UserGate

UserGate SIEM 7.3.x Administrator Guide

Table of Contents

INTRODUCTION

SIEM Architecture

Description

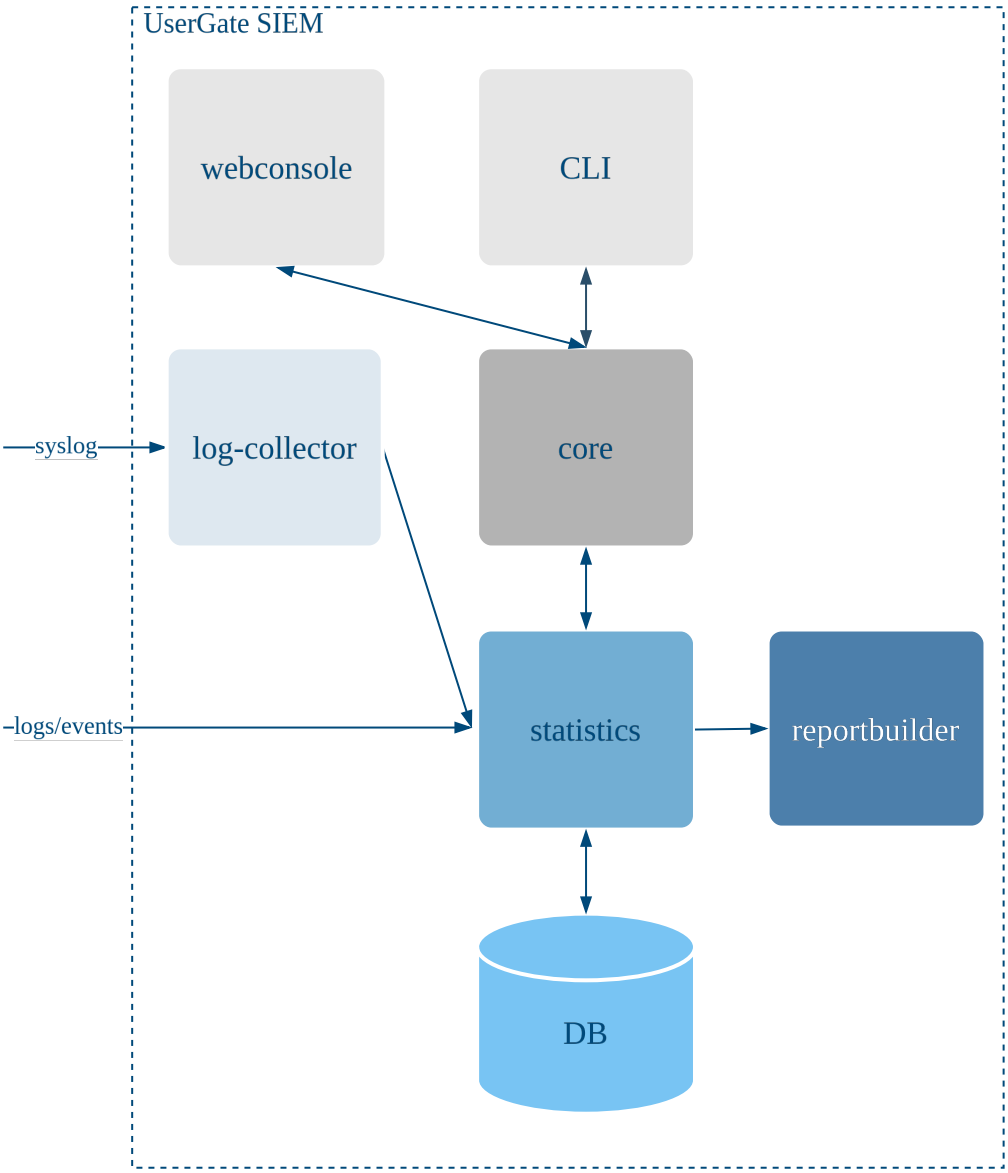
UserGate SIEM (SIEM) is a system that manages security information and information security events. SIEM collects system logs and event data from various devices within the controlled network infrastructure. The data is processed and analyzed, which can identify suspicious activity or signs of known network threats. Depending on the severity level of the threats detected, certain response actions can be triggered, including notifications, creating security incidents for further investigation, and sending commands to certain devices in the network to avert the threat.

The results of data processing are displayed in a single web interface and also provided as report files for studying the characteristics of security incidents. To investigate cybersecurity incidents, an IRP system is used that is part of SIEM. An IRP system is a platform for managing the processes of responding to information security incidents. It allows you to customize the incident investigation process to the needs of a specific company.

The SIEM is delivered as a virtual machine image designed for deployment in a virtual environment.

Solution Architecture

The UserGate SIEM solution is based on the following software modules:



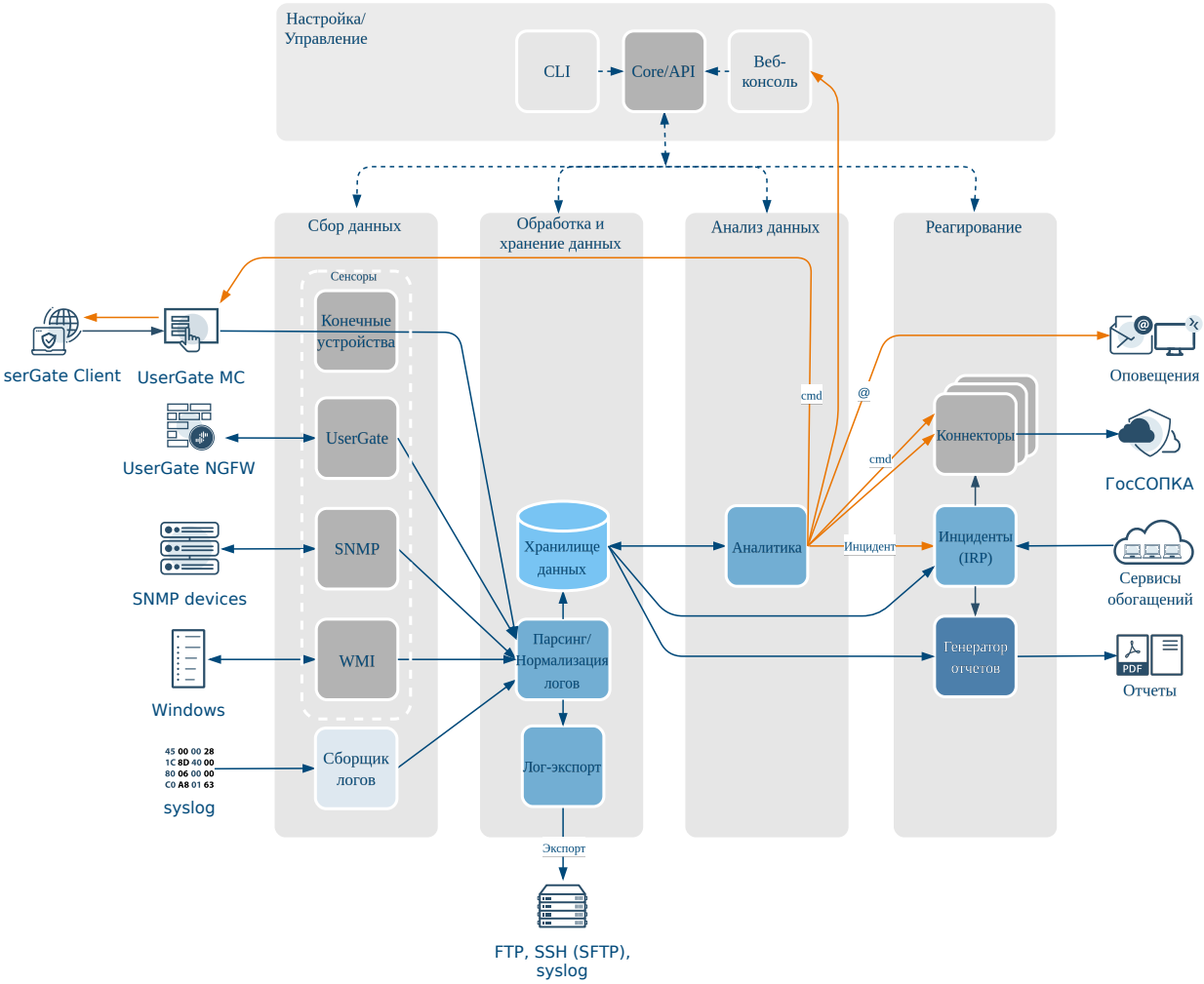
- core: the core module of the system, implementing configuration, management, API, and configuration storage functions.
- statistics: the main functional module of the system, implementing the functions of receiving, processing, analyzing, and storing data, creating security incidents, managing response processes, exporting data, and generating reports.
- log-collector: a module for collecting events from network devices via the syslog protocol.
- DB: the database.
- webconsole: a module for the web-based system management console.
- CLI: a command-line interface module for system management.

- reportbuilder: a module for generating reports in HTML and PDF formats.

Functional Model

The functional model of UserGate SIEM can be described using the following main blocks:

- Data collection block
- Data processing block
- Data analysis block
- Response block
- System configuration and management block



Data Collection

The SIEM collects data from external sources using a log collector (the log-collector module) and sensors (configured and stored in the core module).

The log collector collects events from network devices via the syslog protocol. Configurable syslog rules allow you to filter event records (by time, event severity, object, device name, and application), which eases the search for information of interest.

Sensors collect data from UserGate firewalls (UserGate sensor), endpoints with UserGate Client software installed (endpoint sensor), Windows computers (WMI sensor), and any other network devices capable of transmitting data via SNMP (SNMP sensor).

When the SIEM system is integrated with the UserGate firewall (NGFW), it first connects to NGFW using the parameters configured in the UserGate sensor and sends the connection settings to NGFW. NGFW then accumulates its data in a local cache and transmits them periodically to SIEM's statistics module, directed by a timer.

Using an SNMP sensor, you can connect an SNMP-compatible network device to SIEM to collect and analyze its metrics. SIEM can display any metrics received using SNMP queries. To configure an SNMP sensor, you need to have MIBs (Management Information Bases) for the managed device. MIBs from third-party devices can be imported into the SIEM system.

Using an WMI sensor, you can connect a WMI-compatible network device (a computer running Windows) to SIEM to collect and analyze its data. The WMI sensor settings specify the device address, device login attributes, namespace, and Windows event log parameters to be monitored by the SIEM system.

Endpoints with UserGate Client installed connect to the SIEM indirectly, but through UserGate Management Center. When integrating UserGate SIEM with UserGate MC, an SSH tunnel is established between them, through which configuration parameters and statistics from endpoints integrated into MC are transferred to the SIEM.

Data Processing and Storage

Collected data is sent to the statistics module, where it undergoes preliminary analysis and normalization. During normalization, log records obtained from various sources are standardized to be written to standard SIEM database fields. The normalized records are then transferred to the log export service and data warehouse.

The log export service allows you to export logs (in CEF or JSON format) to external FTP, SSH (SFTP), and syslog servers using customizable rules. Sending to SSH and FTP servers occurs according to a schedule specified in the rule settings or on a one-time basis. For syslog servers, logs are sent immediately after a record is added to the log.

The database tables contain all log records collected both for the SIEM device itself and its connected devices. The data warehouse tables also contain created incidents and alerts.

Device data in the tables is stored by key, which contains the ClusterID. For example, when registering an NGFW in the SIEM, an account is created for it in the statistics module, which contains the ClusterID and token. The token is returned to NGFW and used for authorization.

Logs in the database are cyclically overwritten, providing free disk space necessary for work. Log records (except the event log) are rotated automatically based on the free space on a given partition. Database rotation records are displayed in the SIEM event log. Event log records are not rotated.

Data Analysis

The analytics service also operates in the statistics module. It analyzes security event logs received from configured sensors. During data analysis, the analytics service aggregates and correlates recurring events using analytics rule conditions written in SQL-like syntax. When a rule is triggered, the response action specified for the rule will be taken.

Responce

The following actions can be used to respond to anomalies and security threats identified during data analysis:

- Visualization of data analysis system triggers in the system management console.
- Notification of information security personnel.
- Creation of an information security incident for further investigation.
- Creation of information security incident reports.
- Sending commands to specific network devices to mitigate threats.

SIEM analytics rules define the response actions to be performed when they are triggered. Such actions may include email or SMS notifications, displaying information on a dedicated web page (webhook), sending commands to be executed on a network device, or creating an incident. Creating an incident as a response action allows you to automate the process of cybersecurity incident creation. Information about the triggering of analytics rules and the security

incidents created is displayed online on information screens and dashboards in the SIEM administrator's web console.

Cybersecurity incident investigations are performed using the Incident Response Platform (IRP). The IRP service is integrated with the analytics service and is required for managing cybersecurity incident response processes. During incident investigation, the IRP service utilizes external resources (external enrichment services) to gather additional information. If log records are attached to the incident as evidence, IRP automatically extracts compromise indicators (IP address, URL, domain, file name, and hash) for working with External enrichment services.

The report generation module can be used to create security incident reports in the PDF or HTML format available for download or email distribution.

Using customizable software connectors, the UserGate SIEM system can be connected to various security tools or cybersecurity incident data exchange services. Using a connector with the SSH server type, you can send commands to a connected device in response to a triggered analytics rule. Configuration and Management

Configuration and Management

The Web Console module interacts with most SIEM modules for the purposes of data management and presentation. The module allows you to generate and view reports and logs, present data graphically using dashboard widgets, and configure settings in the web management interface (general SIEM settings, analytics rule settings, security incident management, etc.).

Requests from the web console first go to the core module in a special Web Console Proxy service. Requests to read data directly (without going through the API) are then forwarded to the statistics module. Statistics processes these requests, generates valid SQL queries to the database, and returns the data back through a direct tunnel to the web console.

The SIEM settings can also be configured using the command line interface (CLI module). CLI commands are implemented using an API.

SIEM LICENSING

SIEM Licensing

Basic license

UserGate SIEM versions 7.3.0 and higher licensing is based on platform performance parameters and depends on:

- type of hardware platform (for hardware and software systems);
- the number of supported virtual machine cores (for a virtual image).

If you try to register invalid hardware with a key with performance limitation, an error will appear: Entered PIN code is licensed for another type of UserGate device, or configuration of this server is not licensed, for example, number of actual CPU cores exceeds the number of CPU cores licensed.

> **Note**
> **If a virtual machine is registered with the valid key and additional cores are added in the future, only the number of cores allowed by the license will be active in the virtual machine.**

Starting with version 7.4.0, the **Dashboards** section's license widget displays information about current processor core limits.

The basic license includes the ability to connect an unlimited number of sensors. Without a basic license, sensors cannot be connected.

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

Additionally Licensed Modules

The following modules can be additionally licensed.

Module	Description
Security Updates (SU)	The SU module grants the right to receive SIEM updates, including the updates for the library of log normalization rules. The module is supplied as an annual subscription. After one year, you will need to renew the license to continue receiving updates

Module	Description
Cluster	The module includes a license to allow UserGate SIEM devices to operate in cluster mode. The license term is unlimited.
SIEM Expertise Subscription	The module entitles you to UserGate expertise and includes: • Update of the library of analytics rules; • Update of the library of UserGate remote device management commands. The module is supplied as an annual subscription. After this period, the libraries downloaded while the license was active continue to function, but updates are no longer available. To receive updates, you must renew your license.

License Activation Procedures

Online Activation

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

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

After that, the UserGate device checks the license once a day. If everything is OK, the device operates normally. If the license check is successful, this event is recorded in the logs.

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

Online Activation Procedure

To register the device:

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

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

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

Offline Activation

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

The offline licensing process includes the following steps:

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

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

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

Request generation

To generate a request file for offline license activation:

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

IP address is the IP address of the licensed device.

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

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

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

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

Request activation

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

Applying the license

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

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

2. Select **Finish offline activation**.

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

The licensing process is complete.

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

INITIAL CONFIGURATION

General Information

UserGate SIEM is delivered as a virtual appliance image with four Ethernet interfaces, designed for deployment in a virtual environment.

HSC Deployment

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

Virtual Appliance Deployment

SIEM 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 platforms 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.

Attention!

The correct work of an internal database requires that the virtual environment CPUs support the SSE4.2 micro-instruction set with the x86 architecture. Any x86-based CPU released after 2008 supports SSE4.2.

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

Name	Description
Step 1. Download and unpack the VM image.	Download the latest version of the virtual appliance from the official website, https://www.usergate.com.
Step 2. Import the VM image into your virtualization system.	Instructions on how to import a VM image can be found on the VirtualBox and VMWare websites. For Microsoft Hyper-V and KVM, you need first to create a VM, specify the downloaded image as the VM disk, **and then disable Integration Services** in the settings for the newly created VM.
Step 3. Configure the VM parameters.	Increase the size of the RAM for the VM. In the VM properties, set a minimum of 8GB RAM.
Step 4. Important! Increase the size of the disk for the VM.	The default disk size is 100GB, which is usually not enough to store all logs and settings. In the VM properties, set a disk size of 300GB or more. The recommended size is 1000GB or more.
Step 5. Configure virtual networks.	UserGate SIEM is supplied with two interfaces bound to zones: • **Management**: the first VM interface. • **Trusted** - The 2nd interface of the virtual machine.
Step 6. Perform factory reset.	Start the SIEM VM. During loading, select **Support Menu** and then **Factory reset**. **This is a critical step**. This step is used to configure network adapters and increase the partition size on the hard disk to the full size specified at Step 4.

Connecting to the Device

The port0 interface is configured to receive an IP address automatically from a DHCP server and assigned 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.

Please follow these steps to perform initial configuration:

Name	Description
Step 1. Connect to the management interface.	**When a DHCP Server Is Used**. Connect the port0 interface to the corporate network with a working DHCP server. Turn on the device. After booting, the device will display the IP address to connect to for subsequent product activation. **Static IP address**. Turn on the device. Use the CLI (Command Line Interface) to assign the desired IP address to the port0 interface. For more details on using the CLI, see the chapter Command Line Interface (CLI). Connect to the SIEM web console at that IP address. The address string should look similar to this: https://SIEM_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.	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, the device 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	In the **Interfaces** section, enable the desired network interfaces, assign valid IP addresses that correspond to your

Name	Description
interfaces, and connect UserGate SIEM to the corporate network.	networks, and bind the interfaces to the respective zones. For more details on network interface management, see the Network Interface Configuration chapter. The system is supplied with a number of predefined zones: • Management (management network), port0 interface. • Trusted (LAN). It is assumed that the Trusted zone will connect SIEM to the network that will be used by UserGate gateways to send logs to it and by SIEM to access the Internet. For the SIEM to work, one configured interface is sufficient. Having separate network interfaces for device management and data collection is recommended for security but 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 **DNS** section, specify the IP addresses of your provider's or corporate DNS servers. For more details on DNS management, see the chapter General Settings section.
Step 8. Register the product, if it was not registered at Step 4.	Register the product using the PIN code. For a successful registration, LogAn must have Internet access, and the previous steps must be completed. For more details on product licensing, see the SIEM Licensing chapter.
Step 9. (Optional) Create additional administrators.	In the **Administrators** section, create additional system administrators and grant them the necessary rights (roles).

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

OFFLINE SERVER OPERATIONS

Offline Server Operations (Description)

Some server maintenance operations are carried out when the server is not running and is offline. To perform such operations, select **Support menu** when the server is

booting and then select the desired operation. To access this menu, connect a monitor to a VGA (HDMI) port and a keyboard to a USB port (if these ports exist on the device) or use a special serial cable or a USB-Serial adapter to connect your computer to SIEM. 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 SIEM	Boot UserGate and output diagnostic information about the boot process to the serial port.
UGOS SIEM (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.

DEVICE SETUP

General Settings Section

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

Name	Description
Admin console settings	SIEM interface settings: • The **timezone** for your location. Used in rule schedules and for the correct display of time and date in reports, logs, etc. • **The default interface language** to use by default in the console. • **Automatic session closure timer (min)**: setting the timer for automatically closing a session if the administrator is inactive in the web console.
Server time settings	Configure the time synchronization settings: • **Use NTP servers**: use the NTP servers from the provided list for time synchronization. • **Primary NTP server**: the primary time server address. Default value: pool.ntp.org. • **Secondary NTP server**: the secondary time server address. • **Server time**: allows time setting on the server. The UTC timezone should be used.
Update center	This is where you configure update downloads for the software and system libraries provided on subscription. **Software updates**: configure the update channel (stable, beta), checking for new software updates and downloading offline updates. When installing an update, you can set a restore point for your device. If a restore point has been created, after the update has completed, an option to restore the previous software version will appear in the device's start menu. **Libraries updates**: check for libraries updates, download updates, and configure the automatic library check and download schedule.

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

Name	Description
	The number of change types is not limited.
System DNS servers	Specify valid IP addresses of DNS servers here.
Log database status	The current state of the SIEM server is displayed here: • **State**: shows the current state of the statistics service. • **Device version**: the version of SIEM. • **Metrics**: the number of incoming events for the statistics service (average value over the last 5 seconds).
Log Collector status	The current state of log collector is displayed here: • **State**: shows the current state of the statistics service. • **Metrics**: the number of incoming events for the syslog service (average value over the last 5 seconds).
UserGate Management Center agent	Here you can configure device connection to the central management console that can be used to manage a SIEM device fleet from a single point. • **Enabled/Disabled**: enable or disable management via UGMC. • **UserGate Management Center address**: server address in IPv4 address format, FQDN (IDN address can also be used). • **Device code**: a token required to connect to UGMC.

The UserGate company is continuously working to improve its software and provides SIEM product updates as part of the Security Update license module subscription (for more details on licensing, see the chapter SIEM Licensing). 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 SIEM downtime when planning update installation.

To install updates, follow these steps:

Name	Description
Step 1. Create a backup file.	Create a backup of SIEM state as described in the System Utilities section. 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.

Name	Description
Step 2. Install the updates.	In the **Device management** section, if the **New updates available** notification is present, click **Install now**. The system will install the downloaded updates, and when the installation completes, SIEM will reboot.

Device management

In the **General settings → UserGate → Device management** section, you can configure the following device parameters:

- diagnostics;
- clustering;
- server operations;
- backup;
- exporting and importing settings.

Diagnostics

In this block, you can manage diagnostic parameters required by UserGate technical support to resolve potential issues with the product.

Name	Description
Diagnostic details	The following logging levels are available: • **Off**: diagnostics logs are disabled • **Error**: log only SIEM server errors • **Warning**: log only errors and warnings • **Info**: log only errors, warnings, and additional information • **Debug**: log all possible events Logging at levels **Warning**, **Info** and **Debug** may reduce SIEM performance, so it is recommended to set the levels to **Error** or **Off** unless otherwise suggested by UserGate technical support.
Diagnostics logs	You can: • **Download logs**: download the diagnostic logs for sending them to UserGate support. Web console logs and system logs are available for download. Selected logs can only be

Name	Description
	downloaded after archiving them by clicking **Start archiving logs**. • **Clear log files**: delete archived (not currently active) logs.
Remote assistance	Remote assistance allows a UserGate technical support specialist to securely connect to the UserGate SIEM server to diagnose and resolve issues. To activate the remote assistant, the product must have SSH access to the remote assistance server. When enabled, the remote assistance ID and token are displayed, which must be provided to the UserGate technical support specialist.

Server operations

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

Name	Description
Server operations	• **Reboot**: reboot the SIEM server • **Shutdown**: shutdown the SIEM server
Upstream proxy settings to check licenses and updates	Configure the upstream HTTP(S) proxy server settings for license and software updates for the UserGate server. You must specify the IP address and port of the upstream proxy server. If necessary, specify login and password for authentication on the upstream proxy server.

System backup management

In this section, you can:

- create backups;
- restore the product from a backup;
- configure a schedule for exporting backups to a remote server;
- configure SSH keys.

To create a product backup:

In **General settings → UserGate → Device management → Backup management**, click **Create backup**.

The backup will begin. You can interrupt the process by clicking **Stop**.

When complete, the UserGate SIEM backup will be saved in the file `backup_PRODUCT_NODENAME_DATE.gpg`, where:

- `PRODUCT` is the product type: SIEM;
- `NODENAME` is the product node name;
- `DATE` is the date and time when the backup was created as YYYY-MM-DD-HH-MM. The time is in UTC+0 time zone.

The backup record will be displayed in the product event log.

To restore the product from a backup:

1. In **General settings → UserGate → Device management → Backup management**, click **Restore backup** and confirm the restore.

2. Specify the path to the UserGate SIEM backup file.

Restore will be suggested in the TTY console when the UserGate SIEM server reboots.

Administrators can create export rules that upload backups to remote servers on a schedule.

To create a product backup export rule:

1. In **General settings → UserGate → Device management → Backup management**, click **Add**.

2. On the **General** tab, specify a name for the rule.

3. In the **Remote server** tab, specify the parameters for the remote server:

- type: FTP or SSH;
- address;
- connection port;
- account login and password;
- path to an existing folder for saving export files.

> **Note**
> **You can use SSH keys to authenticate to a remote SSH server. To do this, you must first configure them.**

> **Attention!**
> **If you are creating a rule for an SSH server with SSH key authentication, you must test the connection to this server using the "Test connection" button. This test establishes an initial connection, during which the public key fingerprint is automatically added to the remote server. This ensures the security of subsequent connections.**

4. On the **Schedule** tab, specify the backup export time.

You can select one of the preset values or enter the time manually using cron format: .

When entering the time manually, you can also use the following characters:

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

5 Click **Save**.

You can use SSH keys to authenticate to a remote SSH server. To do this, you need to configure them.

To configure SSH keys:

1. In **General settings → UserGate → Device management → Backup management**, click **Configure SSH key**.

2. Click **Generate new key**.

An SSH key pair (private and public) will be generated. The public key will be displayed in the configuration window, and the private key will be automatically saved on the UserGate SIEM server.

> **Note**
> **If you already have an SSH key pair, you can manually add the private key to the UserGate SIEM server by clicking the "Upload Key" button.**

3. Add the public SSH key to the remote server.

By default, SSH keys are stored in the `/home/user/.ssh/` folder in the `authorized_keys` file.

Exporting and importing settings

In this section, you can export the current UserGate SIEM settings as export files in BIN format. These files may be needed later to restore the product settings or to import them into other SIEM nodes.

Exports can be performed manually or on a schedule. You can export all current settings (except cluster and license data) or just network settings. Network parameters include parameters of zones, interfaces, gateways, and routes. Network settings are configured in **General settings → Network** (see the Network Configuration section).

To export all product settings:

In **General settings → UserGate → Device management → Exporting and importing settings**, click **Export → Export all settings**.

The parameters will be saved in the `siem_core-siem_core@NODENAME_VERSION_DATE.bin` file, where:

- `NODENAME` is the product node name;
- `VERSION` is the UGOS version;
- `DATE` is the date and time when the backup was uploaded as YYYYMMDD_HHMMSS. The time is in UTC+0 time zone.

To export only the product's network settings:

In **General settings → UserGate → Device management → Exporting and importing settings**, click **Export → Export network settings**.

The parameters will be saved in the `network-siem_core-siem_core@NODENAME_VERSION_DATE.bin` file, where:

- `NODENAME` is the product node name;

- `VERSION` is the UGOS version;
- `DATE` is the date and time when the backup was uploaded as YYYYMMDD_HHMMSS. The time is in UTC+0 time zone.

Administrators can create export rules that upload product settings to remote servers on a scheduled basis. If the product nodes are clustered, creating an export rule on one node will propagate it to all nodes in the cluster. The settings for each node will be saved in a separate file during export.

To create a product settings export rule:

1. In **General settings → UserGate → Device management → Export and import settings**, click **Add**.

2. On the **General** tab, specify a name for the rule.

3. In the **Remote server** tab, specify the parameters for the remote server:

- type: FTP or SSH;
- address;
- connection port;
- account login and password;
- path to an existing folder for saving export files.

Note

You can use SSH keys to authenticate to a remote SSH server. To do this, you must first configure them.

Attention!

If you are creating a rule for an SSH server with SSH key authentication, you must test the connection to this server using the "Test connection" button. This test establishes an initial connection, during which the public key fingerprint is automatically added to the remote server. This ensures the security of subsequent connections.

4. On the **Schedule** tab, specify the settings export time.

You can select one of the preset values or enter the time manually using cron format: .

When entering the time manually, you can also use the following characters:

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

5. Click **Save**.

You can restore product settings from export files. These files do not contain cluster or license data, so after restoring the settings, you will need to reactivate the license and configure the clusters. Additionally, if you use multi-factor authentication via TOTP to log in to UserGate SIEM, you must re-add the initialization keys after the restore.

To restore product settings from an export file:

1. In **General settings → UserGate → Device management → Export and import settings**, click **Import**.

2. Select the export file.

3. In the **Import settings** window, select the import type (all settings or network settings only).

4. Click **Start**.

The settings will begin restoring. Once the process is complete, the UserGate SIEM server will reboot.

Administrators

Access to the SIEM web console is controlled by creating additional administrator accounts, assigning them access profiles, defining an administrator password management policy, and configuring web console access at the network zone level in terms of allowing the service in the zone properties.

> **Note**
>
> **A local superuser named Admin is created during the initial setup of SIEM.**

To create additional device administrator accounts, follow these steps:

Name	Description
Step 1. Create an administrator access profile.	In the **Administrators → Administrator profiles** section, click **Add** and enter the desired settings.
Step 2. Create an administrator account and assign it one of the 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. 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. 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.
Permissions	The list of web console tree objects available for delegation. The following access options are available: • No access • Read only • Read and write
User roles	Defines the user roles for performing actions on incidents and analytics rules assigned to the administrators with this profile. By default, there are the following roles: • Administrator

Name	Description
	• Supervisor • Investigator • Analyst The description of the permissions of the roles defined in the system by default is given in the table below.

Permissions for roles created in the system by default:

Role permission	Description	Administrator	Supervisor	Investigator	Analyst
Assignable user	A user with this permission can be assigned to an incident when creating or editing an incident.		+	+	+
Assign incidents	Ability to assign users to incidents when creating or editing an incident.		+	+	+
Close incidents	The ability to close an incident.		+	+	+
Create incidents	The ability to create incidents.		+	+	+
Edit incidents	The ability to edit incidents.		+	+	+
Reopen incidents	The ability to reopen incidents.		+	+	+
Edit watchers	The ability to add and remove watchers.		+	+	+
Add comments	The ability to comment on incidents.		+	+	+
Delete all comments	The ability to delete any comments made on incidents.		+		
Delete own comments	The ability to delete own comments made on incidents.		+	+	+

Role permission	Description	Administrator	Supervisor	Investigator	Analyst
Edit all comments	The ability to edit all comments made on incidents.		+		
Edit own comments	The ability to edit own comments made on incidents.		+	+	+
Create attachments	The ability to create attachments to incidents.		+	+	+
Delete all attachments	The ability to delete all attachments.		+	+	
Delete own attachments	The ability to delete own attachments.		+	+	+
Edit observables	The ability to create and edit observables.		+	+	+
Update enrichments	The ability to update observables' enrichments.		+	+	
Generate report	The ability to generate and download/send reports.		+	+	+
Add triggered alerts/logs to incident	The ability to add triggered alerts/logs in to the incident.		+	+	+
Remove all triggered alerts/logs from incident	The ability to remove all triggered alerts/logs from the incident.		+	+	
Remove own triggered alerts/logs from incident	The ability to remove own triggered alerts/logs from the incident.		+	+	+
Create incident schema	The ability to create incident schemas.		+		
Edit incident schema	The ability to edit incident schemas.		+		

Role permission	Description	Administrator	Supervisor	Investigator	Analyst
Delete incident schema	The ability to delete incident schemas.		+		
Set default incident schema	The ability to set default incident schemas.		+		
Create incident state	The ability to create incident states.	+	+		
Edit incident state	The ability to edit incident states.	+	+		
Delete incident state	The ability to delete incident states.	+	+		
Create incident type	The ability to create incident types.	+	+		
Edit incident type	The ability to edit incident types.	+	+		
Delete incident type	The ability to delete incident types.	+	+		
Create incident resolution	The ability to create incident resolutions.	+	+		
Edit incident resolution	The ability to edit incident resolutions.	+	+		
Delete incident resolution	The ability to delete incident resolutions.	+	+		
Create analytics rule	The ability to create analytics rules.		+	+	
Delete analytics rule	The ability to delete analytics rules.		+		
Edit analytics rule	The ability to edit analytics rules.		+	+	
Enable/disable analytics rule	The ability to enable or disable analytics rules.		+	+	

Role permission	Description	Administrator	Supervisor	Investigator	Analyst
Execute analytics rule	The ability to execute an analytics rule not in real time.		+		
Create response action	The ability to create response actions.		+	+	
Edit response action	The ability to edit response actions.		+	+	
Delete response action	The ability to delete response actions.		+	+	
Enable/disable response action	The ability to enable or disable response actions.		+	+	
Create a UserGate sensor	The ability to create UserGate sensors.	+	+		
Edit a UserGate sensor	The ability to edit UserGate sensors.	+	+		
Enable/disable a UserGate sensor	The ability to enable/ disable UserGate sensors.	+	+		
Delete a UserGate sensor	The ability to delete UserGate sensors.	+	+		
Create SNMP sensor	The ability to create SNMP sensors.	+	+		
Edit SNMP sensors	The ability to edit SNMP sensors.	+	+		
Enable/disable SNMP sensor	The ability to enable/ disable SNMP sensors.	+	+		
Delete a SNMP sensor	The ability to delete SNMP sensors.	+	+		
Create WMI sensor	The ability to create WMI sensors.	+	+		
Edit WMI sensors	The ability to edit WMI sensors.	+	+		

Role permission	Description	Administrator	Supervisor	Investigator	Analyst
Enable/disable WMI sensor	The ability to enable/ disable WMI sensors.	+	+		
Delete a WMI sensor	The ability to delete WMI sensors.	+	+		
Add SNMP MIB file	The ability to add SNMP MIB files.	+	+		
Delete SNMP MIB file	The ability to delete SNMP MIB files.	+	+		
Create connectors	The ability to create connectors.	+	+		
Edit connectors	The ability to edit connectors.	+	+		
Delete connectors	The ability to delete connectors.	+	+		
Create Syslog rule	The ability to create Syslog rules.	+	+		
Delete Syslog rule	The ability to delete Syslog rules.	+	+		
Edit Syslog rule and Syslog connector	The ability to edit Syslog rules and configure Syslog.	+	+		
Enable/disable Syslog rule	The ability to enable or disable Syslog rules.	+	+		
Create email group	The ability to create emails and email groups.	+	+		
Edit email group	The ability to edit emails and email groups.	+	+		
Delete email group	The ability to delete emails and email groups.	+	+		
Create phone groups	The ability to create phones and phone groups.	+	+		

Role permission	Description	Administrator	Supervisor	Investigator	Analyst
Edit phone group	The ability to edit phones and phone groups.	+	+		
Delete phone group	The ability to delete phones and phone groups.	+	+		
Create commands	The ability to create commands to connectors.	+	+		
Edit commands	The ability to edit commands to connectors.	+	+		
Delete commands	The ability to delete commands to connectors.	+	+		
Create notification profile	The ability to create notification profiles.	+	+		
Edit notification profile	The ability to edit notification profiles.	+	+		
Delete notification profile	The ability to edit notification profiles.	+	+		
Create triggered alert category	The ability to create triggered alert categories.	+	+		
Edit triggered alert category	The ability to edit triggered alert categories.	+	+		
Delete triggered alert category	The ability to delete triggered alert categories.	+	+		
Edit enrichment setting	The ability to edit an enrichment setting.	+	+		
Enable/disable enrichment service	The ability to enable/disable enrichment services.	+	+		
Create normalization rule	The ability to create log normalization rules.	+	+		

Role permission	Description	Administrator	Supervisor	Investigator	Analyst
Edit normalization rule	The ability to edit log normalization rules.	+	+		
Delete normalization rule	The ability to delete log normalization rules.	+	+		
Enable/Disable normalization rules	The ability to enable/ disable log normalization rules.	+	+		

For more details on role permissions, see the User Roles and Role Permissions section.

> **Note**
>
> **Do not confuse roles and role permissions with permissions for objects in the management console. Object permissions allow the user to view or edit certain objects, such as incidents, whereas roles and role permissions allow a user to perform certain actions with object elements — e.g., create an incident, add an assignee to it, etc. Generally, for a user to work anywhere in a system, object permissions and certain role permissions need to be delegated to the user.**

An administrator can configure additional administrator account protection settings, such as password complexity and temporary account blocking on exceeding the max failures limit of authentication attempts.

To configure the above settings, follow these steps:

Name	Description
Step 1. Configure the password policy.	In the **Administrators → Administrators** section, click **Configure**.
Step 2. Fill in the relevant fields.	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.

Name	Description
	• **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.

Note

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

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

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

Note

Web console access should not be allowed for zones connected to uncontrolled networks (e.g. the Internet).

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 section. For more details on configuring zone access control, see the section Zone Configuration.

Certificate Management

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

SIEM 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. Use the exported SSL inspection certificate file to set it as the local CA on user computers. • **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, SIEM does not allow the export of private keys for certificates.**

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

Name	Description
Step 1. Start the import procedure.	Click **Import**.
Step 2. Fill in the relevant fields.	Provide values for these fields: • **Name**: the name under which the certificate will be displayed in the certificate list. • **Description**: a description of the certificate. • **Certificate file**: the certificate data file. • **Private key**: 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.

Auth servers

Authentication servers (auth servers) are external sources of user accounts used for authorization in the UserGate SIEM management web console. SIEM 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 SIEM administrators via Active Directory/FreeIPA domains.

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

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

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

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

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

RADIUS Authentication Server

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

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

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

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

TACACS+ Authentication Server

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

To add a 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.

Name	Description
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. For more details on creating and configuring profiles, see the section Authentication Profiles.

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 Roles and Role Permissions

A user role is a set of role permissions. A role permission grants an administrator the ability to perform certain actions – e.g., add or remove an attachment from an

existing incident, create a triggered alert rule, create or close an incident, etc. Roles are assigned to administrator profiles, which are, in turn, assigned to administrators. For more details on creating administrators and administrator profiles, see the section Administrators.

To create a role and assign certain permissions to it, follow these steps:

Name	Description
Step 1. Create a role.	In the **User roles** section, click **Add** and provide a name and description for the new role.
Step 2. Add the desired permissions to the role just created.	In the **Role permissions** section, select the desired permission, and click **Add** to add it to the role created earlier.

The following role permissions can be added for users:

Name	Description
Assignable user	Users with this permission may be assigned to incidents. An assignee can be added during the creation or editing of an incident.
Assign incidents	The ability to assign incidents to other people. An assignee can be added during the creation or editing of an incident.
Close incidents	The ability to close an incident. It can often be a useful arrangement when developers resolve incidents and testers close them. You can close an incident in the **Incidents ➔** tab, where N is the ordinal number of the incident. An incident can only be closed from the states for which a transition to the "Closed" state is configured in the incident schema. For more details, see Incident Settings.
Create incidents	The ability to create incidents. Incidents can be created manually in the **Incidents ➔ Incidents log** tab or automatically when an analytics rule is triggered. For more details on how to create incidents, see the section Creating Security Incidents.
Edit incidents	The ability to edit incidents. You can edit an incident in the **Incidents ➔** tab, where N is the ordinal number of the incident. For more details, see the section Incident Details.

Name	Description
Reopen incidents	The ability to reopen incidents. You can reopen an incident in the **Incidents ➜** tab, where N is the ordinal number of the incident.
Edit watchers	The ability to add and remove watchers. Incident watchers can be added during the creation or editing of an incident.
Add comments	The ability to comment on incidents. You can comment on an incident in the **Incidents ➜** tab, where N is the ordinal number of the incident, in the **Activity** section.
Delete all comments	The ability to delete any comments made on incidents. You can view the comments for an incident in the **Incidents ➜** t ab, where N is the ordinal number of the incident, in the **Activit y** section.
Delete own comments	The ability to delete own comments made on incidents. You can view the comments for an incident in the **Incidents ➜** t ab, where N is the ordinal number of the incident, in the **Activit y** section.
Edit all comments	The ability to edit all comments made on incidents. You can view the comments for an incident in the **Incidents ➜** t ab, where N is the ordinal number of the incident, in the **Activit y** section.
Edit own comments	The ability to edit own comments made on incidents. You can view the comments for an incident in the **Incidents ➜** t ab, where N is the ordinal number of the incident, in the **Activit y** section.
Create attachments	The ability to create attachments to incidents. Attachments can be added to an incident in the **Incidents** tab during the creation or editing of the incident. The attachments are displayed in the **Incidents ➜** tab, where N is the ordinal number of the incident, in the **Attachments** section.
Delete all attachments	The ability to delete all attachments. The incident's attachments are displayed in the **Incidents ➜** tab , where N is the ordinal number of the incident, in the **Attachme nts** section.
Delete own attachments	The ability to delete own attachments.

Name	Description
	The incident's attachments are displayed in the **Incidents →** tab , where N is the ordinal number of the incident, in the **Attachments** section.
Edit observables	The ability to create and edit observables. Observables can be added in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Observables** section. For more details on observables, see the section Incident Details.
Update enrichments	The ability to update observables' enrichments. The list of external enrichment services is available under **Libraries → External enrichment services** on the **Settings** tab. For more details on external enrichment services, see the section External Enrichment Services.
Generate report	The ability to generate and download/send reports. Incident reports can be created in the **Incidents →** tab, where N is the ordinal number of the incident. For more details, see the section Incident Details.
Add triggered alerts/logs to incident	The ability to add triggered alerts/logs in to the incident. Logs can be added in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Logs** section. For more details on logs and triggered alerts, see the sections Analytics Search and Triggered Alerts, respectively.
Remove all triggered alerts/logs from incident	The ability to remove all triggered alerts/logs from the incident. Triggered alerts and logs are displayed in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Triggered alerts** and **Logs** sections, respectively. For more details on logs and triggered alerts, see the sections Analytics Search and Triggered Alerts, respectively.
Remove own triggered alerts/logs from incident	The ability to remove own triggered alerts/logs from the incident. Triggered alerts and logs are displayed in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Triggered alerts** and **Logs** sections, respectively. For more details on logs and triggered alerts, see the sections Analytics Search and Triggered Alerts, respectively.
Create incident schema	The ability to create incident schemas. Incident schemas are available under **Incident settings → Incident schema** in the **Settings** tab. For more details, see the section Incident Settings.

Name	Description
Edit incident schema	The ability to edit incident schemas. Incident schemas are available under **Incident settings → Incident schema** in the **Settings** tab. For more details, see the section Incident Settings.
Delete incident schema	The ability to delete incident schemas. Incident schemas are available under **Incident settings → Incident schema** in the **Settings** tab. For more details, see the section Incident Settings.
Set default incident schema	The ability to set default incident schemas. In UserGate SIEM, one default incident schema is available under **Incident settings → Incident schema** in the **Settings** tab. For more details, see the section Incident Settings.
Create incident state	The ability to create incident states. The list of incident states is displayed under **Incident settings → Incident states** in the **Settings** tab. For more details, see the section Incident Settings.
Edit incident state	The ability to edit incident states. The list of incident states is displayed under **Incident settings → Incident states** in the **Settings** tab. For more details, see the section Incident Settings.
Delete incident state	The ability to delete incident states. The list of incident states is displayed under **Incident settings → Incident states** in the **Settings** tab. For more details, see the section Incident Settings.
Create incident type	The ability to create incident types. Incident types are available in the **Incident settings → Incident types** section of the **General settings** tab. For more details, see the section Incident Settings.
Edit incident type	The ability to edit incident types. Incident types are available in the **Incident settings → Incident types** section of the **General settings** tab. For more details, see the section Incident Settings.
Delete incident type	The ability to delete incident types. Incident types are available in the **Incident settings → Incident types** section of the **General settings** tab. For more details, see the section Incident Settings.

Name	Description
Create incident resolution	The ability to create incident resolutions. The list of incident resolutions is displayed in the **Incident settings → Incident resolutions** section of the **General settings** tab. For more details, see the section Incident Settings.
Edit incident resolution	The ability to edit incident resolutions. The list of incident resolutions is displayed in the **Incident settings → Incident resolutions** section of the **General settings** tab. For more details, see the section Incident Settings.
Delete incident resolution	The ability to delete incident resolutions. The list of incident resolutions is displayed in the **Incident settings → Incident resolutions** section of the **General settings** tab. For more details, see the section Incident Settings.
Create analytics rule	The ability to create analytics rules. Analytics rules can be created in the **Analytics → Analytics rules** tab. For more details, see the Analytics section.
Delete analytics rule	The ability to delete analytics rules. Analytics rules are displayed in the **Analytics → Analytics rules** tab. For more details, see the Analytics section.
Edit analytics rule	The ability to edit analytics rules. Analytics rules are displayed in the **Analytics → Analytics rules** tab. For more details, see the Analytics section.
Enable/disable analytics rule	The ability to enable or disable analytics rules. Analytics rules are displayed in the **Analytics → Analytics rules** tab. For more details, see the Analytics section.
Execute analytics rule	The ability to execute an analytics rule not in real time. Analytics rules are displayed in the **Analytics → Analytics rules** tab. For more details, see the Analytics section.
Create response action	The ability to create response actions. Response actions can be created in the **Analytics --> Response actions** tab. For more details, see the section Response Actions.
Edit response action	The ability to edit response actions. Response actions are displayed in the **Analytics --> Response actions** tab. For more details, see the section Response Actions.

Name	Description
Delete response action	The ability to delete response actions. Response actions are displayed in the **Analytics --> Response actions** tab. For more details, see the section Response Actions.
Enable/disable response action	The ability to enable or disable response actions. Response actions are displayed in the **Analytics --> Response actions** tab. For more details, see the section Response Actions.
Create a UserGate sensor	The ability to create UserGate sensors. UserGate sensors can be created under **Sensors → UserGate sensors** in the **Settings** tab. For more details, see UserGate Sensors.
Edit a UserGate sensor	The ability to edit UserGate sensors. UserGate sensors are available under **Sensors → UserGate sensors** in the **Settings** tab. For more details, see UserGate Sensors.
Enable/disable a UserGate sensor	The ability to enable/disable UserGate sensors. UserGate sensors are available under **Sensors → UserGate sensors** in the **Settings** tab. For more details, see UserGate Sensors.
Delete a UserGate sensor	The ability to delete UserGate sensors. UserGate sensors are available under **Sensors → UserGate sensors** in the **Settings** tab. For more details, see UserGate Sensors.
Create SNMP sensor	The ability to create SNMP sensors. SNMP sensors can be created under **Sensors → SNMP sensors** in the **General settings** tab. For more details, see the SNMP Sensors section.
Edit SNMP sensors	The ability to edit SNMP sensors. SNMP sensors are available under **Sensors → SNMP sensors** in the **General settings** tab. For more details, see the SNMP Sensors section.
Enable/disable SNMP sensor	The ability to enable/disable SNMP sensors. SNMP sensors are available under **Sensors → SNMP sensors** in the **General settings** tab. For more details, see the SNMP Sensors section.

Name	Description
Delete a SNMP sensor	The ability to delete SNMP sensors. SNMP sensors are available under **Sensors → SNMP sensors** in the **General settings** tab. For more details, see the SNMP Sensors section.
Create WMI sensor	The ability to create WMI sensors. WMI sensors can be created under **Sensors → WMI sensors** in the **General settings** tab. For more details, see the section WMI Sensors.
Edit WMI sensors	The ability to edit WMI sensors. WMI sensors are available under **Sensors → WMI sensors** in the **General settings** tab. For more details, see the section WMI Sensors.
Enable/disable WMI sensor	The ability to enable/disable WMI sensors. WMI sensors are available under **Sensors → WMI sensors** in the **General settings** tab. For more details, see the section WMI Sensors.
Delete a WMI sensor	The ability to delete WMI sensors. WMI sensors are available under **Sensors → WMI sensors** in the **General settings** tab. For more details, see the section WMI Sensors.
Add SNMP MIB file	The ability to add SNMP MIB files. MIB files can be added under **Sensors → SNMP MIB management** in the **General settings** tab. For more details, see the SNMP MIB Management section.
Delete SNMP MIB file	The ability to delete SNMP MIB files. MIB files are displayed under **Sensors → SNMP MIB management** in the **General settings** tab. For more details, see the SNMP MIB Management section.
Create connectors	The ability to create connectors. Connectors can be created under **Sensors → Connectors** in the **General settings** tab. For more details, see the Connectors section.
Edit connectors	The ability to edit connectors. Connectors can are available under **Sensors → Connectors** in the **General settings** tab. For more details, see the Connectors section.

Name	Description
Delete connectors	The ability to delete connectors. Connectors can are available under **Sensors → Connectors** in the **General settings** tab. For more details, see the Connectors section.
Create Syslog rule	The ability to create Syslog rules. Syslog rules can be created in the **Log Collector → Syslog** section of the **General settings** tab.
Delete Syslog rule	The ability to delete Syslog rules. Syslog rules are displayed in the **Log Collector → Syslog** section of the **General settings** tab.
Edit Syslog rule and Syslog connector	The ability to edit Syslog rules and configure Syslog. The created Syslog rules are available in the **Log Collector → Syslog** section of the **General settings** tab.
Enable/disable Syslog rule	The ability to enable or disable Syslog rules. Syslog rules are available in the **Log Collector → Syslog** section of the **General settings** tab.
Create email group	The ability to create emails and email groups. Emails and email groups can be created in the **Libraries → Emails** section of the **General settings** tab. For more details, see the Emails section.
Edit email group	The ability to edit emails and email groups. Emails and email groups are available in the **Libraries → Emails** section of the **General settings** tab. For more details, see the E mails section.
Delete email group	The ability to delete emails and email groups. Emails and email groups are available in the **Libraries → Emails** section of the **General settings** tab. For more details, see the E mails section.
Create phone groups	The ability to create phones and phone groups. Phones and phone groups can be created in the **Libraries → Phones** section of the **General settings** tab. For more details, see the Emails section.
Edit phone group	The ability to edit phones and phone groups. Phones and phone groups are available in the **Libraries → Phones** section of the **General settings** tab. For more details, see the Emails section.

Name	Description
Delete phone group	The ability to delete phones and phone groups. Phones and phone groups are available in the **Libraries → Phones** section of the **General settings** tab. For more details, see the Emails section.
Create commands	The ability to create commands to connectors. Commands to connectors can be created under **Libraries → Commands** in the **General settings** tab. For more details, see the Commands section.
Edit commands	The ability to edit commands to connectors. Commands to connectors are available under **Libraries → Commands** in the **General settings** tab. For more details, see the Commands section.
Delete commands	The ability to delete commands to connectors. Commands to connectors are available under **Libraries → Commands** in the **General settings** tab. For more details, see the Commands section.
Create notification profile	The ability to create notification profiles. In the **Libraries → Notification profiles** section of the **General settings** tab, you can create two types of profiles: SMPP and SMTP. For more details on notification profiles, see the section Notification Profiles.
Edit notification profile	The ability to edit notification profiles. The list of profiles is available in the **Libraries → Notification profiles** section of the **General settings** tab. For more details on notification profiles, see the section Notification Profiles.
Delete notification profile	The ability to edit notification profiles. The list of profiles is available in the **Libraries → Notification profiles** section of the **General settings** tab. For more details on notification profiles, see the section Notification Profiles.
Create triggered alert category	The ability to create triggered alert categories. Triggered alert categories can be created in the **Libraries → Triggered alert categories** section of the **General settings** tab. For more details on triggered alert categories, see the section Triggered Alert Categories.
Edit triggered alert category	The ability to edit triggered alert categories. The list of triggered alert categories is available in the **Libraries → Triggered alert categories** section of the **General settings**

Name	Description
	tab. For more details on triggered alert categories, see the section Triggered Alert Categories.
Delete triggered alert category	The ability to delete triggered alert categories. The list of triggered alert categories is available in the **Libraries → Triggered alert categories** section of the **General settings** tab. For more details on triggered alert categories, see the section Triggered Alert Categories.
Edit enrichment setting	The ability to edit an enrichment setting. The list of external enrichment services is available in the **Librar ies → External enrichment services** section of the **General settings** tab. For more details on external enrichment services, see the section External Enrichment Services.
Enable/disable enrichment service	The ability to enable/disable enrichment services. The list of external enrichment services is available in the **Librar ies → External enrichment services** section of the **General settings** tab. For more details on external enrichment services, see the section External Enrichment Services.
Create normalization rule	The ability to create normalization rules. Normalization rules can be created in the **Logs → Custom log normalization** section of the **Logs and reports** tab. For more details on triggered alert categories, see the Custom log normalization section.
Edit normalization rule	The ability to edit normalization rules. Normalization rules are available in the **Logs → Custom log normalization** section of the **Logs and reports** tab. For more details on triggered alert categories, see the Custom log normalization section.
Delete normalization rule	The ability to delete normalization rules. Normalization rules are available in the **Logs → Custom log normalization** section of the **Logs and reports** tab. For more details on triggered alert categories, see the Custom log normalization section.
Enable/Disable normalization rules	The ability to enable/disable normalization rules. Normalization rules are available in the **Logs → Custom log normalization** section of the **Logs and reports** tab. For more details on triggered alert categories, see the Custom log normalization section.

After a role has been created, it can be assigned to administrator profiles.

User Catalogs

Under **Users catalogs**, you can add an LDAP connector to give the SIEM servers the access to the AD server. The access to AD allows you to update user name information in logs imported from various sensors, if necessary.

To create an LDAP Connector, click **Add** and provide these settings:

Name	Description
Enabled	Enables or disables this LDAP connector.
Name	The name of the LDAP connector.
Description	LDAP connector description.
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.
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 you filled in the LDAP connector parameters, you can verify if the configuration is correct by clicking the **Check connection** button. If your settings are correct, the system will report that; otherwise, it will tell you why it cannot connect.

Expanding the System Partition

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

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

Note

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

Clustering and High Availability

General Principles

To build a failover SIEM solution, you must set up two types of clusters — a configuration cluster and a failover cluster.

A configuration cluster is a grouping of several nodes into a single cluster. The nodes in a configuration cluster "see" each other and synchronize their configurations. Some settings are unique for each cluster node, such as network interface settings, gateways, routes, and diagnostic settings.

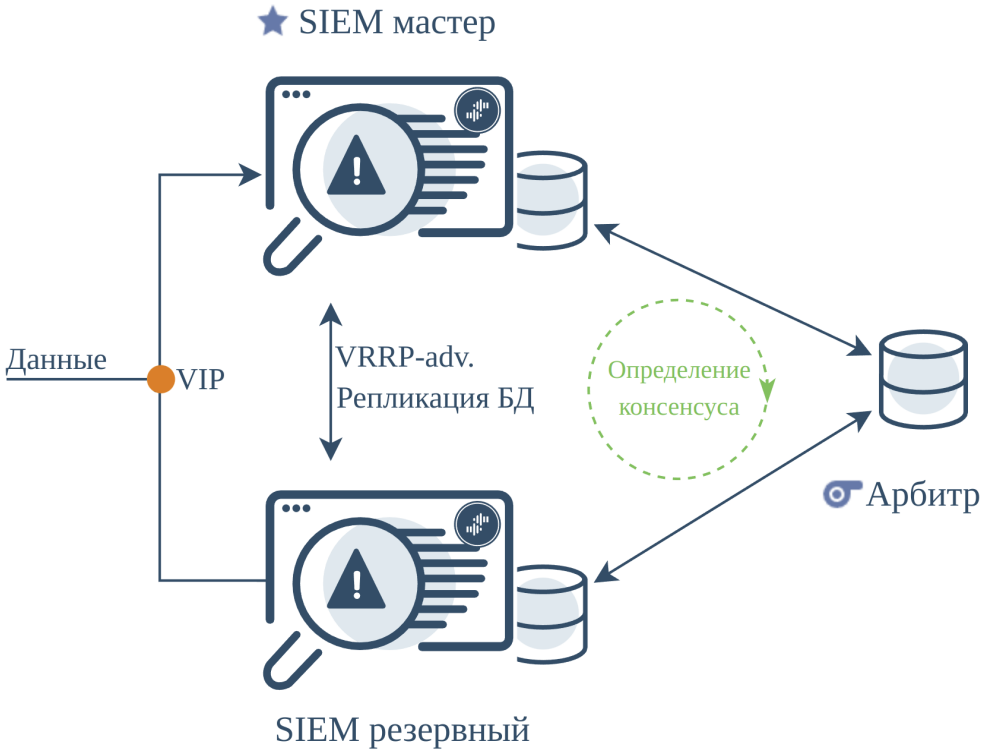
A high availability cluster ensures network operations on the nodes in the configuration cluster, such as a switched virtual IP that migrates from one node to another according to specific rules.

A high availability cluster and a configuration cluster operate on different protocols and in different environments. Information about the high availability cluster status is distributed between nodes via the configuration cluster. This information refers specifically to status information, not to the data the high availability cluster uses to support its operations. The status of cluster nodes is displayed in the web console.

A failover SIEM solution should at least consist of two SIEM nodes and an arbitration node.

The maximum number of nodes in a cluster is four, one of which is the arbitrator.

An arbitration node determines the quorum in a configuration to ensure data consistency. It doesn't act as a full-fledged SIEM (data collection, storage, and processing), but participates in determining the majority according to the distributed consensus algorithm for operations coordination in a failover cluster.



At this stage, a failover SIEM cluster supports the **Active-Passive** operation mode. In the Active-Passive mode, one node acts as the master node processing traffic, while the other acts as a backup. One or more virtual IP addresses are specified for the cluster. The virtual addresses are switched from the master node to one of the backup nodes under the following circumstances:

- A backup node gets no confirmation that the master instance is online — for example, if it is offline or the nodes are unavailable on the network.

- A change in the master node priority. For example, the master node priority is reduced if one or more network interfaces to which virtual IP addresses are assigned are disabled. A node's priority can also be explicitly changed by changing the master node in the device's web console.
- A software failure.

