

Table of Contents

Table of Contents	1
Настройка раздела Пользователи и устройства	2
Настройка групп пользователей	3
Настройки пользователей	4
Настройка серверов аутентификации	5
Настройка профилей аутентификации	8
Настройка Captive-профилей	9
Captive-портал	11
Настройка терминальных серверов	13
Настройка профилей MFA (мультифакторной аутентификации)	14
Просмотр информации об авторизованных пользователях	16
Настройка применения политик к пользователям	17
Настройка UserID агента	18

Настройка групп пользователей

Product: DCFW
Version: 8.x

Настройка групп пользователей производится на уровне **users group**.

Для добавления новой группы пользователей используется команда:

Admin@nodename# create users group <parameter>

Возможно указать следующие параметры:

Параметр	Описание
name	Название группы пользователей.
description	Описание группы пользователей.
transient	Указать: • on — группа для гостевых пользователей. • off — не является группой для гостевых пользователей.
users	Добавление пользователей в группу.
ldap-users	Добавление пользователей LDAP. При добавлении пользователей LDAP необходимо указать LDAP-коннектор (ldap-users connector <ldap-server-name> users + [<domain/user1> <domain/user2> ...]).

Для редактирования информации о группе пользователей необходимо воспользоваться следующей командой (параметры, доступные для обновления, аналогичны с параметрами, доступными при создании группы):

Admin@nodename# set users group <group-name> <parameter>

Для отображения настроек группы используется следующая команда:

Admin@nodename# show users group <group-name>

Примеры команд создания и редактирования группы пользователей:

Admin@nodename# create users group name "Test user group" ldap-users connector "LDAP connector" users [testd.local/user1]
Admin@nodename# show users group "Test user group"

```
name      : Test user group
is-ldap   : off
is-transient : off
users     : user1 user1 (testd.local/user1)
Admin@nodename# set users group "Test user group" users [ user2 ]
Admin@nodename# show users group "Test user group"
```

```
name      : Test user group
is-ldap   : off
is-transient : off
users     : user2; user1 user1 (testd.local/user1)
```

С использованием следующих команд можно удалить группу пользователей или отдельных пользователей группы:

Admin@nodename# delete users group <group-name>

Для удаления локальных пользователей:

Admin@nodename# delete users group <group-name> users [<user1> <user2> ...]

Для удаления пользователей LDAP:

Admin@nodename# delete users group <group-name> ldap-users connector <ldap-server-name> users [<domain/user1> <domain/user2> ...]

Пример удаления из группы пользователя LDAP:

Admin@nodename# delete users group "Test user group" ldap-users connector "LDAP connector" users [testd.local/user1]

Настройки пользователей

Version: 8.x
Product: DCFW

Настройка пользователей производится на уровне **users user**.

Команда для добавления пользователей:

Admin@nodename# create users user <parameter>

Доступно указание следующих параметров:

Параметр	Описание
enabled	Включение/отключение пользователя.
name	Имя пользователя.
login	Логин пользователя — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
password	Пароль пользователя — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
expiration-date	Срок действия учётной записи пользователя. Указывается в формате YYYY-MM-DD.
groups	Группы, в которые будет добавлен пользователь.
ip	IP-адреса для идентификации пользователя; пользователь всегда должен получать доступ в сеть с указанных адресов.
mac	MAC-адреса для идентификации пользователей; пользователь всегда должен получать доступ в сеть с указанных адресов.
ip-range	Диапазон IP-адресов для идентификации пользователя; пользователь всегда должен получать доступ в сеть с адреса из указанного диапазона. Диапазон задаётся в формате: <IP_start-IP_end>.
ip-mac	Идентификация пользователя с помощью комбинации MAC и IP-адресов; пользователь всегда должен получать доступ в сеть с указанных адресов. Указывается в формате <ip-mac>.
vlan-tag	Тег VLAN ля идентификации пользователя.
emails	Почтовые адреса пользователя.
phones	Номера телефонов пользователя.

Для обновления параметров учётной записи пользователя:

Admin@nodename# set users user <user-name> <parameter>

Список доступных параметров аналогичен списку параметров, доступному при создании учётной записи пользователя.

