UserGate

Log Analyzer 7.x Administrator Guide

Table of Contents

INTRODUCTION

Introduction (Description)

UserGate Log Analyzer (LogAn) is an add-on component for UserGate devices. Administrators can use it to:

- Reduce the device load by offloading log processing, reporting, and other statistical data processing to an external LogAn server, thus providing more resources for the device to perform protection and filtering tasks.
- Join logs from multiple UserGate devices for analysis.
- Increase the logging depth by increasing the storage size on the LogAn servers.
- Collect information from third-party devices via SNMP and analyze it.

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

LOGAN LICENSING

LogAn Licensing

Basic license

LogAn is licensed by the number of connected sensors from which it collects information. A sensor can be a UserGate node or any other device that can send information using the SNMP protocol to the LogAn node.

The basic product license is perpetual (software 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 LogAn software updates. The module is issued as an annual subscription. After one year, you will need to renew the license to continue receiving updates.
Sensors	The module determines the number of sensors from which LogAn can collect information. The module is issued for a period of one year and requires annual renewal.
Cluster	The module includes a license to allow UserGate LogAn devices to operate in cluster mode. Available in software version 7.3.0 and higher. The license term is unlimited.

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

Description

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

HSC Deployment

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

Virtual Appliance Deployment

LogAn Virtual Appliance is a quick way to deploy a VM with pre-configured components. The VM image is supplied in the OVF format (Open Virtualization

Format) supported by vendors such as VMWare and Oracle VirtualBox. For Microsoft Hyper-V and KVM, VM disk images are supplied.

Note

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

Attention!

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

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

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

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. Enable LogAn. After booting, LogAn will display the IP address to connect to for subsequent product activation. **Static IP address**Enable LogAn. 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 LogAn web console at that IP address. The address string should look similar to this: https://LogAn_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, LogAn 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.

Name	Description
Step 5. Configure zones, set IP addresses of the network interfaces, and connect UserGate LogAn to the corporate network.	In the **Interfaces** section, enable the desired network interfaces, assign valid IP addresses that correspond to your networks, and bind the interfaces to the respective zones. For more details on network interface management, see the chapter Network Interface Configuration. The system is supplied with a number of predefined zones: • Management (management network), port0 interface. • Trusted (LAN). It is assumed that the Trusted zone will connect LogAn to the network that will be used by UserGate gateways to send logs to it and by LogAn to access the Internet. For the LogAn 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 LogAn 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, LogAn is ready for use. For more detailed configuration, see the relevant chapters of this Guide.

OFFLINE SERVER OPERATIONS

Offline Node Operations

Some node maintenance operations are carried out when the node is not running and is offline. To perform such operations, select **Support menu** when the node 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 LogAn. 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 LOGAN	Boot UserGate node and output diagnostic information about the boot process to the serial port.
UGOS LOGAN (failsafe)	Boot UserGate node 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 node VM. UserGate node data and settings are not reset.
Create backup	Create a full copy of the UserGate node disk on an external USB device. All existing data on the external medium will be deleted.
Restore from backup	Restore UserGate node from an external USB device.
Factory reset	

Name	Description
	Reset UserGate node to its original system state. All data and settings will be lost.
Exit	Log out and reboot the device.

CONFIGURING LOGAN

General Settings Section

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

Name	Description
Admin console settings	LogAn 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.
Server time settings	Configure the time synchronization settings: • **Use NTP servers**: use the NTP servers from the provided list for time synchronization. • **Primary NTP server**: the primary time server address. Default value: pool.ntp.org. • **Secondary NTP server**: the secondary time server address. • **Server time**: allows time setting on the server. The UTC timezone should be used.
System DNS servers	Specify valid IP addresses of DNS servers here.
Updates download schedule	Set up a schedule to download software and library updates. You can also check for updates manually by clicking **Download updates**.
Log Collector status	The current state of the LogAn server is displayed here: • **State**: shows the current state of the statistics service.

Name	Description
	• **Device version**: the version of LogAn.
UserGate Management Center agent	Here you can configure device connection to the central management console that can be used to manage a LogAn 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.

Device management

The **Device management** section is used to configure the basic LogAn settings:

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

Diagnostics

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

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

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

Server operations

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

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

Name	Description
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.

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

To install updates, follow these steps:

Name	Description
Step 1. Create a backup file.	Create a backup of LogAn 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.
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, LogAn will reboot.

System backup management

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

To create a backup, follow these actions:

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

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

To restore the device status, follow these steps:

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

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

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

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

Exporting and importing settings

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

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

To export the settings, follow these steps:

Name	Description
Step 1. Settings Export	Under **Device management → Settings export and import**, click **Export** and select **Export all settings** or **Export network settings**. The system will save: • the current server settings in a file named:

Name	Description
	logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin • the network settings in a file named: network-logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin nodename is the LogAn node name. version is the LogAn version. YYYYMMDD_HHMMSS is the date and time of the settings export in the UTC timezone. For example: logan_core-logan_core@ranreahattha_6.2.0.13494RS-1_20211227_091350.bin or network-logan_core-logan_core@ranreahattha_6.2.0.13494RS-1_20211227_091407.bin.

To apply the exported settings, follow these steps:

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

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

Name	Description
Step 1. Create an export rule.	Under **Device management → Settings export and import**, click **Add** and enter a name and description for the rule.
Step 2. Specify the remote server parameters.	In the **Remote server** tab of the rule, specify the parameters for the remote server: • **Server type**: FTP or SSH • **Address**: the server's IP address • **Port**: the server's port • **Login name**: the user account on the remote server • **Password/Repeat password**: the password for the user account • **Directory path**: the path on the server where the settings will be uploaded

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

Administrators

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

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

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.

Name	Description
	• **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**. This option allows administrator authentication using an authentication profile with a list of available authentication methods, including preconfigured servers such as LDAP, TACACS+, or RADIUS. If an authentication profile specifies multiple authentication methods, each method will be tried in turn until the first one that works. To use this method, the corresponding authentication servers must be correctly created in the **Authentication servers** section (for more information on creating authentication servers, see the Authentication Servers section of the documentation). An authentication profile must also be created in the Authentication profiles section (for more information, see the Authentication Profiles section).

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

A LogAn 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. • **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 LogAn 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

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

To create a new certificate, follow these steps:

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

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

To export a certificate, follow these steps:

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

Name	Description
Step 2. Export the certificate.	Select the export type: • **Export certificate**: export certificate data in the .der format without exporting the certificate's private key. 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, LogAn 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 Log Analyzer management web console. LogAn 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 LogAn 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	

Name	Description
	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.
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 Catalogs

Under **Users catalogs**, you can add an LDAP connector to give the LogAn/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.

Name	Description
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.

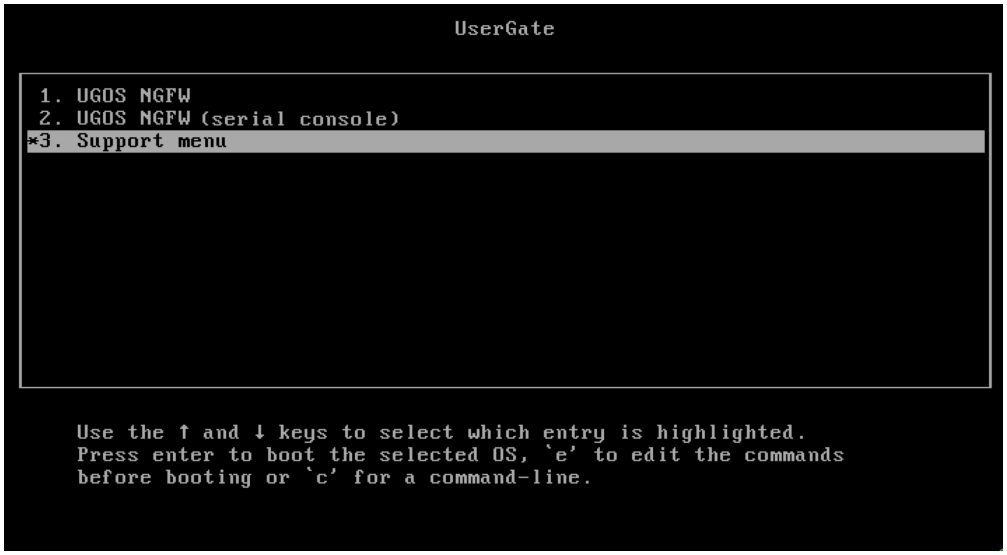
After you filled in the LDAP connector parameters, you can verify if the configuration is correct by clicking the **Check connection** button. If your settings are correct, the system will report that; otherwise, it will tell you why it cannot connect.

Expanding the System Partition

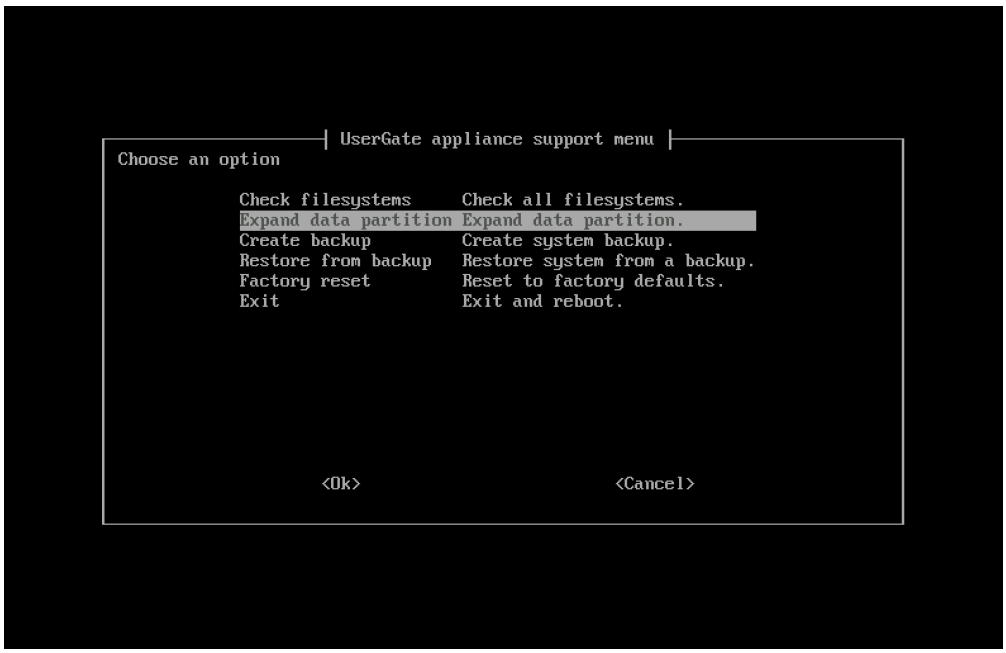
To expand the system partition while preserving the configuration and data of the UserGate node:

1. Use the hypervisor to add a new disk of the required size in the UserGate virtual machine properties.

2. In the UserGate node boot menu, enter the **Support menu** section.



3. In the section that opens, select **Expand data partition** and start the system partition expansion process.



4. When the expansion process is complete, boot the node and check the size of the system partition in the **Disks** widget of the **Dashboard** section.