Creating a failover SIEM cluster

To create a failover SIEM cluster, you must set up a configuration cluster first, then add all the required nodes to it, and finally set up a failover cluster.

Configuration cluster settings

To create a configuration cluster, follow these steps:

1. Perform initial configuration on the first node. See the Initial Configuration chapter.

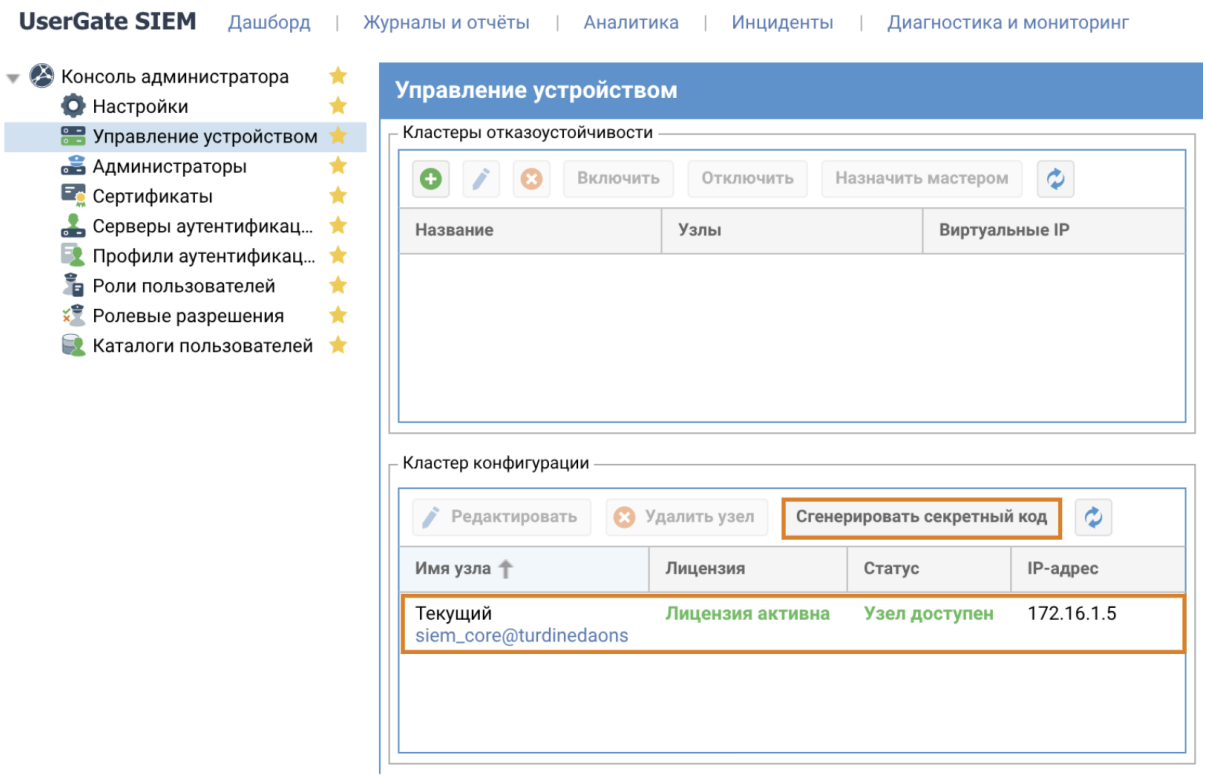
2. On the first node, configure the zone containing the network interfaces through which cluster replication will be carried out.

In the Zones section, create a new dedicated zone for cluster settings replication. Allow the following services in the zone's access settings:

- Administrative console
- Cluster.

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

3. In the **Configuration cluster** section, specify the IP address that will be used to communicate with other cluster nodes.



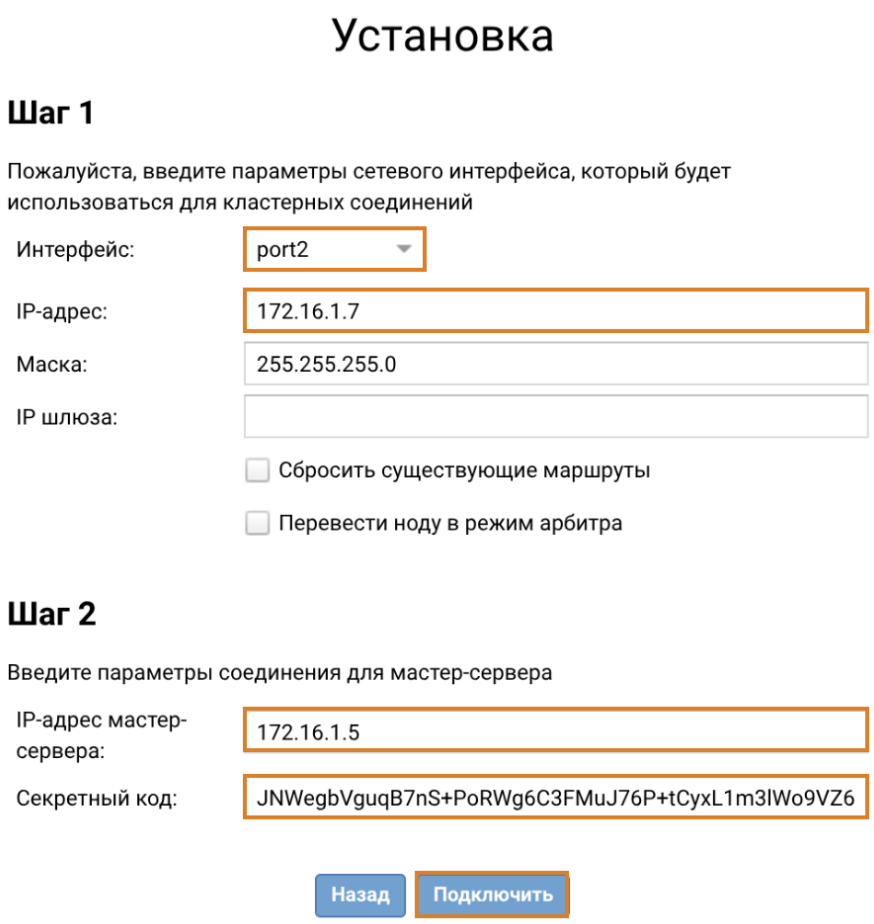
4. Generate a secret code on the first node by clicking the button of the same name in the **Configuration cluster** section. Copy the generated code to the clipboard. This secret code is required for one-time authorization of the next node before adding it to the cluster.

5. Connect the second node to the cluster.

During the initial installation of the second node, connect to its web console and select the installation language.

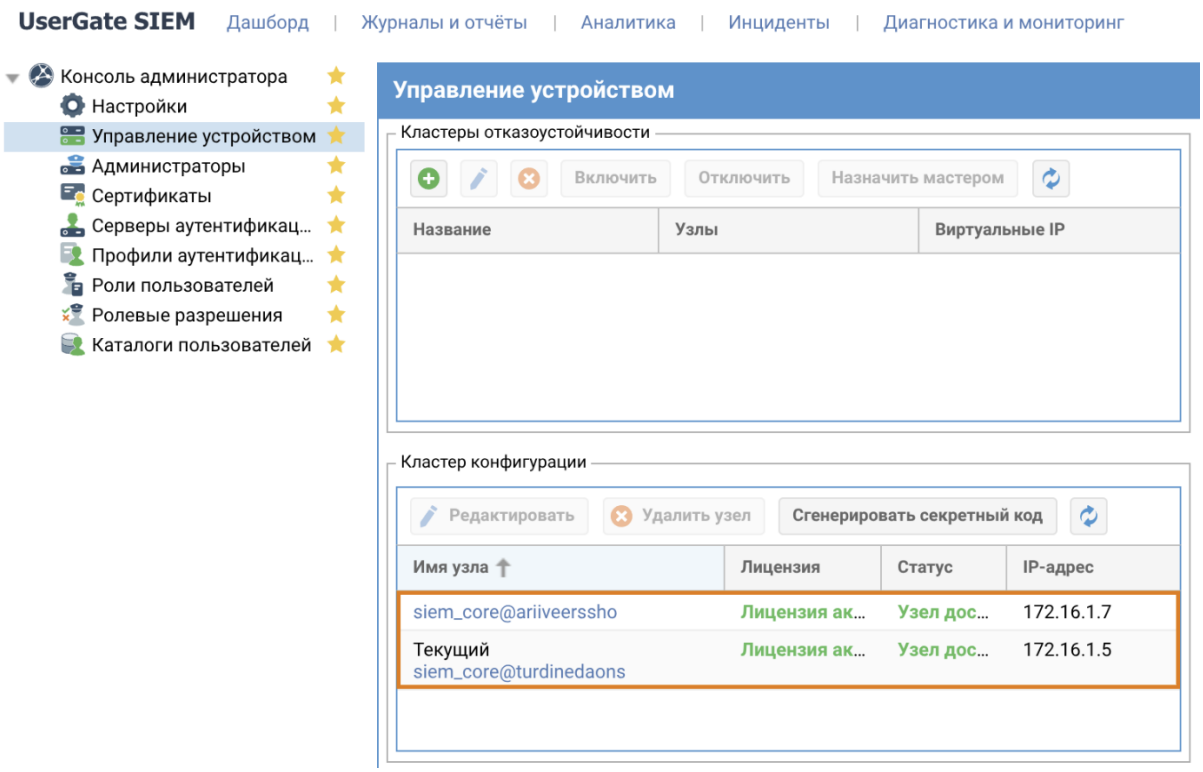
Specify the network interface that will be used to connect to the first cluster node and assign it an IP address. Both cluster nodes must be on the same subnet. Otherwise, you need to specify the IP address of the gateway through which the first cluster node will be accessible.

Specify the IP address of the first node configured at Step 3, enter the secret code, and click **Connect**:



If the IP addresses of the cluster configured at Step 2 are assigned correctly, the second node will be added to the cluster, and the settings from the first cluster node will be replicated on the second one.

The status of the configuration cluster nodes is displayed in the **Configuration cluster** section:



6. Assign zones to the second node's network interfaces. In the web console for the second cluster node, go to the **Network → Interfaces** and assign a correct zone to each network interface. The zones and their settings are obtained as a result of data replication from the first cluster node.

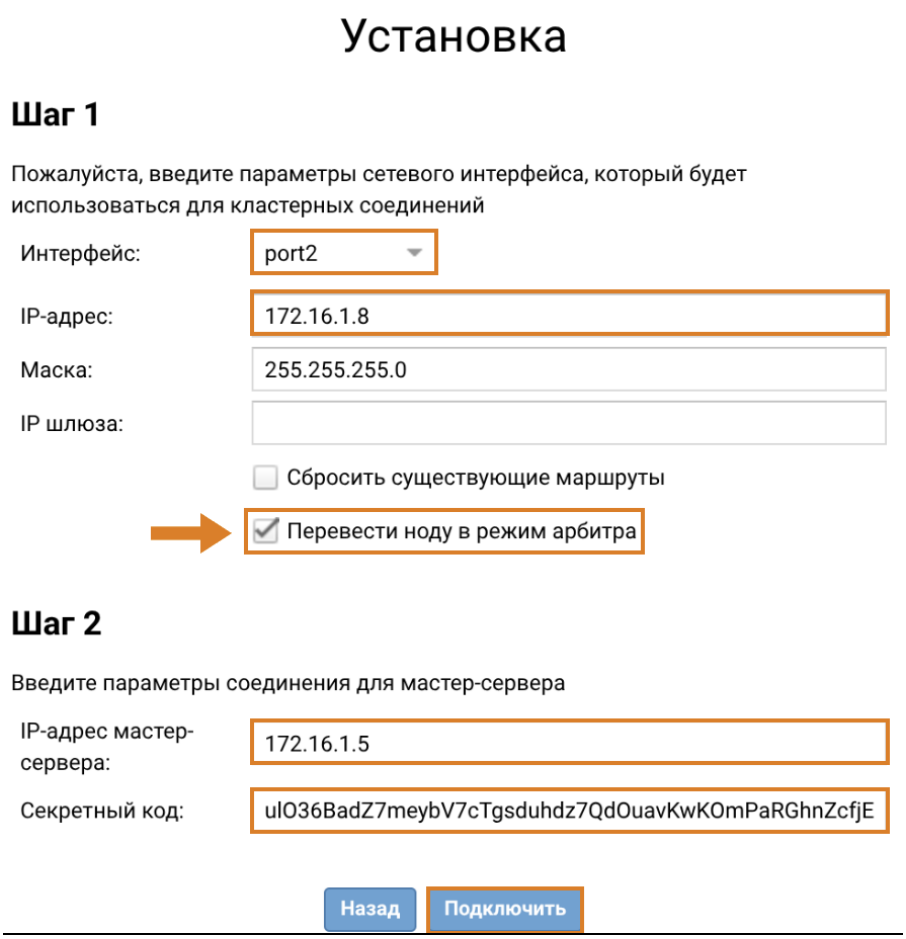
7. Connect the node that will act as the arbitrator to the cluster.

Generate a secret code on the first node by clicking the button of the same name in the **Configuration cluster** section. Copy the generated code to the clipboard. This code is required for one-time authorization of a new node before adding it to the cluster.

During the initial installation of the third node, connect to its web console and select the installation language.

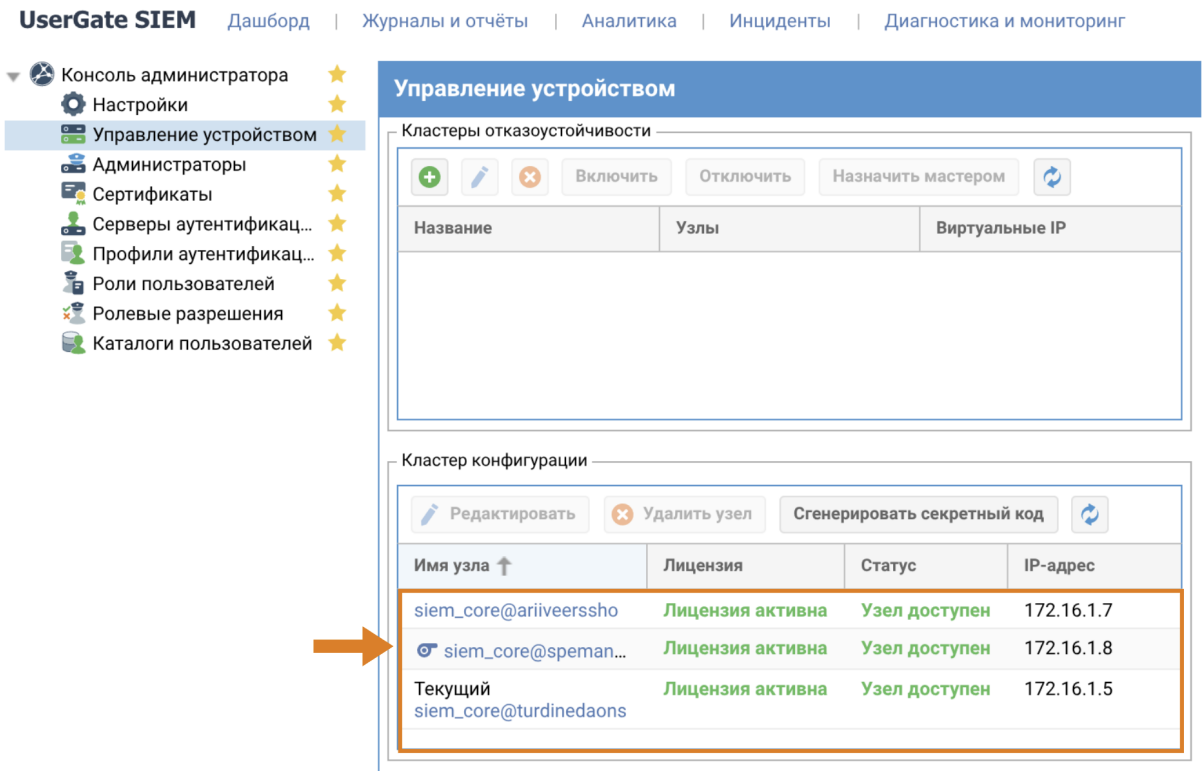
Specify the network interface that will be used to connect to the first cluster node and assign it an IP address. Both cluster nodes must be on the same subnet. Otherwise, you need to specify the IP address of the gateway through which the first cluster node will be accessible. Select the **Switch the node to arbitrator mode** checkbox.

Specify the IP address of the first node configured at Step 3, enter the secret code, and click **Connect**:



If the IP addresses of the cluster configured at Step 2 are assigned correctly, the second node will be added to the cluster, and the settings from the first cluster node will be replicated on the new one.

The status of the configuration cluster nodes is displayed in the **Configuration cluster** section. The arbitrator node is marked in the list of cluster nodes with the corresponding icon:



8. Configure individual parameters for each cluster node (optional). Configure gateways, routes, OSPF and BGP parameters for each node.

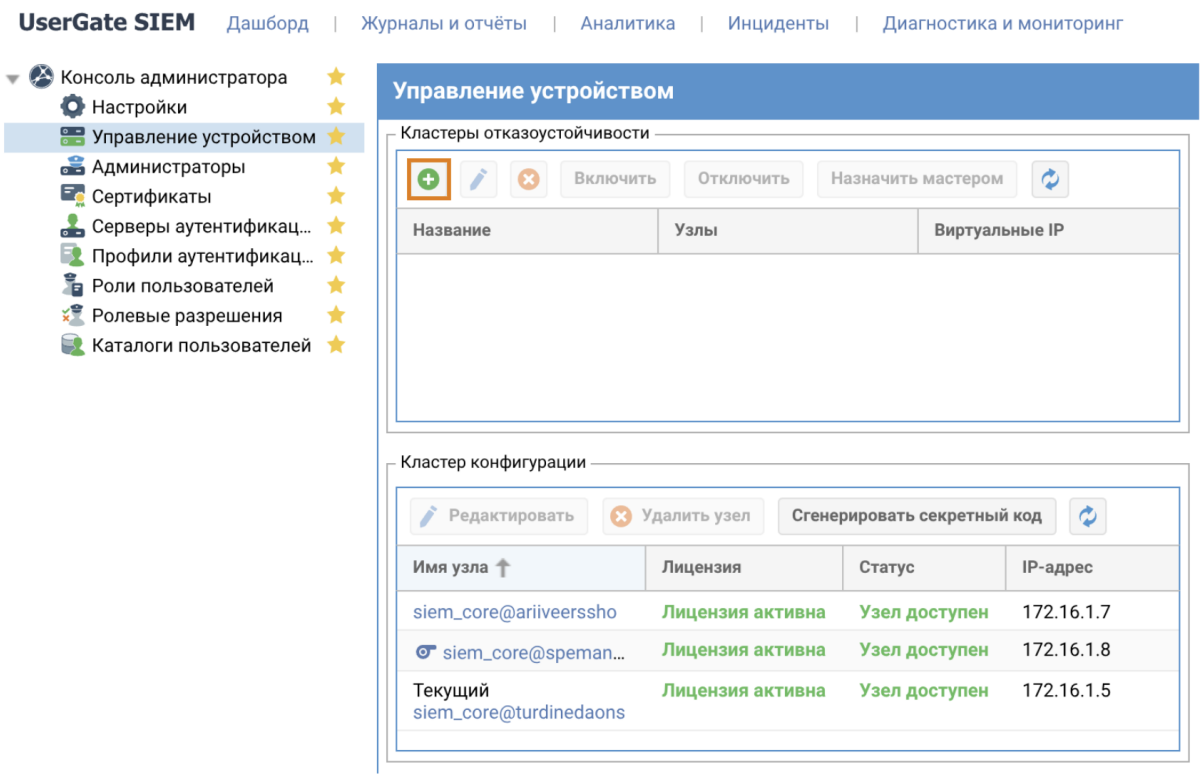
Settings for high availability clusters

Configuration cluster nodes can be combined into a HA cluster. Active-Passive HA cluster mode is currently supported.

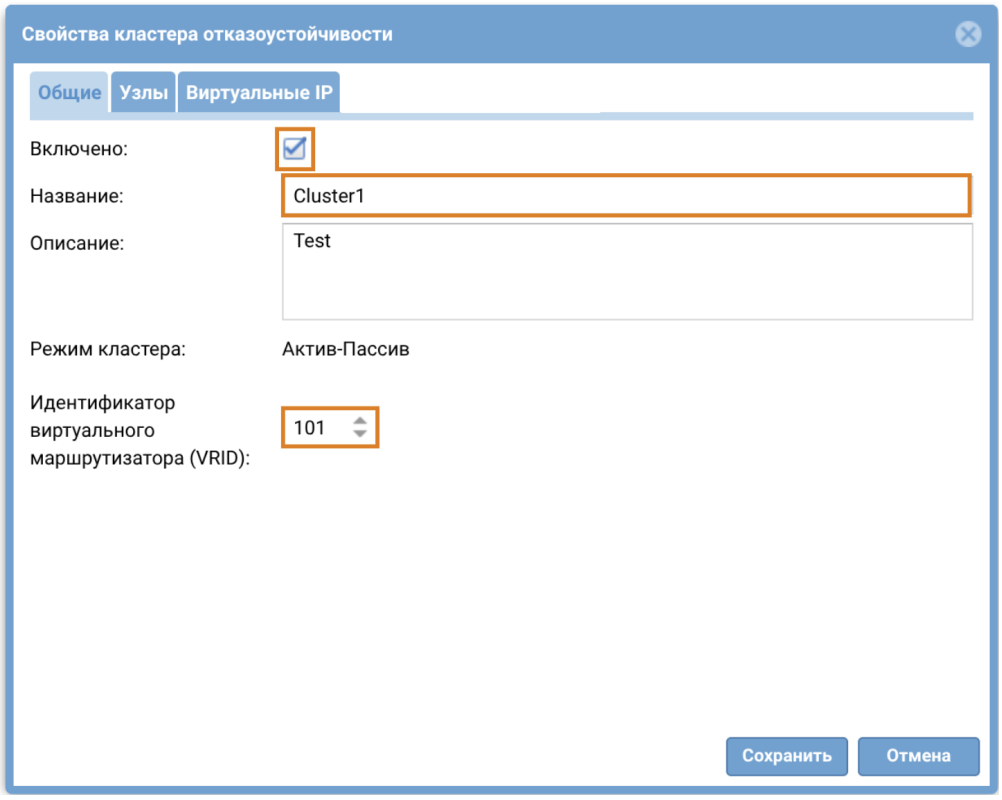
In the Active-Passive mode, one of the SIEM nodes operates as the master node that receives traffic and the rest act as backup. Network interfaces are selected on each cluster node, and IP addresses must be defined for each node.

The administrator assigns virtual IP addresses. Transmitted between these interfaces are VRRP advertisements — messages that nodes use to exchange information about their state.

To create a high availability cluster, click the **+** icon in the **High-availability clusters** section:



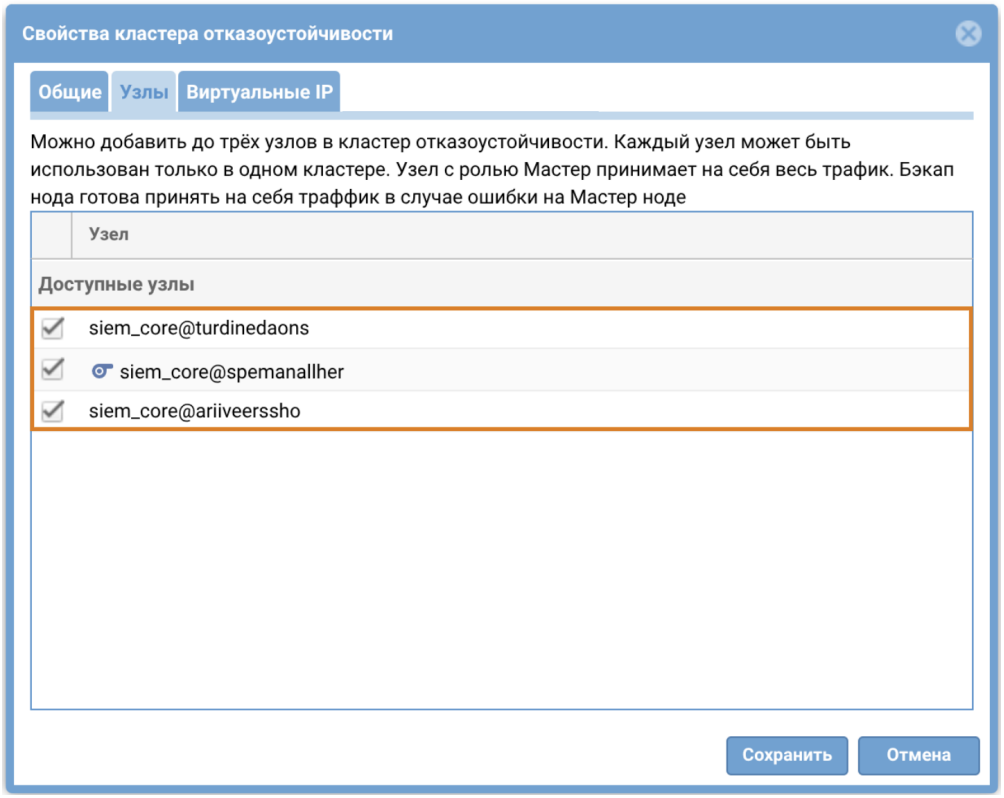
In the high availability cluster properties window that opens, make the following settings:



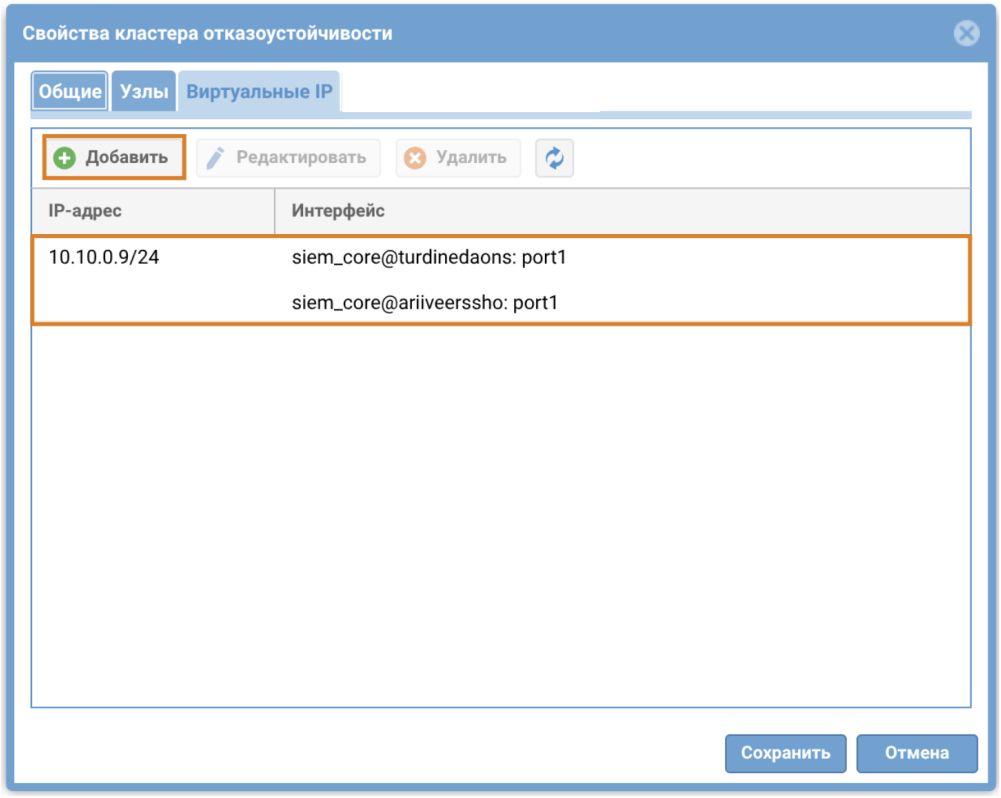
On the **General** tab:

- Specify the HA cluster name.

- Set the virtual router ID. The VRID must be unique for each VRRP cluster on the local network.
- Check the **Enabled** checkbox to enable the cluster.



On the **Nodes** tab, select the configuration cluster nodes that will be included in the created HA cluster.

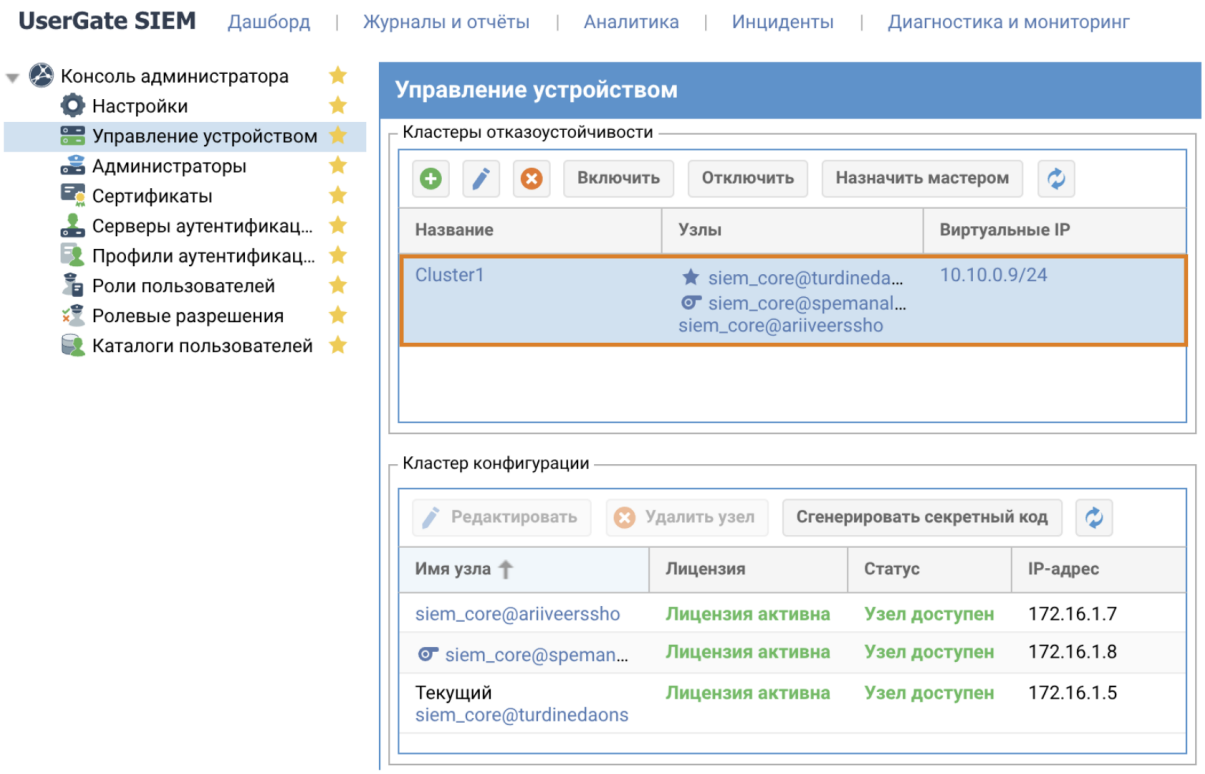


On the **Virtual IPs** tab, specify the virtual IP address and network mask of the HA cluster, and select the primary nodes and ports on which VRRP will run.

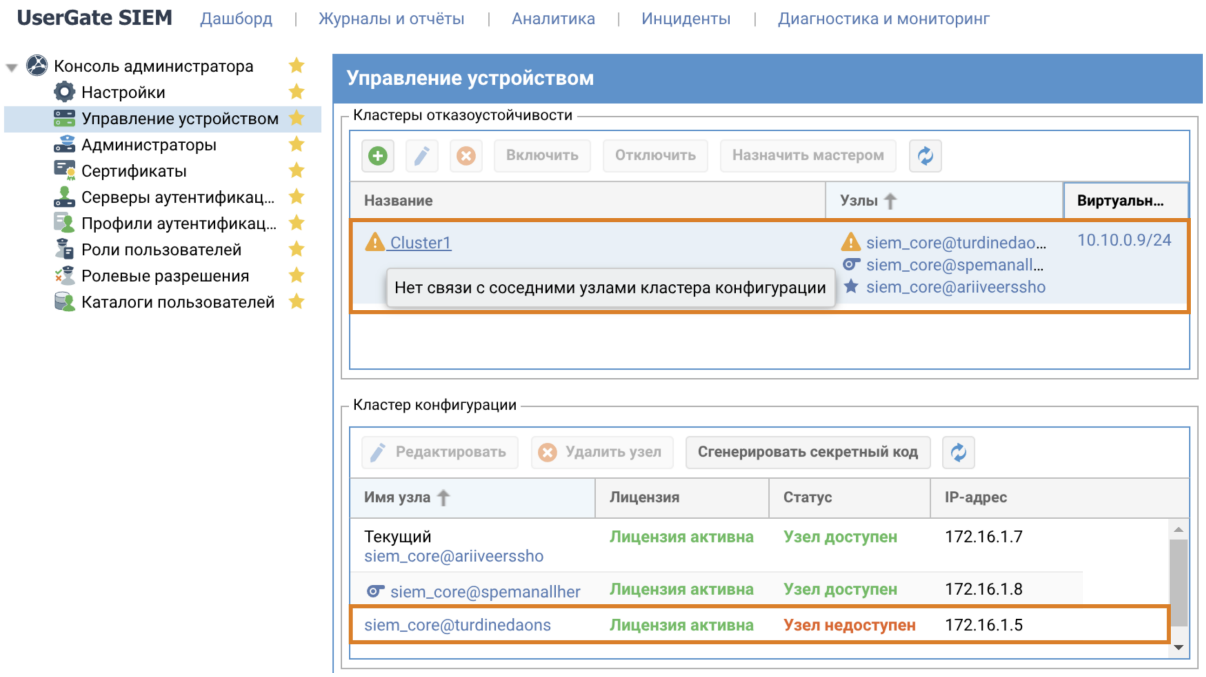
Displaying the HA Cluster Status

The status and roles of the nodes in the cluster can be viewed in the **High availability clusters** section. Node roles are marked with corresponding icons: an asterisk indicates the active master node, and a whistle indicates the arbitrator node.

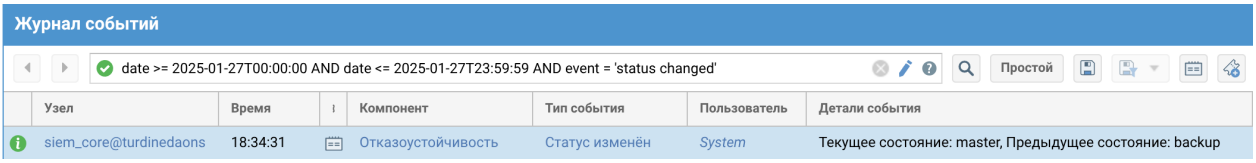
If the cluster is successfully created, its status is displayed as follows:



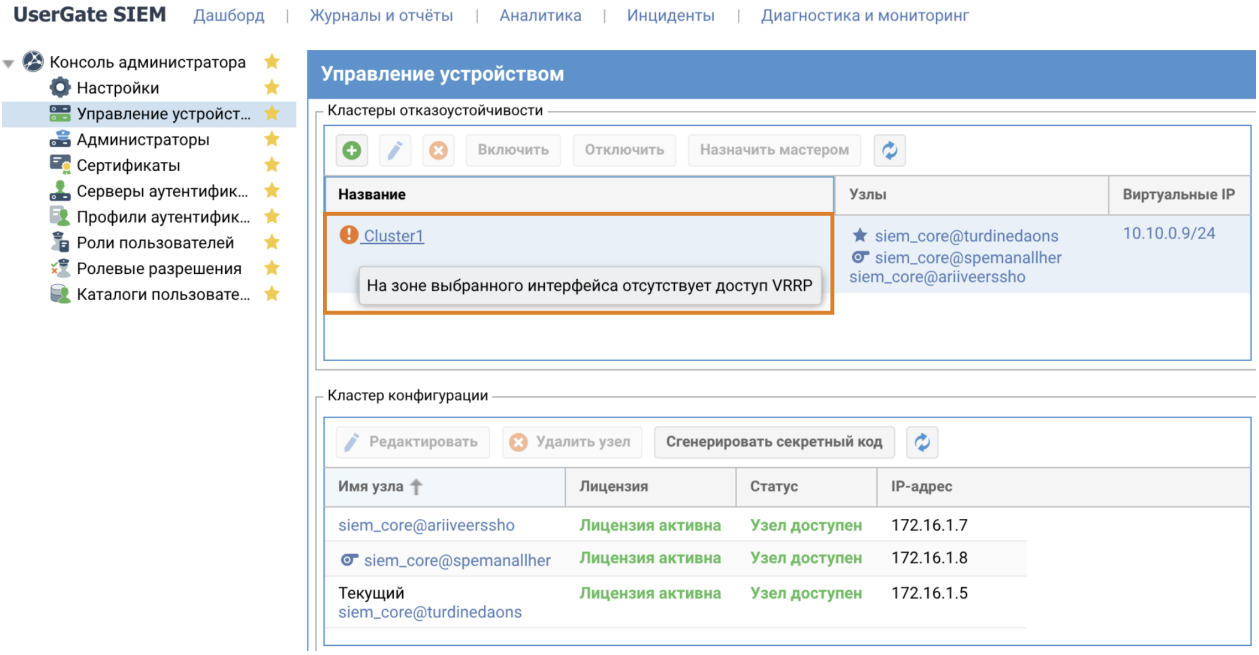
If the cluster master node is unavailable, its role will be transferred to the backup node. The status of the cluster and the unavailable node will change in the web console of the second node. Hovering over the cluster status icon displays a tooltip explaining the reason for the cluster status change:



A corresponding entry will appear in the event log:



If the high availability cluster status is inconsistent, its status is marked with a corresponding icon. When you hover over the icon with the mouse pointer, a tooltip appears explaining the reason for the cluster state:



NETWORK CONFIGURATION

Zone Configuration

A zone in SIEM is a logical aggregation of network interfaces. SIEM 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.

By default, UserGate SIEM is supplied with the following zones:

Name	Description
Management	Used to connect trusted networks from which SIEM management is allowed.

Name	Description
Trusted	Used to connect trusted networks, such as LANs. It is assumed that the Trusted zone will connect SIEM to the network that will be used by UserGate firewalls to send logs to it and by SIEM to access the Internet.

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

SIEM 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, SIEM 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 SIEM servers.
Step 3. (Optional) Configure the access control settings for the zone.	Specify the SIEM-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.

Name	Description
	The following services exist: • **Ping**: enables pinging of SIEM. • **SNMP**: provides SNMP access to SIEM (UDP 161). • **Control XML-RPC**: enables API control of the product (TCP 4041). • **Administrative console**: provides access to the administrative web console (TCP 8010). • **CLI over SSH**: provides server access for management using CLI (command line interface) (TCP port 2200). • **Log Analyzer**: the log analyzer service. Needs to be allowed in zones from which SIEM will receive the data sent by UserGate servers (TCP 22711 or 22699 for devices with software version below 7). • **Log collector**: a service that enables information collection from remote devices using the Syslog protocol (the default port number is 514). For more on network availability requirements, see the appendix Network Environment Requirements.
Step 4. (Optional) Configure the IP spoofing protection settings.	IP spoofing attacks allow a malicious actor to transmit a packet from one network, such as **Trusted**, to another, such as **Management**. To do that, the attacker substitutes the source IP address with an assumed address of the relevant network. In this case, responses to this packet will be sent to the internal address. To protect against this kind of attack, the administrator can specify the source IP address ranges allowed in the selected zone. Network packets with different IP sources will be dropped. Using the Negate checkbox, the administrator can specify the source IP addresses from which packets may not be received on the zone's interfaces. In this case, packets with source IP addresses within those ranges will be rejected. As an example, you can specify "gray" IP address ranges as 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 and enable the **Negate** option.

Network Interface Configuration

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

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

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

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

- VLAN
- Bond.

Creating a VLAN Interface

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

Name	Description
Enabled	Enables the VLAN.
Name	The VLAN name. Assigned automatically based on the physical port name and the VLAN tag.
Description	An optional interface description.
Type	Specify the interface type as Layer 3 or Mirror.
VLAN tag	The sub-interface number. Up to 4094 interfaces can be created.
Node name	The node name in the cluster where this VLAN is being created.
Interface	The physical interface on which the VLAN is being created.
Zone	The zone to which the VLAN belongs.
Alias	An alternative interface name assigned by the administrator. This optional setting is used for working with SNMP. The value is a string with a length of up to 64 characters.

Name	Description
	Important! Cyrillic characters are not allowed in the value.
Networking	The IP address assignment method: no address, a static IP address, or a dynamic IP address obtained using DHCP. The possibility to change MAC address, MTU size, MSS size (available in software version 7.3.0 and higher).

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

Name	Description
	with identical speed and duplex settings. When combined like this, all links in the active aggregation participate in transmission as per IEEE 802.3ad. The choice of interface for packet transmission is determined by the policy. By default, the XOR policy is used, with the xmit_hash policy as a possible alternative. • **Adaptive transmit load balancing**. The outgoing traffic is distributed depending on the load on each slave interface (determined by the download speed). No additional configuration on the switch is required. The incoming traffic is received by the current network card. If this card fails, another card assumes the MAC address of the failed one. • **Adaptive load balancing**. Includes the previous policy plus incoming traffic balancing. No additional configuration on the switch is required. The incoming traffic is balanced through ARP negotiation. The driver intercepts ARP responses sent from the local NICs to the outside and overwrites the source MAC address with one of the unique MAC addresses of the NIC in the bond. Thus, different 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.

Name	Description
Failover MAC	Determines how MAC addresses will be assigned to the bonded slaves in the active-backup mode on switching between slaves. The normal behavior is to use the same MAC address on all slaves. Enumerated options: • **Disabled**: sets the identical MAC address on all slaves during the switching process. • **Active**: the MAC address on the bond interface will always be identical to that on the currently active slave. The MAC addresses on the backup interfaces are not changed. The MAC address on the bond interface changes during the failover processing. • **Follow**: the MAC address on the bond interface will be the same as that on the first slave added to the bond. This MAC is not set on the second and subsequent interfaces while they are in backup mode. That MAC address gets assigned during a failover: when a backup slave interface becomes active, it assumes a new MAC (the one on the bond interface), and the formerly active slave is assigned the MAC that the currently active one used to have.
Xmit hash policy	Determines the hash policy for packet transmission via bonded interfaces in the XOR or IEEE 802.3ad modes. Enumerated options: • **Layer 2**: only MAC addresses are used for hash generation. With this algorithm, the traffic for a particular network host is always sent over the same interface. This algorithm is compatible with IEEE 802.3ad. • **Layer 2+3**: both MAC and IP addresses are used for hash generation. This algorithm is compatible with IEEE 802.3ad. • **Layer 3+4**: IP addresses and transport-layer protocols (TCP or UDP) are used for hash generation. This algorithm is not universally compatible with IEEE 802.3ad, as both fragmented and non-fragmented packets can be transmitted within a single TCP or UDP interaction. Fragmented packets lack the source and destination ports. As a result, packets from the same session can reach the recipient in an order other than the intended one because they are sent via different slaves.
Networking	IP address assignment method: no address, static IP address, or dynamic IP address obtained via DHCP. Ability to change the MAC address, MTU size, and MSS size (available starting with software release 7.3.0 and higher).

Gateway Configuration

To connect SIEM to the Internet, you need to specify the IP addresses 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.
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 SIEM server.
Step 4. Specify the network interface.	Specify the network interface through which the route will be added. If you keep the **Automatically** value, SIEM 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.

SENSORS

General Information

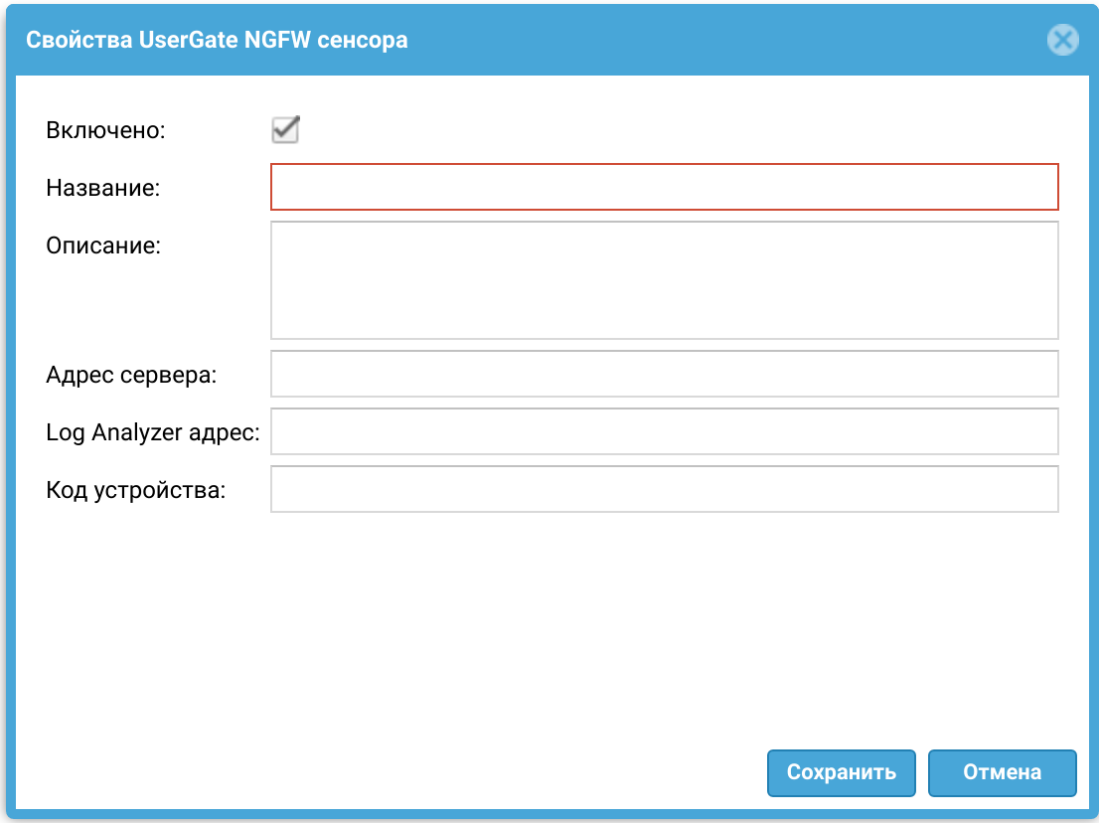
SIEM uses sensors to collect information from various devices for subsequent analysis. A sensor is a SIEM-compatible device that can send certain data to SIEM . A sensor can be NGFW, a UserGate Client endpoint, computers running Windows OS, or any other network device that supports SNMP data transfer.

UserGate Sensors

A UserGate sensor connects a single UserGate firewall device to SIEM. To connect a UserGate sensor, follow these steps:

Name	Description
Step 1. On the UserGate node, enable the **Log Analyzer/SIEM** and **SNMP** services on the required zone.	On the UserGate node that you want to add as a sensor, go to the **Network → Zones** section, select the zone containing the network interfaces through which network communication with the SIEM server will occur, and allow the **Log Analyzer/SIEM** and **SNMP** services.
Step 2. On the UserGate node, copy the device code to the clipboard.	In the UserGate node that you want to add as a sensor, open **Settings → Log Database Status** and copy the device code's value to the clipboard. It will be needed at Step 4.
Step 3. On the SIEM, enable the **Log database** service in the required zone	On /SIEM, go to the **Network → Zones** section, select the zone containing the network interfaces, through which network communication with the UserGate node will occur, and allow the **Log database** service.
Step 4. Create a UserGate sensor.	On the SIEM server, go to **Sensors → UserGate sensors**, click **Add**, and fill in the relevant fields.

These are as follows:



Name	Description
Enabled	Enables or disables this UserGate sensor.
Name	The name of the UserGate sensor.
Description	An optional description of the UserGate sensor.
Server address	The IP address of the UserGate node for which this sensor is being created.
Log Analyzer address	The IP address of the SIEM server that will be used on the UserGate node as the destination for logs. Only those IP addresses are available for selection that are assigned to interfaces in the zones where the Log Analyzer service is allowed.
Device code	Device code received from the UserGate node.

After creating a sensor, the UserGate node starts sending data to SIEM.

> **Note**
>
> **Once the SIEM is connected, the SIEM server will be processing and exporting logs, generating reports, and handling other UserGate sensor statistics.**

The following configuration changes have occurred on the UserGate node:

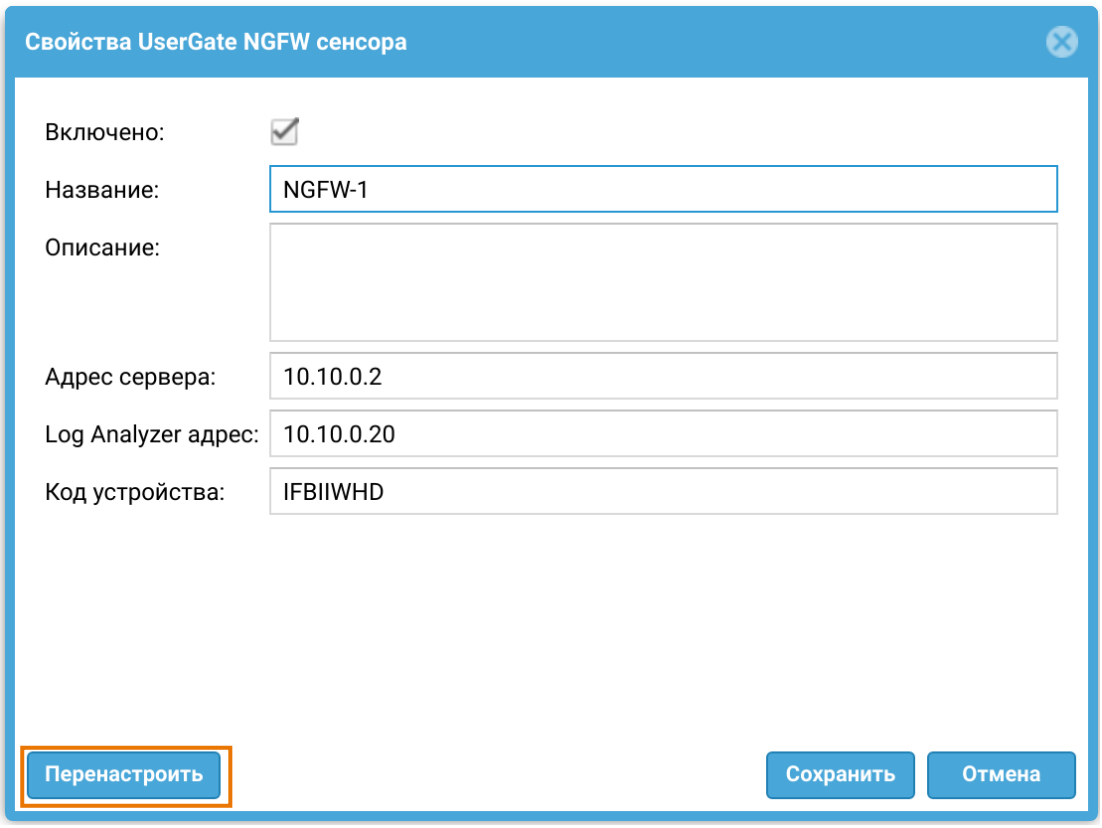
- In the **Settings → Log database status** section, the server address has changed to the address specified when creating the UserGate sensor.
- In the **Diagnostics and monitoring → Notifications → SNMP** section, an SNMP rule has been added that allows SIEM to receive information using the SNMP protocol.

The following new items have been added to SIEM:

- In the **Logs and reports --> Logs** section, records from the newly created UserGate sensors have appeared.
- In the **Dashboard** section, you can now add a new widget, **UserGate sensor graph**, that contains information received from the UserGate sensor.

> **Note**
> **If the administrator changes the SNMP rules on the UserGate node, SIEM will revert these settings or re-create the rule when the sensor is enabled or disabled on the SIEM server.**

Once the UserGate sensor is created, an additional button **Reconfigure** will appear in the sensor settings window:



Clicking the button reconfigures the connection between the SIEM node and the UserGate device. This may be necessary, for example, when changing the IP address or the UserGate device code.

SNMP Sensors

Using an SNMP sensor, the administrator can connect an SNMP-compatible network device to a SIEM server to collect and analyze its metrics. SIEM can display any counters received over SNMP using SNMP queries. To configure an SNMP sensor, you need to have MIBs (Management Information Bases) for the managed device. For more details on managing MIBs, see the section SNMP MIB Management.

To configure an SNMP sensor, follow these steps:

Name	Description
Step 1. Upload the MIB for the device that you want to add for monitoring.	On the SIEM server, go to the **Sensors → SNMP MIB management** and upload the MIB file.
Step 2. Create an SNMP sensor.	On the SIEM server, go to **Sensors → SNMP sensors**, click **Add**, and fill in the relevant fields.

These are as follows:

Name	Description
Enabled	Enables or disables this SNMP sensor.
Name	The name of the SNMP sensor.
Description	An optional description of the SNMP sensor.
Server address	The IP address of the SNMP sensor.
Port	The port number for the SNMP sensor. Normally, TCP port 161 is used for SNMP data queries.
Version	The SNMP protocol version to be used with this sensor. Available options: SNMP v2 and SNMP v3.
Community	SNMP community is a string that identifies the SIEM server and network device for SNMP v2. Use only Latin letters and numbers.
Polling interval (sec.)	The time interval with which the SIEM server will receive data from the network device.
User	For SNMP v3 only. The username used for authentication on the network device.
Authentication type	The authentication mode. The available options are: • No authentication; No encryption (noAuthNoPriv) • Authentication; No encryption (authNoPriv) • Authentication; Encryption (authPriv). The authPriv mode is considered the most secure.
Authentication algorithm	The algorithm used for authentication.

Name	Description
Authentication password	The password used for authentication.
Encryption algorithm	The algorithm used for encryption. DES or AES can be used.
Encryption password	The password used for encryption.
Counters	Specify all data here that SIEM should query from the network device. The counters can be selected from the MIBs uploaded to the device. Choose the desired section in the SNMP tree and add the corresponding counter or specify the SNMP OID and type of the counter in the SNMP string.

After you have successfully added a sensor, you will be able to add a new widget with graphs of SNMP data received from the sensor in the **Dashboard** section.

SNMP MIB Management

In this section, the administrator can add and remove MIBs (Management Information Bases) on SIEM.

For vendor-specific MIBs, contact your device's vendor. SIEM already contains MIBs for the most popular network devices.

WMI Sensors

Using an WMI sensor, the administrator can connect a WMI-compatible network device (a computer running Windows) to SIEM to collect and analyze its metrics.

To create a WMI sensor, go to **Sensors → WMI sensors**, click **Add** and fill in the required fields:

Name	Description
Enabled	Enables or disables this WMI sensor.
Name	The name of the WMI sensor.

Name	Description
Description	An optional description of the sensor.
Server address	IP address of the WMI device.
Namespace	The namespace of identifiers on the WMI device.
Polling interval (sec.)	The time interval with which the WMI sensor will receive data from the network device.
User	The username used for authentication on the network device.
Password	The password used for authentication.
Counters	Specify the Windows event log parameters that SIEM will monitor on the network device.

Endpoint devices

This section contains a list of endpoint devices with UserGate Client software installed.

> **Note**
> **An endpoint device is displayed if the SIEM is selected on the UGMC of this device as the server to send event information, therefore, SIEM must be pre-registered on UGMC.**

The following information is displayed:

- The name of the endpoint device set in UGMC.
- The version of the UserGate Client software installed on the device.
- The last device access time.
- The IP address of the device.
- The NetBIOS name.
- The version of the operating system (OS) of the Device.

The telemetry information.

The SIEM allows to remotely manage UserGate Client devices. To do this, click **Send command** and select the desired action:

- Block networking
- Enable network data transfer
- Kill process When selecting this action, you must specify the process ID.
- Start/stop service. To perform these actions, specify the name of the service.

Connectors

Connectors are used to allow the SIEM device to be connected to various security tools or information security incident data sharing services.

You need to specify the following data to add a connector:

Name	Description
Name	Connector name.
Description	An optional description of the connector.
Server type	Select the server type: • SSH; • HTTP; • HTTPS .
Server address	Type: • IP; • FQDN
IP address	The server's IP address. Specify it if the **IP** server type is selected.
Port	The server's port. Specify it if the **IP** server type is selected.
FQDN	The server's FQDN. Specify it if the **FQDN** server type is selected.

Name	Description
URL path	Used to manage a device via API.
Login name	User login for connector authorization.
Password	Password to the user account required for connector authorization.
Command group	You can only specify a command group for a SSH server; see the Commands section for details.
HTTP headers	You can only specify headers for HTTP and HTTPS servers.

Use the **Test** button to check whether the connector is configured correctly with the SSH server type. You will be prompted to select a command from the specified group to be sent to the connector after you click **Test**; if the command contains variables, additional fields for value input will be displayed.

LOG COLLECTOR

Description

The log collector is used for centralized collection of information from network devices, which facilitates network monitoring, virtual machines, servers, user devices, and applications.

Syslog

This section is used to configure the rules for collecting Unix system log (syslog) events that contain information on the system's operation, status, and security as well as any errors or malfunctions. Syslog rules allow you to filter event records (by time, event severity, object, device name, and application), which eases the search for information of interest.

To use the log collector, you need to configure the server from which information will be collected and the syslog rules.

