Management Center 7.1.0 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 product that allows you to control a large number of managed devices. A managed device can be a UserGate Next-Generation Firewall, a UserGate LogAn data collection and analysis device.

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. Подробнее о лицензировании смотрите в главе Лицензирование UserGate Management Center.
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.
Configure 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. При этом администраторы UGMC ограничены только возможностью управления сервисами UGMC (смотрите главу Настройка UserGate Management Center), не

имея доступа к управлению областями. 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). Администраторы области ограничены только возможностью управления своей областью (смотрите главу Управляемые области), не имея доступа к управлению другими областями или сервисами UGMC. 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:

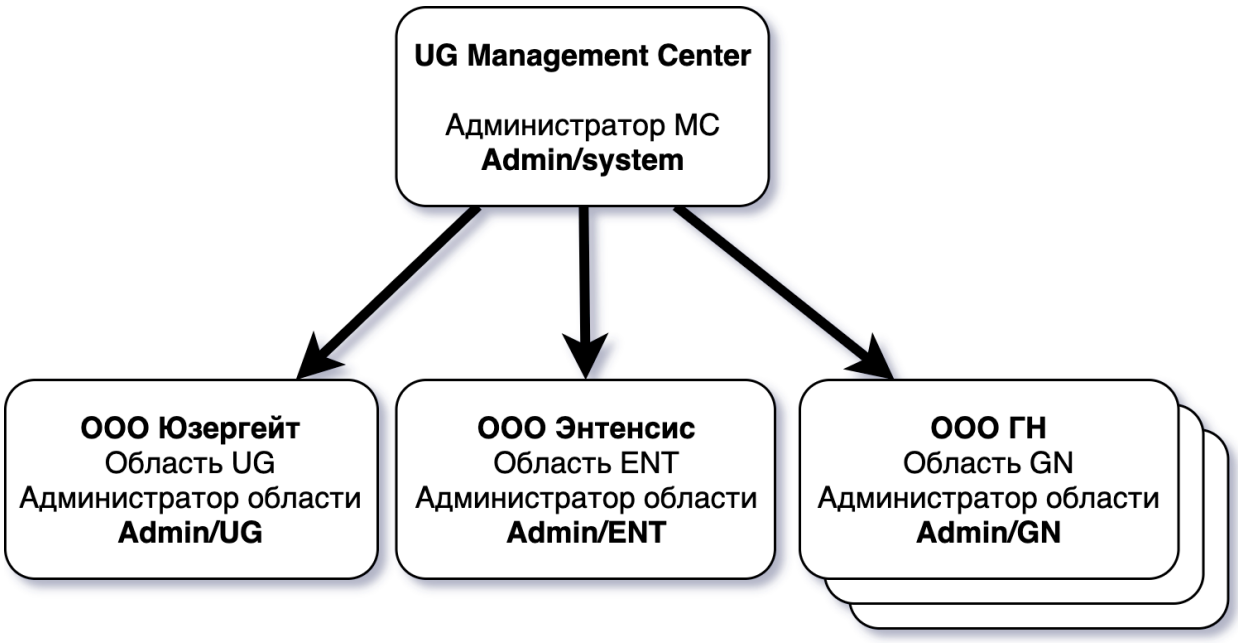
Administrator	Administrator Profile	Access level
Admin/realm_code	Root profile	Full. Administrators and their profiles are created by the UGMC administrator.
AdminRO/realm_code	ReadOnly	View-only access to all realm settings; no modification rights.
AdminTemplates/ realm_code	Templates	Create and modify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

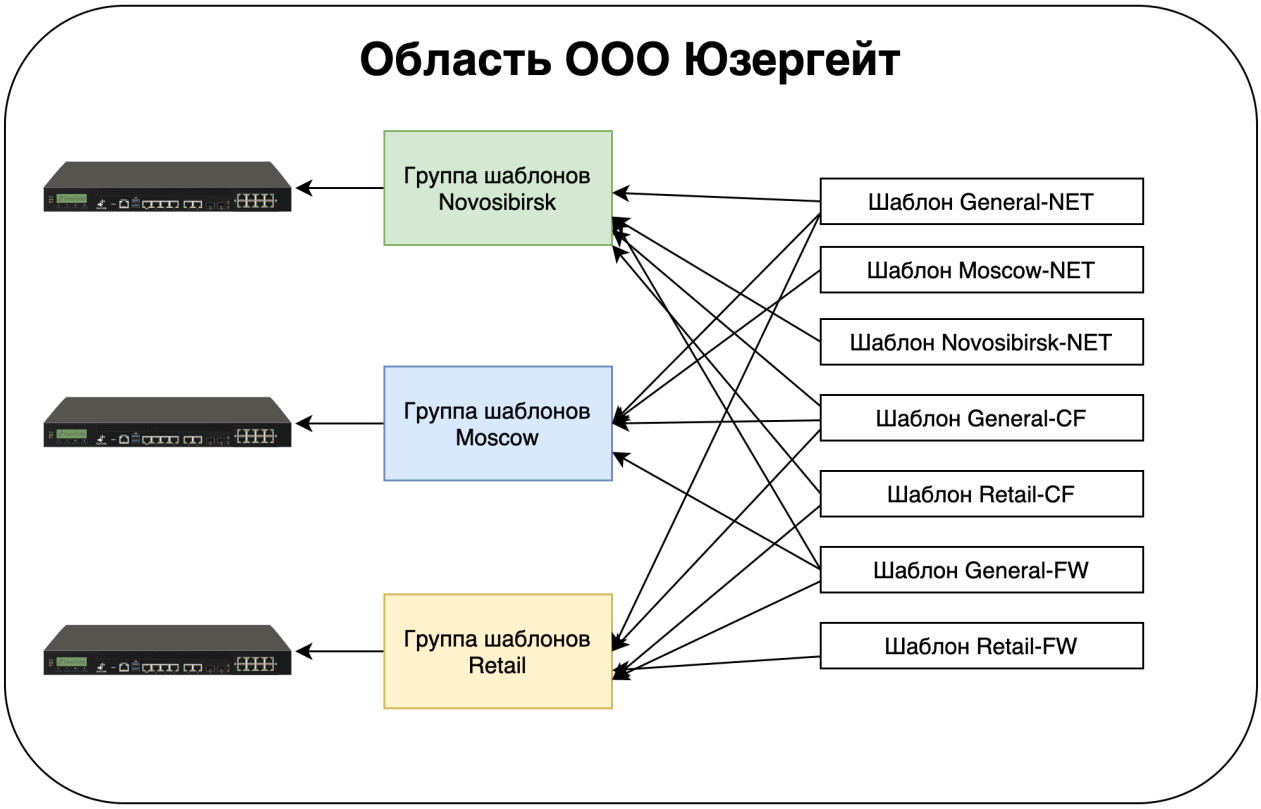
Settings for UserGate device parameters are made within a managed realm using templates and template groups.

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:

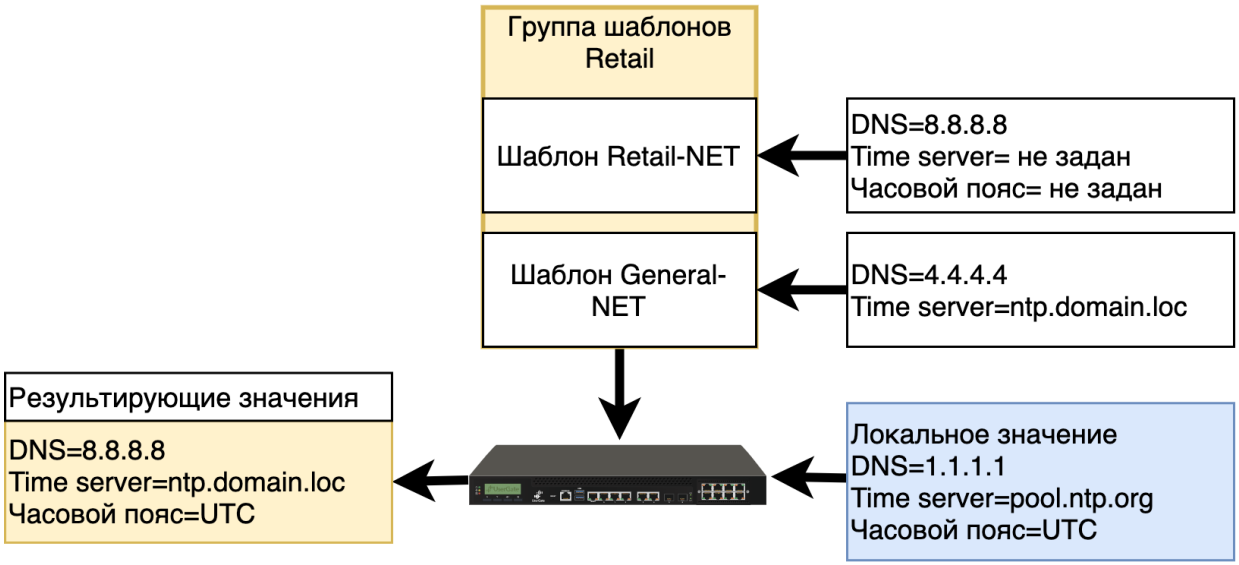
- Parameter settings, such as IP addresses of DNS servers.

- 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.