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

NETWORK CONFIGURATION

Zone Configuration

A zone in LogAn is a logical aggregation of network interfaces. LogAn 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 LogAn is supplied with the following zones:

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

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

LogAn 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, LogAn starts dropping the packets from that address and records the event in the system log. The recommended values are 300 requests per second for the alert threshold and 600 requests per second for the drop threshold. **DoS protection exclusions**: here you can list the server IP addresses that need to be excluded from the protection. This can be useful, e.g., for UserGate gateways that can send large amounts of data to LogAn servers.
	Specify the LogAn-provided services that will be available to clients connected to this zone. It is recommended to disable all

Name	Description
Step 3. (Optional) Configure the access control settings for the zone.	services for zones connected to uncontrolled networks, such as the Internet. The following services exist: • **Ping**: enables pinging of LogAn. • **SNMP**: provides SNMP access to LogAn (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 node access for management using CLI (command line interface) (TCP port 2200). • **Authentication agent**: access to the node for the RADIUS accounting service. • **Log Analyzer**: the Log Analyzer service. Needs to be allowed in zones from which LogAn 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). • **API XML RPC over HTTPS**: allows access to the API over HTTPS (TCP 4443). Available in software version 7.3.3 and higher. For more on network availability requirements, see the appendix Network Environment Requirements.
Step 4. (Optional) Configure the IP spoofing protection settings.	IP spoofing attacks allow a malicious actor to transmit a packet from one network, such as **Trusted**, to another, such as **Management**. To do that, the attacker substitutes the source IP address with an assumed address of the relevant network. In this case, responses to this packet will be sent to the internal address. To protect against this kind of attack, the administrator can specify the source IP address ranges allowed in the selected zone. Network packets with 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.

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

Bonding Network Interfaces

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

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

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

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

Name	Description
	reach the recipient in an order other than the intended one because they are sent via different slaves.
Networking	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.x).

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 LogAn server.
Step 4. Specify the network interface.	Specify the network interface through which the route will be added. If you keep the default value, **Automatically**, LogAn 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.

Gateway Configuration

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

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

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

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

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

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

USERS AND DEVICES

UserID

UserID is a transparent user authentication technology. Data sources for unique user identification include security logs from domain controller operating systems and application and access server logs where users are already authenticated.

To create policies that include users and groups, the firewall must map IP addresses to the users assigned to these addresses and retrieve information about the groups to which they belong. UserID provides several methods for performing this mapping. For example, to obtain user information, UserID can scan server logs for messages from authentication services. Users whose names cannot be mapped to IP addresses can be redirected to a special portal (Captive Portal) for authentication. To obtain group information, the firewall connects directly to LDAP servers.

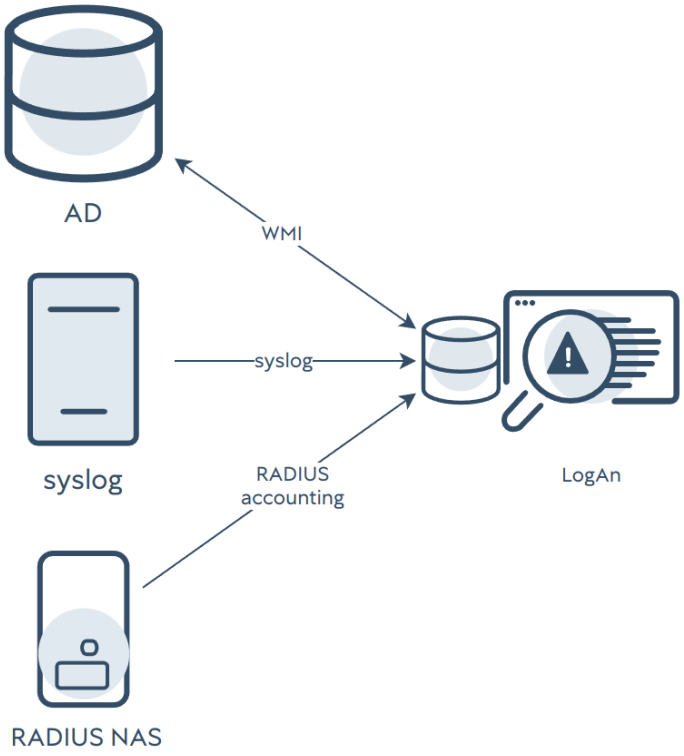
The data sources for authentication in UserID include Microsoft Active Directory logs, data obtained via syslog, or RADIUS accounting messages (in version 7.2.0 and higher).

UserID is completely transparent to end users, meaning they do not need to explicitly authenticate to UserGate NGFW.

How UserID Works

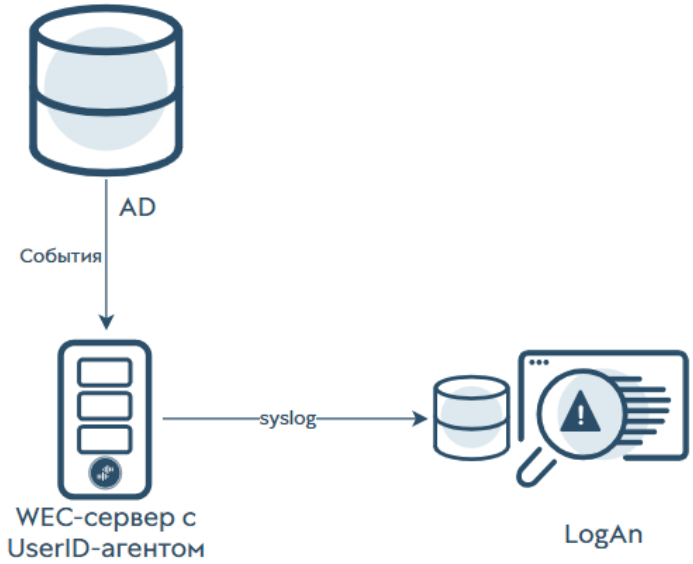
Depending on the usage scenario and configuration, the UserID agent receives data about user authentication events in one of the following ways:

- Direct data collection by the node running the UserID agent from authentication data sources using configured connectors:
    - The UserID agent can connect to the AD domain controller via WMI and read security event logs;
    - The UserID agent can receive syslog messages from third-party servers;
    - The UserID agent can receive RADIUS accounting messages from third-party RADIUS NAS servers.



- Receiving data through an intermediary, i.e. a special software agent that is installed on a domain controller or event collector server (WEC):

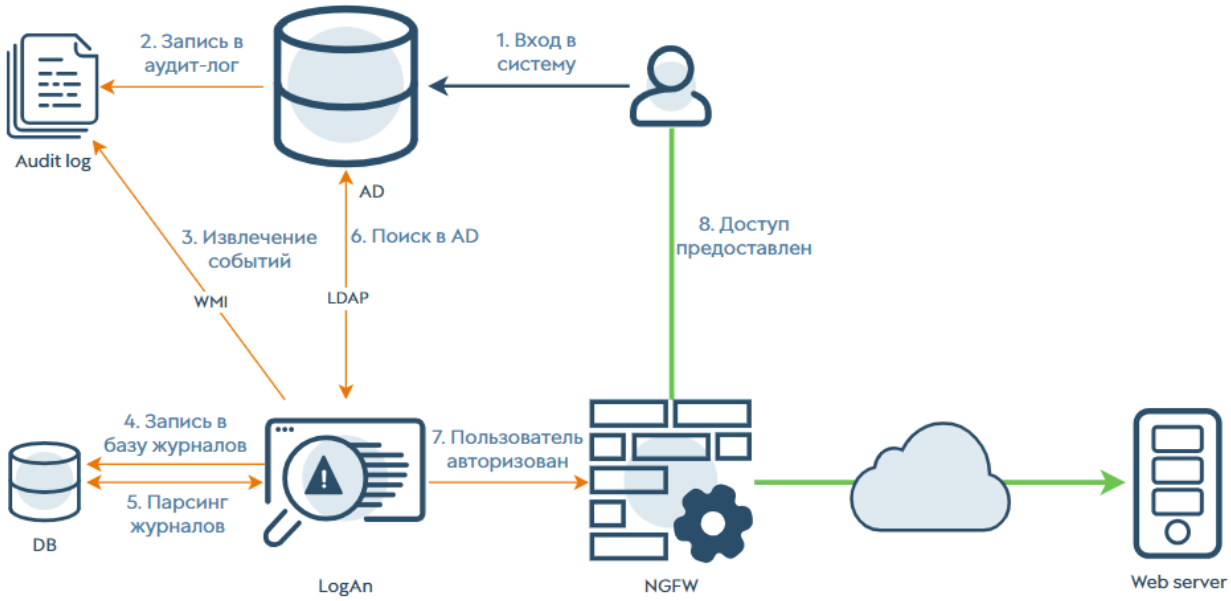
The UserID software agent for AD/WEC is installed on a domain controller (AD) or domain event collector server (WEC), reads the information needed to identify a user from Windows security logs, and forwards it in syslog format to the UserID collector on UserGate Log Analyzer (for more information about the agent, see the UserID Agent for AD/WEC section).



The main advantages of this method of obtaining data from an AD domain are:

- No need to grant external access to the domain controller to collect user authentication data, as is required with WMI access.
- No need to create a special account with special privileges in the domain for the nodes running the UserID agent.

Let's look at how UserID works using the example of a scenario involving interaction with Active Directory as a data source for user authentication via WMI.



The AD domain controller has security event auditing enabled, which records events by configured categories in a dedicated audit log.

After creating and configuring the Microsoft Active Directory UserID agent connector, the UserID agent periodically sends WMI queries to the AD controller to retrieve the following events by Event ID from the audit log:

- 4624: successful logon;
- 4768: request for a Kerberos TGT authentication ticket;
- 4769: request for a Kerberos TGS authentication ticket;
- 4770: Kerberos TGS authentication ticket renewal;
- 4627: group membership information.

These events allow the UserID agent to obtain information about user registration and group membership. The obtained information is written to a dedicated system database on the UserGate Log Analyzer.

Information from Microsoft AD about user logout is not currently processed.

The UserID agent periodically accesses this database, extracting the username, domain, SID, IP address, and list of groups from the records. This data is cached. The database search interval can be configured in the UserID agent settings. The cached user data lifetime is configured in the UserID agent connector settings.

If the list of groups to which the user belongs is not retrieved, the UserID agent contacts the domain controller via LDAP in accordance with the configured authentication profile to obtain group information.

In a scenario using syslog data source servers as the source of user authentication data, the operating principle is similar, except that UserGate Log Analyzer acts as a syslog listener. It receives messages from the syslog sender (the port number and protocol are set in the log collector settings; TCP port 514 by default) and then filters the required events from the received data stream using configured filters from the Syslog UserID Agent Filters library. In this case, the following information is saved to the database: username, IP address, and SID (optional). To obtain information about the groups to which a user is registered, the UserID agent contacts the domain controller via the LDAP protocol in accordance with the configured authentication profile.

In a scenario using RADIUS accounting messages as the source of user authentication data, the operating principle is generally similar. In this scenario, UserGate Log Analyzer acts as a pass-through RADIUS server, receiving RADIUS accounting messages from NAS servers (on port UDP 1813) and verifying the user on the AD domain controller via LDAP in accordance with the configured authentication profile.