To configure the server, go to the **Log Collector → Syslog** section in the administrator web console, click **Configure server** and specify the following data in the **Syslog settings** window that opens:

Name	Description
Enabled	Enable or disable receiving syslog events.
Protocol	The network protocol used for information collection: • TCP • UDP
Port	The port number used to collect syslog events. The default port is 514.
Max session number	The maximum allowed number of concurrent devices connected for message sending.
Secure connection	Enable or disable data flow encryption. For more details on using TLS with Syslog, refer to the relevant documentation.
CA certificate file	The Certification Authority (CA) certificate used to establish a secure connection.
Certificate file	A certificate generated by the user and signed by the Certification Authority (CA). Specify this when configuring a secure connection.
Permitted peers	The list of devices from which SIEM will receive information using a secure connection.

To configure syslog event record filtering rules, provide the following settings:

Name	Description
Enabled	Enable or disable the syslog rule.
Name	The name of the syslog rule.
Description	An optional description of the syslog rule.
Action	Action: • **Allow**: allow incoming messages that match the rule conditions.

Name	Description
	• **Block**: block incoming messages that match the rule conditions.
Timezone	The timezone configured on the remote devices. Incoming messages will be allowed or blocked from the devices that store records in the specified timezone.
Place to	The place in the rule list where this rule will be inserted: at the top, at the bottom, or above the selected existing rule.
Severity	The syslog severity of the event: • **Emergency**: a critical state that affects system health • **Alert**: a state that requires immediate intervention. • **Critical**: a state that requires immediate intervention or signals a fault in the system. • **Error**: messages about system faults • **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 alerts • **Debug**: information useful to developers for debugging applications
Object	The event's category: • **Kernel messages** • **User-level messages** • **Mail system** • **System daemon** • **Security/authorization** • **Syslog messages** • **Line printer subsystem** • **Network news subsystem** • **UUCP subsystem** • **Clock daemon** • **Security/authentication** • **FTP Daemon** • **NTP subsystem** • **Log audit** • **Log alert**

Name	Description
	• **Clock daemon 2** • **Local 0 - Local 7**.
Hostname	The name of the device.
App-Name	The name of the application for which the collection of information should be allowed or blocked. For more details, see the Syslog Applications section.

> **Note**
> **When parsing syslog messages, syslog fields from RFC 3164 (facility, severity, timestamp, hostname, tag, pid) will be written to separate log fields. All additional fields from RFC 5424 will be written to the data field.**

The event will be recorded in **Syslog**. For more details, see the Syslog Log section.

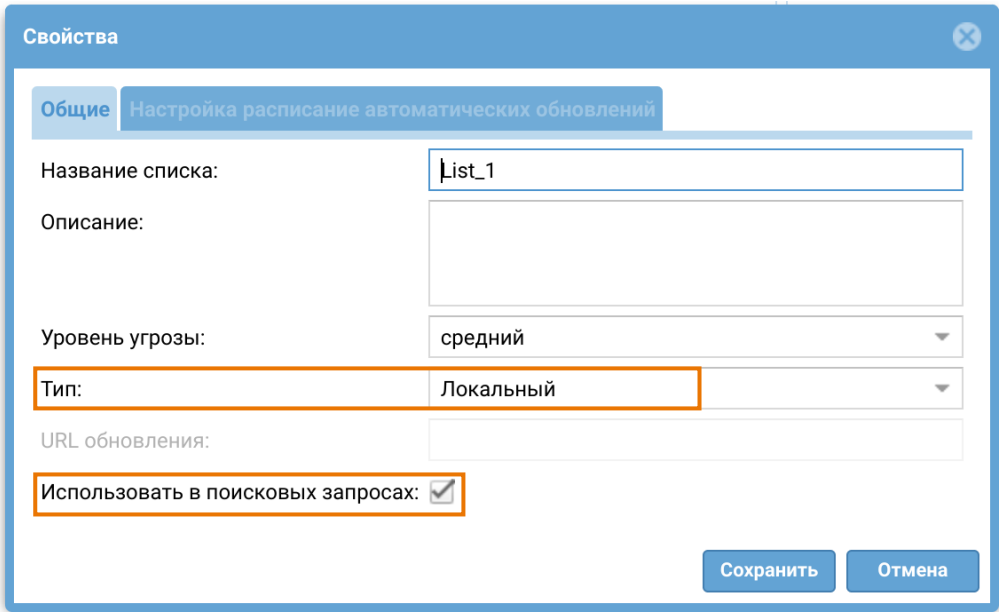
LIBRARIES

IP Addresses

The **IP Addresses** section contains lists of IP address ranges that can be used in search queries.

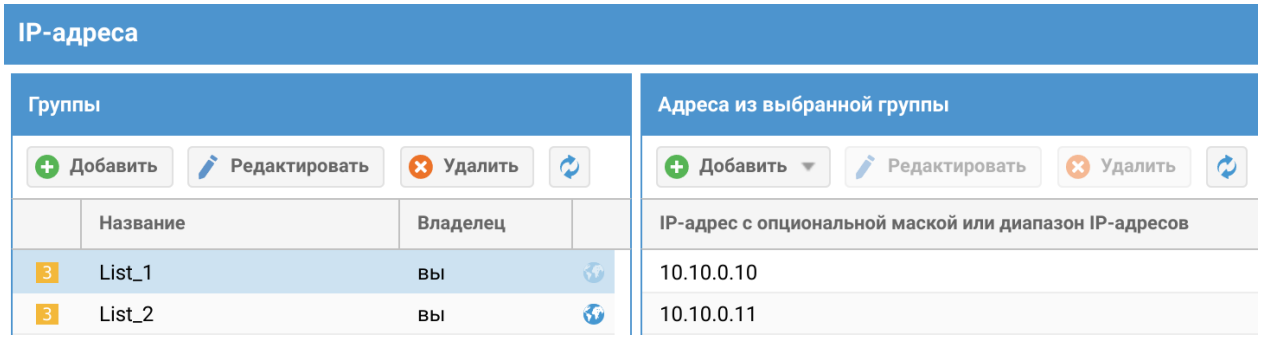
IP address lists are created in the **Groups** panel. They can be **local** or **updatable**.

Local lists are created and stored on the device.



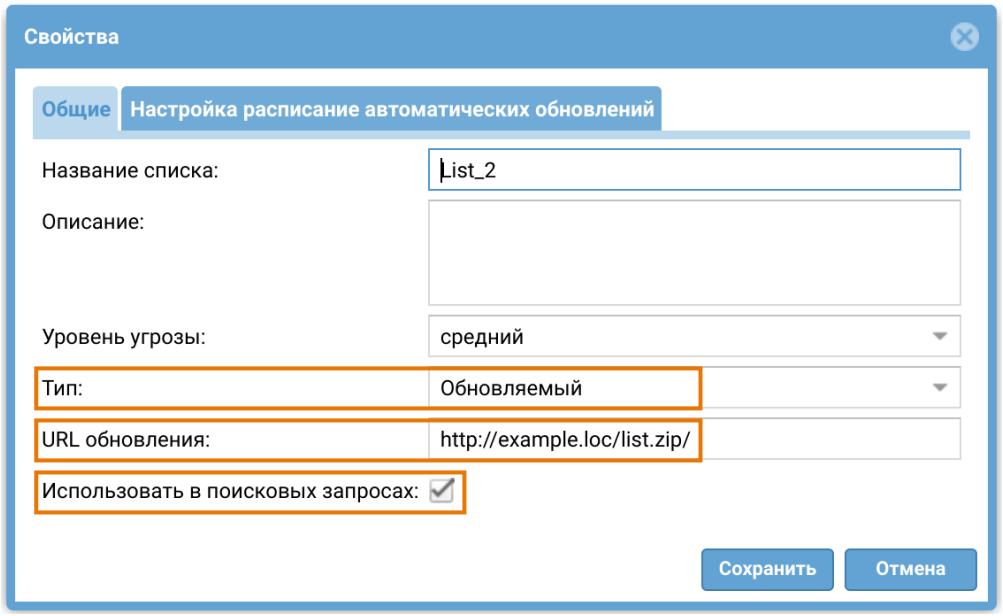
If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

IP addresses are added to these lists manually by the administrator in the **Selected group addresses** pane:



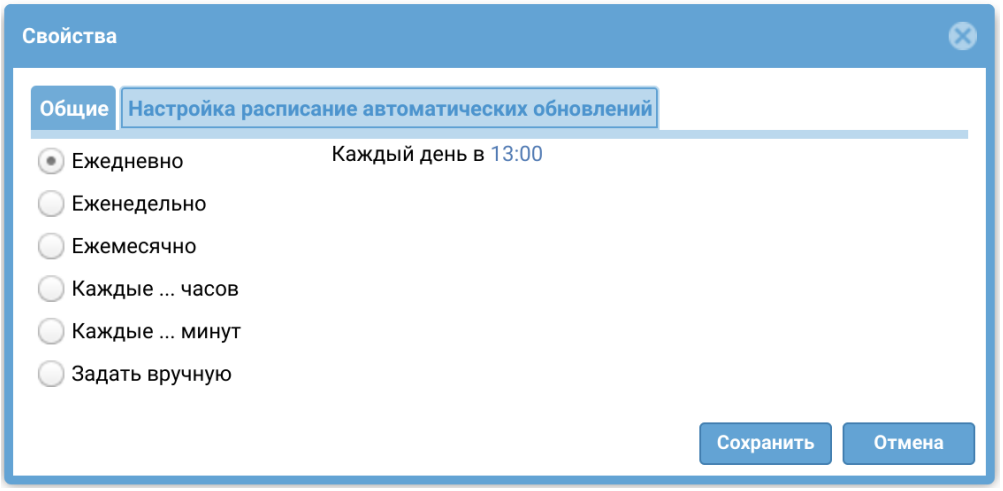
An IP address entry can be in the form of an individual IP address, IP address/subnet mask, or IP address range (192.168.1.5, 192.168.1.0/24, or 192.168.1.5-192.168.2.100, respectively).

Updatable lists receive information about IP addresses from external servers at the update URL specified in the list properties:



If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

On the **Auto updates schedule settings** tab, you can configure the update schedule for this list:



The administrator can create custom updatable IP address lists. To create such a list, follow these steps:

Name	Description
Step 1. Create a file with the desired IP addresses.	Create a file named **list.txt** with the IP address list. The address list is written to a plain text file in a column without any punctuation. Example:

Name	Description

	`x.x.x.x`
	`y.y.y.y`
	`z.z.z.z`

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

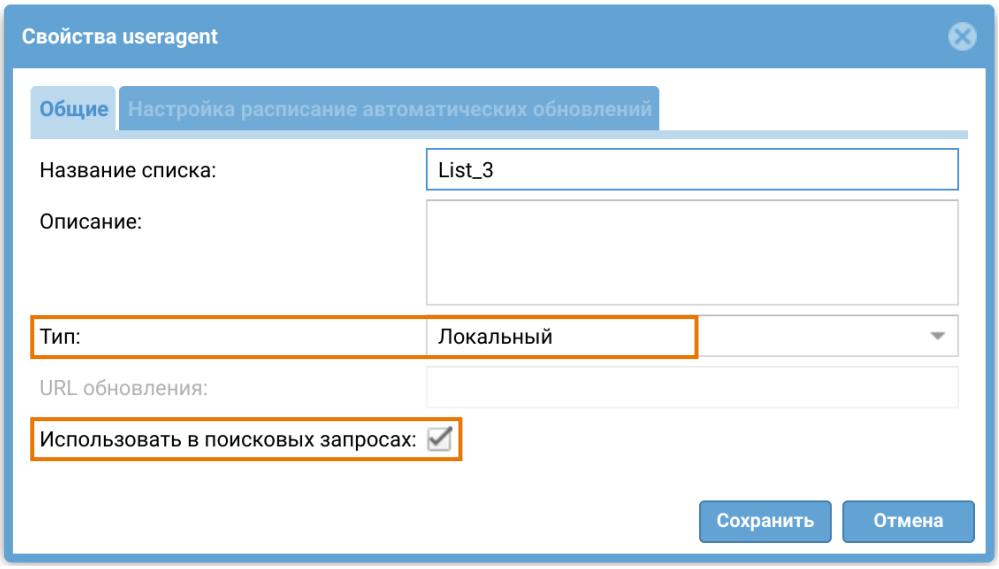
Name	Description
	where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "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".

Browser Useragent

To create browser useragent lists, use the **Libraries → Browser Useragent → Categories** section of the Admin console. They contain information on the types of browsers that users have.

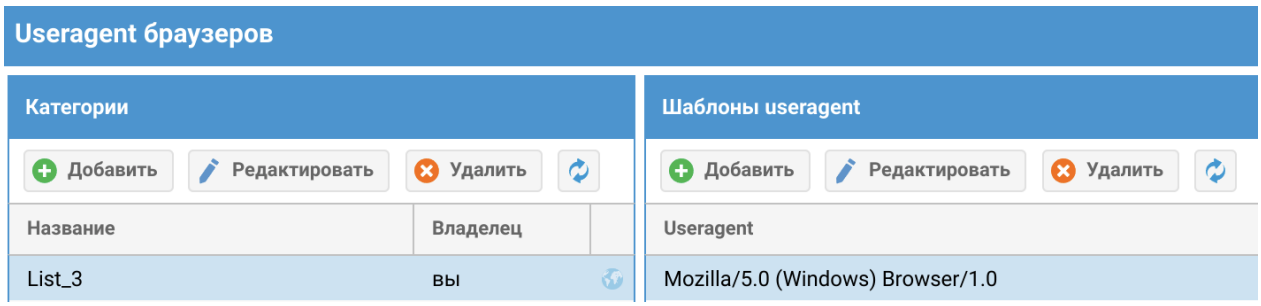
The lists can be **local** or **updatable**.

Local lists are created and stored on the device.

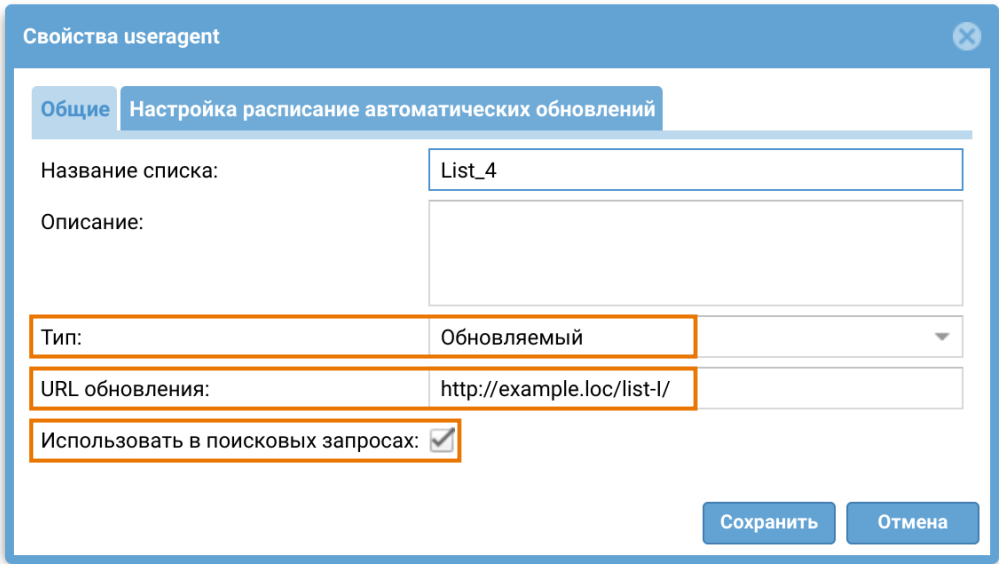


If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

The administrator adds data to them manually on the **Useragent templates** panel. A comprehensive list of useragent strings can be found here: http://www.useragentstring.com/pages/useragentstring.php.

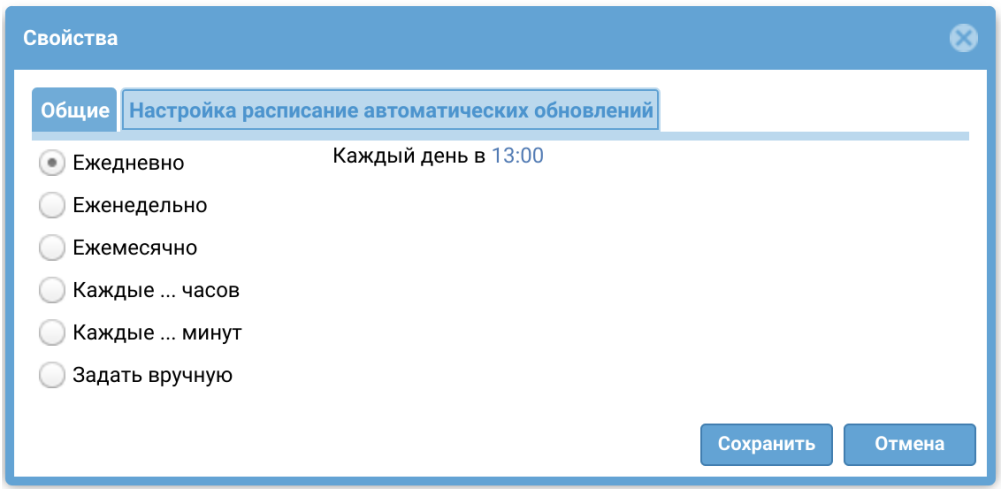


Updatable lists contain information downloaded from external servers at the update URL specified in the list properties:



If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

On the **Auto updates schedule settings** tab, you can configure the update schedule for this list:



The administrator can create custom updatable useragent lists and distribute them centrally to all their managed devices. To create such a list, follow these steps:

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

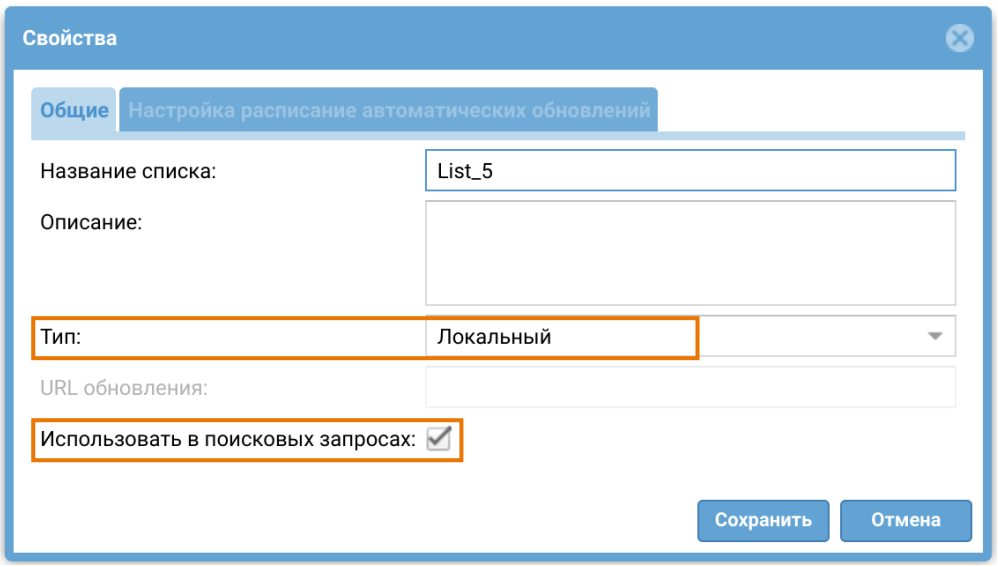
Name	Description
	With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of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

Content Types

The **Content types** section contains lists of content types that can be used in search queries.

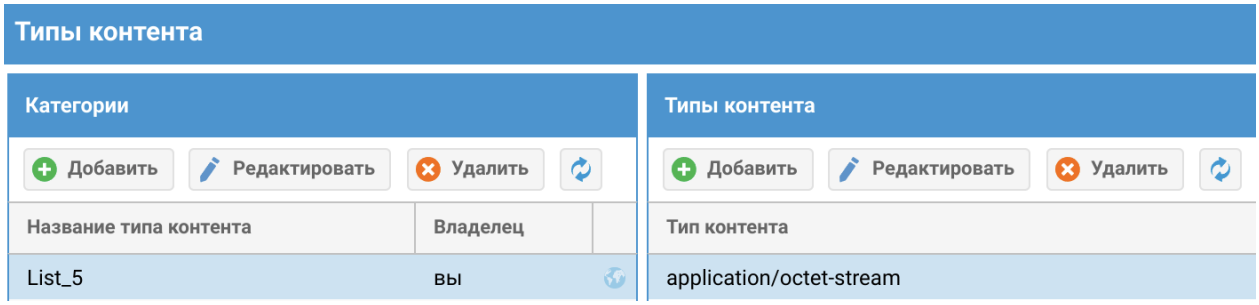
Content type lists are created in the **Categories** panel. They can be **local** or **updatable**.

Local lists are created and stored on the device.

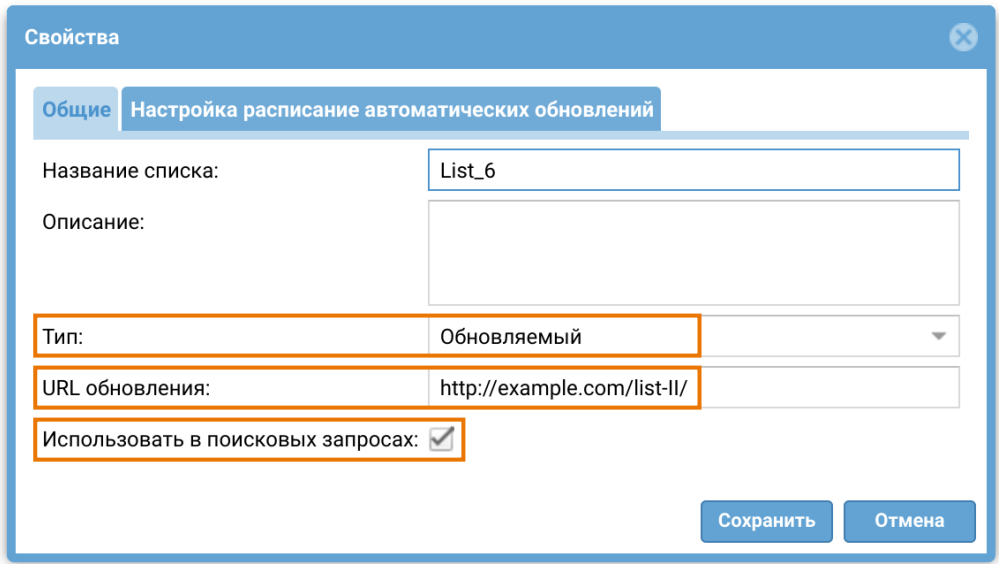


If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

With local lists, administrator manually adds MIME-formatted data to the list on the **Content types** panel. A list of content types and their descriptions can be found at this link: https://www.iana.org/assignments/media-types/media-types.xhtml.

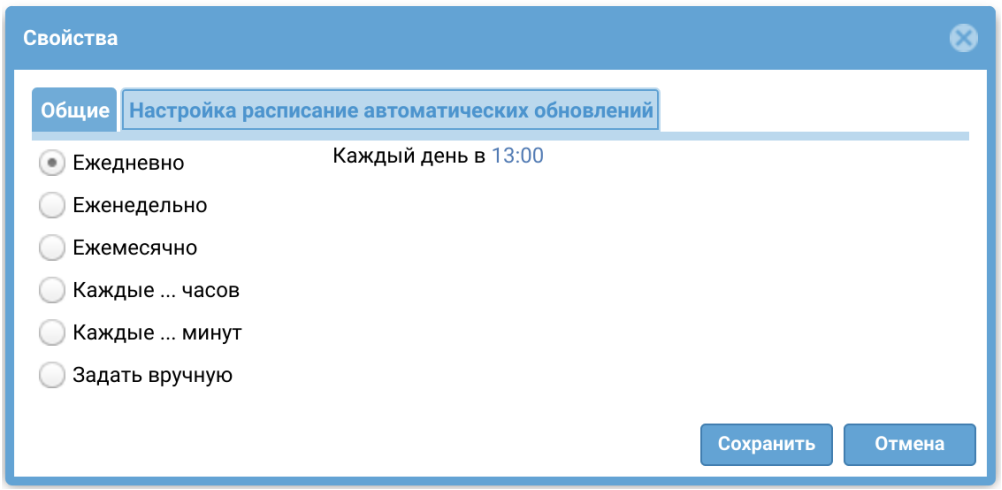


Updatable lists contain data downloaded from external servers at the update URL specified in the list properties:



If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

On the **Auto updates schedule settings** tab, you can configure the update schedule for this list:



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

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

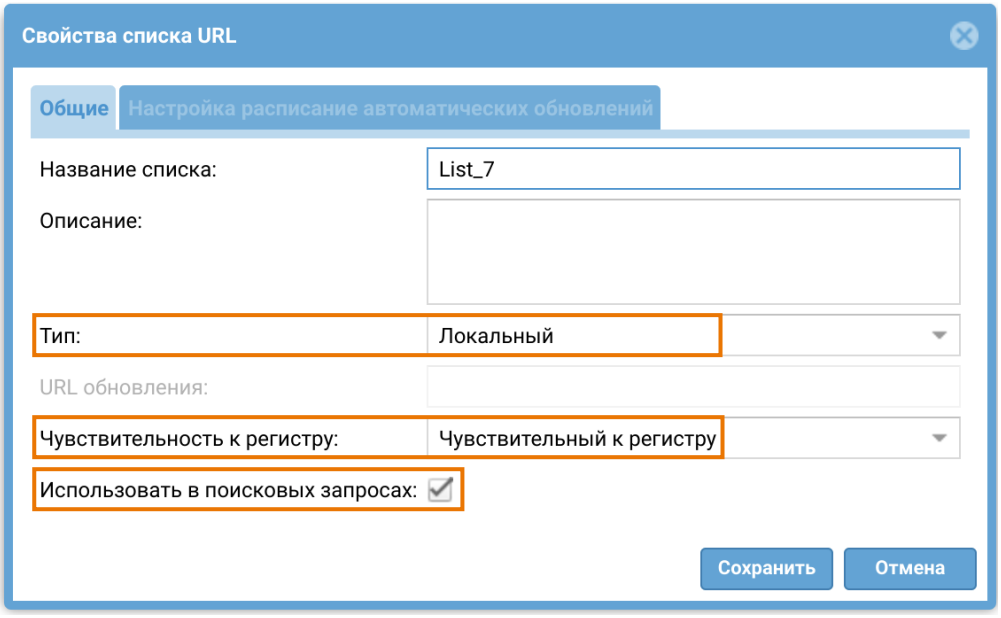
Name	Description
	With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of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

URL Lists

The **URL lists** section contains lists of URLs that can be used in search queries.

URL lists are created in the **URL lists** panel. They can be **local** or **updatable**.

Local lists are created and stored on the device.



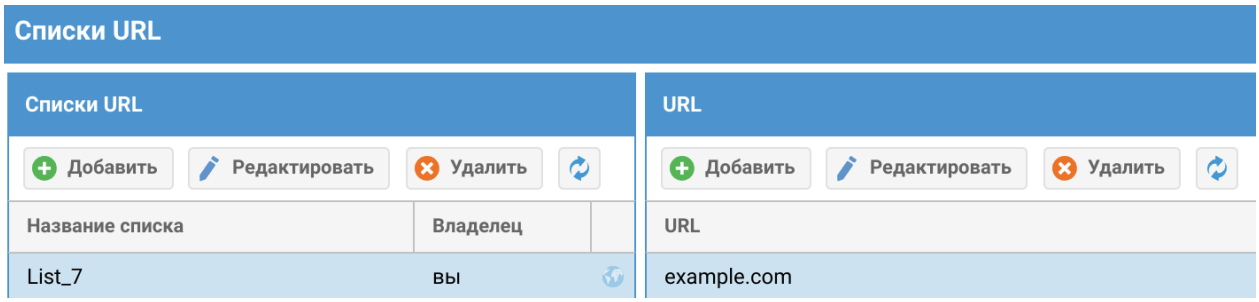
You need to select a category for the list to be created in the **Case sensitivity** field:

- **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.

The list category is set at the time of creation. and cannot be changed afterwards.

If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

Administrator adds data to these lists manually on the **URL** panel.



You can use wildcards such as "^", "$", and "*":

"*": any number of any characters

"^": start of a line

"$": end of a line

The "?" and "#" characters cannot be used.

If a URL entry starts with "http://", "https://", "ftp://" or contains one or more "/" characters, it is considered a URL and used only for HTTP(S) filtering but not DNS filtering. Otherwise, the string is considered a domain name and used for both DNS and HTTP(S) filtering.

To filter by exact URL, use the "^" and "$" characters:

^http://domain.com/exacturl$

To filter by exact URL including all child directories, use the "^" character:

^http://domain.com/exacturl/

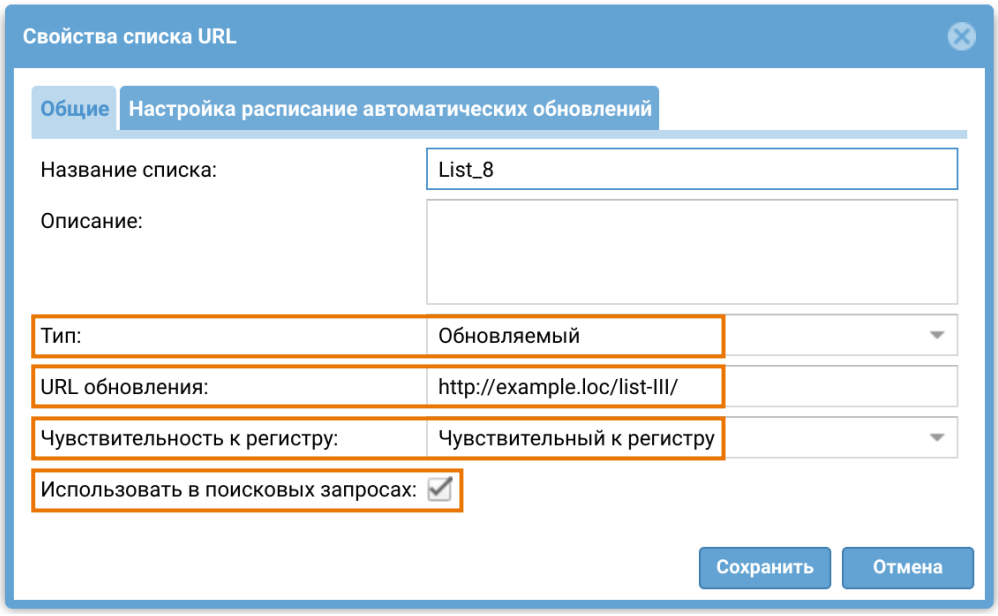
To filter by domain with all possible URLs, use this notation:

domain.com

An example of interpreting URL entries:

Example entry	DNS request processing	HTTP request processing
yahoo.com or *yahoo.com*	Matches the entire domain and its higher (3rd, 4th, etc.) level domains, for example: sport.yahoo.com mail.yahoo.com as well as: qweryahoo.com	Matches the entire domain and all its URLs, as well as higher (3rd, 4th, etc.) level domains, for example: http://sport.yahoo.com http://mail.yahoo.com https://mail.yahoo.com http://sport.yahoo.com/123 http://qwertyahoo.com/
^mail.yahoo.com$	Matches only mail.yahoo.com	Matches only: http://mail.yahoo.com https://mail.yahoo.com
^mail.yahoo.com/$	No match	No match because the last forward slash character defines a URL, but there is no "https" or "http".
^http://finance.yahoo.com/personal-finance/$	No match	Matches only: http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	No match	Matches: http://yahoo.com/12345/whatever/ https://yahoo.com/12345/whatever/

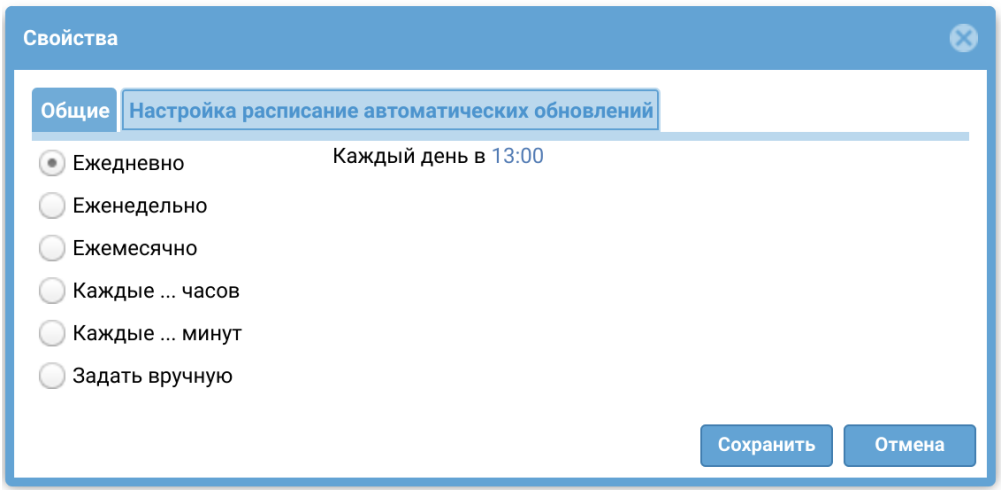
Updatable lists contain data downloaded from external servers at the update URL specified in the list properties:



You need to select a category for the list to be created in the **Case sensitivity** field (for the description of the field, see above):

If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

On the **Auto updates schedule settings** tab, you can configure the update schedule for this list:



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

Name	Description
Step 1. Generate a file with the relevant URL list.	Generate a file named **list.txt** with the URL list in the following format: www.site1.com/url1 www.site2.com/url2

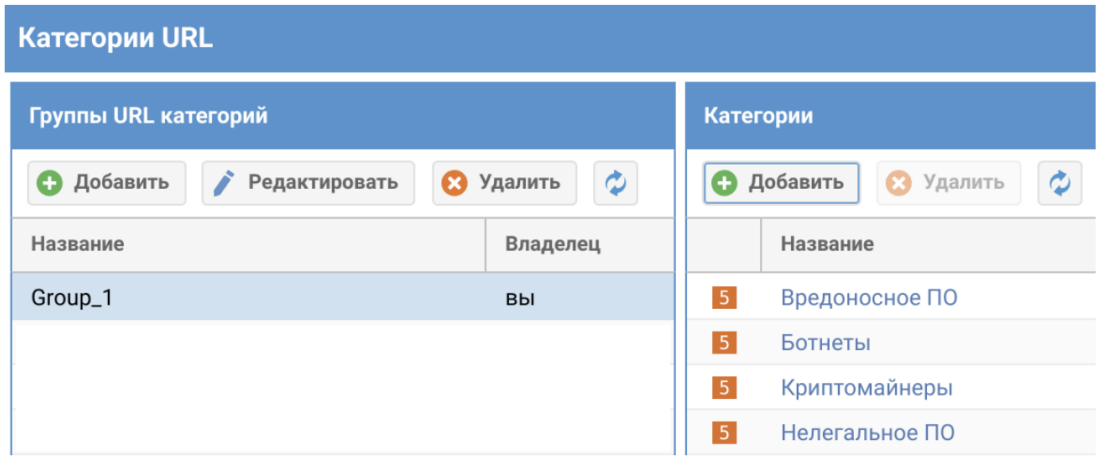
Name	Description
	... www.siteend.com/urlN
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.
Step 4. Upload the files to a web server.	Upload the **list.zip** and **version.txt** files to your website so that they can be downloaded.
Step 5. Create a list and specify an update URL for it.	Create a URL list on each device. When creating the list, select **Updatable** as the list type and enter the address for downloading updates. The device will check for a new version on your website according to the set update download schedule. **Note** **The list URL format is http://x.x.x.x/ or ftp://x.x.x.x/.** The schedule can be configured in the list properties. The available options are: • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7.

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

URL Categories

The **URL categories** section contains category groups that can be used in search queries.

Category groups are created in the **URL category groups** panel. Categories are added to the URL category group in the **Categories** panel.



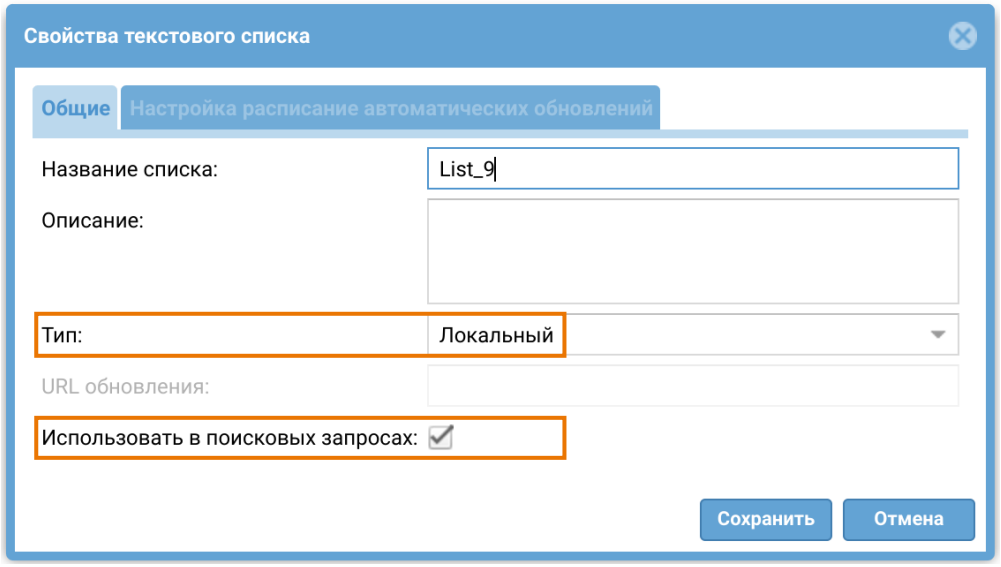
If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

Text Lists

The **Text lists** section contains custom string lists that can be used in search queries. Examples of data that may be present in these lists — the values of hash, MAC addresses, etc.

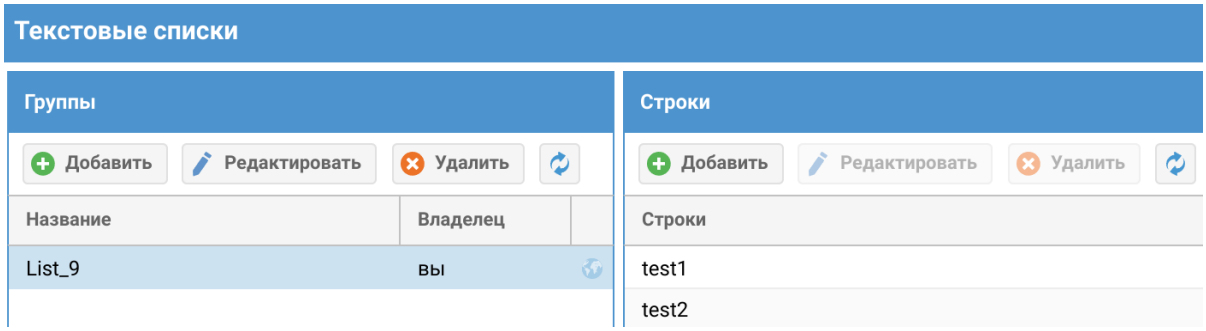
Lists are created in the **Text lists** panel. They can be **local** or **updatable**.

Local lists are created and stored on the device.

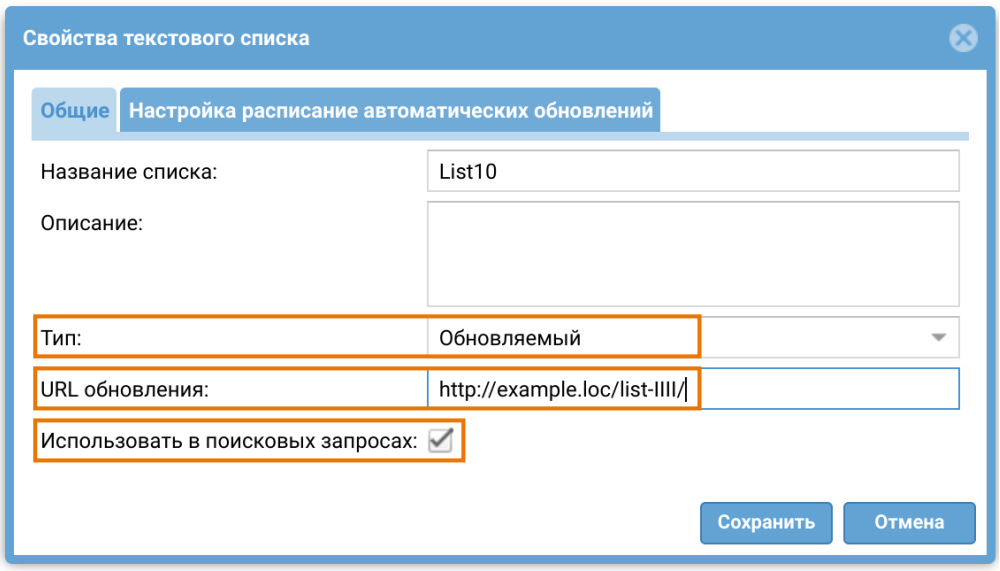


If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

Administrator adds data to these lists manually in the **Strings** panel.

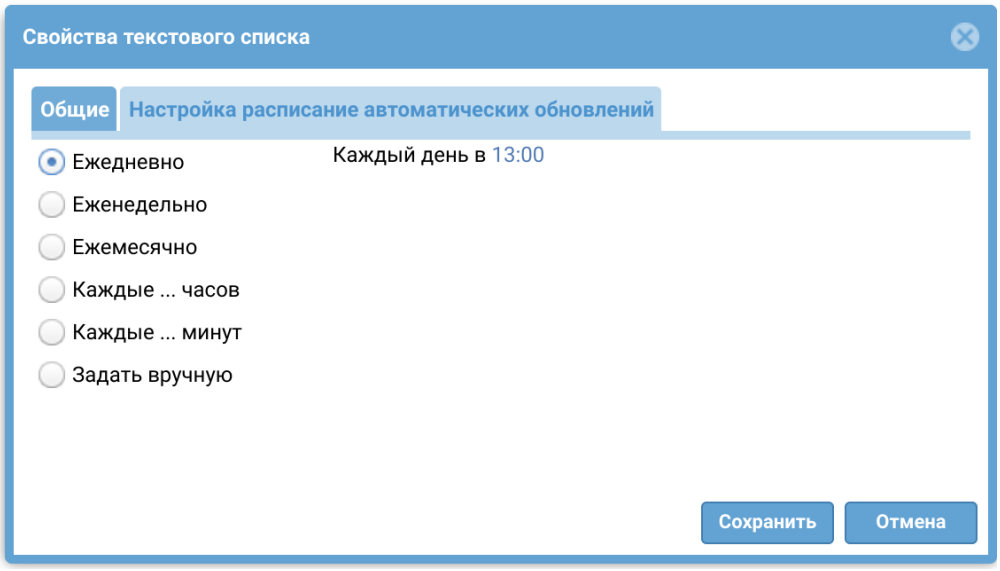


Updatable lists contain data downloaded from external servers at the update URL specified in the list properties:



If the list is intended to be used in search queries, you must set the corresponding checkbox in the properties of the list being created.

On the **Auto updates schedule settings** tab, you can configure the update schedule for this list:



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

Name	Description
Step 1. Generate a file with the relevant list.	Create a text file **list.txt** with the list.
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.

Name	Description
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 4. 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.

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

Emails

The **Emails** library item allows you to create email groups that can later be used in email traffic filtering rules and notifications.

To add a new email group, follow these steps:

Name	Description
Step 1. Create an email group	In the **Email groups** pane, click **Add** and give a name to the new group.
Step 2. Add emails to the group	Highlight the newly created group, click **Add** in the **Emails** pane, and add the desired emails.

The administrator can create updatable email lists and distribute them centrally to UserGate devices. To create such a list, follow these steps:

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

Name	Description
	• 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".

The administrator can export and import mailing address lists using the **Export**/**Import** buttons.

Phones

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

To add a new phone group, follow these steps:

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

The administrator can create updatable phone number lists and distribute them centrally to UserGate devices. To create such a list, follow these steps:

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

The administrator can export and import phone number lists using the **Export**/**Import** buttons.

Commands

Use this section to create groups of commands to be sent to the connectors.

Provide the following settings to create a command group:

Name	Description
Step 1. Create a command list.	In the **Command Groups** panel, click the **Add** button and specify the name, description and type of the list.
Step 2.(Optional) Specify the list update address.	If an updatable list is created, specify the address of the update server. For more details on updatable lists, see later in this chapter.
Step 3. Add commands to the group.	In the **Commands** panel, click the **Add** button and specify the name and the text of the command. Use curly braces {} to define variables. The variables will be substituted with actual values later.

The administrator can create updatable command lists and distribute them centrally to UserGate devices. To create such a list, follow these steps:

Name	Description
Step 1. Create a file with the relevant command list.	Create a file named **list.txt** that contains the command list.
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.
Step 4. Upload the files to a web server.	Upload the **list.zip** and **version.txt** files to your website so that they can be downloaded.
Step 5. Create a command list and specify an update URL for it.	On each UserGate server, create a 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.

Name	Description
	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".

The administrator can export and import command lists using the **Export**/**Import** buttons. For import, you need to create a file containing a list of commands defined in the following format: COMMAND_NAME:COMMAND_TEXT (use curly braces to define variables).

Analytics rules

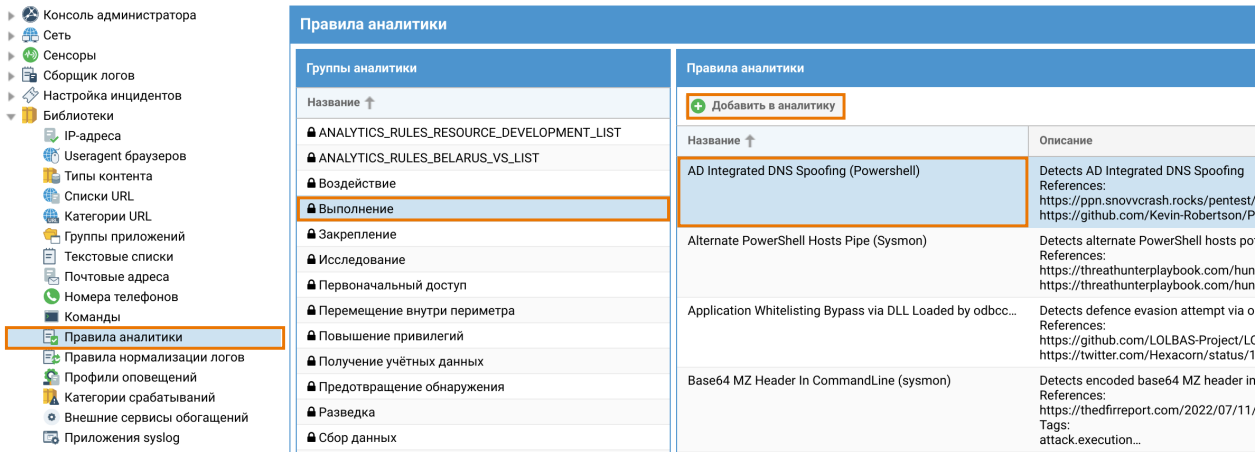
This library contains analytics rules created by the UserGate developers. The library is updated provided that the UserGate SIEM license has a Security Update module.

This library's availability is intended to simplify the creation of analytics rules for UserGate SIEM users. The preset rules from the library may be used as an example

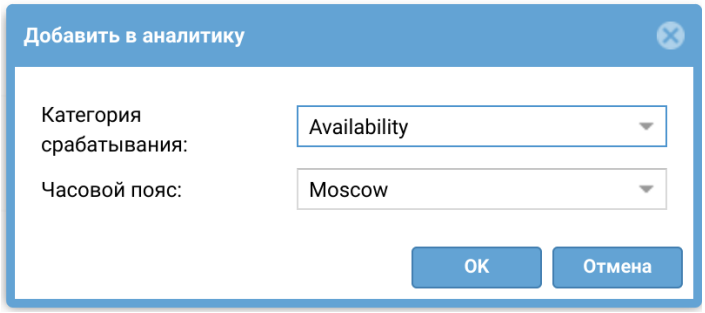
so that you can write your own analytics rules. To do so, users can import rules from the library into their current set of analytics rules as follows:

1. Select an analytics group in the analytics rules library and then select a required rule in the **Analytics rules** area.

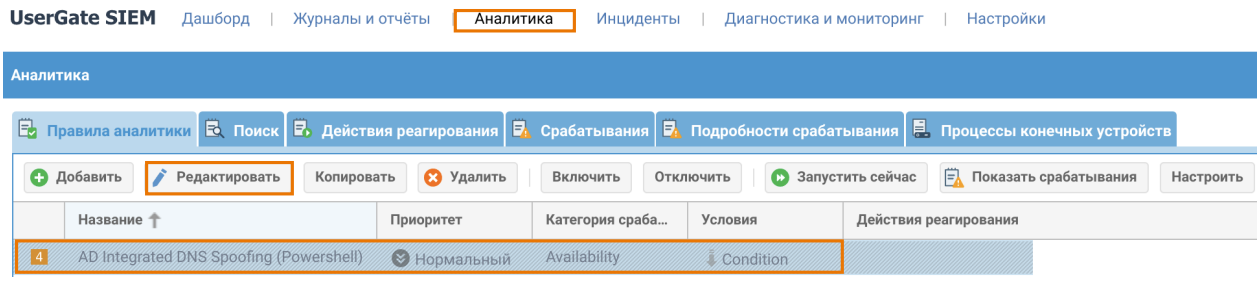
2. Click the **Add to analytics** button on the analytics rules panel:



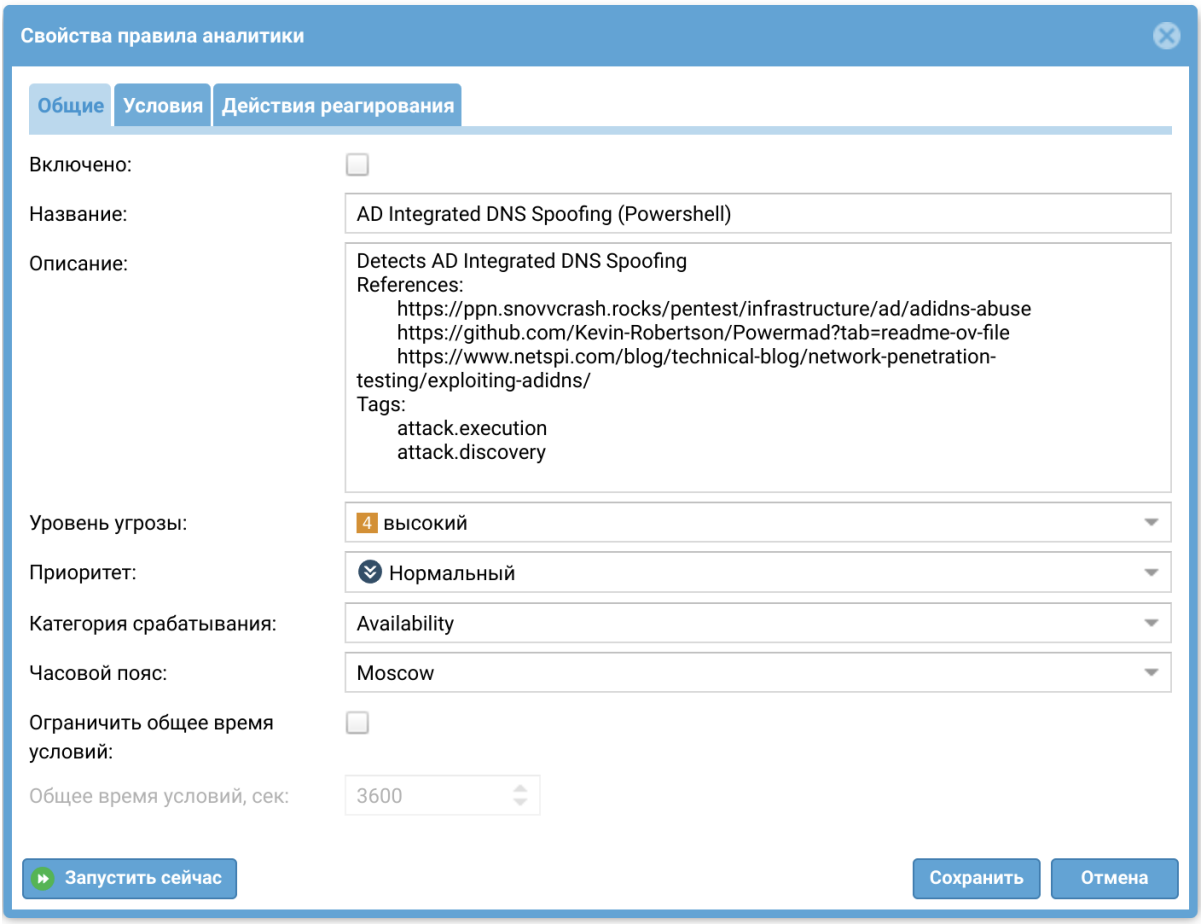
A dialog box will open, and you will be prompted to select a triggered alert category and a time zone for the imported rule:



3. After a rule was imported from the library, it will be available on the **Analytics rules** tab of the **Analytics** section:



4. Users can edit an imported rule's settings. To do so, they need to select the rule and click **Edit** on the toolbar.



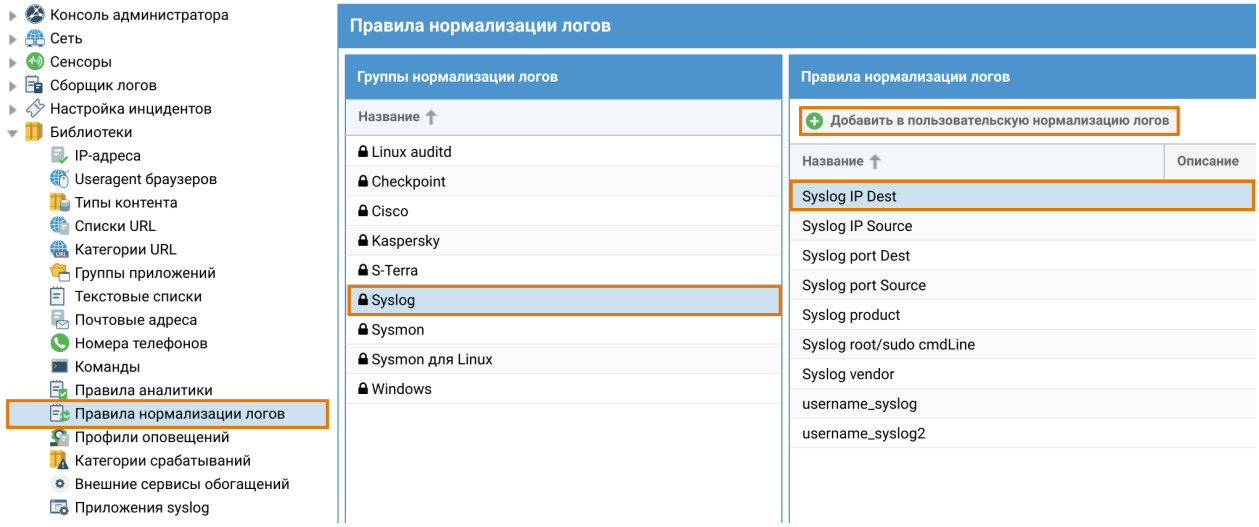
Log Normalization Rules

This library contains log normalization rules created by the UserGate developers. The library is updated provided that the UserGate SIEM license has a Security Update module.

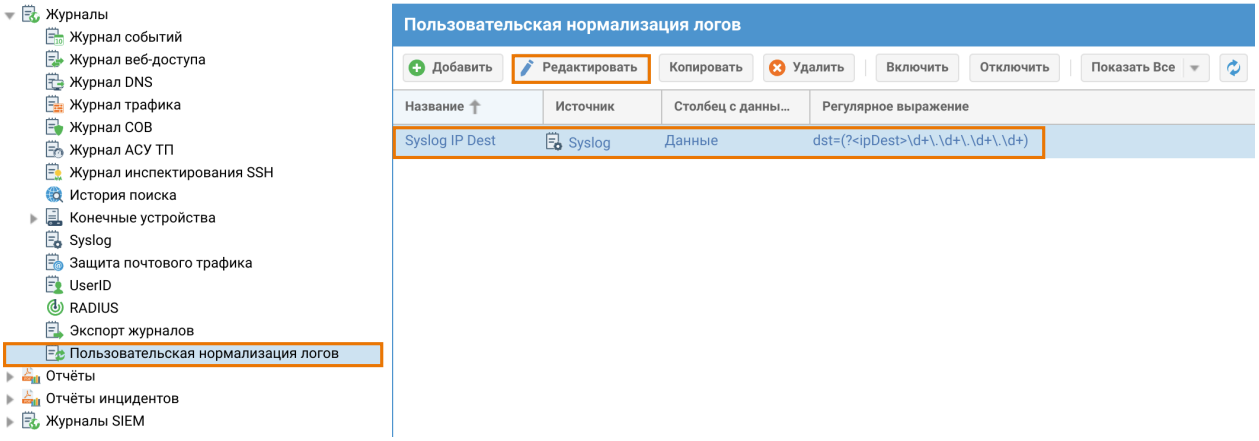
This library's availability is intended to simplify the creation of data correlation rules for UserGate SIEM users. The preset rules from the library may be used as an example so that you can write your own normalization rules. To do so, users can import rules from the library into their current set of normalization rules as follows:

1. Select a normalization group in the log normalization rules library, and then select a required rule in the **Log normalization rules** area.