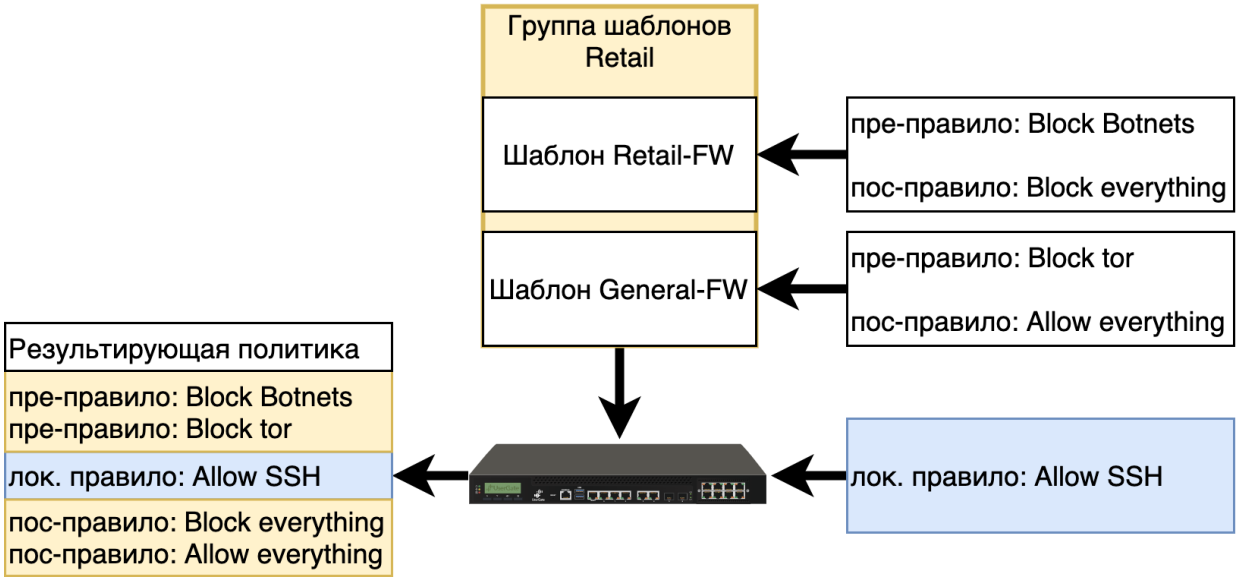
If the values in different templates of the same template group conflict, the value from the uppermost template applies. Local settings for this parameter are ignored.

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.

Версия UGMC	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.

Версия UGMC	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.

Версия UGMC	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;
- FW 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.

Software Updates

UserGate Software Updates

Note

Please note that to switch from versions 6.1.X and 7.0.X to 7.1.0, you will need to export the configuration from the current version.

Name	Description
Step 1. Settings export.	Export the configuration using standard tools in the current version. In the Device management section, click Settings export --> Export and select Export all settings or Expo rt network settings. Create a backup of the current system state.

Name	Description
Step 2. Install the software version.	Install the UserGate version by performing a clean installation.
Step 3. Settings import.	Import the previously saved configuration. In the Device management section, click Settings export --> Import and specify the location of the settings file created earlier. The settings will be applied to the server, after which the server will reboot.

When importing the configuration to version 7.1.0, keep in mind the following:

1. **Firewall rules** that contained **L7** will be forced off, they will have *action = accept* set and the created **L7 profile** will be added. Profiles will be created based on the rules, filters for each application group will be added to these profiles according to the following rules:
    - for the group "All" — *"Any signatures"* filter,
    - for category groups — filter *"category = category name or number"*,
    - for custom groups — filter including signature IDs as *"id IN (...)"*.
2. **IPS profiles** will be converted to the new format during import, new profiles will have one filter *"id IN (...)"*, which will include all IPS signature IDs from the old version of the IPS profile.
3. **You cannot import IPS rules**. The user must reconfigure IDPS himself after the import operation is complete using the new IPS profiles and firewall rules.
4. After importing the IPS and application signatures, you are **required** to run the IPS and application signature update.

UGMC LICENSING

UGMC Licensing

UGMC is licensed by the 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.

A UGMC license grants the right to use the product forever.

The following modules can be additionally licensed:

Name	Description
Security Update (SU) Module	The SU module grants the right to receive: • UGMC software updates • IPS signature updates • L7 application signature updates • Access to compliance library updates. The module is licensed as an annual subscription. After one year, you will need to renew the license to continue receiving updates.
Cluster Module	The module includes a subscription to allow UserGate devices to operate in cluster mode.
Endpoints module	The module includes work with endpoints with UserGate Client software installed, which is one of the components of the UserGate SUMMA ecosystem. Subscription to the module allows to: • Centrally manage the endpoints and their access to the network (except for compliance access control) from the UGMC console. • Collect the endpoint telemetry and security events. The module is perpetual and is issued according to the number of licensed managed endpoint devices.
Network access control at the host level module	An add-on module to the **Endpoints** licensing module. The subscription to the module includes: • Endpoint device security (compliance) validation. • Control of access to the network at the host level based on the results of the check. The module is issued for 1 year. 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 register the product, follow these steps:

Name	Description
Step 1. Go to the Dashboard.	In the console administration section, click the **Dashboard** icon in the top right corner.
Step 2. Register the product in the **License** section.	In the **License** section, click **No license**, enter the PIN code, and complete the registration form.

You can view the status of the installed license in the console administration section: see the **License** widget in the **Dashboard** subsection.

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.

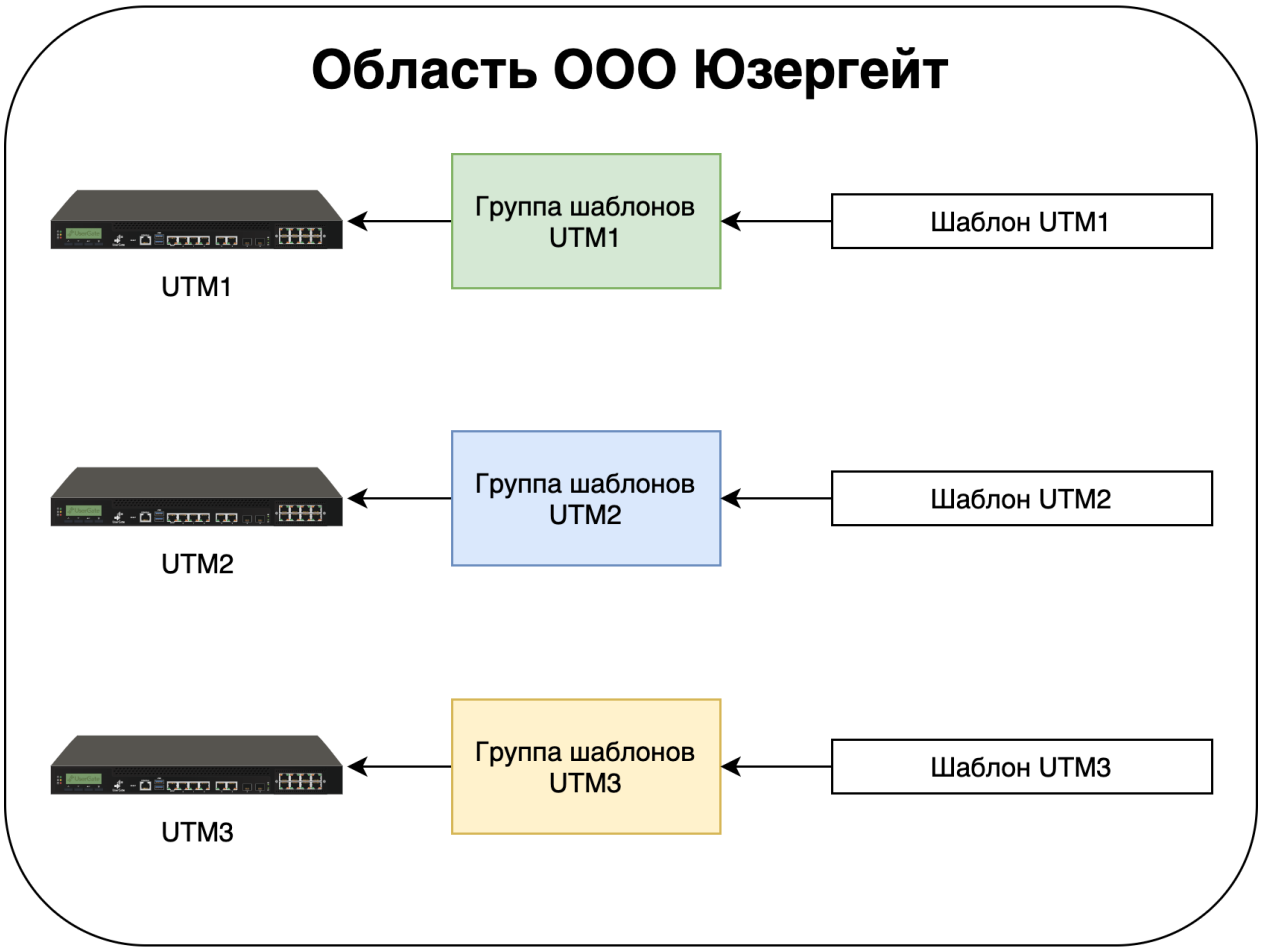
- Bear in mind the rights of local administrators. If you intend to have local administrators, their rights will be restricted by settings configured outside of UGMC templates, and any rules created by local administrators are always placed between pre- and post-rules applied from UGMC.

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.