Using the UserID agent on UserGate Log Analyzer allows you to scale UserID technology to other network devices. Events found in the collected data are sent to UserGate NGFW nodes in accordance with the UserID Sharing policy based on configured redistribution profiles (for more information on profiles, see the Redistribution Profiles section). This policy allows for sending different data to different UserGate NGFW nodes, if necessary. Only the user's GUID, IP address, and list of group IDs of which the user is a member are sent to NGFW. This architecture allows one or more UserGate Log Analyzer servers to centrally collect user information from various sources and then distribute this information centrally and selectively to UserGate NGFW nodes on the network.

In an active-passive cluster configuration of UserGate Log Analyzer, UserID functionality operates exclusively on the active cluster node (Master). However, UserID settings are distributed to all nodes in the cluster. User data collected during the active node's operation is synchronized to the UserGate Log Analyzer collector

and also sent to the passive cluster node. Role changes in the cluster occur without data loss.

> **Note**
>
> **For infrastructures with Active Directory servers and a high flow of authentication events (over 50 events per second), it is recommended to use the AD/WEC agent event collection script instead of WMI technology to ensure proper operation of the UserID function. This is due to the limited performance of WMI technology, which can cause errors when retrieving data and lead to incorrect filtering rules.**

UserID configuration algorithm

To configure UserID, a number of steps must be performed on both the authentication data sources and UserGate Log Analyzer.

Data source side configuration:

- When using Active Directory as a user authentication data source, enable security event auditing. The following categories are required:
  - Audit LogOn;
  - Audit LogOff;
  - Audit Kerberos Authentication Service;
  - Audit Group Membership;
  - Audit Kerberos Service Ticket Operations.
- When working with syslog data source servers, configure log sending to the UserID agent address (i.e., the IP address of the UserGate NGFW; the port number and protocol are set in the UserID agent settings; TCP port 514 by default).
- When working with RADIUS NAS servers, configure RADIUS accounting messages to the UserID agent address (i.e., the IP address of the UserGate NGFW, UDP port 1813).

Configuring on the UserGate Log Analyzer side:

- Create an authentication server for the UserID agent. For more information on creating and configuring authentication servers, see the Authentication Servers section.

- Create an authentication profile for the UserID agent. For more information on creating and configuring authentication profiles, see the Authentication Profiles section.
- For the syslog source server scenario, enable the **Log collector** service in the access control settings of the zone where the syslog sender will be located. For a scenario with RADIUS NAS servers, enable the **Authentication agent** service in the access control settings of the zones where the RADIUS NAS servers will be located. For more information on creating and configuring zones, see the Zone Configuration section.
- Create a UserID-agent connector based on the authentication data retrieval method.
- Configure general UserID agent settings.

Creating a UserID Agent Connector

A UserID agent connector is created in UserGate Log Analyzer web console under **General settings → Users and devices → UserID agent connectors**. Click **Add** on the toolbar and select the type of connector to create:

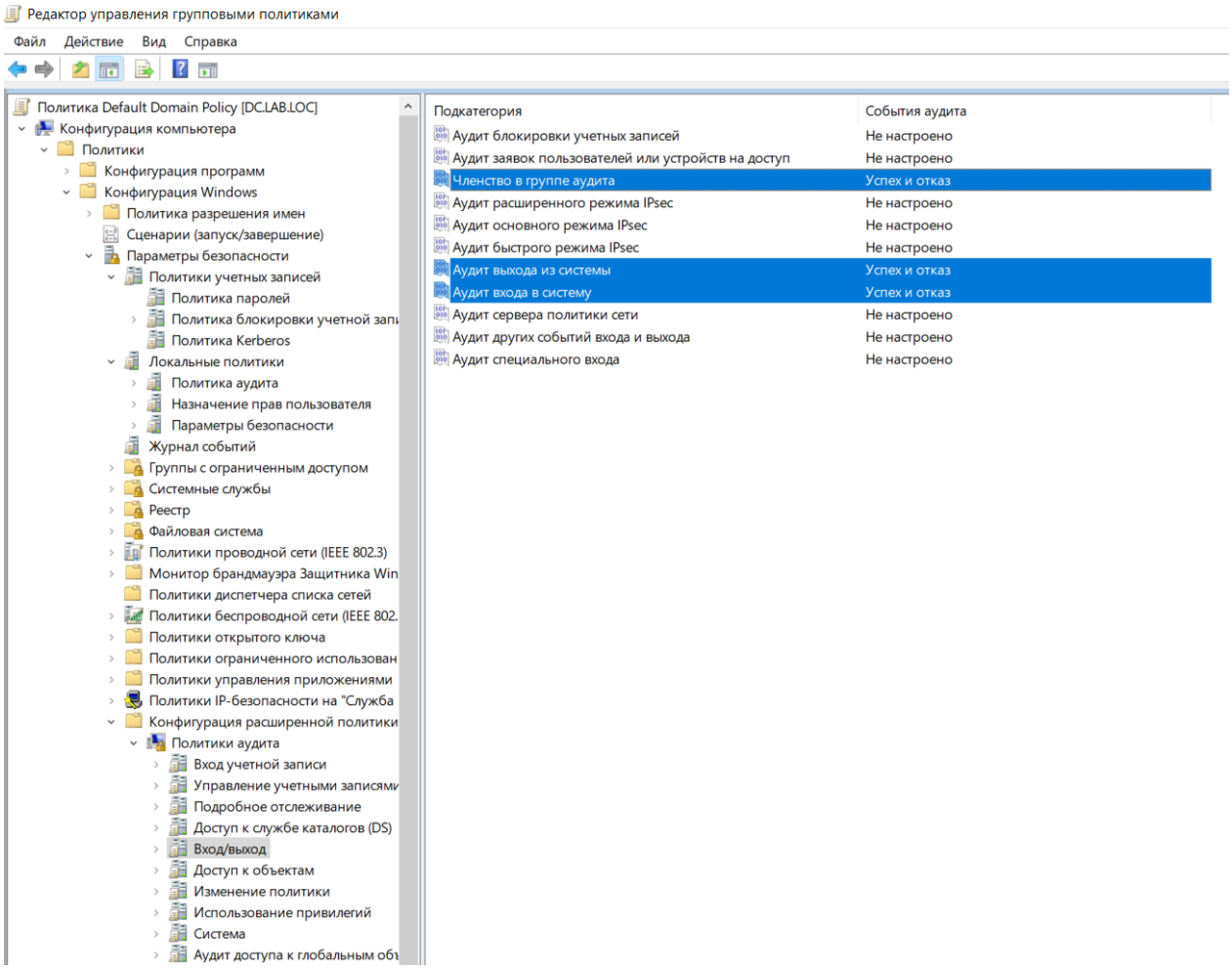
- Microsoft Active Directory;
- Syslog sender;
- RADIUS server.

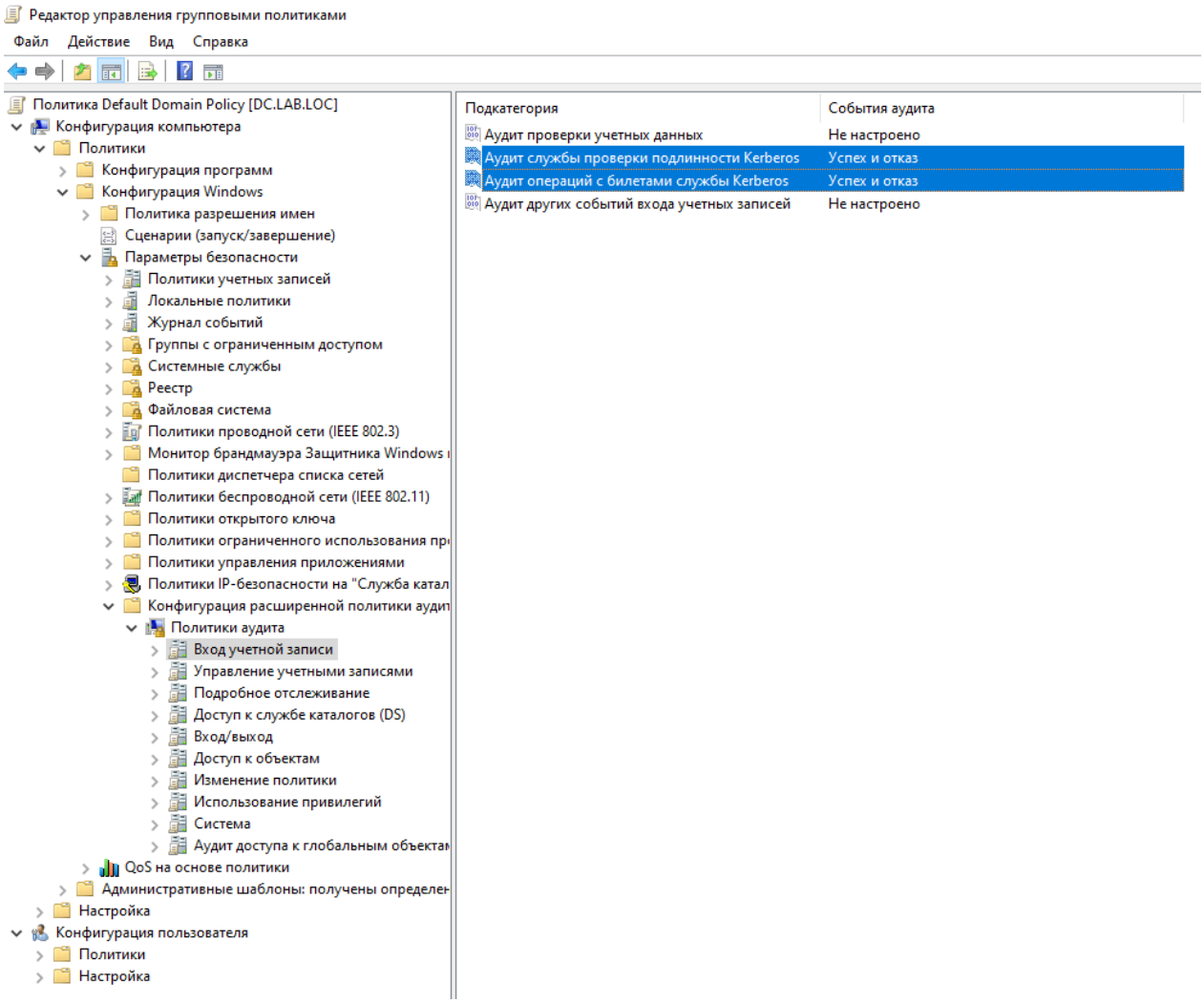
Microsoft AD

If Microsoft Active Directory is used as the source of information:

1. Configure the event source.
2. Configure the UserID agent connector settings for AD monitoring.

To enable event auditing on an AD server, edit the **Audit policies** in default **Domain policy** and **Advanced policy configuration**, as shown in the following screenshots, using the `gpedit.msc` snap-in:


Редактор управления групповыми политиками
Файл Действие Вид Справка
Политика Default Domain Policy [DC.LAB.LOC]
Конфигурация компьютера
Политики
Конфигурация программ
Конфигурация Windows
Политика разрешения имен
Сценарии (запуск/завершение)
Параметры безопасности
Политики учетных записей
Политика паролей
Политика блокировки учетной зап
Политика Kerberos
Локальные политики
Политика аудита
Назначение прав пользователя
Параметры безопасности
Журнал событий
Группы с ограниченным доступом
Системные службы
Реестр
Файловая система
Политики проводной сети (IEEE 802.3)
Монитор брандмауэра Защитника Win
Политики диспетчера списка сетей
Политики беспроводной сети (IEEE 802.
Политики открытого ключа
Политики ограниченного использован
Политики управления приложениями
Политики IP-безопасности на "Служба
Конфигурация расширенной политики
Политики аудита
Вход учетной записи
Управление учетными записями
Подробное отслеживание
Доступ к службе каталогов (DS)
Вход/выход
Доступ к объектам
Изменение политики
Использование привилегий
Система
Аудит доступа к глобальным об
Подкатегория
События аудита
Аудит блокировки учетных записей
Не настроено
Аудит заявок пользователей или устройств на доступ
Не настроено
Членство в группе аудита
Успех и отказ
Аудит расширенного режима IPsec
Не настроено
Аудит основного режима IPsec
Не настроено
Аудит быстрого режима IPsec
Не настроено
Аудит выхода из системы
Успех и отказ
Аудит входа в систему
Успех и отказ
Аудит сервера политики сети
Не настроено
Аудит других событий входа и выхода
Не настроено
Аудит специального входа
Не настроено



To execute WMI queries, create a user with the appropriate privileges using the procedure below.

