Table of Contents

Table of Contents 1
Режим администратора управляемой области 2
- Режим администратора управляемой области (Описание) 3
- Режим конфигурации администратора управляемой области 4
- Общие настройки консоли управляемой области 5
- Администраторы управляемой области 6
- Серверы аутентификации управляемой области 8
- Профили аутентификации управляемой области 11
- Каталоги пользователей управляемой области 12
- Управление межсетевыми экранами UserGate 13
- Управление устройствами UserGate DCFW 17
- Управление устройствами LogAn 21
- Управление конечными устройствами UserGate 23

Режим администратора управляемой области

Режим администратора управляемой области (Описание)

Documentation: ☑
Version: 7.x
Product: UGMC

После создания управляемой области и администратора области можно переключиться в режим управления данной областью. Для этого необходимо выйти из учетной записи администратора UGMC и заново зайти под учетной записью администратора управляемой области. Например, для входа по ssh в консоль управления областью **realm** для администратора области с учетной записью **realmadmin** необходимо указать следующее:

ssh realmadmin/realm@<UGMC-IP-address> -p 2200

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

- **configure** — переход в режим конфигурации.
- **date** — просмотр текущих даты и времени на устройстве.
- **exit** — выход из командной строки.
- **show** — просмотр версии ПО UGOS и статистики по открытым сессиям TCP, UDP, ICMP.
- **clear** — очистить статистику по открытым сессиям.

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

Режим конфигурации администратора управляемой области

Version: 7.x
Product: UGMC
Documentation: ☑

Для перехода в режим конфигурации используется команда:

realmadmin/realm@nodename> configure

После перехода в режим конфигурации командная строка будет выглядеть следующим образом:

realmadmin/realm@nodename#

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

***** — обязательное поле в командах create и ряде других команд;

+ — необязательное/вариативное поле;

> — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

<action> <level> <filter> <configuration_info>

где:

<action> — действие, которое необходимо выполнить.

<level> — уровень конфигурации; уровни соответствуют разделам веб-интерфейса управляемой области в UGMC.

<filter> — идентификатор объекта, к которому происходит обращение.

<configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • **create** — создание новых объектов. • **set** — редактирование всех объектов, а также включение различных параметров. • **show** — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня. • **delete** — удаление объекта или параметра из списка параметров. • **edit** — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой. • **end** — переход на один уровень выше. • **top** — возврат на самый верхний уровень конфигурации. • **import** — импорт конфигурации. • **export** — экспорт конфигурации. • **go** — переход в режим настройки параметров шаблона управляемых устройств. • **exit** — выход из режима конфигурации.
<level>	Уровни в командной строке повторяют веб-интерфейс консоли управления областью: • **ngfw** — соответствует разделу веб-интерфейса **NGFW**. • **endpoint** — соответствует разделу веб-интерфейса **Конечные устройства**. • **logan** — соответствует разделу веб-интерфейса **LogAn**. • **settings** — соответствует разделам веб-интерфейса **Центр управления** — **Настройки, Администраторы, Профили аутентификации**. • **users** — соответствует разделам веб-интерфейса **Центр управления** — **Каталог пользователей**.
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта.
<configuration_info>	Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. **Одиночный аргумент** — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. **Множественные аргументы** используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами.

Общие настройки консоли управляемой области

Version: 7.x
Product: UGMC
Documentation: ☑

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

realmadmin/realm@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 • **api-session-lifetime**: время ожидания сеанса администратора в секундах.
change-tracker	Настройка учета 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: realmadmin/realm@nodename# delete settings general change-tracker event-tracker-types [type1 ...]

Version: 7.x
Product: UGMC
Documentation: ☑

Администратор управляемой области может сам создать дополнительных администраторов своей области аналогично командам, описанным в разделах Настройка прав доступа профилей администраторов и Настройка учетных записей администраторов.

Настройка данного раздела производится на уровне **settings administrators**. В разделе описаны настройка настройка администраторов и их профилей.

Настройка учётных записей администраторов

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

Для создания учётной записи администратора используется следующая команда:

realmadmin/realm@nodename# create settings administrators administrators

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

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

Для редактирования параметров профиля используется команда:

realmadmin/realm@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:

realmadmin/realm@nodename# show settings administrators administrators

Для отображения информации об определённой учётной записи администратора:

realmadmin/realm@nodename# show settings administrators administrators <admin-type> <admin-login>

Настройка прав доступа профилей администраторов

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

Для создания профиля администратора используется следующая команда:

realmadmin/realm@nodename# create settings administrators profiles

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора.
description	Описание профиля администратора.
realm-permissions	Права доступа к управлению области: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.
ngfw-permissions	Права доступа к управлению устройствами NGFW: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.
ep-permissions	Права доступа к управлению конечными устройствами: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.
logan-permissions	Права доступа к управлению устройствами LogAn: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.

Для редактирования профиля используется команда:

realmadmin/realm@nodename# set settings administrators profiles <profile-name> <parameter>

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

realmadmin/realm@nodename# show settings administrators profiles

Для отображения информации об определённом профиле:

realmadmin/realm@nodename# show settings administrators profiles <profile-name>

Чтобы удалить профиль администратора:

realmadmin/realm@nodename# delete settings administrators profiles <profile-name>

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

realmadmin/realm@nodename# show settings administrators admin-sessions

Version: 7.x
Product: UGMC
Documentation: ☑

Серверы аутентификации — это внешние источники учетных записей пользователей для аутентификации в консоли управления области. Работа сервера аутентификации области аналогична работе сервера аутентификации для UGMC, отличие только в месте их использования.

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

Настройка LDAP-коннектора

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

Для создания LDAP-коннектора используется команда:

realmadmin/realm@nodename# create users auth-server ldap <parameter>

Далее необходимо указать следующие параметры:

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

Для редактирования информации о существующем LDAP-коннекторе используется команда:

realmadmin/realm@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:

realmadmin/realm@nodename# show users auth-server ldap <ldap-server-name>

Примеры команд создания и редактирования LDAP-коннектора:

```
realmadmin/realm@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
realmadmin/realm@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
realmadmin/realm@nodename# set users auth-server ldap "New LDAP connector" description "New LDAP connector description"
realmadmin/realm@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:

realmadmin/realm@nodename# delete users auth-server ldap <ldap-server-name> <parameter>

Также возможно удаление 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:

realmadmin/realm@nodename# create users auth-server radius <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.

Параметр	Описание
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:

realmadmin/realm@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:

realmadmin/realm@nodename# show users auth-server radius <radius-server-name>

Примеры команд создания и редактирования RADIUS-сервера:

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

name          : New RADIUS server
enabled       : on
addresses     :
   host    : 10.10.0.9
   port    : 1812
realmadmin/realm@nodename# set users auth-server radius "New RADIUS server" description "New RADIUS server description"
realmadmin/realm@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:

realmadmin/realm@nodename# delete users auth-server radius <radius-server-name> <parameter>

Также возможно удаление 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:

realmadmin/realm@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+:

realmadmin/realm@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+:

realmadmin/realm@nodename# show users auth-server tacacs <tacacs-server-name>

Примеры команд для создания и редактирования сервера TACACS+:

```
realmadmin/realm@nodename# create users auth-server tacacs address 10.10.0.11 name "New TACACS+ server" port 1812 secret 12345 enabled on
realmadmin/realm@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
realmadmin/realm@nodename#set users auth-server tacacs "New TACACS+ server" description "New TACACS+ server description"
realmadmin/realm@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:

realmadmin/realm@nodename# delete users auth-server tacacs <tacacs-server-name>

Профили аутентификации управляемой области

Documentation: ☑
Version: 7.x
Product: UGMC

Профиль позволяет определить набор способов аутентификации пользователей в консоли администрирования UserGate.

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

Для создания профиля аутентификации используется следующая команда:

realmadmin/realm@nodename# create users auth-profile <parameter>

Далее необходимо указать следующие параметры:

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

Команда для редактирования настроек профилей аутентификации:

realmadmin/realm@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:

```
realmadmin/realm@nodename# create users auth-profile name "New LDAP auth profile" auth-methods ldap [ "New LDAP connector" ]
realmadmin/realm@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
realmadmin/realm@nodename# set users auth-profile "New LDAP auth profile" description "New LDAP auth profile description"
realmadmin/realm@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 удаление всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

realmadmin/realm@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):

realmadmin/realm@nodename# delete users auth-profile <auth-profile-name> auth-methods <auth-metod>

Каталоги пользователей управляемой области

Version: 7.x
Product: UGMC
Documentation: ☑

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

ПримечаниеПри настройке политик безопасности серверы аутентификации, настраиваемые в шаблонах управляемых устройств, не используются для добавления пользователей и групп в правила.

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

Для создания каталога используется команда:

realmadmin/realm@nodename# create users catalogs ldap <parameter>

Далее необходимо указать следующие параметры:

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

Для редактирования информации о существующем каталоге используется команда:

realmadmin/realm@nodename# set users catalogs ldap <ldap-server-name> <parameter>

Параметры, доступные для обновления, аналогичны параметрам создания каталога.

Команда для отображения информации о каталоге пользователей:

realmadmin/realm@nodename# show users catalogs ldap <ldap-server-name>

Для удаления каталога используется команда:

realmadmin/realm@nodename# delete users catalogs ldap <ldap-server-name> <parameter>

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

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

Version: 7.x
Product: UGMC
Documentation: ☑

В интерфейсе командной строки UserGate Management Center (UGMC) администраторы управляемой области могут централизованно настраивать параметры межсетевых экранов UserGate. Для этого в режиме конфигурации необходимо выполнить следующее:

1) настроить параметры шаблонов UserGate NGFW;

2) создать группы шаблонов UserGate NGFW;

3) добавить управляемые устройства UserGate NGFW.

Настройка параметров шаблонов UserGate NGFW

Перед настройкой параметров шаблонов UserGate NGFW необходимо создать шаблоны устройств. Рекомендуется создавать отдельные шаблоны для разных категорий параметров, например такие, как шаблон сетевых параметров, шаблон правил межсетевого экрана, шаблон правил фильтрации или шаблон библиотек. Это упростит дальнейшую работу с шаблонами при их объединении в группы. В таблице ниже приведены команды, которые вы можете использовать при создании шаблонов UserGate NGFW.

Действие	Команда	Пример ввода команды
Создание шаблона	create ngfw template name <название шаблона> description <описание шаблона>	realmadmin/realm@nodename# create ngfw template name example_template_1 description for_example_template
Просмотр шаблона	show ngfw template <название шаблона>	realmadmin/realm@nodename# show ngfw template example_template_1
Просмотр всех шаблонов	show ngfw template	realmadmin/realm@nodename# show ngfw template
Изменение названия и описания шаблона	set ngfw template <название шаблона> name <новое название шаблона> description <новое описание шаблона>	realmadmin/realm@nodename# set ngfw template example_template_1 name example_template_2 description for_testing_templete
Удаление шаблона	delete ngfw template <название шаблона>	realmadmin/realm@nodename# delete ngfw template test_template_2

После создания шаблона вы можете настроить его параметры. Эти параметры распространятся на все управляемые устройства UserGate NGFW, к которым будет применен шаблон в составе группы.

При настройке параметров шаблона следует учитывать следующее:

- Значения параметров в шаблоне имеют более высокий приоритет, чем указанные администратором UserGate NGFW локально. Если значение параметра не указано ни в шаблоне, ни на стороне межсетевого экрана, то будет использоваться значение по умолчанию.
- После применения шаблона к управляемым устройствам администраторы могут изменять базовые параметры и параметры сетевых интерфейсов локально на каждом межсетевом экране. Подробная информация об этих параметрах приведена в разделах «Общие настройки» и «Настройка интерфейсов» Руководства администратора UserGate NGFW.
- При настройке параметров сетевых интерфейсов в шаблоне первым физическим интерфейсом, доступным для конфигурирования, будет port1. Интерфейс port0 используется для подключения UserGate NGFW к UGMC. Параметры этого интерфейса настраиваются администратором UserGate NGFW при первоначальной настройке продукта. Локально на UserGate NGFW также можно сконфигурировать и другие сетевые интерфейсы, для этого в параметрах интерфейса шаблона вам необходимо указать свойство on-device (или on-device on).
- Библиотеки элементов шаблона (например, библиотеки IP-адресов, URL-списков, а также типов контента) по умолчанию не содержат данных, в отличие от библиотек UserGate NGFW. Перед настройкой политик в шаблоне необходимо добавить элементы библиотек. Данные библиотек не синхронизируются: если добавленные элементы не используются в политиках шаблона, то они не будут добавлены в библиотеки UserGate NGFW.

Чтобы настроить параметры шаблона UserGate NGFW:

Перейдите в режим настройки параметров шаблона, выполнив команду:

go ngfw-template <название шаблона>

Например:

realmadmin/realm@nodename# go ngfw-template test_template_2

Для настройки параметров шаблона вы можете использовать команды, которые приведены в разделе « Интерфейс командной строки» Руководства администратора UserGate NGFW.

Правила политик в шаблоне не переопределяют правила, созданные администраторами межсетевых экранов UserGate NGFW локально, а добавляются к ним в виде преправил и постправил. Подробная информация о создании правил политик приведена в разделе UserGate Policy Language Руководства администратора UserGate NGFW.

Кроме того, при создании правила в шаблоне вы можете указывать позицию правила относительно преправил или постправил в списке, используя свойства mc_pre и mc_post соответственно. Ниже приведен пример создания постправила:

```
realmadmin/realm@nodename# create network-policy firewall 1 upl-rule \
...DENY
...enabled(true)
...src.zone = Trusted
...dst.zone = Untrusted
...user = unknown
...rule_log(session)
...mc_post
...name("Example of post rule name")
```

Созданное правило отобразится на первой позиции списка постправил. Это правило запрещает передачу трафика из зоны Trusted в зону Untrusted неидентифицированным пользователям.

Создание групп шаблонов UserGate NGFW

После создания шаблонов UserGate NGFW их необходимо объединить в группы. Группа шаблонов позволяет создать единую конфигурацию параметров, которая применяется к одному или нескольким управляемым устройствам. Эта конфигурация формируется в результате слияния параметров всех шаблонов, входящих в группу, с учетом их расположения. В таблице ниже приведены команды, которые вы можете использовать при создании группы шаблонов UserGate NGFW.

Действие	Команда	Пример ввода команды
Создание группы	create ngfw groups name <название группы> description <описание группы> templates [<название шаблона 1> ... <название шаблона n>]	realmadmin/realm@nodename# create ngfw groups name example_group_1 description for_example_group templates [example_template_1]
Изменение названия, описания и набора шаблонов, входящих в группу	set ngfw groups <название группы> name <новое название группы> description <новое описание группы> templates [<название шаблона 1> ... <название шаблона n>]	realmadmin/realm@nodename# set ngfw groups example_group_1 name example_group_2 description for_testing_group
Добавление шаблонов, входящих в группу	set ngfw groups <название группы> templates [<название шаблона 1> ... <название шаблона n>]	realmadmin/realm@nodename# set ngfw groups example_group_2 templates [example_template_2]
Удаление шаблонов, входящих в группу	delete ngfw groups <название группы> templates [<название шаблона 1> ... <название шаблона n>]	realmadmin/realm@nodename# delete ngfw groups example_group_2 templates [example_template_2]

Действие	Команда	Пример ввода команды
Просмотр группы	show ngfw groups <название группы>	realmadmin/realm@nodename# show ngfw groups example_group_2
Просмотр всех групп	show ngfw groups	realmadmin/realm@nodename# show ngfw groups
Удаление группы	delete ngfw groups <название группы>	realmadmin/realm@nodename# delete ngfw groups example_group_2

После создания групп шаблонов вы можете добавить управляемые устройства.

Добавление управляемых устройств UserGate NGFW

Под управляемым устройством понимается логический объект, созданный в управляемой области, которому соответствует реальный UserGate NGFW, подключенный к UGMC. Каждый такой объект во включенном состоянии использует одну лицензию на управляемое устройство.

Перед добавлением управляемого устройства UserGate NGFW вам необходимо на сервере UGMC в свойствах зоны, к которой подключен UserGate NGFW, разрешить использование сервиса **UserGate Management Center**.

Для этого под учетной записью администратора UGMC в интерфейсе командной строки в режиме конфигурации выполните команду:

set network zone <название зоны> enabled-services [Management]

Например:

Admin/system@nodename# set network zone example_zone enabled-services [Management]

Для добавления управляемого устройства UserGate NGFW необходимо:

1) создать устройство в управляемой области UGMC;

2) подключить UserGate NGFW к управляемому устройству.

Создание управляемого устройства

ПримечаниеИнструкция выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы создать управляемое устройство:

1. Выполните команду:

create ngfw devices <параметры управляемого устройства>

Укажите параметры управляемого устройства.

Параметр	Описание
enabled	Состояние: • on — включено; • off — выключено
name	Название
description	Описание
templates-group	Название группы шаблонов, параметры которой должны применяться к управляемому устройству
sync-mode	Режим синхронизации параметров между группой шаблонов и управляемым устройством: • auto — автоматическая синхронизация; • disabled — синхронизация выключена; • manual — запуск синхронизации вручную. В процессе синхронизации к UserGate NGFW применяется конфигурация параметров группы шаблонов. По умолчанию указан автоматический режим. В этом режиме параметры UserGate NGFW синхронизируются с конфигурацией параметров при каждом ее изменении. При необходимости синхронизацию можно отключить. Это может понадобиться, например, если нужно одновременно изменить параметры нескольких шаблонов группы. В этом случае вы можете применить сразу все внесенные изменения, выполнив синхронизацию вручную. Синхронизация для всех управляемых устройств выполняется по команде execute ngfw devices resync (действие доступно в версии 7.4.0 и выше)

Например:

realmadmin/realm@nodename# create ngfw devices enabled on name example_name templates-group example_group sync-mode auto

2. Получите идентификатор созданного управляемого устройства:

show ngfw devices <название управляемого устройства>

Например:

realmadmin/realm@nodename# show ngfw devices example_name