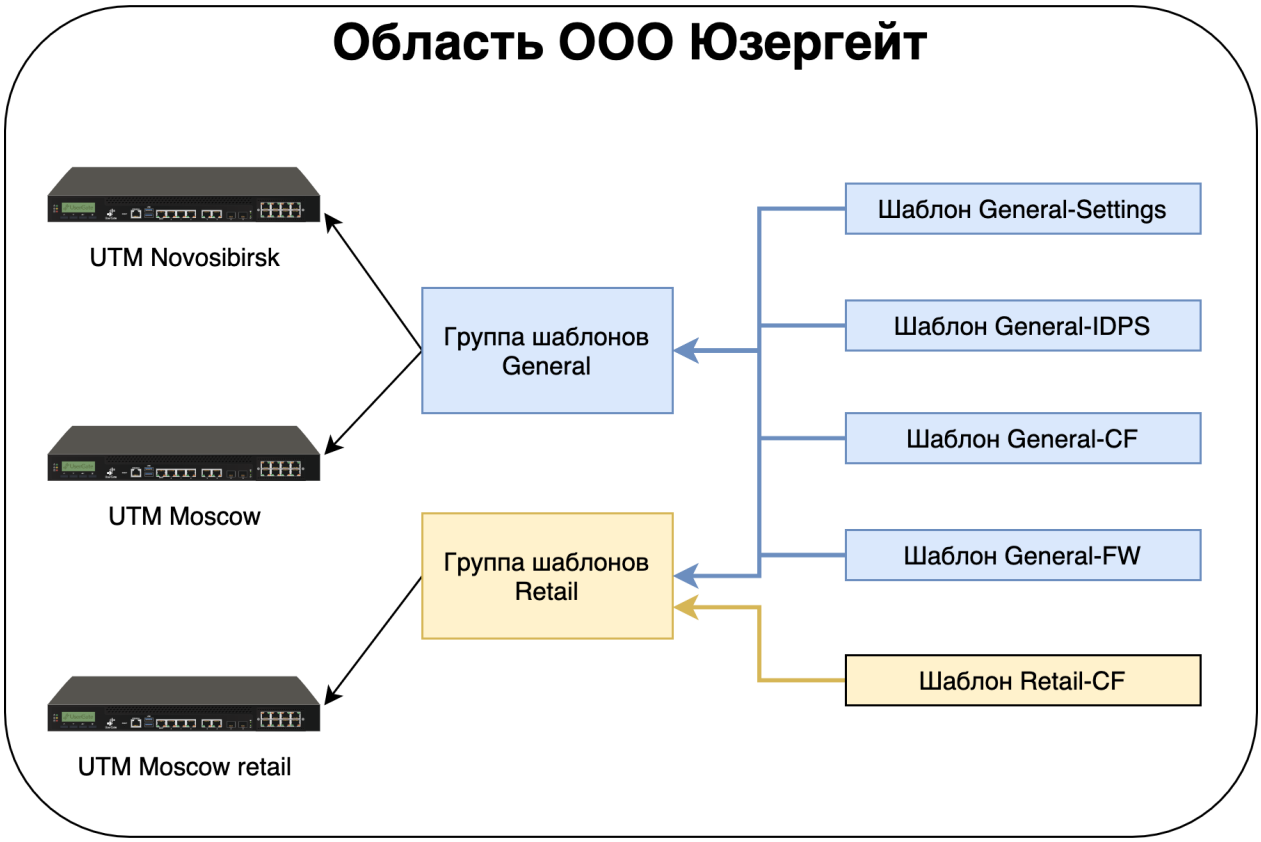
This scenario is recommended for simple implementations with a small number of UserGate NGFWs. An example configuration is shown in the figure below.



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

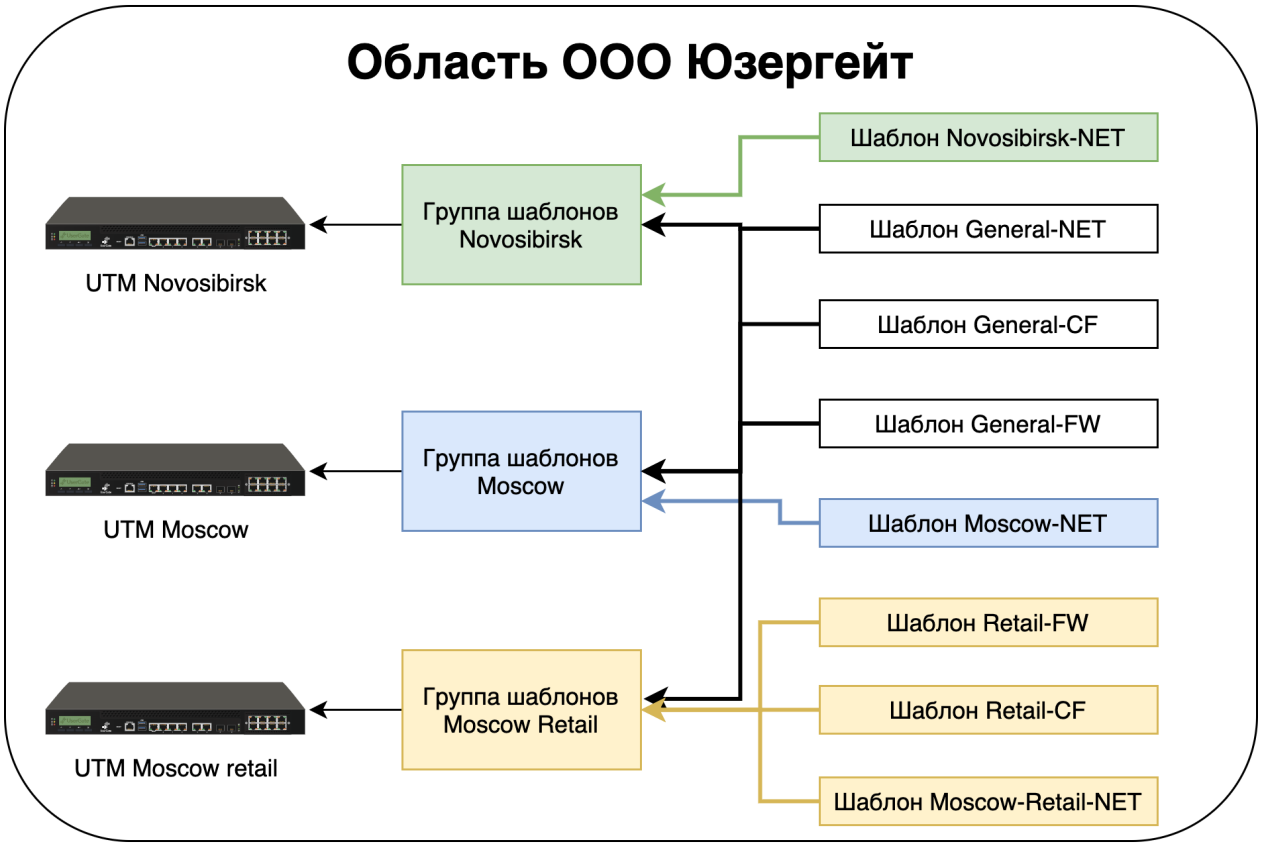
General-FW Template: the global firewall policies

- 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. Перейдите к главе Подключение к UGMC для дальнейшей настройки.

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.**

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.

Name	Description
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* as the login and *usergate* as the password for accessing the CLI.

Other network interfaces are disabled and require further configuration.

To perform the initial configuration, follow these steps:

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

Name	Description
	console will display the IP address to connect to for subsequent product activation. **Static IP address** Start UGMC. Use the CLI 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.
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.

Name	Description
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. Более подробно о лицензировании продукта читайте в главе Лицензирование UGMC.
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. Для выполнения таких операций необходимо во время загрузки сервера выбрать раздел меню **Support menu** и затем одну из требуемых операций. 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	

Name	Description
	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.
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**: allows time setting on the server. The UTC timezone should be used.
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
Шаг 1. Выполнить первоначальную настройку на первом узле кластера.	See the Initial Configuration chapter.
Шаг 2. Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера.	В разделе **Зоны** создать выделенную зону для репликации настроек кластера. 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 of the **Cluster configuration** window, select the current cluster node and click the **Edit** button. Specify the IP address of an interface located in the zone you configured at Step 2.
Шаг 4. Сгенерировать **Секретный код** на первом узле кластера.	В разделе **Управление устройством** нажать на кнопку **Сгенерировать секретный код.** Полученный код скопировать в буфер обмена. 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.

Name	Description
	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.
Шаг 6. Назначить зоны интерфейсам второго узла.	В веб-консоли второго узла кластера в разделе **Сеть → Интерфейсы** необходимо назначить каждому интерфейсу корректную зону. The zones and their settings are obtained as a result of data replication from the first cluster node.
Шаг 7. Настроить параметры, индивидуальные для каждого узла кластера (опционально).	Configure the gateways, routes, and other settings specific to each cluster node.