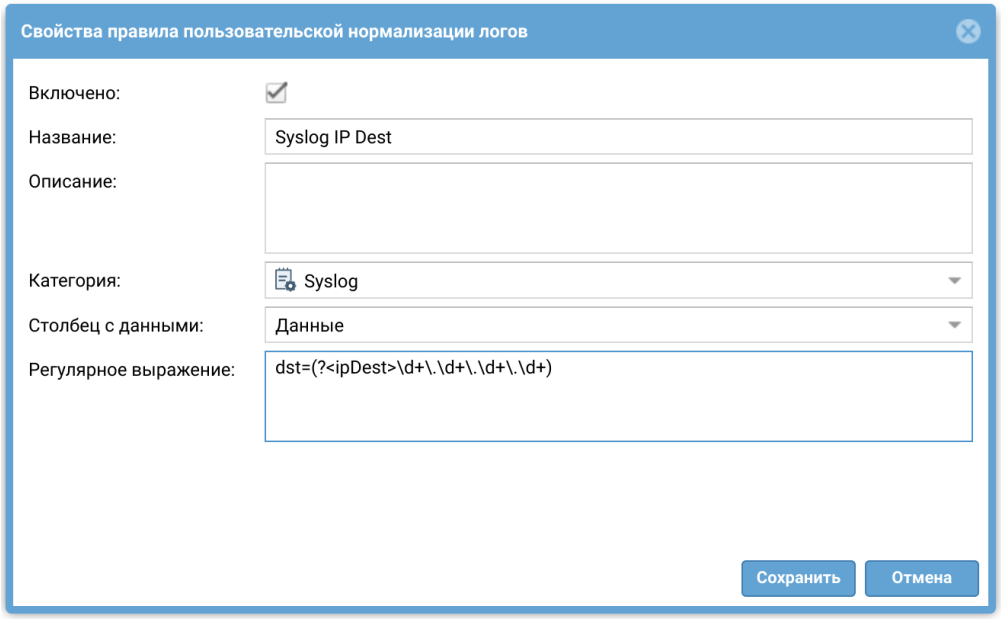
2. Click **Add to custom log normalization** on the normalization rules panel:



3. After a rule was imported from the library, it will be available under the custom log normalization section:



4. Users can edit an imported rule's settings. To do so, they need to select the rule and click **Edit** on the toolbar.



Notification Profiles

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

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

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

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

Name	Description
Authentication	Turns on authentication for SMTP server connection.
Login name	The account name for connecting to the SMTP server.
Password	The account password for connecting to the SMTP server.

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

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

Triggered Alert Categories

The **Triggered alert categories** library item allows you to create categories that can be used to group certain triggers of analytics rules applied to events. For more details on analytics rules, see the Analytics section. The following predefined categories exist:

- **Availability**: analytics rules defining incidents that degrade the availability of information systems.

- **Performance**: analytics rules defining incidents that degrade the performance of information systems.
- **Security**: analytics rules defining incidents that degrade the security of information systems.

External Enrichment Services

The External enrichment services library item represents resources used to collect additional threat information. These sources provide feeds, which are structured, processed data on IP addresses and domains, from which malicious files are distributed along with the corresponding file samples and hashes; lists of phishing websites and the email addresses of phishing message senders; addresses, from which networks are scanned for vulnerabilities; IP addresses, from which brute force attacks are launched; and malware detection signatures.

To use enrichment services, they need to be enabled. Some services require registration and provision of an access key.

Name	Description
dnsgoogle	A web service by Google that provides public DNS servers. Detailed information: https://dns.google/. Types of observables: IP.
urlhaus	The abuse.ch project. The aim of this project is collecting, tracking, and exchanging malware URLs. Detailed information: https://urlhaus.abuse.ch/. Types of observables: Domain, Hash, Host name, IP, URL.
dshield	A system for correlating firewall logs collaboratively. The system collects firewall logs from volunteers all over the world and uses them to analyze attack trends. Detailed information: https://www.dshield.org/xml.html/. Types of observables: Domain, FQDN, IP.
cybercrime	The service provides information on threat levels presented by various objects. Detailed information: http://cybercrime-tracker.net/. Types of observables: Domain, FQDN, IP, URL, Other.
cyberprotect	The service provides information on threat levels presented by various objects.

Name	Description
	Detailed information: https://console.threatscore.cyberprotect.cloud/. Types of observables: Domain, Hash, IP, URL, Useragent.
unshorten	This service allows the target URL of any short URL to be previewed and checked for malicious links. The service does not use the external resource but rather analyzes the response for the requested URL. Types of observables: URL.
ipwhois	The service provides information on IP addresses. Detailed information: https://ipwhois.io/. Types of observables: IP.
ipinfo	A tool for identifying the owner, ISP, and location of a website, domain, or IP address. Detailed information: https://ipinfo.io/. Types of observables: IP. The service requires access credentials to be entered.
hashdd	The service provides a hash database of malicious files and offers various checks to get a thorough understanding of the threat. Detailed information: https://hashdd.com/. Types of observables: Hash. The service requires access credentials to be entered.
urlscan	A service providing information on suspicious, malicious, and phishing URLs. Detailed information: https://urlscan.io/. Types of observables: Domain, FQDN, Hash, IP, URL. The service requires access credentials to be entered.
emailrep	A system collecting data on email addresses, domains, and users. Detailed information: https://emailrep.io/. Types of observables: Mail. The service requires access credentials to be entered.
greynoise	The company focuses on analyzing the Internet's background noise (data packets destined to IP addresses or ports where there is no network device configured to receive them). This kind of filtering helps reduce false triggered events. Detailed information: https://www.greynoise.io/.

Name	Description
	Types of observables: IP. The service requires access credentials to be entered.
abuseip	A project that fights malicious activity on the Internet. Detailed information: https://www.abuseipdb.com/. Types of observables: IP. The service requires access credentials to be entered.
hybridanalysis	A service for checking files for malicious content. Detailed information: https://www.hybrid-analysis.com/. Types of observables: Hash. The service requires access credentials to be entered.

Syslog Applications

The section contains applications that can be used in syslog rules for information collection.

To add an application, follow these steps:

Name	Description
Step 1. Create an application.	Click **Add** and provide a name and description for the application.
Step 2. Specify the application.	Specify the name of the application to which syslog rules will be applied.

DIAGNOSTICS AND MONITORING

Routes

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

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

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

Ping

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

Name	Description
Ping host	The host to be checked.
TTL	The maximum number of intermediate hosts allowed on the path to the host to be pinged.
Interface	The selected interface address will be used as the source address for the ping command, and the interface for sending packets will be selected in accordance with the routing table.
Counter	Number of repetitions.
Show timestamp	Add timestamps to the command output.
Don't resolve names	Use IP addresses without resolving them to domain names.

Traceroute

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

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

DNS Query

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

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

NOTIFICATIONS

Alert Rules

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

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

Specify the following parameters for the rule:

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

SNMP

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

To configure monitoring using SNMP:

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

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

Name	Description
Rule name	The name of the rule.
Server IP address for traps	The IP address of the trap server and the port on which the server will listen for notifications. Usually, it is UDP port 162. This setting is required only if you need to send traps to the notification server.
Community	SNMP community is a string that identifies the UserGate server and SNMP management server for SNMP v2c. Use only Latin letters and numbers.
Context	Optional parameter that defines the SNMP context. Use only Latin letters and numbers. Some devices may have multiple copies of the entire MIB subtree. For example, several virtual routers can be created on the device. Each such virtual router will have a complete MIB subtree. In this case, each virtual router can be specified as a context on the SNMP server. The context is identified by name. When the client makes a request, the context name can be specified. If the context name is not specified, the default context will be requested.
Version	Specify the version of the SNMP protocol used in the rule. Available options: SNMP v2c and SNMP v3.
Allow SNMP queries	

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

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

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

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

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

You can download the following MIB files:

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

UTM-TRAPS-MIB

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

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

UTM-TRAPS-BINDINGS-MIB

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

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

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

UTM-MIB

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

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

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

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

UTM-INTERFACES-MIB

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

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

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

Name	Data type	Description
		(Serial Line Internet Protocol) connection. SLIP is defined in the IETF RFC 1055 standard. • **32**: frame-relay: allows packet-switched data transmission across an interface between user devices and network equipment.
ifMtu	Integer	Maximum size of a network layer packet that can be sent over this interface.
ifSpeed	gauge32	Interface bandwidth in bits per second.
ifPhysAddress	String	Physical interface address (MAC address).
ifAdminStatus	Integer	Interface state assigned by the administrator: • **1**: up: ready to transmit packets • **2**: down: not working • **3**: testing: working in the test mode; cannot transmit work packets.
ifOperStatus	Integer	Current operating status of the interface: • **1**: up: ready to transmit packets • **2**: down: interface cannot transmit data packets • **3**: testing: network interface is being tested; cannot transmit working packets • **4**: unknown: interface state is unknown • **5**: dormant: network interface cannot

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

Name	Data type	Description
		unknown or unsupported protocol was used.
ifOutOctets	counter32	The number of bytes transmitted by the interface, including service bytes.
ifOutUcastPkts	counter32	Number of sent unicast packets, including packets that were dropped or not sent.
ifOutNUcastPkts	counter32	The number of sent multicast and broadcast packets, including packets that were dropped or not sent.
ifOutDiscards	counter32	Number of outgoing packets that were dropped, even if no errors were detected preventing the transmission. Buffer space release may be one of the reasons for dropping.
ifOutErrors	counter32	The number of outgoing packets that could not be transmitted due to errors.
ifOutQLen	gauge32	The send queue length (number of packets).
ifInMulticastPkts	counter32	Number of delivered multicast packets.
ifInBroadcastPkts	counter32	Number of delivered broadcast packets.
ifOutMulticastPkts	counter32	Number of sent multicast packets, including packets that were dropped or not sent.
ifOutBroadcastPkts	counter32	Number of sent broadcast packets, including packets that were dropped or not sent.
ifHCInOctets	counter64	

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

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

UTM-TEMPERATURE-MIB

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

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

Note

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

Note

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

SNMP Parameters

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

Name	Description
SNMP system name	Name of the system which is used by SNMP control subsystem.
SNMP system location	Information on physical location of the SNMP agent.
SNMP system description	Description of the system.

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

SNMP Security Profiles

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

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

Name	Description
Name	SNMP security profile name
Description	SNMP security profile description
User	User name to authenticate the SNMP manager.

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

LOGS AND REPORTS

LOGS

Description

SIEM logs all events that occur during its own operation and that of any servers connected to it. It uses the following logs:

- **Event**: events related to changes in the settings of servers connected to SIEM, user and administrator authentication, updates to various lists, etc.

- **Web access**: a detailed log of all web requests processed by SIEM.
- **DNS**: events related to the DNS traffic.
- **Traffic**: detailed log of all firewall, NAT, DNAT, Port forwarding, and Policy-based routing rules triggered. To log these events you need to enable logging in the required rules for the firewall, NAT, DNAT, Port forwarding, or Policy based routing.
- **IDPS**: events logged by the intrusion detection and prevention system.
- **SCADA**: events logged by SCADA control rules.
- **SSH inspection**: log of triggered SSH inspection rules. To log these events, logging should be enabled.
- **Search history**: user search queries in popular search engines.
- **Endpoint events**: displays events received from endpoints controlled by UserGate Endpoint software, as well as events received from the AD domain controller via WMI.
- **Endpoint rules**: trigger events for the endpoint firewall rules where logging is enabled in the settings.
- **Endpoint applications**: displays applications that were run on the devices.
- **Endpoint hardware**: contains information on the devices connected to end devices.
- **Syslog**: displays messages about events from remote Unix systems received using the syslog protocol.
- **Mail traffic protection**: contains events triggered by mail traffic protection rules that have logging enabled in their settings.
- **UserID**: contains description of events reflecting the result of UserID agent's work.
- **RADIUS log**: contains the events collected by the UserID from the RADIUS accounting data.
- **SIEM event log**: events related to changes in SIEM server settings, user and administrator authentication, updates to various lists, etc.

Log management is automated: logs are cyclically overwritten, providing free disk space necessary for work.

Log records (except the event log) are rotated automatically based on the free space on a given partition. Database rotation records appear in the SIEM event log.

Event log records are not rotated.

Event Log

The Event Log displays events related to changes to the SIEM server settings, such as added/deleted/edited account data, rules, or other items. It also displays all web console login events, Captive-portal user authentication events, etc.

To assist in finding the events of interest, the records can be filtered by various criteria such as the date range, component, severity, or event type.

Administrators can select to display only the columns they need. To do this, click on any of the columns and set the checkmarks for the columns you want to display in the context menu that appears.

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

Web Access Log

The Web access log displays all user requests to the Internet via HTTP and HTTPS. The following information is displayed:

- UserGate node where the event occurred
- Event time
- User
- Actions
- Rule
- Reasons (if a site is blocked)
- Destination URL
- Source zone

- Source IP address
- Source port
- IP dest
- Destination port
- Categories
- Protocol (HTTP)
- Type (HTTP)
- Status code (HTTP)
- MIME (if present)
- Bytes sent/received
- Packets sent
- Referrer (if present)
- Operating system
- browser Useragent

Administrators can select to display only the columns they need. To do this, click on any of the columns and set the checkmarks for the columns you want to display in the context menu that appears.

To assist in finding the events of interest, the records can be filtered by various criteria such as the user account, rule, action, etc.

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

DNS Log

DNS log lists events related to the DNS traffic. To log DNS events on the NGFW, DNS filtering must be enabled in the DNS proxy settings and logging must be enabled in the content filtering rules where DNS traffic is logged.

The following information is displayed:

- Node
- Time
- User
- Rule
- Reasons
- Domain name
- Source zone
- Source IP address
- Source port
- Source MAC address.
- Destination zone
- Destination IP address
- Destination port
- Network protocol
- URL category.
- Information

Administrators can select to display only the columns they need. To do this, click on any of the columns and set the checkmarks for the columns you want to display in the context menu that appears.

To assist in finding the events of interest, the records can be filtered by various criteria such as the protocol, date range, action, etc.

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.

Traffic Log

The Traffic log displays firewall and NAT rule trigger events for rules where logging is enabled. The following information is displayed:

- UserGate node where the event occurred
- Event time
- User
- Action
- Rule
- Application
- Protocol
- Source zone
- Source address
- Source port
- IP dest
- Destination port
- NAT source IP (in case of a NAT rule)
- NAT source port (in case of a NAT rule)
- NAT destination IP (in case of a NAT rule)
- NAT destination port (in case of a NAT rule)
- Bytes sent/received
- Packets.

Administrators can select to display only the columns they need. To do this, click on any of the columns and set the checkmarks for the columns you want to display in the context menu that appears.

To assist in finding the events of interest, the records can be filtered by various criteria such as the user account, rule, action, etc.

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

IDPS Log

The intrusion detection system log displays the triggered IPS signatures for which the logging or blocking action has been set. The following information is displayed:

- PCAP files
- NGFW node where the event occurred
- Time
- Event details
- User
- Action
- Rule
- Signatures
- Application
- Network protocol
- Source zone
- Source IP address
- Source port
- Source MAC address
- Destination zone
- Destination IP address
- Destination port
- Destination MAC address

Administrators can select to display only the columns they need. To do this, click on any of the columns and set the checkmarks for the columns you want to display in the context menu that appears.

To assist in finding the events of interest, the records can be filtered by various criteria such as the protocol, date range, action, etc.

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.

SCADA Log

The SCADA log displays events that triggered SCADA rules that have logging enabled. The following information is displayed:

- NGFW node where the event occurred
- Time
- Action
- Rule
- Source zone
- Source IP address
- Destination IP address
- Destination port
- SCADA protocol.
- SCADA command
- Register address.

Administrators can select to display only the columns they need. To do this, click on any of the columns and set the checkmarks for the columns you want to display in the context menu that appears.

To assist in finding the events of interest, the records can be filtered by various criteria such as the protocol, date range, action, etc.

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.

SSH inspection log

The SSH inspection log shows the triggered SSH inspection rules for which logging is enabled. The following information is displayed:

- UserGate node where the event occurred
- Time
- User
- Action
- Rule
- Command
- Source zone
- Source IP address
- Source port
- Source MAC address.
- Destination zone
- Destination IP address
- Destination port

Administrators can select to display only the columns they need. To do this, click any of the columns and set the check marks for the columns you want to display in the context menu that appears.

To assist in finding the events of interest, the records can be filtered by various criteria such as the protocol, date range, action, etc.

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.

Search History

The **Search history** section displays all user search queries that are configured to be logged in the safe browsing policies. Administrators can select to display only the columns they need. To do this, click on any of the columns and set the checkmarks for the columns you want to display in the context menu that appears.

To assist in finding the events of interest, the records can be filtered by various criteria such as users, date range, search engines, etc.

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

Endpoint Log

The endpoint logs display information received from endpoints controlled by UserGate Client software.

UserGate provides the following logs:

- **Endpoint events**: shows events received from the endpoints.
- **Endpoint rules**: trigger events for the endpoint firewall rules where logging is enabled in the settings.
- **Endpoint applications**: displays applications that were run on the devices.
- **Endpoint hardware**: contains information on the devices connected to end devices.

To assist in finding the events of interest, the records can be filtered by various criteria such as the date range, severity, or event type, etc.

Administrators can select to display only the columns they need. To do this, click on any of the columns and set the checkmarks for the columns you want to display in the context menu that appears.

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

Syslog

Syslog contains events collected by the UserID agent from syslog servers. The log displays user logon events and logout events. The following information is displayed:

Name	Description
	UserGate node where the event occurred.
Time	The time of the event.
Syslog record details	The link to the event.
Rule	The rule related to the syslog message.
Severity	Syslog event level.
Object	Detailed information on the process triggering the message (kernel messages, user-level messages, security/authentication etc.).
Computer name	Computer name where the event took place.
Application	Application triggering the event.
Process ID	PID of the process triggering the event.
Data	The event description.

Mail Security Log

Mail security log displays triggering events for mail security rules for which logging is enabled. The following information is displayed:

- UserGate node where the event occurred
- Time triggered
- User
- Sender

- Recipient
- Rule
- Source zone
- Source IP address
- Source port
- Destination zone
- Destination IP address
- Destination port
- Application
- Application layer protocol
- Bytes sent/received
- Packets sent/received

Administrators can select to display only the columns they need. To do this, click on any of the columns and set the checkmarks for the columns you want to display in the context menu that appears.

To assist in finding the events of interest, the records can be filtered by various criteria such as the protocol, date range, action, etc.

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.

UserID Log

The UserID log contains description of events reflecting the result of UserID agent's work. The following information is displayed:

Name	Description
Node	UserGate node where the event occurred.
Time	The time of the event.

Name	Description
Event details	Shows event details.
Action	The action applied to the event.
Log source	The source of the event received.
User	The UG user triggered the event.
IP address	The IP address of the node where the event occurred.
Information	The event description.

The RADIUS log

The RADIUS log contains the events collected by the UserID from the RADIUS accounting data. The log displays user logon events and logout events. The following information is displayed:

Name	Description
Node	UserGate node where the event occurred.
Time	The time of the event.
Rule ID	ID of the rule triggered to cause the event
User	The user, who triggered the event.
Groups	A string of groups the user is a member of.
Status	User status
Source IP	The IP address of the source where the message came from.
NAS IP address	The IP address of the NAS that authorized the user.
User's IP address	User IP address (framed IP address).

Logs Export

The SIEM logs export feature allows you to upload information to external servers for later analysis or processing.

UserGate SIEM allows you to export the following logs:

- DNS
- Events
- Web access
- IDPS
- SCADA
- SSH inspection
- Traffic
- Endpoint events
- Endpoint rules
- Endpoint applications
- Endpoint hardware.

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 configurations in the **Logs export** section.

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.
One-time export options	Select the range of log exports.
Logs to export	

Name	Description
	Select the log files to export: • DNS • Events • Web access • IDPS • SCADA • SSH inspection • Traffic • Endpoint events • Endpoint rules • Endpoint applications • Endpoint hardware. For each log, you can specify the export syntax: • CEF: Common Event Format (ArcSight) • JSON: JSON format • @CEE: JSON: CEE Log Syntax (CLS) Encoding JSON To select the desired log export format, refer to the documentation for the SIEM system you are using. For a detailed description of log formats, see Description of Log Formats.
Server type	SSH (SFTP), FTP, Syslog.
Server address	IP address or domain name of the server.
Transport	TCP or UDP; applicable only to Syslog servers.
Port	The server port to which the data should be sent.
Protocol	RFC5424 or BSD syslog RFC 3164; applicable only to Syslog servers. Select the protocol compatible with your SIEM system.
Severity	Only for Syslog server type. Optional field; consult the documentation for your SIEM system. Available values: • **Alert**: a state that requires immediate intervention. • **Critical**: a state that requires immediate intervention or signals a fault in the system. • **Errors**: errors detected in the system. • **Warnings**: warnings on potential errors that can occur if no action is taken.

Name	Description
	• **Notice**: events that relate to unusual system behavior but are not errors. • **Info**: informational messages.
Object	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**. • **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.
Repeat password	Confirm the 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.
Schedule	Select schedule for sending logs. Not applicable to the Syslog export method. The available options are: • Daily

Name	Description
	• 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".

Custom Log Normalization

You can use log normalization rules to normalize data received by the SIEM system from different sources (sensors).

Logs coming from different sensors to the SIEM can be processed according to regular expressions specified in the custom normalization rules. As a result, standard SIEM database fields will be populated with values found in the logs.

The order of normalization rules execution is set by the administrator under **Logs and reports → Logs → Custom log normalization**. Subsequent rules may overwrite the values that were normalized and written by the previous rules. You can change a rule's place by dragging and dropping it, or by using the **Down**, **Up**, **Higher**, **Lower** menu buttons.

Log sources and their fields that can be further normalized:

Endpoint Event Log	Syslog
Device (sensorName)	Rule (ruleName)
Data (data)	Computer name (computerName)
Status (status)	Application (applicationName)
Log event source (sourceName).	Process ID (processId)
Incident category (logCategoryString)	Data (data)
Computer name (computerName)	
User (userName)	
Insertion string (insertionString)	
Log file (logFile)	

List of SIEM database fields that can be used to store the data found (i. e. these field names can be specified in regular expressions in normalization rules):

Name	Type
node	String
userId	guid
user	String
ruleId	guid
rule	String
ipSource	ip
ipDest	ip
portSource	integer16
portDest	integer16

Name	Type
macSource	mac
macDest	mac
natIpSource	ip
natIpDest	ip
natPortSource	integer16
natPortDest	integer16
applicationName	String
bytesSent	integer64
bytesRecv	integer64
packetsSent	integer64
packetsRecv	integer64
mime	String
httpMethod	String
referer	url
url	url
statusCode	integer16
userAgent	String
sensor	String
sensorId	guid
processId	String
networkProtocol	ip protocol
status	String
error	Integer

Name	Type
counterId	guid
logCategory	integer16
taskCategory	String
computerName	String
logEventCode	integer16
logEventId	integer16
logEventType	integer16
logFile	String
severity	severity
module	String
component	String
event	String
syslogFacility	integer8
syslogSeverity	integer8
image	String
cmdLine	String
originalFileName	String
parentProcessId	integer64
parentImage	String
parentCommandLine	String
targetObject	String
targetFilename	String
scriptBlockText	String

Name	Type
queryName	String
queryResults	String
workstationName	String
logonId	String
imageLoaded	String
sourceImage	String
targetImage	String
customString1	String
...	String
customString15	String
customNumber1	String
...	String
customNumber5	String
customIp1	ip
customIp2	ip
customDate1	date
customDate2	date

Field types:

Type	Default value	Description
String	""	String of any length.
guid	00000000-0000-0000-0000-00000000000	A string of the form XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, where X is a hexadecimal digit (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, A, B, C, D, E, F).

Type	Default value	Description
ip	0.0.0.0	A string of the form X.X.X.X, where X = 0..255; or X:X:X:X:X:X:X:X, where X = a 4-digit hexadecimal number.
Integer	0	Any non-negative integer.
url	""	A URL string, RFC1738 format.
ip protocol	255	A number 0 .. 255 or string from protocol list below.
severity	unknown	Strings: unknown, critical, error, info, warning.
integer8	0	An integer in the range [0, 255].
integer16	0	An integer in the range [0, 65535].
integer64	0	An integer in the range [0, 2^64-1].
date	1970-01-01T00:00:00	2024-03-06T10:30:00.

The list of protocols accepted for the networkProtocol field (letters can be uppercase or lowercase):

Name	Value
IP	0
ICMP	1
IGMP	2
GGP	3
IP-ENCAP	4
ST	5
TCP	6
CBT	7

Name	Value
EGP	8
IGP	9
BBN-RCC-MON	10
NVP-II	11
PUP	12
ARGUS	13
EMCON	14
XNET	15
CHAOS	16
UDP	17
MUX	18
DCN-MEAS	19
HMP	20
PRM	21
XNS-IDP	22
TRUNK-1	23
TRUNK-2	24
LEAF-1	25
LEAF-2	26
RDP	27
IRTP	28
ISO-TP4	29
NETBLT	30

Name	Value
MFE-NSP	31
MERIT-INP	32
DCCP	33
3PC	34
IDPR	35
XTP	36
DDP	37
IDPR-CMTP	38
TP++	39
IL	40
IPV6	41
SDRP	42
IPV6-ROUTE	43
IPV6-FRAG	44
IDRP	45
RSVP	46
GRE	47
DSR	48
BNA	49
IPSEC-ESP	50
IPSEC-AH	51
I-NLSP	52
SWIPE	53

Name	Value
NARP	54
MOBILE	55
TLSP	56
SKIP	57
IPV6-ICMP	58
IPV6-NONXT	59
IPV6-OPTS	60
ANY HOST INTERNAL PROTOCOL	61
CFTP	62
ANY LOCAL NETWORK	63
SAT-EXPAK	64
KRYPTOLAN	65
RVD	66
IPPC	67
ANY DISTRIBUTED FILE SYSTEM	68
SAT-MON	69
VISA	70
IPCU	71
CPNX	72
CPHB	73
WSN	74
PVP	75

Name	Value
BR-SAT-MON	76
SUN-ND	77
WB-MON	78
WB-EXPAK	79
ISO-IP	80
VMTP	81
SECURE-VMTP	82
VINES	83
IPTM	84
NSFNET-IGP	85
DGP	86
TCF	87
EIGRP	88
OSPFIGP	89
SPRITE-RPC	90
LARP	91
MTP	92
AX.25	93
IPIP	94
MICP	95
SCC-SP	96
ETHERIP	97
ENCAP	98

Name	Value
ANY PRIVATE ENCRYPTION SCHEME	99
GMTP	100
IFMP	101
PNNI	102
PIM	103
ARIS	104
SCPS	105
QNX	106
A/N	107
IPCOMP	108
SNP	109
COMPAQ-PEER	110
IPX-IN-IP	111
VRRP	112
PGM	113
ANY 0-HOP PROTOCOL	114
L2TP	115
DDX	116
IATP	117
STP	118
SRP	119
UTI	120
SMP	121

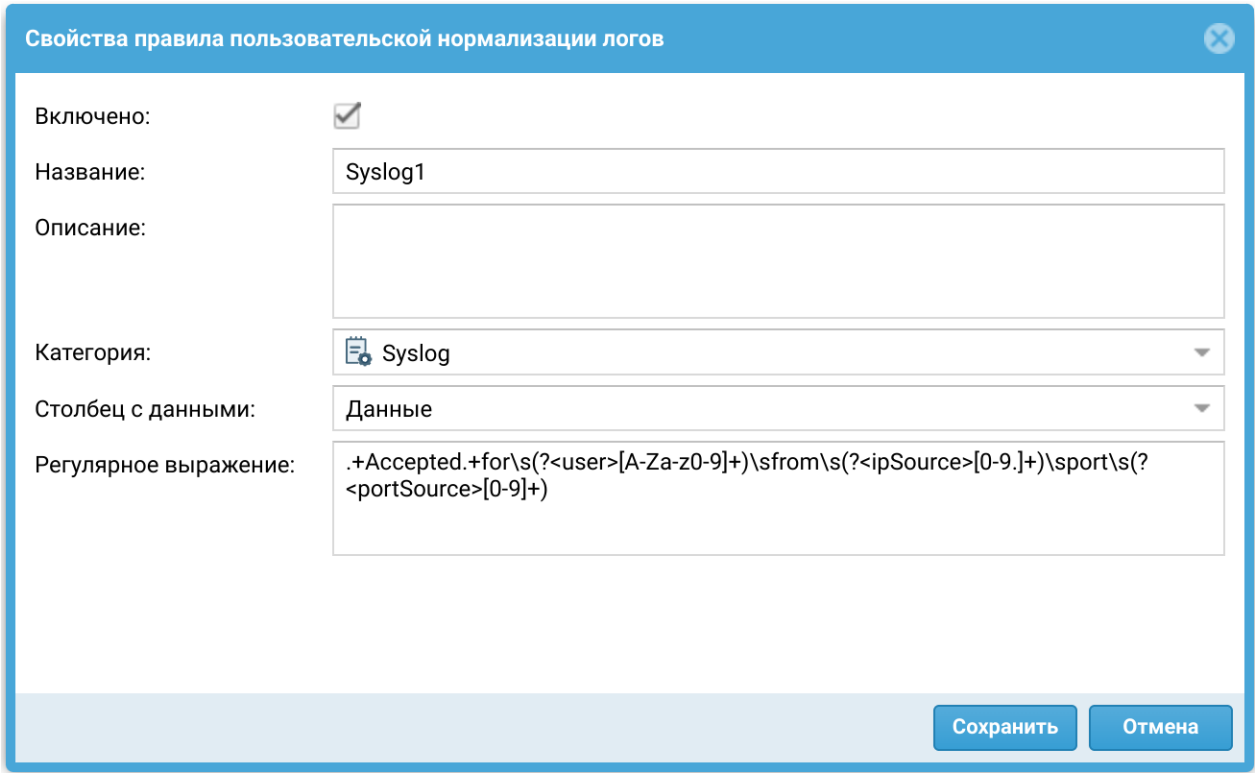
Name	Value
SM	122
PTP	123
IS-IS OVER IPV4	124
FIRE	125
CRTP	126
CRUDP	127
SSCOPMCE	128
IPLT	129
SPS	130
PIPE	131
SCTP	132
FC	133
RSVP-E2E-IGNORE	134
MOBILITY HEADER	135
UDPLITE	136
MPLS-IN-IP	137
MANET	138
HIP	139
SHIM6	140
WESP	141
ROHC	142
USE FOR EXPERIMENTATION AND TESTING	254

Name	Value
RESERVED	255

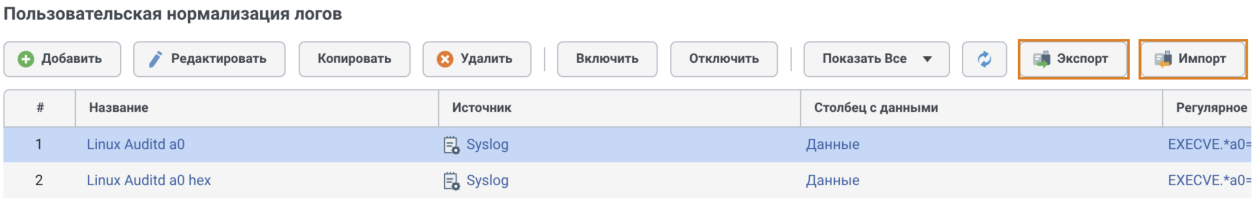
To create a normalization rule, click **Add** under **Logs and reports → Logs → Custom log normalization** and fill in the following fields in the window that opens:

Name	Description
Enabled	Enable/disable custom log normalization rule.
Name	Name of the custom log normalization rule.
Description	Description of the custom log normalization rule.
Category	Select the category (type) of the logs to which this rule is applied: • Endpoint Event Log; • Syslog
Data column	Select the column the data will be extracted from.
Regular Expression	A regular expression string with group names matching the columns to which the values will be written.

Example of a rule that processes syslog category logs, extracts username, ip and port, and writes these values into the corresponding fields in the SIEM database:



The rules of custom normalization can be exported to a binary file or imported into the system by clicking **Export/Import** in the tools menu under **Logs and reports → Logs → Custom log normalization** (available starting from version 7.4.0):



SIEM has an embedded library of log normalization rules that contains reference normalization rules created by the UserGate developers. These rules can be imported into the custom log normalization section and then used to create new rules. You can find more details on the library of rules in the Log Normalization Rules section.

Data Search and Filtering

Usually, logs contain huge numbers of records, and SIEM provides convenient ways to search and filter the raw data for the required information. Administrators can search the contents of the logs in basic and advanced modes.

With a simple search, administrators use a graphic interface to set filters by values of the required log fields, thus filtering out unnecessary information. For example,

administrators can specify a time range of interest, a list of users, categories, etc. Setting the search criteria is intuitive and does not require any special knowledge.

You can create more complex filters in the advanced search mode using a special query language. In the advanced search mode, you can build queries using log fields that are not available in the basic mode. 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 should 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

Name	Description
	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"* 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 making an advanced query, SIEM shows possible field names, applicable operators, and possible values, making it easier for the system operator to make complex queries. When you switch from basic to advanced search mode, SIEM automatically generates a search query string that matches the filter specified in the basic search mode.

REPORTS

General Information

Reports allow administrators to provide different slices of data about security events, configurations, or user actions. Reports can be created automatically according to previously created rules and templates and sent to recipients by email.

The **Reports** section contains four subsections: **Templates**, **Custom report templates**, **Report rules**, and **Generated reports**. To create a report, follow these steps:

Name	Description
Step 1. Create a generate report rule.	Create a rule to generate a report and specify all necessary report parameters.
Step 2. Run the report.	Run the report in manual mode or wait until it runs automatically according to the schedule specified in the rule.
Step 3. Receive the report.	Receive the report by mail if you configured the rule to send the report by mail, or download the report from the **Generated reports** section.

Note

Creating a report can take quite a long time and consume a lot of computing resources.

Templates

A template defines what the report will look like and what fields it will include. Report templates are provided by the UserGate developer.

Here is the list of report templates by category:

- **Custom**: a group of templates for generalized statistics of report rule triggering.

- **Captive portal**: a group of templates for events related to user authentication using the Captive portal.
- **Endpoint applications**: a group of templates with lists of applications that were run on the devices.
- **Endpoint rules**: a group of templates for events of endpoint firewall rule triggering.
- **Endpoint events**: shows events received from the devices that are controlled using the UserGate Endpoint software.
- **Events**: a templates group for events recorded in the event log.
- **IDPS**: a templates group for events recorded in the IDPS log.
- **Mail security**: a group of templates for the events recorded in the mail security log.
- **Network activity**: a templates group for events recorded in the traffic log.
- **Web portal**: a templates group for events related to authentication via SSL VPN.
- **Traffic**: a templates group for events recorded in the traffic log and related to the volume of traffic consumed by users, applications, etc.
- **UserID**: a group of templates to create reports on the UserID agent activity.
- **VPN**: a templates group for events related to VPN.
- **Web activity**: a templates group for events recorded in the web access log.

Each template includes a name, report description, and report presentation type (table, histogram, pie).

Custom Report Templates

Unlike regular report templates provided by the solution vendor, custom templates make it possible to generate reports tailored to user needs. The administrator can select the desired fields to display and set the criteria and possible groupings. The custom reports created in this way can be used in report rules along with the regular predefined reports. To create a custom report template, go to the **Reports --> Custom report templates** section, click **Add**, and provide these settings:

Name	Description
Name	The name of the custom report template.
Description	An optional description of the custom report template.
Category	Select the data source for the template. Available values: • Events • Traffic • Web access • IDPS • SSH inspection • Triggered alerts • Endpoint events • Endpoint rules • Endpoint applications
Filter query	An SQL-like query string that allows you to limit the amount of information used to generate a report based on this template. To construct a query, use field names and values, keywords, and operators. The data fields can be the columns listed below in the **Columns** field. For keywords and operators with examples of their use, see the Data Search and Filtering section.
Sort by	Specify the data field to sort the data by. The sorting can be in the ascending or descending order.
Group by	Specify the data field to group the data by.
Columns	The list of columns available for the specific data source.
Selected	The list of columns selected for display in the report.

Report Rules

Report rules set the parameters of the report to be created, as well as the schedule to run the reports and methods of delivering the reports to users. When creating a report rule, administrators specify the following parameters:

Name	Description
Enabled	Enable or disable the report.
Name	The name of the rule.
Description	Optional field for rule description.
Report language	Language to use in the report.
Time range	Time range for preparation of the report.
Report format	Format (PDF, HTML, XML, CSV) of the report. **Important!** Creating reports in PDF results in a high load on the processor and memory. The larger the report, the higher the load. Do not use the PDF format for custom report templates. The **Detailed list of all visited URLs** and **Detailed list of all visited sites** reports use CSV format, regardless of the format you select.
Number of records	Set a limit on the number of records displayed in reports that have a limit on the number of top records, for example, the top 20 users who encountered errors authenticating in the web console.
Group by limit (if applicable)	Set a limit on the number of records displayed in reports that have a limit on the number of grouped records, for example, the top 10 users by category: a maximum of 10 users will be listed for each category. This restriction applies only to report templates that contain grouping.
Users	Specify users or user groups for which the report will be created. If not specified, the report will be created for all users.
Templates	List of templates used to build the report. You need to add at least one template.
Schedule	Select a schedule to generate reports. The available options are: • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The

Name	Description
	fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 0-12) (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".
Delivery	You can optionally send reports to recipients via the SMTP protocol. To do this, specify the following: • SMTP profile to use for sending reports. For more details about how to configure SMTP profiles, see Notification Profiles. • From: email sender name. • Subject: email subject. • Body: email body. • Recipients: list of the email recipients. The recipients must be added to the lists of the **Emails** library.

Note

Creating a report can take quite a long time and consume a lot of computing resources. It is especially important to consider resource utilization when running reports over a large range of time.

Note

To run a report rule, you do not need to enable it and specify the time when the rule is run. You can manually run any report, including a disabled one, by selecting the rule you want from the list of rules and clicking the Run now button. When created, the report appears under Generated reports.

Generated reports

All generated reports are stored under **Generated reports**. The reports are in PDF or CSV format. For each report the name of the report, which matches the name of the report rule that was used to create this report, the time the report was created, and the size of the report are listed.

To download the report, click **Download**. To delete the report, click **Delete**.

To customize the storage time of the reports (rotation), click the **Configure** button. The default value is 60 days.

INCIDENT REPORTS

General Information

In this section, the administrator can generate reports on information security incidents. Reports can be generated based on the rules and templates created; the report can be downloaded or sent to a connector.

The section contains three subsections: **Incident report templates**, **Incident report rules** and **Generated incident reports**. To create a report, follow these steps:

Name	Description
Step 1. Create a generate report rule.	Create a rule to generate a report and specify all necessary report parameters.
Step 2. Run the report.	Select an incident and generate a report.
Step 3. Receive the report.	Report generation records can be found in the **Generated incident reports** section.

Incident report templates

A template defines what the report will look like and what fields it will include. There are 2 categories of incident report templates:

- **Key-Conclusion format – use these templates to customize the fields to be displayed in the report. You can create your own templates of this type.**
- **Incidents** – a group of templates used to create incident reports. Templates are provided by UserGate.

Each template includes a name, report description, and report presentation type (table, histogram, pie).

Incident report rules

Report rules define the parameters of the report to be created and the methods of delivering the reports to users. When creating a report rule, administrators specify the following parameters:

Name	Description
Name	The name of the rule.
Description	Optional field for rule description.
Report language	Language to use in the report.
Timezone	Time zone to be used to generate the report.
Report format	Format (PDF, HTML) of the report to be generated.
Connector	The connector to which the report should be sent (optional).
Templates	List of templates used to build the report. You need to add at least one template.

Note

Creating a report can take quite a long time and consume a lot of computing resources. It is especially important to consider resource utilization when running reports over a large range of time.

Once a rule is created, you can run a report for the selected incident. The report you generate can be downloaded locally or sent to the selected connector.

Generated incident reports

All the generated reports are stored under **Generated incident reports**. The reports are in PDF or HTML format. For each report, the name (matching the name of the report rule that was used to create this report), the time of creation, and the file with its size are specified. All reports can be downloaded or deleted.

To customize the storage time of the reports (rotation), click the **Configure** button.

ANALYTICS

General Information

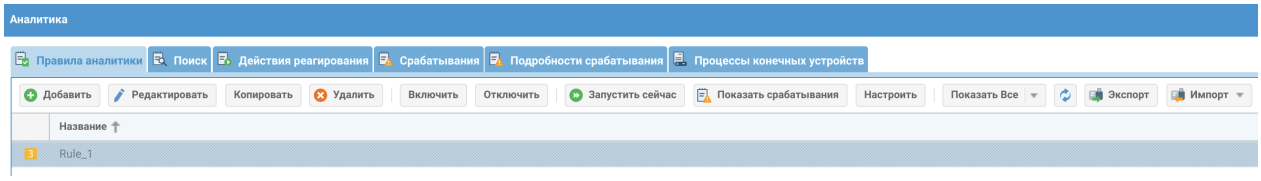
With UserGate SIEM, you can analyze security event logs received from the configured sensors such as UserGate NGFWs, UserGate Client endpoints, third-party network devices that support SNMP communication, and WMI sensors. All data is stored in a single database, making it possible to perform complex searches, correlate repetitive events, aggregate them into security incidents, and simplify the process of incident investigation.

The basic unit of incoming information for UserGate SIEM is an event. An **Event** is a single log record, e.g., a single instance of an IDPS rule triggered on a UserGate NGFW, blocked access to a prohibited resource (triggering of a blocking content filtering rule), successful or failed attempt to access the management console, or other similar occurrences recorded on devices connected to UserGate SIEM. While an individual event may not provide sufficient information about a security threat, multiple events of the same type (e.g., failed attempts to access the management console) or dissimilar events recorded in a specific sequence and coming from different sources can be useful for identifying a threat. This process is called event correlation. A group of events combined under an analytics (correlation) rule is called a **Triggered alert**. A security engineer analyzes the triggered alert, examines the events that caused the alert and can, if necessary, create a security **Incident** based on one or multiple triggered alerts.

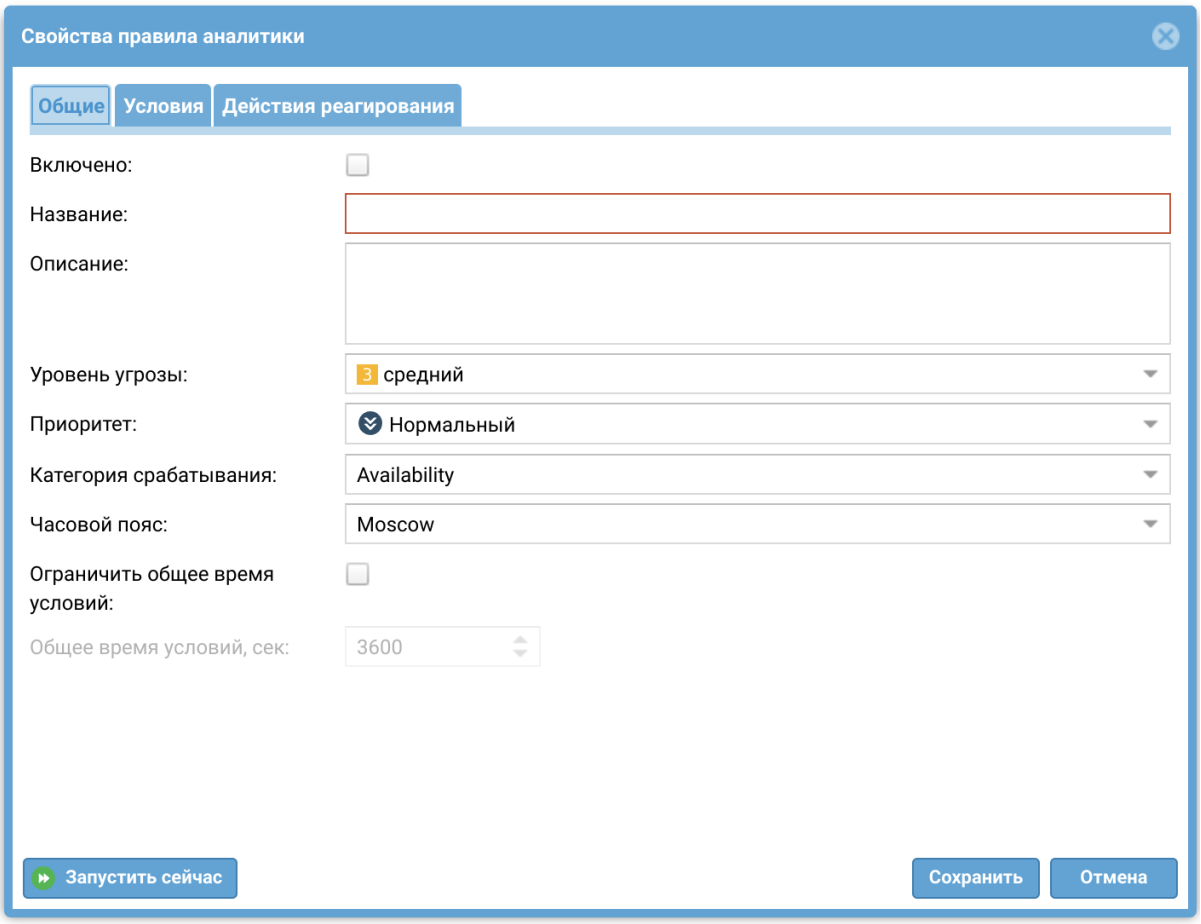
Using analytics rules, the security engineer can automate the process of event correlation and triggered alert generation as well as assign certain **Response actions** to the generated triggered alerts. All of this makes it easier to investigate logged events and contributes to reducing the time between problem detection and resolution.

In the **Analytics** section of the administrator's web interface, you can configure analytics rules, create response actions, and view the trigger log with the details for each triggered alert. These features will be detailed in the relevant chapters below, namely Response Actions, Triggered Alerts, and Triggered Alert Details.

The **Analytics rules** tab allows you to create log event processing rules. By configuring analytics rules, you can perform complex searches on cybersecurity events. The rule is triggered when events from different sources are found to be correlated. Rules can function in two modes: historical (analyze events for the selected time period) and real-time.



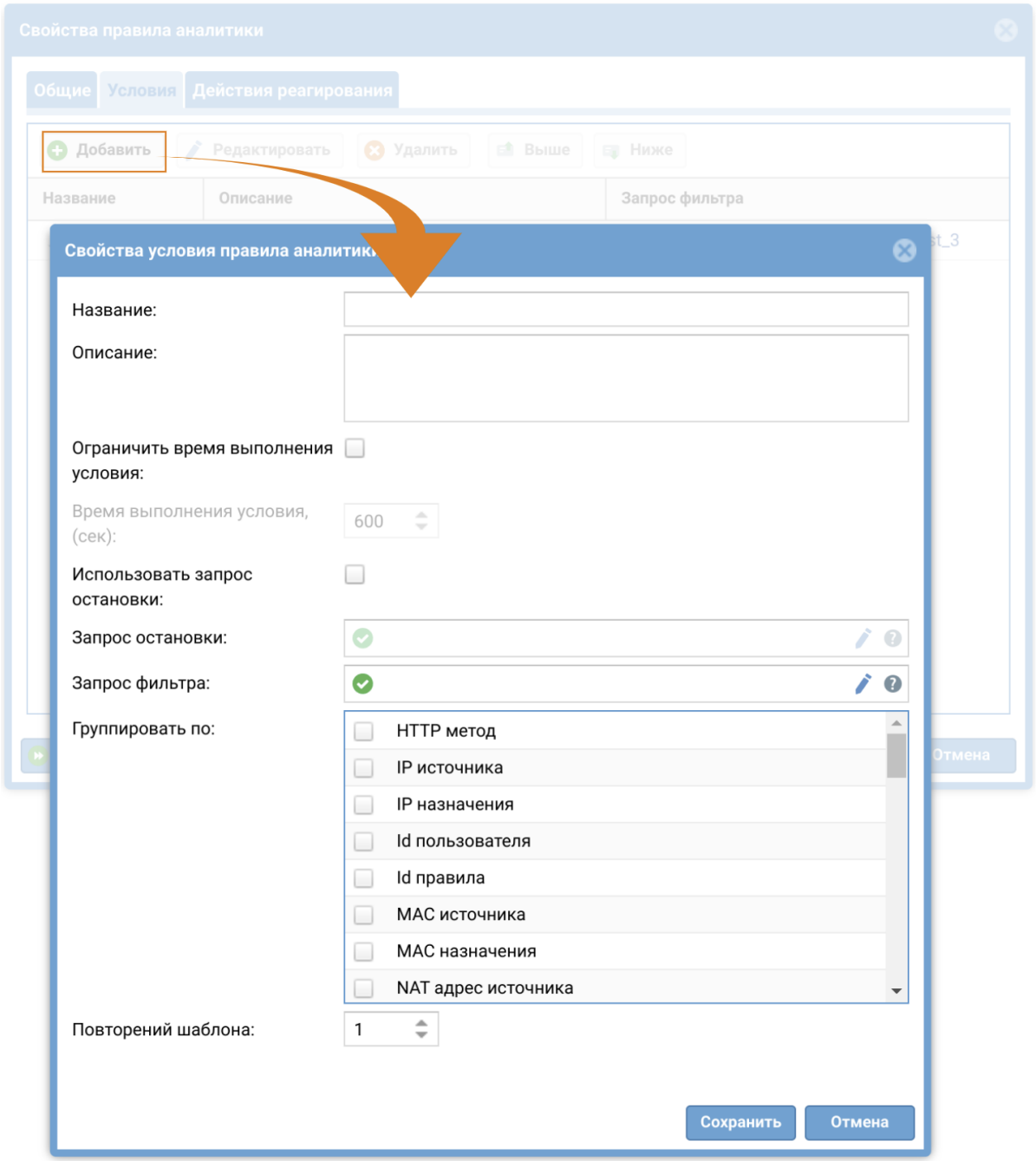
To create a rule, click **Add** on the toolbar. In the analytics rule properties window that opens, configure the rule settings on the **General** tab:



Name	Description
Enabled	Enable or disable the real-time triggering of the analytics rule.
Name	The name of the analytics rule.
Description	An optional description of the analytics rule.
Threat level	The threat level that will be displayed when the rule is triggered. The following threat levels are defined: • **very low**: the events present a very low threat level, and the administrator may choose not to take any action; • **low**: the events present a low threat level, and the administrator may choose not to take any action; • **medium**: the events require attention; • **high**: the events require investigation and response; • **very high**: the events require investigation and urgent response.
Priority	The priority assigned to triggered alerts for this analytics rule: • **low**: low response priority;

Name	Description
	• **normal**: needs attention and may need response; • **important**: needs attention and response; • **critical**: requires urgent response; When the analytics rule is triggered, the priority will indicate the severity of the triggered alert.
Category	The category to which the triggered alert belongs. The following predefined categories are available: • **Security**: incidents that degrade the security of information systems; • **Availability**: incidents that degrade the Availability of information systems; • **Performance**: incidents that degrade the performance of information systems. Additional triggered alert categories can be created in the **Libraries → Triggered alert categories** section of the **General settings** tab.
Timezone	The timezone that analytics rules will use (because the server can collect data from sources located in different timezones).
Limit the total time of conditions	Enable or disable the time limit for all conditions in the rule. If the total time limit is enabled, the analytics rule will be triggered only if all conditions configured in the rule are met the specified number of times within that time period.
Total time of conditions, sec	The time period within which all conditions in the analytics rule must be matched the specified number of times for the rule to be triggered. The time is set in seconds. Specifying the total time of conditions to be met is available when the **Limit the total time of conditions** checkbox is set.

In the **Conditions** tab of the analytics rule properties window, specify one or multiple conditions that will trigger the rule. If there are multiple conditions, they are combined using a Boolean **AND** and evaluated top to bottom. Thus, a rule will be triggered only if all its conditions are matched. To create a condition, click **Add**. Provide the following parameters:



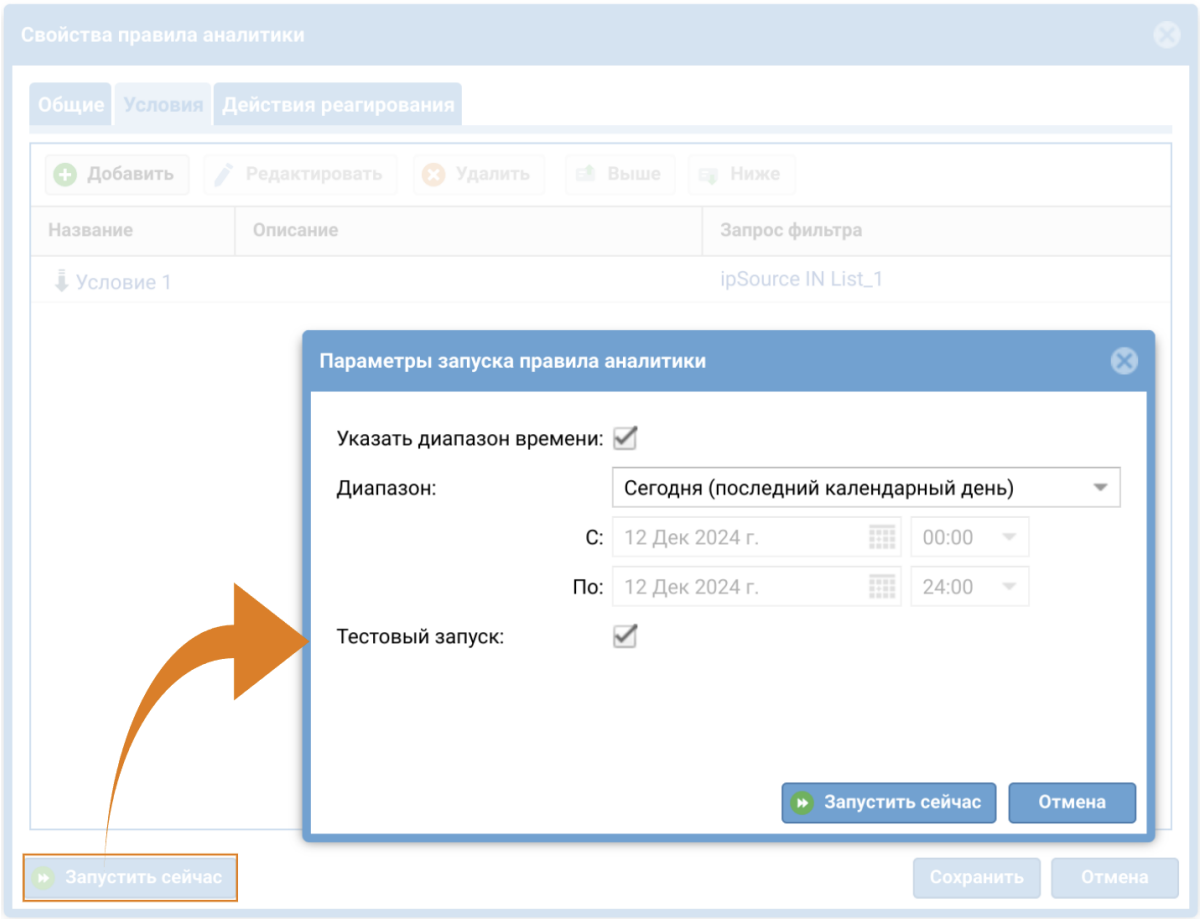
Name	Description
Name	The name of the analytics rule condition.
Description	An optional description of the analytics rule condition.
Limit condition time	Enable or disable the time limit for the condition. If the time limit is enabled, the analytics rule will be triggered only if the condition is matched the specified number of times within that time period.
Condition time, sec	

Name	Description
	The time period within which the condition must be matched the specified number of times for the analytics rule to be triggered. The time is set in seconds. Specifying the time for condition execution is available when the **Limit condition time** checkbox is set.
Use stop query	Enable or disable the use of a break query in the analytics rule.
Stop query	An SQL-like stop search query is executed along with the condition query. To formulate a query, use field names, field values, keywords, and operators (set similarly to a filter query). If, when performing an analysis, at least one record is found that matches the specified stop query, before the specified number of events that match the condition of the analytics rule are found, then the analytics rule will not work, and the counter for the number of records found before the stop query is executed will be reset.
Filter query	An SQL-like condition search query against the log database. To formulate a query, use field names, field values, keywords, and operators. For the query syntax, refer to the section Data Search and Filtering. The query can also be written using the Google/RE2 syntax in the *MATCH* operator. **Example**. Search query: *source = 'wmi log' and logFile = 'Microsoft-Windows-Sysmon/Operational' and logEventId = 1 and data MATCH 'ParentCommandLine:(.*)cmd.exe' and data ~ 'CertReq -Post -config'*. This query will perform a search in the endpoint event log that gets data from the Microsoft-Windows-Sysmon/Operational log. When an event is found indicating the creation of a new process, a search is run for the parent process (i.e. the process that caused the new process to be created) and a *certreq* command invocation with parameters. The *MATCH* part of the query allows you to detect that *certreq* was invoked from *cmd* (the command line). This identifies *cmd.exe* as the parent for the current process. More details on the use of Google/RE2 syntax with the *MATCH* operator can be found here: https://github.com/google/re2/wiki/Syntax.
Group by	The list of parameters by which rules can be grouped as a result of a triggered alert. The fields will be displayed when triggered alert details are viewed.