Команда для просмотра учётной записи пользователя:

Admin@nodename# show users user <user-name>

Пример команд создания и редактирования учетной записи пользователя:

Admin@nodename# create users user name user_2 login user2 password 12345 expiration-date 2023-12-31 ip [192.168.100.112] enabled on
Admin@nodename# show users user user_2

name : user_2
login : user2
enabled : on
expiration-date : December 31, 2023, 00:00
ip : 192.168.100.112
Admin@nodename# set users user user_2 emails [example@example.org]
Admin@nodename# show users user user_2

name : user_2
login : user2
enabled : on
emails : example@example.org
expiration-date : December 31, 2023, 00:00
ip : 192.168.100.112

Для удаления учётной записи пользователя используется следующая команда:

Admin@nodename# delete users user <user-login>

Также имеется возможность удаления определённой информации из учётной записи. Для удаления доступны (при удалении требуется ввод значения параметра):

- groups.
- static-addresses.
- emails.
- phones.

Настройка серверов аутентификации

Version: 8.x
Product: DCFW

Раздел **Серверы аутентификации** позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+, NTLM, SAML IDP. 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 DOMAINusername или username @domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
cache-ttl	Время жизни записей LDAP-кэша. (Опция доступна начиная с релиза UGOS 7.1.3).
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 сервера NTLM

Настройка сервера NTLM производится на уровне **users auth-server ntlm**.

Для создания сервера аутентификации NTLM используется команда со следующей структурой:

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

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя NTLM-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.

Параметр	Описание
domain	IP-адрес или доменное имя сервера NLM.

Команда для обновления информации о NTLM-сервере:

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

Команда для отображения информации о сервере NTLM:

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

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Примеры команд для создания и редактирования сервера NTLM:

```
Admin@nodename# create users auth-server ntlm name "New NTLM server" domain 10.10.0.12 enabled on
Admin@nodename# show users auth-server ntlm "New NTLM server"
```

```
name      : New NTLM server
enabled   : on
domain    : 10.10.0.12
```

```
Admin@nodename# set users auth-server ntlm "New NTLM server" description "New NTLM server description"
Admin@nodename# show users auth-server ntlm "New NTLM server"
```

```
name      : New NTLM server
description : New NTLM server description
enabled   : on
domain    : 10.10.0.12
```

Для удаления сервера:

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

Настройка сервера SAML IDP

Настройка сервера SAML IDP производится на уровне **users auth-server saml-idp**.

Для создания сервера аутентификации SAML IDP используется следующая команда:

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

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название сервера SAML IDP.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
metadata-uri	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML.
certificate	Сертификат, который будет использован в SAML-клиенте.
sso-uri	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
sso-binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-uri	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Команда для обновления информации о сервере SAML IDP:

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

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Команда для отображения информации о сервере SAML IDP:

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

Примеры команд для создания и редактирования сервера SAML IDP:

```
Admin@nodename# create users auth-server saml-idp name "New SAML IDP server" slo-uri http://logout.example.org sso-uri http://login.example.org enabled on
Admin@nodename# show users auth-server saml-idp "New SAML IDP server"
```

```
name      : New SAML IDP server
enabled   : on
certificate : Unused
sso-uri    : http://login.example.org
sso-binding : post
slo-uri    : http://logout.example.org
slo-binding : post
Admin@nodename# set users auth-server saml-idp "New SAML IDP server" description "New SAML IDP server description"
Admin@nodename# show users auth-server saml-idp "New SAML IDP server"
```

```
name      : New SAML IDP server
description : New SAML IDP server description
enabled   : on
certificate : Unused
sso-uri    : http://login.example.org
sso-binding : post
slo-uri    : http://logout.example.org
slo-binding : post
```

Для удаления сервера:

```
Admin@nodename# delete users auth-servers saml-idp <saml-idp-server-name>
```

Настройка профилей аутентификации

Technology: Identification and Authentication
Version: 8.x
Product: DCFW

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

Для создания профиля аутентификации используется следующая команда:

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

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
mfa	Указание профиля мультифакторной аутентификации (если её необходимо использовать). Для указания профиль MFA должен быть создан заранее. Подробнее о создании профилей MFA с использованием интерфейса командной строки читайте в разделе Настройка профилей MFA (мультифакторной аутентификации) .
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 авторизованного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user ; необходима повторная авторизация пользователя на Captive-портале.
max-attempts	Число неудачных попыток авторизации через Captive-портал до блокировки учётной записи пользователя.
lockout-time	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации; указывается в секундах.
auth-methods	Метод аутентификации: • local-user-auth: аутентификация по базе данных локально заведенных пользователей. • policy-accept: не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети; применяется совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy. • http-basic: аутентификация с помощью метода HTTP Basic. • ldap: аутентификация с использованием LDAP-коннектора. • radius: аутентификация с использованием RADIUS-сервера. • tacacs: аутентификация с использованием сервера TACACS+. • ntlm: аутентификация с использованием NTLM-сервера. • saml-idp: аутентификация с использованием сервера SAML IDP.

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
  ldap         : New LDAP connector
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-method>

Настройка Captive-профилей

Technology: Identification and Authentication
Version: 8.x
Product: DCFW

Настройка Captive-профилей производится на уровне **users captive-profiles**.

Для создания Captive-профиля необходимо использовать следующую команду:

Admin@nodename# create users captive-profiles <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название captive-профиля.
description	Описание captive-профиля.
auth-template	Шаблон страницы авторизации.
auth-mode	Метод идентификации, с помощью которого UserGate запомнит пользователя: - ip — Запоминать IP-адрес. После успешной авторизации пользователя через Captive-портал UserGate запоминает IP-адрес пользователя, и все последующие соединения с этого IP-адреса будут относиться к данному пользователю; устанавливается по умолчанию. - cookie — Запоминать cookie. После успешной авторизации пользователя через Captive-портал UserGate добавляет в браузер пользователя cookie, с помощью которого идентифицирует последующие соединения данного пользователя.
auth-profile	Профиль аутентификации, определяющий методы аутентификации. Подробнее о настройке профилей авторизации с использованием CLI смотрите в разделе Настройка профилей аутентификации .
custom-redirect	URL, куда будет перенаправлен пользователь после успешной авторизации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL.
use-cookie	Возможность сохранения авторизации в браузере на указанное время. Для сохранения информации используются cookie. - on. - off.
cookie-exptime	Время, на которое будет сохранена аутентификация; задаётся в часах.
enable-ldap	Возможность выбора домена AD/LDAP на странице авторизации: - on. - off.
use-captcha	Использование CAPTCHA: пользователю будет предложено ввести код, который ему будет показан на странице авторизации Captive-портала: - on. - off.
use-https	Использование HTTPS при отображении страницы авторизации Captive-портала. Необходимо иметь корректно настроенный сертификат для SSL Captive-портала. - on. - off.
notification-profile	Профиль оповещения, который будет использоваться для отсылки гостевым пользователям информации о созданном пользователе и его пароле. Подробнее о настройке профилей оповещений с использованием CLI смотрите в разделе Настройка профилей оповещений .
notification-sender	Отправитель сообщения. Указать имя (в случае использования SMPP-профиля) или email (в случае использования SMTP-профиля).
notification-subject	Тема оповещения при использовании оповещений по email.
notification-body	Тело письма. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль. Текст оповещения обособляется кавычками ("").
exp-time	Дата и время, когда учетная запись временного пользователя будет отключена. Указывается в формате: <i>yyyy-mm-ddThh:mm:ssZ</i> .
session-ttl	Продолжительность времени с момента первой авторизации временного пользователя, по истечении которого его учетная запись будет отключена; задаётся в часах.
password-len	Длина пароля 1 — 15 символов.
password-complexity	Сложность пароля: - num: использование только цифр. - alpha_num: использование букв и цифр. - alpha_num_special: использование букв, цифр и специальных символов.
ta-groups	Группа для временных пользователей, в которую будут помещены создаваемые пользователи.
captive-auth-mode	Выбор метода аутентификации Captive-профиля: - aaa — аутентификация посредством логина/пароля локального пользователя или через AAA-сервер. - pki — аутентификация посредством X.509 сертификатов.
uc-profile	Выбор профиля пользовательского сертификата при аутентификации методом pki.

Для редактирования профиля необходимо использовать следующую команду:

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

При обновлении настроек captive-профиля доступны параметры, аналогичные параметрам, доступным при создании профиля.

