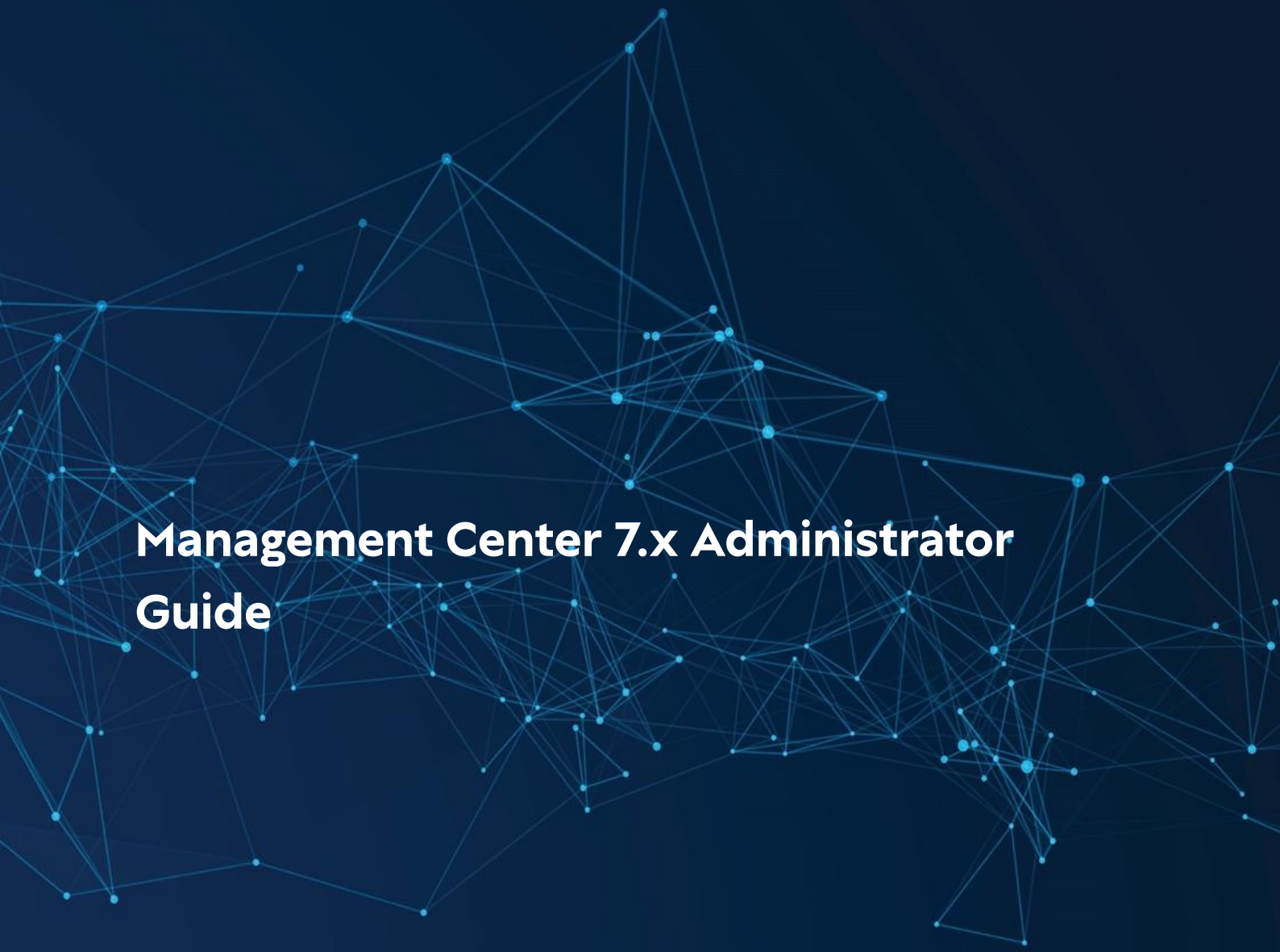
UserGate



Management Center 7.x Administrator Guide

Table of Contents

LEGEND AND ABBREVIATIONS

Legend and abbreviations

Abbreviation	Value
UGMC	UserGate Management Center
NGFW	UserGate Next-Generation Firewall
HSC	Hardware and Software System
SU	Security Update Licensing Module
MR	Managed realm
MD	Managed Device
UG MD	UserGate NGFW Managed Device
LogAn MD	UserGate Log Analyzer Managed Device
SW	Installed software
CPU	Central Processor Unit

INTRODUCTION

Description

UserGate Management Center (UGMC) is a decision that allows you to control numerous managed devices. Managed devices can be UserGate firewalls, LogAn data collection and analysis devices, endpoints with UserGate Client software installed.

UGMC provides a single point of control allowing an administrator to monitor managed devices, apply settings, and create policies applied to device groups to ensure corporate network security. UGMC helps you to manage and maintain a distributed fleet of UserGate Next-Generation Firewalls and LogAn data collection and analysis devices more effectively. The number of managed devices that can be connected is limited only by the license.

UGMC is available as a hardware and software system (HSC, appliance) or as a virtual machine image (virtual appliance) designed to be deployed in a virtual environment.

UGMC Management

Managing a UGMC includes managing services on the console itself and managing the realms created in the console.

Managing UGMC Services

Managing UGMC services includes the following tasks:

Name	Description
Configuring UGMC	• Assign IP addresses • Configure zones • Assign DNS servers • Create connections to LDAP servers • Configure alerts • Create additional UGMC administrators with the required rights. All these settings only affect the operation of the UGMC service and do not affect the administration of managed realms.
Licensing	Acquire a license for the product (enter a PIN code and register the product) and assign managed devices to each managed realm (optional). If no limits have been defined, any realm may use any number of managed devices as long as the total number does not exceed the number of licensed devices. For more information about licensing, see the UserGate Management Center Licensing chapter.
Creating Managed Realms	Create the managed realms. You can create an unlimited number of managed realms.

Name	Description
Creating root administrators for managed realms	Create root administrators for managed realms.

Managing UGMC Realms

Realms are managed by realm administrators. This includes the following tasks:

Name	Description
Create additional realm administrators	When a managed realm is added, a root administrator is created for it. The administrator has the full rights to manage the realm. The root realm administrator can create additional administrators and assign them all their appropriate rights.
Configuring Authentication Servers	Create connections to LDAP servers to allow LDAP users to act as realm administrators.
Create device templates	Create and configure device templates.
Create template groups	Create template groups that contain previously created templates.
Add managed devices	Add managed devices to UGMC and assign them to template groups.

Role-Based Management

During the initial UGMC configuration, creating at least one managed realm will create the following administrators:

- **UGMC Administrator.** Usually, this is the user with the login name Admin. To log in to the console, they must specify the name as Admin/system, where "system" means they are logged in to manage UGMC services and not the managed realm.
- **The root administrator of the realm**. This user can have any login name, e.g., Admin. To log in to the console, they must enter their name as Admin/realm_code, where realm_code is the code of the managed realm.

UGMC Administrators can create additional UGMC administrators and give them special rights (administrator profiles) to manage UGMC services. However, UGMC administrators are only allowed to manage UGMC services (see Configuring

UserGate Management Center) and are not allowed to manage realms. Example of UGMC administrators' access rights:

Administrator	Administrator Profile	Access level
Admin/system	Root profile	Full. The administrator and their profile are created when the UGMC services are initialized.
AdminRO/system	ReadOnly	View-only access to all UGMC services without the ability to modify them.
AdminRealm/system	RO+realms	Create managed realms and their administrators as well as view any other UGMC settings without the right to modify them.
AdminDash/system	Dashboard	Only allowed to view the **Dash board** section.

Root realm administrators can create additional administrators in their realm and assign them special rights (administrator profiles). Realm administrators are only allowed to manage their own realms (see Managed Realms). They cannot manage other realms or UGMC services. The root realm administrator can only be local and cannot be bound to an LDAP directory. Additional administrators created by the root realm administrator can be either local or bound to an LDAP directory. Examples of access rights for realm administrators:

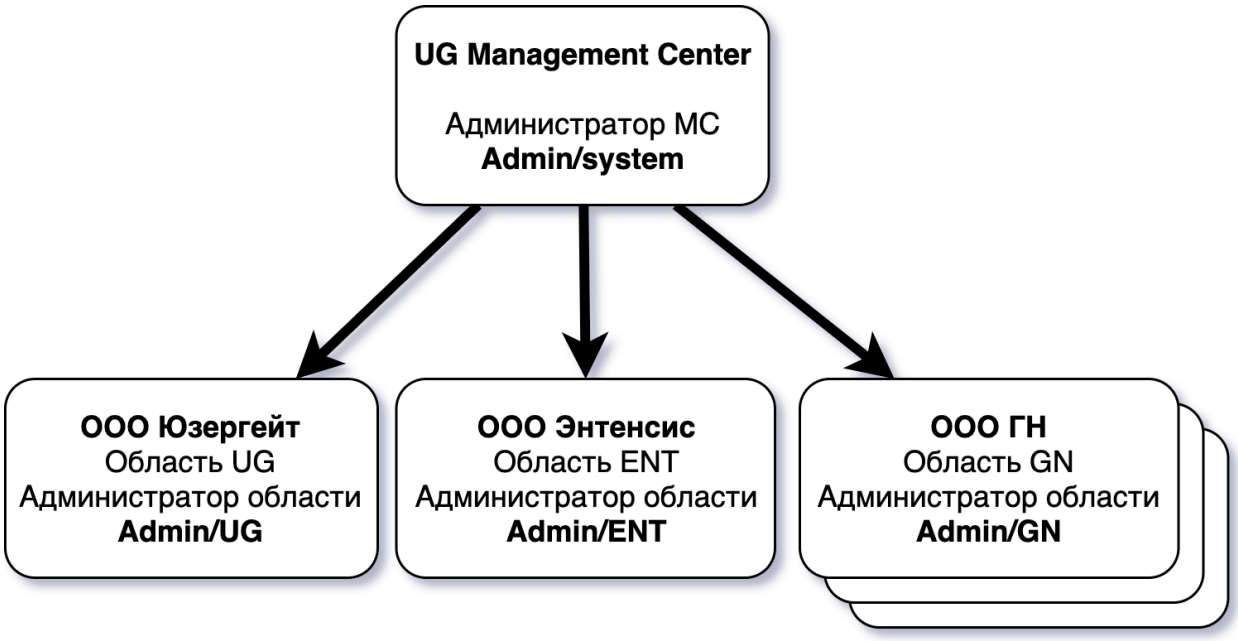
Administrator	Administrator Profile	Access level
Admin/realm_code	Root profile	Full. Administrators and their profiles are created by the UGMC administrator.
AdminRO/realm_code	ReadOnly	View-only access to all realm settings; no modification rights.
AdminTemplates/ realm_code	Templates	Create and modify all realm templates.
AdminTemplateGeneral/ realm_code	TemplateGeneral	Only modify the General template.

Administrator	Administrator Profile	Access level
AdminTemplateGeneralNET /realm_code	TemplateGeneralNET	Only modify network settings in the General template.

Managed Realms

UGMC supports the cloud-based management model, i.e., it allows an administrator to independently manage devices of different enterprises using a single management server. The access rights are defined at the managed realm level. A UserGate managed realm is a logical object that represents a single enterprise or a group of enterprises managed by a single administrator. Each realm has a separate administrator who can only administer one realm assigned to them. Under no circumstances can realm administrators access other realms. UGMC server administrators have the rights to create managed realms and assign administrators to them, but don't have rights to access the objects in these realms. For more information on administrator access rights, see Administrators.

An example of UGMC with multiple managed realms:



To manage UserGate devices in one organization, it is sufficient to create one managed realm.

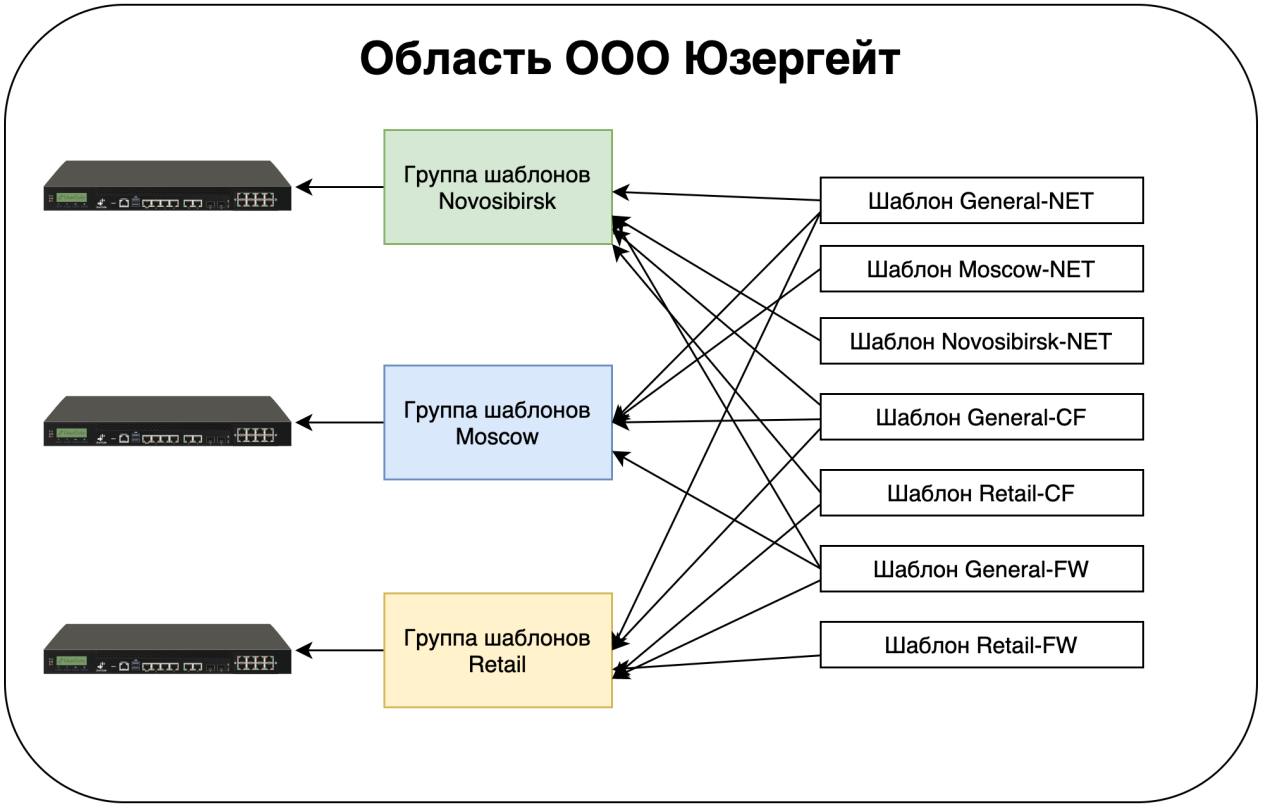
Settings for UserGate device parameters are made within a managed realm using templates and template groups.

Templates and Template Groups

To configure devices within a managed realm, administrators use templates and template groups. A template is a basic component that allows you to configure all settings of the managed devices, e.g. an NGFW: network settings, firewall rules, content filtering, intrusion detection system, etc.

Template groups allow multiple templates to be combined into a single configuration that applies to a managed device. Groups simplify centralized management, allowing you to make basic configurations for all device types using one or more templates in the group. Additionally, to configure any UserGate device individually, you can add separate templates with specific settings. The final settings that will apply to a device are generated by merging all settings specified in the templates of a template group based on their location in the group. Thus, you can define template groups based on the firewall's geographical location (e.g., Singapore, Hong Kong, Dubai, etc.) or business function (e.g., a realm with multiple template groups for managing sales office, development office, production, etc.).

This example shows a realm with multiple template groups for managing a UserGate NGFW:



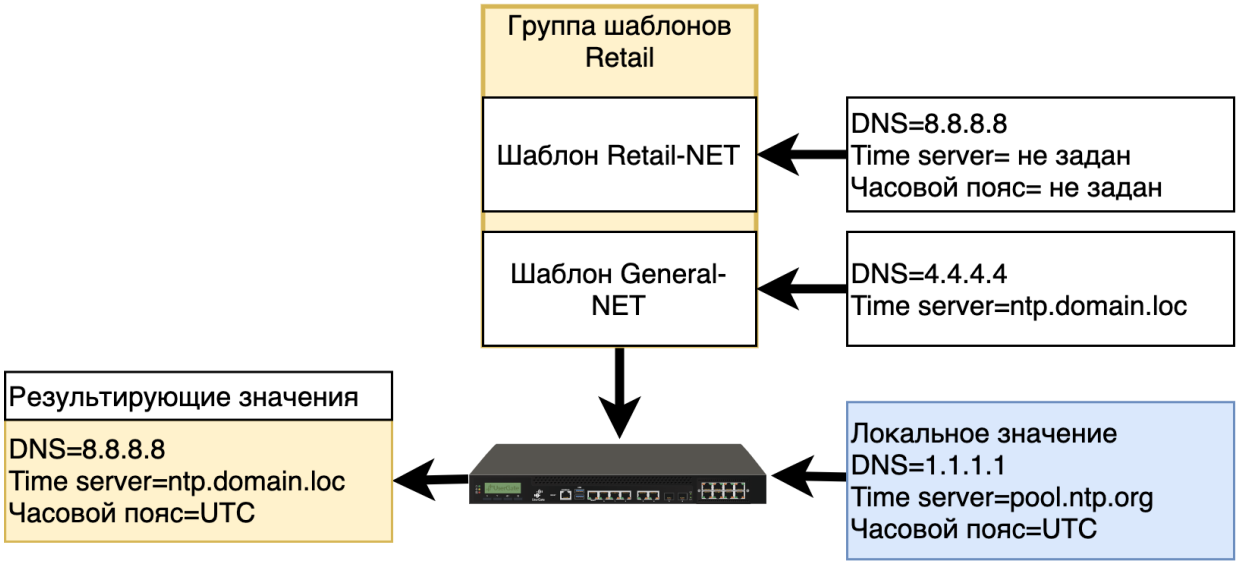
Two types of configurations can be sent to the device:

- Parameter settings, such as IP addresses of DNS servers.
- Policy rules, such as firewall or content filtering rules.

The type of configuration controls how the final value is determined. Policy rules are always passed to all devices, and the final policy is a set of all the rules arranged according to their order in the group template. The rules specified in higher templates are placed at the top of the final list of rules on the device.

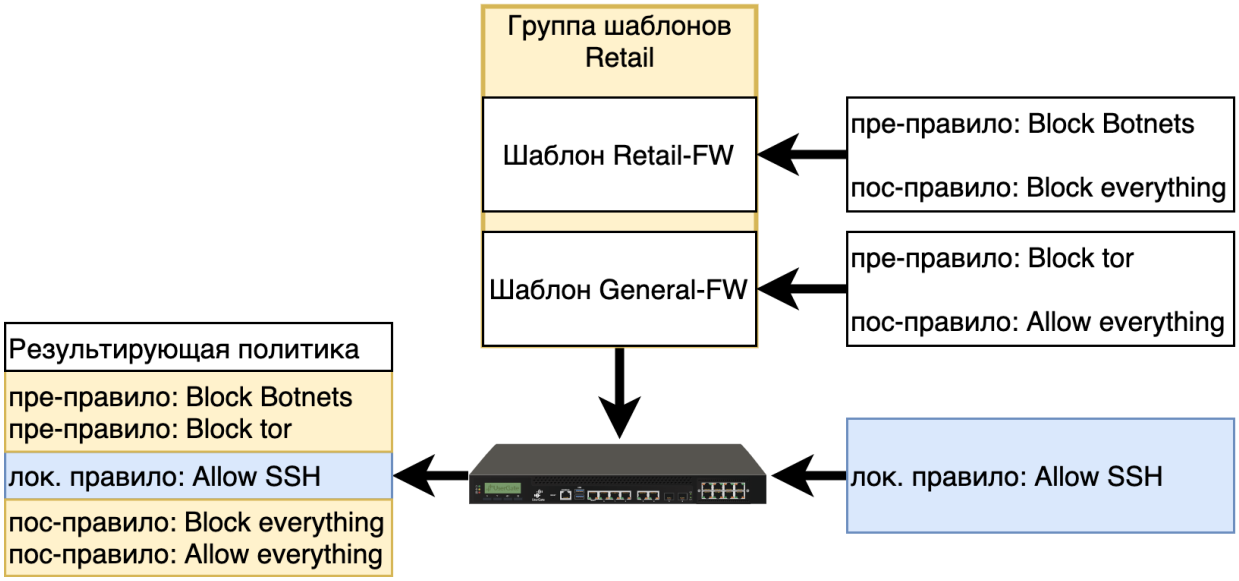
If the values in different templates of the same template group conflict, the value from the uppermost template applies. Local settings for this parameter are ignored.

The example below shows the final value for a parameter defined in multiple templates:



Templates can contain pre-rules and post-rules. These rules refer to rule locations relative to the rules created by the local UserGate NGFW administrator. Pre-rules always reside higher in the rule list and therefore have higher priority than locally created rules. Post-rules always reside lower than locally created rules and therefore have lower priority. The ability to create the two rule types allows realm administrators to define flexible security policy settings by giving local administrators more rights (with post-rules) or fewer (with pre-rules).

This example demonstrates a final policy when using pre-rules, post-rules, and local rules:



Managed Devices

A group of templates always applies to one or more UserGate devices. NGFW, LogAn devices are endpoint managed devices in the UGMC terminology.

To ensure compatibility between different versions of UGMC and managed devices, different versions of the synchronization protocol are used. To enable management of NGFW and LogAn devices from UGMC, the version of the synchronization protocol requested by managed devices must be no higher than that supported by UGMC.

UGMC version	NGFW version	LogAn version
6.x.x	UGMC is compatible with 6.x.x devices. UGMC is not compatible with 7.x.x devices.	LogAn management is not supported.
7.0.x	UGMC is compatible with 6.x.x, 7.0.x devices. For NGFW versions 6.x.x, the synchronization protocol version is lower than that supported by UGMC. In this case, UGMC will determine whether it is possible to convert the configuration to a lower version and, if conversion is possible,	UGMC is compatible with 6.x.x, 7.0.x devices. UGMC is not compatible with 7.1.x devices and higher. Because the device synchronization protocol version is higher than the protocol version supported by UGMC.

UGMC version	NGFW version	LogAn version
	transfer the configuration to the endpoint. If conversion is not possible (the configuration contains parameters that are not available in earlier versions), a synchronization error will be displayed. The error will be shown for the corresponding device in the **NGFW Management → NGFW Devices** section of the realm management console. UGMC is not compatible with NGFW 7.1.x and higher. Because the device synchronization protocol version is higher than the protocol version supported by UGMC.	
7.1.x	UGMC is compatible with 6.x.x, 7.0.x, 7.1.x devices. Starting from version 7.1.x, there have been changes in the configuration of the following components: • Intrusion Detection and Prevention System; • L7 Applications; • VPN; • User authentication (PKI authentication mode added). UGMC 7.1.x has limited support for synchronizing the settings of the above sections when working with NGFW versions lower than 7.1.x. When synchronizing a configuration of UGMC 7.1.x to NGFW versions 6.1.x and 7.0.x previously connected to the MC version below: • **IDPS**: After upgrading the UGMC, the IDPS	UGMC is compatible with 7.0.x, 7.1.x devices. There is no device management for versions 6.x.x.

UGMC version	NGFW version	LogAn version
	rules received from an earlier version of the UGMC will no longer be editable. • **VPN**: after updating UGMC, all settings in this section received from an earlier version of UGMC will no longer be editable. • All firewall rules that specify an application/ IDPS profile will be forcibly disabled before synchronization (i.e., these rules will appear in the UGMC console, but will not work). For NGFW versions 6.x.x and 7.0.x, the synchronization protocol version is lower than that supported by UGMC. In this case, UGMC will determine whether it is possible to convert the configuration to a lower version and, if conversion is possible, transfer the configuration to the endpoint. If conversion is not possible (the configuration contains parameters that are not available in earlier versions), a synchronization error will be displayed. The error will be shown for the corresponding device in the **NGFW Management → NGFW Devices** section of the realm management console.	

Support for earlier UserGate version configuration in UGMC

Support for earlier UserGate version configuration in UGMC 7.1.0

UGMC 7.1.0 has limited support for NGFW versions 6.1.X and 7.0.X, specifically the following system components will not work:

- VPN (NGFW version 7.0 will display VPN settings locked, you won't be able to edit them. The earlier VPN configuration continues to work, but the new one will not come down from the UGMC until NGFW is upgraded to version 7.1.0);
- IPS&L7;
- Authentication to the web console using user certificate profiles (PKI is only supported in NGFW version 7.1);
- Authentication of users in Captive portal using user certificate profiles;
- Firewall rules that use an L7 or IDPS profile, are sent to NGFW 7.0.1/6.1.9 forcibly off.
- If NGFW 7.0 where IDPS rules are configured is connected to UGMC 7.1, the rules will appear in NGFW console as blocked; you won't be able to edit them because the new version of UGMC cannot work with them.

UGMC LICENSING

UserGate MC Licensing

Basic license

UGMC is licensed by the types and number of active managed devices.

When the maximum allowed number is reached, the ability to add new managed devices is blocked. Only active managed devices, i.e., those that are enabled in the **Managed devices** section, count towards the maximum. When there are multiple managed realms, the administrator can allocate the required number of licensed

devices to each realm. The total number of managed devices in all realms cannot exceed the number of licensed devices.

The basic product license is perpetual (software and library updates are not included).

Additionally Licensed Modules

The following modules can be additionally licensed.

Module	Description
Security Updates (SU)	The SU module grants the right to receive updates of: • UGMC software • Intrusion detection system signatures • L7 application signatures • security compliance libraries The module is supplied as an annual subscription. After one year, you will need to renew the license to continue receiving updates.
Sensors	The module defines the type and number of devices managed by UGMC. The module is issued for a period of one year and requires annual paid renewal.
Cluster	The module includes a license to allow UserGate devices to operate in cluster mode. The license term is unlimited.
UserGate Client	This module is designed to work with endpoints with UserGate Client software installed, which is one of the components of the UserGate SUMMA ecosystem. The module subscription includes: • centralized management of endpoints and their network access, excluding access control in accordance with security compliance requirements • collect the endpoint telemetry and security events. Issued based on the number of licensed managed endpoints in sets of 10, 100, 1000, and 10000. The license term is unlimited.
NAC	An add-on module to the UserGate Client module. The module subscription includes: • endpoint security (compliance) validation; • control of access to the network at the node level based on the results of the check.

Module	Description
	Module licenses are supplied for a period of 1 to 5 years and are issued based on the number of licensed endpoints in sets of 10, 100, 1000, and 10,000. When the license expires, access control based on the results of the security compliance check, becomes unavailable. Firewall rules that use HIP profile as one of the conditions stop working. To continue using services, you must renew your license.

License Activation Procedures

Online Activation

During online activation, the UserGate device accesses the licensing server https://reg2.usergate.com. Technical details is sent to the server, including the UserGate software version number, PIN code, product name, device model, etc. The response is the license term and the list of modules permitted by the license.

If any modules that were previously present in the system are not on this list, they are deactivated and their license is revoked. Newly added modules are activated.

During operation of the UserGate device, a license check is performed once per day. Once the license is confirmed, the device resumes normal operation. A successful check is recorded in the event log with a corresponding event.

If the licensing servers are unavailable, 14 connection attempts are made at 120 second intervals. If unsuccessful, the attempts are stopped for 24 hours, followed by 14 more attempts to connect to the activation server again. If the license fails to connect to the activation server during the license validity period, the license is blocked upon expiration (modules with expired license stop working). Each activation server connection error is recorded in the logs.

Online Activation Procedure

To register the device:

1. In the device admin web console, go to the **Dashboards** section,

2. In the **License** widget, click **No license**, enter the PIN code and register the device.

If the node is in a closed perimeter without direct access to the Internet, you can activate or update the license through a proxy server. To do this, select the **Use a proxy server for activation and updates** mode. Then specify the IP address and

port of the upstream proxy server. If necessary, specify the login and password for authentication on the proxy server.

Offline Activation

Offline activation of licenses is required for UserGate devices located in an isolated network without Internet access and without the ability to activate via a proxy server.

The offline licensing process includes the following steps:

1. Request generation: creation of a request file for offline activation on the licensed device.

2. Request activation: processing the generated request file using the offline PIN code activation service.

3. Applying the license: downloading the activated file back to the licensed device.

Request generation

To generate a request file for offline license activation:

1. Access the licensed device using a web browser at the following address: https://<IP-address>:8010?features=offline-reg .

IP address is the IP address of the licensed device.

2. In the device web console, go to the **Dashboards** section.

3. In the **License** widget, click **No license**.

4. In the device activation window, click **Begin offline activation**.

5. Enter your device PIN and download the generated request file for offline activation.

Request activation

From a computer with Internet access, contact the offline activation service (to enter the service, you will need authorization in the Unified authorization center) and activate the generated request file.

Applying the license

Upload the activated file to the licensed device. To do that:

1. In the **Dashboards** section of the licensed device, in the **License** widget, open the offline activation window.

2. Select **Finish offline activation**.

3. Specify the activated file received from the offline activation service.

The licensing process is complete.

For more info on the offline license activation procedure, see the Offline License Activation section.

UGMC IMPLEMENTATION PLANNING

UGMC Implementation Planning (Description)

Deploying UGMC at an enterprise requires careful planning. The better the architectural design of your templates and template groups, the simpler and more flexible will be the process of applying management policies to UserGate devices. UGMC allows you to apply common policies efficiently by grouping them based on geography, functionality, or a mix of different aspects.

When planning your architecture, consider these recommendations:

- Avoid settings conflicts when adding templates to template groups. Conflicts always complicate the management of endpoints. This is the fundamental principle that underlies all recommendations outlined below.
- Assign different settings groups to different templates so that, e.g., a first template contains common managed device settings, a second contains content filtering policies, a third firewall policies, a fourth IDPS policies, etc. By sorting settings groups into different templates, you can prevent conflicts between settings and simplify centralized management.
- Create device-specific settings in different templates than those where global settings are created. For example, create a template with content filtering rules applicable to all managed devices and another template with content filtering rules applicable only to a specific device group. By varying the position of these two templates in the device groups, the administrator can set the correct order of final rules on devices. This recommendation assumes a manageable number of conflicting settings.

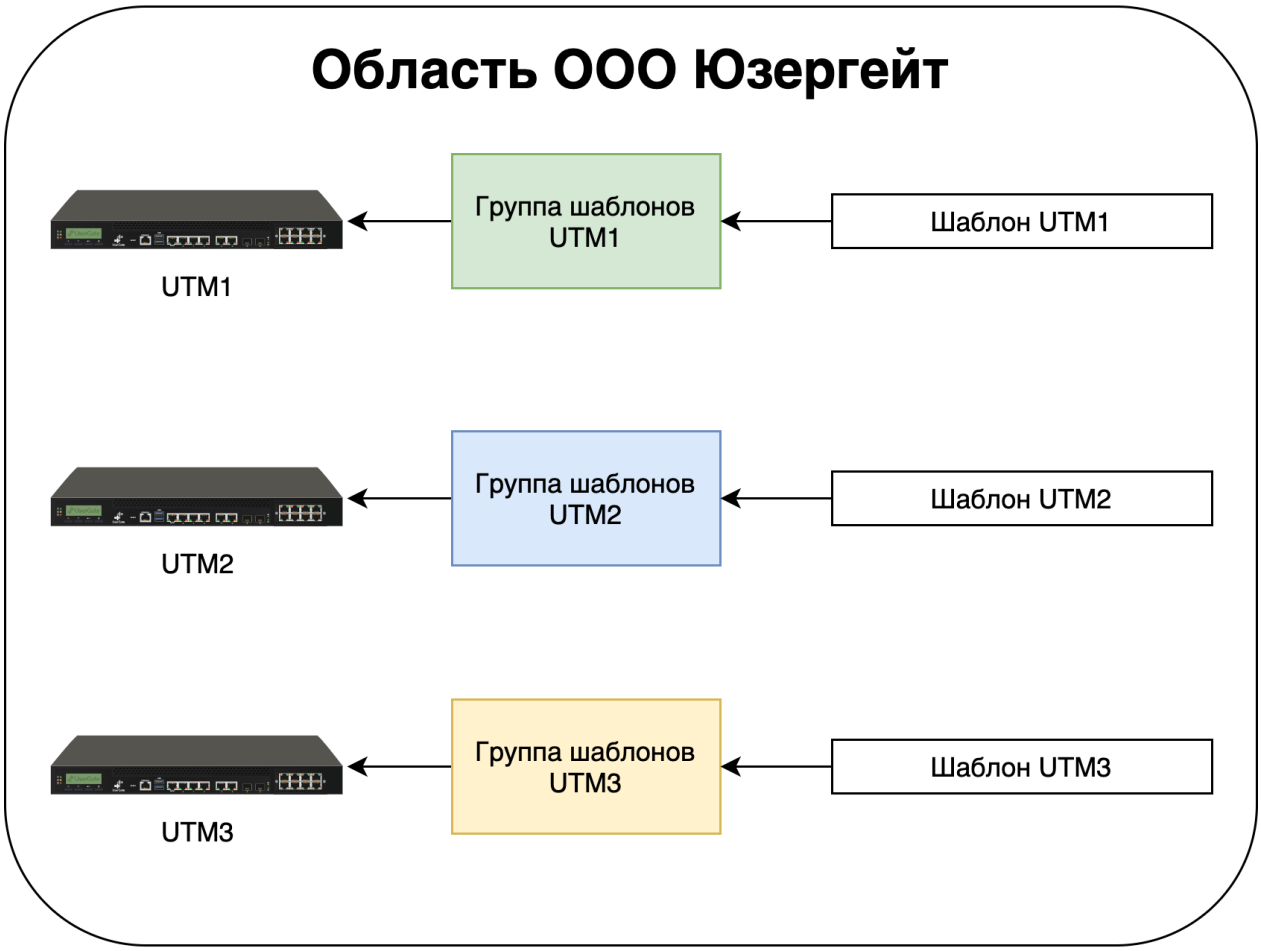
- Bear in mind the rights of local administrators. If you intend to have local administrators, their rights will be restricted by settings configured outside of UGMC templates, and any rules created by local administrators are always placed between pre- and post-rules applied from UGMC.

Consider several typical UGMC implementation scenarios where the UGMC is used to manage UserGate NGFWs.

One Template and One Template Group Per Managed Device

This is the most basic UGMC deployment scenario. The advantages here are the simplicity and transparency of settings, while the drawback is the lack of a centralized policy application, as each of the devices needs its own policy configured. Network connection settings can be made both via UGMC templates and by a local administrator.

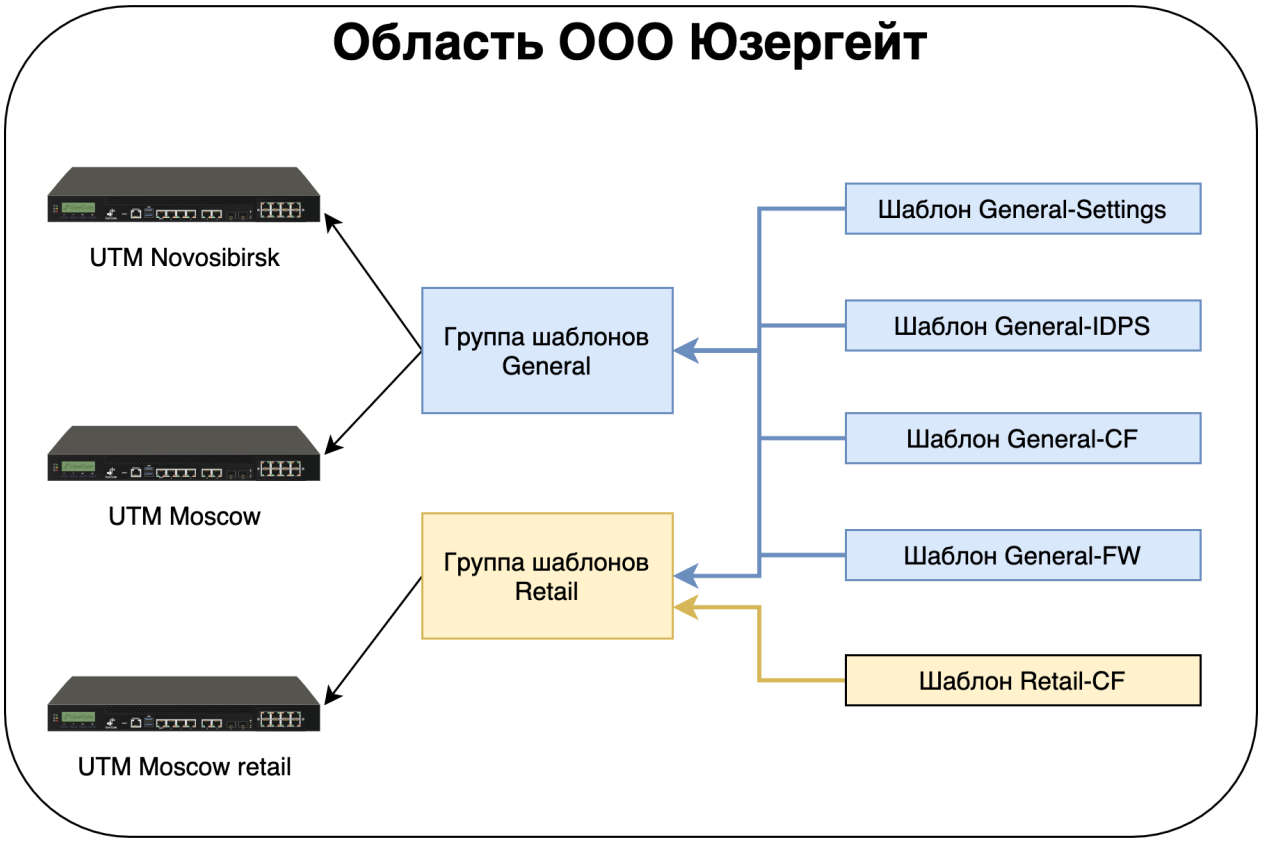
This scenario is recommended for simple implementations with a small number of UserGate NGFWs. An example configuration is shown in the figure below.



Set of Templates with Per-Module Settings, Some Module-Specific Settings for a Certain Managed Device Group, Network Configured Locally

Settings are grouped into templates, each of which contains the settings for a specific module, making it possible to avoid settings conflicts. All templates taken together form a centrally managed policy applied to all managed devices in the company. For managed devices that need a device-specific policy, separate templates are added. Network interfaces are configured by local administrators.

This scenario is recommended for most enterprises. An example configuration is shown in the figure below.



In this example, the templates contain the following settings:

- General-Settings Template: the global settings (timezone, logging level, DNS servers, etc.)
- General-IDPS Template: the global intrusion detection system policies
- General-CF Template: the global content filtering policies

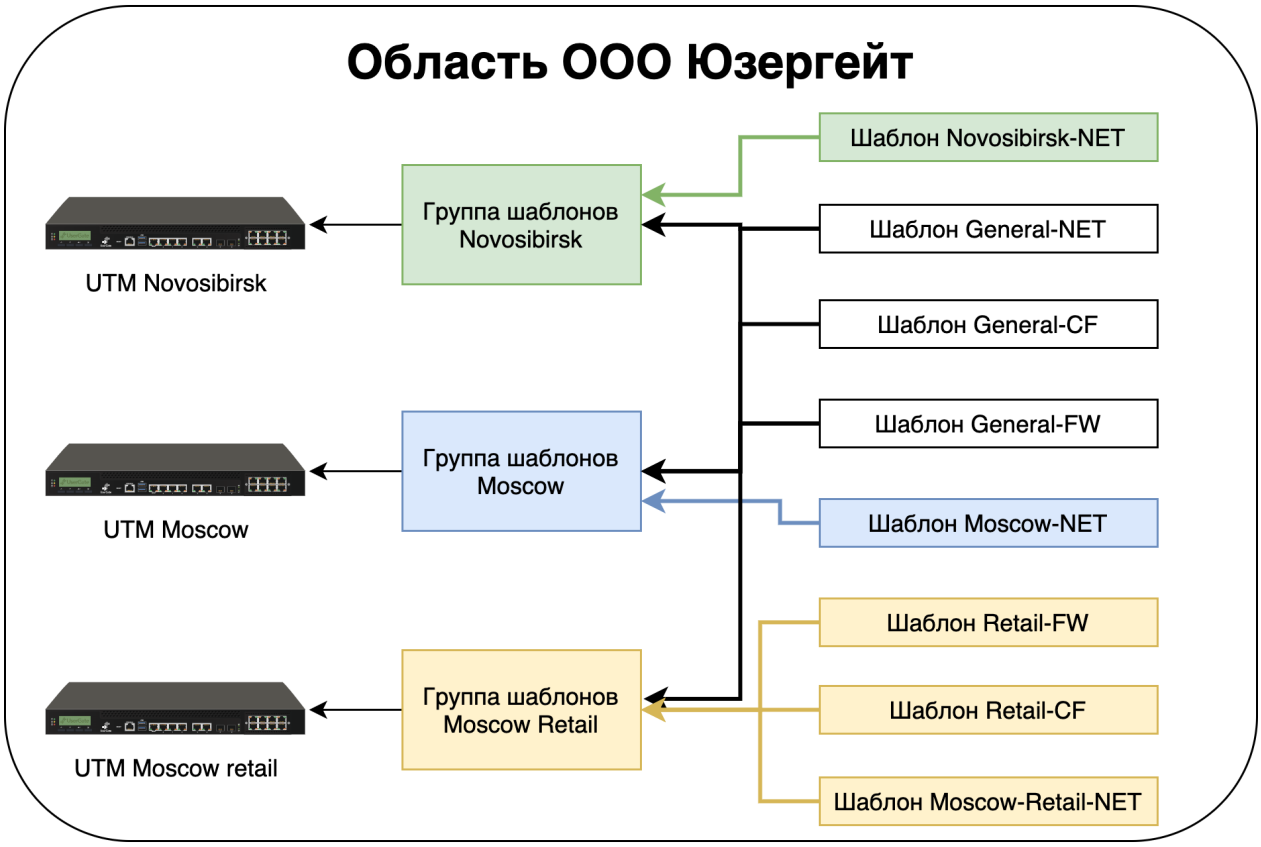
General-FW Template: the global firewall policies

- Retail-CF Template: the content filtering policies specific to retail units.

Set of Templates with Per-Module Settings, Some Module-Specific Settings for a Certain UG Managed Device Group, Network Configured via UGMC

Similar to the previous scenario, but with an additional network settings template for each UserGate NGFW.

This is recommended for most enterprises where centralized network interface configuration is required. An example configuration is shown in the figure below.



In this example, the templates contain the following settings:

- General-NET Template: the global network port settings
- General-CF Template: the global content filtering policies
- General-FW Template: the global firewall policies
- Retail-CF Template: the content filtering policies specific to retail units.

- Dubai-NET Template: the network port settings specific to the Dubai unit
- Singapore-NET Template: the network port settings specific to the Singapore unit
- Singapore-Retail-NET Template: the network port settings specific to the Singapore retail unit.

Example Device Templates

UserGate Management Center is supplied with a default Example realm that includes NGFW templates.

> **Note**
> **The realm and templates it contains are created solely for user convenience. These items can be used or deleted if not needed.**

To log in to the Example realm, use the default realm administrator profile with the login/password of ex_admin/Example.

The following NGFW templates exist in the realm:

- **example_content_template**: example settings for content filtering rules
- **example_firewall_template**: example settings for firewall rules
- **example_settings**: the general UserGate settings (timezone, UI language, server time settings)
- **UserGate Libraries template**: a set of zones and library items such as services, time sets, bandwidth pools, response pages, URL categories, and SSL profiles.

> **Note**
> **When the UserGate Libraries template is deleted, all predefined UserGate items will also be deleted and thus will no longer be available. It is recommended not to delete this template and instead use it directly or a copy of it when configuring policies related to the library items and zones defined in the template.**

INITIAL CONFIGURATION

Initial Configuration

UGMC is available as a hardware and software system (HSC, appliance) or as a virtual machine image (virtual appliance) designed to be deployed in a virtual environment. As a virtual appliance, UGMC is supplied with four Ethernet interfaces. In the form of an HSC, UGMC can have 8 or more Ethernet ports.

HSC Deployment

When UGMC is supplied as an HSC, the software is already installed and ready for initial configuration. For further configuration, skip to the Connecting to UGMC section.

Virtual Appliance Deployment

UserGate Management Center Virtual Appliance is a quick way to deploy a VM with pre-configured components. The VM image is supplied in the OVF format (Open Virtualization Format) supported by vendors such as VMWare and Oracle VirtualBox. For Microsoft Hyper-V and KVM, VM disk images are supplied.

Note

For the correct operation of the VM, 8GB RAM and 2-core virtual CPU are recommended as a minimum. Your hypervisor must support 64-bit operating systems.

Note

For the internal database to function correctly, the x86 architecture SSE4.2 micro-instruction set must be supported by the virtual environment processors. Any processor based on the x86 architecture released after 2008 must support SSE4.2.

To get started with the virtual appliance, follow these steps:

Name	Description
Step 1. Download and unpack the VM image.	Download the latest version of the virtual appliance from the official website, https://www.usergate.com.
Step 2. Import the VM image into your virtualization system.	Instructions on how to import a VM image can be found on the VirtualBox and VMWare websites. For Microsoft Hyper-V and KVM, you need first to create a VM, specify the downloaded image as the VM disk, **and then disable Integration Services** in the settings for the newly created VM.
Step 3. Configure the VM parameters.	Increase the size of the RAM for the VM. In the VM properties, set a minimum of 8GB RAM.
Step 4. Important! Increase the size of the disk for the VM.	The default disk size is 100GB, which is usually not enough to store all logs and settings. In the VM properties, set a disk size of 300GB or more. The recommended size is 500GB or more.
Step 5. Configure virtual networks.	UserGate Management Center is supplied with four interfaces, two of which are bound to zones: • **Management**: the first VM interface. • **Trusted**: the second VM interface intended for the communication with the managed UserGate NGFWs.
Step 6. Perform factory reset.	Start the VM. During loading, select **Support Menu** and then **Factory reset**. **This is a critical step**. UGMC uses this step to configure network adapters and increase the partition size on the hard disk to the size specified at Step 4.

Connecting to UGMC

The port0 interface is configured to receive an IP address automatically from a DHCP server and is bound to the **Management** zone. The initial configuration is done via the administrator's web console connection via the port0 interface.

If it is not possible to assign an IP address to the Management interface automatically using DHCP, it can be set explicitly from the CLI (Command Line Interface). For more details on using the CLI, see the chapter Command Line Interface (CLI).

Note

If the device has not undergone initial setup, use *Admin/system* as the system administrator name and *usergate* as the password for accessing the CLI.

Other network interfaces are disabled and require further configuration.

Please follow these steps to perform initial configuration:

Name	Description
Step 1. Connect to the management interface.	**When a DHCP Server Is Used** Connect the port0 interface to the corporate network with a working DHCP server. Start UGMC. After booting, the UGMC console will display the IP address to connect to for subsequent product activation. **Static IP address** Start UGMC. Use the CLI (Command Line Interface) to assign the desired IP address to the port0 interface. For more details on using the CLI, see the chapter Command Line Interface (CLI). Connect to the UGMC web console at the specified IP address. The address string should look similar to this: https://UGMC_IP_address:8010
Step 2. Select a language.	Select the language that will be used for the rest of the initial configuration.
Step 3. Set a password for the UserGate Management Center root administrator.	Set a login name and a password to log in to the web management interface.
Step 4. Register the system.	Enter the PIN code to activate the product and fill in the registration form. To activate the system, UGMC must have Internet access. If you are unable to register the product at this time, try it again after configuring the network interfaces at Step 8.
Step 5. Configure zones, set IP addresses of the network interfaces, and connect UserGate Management Center to the corporate network.	In the **Interfaces** section, enable the desired network interfaces, assign valid IP addresses that correspond to your networks, and bind the interfaces to the respective zones. For more details on network interface management, see the chapter Network Interface Configuration. The system is supplied with a number of predefined zones: • **Management** (management network), port0 interface. • **Trusted** (LAN). This is assumed to be the zone through which UGMC will connect to the managed devices and access the Internet. For the UGMC to work, one configured interface is sufficient. Having separate network interfaces for UGMC device management and UserGate managed devices management is recommended for security but is not mandatory.

Name	Description
Step 6. Configure the Internet gateway.	In the **Gateways** section, specify the IP address for the Internet gateway on an Internet-connected network interface. Usually, this is the Trusted zone. For more details on configuring Internet gateways, see the Gateway Configuration chapter.
Step 7. Specify the system DNS servers.	In the **General settings** section, specify the IP addresses of your provider's or corporate DNS servers.
Step 8. Register the product, if it was not registered at Step 4.	Register the product using the PIN code. For a successful registration, LogAn must have Internet access, and the previous steps must be completed. For more details on product licensing, see the UGMC Licensing chapter.
Step 9. Create at least one managed realm.	In the **Managed realms → Realms** section, add a managed realm.
Step 10. Create an administrator for the managed realm just created.	In the **Administrators** section, create an administrator profile and grant it rights to manage the newly created realm. Create an administrator with this profile.
Step 11. (Optional) Create additional UGMC administrators.	In the **Administrators** section, create the desired profiles for managing UGMC services and create UGMC administrators with these profiles.

When the above steps are completed, UGMC is ready for use. For more detailed configuration, see the relevant chapters of this Guide.

OFFLINE SERVER OPERATIONS

Offline Server Operations (Description)

Some server maintenance operations are carried out when the server is not running and is offline. To perform such operations, select **Support menu** when the server is booting and then select the desired operation. To access this menu, connect a monitor to a VGA (HDMI) port and a keyboard to a USB port (if these ports exist on the device) or use a special serial cable or a USB-Serial adapter to connect your computer to UGMC. Launch a terminal that supports connecting via a serial port, e.g.

Putty for Windows. Establish a serial port connection using 115200 8n1 as the connection parameters.

During the boot process, the administrator can select from the following boot menu options:

Name	Description
UGOS MC	Boot UserGate and output diagnostic information about the boot process to the serial port.
UGOS MC (failsafe)	Boot UserGate in simplified video mode.
Support menu	Enter the system utilities section and send output to tty1 (the monitor).
Restore previous version	This section is available after updating or creating a system backup.

The system utilities (**Support menu**) section offers the following actions:

Name	Description
Check filesystems	Start a file system check on the device with automatic error correction.
Expand data partition	Expand the data partition to use the entire allocated disk space. This operation is usually carried out after increasing the amount of disk space allocated by the hypervisor to the UserGate VM. UserGate data and settings are not reset.
Create backup	Create a full backup of the UserGate disk on an external USB medium. All existing data on the external medium will be deleted.
Restore from backup	Restore UserGate from an external USB drive.
Factory reset	Reset UserGate to its original system state. All data and settings will be lost.
Exit	Log out and reboot the device.

CONFIGURING UGMC

General Settings

The **General settings** section is used to configure the basic UGMC settings:

Name	Description
Timezone	The timezone for your location. Used in rule schedules and for the correct display of time and date in reports, logs, etc.
Default interface language	The language to use by default in the console.
Automatic session closure timer (min)	Configure the automatic session closure timer that will expire on the absence of administrator activity in the web console.
Server time settings	Configure the time synchronization settings. • **Use NTP servers**: use the NTP servers from the provided list for time synchronization. • **Primary NTP server**: the primary time server address. Default value: pool.ntp.org. • **Secondary NTP server**: the secondary time server address. • **Server time (UTC)**: allows time setting on the server. The UTC timezone should be used.
Update center	Settings for managing the download of UserGate software (UGOS) updates and system libraries required for exporting settings to managed devices (ISO signatures, application signatures, analytics rules, and others). **Software updates**: configure the update channel (stable, beta), checking for new UGOS updates and downloading offline updates. **Libraries updates**: check for libraries updates, download updates, and configure the automatic library check and download schedule. You can check for library updates and download the latest updates by clicking the **Check for updates** link. You can configure automatic library updates by clicking the **Con figure** link.

Name	Description
	You can select from the following schedule options: • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
Change tracker settings	If this option is enabled and **Change types** have been defined, any change to the configuration introduced by the administrator using the web console will require that the administrator specify the change type and a description for the change. Here are some possible examples of change types: • Directive • Order • Scheduled maintenance, etc. The number of change types is not limited.
System DNS servers	Specify valid IP addresses of DNS servers here.

Device management

The **Device management** section is used to configure the following UGMC settings:

- Clustering
- Diagnostics settings
- Server operations
- Backup
- Settings export and import

Clustering and High Availability

UGMC supports two types of clusters:

1. **Configuration cluster**. Nodes combined into a configuration cluster support unified configuration within the cluster.
2. **High Availability (HA) cluster**. Up to 4 configuration cluster nodes can be combined into a HA cluster that supports the Active-Active or Active-Passive operation modes.

