации Captive-портала. Подробнее о профилях SSL смотрите в разделе Настройка профилей SSL. • **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)

Параметр	Описание
modules	Настройка модулей UserGate (уровень **settings general modules**): • **proxy-port**: указать нестандартный номер порта, который будет использоваться для подключения к встроенному прокси-серверу. • **auth-captive**: указать служебный домен, который используется UserGate при авторизации пользователей через Captive-портал. • **logout-captive**: указать служебный домен, который используется пользователями UserGate для окончания сессии (logout). • **block-page-domain**: указать служебный домен, который используется для отображения страницы блокировки пользователям. • **ftp-enabled**: включить/отключить модуль, позволяющий получать доступ к содержимому FTP-серверов из пользовательского браузера. • **ftp-domain**: указать служебный домен, который используется для предоставления пользователям сервиса FTP поверх HTTP. • **tunnel-inspection-zone**: выбрать зону для инспектируемых туннелей. Необходимо указать: ◦ **enabled** — включить/выключить зону. ◦ **name** — указать название зоны. • **snmp-engine-id**: настроить SNMP Engine ID: ◦ **length** <**fixed** | **dynamic**> — длина идентификатора: фиксированная (не более 8 байт; только для типа text) или динамическая (не более 27 байт). ◦ **type** <**ip4** | **ip6** | **mac** | **text** | **octets**> — формат SNMP Engine ID (IPv4, IPv6, MAC-адрес, текст, октеты). ◦ **value** — значение идентификатора. • **terminal-sever-agent**: настроить пароль агентов терминального сервиса. • **lldp**: настроить использование протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети, оповещать устройства о своём существовании, передавать им свои характеристики, а также получать от них аналогичную информацию. При настройке необходимо задать значения: ◦ **transmit-delay** — задержка передачи, указывается время ожидания устройства перед отправкой объявлений соседям после изменения TLV в протоколе LLDP или состояния локальной системы, например, изменение имени хоста или адреса управления. Может принимать значения от 1 до 3600; задаётся в секундах. ◦ **transmit-hold** — значение мультипликатора удержания; произведение значений transmit delay и transmit hold определяет время жизни (TTL) пакетов LLDP. Может принимать значения от 1 до 100.
cache	Настройка кэша прокси-сервера (уровень **settings general cache**): • **caching-mode**: включение или отключение кэширования. ◦ **on**. ◦ **off**. • **exclusions**: список URL, которые не будут кэшироваться. Для удаления исключений: Admin@nodename# delete settings general cache exclusions [<URL>] • **max-cacheable-size**: максимальный размер объектов, которые будут кэшироваться (указывается в Мбайт). • **ram-size**: размер оперативной памяти, отведенный под кэширование (указывается в Мбайт).
log-analyzer	Настройки модуля Log Analyzer (уровень **settings general log-analyzer**): • **use-local-stat-server** — использование локального Log Analyzer: ◦ **on**. ◦ **off**.
pcap	Admin@nodename# set settings general pcap packet-capture-mode <parameter> Настройка захвата пакетов (уровень **settings general pcap**): • **no-capture**: без захвата. • **one-packet**: один пакет. • **previous**: предшествующие пакеты. • **previous-and-following**: предшествующие и последующие пакеты. ◦ **previous-packets**: количество предшествующих пакетов (от 4 до 30 пакетов). ◦ **following-packets**: количество последующих пакетов (от 2 до 15 пакетов).

Параметр	Описание
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@nodename# delete settings general change-tracker event-tracker-types [type1 ...]
management-center	Admin@nodename# set settings general management-center <parameters> 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@nodename# set settings general updates-schedule software schedule <schedule/disabled> Расписание скачивания обновлений библиотек может быть единым: Admin@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled> или может быть настроено отдельно для каждого элемента: Admin@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@nodename# show settings general updates-schedule
upstream-proxy	Настройка перенаправления HTTP трафика на вышестоящий прокси-сервер: • **enabled** — включение/выключение перенаправления трафика на вышестоящий прокси-сервер (on/off). • **mode** — тип вышестоящего прокси-сервера (HTTP(S)/SOCKS5). • **ip** — IP-адрес вышестоящего прокси-сервера. • **port** — порт вышестоящего прокси-сервера. • **auth** — аутентификация на вышестоящем прокси-сервере (on/off). • **name** — логин на вышестоящем прокси-сервере. • **password** — пароль на вышестоящем прокси-сервере.