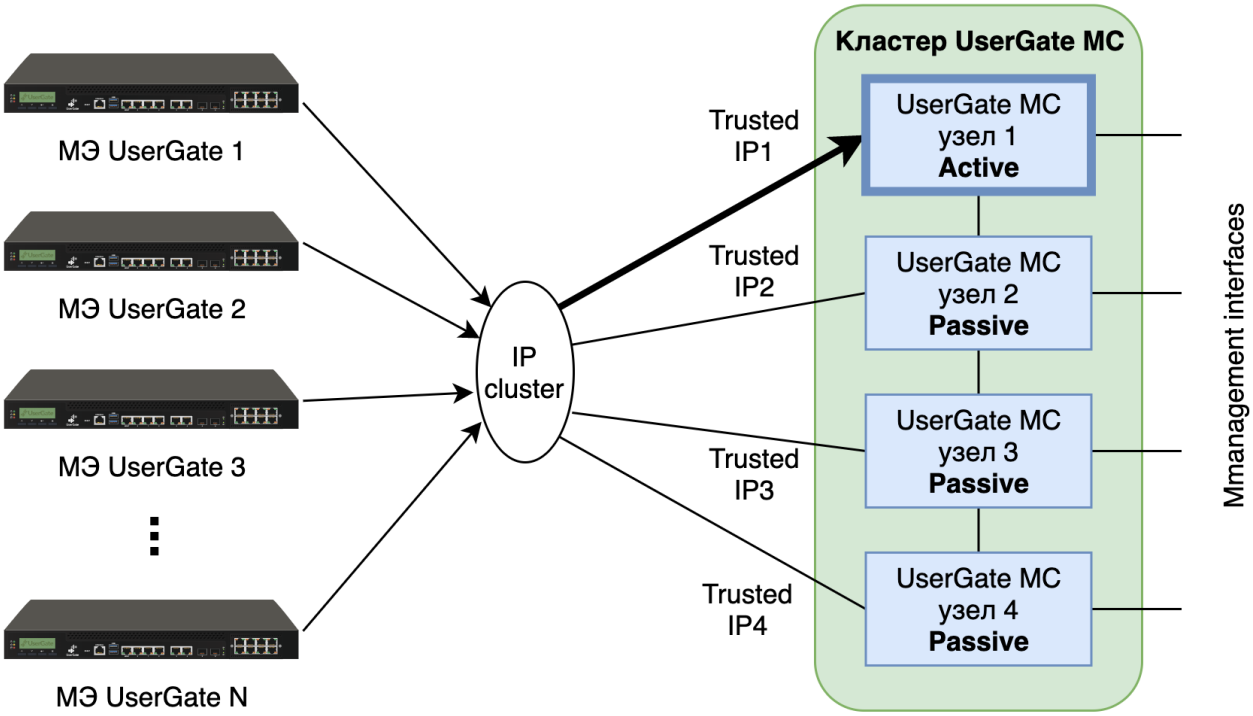
Up to four configuration cluster nodes can be combined into a HA cluster. There can be multiple HA clusters. Поддерживаются 2 режима — **Актив-Актив** и **Актив-Пассив**.

В режиме **Актив-Пассив** один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных. 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.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме **Актив-Пассив**. The network interfaces are configured as follows:

- **Зона Trusted**: IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- **Зона Management**: интерфейсы в зоне Management используются для управления узлами UGMC.



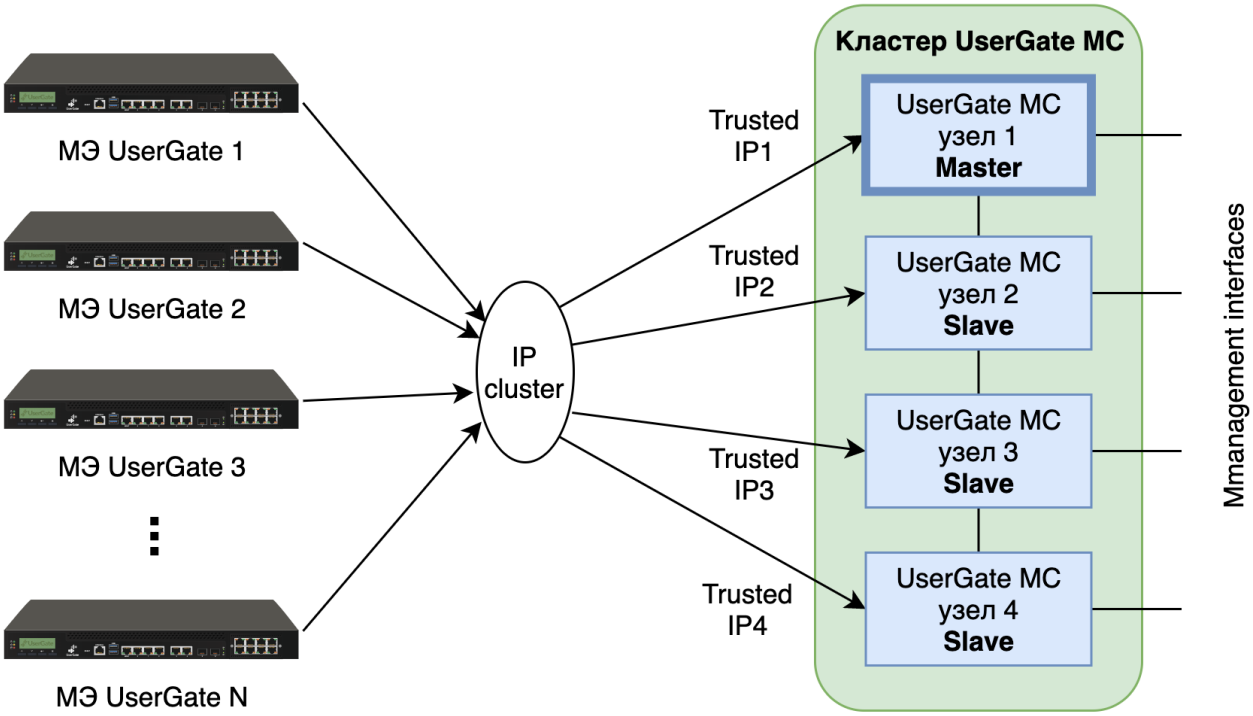
The cluster IP address resides on the UGMC 1 node. If the UGMC 1 node goes offline, the cluster IP address will migrate to the next server, which becomes the master — e.g., UGMC 2.

В режиме **Актив-Актив** один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера. 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.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме **Актив-Актив**. The network interfaces are configured as follows:

- Зона **Trusted**: IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- Зона **Management**: интерфейсы в зоне Management используются для управления узлами UGMC.



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.
Шаг 2. Настроить зоны, интерфейсы которых будут участвовать в отказоустойчивом кластере.	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 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.
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

Name	Description
	asked you to set different values. Any values other than Error (errors only) or Off (disabled) will affect UGMC performance negatively.
Diagnostics logs	• **Download logs**: download the diagnostic logs for sending them to UserGate support. • **Clear logs**: purge logs of content.
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	• **Перезагрузить** — перезагрузка сервера UGMC. • **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)

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
Шаг 1. Создать файл резервного копирования.	Создать резервную копию состояния UGMC в разделе **Управление устройством → Управление резервным копированием → Создание резервной копии**. 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.
Шаг 2. Установить обновления.	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. To interrupt the backup process, press the **Stop** button. 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 backup 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. **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.

Name	Description
	• 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
Шаг 1. Экспорт настроек.	В разделе **Управление устройством → Экспорт и импорт настроек** нажать на ссылку **Экспорт** и выбрать **Экспортировать все настройки** или **Экспортировать сетевые настройки**. The system will save: • текущие настройки сервера под именем: cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin • сетевые настройки под именем: network-cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin nodename — имя узла UserGate Management Center. version — версия UserGate Management Center. YYYYMMDD_HHMMSS is the date and time of the settings export in the UTC timezone. Например, cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084853.bin или network-cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084929.bin.

To apply the exported settings, follow these steps:

Name	Description
Шаг 1. Импорт настроек.	В разделе **Управление устройством → Экспорт и импорт настроек** нажать на ссылку **Импорт** и указать путь к ранее созданному файлу настроек. 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.

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
Шаг 1. Создать правило экспорта.	В разделе **Управление устройством → Экспорт настроек** нажать кнопку **Добавить**, указать имя и описание правила
Шаг 2. Указать параметры удаленного сервера.	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 • **Пароль/Подтверждение пароля** — пароль учетной записи. • **Directory path**: the path on the server where the settings will be uploaded
Шаг 3. Выбрать расписание выгрузки.	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".

Name	Description
	• 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

Access to the UGMC web console is controlled by creating additional administrator accounts, assigning them access profiles, defining an administrator password management policy, and configuring web console access with the correct permissions for the service in the network zone properties.

Note

A local superuser named Admin/system is created during the initial setup of UGMC.

To create additional device administrator accounts, follow these steps:

Name	Description
Шаг 1. Создать профиль доступа администратора.	In the **Administrators → Administrator profiles** section, click **Add** and enter the desired settings.
Шаг 2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора.	In the **Administrators** section, click **Add** and select the desired option. • **Add local administrator**: create a local user, set a password for the user, and assign them one of the access profiles created earlier. • **Add LDAP user**: add a user from an existing domain. This requires a correctly configured LDAP connector in the **Auth servers** section. When logging in to the administrative console, the username must be specified in the user@domain/system or domain\user/system format. Assign this user a profile created earlier. • **Add LDAP group**: add a user group from an existing domain. This requires a correctly configured LDAP connector in the **Auth servers** section. When logging in to the administrative console, the username must be specified in the user@domain/system or domain\user/system format. Assign this user a profile created earlier. • **Add administrator with auth profile**: create a user and assign them an administrator profile created earlier and

Name	Description
	an auth profile (this requires correctly configured auth servers). **Important!** In this section of the management console service settings, only a local administrator can be assigned as a realm administrator. This is because different LDAP servers can be used for authenticating UGMC service administrators and realm administrators. If you need to use LDAP users as realm administrators, they need to be create in the same realm. Более подробно об администраторах области смотрите в разделе Администраторы области.