> **Note**
> **When implementing UGMC in high availability mode, you must complete both the configuration cluster settings and the HA cluster settings.**

A number of settings are specific to each cluster node, e.g., network interface configuration and IP addressing. The node-specific settings are listed below:

Name	Description
Node-specific settings	Diagnostics settings Network interface settings Gateway settings Routes

To create a configuration cluster, follow these steps:

Name	Description
Step 1. Perform initial configuration on the first cluster node.	See the Initial Configuration chapter.
Step 2. On the first cluster node, configure the zone containing the network interfaces through which cluster replication will be carried out.	In the Zones section, create a new dedicated zone for cluster settings replication. Allow the following services in the zone's settings: • Administrative console • Cluster. Do not use zones whose interfaces are connected to untrusted networks (e.g., the Internet) for replication.
Step 3. Specify the IP address that will be used to communicate with other cluster nodes.	In the **Device management** section, go to the **Configuration Cluster** pane, select the current cluster node, and click **Edit**. Specify the IP address of an interface located in the zone you configured at Step 2.
Step 4. Generate a **Secret code** on the first cluster node.	In the **Device management** section, click **Generate secret code**. Copy the resulting code to the clipboard. This master node secret is required for one-time authorization of a second node before adding it to the cluster.
Step 5. Connect a second node to the cluster.	A second and subsequent nodes are added to the cluster during their initialization. If the initialization has already been performed, reboot the device and perform a factory reset. Connect to the web console of the second cluster node and select the installation language. Specify the network interface that will be used to connect to the first cluster node and assign it an IP address. Both cluster nodes must reside in the same subnet — e.g., as is the case when the port2 interfaces of the two nodes are assigned IP addresses 192.168.100.5/24 and 192.168.100.6/24, respectively. Otherwise, you need to specify the IP address of the gateway through which the first cluster node will be accessible. Specify the IP address of the first node configured at Step 3, enter the master node secret, and press the **Connect** button. If the IP addresses of the cluster configured at Step 2 are assigned correctly, the second node will be added to the cluster, and all the settings from the first cluster node will be replicated on the second one.
Step 6. Assign zones to the second node's network interfaces.	In the web console for the second cluster node, go to the **Network → Interfaces** and assign a correct zone to each network interface. The zones and their settings are obtained as a result of data replication from the first cluster node.

Name	Description
Step 7. (Optional) Configure the node-specific settings for each cluster node.	Configure the gateways, routes, and other settings specific to each cluster node.

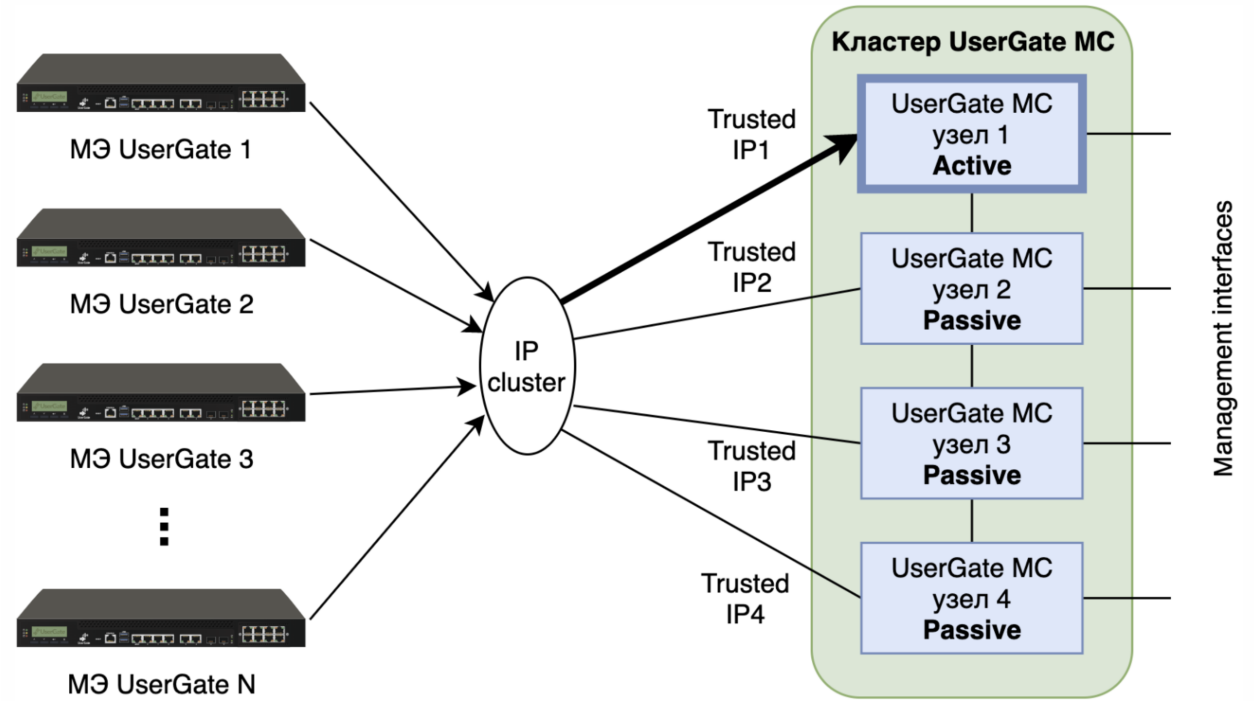
Up to four configuration cluster nodes can be combined into a HA cluster. There can be multiple HA clusters. Two modes are supported, **Active-Active** and **Active-Passive**.

In the **Active-Passive** mode, one of the servers operates as the master node that processes traffic and the rest act as backup. One or more virtual IP addresses are specified for the cluster. The virtual addresses are switched from the master node to one of the backup nodes under the following circumstances:

- A backup server gets no confirmation that the master instance is online — for example, if it is offline or the nodes are unavailable on the network.
- Internet connectivity checking is configured on the master instance.
- A software fault has occurred in UserGate.

An example network diagram for a HA cluster in the **Active-Passive** mode is shown below. The network interfaces are configured as follows:

- **Trusted zone**: IP1, IP2, IP3, IP4, and IP cluster (Trusted).
- **Management zone**: interfaces in this zone are used to manage the UGMC nodes.



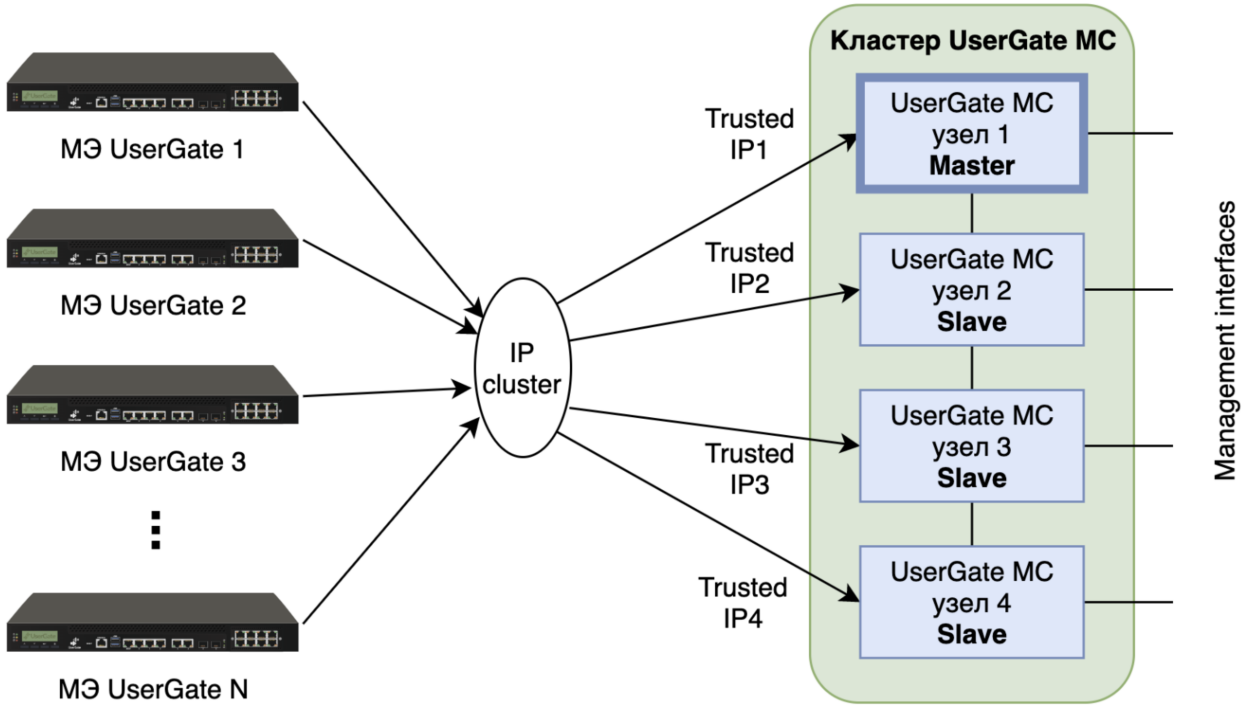
The cluster IP address resides on the UGMC 1 node. If the UGMC 1 node goes offline, the cluster IP address will migrate to the next server, which becomes the master — e.g., UGMC 2.

In the **Active-Active** mode, one of the servers operates as the master node that distributes the traffic among all other cluster nodes. Since the cluster IP address resides on the master node, that node responds to client ARP requests. By consecutively serving MAC addresses of all HA cluster nodes, the master node ensures uniform traffic distribution between all cluster nodes taking account of the need to provide user session continuity. One or more virtual IP addresses are specified for the cluster. The master role is assumed by one of the backup nodes under the following circumstances:

- A backup server gets no confirmation that the master instance is online — for example, if it is offline or the nodes are unavailable on the network.
- Internet connectivity checking is configured on the master instance.
- A software fault has occurred in UserGate.

An example network diagram for a HA cluster in the Active-Active mode is shown below. The network interfaces are configured as follows:

- The **Trusted** zone: IP1, IP2, IP3, IP4, and IP cluster (Trusted).
- The **Management** zone: interfaces in this zone are used to manage the UGMC nodes.



The cluster IP address resides on the UGMC 1 node, which is the master. The traffic is distributed between all cluster nodes. If the UGMC 1 node goes offline, the master role and the cluster IP address will migrate to the next server, e.g., UGMC 2.

To create a HA cluster, follow these steps:

Name	Description
Step 1. Create a configuration cluster.	Create a configuration cluster as described in the previous step.
Step 2. Configure zones whose interfaces will participate in the HA cluster.	In the **Zones** section, you should allow the **VRRP** service for all zones where virtual cluster IP addresses are to be added (the **T rusted** zone on the above diagrams).
Step 3. Create a new HA cluster.	In the **Device management → HA cluster** section, click **Add** and configure the settings for the new HA cluster.

The settings for a HA cluster are listed below:

Name	Description
Enabled	Enable or disable the HA cluster.
Name	The name of the HA cluster.
Description	A description of the HA cluster.

Name	Description
Mode	The HA cluster operating mode: • **Active-Active**: the load is distributed between all cluster nodes. • **Active-Passive**: the load is processed by the master node and switched to a backup instance if the master node is offline.
HA cluster multicast ID	Multiple HA clusters can be created in a single configuration cluster. Session synchronization uses a specific multicast address defined by this parameter. A unique ID must be assigned to each group of HA clusters that requires session synchronization support within the group.
Virtual router ID (VRID)	The VRID must be unique to each VRRP cluster in the local network. If there are no 3rd party VRRP clusters in the network, it is recommended to keep the default setting.
Nodes	Select the configuration cluster nodes to combine into an HA cluster. Here you can also assign the master role to one of the selected nodes.
Virtual IPs	Assign virtual IP addresses and map them to the interfaces of the cluster nodes.

Diagnostics

This section contains the server diagnostics settings that UGMC technical support will need to resolve eventual problems.

Name	Description
Diagnostic details	• **Off**: diagnostics logs are disabled • **Error**: log only server errors • **Warning**: log only errors and warnings • **Info**: log only errors, warnings, and additional information • **Debug**: provide as much detail as possible It is recommended to set **Diagnostic details** to **Error** (errors only) or **Off** (disabled), unless UserGate technical support asked you to set different values. Any values other than Error (errors only) or Off (disabled) will affect UGMC performance negatively.
Diagnostics logs	

Name	Description
	• **Download logs**: download the diagnostic logs for sending them to UserGate support. • **Clear logs** — delete archived (not currently active) logs.
Remote assistance	• **On/Off**: enable/disable the remote assistance mode. Remote assistance allows a UserGate support engineer to connect securely to a UGMC server for troubleshooting using the known values of the Remote assistance ID and token. For a successful activation of remote assistance, UGMC must have SSH access to the UserGate remote assistance server. • **Remote assistance ID**: a randomly generated value that is unique for each remote assistance session. that is unique for each remote assistance session. • **Remote assistance token**: a randomly generated token value. that is unique for each remote assistance session.

Server operations

In this section, you can perform the following server maintenance actions:

Name	Description
Server operations	• **Reboot**: reboot the UGMC server • **Shutdown**: shutdown the UGMC server
Updates channel	Here you can select the update channel for UGMC software: • **Stable**: check for stable software updates and download them (if any) • **Beta**: check for experimental updates and download them (if any)
Server updates	Displays available UGMC updates. Starts the server update process and allows to create a restore point. View a changelog for the update.
Offline updates	Download a file for offline updates.
Upstream proxy settings to check licenses and updates	Configure the upstream HTTP(S) proxy server settings for license and software updates for UGMC.

Name	Description
	You must specify the IP address and port of the upstream proxy server. If necessary, specify login and password for authentication on the upstream proxy server.

The UserGate company is continuously working to improve its software and provides UGMC product updates as part of the Security Update license module subscription (for more details on licensing, see the UGMC Licensing chapter). If there are any updates, a notification to that effect will display in the **Device management** section. As a product update can take quite a while, it is recommended to account for the potential UGMC downtime when planning update installation.

To install updates, follow these steps:

Name	Description
Step 1. Create a backup file.	Create a backup of the UGMC state in the section **Device management → System backup management → Create system backup**. This step is always recommended before applying updates because it will allow you to restore the previous state of the device, should any problems arise during the update process.
Step 2. Install the updates.	In the **Device management** section, if the **New updates available** notification is present, click **Install now**. The system will install the downloaded updates, and when the installation completes, UGMC will reboot.

System backup management

This section allows you to manage UserGate backups, i.e. to set backup export rules, to create a backup, and to restore a UserGate device.

To create a backup, follow these actions:

Name	Description
Step 1. Create a backup	Under **Device management → System backup management**, click **Create backup**. The system will save the current server settings in a file named: backup_PRODUCT_NODE-NAME_DATE.gpg, where *PRODUCT* is the product type: NGFW, LogAn, or MC; *NODE-NAME*is the UserGate node name; *DATE* is the date and time when the backup was created as YYYY-MM-DD-HH-MM. The time is in UTC time zone.

Name	Description
	To interrupt the backup process, click **Stop**. The backup record will be displayed in the device event log.

To restore the device status, follow these steps:

Name	Description
Step 1. Restore the device state	In the **Device management → System backup management**, click **Restore from backup** and specify the path to the previously created settings file to upload it to the server. Restore will be suggested in the tty console when the device reboots.

In addition, the administrator can configure a scheduled file upload to external servers (FTP, SSH). To create a schedule for uploading settings, follow these steps:

Name	Description
Step 1. Create a configuration export rule	In the **Device management → System backup management**, click **Add** and enter a name and description for the rule.
Step 2. Specify the remote server parameters.	In the **Remote server** tab of the rule, specify the parameters for the remote server: • **Server type**: FTP or SSH • **Address**: the server's IP address • **Port**: the server's port • **Login name**: the user account on the remote server • **Password**/**Repeat password**: the password for the user account • **Directory path**: the path on the server where the settings will be uploaded If using an SSH server, you can use key authorization. To import or generate a key, select **SSH key setup** and specify **Generate key** or **Import key**. **Important!** If you re-create a key, the existing SSH key will be deleted. The public key must reside on the SSH server in the user keys directory **/home/user/.ssh/** in the **authorized_keys** file. When initially configuring the SSH backup export rule, connection verification is mandatory (**Check connection** button). When the connection is verified, the fingerprint is placed in known_hosts. The files are not sent without verification.

Name	Description
	Important! If you change the SSH server or reinstall it, the backup files will be unavailable because the fingerprint has changed. This protects you from spoofing.
Step 3. Select the upload schedule.	In the **Schedule** tab of the rule, specify when the settings should be uploaded. If specifying the time in the crontab-format, enter it as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday) Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • The asterisk and dash are also used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

Exporting and importing settings

The administrator can save the current UGMC settings in a file and later restore them on the same or another UGMC server. This is different from a backup in that importing/exporting the settings does not preserve the current state of all system components — only the current settings are saved.

> **Note**
>
> **Importing/exporting the settings does not preserve the interface state or license information. After completing the import, you will need to configure the interfaces and re-register UGMC using the existing PIN code.**

To export the settings, follow these steps:

Name	Description
Step 1. Settings export.	

Name	Description
	Under **Device management → Settings export and import**, click **Export** and select **Export all settings** or **Export network settings**. The system will save: • the current server settings in a file named: cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin • the network settings in a file named network-cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin where nodename is the name of the UserGate Management Center node; version is the version of UserGate Management Center; and YYYYMMDD_HHMMSS is the date and time of the settings export in the UTC timezone. Example: cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084853.bin or network-cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084929.bin.

To apply the exported settings, follow these steps:

Name	Description
Step 1. Import the settings.	In the **Device management → Settings export and import** section, click **Import**, and browse to the path of the settings file created earlier. The settings will be applied to the server, after which the server will reboot.

Note

To correctly import the rules that use updatable UserGate lists (applications, URL categories, etc.), you need to have licenses for the SU and ATP modules as well as pre-downloaded UserGate lists.

For more information on the features of importing cluster solution settings, see the Updating the UGMC Cluster Software section.

In addition, the administrator can configure a scheduled settings upload to external servers (FTP, SSH). To create a schedule for uploading settings, follow these steps:

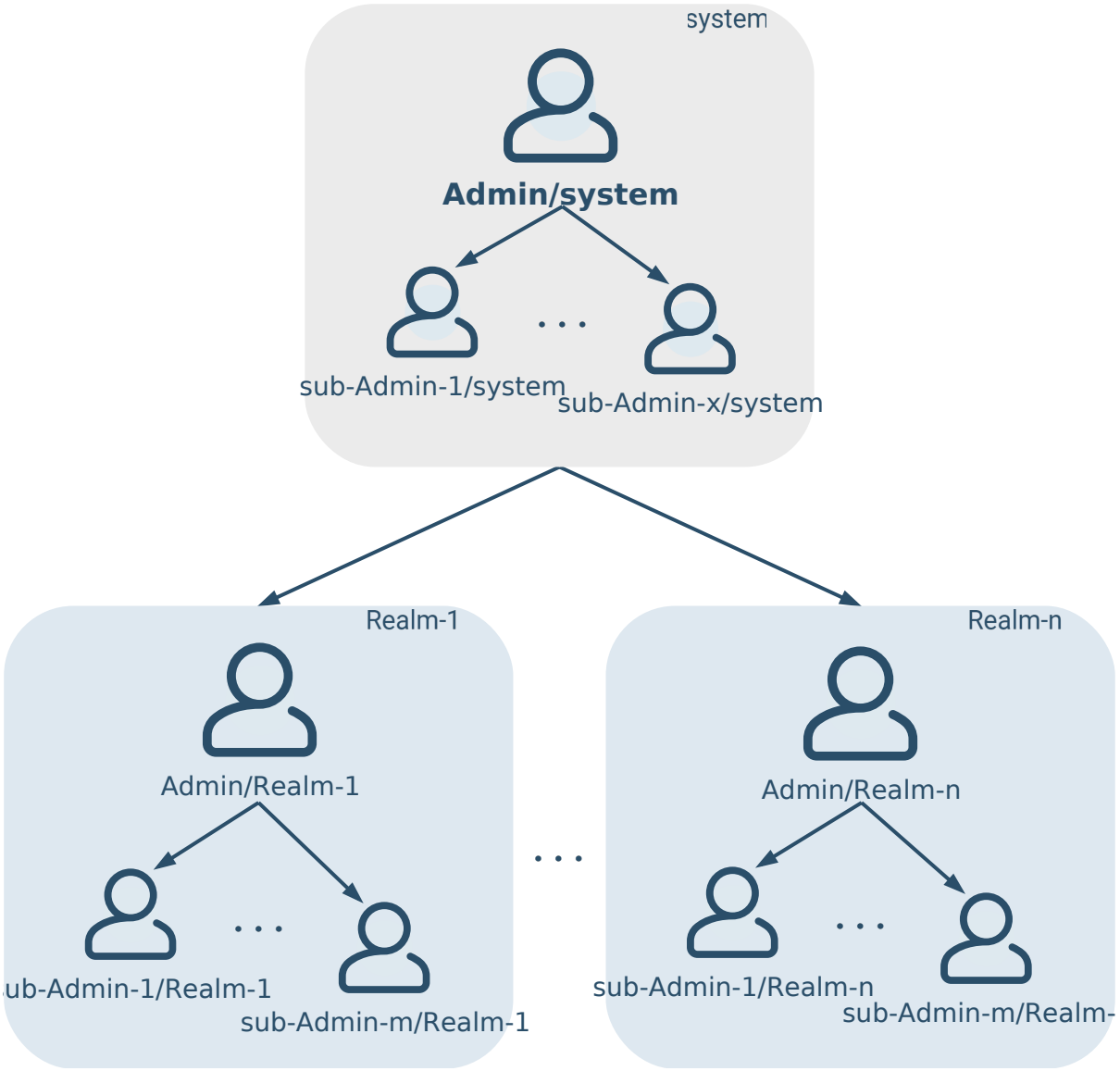
Name	Description
Step 1. Create an export rule.	In the **Device management → Settings export** section, click **Add** and enter a name and description for the rule

Name	Description
Step 2. Specify the remote server parameters.	In the **Remote server** tab of the rule, specify the parameters for the remote server: • **Server type**: FTP or SSH • **Address**: the server's IP address • **Port**: the server's port • **Login name**: the user account on the remote server • **Password/Confirm password**: the password for the user account • **Directory path**: the path on the server where the settings will be uploaded
Step 3. Select the upload schedule.	In the **Schedule** tab of the rule, specify when the settings should be uploaded. If specifying the time in the CRONTAB format, enter it as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday) Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • The asterisk and dash are also used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

Administrators

Hierarchical Administrator Account System

UGMC implements a hierarchical administrator account system. The top level (system) consists of the administrator accounts for the UGMC system itself. The lower level consists of the administrator accounts for managed realms, logical objects designed to manage a group of controlled devices (for more information on managed realms, see the Managing Realms section).



During the initial setup of UGMC, a local administrator with the `Admin/system` login is created, acting as the root administrator of the system. The UGMC administrator can manage general and network settings for UGMC, activate UGMC licenses, create and edit system library items, manage update and backup policies, and monitor UGMC operation using system logs. The UGMC administrator can create additional UGMC sub-administrator accounts, delegating some system management rights to them.

The UGMC administrator also creates managed realms, but does not have permission to manage devices within those realms. To do this, the UGMC administrator creates root administrator accounts for managed realms (`Admin/Realm`). The root administrator of the realm has full rights to manage the realm and the devices within it. They can create servers and realm authentication profiles, user directories, managed device configuration templates, organize templates into configuration groups, and link managed device objects to them. The root administrator of a managed realm can create additional accounts of realm sub-

administrators (`sub-Admin/Realm`) or, in other words, regional administrators, delegating to them the rights to administer only individual allocated devices.

Managing Administrator Accounts

To add an administrator:

1. Create an administrator profile. The profile defines the list of administrator permissions. You can create multiple profiles with different permissions. You can also create a root administrator profile for the realm.

2. Create an administrator account. At this stage, you can choose the administrator authentication method: local, through the LDAP connector, or using an authentication profile.

Creating an Administrator Profile

To create a UGMC administrator profile:

1. In the UGMC management web console, go to the **Management center → Administrators** section, and in the **Administrator profiles** block, click **Add**.

2. In the **Profile settings** window, on the **General** tab, specify the profile name.

3. Select the **UserGate Management Center Administrator** administrator type.

4. On the **Permissions** tab, select what access rights the administrator with this profile will have. You can specify the following access permissions: **No access**, **Read**, **Read and write**.

5. Save the changes.

To create a root administrator profile for the realm:

1. Ensure that the required realm has been created in the system. For more details, see the Creating Managed Realms section.

2. In the UGMC management web console, go to the **Management center → Administrators** section, and in the **Administrator profiles** block, click **Add**.

2. In the **Profile settings** window, on the **General** tab, specify the profile name.

3. Select the administrator type **Realm administrator** and the previously configured managed realm.

4. Save the changes.

Root administrators of realms have all permissions within their realm. In realm management mode, they can create sub-administrator accounts for the realm and manage their access permissions.

Creating a Local Administrator Account

To create a local administrator account:

1. In the UGMC web management console, in the **Management center → Administrators** section, in the **Administrators** block, click **Add** and select **Add local administrator**.

2. In the **Administrator properties** window, specify the administrator's name, login, and password.

3. Select the administrator profile created earlier.

4. Select the **Enabled** checkbox to allow logging in with this account.

5. Save the changes.

> **Important!**
> **Only a local administrator account can be created for the root administrator of the realm. This is because different LDAP servers can be used for authenticating UGMC service administrators and realm administrators. If you need to use LDAP administrators to manage a realm, you must create them in the realm's web interface. For more details on realm administrators, see the Realm Administrators section».**

Creating a LDAP Administrator Account

To create a user account from an existing domain:

1. Make sure that the appropriate LDAP connector is pre-configured in the **Authentication servers** section. For more details on configuring the LDAP connector, see the Authentication Servers section.

2. In the UGMC web management console, in the **Management center → Administrators** section, in the **Administrators** block, click **Add** and select **Add LDAP user**.

3. In the **LDAP administrator properties** window, click **Select**, choose the configured LDAP connector, and then add the desired user's login.

4. Select the administrator profile created earlier.

5. Select the **Enabled** checkbox to allow logging in with this account.

6. Save the changes.

When logging into the web administration interface under this account, you must specify the login in the format `<login>@<domain>/system` or `<domain>\<login>/system`.

To add a user group account from an existing domain:

1. Make sure that the appropriate LDAP connector is pre-configured in the **Authentication servers** section. For more details on configuring the LDAP connector, see the Authentication Servers section.

2. In the UGMC web management console, in the **Management center → Administrators** section, in the **Administrators** block, click **Add** and select **Add LDAP group**.

3. In the **LDAP administrator properties** window, click **Select**, choose the configured LDAP connector, and then add the desired user group login.

4. Select the administrator profile created earlier.

5. Select the **Enabled** checkbox to allow logging in with this account.

6. Save the changes.

When logging into the web administration interface under this account, you must specify the login in the format `<login>@<domain>/system` or `<domain>\<login>/system`.

Creating an Administrator Account with an Authentication Profile

You can manage administrator access to the UGMC web management console using an authentication profile, which lists preconfigured servers such as LDAP, TACACS+, or RADIUS as available authentication methods. If an authentication profile specifies multiple authentication methods, each method will be tried in turn until the first one that works.

To add an administrator account with an authentication profile:

1. Make sure the **Authentication servers** section contains information about the configured authentication server. For more details about the authentication server, see the Authentication Servers section.

2. Make sure that a profile with the required authentication method has been created in the **Authentication profiles** section. For more details on creating profiles, see the Authentication Profiles section.

3. In the UGMC web management console, in the **Management center → Administrators** section, in the **Administrators** block, click **Add** and select **Add administrator with an authentication profile**.

4. In the **Properties of the administrator with an authentication profile** window, specify the administrator's name, login, and password.

5. Select the administrator profile created earlier.

6. Select the authentication profile created earlier.

7. Select the **Enabled** checkbox to allow logging in with this account.

8. Save the changes.

Additional Security Options for Administrator Accounts

A UGMC administrator can configure additional administrator account protection settings, such as password complexity and temporary account blocking on exceeding the max authentication failures time.

> **Note**
> **The advanced administrator account security settings apply only to local accounts. If an account from an external directory (such as LDAP) is selected as the device administrator, the security settings for that account are determined by that external directory.**

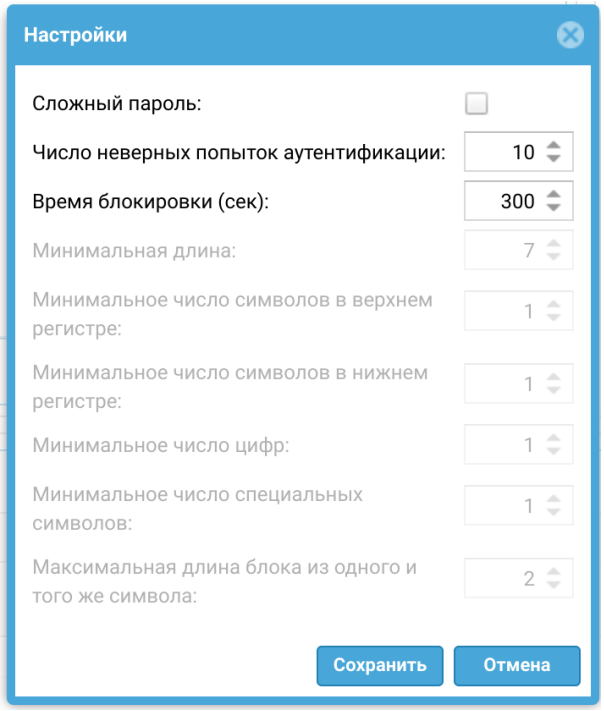
To configure additional security settings:

1. In the **Management center → Administrators** section, in the **Administrators** block, click **Configure**.

2. Configure the required parameters:

   - **Strong password**: enables the additional password complexity settings presented below, such as minimum length, minimum uppercase letters, minimum lowercase letters, minimum digit letters, minimum special characters, and maximum characters repetition block.

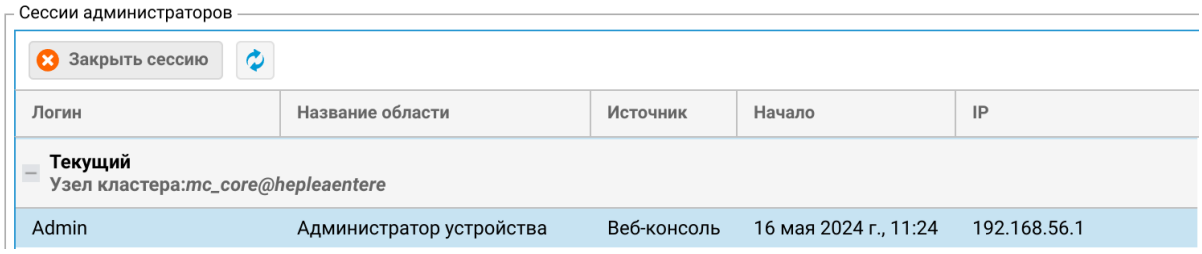
- **Number of invalid auth attempts**: the number of failed attempts to authenticate as an administrator after which the account is blocked for **Block time**.
- **Block time**: the time for which the account is blocked.



3. Save the changes.

Administrator Sessions

The **Administrators → Administrator sessions** section displays all administrators who are logged in to the UGMC administrative web console. Any of the administrator sessions can be reset (closed) if necessary.



Certificates

UGMC uses the secure HTTPS protocol to manage the device To perform these functions, UGMC employs a certificate of **Web console SSL certificate** type.

To create a new certificate, follow these steps:

Name	Description
Step 1. Create a new certificate.	In the **Certificates** section, click **Create**
Step 2. Fill in the relevant fields.	Provide values for these fields: • **Name**: the name under which the certificate will be displayed in the certificate list. • **Description**: a description of the certificate. • **Country**: the country where the certificate is being issued. • **State or province name**: the state or province where the certificate is being issued • **Locality name**: the city or town where the certificate is being issued. • **Organization name**: the name of the organization to which the certificate is being issued. • **Common name**: the certificate name. To ensure compatibility with the majority of browsers, we recommend using only Latin characters. • **E-mail**: your company's email
Step 3. Specify the purpose of the certificate.	After creating the certificate, specify its intended role in UGMC. To do that, select the relevant certificate in the certificate list, click **Edit**, and specify the Web console SSL certificate type. After that, UGMC will restart the web console service and invite you to connect using the new certificate.

UGMC allows you to export certificates created there and import certificates created in other systems — e.g., a certificate issued by a CA that your organization trusts.

To export a certificate, follow these steps:

Name	Description
Step 1. Select a certificate for export.	Select the desired certificate in the certificate list.

Name	Description
Step 2. Export the certificate.	Select the export type: • **Export certificate**: export certificate data in the .der format without exporting the certificate's private key. • **Export CSR**: export a CSR, e.g., to be signed by a CA.

> **Note**
> **It is recommended to save the certificate to be able to restore it later.**

> **Note**
> **For security purposes, UGMC does not allow the export of private keys for certificates.**

To import a certificate, you need to have the certificate files (and, optionally, the private key for the certificate). If you have those, follow the steps below:

Name	Description
Step 1. Start the import procedure.	Click **Import**
Step 2. Fill in the relevant fields.	Provide values for these fields: • Name: the name under which the certificate will be displayed in the certificate list. • Description: a description of the certificate. • Certificate file: upload the certificate data file. • Private key: upload the private key file for the certificate. • Passphrase: specify the private key passphrase (if required). • Certificate's chain: a file containing the upstream CA certificates used when creating this certificate. This field is optional.

Auth servers

Authentication servers (auth servers) are external sources of user accounts used for authorization in the UGMC web console. UGMC supports the following types of authentication servers: LDAP connector, RADIUS, and TACACS+.

LDAP Connector

An LDAP connector allows you to:

- Obtain information on users and groups from Active Directory or other LDAP servers. FreeIPA is supported with an LDAP server.
- Authorize UGMC administrators via Active Directory and FreeIPA domains.

To add an LDAP connector:

1. On the **Management Center** page, under **Management Center → Auth Servers**, click **Add** and select **Add LDAP Connector**.

2. In the **LDAP connector properties** window, specify the name of the LDAP connector.

3. In the **LDAP domain name or IP address** field, specify the IP address of the domain controller, the FQDN of the domain controller, or the FQDN of the domain (e.g., `test.local`). If the domain controller FQDN is specified, UserGate will obtain the domain controller's address using a DNS request. If the domain FQDN is specified, UserGate will use a backup domain controller if the primary one fails.

4. In the **Bind DN (login)** field, specify the login to use to connect to the LDAP server. The login must be specified in the **<domain>\<login>** or **<login>@<domain>** format. This user must be already created in the domain.

5. Specify the user's password for connecting to the domain.

6. If necessary, on the **LDAP domains** tab, add domains served by the specified domain controller. For example, if you are using a domain tree or Active Directory domain forest. You can also specify the short netbios name of the domain here.

7. On the **Search roots** tab, specify the paths from which the system will search for users and groups. Specify the full name, e.g., `ou=Office,dc=example,dc=com`.

8. If necessary, on the **Settings** tab, select the **Use SSL for connections** checkbox to use an SSL connection to connect to the LDAP server.

9. Select the **Enabled** checkbox to start using the LDAP connector, and save your changes.

After creating a server, you should validate the settings by clicking **Check connection**. If your settings are correct, the system will report that; otherwise, it will tell you why it cannot connect.

The LDAP connector configuration is now complete. To log in to the UGMC web management console, LDAP users must specify a login in the format `<domain>\<login>/system` or `<login>@<domain>/system`.

RADIUS Authentication Server

You can authorize users in the UGMC web management console using a RADIUS authentication server, with the console working as a RADIUS client. When authorization is done using a RADIUS server, UGMC sends the username and password information to the RADIUS server, which then responds whether the authentication was successful.

> **Important!**
> **Before performing the steps below, ensure that the RADIUS server is configured to work with UGMC (an entry with the UGMC IP address has been added to the "RADIUS Clients and Servers" section). Otherwise, the server will not respond to requests. An example of RADIUS server configuration is provided in the Authorization using RADUIS section.**

To add a RADIUS server:

1. On the **Management Center** page, under **Management Center → Auth Servers**, click **Add** and select **Add RADIUS server**.

2. In the **Connector RADIUS server properties** window, specify the name of the RADIUS server.

3. Add the RADIUS server IP address and the UDP port on which the RADIUS service listens for authentication requests (default: 1812).

4. In the **Secret** field, enter the password specified when configuring the RADIUS server.

5. Select the **Enabled** checkbox to start using the RADIUS server and save the changes.

To authenticate users in the UGMC web management console using the RADIUS server, you must configure an authentication profile. For more details on creating and configuring profiles, see the Authentication Profiles section.

TACACS+ Authentication Server

You can authorize users in the UGMC web management console using a TACACS+ authentication server. When using a TACACS+ server, UserGate MC transmits the username and password to it, after which the TACACS+ server responds whether authentication was successful or not.

To add a TACACS+ server:

1. On the **Management Center** page, under **Management Center → Auth Servers**, click **Add** and select **Add TACACS+ server**.

2. In the **TACACS+ server properties** window, specify the name of the server.

3. In the **Secret** field, enter the shared key used by the TACACS+ protocol for authentication.

4. Specify the IP address of the TACACS+ server and the UDP port on which the TACACS+ server listens for authentication requests.

5. If you want to use a single TCP connection to the TACACS+ server, select the corresponding checkbox.

6. If necessary, change the TACACS+ server timeout for authentication. The default is 4 seconds.

7. Select the **Enabled** checkbox to start using the RADIUS server and save the changes.

To authenticate users in the UGMC web management console using the TACACS+ server, you must configure an authentication profile. For more details on creating and configuring profiles, see the Authentication Profiles section.

Authentication Profiles

A profile can be used to define a set of methods to be used for user authentication in the UG web management console.

> **Important!**
> **Before adding an authentication profile, you must configure the required authentication server.**

To add an authentication profile:

1. In **Management Center → Authentication Profiles**, click **Add**.

2. In the **Auth profile properties** window, on the **General** tab, specify the profile name.

3. If necessary, configure one or more settings:

   - **Idle time**: the time after which a user's authorization will be revoked if they are inactive (if there are no network packets with the user's IP address). After this, the user will be required to re-authorize.
   - **Session expiration time**: the time after which a user's authorization will be revoked. After this, the user will be required to re-authorize.
   - **Maximum auth attempts (local users)**: the number of failed authentication attempts allowed before a local user account is locked.
   - **Local user lockout time**: the time a local user account will be locked after the specified number of failed authentication attempts has been reached.

4. On the **Authentication methods** tab, click **Add**, and when clicking **Add** to select a preconfigured authentication server: LDAP connector, RADIUS server, or TACACS+ server.

5. Save the changes.

You can now use the created profile when creating administrator accounts.

Libraries of items

IP Addresses

The IP addresses section contains the list of IP address ranges that can be used to configure UGMC. A predefined address list is supplied with the product. The

administrator can add the desired items during use. To add a new address list, follow these steps:

Name	Description
Step 1. Create a list.	In the **Groups** pane, click **Add** and give a name to the IP address list.
Step 2. (Optional) Specify the list update address.	Specify the address of the server where the updatable list is stored. For more details on updatable lists, see later in this chapter.
Step 3. Add IP addresses.	In the **Selected group addresses** pane, click **Add** and enter the addresses. An IP address entry can be in the form of an individual IP address, IP address/subnet mask, or IP address range (192.168.1.5, 192.168.1.0/24, or 192.168.1.5-192.168.2.100, respectively).

The administrator can create custom IP-address lists and distribute them centrally to all devices where UserGate is installed. To create such a list, follow these steps:

Name	Description
Step 1. Create a file with the desired IP addresses.	Create a file named **list.txt** with the IP address list. The address list is written to a plain text file in a column without any punctuation. Example: `x.x.x.x` `y.y.y.y` `z.z.z.z`
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.
Step 4. Upload the files to a web server.	Upload the **list.zip** and **version.txt** files to your website so that they can be downloaded.
Step 5. Create an IP address list and specify an update URL for it.	On each device, create an IP address list. When creating the list, select **Updatable** as the list type and enter the address for downloading updates. The device will check for a new version

Name	Description
	on your website according to the set update download schedule. **Note** The list URL format is http://x.x.x.x/ or ftp://x.x.x.x/. The schedule can be configured in the list properties. The available options are: • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

Emails

The **Emails** library item allows you to create email groups that can later be used in notification rules.

To add a new email group, follow these steps:

Name	Description
Step 1. Create an email group.	In the **Email groups** pane, click **Add** and give a name to the new group.

Name	Description
Step 2. Add emails to the group.	Highlight the group just created, click **Add** in the **Emails** pane, and add the desired email addresses.

The administrator can create custom email lists and distribute them centrally to all computers where UserGate is installed. To create such a list, follow these steps:

Name	Description
Step 1. Create a file with the relevant email list.	Create a file named **list.txt** with the email list.
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.
Step 4. Upload the files to a web server.	Upload the **list.zip** and **version.txt** files to your website so that they can be downloaded.
Step 5. Create an email list and specify an update URL for it.	On each UserGate server, create an email list. When creating the list, select **Updatable** as the list type and enter the address for downloading updates. UserGate will check for a new version on your website according to the set update download schedule. The schedule can be configured in the list properties. The available options are: • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last).

Name	Description
	• A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

Phones

The **Phones** library items allows you to create phone groups that can later be used in SMPP notification rules.

To add a new phone group, follow these steps:

Name	Description
Step 1. Create a phone group.	In the **Phone groups** pane, click **Add** and give a name to the new group.
Step 2. Add phone numbers to the group.	Highlight the group just created, click **Add** in the **Phones** pane, and add the desired phone numbers.

The administrator can create custom phone lists and distribute them centrally to all computers where UserGate is installed. To create such a list, follow these steps:

Name	Description
Step 1. Create a file with the relevant phone list.	Create a file named **list.txt** with the phone list.
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.
Step 4. Upload the files to a web server.	Upload the **list.zip** and **version.txt** files to your website so that they can be downloaded.
Step 5. Create a phone list and specify an update URL for it.	On each UserGate server, create a phone list. When creating the list, select **Updatable** as the list type and enter the address for downloading updates. UserGate will check for a new version on your website according to the set update download

Name	Description
	schedule. The schedule can be configured in the list properties. The available options are: • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

Notification Profiles

A notification profile defines a transport that can be used to deliver notifications to the users. Two types of transport are supported:

- SMTP for delivering messages by email
- SMPP for message delivery by SMS via virtually any cellular provider or the numerous SMS distribution centres.

To create an SMTP notification profile, go to the **Notification profiles** section, click **Add**, select **Add SMTP notification profile**, and fill in the relevant fields:

Name	Description
Name	Profile name.
Description	Profile description.
Host	The IP address of the SMTP server that will be used for sending emails.
Port	The TCP port used by the SMTP server. Usually, SMTP uses port 25, and SMTP with SSL uses port 465. Consult your email server administrator regarding this value.
Connection security	The following outgoing email security options are available: None, STARTTLS, and SSL.
Authentication	Turns on authentication for SMTP server connection.
Login name	The account name for connecting to the SMTP server.
Password	The account password for connecting to the SMTP server.

To create an SMPP notification profile, go to the **Notification profiles** section, click **Add**, select **Add SMPP notification profile**, and fill in the relevant fields:

Name	Description
Name	Profile name.
Description	Profile description.
Host	The IP address of the SMPP server that will be used for sending SMS messages.
Port	The TCP port used by the SMPP server. Usually, SMPP uses port 2775, and SMPP with SSL uses port 3550.
SSL	Specifies whether or not SSL encryption is used.
Login name	The account name for connecting to the SMPP server.
Password	The account password for connecting to the SMPP server.
Phone translation rules	In certain cases, the SMPP provider expects a phone number in a specific format, such as 0123456789. To meet the provider's requirements, you can configure the replacement of the leading phone number digits with others. For example, you can replace the leading +971 with 0.

Expanding the System Partition

To expand the system partition while preserving the configuration and data of the UserGate node, follow these steps:

Name	Description
Step 1. Add a new virtual disk.	Use the hypervisor to add a **new** disk of the required size in the UserGate virtual machine properties.
Step 2. Expand the partition size in the system utilities.	In the UserGate node boot menu, enter the **Support menu** section. In the section that opens, select **Expand data partition** and start the partition expansion process.
Step 3. Check the size of the system partition.	When the expansion process is complete, boot the node and check the size of the system partition in the **Dashboard → Disks** section.

> **Note**
>
> **Expanding the system partition by increasing the size of the *existing* virtual machine disk is only possible if you reset the node to factory settings, i.e. perform a factory reset.**

NETWORK CONFIGURATION

Network Configuration (Description)

This section describes UGMC network settings.

Zone Configuration

A zone in UGMC is a logical aggregation of network interfaces. UGMC security policies use interface zones instead of interfaces themselves.

It is recommended to aggregate interfaces into a zone based on their intended use, e.g., a LAN interface zone, Internet interface zone, management interface zone, etc.

UGMC is supplied with the following default zones:

Name	Description
Management	Used to connect trusted networks from which UGMC management is allowed.
Trusted	Used to connect the managed devices and obtain access to the Internet.

For the UGMC to work, one configured interface is sufficient. Having separate network interfaces for UGMC device management and UserGate MD management is recommended for security but not mandatory.

UGMC administrators can edit the settings for the default zones and create additional zones.

> **Note**
>
> **A maximum of 255 zones can be created.**

To create a zone, follow these steps:

Name	Description
Step 1. Create a new zone.	Click **Add** and provide a name for the new zone.
Step 2. (Optional) Configure the DoS protection settings for the zone.	Configure the network flood protection settings for TCP (SYN-flood), UDP, and ICMP protocols in the zone: • **Alert threshold**: when the number of requests from a single IP address exceeds this threshold, the event is recorded in the system log. • **Drop threshold**: when the number of requests from a single IP address exceeds this threshold, UGMC starts dropping the packets from that address and records the event in the system log. The recommended values are 300 requests per second for the alert threshold and 600 requests per second for the drop threshold. **DoS protection exclusions**: here you can list the server IP addresses that need to be excluded from the protection. This

Name	Description
	can be useful, e.g., for UserGate gateways that can send large amounts of data to LogAn servers.
Step 3. (Optional) Configure the access control settings for the zone.	Specify the UGMC-provided services that will be available to clients connected to this zone. It is recommended to disable all services for zones connected to uncontrolled networks, such as the Internet. The following services exist: • **Ping**: enables pinging of UGMC. • **SNMP**: provides SNMP access to UserGate (UDP 161). • **Administrative console**: provides access to the administrative web console (TCP 8010 and 8300). • **Control XML-RPC**: enables API control of the product (TCP 4042). • **VRRP**: required for combining several NGFWs into a HA cluster (IP protocol 112). • **Cluster**: required for combining several vNGFWs into a cluster (TCP 4369, TCP 9000-9100). • **CLI over SSH**: provides server access for management using CLI (command line interface) (TCP port 2200). • **UserGate Management Center service**: used for connecting NGFWs and LogAn devices (TCP 2022, 9712). • **API XML RPC over HTTPS**: allows access to the API over HTTPS (TCP 4443). Available in software version 7.3.3 and higher. For more on network availability requirements, see the appendix Network Environment Requirements.
Step 4. (Optional) Configure the IP spoofing protection settings.	IP spoofing attacks allow a malicious actor to transmit a packet from one network, such as **Trusted**, to another, such as **Management**. To do that, the attacker substitutes the source IP address with an assumed address of the relevant network. In this case, responses to this packet will be sent to the internal address. To protect against this kind of attack, the administrator can specify the source IP address ranges allowed in the selected zone. Network packets with source IP addresses other than those specified will be discarded. Using the **Negate** checkbox, the administrator can specify the source IP addresses from which packets may not be received on this zone's interfaces. In this case, packets with source IP addresses within those ranges will be rejected. As an example, you can specify "gray" IP address ranges as 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 and enable the **Negate** option.

Network Interface Configuration

The **Interfaces** section displays all physical and virtual network interfaces existing in the system and allows you to modify their settings as well as add VLAN and bond interfaces.

Using the **Edit** button, you can modify the settings for a network interface:

- Enable or disable the interface
- Specify the interface type as Layer 3.
- Assign a zone to the interface
- Modify the physical parameters of the interface, such as the MAC address, MTU size, MSS size.
- Select the IP address assignment type: no address, a static IP address, or a dynamic IP address obtained using DHCP.

Using the **Add** button, you can add the following logical interface types:

- VLAN
- Bond.

Creating a VLAN Interface

Using the **Add VLAN** button, the administrator can create sub-interfaces. To create a VLAN, provide the following settings:

Name	Description
Enabled	Enables the VLAN.
Name	The VLAN name. Assigned automatically based on the physical port name and the VLAN tag.
Description	An optional interface description.
Type	Specify the interface type as Layer 3 or Mirror.
VLAN tag	The sub-interface number. Up to 4094 interfaces can be created.
Node name	The node name in the cluster where this VLAN is being created.

Name	Description
Interface	The physical interface on which the VLAN is being created.
Zone	The zone to which the VLAN belongs.
Alias	An alternative interface name assigned by the administrator. This optional setting is used for working with SNMP. The value is a string with a length of up to 64 characters. **Important!** Cyrillic characters are not allowed in the value.
Networking	The IP address assignment method: no address, a static IP address, or a dynamic IP address obtained using DHCP. The ability to change the MAC address, MTU size, MSS size (available starting with software release 7.3.x).

Bonding Network Interfaces

Using the **Add bond** button, the administrator can bond several physical network interfaces into a single aggregated logical interface to increase the bandwidth or provide high availability. To create a bond, provide the following settings:

Name	Description
Enabled	Enables the bond.
Name	The bond name.
Zone	The zone to which the bond belongs.
Interfaces	One or more network interfaces that will be used to create the bond.
Aggregation mode	The aggregation mode must match the operating mode for the device to which the bond is connected. The options are: • **Round robin**. Packets are sent consecutively, starting from the first available slave and continuing to the last one. This policy is used to provide load balancing and high availability. • **Active backup**. Only one network interface in the bond will be active. Another slave interface can become active only if the currently active interface fails. With this policy, the MAC address of the bond interface is only visible externally through one network port to avoid problems with the switch. This policy is used for high availability. • **XOR**. Transmission is distributed between the slave interfaces using the formula: [(XOR) MOD]. This means that the same NIC sends packets to the same recipients.

Name	Description
	Optionally, the transmission allocation can also be based on the xmit_hash policy. The XOR policy is used to provide load balancing and high availability. • **Broadcast**. Transmits everything on all network interfaces. This policy is used for high availability. • **IEEE 802.3ad**. The default mode, supported by most network switches. Creates aggregated groups of NICs with identical speed and duplex settings. When combined like this, all links in the active aggregation participate in transmission as per IEEE 802.3ad. The choice of interface for packet transmission is determined by the policy. By default, the XOR policy is used, with the xmit_hash policy as a possible alternative. • **Adaptive transmit load balancing**. The outgoing traffic is distributed depending on the load on each slave interface (determined by the download speed). No additional configuration on the switch is required. The incoming traffic is received by the current network card. If this card fails, another card assumes the MAC address of the failed one. • **Adaptive load balancing**. Includes the previous policy plus incoming traffic balancing. No additional configuration on the switch is required. The incoming traffic is balanced through ARP negotiation. The driver intercepts ARP responses sent from the local NICs to the outside and overwrites the source MAC address with one of the unique MAC addresses of the NIC in the bond. Thus, different devices use different server MAC addresses. The incoming traffic is balanced sequentially (round-robin) among the interfaces.
MII monitoring period (msec)	Sets the MII monitoring period in milliseconds. Determines how often the link state will be checked for failures. The default value of 0 disables MII monitoring.
Down delay (msec)	Sets the delay in milliseconds before disabling the interface on a connection failure. This option is only valid for MII monitoring (miimon). The parameter value must be a multiple of miimon, otherwise it will be rounded to the nearest multiple. Default value: 0.
Up delay (msec)	Sets the delay in milliseconds before bringing up the link on discovering that it has been restored. This parameter is only valid with MII monitoring (miimon). The parameter value must be a multiple of miimon, otherwise it will be rounded to the nearest multiple. Default value: 0.
LACP rate	

Name	Description
	Determines the interval between LACPDU packets sent by the partner in the 802.3ad mode. Enumerated options: • **Slow**: requests that the partner send LACPDU packets every 30 seconds. • **Fast**: requests that the partner send LACPDU packets every second.
Failover MAC	Determines how MAC addresses will be assigned to the bonded slaves in the active-backup mode on switching between slaves. The normal behavior is to use the same MAC address on all slaves. Enumerated options: • **Disabled**: sets the identical MAC address on all slaves during the switching process. • **Active**: the MAC address on the bond interface will always be identical to that on the currently active slave. The MAC addresses on the backup interfaces are not changed. The MAC address on the bond interface changes during the failover processing. • **Follow**: the MAC address on the bond interface will be the same as that on the first slave added to the bond. This MAC is not set on the second and subsequent interfaces while they are in backup mode. That MAC address gets assigned during a failover: when a backup slave interface becomes active, it assumes a new MAC (the one on the bond interface), and the formerly active slave is assigned the MAC that the currently active one used to have.
Xmit hash policy	Determines the hash policy for packet transmission via bonded interfaces in the XOR or IEEE 802.3ad modes. Enumerated options: • **Layer 2**: only MAC addresses are used for hash generation. With this algorithm, the traffic for a particular network host is always sent over the same interface. This algorithm is compatible with IEEE 802.3ad. • **Layer 2+3**: both MAC and IP addresses are used for hash generation. This algorithm is compatible with IEEE 802.3ad. • **Layer 3+4**: IP addresses and transport-layer protocols (TCP or UDP) are used for hash generation. This algorithm is not universally compatible with IEEE 802.3ad, as both fragmented and non-fragmented packets can be transmitted within a single TCP or UDP interaction. Fragmented packets lack the source and destination ports. As a result, packets from the same session can

Name	Description
	reach the recipient in an order other than the intended one because they are sent via different slaves.
Networking	The IP address assignment method: no address, a static IP address, or a dynamic IP address obtained using DHCP. The ability to change the MAC address, MTU size, MSS size (available starting with software release 7.3.x).