Настройка управления устройством

Настройка диагностики

На уровне **settings radmin** можно включить или отключить удалённый доступ к серверу для технической поддержки UserGate (**Radmin**). Команда включения/отключения Radmin:

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

Для просмотра состояния Radmin:

Admin@nodename# show settings radmin

Параметры диагностики сервера, необходимые службе технической поддержки при решении проблем, задаются на уровне **settings loglevel**. С помощью следующей команды можно установить необходимы уровень детализации диагностики (отключено; только ошибки; ошибки и предупреждения; ошибки, предупреждения и дополнительная информация; максимум детализации):

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

Для просмотра состояния уровня детализации диагностики:

Admin@nodename# show settings loglevel

value : error

Настройка Radmin-emergency

Для активации удаленного помощника при возникновении проблемы с программным ядром узла администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации UserGate. 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:

Admin@nodename# set radmin-emergency enabled <on | off>

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

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 UserGate 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.

Параметр	Описание
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 сервера UserGate 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 защиты конфигурации от изменений

Для настройки параметров защиты конфигурации (настроек) продукта 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.

- **log** — активирует режим отслеживания изменений конфигурации. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требует задания пароля, который потребуется в случае изменения режима отслеживания.
- **off** — отключает режим отслеживания изменений конфигурации. Требует указания пароля, который был задан при активации режима отслеживания конфигурации.
- **block** — активирует режим отслеживания изменений конфигурации. Требует задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate.

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

Для просмотра текущего режима защиты конфигурации от изменений:

Admin@nodename# show settings change-control config

Настройка защиты исполняемых файлов от изменения

Чтобы настроить защиту параметры защиты исполняемого кода продукта от потенциального несанкционированного изменения:

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

Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate

- **log** — активирует режим отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требует задания пароля, который потребуется в случае изменения режима отслеживания.
- **off** — отключает режим отслеживания несанкционированных изменений исполняемого кода. Требует указания пароля, который был задан при активации режима отслеживания исполняемого кода.
- **block** — активирует режим отслеживания несанкционированных изменений исполняемого кода. Требует задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate. Для возможности отключения созданного правила межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.

Для просмотра текущего режима защиты исполняемых файлов:

Admin@nodename# show settings change-control code

Настройка режима ускоренной обработки сетевого трафика

Для включения/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: DCFW
Version: 8.x

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 configurate-cluster generate-secret-key

Настройка кластера отказоустойчивости

Настройка кластеров отказоустойчивости производится на уровне **settings device-mgmt ha-clusters**.

Для создания кластера отказоустойчивости:

Admin@nodename# create settings device-mgmt ha-clusters

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: • **on**. • **off**.
name	Название кластера отказоустойчивости.
description	Описание кластера отказоустойчивости.
mode	Выбор режима работы кластера: • **active-passive**: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных). • **active-active**: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
session-sync	Настройка синхронизации пользовательских сессий в кластере: • **off** — отключение синхронизации пользовательских сессий. • **on** — включение синхронизации пользовательских сессий. • **ha-cluster-id:** ◦ <num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).

Параметр	Описание
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла (на зоне выбранного интерфейса должен быть разрешён сервис VRRP; подробнее о настройке зон через CLI читайте в разделе Зоны). Добавление виртуального IP-адреса в кластер: Admin@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info> Доступные параметры для <virtual-ips-filter>: • **new**: создать виртуальный IP-адрес для заданного кластера. • <ip>: изменить данные для выбранного виртуального адреса. Доступные параметры для <virtual-ip-info>: • **ip**: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask). • **ha-interfaces**: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка **session-sync** активирована, синхронизироваться будут только TCP сессии.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий.

Пример команды создания кластера:

Admin@nodename# create settings device-mgmt ha-clusters nodes [node_1] name "Test HA cluster" description "Test HA cluster description" mode active-passive enabled on virtual-ips new ha-interfaces [node_1/port3] ip 192.168.1.5/24

Для редактирования настроек кластера:

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

Параметры для редактирования:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: • **on**. • **off**.
name	Название кластера отказоустойчивости.
description	Описание кластера отказоустойчивости.
mode	Выбор режима работы кластера: • **active-passive**: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных). • **active-active**: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
master-node	Назначение мастер-узла кластера отказоустойчивости.
session-sync	Настройка синхронизации сессий в кластере: • **off** — отключение синхронизации пользовательских сессий. • **on** — включение синхронизации пользовательских сессий. • **ha-cluster-id:** ◦ <num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.

Параметр	Описание
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла (на зоне выбранного интерфейса должен быть разрешён сервис VRRP; подробнее о настройке зон через CLI читайте в разделе Зоны). Добавление виртуального IP-адреса в кластер: Admin@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info> Доступные параметры для <virtual-ips-filter>: • **new**: создать виртуальный IP-адрес для заданного кластера. • <ip>: изменить данные для выбранного виртуального адреса. Доступные параметры для <virtual-ip-info>: • **ip**: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask). • **ha-interfaces**: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка **session-sync** активирована, синхронизироваться будут только TCP сессии.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий.