When creating an administrator access profile, specify the following parameters:

Name	Description
Name	Profile name.
Description	Profile description.
Administrator's type	To grant the rights to manage UGMC services, select the **UGMC administrator** type. The **Realm administrator** option should be selected when creating a root administrator for the managed realm.
Managed realm	If you selected the **Realm administrator** option as the **Administrator's type**, you must specify the managed realm for which the root administrator is being created. The realm must exist at that point.
Permissions	The list of web console tree objects available for delegation. The following access options are available: • No access • Read only • Read and write.

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.

To configure the above settings, follow these steps:

Name	Description
Шаг 1. Настроить политику паролей.	In the **Administrators → Administrators** section, click **Configure**.

Name	Description
Шаг 2. Заполнить необходимые поля.	Provide values for these fields: • **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.

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.

The administrator can define the zones from which access to the web console service will be allowed (TCP port 8010).

> **Примечание**
>
> **Не рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети интернет.**

To allow the web console service for a specific zone, go to the zone properties and allow access to the **Administrative console** service in the **Access control** tab. For more details on configuring zone access control, see the section Zone Configuration.

Certificate Management

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**

Name	Description
Шаг 2. Заполнить необходимые поля.	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. • **Email**: 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.
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**
Шаг 2. Заполнить необходимые поля.	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.

UGMC 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 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. Подробнее о создании и настройке профилей читайте в разделе Профили аутентификации UGMC.

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 TACACS+ authentication server, click **Add**, select **Add TACACS+ 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.

Name	Description
Port	The UDP port on which the TACACS+ server listens for authentication requests.
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. Подробнее о создании и настройке профилей читайте в разделе Профили аутентификации UGMC.

UGMC Authentication Profiles

An authentication profile can be used to define a set of methods to be used for user authorization in the UserGate administrative console. When creating or configuring a profile, provide these required settings:

Name	Description
Name	The name of the authentication profile.
Description	An optional description of the profile.
Authentication methods	The user authentication methods configured earlier, such as LDAP connector, RADIUS authentication server, or TACACS+ authentication server.

Libraries of items

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
Шаг 1. Создать группу почтовых адресов.	In the **Email groups** pane, click **Add** and give a name to the new group.
Шаг 2. Добавить почтовые адреса в группу.	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
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл **list.txt** со списком почтовых адресов.
Step 2. Create an archive containing this file.	Поместить файл в архив zip с именем **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.	Разместить у себя на сайте **list.zip и version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список почтовых адресов и указать URL для обновления.	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,

Name	Description
	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".

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
Шаг 1. Создать группу телефонных номеров.	In the **Phone groups** pane, click **Add** and give a name to the new group.
Шаг 2. Добавить номера телефонов в группу.	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
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл **list.txt** со списком номеров.
Step 2. Create an archive containing this file.	Поместить файл в архив zip с именем **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.	Разместить у себя на сайте **list.zip и version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	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 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. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 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.

Name	Description
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.

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 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 4041). • **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).

Name	Description
	• **UserGate Management Center service**: used for connecting NGFWs and LogAn devices (TCP 2022, 9712). For more on network availability requirements, see Appendix 1. 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 and MTU 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.

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. 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.

Name	Description
	• **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 peers 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	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.

Name	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 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 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.

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 **Connectivity 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.

Name	Description
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.

COMMAND LINE INTERFACE (CLI)

Command Line Interface — CLI (Description)

In UGMC, you can perform basic device configuration with the help of the command line interface, or CLI. The administrator can use CLI to run diagnostic commands, such as ping, nslookup, or traceroute, configure the network interfaces and zones, as well as reboot or shut down the device.

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.

To connect to the CLI using a monitor and keyboard, follow these steps:

Name	Description
Step 1. Connect a monitor and keyboard to the UGMC device.	Connect a monitor to a VGA (HDMI) port and a keyboard to a USB port.
Step 2. Log in to the CLI.	

Name	Description
	Log in to the CLI using the login and password for a user with UGMC root administrator permissions (the default is Admin/system).

Note

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 the serial port, follow these steps:

Name	Description
Step 1. Connect to the UserGate Management Center.	Use a special serial cable or a USB-Serial adapter to connect your computer to UGMC.
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). If the UGMC device has not undergone initial configuration, Admin/system should be used as the login name and utm as the password in order to access the CLI.

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.
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. If the UGMC device has not undergone initial

Name	Description
	configuration, Admin/system should be used as the login name and utm as the password in order to access the CLI.

After a successful login to the CLI, you can view the list of available commands using the **help** command. To get detailed help on any command, use this syntax:

help command

For example, to get detailed help on using the iface command to configure network interfaces, invoke this command:

help Iface

The full list of commands is presented below:

Name	Description
help	Lists the available commands.
exit **quit** **Ctrl+D**	Log out of the CLI.
date	View the current server time.
gateway	View or configure the gateway settings. For detailed information, see "gateway help".
iface	A set of commands used to view and configure network interface settings. For detailed information, see "iface help".
license	View the license information.
netcheck	Check the availability of a 3rd party HTTP/HTTPS server. **netcheck [-t TIMEOUT] [-d] URL** Options: -t: the maximum timeout for a server response. -d: request the website's content. Only headers are requested by default.
nslookup	Determine the IP address from a host name.
ping	Ping a specific host.

Name	Description
radmin	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate.
radmin_e	To enable or disable remote access to the server for UserGate technical support in case the UGMC server hangs up.
reboot	Reboot the UserGate Management Center server.
route	Create, modify, or delete a route.
shutdown	Shut down the UGMC server.
traceroute	Traceroute the connection to a specific host.
zone	A set of commands used to view and configure zone settings. For detailed information, see "zone help".

LOGS AND REPORTS

Event Log

The log contains records for events related to changing UserGate Management Center server 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.
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

Name	Description
	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 Appendix 2. 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** • **Security/authorization** • **Log audit** • **Log alert** • **Local 0**. • **Local 1**. • **Local 2**. • **Local 3**. • **Local 4**. • **Local 5**. • **Local 6**.

Name	Description
	• **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 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:

Name	Description
	"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 (according to the number of rotation days) are stored in 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').
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".

Name	Description
	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

NOTIFICATIONS

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 UserGate devices, the root UGMC administrator (or a UGMC administrator with the appropriate rights) must create at least one realm.

Creating managed realms

To create a managed realm, follow these steps as a UGMC administrator:

Name	Description
Step 1. Create a realm.	In the **Managed realms → Realms** section of the web console, click **Add** and fill in the relevant fields.
Step 2. Create an administrator profile of the Realm administrator type.	In the **Administrators → Administrator profiles** section of the web console, click **Add** and create an administrator profile of the Realm administrator type with access rights to the realm created at the previous step.
Step 3. Create a realm administrator.	In the **Administrators → Administrators** web console section, click **Add** and create an administrator with the profile created earlier.

When creating a realm, provide the following settings:

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.

При создании профиля администратора необходимо указать тип администратора — администратор области и в качестве управляемой области указать созданную область. To create a realm administrator, select this realm administrator profile. Подробнее о создании администраторов смотрите в главе данного руководства Администраторы области.

After you have created the realm and its realm administrator, you can proceed to realm management mode. To do that, log out from the UGMC administrator account in the web console 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., <0>Admin/system.

Realm Administrators

Access control to the web management console for the realm is implemented by creating additional realm administrator accounts and assigning them access profiles.

> **Note**
> **When creating a managed realm, the UGMC administrator creates a root administrator for the realm who has full access rights to this realm.**

To create additional realm administrator accounts, follow these steps:

Name	Description
Step 1. Log in to the web management console as the root realm administrator.	Log in to the management console as the root realm administrator created for this realm by entering the login name as *administrator_login/realm_code*, e.g., *Admin/UG*.
Step 2. Create a realm administrator access profile.	In the **Administrators → Administrator profiles** section of the realm management console, click **Add** and provide the desired settings.
Step 3. Create an administrator account and assign it one of the	

Name	Description
administrator profiles created earlier.	In the **Administrators** section, click **Add** and select the desired option. • **Add local administrator**: create a local user, set a password for the user, and assign them one of the access profiles created earlier. • **Add LDAP user**: add a user from an existing domain. This requires a correctly configured LDAP connector in the **Auth servers** section of the realm. When logging in to the administrative console, the username must be specified in the user@domain format. Assign this user a profile created earlier. • **Add LDAP group**: add a user group from an existing domain. This requires a correctly configured LDAP connector in the **Auth servers** section of the realm. When logging in to the administrative console, the username must be specified in the user@domain format. Assign this user a profile created earlier. • **Add administrator with auth profile**: create a user and assign them an administrator profile created earlier and an auth profile (this requires correctly configured auth servers).

When creating an administrator access profile, specify the following parameters:

Name	Description
Name	Profile name.
Description	Profile description.
Realm access permissions	Set permissions to the settings sections of the realm, such as administrators, auth servers, device templates, template groups, managed devices, and logs and reports. The following access options are available: • No access • Read only • Read and write.
Template access permissions	Set the rights to view and/or modify the settings for all or specific existing templates here. The settings are presented as UserGate NGFW console tree objects available for delegation. The following access options are available: • No access • Read only

Name	Description
	• Read and write. For example, you can allow access to network settings for one administrator group and NGFW policies for another.