Gateway Configuration

To connect UGMC to the Internet, you need to specify the IP address(es) of one or more gateways.

If several Internet providers are used for Internet connections, several gateways can be specified. Here is an example of a network configuration with two providers:

- Interface port1 with an IP address of 192.168.11.2 is connected to Internet Provider 1. To enable Internet access via this provider, a gateway with an IP address of 192.168.11.1 must be added.
- Interface port2 with an IP address of 192.168.12.2 is connected to Internet Provider 2. To enable Internet access via this provider, a gateway with an IP address of 192.168.12.1 must be added

When two or more gateways exist, there are two options:

Name	Description
Traffic load balancing between gateways	Set the **Balancing** checkbox and assign a **Weight** to each gateway. In this case, all traffic destined for the Internet will be distributed between the gateways according to the weights assigned (the greater the weight, the larger portion of the traffic will pass through the gateway).
Main gateway with failover	Select one of the gateways as the main and configure the **Conn ectivity checker** by clicking the button with that name. The connectivity checker periodically verifies if the host is accessible from the Internet with the interval specified in the settings and, if the host ceases to be reachable, switches all traffic to the backup gateways in the order they are listed in the console.

By default, the network connectivity checker is configured to use Google's public DNS server (8.8.8.8), but this can be changed to any other host if the administrator so desires.

Routes

This section describes how to specify a route to a network that is behind a specific router. For example, a local network can have a router that combines several IP subnets.

To add a route, follow these steps:

Name	Description
Step 1. Provide a name and description for the route.	In the **Network** section, select **Routes** in the menu and click **Add**. Provide a name for the new route. Optionally, you can also provide a description for the route.
Step 2. Specify the destination address.	Specify the subnet where the route will point to, such as 172.16.20.0/24 or 172.16.20.5/32.
Step 3. Specify the gateway.	Specify the IP address of the gateway through which the above subnet will be accessible. This IP address must be reachable from the UGMC server.
Step 4. Specify the network interface.	Specify the network interface through which the route will be added. If you keep the default value, **Automatically**, UGMC will determine the interface based on the IP address settings of the available network interfaces.
Step 5. Specify the metric.	Specify the metric for the route. The lower the metric value, the higher the route's priority, if there are multiple routes to this network.

LOGS AND REPORTS

Event Log

The log contains records for events related to changing UGMC settings as well as console authorization, server boot/shutdown/reboot, etc.

To assist in finding the events you need, you can filter the records by various criteria, such as date range, component, severity, or event type.

In addition, UserGate Management Center provides an advanced search mode where you can create complex filters using a specialized query language whose syntax is described in the next section, Advanced Search Mode.

After configuring the desired parameters, you can save the resulting filter by clicking **Save as**. The list of saved filters can be viewed in the **Favorite filters** tab.

The administrator can select the columns that will be logged. To do that, point the mouse cursor at the name of any column, click the arrow that will appear to the right of the column name, choose **Columns**, and select the desired parameters in the context menu.

By clicking **Export as CSV**, the administrator can save the filtered log data in a .csv file for subsequent analysis.

Click **Show** to open a window with a detailed event description.

Logs Export

The UserGate logs export feature allows you to upload information to external servers for later analysis or SIEM (security information and event management) processing.

Sending logs to SSH (SFTP), FTP, and Syslog servers is supported. Logs are sent to SSH and FTP servers according to the schedule specified in the configuration or as a one-time action (using the button **Send once**). For Syslog servers, logs are sent immediately after a record is added to the log.

To send logs, you must first create log export rules in the **Logs and Reports → Logs export** section in device administrator mode.

> **Note**
> **Log export settings are not cluster-wide. If UGMC is running in a cluster configuration, log export rules are created separately on each node.**

When creating a configuration, provide the following parameters:

Name	Description
Rule name	The name of the log export rule.

Name	Description
Description	Optional field for rule description.
Logs to export	Select the log files to export: • Events For each log, you can specify the export syntax: • CEF: Common Event Format (ArcSight) • JSON: JSON format • @CEE: JSON: CEE Log Syntax (CLS) Encoding JSON To select the desired log export format, refer to the documentation for the SIEM system you are using. For a detailed description of log formats, see Description of Log Formats.
Server type	SSH (SFTP), FTP, Syslog.
Server address	IP address or domain name of the server.
Transport	TCP or UDP; applicable only to Syslog servers.
Port	The server port to which the data should be sent.
Protocol	RFC5424 or BSD syslog RFC 3164; applicable only to Syslog servers. Select the protocol compatible with your SIEM system.
Severity	Only for Syslog server type. Optional field; consult the documentation for your SIEM system. Available values: • **Alert**: a state that requires immediate intervention. • **Critical**: a state that requires immediate intervention or signals a fault in the system. • **Errors**: errors detected in the system. • **Warnings**: warnings on potential errors that can occur if no action is taken. • **Notice**: events that relate to unusual system behavior but are not errors. • **Info**: informational messages.
Facility	Only for Syslog server type. Optional field; consult the documentation for your SIEM system. Available values: • **User-level messages** • **System daemon**

Name	Description
	• **Security/authorization** • **Log audit** • **Log alert** • **Local 0**. • **Local 1**. • **Local 2**. • **Local 3**. • **Local 4**. • **Local 5**. • **Local 6**. • **Local 7**.
Hostname	Only for Syslog server type. A unique host name identifying the server that sends data to the Syslog server in the FQDN (Fully Qualified Domain Name) format.
App-Name	Only for Syslog server type. Unique name of the application that sends data to the Syslog server.
Login name	The account name for connecting to the remote server. Not applicable to the Syslog export method.
Password	Account password for connecting to the remote server. Not applicable to the Syslog export method.
Directory path	Server directory to copy log files to. Not applicable to the Syslog export method. In a UGMC cluster configuration, when exporting logs from different cluster nodes, you need to specify different directories on the server for each UGMC node, since the log file names on each node are identical.
Schedule	Select schedule for sending logs. Not applicable to the Syslog export method. The available options are: • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The

Name	Description
	fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
Manage logs	Manage temporary log files prepared for sending to remote SSH and FTP servers. When sending logs to SSH and FTP servers, UserGate saves the data to send in temporary files in UTF-8 encoding. Logs for previous days (based on the number of rotation days) are stored as archives; the log for the current day is not archived. The system copies all files created for sending to a remote server according to the specified schedule. It does not clean up or delete the files. This setting allows you to specify the rotation period for temporary files (in days) or delete any of the temporary files manually. The files are rotated once a day.

Note

The administrator can manually save the log directly from the web console. In this case, the data is saved only in CSV format.

Advanced Search Mode

Besides the basic GUI-based search, LogAn provides an advanced search capability, allowing you to create more complex search filters and use a specialized query language. To construct a query, use field names and values, keywords, and operators. You can enter field values using single or double quotes, or without quotes, if the values do not contain spaces. To group multiple conditions, use parentheses.

Separate keywords by spaces. You can use the following keywords:

Name	Description
AND/and	Logical AND: all query conditions must be met.
OR/or	Logical OR: at least one condition should be met.

The following operators define filter conditions:

Name	Description
=	Equal To. Requires that the field value be completely identical to the specified value. For example, ip=172.16.31.1 displays all log entries where the IP field exactly matches 172.16.31.1.
!=	Not Equal To. Field value must not match the specified value. For example, ip!=172.16.31 displays all log entries where the IP field does not match 172.16.31.1.
<=	Less Than or Equal To. Field value must be less than or equal to the specified value. This can only apply to fields that support comparisons, such as date, portSource, portDest, statusCode, etc., for example, date <= '2019-03-28T20:59:59' AND statusCode=303.
>=	Greater Than or Equal To. The field value must be greater than or equal to the specified value. This can only apply to fields that support comparisons, such as date, portSource, portDest, statusCode, etc., for example, date >= "2019-03-13T21:00:00" AND statusCode=200.
<	Less Than. The field value must be less than the specified value. This can only apply to fields that support comparisons, such as date, portSource, portDest, statusCode, etc., for example, date < '2019-03-28T20:59:59' AND statusCode=404.
>	Greater Than. The field value must be greater than the specified value. This can only apply to fields that support comparisons, such as date, portSource, portDest, statusCode, etc., for example, (statusCode>200 AND statusCode<300) OR (statusCode=404).
IN	Allows you to specify multiple values for a field in a query. Provide the list of values in parentheses, for example, category IN (botnets, compromised, 'illegal software', 'phishing and fraud', 'reputation high risk', 'unknown category').

Name	Description
NOT IN	Allows you to specify multiple values for a field in a query. Displays records that do not contain the specified values. Provide the list of values in parentheses, for example, category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud', 'reputation high risk', 'unknown category').
~	Contains. Allows you to specify a substring that the queried field must contain, for example, browser ~ "Mozilla/5.0". This operator is applicable only to fields that contain string data.
!~	Does Not Contain. Allows you to specify a substring that the queried field must not contain, for example, browser !~ "Mozilla/5.0". This operator is applicable only to fields that contain string data.
MATCH	To specify the substring that must be found in the specified field using the MATCH statement, use JSON format and single quotes, for example, details MATCH '\"module\":\"threats\"'. The syntax of queries using this operator is compliant with the RE2 standard. For more details about Google/RE2 syntax, see: https://github.com/google/re2/wiki/Syntax.
NOT MATCH	To specify the substring that must not be found in the specified field using the NOT MATCH statement, use JSON format and single quotes, for example, details NOT MATCH '\"module\":\"threats\"'. The syntax of queries using this operator is compliant with the RE2 standard. For more details about Google/RE2 syntax, see: https://github.com/google/re2/wiki/Syntax.

When you switch from basic to advanced search mode, LogAn automatically generates a search query string that matches the filter specified in the basic search mode.

DIAGNOSTICS AND MONITORING

Routes

The **Routes** section allows you to obtain a list of all routes specified on a particular UserGate host and a particular virtual router on the cluster node. To view routes, click the **Filter** button and specify the types of route that you want to display. You can specify the following route types:

- **Connected**: routes to networks connected directly to UserGate interfaces. These routes are marked with a **C** in the route list.
- **Statically defined**: routes defined statically under **Network → Routes**. These routes are marked with an **K** in the route list.
- **OSPF**: routes received via the OSPF protocol. These routes are marked with an **O** in the route list.
- **BGP**: routes received via the BGP protocol. These routes are marked with a **B** in the route list.

The route list displayed here can be downloaded as a text file by clicking the **Export all routes** button.

Ping

The ping utility can be used to diagnose the availability of network resources. Ping command parameters:

Name	Description
Ping host	The host to be checked.
TTL	The maximum number of intermediate hosts allowed on the path to the host to be pinged.
Interface	The selected interface address will be used as the source address for the ping command, and the interface for sending packets will be selected in accordance with the routing table.

Name	Description
Counter	Number of repetitions.
Show timestamp	Add timestamps to the command output.
Don't resolve names	Use IP addresses without resolving them to domain names.

Traceroute

The traceroute utility allows you to check the path of network packets to a particular host. Traceroute parameters:

Name	Description
Traceroute host	The host to be checked.
Use ICMP	Use ICMP to execute the traceroute command. If not specified, UDP is used.
Interface	Network interface from which to execute the command.
Don't resolve names	Use IP addresses without resolving them to domain names.

DNS Query

DNS queries allow administrators to check the functioning of DNS servers.

Name	Description
DNS query (host)	DNS name to check.
Query source IP	One of the IP addresses assigned to UserGate.
DNS server	DNS server to which the query should be sent.
Port	UDP port used to make the query.
DNS query type	Type of the query.

NOTIFICATIONS

SNMP

UserGate supports monitoring using the SNMP v2c and SNMP v3 protocols. Both SNMP queries and SNMP trap management are supported. This allows you to monitor critical UserGate parameters using the SMNP management software used in your company.

To configure monitoring using SNMP:

1. In the properties of the zone of the interface to which the connection will be made via the SNMP protocol, in the **Access control** tab, enable the **SNMP** service.

2. Create an SNMP rule.

To configure monitoring using SNMP, you need to create SNMP rules. To create an SNMP rule, click the **Add** button under **SNMP** and specify the following parameters:

Name	Description
Rule name	The name of the rule.
Server IP address for traps	The IP address of the trap server and the port on which the server will listen for notifications. Usually, it is UDP port 162. This setting is required only if you need to send traps to the notification server.
Community	SNMP community is a string that identifies the UserGate server and SNMP management server for SNMP v2c. Use only numbers and Latin letters.
Context	Optional parameter that defines the SNMP context. Use only Latin letters and numbers. Some devices may have multiple copies of the entire MIB subtree. For example, several virtual routers can be created on the device. Each such virtual router will have a complete MIB subtree. In this case, each virtual router can be specified as a context on the SNMP server. The context is identified by name. When the client makes a request, the context name can be specified. If the context name is not specified, the default context will be requested.

Name	Description
Version	Specify the version of the SNMP protocol used in the rule. Available options: SNMP v2c and SNMP v3.
Allow SNMP queries	When enabled, allows receiving and processing of SNMP requests from the SNMP manager.
Allow SNMP traps	When enabled, allows sending of SNMP traps to the server configured to receive notifications.
SNMP security profile name	For SNMP v3 only. For more details, see the SNMP Security Profiles section.
Events	Selecting the types of parameters available for monitoring by rule.

Note

Authentication settings for SNMP v2c (community) and SNMP v3 (user, authentication type, authentication algorithm, authentication password, encryption algorithm, encryption password in SNMP security profile) on the SNMP manager must match those of UserGate.

For information on configuring authentication settings for your SNMP manager, refer to the configuration guide for your SNMP management software.

UserGate is assigned the unique **SNMP PEN** (Private Enterprise Number) **45741**.

You can download current UserGate MIB files with monitoring parameters from the device administrator console. To do this, go to the **Diagnostics and monitoring** tab, then click **Download MIB** in the **Notifications → SNMP** section

You can download the following MIB files:

- UTM-TRAPS-MIB
- UTM-TRAPS-BINDINGS-MIB
- UTM-MIB
- UTM-INTERFACES-MIB.
- UTM-TEMPERATURE-MIB.

UTM-TRAPS-MIB

Name	Description
trapCoreCrush	Core crash.
trapStatDown	Statistics service (UserGate Log Analyzer) unavailable.
trapCoreBootstrapEnd	Server booting has finished successfully.
trapDefaultGatewayChanged	Default gateway has been changed.
trapHighSessionsCounter	Conntrack table 90% full.
trapHighUsersCounter	Number of active users has reached 90% of the license threshold.
trapDataPartitionFSStatus	File system status. The file system status changed to "not_clean".
trapStatusChanged	Status of the HA cluster node has been changed.
trapMemberUp	Status of the HA cluster node has been changed to "Connected".
trapMemberDown	HA cluster node has been disconnected.
trapAttackDetected	Detection of an attack by the IDPS.
trapChecksumFailed	Binary files checksum mismatch.
trapHighCPUUsage	High CPU usage (95%).
trapLowMemory	High memory usage (95%).
trapLowLogdiskSpace	Not enough disk space to store logs.
trapRaidStatus	RAID status has been changed.
trapPowerSupply	The first power supply is off.
trapCableStatus	Cable has been connected or disconnected from the interface.
trapHighDiskIOUtilization	High disk load. An alert is sent when the load is >=95% in 5 minutes on at least one of the disk devices.
trapTrafficDrop	A firewall deny rule has been triggered.
trapLDAPServerDown	LDAP server unavailable.

Name	Description
trapCriticalTemperature	Critical temperature on one of the sensors. An alert is sent when one of the operating temperature limits (lower or upper) is crossed. The lower limit of operating temperature is usually 0°C (-40°C for X series devices), the upper limit is 85°C.

UTM-TRAPS-BINDINGS-MIB

Name	Data type	Description
utmSessions	Integer	Current number of active sessions.
utmSessionsMax	Integer	Maximum number of active sessions.
utmUsers	Integer	Current number of active users.
utmUsersMax	Integer	Maximum number of active users.
utmDataPartionFSStatus	Integer	File system status. • **0**: clean • **1**: not clean
utmHAStatus	Integer	Current status of the HA cluster node: • **0**: master node • **1**: slave node • **3**: fault

Name	Data type	Description
utmHAStatusReason	Integer	Reason for the change of the HA cluster node status: • **1**: connection to the node has been lost • **2**: HTTP proxy server unreachable • **3**: no reachable gateway • **4**: DNS server unreachable • **5**: UserGate Management Center node is unreachable
utmCPUUsage	Integer	CPU load (in %).
utmMemory	Integer	RAM usage (in %).
utmLogdiskSpace	Integer	Disk space used for logs (in %).
utmAdaptecRaidStatus	Integer	Current status of RAID (Redundant Array of Independent Disks) built on the Adaptec controller: • **no_raid**. • **0**: optimal: the array is in its optimal state • **1**: degraded: one drive has completely or partially failed • **2**: rebuild: the array rebuild in progress
utmBroadcomRaidStatus	Integer	Current status of RAID (Redundant Array of Independent Disks) built on the Broadcom controller: • **no_raid** • **0**: optimal: the array is in its optimal state • **1**: degraded: one drive has completely or partially failed This

Name	Data type	Description
		status occurs if 2 disks fail. • **2**: partialDegraded: one drive has completely or partially failed • **3**: failed: not operable due to an error • **4**: offline: drive is not available to the RAID controller
utmPowerSupply	Integer	Number of power supplies: • **1**: one power supply • **2**: two power supplies
utmPowerSupplyStatus	Integer	State of the power supply: • **no_power_supplies**. • **0**: off • **1**: on
utmCSCIfName	String	The interface name.
utmCSCStatus	Integer	Status of the network adapter: • **1**: cable connected • **2**: cable disconnected
utmDiskIOUtilization	Integer	Current disk utilization (%).
utmLDAPServerName	String	LDAP server name.
utmLDAPServerAddress	String	LDAP server IP address.
utmThermSensor	String	Name of the temperature sensor.
utmThermValue	Integer	Temperature value measured by the sensor.

UTM-MIB

Name	Data type	Description
vcpuCount	Integer	Number of virtual CPUs in the system.
vcpuUsage	Integer	System virtual processor load; displays the actual number of virtual processors loaded.
usersCounter	Integer	Current number of active users. (*)
sessionsCounter	Integer	Current number of active sessions. (*)
tcpsessionsCounter	Integer	Current number of active TCP sessions. (*)
udpsessionsCounter	Integer	Current number of active UPD sessions. (*)
icmpsessionsCounter	Integer	Current number of active ICMP sessions. (*)
sessionsRate10	Integer	Number of new sessions per second. Average value for the last 10 seconds. (*)
sessionsRate60	Integer	Number of new sessions per second. Average value for the last 60 seconds. (*)
sessionsRate300	Integer	Number of new sessions per second. Average value for the last 300 seconds. (*)
tcpsessionsRate10	Integer	Number of new TCP sessions per second. Average value for the last 10 seconds. (*)
tcpsessionsRate60	Integer	Number of new TCP sessions per second. Average value for the last 60 seconds. (*)
tcpsessionsRate300	Integer	Number of new TCP sessions per second. Average value for the last 300 seconds. (*)
udpsessionsRate10	Integer	

Name	Data type	Description
		Number of new UPD sessions per second. Average value for the last 10 seconds. (*)
udpsessionsRate60	Integer	Number of new UPD sessions per second. Average value for the last 60 seconds. (*)
udpsessionsRate300	Integer	Number of new UPD sessions per second. Average value for the last 300 seconds. (*)
icmpsessionsRate10	Integer	Number of new ICMP sessions per second. Average value for the last 10 seconds. (*)
icmpsessionsRate60	Integer	Number of new ICMP sessions per second. Average value for the last 60 seconds. (*)
icmpsessionsRate300	Integer	Number of new ICMP sessions per second. Average value for the last 300 seconds. (*)
dnsRequestCounter	Integer	Total DNS requests. (*)
dnsBlockedRequestCounter	Integer	Blocked DNS requests. (*)
dnsRequestRate	Integer	DNS requests per second. (*)
httpRequestCounter	Integer	Total HTTP requests. (*)
httpBlockedRequestCounter	Integer	Blocked HTTP requests. (*)
httpRequestRate	Integer	HTTP requests per second. (*)
dataPartitionFSStatus	String	File system status.
haStatus	Integer	The current state of the cluster node.
cpuLoad	Integer	System CPU load (in %).
memoryUsed	Integer	RAM usage (in %).

Name	Data type	Description
logDiskSpace	Integer	Disk space used for logs (in %).
powerSupply1Status	String	State of the first power supply: • **no_power_supplies**. • **on** • **off**
powerSupply2Status	String	State of the second power supply: • **no_power_supplies**. • **on** • **off**
raidType	String	RAID array type.
raidStatus	String	Current status of RAID (Redundant Array of Independent Disks): • **no_raid**. • **0**: optimal: the array is in its optimal state. • **1**: degraded: one drive has completely or partially failed. • **2**: rebuild: RAID rebuild in progress.
diskIOUtilization	Integer	Current disk utilization (%).
diskIOUtilization60	Integer	Disk utilization (%). Average value for the last 60 seconds.
diskIOUtilization300	Integer	Disk utilization (%). Average value for the last 300 seconds.

> **Note**
> **Metrics marked with the (*) symbol in the description are not relevant for *UGMC* and *LogAn*. Metric values for these devices will always be zero.**

UTM-INTERFACES-MIB

Name	Data type	Description
ifNumber	Integer	Number of network interfaces.
ifIndex	Integer	The value is unique for each interface. Available values: from 1 to ifNumber.
ifDescr	String	Interface description.
ifType	Integer	Interface type determined according to the physical/link layer protocol: • **1**: other: unknown type. • **2**: regular1822: defined in BBN Report 1822. • **3**: hdh1822: defined in BBN Report 1822. • **4**: ddn-x25: defined in BBN Report 1822. • **5**: defined in the data link layer standard of the OSI X.25 network mode. • **6**: ethernet-csmacd: Ethernet-type network interface regardless of speed (defined in RFC 3635). • **7**: iso88023-csmacd: defined in IEEE 802.3. • **8**: iso88024-tokenBus: defined in IEEE 8802.4. • **9**: iso88025-tokenRing: network interface uses a Token Ring connection; defined in the IEEE 802.5 standard.

Name	Data type	Description
		• **10**: iso88026-man: defined in the ISO 88026 standard "MAN". • **11**: starLan — defined in the IEEE 802.3e standard. • **12**: proteon-10Mbit — Proteon 10 Mbit. • **13**: proteon-80Mbit — Proteon 80 Mbit. • **14**: hyperchannel — high-speed channel used in ISDN networks. • **15**: fddi — network interface which is using FDDI (Fiber Distributed Data Interface) connection. FDDI is a set of standards for data transmission over fiber-optic lines in local networks. • **16**: lapb — data link layer protocol used to transmit X.25 packets. • **17**: sdlc — data link layer protocol for IBM system network architecture. • **18**: ds1 — can handle 24 simultaneous connections at a total speed of 1.544Mbit/s; also called T1. • **19**: e1 — European analogue of T1. • **20**: basicISDN — used for communication between the subscriber's equipment and the ISDN station. • **21**: primaryISDN — used to connect to backbones connecting local and central automatic telephone stations or network switches.

Name	Data type	Description
		• **22**: propPointToPointSerial — defined in RFC1213. • **23**: ppp — network interface using PPP (Point-To-Point Protocol) connection. • **24**: softwareLoopback — network interface which is a loop adapter. These interfaces are often used for testing; they do not send traffic to the network. • **25**: eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); defined in ISO/IEC 8473-1. • **26**: ethernet-3Mbit: network interface uses a 3Mbit/s Ethernet connection. This version of Ethernet is defined in the IETF standard RFC 895. • **27**: nsip — XNS over IP — used in various data transmission environments. • **28**: slip — network interface which uses SLIP (Serial Line Internet Protocol) connection. SLIP is defined in the IETF RFC 1055 standard. • **29**: ultra — ULTRA Technologies. • **30**: ds3 — high-speed data interface multiplexing DS1 and DS2 signals; also known as T3. • **31**: slip — network interface which uses SLIP (Serial Line Internet Protocol) connection.

Name	Data type	Description
		SLIP is defined in the IETF RFC 1055 standard. • **32**: frame-relay — allows to transmit data with packet switching via an interface between user devices and network devices.
ifMtu	Integer	Maximum size of a network layer packet that can be sent over this interface.
ifSpeed	gauge32	Interface bandwidth in bits per second.
ifPhysAddress	String	Physical interface address (MAC address).
ifAdminStatus	Integer	Interface state assigned by the administrator: • **1**: up — ready to transmit packets. • **2**: down — not working. • **3**: testing — testing mode; working packets cannot be transmitted.
ifOperStatus	Integer	Current operating status of the interface: • **1**: up — the interface is ready to transmit packets. • **2**: down — the interface cannot transmit data packets. • **3**: testing — testing of network interface is performed; working packets cannot be transmitted. • **4**: unknown — the interface is in unknown state.

Name	Data type	Description
		• **5**: dormant — network interface cannot transmit data packets, because it expects an external event. • **6**: notPresente: network interface cannot transmit data packets because a component, usually a piece of hardware, is missing • **7**: lowerLayerDown: network interface cannot transmit data packets because it is running on top of one or more other interfaces, and at least one of those "lower-layer" interfaces is down
ifLastChange	timeticks	SysUpTime value when the interface switches to this state.
ifInOctets	counter32	Number of bytes received by the interface, including service bytes.
ifInUcastPkts	counter32	Number of delivered unicast packets.
fInNUcastPkts	counter32	Number of delivered multicast and broadcast packets.
ifInDiscards	counter32	Number of incoming packets that were dropped, even if no errors were detected preventing the delivery. Buffer space release may be one of the reasons for dropping.
ifInErrors	counter32	Number of incoming packets that contain errors preventing the delivery.

Name	Data type	Description
ifInUnknownProtos	counter32	Number of packets that were received through the interface and dropped because an unknown or unsupported protocol was used.
ifOutOctets	counter32	The number of bytes transmitted by the interface, including service bytes.
ifOutUcastPkts	counter32	Number of sent unicast packets, including packets that were dropped or not sent.
ifOutNUcastPkts	counter32	The number of sent multicast and broadcast packets, including packets that were dropped or not sent.
ifOutDiscards	counter32	Number of outgoing packets that were dropped, even if no errors were detected preventing the transmission. Buffer space release may be one of the reasons for dropping.
ifOutErrors	counter32	The number of outgoing packets that could not be transmitted due to errors.
ifOutQLen	gauge32	The send queue length (number of packets).
ifInMulticastPkts	counter32	Number of delivered multicast packets.
ifInBroadcastPkts	counter32	Number of delivered broadcast packets.
ifOutMulticastPkts	counter32	Number of sent multicast packets, including packets that were dropped or not sent.
ifOutBroadcastPkts	counter32	Number of sent broadcast packets, including packets

Name	Data type	Description
		that were dropped or not sent.
ifHCInOctets	counter64	Identical to **ifInOctets**: number of bytes received by this interface, including service bytes; a counter with the larger capacity is used.
ifHCInUcastPkts	counter64	Identical to **ifInUcastPkts**: number of unicast packets delivered; a counter with the larger capacity is used.
ifHCInMulticastPkts	counter64	Identical to **ifInMulticastPkts**: number of multicast packets delivered; a counter with the larger capacity is used.
ifHCInBroadcastPkts	counter64	Identical to **ifInBroadcastPkts**: number of broadcast packets delivered; a counter with the larger capacity is used.
ifHCOutOctets	counter64	Identical to **ifOutOctets**: number of bytes transmitted by this interface, including service bytes; a counter with the larger capacity is used.
ifHCOutUcastPkts	counter64	Identical to **ifOutUcastPkts**: number of unicast packets sent; this includes packets which were dropped or were not sent; a counter with the larger capacity is used.
ifHCOutMulticastPkts	counter64	Identical to **ifOutMulticastPkts**: number of multicast packets sent; this includes packets which were dropped or were not sent; a counter with the larger capacity is used.
ifHCOutBroadcastPkts	counter64	Identical to **ifOutBroadcastPkts**: number of broadcast packets sent; this includes packets which were dropped or were not sent; a counter

Name	Data type	Description
		with the larger capacity is used.
ifLinkUpDownTrapEnable	Integer	Specifies whether to create a trap when the link status changes: • **1**: enabled • **2**: disabled
ifHighSpeed	gauge32	Current estimated interface bandwidth pool in bit/s, kbit/s, Mbit/s, or Gbit/s.
ifPromiscuousMode	Integer	Promiscuous mode. Available values: • **1**: true: station receives all packets/frames regardless of the destination. • **2**: false: interface receives only packets/frames addressed to this station. The object value does not affect the reception of broadcast and multicast packets/frames.
ifAlias	String	Interface name assigned by the administrator.
ifCounterDiscontinuityTime	timeticks	SysUpTime value when the event occurred that caused one or more interface counters to fail.

UTM-TEMPERATURE-MIB

Name	Data type	Description
termNumber	Integer	Number of temperature sensors on this platform.
thermLowerThreshold	Integer	Lower operating temperature limit.

Name	Data type	Description
thermUpperThreshold	Integer	Upper operating temperature limit.
thermTable	sequence	Table of temperature sensors with readings (thermEntry).
thermEntry	sequence	A specific sensor info: • thermName (string): sensor name. • thermValue (integer): sensor readings. • thermUnit (string): sensor reading unit.

Note

Temperature sensor data will only be displayed for supported hardware platforms. Currently supported devices are UserGate C150, C151, FG, X10. For unsupported platforms or virtual solutions, the sensor table will be empty, and the number of sensors and operating temperature limits will be zero.

Note

If taking a temperature reading from a sensor was not possible, it will not be transmitted in the table, while the thermNumber parameter counts the total number of temperature sensors, even taking into account those that are not working. In this case, the number of sensors in the table and the thermNumber value may not match.

SNMP Parameters

This section allows to specify parameters of providing information over SNMP protocol by the SNMP agent. SNMP parameters are specified for each node separately.

Name	Description
SNMP system name	Name of the system which is used by SNMP control subsystem.

Name	Description
SNMP system location	Information on physical location of the SNMP agent.
SNMP system description	Description of the system.
Engine ID	Each UserGate device has a unique SNMPv3 Engine ID. By default, the Engine ID is generated from the UserGate node name. When editing the Engine ID, you are required to specify its length, type, and value. The length can be defined as **fixed** (max. 8 bytes) or **dynamic** (max. 27 bytes). A fixed ID length is only applicable to the **text** type. The Engine ID can be generated in these formats: • IPv4 (ip4) • IPv6 (ipv6) • MAC address (mac) • Text (text) • Octets (octets).

Alert Rules

This section allows you to define alert rules, which can be used to send notifications about different types of events, for example, a high CPU load or a password sent to the user by SMS. To create an alert rule, follow these steps:

Name	Description
Step 1. Create one or more notification profiles.	See the Notification Profiles section.
Step 2. Create alert recipient groups.	See the Emails and Phones sections.
Step 3. Create an alert rule.	Add a rule on the **Diagnostics and monitoring** tab in the **Notifications → Alert rules** section.

Specify the following parameters for the rule:

Name	Description
Enabled	Enables or disables the rule.

Name	Description
Name	The name of the rule.
Description	A description of the rule.
Notification profile	A previously created notification profile. For SMPP profiles, a tab will open where you can specify recipients as phone numbers. For SMTP profiles, a tab will open where you can specify recipients as email addresses.
From	From whom the notifications will come.
Subject	Notification subject.
Wait for next alert, seconds	Specify the timeout during which the server will not send a message when this rule is triggered again. This setting prevents a flood of messages when an alert rule is triggered frequently.
Events	Specify events for which you want to receive alerts.
Phones	For SMPP profiles, specify the phone groups to which SMS notifications will be sent.
Emails	For SMTP profiles. specify groups of email addresses to which email notifications will be sent.

SNMP Security Profiles

In this section the security profiles for the SNMPv3 manager authentication are configured.

> **Note**
> **SNMP v3 authentication parameters (username, password, authentication type and algorithm, encryption algorithm and password) at the SNMP manager should match SNMP parameters in UserGate.**

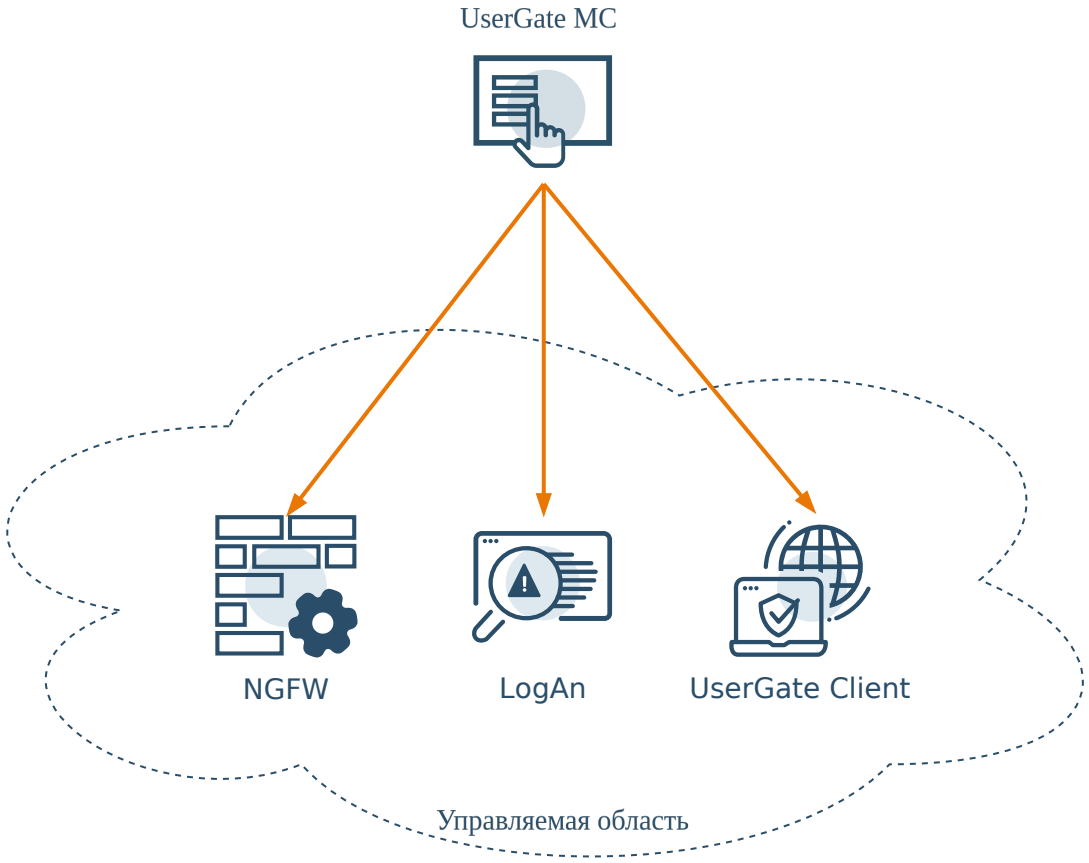
Name	Description
Name	SNMP security profile name
Description	SNMP security profile description

Name	Description
User	User name to authenticate the SNMP manager.
Authentication type	Select an authentication mode for the SNMP manager. The available options are: • No authentication; No encryption (noAuthNoPriv) • Authentication; No encryption (authNoPriv) • Authentication; Encryption (authPriv). The authPriv mode is considered the most secure.
Authentication algorithm	The algorithm used for authentication. Possible to use: • SHA1 • MD5 • SHA224 • SHA256 • SHA384 • SHA512
Authentication password	The password used for authentication.
Encryption algorithm	The algorithm used for encryption. DES or AES can be used.
Encryption password	The password used for encryption.

MANAGING REALMS

Managing Realms (Description)

A UserGate managed realm is a logical object that represents a single enterprise or a group of enterprises managed by a single administrator or group of administrators. To manage devices, the UGMC root administrator (or a UGMC administrator with the appropriate permissions) must create at least one realm and create a root administrator for that realm.



Devices managed using UGMC can include:

- UserGate firewalls (for more information, see the Managing UserGate Firewalls section).
- UserGate LogAn devices (for more information, see the Managing LogAn Devices section).
- Endpoints with UserGate Client software installed (for more information, see the Managing Endpoints section).

Creating Managed Realms

Managed realms are created by the UGMC administrator. To create a managed realm, follow these steps:

1. Create a realm.

2. Create a realm administrator profile.

3. Create a realm administrator.

Creating a Realm

In the **Managed realms → Realms** section of the web console, click **Add** and fill in the relevant fields:

Name	Description
Default realm	If this checkbox is set, you do not need to add the realm name after a slash for authorization in the web console.
Name	The name of the realm, such as UserGate LLC.
Codename	A code consisting of several letters and/or numbers. You will need to enter the realm codename during login to the web console for managing this realm. Example: UG.
Description	Optional description of the realm.
Number of devices	If specified, the realm administrator will be limited to this number of managed devices and will not be able to create more. The specified number cannot exceed the number of licensed connections.

Creating a Realm Administrator Profile

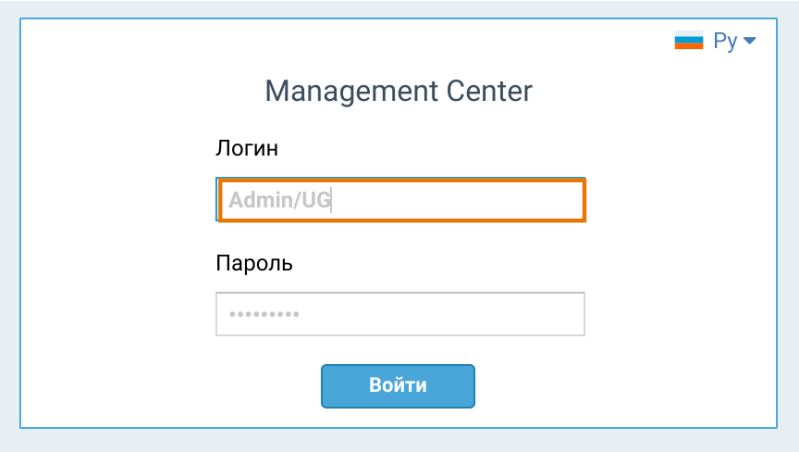
In the **Administrators → Administrator profiles** section of the web console, click **Add** and create an administrator profile of the **Realm administrator** type. Select the realm you have just created as the managed realm.

Creating a Realm Administrator

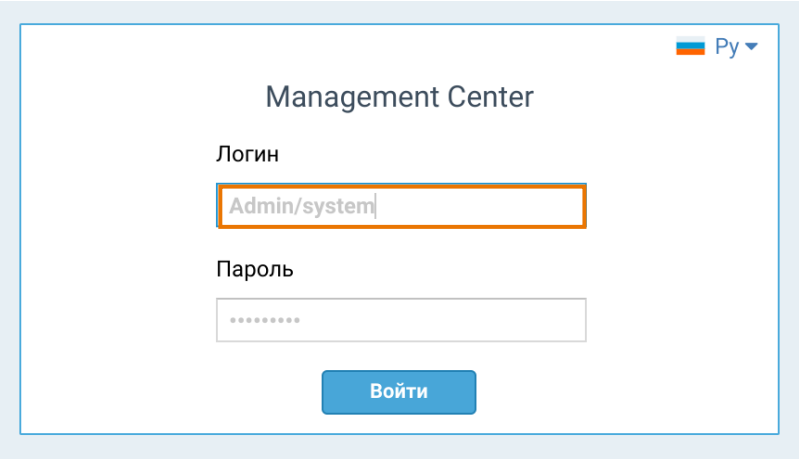
In the **Administrators → Administrators** web console section, click **Add** and create an administrator with the profile created earlier. For more details on creating administrators, see the Realm Administrators chapter in this guide.

After you have created the realm and its realm administrator, you can proceed to realm management mode. To do that, in the web console, log out from the UGMC administrator account and log in again as the administrator for this managed realm. The administrator login name should be entered as

administrator_login/realm_code, e.g., ***Admin/UG***.



To return to the console as the UGMC administrator, enter the login name as *administrator_login/system*, e.g., **Admin/system**.



Realm Administrators

> **Important!**
> **To manage a realm, the UGMC administrator must create a root realm administrator with full permissions for that realm, including the right to add additional realm administrators. For more information on creating a root realm administrator, see the Administrators section.**

The root administrator of a realm can create additional accounts of realm administrators (regional administrators), delegating to them some rights to manage the realm or templates.

To add an additional realm administrator:

1. Log in to the web management console as the root realm administrator, specifying the login in the format `<realm_root_admin_login>/<realm_code>`, for example, `Admin/UG`.

2. Create an authentication profile for the additional realm administrator. The profile defines the administrator's permissions. You can create multiple profiles with different permissions.

3. Create a realm administrator account. At this stage, you can choose the administrator authentication method: local, through the LDAP connector, or using an authentication profile.

Creating an Additional Realm Administrator Profile

To create an additional realm administrator profile:

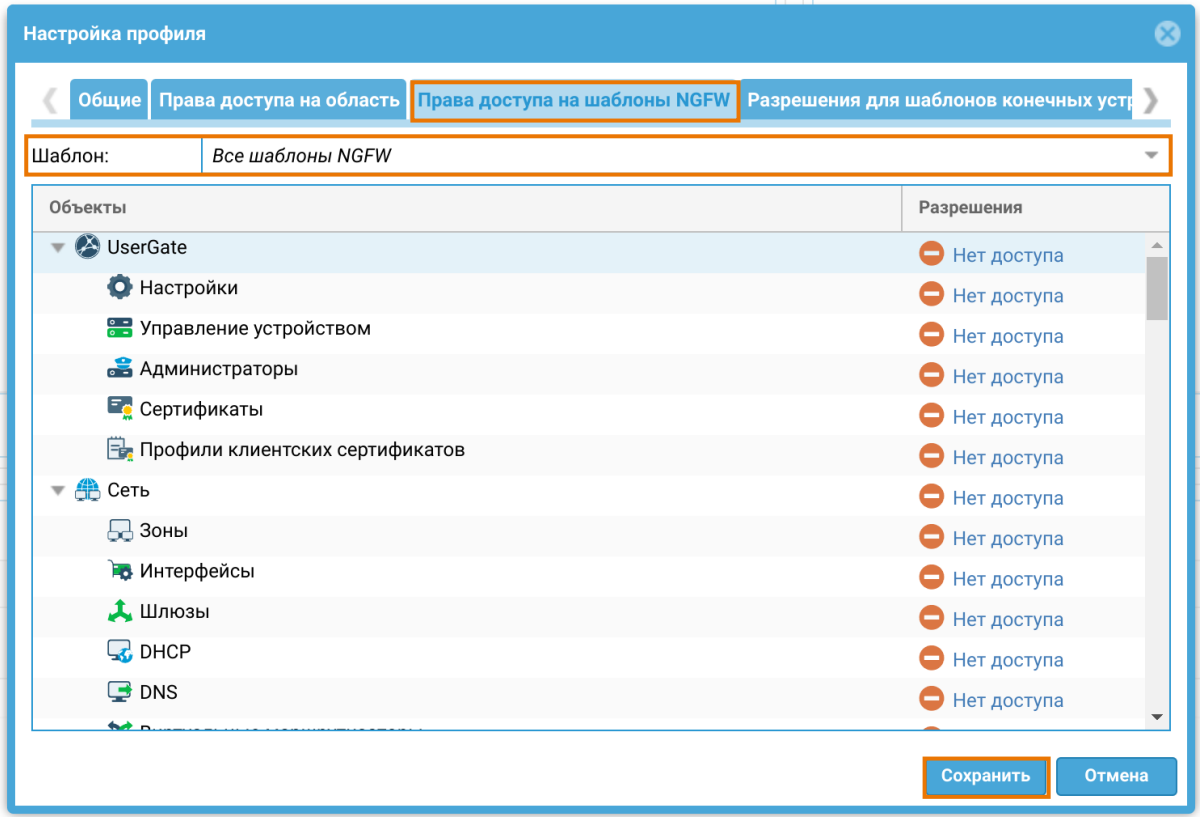
1. In the **Realm management → Management center → Administrators** section, in the **Administrator profiles** block, click **Add**.

2. In the **Profile configuration** window, on the **General** tab, specify a name for the profile and, if desired, a description.

3. On the **Realm access permissions** tab, specify what access rights the administrator with this profile will have. You can specify the following access permissions: **No access**, **Read**, **Read and write**.

4. On the **Template access permissions...** tabs:

   - In the **Template** line, select a specific template or **All templates** to configure access rights.
   - In the list below, specify access rights to the parameters of managed device templates. The parameters are presented as objects in the device web management console tree that can be delegated. You can specify the following access permissions: **No access**, **Read**, **Read and write**.



5. Save the changes.

Creating a Local Administrator Account for a Realm

To create a local administrator account for a realm:

1. In the **Realm management → Management center → Administrators** section, in the **Administrators** block, click **Add** and select **Add local administrator**.

2. In the **Administrator properties** window, specify the administrator's name, login, and password.

3. Select the administrator profile created earlier.

4. Select the **Enabled** checkbox to allow logging in with this account.

5. Save the changes.

Creating a LDAP Administrator Account for a Realm

To create a user account from an existing domain:

1. Make sure that the appropriate LDAP connector is pre-configured in **Realm management → Management center → Auth servers**. For more details on configuring the LDAP connector, see the Realm Authentication Servers section.

2. In the **Administrators** section, in the **Administrators** block, click **Add** and select **Add LDAP user**.

3. In the **LDAP administrator properties** window, click **Select**, choose the configured LDAP connector, and then add the desired user's login.

4. Select the administrator profile created earlier.

5. Select the **Enabled** checkbox to allow logging in with this account.

6. Save the changes.

When logging into the web administration interface under this account, you must specify the login in the format `<login>@<domain>/system` or `<domain>\<login>/system`.

To add a user group account from an existing domain:

1. Make sure that the appropriate LDAP connector is pre-configured in **Realm management → Management center → Auth servers**. For more details on configuring the LDAP connector, see the Realm Authentication Servers section.

2. In the **Administrators** section, in the **Administrators** block, click **Add** and select **Add LDAP group**.

3. In the **LDAP administrator properties** window, click **Select**, choose the configured LDAP connector, and then add the desired user group login.

4. Select the administrator profile created earlier.

5. Select the **Enabled** checkbox to allow logging in with this account.

6. Save the changes.

When logging into the web administration interface under this account, you must specify the login in the format user@domain/system or domain\user/system.

Creating a Realm Administrator Account with an Authentication Profile

As the root administrator of a realm, you can control access for additional realm administrators to the realm web management console using an authentication profile, which specifies preconfigured servers, such as LDAP, TACACS+, or RADIUS, in the list of available authentication methods. If an authentication profile specifies multiple authentication methods, each method will be tried in turn until the first one that works.

To add an additional realm administrator account with an authentication profile:

1. Make sure that the configured authentication server has been added in **Realm management → Management Center → Auth Servers**. For more details about the authentication server, see the Realm Authentication Servers section.

2. Make sure that a profile with the required authentication method has been created in the **Authentication profiles** section. For more details on creating profiles, see the Realm Authentication Profiles section.

3. In the **Administrators** section, in the **Administrators** block, click **Add** and select **Add administrator with auth profile**.

4. In the **Properties of the administrator with an authentication profile** window, specify the administrator's name, login, and password.

5. Select the administrator profile created earlier.

6. Select the authentication profile created earlier.

7. Select the **Enabled** checkbox to allow logging in with this account.

8. Save the changes.

Realm Authentication Servers

Authentication servers (auth servers) are external sources of user accounts used for authorization in the realm management web console. A realm authentication server works similar to a UGMC authentication server, the only difference is where each is used.

LDAP Connector

An LDAP connector allows you to:

- Obtain information on users and groups from Active Directory or other LDAP servers. FreeIPA is supported with an LDAP server.
- Authorize UGMC users via Active Directory/FreeIPA domains.

To create an LDAP connector, click **Add**, select **Add LDAP connector**, and provide the following settings:

Name	Description
Enabled	Enables or disables the use of this authentication server.
Name	The name of the authentication server.
SSL	This specifies whether SSL is required to connect to the LDAP server.
LDAP domain name or IP address	The IP address of the domain controller, the domain controller FQDN or the domain FQDN (e.g., test.local). If the domain controller FQDN is specified, UserGate will obtain the domain controller's address using a DNS request. If the domain FQDN is specified, UserGate will use a backup domain controller if the primary one fails.
Bind DN ("login")	The username for connecting to the LDAP server. Must be in the DOMAIN\username or username@domain format. This user must be already created in the domain.
Password	The user's password for connecting to the domain.
LDAP domains	The list of domains served by the specified domain controller, e.g., in case of a domain tree or an Active Directory domain forest. Here you can also specify the short NetBIOS domain name.
Search roots	The list of LDAP server paths relative to which the system will search for users and groups. Specify the full name, e.g., ou=Office,dc=example,dc=com.

After creating a server, you should validate the settings by clicking **Check connection**. If your settings are correct, the system will report that; otherwise, it will tell you why it cannot connect.

The LDAP connector configuration is now complete. When logging in to the console, LDAP users should specify their usernames in the following formats:

domain\user/system or *user@domain/system*

RADIUS Authentication Server

You can authorize users in the UserGate web console using a RADIUS authentication server, with the console working as a RADIUS client. When authorization is done using a RADIUS server, UserGate sends the username and password information to the RADIUS server, which then responds as to whether or not the authentication was successful.

To add a RADIUS authentication server, click **Add**, select **Add RADIUS server**, and provide the following settings:

Name	Description
Enabled	Enables or disables the use of this authentication server.
Name	The name of the RADIUS authentication server.
Description	An optional description of the server.
Shared secret	Pre-shared key used by the RADIUS protocol for authentication.
Addresses	Specify the server's IP address and the UDP port on which the RADIUS server listens for authentication requests (the default port number is 1812).

To authorize users in UserGate's web interface using a RADIUS server, you need to configure an authentication profile. For more details on creating and configuring profiles, see the section Realm Authentication Profiles.

TACACS+ Authentication Server

You can authorize users in the UserGate administrative console using a TACACS+ authentication server. In this case, UserGate transmits the username and password information to the auth servers, and then the TACACS+ servers respond as to whether the authentication was successful.

To add a RADIUS authentication server, click **Add**, select **Add RADIUS server**, and provide the following settings:

Name	Description
Enabled	Enables or disables the use of this authentication server.
Name	The name of the TACACS+ authentication server.
Description	An optional description of the server.
Secret	Pre-shared key used by the TACACS+ protocol for authentication.
Address	The IP address for the TACACS+ server.
Port	The UDP port on which the TACACS+ server listens for authentication requests.

Name	Description
Use single TCP connection	Use a single TCP connection for communicating with the TACACS+ server.
Timeout (sec.)	The authentication timeout for the TACACS+ server. The default is 4 seconds.

To authorize users in UserGate's web interface using a TACACS+ server, you need to configure an authentication profile. For more details on creating and configuring profiles, see the section Realm Authentication Profiles.

Realm Authentication Profiles

A profile allows you to define a set of authorization methods for administrators in the web console of a managed realm.

> **Important!**
> **Before adding an authentication profile, you must configure the required authentication server.**

To add an authentication profile:

1. In **Realm management → Management center → Authentication profiles**, click **Add**.

2. In the **Auth profile properties** window, on the **General** tab, specify the profile name.

3. If necessary, configure one or more settings:

   - **Idle time**: the time after which a user's authorization will be revoked if they are inactive (if there are no network packets with the user's IP address). After this, the user will be required to re-authorize.
   - **Session expiration time**: the time after which a user's authorization will be revoked. After this, the user will be required to re-authorize.
   - **Maximum auth attempts (local users)**: the number of failed authentication attempts allowed before a local user account is locked.

- **Local user lockout time**: the time a local user account will be locked after the specified number of failed authentication attempts has been reached.

4. On the **Authentication methods** tab, click **Add**, and when clicking **Add** to select a preconfigured authentication server: LDAP connector, RADIUS server, or TACACS+ server.

5. Save the changes.

You can now use the created profile when creating administrator accounts.

User Catalogs

To work with users catalogs, a correctly configured LDAP connector is needed that enables information to be obtained on users and groups from Active Directory or other LDAP servers. The users and groups can be used in configuring policies applied to managed devices.

