UserGate SIEM 7.1.0 Administrator Guide

Table of Contents

INTRODUCTION

Introduction (Description)

UserGate SIEM (SIEM) is a solution based on the UserGate Log Analyzer (LogAn) product that implements functions of a SIEM (Security Information and Event Management) and an IRP (Incident Response Platform) system.

A SIEM system is a system that manages security information and information security events. SIEM collects and stores data from various sources (sensors), such as UserGate Next-Generation Firewalls, UserGate endpoints control and monitoring systems, SNMP sensors, and WMI sensors. The processing result is presented in a unified interface, which makes it easier to study the unique patterns of security incidents. Based on the received data, SIEM in real time uses analytics rules to aggregate and correlate repeating events, producing cybersecurity incidents as a result. Incident response rules provide a way to determine automatically how to respond to information security incidents.

To investigate cybersecurity incidents, an IRP system is used that is part of SIEM. An IRP system is a platform for managing the processes of responding to information security incidents. SIEM allows you to customize the incident investigation process to the needs of a specific company.

SIEM 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.

SIEM LICENSING

SIEM Licensing (Description)

The UserGate SIEM solution is based on the LogAn product. SIEM licensing requires a license with the basic LogAn functions and add-on modules that provide access to SIEM functionality.

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

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

> **Note**
> **When a SIEM module is added to a LogAn license, the administrator is alerted that the server role has changed. The server role will be changed automatically.**

The following modules can be additionally licensed:

Name	Description
Security Update (SU) Module	The SU module grants the right to receive LogAn software updates. The module is licensed as an annual subscription. After one year, you will need to renew the license to continue receiving software updates.
Sensors	This module determines the number of sensors from which LogAn can collect information. The module is licensed as an annual subscription. After one year, you will need to renew to continue the use.
SIEM Functionality Module	This module provides access to the functionality of SIEM and IRP systems: create and configure analytics rules and define response where these rules are triggered. The module entitles you to use the SIEM functionality indefinitely.
SIEM Expertise Subscription Module	An add-on module to the SIEM Functionality licensing module. This module entitles you to obtain UserGate expertise: • Update of the library of analytics rules; • Update of the library of UserGate remote device management commands. The module is licensed as an annual subscription. When the license expires, the libraries you have downloaded while the license was valid remain operational, but they cannot be updated any more: you will need to renew your license to receive updates.

To register the product, follow these steps:

Name	Description
Step 1. Go to the Dashboard.	Click the **Dashboard** icon in the top right corner.
Step 2. Register the product in the **License** section.	In the **License** section, click **No license**, enter the PIN code, and complete the registration form. If a UserGate node is in a closed loop without direct access to the Internet, it is possible to activate/update the license through a proxy server. To do this, select **Use a proxy server for activation and updates**. 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.

You can view the status of the installed license in the **License** widget of the **Dashboard**.

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.

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 2nd interface of the virtual machine.
Step 6. Perform factory reset.	Start the LogAn VM. During loading, select **Support Menu** and then **Factory reset**. **T his 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.

To perform the initial configuration, follow these steps:

Name	Description
Step 1. Connect to the management interface.	**When a DHCP Server Is Used**Connect the port0 interface to the corporate network with a working DHCP server. 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 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.
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.

Name	Description
	• 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 SIEM Licensing chapter.
Step 9. (Optional) Create additional administrators.	In the **Administrators** section, create additional system administrators and grant them the necessary rights (roles).

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

OFFLINE SERVER OPERATIONS

Offline Server Operations (Description)

Some server maintenance operations are carried out when the server is not running and is offline. To perform such operations, select **Support menu** when the server is booting and then select the desired operation. To access this menu, connect a monitor to a VGA (HDMI) port and a keyboard to a USB port (if these ports exist on the device) or use a special serial cable or a USB-Serial adapter to connect your computer to 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 and output diagnostic information about the boot process to the serial port.
UGOS LOGAN (failsafe)	Boot UserGate in simplified video mode.
Support menu	Enter the system utilities section and send output to tty1 (the monitor).
Restore previous version	This section is available after updating or creating a system backup.

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

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

SIEM CONFIGURATION

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. • **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 (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**: purge logs of content.
Remote assistance	• **On/Off**: enable/disable the remote assistance mode. Remote assistance allows a UserGate support engineer to connect securely to a 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.

Name	Description
	• **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.
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 SIEM Licensing). If there are any updates, a notification to that effect will display in the **Device management** section. As a product update can take quite a while, it is recommended to account for the potential LogAn downtime when planning update installation.