```
name                : example_name
enabled             : on
device-code           : 9W8W14UC
templates-group       : example_group
sync-mode           : auto
...
```

Идентификатор управляемого устройства отобразится в выводе команды в параметре device-code. Этот идентификатор потребуется для подключения межсетевого экрана UserGate NGFW к управляемому устройству.

Подключение UserGate NGFW к управляемому устройству

Вы можете подключить UserGate NGFW к управляемому устройству при первоначальной настройке продукта, а также при его дальнейшем использовании (см. инструкцию ниже).

ПримечаниеИнструкция выполняется администратором UserGate NGFW в интерфейсе командной строки в режиме конфигурации.

Чтобы подключить UserGate NGFW к управляемому устройству:

Выполните команду:

set settings general management-center mc-address <IP-адрес UGMC> device-code <идентификатор управляемого устройства> enabled on

Например:

Admin@ngfw-nodename# set settings general management-center mc-address 192.0.2.4 device-code 9W8W14UC enabled on

Вы можете проверить подключение на стороне UGMC.

ПримечаниеИнструкция выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы проверить подключение UserGate NGFW к управляемому устройству:

Выполните команду:

show ngfw devices <название управляемого устройства>

Например:

realmadmin/realm@nodename# show ngfw devices example_name

Параметры подключения отобразятся в выводе команды.

Кластеризация UserGate NGFW

UserGate Management Center позволяет объединять межсетевые экраны UserGate NGFW в кластер конфигурации. Используя шаблоны устройств, вы можете применять одинаковые параметры на всех узлах этого кластера. Кроме того, в UGMC вы можете создать один или несколько кластеров отказоустойчивости на базе узлов кластера конфигурации.

Создание кластера конфигурации

Чтобы создать кластер конфигурации:

1. Выполните первоначальную настройку на первом узле кластера.

2. Настройте на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера (см. раздел « Настройки сети» Руководства администратора UserGate NGFW). В параметре enabled-services должны быть указаны значения ha и Admin Console, разрешающие доступ к соответствующим сервисам.

3. Укажите IP-адрес, который будет использоваться для связи первого узла с другими узлами кластера (см. раздел « Настройка кластеров» Руководства администратора UserGate NGFW).

4. Сгенерируйте секретный код для первого узла кластера (см. раздел « Настройка кластеров» Руководства администратора UserGate NGFW).

5. Подключите первый узел кластера к UGMC в качестве управляемого устройства. При подключении к UGMC каждому узлу кластера присваивается уникальный идентификатор вида node_n, где n — порядковый номер узла.

6. Добавьте в кластер конфигурации второй и последующие узлы, выполнив первоначальную настройку на каждом узле.

7. Настройте параметры узлов кластера. Вы можете выполнить настройку локально на каждом узле или настроить параметры в шаблонах UGMC.

Создание кластера отказоустойчивости

Узлы кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий режимы:

- «активный — активный», в котором один из межсетевых экранов выступает в роли мастер-узла, распределяющего трафик на все остальные узлы кластера;
- «активный — пассивный», в котором один из межсетевых экранов выступает в роли мастер-узла, обрабатывающего транзитный трафик пользователей, а остальные — в качестве резервных, которые находятся в состоянии готовности начать обработку трафика.

Перед созданием кластера отказоустойчивости нужно проверить, что:

- Создан кластер конфигурации.
- На каждом из узлов кластера созданы сетевые интерфейсы, управляемые UGMC. Вы можете назначать виртуальные IP-адреса только интерфейсам, созданным в шаблоне.
- Выполняются требования аналогичные тем, которые предъявляются к узлам при создании кластера отказоустойчивости без использования UGMC (см. раздел « Кластеризация и отказоустойчивость» Руководства администратора UserGate NGFW).

ПримечаниеПеред выполнением инструкции должны быть созданы шаблон сетевых зон и шаблон кластера отказоустойчивости. Инструкция выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы создать кластер отказоустойчивости:

1. Разрешите сервис VRRP для всех сетевых зон, где планируется добавлять кластерный виртуальный IP-адрес, последовательно выполнив команды:

go ngfw-template <название шаблона сетевых зон>

set network zone name <название зоны> enabled-services [VRRP]

Например:

realmadmin/realm@nodename# go ngfw-template template_for_zones

realmadmin/realm@nodename# set network zone name zone_name enabled-services [VRRP]
Template: template_for_zones

2. Настройте параметры кластера отказоустойчивости, последовательно выполнив команды:

go ngfw-template <название шаблона кластера отказоустойчивости>

create settings device-mgmt ha-clusters <параметры кластера отказоустойчивости>

Укажите параметры кластера отказоустойчивости.

Параметр	Описание
enabled	Состояние: • on — включен; • off — выключен
name	Название
description	Описание
mode	Режим работы: • active-active — «активный — активный»; • active-passive — «активный — пассивный»
session-sync	Режим синхронизации пользовательских TCP-сессий: • on — синхронизация включена; • off — синхронизация выключена; • ha-cluster-id: <идентификатор кластера отказоустойчивости> — если в одном кластере конфигурации создано несколько кластеров отказоустойчивости, то выполняется автоматическая синхронизация сессий с использованием мультикастового адреса (кроме сессий, использующих прокси-сервер). Идентификатор кластера отказоустойчивости — уникальное для каждого кластера значение от 0 до 8

Параметр	Описание
session-sync-all	Режим синхронизации всех пользовательских сессий: • on — синхронизация включена; • off — синхронизация выключена
excluded-sync-ips	IP-адреса, с которыми не будут синхронизироваться пользовательские сессии
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID). Уникален для каждого VRRP-кластера в локальной сети. Если в сети нет сторонних VRRP-кластеров рекомендуется оставить значение по умолчанию
nodes	Названия узлов кластера конфигурации для их объединения в кластер отказоустойчивости
virtual-ips <virtual-ips-filter> <virtual-ip-info>	Виртуальные IP-адреса кластера и их назначение сетевым интерфейсам на узлах кластера. Параметр virtual-ips-filter может принимать значения: • new — создание нового виртуального IP-адреса; • <IP-адрес> — изменение существующего виртуального IP-адреса. Параметр virtual-ip-info может принимать значения: • ip <IP-адрес/маска подсети> — назначение виртуального IP-адреса интерфейсу; • ha-interfaces <название узла кластера/название интерфейса> — выбор интерфейса на узле кластера

Version: 7.x
Product: UGMC

Начиная с версии 7.5.0 в интерфейсе командной строки UserGate Management Center (UGMC) администраторы управляемой области могут централизованно управлять подключенными UserGate DCFW. Для этого в режиме конфигурации необходимо выполнить следующее:

1) настроить параметры шаблонов UserGate DCFW;

2) создать группу шаблонов UserGate DCFW;

3) настроить интеграцию UserGate DCFW с UGMC.

Подробнее об объектах, используемых в управляемой области UGMC, таких как шаблоны, группы шаблонов и управляемые устройства — в разделе «Шаблоны и группы шаблонов».

Настройка параметров шаблонов UserGate DCFW

Перед настройкой параметров шаблонов UserGate DCFW необходимо создать шаблоны устройств. Рекомендуется создавать отдельные шаблоны для разных категорий параметров, например такие, как шаблон сетевых параметров или шаблон библиотек. Это упростит дальнейшую работу с шаблонами при их объединении в группы.

В таблице ниже приведены команды, которые вы можете использовать при создании шаблонов UserGate DCFW.

Действие	Команда	Пример ввода команды
Создание шаблона	create dcfw template name <название шаблона> description <описание шаблона>	realmadmin/realm@nodename# create dcfw template name "example template 1" description "for example template"
Просмотр шаблона	show dcfw template <название шаблона>	realmadmin/realm@nodename# show dcfw template "example template 1"
Просмотр всех шаблонов	show dcfw template	realmadmin/realm@nodename# show dcfw template
Изменение названия и описания шаблона	set dcfw template <название шаблона> name <новое название шаблона> description <новое описание шаблона>	realmadmin/realm@nodename# set dcfw template "example template 1" name "example template 2" description "for testing templete"
Удаление шаблона	delete dcfw template <название шаблона>	realmadmin/realm@nodename# delete dcfw template "test template 2"

После создания шаблона вы можете перейти к настройке его параметров. Параметры шаблона распространятся на все управляемые устройства UserGate DCFW, к которым будет применен шаблон в составе группы.

При настройке параметров шаблона UserGate DCFW следует учитывать следующее:

- Значения параметров в шаблоне имеют более высокий приоритет, чем указанные администратором UserGate DCFW локально. Если значение параметра не указано ни в шаблоне, ни на стороне UserGate DCFW, будет использоваться значение по умолчанию.
- После применения шаблона к управляемым устройствам администраторы могут изменять базовые параметры и параметры сетевых интерфейсов локально на каждом UserGate DCFW. Подробная информация об этих параметрах приведена в разделах «Настройка устройства» и «Интерфейсы» Руководства администратора UserGate DCFW.
- При настройке параметров сетевых интерфейсов в шаблоне невозможно конфигурировать интерфейс port0. Первым физическим интерфейсом, доступным для настройки в шаблоне, будет port1.

  Параметры интерфейса port0 настраиваются администратором UserGate DCFW при первоначальной настройке продукта. По умолчанию этот интерфейс используется для подключения UserGate DCFW к UGMC.

  При необходимости можно сконфигурировать сетевые интерфейсы локально на UserGate DCFW, для этого в параметрах интерфейса шаблона должно быть указано свойство on-device (или on-device on).

  Если вы создаете интерфейс в шаблоне, этот интерфейс автоматически будет добавлен в UserGate DCFW. Удаление интерфейса из шаблона не удаляет интерфейс на межсетевом экране. Если требуется удалить интерфейс на межсетевом экране, необходимо сделать это вручную.
- Библиотеки элементов шаблона (например, библиотеки IP-адресов, URL-списков, а также типов контента) по умолчанию не содержат данных, в отличие от библиотек UserGate DCFW (подробнее — в разделе «Библиотеки элементов» Руководства администратора UserGate DCFW). Перед настройкой политик в шаблоне необходимо добавить элементы библиотек.

  Важно!Данные библиотек не синхронизируются: если добавленные элементы не используются в политиках шаблона, они не будут добавлены в библиотеки UserGate DCFW. Поэтому, чтобы на управляемых устройствах отображались, например, списки IP-адресов, созданные в шаблоне, необходимо предварительно добавить эти списки в правила политик шаблона.
  ПримечаниеКорректность работы проприетарных сигнатур СОВ и приложений зависит от актуальности библиотек для этих сигнатур — рекомендуется проверять актуальность библиотек после обновления UGMC или восстановления его параметров. Если по какой-либо причине библиотеки не обновились автоматически, их можно обновить вручную. Действие выполняется администратором UGMC в разделе «Центр управления» ➜ «Настройки» ➜ «Обновления библиотек».

Чтобы настроить параметры шаблона UserGate DCFW:

Перейдите в режим настройки параметров шаблона, выполнив команду:

go dcfw-template <название шаблона>

Например:

realmadmin/realm@nodename# go dcfw-template "test template 2"

Для настройки параметров шаблона вы можете использовать команды, которые приведены в разделе «Интерфейс командной строки» Руководства администратора UserGate DCFW.

ПримечаниеВы можете выйти из режима настройки параметров шаблона, выполнив команду go realm-settings.

Правила политик в шаблоне не переопределяют правила, созданные администраторами межсетевых экранов UserGate DCFW локально, а добавляются к ним в виде преправил и постправил. Подробная информация о создании правил политик межсетевых экранов UserGate приведена в разделе UserGate Policy Language Руководства администратора UserGate NGFW.

Кроме того, при создании правила в шаблоне вы можете указывать позицию правила относительно преправил или постправил в списке, используя свойства mc_pre и mc_post соответственно. Ниже приведен пример создания постправила.