> **Note**
> **When you configure security policies, authentication servers configured in managed device templates are not used to add users and groups to rules.**

To create a catalog, click **Add** and provide these settings:

Name	Description
Enabled	Enables or disables this LDAP connector.
Name	The name of the LDAP connector.
SSL	This specifies whether SSL is required to connect to the LDAP server.
LDAP domain name or IP address	The IP address of the domain controller, the domain controller FQDN or the domain FQDN (e.g., test.local). If the domain controller FQDN is specified, UserGate will obtain the domain controller's address using a DNS request. If the domain FQDN is specified, UserGate will use a backup domain controller if the primary one fails.
Bind DN ("login")	

Name	Description
	The username for connecting to the LDAP server. Must be in the DOMAIN\username or username@domain format. This user must be already created in the domain.
Password	The user's password for connecting to the domain.
LDAP domains	The list of domains served by the specified domain controller, e.g., in case of a domain tree or an Active Directory domain forest. Here you can also specify the short NetBIOS domain name.
Search roots	The list of LDAP server paths relative to which the system will search for users and groups. Specify the full name, e.g., ou=Office,dc=example,dc=com.

After creating a server, you should validate the settings by clicking **Check connection**. If your settings are correct, the system will report that; otherwise, it will tell you why it cannot connect.

To add an LDAP user or user group, in the rule properties click **Add LDAP user/Add LDAP group** in the rule properties, type at least one character present in the names of the desired objects in the search field, and then click **Search** and select the users or groups of interest.

MANAGING USERGATE NEXT-GENERATION FIREWALLS

UserGate NGFW Device Management

In the UserGate Management Center (UGMC) web interface, managed realm administrators can centrally manage connected UserGate NGFWs and configure the settings for these devices. To do that, follow these steps:

1) configure UserGate NGFW template parameters;

2) create a UserGate NGFW template group;

3) configure UserGate NGFW integration with UGMC.

For more information about the objects used in the UGMC managed area, such as templates, template groups, and managed devices, see the Templates and Template Groups section.

> **Important!**
> **Starting with version 7.2.0, the names of objects used in UGMC are now case-sensitive. To avoid naming conflicts when upgrading from earlier versions to version 7.2.0 or higher, the names of all UGMC objects are automatically converted to lowercase. You can change the object names after the upgrade if necessary.**

Configuring UserGate NGFW Template Parameters

Before configuring UserGate NGFW template parameters, you must create device templates. It is recommended to create separate templates for different categories of settings, such as a network settings template or a library template. This will simplify further work with templates when combining them into groups.

To create a UserGate NGFW template:

1. In the **Realm management → NGFW → Templates** section, click **Add**.
2. Specify a name and description for the template.
3. Click **Save**.

   The created template will appear in the **Templates** table. You can now configure its parameters. Template parameters will be applied to all managed UserGate NGFW devices to which the template is applied within the group.

When configuring UserGate NGFW template parameters, consider the following:

- Parameter values in the template override those specified locally by the UserGate NGFW administrator. If a parameter value is not specified either in the template or in UserGate NGFW, the default value will be used.
- UserGate NGFW has a system template, the UserGate Libraries template, which is automatically created in UGMS. This template contains the default UserGate NGFW network zones, as well as libraries of elements such as services, calendars, bandwidth pools, response pages, URL categories, SSL profiles, application profiles, and IPS profiles.

- After applying the template settings to managed devices, administrators can modify basic settings and network interface settings locally on each UserGate NGFW. Detailed information about these parameters is provided in the General Settings and Interface Configuration sections of the UserGate NGFW Administrator's Guide.

- When configuring network interface settings in a template, it is not possible to configure the port0 interface. The first physical interface available for configuration in the template is port1.

  The parameters for the port0 interface are configured by the UserGate NGFW administrator during initial product setup. By default, this interface is used to connect UserGate NGFW to UGMC.

  If necessary, you can configure network interfaces locally on the UserGate NGFW. To do this, select the **Configured on the device** checkbox in the selected template interface settings.

  If you create an interface in a template, this interface will be automatically added to the UserGate NGFW. Removing an interface from a template does not delete the interface from the firewall. If you need to delete an interface from the firewall, you must do so manually.

- Policy rules in a template do not override rules created locally by UserGate NGFW administrators; they are added to them as pre- and post-rules.

- For some policy rules in a template, you can specify the managed devices to which these rules will apply. This action is available in the rule properties window on the **Devices** tab.

  Please note that frequent use of this feature can complicate administrators' understanding of which policy rules will apply to a device.

- Template element libraries (e.g., IP address libraries, URL list libraries, and content type libraries) do not contain data by default, unlike UserGate NGFW libraries (for more information, see the Libraries of Items section of the UserGate NGFW Administrator's Guide). Before configuring policies in the template, you must add library elements.

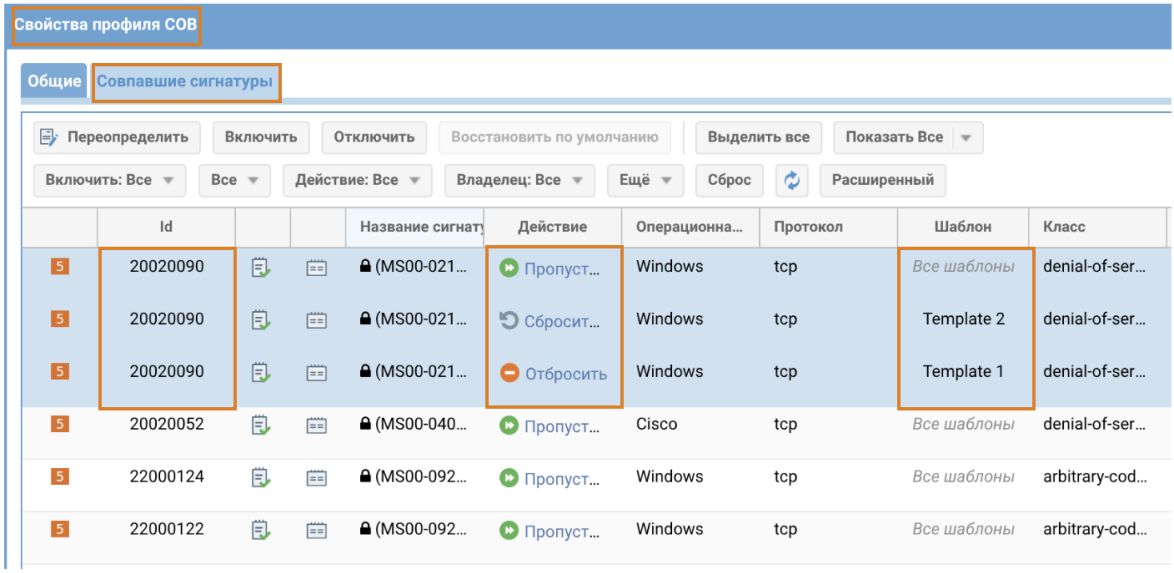
Important!

Library data is not synchronized: if the added elements are not used in the template policies, they will not be added to the UserGate NGFW libraries. Therefore, to display IP address lists created in a template on managed devices, you must first add these lists to the template's policy rules.

Note

The correct operation of proprietary IDPS and application signatures depends on the validity of the libraries for these signatures. We recommend checking the validity of the libraries after updating UGMC or restoring its settings. If for any reason the libraries are not updated automatically, you can update them manually. This action is performed by the UGMC administrator in the Management Center → Settings → Library updates section.

- When creating an IDPS profile in a template, the list of matching signatures may display multiple copies of the same proprietary signature (see the figure below).



This situation occurs when a template overrides the parameters of proprietary IDPS signatures (found in the sidebar under **Libraries → IDPS Signatures** for the selected template), such as the signature detection action. In this case, the

signature associated with the selected template is selected for parameter configuration.

- Starting with version 7.4.0, if the ID of a policy rule created locally on UserGate NGFW matches the ID of a rule created in a template, the template rule will be included in the parameter configuration, and the local rule will be deleted.
- When configuring UserGate NGFW templates for cluster nodes in the configuration properties of non-cluster parameters (for example, in the UserID agent parameter properties), you can specify the cluster node to which these parameters will apply.

To configure UserGate NGFW template parameters:

In the NGFW Configuration section, for the **Template** object, select the template whose parameters you want to configure from the drop-down list.

Template settings are configured in the sidebar sections similar to configuring settings for a local UserGate NGFW (for more information, see the UserGate NGFW Administrator's Guide).

Creating a UserGate NGFW Template Group

After creating UserGate NGFW templates, they must be organized into groups. A template group allows you to create a configuration of settings that will be applied to one or more managed devices. This configuration is formed by merging the settings of all templates within the group, taking into account their location.

To create a UserGate NGFW template group:

1. In the **Realm management → NGFW → Template groups** section, click **Add**.
2. On the **General** tab, specify a name and description for the template group.
3. On the **Templates** tab, click **Add**:
   - Select a template from the list and add it to the group by clicking **Add**.
   - Repeat this step for all templates you want to add to the group.
   - Click **Close**.

The order of the templates in the list corresponds to the order in which the template settings are applied in the configuration. If necessary, you can change the order using the **Up**, **Down**, **Top**, **Bottom** buttons.

You can also create and add new templates by clicking the **Create and add new object** button.

4. Click **Save**.

The created template group will appear in the **Template groups** table. You can now proceed to configuring the UserGate NGFW integration with UGMC.

Configuring the UserGate NGFW Integration with UGMC

Integration with UGMC is configured by creating a logical object in the managed area — a device to which actual UserGate NGFWs will be assigned when they connect to UGMC. Each such logical object, when enabled, uses one managed device license.

Using one device created in the managed area, you can configure the integration with UGMC of a single UserGate NGFW or a cluster of firewalls. For UserGate NGFWs in a cluster, simply connect the first node to UGMC; the remaining nodes will be connected automatically when they are added to the cluster.

To configure the integration of UserGate NGFW with UGMC:

1) Create a device in the managed realm;

2) Connect the UserGate NGFW to UGMC.

All UserGate NGFWs configured for integration with UGMC are called managed devices.

Creating a Device in a Managed Realm

> **Note**
> **The instructions below must be completed by the managed realm administrator in the UGMC web interface.**

To create a device in a managed realm:

1. In the **Realm management → NGFW → Devices** section, click **Add**.

2. On the **General** tab, specify the device parameters:

   - name and description;

- template group whose parameters should be applied to connected UserGate NGFWs;
- the mode for synchronizing parameters between the template group and connected UserGate NGFWs.

  During synchronization, the template group's parameter configuration is applied to the managed devices. Automatic mode is selected by default. In this mode, UserGate NGFW parameters are synchronized with the parameter configuration each time it changes.

  Synchronization can be disabled if necessary. This may be necessary, for example, if you need to simultaneously change the parameters of several template groups. In this case, you can immediately apply all changes made in the **Devices** table by manually synchronizing using the **Sync now** button.

3. If you plan to configure UserGate NGFW integration with an external UserGate Log Analyzer server, enter the UserGate NGFW IP address on the **UserGate address for Logan connection** tab.

4. Click **Save**.

5. Select the created device in the list and obtain the UserGate NGFW connection code by clicking **Actions → Show device unique code**.

6. Save the code for connecting to UserGate NGFW.

In the UGMC interface, you can view the list of created devices.

Connecting UserGate NGFW to UGMC

You can connect UserGate NGFW to UGMC during the initial firewall setup by clicking **Configure by UserGate Management Center**, as well as during subsequent use (see instructions below).

Before following these instructions, you must enable the **UserGate Management Center** service in the zone properties for connecting UserGate NGFW. This step is performed by the UGMC administrator in **Management Center → Zones**. You must also ensure that there is network connectivity between the UserGate NGFW and UGMC servers.

> **Note**
>
> **The instructions below are performed in the UserGate NGFW web interface.**

To connect UserGate NGFW to UGMC:

1. In **Settings → Administrator console → General settings**, in the **UserGate Management Center Agent** section, click **Configure**.

2. Specify the UGMC IP address (e.g., `192.0.2.4`) and the UserGate NGFW connection code generated in the UGMC web interface.

3. Click **Save**.

The connection status will be displayed in the **UserGate Management Center Agent** block as a color indicator:

- Green: connection to the UGMC server established, integration is proceeding normally.
- Red: connection to the UGMC server not established, UserGate NGFW is disabled, or the **UserGate Management Center** agent is stopped.

If the connection is successful, the template group configuration will be applied to UserGate NGFW. The parameters of this configuration (except for basic parameters and network interface parameters) will not be able to be modified on the UserGate NGFW side.

You can also view UserGate NGFW connection information in the UGMC web interface under **Realm management → NGFW → Devices**. UGMC checks the connection to UserGate NGFW on TCP ports 2022 and 9712. For each device in the managed realm, the status and last connection date of the UserGate NGFWs associated with it are displayed, along with additional information, including memory usage and uptime of the firewalls.

In the UGMC interface, you can manage connected UserGate NGFWs.

Viewing the List of Devices in the Managed Area

The **Realm management → NGFW → Devices** section contains a list of devices in the managed realm. In this list, you can:

- Enable and disable devices by clicking the **Enable** and **Disable** buttons, respectively. Disabling a device will disconnect all UserGate NGFWs associated with it from the UGMC server.
- Delete devices by clicking the **Delete** button.
- Edit device parameters by clicking the **Edit** button.
- View device information in a separate window by clicking **Show device details**.

You can also customize the display of devices in the list using the following filters:

- **All**: all devices (default filter).
- **Enabled** and **Disabled**: devices in the selected state.
- **Online**: devices linked to UserGate NGFWs are connected to the UGMC server.
- **Offline**: devices linked to UserGate NGFWs are not connected to the UGMC server.
- **Unlinked**: devices to which UserGate NGFWs are not linked.
- **Consistent devices**: devices linked to UserGate NGFWs with parameters synchronized with the template group configuration.
- **Inconsistent devices**: devices linked to UserGate NGFWs with parameters not synchronized with the template group configuration.

You can also manage parameter synchronization between a template group and UserGate NGFW. Manual and automatic modes are available. Manually, you can initiate synchronization for all managed devices at once (by clicking **Actions → Run full synchronization**) or only for selected devices (by clicking **Sync now**).

In automatic mode, the managed device's parameters are synchronized with the template group's parameter configuration whenever it changes. Additionally, during automatic synchronization, the connected UserGate NGFW sends its status information to UGMC every 20 seconds, updating the device's last synchronization time.

Managing Connected UserGate NGFWs

In **Realm management → NGFW → Devices**, you can manage connected UserGate NGFWs:

- Click **Open console** to access the UserGate NGFW web interface. For clustered UserGate NGFWs, this button opens a node selection window for accessing the web interface for that node.
- Reboot and power off the standalone UserGate NGFW server or each firewall cluster node using the **Reboot** and **Shut down** links, respectively.
- Manage the UserGate NGFW license: activate the license using the **No license** link, check its expiration date using the **Check license** link, and update the license using the **Registered version** link.

- Install software updates (UGOS) downloaded locally to the standalone UserGate NGFW server or firewall cluster node using the **Install the updates** link.
- Modify UserGate NGFW settings by configuring template parameters included in the applied configuration.

UserGate NGFW Clustering

You can combine two or more UserGate NGFW nodes into a configuration cluster and configure them with common traffic processing parameters using templates.

Parameters are synchronized between the nodes in the configuration cluster, ensuring uninterrupted filtering and processing of network traffic if one node is unavailable.

Additionally, you can combine up to four nodes in the configuration cluster into a high availability cluster. This cluster supports the following operating modes:

- "active-active": one of the firewalls operates as the master node that distributes the traffic among all other cluster nodes;
- "active-passive": the primary node handles transit traffic; if this node fails, traffic is redirected to the backup cluster nodes.

In the high availability cluster settings, you can configure session synchronization between nodes (with the exception of sessions using a proxy server). This may be necessary for an "active-passive" cluster; for example, if the primary node is unavailable, you can switch to the backup node without losing established sessions.

Multiple high availability clusters can be created within a single cluster configuration. In this case, you can assign a unique multicast identifier to each high availability cluster, which will be used to synchronize sessions between nodes.

Creating a Configuration Cluster

To create a configuration cluste:

1) configure the first node of the configuration cluster;

2) connect the first node of the configuration cluster to UGMC;

3) add additional nodes to the configuration cluster.

> **Note**
> **The instructions below are performed in the UserGate NGFW interface.**

To configure the first node of the configuration cluster:

1. Perform the initial configuration of UserGate NGFW, which will act as the first node of the cluster, according to the instructions in the Connecting to UserGate NGFW section of the UserGate NGFW Administrator's Guide.

2. Configure the zone through whose interfaces parameter replication between cluster nodes will occur.

   To do this, in **General settings → Network → Zones**, create a new zone or use the default **Cluster** zone. In the zone settings in the **Access control** block, enable the **Administrative console** and **Cluster** services.

   > **Important!**
   > **Do not use zones whose interfaces are connected to untrusted networks (e.g., the Internet) for parameter replication**

3. Specify the IP address of the first node to connect to other cluster nodes.

   To do this, in **General settings → Administrator console → Device management**, in the **Configuration cluster** section, select the first cluster node, click **Edit**, and specify the IP address of the interface that is part of the zone configured in step 2.

4. In the **Configuration cluster** section, click **Generate secret code** and save the generated code. This code will be needed to connect the second and subsequent nodes to the cluster.

After configuring the first node, connect it to UGMC. Upon connection, the node will automatically be assigned the identifier `node_1`. You can now add additional nodes to the configuration cluster.

> **Note**
> **The instructions below are performed during the initial configuration of UserGate NGFW.**

To add an additional node to the configuration cluster:

1. Connect to the UserGate NGFW web interface, which will act as the additional cluster node.

2. Follow the instructions in the initial configuration wizard:

- select the web interface language;
- select the time zone;
- read the license agreement.

3. In the node usage options window, select **Additional cluster node**.

4. In the node configuration window, specify the cluster connection parameters:

- Name, IP address, and subnet mask of the network interface that will be used for the connection.
- If the first and additional cluster nodes are on different subnets, specify the IP address of the gateway through which the first cluster node will be accessible.
- IP address of the first cluster node.
- The connection code obtained when configuring the first cluster node.

5. Click **Connect**.

6. If the connection is successful, the initial configuration wizard will prompt you to enter the cluster node ID. Specify this ID in the format `node_<cluster node number>`, for example, `node_2`.

The secondary node has been added to the configuration cluster. The settings configured on the first node will be automatically replicated to this node. In the UGMC interface, the additional cluster node will appear in the **Realm management → NGFW → Devices** section in the row of the managed device to which the first cluster node was previously connected.

If necessary, you can add additional nodes by repeating the steps in this guide for each one.

Creating a HA Cluster

Before you create an HA cluster:

1. Create a configuration cluster (see instructions above).

2. Make sure that:

- The same requirements are met as those for nodes when creating a HA cluster without UGMC (see the Clustering and High Availability section of the UserGate NGFW Administrator's Guide).
- Network interfaces managed by UGMC are created on each configuration cluster node. You can assign virtual IP addresses only to interfaces created in a template.

2. In UGMC, under the administrator account of the managed realm, do the following:

- In **Realm management → NGFW → Devices**, verify that all nodes of the configuration cluster are accessible.
- Create a network zone template and a HA cluster template.
- In the network zone template, under **General settings → Network → Zones**, allow access to the **VRRP** service for the zones for which you plan to add a cluster virtual IP address (for more details, see the Zone Configuration section of the UserGate NGFW Administrator's Guide).

> **Note**
>
> **The instructions below must be completed by the managed realm administrator in the UGMC web interface.**

To create a HA cluster:

1. In the failover cluster template, under **Administrator console → Device management**, in the **HA Cluster** settings section, click **Add**.

2. On the **General** tab, do the following:

- Enable the cluster.
- Specify a name and, if necessary, a description for the cluster.
- Select the HA cluster operating mode:
  - **Active-Active**: distributes the load between cluster nodes;
  - **Active-Passive**: switches the load to backup nodes if the primary node is unavailable.

- If synchronization of user TCP sessions between cluster nodes is required, select the **Sessions sync** checkbox.

  If other HA clusters are present on the local network, you can specify a unique multicast identifier for the cluster being created, which will be used to synchronize sessions between nodes.

  > **Important!**
  > **Synchronizing sessions between nodes creates a significant load on the cluster.**

  On the **UDP/ICMP Synchronization** tab, you can manage the user session synchronization mode:

  - If you want to synchronize all user sessions between cluster nodes, including UDP and ICMP traffic, select the **Synchronize all sessions** checkbox.
  - If you want to exclude specific user sessions from synchronization, specify the IP addresses to which these sessions are bound.

- Optionally, specify a unique virtual router identifier (VRID).

  If there are no third-party VRRP clusters on the local network, we recommend leaving the default value.

3. On the **Nodes** tab, specify the IDs of the configuration cluster nodes that you want to combine into a failover cluster.

4. On the **Virtual IPs** tab, assign virtual IP addresses to interfaces on the HA cluster nodes. You can only assign virtual IP addresses to interfaces created in templates.

5. Click **Save**.

The created cluster will appear in the **HA cluster** settings. You can view the HA cluster status in the **Realm management → NGFW → Devices** section in the row of the managed device to which the nodes of this cluster are connected.

If you plan to use a captive portal for user authentication on the local network, after creating the HA cluster in one of the UserGate NGFW templates, in the **Administrator console → Settings** section, in the **Modules** for service domain names (e.g., `auth.captive` and `logout.captive`) settings block, specify the

IP address assigned as the cluster virtual address (for more information, see the General Settings section of the UserGate NGFW Administrator Guide).

UserGate NGFW Updates

UGMC receives software (UGOS) and system libraries update files from the UserGate repository under the Security Update module license. All UserGate NGFWs connected to managed devices use the UGMC server as an update source.

In the UGMC interface, you can manage UGOS updates:

- check for update files in the UserGate repository;
- download update files from the repository;
- change update settings for managed devices;
- download update files received in your my.usergate.com account offline if you don't have access to the UserGate repository.

You can also manage system library updates:

- manage automatic library updates on the UGMC server;
- configure the automatic update schedule;
- download update files received in your my.usergate.com account offline if you don't have access to the UserGate repository.

Managing UGOS Updates

You can upload UGOS update files to the UGMC server directly from the UserGate repository or offline.

> **Note**
> **The instructions below are for the managed realm administrator to perform in the UGMC web interface.**

To upload a UGOS update file from the UserGate repository:

1. In **Realm management → NGFW → Software updates**, click **Online updates**.

   The check for UGOS updates in the UserGate repository will begin. Once the check is complete, a list of available update files will be generated.

2. Select the update file from the list and click **Select**.

The update will appear in the **Software updates** table. You can track the status and progress of the download in the corresponding columns.

To upload a UGOS update file offline:

1. In **Realm management → NGFW → Software updates**, click **Import update**.

2. Click **Browse** to select the update file.

The update file will begin uploading. Once the upload is complete, the UGOS update name and version will be displayed in the download window.

3. If necessary, in the **Compatibility** field, specify the UGOS version that is compatible with the uploaded update.

4. Click **Save**.

The update will appear in the **Software updates** table.

After uploading, you must approve the required updates so that they are available for installation on connected UserGate NGFWs. To do this, select the update in the table and click **Approve update**. This action is also available when changing update settings. You can also delete updates in the table by clicking the **Delete update** button.

To change UGOS update settings:

1. In the **Realm management → NGFW → Software updates** section, click the link in the **Name** column for the update.

2. If necessary, on the **General** tab:

- change the update description;
- approve the update using the **Approve update** checkbox.

3. If necessary, on the **Devices** tab, click the **Add** button to add managed devices to which the update will be available.

4. Click **Save**.

UserGate NGFW administrators can manually install uploaded and approved UGOS updates locally on devices.

Managing Library Updates

By default, system libraries on the UGMC server are updated automatically. In the **Realm management → NGFW → Library updates** section, UGMC managed realm administrators can disable automatic updates for a selected library by clicking the **Do not update** button and re-enable them by clicking the **Update automatically** button. Additionally, the **Import update** button allows offline upload of the library update file to the UGMC server.

System libraries located in the UGMC repository are available to all UserGate NGFWs connected as managed devices. These libraries are updated automatically on the UserGate NGFW according to a schedule. You can configure the automatic update schedule on each UserGate NGFW locally (for more information, see the General Settings section of the UserGate NGFW Administrator Guide) or using device templates on UGMC. Below are instructions for configuring a schedule in a template, which is performed by the managed realm administrator in the UGMC web interface.

To configure an automatic update schedule for system libraries:

1. In one of the UserGate NGFW templates, in the **Administrator console → Settings → Library updates** section, for the **Auto updates schedule** option, click **Configure**.

2. Select a library from the list and specify a schedule option for it.

If you select **Advanced**, you can specify the time in cron format: <minutes: 0–59> <hours: 0–23> <days of the month: 1–31> <months: 1–12> <days of the week: 0–6, where 0 is Sunday>.

For manual entry, you can use the following characters:

- (*): all values. For example, in the hour field, the symbol means the backup should run every hour.
- (-): range of values.
- (,): is used as the delimiter of values.
- (/): is used to indicate step between values.

If you select the **Apply for all updates** checkbox, the selected library's schedule will be applied to all libraries in the list.

3. Click **Save**.

Emergency Disconnection of UserGate NGFW from UGMC

If the integration is configured, you can disconnect UserGate NGFW from UGMC using the emergency disconnect command. This command is executed in the UserGate NGFW command line interface in configuration mode (for more information, see the Configuration Mode section of the NGFW Administrator Guide):

```
Admin@nodename# execute mc-force-disconnect <arg>
```

You can specify the following parameters as the argument value (`arg`):

- `keep`: when disconnecting, all objects imported from UGMC (e.g., libraries and policy rules) will be saved locally in UserGate NGFW.
- `delete`: when disconnecting, all objects imported from UGMC (e.g., libraries and policy rules) will be deleted. The exception is objects currently in use; they will be saved locally in UserGate NGFW.

Example:

```
Admin@nodename# execute mc-force-disconnect keep
Admin@nodename# execute mc-force-disconnect delete
```

Note

In version 7.4.0 and later, when disabling UserGate NGFW from UGMC with the `keep` **argument, the** `[MC]` **prefix will be removed from the name of all NGFW objects previously imported from UGMC. If removing the prefix would result in a duplicate name for another existing object, the prefix is not removed.**

Working with templates at the UserGate MC

The UserGate MC has the hierarchical administration system (you can find the detailed information in the Administrators section) and the template method (you can find the detailed information in the Managing UserGate next-generation firewalls section) which allow to manage the device configurations easily.

The devices are managed in the managed realm. The managed realm can include many branches (cities) where the managed devices are located.

The root realm administrator has all rights for realm management. It can create the setting templates for the managed devices, combine the templates into the groups and assign these groups to the managed devices. The root administrator of a managed realm can create additional accounts of realm administrators or, in other words, regional administrators, delegating to them the rights to administer only individual allocated devices in branch offices.

The template groups can include templates that are configured by the realm administrator or by the regional administrators.

The order of the templates in the group matters. It determines the priority of the policies or the objects used by the policies.

The order of applying the rules on the managed device is as follows:

1. The pre-rules of the first template, the pre-rules of the second template etc.
2. The local policy rules on the device.
3. The post-rules of the first template, the post-rules of the second template etc.

It allows to put the rules in any place in the list of the rules of the managed device.

The order of applying the objects that are not the rules is as follows: the first matching object found when iterating the list of the templates of the group is processed, then the second found object is processed etc.

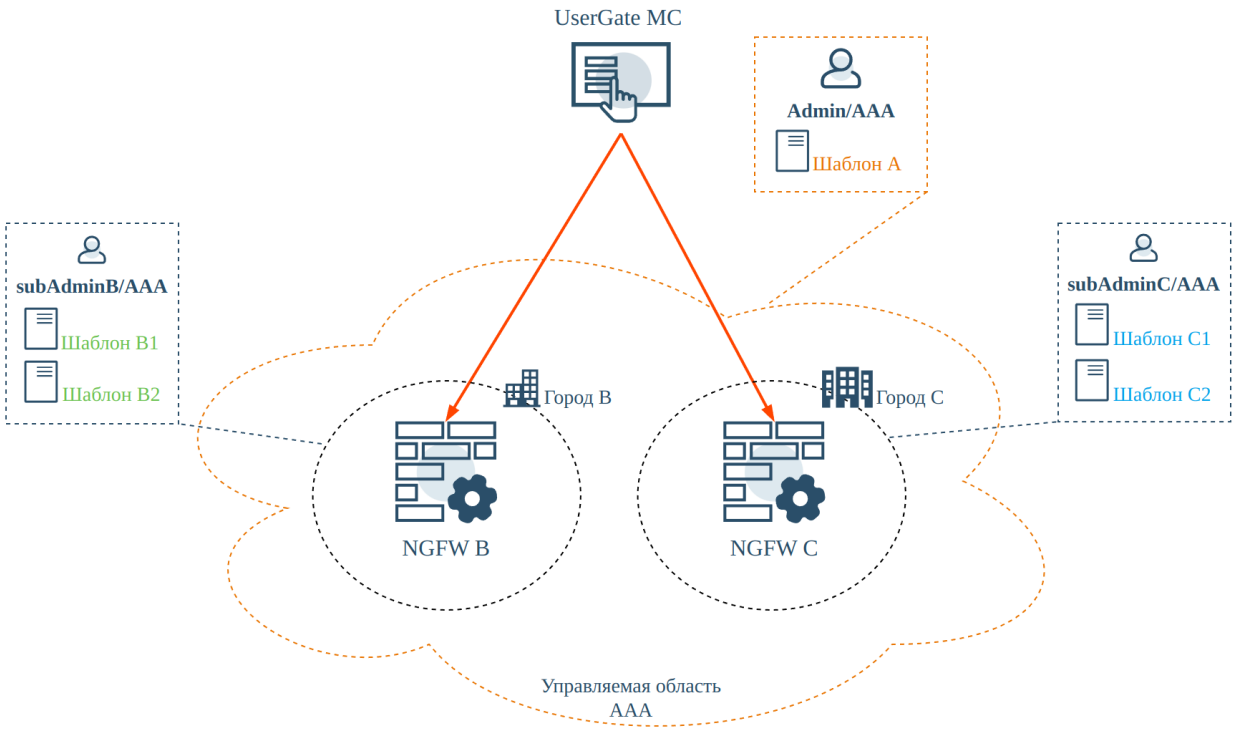
It allows to implement the hierarchical administration system: the realm administrator manages the policies at the organization level, and the regional administrators manage policies at their branches. The realm administrator creates the general policy template for all the branches and adds it to the template groups for the regional devices. It allows to manage the information security policies at the organization level. And the regional administrators perform the local tasks at their branches using their own templates.

Let’s look at two examples of working with templates in the managed realm.

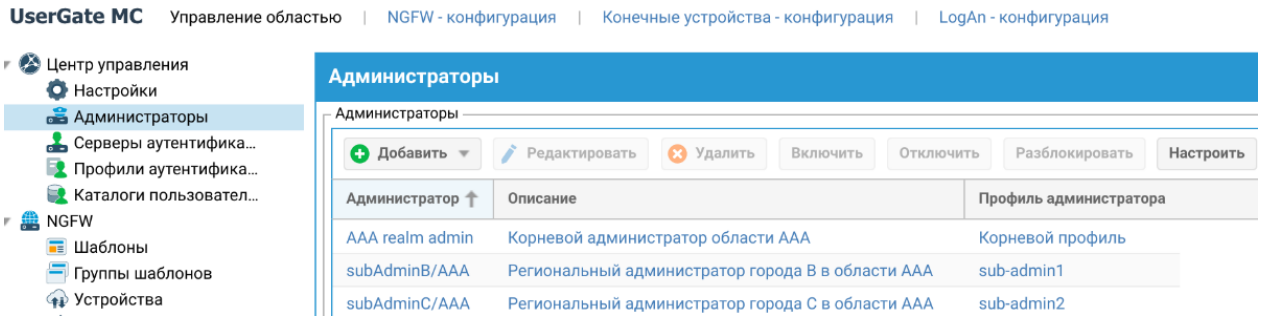
Example 1. Grouping templates

The example of grouping templates for the branches in the managed realm.

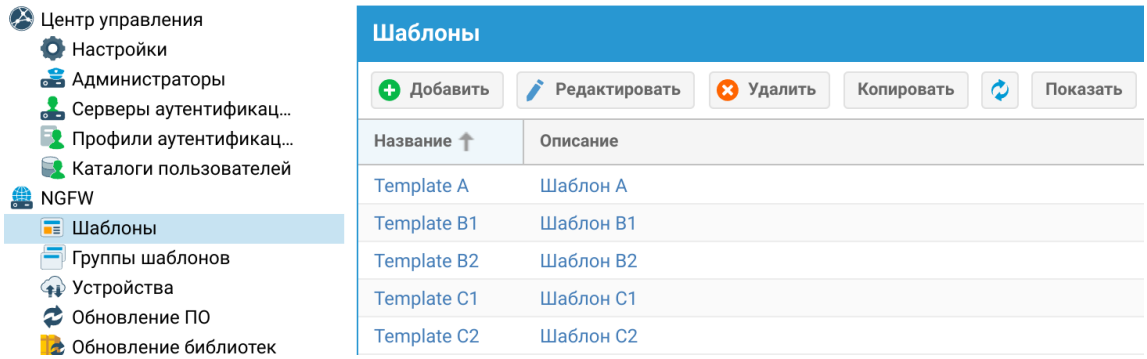
At the UserGate MC the AAA managed realm is created with the root realm administrator **Admin/AAA**.



The realm administrator creates two regional administrators to manage the NGFW nodes in the cities B and C (**subAdminB/AAA** and **subAdminC/AAA** respectively).



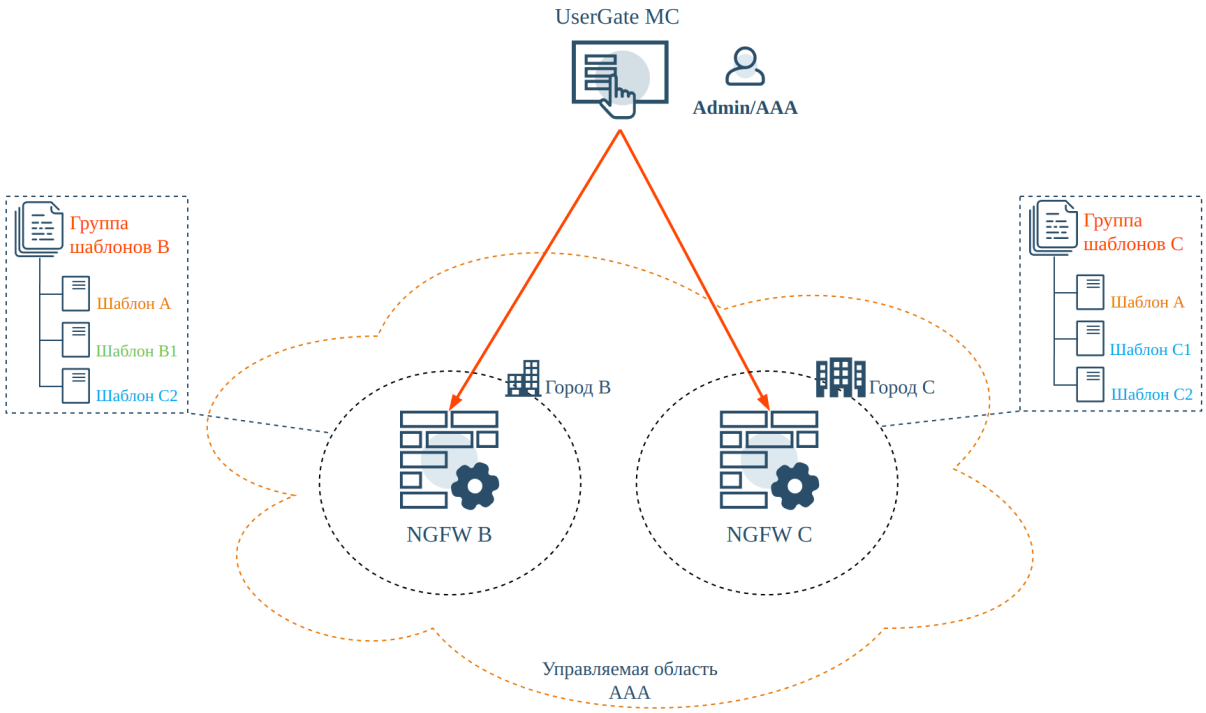
The realm administrator creates the templates to manage the regional nodes and provides the editing permissions for a part of the templates to the regional administrators:



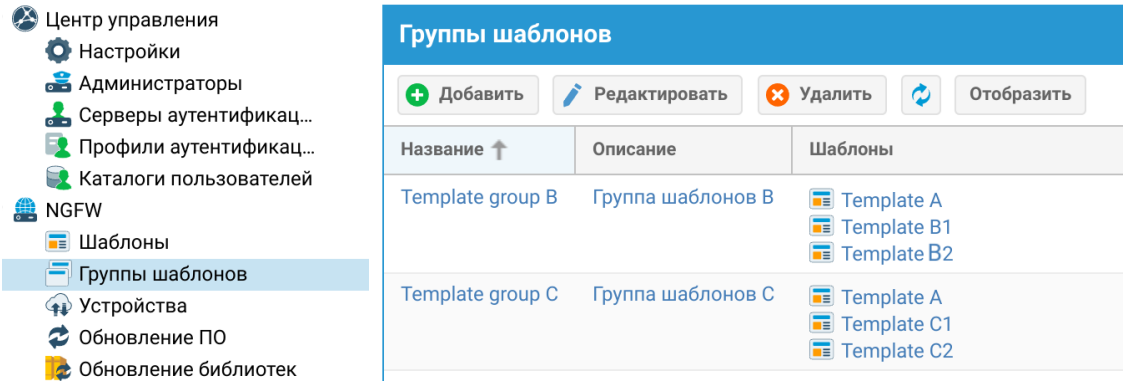
- The template A is used to configure the basic network configuration policies by the realm administrator.

- The templates B1 and B2are used for the local parameters of the node policies at the branch B. The permissions to configure these templates are delegated to the regional administrator in the city B (**subAdminB/AAA**).
- The templates C1 and C2 are used for the local parameters of the node policies in the city C. The permissions to configure these templates are delegated to the regional administrator in the city C (**subAdminC/AAA**).

The realm administrator creates the template groups and it can add any templates created and configured in any region of its realm to these groups.

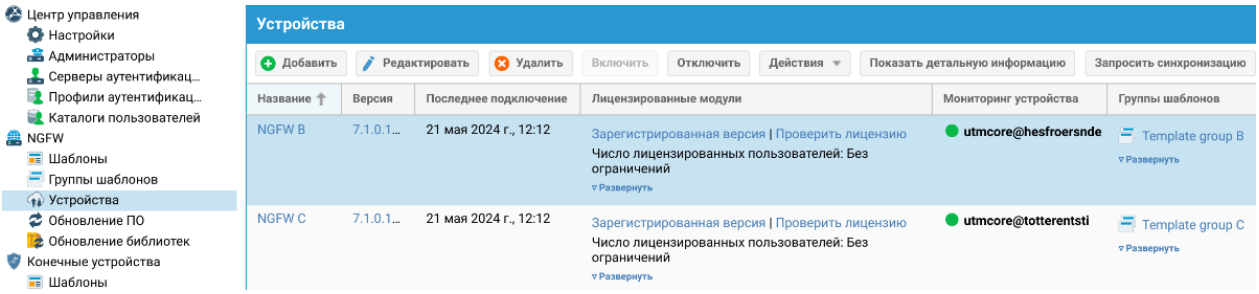


In this example the realm administrator creates a single template group for each city, and it adds to this template group the general template with the basic network configuration policies and templates with the local policy parameters that can be changed by the regional administrators:



- Template group for city B:
    - Template A;
    - Template B1;
    - Template B2;
- Template group for city C:
    - Template A;
    - Template C1;
    - Template C2.

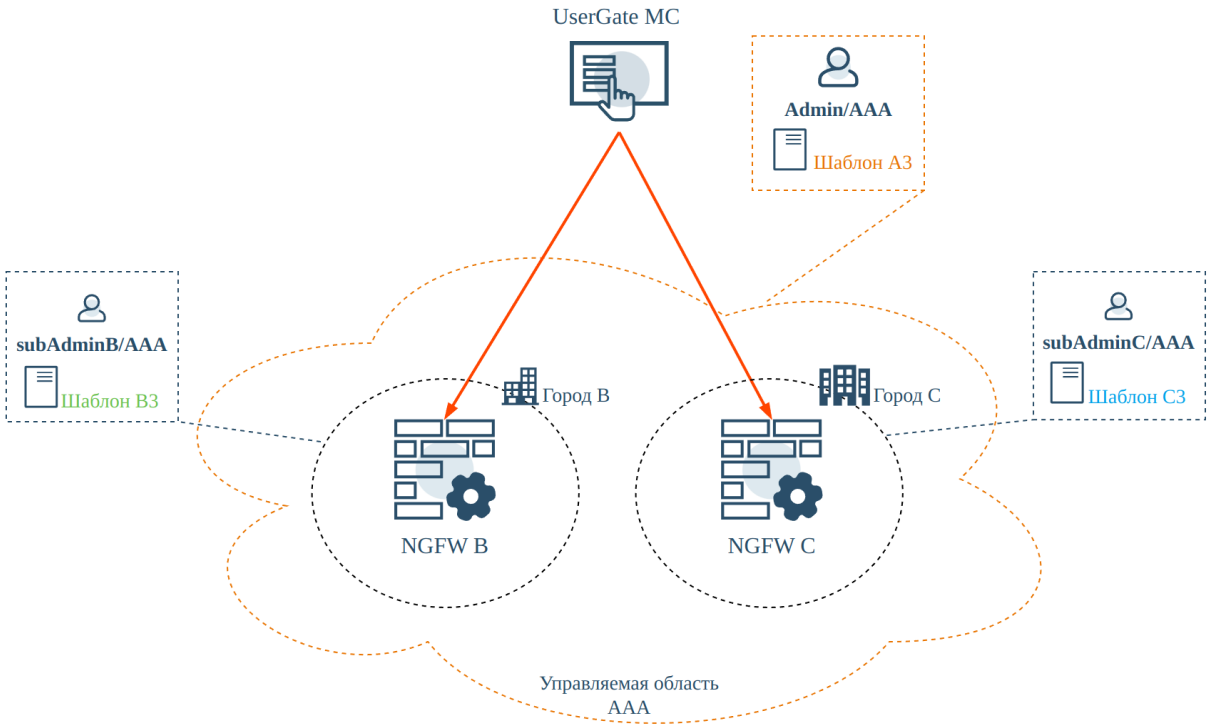
The realm administrator assigns the template groups to the specific managed devices.



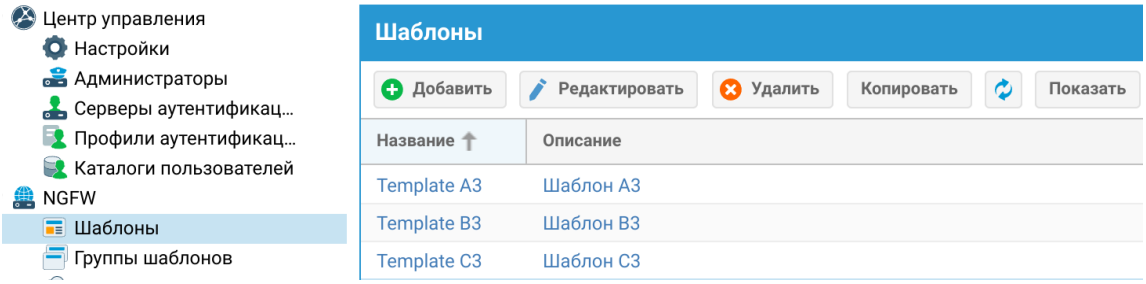
Example 2. The diagram with the main policy

On this diagram there is one central policy, but its specific final form will be different for each region.

As in the Example 1in the AAA managed realm there are two cities B and C. For each city its own NGFW is installed, and they are both connected to the MC. Two regional administrators are created to manage the NGFW nodes in the cities B and C (**subAdminB/AAA** and **subAdminC/AAA** respectively).



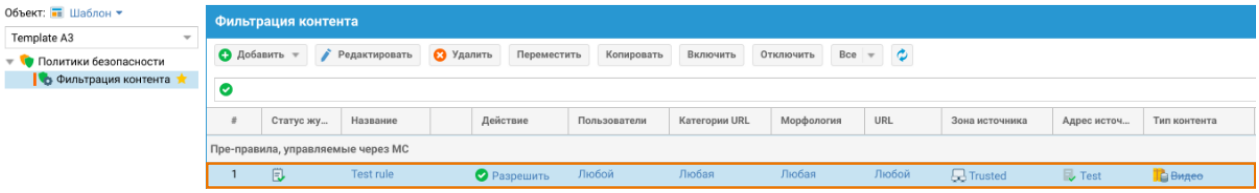
The realm administrator has a general policy template that restricts access to websites hosting video content for the group with Test IP addresses. Each city has its own templates, in which regional administrators define a list of their local addresses for the Test group:

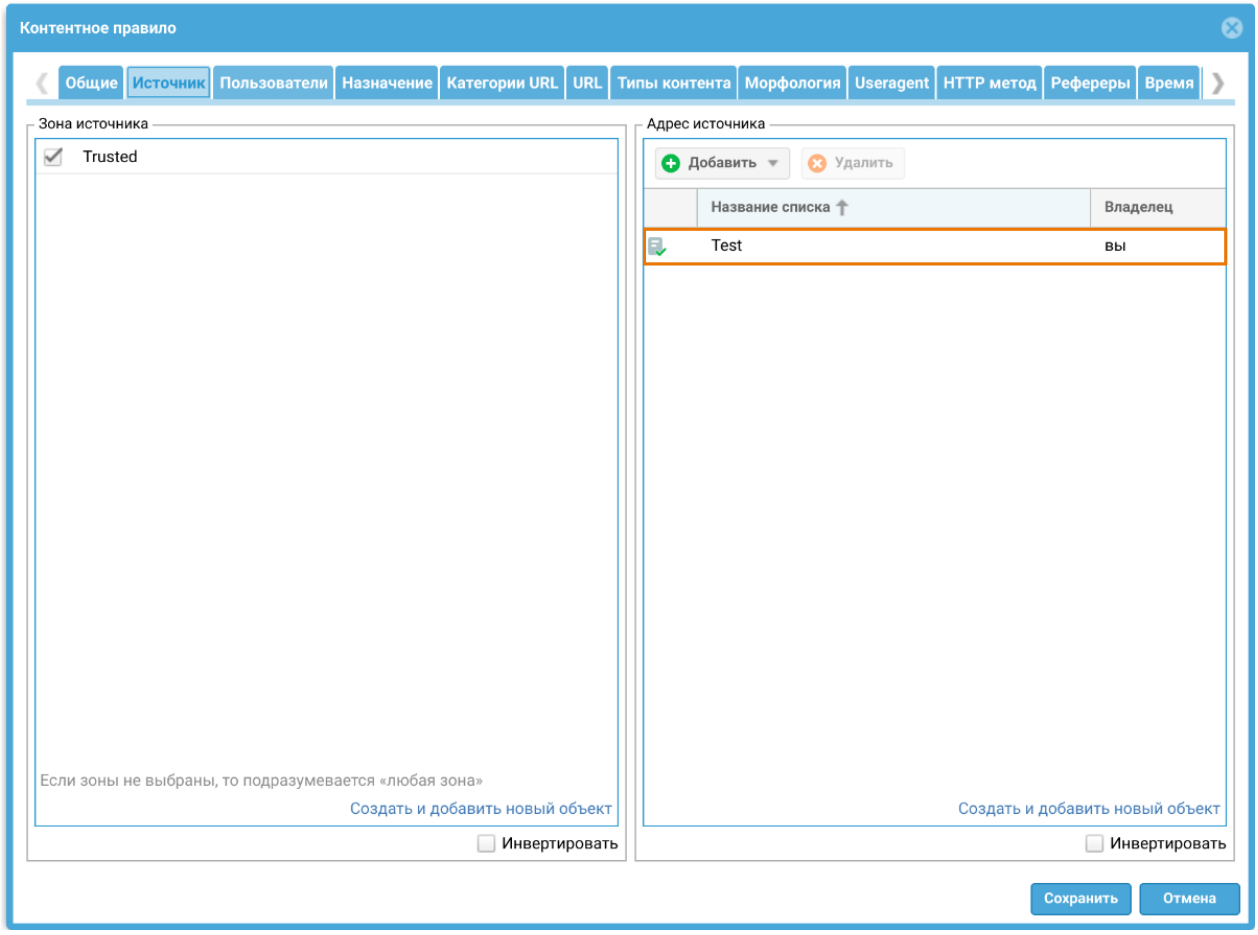


- The template A3 is the general policy template for the realm administrator. This template configures the access restriction to video content.
- Template B3 is for configuring a group of IP addresses to which the policy should be applied. The regional administrator of city B (**subAdminB/AAA**) is delegated rights to configure the parameters of this template.
- Template C3 is for configuring a group of IP addresses to which the policy should be applied. The regional administrator of city C (**subAdminC/AAA**) is delegated rights to configure the parameters of this template.

Configuring templates

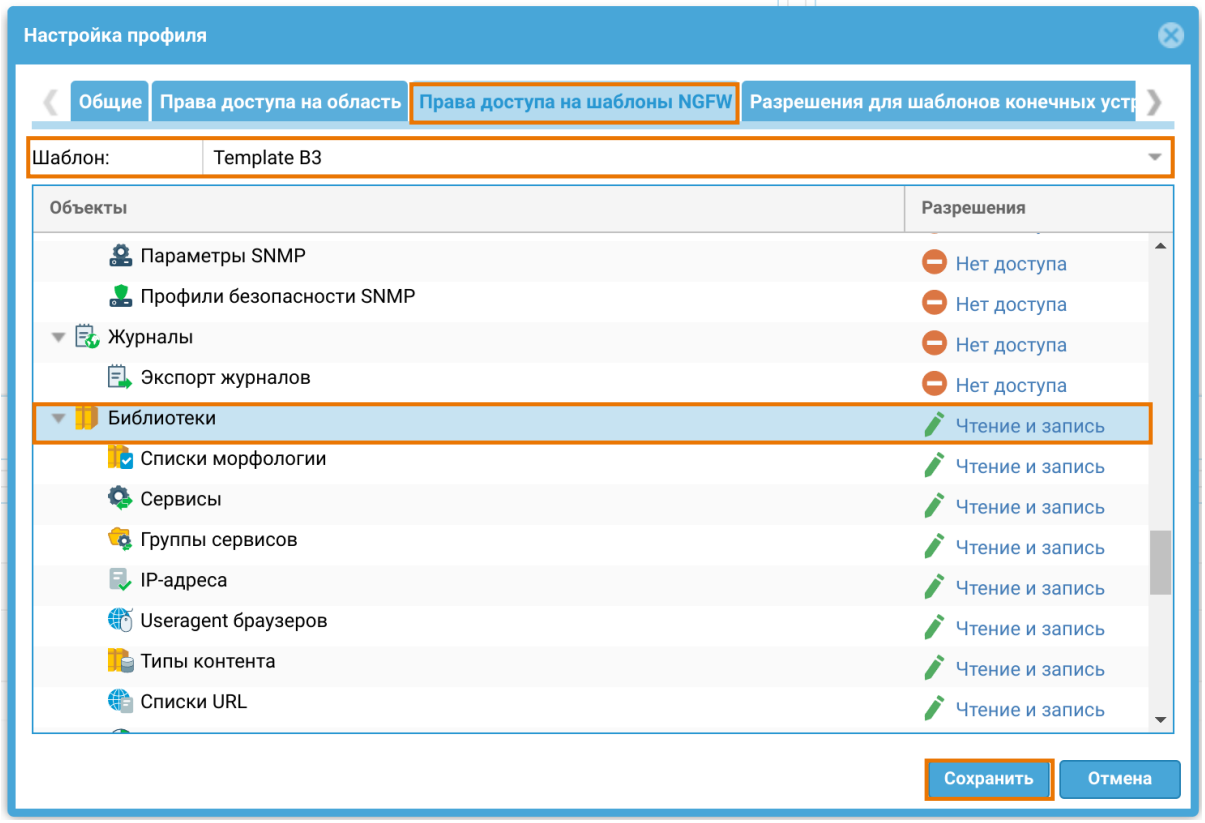
The realm administrator creates the rule for filtering video content in the template A3. In this rule it specifies the IP address group **Test** on the **Source**tab, but the addresses themselves are not specified in the template. The lists of the IP addresses to which the general policy rule will be applied are created in the **Test** address group by the regional administrators in their templates.