> **Attention!**
>
> **These settings are required to connect the agent via WMI using a limited-privilege account.**

1. Create a user account on the domain controller:
   - Go to **Start → Server manager → Tools → Active Directory — Users and computers**.
   - In the appropriate organizational unit (OU), create a **New user** for UserID.
2. Configure group membership for the new user account:
   - Right-click the new user account UserID and select **Properties**.

- Go to the **Group membership** tab.
- Click **Add → Advanced → Search**.
- Select the following groups:
    - **DCOM users**;
    - **Performance log users**;
    - **Remote desktop users**;
    - **Event log readers**.
- Click **OK**.

3. Assign Distributed Component Object Model (DCOM) permissions:

- Go to the Windows menu **Start → Administrative Tools → Component Services**. The **Component Services** window will open.
- Expand **Component Services → Computers → My Computer**.
- Right-click **My Computer** and select **Properties**. The **Properties: My Computer** window will open.
- Go to the **COM Security** tab.
- In the **Access permissions** area, click **Change restrictions**.
- Ensure that **Local access** and **Remote access** are selected for **DCOM users**.
- Click **OK** to save the settings.
- In the **Properties: My Computer** window, under **Launch and activation permissions**, click **Change restrictions**.
- Ensure that **Local launch**, **Remote launch**, **Local activation**, and **Remote activation** are selected for **DCOM users**.
- Click **OK** to save the settings, and then click **OK** again to close the **Properties: My Computer** window.
- Select **File → Exit** to close the **Component services** window.

4. Configure WMI namespace security assignments:

- Go to **Start → Run**.

- Type `wmimgmt.msc` and click **OK**.
- Right-click **WMI control (Local)** and select **Properties**.
- Go to the **Security** tab.
- Click **Security → Add → Advanced → Search**.
- Select the new user account and click **OK** until you return to the Root **Security** window.
- Click **Advanced** and select the added user account.
- Click **Edit**.
- In the **Applies to**: menu, select **This namespace and subnamespace**.
- Ensure that **Execute methods**, **Enable account**, **Enable remotely**, and **Read security** are selected.
- Click **OK** until you return to the `wmimgmt` window.
- Select **File → Exit** to close the `wmimgmt` window.

Attention!

Windows update KB5014692 may cause WMI access errors of the type: *NTSTATUS: NT_STATUS_ACCESS_DENIED*.In this case, you can try adding the following information to the Windows registry:

```
Path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat

Value Name: "RequireIntegrityActivationAuthenticationLevel"

Type: dword

Value Data: 0x00000000
```

When using AD servers as event sources, the UserID agent performs WMI queries to search for events related to successful logon (event ID 4624), Kerberos events (events with numbers: 4768, 4769, 4770), and group membership events (event ID 4627).

In the UserGate Log Analyzer web console, under **General settings → Users and devices → UserID agent connector**, click **Add** and select the connector type to create: **Microsoft AD**.

Specify the following settings:

- **Enabled**: enable/disable receiving logs from the source.
- **Name**: name of the source.
- **Description**: description of the source (optional).
- **Server address**: address of the Microsoft Active Directory server.
- **Protocol** : AD access protocol (WMI).
- **User**: username for connecting to AD.
- **Password**: user password for connecting to AD.
- **Authentication profile**: name of the previously created authentication profile used to search for users found in AD logs.
- **Authenticated user time-to-live (sec)**: the period of time after which the user's session will be terminated, meaning their information will be deleted from the cache on UserGate Log Analyzer. The default value is 2700 seconds (45 minutes).
- **UserID redistribution profile**: select a redistribution profile to define the UserGate devices to which information about users found by the UserID agent is sent.

On the **User catalogs** tab, select the catalogs in which to search for users found in AD logs:

Syslog

If the syslog data source server is used as the information source:

1. Configure the event source.

   For the UserID-agent syslog connector to function correctly, configure the syslog data source server to send logs to the UserID agent address. For more information, see the syslog sender documentation.

General syslog server settings on the UserGate Log Analyzer device are located in **General settings → Log collector → Syslog**. Click **Configure server** on the toolbar.

In the syslog server settings window, configure the syslog connection parameters:

For the TCP protocol:

- **Enabled**: enables or disables the TCP protocol for receiving syslog logs.
- **Port**: the port number used for collecting syslog events. The default port is 514.
- **Max session number**: the maximum number of devices connected simultaneously for sending messages.
- **Secure connection**: enables or disables data stream encryption.
- **CA certificate file**: the certificate of the certification authority used to establish a secure connection.
- **Certificate file**: a certificate created by the user and signed by the certification authority.
- **Permitted peers**: a list of devices from which UserGate Log Analyzer will receive information when using a secure connection.

For the UDP protocol:

- **Enabled**: enables or disables the UDP protocol for receiving syslog logs.
- **Port**: the port number used for collecting syslog events. The default port is 514.

2. Allow collecting information from remote devices via the syslog protocol.

In the access control settings for the zone where the syslog sender is located, allow the **Log collector** service.

3. Configure the UserID agent connector settings for the syslog sender.

In the UserGate Log Analyzer web console, under **General settings → Users and devices → UserID agent connectors**, click **Add** and select **Syslog sender** as the connector type. Next, specify the following information:

- **Enabled**: enable or disable retrieving logs from the source.

- **Name**: the name of the source.
- **Description**: a description of the source (optional).
- **Server address**: the address of the host from which UserGate Log Analyzer will receive events via the syslog protocol.
- **Default domain**: the name of the domain used to search for users found in syslog logs.
- **Time zone**: the time zone set on the source. When using the UserID agent for AD/WEC, the syslog connector should always be set to UTC, regardless of the time settings on the domain controller.
- **Authenticated user time-to-live (sec)**: the period of time after which the user's session will be terminated, meaning their information will be removed from the cache. The default value is 2700 seconds (45 minutes).
- **UserID redistribution profile**: select a redistribution profile to determine the range of UserGate devices to which information about users found by the UserID agent is sent.

On the **Filters** tab, you can select filters to search for the required log entries.

You can create and configure filters under **Libraries → UserID agent Syslog filters**. For more information, see the UserID Agent Syslog Filters section.

On the **User catalogs** tab, select the catalogs in which to search for users found in syslog logs.

RADIUS Accounting

If the source of information is RADIUS accounting messages (available in version 7.2.0 and later):

1. Configure the event source.

For the UserID agent connector to function correctly, configure the NAS server to send RADIUS accounting messages to the UserID agent address (UDP port 1813). For more information, see the NAS server documentation.

2. Allow RADIUS accounting requests from remote devices.

In the access control settings for the zones where the NAS servers are located, enable the **Authentication agent** service.

3. Configure the UserID agent connector settings for the RADIUS server.

In the UserGate Log Analyzer web console, under **General settings → Users and devices → UserID agent connectors**, click **Add** and select the connector type to create: **RADIUS server**. Specify the following parameters:

- **Enabled**: enables or disables retrieving logs from the source.
- **Name**: name of the source.
- **Description**: description of the source (optional).
- **Authenticated user time-to-live (sec)**: the period of time after which the user's session will be terminated, meaning their information will be removed from the cache. The default value is 2700 seconds (45 minutes).
- **Name attribute**: the radius attribute type containing the user's name. Default value: 1.
- **Group attribute**: the radius attribute type containing the user's group. By default, the group is not checked.
- **Default domain**: the name of the domain in which the user will be searched if the request does not explicitly specify the domain the user belongs to.
- **Secret code**: a shared key used by the RADIUS protocol for authentication.
- **UserID redistribution profile**: a redistribution profile for defining the range of UserGate devices to which information about users found by the UserID agent is sent.

The **Addresses** tab specifies the addresses of hosts (NAS servers) from which the UserID agent will receive RADIUS accounting events:

On the **User catalogs** tab, you can select the catalogs in which to search for users found in RADIUS accounting logs:

Configuring UserID Agent

General UserID agent settings are configured in **General settings → Users and devices → UserID agent connectors**. Click the **Configure agent** button on the toolbar:

On the **General** tab, you can configure the data polling intervals:

- **Microsoft Active Directory Monitoring. Polling Interval (sec)** the period for polling Active Directory servers. The default value is 120 seconds.
- **Syslog monitoring interval (sec)**: the period for polling the database to search for user session start/end events from syslog sources. The default value is 60 seconds.
- **RADIUS monitoring interval (sec)**: the period for polling the database to search for user session start/end events from the RADIUS log (available in version 7.2.0 and later). The default value is 120 seconds.

The **Ignore network list** tab specifies lists of IP addresses whose events will be ignored by the UserID agent. Entries about ignored sources will appear in the UserID log:

The list can be created in the **Libraries → IP Addresses** section, or when configuring the agent (**Create and add new object** button). For more information on creating and configuring IP address lists, see the IP Addresses section.

This setting is global and applies to all sources.

The **Ignore user list** tab specifies the names of users whose events will be ignored by the UserID agent. The search is based on the Common Name (CN) of the AD user:

This setting is global and applies to all sources. A record about the ignored user appears in the UserID log.

Important!

When specifying a name, the asterisk (*) character is allowed only at the end of the line.

Note

When connecting UserGate NGFW to UserGate Log Analyzer, UserID agents configured on both devices can run simultaneously. The device agents will run independently of each other. UserID agent log events received by UserGate NGFW, like events from other logs, will be transferred to UserGate Log Analyzer.

Logging

The UserID agent periodically accesses configured data sources. Received events are stored in a service database without any changes. The contents of this database can be viewed in the following logs:

- Enpoints ➜ Event log (events from AD);
- Syslog;
- RADIUS.

In the UserGate Log Analyzer web console, they can be viewed in the **Logs and reports ➜ Logs** section.