```
realmadmin/realm@nodename# create network-policy firewall 1 upl-rule \
...DENY
...enabled(true)
...src.zone = Trusted
...dst.zone = Untrusted
...user = unknown
...rule_log(session)
...mc_post
...name("Example of post rule name")
```

Созданное правило отобразится на первой позиции списка постправил. Это правило запрещает передачу трафика из зоны Trusted в зону Untrusted неидентифицированным пользователям.

Создание групп шаблонов UserGate DCFW

После создания шаблонов UserGate DCFW их необходимо объединить в группы. Группа шаблонов позволяет создать единую конфигурацию параметров, которая применяется к одному или нескольким управляемым устройствам. Эта конфигурация формируется в результате слияния параметров всех шаблонов, входящих в группу, с учетом их расположения.

В таблице ниже приведены команды, которые вы можете использовать при создании группы шаблонов UserGate DCFW.

Действие	Команда	Пример ввода команды

Действие	Команда	Пример ввода команды
Создание группы	create dcfw groups name <название группы> description <описание группы> templates [<название шаблона 1> ... <название шаблона n>]	realmadmin/realm@nodename# create dcfw groups name "example group 1" description "for example group" templates ["example template 1"]
Изменение названия, описания и набора шаблонов, входящих в группу	set dcfw groups <название группы> name <новое название группы> description <новое описание группы> templates [<название шаблона 1> ... <название шаблона n>]	realmadmin/realm@nodename# set dcfw groups "example group 1" name "example group 2" description "for testing group"
Добавление шаблонов, входящих в группу	set dcfw groups <название группы> templates [<название шаблона 1> ... <название шаблона n>]	realmadmin/realm@nodename# set dcfw groups "example group 2" templates ["example template 2" "example template 3"]
Удаление шаблонов, входящих в группу	delete dcfw groups <название группы> templates [<название шаблона 1> ... <название шаблона n>]	realmadmin/realm@nodename# delete dcfw groups "example group 2" templates ["example template 2"]
Просмотр группы	show dcfw groups <название группы>	realmadmin/realm@nodename# show dcfw groups "example group 2"
Просмотр всех групп	show dcfw groups	realmadmin/realm@nodename# show dcfw groups
Удаление группы	delete dcfw groups <название группы>	realmadmin/realm@nodename# delete dcfw groups "example group 2"

Шаблоны применяются в порядке их расположения в группе. Вы можете изменять позицию шаблона с помощью следующих параметров.

Параметр	Описание	Пример ввода команды
edge-position	Перемещение шаблона: • top — в начало группы; • bottom — в конец группы	realmadmin/realm@nodename# set dcfw groups "example group 2" templates ["example template 2"] edge-position top
after	Перемещение шаблона на одну позицию после другого шаблона	realmadmin/realm@nodename# set dcfw groups "example group 2" templates ["example template 2"] after "example template 3"
before	Перемещение шаблона на одну позицию перед другим шаблоном	realmadmin/realm@nodename# set dcfw groups "example group 2" templates ["example template 2"] before "example template 3"

После создания группы шаблонов вы можете перейти к настройке интеграции UserGate DCFW с UGMC.

Настройка интеграции UserGate DCFW с UGMC

Настройка интеграции с UGMC осуществляется путем создания в управляемой области логического объекта — устройства, к которому будут привязаны реальные UserGate DCFW при их подключении к UGMC. Каждый такой логический объект во включенном состоянии использует одну лицензию на управляемое устройство.

С помощью одного устройства, созданного в управляемой области, вы можете настроить интеграцию с UGMC одиночного UserGate DCFW или кластера межсетевых экранов. Для UserGate DCFW, объединенных в кластер, достаточно подключить к UGMC первый узел, остальные узлы будут подключены автоматически при их добавлении в кластер.

Для настройки интеграции UserGate DCFW с UGMC необходимо:

1) создать устройство в управляемой области;

2) подключить UserGate DCFW к UGMC.

Все UserGate DCFW, для которых настроена интеграция с UGMC, называются управляемыми устройствами.

Создание устройства в управляемой области

ПримечаниеИнструкция ниже выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы создать устройство в управляемой области:

1. Выполните команду:

create dcfw devices <параметры устройства>

Укажите параметры устройства.

Параметр	Описание
enabled	Состояние: • on — включено; • off — выключено
name	Название
description	Описание
templates-group	Название группы шаблонов, параметры которой должны применяться к подключенным UserGate DCFW
sync-mode	Режим синхронизации параметров между группой шаблонов и подключенными UserGate DCFW: • auto — автоматическая синхронизация; • disabled — синхронизация выключена; • manual — запуск синхронизации вручную. В процессе синхронизации к управляемым устройствам применяется конфигурация параметров группы шаблонов. По умолчанию указан автоматический режим. В этом режиме параметры UserGate DCFW синхронизируются с конфигурацией параметров при каждом ее изменении. При необходимости синхронизацию можно отключить. Это может понадобиться, например, если нужно одновременно изменить параметры нескольких шаблонов группы. В этом случае вы можете применить сразу все внесенные изменения, выполнив синхронизацию вручную. Синхронизация для всех управляемых устройств выполняется с помощью команды execute dcfw devices resync

Например:

```
realmadmin/realm@nodename# create dcfw devices enabled on name "example name" templates-group "example group" sync-mode auto
```

2. Получите код для подключения созданного устройства к UGMC:

show dcfw devices <название управляемого устройства>

Например:

```
realmadmin/realm@nodename# show dcfw devices "example name"

name                    : example name
enabled                 : on
device-code               : 9W8W14UC
templates-group             : example group
sync-mode               : auto
...
```

Код для подключения межсетевого экрана UserGate DCFW к UGMC отобразится в выводе команды в параметре device-code.

Подключение UserGate DCFW к UGMC

Вы можете подключить UserGate DCFW к UGMC при первоначальной настройке межсетевого экрана, а также при его дальнейшем использовании (см. инструкцию ниже).

Перед выполнением инструкции необходимо в свойствах зоны для подключения UserGate DCFW разрешить использование сервиса **UserGate Management Center**. Для этого под учетной записью администратора UGMC в интерфейсе командной строки в режиме конфигурации выполните команду:

set network zone <название зоны> enabled-services [Management]

Например:

```
Admin/system@nodename# set network zone "example zone" enabled-services [ Management ]
```

ПримечаниеИнструкция выполняется администратором UserGate DCFW в интерфейсе командной строки в режиме конфигурации.

Чтобы подключить UserGate DCFW к UGMC:

Выполните команду:

set settings general management-center mc-address <IP-адрес UGMC> device-code <код для подключения, сгенерированный в UGMC> enabled on

Например:

```
Admin@dcfw-nodename# set settings general management-center mc-address 192.0.2.4 device-code 9W8W14UC enabled on
```

Вы можете проверить подключение на стороне UGMC.

ПримечаниеИнструкция выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы проверить подключение UserGate DCFW к UGMC:

Выполните команду:

show dcfw devices <название устройства, созданного в управляемой области>

Например:

```
realmadmin/realm@nodename# show dcfw devices "example name"
```

Параметры подключения отобразятся в выводе команды.

Кластеризация UserGate DCFW

Вы можете объединять два или более UserGate DCFW (узлов) в кластер конфигурации и настраивать на них единые параметры для работы с трафиком, используя шаблоны.

Между узлами кластера конфигурации выполняется синхронизация параметров, что обеспечивает бесперебойную фильтрацию и обработку сетевого трафика при недоступности одного из узлов.

Кроме того, вы можете объединять до четырех узлов кластера конфигурации в кластер отказоустойчивости. Этот кластер поддерживает следующие режимы работы:

- «активный — активный», в котором один из межсетевых экранов выполняет роль основного узла, распределяя трафик на все остальные узлы кластера;
- «активный — пассивный», в котором обработку транзитного трафика выполняет основной узел, при сбоях в работе этого узла трафик перенаправляется на резервные узлы кластера.

В параметрах кластера отказоустойчивости вы можете настроить синхронизацию сессий между узлами (исключение составляют сессии, использующие прокси-сервер). Это может понадобиться для кластера в режиме «активный — пассивный», например при недоступности основного узла вы можете переключиться на резервный узел без потери установленных сессий.

На базе одного кластера конфигурации может быть создано несколько кластеров отказоустойчивости. В этом случае каждому кластеру отказоустойчивости вы можете присвоить уникальный мультикаст-идентификатор, который будет использоваться для синхронизации сессий между узлами.

Создание кластера конфигурации

Чтобы создать кластер конфигурации:

1. Выполните первоначальную настройку на первом узле кластера.

2. Настройте на первом узле кластера зону, через интерфейсы которой будет выполняться репликация параметров между узлами кластера (см. раздел « Настройки сети» Руководства администратора UserGate DCFW). В параметре enabled-services должны быть указаны значения ha и Admin Console, разрешающие доступ к соответствующим сервисам.

3. Укажите IP-адрес, который будет использоваться для связи первого узла с другими узлами кластера (см. раздел « Настройка кластеров» Руководства администратора UserGate DCFW).

4. Сгенерируйте секретный код для первого узла кластера (см. раздел « Настройка кластеров» Руководства администратора UserGate DCFW).

5. Подключите первый узел кластера к UGMC. В результате подключения узлу будет автоматически присвоен идентификатор node_1.

6. Добавьте дополнительные узлы в кластер конфигурации, выполнив первоначальную настройку на каждом из них. В результате на дополнительные узлы кластера будут автоматически реплицированы параметры, настроенные на первом узле.

Создание кластера отказоустойчивости

Перед созданием кластера отказоустойчивости:

1. Создайте кластер конфигурации (см. инструкцию выше).

2. Проверьте, что:

- Выполняются требования аналогичные тем, что предъявляются к узлам при создании кластера отказоустойчивости без использования UGMC (см. раздел « Кластеризация и отказоустойчивость» Руководства администратора UserGate DCFW).
- На каждом из узлов кластера созданы сетевые интерфейсы, управляемые UGMC. Вы можете назначать виртуальные IP-адреса только тем интерфейсам, которые созданы в шаблоне.

ПримечаниеПеред выполнением инструкции необходимо убедиться, что созданы шаблон сетевых зон и шаблон кластера отказоустойчивости. Инструкция ниже выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы создать кластер отказоустойчивости:

1. В режиме настройки параметров шаблона сетевых зон разрешите доступ к сервису VRRP тем зонам, для которых планируете добавлять кластерный виртуальный IP-адрес. Для этого последовательно выполните команды:

go dcfw-template <название шаблона сетевых зон>

set network zone name <название зоны> enabled-services [VRRP]

Например:

realmadmin/realm@nodename# go dcfw-template "template for zones"

realmadmin/realm@nodename# set network zone name "example zone name" enabled-services [VRRP]
Template: template for zones

ПримечаниеВы можете выйти из режима настройки параметров шаблона, выполнив команду go realm-settings.

2. Настройте параметры кластера отказоустойчивости, последовательно выполнив команды:

go dcfw-template <название шаблона кластера отказоустойчивости>

create settings device-mgmt ha-clusters <параметры кластера отказоустойчивости>

Укажите параметры кластера отказоустойчивости.

Параметр	Описание
enabled	Состояние: • on — включен; • off — выключен
name	Название
description	Описание
mode	Режим работы: • active-active — «активный — активный»; • active-passive — «активный — пассивный»
session-sync	Режим синхронизации пользовательских TCP-сессий: • on — синхронизация включена; • off — синхронизация выключена; • ha-cluster-id: <мультикаст-идентификатор кластера отказоустойчивости> — если в локальной сети присутствуют другие отказоустойчивые кластеры, можно указать уникальный мультикаст-идентификатор создаваемого кластера (значение от 0 до 8), который будет использоваться для синхронизации сессий между узлами
session-sync-all	Режим синхронизации всех пользовательских сессий, включая UDP- и ICMP-трафик: • on — синхронизация включена; • off — синхронизация выключена
excluded-sync-ips	IP-адреса, привязанные к тем пользовательским сессиям, которые требуется исключить из синхронизации
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID) уникальный для каждого VRRP-кластера в локальной сети. Если в сети отсутствуют сторонние VRRP-кластеры, рекомендуется оставить значение по умолчанию
nodes	Идентификаторы узлов кластера конфигурации, которые требуется объединить в кластер отказоустойчивости
virtual-ips <virtual-ips-filter> <virtual-ip-info>	Назначение виртуальных IP-адресов интерфейсам на узлах кластера отказоустойчивости. Параметр virtual-ips-filter может принимать значения: • new — создание нового виртуального IP-адреса; • <IP-адрес> — изменение существующего виртуального IP-адреса. Параметр virtual-ip-info может принимать значения: • ip <IP-адрес / маска подсети> — назначение виртуального IP-адреса интерфейсу; • ha-interfaces <название узла кластера / название интерфейса> — выбор интерфейса на узле кластера

Version: 7.x
Product: UGMC
Documentation: ☑

Для централизованного управления устройствами LogAn в управляемой области необходимо создать шаблоны и группы шаблонов, описывающие настройки LogAn, затем добавить управляемые устройства LogAn и применить к ним созданные ранее шаблоны.

В интерфейсе CLI создание шаблонов и групп шаблонов, а также добавление управляемых устройств LogAn происходит на уровне **logan**.

Шаблоны устройств

Для создания шаблона устройств LogAn используется команда:

realmadmin/realm@nodename# create logan template <name, description>

Для редактирования названия/описания шаблона устройств LogAn используется команда:

realmadmin/realm@nodename# set logan template <name, description>

Для просмотра созданных ранее шаблонов устройств LogAn используется команда:

realmadmin/realm@nodename# show logan template <template-name>

Для удаления созданных ранее шаблонов устройств LogAn используется команда:

realmadmin/realm@nodename# delete logan template <template-name>

После создания шаблона устройств LogAn можно начать производить настройку его параметров. Для этого необходимо перейти в режим настройки параметров шаблона управляемых устройств LogAn следующей командой:

realmadmin/realm@nodename# go logan-template <template-name>

В режиме настройки параметров шаблона доступны те же команды настройки параметров LogAn, которые определены в разделе Интерфейс командной строки Руководства администратора LogAn.

При настройке параметров следует придерживаться следующих правил:

1. Если значение настройки не определено в шаблоне, то ничего передаваться в LogAn не будет. В данном случае в LogAn будет использована либо настройка по умолчанию, либо настройка, которую указал локальный администратор.

ПримечаниеНастройка будет переопределена после изменения данной настройки в шаблоне LogAn администратором области на UGMC.

2. Если настройка параметра выполнена в шаблоне, то эта настройка переопределит значение этой же настройки, назначенной локальным администратором.

После получения настроек с UGMC настройки следующих разделов могут быть изменены локально на Log Analyzer:

- общие настройки устройства;
- настройки сетевых интерфейсов.

3. При настройке сетевых интерфейсов первый физический интерфейс, доступный для конфигурирования — это **port1**. Интерфейс **port0** нельзя настроить с помощью средств UGMC, он всегда настраивается локальным администратором и необходим для обеспечения первичной связи управляемого устройства с UGMC.

4. При настройке сетевых интерфейсов возможно создать интерфейс и оставить его конфигурирование локальному администратору. Для этого необходимо активировать параметр **on-device** (**on-device on**) в настройках сетевого интерфейса.

5. Библиотеки, например, такие как IP-адреса, списки URL, типы контента и другие, по умолчанию не содержат никакого контента в UGMC в отличие от библиотек, создаваемых по умолчанию на устройствах UserGate. Для использования библиотек в политиках UGMC, необходимо предварительно добавить элементы в эти библиотеки.

6. Рекомендуется создавать отдельные шаблоны для разных групп настроек, это позволит избежать конфликтов настроек при объединении шаблонов в группы шаблонов и упростит понимание результирующей настройки, которая будет применена к управляемым устройствам. Например, шаблон сетевых настроек, шаблон библиотек и т.д.

Группы шаблонов

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству. Результирующие настройки, применяемые к устройству, формируются в результате слияния всех настроек шаблонов, входящих в группу шаблонов, с учетом расположения шаблонов внутри группы.

Для создания группы шаблонов LogAn используется команда:

realmadmin/realm@nodename# create logan groups name <group-name> description <group description> templates [teplate1-name template2-name ...] template-enabled <on/off>

Для редактирования группы шаблонов LogAn используется команда:

realmadmin/realm@nodename# set logan groups name <group-name> <description, templates>

Для просмотра созданных ранее групп шаблонов LogAn используется команда:

realmadmin/realm@nodename# show logan groups <group-name>

Для удаления созданных ранее групп шаблонов LogAn используется команда:

realmadmin/realm@nodename# delete logan groups <group-name>

В созданной ранее группе шаблонов возможно удаление входящих в нее шаблонов:

realmadmin/realm@nodename# delete logan groups <group-name> templates [template-name template-name ...]

Добавление устройств LogAn под управление UGMC

Группа шаблонов всегда применяется к одному или нескольким управляемым устройствам LogAn. Для добавления управляемых устройств LogAn в UGMC необходимо выполнить следующие шаги:

1. Обеспечить доступ от управляемого устройства LogAn до UGMC, для этого на UGMC необходимо разрешить сервис **Management** в свойствах контроля доступа зоны, к которой подключены управляемые устройства

2. Создать объект управляемого устройства LogAn.

3. Связать созданный объект управляемого устройства LogAn с реальным устройством UserGate LogAn.

Для обеспечения доступа от управляемого устройства LogAn до UGMC необходимо в режиме администратора UGMC выполнить следующую команду:

Admin/system@nodename# set network zone <zone-nfme> enabled-services [Management]

Для создания объекта управляемого устройства используется команда:

realmadmin/realm@nodename# create logan devices <parameters>

Необходимо указать следующие параметры:

Наименование	Описание
enabled	Включает объект управляемого устройства. Если объект управляемого устройства включен, то он занимает одну лицензию.
name	Название для управляемого устройства. Можно вводить произвольное название.
description	Описание управляемого устройства.

Наименование	Описание
templates-group	Группа шаблонов, настройки которой следует применить к этому управляемому устройству.
sync-mode	Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта: • **auto** — автоматическая синхронизация. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к управляемому устройству, это изменение применяется к управляемому устройству без задержек. • **disabled** — синхронизация выключена. • **manual** — режим синхронизации, при котором настройки применяются однократно при запросе синхронизации.

Для осуществления связи уже настроенного устройства LogAn с UGMC необходимо выполнить следующие шаги:

1. Получить Код устройства

2. Указать IP-адрес UGMC и ввести уникальный код устройства

Код созданного объекта управляемого устройства (**device-code**) можно посмотреть следующей командой:

realmadmin/realm@nodename# show logan devices <device-name>