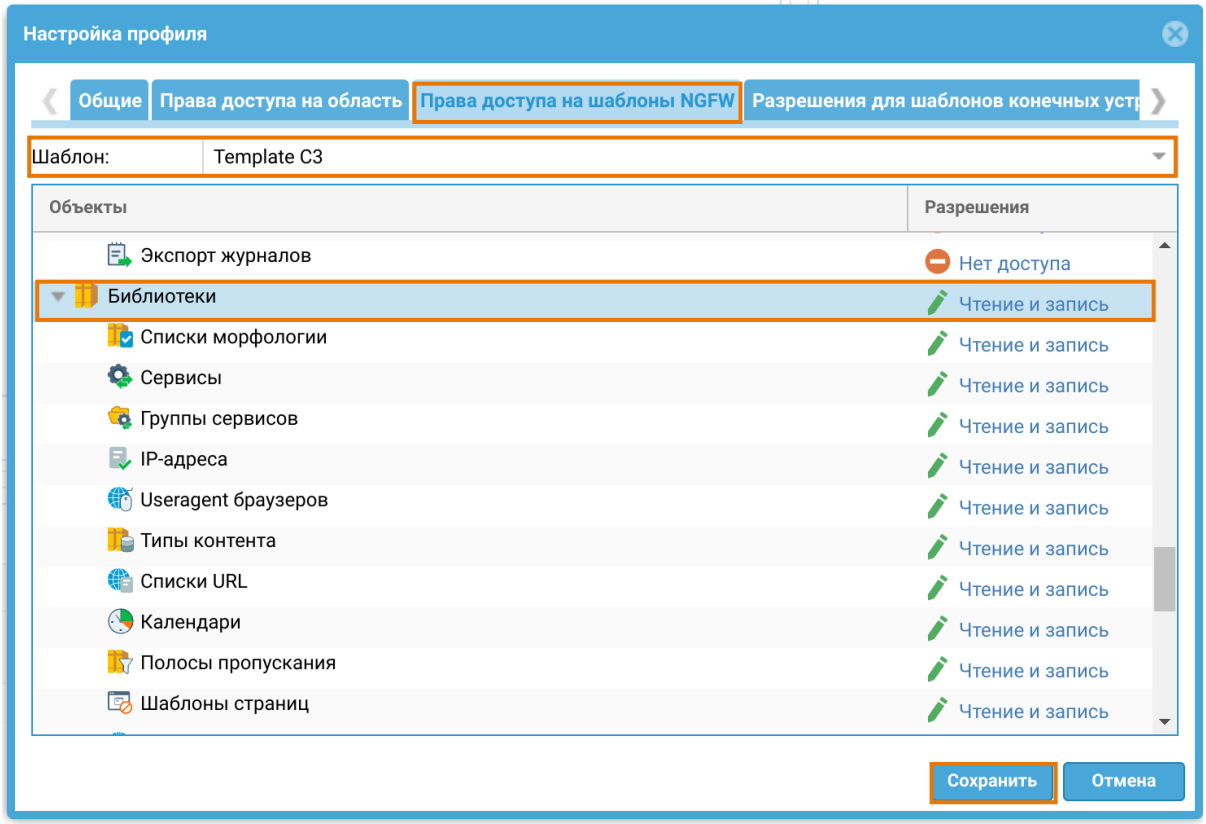


The realm administrator delegates the permissions for configuring the item libraries in the B3 and C3 templates to the regional administrators. To do this, open the web console of the realm administrator and under **Central management → Administrators → Administrator profiles** and in the profiles of the regional administrators provide the read and write permissions for the**Libraries of items** section.

The permissions in the B3 template should be delegated to the regional administrator of the city B:

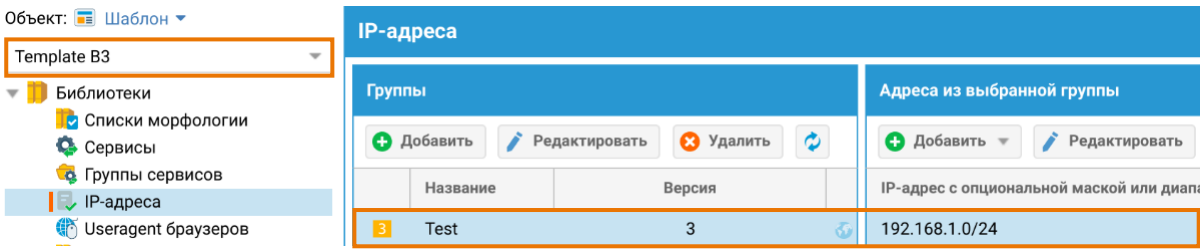


The permissions in the C3 template should be delegated to the regional administrator of the city C:

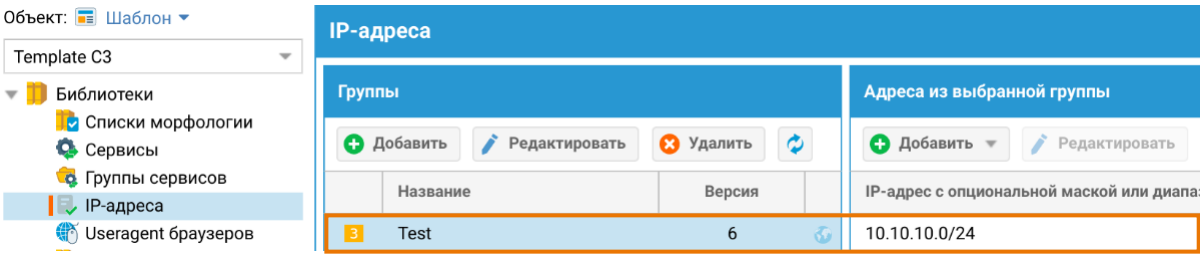


The regional administrators create the **Test** IP address group in their templates. To do this, each regional administrator should log in to the web admin console with their login (**subAdminB/AAA** or **subAdminC/AAA** respectively), open the template settings section (template B3 or template C3 respectively) and create the **Test** IP address group containing the actual addresses:

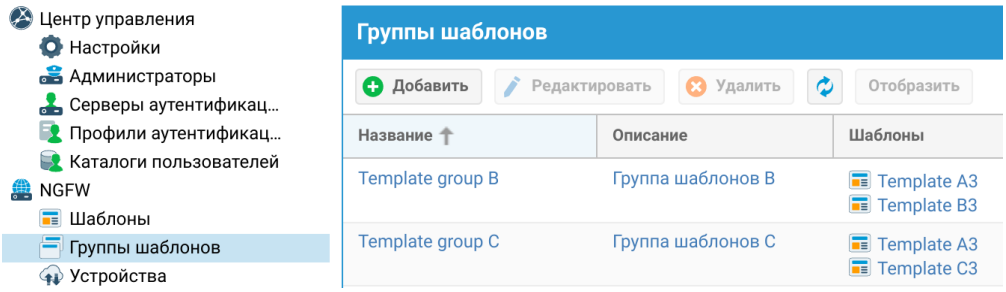
The regional administrator of the city B edits the B3 template:



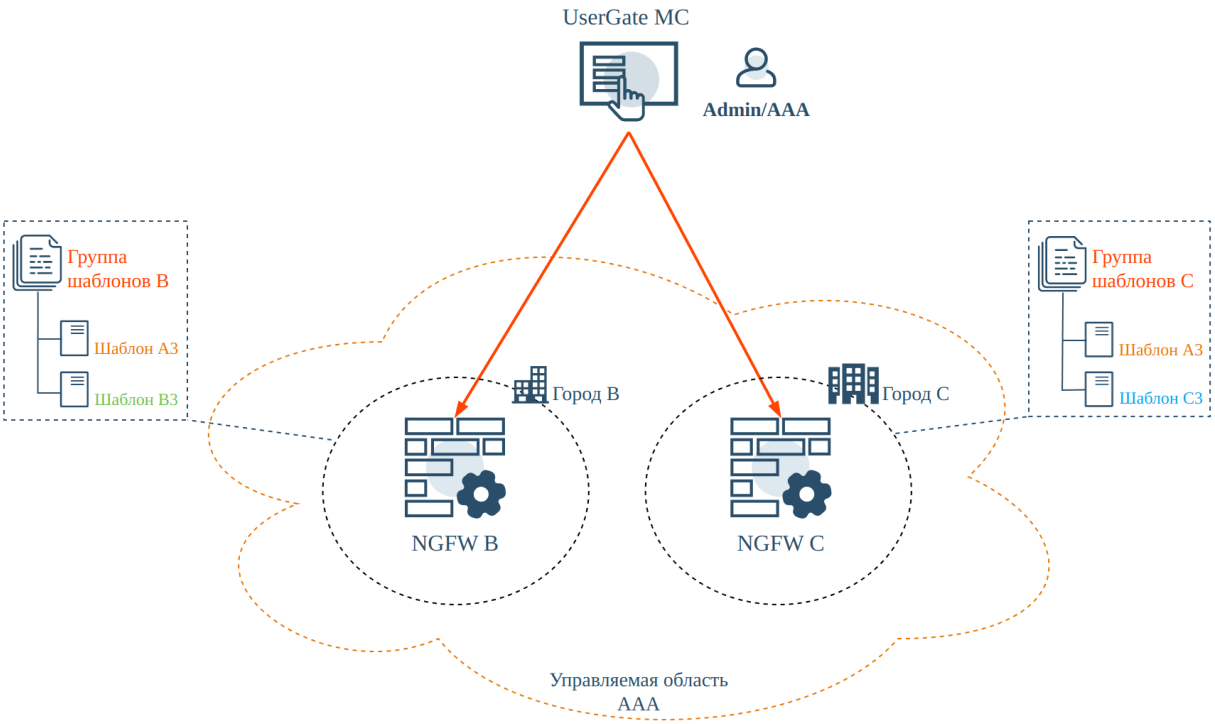
The regional administrator of the city C edits the C3 template:



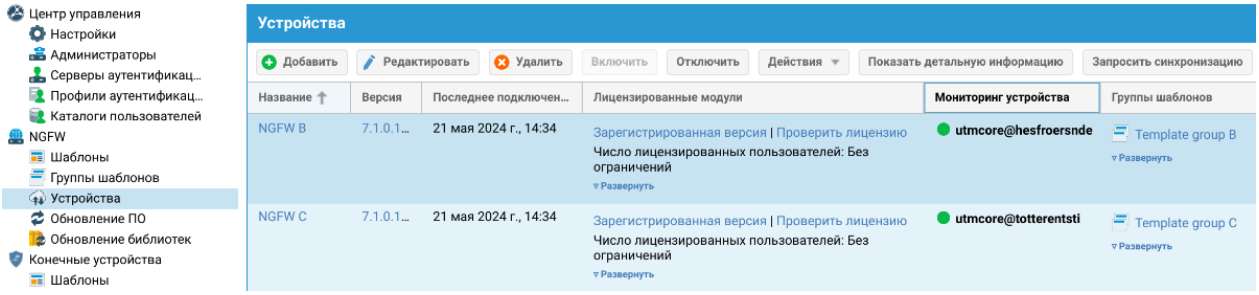
The realm administrator combines the templates into the groups:



- Template group for city B:
  - Template A3;
  - Template B3;
- Template group for city C:
  - Template A3;
  - Template C3.



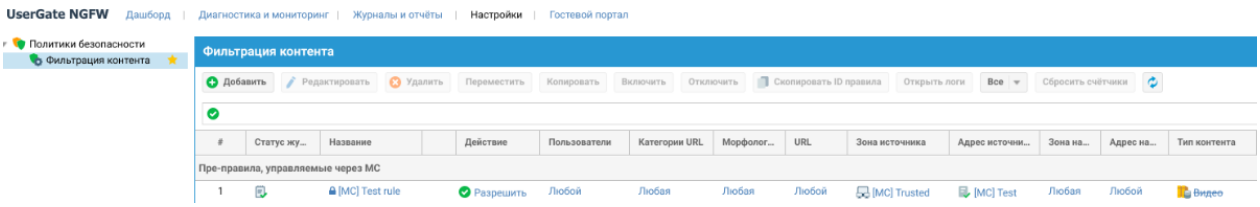
The realm administrator assigns the template groups to the specific managed devices.

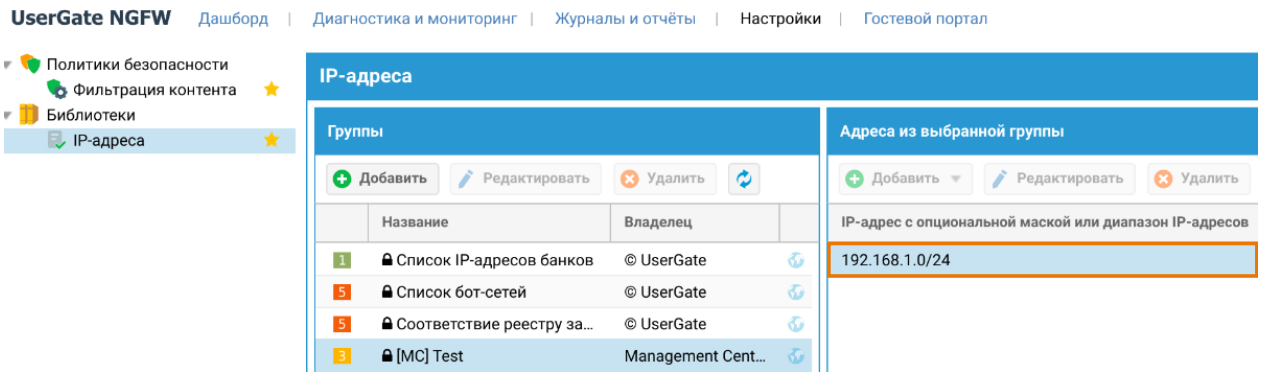


Checking the diagram

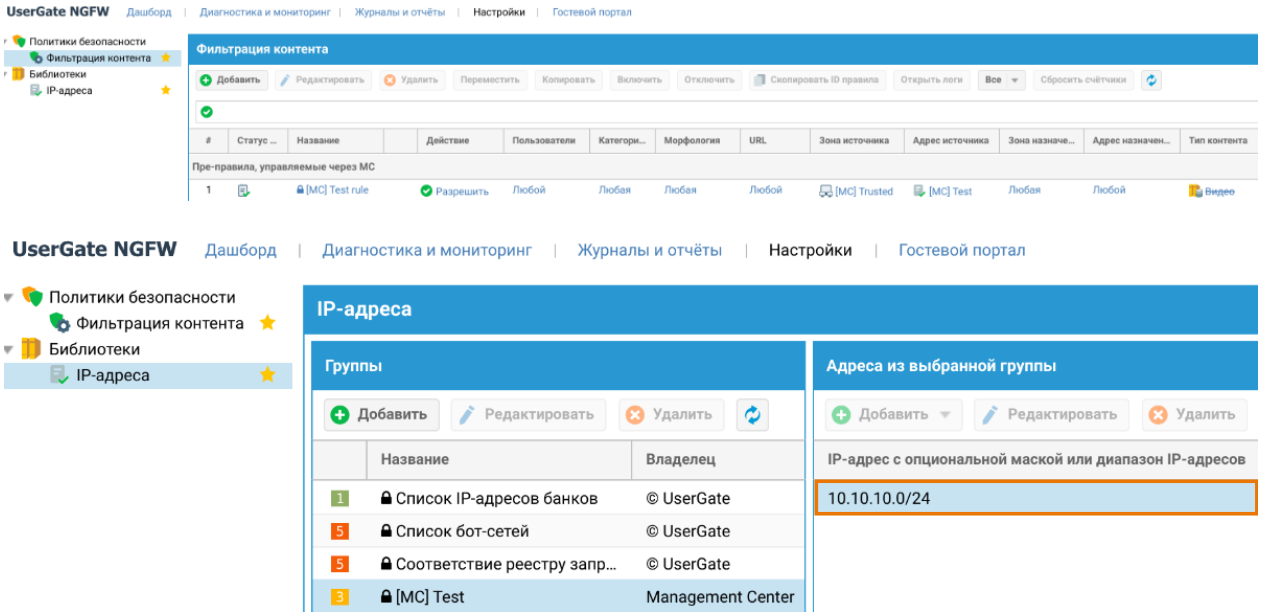
Each regional device has its own policies with its own rules for filtering video content.

NGFW B:





NGFW C:



So here we can see the centralized management of access policy to the websites with video content for the two cities, and the regional characteristics (different subnets) of every branch are taken into account. The realm administrator creates and manages the general policy template, and the regional administrators configure and manage their devices taking the regional parameters into account.

LOGAN DEVICE MANAGEMENT

LogAn Device Management (Description)

The process of centralized LogAn devices management can be divided into the following 4 steps:

1. Create a managed realm. See the Creating Managed Realms section.
2. Create one or more templates, each describing a distinct part of the LogAn settings. For more details, see the LogAn Device Templates section.
3. Combine the relevant templates into a template group in the required order to obtain the correct final manged device configuration. For more details, see the LogAn Template Groups section.
4. Add a managed LogAn device and apply the template group to it. For more details, see the Placing LogAn Devices under UGMC Management section.

If necessary, the parameters in the templates can be changed. These changes will be applied to all managed LogAn devices to which the modified templates apply.

LogAn Device Templates

A template is a basic component that allows you to configure all settings of a firewall: network settings, firewall rules, content filtering rules, intrusion detection system rules, etc. To create a template, go to the **LogAn → Templates** section, click **Add**, and provide a name and optional description for the template.

After creating a template, you can configure its settings. To do that, click **LogAn configuration** in the top menu and select the desired template from the drop-down menu **Select template** that appears.

Template settings are displayed in a tree view, very similar to how they are presented in LogAn. When configuring templates, follow these rules:

1. If the value of a setting is not defined in the template, nothing will be sent to LogAn. In this case, LogAn will use the default setting or a setting configured by a local administrator.
2. If the value of a setting is specified in the template, it will override the value assigned to the same setting by a local administrator.

After receiving the settings from UGMC, the settings for the following sections can be changed locally on Log Analyzer:

- general device settings: the **General settings** tab, **Admin Console → Settings** section;
- network interface settings: **General settings** tab, **Network → Interfaces** section.

> **Note**
> **The setting will be overridden when this setting is changed by the realm administrator in the LogAn template on UGMC.**

3. When configuring network interfaces, the first configurable physical interface is **port1**. The **port0** interface is not available for configuration from UGMC; it is always configured by a local administrator and required for primary communication between the managed device and UGMC.
4. When configuring network interfaces, you can create an interface and delegate its configuration to a local administrator. To do that, set the **Configured on the device** flag in the settings for the network interface.
5. Some settings and policy rules offer the option to apply the setting or rule only to a specific device. To do that, go to the **Managed devices** tab in the setting/rule properties and select the desired managed device. Despite a certain amount of flexibility that this option provides, avoid overusing it because it complicates the understanding of how settings are applied to LogAn device groups.
6. Libraries (e.g., IP addresses, URL lists, content types, etc.) have no predefined content in UGMC, unlike the default libraries created on UserGate devices. To use libraries in UGMC policies, you need first to add items to them.
7. It is recommended to create separate templates for different settings groups to avoid conflicts between settings when templates are combined into template groups and to make it easier to understand the final settings that will be applied to UGC managed devices. For example, you can create separate templates for network settings, libraries, etc.

LogAn Template Groups

Template groups allow multiple templates to be combined into a single configuration that applies to a managed device. The final settings that will apply to a LogAn device

are generated by merging all settings specified in the templates of a template group based on their placement in the group. For more details on final settings, see the Templates and Template Groups section.

To create a templates group, go to the **LogAn → Template groups** section, click **Add**, provide a name and optional description for the template group, and add existing templates to it. After adding the templates, you can arrange them in the desired order using the **Up**, **Down**, **Top**, and **Bottom** buttons to create the required final configuration.

Placing LogAn Devices under UGMC Management

A template group always applies to one or more LogAn devices. The procedure for adding managed devices to UGMC consists of the following steps:

Name	Description
Step 1. Enable access to UGMC from the managed device.	On the UGMC server, allow the **UserGate Management Center** service in the zone to which the managed devices are connected. The UGMC server listens for managed device connections at TCP ports 2022 and 9712. Data transfer between the UGMC server and managed devices occurs over an encrypted data link.
Step 2. Create a managed LogAn device object.	In the **LogAn → Devices** section of the realm management console, click **Add** and provide the desired settings.
Step 3. Link the LogAn managed device object just created to a real LogAn device.	In the LogAn management console, set up the link between UGMC and the device. This can be done during the initial configuration of LogAn or on an already configured LogAn device. Both options are described in detail later in this chapter.

When creating a LogAn managed device object, provide the following settings:

Name	Description
Enabled	Enables the managed device object . When enabled, the managed device object takes up one license.
Name	The name of the managed device. The name can be arbitrary.
Description	Managed device description.
Templates group	The templates group whose settings should be applied to this managed device.

Name	Description
Sync mode	Select the mode used to synchronize the template group settings with the device. There are three options: • **Auto sync**: the settings are applied to the device automatically. A change to any setting in any template of the template group applied to the managed device is propagated immediately to LogAn. • **Disabled**: sync mode is disabled. • **Manual sync**: in this sync mode the settings are applied on clicking the **Sync now** button. This option is useful when many template settings need to be changed and applied to the device at once. In this case, you need to disable synchronization, make the desired changes to the templates, and then enable the Manual sync mode. Regardless of the selected mode, you can start synchronization of all settings for the selected devices (in the **LogAn → Devices** section click **Actions → Run full synchronization**).

To enable LogAn-to-UGMC communication during the initial configuration, follow these steps:

Name	Description
Step 1. Copy the device code.	In UGMC, select the managed device object you created and click **Actions → Show device unique code**. Copy the code to the clipboard.
Step 2. During the initial setup of the LogAn MD, select installation using UGMC.	During the initial setup, at the step where the administrator login and password are set, select the link **Configure by UGMC**.
Step 3. Provide the desired settings for the new node and enter the unique device code.	Specify the following settings: • The network settings for this LogAn MD (IP address, subnet mask, gateway). These settings will be applied to the specified interface. After configuring the network settings, the UGMC server must become accessible over the network from this device. • The name and password for a local administrator. • The IP address of the UGMC server and the unique device code saved at the first step.
Step 4. Check the connection.	After connecting to UGMC, LogAn should receive all settings prepared for it in UGMC. In LogAn, these settings are displayed

Name	Description
	with a lock icon, meaning that a local administrator cannot change them. In the UGMC console, the managed device object will display additional information on the connected device, such as PIN code, serial number, license information, RAM usage, etc.

To enable LogAn-to-UGMC communication for an already configured LogAn device, follow these steps:

Name	Description
Step 1. Copy the device code.	In UGMC, select the managed device object you created and click **Actions → Show device unique code** Copy the code to the clipboard.
Step 2. Specify the IP address of the UGMC server and enter the unique device code.	In the **General settings → UGMC agent**, select **Configure**, specify the IP address of the UGMC server, paste the unique device code, and enable this connection. The UGMC server must be accessible over the network from this LogAn device for a successful completion of this step.
Step 3. Check the connection.	After connecting to UGMC, LogAn should receive all settings prepared for it in UGMC. In LogAn, these settings are displayed with a lock icon, meaning that a local administrator cannot change them. In the UGMC console, the managed device object will display additional information on the connected device, such as PIN code, serial number, license information, RAM usage, etc.

After the LogAn device has been successfully added to UGMC, the administrator can edit, enable/disable, and delete the managed device, as well as:

Name	Description
View advanced managed device state information	In the UGMC console, select the managed device object and click **Show device details**. The following information about the connected managed device will be displayed: • Managed device software version • Managed device PIN code • HSC serial number • Device uptime • Device load metrics such as CPU load, RAM usage, swap file usage

Name	Description
Connect to the managed device console	In the UGMC console, select the managed device object and click **Actions → Open console**. The LogAn console will open in a new window.
Modify settings	In the UGMC console, modify the settings of a template from the template group applied to the managed device. The new settings will be applied to the LogAn device.

In the UserGate Management Center web interface, the administrator can filter the view to display:

- all devices;
- enabled or disabled devices;
- online (connected to UGMC), offline (disconnected from UGMC), or not linked devices (not yet connected to UGMC);
- consistent (managed device synchronized successfully) or inconsistent (with errors detected during managed device synchronization) devices;

Update Management for LogAn Managed Devices

UGMC allows you to create a centralized policy for updating the UserGate software (UGOS) and updatable libraries provided on subscription (URL filtering category database, IDPS, IP address/URL/MIME type lists etc.).

> **Note**
>
> **After adding a LogAn managed device to UGMC management, the device starts automatically downloading all updates from the UGMC server.**

To configure update management using UGMC, follow these steps:

Name	Description
Step 1. Configure an update check schedule.	An update check schedule defines the time and frequency of checking for updates. It can be configured locally on each LogAn device or centrally using UGMC templates. The configuration is done identically in both cases. A local update check schedule is configured in the **General settings** section of the device's web management console. When UGMC is used, the schedule is configured in the **General settings** section of a UGMC template.
Step 2. Configure a software update policy for LogAn devices.	A software update policy allows you to specify an update available for installation on all or selected managed devices. For more details on updating software, see the LogAn Software Updates section.
Step 3. Configure a library update policy for LogAn devices.	A library update policy allows you to select the desired library updates for installing on managed devices. For more details on libraries updates, see the Libraries Updates section.

LogAn Software Updates

From time to time, UserGate issues software updates for UserGate LogAn devices. These updates are uploaded to the UserGate repository from where they can then be downloaded to LogAn devices. If UserGate LogAn is managed from UGMC, it checks automatically for available updates on the UGMC server which acts as a repository. The UserGate repository is used in this case by the UGMC server for obtaining new updates.

In some cases, the UserGate support service can suggest that certain customers install specific updates that are unavailable for download from the repository. Such updates should be added to UGMC by importing them from an update file.

To install updates, follow these steps:

Name	Description
Step 1. Upload the updates to the UGMC repository.	The updates can be uploaded from the UserGate repository or imported manually from an update file. To upload the updates from the repository, go to the **LogAn → Software updates** section and click **Online updates**. The list of updates available for download from the UserGate repository will be displayed. Highlight the desired updates and click **Select**. The selected updates will be uploaded to UGMC. For manual upload, go to the **LogAn → Software Updates** section, click **Import update**, and select the update file. If the update file has no update name and version specified, enter

Name	Description
	these in the corresponding fields. By clicking **Save**, the selected update will be uploaded to UGMC.
Step 2. Approve the update for all or specific devices.	To install an update on all devices, select the update of interest and click **Approve update**. Only one update can be approved for all devices. If you need to install this update on a group of devices (e.g., for testing), specify the managed devices from which this update will be available in the update's properties and set the **Approve update** flag.
Step 3. Install the update.	After an update is approved, it becomes available for downloading for all managed devices or for a group of them. A managed device downloads the update according to its update check schedule. When downloaded, the update can be installed centrally by the administrator from the UGMC console or manually on a specific managed device by the device's administrator.

An update in the UGMC repository has the following properties:

Name	Description
Name	The name of the update. Usually not editable, hard-coded in the update code.
Description	An arbitrary description of the update.
Version	The update version. Not editable, hard-coded in the update code.
Size	The size of the update.
Release	The LogAn release for which this update is issued. Not editable, hard-coded in the update code.
Status	The update's status — for example, downloaded.
Progress	Shows the progress of downloading the update from the UserGate repository.
Update channel	The update channel of the UserGate repository: • **Stable**: stable software updates • **Beta**: experimental updates
Changelog	A link to the list of changes included in this update.

Name	Description
Managed Devices	The list of managed devices for which this update is intended.
Added	The date the update was added to the UGMC repository and the name of the administrator who added it.
Approved	The date the update was approved and the name of the administrator who approved it.

LogAn Libraries Updates

Libraries are updatable resource databases (URL filtering categories, IPS signatures, IP address lists, URLs, MIME types, morphological databases etc.) provided to UserGate customers on a subscription basis. These updates are uploaded to the UserGate repository from where they can then be downloaded to LogAn devices. If LogAn is managed from UGMC, it checks automatically for available updates on the UGMC server which acts as a repository. The UserGate repository is used in this case by the UGMC server for obtaining new updates. By default, UGMC checks for and downloads library updates automatically.

When UGMC does not have access to the UserGate repository, you can import the update manually from an update file you have received in your UserGate client profile (https://my.usergate.com).

Libraries stored in the UGMC repository are available to all LogAn MDs. A managed device downloads the update automatically according to its update check schedule.

A library update in the UGMC repository has the following properties:

Name	Description
Name	The name of the update. Not editable, hard-coded in the update code.
Description	An arbitrary description of the update.
Download	The mode used to download new versions. **Automatically** is installed by default; in this mode, UGMC automatically checks for and downloads new versions in the UserGate repository. If **Manually** is selected, UserGate will not update the selected library automatically.
Size	The size of the update.

USERGATE CLIENT ENDPOINTS MANAGEMENT

Managed Endpoints

A managed endpoint is a user computer with the UserGate Client (UGC) software installed. UserGate Client software is a component of the UserGate SUMMA ecosystem allowing the administrator centrally manage the UGC managed device fleet and obtain device state information from them, such as CPU load, critical events that occurred on specific devices, logs for various services, logs and notifications from antimalware products, and more. The scope of information obtainable from the UGC managed devices will be constantly expanded.

With UserGate Client software, the administrator can flexibly configure security policies using firewall rules that allow filtering traffic based on source/destination addresses, users, services, URL lists and categories, applications, and content types. Security compliance is implemented based on HIP profiles (for more details, see the HIP profiles section).

The telemetry information, OS logs and other endpoint security data is sent to the LogAn event analytics system and can be used to implement automated response to security threats.

> **Note**
> **Currently, endpoints management using MC is only implemented for UserGate Client software for Windows OS.**

Centralized Endpoint Management

Setting up centralized endpoint management consists of the following steps:

1. Create a managed realm. For more details, see the Creating Managed Realms section.

2. Create one or multiple templates, each describing a distinct part of the managed device settings. For more details, see the UGC MD Device Templates section.

3. Combine the templates into a group in the required order to obtain the correct final manged device parameter configuration. For more information, see the UGC Managed Device Template Groups section.

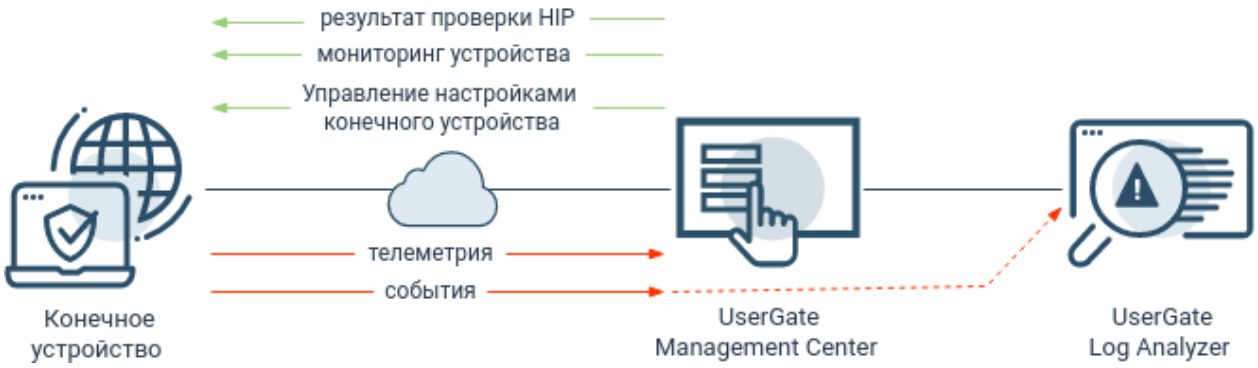
4. Install UserGate Client software on user computers. For more information, see the UserGate Client Installation section.

5. Adding a managed device and applying a template group to it. For more information, see the Placing UGC MD Devices under UGMC Management section.

6. Managing devices from the UGMC console. For more information, see the UGC Device management from the UGMC Console section.

UserGate Client Working in Conjunction with UGMC

When endpoints are connected to the UGMC, the administrator can centrally manage numerous endpoints, flexibly configure security policies using firewall rules, and perform endpoint compliance checks.



Port 4045 is used to register an endpoint device on the UGMC; devices are registered using a pin code. After registration, the endpoint device is assigned a unique ID to communicate with the server in the future.

Once registered, the endpoint requests configuration from the UGMC every 10 seconds. UGMC sends to the endpoint the firewall and VPN settings, general template settings, element libraries, HIP objects, and profiles if they are used in firewall rules. The configuration is sent to the endpoint device if it is changed on the UGMC.

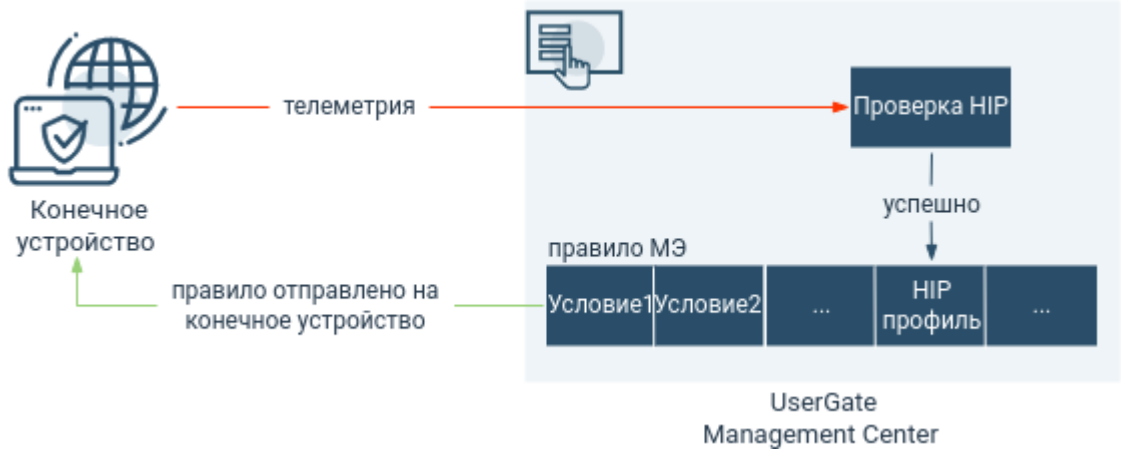
The endpoint sends telemetry (CPU load, disk information, system uptime, etc.) to UGMC, as well as configuration that is used for HIP validation: the information about the system security level (status of antivirus, firewall, automatic system update, BitLocker), the list of running processes and services, list of installed updates, and the information about installed software. The configuration will only be sent in case of changes.

An additional block of information is transmitted to UGMC when the window with information about the endpoint is opened (**Realm management** desktop, **Endpoints → Devices** section). This block contains information about the current time and boot time of the endpoint device (including time zone), USB devices connected to the device, startup items, restore points, processes, services, performance (CPU utilization, memory, disk size and type, UserGate Client status), installed system updates and registry keys (if search was used in the respective tab).

If UserGate Log Analyzer is used: for each active LogAn server, a port in the range of 22000–22711 is opened. This port receives telemetry, Windows logs and other endpoint security data sent to LogAn in transit through UGMC. The received data can be used to analyze and automatically respond to security threats.

HIP Checking in UGMC

UserGate allows to check if an endpoint complies with the security requirements. Compliance checking is based on HIP profiles (see the respective section of the Administrator's Guide for details) and follows this procedure:



The endpoint sends the following data to UGMC:

- the user information;
- the system data (version, edition, netbios name);
- the list of running processes;

- the list of running services;
- the list of installed software (name, vendor, version);
- the registry keys;
- the list of system updates;
- the startup items;
- the information about system security (antimalware, firewall, BitLocker, etc.);
- the information about system restore points.

> **Note**
> **If no HIP profile is specified, the FW rule is applied to all endpoint devices.**

> **Note**
> **If the endpoint OS returns incorrect duplicate information about the same antivirus software installed with different statuses (one with the status enabled, the other with the status disabled), then the worst case (antivirus disabled) is taken into account when checking HIP. The antivirus software database update status is checked only for the enabled antivirus.**

Only HIP profiles specified in the firewall rules as one of the filtering conditions are used to check for compliance with security requirements. The check result is displayed in UGMCenter console in the **Realm Management** under **Endpoints → Devices**. If case of success, the rule is sent to the endpoint device.

UGC Managed Device Templates

A template is a basic component that allows you to configure all settings of a device, such as network settings, firewall rules, content filtering rules, etc. To create a template, go to the **Endpoints → Templates** section, click **Add**, and provide a name and optional description for the template.

After creating a template, you can configure its settings. To do this, go to the desktop **Endpoints — configuration** and select the required template in the drop-down menu.

Template settings are displayed in a tree view. When configuring templates, follow these rules:

1. If the value of a setting is not defined in the template, nothing will be sent to the UGC managed device. In this case, the default setting will be used.
2. Libraries (e.g., IP addresses, URL lists, MIME content type lists, applications, etc.) have no predefined content in UGMC. To use libraries in filtering policies, you need first to add items to them.
3. It is recommended to create separate templates for different settings groups to avoid conflicts between settings when templates are combined into template groups and to make it easier to understand the final settings that will be applied to UGC managed device. For example, you can create separate templates for firewall rules, content filtering rules, libraries, etc.

When creating a template, the administrator can use sections such as "General Settings", "VPN Settings", "Network Policies", and "Libraries".

General Settings

This section defines the general UGC managed device settings:

Name	Description
UserGate client installation settings	These are the settings that control the installation of UserGate client software: • **Collect endpoint data**: collect information on the device (IP address, time of last connection to UGMC, user, computer name, OS version, UGC software version, CPU load, RAM usage, running processes and services, etc.). Default value: **Yes**. If disabled, UGMC will only obtain the following information on the device: IP address, endpoint device name, UGC software and Windows OS versions, current time, device boot time, CPU load, and RAM usage. **Important!** **Disabling endpoint data collection affects how HIP profiles work.** • **Allow network access when UserGate Client stopped**: configure access to the network when the UserGate Client software is stopped.

Name	Description
	Default value: **Yes**. • **Allow user to disable firewall**: allow the user to disable content filtering on the device using the GUI. The options are: ◦ **No**: users are not allowed to disable content filtering. ◦ **Yes**: users are allowed to disable content filtering. ◦ **By code**: users are allowed to disable content filtering on entering a code. To allow a user to disable content filtering, you need to provide or generate a code that the client must enter on the device. You can also specify an expiration time for the code. In addition, when you allow the user to disable content filtering, you can specify how many times or for how long the filtering will be disabled. Default value: **Yes** (filtering can be disabled for 10 minutes without entering a code). **Important!** If you use a counter for the number of times filtering can be disabled (Allowed number of shutdowns), note that the counter is reset each time you change any settings in the Allow user to disable firewall section. • **Allow user to uninstall UserGate Client**: allow the user to uninstall the UserGate Client software. With the **By code** option, you need to provide or generate a code that the user must enter to be able to delete the software. Default value: **Yes**. **Important!** **These settings will not be applied if sync mode is not enabled (the *Sync* checkbox is not set). If the checkbox is not set, the default value will be used.**
Notifications	Configure alerts: • **Show tray icon**: UserGate Client will display an icon in the taskbar notification area. • **Show notification tooltips**: enable or disable sending notifications to the device. If notifications are disabled, the alerts will not display on the endpoint regardless of the settings for specific alert types (device added to/removed from quarantine, resource blocked).

Name	Description
	• **Device added to quarantine message**: send an alert when a device is blocked. To configure the alert, specify the message text and alert type. The alert will be displayed in a pop-up window. • **Device removed from quarantine message**: send an alert when a device is unblocked. To configure the alert, specify the message text and alert type. The alert will be displayed in a pop-up window. • **Resource blocked message**: send an alert when an attempt to visit the URL of a resource was blocked. To configure the alert, specify the message text and alert type. The alert will be displayed in a pop-up window. **Important!** **These settings will not be applied if sync mode is not enabled (the *Sync* checkbox is not set). If the checkbox is not set, the default value will be used.**
LogAn device settings	Specify the LogAn server to which the device will send event information. The LogAn server must be already registered in UGMC. **Important!** **These settings will not be applied if sync mode is not enabled (the *Sync* checkbox is not set). If the checkbox is not set, the default value will be used.**

VPN Settings

This section allows you to configure VPN security profiles that define settings such as the pre-shared key and encryption and authentication algorithms. Multi-factor user authentication, where a one-time TOTP code can be used as the second factor, is also supported. The VPN settings are sent to the UserGate Client MD. The user can select the required VPN server for connecting in the initial GUI window.

> **Note**
> **VPN connections can only be configured for devices that run Windows OS 10 and higher. After the connection is terminated, new connection attempts will be made over the next 40 seconds. If connection is not restored during this time, the user will be shown a VPN server selection window.**

To configure a VPN connection, provide these settings:

Name	Description
Enabled	Enable/disable a rule.
Name	The name of the security profile for connecting to the VPN server.
Description	Profile description.
VPN address	Name (FQDN) or IP address of the VPN server. **Note** **When using FQDN for the connection, if the VPN server name corresponds to multiple IP addresses, the client connects to the first address that responds to requests.**
Protocol	VPN protocols to create a tunnel: • **IPSec L2TP**. Layer 2 Tunneling Protocol (L2TP) is used for creating tunnels and the IPSec protocol for protecting the data during transmission. • **IKEv2 with a certificate**. The IKEv2 protocol is used to create a secure channel, and certificates are used for mutual authentication of the server and the client. **Important!** When generating a client certificate, you need to specify the *CN* field, i.e. the ID of the certificate user. • **IKEv2 with a name and a password**. IKEv2 protocol is used to create a secure channel, and login and password (EAP-MSCHAP v2) are used to verify the client. This method is available only for users of the domain RADIUS server.
IKE mode	IKE mode (specify when selecting the **IPSecL2TP** protocol): **Main** or **Aggressive**.

Name	Description
	The difference between the modes is that the aggressive mode uses fewer packets, which allows for quicker establishment of connections. The aggressive mode does not transmit some negotiation parameters and thus requires that they be configured identically at the opposite ends of the connection. **Main mode**. In the main mode, the devices exchange six messages. During the first exchange (messages 1 and 2), the encryption and authentication algorithms are negotiated. The second exchange (messages 3 and 4) implements the Diffie-Hellman (DH) key exchange. After the second exchange, the IKE service on each device creates a master key to use for authentication. The third exchange (messages 5 and 6) authenticates the reporter and responder of the connection (identity checking) and the information is secured using the encryption algorithm established earlier. **Aggressive mode**. In the aggressive mode, there are 2 exchanges, 3 messages in total. In the first message, the reporter transmits information corresponding to messages 1 and 3 of the main mode — that is, the information on encryption and authentication algorithms as well as the DH key. The second message, transmitted by the responder, contains information corresponding to messages 2 and 4 of the main mode and also authenticates the responder. The third message authenticates the reporter and confirms the exchange.
Pre-shared key	This is a string that must match on the client and server for a successful connection. For **IPSec L2TP** protocol.
Phase 1	In the first phase, IKE security is negotiated. The authentication is done using a pre-shared key in the mode selected earlier. Provide the following settings: • **Key lifetime**: the time period after which the parties re-authenticate and re-negotiate the first-phase settings. • **Dead peer detection interval**: the state and availability of the neighboring devices is checked using the Dead Peer Detection (DPD) mechanism. DPD sends R-U-THERE messages periodically to check if the IPsec neighbor is available. Minimum check interval: 10 seconds; use 0 to disable the check. • **Max failures**: the maximum number of failed discovery requests to an IPsec neighbor after which the neighbor will be considered unavailable. • **Diffie-Hellman groups**: select the Diffie-Hellman group that will be used for key exchange. Instead of the key itself, certain general information is transmitted that the DH key generation algorithm needs to create the shared secret key. The larger the Diffie-Hellman group number, the more bits are used to make the key secure.

Name	Description
	• **Security**: the algorithms are used in their listing order. To reorder the algorithms, drag and drop them with the mouse or use the **Up**/**Down** buttons.
Phase 2	In the second phase, the method for securing IPsec connections is selected. You need to specify the following: • **Key lifetime**: the time period after which the nodes must rotate the encryption key. The lifetime for the second phase is shorter than for the first one, which entails a more frequent key rotation. • **Key lifesize**: the key lifetime can also be expressed in bytes. If both values (**Key lifetime** and **Key lifesize**) are specified, the counter that reaches the limit first will trigger session key re-generation. • **Security**: the algorithms are used in their listing order. To reorder the algorithms, drag and drop them with the mouse or use the **Up**/**Down** buttons.

If multi-factor authentication via one-time TOTP codes is used, the token is entered in a separate window that appears on the endpoint device after a certificate is selected or a login/password is entered.

Note

The use of multi-factor authentication via one-time TOTP codes is only available for IKEv2 connections.

Note

For users of a domain RADIUS server, if the first initialization of a TOTP device is performed via URL, you must additionally enable plain-text authentication (PAP) on the Network Policy Server.

Network Policies

This section contains settings for filtering policies, such as the firewall and content filtering policy.

Using firewall rules, the administrator can allow or deny any type of network traffic flowing to or from the UGC device. Source/destination IP addresses, users and user

groups, services, applications, URL lists and categories, content types, HIP profiles, and rule schedules can all be used as conditions for the rules.

Templates can contain pre-rules and post-rules. Pre-rules always reside higher in the rule list and therefore have higher priority than post-rules. Post-rules always reside lower than pre-rules and therefore have lower priority. The ability to create pre- and post-rules allows the realm administrator to define flexible security policy settings.

Note

The rules are applied top to bottom in their listing order. Only the first rule in which all conditions are matched is applied. This means that more specific rules must be placed higher in the list than more general ones. To change the order in which the rules will be applied, use the Up/Down and Top/Bottom buttons or drag and drop the rules with the mouse.

Note

The "Negate" checkbox changes the condition to the opposite, which corresponds to a Boolean NOT (negation).

Note

If there are no rules created, any traffic flowing from or to the UGC managed device is allowed.

To create a firewall rule, go to the **Network policies → Firewall** section, click **Add**, select the rule's position (pre or post), and provide the desired settings.

Name	Description
Enabled	Enables or disables the rule.
Name	The name of the rule.
Description	A description of the rule.
Apply in	Specifies the scope of application of this rule on UGC managed devices. The options are as follows: • **Inside perimeter**: the rule will be applied if the computer with the UGC software installed is located inside the domain network.

Name	Description
	• **Outside perimeter**: the rule will be applied if the computer with the UGC software installed is located outside the domain network. • **Anywhere**: the rule will be applied regardless of the user computer's location.
Action	The action that the rule will take: • **Deny**: blocks the traffic. • **Allow**: allows the traffic. • **Redirect to proxy**: if the traffic matches the rule's conditions, redirect it to the specified proxy. When this action is selected, the **URL lists, Categories, and Content types** settings are not available.
Logging	Sets whether triggers for this rule should be logged on the LogAn server.
Proxy	If **Redirect to proxy** is selected as the action, the proxy is specified here by selecting a proxy profile.
Users	Specify the LDAP users or user groups to which this firewall rule will be applied. To specify the users, a correctly configured LDAP connector is required. For more details, see the Users Catalogs section.
Source	The lists of source IP addresses for the traffic. **Important!** **Creating rules that simultaneously contain conditions for filtering traffic by source address and URL/URL category/content type is not recommended. Such rules may not work correctly.** The list can be created in advance in the **Libraries → IP addresses** section or during the configuration of the rule. For more details on IP address lists, see the IP Addresses chapter.
Destination	The lists of destination IP addresses for the traffic. The list can be created in advance in the **Libraries → IP addresses** section or during the configuration of the rule. For more details on IP address lists, see the IP Addresses chapter.

Name	Description
Service	The service type, such as HTTP, HTTPS, or a service group. The service or service group can be created in advance in the **Libraries → Services** or **Libraries → Services groups** section, respectively, as well as during the configuration of firewall rules. For more details on services, see the Services chapter.
Applications	List of applications to which this rule applies. The application can be created in advance in the **Libraries → Applications** section or during the configuration of the firewall rule. For more details on applications, see the Applications chapter.
URL Lists	The URL address lists. The URL lists can be created in the **Libraries → URL lists** or in the properties of firewall rules. For more details on working with URL lists, see the URL Lists chapter. **Important!** **When URL lists are used as conditions for traffic filtering, the services must be specified.**
URL categories	UserGate URL Filtering 4.0 category lists. The administrator can control access to categories such as pornography, malicious websites, online casinos, gaming and entertainment websites, social networks, and many others. You can also add URL category groups that can be created in the **Libraries → URL categories** section or during rule configuration. For more details on categories, see the URL Categories chapter. **Important!** **When URL categories are used as conditions for firewall rules, the services must be specified.**
Content types	The content type lists. Video, audio, images, executables, and other types of content can be controlled. Administrators can also create custom content type groups. They can be created in the **Libraries → Content types** section or in the properties of the firewall rule. For more details on working with MIME types, see the Content Types chapter.

Name	Description
	Important! **When content types are used as conditions for firewall rules, the services must be specified.**
Time	The time when this rule will be active. The administrator can add the required time period in the Time Sets section or during the configuration of the rule. **Important!** **The schedule uses the timezone of the device with the UserGate Client software installed.**
HIP profiles	The list of HIP profiles. The firewall rule will be applied only if the device matches the HIP objects specified in the profile. For more details on HIP profiles and objects, see the sections HIP Profiles and HIP Objects, respectively. **Important!** **To filter traffic based on the results of a compliance checking, a license for the NAC module is required.**
Endpoint devices	The specific devices to which this rule will apply. If nothing is specified here, the rule will apply to all devices to which this template is applied.

Libraries of items

This section contains website addresses, IP addresses, applications, and other items used in the configuration of UGC managed device rules.

Services

The Services section contains a list of common services based on the TCP/IP protocol, such as HTTP, HTTPS, FTP, and others. These services can be used in UGC managed device rules. A predefined list of services is supplied with the product. The

administrator can add the desired items during use. To add a new service, follow these steps:

Name	Description
Step 1. Create a service.	Click **Add** and enter the name and a description of the service.
Step 2. Specify the protocol and port.	Click **Add**, select the desired protocol from the list, and specify the destination and (optionally) source ports. To specify a port range, you can use a dash (-), such as 33333-33355.

IP Addresses

The **IP addresses** section contains the list of IP address ranges that can be used in UGC managed device rules.

The administrator can add the desired items during use. To add a new address list, follow these steps:

Name	Description
Step 1. Create a list.	In the **Groups** pane, click **Add** and give a name to the IP address list.
Step 2. (Optional) Specify the list update address.	Specify the address of the server where the updatable list is stored. For more details on updatable lists, see later in this chapter.
Step 3. Add IP addresses.	In the **Selected group addresses** pane, click **Add** and enter the addresses. An IP address entry can be in the form of an IP address or IP address/subnet mask (e.g., 192.168.1.5, 192.168.1.0/24).

The administrator can create custom IP address lists and manage them centrally. To create such a list, follow these steps:

Name	Description
Step 1. Create a file with the desired IP addresses.	Create a file named **list.txt** with the IP address list.
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.

Name	Description
Step 4. Upload the files to a web server.	Upload the **list.zip** and **version.txt** files to your website so that they can be downloaded.
Step 5. Create an IP address list and specify an update URL for it.	On each UserGate server, create an IP address list. When creating the list, select **Updatable** as the list type and enter the address for downloading updates. UserGate will check for a new version on your website according to the set update download schedule. The schedule can be configured in the list properties. The available options are: • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

Application Groups

The **Application Groups** library item allows you to create application groups for more convenient use in network traffic filtering rules. For example, the administrator can create an application group called "Business applications" and place the desired applications there.

The UserGate Client software recognizes the application by its checksum, which enables the administrator to control network access for specific applications in a very precise and selective fashion — for example, allow only a specific application version to access the network and block all other versions.

To add a new application group, follow these steps:

Name	Description
Step 1. Create an application group.	In the **Application groups** pane, click **Add** and give a name to the new group.
Step 2. Add applications.	Highlight the group just created, click **Add** in the **Applications** pane, and enter the name of the application and its checksum. The checksum for a Windows executable must be computed using the SHA1 algorithm — e.g., using the fciv utility.

The user can export and import lists using the **Export** and **Import** buttons. Application list entries or application listing file entries must follow the **APPLICATION_NAME HASH** format.

URL Lists

The URL lists page allows you to create URL lists to be used as black and white lists in content filtering rules.

To configure filtering using URL lists, follow these steps:

Name	Description
Step 1. Create a URL list.	In the **URL lists** pane, click **Add** and set: • List name • Description (optional) • List type: **Local** or **Updatable** • Case sensitivity: ◦ **Case-sensitive**: a list of case-sensitive URLs ◦ **Case-insensitive**: a list of case-insensitive URLs. Using the list of this category avoids having to search through all spelling variants of the same expression that differ in letter case. ◦ **Domain**: a list of domain addresses to use in DNS filtering rules. • Update URL if the list is updatable

Name	Description
Step 2. Add the relevant entries to the new list.	Add URL entries to the new list. You can use wildcards such as "^", "$", and "*": • "*": any number of any characters • "^": start of a line • "$": end of a line The "?" and "#" characters cannot be used.
Step 3. Create an endpoint firewall rule containing one or more lists.	See the Network Policies section.