Примеры редактироания настроек кластера:

Admin@nodename# set settings device-mgmt ha-clusters "Test HA cluster" nodes [node_1 node_2] virtual-ips 192.168.1.5/24 ha-interfaces [node_1/port3 node_2/port3]
...
Admin@nodename# set settings device-mgmt ha-clusters "Test HA cluster" master-node utmcore@iononsteswer

Для удаления кластера:

Admin@nodename# delete settings device-mgmt ha-clusters <cluster-name>

Также доступно удаление отдельных параметров:

- **nodes**.
- **virtual-ips**.

Для отображения информации о всех кластерах отказоустойчивости:

Admin@nodename# show settings device-mgmt ha-cluster

Для отображения информации об определённом кластере:

Admin@nodename# show settings device-mgmt ha-cluster <cluster-name>

Product: DCFW
Version: 8.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 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: • **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 • **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. • **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.
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: DCFW
Version: 8.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. • **ssl-intermediate**: промежуточный сертификат в цепочке удостоверяющих центров. • **ssl-root**: корневой сертификат в цепочке удостоверяющих центров. • **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**.

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.

Параметр	Описание
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. • **ssl-intermediate**: промежуточный сертификат в цепочке удостоверяющих центров. • **ssl-root**: корневой сертификат в цепочке удостоверяющих центров. • **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 параметров устройства

Product: DCFW
Version: 8.x

Изменение параметров устройства производится на уровне **settings device**. Для изменения используется следующая команда (где <setting-name> — название параметра):

Admin@nodename# set settings device <setting-name>

Доступно изменение следующих параметров:

Параметр	Описание
l7	Включение/отключение загрузки модуля L7: • **on**. • **off** По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка устройства UserGate.
sip	Включение/отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** По умолчанию модуль выгружен. **Важно!** После включения для корректной работы модуля необходимо перезагрузить таблицу правил межсетевого экрана (кнопка **Принудительно применить** в разделе **Политики сети → Межсетевой экран**).
h323	Включение/отключение загрузки модуля h323; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** По умолчанию модуль выгружен.
idps	Включение/отключение загрузки модуля IDPS: • **on**. • **off** По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка устройства UserGate.
sunrpc	Включение/отключение загрузки модуля SunRPC: • **on**. • **off** По умолчанию модуль выгружен.
ftp-alg	Включение/отключение загрузки модуля FTP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** **Важно!** Модуль нужно включать для пассивного режима работы FTP. По умолчанию модуль выгружен.
auth-type	Использование подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости: • **ah** — включение подписи. • **pass** — отключение проверки.

Параметр	Описание
fw-drop-invalid	Включение/отключение блокировки пакетов с невалидным набором параметров в полях заголовка: • **on**. • **off** По умолчанию настройка находится в выключенном состоянии. Включение данной опции существенно понижает производительность межсетевого экрана; рекомендуется оставить данную настройку выключенной.
fw-established	Включение/отключение создания одного общего правила межсетевого экрана для обратных пакетов: • **on**. • **off** По умолчанию настройка выключена.
bypass-optimization	Включение/отключение оптимизации инспектирования SSL: • **on**. • **off** По умолчанию настройка выключена.

Для просмотра текущих настроек используйте команду:

Admin@nodename# show settings device

Настройка параметров мониторинга устройства

Product: DCFW
Version: 8.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 smnp-parameter**:

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

Для редактирования доступны следующие параметры:

Наименование	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 smnp**:

Admin@nodename# edit monitoring snmp <parameters>

Для редактирования доступны следующие параметры:

Наименование	Описание
name	Название правила.
enabled	Включение/отключение правила
community	SNMP community — строка для идентификации сервера 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.

Наименование	Описание
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 UserGate DCFW 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 ля аутентификации SNMP-менеджеров используются команды на уровне **monitoring smnp-security-profile**:

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

Для редактирования доступны следующие параметры:

Наименование	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:

Наименование	Описание
enabled	Включает/отключает данное правило.

Наименование	Описание
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 захвата пакетов

Захват пакетов позволяет записать трафик, удовлетворяющий заданным условиям, в pcap-файл для дальнейшего анализа с помощью сторонних средств, например, wireshark. Это бывает необходимо при диагностировании сетевых проблем.

Pcap-фильтры определяют условия, по которым будет записываться трафик. В качестве условий могут выступать адрес источника, порт источника, адрес назначения, порт назначения, протокол IPv4.

Для настройки pcap-фильтров используются команды на уровне **monitoring pcap-filter**:

Admin@nodename# edit monitoring pcap-filter <parameters>

В pcap-правилах указываются интерфейсы UserGate, на которых необходимо записывать трафик, фильтры, созданные ранее, имя и размер файла, в который записывается перехваченный трафик.

Для настройки pcap-правил используются команды на уровне **monitoring pcap-rule**:

Admin@nodename# edit monitoring pcap-rule <parameters>

Настройка профилей клиентских сертификатов

Product: DCFW
Version: 8.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 DCFW 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>