```
name                    : <device-name>
enabled                 : on
device-code               : 7w1lecpt
templates-group           : <template-group-name>
...
```

В консоли управляемого устройства LogAn необходимо добавить IP-адрес управляющего UGMC и указать код созданного объекта управляемого устройства:

Admin@logan-nodename# set settings general management-center mc-address <ugmc-ip-address> device-code 7w1lecpt enabled on

Проверить подключение на стороне UGMC можно командой просмотра управляемого устройства:

realmadmin/realm@nodename# show logan devices <device-name>

Для запуска вручную синхронизации всех настроек управляемых устройств предназначена команда (доступно в версии ПО 7.4.0 и выше):

realmadmin/realm@nodename# execute logan devices resync

Управление обновлениями управляемых устройств

UGMC позволяет создать централизованную политику обновления программного обеспечения UserGate (UGOS) и обновляемыми библиотеками, предоставляемыми по подписке.

ПримечаниеПосле добавления UserGate LogAn под управление UGMC, устройство UserGate автоматически начинает скачивать все обновления с сервера UGMC.

Обновление ПО

Порядок установки обновлений, следующий:

1. Загрузить обновления в репозиторий UGMC. Управление загрузками обновлений в репозиторий UGMC управляется командой:

realmadmin/realm@nodename# set settings general updates-schedule software

Подробнее — в главе Общие настройки в Руководстве администратора UGMC.

2. Утвердить обновление для всех или для конкретных устройств:

realmadmin/realm@nodename# set logan software-updates <sw-update-name> devices <device-name>

3. Провести установку обновления. После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств. Управляемое устройство скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление может быть установлено администратором в консоли UGMC или в ручном режиме администратором управляемого устройства.

Обновление библиотек

Библиотеки — это обновляемые базы ресурсов, предоставляемых по подписке клиентам UserGate (база категорий URL-фильтрации, сигнатуры СОВ, списки IP-адресов, URL, MIME-типов, морфологические базы и другие). Эти обновления выкладываются в репозиторий UserGate, откуда они уже доступны для скачивания UserGate LogAn. Если LogAn подключен к управлению через UGMC, то он проверяет наличие обновлений на сервере UGMC, который сам будет являться репозиторием. Репозиторий UserGate при этом будет использован сервером UGMC для получения новых обновлений. По умолчанию UGMC проверяет и скачивает обновления библиотек автоматически.

Библиотеки, находящиеся в репозитории UGMC доступны всем управляемым устройствам UserGate. Управляемые устройства скачивают и устанавливают доступные обновления автоматически в соответствии с расписанием проверки обновлений.

Для настройки скачивания обновлений в UGMC из репозитория UserGate используется следующая команда:

realmadmin/realm@nodename#set logan libraries-updates <library-name> download <auto/manual>

Version: 7.x
Product: UGMC

Для централизованного управления конечными устройствами UserGate в управляемой области необходимо создать шаблоны и группы шаблонов, описывающие настройки конечных устройств, затем добавить управляемые конечные устройства и применить к ним созданные ранее шаблоны.

В интерфейсе CLI создание шаблонов, групп шаблонов и добавление управляемых конечных устройств происходит на уровне **endpoint**.

Шаблоны устройств

Для создания шаблона конечных устройств используется команда:

realmadmin/realm@nodename# create endpoint template <name, description>

Для редактирования названия/описания шаблона конечных устройств используется команда:

realmadmin/realm@nodename# set endpoint template <name, description>

Для просмотра созданных ранее шаблонов конечных устройств используется команда:

realmadmin/realm@nodename# show endpoint template <template-name>

Для удаления созданных ранее шаблонов конечных устройств используется команда:

realmadmin/realm@nodename# delete endpoint template <template-name>

После создания шаблона конечных устройств можно начать производить настройку его параметров. Для этого необходимо перейти в режим настройки параметров шаблона управляемых устройств следующей командой:

realmadmin/realm@nodename# go endpoint-template <template-name>

При настройке параметров шаблона следует придерживаться следующих правил:

1. Если значение настройки не определено в шаблоне, то ничего передаваться в управляемое устройство не будет. В данном случае будет использована настройка по умолчанию.

2. Библиотеки, например, такие как IP-адреса, списки URL, списки типов контента MIME, приложения и другие, по умолчанию не содержат никакого контента в UGMC. Для использования библиотек в политиках фильтрации, необходимо предварительно добавить элементы в эти библиотеки.

3. Рекомендуется создавать отдельные шаблоны для разных групп настроек, это позволит избежать конфликтов настроек при объединении шаблонов в группы шаблонов и упростит понимание результирующей настройки, которая будет применена к управляемому устройству.

При создании шаблона администратор может использовать следующие разделы — Общие настройки, Настройки VPN, Библиотеки.

Общие настройки

В этом разделе устанавливаются параметры общих настроек управляемого устройства. Для настройки параметров используется следующая команда:

realmadmin/realm@nodename# set settings general <parameters>

Параметры для настройки:

Параметр	Описание
installation-settings	Настройки инсталляции ПО UserGate Client: • **collect-ep-data**: сбор информации о конечном устройстве (IP-адрес, время последнего подключения к UGMC, пользователь, имя компьютера, версия ОС, версия ПО UserGate Client, загрузка CPU и памяти, запущенные процессы, сервисы и т.д.). Значение по умолчанию: enabled. Если отключить данную функцию, то UGMC будет получать информацию только об IP-адресе, имени конечного устройства, версии ПО UserGate Client и ОС Windows, текущем времени и времени загрузки устройства, загрузке CPU и памяти. Важно! Отключение сбора информации о конечном устройстве влияет на работу профилей HIP. • **network-access**: настройка сетевого доступа при остановленном ПО UserGate Client. Значение по умолчанию: enabled. • **firewall-access**: разрешение пользователю самостоятельно, используя графический интерфейс, отключать контентную фильтрацию на конечном устройстве: ◦ **off** — не разрешать самостоятельно отключать контентную фильтрацию. ◦ **on** — разрешить самостоятельно отключать контентную фильтрацию. ◦ **by code** — разрешить самостоятельно отключать контентную фильтрацию с использованием кода. Для разрешения пользователю самостоятельно отключать контентную фильтрацию необходимо указать/сгенерировать код, который клиент должен ввести на конечном устройстве; также можно указать срок действия кода (code-expiration-date). При разрешении пользователю отключать фильтрацию самостоятельно можно указать количество разрешённых отключений (number-of-shutdowns) и/или время, на которое фильтрация будет отключена (duration). Значение по умолчанию: on (отключение фильтрации на 10 минут без использования кода). Важно! В случае использования счётчика количества отключений: если внести изменения в настройки разрешения отключения межсетевого экрана, то счётчик на конечном устройстве обнулится. • **uninstall-access**: возможность удаления ПО UserGate Client. При использовании опции uninstall-code (Разрешить с использованием кода) необходимо указать/сгенерировать код, который необходимо ввести клиенту при удалении ПО. Значение по умолчанию: enabled. **Важно!**Настройки не будут применены, если не включена синхронизация (параметр sync on). Иначе будут использованы значения по умолчанию.
notification	Настройка оповещений: • **show-icons**: отображение иконки UserGate Client в области уведомлений на панели задач. • **notification-tooltips**: включение/отключение отправки оповещений на конечное устройство. Если оповещения отключены, то уведомления не будут отображаться на конечном устройстве вне зависимости от настроек отдельных уведомлений (о добавлении/удалении устройства из карантина, блокировке ресурса). • **add-to-quarantine-message**: отправка уведомлений о блокировке устройства. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. • **remove-from-quarantine-message**: отправка уведомлений о разблокировке устройства. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. • **resource-blocked-message**: отправка уведомления при блокировке перехода по адресу электронного ресурса. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. **Важно!**Настройки не будут применены, если не включена синхронизация (параметр sync on). Иначе будут использованы значения по умолчанию.
logan-device	Установка для конечного устройства сервера LogAn, на которое устройство будет отсылать информацию о событиях. Сервер LogAn должен быть предварительно зарегистрирован в UGMC. **Важно!**Настройки не будут применены, если не включена синхронизация (параметр sync on). Иначе будут использованы значения по умолчанию.

Настройка VPN

Данный раздел позволяет настроить профили безопасности VPN, которые определяют такие настройки, как общий ключ шифрования (Pre-shared key), протокол соединения и алгоритмы для шифрования и

аутентификации. Настройки VPN передаются на управляемое устройство UserGate Client; пользователь сможет выбрать необходимый VPN-сервер для подключения в начальном окне графического интерфейса.

ПримечаниеНастройка VPN-соединений возможна только для конечных устройств с версией ОС Windows 10 и выше. После разрыва соединения попытки подключения будут производиться в течение 40 секунд. Если за это время соединение не будет установлено, то у пользователя отобразится окно для выбора VPN-сервера.

Для настройки параметров используется следующая команда:

realmadmin/realm@nodename# create settings vpn-settings <parameters>

Для настройки профиля VPN-сервера необходимо указать:

Параметр	Описание
enabled	Включение/отключение правила.
name	Название профиля безопасности для подключения к серверу VPN.
descriptipon	Описание профиля.
vpn-address	Имя (FQDN) или IP-адрес VPN-сервера. **Примечание**При использовании FQDN для подключения, если имени VPN-сервера соответствует несколько IP-адресов, клиент устанавливает соединение по первому адресу, который отвечает на запросы.
protocol	VPN-протоколы для создания туннеля: • **ipsec2**. Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec. • i**kev2-with-certificate**. Для создания защищенного канала будет использоваться протокол IKEv2, а для взаимной проверки подлинности сервера и клиента — сертификаты. **Важно!** При генерации клиентского сертификата обязательно должно быть указано поле CN — идентификатор пользователя, которому этот сертификат предназначается. • **ikev2**. Для создания защищенного канала будет использоваться протокол IKEv2, а для проверки клиента — логин и пароль (EAP-MSCHAP v2). Данный метод доступен только для пользователей доменного RADIUS-сервера.
ike-mode	Режим IKE (указать при выборе опции протокола IPsec L2TP): main, aggressive. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения.
psk	Строка, которая должна совпадать на сервере и клиенте для успешного подключения. Указывается для протокола IPsec L2TP.
Фаза 1	Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • **phase1-key-lifetime** - по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • **dpd-interval** - для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Минимальный интервал проверки: 10 секунд; значение 0 отключает проверку. • **dpd-max-failures** - максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным. • **dh-groups** - выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • **phase1-security** - алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки Выше/Ниже.
Фаза 2	Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • **phase2-key-lifetime**. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще. • **key-lifesize-enabled, key-lifesize**. Время жизни ключа может быть задано в байтах. Если заданы оба значения (key-lifetime и key-lifesize), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. • **phase2-security** - алгоритмы аутентификации и шифрования.

Библиотеки элементов

Данный раздел содержит в себе адреса-сайтов, IP-адреса, приложения и прочие элементы, которые используются при настройке правил управляемых устройств UGC.

Настройка библиотек в шаблонах конечных устройств происходит на уровне **libraries**.

Для создания списков используется команда:

realmadmin/realm@nodename# create libraries <parameters>

Для редактирования ранее созданных списков используется команда:

realmadmin/realm@nodename# set libraries <parameters>

Для просмотра ранее созданных списков используется команда:

realmadmin/realm@nodename# show libraries <parameters>

Для удаления ранее созданных списков используется команда:

realmadmin/realm@nodename# delete libraries <parameters>

Сервисы

Раздел **Сервисы** содержит список общеизвестных сервисов, основанных на протоколе TCP/IP, например, таких, как HTTP, HTTPS, FTP и другие. Данные сервисы могут быть использованы при построении правил управляемых устройств UGC. Первоначальный список сервисов поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы.

Для создания списков сервисов используется команда:

realmadmin/realm@nodename# create libraries services <parameters>

В качестве параметров указываются название и описание списка, необходимый протокол, порты назначения и источника.

Группы сервисов

Списки из библиотеки сервисов могут быть объединены в группы. Для создания группы сервисов используется команда:

realmadmin/realm@nodename# create libraries service-groups <parameters>

В качестве параметров в команде указываются название и описание списка, указываются необходимые списки сервисов, например:

realmadmin/realm@nodename# create libraries service-groups name <service-group-name> services [service-name1 service-name2 ...]

IP-адреса

Раздел **IP-адреса** содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил управляемых устройств UGC.

Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка IP-адресов используется команда:

realmadmin/realm@nodename# create libraries ip-list <parameters>

Далее необходимо задать следующие параметры:

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

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

realmadmin/realm@nodename# set libraries ip-list <ip-list-name> <parameter>

Чтобы добавить в список новые адреса:

realmadmin/realm@nodename# set libraries ip-list <ip-list-name> [<ip1> <ip2> ...]

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

realmadmin/realm@nodename# delete libraries ip-list <ip-list-name>
realmadmin/realm@nodename# delete libraries ip-list <ip-list-name> ips [<ip1> <ip2>...]

Команда отображения информации о всех имеющихся списках:

realmadmin/realm@nodename# show libraries ip-list

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

realmadmin/realm@nodename# show libraries ip-list <ip-list-name>

Также доступен просмотр содержимого списка IP-адресов:

realmadmin/realm@nodename# show libraries ip-list <ip-list-name> items

Группы приложений

Элемент библиотеки **Группы приложений** позволяет создать группы приложений для более удобного использования в правилах фильтрации сетевого трафика.

ПО UserGate Client определяет приложение по его контрольной сумме, что дает администратору возможность очень точно и выборочно управлять доступом в сеть для определенных приложений, например, разрешать доступ в сеть только для определенной версии приложения, блокируя при это все остальные версии данного приложения.

Для добавления новой группы приложений используется команда:

realmadmin/realm@nodename# create libraries application-groups <parameters>

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: • **very-low** — очень низкий уровень угрозы. • **low** — низкий уровень угрозы. • **medium** — средний уровень угрозы. • **high** — высокий уровень угрозы. • **very-high** — высокий уровень угрозы.

Параметр	Описание
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
apps	Указание названия (**name**) и контрольной суммы (**hash**) приложения. Контрольная сумма исполняемого файла Windows должна быть определена по алгоритму SHA1, например, с помощью утилиты fciv.

Для редактирования группы приложений используется команда:

realmadmin/realm@nodename# set libraries application-groups <group-name> <parameter>

Чтобы добавить в список новые приложения:

realmadmin/realm@nodename# set libraries application-groups <group-name> apps new name <app-name> hash <app-hash>

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

realmadmin/realm@nodename# delete libraries application-groupst <group-name>
realmadmin/realm@nodename# delete libraries application-groups <group-name> apps <app-name>

Команда отображения информации о всех имеющихся списках:

realmadmin/realm@nodename# show libraries application-groups

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

realmadmin/realm@nodename# show libraries application-groups <group-name>

Также доступен просмотр содержимого списка IP-адресов:

realmadmin/realm@nodename# show libraries application-groups <group-name> apps

Списки URL

Раздел предназначен для задания списков указателей URL, которые могут быть использованы в правилах контентной фильтрации в качестве черных и белых списков.

Настройка списков URL производится на уровне **libraries url-list**.

Для добавления нового списка URL предназначена следующая команда:

realmadmin/realm@nodename# create libraries url-list <parameters>

Далее указывается следующая информация:

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

Для редактирования списка URL используется команда:

realmadmin/realm@nodename# set libraries url-list <url-list-name> <parameters>

Параметры, значения которых можно обновить, представлены в таблицы выше.

Далее представлены команды, с использованием которых доступно удаление всего списка URL или отдельных адресов URL:

realmadmin/realm@nodename# delete libraries url-list <url-list-name>
realmadmin/realm@nodename# delete libraries url-list <url-list-name> urls [<url> ...]

Для просмотра информации о всех списках URL, об определённом списке URL или об адресах, входящих в определённый список, используются команды:

realmadmin/realm@nodename# show libraries url-list <url-list-name>
realmadmin/realm@nodename# show libraries url-list <url-list-name> urls

Категории URL

Элемент библиотеки **Категории URL** позволяет создать группы категорий UserGate URL filtering для более удобного использования в правилах фильтрации контента. Например, администратор может создать группу категорий «Бизнес категории» и поместить в нее необходимые категории.

Раздел находится на уровне **libraries url-categories**.

Для создания группы категорий URL используется следующая команда:

realmadmin/realm@nodename# create libraries url-categories <parameter>

Параметры, которые необходимо указать:

Параметр	Описание
name	Название группы URL-категорий.
description	Описание группы.
categories	Категории URL, которые необходимо добавить в группу.

Команда для редактирования параметров группы:

realmadmin/realm@nodename# set libraries url-categories <list-name> <parameter>

Для добавления категорий URL в существующую группу:

realmadmin/realm@nodename# set libraries url-categories <list-name> categories [<url-category> ...]

Команды для удаления группы URL-категорий:

realmadmin/realm@nodename# delete libraries url-categories <list-name>

или отдельных категорий из группы:

realmadmin/realm@nodename# delete libraries url-categories <list-name> categories [<url-category> ...]

Команды для просмотра информации о всех группах URL-категорий:

realmadmin/realm@nodename# show libraries url-categories

об определённой группе:

realmadmin/realm@nodename# show libraries url-categories <list-name>

Чтобы отобразить список категорий URL, входящих в группу:

realmadmin/realm@nodename# show libraries url-categories <list-name> categories

Тип контента

С помощью фильтрации типов контента доступна возможность управления видео и аудио контентом, изображениями, исполняемыми файлами и другими типами.

Раздел **Типы контента** находится на уровне **libraries content-types**.

Добавление нового списка типов контента доступно с использованием следующей команды:

realmadmin/realm@nodename# create libraries content-types <parameters>

Далее указывается следующая информация:

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

Для редактирования списка используется следующая команда:

realmadmin/realm@nodename# set libraries content-types <content-types-list-name> <parameter>

Параметры, доступные для обновления, представлены в таблице выше.

Следующая команда используется для удаления списка с типами контента:

realmadmin/realm@nodename# delete libraries content-types <content-types-list-name>

Также доступно удаление отдельных типов контента из списка:

realmadmin/realm@nodename# delete libraries content-types <content-types-list-name> mime [<mime-type> ...]

Следующие команды используются для отображения информации о списках типов контента:

realmadmin/realm@nodename# show libraries content-types
realmadmin/realm@nodename# show libraries content-types <content-types-list-name>

Для отображения типов контента, содержащихся в списке, используется команда:

realmadmin/realm@nodename# show libraries content-types <content-types-list-name> mime

Календари

Календари позволяют создать временные интервалы, которые затем можно использовать в правилах. Администратор может добавлять необходимые ему элементы в процессе работы.

Данный раздел находится на уровне **libraries time-sets**.

Для создания группы используется следующая команда:

realmadmin/realm@nodename# create libraries time-sets <parameter>

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название группы.
description	Описание группы.
time-set	• **interval-name** — название интервала повторения. • **type** — тип интервала повторения: ◦ **daily** — ежедневно: ▪ **time-from** — время начала (указывается в формате HH:MM). ▪ **time-to** — время окончания (указывается в формате HH:MM). ▪ **all-day on** — весь день. ◦ **weekly** — каждую неделю: ▪ **time-from** — время начала (указывается в формате HH:MM). ▪ **time-to** — время окончания (указывается в формате HH:MM). ▪ **all-day on** — весь день. ▪ **days [Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun]** — дни недели. ◦ **monthly** — каждый месяц: ▪ **time-from** — время начала (указывается в формате HH:MM). ▪ **time-to** — время окончания (указывается в формате HH:MM). ▪ **all-day on** — весь день. ▪ **days** — числа месяца (от 1 до 31). ◦ **fixed** — единовременно: ▪ **time-from** — время начала (указывается в формате HH:MM). ▪ **time-to** — время окончания (указывается в формате HH:MM). ▪ **all-day on** — весь день. ▪ **fixed-date** — нужная дата (указывается в формате YYYY-MM-DD). ◦ **span** — повторяющиеся события: ▪ **time-from** — время начала (указывается в формате HH:MM). ▪ **time-to** — время окончания (указывается в формате HH:MM). ▪ **all-day on** — весь день. ▪ **fixed-date-from** — дата начала (указывается в формате YYYY-MM-DD). ▪ **fixed-date-to** — дата окончания (указывается в формате YYYY-MM-DD). ◦ **range** — диапазон дат: ▪ **time-from-enabled <on** | **off>** — включение/отключение указания даты начала интервала. ▪ **fixed-date-from** — дата начала (указывается в формате YYYY-MM-DD). ▪ **time-from** — время начала (указывается в формате HH:MM). ▪ **time-to-enabled <on** | **off>** — включение/отключение указания даты окончания интервала. ▪ **fixed-date-to** — дата окончания (указывается в формате YYYY-MM-DD). ▪ **time-to** — время окончания (указывается в формате HH:MM).

Для редактирования календаря:

realmadmin/realm@nodename# set libraries time-sets <time-sets-name> <parameter>

Параметры, доступные для обновления, представлены в таблице выше.

Для редактирования интервала, заданного в календаре:

realmadmin/realm@nodename# set libraries time-sets <time-sets-name> ... time-set <time-set-type> (<time-set-filter>)

Далее указываются новые значения; <time-set-filter> — фильтр из текущих значений интервала.

Добавление нового элемента в существующую группу:

realmadmin/realm@nodename# create libraries time-sets <time-sets-name> ... time-set <time-set-type> new

Команда для удаления группы элементов:

realmadmin/realm@nodename# delete libraries time-sets <time-sets-name>

Для удаления элемента календаря:

realmadmin/realm@nodename# delete libraries time-sets <time-sets-name> <time-set-type> (<time-set-filter>)

Для отображения информации о всех календарях:

realmadmin/realm@nodename# show libraries time-sets

Для отображения информации об определённом календаре:

realmadmin/realm@nodename# show libraries time-sets <time-sets-name>

Для отображения информации об элементах группы с одинаковым типом повторения:

realmadmin/realm@nodename# show libraries time-sets <time-sets-name> <time-set-type>

Группы шаблонов

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству. Результирующие настройки, применяемые к устройству, формируются в результате слияния всех настроек шаблонов, входящих в группу шаблонов, с учетом расположения шаблонов внутри группы.

Для создания группы шаблонов конечных устройств используется команда:

realmadmin/realm@nodename# create endpoint groups name <group-name> description <group description> templates [teplate1-name template2-name ...]

Для редактирования группы шаблонов конечных устройств используется команда:

realmadmin/realm@nodename# set endpoint groups name <group-name> <description, templates>

Для просмотра созданных ранее групп шаблонов конечных устройств используется команда:

realmadmin/realm@nodename# show endpoint groups <group-name>

Для удаления созданных ранее групп шаблонов конечных устройств используется команда:

realmadmin/realm@nodename# delete endpoint groups <group-name>

В созданной ранее группе шаблонов возможно удаление входящих в нее шаблонов:

realmadmin/realm@nodename# delete endpoint groups <group-name> templates [template-name template-name ...]

Добавление конечных устройств UGC под управление UGMC

Для управления устройствами они должны быть добавлены в UGMC. Добавление конечных устройств UGC возможно двумя способами:

1. Добавление конечных устройств UGC по одному устройству. Данный вариант подходит для компаний с небольшим количеством управляемых устройств UGC.

2. Массовое добавление устройств. Вариант для компаний с большим количеством устройств.

Добавление по одному устройству

1. На UGMC необходимо разрешить сервис **Контроль конечных устройств** в свойствах контроля доступа зоны, к интерфейсу которой подключаются управляемое устройство.

2. Необходимо создать запись для конечного устройства UGC в UGMC.

3. Получить уникальный код созданного устройства.

4. Установить ПО UGC на конкретное устройство (компьютер) пользователя.

Для разрешения сервиса **Контроль конечных устройств** в свойствах контроля доступа зоны, к интерфейсу которой подключаются управляемое устройство, необходимо в режиме администратора UGMC выполнить следующую команду:

Admin/system@nodename# set network zone <zone-nfme> enabled-services ["Device net"]

Для создания записи для конечного устройства UGC используется команда:

realmadmin/realm@nodename# create endpoint devices <parameters>

Необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение объекта управляемого устройства UGC.
licensed	Лицензирование конечного устройства: on/off. Если on, то он использует одну лицензию. В случае отсутствия лицензии конечное устройство не сможет подключиться к UGMC. Если параметр будет поставлен в off после регистрации устройства на UGMC, то: • правила межсетевого экрана, полученные от MC ранее, продолжают работать; • подключение по VPN с настройками, полученными ранее от MC доступно; • новые настройки конечное устройство от MC не получает.
name	Название для управляемого устройства UGC. Можно вводить произвольное название.
description	Описание управляемого устройства UGC.
templates-group	Группа шаблонов, настройки которой следует применить к этому управляемому устройству UGC. Настройки (политики) применятся после синхронизации с UGMC.
sync-mode	Режим синхронизации: отключено (**disabled**), автоматическая (**auto**) или ручная (**manual**) синхронизация.

Для получения уникального кода созданного устройства (**device-code**) используется команда:

realmadmin/realm@nodename# show endpoint devices <device-name>