If you want to block an exact address, use the "^" and "$" characters:

^http://domain.com/exacturl$

To block an exact URL with all child directories, use the "^" character:

^http://domain.com/exacturl/

To block a domain with all possible URLs, use this notation:

domain.com

An example of interpreting URL entries:

Example entry	HTTP request processing
yahoo.com or *yahoo.com*	The entire domain along with all its URLs and 3rd level domains are blocked, e.g.: http://sport.yahoo.com http://mail.yahoo.com https://mail.yahoo.com http://sport.yahoo.com/123
^mail.yahoo.com$	Only this address is blocked: http://mail.yahoo.com https://mail.yahoo.com
^mail.yahoo.com/$	Nothing is blocked, since the last forward slash character defines a URL, but there is no "https" or "http".
^http://finance.yahoo.com/personal-finance/$	Only this address is blocked: http://finance.yahoo.com/personal-finance/

Example entry	HTTP request processing
^yahoo.com/12345/	These are blocked: http://yahoo.com/12345/whatever/ https://yahoo.com/12345/whatever/

The administrator can create custom lists and distribute them centrally. To create such a list, follow these steps:

Name	Description
Step 1. Generate a file with the relevant URL list.	Generate a file named **list.txt** with the URL list in the following format: *www.site1.com/url1* *www.site2.com/url2* ... *www.siteend.com/urlN*
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.
Step 4. Upload the files to a web server.	Upload the **list.zip** and **version.txt** files to your website so that they can be downloaded.
Step 5. Create a content type list and specify an update URL for it.	On each UserGate server, create a URL list. When creating the list, select **Updatable** as the list type and enter the address for downloading updates. UserGate will check for a new version on your website according to the set update download schedule. The schedule can be configured in the list properties. The available options are: • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23)

Name	Description
	(days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

URL Categories

The **URL categories** library item allows you to create UserGate URL Filtering category groups for more convenient use in content filtering rules. For example, the administrator can create a category group called "Business categories" and place the desired categories there.

To add a new category group, follow these steps:

Name	Description
Step 1. Create a category group.	In the **URL category groups** pane, click **Add** and give a name to the new group.
Step 2. Add categories.	Highlight the group just created, click **Add** in the **Categories** pane, and select the desired categories from the list.

Content types

Using content type filtering, you can control the video and audio content, images, executables, and other content types.

To configure filtering by content type, follow these steps:

Name	Description
Step 1. Create a content type list.	In the **Categories** pane, click <0>Add and give a name to the new content type list. Optionally, provide a description and update URL for the list.

Name	Description
Step 2. Add the relevant MIME types to the new list.	Add the relevant content type to the list in the MIME format. You can find descriptions of various MIME types on the Internet — for example, see this link: https://www.iana.org/assignments/media-types/media-types.xhtml. For example, to block *.doc documents, add the "application/msword" MIME type.
Step 3. Create a content filtering rule containing one or more lists.	See the Network Policies section.

The administrator can create custom content type lists and distribute them centrally. To create such a list, follow these steps:

Name	Description
Step 1. Create a file with the relevant content types.	Generate a file named **list.txt** with the content type list.
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.
Step 4. Upload the files to a web server.	Upload the **list.zip** and **version.txt** files to your website so that they can be downloaded.
Step 5. Create a content type list and specify an update URL for it.	On each UserGate server, create a content type list. When creating the list, select **Updatable** as the list type and enter the address for downloading updates. UserGate will check for a new version on your website according to the set update download schedule. The schedule can be configured in the list properties. The available options are: • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced.

Name	Description
	With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "/2" in the "hours" field means "every two hours".

Time Sets

The Time sets section allows you to define time intervals that can later be used in rules. The administrator can add the desired items during use. To add a new time set, follow these steps:

Name	Description
Step 1. Create a time set.	In the **Groups** pane, click **Add** and provide the name and a description for the new time set.
Step 2. Add time intervals to the time set.	In the **Group** items pane, click **Add** and add an interval. Give a name to the new interval and specify the time.

UGC Managed Device Template Groups

Template groups allow multiple templates to be combined into a single configuration that applies to a managed device. The final settings that will apply to a device are generated by merging all settings specified in the templates of a template group based on their location in the group. For more details on final settings, see the Templates and Template Groups section.

To create a templates group, go to the **Endpoints → Template groups** section, click **Add**, provide a name and optional description for the template group, and add

existing templates to it. After adding the templates, you can arrange them in the desired order using the **Up**, **Down**, **Top**, and **Bottom** buttons to create the required final configuration.

Placing UGC Devices under UGMC Management

To manage devices, you need to add them to UGMC. UGC managed devices can be added in two ways:

1. Adding one UGC managed device at a time. Suitable for companies with only a few UGC managed devices.
2. Bulk addition of devices, suitable for companies with a larger number of devices.

Adding Single Devices

To add a single UGC managed device, follow these steps:

Name	Description
Step 1. Enable access from the UGC managed devices to UGMC.	On the UGMC server, allow the **Endpoints control** service in the access control section of the zone to which the managed device is connected. The UGMC server listens for UGC managed device connections at TCP ports 4045 and 9712. Data transfer between the UGMC server and managed devices occurs over an encrypted data link.
Step 2. Create an entry for the UGC managed device in UGMC.	In the **Endpoints → Devices** section of the realm management console, click **Add** and provide the desired settings.
Step 3. Display the unique code for the new device.	In the **Endpoints → Devices** section of the realm management console, select a record, click **Show device unique code**, and note it. This code will need to be entered when the UGC software is installed on a specific user device (computer).
Step 4. Install the UGC software on the specific user device (computer).	Install the UGC software on the specific user computer (endpoint). In the setup wizard, enter the IP address of UGMC and the unique device code created at the previous step. For more details about installing the software on devices, see the UserGate Client Software Installation section.

When creating a UGC managed device record, provide the following settings:

Name	Description
Enabled	Enables the UGC managed device object .
Licensed	Endpoint licensing: if the flag is set, then it uses one license. If there is no license, the endpoint will not be able to connect to the UGMC. If the flag is removed after registering the device with UGMC, then: • firewall rules earlier received from the MC continue to work; • VPN connection with settings previously received from the MC is available; • The endpoint does not receive new settings from the MC.
Name	The name of the UGC managed device. The name can be arbitrary.
Description	The description of the UGC managed device.
Template Groups	The templates group whose settings should be applied to this managed device. The parameters will be applied after synchronization with UGMC.
Sync mode	The synchronization mode: disabled, automatic, or manual sync.

Adding Devices In Bulk

To bulk-add UGC managed devices, follow these steps:

Name	Description
Step 1. Enable access from the UGC managed devices to UGMC.	On the UGMC server, allow the **Endpoints control** service in the access control section of the zone to which the managed devices are connected. The UGMC server listens for UGC managed device connections at TCP ports 4045 and 9712. Data transfer between the UGMC server and managed devices occurs over an encrypted data link.
Step 2. Create a code for the device group.	In the **Endpoints → Endpoint codes** section of the realm management console, click **Add** and provide the desired settings.
	In the **Endpoints → Endpoint codes** section of the realm management console, click **Endpoint unique code** and note the

Name	Description
Step 3. Display the unique code for the new device group.	code. This code will need to be entered when the UGC software is installed on the device group.
Step 4. Install the UGC software on user devices.	Install the UGC software on user computers (endpoints). In the setup wizard or Active Directory administrative template, enter the unique device group code created at the previous step and the IP address of the UGMC interface to which the managed devices will be connected. Upon completion of the software installation, an entry is automatically created for each UGMC device in the **Endpoints → Devices** section, and each device receives all settings from the template group applied to it. For more details about installing the software on devices, see the UserGate Client Software Installation section.

When creating a code for a device group, provide the following settings:

Name	Description
Enabled	Enables the code. When disabled, the code cannot be used for adding new devices, but all devices created earlier with the same code will continue working.
Name	The name of the code. The name can be arbitrary.
Description	Code description.
Template Groups	The template group whose settings should be applied to UGC managed devices activated using this code. The parameters will be applied after synchronization with UGMC.

Note

After registering an endpoint with the code, you can change the template group used individually for each device. In case of problems, reinstallation of the UserGate Client software and the need to re-register on the UGMC, you are required to use the procedure for reconnecting the device (in the *Managing realm → Endpoints → Devices* section click *Reconnect device*). If you re-register an endpoint with a common code, then a new registration record for the endpoint will be created on UGMC with the device linked to the group of templates specified in the code settings. Previous registration information will also be saved.

UGC Device management from the UGMC Console

A UGC managed device added to UGMC will appear in the realm management web console in **Endpoints → Devices**.

In **Endpoints → Devices**, you can do the following with the managed devices:

- Add a new endpoint device Adding a new endpoint was discussed earlier in the Placing UGC Managed Devices Under UGMC Management section).
- Edit the endpoint device's properties, i.e., update the device name, description, template groups applied to it, and synchronization type.
- Delete the selected endpoint device.
- Enable/disable endpoint device synchronization.
- Enable/disable all network connectivity.
- Specify how frequently the connection between UGMC and UGC managed devices should be synchronized.
- Display the unique device code required for connecting the UGC managed devices to UGMC.
- Reconnect a device i.e. re-register an endpoint device in UGMC. The connection code will be re-generated.
- Start forced synchronization.
- Display the settings applicable to this endpoint device (**Preview** button).

In this section, you can also view the following parameters for each endpoint device:

Name	Description
Name	Name of the endpoint device.
Version	Version of the UserGate Client software installed on the device.
Last access time	The date and time when the endpoint device was last connected.
Telemetry	

Name	Description
	The following information is displayed: • The IP address of the endpoint device used for Internet access. • The NetBIOS name. • The time of the last connection of the UGC managed device to the UGMC. • The user whose account was used to log in. • The computer's name in the local network. • The OS version installed on the endpoint device. • The version of the UserGate Client software installed on the device. • The UserGate client CPU used (extent to which the endpoint device's CPU is loaded by the client). • The UserGate client memory used (how much RAM is consumed by the UserGate client). • The physical RAM usage (how much RAM is used on the endpoint device). • The virtual memory usage (how much virtual memory is used on the endpoint device).
Endpoint device monitoring	Shows detailed endpoint system information. A more in-depth discussion of this topic will follow. If a configuration sync failure occurs for the endpoint device, click **View report** to view a report that will show the time of the last connection to the managed device, the rule name, the object type, the reason for the sync failure, and a description of the error. The sync failure does not change how firewall rules are applied to the endpoint device when errors occur (i.e., the firewall rules set during the last successful synchronization remain in effect); service and process management as well as registry queries are still available.
Endpoints templates group	The template groups applied to the UGC managed devices. The creation of template groups was discussed earlier in the UGC Managed Device Template Groups chapter.
HIP profiles	The list of HIP profiles. An HIP profile will appear in the list only if it is used in firewall rules. A color status indication tells whether the endpoint device matches the HIP profile: • Green: the endpoint matches the profile. • Red: the endpoint does not match the profile.

Name	Description
	In case of a profile mismatch, you can click **View report** to view a report that will show the time when data was last received, the HIP profile and object names, the object type, and the mismatching element of the object. For more details, see the HIP Profiles section.
LogAn devices	The name of the UserGate Log Analyzer server to which the endpoint device sends diagnostics logs and telemetry data.
Last successful sync time	The mode, date, and time of the last successful synchronization of the endpoint device with UGMC. The mode can be one of the following: • **Auto sync**: the settings are applied to the device automatically. A change to any setting in any template of the template group applied to the managed device is propagated immediately. • **Disabled**: sync mode is disabled. • **Manual sync**: in this sync mode the settings are applied on clicking the **Sync now** button. This option is useful when many template settings need to be changed and applied to the device at once. In this case, you need to disable synchronization, make the desired changes to the templates, and then enable the Manual sync mode.

The Endpoint device monitoring tab is needed for monitoring the state of a UGC managed devices. It shows the following parameters of the endpoint device:

Name	Description
General	General information about the device (computer name, OS type and version, UserGate Client software version, IP address, system boot time, and the current device time in the timezone set on the endpoint device) and about the user whose account was used to log in (user's profile photo, name, and status, account type (local or domain), phone, and email). **Important!** To display complete information about domain users, you need to connect the LDAP connector in the **Management Center → User Catalogs** section.
Performance	The following information is displayed: • CPU usage, i.e. the loading on the central processor. • Endpoint device CPU usage by the UserGate Client process. • Endpoint device virtual memory information. • Physical RAM information.

Name	Description
	• Client memory used by the UserGate Client. • Disk information: the disk size, type, and performance. • UGC managed devices status, or the status of the UserGate Client: online/offline (endpoint device availability) or disabled (UserGate Client was disabled from UGMC using the **Disable** button).
Connection security	The security information for the endpoint device, namely status of firewall, antimalware, Windows Update, and Windows Security Center, as well as disk encryption (BitLocker) information.
USB devices	Information about the connected USB devices: • Device **ID**: the VID/PID (Vendor ID/Product ID) pair and the device version number. • The **name** of the device. • **USB class**: e.g., mouse or printer. • **Service**: the drivers used for working with the device.
Startup items	The list of applications configured to start automatically on system login.
Processes	The list of processes running on the endpoint device. By clicking **Kill process**, you can terminate a process on the endpoint device from UGMC.
Services	The list of services running/stopped on the endpoint device. By clicking **Stop service**/**Start service**, you can attempt to stop or start a service on the UGC managed devices from UGMC.
Registry keys	View the registry. Available values: • **HKEY_LOCAL_MACHINE**. • **HKEY_USERS**. You can search for registry keys. To do that, click **Find** (displayed when the mouse cursor is pointed at the directory name).
Installed software	The list of software installed on the UGC managed device showing the vendor name and version number.
Installed updates	The list of updates installed on the UGC managed device showing the Microsoft KB number, product information, vendor name, and installation date.

Name	Description
Restore points	The list of available restore points and information about them.

In the UserGate Management Center web interface, you can filter the UserGate Client MDs available to display:

- enabled or disabled endpoint devices;
- blocked or non-blocked endpoint devices;
- online (connected to UGMC), offline (disconnected from UGMC), or not linked (not yet connected to UGMC) endpoint devices;
- consistent (Endpoint synchronized successfully) or inconsistent endpoint devices (with errors detected during MD synchronization);
- meeting or not meeting the security requirements.

In addition, an advanced search mode is provided that allows you to create complex search filters using a specialized query language.

UserGate Client Software Installation

Description

This article covers the installation of UserGate Client software for Windows.

The UserGate Client software product can be installed on computers running Windows OS 7/8/10/11. The minimum system requirements are 2 GB RAM, CPU speed of at least 2 GHz, and 200 MB of free disk space.

The UserGate Client software is supplied as a Windows .msi or .exe setup file that can be installed manually or by using automation features.

To install the software manually, execute the setup file suitable for your system (32-bit or 64-bit). During the installation, the agent setup wizard will launch and invite you to enter the connection settings for UserGate Management Center such as the IP address of UGMC and the device code created in the Management Center.

> **Note**
>
> **To postpone the connection to UserGate Management Center, click *Cancel*.**

> **Note**
>
> **After the installation of the UserGate Client software, the computer will be rebooted. This is required for the application to work correctly.**

Automated software installation is performed using Microsoft Active Directory Group Policies. To publish the application in Active Directory, you need an .msi setup file and the administrative template UserGateClient.adm where the IP address of UGMC and the devices code created in the Management Center are specified.

When the installation is completed, UserGate Client receives the configuration assigned to it in UGMC and sends the endpoint system information to the Management Center.

The following information is available on a device:

Name	Description
General	Endpoint system information (user, computer name, IP address for Internet access, Windows OS version) and VPN connection information (connection status, VPN IP address of the device, number of bytes sent/received since the VPN connection was established, uptime). You can also configure the following parameters: • **Save login**: stores the user login name for VPN connection after the endpoint reboot; • **Reconnect**: reconnects to the VPN server in case of a connection failure. If the connection is lost, the user will be shown the initial GUI window. If the reconnect option is active, the application will make repeated attempts to connect to the server; if the function is disabled, the initial window with server selection will be displayed. The window will be displayed in the center of the screen (if the **Popup in center** checkbox is active) or at its last location. • **Popup in center**: displays the initial GUI window in the center of the screen if the VPN connection is lost.
Logs	This section contains the following information: • **Logging level**: the diagnostic detail level. The options are: ◦ **Off**: disable the diagnostics log ◦ **Error**: log only errors ◦ **Warning**: log only errors and warnings ◦ **Info**: log only errors, warnings, and additional information

Name	Description
	◦ **Debug**: provide as much detail as possible The log is located at %ALLUSERSPROFILE% \UserGate\UserGate Client\var\log\usergateclient\ug_client.txt. • **Tooltips history**: notification history. • **Export logs**: download the diagnostics log (when done, the directory where the diagnostics log file was saved will open).
Network	The following information is displayed: • **IPCONFIG**: information on all network adapters and the current TCP/IP configuration. • **ROUTING**: entries from the local routing table. • **SOCKETS**: the list of active connections (port type, addresses, connection state, process ID). To copy the information, click **Copy**.
Policy	Here you can view the security information for the device (status of firewall, antimalware, Windows Update, and Windows Security Center). The status values indicated are as follows: • **Yellow**: disabled • **Green**: enabled
Advanced	This section controls content filtering (the ability of a user to disable content filtering according to policies configured on the UserGate Management Center server).

The connection data for UserGate Management Center (IP address and code for connecting the managed device) are specified in the file: %PROGRAMFILES% \UserGate\UserGate Client\usergateclient\bin\endpoint_gui.

UserGate Client Software Installation Recommendations

This section describes additional managed device settings that enhance the event audit capabilities of Microsoft Windows operating systems and make the audit more informative.

> **Note**
> **To be able to send endpoint logs to UserGate Log Analyzer in English, you must install the language pack *English (US)*; English should be available for selection as the interface language.**

> **Note**
> **The settings presented in this section are merely suggestions.**

1. Install the Sysmon utility that provides in-depth information on process creation, network connections, and changes in file creation times. Detailed information about the utility and the setup file can be found at this link.

2. Add a registry key to enable querying of the Sysmon log (Microsoft-Windows-Sysmon/Operational) and sending it to the UserGate Log Analyzer server. To add the key, use the Registry Editor application or run this command:

   REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-Sysmon/Operational"

1. Enable logging for all PowerShell commands and resulting output.

   REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" /v EnableScriptBlockLogging /t REG_DWORD /d 1

> **Note**
> **To quickly launch the Registry Editor application, use the Win+R keyboard shortcut, type regedit, and press Enter.**

If you use Registry Editor for the task, create a variable named **EnableScriptBlockLogging** under the **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogg** registry key and specify a data type of **REG_DWORD** and a value of **1**.

> **Note**
> **This setting can be configured under HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER, with HKEY_LOCAL_MACHINE having priority over HKEY_CURRENT_USER.**

Add a registry key to enable querying of the PowerShell log (Microsoft-Windows-Powershell/Operational) and sending it to the UserGate Log Analyzer server:

REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-Powershell/Operational"

1. Enable recording of additional details of command-line process creation events in the security event log (this data will be added to the "4688: Process created" process creation event). To enable the key, use the Registry Editor application or run this command:

   REG ADD "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\Audit\" /v ProcessCreationIncludeCmdLine_Enabled /t REG_DWORD /d 1

If you use Registry Editor for the task, create a variable named **ProcessCreationIncludeCmdLine_Enabled** under the **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit** registry key and specify a data type of **REG_DWORD** and a value of **1**.

> **Note**
> **This setting is supported on devices running Windows Server 2012 R2 or later and Windows 8.1 or later OS versions.**

Windows Log Events

UserGate Client provides the ability to display events in the Windows application log. Logging of the following events has been added:

- starting and stopping the service (the **UG0101 Service started**, **UG0102 Service stopped** events);
- connection to MC and loss of connection (the **UG0201 MC connected**, **UG0202 MC connection lost** events);

- connection via VPN and termination of the session, including connection errors: server unavailability, incorrectly specified data (the **UG0301 VPN connected**, **UG0302 VPN disconnected** events);
- receiving configuration from Management Center (the **UG0401 MC rules propagated** event).

HIP Profiles

The Host Information Profile (HIP) is a way to collect and analyze information on the level of security of a device with the UserGate Client software installed. An HIP profile is a set of HIP objects used to check if the device meets the security (compliance) requirements. You can use an HIP profile to configure flexible policies for access to a network zone or application.

For devices, only those HIP profiles will be displayed which are used in firewall rules.

> **Note**
>
> **To verify compliance and the operation of filtering rules that use a HIP profile as a condition, a *Network access control at the host level* module license is required.**

When creating a profile, provide the following settings:

Name	Description
Name	HIP profile name.
Description	(Optional) description of the HIP profile.
HIP Objects	Select a Boolean operator (AND, OR, NAND, NOR) and HIP objects here. For more details on object creation, see the HIP Objects section.

HIP Objects

HIP objects allow you to configure compliance criteria for endpoint devices and can be used as conditions in security policies.

> **Note**
> **To specify certain conditions, a licensed *Security Updates* module is required that enables downloading library updates.**

To add an object, provide these settings:

Name	Description
Name	The name of the HIP object.
Description	(Optional) description of the HIP object.
OS version	The version of the operating system on the user device. When using the **=** and **!=** operators, specify the full version of Windows.
UserGate client version	The version of the UserGate client software.
Connection security	Endpoint security component statuses: • Firewall; • Antimalware; • Automatic Update; • Bitlocker. **Important!** BitLocker is considered enabled if it is enabled on at least one of the disks.
Products	Conformance check of the software installed on the endpoint: • **Antimalware**. Conformance check of the antimalware software on the user device: ◦ **Enabled**: check the software status ◦ **Antivirus databases updated**: checking the relevance of the databases (yes, no, do not check) is performed only if the antivirus status check is explicitly enabled at the previous step; ◦ **Version**: the version of the software ◦ **Vendor**: the device vendor and product name. • **Firewall**. Conformance check of the firewall on the device. You need to specify the following parameters: ◦ **Installed**: check if the software is installed ◦ **Enabled**: check the software status (yes, no, or do not check) ◦ **Version**: the version of the software

Name	Description
	◦ **Vendor**: the device vendor and product name • **Backup**. Conformance check of the backup software: ◦ **Installed**: check if the software is installed ◦ **Version**: the version of the software ◦ **Vendor**: the device vendor and product name. • **Disk encryption**. Checking the disk encryption programs installed on the endpoint device: ◦ **Installed**: check if the software is installed ◦ **Version**: the version of the software ◦ **Vendor**: the device vendor and product name. • **DLP**. Conformance check of the data leak protection system on the device: ◦ **Installed**: check if the software is installed ◦ **Version**: the version of the software ◦ **Vendor**: the device vendor and product name. • **Update management.** Check for current updates. ◦ **Installed**: check if the software is installed ◦ **Version**: the version of the software ◦ **Vendor**: the device vendor and product name.
Processes	Check the processes running on the device.
Running services	Check the services running on the device.
Registry keys	Microsoft Windows registry key is a registry where OS settings and parameters are stored. The following types of registry values are supported: • **REG_SZ**: a null-terminated Unicode or ANSI string • **REG_BINARY**: binary data of any form • **REG_DWORD**: a 32-bit number The following registry keys can be checked: • **HKEY_LOCAL_MACHINE** • **HKEY_USERS** **Important!** The path specification begins with a backslash (****), such as \HKEY_LOCAL_MACHINE, followed by the full registry path with backslash (****) used as the separator. For a description of registry keys, see the Microsoft documentation.

Name	Description
Installed updates	Check that a specific update is installed on the device. The Microsoft Knowledge Base (KB) article number must be specified, e.g., KB5013624.

Collecting and Analyzing Data from UGC Devices

LogAn is a UserGate product within the UserGate SUMMA ecosystem. LogAn is installed on a separate server, making it possible to ensure high reliability and good scalability of the system. LogAn offers the ability to collect and analyze data from different devices as well as monitor security events and create reports. For more details on LogAn, refer to the corresponding documentation.

To be able to send data to a LogAn server, it needs to be assigned using an endpoints template. To send logs and telemetry data from UG Client to the UG LogAn server, a port from the range 22000-22711 is used that is automatically allocated in UGMC for this endpoint device; the data is transferred via UGMC. The configuration of a LogAn server for endpoint devices is done using endpoint templates. For more details, see the General Settings section.

Using the received data, LogAn analyzes past events and monitors user activity. Events received from UGC managed devices are recorded in the following logs:

- Endpoint events
- Endpoint rules
- Endpoint applications
- Endpoint hardware.

To view data from UGC devices, use the **Logs and reports → Logs → Endpoints** section of the web console.

The generation of these logs is discussed below in the Endpoint events, Endpoint rules, Endpoint Application Log, and Endpoint Hardware Log sections.

Endpoint Event Log

The endpoint event log (Endpoint events) shows events received from endpoint devices that are managed using the UserGate Client software.

> **Note**
> **To be able to send endpoint logs to LogAn in English, you must install the language pack *English (US)*; English should be available for selection as the interface language.**

To assist in finding the events you need, you can filter the records by various criteria, such as date range, severity, or event type, etc.

In addition, LogAn provides an advanced search mode where you can create complex search filters using a specialized query language.

After configuring the desired parameters, you can save the resulting filter by clicking **Save as**. The list of saved filters can be viewed in the **Favorite filters** tab.

The administrator can select the columns that will be logged. To do that, point the mouse cursor at the name of any column, click the arrow that will appear to the right of the column name, choose **Columns**, and select the desired parameters in the context menu.

The endpoint events log shows the following information:

Name	Description
Node	The ID of the endpoint device or node on which the sensor is running.
Time	Event time Displayed in the timezone set in LogAn.
Endpoint/sensor	The name of the computer.
Log level	The event type: • **Audit Success**: a security log event that occurs on successful access to the audited resources • **Audit Failure**: a security log event that occurs on an unsuccessful attempt to access the audited resources • **Error**: indicates significant problems that can cause functionality or data loss • **Information**: informational events that usually do not require administrator attention • **Warning**: events that indicate problems that do not need urgent fixing but can cause errors in the future.
Data	Detailed information about the event.
Log event source	The source of the logged events.

Name	Description
Log category	The log category that is required to classify the events. The data is taken from Windows EventLog. Each source can define its own category IDs. Applicable to endpoint event log records.
Incident category	The category of the incident.
Computer name	The full name of the computer.
Username.	The name of the user whose account was used to log in to the endpoint device.
Log event code	The code corresponding to a specific event.
Log event ID	The ID of the log event that determines the primary ID of the event.
Log event type	The type of the log event corresponding to a specific log level: • 1: error log level • 2: warning log level • 3: information log level • 4: audit success log level • 5: audit failure log level
Insertion string	Contains the EventData block of the Windows event.
Log file	The type of the log file where the event is recorded: • **Application** (application log file): for application and service events. • **Security** (security log file): for audit system events. • **System** (system log file): for device driver events. • **CustomLog**: contains events logged by applications that create a custom log. The use of a custom log allows an application to control the log size or attach access control lists for security purposes without affecting other applications.

Click **Show** to view the selected endpoint event log record details.

Click **Add to incident** to add the log record to the incident information.

By clicking **Export as CSV**, the administrator can save the filtered log data in a .csv file for subsequent analysis.

Endpoint Rule Log

The endpoint rule log (Endpoint rules) shows firewall trigger events for endpoint devices in which **Logging** is enabled in the settings. The configuration of firewall rules is discussed in the Network Policies section.

To assist in finding the events you need, you can filter the log records for firewall rule triggers by various criteria such as the date range, rule name, etc.

In addition, UserGate LogAn provides an advanced search mode where you can create complex search filters using a specialized query language.

After configuring the desired parameters, you can save the resulting filter by clicking **Save as**. The list of saved filters can be viewed in the **Favorite filters** tab.

The administrator can select the columns that will be logged. To do that, point the mouse cursor at the name of any column, click the arrow that will appear to the right of the column name, choose **Columns**, and select the desired parameters in the context menu.

The endpoint rule log shows the following information:

Name	Description
Node	The endpoint ID.
Time	The time when the rule was triggered. Displayed in the timezone set in LogAn.
Endpoint	The name of the computer.
Action	The action to be taken when the rule is matched: • Allow • NAT • Deny.
Rule	The name of the firewall rule.
Application	The application used to access the resource.
Domain	The domain name to which the connection was established.
URL categories	The website categories that apply to the destination address. The categories will be displayed only if there are rules with the URL categories match condition.

Name	Description
Content type	Displays the content type.
Network protocol	The transport protocol used to connect to the resource.
Source IP	The source IP address for the traffic.
Source port	The port number used for connection.
IP dest	The destination IP address for the traffic.
Destination port.	The destination port number used by the transport protocol.

Click **Show** to view the details for the selected endpoint rule log record.

Click **Add to incident** to add the log record to the incident information.

By clicking **Export as CSV**, the administrator can save the filtered log data in a .csv file for subsequent analysis.

Endpoint Application Log

The endpoint application log (Endpoint applications) shows the applications that were run on the endpoint devices.

To assist in finding the events of interest, the records can be filtered by various criteria.

In addition, UserGate LogAn provides an advanced search mode where you can create complex search filters using a specialized query language.

You can save the configured filter by clicking **Save as**. The saved filter will be available in the **Favorite filters** tab.

The administrator can select the columns that will be logged. To do that, point the mouse cursor at the name of any column, click the arrow that will appear to the right of the column name, choose **Columns**, and select the desired parameters in the context menu.

The endpoint application log shows the following information:

Name	Description
Node	The endpoint ID.
Time	

Name	Description
	The time when the application was started on the endpoint device. Displayed in the timezone set in LogAn.
Endpoint	The name of the computer.
Action	Application start or stop.
Hash	The application hash.
Application	The name of the application that was started or stopped.
Version	The application version.
Subject	The certificate owner.
Issuer	The issuer of the application's certificate.
Process ID	The process ID (PID) of the application.
User	The user who started the application.
Command line	The command used to start the application.

Click **Show** to open a window with the details for the application log record.

Click **Add to incident** to add the log record to the incident information.

By clicking **Export as CSV**, the administrator can save the filtered log data in a .csv file for subsequent analysis.

Endpoint Hardware Log

The endpoint hardware log (Endpoint hardware) shows information about devices connected to UGC managed devices.

To assist in finding the events of interest, the records can be filtered by various criteria.

In addition, LogAn provides an advanced search mode where you can create complex search filters using a specialized query language.

You can save the configured filter by clicking **Save as**. The saved filter will be available in the **Favorite filters** tab.

The administrator can select the columns that will be logged. To do that, point the mouse cursor at the name of any column, click the arrow that will appear to the right of the column name, choose **Columns**, and select the desired parameters in the context menu.

The endpoint hardware log shows the following information:

Name	Description
Node	The endpoint ID.
Time	The date and time when the event was logged.
Endpoint	The name of the endpoint device.
Action	Adding or removing the device.
Device	The name of the device that was added or removed.
Device ID	The ID of the added or removed device.
Service	The drivers used for working with the device.

Click **Show** to open a window with the details for the endpoint hardware log record.

Click **Add to incident** to add the log record to the incident information.

By clicking **Export as CSV**, the administrator can save the filtered log data in a .csv file for subsequent analysis.

COMMAND LINE INTERFACE (CLI)

GENERAL PROVISIONS

General Provisions (Description)

In UserGate MC (UGMC), you can perform device configuration with the help of the command-line interface, or CLI.

CLI can be useful for troubleshooting network problems or when access to the web console is lost — for example, due to an incorrectly set interface IP address or erroneous zone access control settings that block connections to the web interface.

You can connect to the CLI using the standard VGA/keyboard ports (if physically present on the UGMC equipment), via the serial port, or via SSH over the network.

> **Attention!**
> **If the device has not undergone initial setup, use *Admin* as the login and *usergate* as the password for accessing the CLI.**

To connect to the CLI using a monitor and keyboard, follow these steps:

Name	Description
Step 1. Connect a monitor and keyboard to the device	Connect a monitor to a VGA (HDMI) port and a keyboard to a USB port.
Step 2. Log in to the CLI.	Log in to the CLI using the login and password for a user with UGMC root administrator permissions (the default is Admin/system).

To connect to the CLI using the serial port, follow these steps:

Name	Description
Step 1. Connect to the device	Use a special serial cable or a USB-Serial adapter to connect your computer to the device.
Step 2. Launch a terminal.	Launch a terminal that supports serial port connection, such as Putty for Windows or minicom for Linux. Establish a serial port connection using 115200 8n1 as the connection parameters.
Step 3. Log in to the CLI.	Log in to the CLI using the login and password for a user with UGMC root administrator permissions (the default is Admin/system).

To connect to the CLI using the SSH protocol, follow these steps:

Name	Description
Step 1. Allow CLI (SSH) access for the selected zone.	Allow SSH access for the CLI protocol in the settings for the zone to which you want to connect for CLI management. The TCP port 2200 will be opened.

Name	Description
Step 2. Launch an SSH terminal.	Launch an SSH terminal on your computer, such as SSH for Linux or Putty for Windows. Specify UGMC address as the IP address, 2200 as the connection port, and the login of a user with root administrator permissions as the CLI login name (the default is Admin/system). For Linux, the connection command should look like this: *ssh Admin/system@IPUserGateMC -p 2200*
Step 3. Log in to the CLI.	Log in to the CLI using the password for the user specified in the previous step.

Upon successful authorization for CLI access, a command prompt will be displayed (diagnostics mode). To view the current available options or use autocomplete, press **Tab**. Available values:

- **configure**: switch to the configuration mode
- **date**: view the current device date and time
- **dig**: check the DNS record for a domain.
- **exit**: exit the command line
- **netcheck**: check the availability of a 3rd party HTTP/HTTPS server
- **ping**: ping a specific host
- **reboot**: reboot the device
- **shutdown**: shutting down the device
- **traceroute**: trace the connection route to a specific host

These commands are available in the configuration mode. For more details, see the Execute Commands sections.

To abort the current command, press **Ctrl+C**; to view command history, use the ↑ and ↓ keys.

All CLI commands have the following structure:

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

where:

<action> is the action to be performed;

<level> is the configuration level corresponding to the NGFW web interface section;

<filter> is the identifier of the object being accessed; and

<configuration_info> is the set of parameter values to be applied to the <filter> object.

CLI supports multi-line command entry. To move to a new line, add "\" at the end of the current one. Starting from the second line, entering "\" is not required; to finish the entry, enter one empty line.

COMMANDS AVAILABLE PRIOR TO INITIAL NODE SETUP

Commands Available Prior to Initial Node Setup (Description)

If the device has not undergone initial configuration, diagnostics and monitoring commands are fully available in the CLI, but only network configuration commands are available in the configuration mode (zone, interface, gateway, and virtual router configuration as well as enabling/disabling remote access to the radmin-emergency server).

INITIAL SETUP

Initial Setup (Description)

There are several ways to perform the device initial setup using the CLI.

Install UserGate as the master node.

To set the device as the master node, use this command:

```
Admin/system@nodename# execute install master
```

Specify the following parameters:

Parameter	Description
login	Set admin name.
password	Set a password for the administrator account. You can also set the password on pressing **Enter** after typing in the administrator login; the password must be entered twice.

Install UserGate as a slave node.

To set the node as a slave node, use this command:

```
Admin/system@nodename# execute install slave
```

Specify the following parameters:

Parameter	Description
interface	The interface for connecting to the cluster.
slave-ip	The IP address that will be assigned to the interface used for connecting to the cluster.
gateway-address	Gateway IP address. A gateway is required if the nodes are in different subnets.
master-ip	The master node IP address.
master-secret	The master node secret used to connect the node to the cluster.
login	System administrator login.
password	The password for the administrator account.

After the initial setup, the full management functionality will be available from the CLI.

CONFIGURATION MODE

Configuration Mode (Description)

To enter the configuration mode, use the following command:

```
Admin/system@nodename> configure
```

Once you enter the configuration mode, the command line will be as follows:

```
Admin/system@nodename#
```

To view a hint about the current possible values or to autocomplete commands, press the **Tab** key. The following symbols can be used in the hint:

*****— a required field in the create command and some others

+— an optional/variable field

> — a nested field; after entering it the previous list of fields becomes unavailable, a new list of fields appears that can be entered

Example:

```
Admin/system@nodename# set network zone Trusted
* name                    Name
+ antispoof-enable        Enable/Disable IP spoofing protection
+ antispoof-negate        Enable/Disable Negate ip-spoof addresses
+ description             Description
+ enabled-services        Services list to enable
+ geoip                   IP spoofing protection by geo IP code
+ ip-list                 IP spoofing protection by IP list
> dos-protection-icmp     Confugure DoS protection per IP for ICMP
```

```
packets
> dos-protection-syn      Confugure DoS protection per IP for SYN
packets
> dos-protection-udp      Confugure DoS protection per IP for UDP
packets
> service-addresses       Access control service addresses
```

General Command Structure in Configuration Mode

CLI commands have the following structure:

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

where:

<action> is the action to be performed;

<level> is the configuration level corresponding to the UGMC web interface section;

<filter> is the identifier of the object being accessed; and

<configuration_info> is the set of parameter values to be applied to the <filter> object.

Name	Description
<action>	The following actions are available in the configuration mode: • **execute**: execute commands not related to UserGate configuration (ping, date, traceroute, etc.). The command is available regardless of the configuration level (<level>). • **set**: edit all objects and enable various parameters, e.g. radmin. • **end**: go one level up. • **show**: display the current values. You can use this at any configuration level. Displays everything below the current level. • **edit**: go to a specific configuration level. The configuration level is displayed under the command line. • **top**: go back to the topmost configuration level. • **exit**: exit the configuration mode. • **export**: export the configuration.

Name	Description
	• **import**: import the configuration. • **create**: create new objects. • **delete**: delete an object or a parameter from the parameter list. For example, to view information about all interfaces, run the following command: `Admin/system@nodename# show network interface` To go to the **network interface level, use the following command.** The current level will be displayed under the command line: `Admin/system@nodename# edit network interface` `Admin/system@nodename#` `Level: network interface` After you go to the **network interface** level, use the show command to show all interfaces without specifying a level: `Admin/system@nodename# show` `adapter:` `port0` `interface-name : port0` `node-name : node1` `zone : Management` `enabled : on` `ip-addresses : 192.168.56.3/24` `iface-mode : dhcp` `...` `...` `...` `Level: network interface` To return from the **network interface** level back to the general level of the configuration mode, use the **end** command:

Name	Description
	`` Admin/system@nodename# end Level: network interface Admin/system@nodename# end Level: network Admin/system@nodename# ```
<level>	Levels in the command line follow the UGMC system console web interface: • **network**: corresponds to the **Network** section of the web interface. • **settings**: corresponds to the **UserGate** section of the web interface. • **users**: corresponds to the **Users and devices** section of the web interface. • **libraries**: corresponds to the **Libraries** section of the web interface. • **monitoring**: corresponds to the **Diagnostics and monitoring** section of the web interface. • **realms**: corresponds to the **Managed Realms** section of the web interface.
<filter>	ID of the object which is being accessed. Objects are identified by their name. If there are objects with identical names or it is more convenient to identify objects by another parameter, specify <configuration_info> in parentheses (this is discussed later in the section). This will find an object matching all the fields specified in parentheses. For example, you need to display information about the port0 interface on another cluster node. The command ``` Admin/system@nodename# show network interface adapter port0 ``` will display information about the interface port0 on the current UGMC node. To preview information about the port0 interface on another node (named another_node for instance), you need to explicitly specify the node name in parentheses: ``` Admin/system@nodename# show network interface adapter (node-name another_nodename interface port0) ```

Name	Description
	Important! Parentheses should be separated by spaces on both sides.
<configuration_info>	Set of parameter-argument pairs. where the parameter is the name of the field for which you need to set the argument. Arguments can be single-valued or multi-valued. **A single-valued argument** is the value of the parameter. If the string contains spaces, use quotation marks. For example, you need to create an authentication profile named New profile: `Admin/system@nodename# create users auth-profile name "New profile"` **Multi-valued arguments** are used to set multiple values of a parameter; include them in square brackets and separate by spaces. For example, you need to create a list of IP addresses in the element library and add two IP addresses 10.10.0.1 and 10.10.0.2 to it: `Admin/system@nodename# create libraries ip-list name testlist ips [ 10.10.0.1 10.10.0.2 ]` **Important!** Square brackets should be separated by spaces on both sides.

Execute Commands

These commands have the following structure:

```
Admin/system@nodename# execute <command-name>
```

Available commands:

Parameter	Description
traceroute	Traceroute the connection to a specified host. Available parameters: • **hostname <ip-or-domain>**: IP address or domain name for which tracing is performed.

Parameter	Description
	• **interface <iface-name>**: the interface from which packets will be sent • **not-map-ip**: do not search the hostname for the IP address when displaying • **use-icmp-echo**: use ICMP echo. • **port**: specify a port instead of the default port (1-65535). • **min-interval**: minimum interval between packets. `Admin/system@nodename# execute traceroute hostname <hostname>`
termination	Close the administrator sessions. For more details, see Managing Administrator Sessions.
ping	Ping a specific host. Available parameters: • **hostname**: the IP address or domain name of the server. • **count**: the number of echo requests to send. If not specified, the system will send the packets until the user terminates the connection (to terminate sending, press Ctrl+C). • **numeric**: do not resolve names. • **timestamp**: display timestamps. • **interval**: the time between sent packets (in seconds). • **ttl**: the packet's time to live. • **interface**: the address of the selected interface will be used as the source address for running ping. • **mtu**: the MTU size of the sent packets. • **virtual-router**: virtual router name. `Admin/system@nodename# execute ping hostname <hostname> count <number>`
reboot	Rebooting the device.
date	View the current date and time on the server.
shutdown	Shutting down the device.
netcheck	

Parameter	Description
	Check the availability of a third-party HTTP/HTTPS server. You can use the following parameters: • **address**: the host's domain name for checking availability over TCP or URL for HTTP • **dns-ip**: the DNS server's IP address • **dns-tcp**: use TCP instead of UDP for DNS request • **check-cert**: check the SSL certificate • **type**: check availability over: ◦ **http** ◦ **tcp** (if no port is specified, port 80 is used by default). • **data**: request the site content. Only headers are requested by default. • **timeout**: the maximum time to wait for a reply from the web server. • **user-agent** : parameter for specifying the browser type (useragent). Some websites may only allow access from certain browsers. The parameter value is specified in double quotes. `Admin/system@nodename# execute netcheck type tcp address <host-domain-name> data on` `Admin/system@nodename# execute netcheck address <host-domain-name>`
dig	Check the domain DNS record. • **hostname**: the host's domain name or IP address for reverse lookup • **reverse-lookup**: get the host from the IP address • **dns**: specify the IP address of the DNS server • **tcp**: use TCP instead of UDP. `Admin/system@nodename# execute dig hostname <host-domain-name>` `Admin/system@nodename# execute dig hostname <IP-address> reverse-lookup on`

Parameter	Description
update	Available starting from software version 7.3.0. Update: • **software-updates**: software update • **libraries-updates<**: library update. You can update all libraries at once or individual libraries.

Some commands presented above are also available in diagnostic and monitoring mode. To execute them, use the following command:

```
Admin/system@nodename> <command-name>
```

DEVICE SETUP

Device Setup (Description)

UserGate General Settings

You configure the device general settings at the **settings general** level. This is the command structure to configure one of the sections (<settings-module>):

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

You can configure the following sections:

Parameter	Description
admin-console	Admin console settings (**settings general admin-console** level): • **timezone**: time zone for your location. Used in rule schedules and for the correct display of time and date in reports, logs, etc. • **language**: interface language: ◦ **ru**: Russian ◦ **en**: English

Parameter	Description
	• **api-session-lifetime**: admin session timeout in seconds.
server-time	Configure the exact time settings (**settings general server-time** level): • **ntp-enabled**: enable/disable the use of NTP servers: ◦ **on** ◦ **off** • **primary-ntp-server**: specify the primary ntp server. • **second-ntp-server**: specify a backup ntp server. • **time**: set server time (format: yyyy-mm-ddThh:mm:ss, e.g. 2022-02-15T12:00:00; UTC time zone).
change-tracker	Configure change tracker (**settings general change-tracker** level): • **enabled**: enable/disable change tracker. ◦ **on** ◦ **off** • **event-tracker-types**: change types are set by an administrator. To delete a change type, use the following command: `Admin/system@nodename# delete settings general change-tracker event-tracker-types [ type1 ... ] ]`
updates-schedule	Configure the schedule to download software and library updates (**settings general updates-schedule** level). To configure a schedule to update UserGate software, use the following command: `Admin/system@nodename# set settings general updates-schedule software schedule <schedule/disabled>` You can set up a single schedule to download library updates: `Admin/system@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled>`

Parameter	Description
	or an individual schedule for each item: `Admin/system@nodename# set settings general updates-schedule libraries [ lib-module ... ] schedule <schedule/disabled>` The time is set in the Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours". To view the update schedule, use the following command: `Admin/system@nodename# show settings general updates-schedule`

Configuring device management

Configuring radmin emergency

To activate the remote assistant when a problem with the node's core software arises, the administrator can log in to the CLI using the root administrator account created when UserGate was initialized. Usually, this is the Admin account; however, it is not always so. To log in, specify the name as Admin/system@emergency and use the root administrator password as the password. To enable/disable remote access to the server for technical support in such cases, use the following command:

```
Admin/system@emergency# set radmin-emergency enabled <on | off>
```

Parameter	Description
interface	The interface name.
ip-addr	Interface IP address and mask.
gateway-address	Gateway IP address.

Configuring server operations

To set an update channel, use the following command:

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

To view any updates and the selected update channel, use the following command:

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

To configure the device license activation and software updates via an external proxy, use the following command:

```
Admin@UGOS# set settings device-mgmt licensing-upstream-proxy
<parameters>
```

The additional parameters are as follows:

Parameter	Description
enabled	Enabling/disabling license activation and software update mode via an external proxy server: • **on**: enabled • **off**: disabled
ip	The external proxy's IP address.
port	The external proxy's port.
auth	Authentication with the external proxy: • **on**: enabled

Parameter	Description
	• **off**: disabled
name	The external proxy login name.
password	The external proxy password.

To view the settings for UserGate device license activation and software updates via an external proxy, use the following command:

```
Admin@UGOS# show settings device-mgmt licensing-upstream-proxy
```

System backup management

A device backup is created at the **settings device-mgmt** level. To create a backup rule and upload files to external FTP/SSH servers, use the following command:

```
Admin/system@nodename# create settings device-mgmt settings-backup
<parameters>
```

The available parameters include:

Parameter	Description
enabled	Enable/disable the device backup rule.
name	The name of the backup rule.
description	A description of the backup rule.
type	Select a remote server to export files: • **ssh** • **ftp**
address	Remote server IP address.
port	Port:
login	Remote server login name.
password	Password for the login name.

Parameter	Description
path	Directory path to upload the files to.
schedule	The backup file export schedule. The time is set in the Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

To edit an existing device backup rule, use the following command:

```
Admin/system@nodename# set settings device-mgmt settings-backup <rule-name>
```

You can use the same set of parameters as when creating rules.

To delete a backup rule:

```
Admin/system@nodename# delete settings device-mgmt settings-backup <rule-name>
```

To display a backup rule:

```
Admin/system@nodename# show settings device-mgmt settings-backup <rule-name>
```

In the rule edit, delete, or display commands, <filter> can include the parameters specified in an existing rule in addition to the rule name (this can be helpful if there are multiple rules with the same name). Parameters used to identify an export rule are similar to those of the **set** command.

Settings Export

You create and configure export settings rules at the **settings device-mgmt settings-export** level.

To create an export settings rule, use the following command:

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

Available parameters:

Parameter	Description
enabled	Enable/disable an export settings rule for the UserGate server.
name	Export rule name.
description	Export rule description.
type	Select a remote server to export settings: • **ssh** • **ftp**
address	Remote server IP address.
port	Port:
login	Remote server login name.
password	Password for the login name.
path	Directory path to upload the settings to.
schedule	Schedule for settings export. The time is set in the Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23".

Parameter	Description
	• An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

To update an existing rule to export the device settings, use the following command:

```
Admin/system@nodename# set settings device-mgmt settings-export <rule-name>
```

You can use the same set of parameters as when creating rules.

To delete a rule to export settings, use the following command:

```
Admin/system@nodename# delete settings device-mgmt settings-export <rule-name>
```

To display a rule to export settings, use the following command:

```
Admin/system@nodename# show settings device-mgmt settings-export <rule-name>
```

For update, delete or display rule commands, you can set <filter> not only to the rule name, but also to the parameters specified in an existing rule (this may be helpful if there is more than one rule with the same name). Parameters used to identify an export rule are similar to those of the **set** command.

Cluster Settings

Configuration cluster settings

This section is located at the **settings device-mgmt configuration-cluster** level.

To update an existing cluster mode, use the following command:

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

Available parameters:

Parameter	Description
name	Change the cluster node name.
description	Update the cluster node description.
ip	Set the IP address of the interface included in the zone allocated to the cluster.

To delete and display cluster node settings, use the following commands:

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

To generate a secret code for adding a new node to the configuration cluster, use the following command:

```
Admin/system@nodename# execute configurate-cluster generate-secret-key
```

Settings for high availability clusters

You apply settings to HA clusters at the **settings device-mgmt ha-cluster** level.

To create an HA cluster, use the following command:

```
Admin/system@nodename# create settings device-mgmt ha-clusters
```

Provide the following parameters:

Parameter	Description
enabled	Enable/disable the HA cluster: • **on** • **off**
name	HA cluster name.
description	HA cluster description.
mode	Select cluster operation mode: • **active-passive**: Active-Passive mode (one server operates as the master node that processes traffic while the remaining servers act as backup). • **active-active**: Active-Active mode (one server operates as the master node that distributes traffic to all other nodes in the cluster).
session-sync	Configure user session synchronization in the cluster: • **off**: disable user session synchronization • **on**: enable user session synchronization • **ha-cluster-id:** ◦ <num>: HA cluster multicast ID (can take values of 0 to 8). User session synchronization (except for sessions that use a proxy server, such as HTTP/S traffic) is enabled automatically.
virtual-router-id	Virtual Router ID (VRID).
nodes	Select configuration cluster nodes to combine them into an HA cluster.
virtual-ips	Set the virtual IP address for the cluster and select an interface for each node (the VRRP service should be enabled in the selected interface zone; for more details on how to configure zones using the CLI, see the Zones section). To add a virtual IP address to the cluster, use the following command: `Admin/system@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info>`

Parameter	Description
	Available parameters for <virtual-ips-filter>: • **new**: create a virtual IP address for the specific cluster. • <ip>: change data for the selected virtual address. Available parameters for <virtual-ip-info>: • **ip**: set an IP address for the HA cluster (format: IP/mask). • **ha-interfaces**: set interfaces for the cluster nodes (format: node-name/interface).
session-sync-all	Enable/disable synchronizing all user sessions, including UDP/ICMP sessions. If this is disabled and **session-sync** enabled, only TCP sessions will be synchronized.
excluded-sync-ips	Specify the IP for which synchronization is disabled for all user sessions.

Example cluster creation command:

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

To edit the cluster settings, use the following command:

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

The following parameters are available:

Parameter	Description
enabled	Enable/disable the HA cluster: • **on** • **off**
name	HA cluster name.
description	HA cluster description.

Parameter	Description
mode	Select cluster operation mode: • **active-passive**: Active-Passive mode (one server operates as the master node that processes traffic while the remaining servers act as backup). • **active-active**: Active-Active mode (one server operates as the master node that distributes traffic to all other nodes in the cluster).
master-node	Assign the master node in the HA cluster.
session-sync	Configure session synchronization in the cluster: • **off**: disable user session synchronization • **on**: enable user session synchronization • **ha-cluster-id:** ◦ <num>: HA cluster multicast ID (can take values of 0 to 8). User session synchronization (except for sessions that use a proxy server, such as HTTP/S traffic) is enabled automatically.
virtual-router-id	Virtual Router ID (VRID).
nodes	Select configuration cluster nodes to combine them into an HA cluster.
virtual-ips	Set the virtual IP address for the cluster and select an interface for each node (the VRRP service should be enabled in the selected interface zone; for more details on how to configure zones using the CLI, see the Zones section). To add a virtual IP address to the cluster, use the following command: `Admin/system@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info>` Available parameters for <virtual-ips-filter>: • **new**: create a virtual IP address for the specific cluster. • <ip>: change data for the selected virtual address. Available parameters for <virtual-ip-info>: • **ip**: set an IP address for the HA cluster (format: IP/mask).

Parameter	Description
	• **ha-interfaces**: set interfaces for the cluster nodes (format: node-name/interface).
session-sync-all	Enable/disable synchronizing all user sessions, including UDP/ICMP sessions. If this is disabled and **session-sync** enabled, only TCP sessions will be synchronized.
excluded-sync-ips	Specify the IP for which synchronization is disabled for all user sessions.

Example commands for editing the cluster settings:

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

To delete a cluster, use the following command:

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

You can also delete individual parameters:

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

To display information about all HA clusters, use the following command:

```
Admin/system@nodename# show settings device-mgmt ha-cluster
```

To display information about a specific HA cluster, use the following command:

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

Configuring Device Console Access Control

This section is configured at the **settings administrators** level. This section describes how to configure account security settings, administrators, and their profiles.

General access settings

In this section, you can configure additional security options for administrator accounts. This is configured at the **settings administrators general** level.