Команда для отображения настроек captive-профиля:

Admin@nodename# show users captive-profiles <captive-profile-name>

Пример создания и редактирования captive-профиля:

Admin@nodename# create users captive-profiles name "New captive profile" auth-profile "LDAP auth profile" captive-auth-mode aaa enable-ldap on

```
Admin@nodename# set users captive-profiles "New captive profile" use-https on
```

Для удаления профиля используется команда:

```
Admin@nodename# delete users captive-profiles <captive-profile-name>
```

Также, с использованием следующей команды, доступно удаление групп для временных пользователей (всегда должна быть указана хотя бы одна группа для временных пользователей):

```
Admin@nodename# delete users captive-profiles <captive-profile-name> ta-groups
```

Version: 8.x
Technology: Identification and Authentication
Product: DCFW

В данном разделе описана настройка правил Captive-портала; настройка производится на уровне **users captive-portal**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Параметры правил captive-портала:

Параметр	Описание
OK PASS	Действия правила Captive-портала: OK - использовать аутентификацию. PASS - не использовать аутентификацию.
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
name	Название правила captive-портала. Например: name("Captive rule example") .
desc	Описание правила captive-портала. Чтобы задать описание правила: desc("Captive portal rule example set via CLI") .
profile	Captive-профиль указывается при использовании аутентификации на captive-портале. Например, profile("Example Captive profile") . Подробнее о создании и настройке captive-профилей читайте в разделе Настройка Captive-профилей .
rule_log	Включение/отключение записи срабатывания в журнал правил: rule_log(yes) или rule_log(true). rule_log(no) или rule_log(false). Если параметр не указан, то функция журналирования отключена.
src.zone	Зона источника. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: dst.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url() ; в скобках необходимо указать название списка URL.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Пример создания и редактирования правила captive-портала с использованием UPL:

```
Admin@nodename# create users captive-portal 1 upl-rule OK \  
...profile("New captive profile") \  
...rule_log(true) \  
...name("Captive portal rule new") \  
...  
Admin@nodename# show users captive-portal 1  
% ----- 1 -----  
OK \  
  rule_log(yes) \  
  profile("New captive profile") \  
  enabled(false) \  
  id("676df2b1-03e9-42b2-8375-0b8f78c4c47c") \  
  name("Captive portal rule new")  
  
Admin@nodename# set users captive-portal 1 upl-rule OK \  
...src.zone = Trusted \  
...dst.zone = Untrusted  
...  
Admin@nodename# show users captive-portal 1  
% ----- 1 -----  
OK \  
  src.zone = Trusted \  
  dst.zone = Untrusted \  
  rule_log(yes) \  

```

```
profile("New captive profile") \
enabled(false) \
id("676df2b1-03e9-42b2-8375-0b8f78c4c47c") \
name("Captive portal rule new")
```

Настройка терминальных серверов

Technology: Identification and Authentication
Version: 8.x
Product: DCFW

В данном разделе описана настройка терминальных серверов с использованием интерфейса командной строки. Настройка производится на уровне **users terminal-servers**.

Для создания терминального сервера необходимо ввести следующую команду:

Admin@nodename# create users terminal-servers <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение терминального сервера: • on. • off.
name	Название терминального сервера.
description	Описание терминального сервера.
hosts	IP-адрес хоста. Для добавления нескольких адресов укажите их через пробел.

Команда для редактирования параметров (параметры приведены выше в таблице) терминального сервера:

Admin@nodename# set users terminal-servers <terminal-server-name> <parameter>

Команда для отображения информации о терминальном сервере:

Admin@nodename# show users terminal-servers <terminal-server-name>

Пример создания и редактирования терминального сервера:

Admin@nodename# create users terminal-servers name "Test terminal server" hosts [10.10.0.20] enabled on
Admin@nodename# show users terminal-servers "Test terminal server"

name : Test terminal server
enabled : on
hosts : 10.10.0.20

Admin@nodename# set users terminal-servers "Test terminal server" description "Test terminal server description"
Admin@nodename# show users terminal-servers "Test terminal server"

name : Test terminal server
description : Test terminal server description
enabled : on
hosts : 10.10.0.20