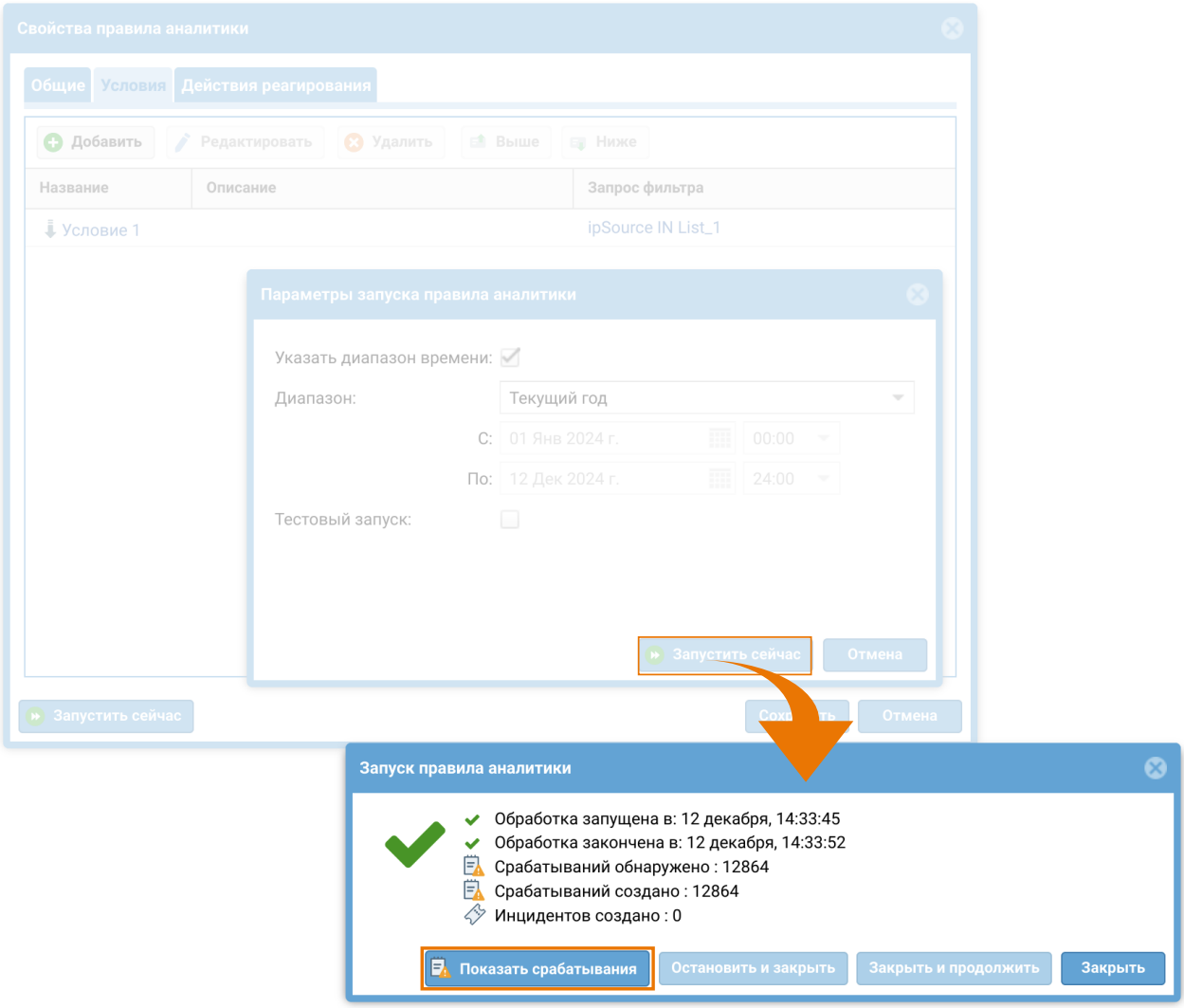
Name	Description
	The parameters that can be used for grouping are described in the Analytics Search section. When grouping categories are specified, the analytics rule will be triggered only if the condition is matched for this specific category the number of times specified in the **Pattern repeats** field.
Pattern repeats	How many times the condition must be matched for the rule to be triggered. This can be used with or without the **Limit condition time** setting.

The **Run now** button, located at the bottom of the analytics rule properties window, runs event analysis for a certain time range (historical mode). In the window that opens, specify the time range for analysis. If the **Use time range** checkbox is not set, the analysis is run using the created analytics rule over the entire time span covered by the whole event database.

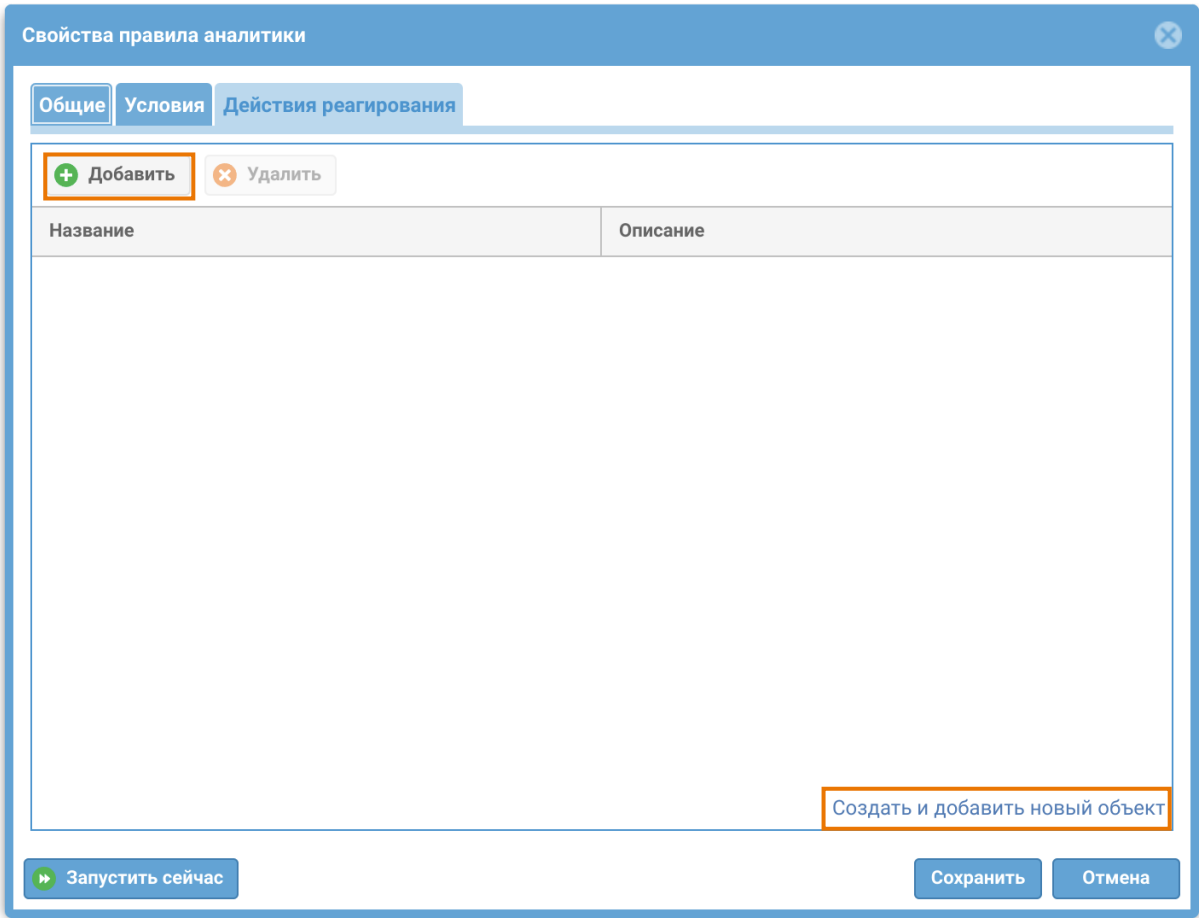
You can also run the rule without writing to the alert log — e.g., to check if the rule works correctly or just view the number of triggered alerts. To do that, set the **Test run** checkbox:



When the analysis is completed, you can click **Show triggered alerts** in the **Analytics rule execution** window to open the alert log and view the triggered alert details for the rule.

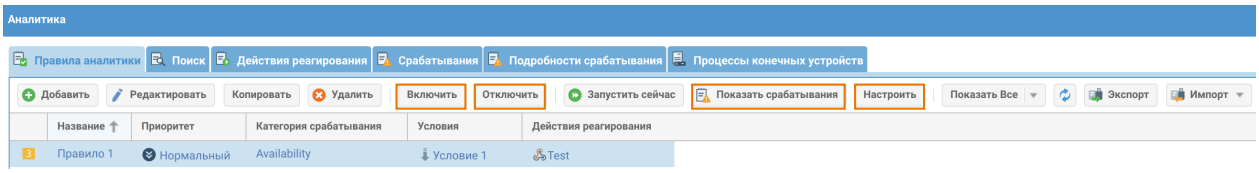


In the **Response actions** tab of the analytics rule properties window, you can add actions to be performed automatically when the analytics rule is triggered. Response actions can be created by clicking **Create and add new object** or added from the list of existing actions by clicking **Add**:



For more details on response actions and how to configure them, see the section Response Actions.

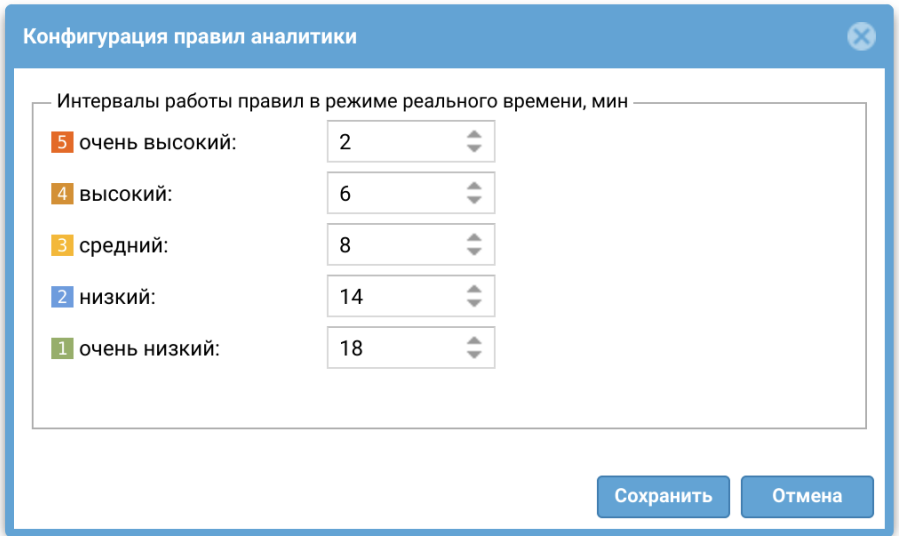
To run the rule in real time, click **Enable** on the analytics section's toolbar. To stop the execution of the selected analytics rule, click **Disable**.



The created rules can be edited, deleted, and copied. By clicking **Show triggered alerts** on the analytics section's toolbar, you can view a log showing quick details about all triggered alerts for this rule. You can also configure the rule list to display all rules or only enabled/disabled rules.

SIEM has an embedded library of analytics rules that contains reference analytics rules created by the UserGate developers. These rules can be imported into the analytics section and then used to create new rules. For more details, see the section Analytics Rules.

The **Configure** button on the analytics section's toolbar allows you to set time intervals for real-time analytics rule execution depending on the rule's severity level:



Export and import are also available for analytics rules. Rules are imported in binary or YAML format. Rules can only be exported in binary format; the selected rules or all created ones are exported if no rules were selected.

When configuring conditions for analytics rules, you can group events by parameters used in SIEM, NGFW, and endpoint log records. For a list of parameters that can be used for event grouping, see the table in the Analytics Search section.

Examples of Analytics Rule Configuration

Here are some examples of setting up analytics rules.

Example 1. Search for brute force attempts

A brute force attack is a method of cracking user accounts by guessing their passwords. The essence of the approach is sequential automated iteration over of all possible character combinations to determine the correct one.

After configuring the general settings, such as rule name, description, threat level, priority, triggered alert category, and timezone, several conditions were specified.

```
source = 'endpoint events log' AND logEventId = 4625 AND data MATCH
'Failure Reason:(\s*)Unknown user name or bad password.'
```

This condition performs a search of the endpoint event log for an event ID of 4625 corresponding to a failed account authorization attempt. The MATCH part of the

condition specifies the reason for denied authorization as an invalid login or password.

For more details on event 4625, see the relevant documentation: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625.

```
source = 'endpoint events log' AND logEventId = 4672
```

This condition performs a search of the endpoint event log for an event ID of 4672 corresponding to a successful authorization where special privileges are assigned to the current session.

For more details on event 4672, see the relevant documentation: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4672.

```
source = 'endpoint events log' AND logEventId = 4624
```

This condition performs a search of the endpoint event log for an event ID of 4624 corresponding to a successful user login to the system.

For more details on event 4624, see the relevant documentation: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624.

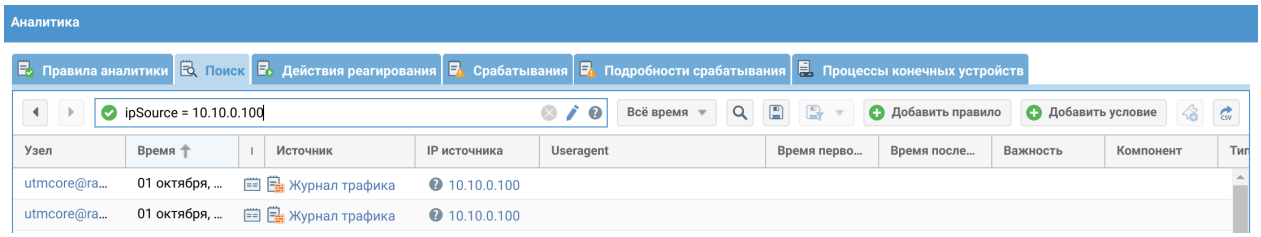
Example 2. Detect file ownership change

This example shows how to write an analytics rule using the syslog event source. The rule detects when the file owner changes to root using the chown utility. The condition is specified with the following line:

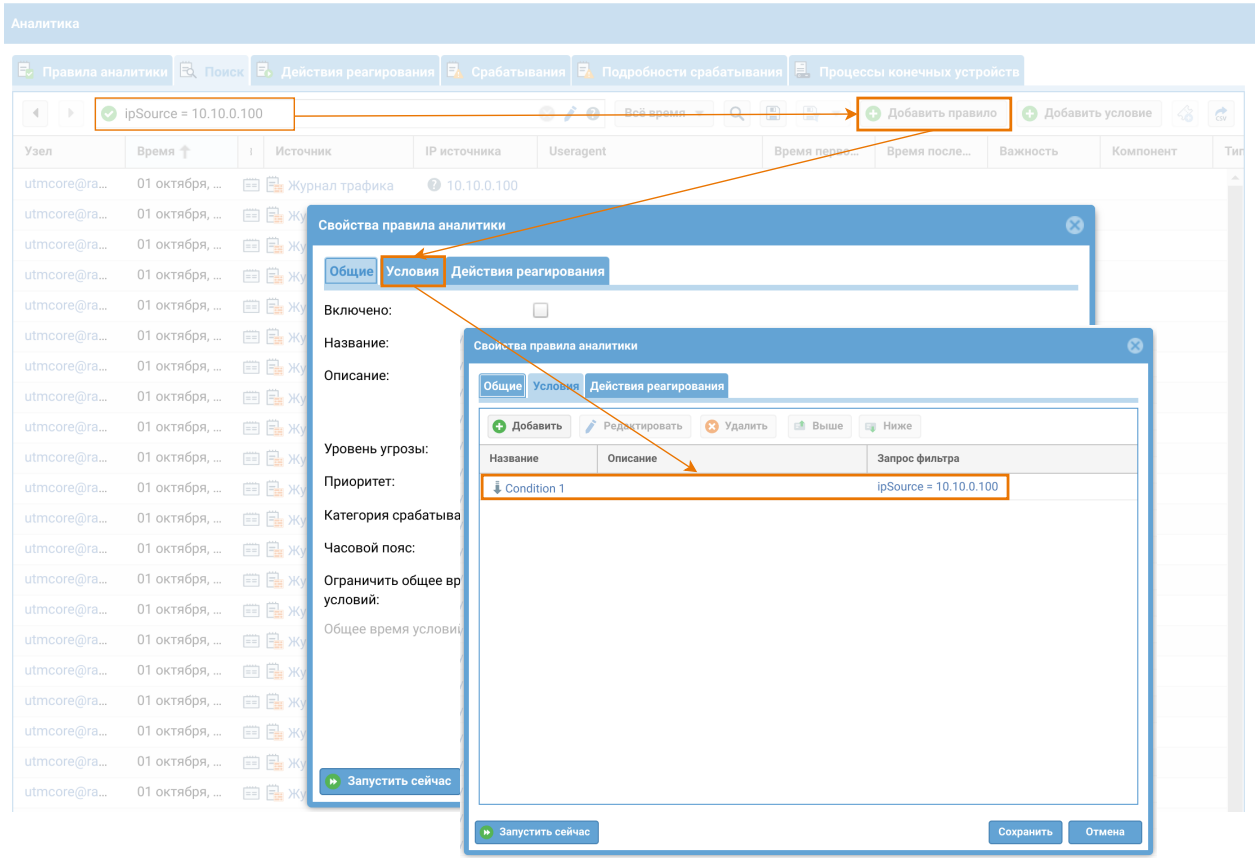
```
source = 'syslog' AND data ~ 'COMMAND=/bin/chown root' AND
applicationName = 'sudo'
```

Analytics Search

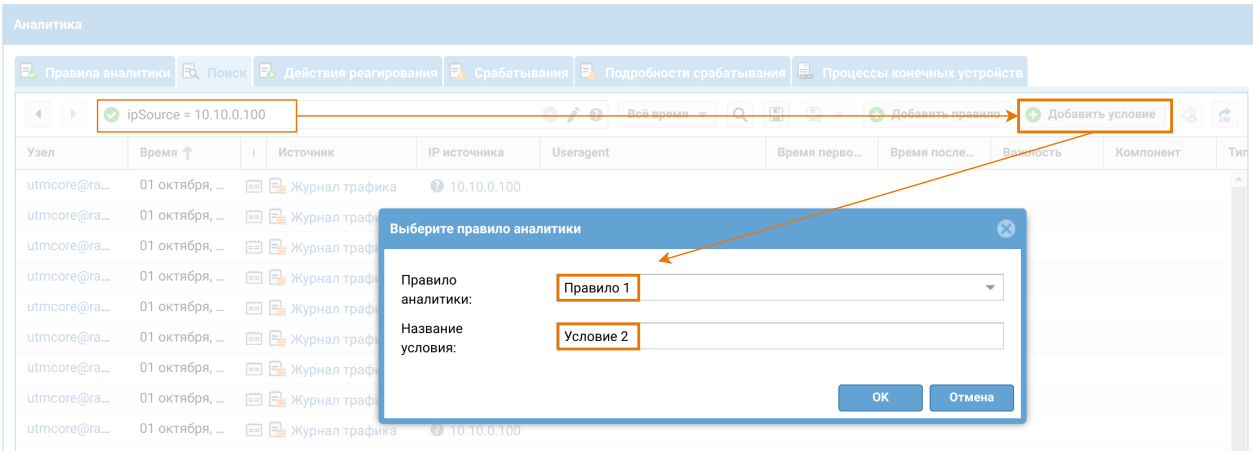
The **Analytics search** tab displays a list of all log events from the connected sensors and UserGate SIEM log events. To search for events of interest, use the search field to create an SQL-like search query. To formulate a query, use field names, field values, keywords, and operators. For the query syntax, refer to the section Data Search and Filtering. The query can also be written using the Google/RE2 syntax in a MATCH operator.



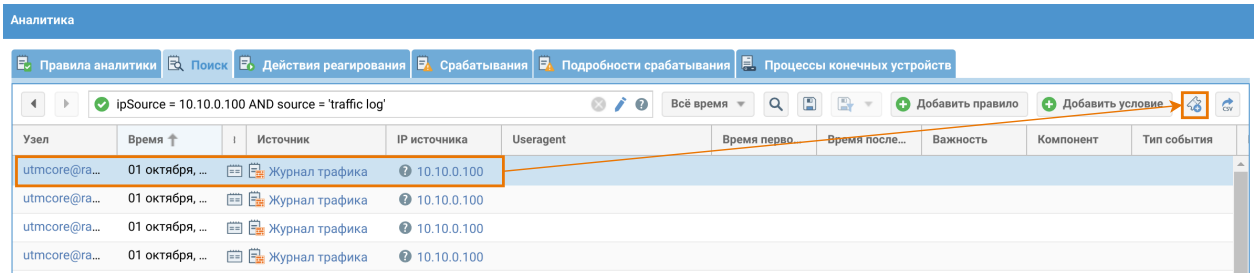
By clicking **Add rule**, you can add a new analytics rule that will use the search query you have entered as the filter query. For more details on analytics rules, see the Analytics section.



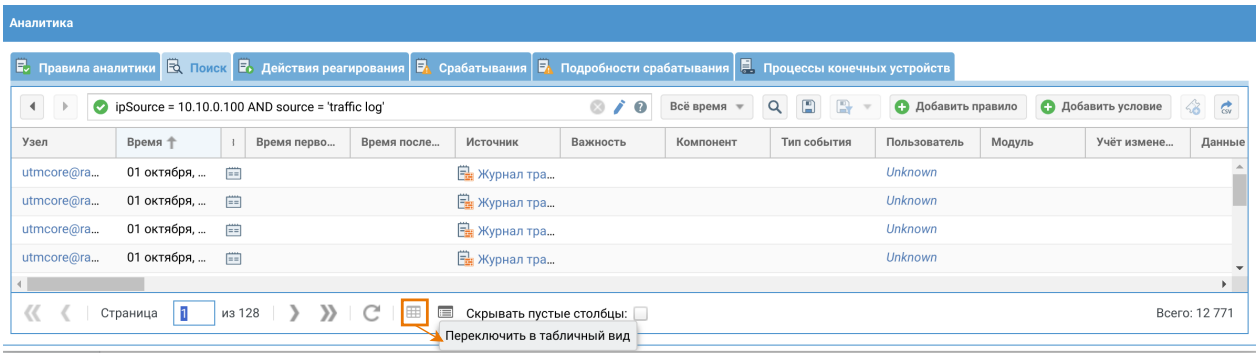
In addition, by clicking **Add condition**, you can create a condition from the entered search query and add it to the analytics rule created earlier. When adding a condition, specify the analytics rule and a name for the condition:

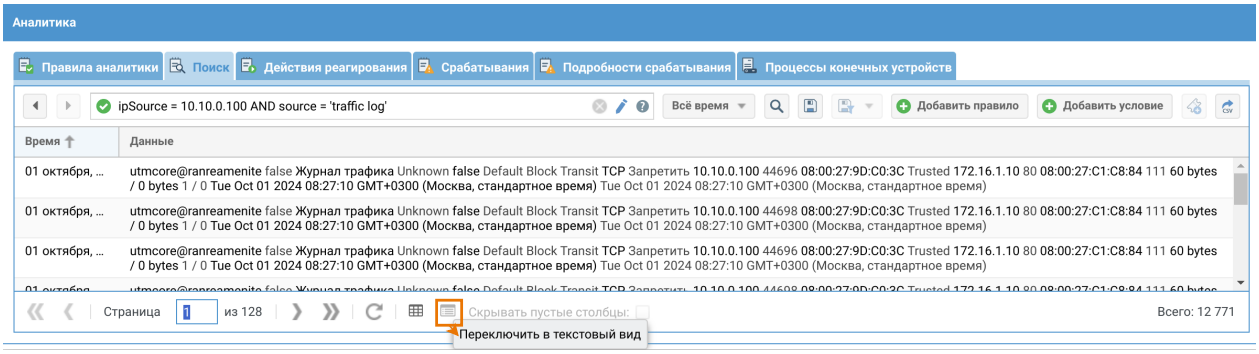


The selected event can be added to an incident by clicking **Add to incident**. For more details about incidents, see the chapter Incident Settings



Two event data views can be used: table and plain text. To switch to the desired view, on the bottom panel of the interface click **Switch to plain text view** or **Switch to table view**:





The **Analytics search** tab displays the following event information.

Name in database	Name in search query	Description
Node	node	The node name of the NGFW or SIEM device.
Time	date	The time when the event occurred or the analytics rule was triggered. Displayed in the timezone set in UserGate SIEM.
First event time	triggeredAlertFirstEventDate	For the triggered alert log: the time of the first event included in the triggered alert for the analytics rule.
Last event time	triggeredAlertLastEventDate	For the triggered alert log: the time of the last event included in the triggered alert for the analytics rule.
Source	source	The log where the event was recorded: SIEM, NGFW, endpoint, or triggered alert logs.
Severity	severity	The event category for NGFW and SIEM event logs: • **Info**: events that normally do not require administrator attention • **Warning**: events that indicate possible problems • **Error**: events that indicate errors • **Critical**: events that indicate critical errors that can affect functionality.
Component	component	The component where the event occurred (e.g., updates, settings, console authorization, analytics, etc.). Applicable to NGFW and SIEM event log records.

Name in database	Name in search query	Description
Event type	event	The event type from an NGFW or SIEM event log (e.g., check, download, update installation, successful/failed authorization, parameter search, etc.).
User	user	The name of the user whose account was used to log in to the NGFW, SIEM, or endpoint device. Applicable to NGFW, SIEM, and endpoint event log records as well as web access, traffic, IDPS, and triggered alert log records.
Module	module	he module where the event occurred (e.g., Web console, Core, VPN server, etc.). Applicable to NGFW and SIEM event log records.
Change tracker	changeTracker	The type of the change (SIEM or NGFW event log). The possible change types can be specified by the user.
Data	data	Detailed information about the event. Applicable to endpoint event log and Syslog records.
Information	details	Detailed information about the event from SIEM and NGFW event logs.
Rule	rule	The name of the analytics, firewall, content filtering, SCADA, or IDPS rule.
Action	action	The action configured in the firewall, content filtering, SCADA, or IDPS rules: • **Allow** (allow/pass/ allow_webaccess): for firewall, IDPS, or content filtering rules

Name in database	Name in search query	Description
		• **Safe browsing** ('safe browsing') • **Captive portal** ('captive portal') • **Warning** (warning): for content filtering rules • **Alert** (alert): applicable to DoS protection in a zone • **NAT** (nat) • **DNAT** (dnat) • **Port forwarding** ('port forwarding') • **Policy-based routing** ('policy based routing') • **Network mapping** ('network mapping') • **Deny** (deny/drop/deny_webaccess): for firewall, IDPS, or content filtering rules • **Decrypt** (decrypt): for inspection rules • **Log** (log): for IDPS rules • **Pass** (pass): for SCADA rules • **Drop** (drop): for SCADA rules.
Application	application	Application name. Applicable to traffic, IDPS, Syslog, and endpoint rule and application log records.
Application threat	applicationThreat	Application threat level. Applicable to web access, traffic and IDPS log records.
Network protocol	networkProtocol	The transport connection protocol used to access the resource. Applicable to traffic, IDPS, and endpoint rule log records.
Application layer protocol	httpProtocol	

Name in database	Name in search query	Description
		The HTTP protocol version. Applicable to web access log records.
URL categories	urlCategory	Categories to which the website belongs. Applicable to web access and endpoint rule log records.
URL category threat	urlCategoryThreat	Threat level for the URL category. Applicable to web access log records.
Reasons		The reasons (e.g., for blocking) from the web access log.
HTTP method	httpMethod	The HTTP method (the main operation on the resource). • **OPTIONS**: used to determine the web server capabilities or connection parameters for a specific resource • **GET**: used to request the content of the specified resource • **HEAD**: similar to GET, except that the body is omitted from the server response • **POST**: used to send user data to the specified resource • **PUT**: used to upload the request content to the URI specified in the request • **PATCH**: similar to PUT but applied only to a part of the resource • **DELETE**: deletes the specified resource • **TRACE**: returns the received request so that the client can see what information is added or modified in

Name in database	Name in search query	Description
		the request by intermediate servers • **CONNECT**: transforms the request connection into a transparent TCP/IP tunnel. Applicable to web access log records.
HTTP status code	statusCode	The status code from the first line of the HTTP server response. Applicable to web access log records.
Content type	mime	The type of the content. Applicable to web access and endpoint rule logs.
URL	url	The URL of the resource that was accessed. Applicable to web access log records.
Referer	referer	The URL of the previous page (if any). Applicable to web access log records.
Operating system	operatingSystem	The operating system type on the user device. Applicable to web access and IDPS log records.
Useragent	userAgent	Browser useragent. Applicable to web access log records.
Signatures	signature	The name of the triggered IPS signature. Applicable to IDPS log records.
Signature threat	signatureThreat	Signature threat level. Applicable to IDPS log records.
Source zone	zoneSource	The source zone. Applicable to web access, traffic, SCADA, and IDPS log records.
Source IP	ipSource	The source IP address for the traffic. Applicable to web

Name in database	Name in search query	Description
		access, traffic, SCADA, IDPS, and endpoint rule log records.
Source port	portSource	The source port number used for connection. Applicable to web access, traffic, IDPS, and endpoint rule log records.
Source MAC address	macSource	Source MAC address. Applicable to traffic and IDPS log records.
Destination zone	zoneDest	The destination zone. Applicable to web access, traffic, IDPS, and endpoint rule log records.
IP dest	ipDest	The destination IP address for the traffic. Applicable to web access, traffic, SCADA, IDPS, and endpoint rule log records.
Destination port.	portDest	The destination port number used by the transport protocol. Applicable to web access, traffic, SCADA, IDPS, and endpoint rule log records.
Destination MAC address	macDest	Destination MAC address. Applicable to traffic and IDPS log records.
NAT source IP	natIpSource	The NAT source IP address (if NAT rules are configured). Applicable to traffic log records.
NAT source port	natPortSource	The NAT source port (if NAT rules are configured). Applicable to traffic log records.
NAT destination IP	natIpDest	The NAT destination IP address (if NAT rules are configured). Applicable to traffic log records.
NAT destination port	natPortDest	The NAT destination port (if NAT rules are configured).

Name in database	Name in search query	Description
		Applicable to traffic log records.
Bytes sent/received	bytesSent/bytesRecv	The amount of data sent and received. Applicable to traffic and web access log records.
Packets sent/received	packetSent/packetRecv	The number of packets sent and received. Applicable to traffic and web access log records.
Endpoint/sensor	sensor	The name of the endpoint device/sensor. Applicable to endpoint event log records.
Counter	counter	The name of the counter added to the WMI and SNMP sensor. Applicable to endpoint event log records.
SNMP object	snmpObject	The SNMP object ID (SNMP OID). Applicable to endpoint event log records.
SNMP object type	snmpObjectType	The SNMP object type. Applicable to endpoint event log records.
Status	status	The result of the WMI or SNMP query (OK or Error). Applicable to endpoint event log records.
Error	error	The WMI or SNMP error that occurred as a result of the query. Applicable to endpoint event log records.
SCADA protocol	scadaProtocol	The SCADA (Supervisory Control And Data Acquisition) protocol. • **IEC 104** • **Modbus**. • **DNP3** (Distributed Network Protocol). • **MMS** (Manufacturing Message Specification).

Name in database	Name in search query	Description
		• **OPC UA** (Open Platform Communications Unified Architecture). Applicable to SCADA log records.
Log level	logLevel	The type of the event: • **Audit Success**: a security log event that occurs on successful access to the audited resources • **Audit Failure**: a security log event that occurs on failed access to the audited resources • **Error**: points to significant problems that can cause loss of functionality or data • **Information**: an informational event that usually does not require administrator attention • **Warning**: points to problems that do not need urgent fixing but can cause errors in the future. Applicable to endpoint event log records.
Log event source	logEventSource	The name of the software that logged the event. Applicable to endpoint event log records.
Log category	logCategory	The log category that is needed 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.
Task category	taskCategory	

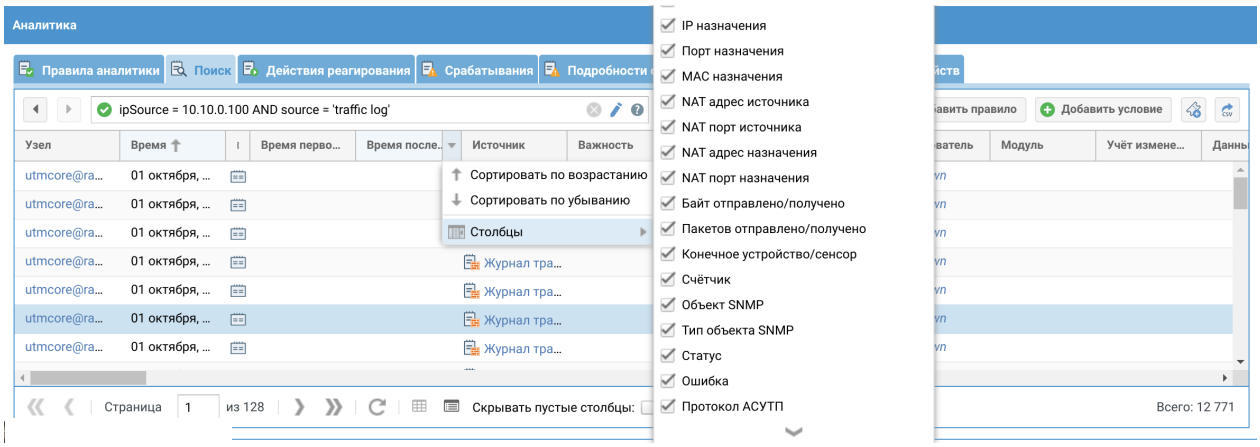
Name in database	Name in search query	Description
		The category of the task. Applicable to endpoint event log records.
Computer name	computerName	The full name of the endpoint device. Applicable to endpoint event log and Syslog records.
Log event code	logEventCode	The log event code corresponding to a specific event. Applicable to endpoint event log records.
Log event ID	logEventId	The log event ID that determines the primary ID of the event. Applicable to endpoint event log records.
Log event type	logEventType	The type of the log event. This is a numeric parameter that represents the log level: • 1: error log level • 2: warning log level • 3: information log level • 4: audit success log level • 5: audit failure log level Applicable to endpoint event log records.
Insertion string	insertionString	Contains the EventData block of the Windows event. Applicable to endpoint event log records.
Log file	logFile	Shows information from the endpoint event log, i.e. important software and hardware events. The following log file types exist: • **Application** (application log file): for application and service events.

Name in database	Name in search query	Description
		• **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. Applicable to endpoint event log records.
Command	scadaCommand	The SCADA control command (e.g., read or write). Applicable to SCADA log records.
Registry address	scadaAddress	The address of the register on which the operation (read or write) should be performed. Applicable to SCADA log records.
ASDU number	scadaAsdu	The ASDU address (COA, or Common Object Address). Refers to the IEC-104 protocol. Applicable to SCADA log records.
Device ID	scadaDevice	The unique device number from the OPC server database. Used with the OPC UA protocol. Applicable to SCADA log records.
Variable name	scadaVarname	The name of the variable. Parameter is mainly used for real-time data exchange. Refers to the MMS protocol. Applicable to SCADA log records.

Name in database	Name in search query	Description
Hash	hash	The application's hash. This is a parameter in the endpoint application log.
Object	facility	The event type. Applicable to Syslog records. Available values: • Kernel messages • User-level messages • Mail system • System daemon • Security/authorization • Syslog messages • Line printer subsystem • Network news subsystem • UUCP subsystem • Clock daemon • Security/authentication • FTP Daemon • NTP subsystem • Log audit • Log alert • Clock daemon 2 • Local 0-Local7.
Severity	syslogSeverity	The event severity for Syslog. • **Emergency**: a critical state that affects system health • **Alert**: a state that requires immediate intervention. • **Critical**: a state that requires immediate intervention or signals a fault in the system. • **Error**: non-critical system faults • **Warnings**: warnings on potential errors that can

Name in database	Name in search query	Description
		occur if no action is taken. • **Notice**: events that relate to unusual system behavior but are not errors. • **Info**: informational alerts • **Debug**: information useful to developers for debugging applications
Process ID	processId	The process identifier. Applicable to Syslog records.

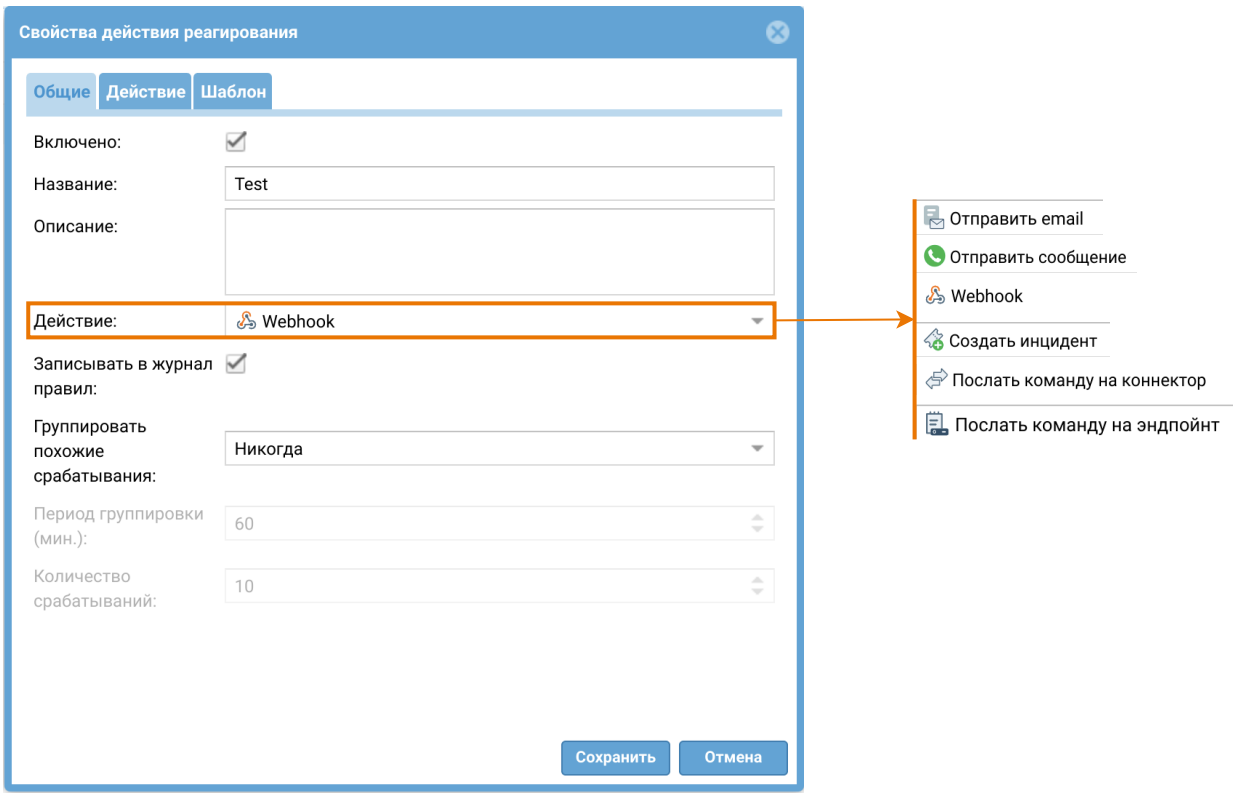
The administrator can select to display only the columns they need. To do that, point the mouse cursor at the name of any column, click the arrow that will appear to the right of the column name, choose **Columns**, and select the desired parameters in the context menu:



Response Actions

Response actions determine how to respond when cybersecurity analytics rules are triggered. You can use the UserGate SIEM to flexibly customize rules with variables of analytics rule triggering categories.

Actions can be created in the **Analytics → Response actions** tab. When adding an action, provide the following settings:



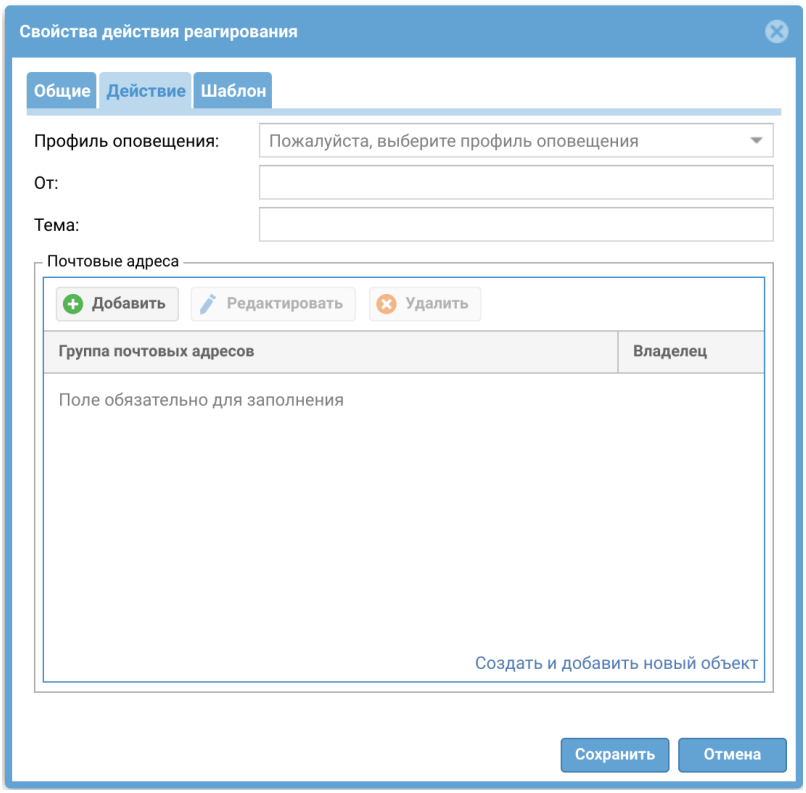
Name	Description
Enabled	Enables or disables the response action.
Name	The name of the response action.
Description	A description of the response action. This field is optional.
Action	The action that should be taken when the analytics rule is triggered. Will be applied if specified in the analytics rule properties. The following response actions are available: • **Send email**: send an email to the selected addresses. The procedure of configuring the **Send email** action will be discussed later in the Send Email Action section. • **Send message**: send a message to the specified phone numbers. The procedure of configuring the **Send message** action will be discussed later in the Send Message Action section. • **Webhook**: receive an alert on the rule trigger on the webpage whose address is specified in the action settings. The procedure of configuring the **Webhook** action will be discussed later in the Webhook Action section. • **Create incident**: automatically create an incident when the analytics rule is triggered. The procedure of configuring the **Create**

Name	Description
	incident action is described in the Incident Settings section. • **Send Command To Connector**: send a command to the selected connector. The procedure of configuring the Send Command To Connector action is described in the <0>Send Command To Connector Action section. • **Send Command To Endpoint** send a command to an endpoint with UserGate Client software installed. For more details, see Send Command To Endpoint Action.
Enable logging	Enables or disables the logging of response action triggers. The data is recorded in the SIEM event log that can be viewed in the **Logs and reports → Logs → Event log** tab.
Group similar triggered alerts	When configuring response actions, you can enable the grouping of triggered alerts for convenience. The following grouping options are available: • **Never**. • **For period of time**: the response action will be performed if at least one triggered alert occurs during the specified period of time. • **By number of triggered alerts**: the response action will be performed only after the specified number of triggered alerts.
Grouping time period (min.)	The grouping time period in minutes. This setting is available only when grouping for a period of time is selected.
Number of triggered events	The number of triggered alerts required for the grouping to happen. This setting is available only when grouping by the number of triggered alerts is selected.

The created response actions can be edited, deleted, copied, enabled, and disabled. You can also configure the response action list to display all actions, only enabled actions, or only disabled actions.

Send Email Action

If you selected Send email as the response action, provide the following settings in the rule properties:



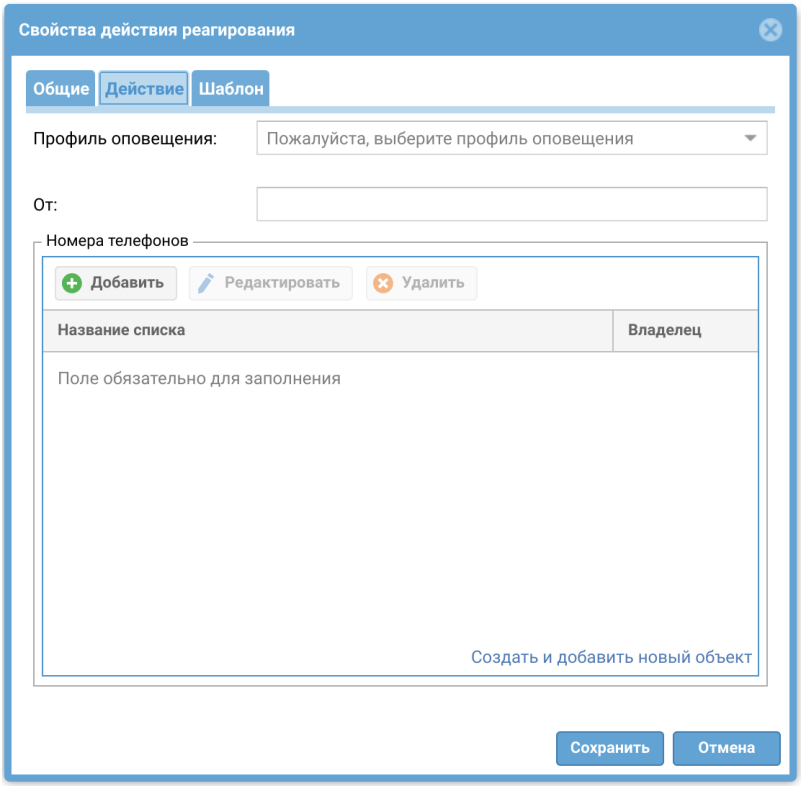
Name	Description
Notification profile	The SMTP notification profile to be used for sending emails. For more details on configuring SMTP profiles, see the Notification Profiles chapter.
From	The sender name.
Subject	The email subject.
Emails	The list of recipient email addresses. The recipients must be added to the lists under **Settings → Libraries → Emails**. For more details on adding emails, see the section Emails.

The alert email template that can include the values of various variables related to the triggered alert is created on the **Template** tab.

For more details, see the Alert Template and Notification and command variables sections.

Send Message Action

If you selected Send Message as the response action, provide the following settings in the rule properties:



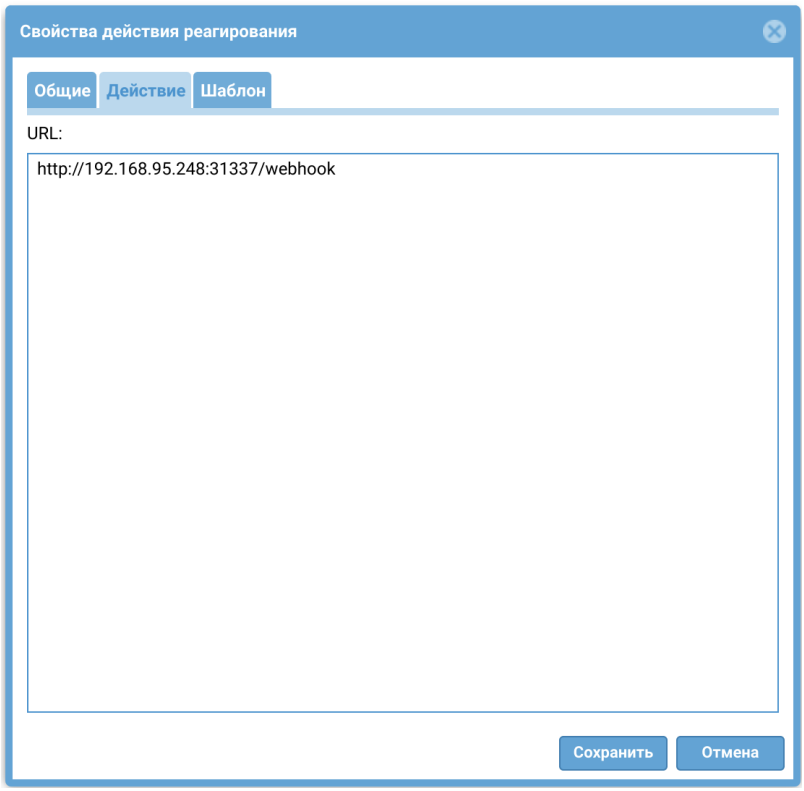
Name	Description
Notification profile	The SMPP notification profile to be used for sending messages. For more details on configuring SMPP profiles, see the Notification Profiles chapter.
From	The sender name.
Phones	The list of recipient phone numbers. The recipients must be added to the lists under **Settings → Libraries → Phones**. For more details on adding phone numbers, see the section Phones.

The message template that can include the values of various variables related to the triggered alert is created on the **Template** tab.

For more details, see the Alert Template and Notification and command variables sections.

Webhook Action

To configure a webhook in the response action rule properties, provide the following settings:



Name	Description
URL	The URL of the website where notifications about rule triggers will be displayed.

The notification template that can include the values of various variables related to the triggered alert is created on the **Template** tab.

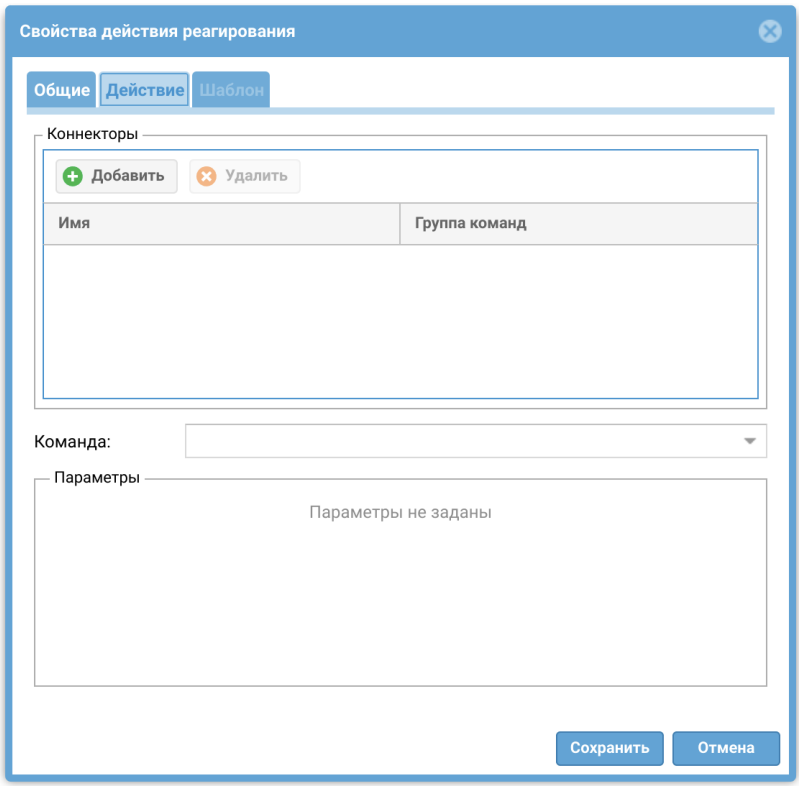
For more details, see the Alert Template and Notification and Command Variables sections.

You can test the webhook feature using this service: https://webhook.site. To do that, go to the Webhook.site website, copy the generated link, and paste it into the **URL** field on the **Actions** tab of the response action rule properties.

An example of SIEM and Telegram integration to send notifications by means of webhook is shown in the Sending SIEM Notifications in Telegram section.

Send Command To Connector action

You can configure a response action of sending a command to a connector:

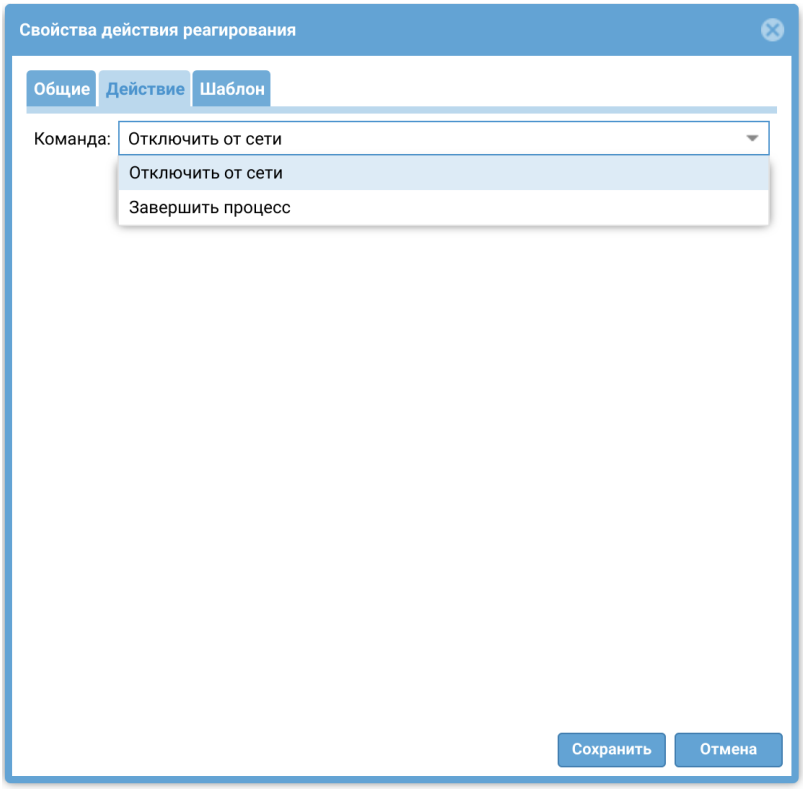


The following parameters must be specified for a response action of sending a command to be executed on a connector:

Name	Description
Connectors	Select the devices to which the command should be sent when an analytics rule is triggered. The connector must be added and configured in advance under **Sensors → Connectors** in the **Settings** tab in the UserGate SIEM web management interface (see Connectors for more information). **Important!** Only connectors with the same command group can be selected.
Command	Specify the command that will be sent to the connector for execution; the commands of the group specified for the selected connectors are available. If there are variables in the command, additional fields will be displayed where values should be specified. See Commands for more details on the commands.

Send Command To Endpoint action

You can configure a response action of sending a command to a device with the UserGate Client software installed.

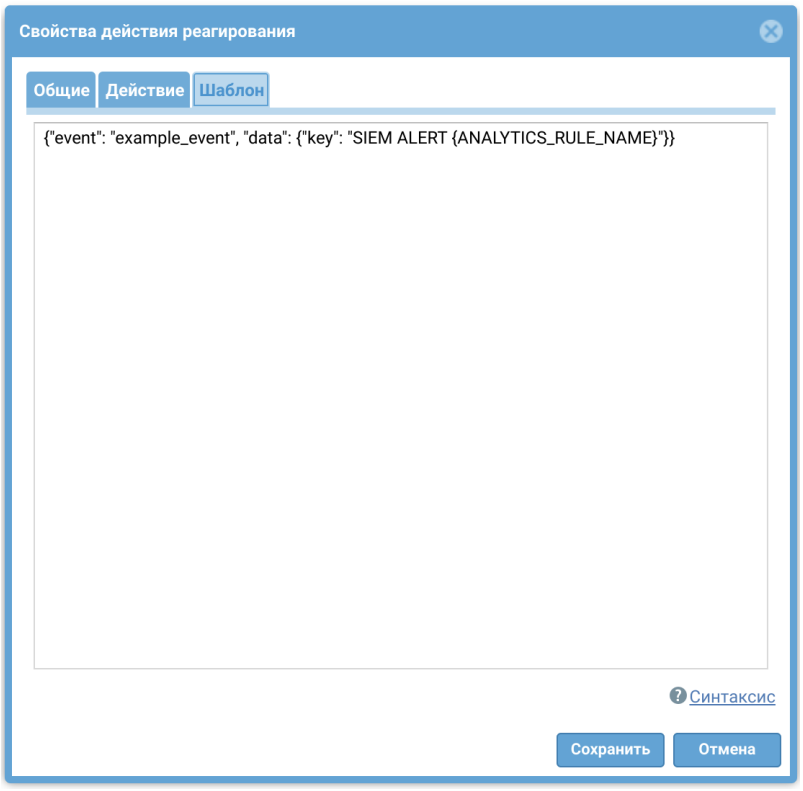


Available commands:

- **Block networking** – disable access to the Internet.
- **Kill process** – terminate the process specified in the filter query.

Alert Template

In the **Template** tab, enter the alert text. In addition to fixed test, you can send data related to the triggered alert or its log records.



To send data related to the triggered alert, enter the corresponding parameter name from the table into the text field in the **Template** tab. For example, if you enter **{ANALYTICS_RULE_NAME}**, the email, SMS, or webhook alert text will show the name of the triggered analytics rule. If you fill in the template at the time of configuring the **Create incident** action, the text will be displayed in the incident description.

Notification and command variables

Note The field is case-sensitive. Variable names must be entered in UPPERCASE in curly brackets (as shown in the table).

Note You can use variables in commands and notifications if they have been selected under *Analytics ➜ Analytics Rules ➜ Event Grouping Conditions.*

Name	Description
{ANALYTICS_RULE_NAME}	The name of the analytics rule.
{ANALYTICS_RULE_DESCRIPTION}	A description of the analytics rule.
{NAME}	The name of a specific triggered alert.
{TIME}	The time when the analytics rule was triggered.

Name	Description
{TRIGGERED_ALERTS_NUMBER}	The number of triggered alerts.
{FIRST_TRIGGERED_ALERT_TIME}	The time when the first triggered alert occurred.
{LAST_TRIGGERED_ALERT_TIME}	The time when the last triggered alert occurred.
{TRIGGERED_ALERTS_NAMES}	The list of triggered alert names if grouping is used.
{FIRST_EVENT_TIME}	The time of the first event included in the triggered alert for the analytics rule.
{LAST_EVENT_TIME}	The time of the last event included in the triggered alert for the analytics rule.
{THREAT_LEVEL}	The specified threat level.
{CATEGORY}	The category to which the triggered alert belongs.
{PRIORITY}	The priority of the triggered analytics rule alert.
{ADMINISTRATOR_NAME}	The name of the administrator who created the analytics rule.
{USER_NAME}	The username.
{SOURCE_ZONE}	Source zone
{DESTINATION_ZONE}	Destination zone
{SOURCE_COUNTRY}	The source country.
{DESTINATION_COUNTRY}	The destination country.
{SOURCE_IP}	Source IP address
{SOURCE_PORT}	Source port
{DESTINATION_IP}	Destination IP address
{DESTINATION_PORT}	Destination port
{SOURCE_ZONE_ALL}	The source zones of all events that caused the triggered alert.