The UserID agent periodically accesses the service database and extracts the username, SID, domain, IP address, and group lists from event records. The results of event record processing are written to the UserID log. You can view it in the same section: **Logs and reports ➜ Logs**.

For more information on data source and UserID agent logs, see the Logs section.

A description of the UserID log export formats is available in the Appendix in the Description of Log Formats section.

Redistribution Profiles

Description

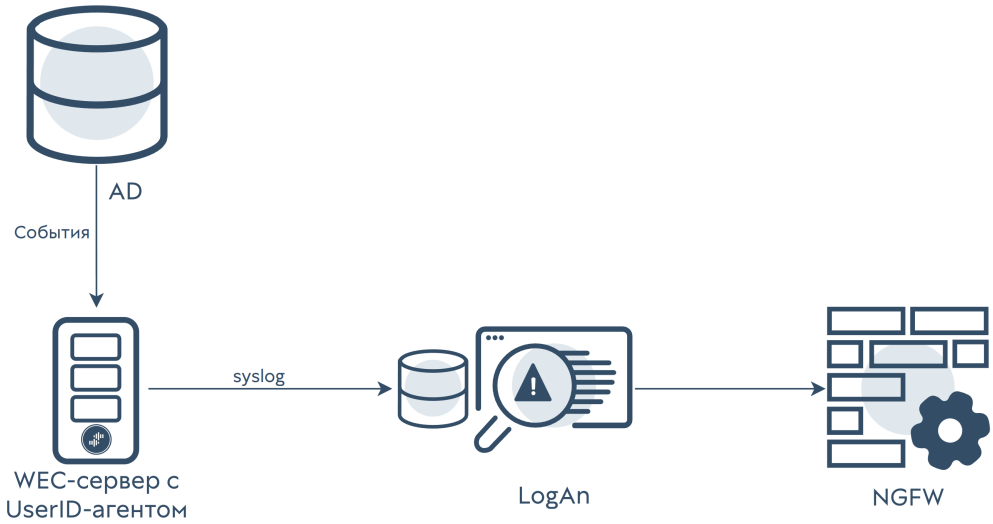
These profiles are used to define the range of UserGate devices to which information about users found by the UserID agent is sent. To add a profile, click the **Add** button and configure the profile.

Name	Description
Name	Profile name.
Description	An optional description of the profile.
UserGate Sensors	A list of UserGate devices to which information about found users will be sent. You can add sensors under**Sensors➜ UserGate sensors** in **Settings**.

> **Note**
> **By default, the *Share with all UserGate sensors* profile is created, and when selected, user information is sent to all LogAn sensors.**

UserID agent for AD/WEC

The UserID agent for the AD/WEC is installed on the domain controller (AD) or the WEC (Windows Event Collector) server. The agent reads the user authentication information from the Windows security logs and transmits it to the UserID collector on the UserGate device in the syslog format.



Main Agent Properties

The main UserID agent properties for the AD/WEC:

- Operation as a service.
- Configuring the working parameters in the configuration file.
- Logging the data in the file and its rotation (with the ability to turn on/off the debug mode).
- Reading the logs and sending the user data to the UserID collector via syslog.

Settings

The parameters for the configuration file:

- EventFileNames: the log file names to be read, comma separated. Default value: Security.
- MaxLogSize: maximum size of the log file, MB. The default value is 10.
- ServerAddress: addresses and ports for the servers. Example: server1:port1,server2:port2.
- EventIDs: numbers of the events to be forwarded. For example, 4624, 4634 (IDs for the login and logout events).
- DebugLogs: turning the debug mode on/off. 0: log the main events, 1: perform the extended logging. The default value is 1.

Configuration file syntax:

- The parameters are comma separated.
- The lines starting with ";", "#" and "[" symbols are ignored, spaces around the commas are ignored as well.

Configuration example:

```
ServerAddress=192.168.30.254:514
MaxLogSize=10
EventIDs=4634, 4624
EventFileNames=Security
DebugLogs=1
```

Installation

To install the agent, copy useridagent.exe file in any folder on the server and save the configuration file useridagent.cfg in the same folder.

Installing the service for running in the background mode under the system account:

```
useridagent.exe /installservice
```

Starting the service:

```
net start UserIDAgent
```

Stopping the service:

```
net stop UserIDAgent
```

Removing the service:

```
useridagent.exe /uninstallservice
```

Logging

The agent will log the event information in the text file. The maximum size of the file is determined by the *MaxLogSize* configuration parameter. The log file will be created in the same folder where the executable file is located. When the size of the log file exceeds the maximum size, the active log file is renamed to *.bak file, and the previous *.bak file is removed. The active log file will be recorded from the beginning. If you need to store all the service operation logs, you must use external means to copy and store the logs in another directory.

SENSORS

General Information

LogAn uses sensors to collect information from various devices for subsequent analysis. A sensor is a LogAn-compatible device that can send certain data to a LogAn 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 LogAn. 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 LogAn server will occur, and allow the **Log Analyzer/SIEM** and **SNMP** services.
Step 2. On the UserGate node, copy the token to the clipboard.	In the UserGate node that you want to add as a sensor, open **Settings → Log Database Status** and copy the token value to the clipboard. It will be needed at Step 4.
Step 3. On the LogAn, enable the Log database service in the required zone	On LogAn, 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 LogAn 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 LogAn 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.
Token	The token received on the UserGate node.

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

> **Note**
> **Once the LogAn is connected, the LogAn 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 LogAn to receive information using the SNMP protocol.

The following new items have been added to LogAn:

- 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, LogAn will revert these settings or re-create the rule when the sensor is enabled or disabled on the LogAn server.**

SNMP Sensors

Using an SNMP sensor, the administrator can connect an SNMP-compatible network device to a LogAn server to collect and analyze its metrics. LogAn 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 LogAn server, go to the **Sensors → SNMP MIB management** and upload the MIB file.
Step 2. Create an SNMP sensor.	On the LogAn 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 LogAn server and network device for SNMP v2. Use only Latin letters and numbers.
Polling interval (sec.)	The time interval with which the LogAn 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.
Authentication password	The password used for authentication.

Name	Description
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 LogAn 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 LogAn.

For vendor-specific MIBs, contact your device's vendor. LogAn 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 LogAn 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.
Description	An optional description of the sensor.

Name	Description
Server address	The 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 LogAn 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 LogAn is selected on the UGMC of this device as the server to send event information, therefore, LogAn 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 LogAn 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.

LOG COLLECTOR

General Information

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 **General settings** tab of LogAn's web interface and provide the following settings:

Name	Description
Enabled	Enable or disable receiving syslog events.
Protocol	The network protocol used for information collection: • TCP

Name	Description
	• 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 LogAn 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. • **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.

Name	Description
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** • **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 section Syslog Applications.

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

LIBRARIES

IP Addresses

The **IP Addresses** section contains a list of IP address ranges that are used in zone and UserID settings. To add a new address list, follow these steps:

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

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

Name	Description
Step 1. Create a file with the desired IP addresses.	Create a file named **list.txt** with the IP address list. The address list is written to a plain text file in a column without any punctuation. Example: `x.x.x.x` `y.y.y.y` `z.z.z.z`
	Put the file in a ZIP archive named **list.zip**.

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

Name	Description
	• An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

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

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

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 **Phones** 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,

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".

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

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.

Name	Description
Connection security	The following outgoing email security options are available: None, STARTTLS, and SSL.
Authentication	Turns on authentication for SMTP server connection.
Login name	The account name for connecting to the SMTP server.
Password	The account password for connecting to the SMTP server.

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

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

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.

UserID Agent Syslog Filters

When using Syslog as an event source, UserGate filters events according to the agent's UserID filters specified by Syslog. Syslog filters are standard regular expressions that users can write themselves. Two types of filters are provided as standard:

Name	Description
SSH Authentication	A filter to track SSH login/logout events in syslog logs.
Unix PAM Authentication	A filter to track user logon/logoff events using **Pluggable Authentication Modules** (PAM) technology in syslog logs.
UserGate WEC Agent	A filter designed to track events transmitted via syslog from the UserID agent for AD/WEC servers. (Available starting from version 7.2.0)

Note

You can create additional rules using regular expressions. Thus, syslog filters are a versatile tool that can be used in almost any case.

The found events are displayed on the **Logs and reports**, under **Logs → UserID Agent → Syslog**.

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: the array rebuild in progress
utmBroadcomRaidStatus	Integer	Current status of RAID (Redundant Array of Independent Disks) built on the Broadcom controller: • **no_raid** • **0**: optimal: the array is in its optimal state • **1**: degraded: one drive has completely or partially failed This

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

UTM-MIB

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

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

Name	Data type	Description
logDiskSpace	Integer	Disk space used for logs (in %).
powerSupply1Status	String	State of the first power supply: • **no_power_supplies**. • **on** • **off**
powerSupply2Status	String	State of the second power supply: • **no_power_supplies**. • **on** • **off**
raidType	String	RAID array type.
raidStatus	String	Current status of RAID (Redundant Array of Independent Disks): • **no_raid**. • **0**: optimal: the array is in its optimal state • **1**: degraded: one drive has completely or partially failed • **2**: rebuild: the 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*. 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	Information about the interface, which may include the manufacturer name, product name, and interface hardware version.
ifType	Integer	Interface type determined according to the physical/link layer protocol: • **1**: other: unknown type. • **2**: regular1822: defined in BBN Report 1822. • **3**: hdh1822: defined in BBN Report 1822. • **4**: ddn-x25: defined in BBN Report 1822. • **5**: defined in the data link layer standard of the OSI X.25 network mode. • **6**: ethernet-csmacd: Ethernet-type network interface regardless of speed (defined in RFC 3635). • **7**: iso88023-csmacd: defined in IEEE 802.3. • **8**: iso88024-tokenBus: defined in IEEE 8802.4. • **9**: iso88025-tokenRing: network interface uses

Name	Data type	Description
		a Token Ring connection; defined in the IEEE 802.5 standard. • **10**: iso88026-man: defined in the ISO 88026 standard "MAN". • **11**: starLan — defined in the IEEE 802.3e standard. • **12**: proteon-10Mbit — Proteon 10 Mbit. • **13**: proteon-80Mbit — Proteon 80 Mbit. • **14**: hyperchannel — high-speed channel used in ISDN networks. • **15**: fddi — network interface which is using FDDI (Fiber Distributed Data Interface) connection. FDDI is a set of standards for data transmission over fiber-optic lines in local networks. • **16**: lapb — data link layer protocol used to transmit X.25 packets. • **17**: sdlc — data link layer protocol for IBM system network architecture. • **18**: ds1 — can handle 24 simultaneous connections at a total speed of 1.544Mbit/s; also called T1. • **19**: e1 — European analogue of T1. • **20**: basicISDN — used for communication between the subscriber's equipment and the ISDN station. • **21**: primaryISDN — used to connect to backbones connecting local and central

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

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

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

Name	Data type	Description
		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 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.