Команда удаления терминального сервера:

Admin@nodename# delete users terminal-servers <terminal-server-name>

Также возможно удаление отдельных хостов. Для удаления необходимо уточнить их адреса:

Admin@nodename# delete users terminal-servers <terminal-server-name> hosts

Настройка профилей MFA (мультифакторной аутентификации)

Technology: Identification and Authentication
Version: 8.x
Product: DCFW

Данный раздел описывает настройку профилей мультифакторной аутентификации с использованием CLI. Настройка профилей MFA производится на уровне **users mfa-profiles**. Можно создать несколько типов профилей:

- MFA через TOTP**: использование токена TOTP (Time-based One Time Password) в качестве второго фактора аутентификации.
- MFA через email**: использование одноразового пароля, полученного по email, в качестве второго фактора аутентификации.
- MFA через SMS**: использование одноразового пароля, полученного по SMS, в качестве второго фактора аутентификации.

Для создания профиля мультифакторной аутентификации используется команда:

```
Admin@nodename# create users mfa-profiles <parameter>
```

Команда для удаления профиля мультифакторной аутентификации:

```
Admin@nodename# delete users mfa-profiles <mfa-name>
```

Для отображения информации о всех профилях или об определённом профиле MFA используются следующие команды:

```
Admin@nodename# show users mfa-profiles  
Admin@nodename# show users mfa-profiles <mfa-name>
```

Настройка MFA через TOTP

Команда для добавления нового профиля мультифакторной аутентификации через TOTP:

```
Admin@nodename# create users mfa-profiles totp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
show-qr-code	QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента.
notification-profile	Выбор профиля оповещения.
notification-sender	Отправитель сообщения. Указать имя (в случае использования SMPP-профиля) или email (в случае использования SMTP-профиля).
notification-subject	Тема оповещения при использовании оповещений по email.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").

Команда для редактирования параметров профиля мультифакторной аутентификации через TOTP:

```
Admin@nodename# set users mfa-profiles totp <mfa-totp-name> <parameter>
```

Параметры, доступные для редактирования, совпадают с параметрами, доступными при создании профиля.

Пример создания и редактирования профиля мультифакторной аутентификации через TOTP:

```
Admin@nodename# create users mfa-profiles totp name "Test TOTP MFA profile" notification-profile pass show-qr-code on  
Admin@nodename# show users mfa-profiles totp "Test TOTP MFA profile"
```

```
name          : Test TOTP MFA profile  
show-qr-code  : on  
notification-profile : pass  
notification-body : Your authentication code is {2fa_auth_code}! Do not share it with anybody!  
Admin@nodename# set users mfa-profiles totp "Test TOTP MFA profile" description "Test TOTP MFA profile description"  
Admin@nodename# show users mfa-profiles totp "Test TOTP MFA profile"
```

```
name          : Test TOTP MFA profile  
description    : Test TOTP MFA profile description  
show-qr-code  : on  
notification-profile : pass  
notification-body : Your authentication code is {2fa_auth_code}! Do not share it with anybody!
```

Настройка MFA через email

Команда для добавления нового профиля мультифакторной аутентификации через email:

```
Admin@nodename# create users mfa-profiles smtp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
notification-profile	Выбор профиля оповещения.
notification-sender	Email отправителя сообщения.
notification-subject	Тема оповещения.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").
code-lifetime	Срок действия одноразового пароля; указывается в секундах.

Команда для редактирования параметров профиля мультифакторной аутентификации через email:

```
Admin@nodename# set users mfa-profiles smtp <mfa-email-profile> <parameter>
```

Параметры, доступные для обновления, совпадают с параметрами, доступными при создании профиля.