Name	Description
{DESTINATION_ZONE_ALL}	The destination zones of all events that caused the triggered alert.
{SOURCE_COUNTRY_ALL}	The source countries of all events that caused the triggered alert.
{DESTINATION_COUNTRY_ALL}	The destination countries of all events that caused the triggered alert.
{SOURCE_IP_ALL}	The source IP addresses of all events that caused the triggered alert.
{SOURCE_PORT_ALL}	The source port numbers of all events that caused the triggered alert.
{DESTINATION_IP_ALL}	The destination IP addresses of all events that caused the triggered alert.
{DESTINATION_PORT_ALL}	The destination port numbers of all events that caused the triggered alert.

Triggered Alerts

The **Triggered alerts** tab shows the list of triggered alerts for analytics rules with brief details about each one. A triggered alert is a set of events grouped under an analytics rule.

The following triggered alert details are shown.

Name	Description
Node	A unique code corresponding to the device.
Time	The date and time when the analytics rule was triggered.
ID	The triggered alert ID.
First event time	The time of the first event included in the triggered alert for the analytics rule.
Last event time	The time of the last event included in the triggered alert for the analytics rule.

Name	Description
Events number	The number of events included in the triggered alert for the analytics rule.
Rule	The name of the triggered analytics rule.
Category	The category to which the triggered alert belongs. The following predefined categories are available: • **Security**: incidents that degrade the security of information systems. • **Availability**: incidents that degrade the availability of information systems. • **Performance**: incidents that degrade the performance of information systems. Additional triggered analytics rule categories can be created in the **Libraries → Triggered alert categories** section of the **General settings** tab.
Priority	The priority of the triggered alert specified in the analytics rule settings: • **Low**: low response priority • **Normal**: needs attention and may need response • **Important**: needs attention and response • **Critical**: requires urgent response. The priority indicates the severity of the triggered alert.
User	The username.
Signatures	The name of the triggered IPS signature.
Source zone	The zone from which connection is established.
Source IP	The source IP address.
Source port	The source port.
Destination zone	The destination zone.
IP dest	The destination IP address.
Destination port.	The destination port.

The administrator can select to display only the columns they need. 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.

Two search modes are available, basic and advanced. The basic mode uses a GUI, while the advanced mode allows you to create more complex search filters using a specialized query language whose syntax is described in the Data Search and Filtering section.

To save the configured filter, click **Save as**. To view the list of saved search filters, click **Favorite filters**.

To view the triggered alert details (brief information about the selected triggered alert), click **Show**.

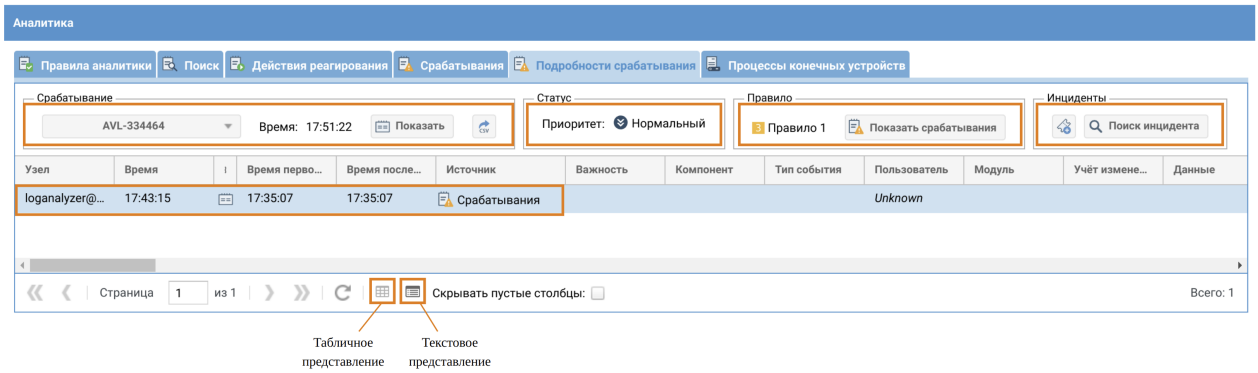
Clicking the **Show details** button will take you to the <0>Triggered alert details tab showing details about the selected triggered alert. The **Triggered Alert Details** tab is discussed in the Triggered Alert Details section.

The selected triggered analytics rule alert can be added to an incident by clicking **Add to incident**.

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

Triggered Alert Details

The Triggered alert details tab shows detailed information on the triggered analytics rule alert and all events that caused it.



The data can be viewed as a table or as plain text. To switch between these views, click **Switch to plain text view** or **Switch to table view** at the bottom of the screen.

The following details about the triggered alert are displayed.

Name	Description
Triggered alert	The triggered alert ID.
Time	The time when the analytics rule was triggered. Displayed in the timezone set in UserGate SIEM.
Priority	The priority of the triggered alert configured in the settings: • **Low**: low response priority • **Normal**: needs attention and may need response • **Important**: needs attention and response • **Critical**: requires urgent response.
Rule	The name of the triggered analytics rule.
Find incident	Click this button to find incidents where this triggered alert is used.
Event list	The list of events that caused the triggered alert.

Clicking the **Show triggered alerts** button will take you to the **Triggered alerts** tab showing the list of triggered alerts for the selected analytics rule.

Endpoint processes

The **Endpoint processes** tab displays a list of processes of devices with UserGate Client software installed. Use it to trace the chain of process calls, understand

startup parameters and view useful information about the file. The tab has two panels: **Process Log** and **Process**.

The **Process Log** panel displays the list of endpoint processes (running application processes, background processes, Windows processes) that pass information to SIEM. The following information can be viewed:

- Run date and time.
- The name of the endpoint device.
- Application
- Process ID.

Records can be conveniently filtered by various criteria, such as date range, app name, process ID, etc. You can also use advanced search to set up complex filters; the advanced search mode uses a special query language the syntax of which is covered later in the Data Search and Filtering section.

Administrators can select to display only the columns they need. 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.

Select a process to view the process tree and the process details. The process tree and details will be displayed in the **Process** panel.

Using Library Lists in Search Queries

In SIEM, you can use lists from libraries in search queries wherever they exist — in analytics rules, search requests, logs, dashboards, and custom reports.

Data is added to lists either manually (for local lists) or via an external update URL specified in the settings (for updatable lists). If lists are used in the trigger filters of analytics rules, new search elements will be added to the rules dynamically as they are added to the lists.

This feature is supported for the following list types:

List type	Query field
IP Addresses	ipSource, ipDest, natIpSource, natIpDest

List type	Query field
URL Lists	url
Content types	mime
Browser Useragent	userAgent
URL Categories	urlCategory
Text Lists	user, rule, zoneSource, zoneDest, macSource, macDest, applicationName, httpProtocol, httpMethod, referer, sensor, computerName, logFile, data, hash, cmdLine, device, service, image, originalFilename, parentImage, parentCommandLine, targetObject, targetFilename, scriptBlockText, queryName, queryResult, workstationName, logonId, imageLoaded, sourceImage, targetImage, customString1.. customString15

To use a list in queries, you need to:

1. Create a list with the **Use in search queries** option enabled.

2. Add list items to it.

3. Add the list to the search query.

You can find more details on supported types of lists in the Libraries section. When the **Use in search queries** option is enabled in a list's properties, an internal database dictionary containing the list's contents and a list change event handler are created.

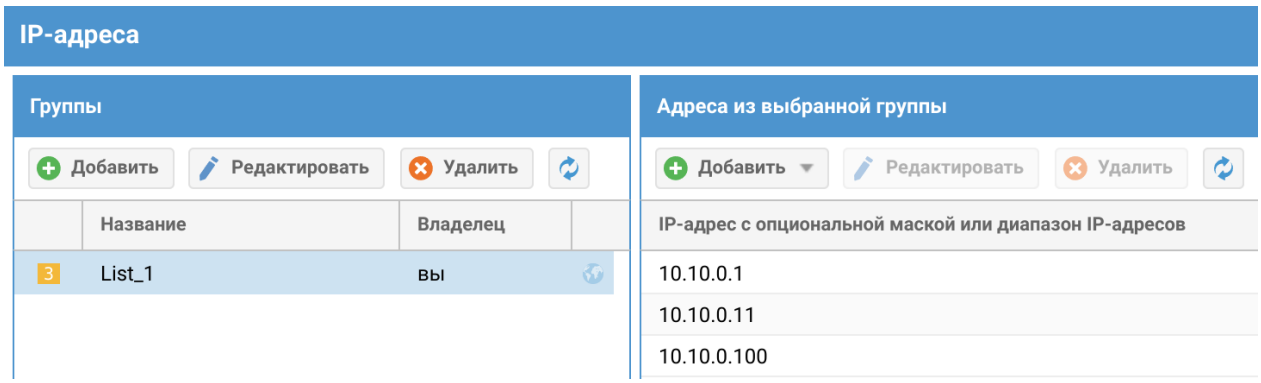
In search queries, lists can be used with the **IN** and **NOT IN** operators. Syntax: <field name> **IN** <list name>. When receiving queries, the values from the query are compared with the values from the dictionary.

For IP lists, a query like: *ipSource IN list_1* checks whether ipSource is in any of the IP address ranges from list_1.

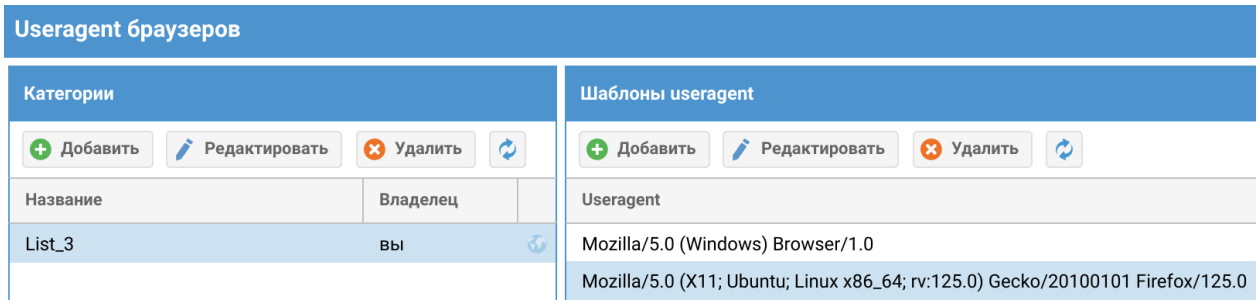
For browser useragents, content types, URL lists, URL categories, and text lists, the queries *userAgent IN list_1, mime IN list_2, url IN list_3, urlCategory IN games, signatureName IN list1* check whether the field value is equal to any value in the list.

Example

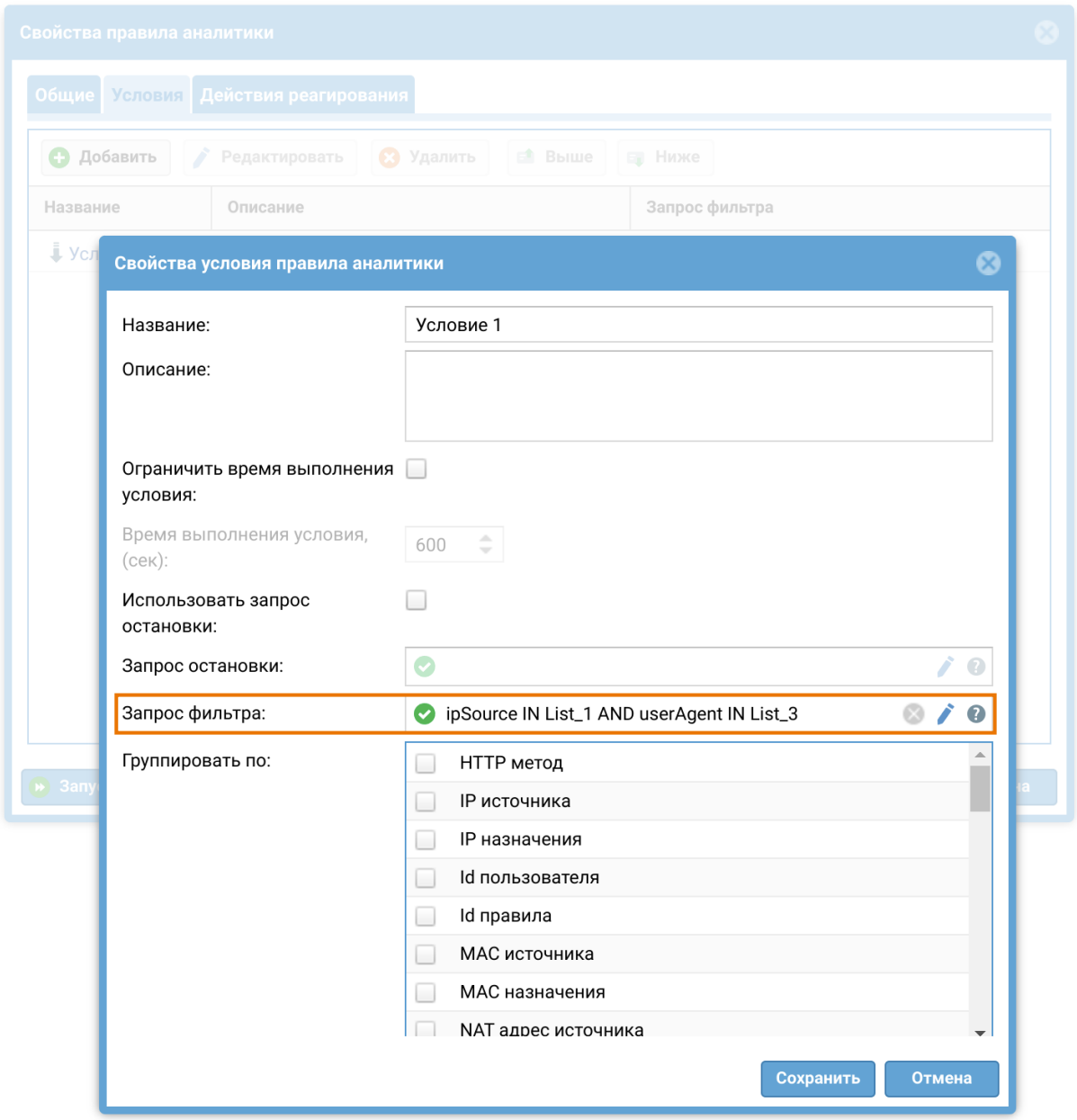
1. Create a list of IP addresses with the following contents:



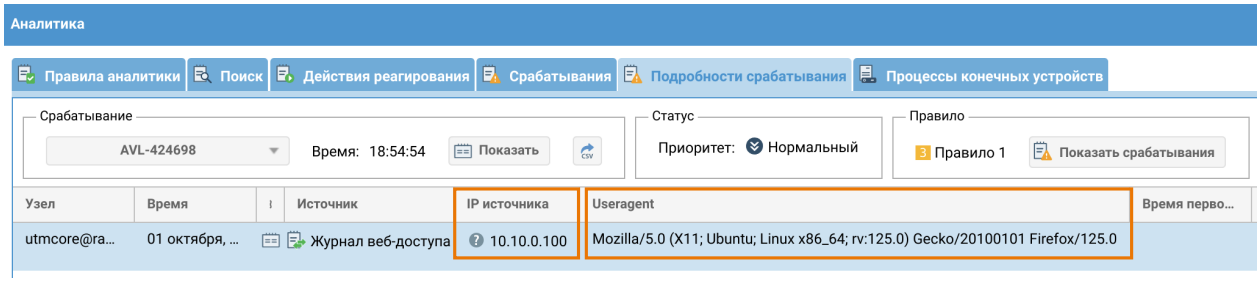
2. Create a list of browser useragent values with the following contents:



3. Add the created lists to the analytics rule condition filter:



As a result of the rule execution, a trigger will occur based on the selected filters with lists in the rule trigger condition:



INCIDENTS

General Information

The **Incidents** section provides access to the functionality of UserGate SIEM's built-in IRP (Incident Response Platform) system. An incident is a cybersecurity event or a set of cybersecurity events needing investigation. UserGate SIEM allows you to customize the incident investigation process to the needs of a specific company. (For more details, see the section Incident Settings.)

The IRP system is tightly integrated with the SIEM system whose functionality is available in the Analytics section. In the **Analytics** section, you can set incident creation as a response action, thereby automating the process of cybersecurity incident creation (for more details about configuring response actions, see the Response Actions section).

Besides the automatic mode of creation, incidents can also be created manually by a cybersecurity engineer (for more details, see the section Creating Security Incidents).

Incident Settings

Incident investigation is a multi-stage process where the incident is assigned a certain **State** at each stage, e.g., **Open → Need more info → In progress → Closed**. Transition between states is possible based on certain rules set by the administrator — e.g., a direct transition from **Open** to **Closed** is not allowed. The possible incident state transitions are defined in an **Incident schema**.

When the investigation of an incident is completed, a **Resolution** is assigned to the incident, such as "False positive", "True positive", "Completed", etc.

The **Incident type** is selected at the time of incident creation and determines the purpose of the incident. Examples of incident types are "Security incident", "Task", etc.

The **Incident schema** brings together the incident states, possible state transitions, resolutions, and incident types to form an integrated process of cybersecurity incident investigation.

UserGate SIEM allows you to customize the incident investigation process to the needs of a specific company. After the initial configuration of the resolution, an incident schema with the default name of **Incident** is created. The system administrator can edit the existing schema or create a new one. Multiple incident schemas can be created but only one, the active schema, can be used.

To create a new incident schema, follow these steps:

Name	Description
Step 1. Create the desired incident resolutions	Under **Incident settings → Incident resolutions**, click **Add**, provide a name and description for the resolution being created and click <0>Save.
Step 2. Create incident types	Under **Incident settings → Incident types**, click **Add**, provide a name and description for the incident type being created and click <0>Save.
Step 3. Create incident states	Under **Incident settings → Incident states**, click Add and provide the name, description, and group for the incident state being created. A state group determines the position of the state in the state schema. There are three types of group: • **Open**: assigned to incident states in which the work on the incident is not started yet or paused. Usually, these are initial incident states, such as "Created". All states from this group are marked blue in the web console. • **In Progress**: assigned to incident states in which the work on the incident is in progress but not completed yet. These are intermediate incident states, such as "In progress" or "Investigation". All states from this group are marked yellow in the web console. • **Closed**: assigned to incident states in which the work on the incident is completed. These are final incident states, such as "Completed" or "Closed". To transition to a state from this group, you need to provide a resolution for the incident, such as "False positive", "True positive", or "Completed". All states from this group are marked green in the web console. When you have defined all fields, click **Save**.
Step 4. Create incident schema	Under **Incident settings → Incident schema**, click Add and provide the following settings: • Set active: make this schema active. Only one schema can be active; if another schema was active before, this action will make it inactive, and all new and existing incidents will use the new schema. • Schema: the name of the schema.

Name	Description
	• Prefix: the prefix that will be used to assign IDs to incidents being created. An ID will have the format of "-", e.g., "INC-99". • Description: an optional description of the schema. • Workflow states: all states that the incident can take during its lifecycle. Add all incident states here that you created at the previous step. • Initial state: the state that an incident will take on creation. • Transitions: specify all possible state transitions here and give them names. For example, create a transition named **Activate** that will take the incident from an **Open** state to an **In Progress** state. An incident can be transitioned between states only if a transition is defined between them. • Incident resolutions: the list of the possible incident resolutions. A resolution is required when the ticket investigation is being completed, i.e. transitioned to a **Clo sed** state. Select all the required resolutions that you created earlier. • Incident types: the incident types that can be used with this schema.
Step 5. Activate the incident schema	After creating an incident schema, it needs to be activated. To do that, set the **Set active** checkbox in the incident schema settings.

Incident Dashboard

This tab displays the current states of cybersecurity incidents created in UserGate SIEM. Reports are presented as widgets, which can be customized by the system administrator. You can add, delete, move, and resize widgets on the Dashboard page.

Some widgets allow you to customize the display, specify data filtering, and configure other settings. To configure a widget, click the gearwheel icon in the upper right corner. Not all parameters listed below are available for every type of widget.

Name	Description
Name	The widget name to display in the Dashboard.
Chart	

Name	Description
	Select the desired data view: • Number • Column chart • Table
Filter query	SQL-like query string that allows you to limit the amount of information used to build a widget.
Description	A description of the widget.
Number of records	Maximum number of records to display.

Incidents Log

The **Incidents log** tab shows the list of existing cybersecurity incidents with the details shown in the following table:

Name in database	Name in search query	Description
Created	date	The date and time of incident creation.
Updated	updateDate	The date and time of the last update.
ID	incidentPrefix	The incident's prefix (INC-N, where N is the ordinal number of the incident, starting from 0).
Name	incidentName	The name of the incident.
Rule	rule	The name of the analytics rule the triggering of which caused the automatic creation of the incident as a result of the **Crea te incident** response action configured for the rule.
Status	status	The incident's state.

Name in database	Name in search query	Description
		There are three state groups that determine the position of the state in the state schema: • **Open**: assigned to incident states in which the work on the incident is not started yet or paused. Usually, these are initial incident states, such as "Created". All states from this group are marked blue in the web console. • **In Progress**: assigned to incident states in which the work on the incident is in progress but not completed yet. These are intermediate incident states, such as "In progress" or "Investigation". All states from this group are marked yellow in the web console. • **Closed**: assigned to incident states in which the work on the incident is completed. These are final incident states, such as "Completed" or "Closed". To transition to a state from this group, you need to provide a resolution for the incident, such as "False positive", "True positive", or "Completed". All states from this group are marked green in the web console. In UserGate, a schema named "Incident" is created by default that includes transitions between all possible states. Incident

Name in database	Name in search query	Description
		schemas can be added under **Settings → Incident settings → Incident schema**. Additional incident states can be defined in the **Settings → Incident settings → Incident states** tab. For more details, see the section Incident Settings.
Resolution	resolution	The resolution of the incident. The following predefined resolutions are available: • **False positive**: the incident is a false positive • **True positive**: the incident is a true positive • **Duplicate**: the problem is a duplicate of an existing one • **Won't do**: the task cannot be accomplished • **Done**: the problem is resolved. Additional incident resolutions can be defined in the **Settings → Incident settings → Incident resolutions** tab. For more details, see the section Incident Settings.
Type	type	The incident type. By default, two incident types are available: a security incident and a task. Additional incident types can be defined in the **Settings → Incident settings → Incident types** section. For more details, see the section Incident Settings.
Priority	priority	

Name in database	Name in search query	Description
		Incident priority: • Low • Normal • Important • Critical.
Reporter	reporter	The name of the administrator who created the incident.
Last change by	lastChangeBy	The name of the administrator who made the last change.
Assignee	assignee	The name of the administrator assigned to the incident.
Activity		The number of comments, triggered analytics rule alerts, and event logs added to the incident.

The administrator can select to display only the columns they need. 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.

You can filter incidents using the parameters shown in the table. Two filter modes are available, basic and advanced (for more details on the advanced search mode, see the Data Search and Filtering section).

You can save a configured filter by clicking **Save as**. To view the list of saved search filters, click **Favorite filters**.

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

Creating Security Incidents

The **Incidents log** tab can also be used to create cybersecurity incidents. To create and work with cybersecurity incidents, the user needs certain role permissions (for more details, see the User Roles and Role Permissions section).

To create an incident, click **Create incident**. and provide the following parameters:

Name	Description
Name	The name of the cybersecurity incident.
Type	The incident type. By default, two incident types are available: a security incident and a task. Additional incident types can be defined under **Settings → Incident settings → Incident types**. For more details, see the section Incident Settings.
Priority	Assign a priority to the incident: • Low • Normal • Important • Critical.
Assignee	Add an assignee to the incident.
Watchers	Provide a list of employees who will watch the incident and receive an alert on any updates to it.
Attachments	Attach files here related to the incident.
Description	Enter a description of the incident.

Incident Details

Clicking the **Show** button will take you to a new tab (with the name formed of the ID and the entered incident name) showing details about the selected incident. In this tab, you can also **Edit** and **Comment** on the incident, **Assign** a different person to the incident, and change the **Workflow** state. In addition to the incident details displayed in the **Incidents log** tab (see more in the Incidents Log section), you can view the following information.

The **Triggered alerts** section shows the triggered analytics rule alerts added to the incident. For more details, see the section Triggered Alerts. To add triggered alerts to the incident, click **Add to incident**. and select the triggered alerts to be added to the incident. To view the details for a triggered alert for analytics rule, select it and click **Show details**. You can also view triggered alert details by clicking **Show**. To remove the triggered alert for analytics rule from the incident, click **Remove from incident**.

By clicking **Export as CSV**, you can save the list of triggered analytics rule alerts added to incidents in a .csv file for subsequent analysis.

The **Logs** section displays detailed information about events from all logs (for more details on log records, see the section Analytics Search). To add events to the incident, click **Add to incident** select the events to be added. To remove unneeded events, use the **Remove from incident** button.

The **Observables** section displays the observation results for the objects specified in the settings. Observables are needed to simplify the analysis of a cybersecurity incident, make the right decision, and reduce the time spent on the incident. The relevant information is obtained with the help of enrichment services (for more on these, see the section External Enrichment Services). To view the detailed information provided by an enrichment service, open the enrichment service settings by clicking on the service.

To create an observable, click **Add**. and provide the settings shown in the table below.

Name	Description
Observable type	Select one of the following observable types: • **Autonomous system**: a system of IP networks and routers under unified management • **Domain**: the name of an Internet website. • **File**: a file to collect information about. • **File name**: the name of a file to collect information about. • **FQDN**: a fully qualified domain name. • **Hash**: a hash of some file, e.g. a file added to the incident • **Host name**: the label of a device connected to a computer network and used for device identification. • **IP**: a unique address identifying the device in a computer network. • **Mail**: an email address. • **Mail subject**: the contents of the email's subject field. • **Registry**: a Microsoft Windows registry key is a directory where the settings and parameters of the operating system are stored. • **URI path**: a character sequence identifying an abstract or physical resource. • **URL**: the individual Internet address of the resource. • **Useragent**: an alphanumeric string identifying the software that sends a request to the server and at the same time requests access to a website.

Name	Description
	• **Other**.
Value	Specify the object to deal with, such as an IP address, domain, etc.
Attack type	Select one of the following attack types: • **BotNet**: a network of infected computers controlled remotely by malicious actors • **Phishing**: a type of Internet scam that aims to get access to confidential user data such as logins and passwords. • **Malware**: any software that attempts to infect a computer or mobile device • **DDoS**: a method of bringing a website down by sending numerous requests to it that overwhelm the network • **Traffic hijack**: malicious redirection of traffic • **Network scanning**: scanning network nodes for vulnerabilities • **Brute force**: a method of cracking user accounts by guessing their passwords • **Compromised**: an actual or suspected case of unauthorized access to protected information • **Spam**: mass distribution of unsolicited email messages of commercial, political, or other nature using specialized software • **Other**.
TLP	A TLP (Traffic Light Protocol) marking of confidential information. The following TLP marks are possible: • **RED**: the information is highly confidential • **AMBER**: the information can be shared within the organization when necessary • **GREEN**: the information can be widely distributed within a certain community • **WHITE**: the information can be distributed freely and does not infringe copyright.
Is IoC?	Set this checkbox if the object is a potential indicator of compromise.
Services	The list of services used to obtain additional information on the observable objects. Displayed automatically after selecting the observable type. Available under **Settings → Libraries →**

Name	Description
	External enrichment services section. For more details, see the section External Enrichment Services.
Updated	The date and time when the service was last updated.

To edit or remove observables, use the **Edit** or **Remove** buttons, respectively.

In the **Activity** section, you can view the comments for the incident and its change history (adding watchers, changing the workflow state, etc.).

To generate a report on the incident, click **Generate report** and select:

- **Incident report**: a custom report that can be generated in English or Russian using PDF or HTML formats. You can use the templates listed under **Logs and reports → Incident reports → Incident report rules**.

Sending Cybersecurity Incident Reports to GosSOPKA

GosSOPKA is a state system for the detection, prevention and mitigation of the consequences of computer attacks on the information resources of the Russian Federation. The purpose of GosSOPKA is protecting the critical information infrastructure (CII), whose owners are required to register with and connect to the system. GosSOPKA can also be joined on a voluntary basis for increased cybersecurity and more effective incident detection and response.

UserGate SIEM implements the ability to send reports on computer attacks, incidents, and vulnerabilities in a standardized format via a GosSOPKA account.

To send reports, you need to:

1. Register and connect to a GosSOPKA account independently.

This is necessary to set up interworking and the automated exchange of information about the recorded cybersecurity incidents and methods of their prevention with GosSOPKA.

2. Add an encryption gateway to enable interworking with NCCCI (National Coordination Centre for Computer Incidents, the main data center for GosSOPKA).

You can use hardware and software systems by Infotecs (ViPNet), Security Code (Continent), and S-Terra (S-Terra Gateway) for self-connection to GosSOPKA.

> **Note**
> **Do not specify the encryption gateway as the default gateway.**

3. Add DNS servers for resolving GosSOPKA account addresses.

Add DNS servers with IP addresses of 10.0.100.49 and 10.0.100.50 to be able to resolve GosSOPKA account addresses.

> **Note**
> **No more than three servers can be added to the list of system DNS servers. GosSOPKA servers cannot be used for resolving Internet domain names.**

4. Configure a static route to the GosSOPKA network to provide connectivity to the DNS servers specified at step 3.

To provide connectivity to the GosSOPKA servers, add a static route with a destination address of 10.0.100.0/24. For more details on configuring routes, see the Routes section.

5. Configure the connection to a GosSOPKA account from UserGate SIEM to enable sending reports.

In UserGate SIEM, there is a predefined **Gossopka** connector that provides interworking with GosSOPKA.

To configure the connector, go to the **Settings** tab in the **Sensors → Connector** section. Use the **Gossopka** connector created in UserGate SIEM by default; you must specify the FQDN of your personal account instead of the default (the default value reflects the format in which the field value should be specified), login/password, and API key, which is added to the HTTP headers field.

6. Configure the report template.

A predefined template named **GOSSOPKA incident info** exists that conforms to GosSOPKA's report requirements. Fill in this form that will be used for report generation.

Name	Description
Organization name	The name of the organization.
Category	

Name	Description
	The alert category: • Computer incident alert • Computer attack alert • Vulnerability alert.
Security Event type	The type of cybersecurity event: • Controlled resource hijacked for use in malware infrastructure • Resource slowed down due to DDoS • Malware infection • Network traffic hijacking • Controlled resource used for phishing • Account compromised • Unauthorized modification of information • Unauthorized disclosure of information • Resource publishes information prohibited by Russian legislation • Spam sent from controlled resource • Successful vulnerability exploit.
Incident response status	The status of the incident response: • Measures taken • Response actions in progress • Response actions resumed.
GosSOPKA intervention required	Set this checkbox if intervention from GosSOPKA is required.
Security event summary	A summary of the cybersecurity event.
Means or method of incident detection	Information about the method and hardware/software that were used to detect the incident.
Date and time of incident detection	The date and time of incident detection are filled in automatically.
Date and time of incident closure	The date and time of incident closure are filled in automatically.
TLP restriction mark	

Name	Description
	A TLP (Traffic Light Protocol) marking of confidential information. The following TLP marks are possible: • **RED**: the information is highly confidential • **AMBER**: the information can be shared within the organization when necessary • **GREEN**: the information can be widely distributed within a certain community • **WHITE**: the information can be distributed freely and does not infringe copyright.
Availability impact	The potential impact on the availability of the information resources: • None • Low • High.
Integrity impact	The potential impact on the integrity of the information resources: • None • Low • High.
Confidentiality impact	The potential impact on confidentiality (restriction of access to information resources, provision of access for authorized users only, prevention of disclosure to unauthorized persons): • None • Low • High.
Summary of other impacts	A summary of incident impacts other than those listed above.
Name of controlled resource where incident was detected	The name of the controlled information resource of a CII object where a computer incident, computer attack, or vulnerability was detected.
CII object category info	The importance category assigned to the CII object: • Resource is not a CII object • Uncategorized CII object (object considered unimportant) • 3rd importance category CII object (lowest)

Name	Description
	• 2nd importance category CII object • 1st importance category CII object (highest).
CII object industry	The industry to which the CII object belongs (e.g., banking, healthcare, etc.).
Internet connectivity	Internet connectivity: • **Yes** • **No**.
Country/region	Code according to ISO-3166-2.
Locality or geolocation	The name or geographic coordinates of the locality. The coordinates are given in the following format: *latitude* N, *longitude* E.

7. Generate and send the cybersecurity incident report.

The report can be generated in the incident details tab by clicking **Generate report → GOSSOPKA report**. To send the report, select the connector configured earlier, click **Send via net**,

fill in the required form fields (the majority of the fields will be auto-filled from the **GOSSOPKA incident** info template), and click **OK**. If the connection is successful, the UserGate SIEM server will send the report via the connector to your GosSOPKA account.

The fact of sending the report will be recorded in SIEM's event log.

COMMAND LINE INTERFACE (CLI)

GENERAL PROVISIONS

General Provisions (Description)

UserGate SIEM supports a command line interface (CLI) for device configuration.

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 SSH protocol over the network.

> **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, follow these steps:

1. In **Settings → Network → Zones**, for the zone you want to connect to for CLI management, allow access for the CLI protocol over SSH. The TCP port 2200 will be opened.

2. Launch an SSH terminal on your computer, such as SSH for Linux or Putty for Windows. Specify the SIEM device address, 2200 as the connection port, and a username with root administrator privileges (by default, Admin with the "usergate" password) as the username. For Linux, the connection command should look like this:

```
ssh Admin@<IP-SIEM> -p 2200
```

After successful authentication, a line will appear in the CLI waiting for a command to be entered (diagnostic mode). To view current possible values or autocomplete a command, use the "Tab" key. The following commands are available in diagnostic mode:

- **configure**: switch to the configuration mode
- **date**: view the current device date and time
- **dig**: check the DNS record for a domain.
- **exit**: exit the command line
- **netcheck**: check the availability of a 3rd party HTTP/HTTPS server
- **show**: view network settings, software version, statistics of active sessions

- **clear**: clears statistics data for active sessions and network interfaces
- **ping**: ping a specific host
- **reboot**: reboot the device
- **shutdown**: shutting down the device
- **traceroute**: trace the connection route to a specific host

These commands are also available in configuration mode. For more information, see the Execute Commands section.

To abort the current command, press Ctrl+C; to view command history, use the ↑ or ↓ keys.

All CLI commands have the following structure:

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

Where:

<action> is the action to be performed;

<level> is the configuration level corresponding to the NGFW web interface section;

<filter> is the identifier of the object being accessed; and

<configuration_info> is the set of parameter values to be applied to the <filter> object.

COMMANDS AVAILABLE PRIOR TO INITIAL NODE SETUP

Commands Available Prior to Initial Node Setup (Description)

If the device has not undergone initial configuration, diagnostics and monitoring commands are fully available in the CLI, but only network configuration commands are available in the configuration mode (zone, interface, gateway, and virtual router configuration as well as enabling/disabling remote access to the radmin-emergency server).

INITIAL SETUP

Initial Setup (Description)

The initial setup of the device using the command line interface.

To configure the device, use the following command:

```
Admin@nodename# execute install master
```

Specify the following parameters:

Parameter	Description
login	Set admin name.
password	Set a password for the administrator account. You can also set the password on pressing **Enter** after typing in the administrator login; the password must be entered twice.

CONFIGURATION MODE

Configuration Mode (Description)

To enter the configuration mode, use the following command:

```
Admin@nodename> configure
```

Once you enter the configuration mode, the command line will be as follows:

```
Admin@nodename#
```

To view a hint about the current possible values or to autocomplete commands, press the **Tab** key. The following symbols can be used in the hint:

***** — a required field in the create command and some others

+ — an optional/variable field

> — a nested field; after entering it the previous list of fields becomes unavailable, a new list of fields appears that can be entered

Example:

```
Admin/system@nodename# set network zone Trusted
* name                    Name
+ antispoof-enable        Enable/Disable IP spoofing protection
+ antispoof-negate        Enable/Disable Negate ip-spoof addresses
+ description             Description
+ enabled-services        Services list to enable
+ geoip                   IP spoofing protection by geo IP code
+ ip-list                 IP spoofing protection by IP list
> dos-protection-icmp     Confugure DoS protection per IP for ICMP
packets
> dos-protection-syn      Confugure DoS protection per IP for SYN
packets
> dos-protection-udp      Confugure DoS protection per IP for UDP
packets
> service-addresses       Access control service addresses
```

General Command Structure in Configuration Mode

CLI commands have the following structure:

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

where:

<action> is the action to be performed;

<level> is the configuration level corresponding to the SIEM web interface section;

<filter> is the identifier of the object being accessed; and

<configuration_info> is the set of parameter values to be applied to the <filter> object.

Name	Description
<action>	The following actions are available in the configuration mode: • **execute**: execute commands not related to UserGate configuration (ping, date, traceroute, etc.). The command is available regardless of the configuration level (<level>). • **set**: edit all objects and enable various parameters, e.g. radmin. • **end**: go one level up. • **show**: display the current values. You can use this at any configuration level. Displays everything below the current level. • **edit**: go to a specific configuration level. The configuration level is displayed under the command line. • **top**: go back to the topmost configuration level. • **exit**: exit the configuration mode. • **export**: export the configuration. • **import**: import the configuration. • **create**: create new objects. • **delete**: delete an object or a parameter from the parameter list. For example, to view information about all interfaces, run the following command: `Admin@nodename# show network interface`

Name	Description

	To go to the **network interface** level, use the following command. The current level will be displayed under the command line:
	
	`Admin@nodename# edit network interface`
	`Admin@nodename#`
	`Level: network interface`
	
	After you go to the **network interface** level, use the show command to show all interfaces without specifying a level:
	
	`Admin@nodename# show`
	
	`adapter:`
	`  port0`
	`  type  : adapter`
	`  interface-name  : port0`
	`  node-name  : node`
	`  zone  : Management`
	`  enabled  : on`
	`  ip-addresses  : 192.168.56.3/24`
	`  iface-mode  : dhcp`
	`...`
	`...`
	`...`
	`Level: network interface`
	
	To return from the **network interface** level back to the general level of the configuration mode, use the **end** command:
	
	`Admin@nodename# end`
	`Level: network interface`
	`Admin@nodename# end`
	`Level: network`
	`Admin@nodename#`

Name	Description
<level>	Levels in the command line follow the SIEM system console web interface: • **network**: corresponds to the **Network** section of the web interface. • **settings**: corresponds to the **UserGate** section of the web interface. • **users**: corresponds to the **Users and devices** section of the web interface. • **libraries**: corresponds to the **Libraries** section of the web interface. • **monitoring**: corresponds to the **Diagnostics and monitoring** section of the web interface. • **sensors**: corresponds to the **Sensors** section of the web interface. • **analytics**: corresponds to the **Analytics** section of the web interface. • **incident**: corresponds to the **Incidents** section of the web interface.
<filter>	ID of the object which is being accessed. Objects are identified by their name. If there are objects with identical names or it is more convenient to identify objects by another parameter, specify <configuration_info> in parentheses. This will find an object matching all the fields specified in parentheses.
<configuration_info>	Set of parameter-argument pairs. where the parameter is the name of the field for which you need to set the argument. Arguments can be single-valued or multi-valued. **A single-valued argument** is the value of the parameter. If the string contains spaces, use quotation marks. For example, you need to create an authentication profile named New profile: `Admin@nodename# create users auth-profile name "New profile"` **Multi-valued arguments** are used to set multiple values of a parameter; include them in square brackets and separate by spaces. For example, you need to create a list of IP addresses in the element library and add two IP addresses 10.10.0.1 and 10.10.0.2 to it:

Name	Description
	`Admin@nodename# create libraries ip-list name testlist ips [ 10.10.0.1 10.10.0.2 ]` **Important!** Square brackets should be separated by spaces on both sides.

Execute Commands

These commands have the following structure:

```
Admin@nodename# execute <command-name>
```

Available commands:

Parameter	Description
traceroute	Traceroute the connection to a specified host. Available parameters: • **hostname <ip-or-domain>**: IP address or domain name for which tracing is performed. • **interface <iface-name>**: the interface from which packets will be sent • **not-map-ip**: do not search the hostname for the IP address when displaying • **use-icmp-echo**: use ICMP echo. • **port**: specify a port instead of the default port (1-65535). • **min-interval**: minimum interval between packets. `Admin@nodename# execute traceroute hostname <hostname>`
termination	Close the administrator sessions. For more details, see Managing Administrator Sessions.
ping	Ping a specific host. Available parameters: • **hostname**: the IP address or domain name of the server. • **count**: the number of echo requests to send. If not specified, the system will send the packets until the user

Parameter	Description
	terminates the connection (to terminate sending, press Ctrl+C). • **numeric**: do not resolve names. • **timestamp**: display timestamps. • **interval**: the time between sent packets (in seconds). • **ttl**: the packet's time to live. • **interface**: the address of the selected interface will be used as the source address for running ping. • **mtu**: the MTU size of the sent packets. • **virtual-router**: virtual router name. `Admin@nodename# execute ping hostname <hostname> count <number>`
reboot	Rebooting the device.
date	View the current date and time on the server.
shutdown	Shutting down the device.
netcheck	Check the availability of a third-party HTTP/HTTPS server. You can use the following parameters: • **address**: the host's domain name for checking availability over TCP or URL for HTTP • **dns-ip**: the DNS server's IP address • **dns-tcp**: use TCP instead of UDP for DNS request • **check-cert**: check the SSL certificate • **type**: check availability over: ◦ **http** ◦ **tcp** (if no port is specified, port 80 is used by default). • **data**: request the site content. Only headers are requested by default. • **timeout**: the maximum time to wait for a reply from the web server. • **user-agent**: parameter to specify the browser type (useragent). Some sites may only allow access from certain browsers. The parameter value is specified in double quotes.

Parameter	Description
	`Admin@nodename# execute netcheck type tcp address <host-domain-name> data on` `Admin@nodename# execute netcheck address <host-domain-name>`

dig	Check the domain DNS record.
	• **hostname**: the host's domain name or IP address for reverse lookup
	• **reverse-lookup**: get the host from the IP address
	• **dns**: specify the IP address of the DNS server
	• **tcp**: use TCP instead of UDP.
	`Admin@nodename# execute dig hostname <host-domain-name>`
	`Admin@nodename# execute dig hostname <IP-address> reverse-lookup on`

license	The product registration command has the following structure: `Admin@nodename# execute license activate <pin-code>` Provide your product activation code a <pin-code>.

Some commands presented above are also available in diagnostic and monitoring mode. To execute them, use the following command:

```
Admin@nodename> <command-name>
```

DEVICE SETUP

Device Setup (Description)

General Device Settings

You configure the device general settings at the **settings general** level. This is the command structure to configure one of the sections (<settings-module>):

```
Admin@nodename# set settings general <settings-module>
```

You can configure the following sections:

Parameter	Description
admin-console	Admin console settings (**settings general admin-console** level): • **timezone**: time zone for your location. Used in rule schedules and for the correct display of time and date in reports, logs, etc. • **language**: interface language: ◦ **ru**: Russian ◦ **en**: English • **api-session-lifetime**: admin session timeout in seconds.
server-time	Configure the exact time settings (**settings general server-time** level): • **ntp-enabled**: enable/disable the use of NTP servers: ◦ **on** ◦ **off** • **primary-ntp-server**: specify the primary ntp server. • **second-ntp-server**: specify a backup ntp server. • **time**: set server time (format: yyyy-mm-ddThh:mm:ss, e.g. 2022-02-15T12:00:00; UTC time zone).
change-tracker	Configure change tracker (**settings general change-tracker** level): • **enabled**: enable/disable change tracker. ◦ **on** ◦ **off** • **event-tracker-types**: change types are set by an administrator. To delete a change type, use the following command:

Parameter	Description
	`Admin/system@nodename# delete settings general change-tracker event-tracker-types [ type1 ... ] ]`
management-center	Configure UserGate Management Center agent (**settings general management-center** level): • **enabled**: enable/disable the UserGate Management Center agent. ◦ **on** ◦ **off** • **mc-address**: UserGate Management Center server address. • **device-code**: unique device code to connect to the UserGate Management Center.

updates-schedule	Configure the schedule to download software and library updates (**settings general updates-schedule** level).
	To configure a schedule to update UserGate software, use the following command:
	`Admin/system@nodename# set settings general updates-schedule software schedule <schedule/disabled>`
	You can set up a single schedule to download library updates:
	`Admin/system@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled>`
	or an individual schedule for each item:
	`Admin/system@nodename# set settings general updates-schedule libraries [ lib-module ... ] schedule <schedule/disabled> ] schedule <schedule/disabled>`

Parameter	Description
	The time is set in the Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours". To view the update schedule, use the following command: `Admin/system@nodename# show settings general updates-schedule`

Configuring device management

Configuring radmin emergency

To activate the remote assistant when a problem with the device's core software arises, the administrator can log in to the CLI using the root administrator account created when the node was initialized. Usually, this is the Admin account; however, it is not always so. To log in, specify the name as Admin@emergency and use the root administrator password as the password. To enable/disable remote access to the server for technical support in such cases, use the following command:

```
Adminm@emergency@SIEM# set radmin-emergency enabled <on | off>
```

Parameter	Description
interface	The interface name.
ip-addr	Interface IP address and mask.
gateway-address	Gateway IP address.

Configuring server operations

To set an update channel, use the following command:

```
Admin@nodename# set settings device-mgmt updates-channel <stable |
beta>
```

To view any updates and the selected update channel, use the following command:

```
Admin@nodename# show settings device-mgmt updates-channel
```

To configure the device license activation and software updates via an external proxy, use the following command:

```
Admin@nodename# set settings device-mgmt licensing-upstream-proxy
<parameters>
```

The additional parameters are as follows:

Parameter	Description
enabled	Enabling/disabling license activation and software update mode via an external proxy server: • **on**: enabled • **off**: disabled
ip	The external proxy's IP address.
port	The external proxy's port.
auth	Authentication with the external proxy: • **on**: enabled • **off**: disabled
name	The external proxy login name.
password	The external proxy password.

To view the settings for device license activation and software updates via an external proxy, use the following command:

```
Admin@nodename# show settings device-mgmt licensing-upstream-proxy
```

System backup management

A device backup is created at the **settings device-mgmt** level. To create a backup rule and upload files to external FTP/SSH servers, use the following command:

```
Admin@nodename# create settings device-mgmt settings-backup
<parameters>
```

The available parameters include:

Parameter	Description
enabled	Enable/disable the device backup rule.
name	The name of the backup rule.
description	A description of the backup rule.
type	Select a remote server to export files: • **ssh** • **ftp**
address	Remote server IP address.
port	Port:
login	Remote server login name.
password	Password for the login name.
path	Directory path to upload the files to.
schedule	The backup file export schedule. The time is set in the Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last).

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

To edit an existing device backup rule, use the following command:

```
Admin@nodename# set settings device-mgmt settings-backup <rule-name>
```

You can use the same set of parameters as when creating rules.

To delete a backup rule:

```
Admin@nodename# delete settings device-mgmt settings-backup <rule-name>
```

To display a backup rule:

```
Admin@nodename# show settings device-mgmt settings-backup <rule-name>
```

In the rule edit, delete, or display commands, <filter> can include the parameters specified in an existing rule in addition to the rule name (this can be helpful if there are multiple rules with the same name). Parameters used to identify an export rule are similar to those of the **set** command.

Settings Export

You create and configure export settings rules at the **settings device-mgmt settings-export** level.

To create an export settings rule, use the following command:

```
Admin@nodename# create settings device-mgmt settings-export
( <parameters> )
```

Available parameters:

Parameter	Description
enabled	Enable/disable an export settings rule for the UserGate server.
name	Export rule name.
description	Export rule description.
type	Select a remote server to export settings: • **ssh** • **ftp**
address	Remote server IP address.
port	Port:
login	Remote server login name.
password	Password for the login name.
path	Directory path to upload the settings to.
schedule	Schedule for settings export. The time is set in the Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

To update an existing rule to export the device settings, use the following command:

```
Admin@nodename# set settings device-mgmt settings-export <rule-name>
```

You can use the same set of parameters as when creating rules.

To delete a rule to export settings, use the following command:

```
Admin@nodename# delete settings device-mgmt settings-export <rule-name>
```

To display a rule to export settings, use the following command:

```
Admin@nodename# show settings device-mgmt settings-export <rule-name>
```

For update, delete or display rule commands, you can set <filter> not only to the rule name, but also to the parameters specified in an existing rule (this may be helpful if there is more than one rule with the same name). Parameters used to identify an export rule are similar to those of the **set** command.

Configuring Device Console Access Control

This section is configured at the **settings administrators** level. This section describes how to configure account security settings, administrators, and their profiles.

General access settings

In this section, you can configure additional security options for administrator accounts. This is configured at the **settings administrators general** level.

To change the parameters, use the following command:

```
Admin@nodename# set settings administrators general
```

The following parameters are available:

Parameter	Description
password	Change the current administrator password.
unblock	Unblock an administrator.
strong-password	

Parameter	Description
	Use a strong password: • **on** • **off**
num-auth-attempts	Maximum number of incorrect authentication attempts.
block-time	Time to block an account if the maximum number of authentication attempts is reached by the administrator (in seconds, max value is 3600 seconds).
min-length	Minimum password length (max value is 100 characters).
min-uppercase	Minimum number of uppercase characters (max value is 100 characters).
min-lowercase	Minimum number of lowercase characters (max value is 100 characters).
min-digits	Minimum number of digits (max value is 100 characters).
spec-characters	Minimum number of special characters (max value is 100 characters).
char-repetition	Maximum single character repetition block length (max value is 100 characters).

Examples of editing account parameters:

```
Admin@nodename# set settings administrators general block-time 400
```

To view the current security settings for administrator accounts, use the following command:

```
Admin@nodename# show settings administrators general

strong-password      : off
block-time           : 400
min-length           : 7
min-uppercase        : 1
min-lowercase        : 1
min-digits           : 1
```

```
spec-characters      : 1
char-repetition      : 2
num-auth-attempts    : 10
```

Configuring administrator accounts

You configure administrator accounts at the **settings administrators administrators** level.

To create an administrator account, use the following command:

```
Admin@nodename# create settings administrators administrators
```

Specify the administrator account type (local, LDAP user, LDAP group, with auth profile) and the respective parameters:

Parameter	Description
local	Add a local administrator: • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: administrator login name. • **display-name**: the administrator's display name. • **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. • **password**: administrator password.
ldap-user	Add a user from the existing domain (you need to have the LDAP connector configured correctly; for more details, see the Configuring LDAP Connectors section): • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: the administrator's login name in the **domain\user** format. When providing this parameter, use the following command structure: • **display-name**: the administrator's display name. • **connector**: the name of a previously configured LDAP connector.

Parameter	Description
	• **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. `Admin@nodename# create settings administrators administrators ldap-user admin-profile "test profile 1" connector "LDAP connector" description "Admin as domain user" login testd.local\user1 enabled on`
ldap-group	Add a user group from the existing domain (you need to have the LDAP connector configured correctly; for more details, see the Configuring LDAP Connectors section): • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: administrator login name • **display-name**: the administrator's display name. • **connector**: the name of the used LDAP connector. • **description**: administrator account description. • **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. `Admin@nodename# create settings administrators administrators ldap-group admin-profile "test profile 1" connector "LDAP connector" description "Domain admin group" login testd.local\users enabled on`
admin-auth-profile	Add an administrator with an auth profile (you need to have the auth servers configured correctly; for more details, see the Configuring Authentication Servers section): • **enabled**: enable/disable an administrator account: ◦ **on** ◦ **off** • **login**: administrator login name. • **display-name**: the administrator's display name. • **description**: administrator account description.

Parameter	Description
	• **admin-profile**: administrator profile. For more details about creating administrator profiles, see below. • **auth-profile**: select an auth profile from those created earlier; for more details about auth profiles, see the section Configuring Authentication Profiles.

To edit the profile parameters, use the following command:

```
Admin@nodename# set settings administrators administrators <admin-type>
<admin-login>
```

The command's parameters are similar to those used for administrator profile creation.

To display information about all administrator accounts, use the following command:

```
Admin@nodename# show settings administrators administrators
```

To display information about an individual administrator account, use the following command:

```
Admin@nodename# show settings administrators administrators <admin-
type> <admin-login>
```

Example of the command execution:

```
Admin@nodename# show settings administrators administrators ldap-user
testd.local\user1

login            : testd.local\user1
enabled          : on
type             : ldap_user
locked           : off
admin-profile    : test profile 1
```

To delete an account, use the following command:

```
Admin@nodename# delete settings administrators administrators <admin-
type> <admin-login>
```

Example of the command:

```
Admin@nodename# delete settings administrators administrators ldap-user
testd.local\user1
```

Configuring Permissions for Administrator Profiles

The permissions of administrator profiles are configured at the **settings administrators profiles** level.

To create an administrator profile, use the following command:

```
Admin@nodename# create settings administrators profiles
```

Provide the following parameters:

Parameter	Description
name	Administrator profile name.
description	Administrator profile description.
roles	Selecting a role for the administrator profile. For more details on roles, see the User Roles and Role Permissions section.
permissions	Permissions: • **no-access**: no access • **read**: read-only • **write**: read and write

To edit the profile, use the following command:

```
Admin@nodename# set settings administrators profiles <profile-name>
<parameter>
```

The command's parameters are similar to those used for administrator profile creation.

To view information about all administrator profiles, use the following command:

```
Admin@nodename# show settings administrators profiles
```

To display information about a specific profile, use the following command:

```
Admin@nodename# show settings administrators profiles <profile-name>
```

To delete an administrator profile, use the following command:

```
Admin@nodename# delete settings administrators profiles <profile-name>
```

Managing Administrator Sessions

The following commands allow you to view the active sessions of administrators who have been authenticated in the web console or CLI and close the sessions (this is done at the **settings administrators admin-sessions** level).

To view administrator sessions for the device, use the following command. You can view an individual administrator's session; to do so, browse the IP address list and select the address used to authenticate the administrator.

```
Admin@nodename# show settings administrators admin-sessions
```

To display sessions, you can use a filter:

- **ip**: IP address from which the administrator logged in.
- **source**: where authentication was made: CLI (**cli**), web console (**web**) or SSH connection (**ssh**).
- **admin-login**: administrator name.

```
Admin@nodename# show settings administrators admin-sessions ( node
<node-name> ip <session-ip> source <cli | web | ssh> admin-login
<administrator-login> )
```

To close an administrator session, use the following command. Select the IP address from which the administrator was authenticated, from the list.

```
Admin@nodename# execute termination admin-sessions <IP-address/
connection type>
```

Example of the command execution:

```
Admin@nodename# show settings administrators admin-sessions

admin-login           : Admin
source                : ssh
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : <node-name>

admin-login           : Admin
source                : web
session_start_date    : 2023-08-10T11:33:10Z
ip                    : 10.0.2.2
node                  : <node-name>

Admin@nodename# execute termination admin-sessions 10.0.2.2/web

Admin@nodename# show settings administrators admin-sessions

admin-login           : Admin
source                : ssh
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : <node-name>
```

When closing administrator sessions, you can use a filter (<filter>). Enabled filtering options are the same as those for the **show** command.

```
Admin@nodename# execute termination admin-sessions ( node <node-name>
ip <session-ip> source <cli | web | ssh> admin-login <administrator-
login> )
```

Configuring Certificates

The **Certificates** section is located at the **settings certificates** level.

To import certificates, use the following command:

```
Admin@nodename# import settings certificates
```

Parameters:

Parameter	Description
name	The name under which the certificate will be displayed in the certificate list.
description	Certificate description.
certificate-data	The certificate's date in PEM format.
private-key	The certificate private key in PEM format.
passphrase	The private key passphrase (if required).
certificate-chain	Certificate's chain of the upstream CA certificates used when creating this certificate, in PEM format.

To export certificates, the entire certificate's chain, use the following command:

```
Admin@nodename# export settings certificates <certificate-name>
Admin@nodename# export settings certificates <certificate-name> with-
chain on
```

To create a certificate and CSR, use the following command:

```
Admin@nodename# create settings certificates type <certificate | csr>
```

Provide the following parameters:

Parameter	Description
name	Certificate name.
description	Certificate description.
country	Country where the certificate is being issued.
state	Region/state where the certificate is being issued.
locality	Locality name where the certificate is being issued.
organization	Organization name for which the certificate is being issued.
common-name	Certificate name. To ensure compatibility with the majority of browsers, we recommend using only Latin characters.
email	Company email.

To manage a certificate, use the following command:

```
Admin@nodename# set settings certificates <certificate-name>
```

Available parameters:

Parameter	Description
name	Certificate name.
description	Certificate description.
role	Certificate type: • **web-cert-chain**: web console certificate's chain. • **web-ssl**: certificate used to create a secure HTTPS administrator connection to the UserGate web console. • **none**.
certificate-chain	Certificate's chain in PEM format.

To delete a certificate, use the following command:

```
Admin@nodename# delete settings certificates <certificate-name>
```

To view information about all or individual certificates, use the following command:

```
Admin@nodename# show settings certificates
Admin@nodename# show settings certificates <certificate-name>
```

Configuring Authentication Servers

The Auth servers section allows you to configure an LDAP connector, RADIUS, TACACS+ servers. You configure auth servers at the **users auth-server** level. We will consider it in the respective sections below.

Configuring LDAP connectors

An LDAP connector is configured at the **users auth-servers ldap** level.

To create an LDAP connector, use the following command:

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

Provide the following parameters:

Parameter	Description
name	LDAP connector name.
enabled	Enable/disable the auth server.
description	LDAP connector description.
ssl	Values: • **on**: use an SSL connection to connect to the LDAP server • **off**: connect to the LDAP server without using an SSL connection.

Parameter	Description
address	Controller IP address or the LDAP domain name.
bind-dn	The username used to connect to the server. Format: DOMAIN\username or username@domain. The user must be a user in the domain.
password	The user's password for connecting to the domain.
domains	List of domains served by the domain controller.
search-roots	The list of LDAP server paths relative to which the system will search for users and groups. Specify the full name, e.g., ou=Office,dc=example,dc=com. If the search paths are not specified, the system will search over the entire directory, starting from the root.