```
name                : <device-name>
enabled             : on
device-code           : g8wkh31z
templates-group       : <group-name>
sync-mode           : auto
```

Установка ПО UGC на компьютер пользователя описана в разделе Установка UserGate Client.

Массовое добавление устройств

1. На UGMC необходимо разрешить сервис **Контроль конечных устройств** в свойствах контроля доступа зоны, к интерфейсу которой подключаются управляемое устройство.

2. Создать код для группы конечных устройств.

3. Получить уникальный код для группы устройств.

4. Установить ПО UGC на конкретное устройство (компьютер) пользователя.

Для разрешения сервиса **Контроль конечных устройств** в свойствах контроля доступа зоны, к интерфейсу которой подключаются управляемое устройство, необходимо в режиме администратора UGMC выполнить следующую команду:

Admin/system@nodename# set network zone <zone-nfme> enabled-services ["Device net"]

Для создания кода для группы конечных устройств используется команда:

realmadmin/realm@nodename# create endpoint codes <parameters>

Необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение объекта управляемого устройства UGC.
name	Название для управляемого устройства UGC. Можно вводить произвольное название.
description	Описание управляемого устройства UGC.
group	Группа шаблонов, настройки которой следует применить к этому управляемому устройству UGC. Настройки (политики) применятся после синхронизации с UGMC.

Для получения уникального кода для группы устройств (**device-code**) используется команда:

realmadmin/realm@nodename# show endpoint codes <code-name>

name : <code-name>
enabled : on
group : <groupe-name>
device-code : 4shmps46

Установка ПО UGC на компьютер пользователя описана в разделе Установка ПО UserGate Client.

Для запуска вручную синхронизации всех настроек управляемых устройств предназначена команда (доступно начиная с релиза ПО 7.4.0):

realmadmin/realm@nodename# execute endpoint devices resync

HIP-объекты

Объекты HIP позволяют настроить критерии соответствия для конечных устройств и могут быть использованы в качестве одного из условий при настройке политик безопасности.

Для создания HIP объекта используется команда:

realmadmin/realm@nodename# create endpoint hip-object <parameters>

Необходимо указать следующие параметры:

Параметр	Описание
name	Название объекта HIP.
description	Описание объекта HIP (опционально).
os-version	Версия операционной системы устройства пользователя. При использовании операторов = и != необходимо указывать полную версию Windows.
ug-client-version	Версия ПО UserGate Client.
security	Статусы компонентов безопасности конечного устройства: • firewall — межсетевой экран; • virus-protection — Антивирус; • automatic-update — Автоматическое обновление; • bitlocker. Важно! BitLocker считается включенным, если он включен хотя бы на одном из дисков.
products	Проверка соответствия программного обеспечения, установленного на конечном устройстве: • antimalware. Проверка соответствия антивирусного ПО на устройстве пользователя. ◦ enabled: проверка статуса ПО; ◦ database-updated: проверка актуальности баз (да, нет, не проверять); ◦ version ПО; ◦ vendor: производитель и название продукта. • firewall. Проверка соответствия межсетевого экрана на конечном устройстве. При настройке необходимо указать: ◦ installed: проверка наличия установленного ПО; ◦ enabled: проверка статуса ПО (да, нет, не проверять); ◦ version ПО; ◦ vendor: производитель и название продукта; • backup. Проверка ПО для резервного копирования: ◦ installed: проверка наличия установленного ПО; ◦ version ПО; ◦ vendor: производитель и название продукта. • disk-encryption. Проверка установленных на конечном устройстве программ для шифрования диска: ◦ installed: проверка наличия установленного ПО; ◦ version ПО; ◦ vendor: производитель и название продукта. • dlp. Проверка соответствия системы предотвращения утечек информации. ◦ installed: проверка наличия установленного ПО; ◦ version ПО; ◦ vendor: производитель и название продукта. • patch-management. Проверка актуальности обновления. ◦ installed: проверка наличия установленного ПО; ◦ version ПО; ◦ vendor: производитель и название продукта.
processes	Проверка процессов, запущенных на конечном устройстве.
running-services	Проверка служб, запущенных на конечном устройстве.

Параметр	Описание
registry-keys	Ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. Поддерживаются следующие типы параметров реестра: • REG_SZ: строка Unicode или ANSI с нулевым символом в конце. • REG_BINARY: двоичные данные в любой форме. • REG_DWORD: 32-разрядное число. Доступна проверка ключей следующих разделов реестра: • HKEY_LOCAL_MACHINE • HKEY_USERS Важно! Путь указывается с использованием обратного слэша (\), например, \HKEY_LOCAL_MACHINE, после которых через (\) указывается полный путь к параметру. Описание ключей реестра читайте в документации Microsoft (https://docs.microsoft.com/ru-ru/troubleshoot/developer/webapps/iis/general/use-registry-keys).
installed-updates	Проверка наличия указанного обновления на конечном устройстве. Необходимо указать номер статьи базы знаний Microsoft (KB), например, KB5013624.

HIP-профили

HIP-профили представляют собой набор объектов HIP и предназначены для проверки соответствия конечного устройства требованиям безопасности (комплаенса). С использованием профилей HIP можно настроить гибкие политики доступа к зоне сети или приложению.

Для создания HIP-профиля используется команда:

realmadmin/realm@nodename# create endpoint hip-objects <parameters>

Необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля HIP.
description	Описание профиля HIP (опционально).
hip-objects	Выбор логического элемента (and, or, and-not, or-not) и объектов HIP. Подробнее о HIP-объектах — в разделе «Настройка проверки требований безопасности (HIP)»