Пример создания и редактирования профиля мультифакторной аутентификации через email:

```
Admin@nodename# create users mfa-profiles smtp name "Test SMTP MFA profile" notification-profile "Example SMTP profile" notification-sender sender@example.org notification-subject "Test notification subj" notification-body "Test notification te  
Admin@nodename# show users mfa-profiles smtp "Test SMTP MFA profile"
```

```
name          : Test SMTP MFA profile  
notification-profile : Example SMTP profile  
notification-sender  : sender@example.org
```

```
notification-subject : Test notification subj
notification-body    : Test notification text
code-lifetime       : 60
Admin@nodename# set users mfa-profiles smtp "Test SMTP MFA profile" code-lifetime 70
Admin@nodename# show users mfa-profiles smtp "Test SMTP MFA profile"

name                : Test SMTP MFA profile
notification-profile : Example SMTP profile
notification-sender  : sender@example.org
notification-subject : Test notification subj
notification-body    : Test notification text
code-lifetime       : 70
```

Настройка MFA через SMS

Команда для добавления нового профиля мультифакторной аутентификации через SMS:

```
Admin@nodename# create users mfa-profiles smpp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
notification-sender	Имя отправителя сообщения.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будут заменена на одноразовый пароль. Текст оповещения обособляется кавычками (").
code-lifetime	Срок действия одноразового пароля; указывается в секундах.

Команда для редактирования параметров профиля мультифакторной аутентификации через SMS:

```
Admin@nodename# set users mfa-profiles smpp <mfa-sms-profile> <parameter>
```

Параметры, доступные для обновления, совпадают с параметрами, доступными при создании профиля.

Пример создания и редактирования профиля мультифакторной аутентификации через SMS:

```
Admin@nodename# create users mfa-profiles smpp name "Test SMPP MFA profile" notification-profile "Example SMPP profile" notification-sender Tes_sender notification-body "Test notification text"
Admin@nodename# show users mfa-profiles smpp "Test SMPP MFA profile"
```

```
name                : Test SMPP MFA profile
notification-profile : Example SMPP profile
notification-sender  : Tes_sender
notification-body    : Test notification text
code-lifetime       : 60
Admin@nodename# set users mfa-profiles smpp "Test SMPP MFA profile" code-lifetime 80
Admin@nodename# show users mfa-profiles smpp "Test SMPP MFA profile"
```

```
name                : Test SMPP MFA profile
notification-profile : Example SMPP profile
notification-sender  : Tes_sender
notification-body    : Test notification text
code-lifetime       : 80
```

Просмотр информации об авторизованных пользователях

Version: 8.x
Product: DCFW

Для просмотра информации об авторизованных пользователях используется следующая команда интерфейса командной строки в режиме мониторинга:

```
Admin@nodename> show user-auth
```

Для просмотра деталей аутентификационной сессии определенного пользователя используется команда:

```
Admin@nodename> show user-auth <user name>
```

Для удаления сессии определенного пользователя используется команда:

```
Admin@nodename> clear user-auth <parameter>
```

где в качестве параметра может использоваться как имя пользователя, так и его IP-адрес.

Настройка применения политик к пользователям

Version: 8.x
Product: DCFW

Для локальных пользователей устройств UserGate политики применяются автоматически.

Если пользователи проходят аутентификацию через LDAP-коннектор, NTLM или Kerberos, то для применения политик к пользователям (в случаях добавления новой LDAP-группы или пользователя в группу, создания правила и применения его к группе LDAP) необходимо сбросить сессии всех пользователей и произвести очистку кэша LDAP-записей на UserGate.

С помощью интерфейса командной строки CLI можно сбросить сессии отдельных пользователей. Команда выполняется в режиме конфигурации (configure), для выполнения команды необходимо знать IP-адрес пользователя:

```
Admin@nodename# execute termination user-sessions ip <IP-address>
```

Для очистки кэша используется команда:

```
Admin@nodename# execute cache ldap-clear
```

Настройка UserID агента

Version: 8.x
Product: DCFW

UserID агент предназначен для осуществления прозрачной аутентификации на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Microsoft Active Directory (посредством протокола WMI), Syslog (посредством стандартизированного протокола syslog [RFC 3164](#), [RFC 5424](#), [RFC 6587](#)) и RADIUS (начиная с релиза ПО 7.2.0). Подробнее о схеме работы UserID агента читайте в разделе [Пользователи и устройства](#) Руководства администратора DCFW.

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

Настройка параметров UserID агента

Общие параметры UserID агента настраиваются с помощью команды:

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

При настройке необходимо установить следующие параметры:

Параметр	Описание
polling-interval	Период опроса серверов Active Directory. Значение по умолчанию - 120 секунд.
syslog-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников.
radius-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей по RADIUS-логу. (Опция доступна начиная с релиза ПО 7.2.0).
ignore-network-list	Списки IP-адресов, события от которых будут проигнорированы агентом UserID. Запись об игнорировании источника появится в журнале Агент UserID . Список может быть создан в разделе библиотек (IP-адреса) . Данная настройка является глобальной и относится ко всем источникам.
ignore-user-list	Имена пользователей, события от которых будут проигнорированы агентом UserID. Поиск производится по Common Name (CN) пользователя AD. Данная настройка является глобальной и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID . Важно! При задании имени допустимо использовать символ астериск (*), но только в конце строки.
tcp-enabled	Протокол TCP для приёма журналов по протоколу syslog: - on; - off.
udp-enabled	Протокол UDP для приёма журналов по протоколу syslog: - on; - off.

Настройка источника событий

Microsoft Active Directory

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

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

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника (опционально).
address	Адрес Microsoft Active Directory.
protocol	Протокол доступа к AD (WMI).
login	Имя пользователя для подключения к AD.
password	Пароль пользователя для подключения к AD.
auth-profile	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах AD.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).

Для редактирования ранее созданного источника событий Active Directory предназначена команда:

Admin@nodename# set users userid-agent active-directory <source-name> <parameters>

Параметры для редактирования аналогичны параметрам, используемым при создании источника событий типа Microsoft Active Directory в таблице выше.

Для просмотра параметров ранее созданных источников событий Active Directory предназначена команда:

Admin@nodename# show users userid-agent active-directory
Admin@nodename# show users userid-agent active-directory <source-name>

Для удаления ранее созданного источника событий Active Directory предназначена команда:

Admin@nodename# delete users userid-agent active-directory <source-name>

Syslog-sender

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

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

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.

Параметр	Описание
name	Название источника.
description	Описание источника.
address	Адрес хоста, с которого UserGate будет получать события по протоколу syslog.
default-domain	Название домена, который используется для поиска найденных в журналах syslog пользователей.
timezone	Часовой пояс, установленный на источнике.
filters	Фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе Библиотеки → Syslog фильтры UserID агента . Подробнее читайте в разделе Syslog фильтры UserID агента .
auth-profile	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах syslog .
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).

Для редактирования ранее созданного источника событий отправителя syslog предназначена команда:

```
Admin@nodename# set users userid-agent syslog-sender <source-name> <parameters>
```

Параметры для редактирования аналогичны параметрам, используемым при создании источника событий типа syslog-sender в таблице выше.

Для просмотра параметров ранее созданных источников событий syslog предназначена команда:

```
Admin@nodename# show users userid-agent syslog-sender
Admin@nodename# show users userid-agent syslog-sender <source-name>
```

Для удаления ранее созданного источника событий syslog предназначена команда:

```
Admin@nodename# delete users userid-agent syslog-sender <source-name>
```

RADIUS-server

Данная опция доступна начиная с релиза ПО 7.2.0.

Для добавления RADIUS-сервера в качестве источника событий предназначена следующая команда:

```
Admin@nodename# create users userid-agent radius-server <parameters>
```

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника.
address	Адреса хостов, с которых UserGate будет получать события по протоколу RADIUS.
server-secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
default-domain	Имя домена, в котором будет производиться поиск пользователя в случае, если в запросе не было явно указано какому домену принадлежит пользователь.
attribute-for-group	Номер radius attribute type, в котором находится группа пользователя, по умолчанию группа не проверяется.
attribute-for-name	Номер radius attribute type, в котором находится имя пользователя, по умолчанию 1.
auth-profile	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах RADIUS.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).

Для редактирования ранее созданного источника событий RADIUS предназначена команда:

```
Admin@nodename# set users userid-agent radius-server <source-name> <parameters>
```

Параметры для редактирования аналогичны параметрам, используемым при создании источника событий типа RADIUS в таблице выше.

Для просмотра параметров ранее созданных источников событий RADIUS предназначена команда:

```
Admin@nodename# show users userid-agent radius-server
Admin@nodename# show users userid-agent radius-server <source-name>
```

Для удаления ранее созданного источника событий RADIUS предназначена команда:

```
Admin@nodename# delete users userid-agent radius-server <source-name>
```