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

Name	Data type	Description
		with the larger capacity is used.
ifHCOutBroadcastPkts	counter64	Identical to **ifOutBroadcastPkts**: number of broadcast packets sent; this includes packets which were dropped or were not sent; a counter with the larger capacity is used.
ifLinkUpDownTrapEnable	Integer	Specifies whether to create a trap when the link status changes: • **1**: enabled • **2**: disabled
ifHighSpeed	gauge32	Current estimated interface bandwidth pool in bit/s, kbit/s, Mbit/s, or Gbit/s.
ifPromiscuousMode	Integer	Promiscuous mode. Available values: • **1**: true: station receives all packets/frames regardless of the destination. • **2**: false: interface receives only packets/frames addressed to this station. The object value does not affect the reception of broadcast and multicast packets/frames.
ifAlias	String	The interface name specified by the administrator when configuring the interface.
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.
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.
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.
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

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

- **Events**: events related to changes in LogAn server settings, user and administrator authentication, updates to various lists, etc.
- **Web access**: a detailed log of all web requests processed by LogAn.
- **DNS**: contains 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 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 log**: contains description of events showing the result of the UserID agent's work.

- **RADIUS log**: contains the events collected by the UserID from the RADIUS accounting data.

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 will be displayed in the event LogAn log.

Event log records are not rotated.

Event Log

The Event Log displays events related to changes to the LogAn 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 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
Node	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.

Name	Description
Time	The time of the event.
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.

Logs Export

LogAn's log export feature allows you to upload information to external servers for subsequent analysis or processing in SIEM (security information and event management) systems.

UserGate LogAn allows you to export the following logs:

- DNS Log;
- Event log;
- Web Access Log;
- IDPS Log;
- SCADA Log;
- SSH inspection log;
- Traffic Log;
- Endpoint Event Log;
- Endpoint Rule Log;
- Endpoint Application Log;
- 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. The option is available in software version 7.2.0 and higher.
Logs to export	Select the log files to export: • DNS Log; • Event log; • Web Access Log; • IDPS Log; • SCADA Log; • SSH inspection log; • Traffic Log; • Endpoint Event Log; • Endpoint Rule Log; • Endpoint Application Log; • 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 Appendix 2. Description of Log Formats.
Server type	SSH (SFTP), FTP, Syslog.

Name	Description
Server address	IP address or domain name of the server.
Transport	TCP or UDP; applicable only to Syslog servers.
Port	The server port to which the data should be sent.
Protocol	RFC5424 or BSD syslog RFC 3164; applicable only to Syslog servers. Select the protocol compatible with your SIEM system.
Severity	Only for Syslog server type. Optional field; consult the documentation for your SIEM system. Available values: • Alert: a state that requires immediate intervention; • Critical: a state that requires immediate intervention or signals a fault in the system; • Errors: errors detected in the system; • Warnings: warnings on potential errors that can occur if no action is taken; • Notice: events that relate to unusual system behavior but are not errors; • Info: informational messages.
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.

Name	Description
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 • 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".

Data Search and Filtering

Usually, logs contain huge numbers of records, and LogAn 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,

Name	Description
	statusCode, etc., for example: *date >= "2019-03-13T21:00:00" AND statusCode=200*.
<	Less Than. The field value must be less than the specified value. This can only apply to fields that support comparisons, such as date, portSource, portDest, statusCode, etc., for example: *date < '2019-03-28T20:59:59' AND statusCode=404*.
>	Greater Than. The field value must be greater than the specified value. This can only apply to fields that support comparisons, such as date, portSource, portDest, statusCode, etc., for example: *(statusCode>200 AND statusCode <300) OR (statusCode=404)*.
IN	Allows you to specify multiple values for a field in a query. Provide the list of values in parentheses, for example, *category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')*.
NOT IN	Allows you to specify multiple values for a field in a query. Displays records that do not contain the specified values. Provide the list of values in parentheses, for example, *category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')*.
~	Contains. Allows you to specify a substring that the queried field must contain, for example, *browser ~ "Mozilla/5.0"* 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\"'

Name	Description
	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, LogAn 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, LogAn automatically generates a search query string that matches the filter specified in the basic search mode.

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).

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 group of templates for events recorded in the event log.
- **IDPS**: a group of templates 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 group of templates for events recorded in the traffic log.
- **Web portal**: a group of templates for events related to authentication via SSL VPN.
- **Traffic**: a group of templates 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 group of templates for events related to VPN.
- **Web activity**: a group of templates 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.

COMMAND LINE INTERFACE (CLI)

GENERAL PROVISIONS

General Provisions (Description)

In UserGate LogAn, you can perform device configuration with the help of the command-line interface, or CLI.

CLI can be useful for troubleshooting network problems or when access to the web console is lost — for example, due to an incorrectly set interface IP address or erroneous zone access control settings that block connections to the web interface.

You can connect to the CLI using the standard VGA/keyboard ports (if physically present on the UserGate LogAn equipment), via the serial port, or via SSH over the network.

Attention!

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

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

Name	Description
Step 1. Connect a monitor and keyboard to the device	Connect a monitor to a VGA (HDMI) port and a keyboard to a USB port.
Step 2. Log in to the CLI.	Log in to the CLI using the login and password for a user with the root administrator permissions (the default is Admin).

To connect to the CLI using the serial port, follow these steps:

Name	Description
Step 1. Connect to the device	Use a special serial cable or a USB-Serial adapter to connect your computer to the device.
Step 2. Launch a terminal.	Launch a terminal that supports serial port connection, such as Putty for Windows or minicom for Linux. Establish a serial port connection using 115200 8n1 as the connection parameters.
Step 3. Log in to the CLI.	Log in to the CLI using the login and password for a user with the root administrator permissions (the default is Admin).

To connect to the CLI using the SSH protocol, follow these steps:

Name	Description
Step 1. Allow CLI (SSH) access for the selected zone.	Allow SSH access for the CLI protocol in the settings for the zone to which you want to connect for CLI management. The TCP port 2200 will be opened.
Step 2. Launch an SSH terminal.	Launch an SSH terminal on your computer, such as SSH for Linux or Putty for Windows. Specify LogAn address as the IP address, 2200 as the connection port, and the login of a user with root administrator permissions as the CLI login name (the default is Admin). For Linux, the connection command should look like this: *ssh Admin@IPUserGateLogAn -p 2200*
Step 3. Log in to the CLI.	Log in to the CLI using the password for the user specified in the previous step.

After successful authentication, a line will appear in the CLI waiting for a command to be entered (diagnostic mode). To view the current available options or use autocomplete, press **Tab**. Available values:

- **configure**: switch to the configuration mode
- **date**: view the current device date and time
- **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 available in the configuration mode. For more details, see the Execute Commands section.

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

All CLI commands have the following structure:

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

where:

<action> is the action to be performed;

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

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

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

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; levels correspond to the LogAn web interface sections.

<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.

Name	Description
	For example, to view information about all interfaces, run the following command: `Admin@nodename# show network interface` To go to the **network interface level, use the following command.** The current level will be displayed under the command line: `Admin@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`

Name	Description
	`` Admin@nodename# end Level: network Admin@nodename# ```
<level>	Levels in the command line follow the LogAn 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.
<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 for specifying the browser type (useragent). Some websites 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>```

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@LogAn# 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@UGOS# set settings device-mgmt licensing-upstream-proxy
<parameters>
```

The additional parameters are as follows:

Parameter	Description
enabled	Enabling/disabling license activation and software update mode via an external proxy server: • **on**: enabled • **off**: disabled
ip	The external proxy's IP address.
port	The external proxy's port.
auth	Authentication with the external proxy: • **on**: enabled • **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@UGOS# show settings device-mgmt licensing-upstream-proxy
```

System backup management

A device backup is created at the **settings device-mgmt** level. To create a backup rule and upload files to external FTP/SSH servers, use the following command:

```
Admin@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.
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 current LogAn 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	Passphrase: specify 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 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.
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.

Parameter	Description
	• **alert-threshold**: alert threshold; if the number of requests exceeds this value, the event is recorded in the system log. • **drop-threshold**: packet drop threshold; if the number of requests exceeds this value, UserGate drops packets and records this event in the system log. • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.
dos-protection-udp	Protect the zone against network flooding for UDP protocol: • **enabled**: enable/disable the protection. ◦ **on** ◦ **off** • **aggregate**: ◦ **on**: count all packets incoming to the zone's interfaces ◦ **off**: count packets for each IP address separately. • **alert-threshold**: alert threshold; if the number of requests exceeds this value, the event is recorded in the system log. • **drop-threshold**: packet drop threshold; if the number of requests exceeds this value, UserGate drops packets and records this event in the system log. • **excluded-ips**: list of IP addresses of servers that should be excluded from protection.

Parameter	Description
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: • **PING**: allow use of the ping command to a UserGate address. • **SNMP**: provides SNMP access to UserGate (UDP 161). • **Control XML RPC**: XML RPC for management. Allows product management via API (TCP 4040). • **CLI over SSH**: access to server to manage it via CLI, port TCP 2200. • **Log Analyzer**: the Log Analyzer service. Needs to be allowed in zones from which LogAn will receive the data sent by UserGate servers (TCP 1269). • **Log collector**: a service that enables information collection from remote devices using the Syslog protocol (the default port number is 514). • **Administrative Console**: access to the management web console (TCP 8001). • **Auth Agent**: RADIUS accounting authentication service (UDP 1813). (Available starting from version 7.2.0)
service-addresses	Allowed IP addresses for services: • **service**: select services (the list corresponds to **enabled-services**).

Parameter	Description
	• **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.
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	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** • **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.

Parameter	Description
	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. **Important!** You cannot delete the specified parameters.
ip-addresses	Assign an IP address to the interface. The IP addresses are specified as **[<ip_address/mask>]** or **[<ip_address/mask> <ip_address/mask>]**. In case of several IP addresses (with space used as the separator), the subnet mask is entered in the decimal format. **Important!** Make sure to separate the square brackets with spaces on both sides.
mac	Interface MAC address.
mtu	Specify the MTU size.
mss	Specifying the MSS size (available starting from version 7.3.x): 0, or starting from 4 to the value specified in MTU minus 40.

To delete an adapter or its parameters, use the following command:

```
Admin@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	

Parameter	Description
	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.
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	Specifying the MSS size (available starting from version 7.3.x): 0, or starting from 4 to the value specified in MTU minus 40.
dhcp-relay	Settings for the DHCP relay on the interface. You need to specify the following: • **enabled**: enable/disable the relay: ◦ **on** ◦ **off** • **utm-address**: IP address of the UserGate interface on which the relay function is added. • **server-address**: addresses of DHCP servers where DHCP requests from clients should be redirected.

To edit an existing VLAN, use the following command:

```
Admin@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.

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.
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).

Parameter	Description
	◦ **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 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.

Parameter	Description
	• **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. • **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.

Parameter	Description
	• 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.
mtu	Specify the MTU size.
mss	Specifying the MSS size (available starting from version 7.3.x): 0, or starting from 4 to the value specified in MTU minus 40.

To update an existing bond interface, use the following command:

```
Admin@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.

Parameter	Description
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.);

Parameter	Description
	• **auto**: after selecting this option, the port will be detected automatically. This option is available for nodes that have been initialized. For nodes that have not been initialized, the option is available starting with software release 7.3.0.
ip	Gateway IP address.
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**
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.