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.

Name	Description
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.

Name	Description
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. Подробнее о создании и настройке профилей читайте в разделе Профили аутентификации области.

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.
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. Подробнее о создании и настройке профилей читайте в разделе Профили аутентификации области.

Realm Authentication Profiles

An authentication profile can be used to define a set of methods to be used for user authorization in the UserGate administrative console. When creating or configuring a profile, provide these required settings:

Name	Description
Name	The name of the authentication profile.
Description	An optional description of the profile.
Authentication methods	The user authentication methods configured earlier, such as LDAP connector, RADIUS authentication server, or TACACS+ authentication server.

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

Name	Description
	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.

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

Managing UserGate Next-Generation Firewalls (Description)

The process of centralized UserGate NGFW 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 NGFW settings. For more details, see the section Device Templates.

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 Template Groups section.

4. Add a managed device (NGFW) and apply the template group to it. For more details, see the Placing UserGate Devices under UGMC Management section.

If necessary, the template-based settings can be changed so that the changes are applied to all NGFWs to which these templates are applicable.

UGMC allows you to create and manage configuration and high availability clusters. For a detailed discussion of cluster management, see the UserGate NGFW Clustering Using UGMC section.

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 **NGFW management → Device 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 **Templates management** in the top menu and select the desired template from the drop-down menu that appears.

Template settings are displayed in a tree view, very similar to how they are presented in a UserGate NGFW. 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 UserGate NGFW. In this case, the UserGate NGFW will use the default setting or a setting configured by a local UserGate NGFW 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 Management Center, the settings for the following sections can be changed locally on the NGFW:

   - general device settings: the **General settings** tab, **UserGate → General 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 NGFW template on UGMC.**

3. Policy rules do not override rules created by a local administrator but supplement them as pre- and post-rules instead. Подробно о применении правил смотрите раздел данного руководства Шаблоны и группы шаблонов.

4. 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 devices and UGMC.

5. 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** checkbox in the settings for the network interface.

6. 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 UserGate NGFW groups.

7. Libraries (e.g., IP addresses, URL lists, content types, etc.) have no predefined content in UGMC, unlike the default libraries created on UserGate NGFW devices. To use libraries in UGMC policies, you need first to add items to them. Library items are not synchronized; if a list was created but is not used in any policy, this list will not appear in a NGFW library section.

8. 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, firewall rules, content filtering rules, 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 placement in the group. Подробнее о результирующих настройках смотрите главу руководства Шаблоны и группы шаблонов.

To create a templates group, go to the **NGFW management → 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 UserGate Devices under UGMC Management

A templates group always applies to one or more UserGate NGFW devices. The procedure for adding a managed device to UserGate Management Center 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 device object.	In the **NGFW management → NGFW devices** section of the realm management console, click **Add** and provide the desired settings.
Step 3. Link the managed device object just created to a real UserGate NGFW device.	In the UserGate NGFW management console, set up the link between UGMC and the device. This can be done during the initial configuration of a UserGate NGFW or on an already configured NGFW. Both options are described in detail later in this chapter.

When creating a 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	

Name	Description
	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 sync**: the sync is enabled. The settings are applied to the device. A change to any setting in any template of the template group applied to the managed device is propagated immediately to NGFW. • **Disabled**: sync mode is disabled. • **Manual sync**: in this sync mode the settings are applied once 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 **NGFW Management → NGFW Devices** section click **Actions → Run full synchronization**).

To enable MD-to-UGMC communication during the initial configuration of a UserGate NGFW, follow these steps:

Name	Description
Step 1. Copy the device code	In UGMC, select the managed device object you created and click **Show device unique code**. Copy the code to the clipboard.
Step 2. During the initial setup of the NGFW, 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: • GThe network settings for this UserGate NGFW (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 NGFW. • 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.

Name	Description
Step 4. Check the connection	After connecting to UGMC, the UserGate NGFW should receive all settings prepared for it in UGMC. In the NGFW, 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.

To enable MD-to-UGMC communication for an already configured NGFW, follow these steps:

Name	Description
Step 1. Copy the device code	In UGMC, select the managed device object you created and click **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 NGFW for a successful completion of this step.
Step 3. Check the connection	After connecting to UGMC, the UserGate NGFW should receive all settings prepared for it in UGMC. In the NGFW, 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 UserGate firewall has been successfully added to UGMC, the managed device administrator can do the following:

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 device will be displayed: • Device software version • Device PIN code • HSC serial number • Device uptime • Device load metrics such as CPU load, RAM usage, swap usage, and the number of users connected via the device.
Connect to the managed device console	In the UGMC console, select the managed device object and click **Open console**. The UserGate NGFW 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 UserGate NGFW.

13.4 UserGate NGFW Clustering Using UGMC

Device templates allow you to combine several UserGate devices into a configuration cluster with unified settings on all cluster nodes and to create one or more high availability (HA) clusters from configuration cluster nodes.

For more details on the clustering modes used in UserGate, see the **Clustering and High Availability** section of **UserGate 6 Administrator Guide**.

Configuration cluster

The process of creating a UGMC-managed configuration cluster is virtually identical to creating a standalone cluster. The only difference is that the first cluster node must be placed under UGMC management before the configuration cluster is created. Each configuration cluster node connected to UGMC is assigned a **node identifier**, which is a unique identifier that looks like *node_1, node_2, node_3*, etc.

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 of **UserGate 6 Administrator Guide**.

Name	Description
Step 2. On the first cluster node, configure the zone containing the network interfaces through which cluster replication will be carried out.	В разделе **Зоны** создать выделенную зону для репликации настроек кластера или использовать существующую (**Cluster**). 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 the first configuration cluster node to UGMC	The first node is connected in exactly the same way as a standalone UserGate device. The connection procedure is described in detail in the Placing UserGate Devices under UGMC Management section. The first node is automatically assigned an ID of *node_1*.
Step 6. Connect a second node to the cluster	**Important!** A second and subsequent nodes can only be added to the configuration cluster during their initialization. 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. Оба узла кластера должны находиться в одной подсети, например, интерфейсам eth2 обоих узлов назначены IP-адреса 192.168.100.5/24 и 192.168.100.6/24. Otherwise, you need to specify the IP address of the gateway through which the first cluster node will be accessible. Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку **Подключить**. If the cluster IP addresses configured at Step 2 are assigned correctly, the system will invite you to assign a cluster ID to the device being added as *node_2, node_3, node_4*, etc. The *node_1* ID has been already issued to the first cluster node. After assigning the ID, the second cluster node will be added to the cluster, and all settings of the first node will be replicated on the second one.

Name	Description
	When successfully added to the cluster, the node will be displayed with its selected ID as the second node in the managed device list.

The settings for the added node (including interface, zone, and filtering policy settings) can be configured locally or via UGMC template policies. If they had already been configured in UGMC templates by the time the second node was connected, they will be applied to the new node immediately after adding it to the cluster.

A third and subsequent nodes are added to the configuration cluster in a similar fashion.

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. You can build several HA clusters. To create a HA cluster using UGMC, the following conditions must be met:

Name	Description
Configuration cluster present	A configuration cluster must already be created and display correctly in the managed device list.
UGMC-managed interfaces present	On UserGate devices, interfaces created and managed from UGMC must be present. Virtual IP addresses can only be assigned to interfaces that were created in UGMC templates.
HA cluster requirements met	All requirements applicable to the nodes of an HA cluster being created without using UGMC must be met. For more details on HA clusters, see the **Clustering and High Availability** section of **UserGate 6 Administrator Guide**.

To create an HA cluster, follow these steps:

Name	Description
Step 1. Configure zones whose interfaces will participate in the HA cluster	In a **UGMC** template where zones are configured for managed devices, allow the VRRP service in the **Zones** section for all zones where you plan to add a virtual cluster IP address.
Step 2. Create a HA cluster	In one of the **UGMC** templates, go to the **Device management → HA cluster** section, click **Add**, and configure the settings for the new HA cluster.
Step 3. Specify a virtual IP address for the auth.captive, logout.captive,	If captive-portal authorization is to be used, the system host names auth.captive and logout.captive used by the authorization procedures in the captive portal must resolve to

Name	Description
block.captive, and ftpclient.captive hosts.	the IP address assigned as the virtual cluster address. These settings can be configured in the **General settings** section of a **UGMC** template. They are described in more detail in the **Device Setup** section of **UserGate 6 Administrator Guide**.

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.
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.
Sessions sync	Enables user session synchronization mode between all nodes in the HA cluster. When enabled, this option makes switching users between devices transparent to the users themselves but adds significant load on the UserGate platform. The option is only relevant for the Active-Passive cluster mode.
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. The cluster nodes are represented by the IDs assigned to the nodes of the configuration cluster when it was created.
Virtual IPs	Assign virtual IP addresses and map them to the interfaces of the cluster nodes. Only interfaces created in a UGMC template can be used here.

Update Management for Managed Devices

UserGate Management Center 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/content type lists etc.).

> **Note**
>
> **After adding a UserGate NGFW to UGMC management, the UserGate 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 UserGate 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. For more details on how to configure an update check schedule, see the **General Settings** chapter of **UserGate 6 Administrator Guide**.
Step 2. Configure a software update policy for UserGate devices	A software update policy allows you to specify an update available for installation on all or selected MDs. For more details on updating software, see the Software Updates section.
Step 3. Configure a library update policy for UserGate devices	A library update policy allows you to select the desired library updates for installing on MDs. For more details on libraries updates, see the Libraries Updates section.