To install updates, follow these steps:

Name	Description
Step 1. Create a backup file.	Создать резервную копию состояния LogAn, как это описано в разделе Системные утилиты. 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. To interrupt the backup process, press the **Stop** button. The backup record will be displayed in the device event log.

To restore the device status, follow these steps:

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

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

Name	Description
Step 1. Create a backup export rule	In the **Device management → System backup management**, click **Add** and enter a name and description for the rule.
Step 2. Specify the remote server parameters	In the **Remote server** tab of the rule, specify the parameters for the remote server: • **Server type**: FTP or SSH • **Address**: the server's IP address • **Port**: the server's port • **Login name**: the user account on the remote server • **Password**/**Repeat password**: the password for the user account • **Directory path**: the path on the server where the settings will be uploaded If using an SSH server, you can use key authorization. To import or generate a key, select **SSH key setup** and specify **Generate key** or **Import key**. **Important!** If you re-create a key, the existing SSH key will be deleted. The public key must reside on the SSH server in the user keys directory **/home/user/.ssh/** in the **authorized_keys** file. When initially configuring the SSH backup export rule, connection verification is mandatory (**Check connection** button). When the connection is verified, the fingerprint is placed in known_hosts. The files are not sent without verification. **Important!** If you change the SSH server or reinstall it, the backup files will be unavailable, because the fingerprint has changed. This protects you from spoofing.
Step 3. Select the upload schedule	In the **Schedule** tab of the rule, specify when the settings should be uploaded. If specifying the time in the crontab-format, enter it as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday) Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • 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.

Name	Description
	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. Export the settings.	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: 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. Examples: logan_core-logan_core@ranreahattha_6.2.0.13494RS-1_20211227_091350.bin; 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
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. • **Add LDAP user**: add a user from an existing domain. This requires a correctly configured LDAP connector in the **Auth servers** section. When logging in to the administrative console, the username must be specified in the user@domain format. Assign this user a profile created earlier. • **Add LDAP group**: add a user group from an existing domain. This requires a correctly configured LDAP connector in the **Auth servers** section. When logging in to the administrative console, the username must be specified in the user@domain format. Assign this user a profile created earlier. • **Add administrator with auth profile**: create a user and assign them an administrator profile created earlier and an auth profile (this requires correctly configured auth servers).

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

Name	Description
Name	Profile name.

Name	Description
Description	Profile description.
Permissions	The list of web console tree objects available for delegation. The following access options are available: • No access • Read only • Read and write.
User roles	Defines the user roles for performing actions on incidents and analytics rules assigned to the administrators with this profile. For more details on roles, see the User Roles and Role Permissions section.

Note

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

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**.

Name	Description
	• **Block time**: the time for which the account is blocked.

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.

Name	Description
	• **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.
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.

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

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

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

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

RADIUS Authentication Server

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

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

Name	Description
Enabled	Enables or disables the use of this authentication server.

Name	Description
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.

Name	Description
Timeout (sec.)	The authentication timeout for the TACACS+ server. The default is 4 seconds.

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

Authentication Profiles

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

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

User Roles and Role Permissions

A user role is a set of role permissions. A role permission grants an administrator the ability to perform certain actions – e.g., add or remove an attachment from an existing incident, create a triggered alert rule, create or close an incident, etc. Roles are assigned to administrator profiles, which are, in turn, assigned to administrators. For more details on creating administrators and administrator profiles, see the section Administrators.

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

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

Name	Description
Step 2. Add the desired permissions to the role just created.	

The following role permissions can be added for users:

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

Name	Description
	You can comment on an incident in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Activity** section.
Delete all comments	The ability to delete any comments made on incidents. You can view the comments for an incident in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Activity** section.
Delete own comments	The ability to delete own comments made on incidents. You can view the comments for an incident in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Activity** section.
Edit all comments	The ability to edit all comments made on incidents. You can view the comments for an incident in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Activity** section.
Edit own comments	The ability to edit own comments made on incidents. You can view the comments for an incident in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Activity** section.
Create attachments	The ability to create attachments to incidents. Attachments can be added to an incident in the **Incidents** tab during the creation or editing of the incident. The attachments are displayed in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Attachments** section.
Delete all attachments	The ability to delete all attachments. The incident's attachments are displayed in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Attachments** section.
Delete own attachments	The ability to delete own attachments. The incident's attachments are displayed in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Attachments** section.
Edit observables	The ability to create and edit observables. Observables can be added in the **Incidents →** tab, where N is the ordinal number of the incident, in the **Observables** section. For more details on observables, see the section Incident Details.
Update enrichments	The ability to update observables' enrichments.