To change the parameters, use the following command:

```
Admin/system@nodename# set settings administrators general
```

The following parameters are available:

Parameter	Description
password	Change the current administrator password.
unblock	Unblock an administrator.
strong-password	Use a strong password: • **on** • **off**
num-auth-attempts	Maximum number of incorrect authentication attempts.
block-time	Time to block an account if the maximum number of authentication attempts is reached by the administrator (in seconds, max value is 3600 seconds).
min-length	Minimum password length (max value is 100 characters).
min-uppercase	Minimum number of uppercase characters (max value is 100 characters).
min-lowercase	Minimum number of lowercase characters (max value is 100 characters).
min-digits	Minimum number of digits (max value is 100 characters).

Parameter	Description
spec-characters	Minimum number of special characters (max value is 100 characters).
char-repetition	Maximum single character repetition block length (max value is 100 characters).

Examples of editing account parameters:

```
Admin/system@nodename# set settings administrators general block-time
400
```

To view the current security settings for administrator accounts, use the following command:

```
Admin/system@nodename# show settings administrators general

strong-password      : off
block-time           : 400
min-length           : 7
min-uppercase        : 1
min-lowercase        : 1
min-digits           : 1
spec-characters      : 1
char-repetition      : 2
num-auth-attempts    : 10
```

Configuring administrator accounts

You configure administrator accounts at the **settings administrators administrators** level.

To create an administrator account, use the following command:

```
Admin/system@nodename# create settings administrators administrators
```

Specify the administrator account type (local, LDAP user, LDAP group, with auth profile) and the respective parameters:

Parameter	Description
local	Add a local administrator: • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: administrator login name. • **display-name**: the administrator's display name. • **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. • **password**: administrator password.
ldap-user	Add a user from the existing domain (you need to have the LDAP connector configured correctly; for more details, see the Configuring LDAP Connectors section): • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: the administrator's login name in the **domain\user** format. When providing this parameter, use the following command structure: • **display-name**: the administrator's display name. • **connector**: the name of a previously configured LDAP connector. • **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. `Admin/system@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	Add a user group from the existing domain (you need to have the LDAP connector configured correctly; for more details, see the Configuring LDAP Connectors section): • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off**

Parameter	Description
	• **login**: administrator login name • **display-name**: the administrator's display name. • **connector**: the name of the used LDAP connector. • **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. `Admin/system@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	Add an administrator with an auth profile (you need to have the auth servers configured correctly; for more details, see the Configuring Authentication Servers section): • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: administrator login name. • **display-name**: the administrator's display name. • **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. • **auth-profile**: select an auth profile from those created earlier; for more details about auth profiles, see the section Configuring Authentication Profiles.

To edit the profile parameters, use the following command:

```
Admin/system@nodename# set settings administrators administrators
<admin-type> <admin-login>
```

The command's parameters are similar to those used for administrator profile creation.

To display information about all administrator accounts, use the following command:

```
Admin/system@nodename# show settings administrators administrators
```

To display information about an individual administrator account, use the following command:

```
Admin/system@nodename# show settings administrators administrators
<admin-type> <admin-login>
```

Example of the command execution:

```
Admin/system@nodename# show settings administrators administrators
ldap-user testd.local\user1

login            : testd.local\user1
enabled          : on
type             : ldap_user
locked           : off
admin-profile    : test profile 1
```

To delete an account, use the following command:

```
Admin/system@nodename# delete settings administrators administrators
<admin-type> <admin-login>
```

Example of the command:

```
Admin/system@nodename# delete settings administrators administrators
ldap-user testd.local\user1
```

Configuring Permissions for Administrator Profiles

The permissions of administrator profiles are configured at the **settings administrators profiles** level.

To create an administrator profile, use the following command:

```
Admin/system@nodename# create settings administrators profiles
```

Provide the following parameters:

Parameter	Description
name	Administrator profile name.
description	Administrator profile description.
admin-type	Administrator role: • **device**: UGMC device administrator • **realm**: administrator of the managed realm
permissions	Permissions: • **no-access**: no access • **read**: read-only • **write**: read and write

To edit the profile, use the following command:

```
Admin/system@nodename# set settings administrators profiles <profile-
name> <parameter>
```

The command's parameters are similar to those used for administrator profile creation.

To view information about all administrator profiles, use the following command:

```
Admin/system@nodename# show settings administrators profiles
```

To display information about a specific profile, use the following command:

```
Admin/system@nodename# show settings administrators profiles <profile-
name>
```

To delete an administrator profile, use the following command:

```
Admin/system@nodename# delete settings administrators profiles
<profile-name>
```

Managing Administrator Sessions

The following commands allow you to view the active sessions of administrators who have been authorized in the web console or CLI and close the sessions (this is done at the **settings administrators admin-sessions** level).

To view administrator sessions for the current UserGate node, use the following command. You can view an individual administrator's session; to do so, browse the IP address list and select the address used to authenticate the administrator.

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

To display sessions, you can use a filter:

- **ip**: IP address from which the administrator was authorized.
- **source**: where authorization was made: CLI (**cli**), web console (**web**) or SSH connection (**ssh**).
- **admin-login**: administrator name.
- **node**: UserGate cluster node.

```
Admin/system@nodename# show settings administrators admin-sessions
( node <node-name> ip <session-ip> source <cli | web | ssh> admin-login
<administrator-login> )
```

To close an administrator session, use the following command. Select the IP address from which the administrator was authorized, from the list.

```
Admin/system@nodename# execute termination admin-sessions <IP-address/
connection type>
```

Example of the command execution:

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

admin-login           : Admin
source                : ssh
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : utmcore@dineanoulwer

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

Admin/system@nodename# execute termination admin-sessions 10.0.2.2/web

Admin/system@nodename# show settings administrators admin-sessions

admin-login           : Admin
source                : ssh
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : utmcore@dineanoulwer
```

When closing administrator sessions, you can use a filter (<filter>). Enabled filtering options are the same as those for the **show** command.

```
Admin/system@nodename# execute termination admin-sessions ( node <node-
name> ip <session-ip> source <cli | web | ssh> admin-login
<administrator-login> )
```

Configuring Certificates

The **Certificates** section is located at the **settings certificates** level.

To import certificates, use the following command:

```
Admin/system@nodename# import settings certificates
```

Parameters:

Parameter	Description
name	Certificate name that will be listed.
description	Certificate description.
certificate-data	Certificate in PEM format.
certificate-chain	Certificate's chain in PEM format.
private-key	Private key in PEM format.
passphrase	Passphrase for the private key or PKCS12 container (optional value).

To export certificates, the entire certificate's chain, use the following command:

```
Admin/system@nodename# export settings certificates <certificate-name>
Admin/system@nodename# export settings certificates <certificate-name>
with-chain on
```

To create a certificate and CSR, use the following command:

```
Admin/system@nodename# create settings certificates type <certificate |
csr>
```

Provide the following parameters:

Parameter	Description
name	Certificate name.
description	Certificate description.
country	Country where the certificate is being issued.

Parameter	Description
state	Region/state where the certificate is being issued.
locality	Locality name where the certificate is being issued.
organization	Organization name for which the certificate is being issued.
common-name	Certificate name. To ensure compatibility with the majority of browsers, we recommend using only Latin characters.
email	Company email.

To manage a certificate, use the following command:

```
Admin/system@nodename# set settings certificates <certificate-name>
```

Available parameters:

Parameter	Description
name	Certificate name.
description	Certificate description.
role	Certificate type: • **web-cert-chain**: web console certificate's chain. • **web-ssl**: certificate used to create a secure HTTPS administrator connection to the UserGate web console. • **none**.
certificate-chain	Certificate's chain in PEM format.

To delete a certificate, use the following command:

```
Admin/system@nodename# delete settings certificates <certificate-name>
```

To view information about all or individual certificates, use the following command:

```
Admin/system@nodename# show settings certificates
Admin/system@nodename# show settings certificates <certificate-name>
```

Configuring Authentication Servers

The Auth servers section allows you to configure an LDAP connector, RADIUS, TACACS+ servers. You configure auth servers at the **users auth-server** level. We will consider it in the respective sections below.

Configuring LDAP connectors

An LDAP connector is configured at the **users auth-servers ldap** level.

To create an LDAP connector, use the following command:

```
Admin/system@nodename# create users auth-server ldap <parameter>
```

Provide the following parameters:

Parameter	Description
name	LDAP connector name.
enabled	Enable/disable the auth server.
description	LDAP connector description.
ssl	Values: • **on**: use an SSL connection to connect to the LDAP server • **off**: connect to the LDAP server without using an SSL connection.
address	Controller IP address or the LDAP domain name.
bind-dn	The username used to connect to the server. Format: DOMAIN\username or username@domain. The user must be a user in the domain.
password	The user's password for connecting to the domain.
domains	List of domains served by the domain controller.
search-roots	The list of LDAP server paths relative to which the system will search for users and groups. Specify the full name, e.g., ou=Office,dc=example,dc=com. If the search paths are not

Parameter	Description
	specified, the system will search over the entire directory, starting from the root.

To edit information about an existing LDAP connector, use the following command:

```
Admin/system@nodename# set users auth-server ldap <ldap-server-name>
<parameter>
```

The parameters available to update are the same as those for creating an LDAP connector.

To display information on an LDAP connector, use the following command:

```
Admin/system@nodename# show users auth-server ldap <ldap-server-name>
```

Example commands to create and edit an LDAP connector:

```
Admin/system@nodename# create users auth-server ldap name "New LDAP
connector" ssl on address 10.10.0.10 bind-dn ug@testd.local password
12345 domains [ testd.local ] search-roots [ dc=testd,dc=local ]
enabled on
Admin/system@nodename# show users auth-server ldap "New LDAP connector"

name             : New LDAP connector
enabled          : on
ssl              : on
address          : 10.10.0.10
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
Admin/system@nodename# set users auth-server ldap "New LDAP connector"
description "New LDAP connector description"
Admin/system@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
```

To delete an LDAP connector, use the following command:

```
Admin/system@nodename# delete users auth-server ldap <ldap-server-name>
<parameter>
```

You can also delete individual parameters of an LDAP connector. You can delete the following parameters:

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

Configuring RADIUS Servers

A RADIUS server is configured at the **users auth-servers radius** level.

To create a RADIUS auth server, use the following command:

```
Admin/system@nodename# create users auth-server radius <parameter>
```

Provide the following parameters:

Parameter	Description
name	The RADIUS server name.
enabled	Enable/disable the auth server.
description	Auth server description.
secret	Pre-shared key used by the RADIUS protocol for authentication.
addresses	

Parameter	Description
	IP address and the UDP port on which the RADIUS server listens to requests (default port: 1812). Format: <ip:port>.

To update information about a RADIUS server, use the following command:

```
Admin/system@nodename# set users auth-server radius <radius-server-
name> <parameter>
```

The parameters you can update are the same as those used to create an auth server.

To display information about a RADIUS server, use the following command:

```
Admin/system@nodename# show users auth-server radius <radius-server-
name>
```

Example commands to create and edit a RADIUS server:

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

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

To delete a server, use the following command:

```
Admin/system@nodename# delete users auth-server radius <radius-server-
name> <parameter>
```

You can also delete individual parameters of a RADIUS server. You can delete the following parameters:

- **addresses**

Configuring a TACACS+ server

A TACACS+ server is configured at the **users auth-servers tacacs** level.

To create a TACACS+ auth server, use the following command:

```
Admin/system@nodename# create users auth-server tacacs <parameter>
```

Provide the following parameters:

Parameter	Description
name	TACACS+ server name.
enabled	Enable/disable the server.
description	Auth server description.
secret	Pre-shared key used by the TACACS+ protocol for authentication.
address	The IP address for the TACACS+ server.
port	The UDP port on which the TACACS+ server listens for authentication requests. By default, UDP port 1812 is used.
single-connection	Use a single TCP connection for communicating with the TACACS+ server.

Parameter	Description
timeout	The authentication timeout for the TACACS+ server. The default is 4 seconds.

To edit information about a TACACS+ server, use the following command:

```
Admin/system@nodename# set users auth-server tacacs <tacacs-server-
name> <parameter>
```

The parameters you can update are the same as those used to create an auth server.

To display information about a TACACS+ server, use the following command:

```
Admin/system@nodename# show users auth-server tacacs <tacacs-server-
name>
```

Example commands to create and edit a TACACS+ server:

```
Admin/system@nodename# create users auth-server tacacs address
10.10.0.11 name "New TACACS+ server" port 1812 secret 12345 enabled on
Admin/system@nodename# show users auth-server tacacs "New TACACS+
server"

name                  : New TACACS+ server
enabled               : on
address               : 10.10.0.11
port                  : 1812
single-connection     : off
timeout               : 4
Admin/system@nodename# set users auth-server tacacs "New TACACS+
server" description "New TACACS+ server description"
Admin/system@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
```

To delete a server, use the following command:

```
Admin/system@nodename# delete users auth-server tacacs <tacacs-server-
name>
```

Configuring Authentication Profiles

You configure auth profiles at the **users auth-profile** level.

To create an auth profile, use the following command:

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

Provide the following parameters:

Parameter	Description
name	Profile name.
description	Profile description.
idle-time	Idle time before disconnection (in seconds). After the specified time without activity the user's status will change to Unknown user.
expiration-time	Authenticated user time-to-live (in seconds). After the specified time the user's status will change to Unknown user and they will have to authenticate again.
max-attempts	Max authentication failures allowed before the user account is locked.
lockout-time	Time (in seconds) for which the user account is locked if the specified max number of failures is reached.

Parameter	Description
auth-methods	Authentication method: • **ldap**: authentication using an LDAP connector. • **radius**: authentication using a RADIUS server. • **tacacs**: authentication using a TACACS+ server.

To edit authentication profile parameters, use the following command:

```
Admin/system@nodename# set users auth-profile <auth-profile-name>
<parameter>
```

The list of parameters available to update is the same as for the **create** command.

Example of creating and editing a user authentication profile:

```
Admin/system@nodename# create users auth-profile name "New LDAP auth
profile" auth-methods ldap [ "New LDAP connector" ]
Admin/system@nodename# show users auth-profile "New LDAP auth profile"

name                : New LDAP auth profile
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic          : off
    local-user-auth     : off
    policy-accept       : off
Admin/system@nodename# set users auth-profile "New LDAP auth profile"
description "New LDAP auth profile description"
Admin/system@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
```

You can use the command line interface to delete an entire profile or individual authentication methods specified in a profile. To do this, use the following commands.

To delete an authentication profile:

```
Admin/system@nodename# delete users auth-profile <auth-profile-name>
```

To delete authentication methods configured in a profile, you need to specify an authentication method (available authorization methods are listed in the table above):

```
Admin/system@nodename# delete users auth-profile <auth-profile-name>
auth-methods <auth-metod>
```

NETWORK CONFIGURATION

Zones

This section is located at the **network zone** level. To create a new zone, use the following command:

```
Admin/system@nodename# create network zone
```

Provide the following zone parameters:

Parameter	Description
name	Zone name.
description	Zone description.
dos-protection-syn	Protect the zone against network flooding for TCP protocol (SYN-flood): • **enabled**: enable/disable the protection. ◦ **on** ◦ **off** • **aggregate**: ◦ **on**: count all packets incoming to the zone's interfaces ◦ **off**: count packets for each IP address separately. • **alert-threshold**: alert threshold; if the number of requests exceeds this value, the event is recorded in the system log. • **drop-threshold**: packet drop threshold; if the number of requests exceeds this value, UserGate drops packets and records this event in the system log. • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
dos-protection-udp	Protect the zone against network flooding for UDP protocol: • **enabled**: enable/disable the protection. ◦ **on** ◦ **off** • **aggregate**: ◦ **on**: count all packets incoming to the zone's interfaces ◦ **off**: count packets for each IP address separately. • **alert-threshold**: alert threshold; if the number of requests exceeds this value, the event is recorded in the system log. • **drop-threshold**: packet drop threshold; if the number of requests exceeds this value, UserGate drops packets and records this event in the system log. • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
dos-protection-icmp	

Parameter	Description
	Protect the zone against network flooding for ICMP protocol: • **enabled**: enable/disable the protection. ◦ **on** ◦ **off** • **aggregate**: ◦ **on**: count all packets incoming to the zone's interfaces ◦ **off**: count packets for each IP address separately. • **alert-threshold**: alert threshold; if the number of requests exceeds this value, the event is recorded in the system log. • **drop-threshold**: packet drop threshold; if the number of requests exceeds this value, UserGate drops packets and records this event in the system log. • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
enabled-services	Zone access control settings: • **"Any ICMP"**: allow use of the ping command to a UserGate address. • **SNMP**: provides SNMP access to UserGate (UDP 161). • **rpc**: control XML-RPC: enables API control of the product (TCP 4040). • **VRRP**: required for combining several UserGate nodes into a HA cluster (IP protocol 112). • "CLI over SSH": access to server to manage it via CLI, port TCP 2200. • **Cluster**: service required to combine multiple UserGate nodes into a cluster (TCP 4369, TCP 9000-9100). • **"Admin Console"**: access to the management web console (TCP 8001).
service-addresses	Allowed IP addresses for services: • **service**: select services (the list corresponds to **enabled-services**). • **allowed-addresses**: the allowed IP addresses. The options are: ◦ **geoip**: a GeoIP code ◦ **ip-list**: an IP address list previously configured in the item library.

Parameter	Description
antispoof-enable	Enable/disable IP spoofing protection: • **on** • **off**
antispoof-negate	Enumerated options: • **on** • **off** If **antispoof-negate on** is enabled, the interfaces in that zone will not receive packets from the source addresses specified in the value **ip-spoofing-networks**. In this case packets with specified source IP addresses will be discarded.
sessions-limit-enabled	Enable the limit on the number of concurrent sessions from a single IP address: • **on** • **off**
sessions-limit-exclusions	Add a list of IP addresses to which the concurrent session limit will not apply.
sessions-limit-threshold	The maximum allowed number of sessions originating from a single IP address.
geoip	GeoIP codes that are used in IP spoofing protection.
ip-list	List of IP addresses that are used in IP spoofing protection.

Example command to create a zone:

```
Admin/system@nodename# create network zone name Test_zone description
"Test_zone description" antispoof-enable on enabled-services [ "Any
ICMP" DNS ] dos-protection-icmp enabled on
```

To edit zone parameters, use the following command:

```
Admin/system@nodename# set network zone <zone-name>
```

To edit zone parameters, use the following command:

```
Admin/system@nodename# set network zone Test_zone dos-protection-syn
enabled on
```

To delete a zone or its parameters, use the following command:

```
Admin/system@nodename# delete network zone <zone-name>
```

You can delete the following parameters:

Parameter	Description
dos-protection-syn	Protect the zone against network flooding for TCP protocol (SYN-flood): • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
dos-protection-udp	Protect the zone against network flooding for UDP protocol: • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
dos-protection-icmp	Protect the zone against network flooding for ICMP protocol: • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
enabled-services	The previously configured zone access control settings
geoip	GeoIP codes that are used in IP spoofing protection.
ip-list	List of IP addresses that are used in IP spoofing protection.

The following command is used to view zone settings:

```
Admin/system@nodename# show network zone <zone-name>
```

Interfaces

You apply interface settings at the **network interface** level.

Adapter settings

Network adapters are configured at the **network interface adapter** level.

You cannot create a network adapter. To update an existing network adapter, use the command:

```
Admin/system@nodename# set network interface adapter <adapter_name>
```

Provide the following network adapter parameters:

Parameter	Description
enabled	Enable/disable a network interface: • **on** • **off**
description	Network interface description.
alias	The interface's alias.
iface-type	Interface type: • **l3**: interface works in Layer 3 mode (you can assign an IP address and use it in firewall, content filtering, and other rules; this is the standard interface operation mode). • **mirror**: interface works in Mirror mode (it can receive traffic from the network equipment SPAN port to analyze it).
iface-mode	IP address assignment mode: • **dhcp**: obtain a dynamic IP address via DHCP. • manual: no address. Static mode is set automatically when an IP address is assigned to the interface.
zone	Zone to which the interface belongs.
link-info	Settings for network interface parameters: • **bc_forwarding**: control forwarding the directed broadcast packets arriving at the specified interface. • **proxy_arp**, **proxy_arp_vlan**: Proxy ARP mechanism. With **proxy_arp**, UserGate will respond to ARP requests for

Parameter	Description
	addresses outside the interface's network; with **proxy_arp_vlan**, UserGate will respond to ARP requests for addresses that belong to the interface's network. To specify them, use the following format: `Admin/system@nodename# create network interface <iface-type> … link-info [ key/value ]` where key is the parameter name. which can include lowercase Latin letters (a-z) and underscore (_), and value is the parameter value. Parameter values can only be integers. For example, use proxy_arp/1 to enable the Proxy ARP mechanism and proxy_arp/0 to disable it. The link-info field is displayed only when adding parameters. **Important!**You cannot delete the specified parameters.
ip-addresses	Assign an IP address to the interface. The IP addresses are specified as **[<ip_address/mask>]** or **[<ip_address/mask> <ip_address/mask>]**. In case of several IP addresses (with space used as the separator), the subnet mask is entered in the decimal format. **Important!** Make sure to separate the square brackets with spaces on both sides.
mac	Interface MAC address.
mtu	Specify the MTU size.
mss	Specifying the MSS size (available starting from version 7.3.x): 0, or starting from 4 to the value specified in MTU minus 40.

To delete an adapter or its parameters, use the following command:

```
Admin/system@nodename# delete network interface adapter <adapter-name>
```

You can delete the following parameters:

Parameter	Description
ip-addresses	Specified IP address.

Parameter	Description
dhcp-relay server-address	DHCP server IP address.

To display information about all network adapters, use the following command:

```
Admin/system@nodename# show network interface adapter
```

To display the adapter information, use the following command:

```
Admin/system@nodename# show network interface adapter <adapter-name>
```

Configuring a VLAN

VLAN interfaces are configured at the **network interface vlan** level.

To add a new VLAN interface, use the following command:

```
Admin/system@nodename# create network interface vlan
```

Parameters:

Parameter	Description
enabled	Enable/disable a VLAN interface: • **on** • **off**
description	Interface description.
alias	The interface's alias.
iface-type	Interface type: • **l3**: Layer 3 (you can assign an IP address and use it in firewall, content filtering, and other rules; this is the standard interface operation mode). • **mirror**: interface works in Mirror mode (it can receive traffic from the network equipment SPAN port to analyze it).

Parameter	Description
iface-mode	IP address assignment mode: • **dhcp**: obtain a dynamic IP address via DHCP. • manual: no address. Static mode is set automatically when an IP address is assigned to the interface.
tag	VLAN tag. Up to 4094 interfaces can be created.
node-name	Cluster node name where the VLAN is created.
interface	The physical interface on which the VLAN is being created.
zone	Zone to which the interface belongs.
link-info	Settings for network interface parameters: • **bc_forwarding**: control forwarding the directed broadcast packets arriving at the specified interface. • **proxy_arp**, **proxy_arp_vlan**: Proxy ARP mechanism. With **proxy_arp**, UserGate will respond to ARP requests for addresses outside the interface's network; with **proxy_arp_vlan**, UserGate will respond to ARP requests for addresses that belong to the interface's network. To specify them, use the following format: `Admin/system@nodename# create network interface <iface-type> … link-info [ key/value ]` where key is the parameter name. which can include lowercase Latin letters (a-z) and underscore (_), and value is the parameter value. Parameter values can only be integers. For example, use proxy_arp/1 to enable the Proxy ARP mechanism and proxy_arp/0 to disable it. The link-info field is displayed only when adding parameters. **Important!**You cannot delete the specified parameters.
ip-addresses	Assign an IP address to the interface. The IP addresses are specified as **[<ip_address/mask>]** or **[<ip_address/mask> <ip_address/mask>]**. In case of several IP addresses (with space used as the separator), the subnet mask is entered in the decimal format.

Parameter	Description
	Important! Make sure to separate the square brackets with spaces on both sides.
mac	Interface MAC address.
mtu	Specify the MTU size.
mss	Specifying the MSS size (available starting from version 7.3.x): 0, or starting from 4 to the value specified in MTU minus 40.
dhcp-relay	Settings for the DHCP relay on the interface. You need to specify the following: • **enabled**: enable/disable the relay: ◦ **on** ◦ **off** • **utm-address**: IP address of the UserGate interface on which the relay function is added. • **server-address**: addresses of DHCP servers where DHCP requests from clients should be redirected.

To edit an existing VLAN, use the following command:

```
Admin/system@nodename# set network interface vlan <vlan-name>
```

The parameters available for setting are the same as those for creating a VLAN, except for **tag**, **node-name**, and **interface** (you cannot change these parameter values).

To delete a VLAN interface or its parameters, use the following command:

```
Admin/system@nodename# delete network interface vlan <vlan-name>
```

You can delete the following parameters:

Parameter	Description
ip-addresses	Specified IP address.
dhcp-relay server-address	DHCP server IP address.

To display information about all VLAN interfaces, use the following command:

```
Admin/system@nodename# show network interface vlan
```

To display information about a single interface, use the following command:

```
Admin/system@nodename# show network interface vlan <vlan-name>
```

Properties of bond interfaces

You configure bond interface properties at the **network interface bond** level.

To create a bond interface, use the following command:

```
Admin/system@nodename# create network interface bond
```

You need to specify the following parameters:

Parameter	Description
enabled	Enable/disable the interface: • **on** • **off**
interface-name	Enter a number to include in the interface name (for example, if you enter 1 the interface name will be bond1).
description	Interface description.
alias	The interface's alias.
node-name	Cluster node where the bond interface is created.
zone	Zone to which the bond belongs.
link-info	Settings for network interface parameters: • **bc_forwarding**: control forwarding the directed broadcast packets arriving at the specified interface. • **proxy_arp**, **proxy_arp_vlan**: Proxy ARP mechanism. With **proxy_arp**, UserGate will respond to ARP requests for addresses outside the interface's network; with **proxy_ar**

Parameter	Description
	p_vlan, UserGate will respond to ARP requests for addresses that belong to the interface's network. To specify them, use the following format: `Admin/system@nodename# create network interface <iface-type> … link-info [ key/value ]` where key is the parameter name. which can include lowercase Latin letters (a-z) and underscore (_), and value is the parameter value. Parameter values can only be integers. For example, use proxy_arp/1 to enable the Proxy ARP mechanism and proxy_arp/0 to disable it. The link-info field is displayed only when adding parameters. **Important!**You cannot delete the specified parameters.
bonding	Additional bond interface parameters: • **mode**: bond operation mode. The available options: ◦ **round-robin**: Round robin mode (packets are sent sequentially starting with the first available interface and ending with the last one. This policy is used to provide load balancing and high availability.) ◦ **active-backup**: Active backup mode (only one network interface in the bond will be active. Another slave interface can become active only if the currently active interface fails. With this policy, the MAC address of the bond interface is only visible externally through one network port to avoid problems with the switch. This policy is used to provide high availability). ◦ **xor**: XOR mode (the transmission is allocated among the NICs using the following formula: [(XOR) MOD]. This means that the same NIC sends packets to the same recipients. Optionally, the transmission allocation can also be based on the xmit_hash policy. The XOR policy is used for load balancing and high availability). ◦ **broadcast**: Broadcast mode (broadcasts everything to all network interfaces. This policy is used for high availability). ◦ **802.3ad**: IEEE 802.3ad mode (the default mode supported by most network switches. Creates aggregated groups of NICs with identical speed

Parameter	Description
	and duplex settings. When combined like this, all links in the active aggregation participate in transmission as per IEEE 802.3ad. The choice of interface for packet transmission is determined by the policy. By default, the XOR policy is used, with the xmit_hash policy as a possible alternative). ◦ **transmit**: Adaptive transmit load balancing mode (outgoing traffic is distributed depending on the loading of each NIC (determined by the load speed). No additional configuration on the switch is required. The incoming traffic is received by the current network card. If this card fails, another card assumes the MAC address of the failed one). ◦ **load**: Adaptive load balancing mode. Includes the previous policy plus incoming traffic balancing. No additional configuration on the switch is required. The incoming traffic is balanced through ARP negotiation. The driver intercepts ARP responses sent from the local NICs to the outside and overwrites the source MAC address with one of the unique MAC addresses of the NIC in the bond. Thus, different peers use different server MAC addresses. The incoming traffic is balanced sequentially (round-robin) among the interfaces. • **mii-monitoring**: MII monitoring period in milliseconds. Determines how often the link state will be checked for failures. • **down-delay**: delay time (in milliseconds) before an interface is disabled if a connection failure occurs. This option is only valid for MII monitoring (miimon). The parameter value must be a multiple of miimon, • **up-delay**: delay time in milliseconds before deploying the channel if it is detected to be restored. This parameter is only valid with MII monitoring (miimon). The parameter value must be a multiple of miimon, • **lacp-rate**: interval with which the partner transmits LACPDU packets in 802.3ad mode. Enumerated options: ◦ **slow**: requests that the partner send LACPDU packets every 30 seconds. ◦ **fast**: requests that the partner send LACPDU packets every second. • **failover-mac**: define the assignment type of MAC addresses to bond interfaces in Active backup mode when switching interfaces. Enumerated options: ◦ **disabled**: the same MAC address is set on all interfaces during switching.

Parameter	Description
	◦ **active**: the MAC address on the bond interface will always be identical to that on the currently active slave. The MAC addresses on the backup interfaces are not changed. The MAC address on the bond interface changes during the failover processing. ◦ **follow**: the MAC address on the bond interface will be the same as that on the first slave added to the bond. This MAC is not set on the second and subsequent interfaces while they are in backup mode. That MAC address gets assigned during a failover: when a backup slave interface becomes active, it assumes a new MAC (the one on the bond interface), and the formerly active slave is assigned the MAC that the currently active one used to have. • **xmit-hash**: define a hash policy for sending packets over bond interfaces in XOR or IEEE 802.3ad mode. Enumerated options: ◦ **l2**: use only MAC addresses to generate the hash. With this algorithm, the traffic for a particular network host is always sent over the same interface. This algorithm is compatible with IEEE 802.3ad. ◦ **l2-3**: use both MAC and IP addresses to generate the hash. This algorithm is compatible with IEEE 802.3ad. ◦ l3-4: uses IP addresses and transport layer protocols (TCP or UDP) to generate the hash. This algorithm is not universally compatible with IEEE 802.3ad, as both fragmented and non-fragmented packets can be transmitted within a single TCP or UDP interaction. Fragmented packets lack the source and destination ports. As a result, packets from the same session can reach the recipient in an order other than the intended one because they are sent via different slaves. • **interface**: interfaces to be bonded.
iface-mode	IP address assignment mode: • **dhcp**: obtain a dynamic IP address via DHCP. • manual: no address. Static mode is set automatically when an IP address is assigned to the interface.

Parameter	Description
iface-type	The type of interface to be created: • **l3**: a Layer 3 interface • **mirror**: a mirroring interface.
ip-addresses	Assign an IP address to the interface. The IP addresses are specified as **[<ip_address/mask>]** or **[<ip_address/mask> <ip_address/mask>]**. In case of several IP addresses (with space used as the separator), the subnet mask is entered in the decimal format. **Important!** Make sure to separate the square brackets with spaces on both sides.
mac	Interface MAC address.
mtu	Specify the MTU size.
mss	Specifying the MSS size (available starting from version 7.3.x): 0, or starting from 4 to the value specified in MTU minus 40.

To update an existing bond interface, use the following command:

```
Admin/system@nodename# set network interface bond <bond-name>
```

The parameters available for setting are the same as those for creating a bond interface, except for **interface-name** and **node-name** (you cannot change the values of these parameters).

To delete a bond interface or its parameters, use the following command:

```
Admin/system@nodename# delete network interface bond <bond-name>
```

You can delete the following parameters:

Parameter	Description
ip-addresses	Specified IP address.
dhcp-relay server-address	DHCP server IP address.
bonding interface	Bonded interfaces.

To display information about all bond interfaces, use the following command:

```
Admin/system@nodename# show network interface bond
```

To display information about a single interface, use the following command:

```
Admin/system@nodename# show network interface bond <bond-name>
```

Gateways

This section is located at the **network gateway** level.

To add a new gateway, use the following command:

```
Admin/system@nodename# create network gateway
```

Available parameters:

Parameter	Description
enabled	Enable/disable the gateway: • **on** • **off**
name	Gateway name.
description	Gateway description.
interface	Interface used to access the Internet: • Select a specific port (**port0**, **port1**, **port2**, etc.); • **auto**: after selecting this option, the port will be detected automatically. This option is available for nodes that have been initialized. For nodes that have not been initialized, the option is available starting with software release 7.3.0.
ip	Gateway IP address.

Parameter	Description
node-name	Select the cluster node for which the gateway is configured.
weight	Gateway weight (the greater the weight, the greater the share of traffic goes through the gateway).
balancing	Balancing mode: all traffic to the Internet will be distributed between the gateways according to their weights: • **on** • **off**
default	Use this gateway as the default gateway: • **on** • **off**

To update gateway parameters, use the following command:

```
Admin/system@nodename# set network gateway <gateway-name>
```

You can use the same set of parameters as when creating a gateway.

To delete a gateway, use the following command:

```
Admin/system@nodename# delete network gateway <gateway-name>
```

To display information about all gateways, use the following command:

```
Admin/system@nodename# show network gateway
```

To display information about a single gateway, use the following command:

```
Admin/system@nodename# show network gateway <gateway-name>
```

Routing Configuration

This section describes how to configure routing using the CLI. These settings are applied at the **network routes** level.

To add a new static route, use the following command:

```
Admin/system@nodename# create network routes <parameters>
```

Specify the parameters:

Parameter	Description
enabled	Enable/disable usage of a static route: • **on** • **off**
name	Route name.
description	Route description.
node-name	Select a cluster node to configure routing.
type	Route type: • **unicast**: the standard route type. Forwards the traffic destined for the specified address via the specified gateway. • **unreachable**: drops the traffic. and sends the "Host unreachable" (type 3 code 1) ICMP message to the source. • **prohibit**: drops the traffic. and sends the "Host unreachable" (type 3 code 13) ICMP message to the source. • **blackhole**: drops the traffic without informing the source that the data did not reach the recipient.
destination-ip	IP address of the destination subnet, format: <ip/mask>.
gateway	IP address of the gateway through which the specified subnet will be reachable. The IP address must be reachable from the device.
interface	Interface through which the route is added.

Parameter	Description
metric	Route metric. The lower the metric, the higher the priority of the route (if there is more than one route to a network).

Example of adding a static route:

```
Admin/system@nodename# create network routes name test_route
description "Test static route" destination-ip 192.168.200.0/2
4 gateway 192.168.100.100 interface port1 type unicast metric 1 enabled
on
Admin/system@nodename#

Admin/system@nodename# show network routes test_route

name              : test_route
description       : Test static route
enabled           : on
node-name         : testnode1
interface         : port1
type              : unicast
destination-ip    : 192.168.200.0/24
gateway           : 192.168.100.100
metric            : 1
```

To change the parameters of an existing static route, use the following command:

```
Admin/system@nodename# set network routes <route-name>
```

The parameters available to change are listed in the table above.

To delete a static route, use the following command:

```
Admin/system@nodename# delete network routes <route-name>
```

Example of deleting a static route:

```
Admin/system@nodename# delete network routes test_route
```

To display static routes, use the following command:

```
Admin/system@nodename# show network routes
```

DNS Configuration

You configure system DNS servers at the **network dns system-dns-servers** level.

To add new DNS servers or update the list of existing ones, use the following commands:

```
Admin/system@nodename# set network dns system-dns-servers ip [ <ip>
<ip> ... ] ]
```

To delete the entire list of DNS server addresses, use the following command:

```
Admin/system@nodename# delete network dns system-dns-servers
```

To delete individual servers, use the following command:

```
Admin/system@nodename# delete network dns system-dns-servers ip [ <ip>
<ip> ... ]
```

To display the list of system DNS servers, use the following command:

```
Admin/system@nodename# show network dns
```

SETTING UP MONITORING

Configuring Device Monitoring Settings

Configuring device monitoring parameters in the CLI interface is done in configuration mode at the **monitoring** level. Commands at this level allow you to manage the configuration of SNMP device parameters, SNMP monitoring rules, security profiles for authenticating SNMP managers, and notification rules. Read more about monitoring and notification rules in the Notifications section.

Configuring SNMP Device Parameters

To configure the SNMP device parameters, use commands at the **monitoring smnp-parameter** level:

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

You can edit the following parameters:

Parameter	Description
agent-name	Name of the system which is used by SNMP control subsystem.
location	Information on physical location of the SNMP agent.
description	Description of the system.
Engine ID	Each UserGate device has a unique SNMPv3 Engine ID. By default, the Engine ID is generated from the UserGate node name. When editing the Engine ID, you are required to specify its length (**length**), type, and value. The length can be defined as fixed (max. 8 bytes) or dynamic (max. 27 bytes). A fixed ID length is only applicable to the **text** type. The Engine ID can be generated in these formats: • **ip4**: IPv4 • **ipv6**: IPv6 • **mac**: MAC address • **text**: text • **octets**: octets

Read more about the SNMP parameters of the UserGate device in the SNMP section.

Configuring SNMP Monitoring Rules

To configure device monitoring rules via SNMP, commands are used at the **monitoring snmp** level:

```
Admin/system@nodename# edit monitoring snmp <parameters>
```

You can edit the following parameters:

Parameter	Description
name	The name of the rule.
enabled	Enable/disable a rule
community	SNMP community — the string for UserGate server identification and SNMP server identification for SNMP v2c. Use only numbers and Latin letters.
context	Optional parameter that defines the SNMP context. Use only Latin letters and numbers. Some devices may have multiple copies of the entire MIB subtree. For example, several virtual routers can be created on the device. Each such virtual router will have a complete MIB subtree. In this case, each virtual router can be specified as a context on the SNMP server. The context is identified by name. When the client makes a request, the context name can be specified. If the context name is not specified, the default context will be requested.
version	Specify the version of the SNMP protocol used in the rule. Available options: SNMP v2c and SNMP v3.
query	When enabled, allows receiving and processing of SNMP requests from the SNMP manager.
trap	When enabled, allows sending of SNMP traps to the server configured to receive notifications.
trap-host	Server IP address for traps. This setting is required only if you need to send traps to the notification server.
trap-port	The port on which the server listens for notifications. Usually, it is UDP port 162. This setting is required only if you need to send traps to the notification server.
security-profile	

Parameter	Description
	For SNMP v3 only. For more details, see the SNMP Security Profiles section.
events	Selecting the types of parameters available for monitoring by rule.

For the SNMP manager to work with the UserGate device, it is necessary to enable the **SNMP** service in the access control settings in the zone properties of the interface to which the connection will be made via the SNMP protocol. For more information about setting up zones in the CLI, see the Network Settings section.

Configuring SNMP Security Profiles

To configure security profiles to authenticate SNMP managers, use commands at the **monitoring smnp-security-profile** level:

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

You can edit the following parameters:

Parameter	Description
name	SNMP security profile name
description	SNMP security profile description
username	User name to authenticate the SNMP manager.
auth-type	Select an authentication mode for the SNMP manager. The available options are: • **none**: no authentication, no encryption • **no-encrypt** : authentication, no encryption • **encrypt**: authentication, encryption The authPriv mode is considered the most secure.
auth-alg	The algorithm used for authentication. Possible to use: • **sha** • **md5** • **sha224**

Parameter	Description
	• **sha256** • **sha384** • **sha512**
auth-password	The password used for authentication.
encrypt-alg	The algorithm used for encryption. DES or AES can be used.
encrypt-password	The password used for encryption.

Configuring Notification Rules

To configure alert rules, use commands at the **monitoring alert-rules** level:

```
Admin/system@nodename# edit monitoring alert-rules <parameters>
```

You can edit the following parameters:

Parameter	Description
enabled	Enables/disables the rule.
name	The name of the rule.
description	A description of the rule.
notification-profile	A previously created notification profile.
sender	From whom the notifications will come.
subject	Notification subject.
timeout	The time during which the server will not send a message when this rule is triggered again. This setting prevents a flood of messages when an alert rule is triggered frequently.
events	Events for which you want to receive alerts.
phones	For SMPP profiles, The phone groups to which SMS notifications will be sent.
emails	For SMTP profiles. The groups of email addresses to which email notifications will be sent.

CONFIGURING LIBRARIES

Configuring Libraries (Description)

Configuring IP addresses

This section is located at the **libraries ip-list** level.

To create an IP address group, use the following command:

```
Admin/system@nodename# create libraries ip-list <parameter>
```

Provide the following parameters:

Parameter	Description
name	Address list name.
description	List description.
threat-lvl	Threat level: • **very-low**: very low threat level • **low**: low threat level • **medium**: medium threat level • **high**: high threat level • **very-high**: very high threat level.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last).

Parameter	Description
	• A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
lists	Select existing IP lists to add to the list being created.
ips	IP addresses or a range of IP addresses to include in the list. Format: <ip>, <ip/mask>, or <ip_range_start-ip_range_end>.

To edit a list (parameters available to update are identical to those used to create a list), use the following command:

```
Admin/system@nodename# set libraries ip-list <ip-list-name> <parameter>
```

To add new addresses to a list, use the following command:

```
Admin/system@nodename# set libraries ip-list <ip-list-name> [ <ip1>
<ip2> ... ] ]
```

To delete an entire address list or individual IP addresses it contains, use the following commands:

```
Admin/system@nodename# delete libraries ip-list <ip-list-name>
Admin/system@nodename# delete libraries ip-list <ip-list-name> ips
[ <ip1> <ip2>... ] ]
```

To display information about all existing lists, use the following command:

```
Admin/system@nodename# show libraries ip-list
```

To display information about an individual list, specify the IP address list name:

```
Admin/system@nodename# show libraries ip-list <ip-list-name>
```

To display the contents of an IP address list, use the following command:

```
Admin/system@nodename# show libraries ip-list <ip-list-name> items
```

Configuring email addresses

This section is located at the **libraries email-list** level.

To add a new email group, use the following command:

```
Admin/system@nodename#& create libraries email-list <parameter>
```

Specify the parameters:

Parameter	Description
name	Email group name.
description	Email group description.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples:

Parameter	Description
	"2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
emails	Emails to add to the group.

To edit information about an email group, use the following command:

```
Admin/system@nodename# set libraries email-list <email-list-name>
<parameter>
```

The parameters available to update are the same as those for creating an email group.

To delete a group or individual emails from it, use the following commands:

```
Admin/system@nodename# delete libraries email-list <email-list-name>
Admin/system@nodename# delete libraries email-list <email-list-name>
emails [ <email> ... ] ]
```

To view information about all existing groups, about individual groups, or about emails in a group, use the following commands:

```
Admin/system@nodename# show libraries email-list
Admin/system@nodename# show libraries email-list <email-list-name>
Admin/system@nodename# show libraries email-list <email-list-name>
emails
```

Configuring phones

The **Phones** section is configured at the **libraries phone-list** level.

To create a phone group, use the following command:

```
Admin/system@nodename# create libraries phone-list <parameter>
```

Provide the following parameters:

Parameter	Description
name	Phone group name.
description	Phone group description.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
phones	Phones to add to the group.

To edit information about a phone group, use the following command:

```
Admin/system@nodename# set libraries phone-list <phone-list-name>
<parameter>
```

The parameters available to update are listed in the table above.

To delete a group or individual phones from it, use the following commands:

```
Admin/system@nodename# delete libraries phone-list <phone-list-name>
Admin/system@nodename# delete libraries phone-list <phone-list-name>
phones [ <phone> ... ] ]
```

To view information about all existing groups, use the following command:

```
Admin/system@nodename# show libraries phone-list
```

To view information about an individual phone group, use the following command:

```
Admin/system@nodename# show libraries phone-list <phone-list-name>
```

To display phones included in a group, use the following command:

```
Admin/system@nodename# show libraries phone-list <phone-list-name>
phones
```

Configuring notification profiles

You configure notification profiles for SMTP (via email) and SMPP (via SMS) at the **libraries notification-profiles** level.

To add a new SMTP notification profile:

```
Admin/system@nodename# create libraries notification-profiles smtp
<parameter>
```

Specify the following parameters:

Parameter	Description
name	Profile name.
description	Profile description.
host	The IP address or FQDN of the SMTP server that will be used for sending emails.
port	The TCP port used by the SMTP server. Usually, SMTP uses port 25, and SMTP with SSL uses port 465. Consult your email server administrator regarding this value.
connection-security	The following outgoing email security options are available: • **none**.

Parameter	Description
	• **starttls**. • **ssl**.
authentication	Enable/disable authorization when connecting to the SMTP server: • **on** • **off**
login	Login name to connect to the SMTP server.
password	Password to connect to the SMTP server.

To create an SMS (SMPP) notification profile, use the following command:

```
Admin/system@nodename# create libraries notification-profiles smpp
<parameter>
```

Provide the following parameters:

Parameter	Description
name	Profile name.
description	Profile description.
host	IP address or FQDN of an SMPP server to use to send SMS.
port	TCP port to use to connect to the SMPP server. Usually, the port used for the SMPP protocol is 2775, when using SSL — 3550.
ssl	Enable/disable SSL encryption: • **on** • **off**
login	The account name for connecting to the SMPP server.
password	The account password for connecting to the SMPP server.
phone-translation-rules	Phone translation rules. These rules are used to ensure that the provider requirements are met.

Parameter	Description
	For example, to replace all numbers starting with +7 to 8, use the following command: `Admin/system@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [ +7¦8 ]`
source-ton	Type of number for the event source: • **0**: unknown • **1**: international • **2**: national • **3**: network specific • **4**: subscriber number • **5**: alphanumeric • **6**: abbreviated.
dest-ton	Type of number for destination: • **0**: unknown • **1**: international • **2**: national • **3**: network specific • **4**: subscriber number • **5**: alphanumeric • **6**: abbreviated.
source-npi	Numbering Plan Indicator for the source: • **0**: Unknown. • **1**: ISDN/telephone numbering plan (E.163/E.164) • **3**: data numbering plan (X.121) • **4**: telex numbering plan (F.69) • **6**: land Mobile (E.212) • **8**: national numbering plan • **9**: private numbering plan • **10**: ERMES numbering plan (ETSI DE/PS 3 01-3) • **13**: Internet (IP). • **18**: WAP Client Id (to be defined by WAP Forum).

Parameter	Description
dest-npi	Numbering Plan Indicator for the destination: • **0**: Unknown. • **1**: ISDN/telephone numbering plan (E.163/E.164) • **3**: data numbering plan (X.121) • **4**: telex numbering plan (F.69) • **6**: land Mobile (E.212) • **8**: national numbering plan • **9**: private numbering plan • **10**: ERMES numbering plan (ETSI DE/PS 3 01-3) • **13**: Internet (IP). • **18**: WAP Client Id (to be defined by WAP Forum).

To edit a notification profile, use the following command:

```
Admin/system@nodename# set libraries notification-profiles <smtp |
smpp> <profile-name> <parameter>
```

SMTP and SMPP profile parameters available to change are listed in the respective tables above.

To delete a profile, use the following command:

```
Admin/system@nodename# delete libraries notification-profiles <smtp |
smpp> <profile-name>
```

You can also delete phone translation rules from SMPP notifications:

```
Admin/system@nodename# delete libraries notification-profiles smpp
<profile-name> phone-translation-rules [ phone1¦phone2 ]
```

To display information about all existing notification profiles, use the following command:

```
Admin/system@nodename# show libraries notification-profiles
```

To display information about all notification profiles of a specific type, use the following command:

```
Admin/system@nodename# show libraries notification-profiles <smtp |
smpp>
```

To display information about an individual notification profile, use the following command:

```
Admin/system@nodename#show libraries notification-profiles <smtp |
smpp> <profile-name>
```

MANAGING REALMS

Setting up Managed Realms

To be able to manage realms, the UGMC administrator must perform the following steps:

1. Create a realm.
2. Create an administrator profile of the Realm administrator type.
3. Create a realm administrator.

For more information about managing realms in UGMC, see the Managing Realms section.

Creation of a managed realm

Managed realms are configured at the **realms** level.

To create a managed realm, use the following command:

```
Admin/system@nodename# create realm <parameters>
```

Provide the following parameters:

Parameter	Description
name	The managed realm name.
description	**The managed realm description.**
code-name	Codename. Consists of several letters and/or numbers. You will need to enter the realm code name during login to the console for managing this realm. Example: UG.
is-default	**Default realm. If this option is enabled, you do not need to add the realm name after a slash for authentication in the console.**
max-devices	The maximum number of managed UserGate NGFW devices in the realm.
max-ep-devices	The maximum number of managed endpoints (UserGate Client) in the realm.

Example command to create a managed realm:

```
Admin/system@nodename# create realms name "Test realm" code-name
tstrlm1 is-default on max-devices 10 max-ep-devices 100
```

Example command to view available managed realms:

```
Admin/system@nodename# show realms

Example realm
    name              : Example realm
    is-default        : off
    description       : Example realm created for demo purpose. Can be
changed or deleted if necessary.
    code-name         : EX
    num-devices       : 1
    num-ep-devices    : 0
    max-devices       : unlimited
    max-ep-devices    : unlimited

Test realm
```

```
    name              : Test realm
    is-default        : on
    code-name         : tstrlm1
    num-devices       : 0
    num-ep-devices    : 0
    max-devices       : 10
    max-ep-devices    : 100
```

Example command to edit the parameters of previously created managed realms:

```
Admin/system@nodename# set realms "Test realm" max-devices 50
Admin/system@nodename# show realms "Test realm"

name              : Test realm
is-default        : off
code-name         : tstrlm1
num-devices       : 0
num-ep-devices    : 0
max-devices       : 50
max-ep-devices    : 100
```

Example command to delete a previously created managed realm:

```
Admin/system@nodename# delete realms "Test realm"
```

Creating a Managed Realm Administrator

To manage a previously created realm, you need to create the realm administrator.

An administrator profile of the realm administrator type is created as described in Configuring Permissions for Administrator Profiles.

Realm administrator accounts are created as described in Setting up administrator accounts.

ADMINISTRATOR FOR MANAGED REALMS MODE

Administrator for Managed Realms Mode (Description)

After you have created the managed realm and the realm administrator, you can proceed to the realm management mode. To do that, log out from the UGMC administrator account and log in again as the administrator for this managed realm. For example, to log in via SSH to the management console of the **realm** realm with the **realmadmin** realm administrator account, specify the following:

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

After successful authentication, a line will appear in the CLI waiting for a command to be entered (diagnostic mode). To view the current available options or use autocomplete, press **Tab**. Available values:

- **configure**: switch to the configuration mode
- **date**: view the current device date and time
- **exit**: exit the command line
- **show**: view the UGOS software version and statistics on open TCP, UDP, and ICMP sessions
- **clear**: clear statistics on open sessions

To abort the current command, press **Ctrl+C**; to view command history, use the ↑ and ↓ keys.

Administrator for Managed Realms Configuration Mode

To enter the configuration mode, use the following command:

```
realmadmin/realm@nodename> configure
```

Once you enter the configuration mode, the command line will be as follows:

```
realmadmin/realm@nodename#
```

To view a hint about the current possible values or to autocomplete commands, press the **Tab** key. The following symbols can be used in the hint:

*****— a required field in the create command and some others

+— an optional/variable field

> — a nested field; after entering it the previous list of fields becomes unavailable, a new list of fields appears that can be entered

General Command Structure in Configuration Mode

CLI commands have the following structure:

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

where:

<action> is the action to be performed;

<level> is the configuration level corresponding to the managed realm web interface section in UGMC;

<filter> is the identifier of the object being accessed; and

<configuration_info> is the set of parameter values to be applied to the <filter> object.

Name	Description
<action>	The following actions are available in the configuration mode: • **create**: create new objects. • **set**: edit all objects and enable various parameters. • **show**: display the current values. You can use this at any configuration level. Displays everything below the current level.

Name	Description
	• **delete**: delete an object or a parameter from the parameter list. • **edit**: go to a specific configuration level. The configuration level is displayed under the command line. • **end**: go one level up. • **top**: go back to the topmost configuration level. • **import**: import the configuration. • **export**: export the configuration. • **go**— switching to the mode for setting parameters for the template of managed devices. • **exit**: exit the configuration mode.
<level>	The levels in the command line follow the realm management console web interface: • **ngfw**: corresponds to the **NGFW** section of the web interface. • **endpoint**: corresponds to the **Endpoints** section of the web interface. • **logan**: corresponds to the **LogAn** section of the web interface. • **settings**: corresponds to the **Management Center** — **General Settings, Administrators, Authentication Profiles** sections of the web interface. • **users**: corresponds to the **Management Center** — **Users catalog** sections of the web interface.
<filter>	ID of the object which is being accessed. Objects are identified by their name.
<configuration_info>	Set of parameter-argument pairs. where the parameter is the name of the field for which you need to set the argument. Arguments can be single-valued or multi-valued. **A single-valued argument** is the value of the parameter. If the string contains spaces, use quotation marks. **Multi-valued arguments** are used to set multiple values of a parameter; include them in square brackets and separate by spaces.

General Settings of the Managed Realm Console

You configure general settings of the managed realm console at the **settings general** level. This is the command structure to configure one of the sections (<settings-module>):