To edit information about an existing LDAP connector, use the following command:

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

The parameters available to update are the same as those for creating an LDAP connector.

To display information on an LDAP connector, use the following command:

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

Example commands to create and edit an LDAP connector:

```
Admin@nodename# create users auth-server ldap name "New LDAP connector"
ssl on address 10.10.0.10 bind-dn ug@testd.local password 12345 domains
[ testd.local ] search-roots [ dc=testd,dc=local ] enabled on
Admin@nodename# show users auth-server ldap "New LDAP connector"

name              : New LDAP connector
enabled           : on
ssl               : on
address           : 10.10.0.10
```

```
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
Admin@nodename# set users auth-server ldap "New LDAP connector"
description "New LDAP connector description"
Admin@nodename# show users auth-server ldap "New LDAP connector"

name             : New LDAP connector
description      : New LDAP connector description
enabled          : on
ssl              : on
address          : 10.10.0.10
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
```

To delete an LDAP connector, use the following command:

```
Admin@nodename# delete users auth-server ldap <ldap-server-name>
<parameter>
```

You can also delete individual parameters of an LDAP connector. You can delete the following parameters:

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

Configuring RADIUS Servers

A RADIUS server is configured at the **users auth-servers radius** level.

To create a RADIUS auth server, use the following command:

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

Provide the following parameters:

Parameter	Description
name	The RADIUS server name.
enabled	Enable/disable the auth server.
description	Auth server description.
secret	Pre-shared key used by the RADIUS protocol for authentication.
addresses	IP address and the UDP port on which the RADIUS server listens to requests (default port: 1812). Format: <ip:port>.

To update information about a RADIUS server, use the following command:

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

The parameters you can update are the same as those used to create an auth server.

To display information about a RADIUS server, use the following command:

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

Example commands to create and edit a RADIUS server:

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

name           : New RADIUS server
enabled        : on
addresses      :
    host    : 10.10.0.9
    port    : 1812
Admin@nodename# set users auth-server radius "New RADIUS server"
description "New RADIUS server description"
Admin@nodename# show users auth-server radius "New RADIUS server"
```

```
name           : New RADIUS server
description    : New RADIUS server description
enabled        : on
addresses      :
    host    : 10.10.0.9
    port    : 1812
```

To delete a server, use the following command:

```
Admin@nodename# delete users auth-server radius <radius-server-name>
<parameter>
```

You can also delete individual parameters of a RADIUS server. You can delete the following parameters:

- **addresses**

Configuring a TACACS+ server

A TACACS+ server is configured at the **users auth-servers tacacs** level.

To create a TACACS+ auth server, use the following command:

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

Provide the following parameters:

Parameter	Description
name	TACACS+ server name.
enabled	Enable/disable the server.
description	Auth server description.
secret	Pre-shared key used by the TACACS+ protocol for authentication.
address	The IP address for the TACACS+ server.
port	

Parameter	Description
	The UDP port on which the TACACS+ server listens for authentication requests. By default, UDP port 1812 is used.
single-connection	Use a single TCP connection for communicating with the TACACS+ server.
timeout	The authentication timeout for the TACACS+ server. The default is 4 seconds.

To edit information about a TACACS+ server, use the following command:

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

The parameters you can update are the same as those used to create an auth server.

To display information about a TACACS+ server, use the following command:

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

Example commands to create and edit a TACACS+ server:

```
Admin@nodename# create users auth-server tacacs address 10.10.0.11 name
"New TACACS+ server" port 1812 secret 12345 enabled on
Admin@nodename# show users auth-server tacacs "New TACACS+ server"

name                  : New TACACS+ server
enabled               : on
address               : 10.10.0.11
port                  : 1812
single-connection     : off
timeout               : 4
Admin@nodename# set users auth-server tacacs "New TACACS+ server"
description "New TACACS+ server description"
Admin@nodename# show users auth-server tacacs "New TACACS+ server"

name                  : New TACACS+ server
```

```
description          : New TACACS+ server description
enabled              : on
address              : 10.10.0.11
port                 : 1812
single-connection    : off
timeout              : 4
```

To delete a server, use the following command:

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

Configuring Authentication Profiles

You configure auth profiles at the **users auth-profile** level.

To create an auth profile, use the following command:

```
Admi@nodename# create users auth-profile <parameter>
```

Provide the following parameters:

Parameter	Description
name	Profile name.
description	Profile description.
idle-time	Idle time before disconnection (in seconds). After the specified time without activity the user's status will change to Unknown user.
expiration-time	Authenticated user time-to-live (in seconds). After the specified time the user's status will change to Unknown user and they will have to authenticate again.
max-attempts	Max authentication failures allowed before the user account is locked.

Parameter	Description
lockout-time	Time (in seconds) for which the user account is locked if the specified max number of failures is reached.
auth-methods	Authentication method: • **ldap**: authentication using an LDAP connector. • **radius**: authentication using a RADIUS server. • **tacacs**: authentication using a TACACS+ server.

To edit authentication profile parameters, use the following command:

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

The list of parameters available to update is the same as for the **create** command.

Example of creating and editing a user authentication profile:

```
Admin@nodename# create users auth-profile name "New LDAP auth profile"
auth-methods ldap [ "New LDAP connector" ]
Admin@nodename# show users auth-profile "New LDAP auth profile"

name                : New LDAP auth profile
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic          : off
    local-user-auth     : off
    policy-accept       : off
Admin@nodename# set users auth-profile "New LDAP auth profile"
description "New LDAP auth profile description"
Admin@nodename# show users auth-profile "New LDAP auth profile"

name                : New LDAP auth profile
description         : New LDAP auth profile description
max-attempts        : 5
```

```
idle-time          : 900
expiration-time    : 86400
lockout-time       : 300
mfa                : none
auth-methods       :
    http-basic          : off
    local-user-auth     : off
    policy-accept       : off
    ldap                : New LDAP connector
```

You can use the command line interface to delete an entire profile or individual authentication methods specified in a profile. To do this, use the following commands.

To delete an authentication profile:

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

To delete authentication methods configured in a profile, you need to specify an authentication method (available authorization methods are listed in the table above):

```
Admin@nodename# delete users auth-profile <auth-profile-name> auth-
methods <auth-metod>
```

User Roles

A user role is a set of role permissions. A role permission grants an administrator the ability to perform certain actions – e.g., add or remove an attachment from an existing incident, create a triggered alert rule, create or close an incident, etc. Roles are assigned to administrator profiles, which are, in turn, assigned to administrators.

User roles are created and configured at the **users roles** level.

To create roles and assign role permissions, use the command:

```
Admin@nodename# create users roles <role-name> description <role-
description> permissions [ <permissions> ]
```

You can find more details on roles and the list of current role permissions in the User Roles and Role Permissions section of the SIEM Administrator Guide.

To edit previously created roles and role restrictions, use the command:

```
Admin@nodename# set users roles <role-name> description <role-
description> permissions [ <permissions> ]
```

To remove previously created roles or individual role permissions in previously created roles, use the command:

```
Admin@nodename# delete users roles <role-name> permissions
[ <permissions> ]
```

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.

User catalogs are created and configured at the **users catalogs ldap** level.

To create a catalog, use the following command:

```
Admin@nodename# create users catalogs ldap <parameter>
```

Provide the following parameters:

Parameter	Description
name	LDAP connector name.
enabled	Enable/disable the auth server.

Parameter	Description
description	LDAP connector description.
ssl	Values: • **on**: use an SSL connection to connect to the LDAP server • **off**: connect to the LDAP server without using an SSL connection.
address	Controller IP address or the LDAP domain name.
bind-dn	The username used to connect to the server. Format: DOMAIN\username or username@domain. The user must be a user in the domain.
password	The user's password for connecting to the domain.
domains	List of domains served by the domain controller.
search-roots	The list of LDAP server paths relative to which the system will search for users and groups. Specify the full name, e.g., ou=Office,dc=example,dc=com. If the search paths are not specified, the system will search over the entire directory, starting from the root.

To edit information about an existing catalog, use the following command:

```
Admin@nodename# set users catalogs ldap <ldap-server-name> <parameter>
```

The parameters available to update are the same as those for creating a catalog.

To display information about a user catalog, use the following command:

```
Admin@nodename# show users catalogs ldap <ldap-server-name>
```

To delete a catalog, use the following command:

```
Admin@nodename# delete users catalogs ldap <ldap-server-name>
<parameter>
```

You can also delete individual parameters of an LDAP connector. You can delete the following parameters:

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

NETWORK CONFIGURATION

Zones

This section is located at the **network zone** level. To create a new zone, use the following command:

```
Admin@nodename# create network zone
```

Provide the following zone parameters:

Parameter	Description
name	Zone name.
description	Zone description.
dos-protection-syn	Protect the zone against network flooding for TCP protocol (SYN-flood): • **enabled**: enable/disable the protection. ◦ **on** ◦ **off** • **aggregate**: ◦ **on**: count all packets incoming to the zone's interfaces ◦ **off**: count packets for each IP address separately. • **alert-threshold**: alert threshold; if the number of requests exceeds this value, the event is recorded in the system log. • **drop-threshold**: packet drop threshold; if the number of requests exceeds this value, UserGate drops packets and records this event in the system log.

Parameter	Description
	• **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
dos-protection-udp	Protect the zone against network flooding for UDP protocol: • **enabled**: enable/disable the protection. ◦ **on** ◦ **off** • **aggregate**: ◦ **on**: count all packets incoming to the zone's interfaces ◦ **off**: count packets for each IP address separately. • **alert-threshold**: alert threshold; if the number of requests exceeds this value, the event is recorded in the system log. • **drop-threshold**: packet drop threshold; if the number of requests exceeds this value, UserGate drops packets and records this event in the system log. • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
dos-protection-icmp	Protect the zone against network flooding for ICMP protocol: • **enabled**: enable/disable the protection. ◦ **on** ◦ **off** • **aggregate**: ◦ **on**: count all packets incoming to the zone's interfaces ◦ **off**: count packets for each IP address separately. • **alert-threshold**: alert threshold; if the number of requests exceeds this value, the event is recorded in the system log. • **drop-threshold**: packet drop threshold; if the number of requests exceeds this value, UserGate drops packets and records this event in the system log. • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
enabled-services	Zone access control settings: • **"Any ICMP"**: allow use of the ping command to a UserGate address. • **SNMP**: provides SNMP access to UserGate (UDP 161).

Parameter	Description
	• **rpc**: control XML-RPC: enables API control of the product (TCP 4040). • **VRRP**: required for combining several UserGate nodes into a HA cluster (IP protocol 112). • "CLI over SSH": access to server to manage it via CLI, port TCP 2200. • **Cluster**: service required to combine multiple UserGate nodes into a cluster (TCP 4369, TCP 9000-9100). • **"Admin Console"**: access to the management web console (TCP 8001).
service-addresses	Allowed IP addresses for services: • **service**: select services (the list corresponds to **enabled-services**). • **allowed-addresses**: the allowed IP addresses. The options are: ◦ **geoip**: a GeoIP code ◦ **ip-list**: an IP address list previously configured in the item library.
antispoof-enable	Enable/disable IP spoofing protection: • **on** • **off**
antispoof-negate	Enumerated options: • **on** • **off** If **antispoof-negate on** is enabled, the interfaces in that zone will not receive packets from the source addresses specified in the value **ip-spoofing-networks**. In this case packets with specified source IP addresses will be discarded.
sessions-limit-enabled	Enable the limit on the number of concurrent sessions from a single IP address: • **on** • **off**
sessions-limit-exclusions	Add a list of IP addresses to which the concurrent session limit will not apply.

Parameter	Description
sessions-limit-threshold	The maximum allowed number of sessions originating from a single IP address.
geoip	GeoIP codes that are used in IP spoofing protection.
ip-list	List of IP addresses that are used in IP spoofing protection.

Example command to create a zone:

```
Admin@nodename# create network zone name Test_zone description
"Test_zone description" antispoof-enable on enabled-services [ "Any
ICMP" DNS ] dos-protection-icmp enabled on
```

To edit zone parameters, use the following command:

```
Admin@nodename# set network zone <zone-name>
```

To edit zone parameters, use the following command:

```
Admin@nodename# set network zone Test_zone dos-protection-syn enabled
on
```

To delete a zone or its parameters, use the following command:

```
Admin@nodename# delete network zone <zone-name>
```

You can delete the following parameters:

Parameter	Description
dos-protection-syn	Protect the zone against network flooding for TCP protocol (SYN-flood): • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
dos-protection-udp	

Parameter	Description
	Protect the zone against network flooding for UDP protocol: • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
dos-protection-icmp	Protect the zone against network flooding for ICMP protocol: • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
enabled-services	The previously configured zone access control settings
geoip	GeoIP codes that are used in IP spoofing protection.
ip-list	List of IP addresses that are used in IP spoofing protection.

The following command is used to view zone settings:

```
Admin@nodename# show network zone <zone-name>
```

Interfaces

You apply interface settings at the **network interface** level.

Adapter settings

Network adapters are configured at the **network interface adapter** level.

You cannot create a network adapter. To update an existing network adapter, use the command:

```
Admin@nodename# set network interface adapter <adapter_name>
```

Provide the following network adapter parameters:

Parameter	Description
enabled	Enable/disable a network interface: • **on**

Parameter	Description
	• **off**
description	Network interface description.
alias	The interface's alias.
iface-type	Interface type: • **l3**: interface works in Layer 3 mode (you can assign an IP address and use it in firewall, content filtering, and other rules; this is the standard interface operation mode). • **mirror**: interface works in Mirror mode (it can receive traffic from the network equipment SPAN port to analyze it).
iface-mode	IP address assignment mode: • **dhcp**: obtain a dynamic IP address via DHCP. • manual: no address. Static mode is set automatically when an IP address is assigned to the interface.
zone	Zone to which the interface belongs.
link-info	Settings for network interface parameters: • **bc_forwarding**: control forwarding the directed broadcast packets arriving at the specified interface. • **proxy_arp**, **proxy_arp_vlan**: Proxy ARP mechanism. With **proxy_arp**, UserGate will respond to ARP requests for addresses outside the interface's network; with **proxy_arp_vlan**, UserGate will respond to ARP requests for addresses that belong to the interface's network. To specify them, use the following format: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` where **key** is the parameter name. which can include lowercase Latin letters (a-z) and underscore (_), and **value** is the parameter value. Parameter values can only be integers. For example, use proxy_arp/1 to enable the Proxy ARP mechanism and proxy_arp/0 to disable it. The link-info field is displayed only when adding parameters.

Parameter	Description
	Important!You cannot delete the specified parameters.
ip-addresses	Assign an IP address to the interface. The IP addresses are specified as **[<ip_address/mask>]** or **[<ip_address/mask> <ip_address/mask>]**. In case of several IP addresses (with space used as the separator), the subnet mask is entered in the decimal format. **Important!** Make sure to separate the square brackets with spaces on both sides.
mac	Interface MAC address.
mtu	Specify the MTU size.
mss	Specify MSS size (available in software version 7.3.0 and higher): 0, or starting from 4 to the value specified in MTU minus 40.

To delete an adapter or its parameters, use the following command:

```
Admin@nodename# delete network interface adapter <adapter-name>
```

You can delete the following parameters:

Parameter	Description
ip-addresses	Specified IP address.
dhcp-relay server-address	DHCP server IP address.

To display information about all network adapters, use the following command:

```
Admin@nodename# show network interface adapter
```

To display the adapter information, use the following command:

```
Admin@nodename# show network interface adapter <adapter-name>
```

Configuring a VLAN

VLAN interfaces are configured at the **network interface vlan** level.

To add a new VLAN interface, use the following command:

```
Admin@nodename# create network interface vlan
```

Parameters:

Parameter	Description
enabled	Enable/disable a VLAN interface: • **on** • **off**
description	Interface description.
alias	The interface's alias.
iface-type	Interface type: • **l3**: Layer 3 (you can assign an IP address and use it in firewall, content filtering, and other rules; this is the standard interface operation mode). • **mirror**: interface works in Mirror mode (it can receive traffic from the network equipment SPAN port to analyze it).
iface-mode	IP address assignment mode: • **dhcp**: obtain a dynamic IP address via DHCP. • manual: no address. Static mode is set automatically when an IP address is assigned to the interface.
tag	VLAN tag. Up to 4094 interfaces can be created.
node-name	Cluster node name where the VLAN is created.
interface	The physical interface on which the VLAN is being created.
zone	Zone to which the interface belongs.

Parameter	Description
link-info	Settings for network interface parameters: • **bc_forwarding**: control forwarding the directed broadcast packets arriving at the specified interface. • **proxy_arp**, **proxy_arp_vlan**: Proxy ARP mechanism. With **proxy_arp**, UserGate will respond to ARP requests for addresses outside the interface's network; with **proxy_arp_vlan**, UserGate will respond to ARP requests for addresses that belong to the interface's network. To specify them, use the following format: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` where **key** is the parameter name. which can include lowercase Latin letters (a-z) and underscore (_), and **value** is the parameter value. Parameter values can only be integers. For example, use proxy_arp/1 to enable the Proxy ARP mechanism and proxy_arp/0 to disable it. The link-info field is displayed only when adding parameters. **Important!**You cannot delete the specified parameters.
ip-addresses	Assign an IP address to the interface. The IP addresses are specified as **[<ip_address/mask>]** or **[<ip_address/mask> <ip_address/mask>]**. In case of several IP addresses (with space used as the separator), the subnet mask is entered in the decimal format. **Important!** Make sure to separate the square brackets with spaces on both sides.
mac	Interface MAC address.
mtu	Specify the MTU size.
mss	Specify MSS size (available in software version 7.3.0 and higher): 0, or starting from 4 to the value specified in MTU minus 40.
dhcp-relay	Settings for the DHCP relay on the interface. You need to specify the following: • **enabled**: enable/disable the relay: ◦ **on** ◦ **off**

Parameter	Description
	• **utm-address**: IP address of the UserGate interface on which the relay function is added. • **server-address**: addresses of DHCP servers where DHCP requests from clients should be redirected.

To edit an existing VLAN, use the following command:

```
Admin@nodename# set network interface vlan <vlan-name>
```

The parameters available for setting are the same as those for creating a VLAN, except for **tag**, **node-name**, and **interface** (you cannot change these parameter values).

To delete a VLAN interface or its parameters, use the following command:

```
Admin@nodename# delete network interface vlan <vlan-name>
```

You can delete the following parameters:

Parameter	Description
ip-addresses	Specified IP address.
dhcp-relay server-address	DHCP server IP address.

To display information about all VLAN interfaces, use the following command:

```
Admin@nodename# show network interface vlan
```

To display information about a single interface, use the following command:

```
Admin@nodename# show network interface vlan <vlan-name>
```

Properties of bond interfaces

You configure bond interface properties at the **network interface bond** level.

To create a bond interface, use the following command:

```
Admin@nodename# create network interface bond
```

You need to specify the following parameters:

Parameter	Description
enabled	Enable/disable the interface: • **on** • **off**
interface-name	Enter a number to include in the interface name (for example, if you enter 1 the interface name will be bond1).
description	Interface description.
alias	The interface's alias.
node-name	Cluster node where the bond interface is created.
zone	Zone to which the bond belongs.
link-info	Settings for network interface parameters: • **bc_forwarding**: control forwarding the directed broadcast packets arriving at the specified interface. • **proxy_arp**, **proxy_arp_vlan**: Proxy ARP mechanism. With **proxy_arp**, UserGate will respond to ARP requests for addresses outside the interface's network; with **proxy_arp_vlan**, UserGate will respond to ARP requests for addresses that belong to the interface's network. To specify them, use the following format: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` where **key** is the parameter name. which can include lowercase Latin letters (a-z) and underscore (_), and **value** is the parameter value. Parameter values can only be integers. For example, use proxy_arp/1 to enable the Proxy ARP mechanism and proxy_arp/0 to disable it. The link-info field is displayed only when adding parameters.

Parameter	Description
	Important!You cannot delete the specified parameters.
bonding	Additional bond interface parameters: • **mode**: bond operation mode. The available options: ◦ **round-robin**: Round robin mode (packets are sent sequentially starting with the first available interface and ending with the last one. This policy is used to provide load balancing and high availability.) ◦ **active-backup**: Active backup mode (only one network interface in the bond will be active. Another slave interface can become active only if the currently active interface fails. With this policy, the MAC address of the bond interface is only visible externally through one network port to avoid problems with the switch. This policy is used to provide high availability). ◦ **xor**: XOR mode (the transmission is allocated among the NICs using the following formula: [(XOR) MOD]. This means that the same NIC sends packets to the same recipients. Optionally, the transmission allocation can also be based on the xmit_hash policy. The XOR policy is used for load balancing and high availability). ◦ **broadcast**: Broadcast mode (broadcasts everything to all network interfaces. This policy is used for high availability). ◦ **802.3ad**: IEEE 802.3ad mode (the default mode supported by most network switches. Creates aggregated groups of NICs with identical speed and duplex settings. When combined like this, all links in the active aggregation participate in transmission as per IEEE 802.3ad. The choice of interface for packet transmission is determined by the policy. By default, the XOR policy is used, with the xmit_hash policy as a possible alternative). ◦ **transmit**: Adaptive transmit load balancing mode (outgoing traffic is distributed depending on the loading of each NIC (determined by the load speed). No additional configuration on the switch is required. The incoming traffic is received by the current network card. If this card fails, another card assumes the MAC address of the failed one). ◦ **load**: Adaptive load balancing mode. Includes the previous policy plus incoming traffic balancing. No additional configuration on the switch is required. The incoming traffic is balanced through ARP

Parameter	Description
	negotiation. The driver intercepts ARP responses sent from the local NICs to the outside and overwrites the source MAC address with one of the unique MAC addresses of the NIC in the bond. Thus, different peers use different server MAC addresses. The incoming traffic is balanced sequentially (round-robin) among the interfaces. • **mii-monitoring**: MII monitoring period in milliseconds. Determines how often the link state will be checked for failures. • **down-delay**: delay time (in milliseconds) before an interface is disabled if a connection failure occurs. This option is only valid for MII monitoring (miimon). The parameter value must be a multiple of miimon, • **up-delay**: delay time in milliseconds before deploying the channel if it is detected to be restored. This parameter is only valid with MII monitoring (miimon). The parameter value must be a multiple of miimon, • **lacp-rate**: interval with which the partner transmits LACPDU packets in 802.3ad mode. Enumerated options: ◦ **slow**: requests that the partner send LACPDU packets every 30 seconds. ◦ **fast**: requests that the partner send LACPDU packets every second. • **failover-mac**: define the assignment type of MAC addresses to bond interfaces in Active backup mode when switching interfaces. Enumerated options: ◦ **disabled**: the same MAC address is set on all interfaces during switching. ◦ **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.

Parameter	Description
	• **xmit-hash**: define a hash policy for sending packets over bond interfaces in XOR or IEEE 802.3ad mode. Enumerated options: ◦ **l2**: use only MAC addresses to generate the hash. With this algorithm, the traffic for a particular network host is always sent over the same interface. This algorithm is compatible with IEEE 802.3ad. ◦ **l2-3**: use both MAC and IP addresses to generate the hash. This algorithm is compatible with IEEE 802.3ad. ◦ l3-4: uses IP addresses and transport layer protocols (TCP or UDP) to generate the hash. This algorithm is not universally compatible with IEEE 802.3ad, as both fragmented and non-fragmented packets can be transmitted within a single TCP or UDP interaction. Fragmented packets lack the source and destination ports. As a result, packets from the same session can reach the recipient in an order other than the intended one because they are sent via different slaves. • **interface**: interfaces to be bonded.
iface-mode	IP address assignment mode: • **dhcp**: obtain a dynamic IP address via DHCP. • manual: no address. Static mode is set automatically when an IP address is assigned to the interface.
iface-type	The type of interface to be created: • **l3**: a Layer 3 interface • **mirror**: a mirroring interface.
ip-addresses	Assign an IP address to the interface. The IP addresses are specified as **[<ip_address/mask>]** or **[<ip_address/mask> <ip_address/mask>]**. In case of several IP addresses (with space used as the separator), the subnet mask is entered in the decimal format. **Important!** Make sure to separate the square brackets with spaces on both sides.
mac	Interface MAC address.

Parameter	Description
mtu	Specify the MTU size.
mss	Specify MSS size (available in software version 7.3.0 and higher): 0, or starting from 4 to the value specified in MTU minus 40.

To update an existing bond interface, use the following command:

```
Admin@nodename# set network interface bond <bond-name>
```

The parameters available for setting are the same as those for creating a bond interface, except for **interface-name** and **node-name** (you cannot change the values of these parameters).

To delete a bond interface or its parameters, use the following command:

```
Admin@nodename# delete network interface bond <bond-name>
```

You can delete the following parameters:

Parameter	Description
ip-addresses	Specified IP address.
dhcp-relay server-address	DHCP server IP address.
bonding interface	Bonded interfaces.

To display information about all bond interfaces, use the following command:

```
Admin@nodename# show network interface bond
```

To display information about a single interface, use the following command:

```
Admin@nodename# show network interface bond <bond-name>
```

Gateways

This section is located at the **network gateway** level.

To add a new gateway, use the following command:

```
Admin@nodename# create network gateway
```

Available parameters:

Parameter	Description
enabled	Enable/disable the gateway: • **on** • **off**
name	Gateway name.
description	Gateway description.
interface	Interface used to access the Internet: • Select a specific port (**port0**, **port1**, **port2**, etc.); • **auto**: after selecting this option, the port will be detected automatically.
ip	Gateway IP address.
node-name	Select the cluster node for which the gateway is configured.
weight	Gateway weight (the greater the weight, the greater the share of traffic goes through the gateway).
balancing	Balancing mode: all traffic to the Internet will be distributed between the gateways according to their weights: • **on** • **off**
default	Use this gateway as the default gateway: • **on** • **off**

To update gateway parameters, use the following command:

```
Admin@nodename# set network gateway <gateway-name>
```

You can use the same set of parameters as when creating a gateway.

To delete a gateway, use the following command:

```
Admin@nodename# delete network gateway <gateway-name>
```

To display information about all gateways, use the following command:

```
Admin@nodename# show network gateway
```

To display information about a single gateway, use the following command:

```
Admin@nodename# show network gateway <gateway-name>
```

Routing Configuration

This section describes how to configure routing using the CLI. These settings are applied at the **network routes** level.

To add a new static route, use the following command:

```
Admin@nodename# create network routes <parameters>
```

Specify the parameters:

Parameter	Description
enabled	Enable/disable usage of a static route: • **on** • **off**

Parameter	Description
name	Route name.
description	Route description.
node-name	Select a cluster node to configure routing.
type	Route type: • **unicast**: the standard route type. Forwards the traffic destined for the specified address via the specified gateway. • **unreachable**: drops the traffic. and sends the "Host unreachable" (type 3 code 1) ICMP message to the source. • **prohibit**: drops the traffic. and sends the "Host unreachable" (type 3 code 13) ICMP message to the source. • **blackhole**: drops the traffic without informing the source that the data did not reach the recipient.
destination-ip	IP address of the destination subnet, format: <ip/mask>.
gateway	IP address of the gateway through which the specified subnet will be reachable. The IP address must be reachable from the device.
interface	Interface through which the route is added.
metric	Route metric. The lower the metric, the higher the priority of the route (if there is more than one route to a network).

Example of adding a static route:

```
Admin@nodename# create network routes name test_route description "Test
static route" destination-ip 192.168.200.0/2
4 gateway 192.168.100.100 interface port1 type unicast metric 1 enabled
on
Admin@nodename#

Admin@nodename# show network routes test_route

name              : test_route
description       : Test static route
```

```
enabled           : on
node-name         : testnode1
interface         : port1
type              : unicast
destination-ip    : 192.168.200.0/24
gateway           : 192.168.100.100
metric            : 1
```

To change the parameters of an existing static route, use the following command:

```
Admin@nodename# set network routes <route-name>
```

The parameters available to change are listed in the table above.

To delete a static route, use the following command:

```
Admin@nodename# delete network routes <route-name>
```

Example of deleting a static route:

```
Admin@nodename# delete network routes test_route
```

To display static routes, use the following command:

```
Admin@nodename# show network routes
```

DNS Configuration

You configure system DNS servers at the **network dns system-dns-servers** level.

To add new DNS servers or update the list of existing ones, use the following commands:

```
Admin@nodename# set network dns system-dns-servers ip [ <ip> <ip> ... ]
```

To delete the entire list of DNS server addresses, use the following command:

```
Admin@nodename# delete network dns system-dns-servers
```

To delete individual servers, use the following command:

```
Admin@nodename# delete network dns system-dns-servers ip [ <ip>
<ip> ... ]
```

To display the list of system DNS servers, use the following command:

```
Admin@nodename# show network dns
```

CONFIGURING LIBRARIES

Configuring Libraries (Description)

Configuring IP addresses

This section is located at the **libraries ip-list** level.

To create an IP address group, use the following command:

```
Admin@nodename# create libraries ip-list <parameters>
```

Provide the following parameters:

Parameter	Description
name	Address list name.
description	List description.
threat-lvl	

Parameter	Description
	Threat level: • **very-low**: very low threat level • **low**: low threat level • **medium**: medium threat level • **high**: high threat level • **very-high**: very high threat level.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
lists	Select existing IP lists to add to the list being created.
ips	IP addresses or a range of IP addresses to include in the list. Format: <ip>, <ip/mask>, or <ip_range_start-ip_range_end>.
use-in-search-queries	Should the list be used in search queries: • **on** • **off**

To edit a list (parameters available to update are identical to those used to create a list), use the following command:

```
Admin@nodename# set libraries ip-list <ip-list-name> <parameters>
```

To add new addresses to a list, use the following command:

```
Admin@nodename# set libraries ip-list <ip-list-name> [ <ip1>
<ip2> ... ]
```

To delete an entire address list or individual IP addresses it contains, use the following commands:

```
Admin@nodename# delete libraries ip-list <ip-list-name>
Admin@nodename# delete libraries ip-list <ip-list-name> ips [ <ip1>
<ip2>... ]
```

To display information about all existing lists, use the following command:

```
Admin@nodename# show libraries ip-list
```

To display information about an individual list, specify the IP address list name:

```
Admin@nodename# show libraries ip-list <ip-list-name>
```

To display the contents of an IP address list, use the following command:

```
Admin@nodename# show libraries ip-list <ip-list-name> items
```

Configure Browser Useragents

This section is located at the **libraries useragents** level.

To create a browser useragent list, use the following command:

```
Admin@nodename# create libraries useragents <parameters>
```

Provide the following parameters:

Parameter	Description
name	The list name.

Parameter	Description
description	List description.
patterns	The useragent description string. A comprehensive list of useragent strings can be found here: http://www.useragentstring.com/pages/useragentstring.php.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
use-in-search-queries	Should the list be used in search queries: • **on** • **off**

To edit a list (parameters available to update are identical to those used to create a list), use the following command:

```
Admin@nodename# set libraries useragents <list-name> <parameters>
```

To delete an entire list of useragents or individual useragents from the list by pattern, use the following commands:

```
Admin@nodename# delete libraries useragents <list-name>
Admin@nodename# delete libraries useragents <list-name> <patterns>
```

To display information about all existing lists, use the following command:

```
Admin@nodename# show libraries useragents
```

To display the details for a specific list, specify its name:

```
Admin@nodename# show libraries useragents <list-name>
```

You can also view the contents of a specific useragent list:

```
Admin@nodename# show libraries useragents <list-name> patterns
```

Configuring content types

This section is located at the **libraries content-types** level.

To create a content type list, use the following command:

```
Admin@nodename# create libraries content-types <parameters>
```

Provide the following parameters:

Parameter	Description
name	The list name.
description	List description.
mime	The data in the MIME format. A list of content types and their descriptions can be found at this link: https://www.iana.org/assignments/media-types/media-types.xhtml.
type	List type: • **local**: local

Parameter	Description
	• **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
use-in-search-queries	Should the list be used in search queries: • **on** • **off**

To edit a list (parameters available to update are identical to those used to create a list), use the following command:

```
Admin@nodename# set libraries content-types <list-name> <parameters>
```

To delete an entire list of content types or individual content types from the list, use the following commands:

```
Admin@nodename# delete libraries content-types <list-name>
Admin@nodename# delete libraries content-types <list-name> mime
[ <mime1> <mime2>... ] ]
```

To display information about all existing lists, use the following command:

```
Admin@nodename# show libraries content-types
```

To display the details for a specific list, specify its name:

```
Admin@nodename# show libraries content-types <list-name>
```

You can also display the content type list:

```
Admin@nodename# show libraries content-types <list-name> mime
```

Configuring URL lists

This section is located at the **libraries url-list** level.

To create a URL list, use the following command:

```
Admin@nodename# create libraries url-list <parameters>
```

Provide the following parameters:

Parameter	Description
name	The list name.
description	List description.
case-sensitivity	URL case sensitivity: • **sensitive**: sensitive to the case of letters in the address. • **insensitive**: insensitive to the case of letters in the address. • **domain**: list of domain addresses.
urls	URLs to add to the list.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format.

Parameter	Description
	Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
use-in-search-queries	Should the list be used in search queries: • **on** • **off**

To edit a list (parameters available to update are identical to those used to create a list), use the following command:

```
Admin@nodename# set libraries url-list <list-name> <parameters>
```

To delete an entire URL list or individual URLs from the list, use the following commands:

```
Admin@nodename# delete libraries url-list <list-name>
Admin@nodename# delete libraries url-list <list-name> urls [ <url1>
<url2>... ] ]
```

To display information about all existing lists, use the following command:

```
Admin@nodename# show libraries url-list
```

To display the details for a specific list, specify its name:

```
Admin@nodename# show libraries url-list <list-name>
```

To display the contents of a URL list, use the following command:

```
Admin@nodename# show libraries url-list <list-name> urls
```

Configuring email addresses

This section is located at the **libraries email-list** level.

To add a new email group, use the following command:

```
Admin@nodename#& create libraries email-list <parameter>
```

Specify the parameters:

Parameter	Description
name	Email group name.
description	Email group description.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples:

Parameter	Description
	"2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
emails	Emails to add to the group.

To edit information about an email group, use the following command:

```
Admin@nodename# set libraries email-list <email-list-name> <parameter>
```

The parameters available to update are the same as those for creating an email group.

To delete a group or individual emails from it, use the following commands:

```
Admin@nodename# delete libraries email-list <email-list-name>
Admin@nodename# delete libraries email-list <email-list-name> emails
[ <email> ... ]
```

To view information about all existing groups, about individual groups, or about emails in a group, use the following commands:

```
Admin@nodename# show libraries email-list
Admin@nodename# show libraries email-list <email-list-name>
Admin@nodename# show libraries email-list <email-list-name> emails
```

Configuring phones

The **Phones** section is configured at the **libraries phone-list** level.

To create a phone group, use the following command:

```
Admin@nodename# create libraries phone-list <parameter>
```

Provide the following parameters:

Parameter	Description
name	Phone group name.
description	Phone group description.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
phones	Phones to add to the group.

To edit information about a phone group, use the following command:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

The parameters available to update are listed in the table above.

To delete a group or individual phones from it, use the following commands:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
Admin@nodename# delete libraries phone-list <phone-list-name> phones
[ <phone> ... ]
```

To view information about all existing groups, use the following command:

```
Admin@nodename# show libraries phone-list
```

To view information about an individual phone group, use the following command:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

To display phones included in a group, use the following command:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Configure Commands

Use this section to create groups of commands to be sent to the connectors.

To create a command list, use the following command:

```
Admin@nodename# create libraries commands-list name <command-list-name>
type <local | updatable> commands new <command-string>
```

To edit the existing command list, use the following command:

```
Admin@nodename# set libraries commands-list <command-list-name>
commands <command-string>
```

To view the existing command list, use the following command:

```
Admin@nodename# show libraries commands-list <command-list-name>
```

To delete the existing command list or individual commands in the list, use the following command:

```
Admin@nodename# delete libraries commands-list <command-list-name>
```

```
Admin@nodename# delete libraries commands-list <command-list-name>
commands <command-string>
```

Configuring notification profiles

You configure notification profiles for SMTP (via email) and SMPP (via SMS) at the **libraries notification-profiles** level.

To add a new SMTP notification profile:

```
Admin@nodename# create libraries notification-profiles smtp <parameter>
```

Specify the following parameters:

Parameter	Description
name	Profile name.
description	Profile description.
host	The IP address or FQDN of the SMTP server that will be used for sending emails.
port	The TCP port used by the SMTP server. Usually, SMTP uses port 25, and SMTP with SSL uses port 465. Consult your email server administrator regarding this value.
connection-security	The following outgoing email security options are available: • **none**. • **starttls**. • **ssl**.
authentication	Enable/disable authorization when connecting to the SMTP server: • **on** • **off**
login	Login name to connect to the SMTP server.
password	Password to connect to the SMTP server.

To create an SMS (SMPP) notification profile, use the following command:

```
Admin@nodename# create libraries notification-profiles smpp <parameter>
```

Provide the following parameters:

Parameter	Description
name	Profile name.
description	Profile description.
host	IP address or FQDN of an SMPP server to use to send SMS.
port	TCP port to use to connect to the SMPP server. Usually, the port used for the SMPP protocol is 2775, when using SSL — 3550.
ssl	Enable/disable SSL encryption: • **on** • **off**
login	The account name for connecting to the SMPP server.
password	The account password for connecting to the SMPP server.
phone-translation-rules	Phone translation rules. These rules are used to ensure that the provider requirements are met. For example, to replace all numbers starting with +7 to 8, use the following command: `Admin@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [ +7¦8 ]`
source-ton	Type of number for the event source: • **0**: unknown • **1**: international • **2**: national • **3**: network specific • **4**: subscriber number • **5**: alphanumeric

Parameter	Description
	• **6**: abbreviated.
dest-ton	Type of number for destination: • **0**: unknown • **1**: international • **2**: national • **3**: network specific • **4**: subscriber number • **5**: alphanumeric • **6**: abbreviated.
source-npi	Numbering Plan Indicator for the source: • **0**: Unknown. • **1**: ISDN/telephone numbering plan (E.163/E.164) • **3**: data numbering plan (X.121) • **4**: telex numbering plan (F.69) • **6**: land Mobile (E.212) • **8**: national numbering plan • **9**: private numbering plan • **10**: ERMES numbering plan (ETSI DE/PS 3 01-3) • **13**: Internet (IP). • **18**: WAP Client Id (to be defined by WAP Forum).
dest-npi	Numbering Plan Indicator for the destination: • **0**: Unknown. • **1**: ISDN/telephone numbering plan (E.163/E.164) • **3**: data numbering plan (X.121) • **4**: telex numbering plan (F.69) • **6**: land Mobile (E.212) • **8**: national numbering plan • **9**: private numbering plan • **10**: ERMES numbering plan (ETSI DE/PS 3 01-3) • **13**: Internet (IP). • **18**: WAP Client Id (to be defined by WAP Forum).

To edit a notification profile, use the following command:

```
Admin@nodename# set libraries notification-profiles <smtp | smpp>
<profile-name> <parameter>
```

SMTP and SMPP profile parameters available to change are listed in the respective tables above.

To delete a profile, use the following command:

```
Admin@nodename# delete libraries notification-profiles <smtp | smpp>
<profile-name>
```

You can also delete phone translation rules from SMPP notifications:

```
Admin@nodename# delete libraries notification-profiles smpp <profile-
name> phone-translation-rules [ phone1¦phone2 ]
```

To display information about all existing notification profiles, use the following command:

```
Admin@nodename# show libraries notification-profiles
```

To display information about all notification profiles of a specific type, use the following command:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp>
```

To display information about an individual notification profile, use the following command:

```
Admin@nodename#show libraries notification-profiles <smtp | smpp>
<profile-name>
```

Configure Triggered Alert Categories

The **Triggered alert categories** library item allows you to create categories that can be used to group certain triggers of analytics rules applied to events. For more

details on analytics rules, see the Analytics section. The following predefined categories exist:

- **Availability**: analytics rules defining incidents that degrade the availability of information systems.
- **Performance**: analytics rules defining incidents that degrade the performance of information systems.
- **Security**: analytics rules defining incidents that degrade the security of information systems.

To create triggered alert categories, use the following command:

```
Admin@nodename# create libraries alert-categories name <category-name>
key <category-key>
```

To edit triggered alert categories, use the following command:

```
Admin@nodename# set libraries alert-categories name <category-name> key
<category-key>
```

To view the existing triggered alert categories, use the following command:

```
Admin@nodename# show libraries alert-categories name <category-name>
```

To delete the existing triggered alert categories, use the following command:

```
Admin@nodename# delete libraries alert-categories name <category-name>
```

Configure External Enrichment Services

The External enrichment services library item represents resources used to collect additional threat information. These sources provide feeds, which are structured, processed data on IP addresses and domains, from which malicious files are distributed along with the corresponding file samples and hashes; lists of phishing websites and the email addresses of phishing message senders; addresses, from which networks are scanned for vulnerabilities; IP addresses, from which brute force attacks are launched; and malware detection signatures. For more on the available

services, see the External Enrichment Services section of the SIEM Administrator Guide.

To use enrichment services, they need to be enabled. For some of the enrichment services, the user needs to register and provide an access key.

To edit external enrichment services, use the following command:

```
Admin@nodename# set libraries enrichment-services <service-name>
```

To view external enrichment services, use the following command:

```
Admin@nodename# show libraries enrichment-services <service-name>
```

Configuring Syslog filters

Syslog filters are created and configured at the **libraries syslog-filters** level.

To create a syslog filter, use the following command:

```
Admin@nodename# create libraries syslog-filters <parameter>
```

Specify the following parameters:

Parameter	Description
name	Filter name.
description	Filter description.
login-address	String used to look up user IP address in syslog message.
login-event	String used to look up user login event in syslog message.
login-username	String used to look up username in syslog message.
logout-address	String used to look up user IP address in syslog message.
logout-event	String used to look up user logout event in syslog message.
logout-username	String used to look up username in syslog message.

To edit information on a syslog filter, use the following command:

```
Admin@nodename# set libraries syslog-filters <filter-name> <parameter>
```

Parameters which could be updated are the same parameters which are specified when creating a filter.

To display information on a syslog filter, use the following command:

```
Admin@nodename# show libraries syslog-filters <filter-name>
```

To remove a syslog filter, use the following command:

```
Admin@nodename# delete libraries syslog-filters <filter-name>
```

Configuring syslog Applications

You configure syslog applications at the **libraries syslog-application** level.

The command for creating the syslog applications:

```
Admin@nodename# create libraries syslog-application <parameter>
```

Specify the following parameters:

Parameter	Description
name	Application name.
description	Application description.
app-name	The name of the application displayed in the logs.

SETTING UP SENSORS

Sensor Configuration (Description)

SIEM uses sensors to collect information from various devices for subsequent analysis. A sensor is a SIEM-compatible device that can send certain data to a SIEM server. A sensor can be a UserGate NGFW device, a UserGate Client endpoint, or any other network device that supports SNMP data transfer.

UserGate Sensors

A UserGate sensor connects a single UserGate firewall device to SIEM. To connect a UserGate sensor, follow these steps:

1. On **NGFW** allow the **Log Analyzer** and **SNMP** services in the required zone settings:

```
Admin@ngfw-nodename# set network zone <zone-name> enabled-services
[ SNMP "Log Analyzer" ]
```

2. On **NGFW**, receive the device token:

```
Admin@ngfw-nodename# show settings general log-analyzer

state              : ready
logan-server       : 127.0.0.1
logan-version      : 7.1.0.
device-version     : 7.1.0.
device-code        : 9R4FCVET
```

3. In SIEM, allow the **Log database** service in the required zone properties:

```
Admin@nodename# set network zone <zone-name> enabled-services [ "Log
Analyzer" ]
```

4. Create a UserGate sensor.

To create a UserGate sensor, use the following command:

```
Admin@ndefornaledo# create sensors ug-sensors <parameters>
```

Specify the following parameters:

Parameter	Description
enabled	Enables or disables this UserGate sensor.
name	The name of the UserGate sensor.
description	An optional description of the UserGate sensor.
address	The IP address of the UserGate node for which this sensor is being created.
SIEM-address	The IP address of the SIEM server that will be used on the UserGate node as the destination for logs. Only those IP addresses are available for selection that are assigned to interfaces in the zones where the Log Analyzer service is allowed.
device-code	The token received on the UserGate node.

After creating a sensor, the UserGate node starts sending data to SIEM.

To view UserGate sensors, use the following command:

```
Admin@nodename# show sensors ug-sensors
```

SNMP Sensors

Using an SNMP sensor, the administrator can connect an SNMP-compatible network device to a SIEM server to collect and analyze its metrics. SIEM can display any counters received over SNMP using SNMP queries. To configure an SNMP sensor, you need to have MIBs (Management Information Bases) for the managed device.

To configure an SNMP sensor, follow these steps:

1. Upload the MIB for the device that you want to add for monitoring.

2. Create an SNMP sensor.

```
Admin@nodename# create sensors snmp-sensors <parameters>
```

Next, specify the following parameters:

Name	Description
enabled	Enables or disables this SNMP sensor.
name	The name of the SNMP sensor.
description	An optional description of the SNMP sensor.
ip	The IP address of the SNMP sensor.
port	The port number for the SNMP sensor. Normally, TCP port 161 is used for SNMP data queries.
version	The SNMP protocol version to be used with this sensor. Available options: SNMP v2 (**2**) and SNMP v3 (**3**).
community	SNMP community is a string that identifies the SIEM server and network device for SNMP v2. Use only Latin letters and numbers.
interval	The time interval in seconds with which the SIEM server will receive data from the network device.
username	For SNMP v3 only. The username used for authentication on the network device.
auth-type	The authentication mode. The available options are: • No authentication, no encryption (**none**). • Authentication, no encryption (**no-encrypt**). • Authentication, encryption (**encrypt**).
auth-alg	The algorithm used for authentication: • **md5** • **sha** • **sha224** • **sha256** • **sha284**; • **sha512**
auth-password	The password used for authentication.
encrypt-alg	The algorithm used for encryption. DES or AES can be used.
encrypt-password	The password used for encryption.

Name	Description
counters	Specify all data here that SIEM should query from the network device. The counters can be selected from the MIBs uploaded to the device. Put the SNMP OID counter in square brackets [].

To view SNMP sensors, use the following command:

```
Admin@nodename# show sensors snmp-sensors
```

WMI Sensors

Using an WMI sensor, the administrator can connect a WMI-compatible network device (a computer running Windows) to SIEM to collect and analyze its metrics.

To create a WMI sensor, use the following command:

```
Admin@nodename# create sensors wmi-sensors <parameters>
```

Next, specify the following parameters:

Name	Description
enabled	Enables or disables this sensor.
name	Sensor name.
description	An optional description of the sensor.
ip	Sensor IP address.
login	The username for connecting to the device.
password	The user's password for connecting to the device.
namespace	ID namespace.
polling-interval	Polling interval in seconds.
counters	Specify the data which will be monitored by SIEM on the network device: • **name**: the counter name.

Name	Description
	• **type**: the counter type (windows-event-logs). • **filter-query**: WQL request (for example, Logfile='Security').

To view WMI sensors, use the following command:

```
Admin@nodename# show sensors wmi-sensors
```

Endpoint devices

An endpoint with the UserGate Client software installed is displayed when this SIEM device is selected on UGMC as a server for transmitting event information, while SIEM must be pre-registered on UGMC (read more in the LogAn Device Management section).

To view the endpoint data, run the following command:

```
Admin@nodename# show sensors endpoint-devices
```

Connectors

Connectors are used to allow the SIEM device to be connected to various security tools to collect information.

To add a connector, use the following command:

```
Admin@nodename# create sensors connectors <parameters>
```

You need to specify the following data:

Parameter	Description
name	Connector name.
description	An optional description of the connector.
server-type	

Parameter	Description
	Select the server type: • **SSH** • **HTTP** • **HTTPS**
address-format	Type: • **ip** • **fqdn**
ip	The server's IP address. Specify it if the **IP** server type is selected.
port	The server's port. Specify it if the **IP** server type is selected.
fqdn	The server's FQDN. Specify it if the **FQDN** server type is selected.
url-path	Used to manage a device via API.
login	User login for connector authorization.
password	Password to the user account required for connector authorization.
connamd-group	You can only specify a command group for a SSH server; see the Commands section for details.
headers	You can only specify headers for HTTP and HTTPS servers.

To edit the existing connector, use the following command:

```
Admin@nodename# create sensors connectors <connector-name> <parameters>
```

To view parameters of connectors created earlier, use the following command:

```
Admin@nodename# show sensors connectors <connector-name>
```

To remove previously created connectors, use the following command:

```
Admin@nodename# delete sensors connectors <connector-name>
```

SETTING UP MONITORING

Configuring Device Monitoring Settings

Configuring device monitoring parameters in the CLI interface is done in configuration mode at the **monitoring** level. Commands at this level allow you to manage the configuration of SNMP device parameters, SNMP monitoring rules, security profiles for authenticating SNMP managers, and notification rules. Read more about monitoring and notification rules in the Notifications section.

Configuring SNMP Device Parameters

To configure the SNMP device parameters, use commands at the **monitoring smnp-parameter** level:

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

You can edit the following parameters:

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

Parameter	Description
	• **mac**: MAC address • **text**: text • **octets**: octets

Read more about the SNMP parameters of the UserGate device in the SNMP section.

Configuring SNMP Monitoring Rules

To configure device monitoring rules via SNMP, commands are used at the **monitoring snmp** level:

```
Admin@nodename# edit monitoring snmp <parameters>
```

You can edit the following parameters:

Parameter	Description
name	The name of the rule.
enabled	Enable/disable a rule
community	SNMP community: the string for UserGate server identification and SNMP management server identification for SNMP v2c. Use only Latin letters and numbers.
context	Optional parameter that defines the SNMP context. Use only Latin letters and numbers. Some devices may have multiple copies of the entire MIB subtree. For example, several virtual routers can be created on the device. Each such virtual router will have a complete MIB subtree. In this case, each virtual router can be specified as a context on the SNMP server. The context is identified by name. When the client makes a request, the context name can be specified. If the context name is not specified, the default context will be requested.
version	Specify the version of the SNMP protocol used in the rule. Available options: SNMP v2c and SNMP v3.
query	When enabled, allows receiving and processing of SNMP requests from the SNMP manager.

Parameter	Description
trap	When enabled, allows sending of SNMP traps to the server configured to receive notifications.
trap-host	Server IP address for traps. This setting is required only if you need to send traps to the notification server.
trap-port	The port on which the server listens for notifications. Usually, it is UDP port 162. This setting is required only if you need to send traps to the notification server.
security-profile	For SNMP v3 only. For more details, see the SNMP Security Profiles section.
events	Selecting the types of parameters available for monitoring by rule.

For the SNMP manager to work with the UserGate device, it is necessary to enable the **SNMP** service in the access control settings in the zone properties of the interface to which the connection will be made via the SNMP protocol. For more information about setting up zones in the CLI, see the Network Settings section.

Configuring SNMP Security Profiles

To configure security profiles to authenticate SNMP managers, use commands at the **monitoring smnp-security-profile** level:

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

You can edit the following parameters:

Parameter	Description
name	SNMP security profile name
description	SNMP security profile description
username	User name to authenticate the SNMP manager.
auth-type	Select an authentication mode for the SNMP manager. The available options are: • **none**: no authentication, no encryption • **no-encrypt** : authentication, no encryption • **encrypt**: authentication, encryption

Parameter	Description
	The authPriv mode is considered the most secure.
auth-alg	The algorithm used for authentication. Possible to use: • **sha** • **md5** • **sha224** • **sha256** • **sha384** • **sha512**
auth-password	The password used for authentication.
encrypt-alg	The algorithm used for encryption. DES or AES can be used.
encrypt-password	The password used for encryption.

Configuring Notification Rules

To configure alert rules, use commands at the **monitoring alert-rules** level:

```
Admin@nodename# edit monitoring alert-rules <parameters>
```

You can edit the following parameters:

Parameter	Description
enabled	Enables/disables the rule.
name	The name of the rule.
description	A description of the rule.
notification-profile	A previously created notification profile.
sender	From whom the notifications will come.
subject	Notification subject.
timeout	The timeout during which the server will not send a message when this rule is triggered again. This setting prevents a flood of messages when an alert rule is triggered frequently.

Parameter	Description
events	Events for which you want to receive alerts.
phones	For SMPP profiles, The phone groups to which SMS notifications will be sent.
emails	For SMTP profiles. The groups of email addresses to which email notifications will be sent.

CONFIGURING INCIDENTS

Incident Configuration (Description)

The **Incidents** section provides access to the functionality of UserGate SIEM's built-in IRP (Incident Response Platform) system. An incident is a cybersecurity event or a set of cybersecurity events needing investigation. UserGate SIEM allows you to customize the incident investigation process to the needs of a specific company.

You can find more details on IRP system's functionality in the Incidents section of the SIEM User Guide.

Incident settings in the CLI are configured at the **incident** level.

To create a custom incident investigation schema, you must:

1. Create the desired incident resolutions.
2. Create incident types.
3. Create incident states.
4. Create an incident schema.
5. Activate the incident schema.

To create an incident resolution, use the following command:

```
Admin@nodename# create incident resolutions name <incident-name>
description <incident-description>
```

To create incident types, use the following command:

```
Admin@nodename# create incident types name <incident-type-name>
description <incident-type-description>
```

To create an incident state, use the following command:

```
Admin@nodename# create incident states name <incident-state-name>
description <incident-state-description> group <open|closed|progress>
```

To create an incident schema, use the following command:

```
Admin@nodename# create incident schema <parameters>
```

The following incident schema parameters are available for editing:

Parameter	Description
name	Scheme name.
description	Scheme description.
prefix	The prefix that will be used when assigning identifiers to created incidents. The identifier will have the following format: prefix - sequential number, for example, INC-99.
initial-state	The initial state an incident takes when it is created.
workflow-states	Workflow states: all states that the incident can take during its lifecycle.
incidents-resolutions	Incident resolutions: the list of the possible incident resolutions.
incidents-types	Incident types that can be used with this schema.
transition	All possible transitions between states.

The **set** (edit), **show**, and **delete** commands are also available for all stages of incident scheme creation.

CONFIGURING ANALYTICS

Configuring Analytics (Description)

UserGate SIEM allows you to analyze security event logs received from configured sensors. All data is stored in a single database, making it possible to perform complex searches, correlate repetitive events, aggregate them into security incidents, and simplify the process of incident investigation. You can find more details on SIEM architecture and operation principles in the Analytics section of the SIEM Administrator Guide.

The CLI interface allows you to create and configure analytics rules and response actions. Using analytics rules, security engineers can automate the process of event correlation and triggering, as well as assign specific system responses to triggered events. All of this makes it easier to investigate logged events and contributes to reducing the time between problem detection and resolution.

Analytics rules and response actions in the CLI are created and configured at the **analytics** level.

Analytics rules

Log events are processed using analytics rules. By configuring analytics rules, you can perform complex searches on cybersecurity events. The rule is triggered when events from different sources are found to be correlated.

To create an analytics rule, use the following command:

```
Admin@nodename# create analytics analytics-rules <parameters>
```

Provide the following parameters:

Parameter	Description
enabled	**on**/**off**: enable or disable the real-time triggering of the analytics rule.
name	The name of the analytics rule.
description	A description of the analytics rule.

Parameter	Description
threat-level	The threat level that will be displayed when the rule is triggered. • **informational**: the events present a very low threat level, and the administrator may choose not to take any action; • **low**: the events present a low threat level, and the administrator may choose not to take any action. • **medium**: the events that trigger the analytics rule require attention. • **high**: the events require investigation and response. • **critical**: the events require investigation and urgent response.
priority	The priority assigned to triggered alerts for this analytics rule: • **low**: low response priority. • **normal**: needs attention and may need response. • **important**: needs attention and response. • **critical**: requires urgent response. When the analytics rule is triggered, the priority will indicate the severity of the triggered alert.
alert-category	The category to which the triggered alert belongs. The following predefined categories are available: • **security**: incidents that degrade the security of information systems. • **availability**: incidents that degrade the availability of information systems. • **performance**: incidents that degrade the performance of information systems. Additional trigger categories can be created in the **Trigger categories** library. For more details, see the Configure Triggered Alert Categories section.
timezone	The timezone that analytics rules will use (because the server can collect data from sources located in different timezones).
response-actions	Select response actions that will be executed automatically when an analytics rule is triggered. For more information on creating and configuring response actions, see the Response Actions section.
conditions	Specify rule trigger conditions.

The trigger conditions specified when creating an analytics rule have the following configuration options:

Parameter	Description
name	The name of the analytics rule condition.
description	Description of the analytics rule condition.
condition-time-enabled	Enable or disable the time limit for evaluating this condition. If the time limit is enabled, the analytics rule will be triggered only if the condition is matched the specified number of times within that time period.
condition-time	The time period within which the condition must be matched the specified number of times for the analytics rule to be triggered. The time is set in seconds. Specifying the condition execution time is available when the **c ondition-time-enabled** parameter is enabled.
break-query-enabled	Enable/disable the use of a stop query in an analytics rule.
break-query	An SQL-like stop search query is executed along with the condition query. To formulate a query, use field names, field values, keywords, and operators (set similarly to a filter query). If, when performing an analysis, at least one record is found that matches the specified stop query, before the specified number of events that match the condition of the analytics rule are found, then the analytics rule will not work, and the counter for the number of records found before the stop query is executed will be reset.
filter-query	An SQL-like condition search query against the log database. To formulate a query, use field names, field values, keywords, and operators. For the query syntax, refer to the section Data Search and Filtering. The query can also be written using Google/RE2 syntax in the MATCH operator. Learn more about Google/RE2 syntax in the MATCH operator: https://github.com/google/re2/wiki/Syntax.
group-by	The list of parameters by which rules can be grouped as a result of a triggered alert. The fields will be displayed when triggered alert details are viewed. The parameters that can be used for grouping are described in the Analytics Search section. When specifying categories for grouping, the analytics rule will only be triggered if the condition is met for the selected

Parameter	Description
	category the specified number of times, as specified in the **pattern-repeats** parameter field.
pattern-repeats	How many times the condition must be matched for the rule to be triggered. This parameter can be used with or without the **condition-time-enabled** parameter.

The following commands are also available for analytics rules: **set** (edit), **show**), and **delete**.

Response Actions

Response actions determine how to respond when cybersecurity analytics rules are triggered. You can use the UserGate SIEM to flexibly customize rules with variables of analytics rule triggering categories.

To create a response action, use the following command:

```
Admin@nodename# create analytics response-actions <parameters>
```

Provide the following parameters:

Parameter	Description
enabled	on/off: enable/disable the response rule.
name	Name of the response rule.
description	A description of the response rule.
action	The action that should be taken when the analytics rule is triggered. Will be applied if specified in the analytics rule properties. The following response actions are available: • **send-email**: send an email to the selected addresses. The procedure of configuring the **Send email** action will be discussed later in the Send Email Action section. • **send-message**: sends a message to the specified phone numbers. The procedure of configuring the **Send message** action will be discussed later in the Send Message Action section. • **webhook**: receive an alert on the rule trigger on the webpage whose address is specified in the action

Parameter	Description
	settings. The procedure of configuring the **Webhook** action will be discussed later in the Webhook Action section. • **create-incident**: automatically create an incident when the analytics rule is triggered. The procedure of configuring the **Create incident** action is described in the Incident Settings section. • **send-command-to-connector**: send a command to the selected connector. The procedure of configuring the "Send command to connector" action is described in the Send command to connector action section. • **send-command-to-endpoint** send a command to an endpoint with UserGate Client software installed. For more information, see the Send Command to Endpoint Action section.
enable-logging	Enables or disables the logging of response action triggers. The data is recorded in the SIEM event log.
grouping	When configuring response actions, you can enable the grouping of triggered alerts for convenience. The following grouping options are available: • **never**: never. • **period** : the response action will be performed if at least one triggered alert occurs during the specified period of time. • **number** : the response action will be performed only after the specified number of triggered alerts.
time-period	The grouping time period in minutes. This setting is available only when grouping for a period of time is selected.
alerts-number	The number of triggered alerts required for the grouping to happen. This setting is available only when grouping by the number of triggered alerts is selected.

The **set** (edit), **show**, and **delete** commands are also available for responce actions.

Send Email Action

If you selected Send email as the response action, provide the following settings in the rule properties.

Name	Description
notification-profile	The SMTP notification profile to be used for sending emails. For more details on configuring SMTP profiles, see the Configuring Notification Profiles section.
sender	The sender name.
subject	The email subject.
emails	The list of recipient email addresses. Recipients must be added to lists in the item library. For information on adding email addresses, see Configuring Email Addresses.
template	The alert email template that can include the values of various variables related to the triggered alert. For more details, see the Alert Template and Notification and command variables sections.

Send Message Action

If you selected Send Message as the response action, provide the following settings in the rule properties.

Name	Description
notification-profile	The SMPP notification profile to be used for sending messages. For more details on configuring SMPP profiles, see the Configuring Notification Profiles section.
sender	The sender name.
phones	The list of recipient phone numbers. Recipients must be added in the item library. For more details on adding phone numbers, see the Configuring Phones section.
template	The message template that can include the values of various variables related to the triggered alert. For more details, see the Alert Template and Notification and command variables sections.

Webhook Action

To configure a webhook in the response action rule properties, provide the following settings.

Name	Description
url	The URL of the website where notifications about rule triggers will be displayed.
template	The alert template that can include the values of various variables related to the triggered alert. For more details, see the Alert Templateand Notification and command variables sections.

You can test the webhook feature using this service: https://webhook.site. To do that, go to the Webhook.site website and copy the generated link. and paste it into the **url** field of the **action** parameter of the response action rule properties.

Send Command to Connector Action

You can configure a response action of sending a command to a connector.

The following parameters must be specified for a response action of sending a command to be executed on a connector:

Name	Description
connectors	Select the devices to which the command should be sent when an analytics rule is triggered. The connector must be added and configured in advance. For more information, see the Connectors section. **Important!** Only connectors with the same command group can be selected.
command	Specify the command that will be sent to the connector for execution; the commands of the group specified for the selected connectors are available. If there are variables in the command, additional fields will be displayed where values should be specified. See Commands for more details on the commands.

Send Command to Endpoint Action

You can configure a response action of sending a command to a device with the UserGate Client software installed. Available commands:

- **block**: blocking access to the Internet.
- **kill**: terminate the process specified in the filter query.

Alert Template

The **template** parameter must contain the notification text. In addition to fixed test, you can send data related to the triggered alert or its log records.

To send data related to the triggered alert, enter the corresponding parameter name from the table into the **template** field. For example, if you enter **{ANALYTICS_RULE_NAME}**, the email, SMS, or webhook alert text will show the name of the triggered analytics rule. If you fill in the template at the time of configuring the **Create incident** action, the text will be displayed in the incident description.

DASHBOARD

Dashboard (Description)

This section allows you to view the current state of the Log Analyzer server and servers connected to it for sending logs as well as the servers' boot status, license status, and more.

Reports are presented as widgets, which can be customized by the system administrator as required. You can add, delete, move, and resize widgets on the **Dashboard** page. By default, pages with widgets UserGate SIEM (displaying the status of the SIEM server), NOC (Network Operation Center) and SOC (Security Operation Center), Triggers (triggering of analytics rules) are created.

Some widgets allow you to customize the display, specify data filtering, and configure other settings. To configure a widget, click the gearwheel icon in the upper right corner. Not all parameters listed below are available for every type of widget.

Name	Description
Name	Name of widget to display in the Dashboard.
Description	Optional widget description.
Number of records	Maximum number of records to display.
Group by	Data field by which to group the data.
Chart	

Name	Description
	Select how the data is presented. Available values: • Number • Pie chart • Column chart • Bar chart • Table • Line chart • World map
Filter query	SQL-like query string that allows you to limit the amount of information used to build a widget. To construct a query, use field names and values, keywords, and operators. For keywords and operators with examples of their use, see the Data Search and Filtering section.
Sensor	The sensor that provides data for this widget.

TECHNICAL SUPPORT

Technical Support Section

The technical support section on the company's website contains additional information on setting up the device. Here you can also submit a request to resolve any equipment issues that may arise.

ADMIN

Admin (description)

This section allows registered administrators to change their passwords, update some profile settings and log out.

Name	Description
Change password	To change your password, enter your current password and then the new one twice.
Preferences	• Show items per page: number of lines to display in one dialog box, such as a list of firewall rules. • Night mode: set the dark theme for the UGOS GUI. • Favorite filters: rename or delete filters for various logs created by this user.
Logout	End the session in the web console of the device.

FAVORITES

Favorites (Description)

The web interface allows you to filter the displayed sections by adding them to favorites and search for sections by their name. You can use filtering to hide unused sections. Displaying only the favorite sections does not affect the device functionality or configuration. To add a section to favorites, click the asterisk next to the section name. To customize the display, use the **Favorites Only** switch at the bottom of the panel.

APPLICATIONS

Network Environment Requirements

Service	Protocol	Port	Outbound/ Inbound	Function
Web console	TCP	8010	Inbound (to SIEM web console)	Access to the management web interface of a device.
CLI over SSH	TCP	2200	Inbound (to CLI over SSH)	Access to the UserGate command line interface (CLI) over SSH.
XML-RPC	TCP	4041	Inbound (to UserGate via API)	UserGate device management via API.
Remote assistance	TCP	22	Outbound (to technical support servers)	Remote access to a technical support server. Access to servers: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.
NTP	UDP	123	Outbound (to a time server)	Time synchronization.
DNS	UDP	53	Outbound (to DNS servers)	The service that resolves domain names into IP addresses.

Service	Protocol	Port	Outbound/ Inbound	Function
UserGate server registration	TCP	443	Outbound (to the registration server)	Access to the UserGate product registration server (reg2.usergate.com).
Update software and libraries	TCP	443	Outbound (to update servers)	Update software and library items: access to updates.usergate.com.
Communication with UGMC	TCP	9712	Outbound (from SIEM to UGMC)	Initial communication and exchange of encryption keys with the UGMC server.
		2022	Outbound (from SIEM to UGMC)	Build an SSH tunnel to exchange data using the received keys.
SIEM service	TCP	9713	Outbound (from SIEM to NGFW)	Initial communication and exchange of encryption keys with the NGFW server.
		2023	Outbound (from SIEM to NGFW)	Build an SSH tunnel to exchange data using the received keys.
	TCP	22699 (receive data from NGFW	Inbound (from NGFW to SIEM)	The SIEM log collection service.

Service	Protocol	Port	Outbound/ Inbound	Function
		6.x.x), 22711 (receive data from NGFW 7.x.x that uses SSL)		
SNMP	UDP	161	Inbound (to SIEM)	Access to the UserGate server via SNMP.
Log Collector	TCP/UDP	514	Inbound (to SIEM)	A service that collects information from remote devices using the Syslog protocol.
SMTP	TCP	25	Outbound (to a mail server)	Send alerts to email.
DHCP	UDP	67, 68	Outbound (IP address request from UserGate to a DHCP server)	DHCP service.
LDAP	TCP	389, 636	Outbound (to LDAP connector)	Execute LDAP requests (389 for LDAP and 636 for LDAP over SSL).
RADIUS	UDP	1812	Outbound (to a RADIUS authenticatio n server)	User authenticatio n via the RADIUS protocol.
TACACS+	TCP	49	Outbound (to a TACACS+ authenticatio n server)	User authenticatio n via the TACACS+ protocol.
FTP (logs export)	TCP	21		

Service	Protocol	Port	Outbound/ Inbound	Function
			Outbound (to an FTP server)	Export logs to an FTP server.
SSH (logs export)	TCP	22	Outbound (to an SSH server)	Export logs to an SSH server.
Syslog (logs export)	TCP/UDP	514	Outbound (to the Syslog server)	Export logs to a Syslog server.

DESCRIPTION OF LOG FORMATS

Logs Export in CEF Format

Event Log Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	events
	Origin	Module where the event occurred.	admin_console

Field type	Field name	Description	Example value
	Severity	The severity of the event.	Available values: • 1: info • 4: warning • 7: error • 10: critical
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Event type.	login_successful
	suser	The username.	Admin
	src	Source IPv4 address.	192.168.117.254
	cat	Component where the event occurred.	console_auth
	cs1Label	This field is used for event details.	Attributes
	cs1	Event details in JSON format.	{"name":"MIME_BUI LTIN_COMPOSITE", "module":"nlist_imp ort"}

Web access log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW

Field type	Field name	Description	Example value
	Device Version	Product version.	7
	Source	Log name.	webaccess
	Name	Source type.	log
	Threat Level	Threat level for the URL category.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Action taken by the device according to the configured policies.	captive
	reason	The reason why the event was created, e.g. the reason for the site block.	{"id": 39,"name":"Social Networking","threat _level":3}
	proto	Level 4 protocol used.	TCP
	app	Application layer protocol and its version.	HTTP/1.1
	suser	The username.	user_example (Unknown, if the user is unknown)

Field type	Field name	Description	Example value
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	requestMethod	Method used to access the URL address (POST, GET, etc.).	GET
	request	In the case of an HTTP request, the field contains the URL of the requested resource and the protocol used.	http://www.secure.com
	requestContext	Request source URL (HTTP referer).	https://www.google.com/
	requestClientApplication	Browser useragent.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Number of transmitted inbound bytes (data transferred from the source to the destination).	231
	out	Number of transmitted outbound bytes (data transferred from the destination to the source).	40

Field type	Field name	Description	Example value
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Default Allow
	cs2Label	Indicates the source zone.	Source Zone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the source country.	Source Country
	cs3	Source country name.	AE (a two-letter country code is displayed)
	cs4Label	Indicates the destination zone.	Destination Zone
	cs4	Destination zone name.	Untrusted
	cs5Label	Indicates the destination country.	Destination Country
	cs5	Destination country name.	AE (a two-letter country code is displayed)
	cs6Label	Indicates if the content was decrypted.	Decrypted
	cs6	Decrypted or not.	true, false
	flexString1Label	Refers to the content type.	Media type
	flexString1	The type of the content.	text/html

Field type	Field name	Description	Example value
	flexString2Label	Indicates the category of the requested URL.	URL Categories
	flexString2	URL category.	Computers & Technology
	cn1Label	Indicates the number of packets transmitted from the source to the destination.	Packets sent
	cn1	Number of packets transmitted from the source to the destination.	3
	cn2Label	Indicates the number of packets transmitted from the destination to the source.	Packets received
	cn2	Number of packets transmitted from the destination to the source.	1
	cn3Label	Specifies the server's original response.	Response
	cn3	Status code.	302

CEF Compact Web Access Log Format:

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7

Field type	Field name	Description	Example value
	Source	Log name.	webaccess
	Name	Source type.	log
	Threat Level	Threat level for the URL category.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Action taken by the device according to the configured policies.	captive
	reason	The reason why the event was created, e.g. the reason for the site block.	{"id": 39,"name":"Social Networking","threat _level":3}
	proto	Level 4 protocol used.	TCP
	app	Application layer protocol and its version.	HTTP/1.1
	suser	The username.	user_example (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.10.10

Field type	Field name	Description	Example value
	spt	Source port	Values: 0-65535.
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	requestMethod	Method used to access the URL address (POST, GET, etc.).	GET
	request	In the case of an HTTP request, the field contains the URL of the requested resource and the protocol used.	http://www.secure.com
	requestContext	Request source URL (HTTP referer).	https://www.google.com/
	requestClientApplication	Browser useragent.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Number of transmitted inbound bytes (data transferred from the source to the destination).	231
	out	Number of transmitted outbound bytes (data transferred from the destination to the source).	40
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1		Default Allow

Field type	Field name	Description	Example value
		Name of the rule triggered to cause the event.	
	cs2Label	Indicates the source zone.	SrcZone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the destination zone.	DstZone
	cs3	Destination zone name.	Untrusted
	flexString1Label	Indicates the category of the requested URL.	URLCats
	flexString1	URL category.	Computers & Technology
	cn1Label	Specifies the server's original response.	Response
	cn1	Status code.	302

Note

Some field values are truncated to 80 characters, this is a general rule for the compact format. For example, a list of URL categories, URL, username, rule name, zone name, etc.

DNS log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7

Field type	Field name	Description	Example value
	Source	Log name.	dns
	Name	Source type.	log
	Threat Level	Threat level for the URL category.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1701085036026
	deviceExternalId	The unique name of the device that generated the event.	utmcore@ntoorereaeda
	act	Action taken by the device according to the configured policies.	block
	reason	The reason why the event was created, e.g. the URL category on which the rule was triggered.	{"url_cats":[{"id":37,"name":"Search Engines & Portals","threat_level":1}]}
	proto	Level 4 protocol used.	UDP
	dhost	The destination host name, whose address is determined using the DNS server.	google.com
	app	Application layer protocol	DNS

Field type	Field name	Description	Example value
	suser	The username.	user1 (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.0.11
	spt	Source port	Values: 0-65535.
	smac	Source MAC address.	FA:16:3E:65:1C:B4
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535. Port 53 is normally used for DNS.
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Rule1
	cs2Label	Indicates the source zone.	Source Zone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the source country.	Source Country
	cs3	Source country name.	AE (a two-letter country code is displayed)
	cs4Label	Indicates the destination zone.	Destination Zone
	cs4	Destination zone name.	Untrusted
	cs5Label	Indicates the destination country.	Destination Country

Field type	Field name	Description	Example value
	cs5	Destination country name.	AE (a two-letter country code is displayed)
	cs6Label	Indicates the data being transmitted.	Data
	cs6	The transmitted data.	{"question": [{"domain":"google.com","type":"A","class":"IN"}], "answer": [{"domain":"google.com","type":"TXT","class":"IN","ttl": 5,"data":"Blocked"}, {"domain":"google.com","type":"A","class":"IN","ttl": 5,"data":"10.10.0.1"}] }
	flexString1Label	Indicates the category of the requested URL.	URL Categories
	flexString1	URL category.	Search Engines & Portals

DNS log format **CEF Compact**:

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	dns
	Name	Source type.	log
	Threat Level	Threat level for the URL category.	Available values: 2, 4, 6, 8, 10 (the set

Field type	Field name	Description	Example value
			threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1701085036026
	deviceExternalId	The unique name of the device that generated the event.	utmcore@ntoorereaeda
	act	Action taken by the device according to the configured policies.	block
	reason	The reason why the event was created, e.g. the URL category on which the rule was triggered.	{"url_cats":[{"id":37,"name":"Search Engines & Portals","threat_level":1}]}
	proto	Level 4 protocol used.	UDP
	dhost	The destination host name, whose address is determined using the DNS server.	google.com
	app	Application layer protocol	DNS
	suser	The username.	user1 (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.0.11

Field type	Field name	Description	Example value
	spt	Source port	Values: 0-65535.
	smac	Source MAC address.	FA:16:3E:65:1C:B4
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535. Port 53 is normally used for DNS.
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Rule1
	cs2Label	Indicates the source zone.	SrcZone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the destination zone.	DstZone
	cs3	Destination zone name.	Untrusted
	cs4Label	Indicates the data being transmitted.	Data
	cs4	The transmitted data.	{"question":[{"domain":"google.com","type":"A","class":"IN"}], "answer":[{"domain":"google.com","type":"TXT","class":"IN","ttl":5,"data":"Blocked"},{"domain":"google.com","type":"A","class":"IN","ttl":5,"data":"10.10.0.1"}] }

Field type	Field name	Description	Example value
	flexString1Label	Indicates the category of the requested URL.	URLCats
	flexString1	URL category.	Search Engines & Portals

Traffic log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	traffic
	Rule Type	Type of the rule triggered to cause the event.	firewall
	Threat Level	Application threat level.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Action taken by the device according to the	accept

Field type	Field name	Description	Example value
		configured policies.	
	proto	Level 4 protocol used.	TCP or UDP
	app	Triggered application name	my_app
	suser	The username.	user_example (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	smac	Source MAC address.	00:50:56:80:28:08
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	dmac	Destination MAC address.	00:50:56:80:7D:21
	in	Number of transmitted inbound bytes (data transferred from the source to the destination).	231
	out	Number of transmitted outbound bytes (data transferred from the destination to the source).	40
	sourceTranslatedAddress	Source address after reassignment (if NAT rules are configured).	192.168.174.134 (0.0.0.0 if not)

Field type	Field name	Description	Example value
	sourceTranslatedPort	Source port after reassignment (if NAT rules are configured).	Values: 0-65535 (0 if not)
	destinationTranslatedAddress	Destination address after reassignment (if NAT rules are configured).	192.226.127.130 (0.0.0.0 if not)
	destinationTranslatedPort	Destination port after reassignment (if NAT rules are configured).	Values: 0-65535 (0 if not)
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Allow trusted to untrusted
	cs2Label	Indicates the source zone.	Source Zone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the source country.	Source Country
	cs3	Source country name.	AE (a two-letter country code is displayed)
	cs4Label	Indicates the destination zone.	Destination Zone
	cs4	Destination zone name.	Untrusted
	cs5Label	Indicates the destination country.	Destination Country
	cs5	Destination country name.	AE (a two-letter country code is displayed)

Field type	Field name	Description	Example value
	cn1Label	Indicates the number of packets transmitted from the source to the destination.	Packets sent
	cn1	Number of packets transmitted from the source to the destination.	3
	cn2Label	Indicates the number of packets transmitted from the destination to the source.	Packets received
	cn2	Number of packets transmitted from the destination to the source.	1

Traffic log format **CEF Compact**:

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	traffic
	Rule Type	Type of the rule triggered to cause the event.	firewall
	Threat Level	Application threat level.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.

Field type	Field name	Description	Example value
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Action taken by the device according to the configured policies.	accept
	proto	Level 4 protocol used.	TCP or UDP
	app	Triggered application name	my_app
	suser	The username.	user_example (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	smac	Source MAC address.	00:50:56:80:28:08
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	dmac	Destination MAC address.	00:50:56:80:7D:21
	in	Number of transmitted inbound bytes (data transferred	231

Field type	Field name	Description	Example value
		from the source to the destination).	
	out	Number of transmitted outbound bytes (data transferred from the destination to the source).	40
	sourceTranslatedAddress	Source address after reassignment (if NAT rules are configured).	192.168.174.134 (0.0.0.0 if not)
	sourceTranslatedPort	Source port after reassignment (if NAT rules are configured).	Values: 0-65535 (0 if not)
	destinationTranslatedAddress	Destination address after reassignment (if NAT rules are configured).	192.226.127.130 (0.0.0.0 if not)
	destinationTranslatedPort	Destination port after reassignment (if NAT rules are configured).	Values: 0-65535 (0 if not)
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Allow trusted to untrusted
	cs2Label	Indicates the source zone.	SrcZone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the destination zone.	DstZone
	cs3	Destination zone name.	Untrusted

IDPS log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	idps
	Signature	Name of the triggered IPS signature.	BlackSun Test
	Threat Level	Signature threat level.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Action taken by the device according to the configured policies.	accept
	proto	Level 4 protocol used.	TCP or UDP
	app	Application layer protocol	HTTP

Field type	Field name	Description	Example value
	suser	The username.	user_example (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	in	Number of transmitted inbound bytes (data transferred from the source to the destination).	231
	out	Number of transmitted outbound bytes (data transferred from the destination to the source).	40
	msg	Signature threat level and name.	[2] BlackSun
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	IDPS Rule Example
	cs2Label	Indicates the source zone.	Source Zone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the source country.	Source Country
	cs3		

Field type	Field name	Description	Example value
		Source country name.	AE (a two-letter country code is displayed)
	cs4Label	Indicates the destination zone.	Destination Zone
	cs4	Destination zone name.	Untrusted
	cs5Label	Indicates the destination country.	Destination Country
	cs5	Destination country name.	AE (a two-letter country code is displayed)

IDPS log format **CEF Compact**:

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	idps
	Signature	Name of the triggered IPS signature.	BlackSun Test
	Threat Level	Signature threat level.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds	1652344423822

Field type	Field name	Description	Example value
		since January 1, 1970).	
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Action taken by the device according to the configured policies.	accept
	proto	Level 4 protocol used.	TCP or UDP
	app	Application layer protocol	HTTP
	suser	The username.	user_example (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	in	Number of transmitted inbound bytes (data transferred from the source to the destination).	231
	out	Number of transmitted outbound bytes (data transferred from the destination to the source).	40

Field type	Field name	Description	Example value
	msg	Signature threat level and name.	[2] BlackSun
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	IDPS Rule Example

SCADA log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	scada
	Name	Source type.	log
	PDU Severity	SCADA severity.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 5: very high
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica

Field type	Field name	Description	Example value
	act	Action taken by the device according to the configured policies.	accept
	app	Application layer protocol	Modbus
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Scada Rule Example
	cs2Label	Indicates the source zone.	Source Zone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the source country.	Source Country
	cs3	Source country name.	AE (a two-letter country code is displayed)
	cs4Label	Indicates the destination zone.	Destination Zone
	cs4	Destination zone name.	Untrusted
	cs5Label	Indicates the destination country.	Destination Country

Field type	Field name	Description	Example value
	cs5	Destination country name.	AE (a two-letter country code is displayed)
	cs6Label	Refers to the device information.	PDU Details
	cs6	Device details in JSON format.	{"protocol":"modbus","pdu_severity":0,"pdu_func":"3","pdu_address":0,"mb_value":0,"mb_quantity":0,"mb_payload":"AAIAAA==","mb_message":"response","mb_addr":0}

SSH inspection log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	ssh
	Name	Source type.	log
	Threat Level	Application threat level.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.

Field type	Field name	Description	Example value
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Action taken by the device according to the configured policies.	accept
	app	Application layer protocol	SSH or SFTP
	suser	The username.	user_example (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	smac	Source MAC address.	FA:16:3E:65:1C:B4
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	SSH inspection rule
	cs2Label	Indicates the source zone.	Source Zone
	cs2	Source zone name.	Trusted

Field type	Field name	Description	Example value
	cs3Label	Indicates the source country.	Source Country
	cs3	Source country name.	AE (a two-letter country code is displayed)
	cs4Label	Indicates the destination zone.	Destination Zone
	cs4	Destination zone name.	Untrusted
	cs5Label	Indicates the destination country.	Destination Country
	cs5	Destination country name.	AE (a two-letter country code is displayed)
	cs6Label	Refers to the command transmitted via SSH.	Command
	cs6	Command transmitted via SSH, in JSON format.	whoami

SSH Inspection Log Format **CEF Compact**:

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	ssh
	Name	Source type.	log

Field type	Field name	Description	Example value
	Threat Level	Application threat level.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Action taken by the device according to the configured policies.	accept
	app	Application layer protocol	SSH or SFTP
	suser	The username.	user_example (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	smac	Source MAC address.	FA:16:3E:65:1C:B4
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	cs1Label	Indicates that a rule was triggered.	Rule

Field type	Field name	Description	Example value
	cs1	Name of the rule triggered to cause the event.	SSH inspection rule
	cs2Label	Indicates the source zone.	SrcZone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the destination zone.	DstZone
	cs3	Destination zone name.	Untrusted
	cs4Label	Refers to the command transmitted via SSH.	Command
	cs4	Command transmitted via SSH, in JSON format.	whoami

Mail Security Log Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	mailsecurity
	Name	Source type.	log
	Threat Level	Application threat level.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no

Field type	Field name	Description	Example value
			category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@einerson stal
	act	Action taken by the device according to the configured policies.	mark
	app	Application layer protocol	SMTP
	suser	The username.	user_example (Unknown, if the user is unknown)
	src	Source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	dst	Destination IPv4 address.	10.10.10.10
	dpt	Destination port	Values: 0-65535.
	in	Number of transmitted inbound bytes (data transferred from the source to the destination).	10
	out	Number of transmitted outbound bytes (data transferred from the	10

Field type	Field name	Description	Example value
		destination to the source).	
	cs1Label	Indicates the rule name.	Rule
	cs1	Name for the mail security rule.	Mail security rule
	cs2Label	Indicates the source zone.	Source Zone
	cs2	Source zone	Untrusted
	cs3Label	Indicates the country of the traffic source.	Source Country
	cs3	Traffic source country.	AE (a two-letter country code is displayed)
	cs4Label	Indicates the traffic destination zone.	Destination Zone
	cs4	Traffic destination zone name.	Untrusted
	cs5Label	Indicates the country of the traffic destination.	Destination Country
	cs5	The destination country.	AE (a two-letter country code is displayed)
	cs6Label	Indicates the recipient's address.	To
	cs6	Recipient's email.	receiver@example.com
	flexString1Label	Indicates the sender's address.	From
	flexString1	Sender's email.	sender@example.com

Field type	Field name	Description	Example value
	cn1Label	Indicates the number of packets transmitted from the source to the destination.	Packets sent
	cn1	Number of packets transmitted from the source to the destination.	3
	cn2Label	Indicates the number of packets transmitted from the destination to the source.	Packets received
	cn2	Number of packets transmitted from the destination to the source.	1

Mail traffic protection log format **CEF Compact**:

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	mailsecurity
	Name	Source type.	log
	Threat Level	Application threat level.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received	1652344423822

Field type	Field name	Description	Example value
		(in milliseconds since January 1, 1970).	
	deviceExternalId	The unique name of the device that generated the event.	utmcore@einerson stal
	act	Action taken by the device according to the configured policies.	mark
	app	Application layer protocol	SMTP
	suser	The username.	user_example (Unknown, if the user is unknown)
	src	Source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	dst	Destination IPv4 address.	10.10.10.10
	dpt	Destination port	Values: 0-65535.
	in	Number of transmitted inbound bytes (data transferred from the source to the destination).	10
	out	Number of transmitted outbound bytes (data transferred from the destination to the source).	10
	cs1Label	Indicates the rule name.	Rule

Field type	Field name	Description	Example value
	cs1	Name for the mail security rule.	Mail security rule
	cs2Label	Indicates the source zone.	SrcZone
	cs2	Source zone	Untrusted
	cs4Label	Indicates the traffic destination zone.	DstZone
	cs4	Traffic destination zone name.	Untrusted
	cs5Label	Indicates the sender's address.	From
	cs5	Sender's email.	sender@example.com
	cs6Label	Indicates the recipient's address.	To
	cs6	Recipient's email.	receiver@example.com

Endpoint Event Log Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	endpoint_log
	Name	Source type.	log
	Severity	The severity of the event.	Available values: • 1 — error; • 2 — warning;

Field type	Field name	Description	Example value
			• 3 — info; • 4 — audit success; • 5 — audit failure.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	ID of the device generated this event.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	msg	Detailed information about the event.	Windows Defender state successfully changed to SECURITY_PRODUCT_STATE_ON.
	suser	The username.	Admin
	cs1Label	Specifies the endpoint device ID.	endpointId
	cs1	Endpoint device or sensor ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Indicates the name of the endpoint device or the sensor.	endpointName
	cs2	Endpoint device or sensor name.	DESKTOP-0731NFQ
	cs3Label	Indicates the event type.	logLevel
	cs3	Event type.	Success audit, Warning, Details, Rejection audit, Error

Field type	Field name	Description	Example value
	cs4Label	Specifies the event category.	logCategoryString
	cs4	The event's category.	Special Logon
	cs5Label	Indicates the log type.	logFile
	cs5	Type of the log containing important information on the software and hardware events.	Security (security log file), Application (application log file), System (system log file), Windows PowerShell
	cs6Label	Indicates the log event source.	sourceName
	cs6	Log event source.	Microsoft-Windows-Security-Auditing
	cn1Label	Indicates the log event code.	logEventCode
	cn1	Log event code.	1154
	cn2Label	Indicates the event ID.	logEventId
	cn2	Event ID.	10016
	cn3Label	Indicates the log event type.	logEventType
	cn3	Log event type.	1 (error), 2 (warning), 3 (information), 4 (audit success), 5 (audit failure).
	flexString1Label	Indicates the insertion string.	insertionString
	flexString1		

Field type	Field name	Description	Example value
		The insertion string is the EventData block of the Windows event data.	Windows DefenderSECURITY_PRODUCT_STATE_ON

Endpoint Rule Log Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	endpoint_log
	Name	Source type.	log
	Threat Level	Threat level for the URL category.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	ID of the device generated this event.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Action taken by the device according to the configured policies.	accept

Field type	Field name	Description	Example value
	proto	Level 4 protocol used.	TCP
	shost	Hostname.	www.google.com
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	filePath	Application to which the firewall rule was applied.	C:\\Program Files (x86)\\Microsoft\ \Edge\ \Application\ \msedge.exe
	cs1Label	Specifies the endpoint device ID.	endpointId
	cs1	Endpoint device or sensor ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Specifies the endpoint device NetBIOS name.	endpointName
	cs2	Endpoint device NetBIOS name.	DESKTOP-0731NFQ
	cs3Label	Specifies the rule, which resulted to creating this log record.	Rule
	cs3	The name of the rule.	Test rule name
	flexString1Label	Refers to the content type.	Media type

Field type	Field name	Description	Example value
	flexString1	The type of the content.	text/html
	flexString2Label	Indicates the category of the requested URL.	Categories
	flexString2	URL category.	Computers & Technology

Endpoint rules log format **CEF Format**:

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	endpoint_log
	Name	Source type.	log
	Threat Level	Threat level for the URL category.	Available values: 2, 4, 6, 8, 10 (the set threat level multiplied by 2); Unknown, if no category is defined.
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	ID of the device generated this event.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Action taken by the device according to the	accept

Field type	Field name	Description	Example value
		configured policies.	
	proto	Level 4 protocol used.	TCP
	shost	Hostname.	www.google.com
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	filePath	Application to which the firewall rule was applied.	C:\\Program Files (x86)\\Microsoft\ \Edge\ \Application\ \msedge.exe
	cs1Label	Specifies the endpoint device ID.	endpointId
	cs1	Endpoint device or sensor ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Specifies the endpoint device NetBIOS name.	endpointName
	cs2	Endpoint device NetBIOS name.	DESKTOP-0731NFQ
	cs3Label	Specifies the rule, which resulted to creating this log record.	Rule
	cs3	The name of the rule.	Test rule name

Endpoint Application Log Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	endpoint_applications
	Name	Source type.	log
	Threat Level	Default value.	0
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	ID of the device generated this event.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Action (application start or stop).	start, stop
	suser	User	DESKTOP-0731NFQ\User
	filePath	Path to the file.	C:\\Windows\\system32\\cmd.exe
	spid	Process ID.	3860
	fileHash	The application hash.	B4979A9F970029889713D756C3F123643DDE73DA
	cs1Label	Specifies the endpoint device ID.	endpointId
	cs1	The endpoint ID.	

Field type	Field name	Description	Example value
			35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Specifies the endpoint device NetBIOS name.	endpointName
	cs2	Endpoint device NetBIOS name.	DESKTOP-0731NFQ
	cs3Label	Indicates the command line.	cmdLine
	cs3	Command line prompt.	C:\\Windows\\system32\\sc.exe start w32time task_started
	cs4Label	Indicates the Session ID.	sessionId
	cs4	Session ID.	1656395717

Endpoint Hardware Log Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	endpoint_hardware
	Name	Source type.	log
	Threat Level	Default value.	0
CEF [extension]	**rt**	Time when the event was received (in milliseconds	1652344423822

Field type	Field name	Description	Example value
		since January 1, 1970).	
	deviceExternalId	ID of the device generated this event.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Action (connect or remove a device).	add_device, remove_device
	sourceServiceName	A Windows driver that allows the computer to communicate with hardware/device.	USBHUB3
	cs1Label	Specifies the endpoint device ID.	endpointId
	cs1	The endpoint ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Specifies the endpoint device NetBIOS name.	endpointName
	cs2	Endpoint device NetBIOS name.	DESKTOP-0731NFQ
	cs3Label	Specifies the ID of the device being connected or removed.	deviceId
	cs3	Device ID.	USB\ \VID_0E0F&PID_0002\ \6&201153C1&0&8
	cs4Label	Indicates the device name.	deviceName
	cs4	The name of the device.	Kingston DataTraveler 2.0 USB Device

Syslog Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	syslog
	Name	Source type.	log
	Threat Level	Threat level.	Available values: • 0: emergencies • 1: alerts • 2: critical • 3: errors • 4: warnings • 5 — notifications; • 6 — informational; • 7: debugging
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1701085036026
	deviceExternalId	The unique name of the device that generated the event.	utmcore@ntoorereaeda
	msg	The event description.	[3603:3603:1128/175000.938565:ERROR:CONSOLE(6)] "console.assert", source: devtools://devtools/bundled/

Field type	Field name	Description	Example value
			devtools-frontend/front_end/panels/console/console.js (6)
	cn1Label	Indicates the source type of Syslog events. For more information about Syslog facility values, see RFC 5424.	Facility
	cn1	Syslog event source type. Example: user-level messages.	1
	cs1Label	Indicates the name of the device where the event occurred.	Hostname
	cs1	The name of the computer where the event occurred.	node1
	cs2Label	Indicates the application that caused the event.	Tag
	cs2	The application that caused the event.	org.gnome.Shell.desktop
	cs3Label	Indicates the process ID of the event.	ProcessID
	cs3	PID of the process triggering the event.	3036
	cs4Label	Indicates that a rule was triggered.	Rule

Field type	Field name	Description	Example value
	cs4	Name of the rule triggered to cause the event.	Example: Allow user-level messages

RADIUS log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	radius
	Name	Source type.	log
	Threat Level	Threat level.	Available values: • 0: emergencies • 1: alerts • 2: critical • 3: errors • 4: warnings • 5 — notifications; • 6 — informational; • 7: debugging
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1701085036026
	deviceExternalId	The unique name of the device that generated the event.	utmcore@ntoorereaeda

Field type	Field name	Description	Example value
	act	User status (acct_status_type).	start, stop, interim update, accounting-on, accounting-off
	suser	The username.	**Unknown, if the user is unknown.**
	src_ip	The IP address of the source where the message came from.	192.168.57.4
	dst	The IP address of the NAS that authorized the user.	172.16.1.4
	dvc	User IP address (framed IP address).	192.168.57.29
	cs1Label	Indicates the group the user is a member of.	user groups
	cs1	A string of groups the user is a member of.	test_group

UserID log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	userid
	Name	Source type.	log
CEF [extension]	**rt**	Time when the event was received	1701085036026

Field type	Field name	Description	Example value
		(in milliseconds since January 1, 1970).	
	deviceExternalId	The unique name of the device that generated the event.	utmcore@ntoorereaeda
	act	Action taken by the device according to the configured policies.	login
	reason	The reason why the event was created.	{"user_groups_sids": ["S-1-5-21-3795870133-5220325-2125745684-513","S-1-5-21-3795870133-5220325-2125745684-512"], "user_sid":"S-1-5-21-3795870133-5220325-2125745684-1103","login":"user1","domain":"DEV","event_id":4624}
	suser	The username.	user1 (Unknown, if the user is unknown)
	src	Traffic source IPv4 address.	10.10.0.11
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	dev.local

Export logs in JSON format

Event log description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	The unique name of the device that generated the event.	utmcore@ersthetatica
ip_address	IPv4 address of the event source.	192.168.174.134
attributes	Event details in JSON format.	{"rule":{"logrotate": 12,"attributes": {"timezone":"UAE/ Dubai"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}
event_type	Event type.	logexport_rule_updated
event_severity	Event severity.	info, warning, error, or critical
event_origin	Module where the event occurred.	core
event_component	Component where the event occurred.	console_auth
user	Username.	{"guid":"37333739-3733-3734-3635-366400000000","name":"System","groups":[]}}

Web access log description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Session ID.	

Field name	Description	Example value
		a7a3cd49-8232-4f1a-962a-3659af89e96f (if System: 00000000-0000-0000-0000-000000000000)
node	The unique name of the device that generated the event.	utmcore@ersthetatica
reasons	The reason why the event was created, e.g. the reason for the site block.	"url_cats":[{"id": 39,"name":"Social Networking","threat_level":3}]
proto	Level 4 protocol used.	TCP
host	Hostname.	www.google.com
action	Action taken by the device according to the configured policies.	block
bytes_sent	Number of bytes transmitted from the source to the destination.	52
bytes_recv	Number of packets transmitted from the destination to the source.	100
packets_sent	Number of packets transmitted from the source to the destination.	2
packets_recv	Number of bytes transmitted from the destination to the source.	5
request_method	Method used to access the URL address (POST, GET, etc.).	GET
url	Contains the URL of the requested resource and the protocol used.	http://www.secure.com
media_type	The type of the content.	application/json
status_code	Status code.	302

Field name			Description	Example value
http_referer			Request source URL (HTTP referer).	https://www.google.com/
decrypted			Indicates if the content was decrypted.	true, false
useragent			Browser useragent.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
application		**id**	Application ID.	20
		name	Application name.	Youtube
		threat_level	Application threat level.	0
		app_protocol	Application layer protocol and its version.	HTTP\/1.1"
url_categories	**id**		ID of the category to which the URL belongs.	39
	threat_level		Threat level for the URL category.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	name		Name of the category to which the URL belongs.	Social Networking
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Source zone name.	Trusted
	country		Traffic source country.	AE (a two-letter country code is displayed)
	ip		Source IPv4 address.	10.10.10.10
	port		Source port	Values: 0-65535.

Field name			Description	Example value
	mac		source MAC address	01:23:45:67:89:AB
destination	**zone**	**guid**	Unique ID of the traffic destination zone.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Traffic destination zone name.	Untrusted
	country		The destination country.	AE (a two-letter country code is displayed)
	ip		Destination IPv4 address.	192.168.174.134
	port		Destination port	Values: 0-65535.
	mac		Destination MAC address.	01:23:45:67:89:AB
rule	**guid**		Unique ID of the rule triggered to cause the event.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name		The name of the rule.	Default allow
	type		Triggered rule type.	
user	**guid**		Unique ID of the user.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Username.	user_name
	groups	**guid**	Unique ID of the group the user is a member of.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Name of the group the user is a member of.	Default Group

DNS log description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Session ID.	00000000-0000-0000-0000-000000000000

Field name		Description	Example value
node		The unique name of the device that generated the event.	utmcore@ntoorereaeda
reasons		The reason why the event was created, e.g. the URL category on which the rule was triggered.	{"url_cats":[{"id": 37,"name":"Search Engines & Portals","threat_level":1}]}
proto		Level 4 protocol used.	UDP
host		Hostname.	google.com
data		Indicates the data being transmitted.	{"question": [{"domain":"google.com","type" :"A","class":"IN"}], "answer": [{"domain":"google.com","type" :"TXT","class":"IN","ttl": 5,"data":"Blocked"}, {"domain":"google.com","type": "A","class":"IN","ttl": 5,"data":"10.10.0.1"}]}
url_categories	**id**	ID of the triggered URL category.	37
	threat_level	Threat level of the triggered category.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	name	Name of the triggered category.	Search Engines & Portals
action		Action taken by the device according to the configured policies.	block
application	**id**	Application ID.	5
	name	Application name.	

Field name			Description	Example value
		threat_level	Application threat level.	0
		app_protocol	Application layer protocol	DNS
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Traffic source zone name.	Trusted
	country		Source country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic source.	10.10.10.10
	port		Source port	Values: 0-65535.
	mac		Source MAC address.	01:23:45:67:89:AB
destination	**zone**	**guid**	Unique ID of the traffic destination zone.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Traffic destination zone name.	Untrusted
	country		Destination country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic destination.	104.19.197.151
	port		Destination port.	Values: 0-65535. Port 53 is normally used for DNS.
	mac		Destination MAC address	01:23:45:67:89:AB
rule	**guid**		Unique ID of the rule triggered to cause the event.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Name of the rule triggered to cause the event.	Rule1
	Type		Triggered rule type.	

Field name			Description	Example value
user	**guid**		Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		The username.	user1
	groups	**guid**	Unique ID of the group the user is a member of.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Name of the group the user is a member of.	Default Group

Traffic log description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Session ID.	a7a3cd49-8232-4f1a-962a-3659af89e96f (if System: 00000000-0000-0000-0000-000000000000)
node	The unique name of the device that generated the event.	utmcore@ersthetatica
proto	Level 4 protocol used.	TCP or UDP
action	Action taken by the device according to the configured policies.	accept
bytes_sent	Number of bytes transmitted from the source to the destination.	100
bytes_recv	Number of bytes transmitted from the destination to the source.	6
packets_recv		1

Field name			Description	Example value
			Number of packets transmitted from the destination to the source.	
packets_sent			Number of packets transmitted from the source to the destination.	1
json_data			Additional data.	null
application	**id**		Application ID.	195
	threat_level		Application threat level.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	app_protocol		Application layer protocol	HTTP
	name		Application name.	Youtube
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Traffic source zone name.	Trusted
	country		Source country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic source.	10.10.10.10
	port		Source port	Values: 0-65535.
destination	**zone**	**guid**	Unique ID of the traffic destination zone.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Traffic destination zone name.	Untrusted
	country		Destination country name.	AE (a two-letter country code is displayed)

Field name			Description	Example value
	ip		IPv4 address of the traffic destination.	104.19.197.151
	port		Destination port.	Values: 0-65535.
nat	**source**	**ip**	Source address after reassignment (if NAT rules are configured).	192.168.117.85 (if NAT is not configured then **"nat":null**)
		port	Source port after reassignment (if NAT rules are configured).	Values: 0-65535 (if NAT is not configured then **"nat":null**)
	destination	**ip**	Destination address after reassignment (if NAT rules are configured).	64.233.164.198 (if NAT is not configured then **"nat":null**)
		port	Source port after reassignment (if NAT rules are configured).	Values: 0-65535 (if NAT is not configured then **"nat":null**)
rule	**guid**		Unique ID of the rule triggered to cause the event.	59e38e06-533a-4771-9664-031c3e8b2e1f
	type		Rule type.	firewall
	name		Name of the rule triggered to cause the event.	Allow trusted to untrusted
user	**guid**		Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		The username.	Admin
	groups	**guid**	Unique ID of the group the user is a member of.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Name of the group the user is a member of.	Default Group

IDPS log description

Field name		Description	Example value
timestamp		Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Session ID.	a7a3cd49-8232-4f1a-962a-3659af89e96f (if System: 00000000-0000-0000-0000-000000000000)
node		The unique name of the device that generated the event.	utmcore@ersthetatica
proto		Level 4 protocol used.	TCP or UDP
action		Action taken by the device according to the configured policies.	accept
bytes_sent		Number of bytes transmitted from the source to the destination.	100
bytes_recv		Number of bytes transmitted from the destination to the source.	6
packets_sent		Number of packets transmitted from the source to the destination.	1
packets_recv		Number of packets transmitted from the destination to the source.	1
json_data		Additional data.	null
application	**id**	Application ID.	195
	threat_level	Application threat level.	Available values: • 1: very low • 2: low • 3: medium • 4: high

Field name			Description	Example value
				• 5: very high
	name		Application name.	Youtube
	app_protocol		Application layer protocol	HTTP
user	**guid**		Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		The username.	Admin
	groups	**guid**	Unique ID of the group the user is a member of.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Name of the group the user is a member of.	Default Group
rule	**guid**		Unique ID of the rule triggered to cause the event.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Name of the rule triggered to cause the event.	Allow trusted to untrusted
	type		Triggered rule type	idps
signatures	**id**		ID of the triggered signature.	999999
	threat_level		Threat level of the triggered signature.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	name		Name of the triggered signature.	BlackSun Test
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Traffic source zone name.	Trusted

Field name			Description	Example value
	country		Source country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic source.	10.10.10.10
	port		Source port	Values: 0-65535.
	mac		Source MAC address.	01:23:45:67:89:AB
destination	**zone**	**guid**	Unique ID of the traffic destination zone.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Traffic destination zone name.	Untrusted
	country		Destination country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic destination.	104.19.197.151
	port		Destination port	Values: 0-65535.
	mac		Destination MAC address.	01:23:45:67:89:AB

SCADA log description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
pdu_severity	SCADA severity.	1
pdu_func	Function code (instructs the slave what data the master requires from it or what action to perform).	12
pdu_address	Registry address with which the operation should be performed.	3154
node		utmcore@ersthetatica

Field name		Description	Example value
		The unique name of the device that generated the event.	
details	**pdu_varname**	Variable name. Parameter is mainly used for real-time data exchange. Refers to the MMS protocol.	VAR
	pdu_device	Address of the device used in the MMS and OPCUA protocols.	DEV
	mb_write_quantity	Number of values to write (Read Write Register command).	998
	mb_write_addr	Start register address to write (Read Write Register command).	776
	mb_value	Value to write (for Write Single Coil, Write Single Register commands).	322
	mb_unit_id	Device address.	186
	mb_read_quantity	Number of values to read (Read Write Register command).	658
	mb_read_addr	Start registry address to read (Read Write Register command).	122
	mb_quantity	Number of values to read.	875
	mb_payload	Register values (for Read Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil commands).	75be5ecdc24f9883
	mb_or_mask	OR mask value of the Mask Write Register command.	1024
	mb_message	Modbus message.	exception

Field name			Description	Example value
	mb_exception_code		Error code. For the error_response message type.	255
	mb_and_mask		AND mask value of the Mask Write Register command.	121
	mb_addr		Register address.	3154
	iec104_msgtype		Type of the query.	request, response, error_response
	iec104_ioa		Address of information object, which allows the receiving party to unambiguously identify the type of event.	23
	iec104_cot		Reason for transmitting an Application Protocol Data Unit (APDU).	6
	iec104_asdu		ASDU address (COA — Common Object Address). Refers to the IEC-104 protocol.	123
app_protocol			Application layer protocol	Modbus
action			Action taken by the device according to the configured policies.	pass
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Traffic source zone name.	Trusted
	country		Source country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic source.	10.10.10.10
	port		Source port	Values: 0-65535.
destination	**zone**	**guid**	Unique ID of the traffic destination zone.	3c0b1253-f069-4060-903b-5fec4f465db0

Field name			Description	Example value
		name	Traffic destination zone name.	Untrusted
	country		Destination country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic destination.	104.19.197.151
	port		Destination port.	Values: 0-65535.
rule	**guid**		Unique ID of the rule triggered to cause the event.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Name of the rule triggered to cause the event.	SCADA Sample Rule

SSH inspection log description

Field name		Description	Example value
timestamp		Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		The unique name of the device that generated the event.	utmcore@ersthetatica
command		Command sent via SSH.	whoami
action		Action taken by the device according to the configured policies.	block
application	**id**	Application ID.	195
	name	Application name.	
	threat_level	Application threat level.	Available values: from 2 to 10 (set application threat level multiplied by 2).
	app_protocol	Application layer protocol	SSH or SFTP

Field name			Description	Example value
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Traffic source zone name.	Trusted
	country		Source country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic source.	10.10.10.10
	port		Source port	Values: 0-65535.
	mac		Source MAC address.	FA:16:3E:65:1C:B4
destination	**zone**	**guid**	Unique ID of the traffic destination zone.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Traffic destination zone name.	Untrusted
	country		Destination country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic destination.	104.19.197.151
	port		Destination port	Values: 0-65535.
	mac		Destination MAC address.	01:23:45:67:89:AB
rule	**guid**		Unique ID of the rule triggered to cause the event.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Name of the rule triggered to cause the event.	SSH Rule Example
	type		Triggered rule type.	ssh
user	**guid**		Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		The username.	Admin

Field name			Description	Example value
	groups	**guid**	Unique ID of the group the user is a member of.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Name of the group the user is a member of.	Default Group

Mail Security Log Description

Field name		Description	Example value
timestamp		Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		The unique name of the device that generated the event.	utmcore@ersthetatica
action		Action taken by the device according to the configured policies.	mark
bytes_sent		Number of bytes transmitted from the source to the destination.	0
bytes_recv		Number of bytes transmitted from the destination to the source.	0
packets_sent		Number of packets transmitted from the source to the destination.	0
packets_rcv		Number of packets transmitted from the destination to the source.	0
decrypted		Indicates if the content was decrypted.	true, false
from		Sender email.	sender@example.com
to		Recipient email.	receiver@example.com
application	**id**	Application ID.	9

Field name			Description	Example value
		name	Application name.	
		threat_level	Application threat level.	Available values: from 2 to 10 (set application threat level multiplied by 2).
		app_protocol	Application layer network protocol.	SMTP
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Traffic source zone name.	Trusted
	country		Source country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic source.	10.10.10.10
	port		Source port	Values: 0-65535.
	mac		Source MAC address.	01:23:45:67:89:AB
destination	**zone**	**guid**	Unique ID of the traffic destination zone.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Traffic destination zone name.	Untrusted
	country		Destination country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic destination.	10.10.10.10
	port		Destination port	Values: 0-65535.
	port		Destination MAC address.	01:23:45:67:89:AB
rule	**guid**		Unique ID of the rule triggered to cause the event.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Name of the rule triggered to cause the event.	Mail security rule
	type		Triggered rule type.	Mail security rule

Field name			Description	Example value
user	**guid**		Unique ID of the user.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		The username.	user_name
	groups	**guid**	Unique ID of the group the user is a member of.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Name of the group the user is a member of.	Default Group

Endpoint Event Log Description

Field name	Description	Example value
user_name	The username.	DESKTOP-0731NFQ\\Username
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
status	The result of executing a WMI or SNMP query.	OK, Error
source_name	Log event source.	Microsoft-Windows-Security-Auditing
endpoint_name	Endpoint device or sensor name.	DESKTOP-0731NFQ
endpoint_id	Endpoint device or sensor ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
node	The ID of the endpoint device or node on which the sensor is running.	35fb5820-74db-4eac-b05b-d01bc284c4e8
log_level	Event type.	Success audit, Warning, Details, Rejection audit, Error
log_file	Type of the log containing important information on the software and hardware events.	Security (security log file), Application (application log file), System (system log file), Windows PowerShell

Field name	Description	Example value
log_event_type	Log event type.	1 (error), 2 (warning), 3 (information), 4 (audit success), 5 (audit failure).
log_event_id	Event ID.	4672
log_event_code	Log event code.	14056
log_category_string	The event's category.	Special Logon
insertion_string	The insertion string is the EventData block of the Windows event data.	Windows DefenderSECURITY_PRODUCT_STATE_ON
error	The WMI or SNMP error that occurred as a result of the query.	0
data	Detailed information about the event.	The startup type of the "Windows Module Installer" service has been changed from "Automatic" to "Manual".
counter_id	The ID of the counter added to the WMI and SNMP sensor.	35fb5820-74db-4eac-b05b-d01bc284c4e8
computer_name	Computer name	DESKTOP-0731NFQ

Endpoint Rule Log Description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Session ID.	00000006-0000-0000-f04d-14bdad0f01bb
proto	Level 4 protocol used.	TCP
host	Hostname.	www.google.com
action	Action taken by the device according to the configured policies.	drop, accept, nat

Field name		Description	Example value
endpoint_name		Endpoint device name.	DESKTOP-0731NFQ
endpoint_id		The endpoint ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
media_type		The type of the content.	application/json
app_name		Application to which the firewall rule was applied.	C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
source	**ip**	Source IPv4 address.	10.10.10.10
	port	Source port	Values: 0-65535.
destination	**ip**	Destination IPv4 address.	104.19.197.151
	port	Destination port.	Values: 0-65535.
rule	**guid**	Unique ID of the rule triggered to cause the event.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name	Name of the rule triggered to cause the event.	Default allow
	type	Triggered rule type.	
url_categories	**id**	ID of the category to which the URL belongs.	39
	threat_level	Threat level for the URL category.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	name	Name of the category to which the URL belongs.	Social Networking

Endpoint Application Log Description

Field name	Description	Example value
user_name	Name of the user whose account is logged in on the endpoint device.	DESKTOP-0731NFQ\\User
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
endpoint_name	Endpoint device or sensor name.	DESKTOP-0731NFQ
endpoint_id	Endpoint device or sensor ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
process_id	Process ID.	3916
hash	The application hash.	B4CE5C3495FEA0A4FDBAC8ABDCD199F7E4CA8C1F
app_name	Application that was started/stopped.	C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
action	Action (application start or stop).	start, stop
version	The application version.	6.2.19041.746
subject	Signature subject.	Microsoft Corporation
issuer	The issuer of the application's certificate.	Microsoft Windows Production PCA 2011
cmd_line	Command line prompt.	C:\\Windows\\system32\\svchost.exe -k wsappx -p -s AppXSvc
session_id	Session ID.	1656038456

Endpoint Hardware Log Description

Field name	Description	Example value
timestamp		2022-05-12T08:11:46.15869Z

Field name	Description	Example value
	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	
endpoint_name	Endpoint device or sensor name.	DESKTOP-0731NFQ
endpoint_id	Endpoint device or sensor ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
action	Action (connect or remove a device).	add_device, remove_device
device_name	The name of the device that was added or removed.	Generic USB Hub
device_id	Device ID.	USB\\VID_0E0F&PID_0002\\6&201153C1&0&7
service	A Windows driver that allows the computer to communicate with hardware/device.	USBHUB3

Syslog Description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	The unique name of the device that generated the event.	utmcore@ntoorereaeda
syslog_facility	Syslog event source type. Example: user-level messages. For more information about Syslog facility values, see RFC 5424.	1
syslog_severity	Syslog event severity level. Example: warning. For more information about Syslog severity values, see RFC 5424.	4

Field name		Description	Example value
computer_name		The name of the device where the event occurred.	node1
app_name		Application triggering the event.	org.gnome.Shell.desktop
process_id		PID of the process triggering the event.	3036
data		The event description.	[3603:3603:1130/125201.838651:ERROR:CONSOLE(6)] \"console.assert\", source: devtools://devtools/bundled/devtools-frontend/front_end/panels/console/console.js (6)
rule	**guid**	Unique ID of the rule triggered to cause the event.	16535060-5a1a-4e92-8331-239406ec34da
	name	Name of the rule triggered to cause the event.	Example: Allow user-level messages
	type	Triggered rule type.	

RADIUS log description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	The unique name of the device that generated the event.	utmcore@ntoorereaeda
event_type	User status (acct_status_type).	start, stop, interim update, accounting-on, accounting-off
action	Action taken by the device according to the configured policies.	login
src_ip	The IP address of the source where the message came from.	192.168.57.4

Field name			Description	Example value
nas_ip			The IP address of the NAS that authorized the user.	172.16.1.4
framed_ip			User's IP address.	192.168.57.29
rule	**guid**		Unique ID of the rule triggered to cause the event.	16535060-5a1a-4e92-8331-239406ec34da
user	**guid**		Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f
	name		The username.	user_name
	groups	**guid**	Unique ID of the group the user is a member of.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Name of the group the user is a member of.	test_group

UserID log description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	The unique name of the device that generated the event.	utmcore@ntoorereaeda
reasons	The reason why the event was created.	{\"user_groups_sids\": [\"S-1-5-21-3795870133-522032 5-2125745684-513\", \"S-1-5-21-3795870133-522032 5-2125745684-512\", \"S-1-5-21-3795870133-522032 5-2125745684-572\"], \"user_sid\": \"S-1-5-21-3795870133-522032 5-2125745684-1103\",\"login\": \"user1\",\"domain\":\"DEV\", \"event_id\":4624}

Field name			Description	Example value
action			Action taken by the device according to the configured policies.	login
src_ip			IPv4 address of the event source.	10.10.0.11
rule	**guid**		Unique ID of the rule triggered to cause the event.	16535060-5a1a-4e92-8331-239406ec34da
	name		Name of the rule triggered to cause the event.	dev.local
	type		Triggered rule type.	syslog
user	**guid**		Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f
	name		The username.	user1
	groups	**guid**	Unique ID of the group the user is a member of.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Name of the group the user is a member of.	CN=Domain Users,CN=Users,DC=dev,DC=local