Software Updates

From time to time, UserGate issues software updates for UserGate NGFWs. These updates are uploaded to the UserGate repository (http://static.usergate.com) from where they can then be downloaded to NGFWs. If a UserGate NGFW is managed from Management Center, it checks automatically for available updates on the Management Center 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 **NGFW management → 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 **NGFW management → Software Updates** section, click **Import update**, and select the update file. If the update file has no update name and version specified, enter 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** checkbox.
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. An MD downloads the update according to its update check schedule. When downloaded, the update can be installed centrally by the administrator from the MC 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.

Name	Description
Size	The size of the update.
Release	The UserGate 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.
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.

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 (http://static.usergate.com) from where they can then be downloaded to UserGate NGFWs. If a UserGate NGFW is managed from Management Center, it checks automatically for available updates on the Management Center 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 UserGate MDs. An MD 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.
Version	The version of the library update.
Updated	The date and time when the specific library was last updated.

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 template-based settings can be changed so that the changes are applied to all LogAn managed devices to which these templates are applicable.

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 management → 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 templates** in the top menu and select the desired template from the drop-down menu 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 Management Center, 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 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. Подробнее о результирующих настройках смотрите главу руководства Шаблоны и группы шаблонов.

To create a templates group, go to the **LogAn management → 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.

Name	Description
Step 2. Create a LogAn managed device object.	In the **LogAn management → 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 NGFW 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.
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 Management → 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 LogAn, 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 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.

Name	Description
	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
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 (https://static.usergate.com) from where they can then be downloaded to LogAn. If a UserGate LogAn MD is managed from Management Center, it checks automatically for available updates on the Management Center 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 management → 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 management → Software updates** section, click **Import update**, and select the update file. If the update file has no update name and version specified, enter these in the corresponding fields. By clicking **Sa ve**, 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.

Name	Description
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.
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 (https://static.usergate.com) from where they can then be downloaded to LogAn. If a LogAn MD is managed from Management Center, it checks automatically for available updates on the Management Center 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 UserGate Client Endpoints

A managed endpoint is a user computer running Windows with the UserGate Client software installed (UGC). 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, Windows logs and other endpoint security data is sent to the UserGate LogAn event analytics system and can be used to implement automated response to security threats.

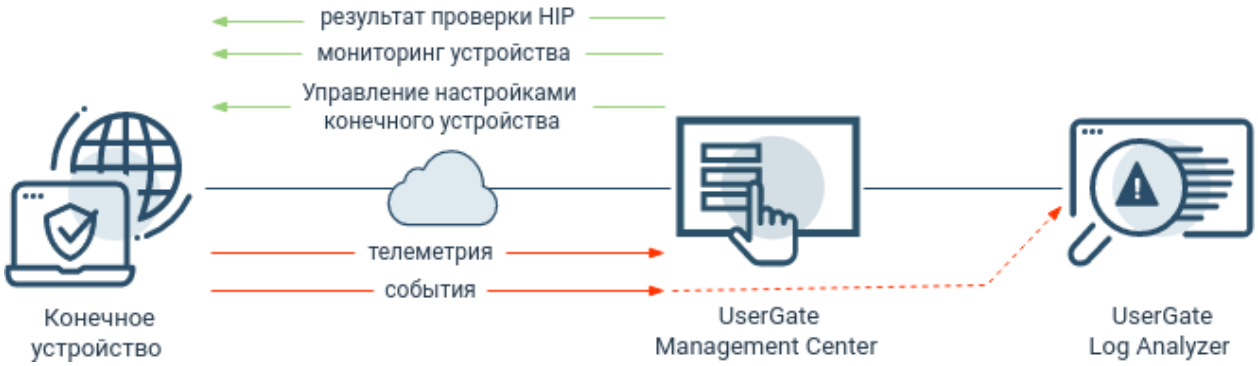
UserGate Client Endpoints Management (Description)

The process of centralized UGC device management can be divided into the following steps:

1. Create a managed realm. See the Creating Managed Realms section.
2. Create one or multiple templates, each describing a distinct part of the UGC managed device settings. For more details, see the UGC Device Templates section.
3. Combine the relevant templates into a template group in the required order to obtain the correct final manged UGC device configuration. For more details, see the UGC Managed Device Template Groups section.
4. Install UserGate Client software on user computers. For more details, see the UserGate Client Software Installation section.
5. Add a UGC MD and apply the template group to it. For more details, see the Placing UGC Managed Devices under UGMC Management section.
6. UGC Device management from the UGMC Console. For more details, 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 a large number of 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.

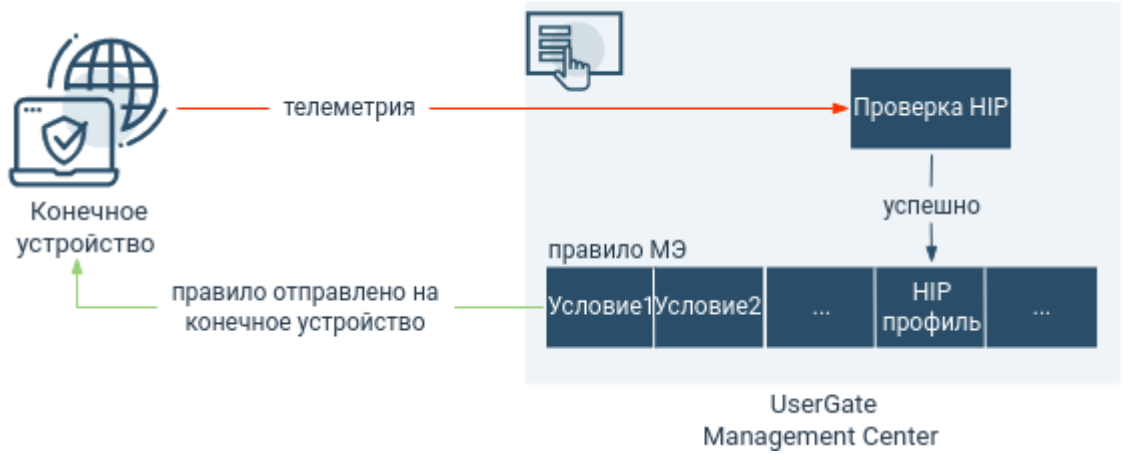
The endpoint sends telemetry (CPU load, disk information, system uptime, etc.) to UGMC, as well as configuration that is used for HIP validation: the information about the system security level (status of antivirus, firewall, automatic system update, BitLocker), the list of running processes and services, list of installed updates, and the information about installed software. We'll discuss compliance checking in more detail later. 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 it allows to check if an endpoint device 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.**

Only HIP profiles specified in the firewall rules as one of the filtering conditions are used to check compliance. 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. Default value: **Yes**.

Name	Description
	• **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* flag). If the flag 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* flag). If the flag 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* flag). If the flag 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	Host name (FQDN) or the IP address of the VPN server. **Important!** Please note that if you specify the VPN server address as FQDN, there is no IP address enumeration. If the DNS server returns several addresses, an attempt to connect to the first address in the list will be made.
Протокол	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**. 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. **Основной режим**. In the main mode, the devices exchange six messages. During the first exchange (messages 1 and 2), the

Name	Description
	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. **Агрессивный режим**. 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. Минимальный интервал проверки: 10 секунд; значение 0 отключает проверку. • **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. • **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	

Name	Description
	In the second phase, the method for securing IPsec connections is selected. You need to specify the following: • **Время жизни ключа**. 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. • **Максимальный размер данных, шифруемых одним ключом**. the key lifetime can also be expressed in bytes. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. • **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.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. 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.

Примечание

Чекбокс Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

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. • **Outside perimeter**: the rule will be applied if the computer with the UGC software installed is located outside the domain network.

Name	Description
	• **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. For more details on proxy profiles, see the Proxy Profiles chapter.
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.
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.

Name	Description
	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. **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 **Network access control at the host level** module is required.

Name	Description
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
Шаг 1. Создать сервис.	Нажать на кнопку **Добавить**, дать сервису название, ввести комментарий.
Шаг 2. Указать протокол и порт.	Нажать на кнопку **Добавить**, выбрать из списка необходимый протокол, указать порты назначения и, опционально, порты источника. 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.

Name	Description
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.	Поместить файл в архив zip с именем **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 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,

Name	Description
	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".

Applications

Элемент библиотеки **Приложения** позволяет создать группы приложений для более удобного использования в правилах фильтрации сетевого трафика. 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
Шаг 1. Создать группу приложений.	In the **Application groups** pane, click **Add** and give a name to the new group.
Шаг 2. Добавить приложения.	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.

Proxy Profiles

This section allows you to configure proxies to which the TCP traffic matching the rules will be redirected with the **Redirect to proxy** action.

Name	Description
Name	The proxy profile name.
Description	Profile description.
IP address	The IP address of the proxy server to which the traffic will be redirected.
Port	The port number of the proxy server to which the traffic will be redirected.

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
Шаг 1. Создать список URL.	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
Шаг 2. Добавить необходимые записи в новый список.	Add URL entries to the new list. You can use wildcards such as "^", "$", and "*": • "*": any number of any characters • "^": start of a line

Name	Description
	• "$": 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/
^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
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл **list.txt** со списком URL в следующем формате: *www.site1.com/url1* *www.site2.com/url2* ... *www.siteend.com/urlN*
Step 2. Create an archive containing this file.	Поместить файл в архив zip с именем **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.
Шаг 5. Создать список типа контента и указать URL для обновления.	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) (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".