```
realmadmin/realm@nodename# set settings general <settings-module>
```

You can configure the following sections:

Parameter	Description
admin-console	Admin console settings (**settings general admin-console** level): • **timezone**: time zone for your location. Used in rule schedules and for the correct display of time and date in reports, logs, etc • **api-session-lifetime**: admin session timeout in seconds.
change-tracker	Configure change tracker (settings general change-tracker level): • **enabled**: enable/disable change tracker. ◦ **on** ◦ **off** • **event-tracker-types**: change types are set by an administrator. To delete a change type, use the following command: `realmadmin/realm@nodename# delete settings general change-tracker event-tracker-types [ type1 ... ] ]`

Managed Realm Administrators

Realm administrator can create additional administrators in its area similar to the commands described in the Configuring permissions for administrator profiles and Configuring administrator accounts sections.

This section is configured at the **settings administrators** level. In this section configuring administrators and their profiles is described.

Configuring administrator accounts

You configure administrator accounts at the **settings administrators administrators** level.

To create an administrator account, use the following command:

```
realmadmin/realm@nodename# create settings administrators
administrators
```

Specify the administrator account type (local, LDAP user, LDAP group, with auth profile) and the respective parameters:

Parameter	Description
local	Add a local administrator: • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: administrator login name. • **display-name**: the administrator's display name. • **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. • **password**: administrator password.
ldap-user	Add a user from the existing domain (you need to have the LDAP connector configured correctly; for more details, see the Configuring LDAP Connectors section): • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: the administrator's login name in the **domain\user** format. When providing this parameter, use the following command structure: • **display-name**: the administrator's display name. • **connector**: the name of a previously configured LDAP connector.

Parameter	Description
	• **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. `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	Add a user group from the existing domain (you need to have the LDAP connector configured correctly; for more details, see the Configuring LDAP Connectors section): • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: administrator login name • **display-name**: the administrator's display name. • **connector**: the name of the used LDAP connector. • **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. `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	Add an administrator with an auth profile (you need to have the auth servers configured correctly; for more details, see the Configuring Authentication Servers section): • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: administrator login name. • **display-name**: the administrator's display name. • **description**: administrator account description.

Parameter	Description
	• **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. • **auth-profile**: select an auth profile from those created earlier; for more details about auth profiles, see the section Configuring Authentication Profiles.

To edit the profile parameters, use the following command:

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

The command's parameters are similar to those used for administrator profile creation.

To display information about all administrator accounts, use the following command:

```
realmadmin/realm@nodename# show settings administrators administrators
```

To display information about an individual administrator account, use the following command:

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

Configuring Permissions for Administrator Profiles

The permissions of administrator profiles are configured at the **settings administrators profiles** level.

To create an administrator profile, use the following command:

```
realmadmin/realm@nodename# create settings administrators profiles
```

Provide the following parameters:

Parameter	Description
name	Administrator profile name.
description	Administrator profile description.
realm-permissions	Realm management access permissions: • **no-access**: no access • **read**: read-only • **write**: read and write
ngfw-permissions	NGFW device management access permissions: • **no-access**: no access • **read**: read-only • **write**: read and write
ep-permissions	Endpoint management access permissions: • **no-access**: no access • **read**: read-only • **write**: read and write
logan-permissions	LogAn devices management access permissions: • **no-access**: no access • **read**: read-only • **write**: read and write

To edit the profile, use the following command:

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

The command's parameters are similar to those used for administrator profile creation.

To view information about all administrator profiles, use the following command:

```
realmadmin/realm@nodename# show settings administrators profiles
```

To display information about a specific profile, use the following command:

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

To delete an administrator profile, use the following command:

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

To view administrator sessions for the current realm, use the following command. You can view an individual administrator's session; to do so, browse the IP address list and select the address used to authenticate the administrator.

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

Managed Realm Authentication Servers

Authentication servers (auth servers) are external sources of user accounts used for authentication in the realm management console. A realm authentication server works similar to a UGMC authentication server, the only difference is where each is used.

The **Auth servers** section allows you to configure an LDAP connector, RADIUS, TACACS+ servers. You configure auth servers at the **users auth-server** level. We will consider it in the respective sections below.

Configuring LDAP connectors

An LDAP connector is configured at the **users auth-servers ldap** level.

To create an LDAP connector, use the following command:

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

Provide the following parameters:

Parameter	Description
name	LDAP connector name.
enabled	Enable/disable the auth server.
description	LDAP connector description.
ssl	Values: • **on**: use an SSL connection to connect to the LDAP server • **off**: connect to the LDAP server without using an SSL connection.
address	Controller IP address or the LDAP domain name.
bind-dn	The username used to connect to the server. Format: DOMAIN\username or username@domain. The user must be a user in the domain.
password	The user's password for connecting to the domain.
domains	List of domains served by the domain controller.
search-roots	The list of LDAP server paths relative to which the system will search for users and groups. Specify the full name, e.g., ou=Office,dc=example,dc=com. If the search paths are not specified, the system will search over the entire directory, starting from the root.

To edit information about an existing LDAP connector, use the following command:

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

The parameters available to update are the same as those for creating an LDAP connector.

To display information on an LDAP connector, use the following command:

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

Example commands to create and edit an LDAP connector:

```
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
```

To delete an LDAP connector, use the following command:

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

You can also delete individual parameters of an LDAP connector. You can delete the following parameters:

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

Configuring RADIUS Servers

A RADIUS server is configured at the **users auth-servers radius** level.

To create a RADIUS auth server, use the following command:

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

Provide the following parameters:

Parameter	Description
name	The RADIUS server name.
enabled	Enable/disable the auth server.
description	Auth server description.
secret	Pre-shared key used by the RADIUS protocol for authentication.
addresses	IP address and the UDP port on which the RADIUS server listens to requests (default port: 1812). Format: <ip:port>.

To update information about a RADIUS server, use the following command:

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

The parameters you can update are the same as those used to create an auth server.

To display information about a RADIUS server, use the following command:

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

Example commands to create and edit a RADIUS server:

```
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
```

To delete a server, use the following command:

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

You can also delete individual parameters of a RADIUS server. You can delete the following parameters:

- **addresses**

Configuring a TACACS+ server

A TACACS+ server is configured at the **users auth-servers tacacs** level.

To create a TACACS+ auth server, use the following command:

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

Provide the following parameters:

Parameter	Description
name	TACACS+ server name.
enabled	Enable/disable the server.
description	Auth server description.
secret	Pre-shared key used by the TACACS+ protocol for authentication.
address	The IP address for the TACACS+ server.
port	The UDP port on which the TACACS+ server listens for authentication requests. By default, UDP port 1812 is used.
single-connection	Use a single TCP connection for communicating with the TACACS+ server.
timeout	The authentication timeout for the TACACS+ server. The default is 4 seconds.

To edit information about a TACACS+ server, use the following command:

```
realmadmin/realm@nodename# set users auth-server tacacs <tacacs-server-
name> <parameter>
```

The parameters you can update are the same as those used to create an auth server.

To display information about a TACACS+ server, use the following command:

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

Example commands to create and edit a TACACS+ server:

```
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
```

To delete a server, use the following command:

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

Managed Realm Authentication Profiles

A profile can be used to define a set of methods to be used for user authentication in the UserGate administrative console.

You configure auth profiles at the **users auth-profile** level.

To create an auth profile, use the following command:

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

Provide the following parameters:

Parameter	Description
name	Profile name.
description	Profile description.
auth-methods	Authentication method: • **ldap**: authentication using an LDAP connector. • **radius**: authentication using a RADIUS server. • **tacacs**: authentication using a TACACS+ server.
expiration-time	Authorized user time-to-live (in seconds). After the specified time the user's status will change to Unknown user and they will have to authenticate again.
idle-time	Idle time before disconnection (in seconds). After the specified time without activity the user's status will change to Unknown user.
lockout-time	Time (in seconds) for which the user account is locked if the specified max number of failures is reached.
max-attempts	Max authentication failures allowed before the user account is locked.

To edit authentication profile parameters, use the following command:

```
realmadmin/realm@nodename# set users auth-profile <auth-profile-name>
<parameter>
```

The list of parameters available to update is the same as for the **create** command.

Example of creating and editing a user authentication profile:

```
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
```

You can use the command line interface to delete an entire profile or individual authentication methods specified in a profile. To do this, use the following commands.

To delete an authentication profile:

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

To delete authentication methods configured in a profile, you need to specify an authentication method (available authorization methods are listed in the table above):

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

Managed realm user catalogs

To work with users catalogs, a correctly configured LDAP connector is needed that enables information to be obtained on users and groups from Active Directory or other LDAP servers. The users and groups can be used in configuring policies applied to managed devices.

> **Note**
> **When you configure security policies, authentication servers configured in managed device templates are not used to add users and groups to rules.**

User catalogs are created and configured at the **users catalogs ldap** level.

To create a catalog, use the following command:

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

Provide the following parameters:

Parameter	Description
name	LDAP connector name.
enabled	Enable/disable the auth server.
description	LDAP connector description.
ssl	Values: • **on**: use an SSL connection to connect to the LDAP server • **off**: connect to the LDAP server without using an SSL connection.
address	Controller IP address or the LDAP domain name.
bind-dn	The username used to connect to the server. Format: DOMAIN\username or username@domain. The user must be a user in the domain.
password	The user's password for connecting to the domain.
domains	List of domains served by the domain controller.
search-roots	The list of LDAP server paths relative to which the system will search for users and groups. Specify the full name, e.g., ou=Office,dc=example,dc=com. If the search paths are not specified, the system will search over the entire directory, starting from the root.

To edit information about an existing catalog, use the following command:

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

The parameters available to update are the same as those for creating a catalog.

To display information about a user catalog, use the following command:

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

To delete a catalog, use the following command:

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

You can also delete individual parameters of an LDAP connector. You can delete the following parameters:

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

Managing UserGate Next-Generation Firewalls

The UserGate Management Center (UGMC) command-line interface allows managed realm administrators to centrally configure UserGate firewall settings. To do this in configuration mode you need to do the following:

1) configure UserGate NGFW template parameters

2) create UserGate NGFW template groups

3) add UserGate NGFW managed devices

Configuring UserGate NGFW Template Parameters

Before configuring UserGate NGFW template parameters, you must create device templates. It is recommended to create separate templates for different categories of settings, such as a network settings template, a firewall rules template, a filtering rules template, or a library template. This will simplify further work with templates when combining them into groups. The table below shows the commands you can use when creating UserGate NGFW templates.

Action	Command	Example of the command
Creating a template	`create ngfw template name <template name> description <template description>`	`realmadmin/realm@nodename# create ngfw template name example_template_1 description for_example_template`
Viewing a template	`show ngfw template <template name>`	`realmadmin/realm@nodename# show ngfw template example_template_1`

Action	Command	Example of the command
Viewing all templates	`show ngfw template`	`realmadmin/realm@nodename# show ngfw template`
Changing the template name and description	`set ngfw template <template name> name <new template name> description <new template description>`	`realmadmin/realm@nodename# set ngfw template example_template_1 name example_template_2 description for_testing_templete`
Deleting a template	`delete ngfw template <template name>`	`realmadmin/realm@nodename# delete ngfw template test_template_2`

After creating a template, you can configure its parameters. These parameters will be applied to all managed UserGate NGFW devices to which the template is applied within the group.

When configuring template parameters, consider the following:

- Parameter values in the template override those specified locally by the UserGate NGFW administrator. If a parameter value is not specified either in the template or on the firewall, the default value will be used.
- After applying the template to managed devices, administrators can change basic parameters and network interface parameters locally on each firewall. Detailed information about these parameters is provided in the General Settings and Interface Configuration sections of the UserGate NGFW Administrator's Guide.
- When configuring network interface parameters in a template, the first physical interface available for configuration will be port1. Port0 is used to connect UserGate NGFW to UGMC. The parameters for this interface are configured by the UserGate NGFW administrator during initial product setup. You can also configure other network interfaces locally on UserGate NGFW by specifying the `on-device` (or `on-device on`) property in the template interface parameters.
- Template element libraries (e.g., IP address libraries, URL list libraries, and content type libraries) do not contain data by default, unlike UserGate NGFW libraries. Before configuring policies in the template, you must add library elements. Library data is not synchronized: if the added elements are not used in the template policies, they will not be added to the UserGate NGFW libraries.

To configure UserGate NGFW template parameters:

Switch to template settings mode by running the command:

`go ngfw-template <template name>`

Example:

```
realmadmin/realm@nodename# go ngfw-template test_template_2
```

To configure template parameters, you can use the commands described in the Command Line Interface section of the UserGate NGFW Administrator's Guide.

Policy rules in a template do not override rules created locally by UserGate NGFW administrators; they are added to them as pre- and post-rules. Detailed information on creating policy rules is provided in the UserGate Policy Language section of the UserGate NGFW Administrator's Guide.

In addition, when creating a rule in a template, you can specify the rule's position relative to pre- or post-rules in the list using the `mc_pre` and `mc_post` properties, respectively. Below is an example of creating a post-rule:

```
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")
```

The created rule will appear at the top of the post-rule list. This rule prohibits unidentified users from passing traffic from the Trusted zone to the Untrusted zone.

Creating UserGate NGFW Template Groups

After creating UserGate NGFW templates, they must be organized into groups. A template group allows you to create a single configuration of settings that applies to one or more managed devices. This configuration is formed by merging the settings

of all templates within the group, taking into account their location. The table below lists the commands you can use when creating a UserGate NGFW template group.

Action	Command	Example of the command
Creating a group	`create ngfw groups name <group name> description <group description> templates [ <template name 1> ... <template name n> ]`	`realmadmin/ realm@nodename# create ngfw groups name example_group_1 description for_example_group templates [ example_template_1 ]`
Changing the name, description, and set of templates included in a group	`set ngfw groups <group name> name <new group name> description <new group description> templates [ <template name 1> ... <template name n> ]`	`realmadmin/ realm@nodename# set ngfw groups example_group_1 name example_group_2 description for_testing_group`
Adding templates included in a group	`set ngfw groups <group name> templates [ <template name 1> ... <template name n> ]`	`realmadmin/ realm@nodename# set ngfw groups example_group_2 templates [ example_template_2 ]`
Deleting templates included in a group	`delete ngfw groups <group name> templates [ <template name 1> ... <template name n> ]`	`realmadmin/ realm@nodename# delete ngfw groups example_group_2 templates [ example_template_2 ]`
Viewing a group	`show ngfw groups <group name>`	`realmadmin/ realm@nodename# show ngfw groups example_group_2`
Viewing all groups	`show ngfw groups`	`realmadmin/ realm@nodename# show ngfw groups`
Delete a group	`delete ngfw groups <group name>`	`realmadmin/ realm@nodename# delete ngfw groups example_group_2`

Once you have created template groups, you can add managed devices.

Adding UserGate NGFW Managed Devices

A managed device is a logical object created in a managed realm that corresponds to a real UserGate NGFW connected to UGMC. Each such object, when enabled, uses one managed device license.

Before adding a managed UserGate NGFW device, you must enable the **UserGate Management Center** service on the UGMC server in the properties of the zone to which UserGate NGFW is connected.

To do this, run the following command in the command line interface in configuration mode as the UGMC administrator:

```
set network zone <zone name> enabled-services [ Management ]
```

Example:

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

To add a UserGate NGFW managed device:

1) Create a device in the UGMC managed realm;

2) Connect UserGate NGFW to the managed device.

Creating a managed device

> **Note**
> **This instruction must be performed by the managed realm administrator in the UGMC command line interface in configuration mode.**

To create a managed device

1. Run the command:

   ```
   create ngfw devices <managed device parameters>
   ```

   Specify the managed device parameters.

Parameter	Description
`enabled`	State • `on`: enabled • `off`: disabled
`name`	Name
`description`	Description
`templates-group`	The name of the template group whose parameters should be applied to the managed device.
`sync-mode`	Parameter synchronization mode between a template group and a managed device: • `auto`: automatic sync; • `disabled`: the sync is disabled • `manual`: manual start of synchronization During synchronization, the template group's parameter configuration is applied to UserGate NGFW. Automatic mode is selected by default. In this mode, UserGate NGFW parameters are synchronized with the parameter configuration each time it changes. Synchronization can be disabled if necessary. This may be necessary, for example, if you need to simultaneously change the parameters of several template groups. In this case, you can apply all changes at once by manually synchronizing. Synchronization for all managed devices is performed by the `execute ngfw devices resync` command (available in version 7.4.0 and later).

Example:

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

2. Get the ID of the created managed device:

`show ngfw devices <managed device name>`

Example:

```
realmadmin/realm@nodename# show ngfw devices example_name

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

The managed device ID will appear in the command output in the `device-code` parameter. This ID will be needed to connect the UserGate NGFW firewall to the managed device.

Connecting UserGate NGFW to a Managed Device

You can connect UserGate NGFW to a managed device during the initial product setup, as well as during subsequent use (see instructions below).

> **Note**
>
> **This instruction is executed by the UserGate NGFW administrator in the command line interface in configuration mode.**

To connect UserGate NGFW to a managed device:

Run the command:

```
set settings general management-center mc-address <UGMC IP address>
device-code <managed device ID> enabled on
```

Example:

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

You can test the connection on the UGMC side.

> **Note**
> **This instruction must be performed by the managed realm administrator in the UGMC command line interface in configuration mode.**

To test the connection between UserGate NGFW and the managed device:

Run the command:

`show ngfw devices <managed device name>`

Example:

```
realmadmin/realm@nodename# show ngfw devices example_name
```

Connection parameters will be displayed in the command output.

UserGate NGFW Clustering

UserGate Management Center allows you to combine UserGate NGFW firewalls into a configuration cluster. Using device templates, you can apply the same settings to all nodes in this cluster. Additionally, in UGMC, you can create one or more failover clusters based on the nodes of a configuration cluster.

Creating a Configuration Cluster

To create a configuration cluster:

1. Perform initial configuration on the first cluster node.

2. Configure a zone on the first cluster node through whose interfaces cluster replication will be performed (see the Network Settings section of the UserGate NGFW Administrator's Guide). The `enabled-services` parameter must be set to the values `ha` and `Admin Console`, allowing access to the corresponding services.

3. Specify the IP address that will be used for communication between the first node and other cluster nodes (see the Cluster Settings section of the UserGate NGFW Administrator's Guide).

4. Generate a secret code for the first cluster node (see the Cluster Settings section of the UserGate NGFW Administrator's Guide).

5. Connect the first cluster node to UGMC as a managed device. When connecting to UGMC, each cluster node is assigned a unique identifier of the form `node_n`, where `n` is the node's serial number.

6. Add the second and subsequent nodes to the configuration cluster, performing the initial configuration on each node.

7. Configure cluster node settings. You can configure the settings locally on each node or configure the settings in UGMC templates.

Creating a HA Cluster

Configuration cluster nodes can be combined into a failover cluster that supports the following modes:

- "active-active": one of the firewalls operates as the master node that distributes the traffic among all other cluster nodes;
- "active-passive": one of the firewalls acts as the master node and processes the transit user traffic. The other firewalls act as the backup nodes, and they are ready to start processing the traffic.

Before creating a failover cluster, you need to check that:

- The configuration cluster is created.
- Network interfaces managed by UGMC are created on each cluster node. You can assign virtual IP addresses only to interfaces created in a template.
- The requirements are the same as those for nodes creating a failover cluster without UGMC (see the Clustering and High Availability section of the UserGate NGFW Administrator's Guide).

> **Note**
> **Before executing this instruction, a network zone template and a failover cluster template must be created. This instruction must be performed by the managed realm administrator in the UGMC command line interface in configuration mode.**

To create a HA cluster:

1. Enable the VRRP service for all network zones where you plan to add a clustered virtual IP address by running the following commands in sequence:

```
go ngfw-template <network zone template name>
```

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

Example:

```
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. Configure the failover cluster settings by running the following commands in sequence:

`go ngfw-template <failover cluster template name>`

`create settings device-mgmt ha-clusters <failover cluster settings>`

Specify the failover cluster settings.

Parameter	Description
`enabled`	State • `on`: enabled • `off`: disabled
`name`	Name
`description`	Description
`mode`	Mode of operation: • `active-active` • `active-passive`
`session-sync`	User TCP session synchronization mode: • `on`: the sync is enabled • `off`: the sync is disabled • `ha-cluster-id: <failover cluster identifier>`: If multiple failover clusters are created in a single configuration cluster, automatic session synchronization is performed using a multicast address (except for sessions using a proxy server).

Parameter	Description
	The failover cluster identifier is a unique value from 0 to 8 for each cluster.
`session-sync-all`	Synchronization mode for all user sessions: • `on`: the sync is enabled • `off`: the sync is disabled
`excluded-sync-ips`	IP addresses with which user sessions will not be synchronized.
`virtual-router-id`	Virtual Router ID (VRID). Unique for each VRRP cluster on the local network. If there are no 3rd party VRRP clusters in the network, it is recommended to keep the default setting
`nodes`	Configuration cluster nodes names to combine them into an HA cluster
`virtual-ips <virtual-ips-filter> <virtual-ip-info>`	Cluster virtual IP addresses and their assignment to network interfaces on cluster nodes. The `virtual-ips-filter` parameter can take the following values: • `new`: create a new virtual IP address; • `<IP address>`: modify an existing virtual IP address. The `virtual-ip-info` parameter can take the following values: • `ip` : assign a virtual IP address to an interface; • `ha-interfaces <cluster node name/interface name>`: select an interface on a cluster node.

UserGate Endpoints Management

For centralized UserGate endpoint management in the managed realm, you must create templates and template groups describing the endpoint settings, add the managed endpoints, and apply the previously created templates to them.

In the CLI interface, templates and template groups are created and the managed endpoints are added at the **endpoint** level.

Device Templates

To create an endpoint template, use the following command:

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

To edit an endpoint template name/description, use the following command:

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

To view previously created endpoint templates, use the following command:

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

To remove previously created endpoint templates, use the following command:

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

After creating an endpoint template, you can configure its settings. To do that, switch to the mode for setting template parameters of managed devices by running the following command:

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

When configuring template parameters, follow these rules:

1. If the value of a setting is not defined in the template, nothing will be sent to the managed device. In this case, the default setting will be used.

2. Libraries (e.g., IP addresses, URL lists, MIME content type lists, applications, etc.) have no predefined content in UGMC. To use libraries in filtering policies, you need first to add items to them.

3. It is recommended to create separate templates for different settings groups to avoid conflicts between settings when templates are combined into template groups and to make it easier to understand the final settings that will be applied to managed device.

When creating a template, the administrator can use sections such as "General Settings", "VPN Settings", and "Libraries".

General Settings

This section contains information on setting the general parameters of managed devices. To configure the parameters, use the following command:

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

The following parameters can be configured:

Parameter	Description
installation-settings	These are the settings that control the installation of UserGate client software: • **collect-ep-data**: collect information on the device (IP address, time of last connection to UGMC, user, computer name, OS version, UserGate Client software version, CPU load, RAM usage, running processes and services, etc.). Default value: enabled. If disabled, UGMC will only obtain the following information on the device: IP address, endpoint device name, UserGate Client software and Windows OS versions, current time, device boot time, CPU load, and RAM usage. Important! Disabling endpoint data collection affects how HIP profiles work. • **network-access**: configure access to the network when the UserGate Client software is stopped. Default value: enabled. • **firewall-access**: allow the user to disable content filtering on the endpoint device using the GUI. The options are: ◦ **off**: users are not allowed to disable content filtering. ◦ **on**: users are allowed to disable content filtering. ◦ **by code**: users are allowed to disable content filtering on entering a code. To allow a user to disable content filtering, you need to provide or generate a code that the client must enter on the device. You can also specify an expiration time for the code (code-expiration-date). In addition, when you allow the user to disable content filtering, you can specify how many times (number-of-

Parameter	Description
	shutdowns) and/or for how long (duration) the filtering will be disabled. Default value: on (filtering can be disabled for 10 minutes without entering a code). Important! If you use a counter for the number of times filtering can be disabled (Allowed number of shutdowns), note that the counter is reset each time you change any settings in the Allow user to disable firewall section. • **uninstall-access**: allow the user to uninstall the UserGate Client software. With the uninstall-code option, you need to provide or generate a code that the user must enter to be able to delete the software. Default value: enabled. **Important!** **These settings will not be applied if sync mode is not enabled (the sync on parameter). Otherwise, default values will be used.**
notification	Configure alerts: • **show-icons**: UserGate Client will display an icon in the taskbar notification area. • **notification-tooltips**: enable or disable sending notifications to the device. If notifications are disabled, the alerts will not display on the endpoint regardless of the settings for specific alert types (device added to/removed from quarantine, resource blocked). • **add-to-quarantine-message**: send an alert when a device is blocked. To configure the alert, specify the message text and alert type. The alert will be displayed in a pop-up window. • **remove-from-quarantine-message**: send an alert when a device is unblocked. To configure the alert, specify the message text and alert type. The alert will be displayed in a pop-up window. • **resource-blocked-message**: send an alert when an attempt to visit the URL of a resource was blocked. To configure the alert, specify the message text and alert type. The alert will be displayed in a pop-up window.

Parameter	Description
	Important! **These settings will not be applied if sync mode is not enabled (the sync on parameter). Otherwise, default values will be used.**
logan-device	Specify the LogAn server to which the device will send event information. The LogAn server must be already registered in UGMC. **Important!** **These settings will not be applied if sync mode is not enabled (the sync on parameter). Otherwise, default values will be used.**

VPN Settings

This section allows you to configure VPN security profiles that define settings such as the pre-shared key and encryption and authentication algorithms. The VPN settings are sent to the UserGate Client MD. The user can select the required VPN server for connecting in the initial GUI window.

Note

VPN connections can only be configured for devices that run Windows OS 10 and higher. After the connection is terminated, new connection attempts will be made over the next 40 seconds. If connection is not restored during this time, the user will be shown a VPN server selection window.

To configure the parameters, use the following command:

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

To configure a VPN connection, provide these settings:

Parameter	Description
enabled	Enable/disable a rule.
name	The name of the security profile for connecting to the VPN server.
descriptipon	Profile description.
vpn-address	Name (FQDN) or IP address of the VPN server. **Note** **When using FQDN for the connection, if the VPN server name corresponds to multiple IP addresses, the client connects to the first address that responds to requests.**
protocol	VPN protocols to create a tunnel: • **ipsec2**. Layer 2 Tunneling Protocol (L2TP) is used for creating tunnels and the IPsec protocol for protecting the data during transmission. • i**kev2-with-certificate**. The IKEv2 protocol is used to create a secure channel, and certificates are used for mutual authentication of the server and the client. **Important!** When generating a client certificate, you need to specify the CN field, i.e. the ID of the certificate user. • **ikev2**. IKEv2 protocol is used to create a secure channel, and login and password (EAP-MSCHAP v2) are used to verify the client. This method is available only for users of the domain RADIUS server.
ike-mode	IKE mode (you must specify it when the IPsec L2TP protocol is used): main, aggressive. The difference between the modes is that the aggressive mode uses fewer packets, which allows for quicker establishment of connections. The aggressive mode does not transmit some negotiation parameters and thus requires that they be configured identically at the opposite ends of the connection.
psk	This string must match on the client and server for a successful connection. For IPSec L2TP protocol.
Phase 1	

Parameter	Description
	In the first phase, IKE security is negotiated. The authentication is done using a pre-shared key in the mode selected earlier. Provide the following settings: • **phase1-key-lifetime**: the time period after which the parties re-authenticate and re-negotiate the first-phase settings. • **dpd-interval**: the state and availability of the neighboring devices is checked using the Dead Peer Detection (DPD) mechanism. DPD sends R-U-THERE messages periodically to check if the IPsec neighbor is available. Minimum check interval: 10 seconds; use 0 to disable the check. • **dpd-max-failures**: the maximum number of failed discovery requests to an IPsec neighbor after which the neighbor will be considered unavailable. • **dh-groups**: select the diffie-Hellman group that will be used for key exchange. Instead of the key itself, certain general information is transmitted that the DH key generation algorithm needs to create the shared secret key. The larger the Diffie-Hellman group number, the more bits are used to make the key secure. • **phase1-security**: the authentication and encryption algorithms are used in their listing order. To reorder the algorithms, drag and drop them with the mouse or use the Up/Down buttons.
Phase 2	In the second phase, the method for securing IPsec connections is selected. You need to specify the following: • **phase2-key-lifetime**. the time period after which the nodes must rotate the encryption key. The lifetime for the second phase is shorter than for the first one, which entails a more frequent key rotation. • **key-lifesize-enabled, key-lifesize**. the key lifetime can also be expressed in bytes. If both values (key-lifetime and key-lifesize) are set, the counter that first reaches the limit will trigger re-creating the session keys. • **phase2-security**: authentication and encryption algorithms.

Libraries of items

This section contains website addresses, IP addresses, applications, and other items used in the configuration of UGC managed device rules.

Configuration of libraries in endpoint templates occurs at the **libraries** level.

To create a list, use the following command:

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

To edit the previously created lists, use the following command:

```
realmadmin/realm@nodename# set libraries <parameters>
```

To view the previously created lists, use the following command:

```
realmadmin/realm@nodename# show libraries <parameters>
```

To delete the previously created lists, use the following command:

```
realmadmin/realm@nodename# delete libraries <parameters>
```

Services

The **Services** section contains a list of common services based on the TCP/IP protocol, such as HTTP, HTTPS, FTP, and others. These services can be used in UGC managed device rules. A predefined list of services is supplied with the product. The administrator can add the desired items during use.

To create service lists, use the following command:

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

The configured parameters include the name and description of the list, the required protocol, the destination port, and the source port.

Services Groups

The lists from the service library can be combined into groups. To create a service group, use the following command:

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

The command parameters include the name and description of the list, the required service lists, for example:

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

IP Addresses

The **IP addresses** section contains the list of IP address ranges that can be used in UGC managed device rules.

The administrator can add the desired items during use. To add a new IP address list, use the following command:

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

Provide the following parameters:

Parameter	Description
name	Address list name.
description	List description.
threat-lvl	Threat level: • **very-low**: very low threat level • **low**: low threat level • **medium**: medium threat level • **high**: high threat level • **very-high**: very high threat level.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format.

Parameter	Description
	Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
lists	Select existing IP lists to add to the list being created.
ips	IP addresses or a range of IP addresses to include in the list. Format: <ip>, <ip/mask>, or <ip_range_start-ip_range_end>.

To edit a list (parameters available to update are identical to those used to create a list), use the following command:

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

To add new addresses to a list, use the following command:

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

To delete an entire address list or individual IP addresses it contains, use the following commands:

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

To display information about all existing lists, use the following command:

```
realmadmin/realm@nodename# show libraries ip-list
```

To display information about an individual list, specify the IP address list name:

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

To display the contents of an IP address list, use the following command:

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

Application Groups

The **Application Groups** library item allows you to create application groups for more convenient use in network traffic filtering rules.

The UserGate Client software recognizes the application by its checksum, which enables the administrator to control network access for specific applications in a very precise and selective fashion — for example, allow only a specific application version to access the network and block all other versions.

To add a new application group, use the following command:

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

Provide the following parameters:

Parameter	Description
name	Address list name.
description	List description.
threat-lvl	Threat level: • **very-low**: very low threat level • **low**: low threat level • **medium**: medium threat level • **high**: high threat level • **very-high**: very high threat level.

Parameter	Description
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
apps	The name (**name**) and the checksum (**hash**) of the application. The checksum for a Windows executable must be computed using the SHA1 algorithm — e.g., using the fciv utility.

To edit an application group, use the following command:

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

To add new applications to the list, use the following command:

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

To delete an entire address list or individual IP addresses it contains, use the following commands:

```
realmadmin/realm@nodename# delete libraries application-groupst <group-
name>
```

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

To display information about all existing lists, use the following command:

```
realmadmin/realm@nodename# show libraries application-groups
```

To display information about an individual list, specify the IP address list name:

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

To display the contents of an IP address list, use the following command:

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

URL Lists

The URL lists section allows you to create URL lists to be used as black and white lists in content filtering rules.

You configure URL lists at the **libraries url-list** level.

To add a new URL list, use the following command:

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

Specify the following parameters:

Parameter	Description
name	URL list name.
description	URL list description.
type	List type: • **local**: local

Parameter	Description
	• **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
urls	URLs to add to the list.
case-sensitivity	Case sensitivity in URL writing: • **sensitive**: sensitive to the case of letters in the address • **insensitive**: insensitive to the case of letters in the address • **domain**: list of domain addresses

To edit the URL list, use the following command:

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

The parameters for which values are available to update are listed in the table above.

To delete an entire URL list or individual URLs from it, use the following commands:

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

To display information about all URL lists, a specific URL list, or about the addresses from a specific list, use the following commands:

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

URL Categories

The **URL categories** library item allows you to create UserGate URL Filtering category groups for more convenient use in content filtering rules. For example, the administrator can create a category group called "Business categories" and place the desired categories there.

This section is located at the **libraries url-categories** level.

To create a URL category group, use the following command:

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

You need to specify the following parameters:

Parameter	Description
name	URL category group name.
description	Group description.
categories	URL categories to add to the group.

To edit group parameters, use the following command:

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

To add URL categories to an existing group, use the following command:

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

To delete a URL category group, use the following command:

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

To delete individual categories from a group, use the following command:

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

To display information about all URL category groups, use the following command:

```
realmadmin/realm@nodename# show libraries url-categories
```

To display information about an individual URL category group, use the following command:

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

To display a list of URL categories in a group, use the following command:

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

Content type

Using content type filtering, you can control the video and audio content, images, executables, and other content types.

Content types section is located at the **libraries content-types** level.

To add a new content type list, use the following command:

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

Specify the following parameters:

Parameter	Description
name	Content type list name.

Parameter	Description
description	List description.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
mime	Content types to add to the list. A list of content types and their descriptions can be found at this link: https://www.iana.org/assignments/media-types/media-types.xhtml.

To edit the list, use the following command:

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

The parameters available to update are listed in the table above.

To delete a content type list, use the following command:

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

To delete individual content types from the list, use the following command:

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

To display information about the content type lists, use the following commands:

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

To display content types included in a list, use the following command:

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

Time Sets

The Time sets section allows you to define time intervals that can later be used in rules. The administrator can add the desired items during use.

This section is located at the **libraries time-sets** level.

To create a group, use the following command:

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

Provide the following parameters:

Parameter	Description
name	Group name.
description	Group description.
time-set	• **interval-name**: repetition interval name. • **type**: repetition interval type: ◦ **daily**: daily: ■ **time-from**: start time (format: HH:MM). ■ **time-to**: end time (format: HH:MM). ■ **all-day on**: all day.

Parameter	Description
	◦ **weekly**: every week: ■ **time-from**: start time (format: HH:MM). ■ **time-to**: end time (format: HH:MM). ■ **all-day on**: all day. ■ **days [Mon | Tue | Wed | Thu | Fri | Sat | Sun]**: days of the week. ◦ **monthly**: every month: ■ **time-from**: start time (format: HH:MM). ■ **time-to**: end time (format: HH:MM). ■ **all-day on**: all day. ■ **days**: days of the month from 1 to 31. ◦ **fixed**: one time: ■ **time-from**: start time (format: HH:MM). ■ **time-to**: end time (format: HH:MM). ■ **all-day on**: all day. ■ **fixed-date**: desired date (format: YYYY-MM-DD). ◦ **span**: repeating events: ■ **time-from**: start time (format: HH:MM). ■ **time-to**: end time (format: HH:MM). ■ **all-day on**: all day. ■ **fixed-date-from**: start date (format: YYYY-MM-DD). ■ **fixed-date-to**: end date (format: YYYY-MM-DD). ◦ **range**: date range: ■ **time-from-enabled <on | off>**: enable/disable setting the interval start date. ■ **fixed-date-from**: start date (format: YYYY-MM-DD). ■ **time-from**: start time (format: HH:MM). ■ **time-to-enabled <on | off>**: enable/disable setting the interval end date. ■ **fixed-date-to**: end date (format: YYYY-MM-DD). ■ **time-to**: end time (format: HH:MM).

To edit a time set, use the following command:

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

The parameters available to update are listed in the table above.

To edit an interval specified for a time set, use the following command:

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

The new values are then specified as follows; <time-set-filter> — filter for interval current values.

To add a new item to an existing group, use the following command:

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

To delete a group of items, use the following command:

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

To delete an item from a time set, use the following command:

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

To display information about all time sets, use the following command:

```
realmadmin/realm@nodename# show libraries time-sets
```

To display information about an individual time set, use the following command:

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

To display information about group items with the same repeat type, use the following command:

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

Template Groups

Template groups allow multiple templates to be combined into a single configuration that applies to a managed device. The final settings that will apply to a device are generated by merging all settings specified in the templates of a template group based on their location in the group.

To create an endpoint template group, use the following command:

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

To edit an endpoint template group, use the following command:

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

To view previously created endpoint template groups, use the following command:

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

To remove previously created endpoint template groups, use the following command:

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

You can remove the templates from the template group created earlier:

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

Placing UGC Endpoints under UGMC Management

To manage devices, you need to add them to UGMC. UGC endpoints can be added in two ways:

1. Adding one UGC endpoint at a time. Suitable for companies with only a few UGC managed devices.

2. Bulk addition of devices, suitable for companies with a larger number of devices.

Adding one device at a time

1. On the UGMC server, allow the **Endpoints control** service in the access control settings of the zone to which the managed device is connected.

2. Create the record for the UGC endpoint in UGMC.

3. Get the unique code for the new device.

4. Install the UGC software on the specific user device (computer).

To allow the **Endpoints control** service in the access control properties of the zone to which the managed device is connected, use the following command in UGMC administrator mode:

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

To create an entry for a UGC endpoint, use the following command:

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

Provide the following settings:

Parameter	Description
enabled	Enables the UGC managed device object .
licensed	

Parameter	Description
	Endpoint licensing: on/off. If the parameter is on, the endpoint uses one license. If there is no license, the endpoint will not be able to connect to the UGMC. If the parameter is set to off after registering the device with UGMC, then: • firewall rules earlier received from the MC continue to work; • VPN connection with settings previously received from the MC is available; • The endpoint does not receive new settings from the MC.
name	The name of the UGC managed device. The name can be arbitrary.
description	The description of the UGC managed device.
templates-group	The templates group whose settings should be applied to this UGC managed device. The settings (policies) will be applied after synchronization with UGMC.
sync-mode	The synchronization mode: **disabled**, **auto**, or **manual** sync.

To get the unique code of the created device (**device-code**), use the following command:

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

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

To install the UGC software on the user computer, follow the instructions in the UserGate Client Software Installation section.

Bulk addition of devices

1. On the UGMC server, allow the **Endpoints control** service in the access control settings of the zone to which the managed device is connected.

2. Create a code for the device group.

3. Get the unique code for the device group.

4. Install the UGC software on the specific user device (computer).

To allow the **Endpoints control** service in the access control properties of the zone to which the managed device is connected, use the following command in UGMC administrator mode:

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

To create a code for the endpoint group, use the following command:

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

Provide the following settings:

Parameter	Description
enabled	Enables the UGC managed device object .
name	The name of the UGC managed device. The name can be arbitrary.
description	The description of the UGC managed device.
group	The templates group whose settings should be applied to this UGC managed device. The settings (policies) will be applied after synchronization with UGMC.

To get the unique code of the device group (**device-code**), use the following command:

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

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

To install the UGC software on the user computer, follow the instructions in the UserGate Client Software Installation section.

To start the synchronization of all managed devices' settings manually, run a specific command (available starting from version 7.4.0):

```
realmadmin/realm@nodename# execute endpoint devices resync
```

HIP Objects

HIP objects allow you to configure compliance criteria for endpoint devices and can be used as conditions in security policies.

To create a HIP object, use the following command:

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

Provide the following settings:

Parameter	Description
name	The name of the HIP object.
description	(Optional) description of the HIP object.
os-version	The version of the operating system on the user device. When using the = and != operators, specify the full version of Windows.
ug-client-version	The version of the UserGate client software.
security	Endpoint security component statuses: • firewall • virus-protection • automatic-update • bitlocker.

Parameter	Description
	Important! BitLocker is considered enabled if it is enabled on at least one of the disks.
products	Conformance check of the software installed on the endpoint: • antimalware. Conformance check of the antimalware software on the user device: ◦ enabled: check the software status ◦ database-updated: checking database relevance (yes, no, or do not check) ◦ software version ◦ vendor: the vendor and product name • firewall. Conformance check of the firewall on the device. You need to specify the following parameters: ◦ installed: check if the software is installed ◦ enabled: check the software status (yes, no, or do not check) ◦ software version ◦ vendor: the vendor and product name; • backup. Conformance check of the backup software: ◦ installed: check if the software is installed ◦ software version ◦ vendor: the vendor and product name • disk-encryption. Checking the disk encryption programs installed on the endpoint device: ◦ installed: check if the software is installed ◦ software version ◦ vendor: the vendor and product name • dlp. Conformance check of the data leak protection system on the device: ◦ installed: check if the software is installed ◦ software version ◦ vendor: the vendor and product name • patch-management. Check for current updates. ◦ installed: check if the software is installed ◦ software version ◦ vendor: the vendor and product name
processes	Check the processes running on the device.
running-services	Check the services running on the device.

Parameter	Description
registry-keys	Microsoft Windows registry key is a registry where OS settings and parameters are stored. The following types of registry values are supported: • REG_SZ: a null-terminated Unicode or ANSI string. • REG_BINARY: binary data of any form. • REG_DWORD: a 32-bit number The following registry keys can be checked: • HKEY_LOCAL_MACHINE • HKEY_USERS Important! The path specification begins with a backslash (\), such as \HKEY_LOCAL_MACHINE, followed by the full registry path with backslash (\) used as the separator. For a description of the various registry keys, refer to the Microsoft documentation (https://docs.microsoft.com/en-us/troubleshoot/developer/webapps/iis/general/use-registry-keys).
installed-updates	Check that a specific update is installed on the device. The Microsoft Knowledge Base (KB) article number must be specified, e.g., KB5013624.

HIP Profiles

An HIP profile is a set of HIP objects used to check if the device meets the security (compliance) requirements. You can use an HIP profile to configure flexible policies for access to a network zone or application.

To create a HIP profile, use the following command:

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

Provide the following settings:

Parameter	Description
name	HIP profile name.
description	(Optional) description of the HIP profile.
hip-objects	

Parameter	Description
	Select a Boolean operator (and, or, and-not, or-not) and HIP objects here. For more details on object creation, see the HIP Objects section.

LogAn Device Management

For centralized LogAn device management in the managed realm, you must create templates and template groups describing the LogAn settings, add the managed LogAn devices, and apply the previously created templates to them.

In the CLI interface, templates and template groups are created and the managed LogAn devices are added at the **logan** level.

Device Templates

To create a LogAn device template, use the following command:

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

To edit a LogAn device template name/description, use the following command:

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

To view a previously created LogAn device template, use the following command:

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

To delete a previously created LogAn device template, use the following command:

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

After creating a LogAn device template, you can configure its settings. To do that, switch to the mode of setting parameters for the template of LogAn managed devices by running the following command:

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

In the template parameter setting mode, the same commands for setting LogAn parameters are available as those defined in the Command Line Interface section of the LogAn Administrator Guide.

When configuring templates, follow these rules:

1. If the value of a setting is not defined in the template, nothing will be sent to LogAn. In this case, LogAn will use the default setting or a setting configured by a local administrator.

> **Note**
> **The setting will be overridden when this setting is changed by the realm administrator in the LogAn template on UGMC.**

2. If the value of a setting is specified in the template, it will override the value assigned to the same setting by a local administrator.

After receiving the settings from UGMC, the settings for the following sections can be changed locally on Log Analyzer:

- general device settings;
- network interface settings.

3. When configuring network interfaces, the first configurable physical interface is **port1**. The **port0** interface is not available for configuration from UGMC; it is always configured by a local administrator and required for primary communication between the managed device and UGMC.

4. When configuring network interfaces, you can create an interface and delegate its configuration to a local administrator. To achieve that, turn on the **on-device** (**on-device on**) parameter in the network interface settings.

5. Libraries (e.g., IP addresses, URL lists, content types, etc.) have no predefined content in UGMC, unlike the default libraries created on UserGate devices. To use libraries in UGMC policies, you need first to add items to them.

6. It is recommended to create separate templates for different settings groups to avoid conflicts between settings when templates are combined into template groups and to make it easier to understand the final settings that will be applied to UGC

managed devices. For example, you can create separate templates for network settings, libraries, etc.

Template Groups

Template groups allow multiple templates to be combined into a single configuration that applies to a managed device. The final settings that will apply to a device are generated by merging all settings specified in the templates of a template group based on their location in the group.

To create a LogAn template group, use the following command:

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

To edit a LogAn template group, use the following command:

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

To view a previously created LogAn template group, use the following command:

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

To remove previously created LogAn template groups, use the following command:

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

You can remove the templates from the template group created earlier:

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

Placing LogAn Devices under UGMC Management

A template group always applies to one or more LogAn devices. To add managed LogAn devices to UGMC, follow these steps:

1. Provide access from the managed LogAn devices to UGMC. To do that, on the UGMC, allow the **Management** service in the access control properties of the zone, to which the managed devices are connected.

2. Create a managed LogAn device object.

3. Link the LogAn managed device object just created to a real UserGate LogAn device.

To provide access from the managed LogAn devices to UGMC, run the following command in the UGMC administrator mode:

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

To create a managed device object, use the following command:

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

Provide the following settings:

Name	Description
enabled	Enables the managed device object. When enabled, the managed device object takes up one license.
name	The name of the managed device. The name can be arbitrary.
description	Managed device description.
templates-group	The templates group whose settings should be applied to this managed device.
sync-mode	Select the mode used to synchronize the template group settings with the device. There are three options: • **auto**: automatic sync. A change to any setting in any template of the template group applied to the managed device is propagated immediately to the managed device.

Name	Description
	• **disabled**: sync mode is disabled. • **manual**: in this sync mode the settings are applied once upon a sync request.

To enable LogAn-to-UGMC communication for an already configured LogAn device, follow these steps:

1. Get the device code.

2. Specify the IP address of the UGMC server and enter the unique device code

To display the code of the created managed device object (**device-code**), run the following command:

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

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

In the LogAn managed device console, add the IP address of the controlling UGMC and specify the code of the created managed device object:

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

To check the connection on the UGMC side, run the command for displaying the managed device:

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

To start the synchronization of all managed devices' settings manually, you must run a specific command (available starting from version 7.4.0):

```
realmadmin/realm@nodename# execute logan devices resync
```

Update Management for Managed Devices

UGMC allows you to create a centralized policy for updating the UserGate software (UGOS) and updatable libraries provided on subscription.

> **Note**
> **After adding a UserGate LogAn to UGMC management, the UserGate device starts automatically downloading all updates from the UGMC server.**

Software Updates

To install updates, follow these steps:

1. Upload the updates to the UGMC repository. To manage uploading updates to the UGMC repository, use the following command:

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

For more detailed information, refer to the General Settings section of the UGMC Administrator Guide.

2. Approve the update for all or specific devices:

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

3. Install the update. After an update is approved, it becomes available for downloading for all managed devices or for a group of them. A managed device downloads the update according to its update check schedule. When downloaded, the update can be installed centrally by the administrator from the UGMC console or manually on a specific managed device by the device's administrator.

Libraries Updates

Libraries are updatable resource databases (URL filtering categories, IPS signatures, IP address lists, URLs, MIME types, morphological databases etc.) provided to UserGate customers on a subscription basis. These updates are uploaded to the UserGate repository from where they can then be downloaded to UserGate LogAn.

If LogAn is managed from UGMC, it checks automatically for available updates on the UGMC server which acts as a repository. The UserGate repository is used in this case by the UGMC server for obtaining new updates. By default, UGMC checks for and downloads library updates automatically.

Libraries stored in the UGMC repository are available to all UserGate MDs. A managed device downloads the update automatically according to its update check schedule.

To configure downloading updates to the UGMC from the UserGate repository, use the following command:

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

ADMIN

General Information

This section allows registered administrators to change their passwords, update some profile settings and log out.

Name	Description
Change password	To change your password, enter your current password and then the new one twice.
Preferences	• Show items per page: number of lines to display in one dialog box, such as a list of firewall rules. • Night mode: set the dark theme for the UGOS GUI.
Logout	End the session in the web console of the device.

FAVORITES

Favorites (Description)

The web interface allows you to filter the displayed sections by adding them to favorites and search for sections by their name. You can use filtering to hide unused sections. Displaying only the favorite sections does not affect the device functionality or configuration. To add a section to favorites, click the asterisk next to the section name. To customize the display, use the **Favorites Only** switch at the bottom of the panel.

Managed device templates of the realm management console (**NGFW → Configuration**, **Endpoints → Configuration**, **LogAn → Configuration** desktops) can also display only the sections in which the settings were made.

APPLICATIONS

Network Environment Requirements

Service	Protocol	Port	Outbound/ Inbound	Function
Web console	TCP	8010	Inbound (to the UserGate Management Center web console)	Access to the management web interface of a device.
	TCP	8300	Inbound (to the web console of a UserGate NGFW connected to UGMC)	Access to the web management interface of a UserGate NGFW connected to UGMC.
CLI over SSH	TCP	2200		

Service	Protocol	Port	Outbound/ Inbound	Function
			Inbound (to CLI over SSH)	Access to the UserGate command line interface (CLI) over SSH.
XML-RPC	TCP	4041	Inbound (to UserGate via API)	UserGate device management via API.
Remote assistance	TCP	22	Outbound (to technical support servers)	Remote access to a technical support server. Access to servers: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.
NTP	UDP	123	Outbound (to a time server)	Time synchronization.
DNS	UDP	53	Outbound (from UserGate to a DNS server)	The service that resolves domain names into IP addresses.
UserGate server registration	TCP	443	Outbound (to the registration server)	Access to the UserGate product registration server (reg2.usergate.com).

Service	Protocol	Port	Outbound/ Inbound	Function
Update software and libraries	TCP	443	Outbound (to update servers)	Update software and library items: access to updates.usergate.com.
Replicate settings	TCP	4369	Inbound (from the first cluster node to the second and subsequent nodes)	This service is required for the configuration cluster to work. Set up a control connection.
		9000-9100	Inbound (receive configuration from the first cluster node)	Transmit information about cluster configuration changes (replicate settings).
UserGate Management Center service	TCP	9712	Inbound (to UGMC from NGFW)	Initial communication setup and encryption key exchange between the managed devices and the UserGate Management Center server.
		2022	Inbound (to UGMC from NGFW)	Build an SSH tunnel to exchange data using the received keys.

Service	Protocol	Port	Outbound/ Inbound	Function
Endpoints control (starting from version 7.1.0)	TCP	9712	Inbound (to UGMC from UG Client)	Initial communication setup and encryption key exchange between the UserGate Client managed devices and the UserGate Management Center server.
		4045	Inbound (to UGMC from UG Client)	Build an SSL tunnel to exchange data using the key received during the initial communication setup.
		22000-22711	Inbound (to UGMC from UG Client)	Transmit logs and telemetry data from UG Client to UG LogAn via the UGMC.
LDAP	TCP	389, 636	Outbound (to LDAP connector)	Execute LDAP requests (389 for LDAP and 636 for LDAP over SSL).
SNMP	UDP	161	Inbound (to UserGate)	Access to the UserGate server via SNMP.
SMTP	TCP	25		Send alerts to email.

Service	Protocol	Port	Outbound/ Inbound	Function
			Outbound (to the mail server)	
DHCP	UDP	67, 68	Outbound (IP address request from UserGate to a DHCP server)	DHCP service.
FTP (log export) (starting from version 7.1.0)	TCP	21	Outbound (to an FTP server)	Export logs to an FTP server.
SSH (log export) (starting from version 7.1.0)	TCP	22	Outbound (to an SSH server)	Export logs to an SSH server.
Syslog (log export) (starting from version 7.1.0)	TCP/UDP	514	Outbound (to the Syslog server)	Export logs to a Syslog server.
Manual site checking by category	TCP	80/443	Outbound (to updates.usergate.com)	Manual site checking by category.

Description of Log Formats

Event Log Format

CEF

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7

Field type	Field name	Description	Example value
	Source	Log type.	events
	Origin	Module where the event occurred.	admin_console
	Severity	The severity of the event.	Available values: • 0: info • 6: warning • 8: error • 10: critical
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	mc_core@einerson stal
	suser	The username.	Administrator (Admin)
	cat	Component where the event occurred.	console_auth
	act	Event type.	administrator_login
	src	Source IPv4 address.	192.168.117.254
	cs1Label	This field is used for event details.	Attributes
	cs1	Event details in JSON format.	{"login":"ex_admin", "realm_id":"31d8fcb6-e51d-4e3f-b799-181d31a45b06"}

JSON

Field name	Description	Example value
user	The username.	Admin
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
ip_address	IPv4 address of the event source.	192.168.174.134
node	The unique name of the device that generated the event.	mc_core@einersonstal
attributes	Event details in JSON format.	{"rule":{"logrotate": 12,"attributes": {"timezone":"Asia/ Dubai"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}
event_type	Event type.	logexport_rule_updated
event_severity	The severity of the event.	info, warning, error, or critical
event_origin	Module where the event occurred.	core
event_component	Component where the event occurred.	console_auth