Parameter	Description
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 <parameter>
```

Provide the following parameters:

Parameter	Description
name	Address list name.
description	List description.
threat-lvl	Threat level: • **very-low**: very low threat level • **low**: low threat level • **medium**: medium threat level • **high**: high threat level • **very-high**: very high threat level.
type	List type: • **local**: local • **updatable**: if the list is updatable, specify URL address for downloading updates (**url**). List update frequency is set by the **schedule** parameter in the crontab format. Crontab format: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6; where 0 is Sunday). You can set each field as follows: • An asterisk (*) denotes the entire range (from the first number to the last).

Parameter	Description
	• A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".
lists	Select existing IP lists to add to the list being created.
ips	IP addresses or a range of IP addresses to include in the list. Format: <ip>, <ip/mask>, or <ip_range_start-ip_range_end>.

To edit a list (parameters available to update are identical to those used to create a list), use the following command:

```
Admin@nodename# set libraries ip-list <ip-list-name> <parameter>
```

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
```

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
```

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	

Parameter	Description
	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:

Parameter	Description
	`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 • **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.

Parameter	Description
	• **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>
```

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.

CONFIGURING THE USERS AND DEVICES SECTION

Configuring UserID Agent

The User'ID agent is designed to perform transparent authentication on selected UserGate devices. It uses Microsoft Active Directory logs (via the WMI protocol), Syslog (via the standardized syslog protocol RFC 3164, RFC 5424, RFC 6587), and RADIUS (starting with software release 7.2.0) as the source of the authentication data. The detailed information on the UserID agent can be found in the Users and Devices section of the NGFW Administrator Guide.

You configure UserID in the CLI at the **users userid-agent** level.

Configuring the UserID agent settings

The general settings of a UserID agent are configured using the following command:

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

To configure, you need to specify the following parameters:

Parameter	Description
polling-interval	Active Directory servers polling interval. The default value is 120 seconds.
syslog-monitoring-interval	Database poll period to look for syslog-source user session start/end events.
radius-monitoring-interval	Database poll period to look for user session start/end events in the RADIUS log. (This option is available starting from software version 7.2.0 and up).
ignore-network-list	Lists of IP addresses the events from which should be ignored by the UserID agent. A record about the ignored source appears in the **UserID agent** log. The list can be created in the libraries**(IP addresses)** section. This setting is global and applies to all sources.
ignore-user-list	Names of users the events from which should be ignored by the UserID agent. The search is based on the Common Name (CN) of the AD user. This setting is global and applies to all sources. A record about the ignored user appears in the UserID log. **Important!** When specifying a name, you can use the asterisk (*), but only at the end of a string.

Parameter	Description
sync	Synchronizing users with NGFW: • **on** • **off**

Configuring Event Source

Microsoft Active Directory

To add Microsoft Active Directory as an event source, use the following command:

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

To configure, you need to specify the following parameters:

Parameter	Description
enabled	Enable/disable receiving logs from the source.
name	The source name.
description	An optional description of the source.
address	Microsoft Active Directory address.
protocol	AD access protocol (WMI).
login	The username for connecting to AD.
password	The user's password for connecting to AD.
sharing-profile	A redistribution profile that describes the range of UserGate devices to which information about the found users will be sent. For more details, see Redistribution Profile.
expiration-time	The period of time after which the user's session will be forcibly terminated. The default value is 2700 seconds (45 minutes).
users-catalogs	Here you can select the LDAP connector to use to search for user information found in the logs by the UserID agent. You can select a previously configured directory or add a new directory.

Syslog-senders

To add a syslog sender as an event source, use the following command:

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

To configure, you need to specify the following parameters:

Parameter	Description
enabled	Enable/disable receiving logs from the source.
name	The source name.
description	The source description.
address	The host address from which UserGate will receive syslog events.
default-domain	The name of the domain used to search for users found in syslog logs.
timezone	The time zone set on the source.
sharing-profile	A redistribution profile that describes the range of UserGate devices to which information about the found users will be sent. For more details, see Redistribution Profile.
filters	Filters to find the necessary log entries. You can create and configure filters under **Libraries → UserID agent syslog filters of the agent.** For more details, see UserID agent Syslog filters.
users-catalogs	Here you can select the LDAP connector to use to search for user information found in the logs by the UserID agent. You can select a previously configured directory or add a new directory.
expiration-time	The period of time after which the user's session will be forcibly terminated. The default value is 2700 seconds (45 minutes).

RADIUS server

This option is available starting from software version 7.2.0 and up.

To add a RADIUS server as an event source, use the following command:

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

To configure, you need to specify the following parameters:

Parameter	Description
enabled	Enable/disable receiving logs from the source.
name	The source name.
description	The source description.
address	The host addresses from which UserGate will receive RADIUS events.
server-secret	Pre-shared key used by the RADIUS protocol for authentication.
default-domain	The name of the domain in which the user will be searched if the request does not explicitly indicate which domain the user belongs to.
sharing-profile	A redistribution profile that describes the range of UserGate devices to which information about the found users will be sent. For more details, see Redistribution Profile.
attribute-for-group	The radius attribute type number in which the user's group resides, by default the group is not checked.
attribute-for-name	The radius attribute type number in which the username resides, 1 by default.
users-catalogs	Here you can select the LDAP connector to use to search for user information found in the logs by the UserID agent. You can select a previously configured directory or add a new directory.
expiration-time	The period of time after which the user's session will be forcibly terminated. The default value is 2700 seconds (45 minutes).

Configuring the UserID redistribution profile

The UserID redistribution profiles are used to define the range of the UserGate devices to which information about the users found by the UserID agent is sent.

The UserID redistribution profiles are configured in CLI at the **users sharing-profile** level.

To configure the profile, run the following command:

```
Admin@nodename# create users sharing-profile <parameters>
```

To configure, you need to specify the following parameters:

Parameter	Description
name	Profile name.
description	An optional description of the profile.
sensors	Select the UserGate sensors to which information about the users will be sent.

SETTING UP SENSORS

Sensor Configuration (Description)

LogAn uses sensors to collect information from various devices for subsequent analysis. A sensor is a LogAn-compatible device that can send certain data to a LogAn 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 LogAn. To connect a UserGate sensor, follow these steps:

```
Admin@ngfw-nodename# set network zone <zone-name> enabled-services
[ SNMP "Log Analyzer" ]
```

```
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
```

```
Admin@nodename# set network zone <zone-name> enabled-services [ "Log
Analyzer" ]
```

To create a UserGate sensor, use the following command:

```
Admin@ndefornaledo# create sensors ug-sensors <parameters>
```

1. On **NGFW** allow the **Log Analyzer** and **SNMP** services in the required zone settings:
2. On **NGFW**, receive the device token:
3. On LogAn allow the **Log Analyzer** service in the required zone settings:
4. Create a UserGate sensor.

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.
logan-address	The IP address of the LogAn 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.

Parameter	Description
device-code	The token received on the UserGate node.

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

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 LogAn server to collect and analyze its metrics. LogAn 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:

```
Admin@nodename# create sensors snmp-sensors <parameters>
```

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.

Name	Description
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 LogAn server and network device for SNMP v2. Use only Latin letters and numbers.
interval	The time interval in seconds with which the LogAn 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.
counters	Specify all data here that LogAn should query from the network device. The counters can be selected from the MIBs uploaded to the device. Put the counter SNMP OID 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 LogAn 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 LogAn on the network device: • **name**: the counter name. • **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 LogAn device is selected on UGMC as a server for transmitting event information, while LogAn must be pre-registered on UGMC.

To view the endpoint data, run the following command:

```
Admin@nodename# show sensors endpoint-devices
```

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.

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

Read more about the SNMP parameters of the UserGate device in the SNMP section.