URL Categories

Элемент библиотеки **Категории URL** позволяет создать группы категорий UserGate URL filtering для более удобного использования в правилах фильтрации контента. 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
Шаг 1. Создать группу категорий.	In the **URL category groups** pane, click **Add** and give a name to the new group.
Шаг 2. Добавить категории.	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
Шаг 1. Создать список типов контента.	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.
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.

Name	Description
Шаг 3. Создать правило фильтрации контента, содержащее один или несколько списков.	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
Шаг 1. Создать файл с необходимыми типами контента.	Создать файл **list.txt** со списком типов контента.
Step 2. Create an archive containing this file.	Поместить файл в архив zip с именем **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.
Шаг 5. Создать список типа контента и указать URL для обновления.	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. 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,

Name	Description
	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
Шаг 1. Создать календарь.	В панели **Группы** нажать на кнопку **Добавить**, указать название календаря и его описание.
Шаг 2. Добавить временные интервалы в календарь.	В панели **Элементы** нажать на кнопку **Добавить** и добавить интервал. 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 to UGMC from the UGC managed device.	On the UGMC server, allow the **Endpoints control** service in the zone interface 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.

Name	Description
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 UGC managed device. The settings (policies) 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 to UGMC from the UGC managed devices.	On the UGMC server, allow the **Endpoints control** service in the zone interface 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.
Step 3. Display the unique code for the new device group.	In the **Endpoints → Endpoint codes** section of the realm management console, click **Endpoint unique code** and note the code. This code will need to be entered when the UGC software is installed on the device group.

Name	Description
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 this 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	A description of the code.
Template Groups	The template group whose settings should be applied to UGC managed devices activated using this code. The settings (policies) 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 *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 (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.
- Задание частоты синхронизации соединений UGMC и управляемых устройств UGC.
- Отображение уникального кода устройства, необходимого для подключения управляемых устройств UGC к 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	The following information is displayed: • The IP address of the endpoint device used for Internet access. • The NetBIOS name.

Name	Description
	• Время последнего подключения управляемого устройства UGC к 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. В случае возникновения ошибки синхронизации конфигурации конечного устройства доступен просмотр отчёта (нажать **Показать отчёт**), в котором отображены время последнего подключения к управляемому устройству, название правила, тип объекта, ставшего причиной сбоя синхронизации, и описание ошибки. 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. В случае несоответствия к просмотру доступен отчёт (нажмите **Посмотреть отчёт**), содержащий информацию о времени последнего получения данных, название профиля и объекта HIP, тип и несоответствующий элемент объекта.

Name	Description
	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 to the device. • **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. • Client memory used by the UserGate Client. • Disk information: the disk size, type, and performance.

Name	Description
	• 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: • **Идентификатор** устройства: пара идентификаторов VID/PID (Vendor ID/Product ID) и номер версии устройства. • **Название** устройства. • **USB класс**, например mouse, printer. • **Сервис**: драйверы, использующиеся для работы с устройством.
Startup items	The list of applications configured to start automatically on system login.
Processes	The list of processes running on the endpoint device. Нажатие кнопки **Завершить процесс** позволяет завершить процесс на конечном устройстве, используя 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. Для этого необходимо нажать **Найти** (отображается при наведении указателя мыши на название каталога).
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

The UserGate Client software product can be installed on computers running Windows OS 7/8/10/11. The minimum system requirements are 2GB RAM, CPU speed of at least 2GHz, and 200MB 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. Для публикации приложения в Active Directory требуется msi-файл с инсталлятором и административный шаблон UserGateClient.adm, который используется для указания IP-адреса UGMC и кода конечных устройств, созданного в центре управления.

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 leve**l: the diagnostic detail level. The options are: ◦ **Off**: отключить ведение журнала диагностики. ◦ **Error**: журналировать только ошибки. ◦ **Warning**: log only errors and warnings

Name	Description
	◦ **Info**: log only errors, warnings, and additional information ◦ **Debug**: provide as much detail as possible Журнал находится: %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). Чтобы скопировать информацию нажмите **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).

Данные для подключения к UserGate Management Center (IP-адрес и код для подключения УУ UGC) указываются: %PROGRAMFILES%\UserGate\UserGate Client\usergateclient\bin\endpoint_gui.

Рекомендации по установке ПО UserGate Client

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.

Примечание

Настройки, представленные в данном разделе, носят рекомендательный характер.

1. Install the Sysmon utility that provides in-depth information on process creation, network connections, and changes in file creation times. Подробная информация и файл установки доступны по ссылке.
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

Примечание

Для быстрого запуска приложения Редактор реестра используйте сочетание клавиш Win+R и введите regedit.

В случае включения через Редактор реестра необходимо создать переменную **EnableScriptBlockLogging** в каталоге **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogg** указав тип данных **REG_DWORD** и значение **1**.

Примечание

Данная настройка возможна в реестрах HKEY_LOCAL_MACHINE и 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

В случае включения через Редактор реестра необходимо создать переменную **ProcessCreationIncludeCmdLine_Enabled** в каталоге **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit** указав тип данных **REG_DWORD** и значение **1**.

Примечание

Данная настройка поддерживается на устройствах с версией ОС не ниже Windows Server 2012 R2 и Windows 8.1.

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: • **Антивирус**. Conformance check of the antimalware software on the user device: ◦ **Enabled**: check the software status ◦ **Antimalware database updated**: checking database relevance (yes, no, or do not check) ◦ **Version**: the version of the software ◦ **Вендор**: производитель и название продукта. • **Межсетевой экран**. 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 ◦ **Vendor**: the device vendor and product name • **Резервное копирование**. Conformance check of the backup software: ◦ **Installed**: check if the software is installed ◦ **Version**: the version of the software ◦ **Вендор**: производитель и название продукта.

Name	Description
	• **Шифрование диска**. Conformance check of disk encryption programs installed on the endpoint: ◦ **Installed**: check if the software is installed ◦ **Version**: the version of the software ◦ **Вендор**: производитель и название продукта. • **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 ◦ **Вендор**: производитель и название продукта. • **Update management.** Check for current updates. ◦ **Installed**: check if the software is installed ◦ **Version**: the version of the software ◦ **Вендор**: производитель и название продукта.
Processes	Check the processes running on the device.
Running services	Check the services running on the device.
Registry keys	Ключ реестра Microsoft Windows - каталог, в котором хранятся настройки и параметры операционной системы. The following types of registry values are supported: • **REG_SZ**: строка Unicode или ANSI с нулевым символом в конце. • **REG_BINARY**: двоичные данные в любой форме. • **REG_DWORD**: 32-разрядное число. 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. Описание ключей реестра читайте в документации Microsoft (https://docs.microsoft.com/ru-ru/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.

Collecting and Analyzing Data from UGC Devices

LogAn является продуктом компании UserGate, входящим в состав экосистемы UserGate SUMMA. LogAn устанавливается на отдельном сервере, использование которого позволяет обеспечить высокую надёжность и хорошую масштабируемость системы. LogAn предоставляет возможность осуществления сбора и анализа данных с различных устройств, мониторинга событий безопасности и создания отчётов. For more details on LogAn, refer to the corresponding documentation.

Для отправки данных на сервер LogAn, его необходимо назначить, используя шаблон конечных устройств. 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 MC 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.

Для просмотра данных с устройств UGC используется раздел веб-консоли **Журналы и отчёты → Журналы → Конечные устройства**.

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 whose syntax is described later in the Advanced Search Mode section.

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.

Name	Description
Log level	The event type: • **Аудит успеха** (Audit Success): событие журнала безопасности, которое происходит при успешном обращении к аудируемым ресурсам. • **Аудит отказа** (Audit Failure): событие журнала безопасности, которое происходит при неуспешном обращении к аудируемым ресурсам. • **Ошибка** (Error): событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных. • **Сведения** (Information): информационные события, которые, как правило, не требуют внимания администратора. • **Предупреждение** (Warning): события указывают на проблемы, которые не требуют немедленного исправления, однако могут привести к ошибкам в будущем.
Data	Detailed information about the event.
Log event source	The source of the logged events.
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.

Name	Description
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.

С использованием кнопки **Показать** можно просмотреть выбранную запись журнала событий конечных устройств.

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

Журнал правил конечных устройств отображает события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включена функция **Журналирование**. 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 whose syntax is described later in the Advanced Search Mode section.

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 device ID.
Time	The time when the rule was triggered. Displayed in the timezone set in LogAn.
Endpoint device	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.
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.

Нажав кнопку **Показать**, можно просмотреть подробную информацию о выбранной записи журнала правил конечных устройств.

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 whose syntax is described later in the Advanced Search Mode section.

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 device ID.
Time	The time when the application was started on the endpoint device. Displayed in the timezone set in LogAn.
Endpoint device	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.

Name	Description
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 whose syntax is described later in the Advanced Search Mode section.

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. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

The endpoint hardware log shows the following information:

Name	Description
Node	The endpoint device ID.
Time	The date and time when the event was logged.

Name	Description
Endpoint device	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.

Нажатие кнопки **Показать** позволяет открыть окно с информацией о записи журнала аппаратуры конечных устройств.

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.

ADMIN

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