Configuring SNMP Monitoring Rules

To configure device monitoring rules via SNMP, commands are used at the **monitoring snmp** level:

```
Admin@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

Parameter	Description
	context on the SNMP server. The context is identified by name. When the client makes a request, the context name can be specified. If the context name is not specified, the default context will be requested.
version	Specify the version of the SNMP protocol used in the rule. Available options: SNMP v2c and SNMP v3.
query	When enabled, allows receiving and processing of SNMP requests from the SNMP manager.
trap	When enabled, allows sending of SNMP traps to the server configured to receive notifications.
trap-host	Server IP address for traps. This setting is required only if you need to send traps to the notification server.
trap-port	The port on which the server listens for notifications. Usually, it is UDP port 162. This setting is required only if you need to send traps to the notification server.
security-profile	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

Parameter	Description
description	SNMP security profile description
username	User name to authenticate the SNMP manager.
auth-type	Select an authentication mode for the SNMP manager. The available options are: • **none**: no authentication, no encryption • **no-encrypt** : authentication, no encryption • **encrypt**: authentication, encryption The authPriv mode is considered the most secure.
auth-alg	The algorithm used for authentication. Possible to use: • **sha** • **md5** • **sha224** • **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.

Parameter	Description
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.
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.

DASHBOARD

Working with Dashboards and Widgets

In UserGate LogAn, you can monitor the current status of your device and the sensors connected to it, as well as information about their loading, license status, and other details. This data is presented as widgets on the **Dashboards** page. You can customize widgets according to your requirements.

> **Note**
>
> **You can view and edit dashboards if your account's access profile has the appropriate permissions configured.**

You can add new dashboards, rename them, and delete them, select the desired widgets from the collections supplied with the product, and change the composition of widgets on dashboards, their location, and size. There are predefined dashboards

with widgets for Log Analyzer (UserGate LogAn state), NOC (Network Operation Center), and SOC (Security Operation Center).

Depending on the data type, widgets are divided into collections:

- **Network Operations Center**;
- **Security Operations Center**;
- **VPN group**;
- **Endpoints**;
- **Syslog**

The widgets in the **Security Operations Center** and **VPN Group**, **Endpoints** and **Syslog** collections graphically present data from UserGate LogAn logs. Therefore, in order for the data to be displayed in the widget, you need to set up the appropriate rules and enable event logging for them. For example, if a VPN is configured and logging is enabled, you can track statistics for widgets in the **VPN Group** collection.

By default, the widget displays data for the last hour. You can change the period for each widget by selecting a preset option in the upper right part of the widget. In chart widgets, you can also highlight a portion of a period to get a closer look at a specific part of the chart. To return to the original scale, double-click the left mouse button.

Widget Configuration

For some widgets, you can filter data and customize how it is displayed. If the setting is available, a gear icon will appear in the upper right corner of the widget.

To configure a widget:

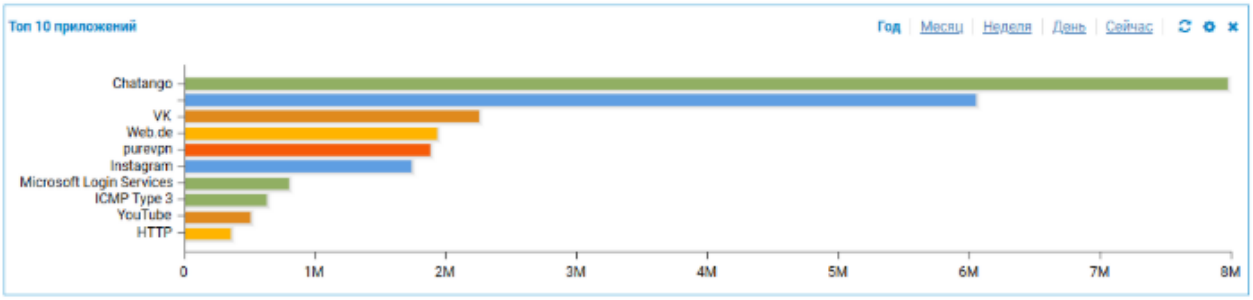
1. Click on the gear icon in the upper right corner of the desired widget.
2. In the **Widget settings** window, perform one or more actions (depending on the widget type, the set of parameters may differ):
    - change the widget name;
    - specify the maximum number of entries to be displayed in the widget;
    - select the value by which the data in the widget will be grouped;
    - select the type of chart or table in which the data will be presented;

- use an SQL query to set up filtering of the data displayed in the widget;
- add the widget description;
- using the **Add** button, select the sensors whose data will be displayed in the widget.

1. Click **Save**.

An Example of Data Filtering in a Widget

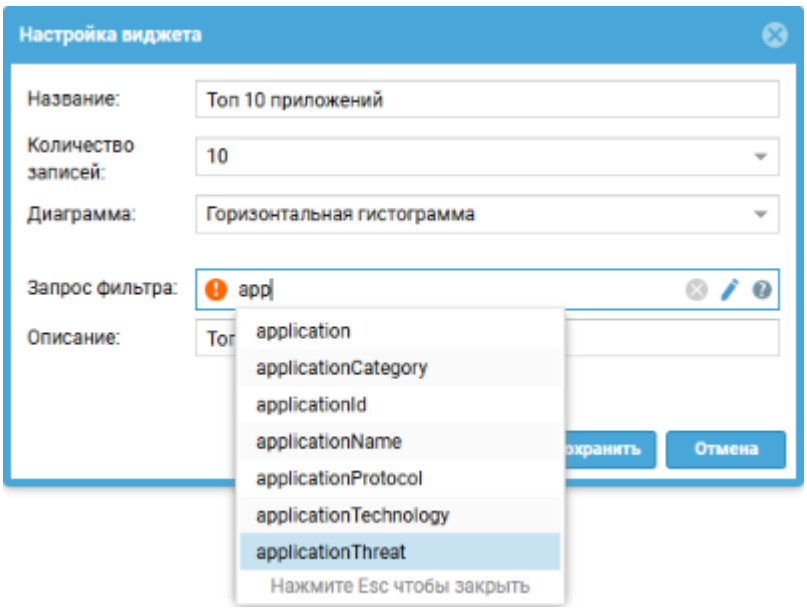
A **Top 10 Applications** widget has been added to the dashboard, which by default displays various applications, including those that pose no threat.



To enable the widget to track only dangerous applications, you need to configure additional data filtering using an SQL query in the **Widget settings** window in the **Filter query** field.

SQL queries use the same syntax as logs to search and filter data. For keywords and operators with examples of their use, see the Data Search and Filtering section. The parameter values are collected from events in the log.

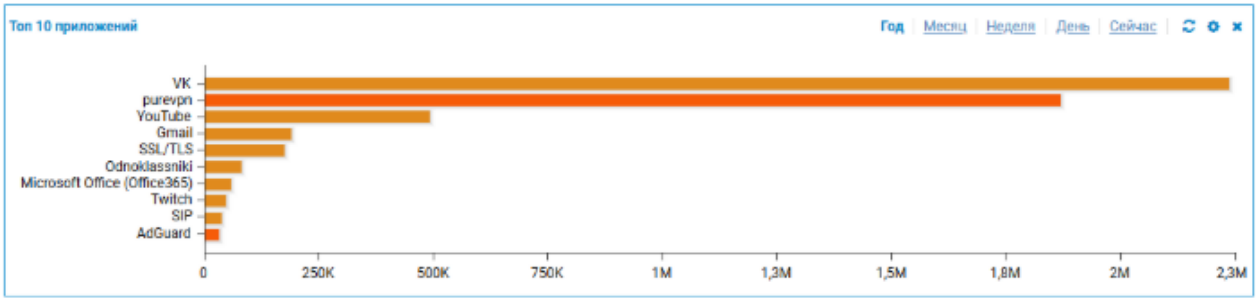
When you enter a query, a list of available operators, parameters, and their values is displayed in the field, from which you can form the desired query.



The query to filter dangerous and very dangerous applications looks like this:

```
applicationThreat in (high, 'very high')
```

Once setup and data updates are complete, the widget will only display dangerous and very dangerous apps.



TECHNICAL SUPPORT

Technical Support (Description)

Visit the technical support section on the UserGate website, https://support.usergate.com/, for more information on how to configure LogAn. This is also where you can submit a ticket to resolve your problem.

ADMIN

General Information

This section allows registered administrators to change their passwords, update some profile settings and log out.

Name	Description
Change password	To change your password, enter your current password and then the new one twice.
Preferences	• Show items per page: number of lines to display in one dialog box, such as a list of firewall rules. • Night mode: set the dark theme for the UGOS GUI. • 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 LogAn 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.

Service	Protocol	Port	Outbound/ Inbound	Function
DNS	UDP	53	Outbound (to DNS servers)	The service that resolves domain names into IP addresses.
UserGate server registration	TCP	443	Outbound (to the registration server)	Access to the UserGate product registration server (reg2.usergate.com).
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 LogAn to UGMC)	Initial communication and exchange of encryption keys with the UGMC server.
		2022	Outbound (from LogAn to UGMC)	Build an SSH tunnel to exchange data using the received keys.
LogAn service	TCP	9713	Outbound (from LogAn to NGFW)	Initial communication and exchange of encryption keys with the NGFW server.
		2023	Outbound (from LogAn to NGFW)	Build an SSH tunnel to exchange data using

Service	Protocol	Port	Outbound/ Inbound	Function
				the received keys.
	TCP	22699 (receive data from NGFW 6.x.x), 22711 (receive data from NGFW 7.x.x that uses SSL)	Inbound (from NGFW to LogAn)	The LogAn log collection service.
SNMP	UDP	161	Inbound (to LogAn)	Access to the UserGate server via SNMP.
Log Collector	TCP/UDP	514	Inbound (to LogAn)	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		

Service	Protocol	Port	Outbound/ Inbound	Function
			Outbound (to a TACACS+ authenticatio n server)	User authenticatio n via the TACACS+ protocol.
FTP (logs export)	TCP	21	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
	Severity		

Field type	Field name	Description	Example value
		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_BUILTIN_COMPOSITE", "module":"nlist_import"}

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

Field type	Field name	Description	Example value
	cs5Label	Indicates the destination country.	Destination Country
	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

Field type	Field name	Description	Example value
	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.	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","

Field type	Field name	Description	Example value
			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.	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

Field type	Field name	Description	Example value
	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 from the source to the destination).	231
	out	Number of transmitted outbound bytes (data transferred	40

Field type	Field name	Description	Example value
		from the destination to the source).	
	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.	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

Field type	Field name	Description	Example value
	cs4	Destination zone name.	Untrusted
	cs5Label	Indicates the destination country.	Destination Country
	cs5	Destination country name.	AE (a two-letter country code is displayed)
	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

Field type	Field name	Description	Example value
	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 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

Field type	Field name	Description	Example value
	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)
	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

Field type	Field name	Description	Example value
	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

Field type	Field name	Description	Example value
	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
	msg	Signature threat level and name.	[2] BlackSun

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.	IDPS 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
	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

Field type	Field name	Description	Example value
	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
	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.

Field type	Field name	Description	Example value
	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

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

Field type	Field name	Description	Example value
			• 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
	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

Field type	Field name	Description	Example value
	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 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

Field type	Field name	Description	Example value
	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 (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		Rule

Field type	Field name	Description	Example value
		Indicates that a rule was triggered.	
	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
	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
	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.

Field type	Field name	Description	Example value
	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.	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

Field type	Field name	Description	Example value
	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 (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.

Field type	Field name	Description	Example value
	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
	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)

Field type	Field name	Description	Example value
	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
	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

Field type	Field name	Description	Example value
	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 (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	10

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).	10
	cs1Label	Indicates the rule name.	Rule
	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

Field type	Field name	Description	Example value
	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; • 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

Field type	Field name	Description	Example value
	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
	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

Field type	Field name	Description	Example value
	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	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	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 taken by the device according to the configured policies.	accept
	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

Field type	Field name	Description	Example value
	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
	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	1652344423822

Field type	Field name	Description	Example value
		(in milliseconds since January 1, 1970).	
	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
	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

Field type	Field name	Description	Example value
	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

Field type	Field name	Description	Example value
	spid	Process ID.	3860
	fileHash	The application hash.	B4979A9F970029889713D756C3F123643DDE73DA
	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	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

Field type	Field name	Description	Example value
	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 since January 1, 1970).	1652344423822
	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_00

Field type	Field name	Description	Example value
			02\ \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

Field type	Field name	Description	Example value
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/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

Field type	Field name	Description	Example value
	cs2Label	Indicates the application that caused the event.	Tag
	cs2	Application triggering 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
	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
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1701085036026

Field type	Field name	Description	Example value
	deviceExternalId	The unique name of the device that generated the event.	utmcore@ntoorereaeda
	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

Field type	Field name	Description	Example value
	Source	Log name.	userid
	Name	Source type.	log
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.	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

Field type	Field name	Description	Example value
	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":"Asia/ 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	The module in which the event occurred.	core
event_component	The component in which 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.	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		http://www.secure.com

Field name			Description	Example value
			Contains the URL of the requested resource and the protocol used.	
media_type			The type of the content.	application/json
status_code			Status code.	302
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_pr otocol	Application layer protocol and its version.	HTTP\/1.1"
url_cat egories	**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

Field name			Description	Example value
	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.
	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
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

Field name			Description	Example value
action			Action taken by the device according to the configured policies.	block
application		**id**	Application ID.	5
		name	Application name.	
		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

Field name			Description	Example value
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.	
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		100

Field name			Description	Example value
			Number of bytes transmitted from the source to the destination.	
bytes_recv			Number of bytes transmitted from the destination to the source.	6
packets_recv			Number of packets transmitted from the destination to the source.	1
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.

Field name			Description	Example value
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.
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

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

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

Field name			Description	Example value
application	**id**		Application ID.	195
	threat_level		Application threat level.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 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

Field name			Description	Example value
	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
	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		The unique name of the device that generated the event.	utmcore@ersthetatica
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

Field name		Description	Example value
	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
	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

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.
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.
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

Field name			Description	Example value
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
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

Field name			Description	Example value
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
	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

Field name			Description	Example value
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
		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

Field name			Description	Example value
	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
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

Field name	Description	Example value
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
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
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

Field name		Description	Example value
	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

Field name	Description	Example value
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	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
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		utmcore@ntoorereaeda

Field name		Description	Example value
		The unique name of the device that generated the event.	
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
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

Field name		Description	Example value
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
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	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			

Field name			Description	Example value
			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}
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-4e92-8331-23 9406ec34da
	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: 00000000-0000-0000-000 0-000000000000.	745591c3-9d21-092d-8db4-5 b9b0000044f
	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=l ocal