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

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

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

Name	Description
	UserGate sensors can be created under **Sensors → UserGate sensors** in the **Settings** tab. For more details, see UserGate Sensors.
Edit a UserGate sensor	The ability to edit UserGate sensors. UserGate sensors are available under **Sensors → UserGate sensors** in the **Settings** tab. For more details, see UserGate Sensors.
Enable/disable a UserGate sensor	The ability to enable/disable UserGate sensors. UserGate sensors are available under **Sensors → UserGate sensors** in the **Settings** tab. For more details, see UserGate Sensors.
Delete a UserGate sensor	The ability to delete UserGate sensors. UserGate sensors are available under **Sensors → UserGate sensors** in the **Settings** tab. For more details, see UserGate Sensors.
Create SNMP sensor	The ability to create SNMP sensors. SNMP sensors can be created under **Sensors → SNMP sensors** in the **General settings** tab. For more details, see the SNMP Sensors section.
Edit SNMP sensors	The ability to edit SNMP sensors. SNMP sensors are available under **Sensors → SNMP sensors** in the **General settings** tab. For more details, see the SNMP Sensors section.
Enable/disable SNMP sensor	The ability to enable/disable SNMP sensors. SNMP sensors are available under **Sensors → SNMP sensors** in the **General settings** tab. For more details, see the SNMP Sensors section.
Delete a SNMP sensor	The ability to delete SNMP sensors. SNMP sensors are available under **Sensors → SNMP sensors** in the **General settings** tab. For more details, see the SNMP Sensors section.
Create WMI sensor	The ability to create WMI sensors. WMI sensors can be created under **Sensors → WMI sensors** in the **General settings** tab. For more details, see the section WMI Sensors.
Edit WMI sensors	The ability to edit WMI sensors.

Name	Description
	WMI sensors are available under **Sensors → WMI sensors** in the **General settings** tab. For more details, see the section WMI Sensors.
Enable/disable WMI sensor	The ability to enable/disable WMI sensors. WMI sensors are available under **Sensors → WMI sensors** in the **General settings** tab. For more details, see the section WMI Sensors.
Delete a WMI sensor	The ability to delete WMI sensors. WMI sensors are available under **Sensors → WMI sensors** in the **General settings** tab. For more details, see the section WMI Sensors.
Add SNMP MIB file	The ability to add SNMP MIB files. MIB files can be added under **Sensors → SNMP MIB management** in the **General settings** tab. For more details, see the SNMP MIB Management section.
Delete SNMP MIB file	The ability to delete SNMP MIB files. MIB files are displayed under **Sensors → SNMP MIB management** in the **General settings** tab. For more details, see the SNMP MIB Management section.
Create Syslog rule	The ability to create Syslog rules. Syslog rules can be created in the **Log Collector → Syslog** section of the **General settings** tab.
Delete Syslog rule	The ability to delete Syslog rules. Syslog rules are displayed in the **Log Collector → Syslog** section of the **General settings** tab.
Edit Syslog rule and Syslog connector	The ability to edit Syslog rules and configure Syslog. The created Syslog rules are available in the **Log Collector → Syslog** section of the **General settings** tab.
Enable/disable Syslog rule	The ability to enable or disable Syslog rules. Syslog rules are available in the **Log Collector → Syslog** section of the **General settings** tab.
Create email group	The ability to create emails and email groups. Emails and email groups can be created in the **Libraries → Emails** section of the **General settings** tab. For more details, see the section Phones.

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

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

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

User Catalogs

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

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

Expanding the system partition

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

Name	Description
Step 1. Add an new virtual disk.	Use the hypervisor to add a **new** disk of the required size in the UserGate virtual machine properties.
Step 2. Expand the partition size in the system utilities.	In the UserGate node boot menu, enter the **Support menu** section.

Name	Description
	In the section that opens, select **Expand data partition** and start the partition expansion process.
Step 3. Check the size of the system partition.	When the expansion process is complete, boot the node and check the size of the system partition in the **Dashboard → Disk s** section.

Note

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

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.
Step 3. (Optional) Configure the access control settings for the zone.	Specify the LogAn-provided services that will be available to clients connected to this zone. It is recommended to disable all services for zones connected to uncontrolled networks, such as the Internet. The following services exist: • **Ping**: enables pinging of LogAn. • **SNMP**: provides SNMP access to LogAn (UDP 161). • **Control XML-RPC**: enables API control of the product (TCP 4040). • **Administrative console**: provides access to the administrative web console (TCP 8010). • **CLI over SSH**: provides server access for management using CLI (command line interface) (TCP port 2200).

Name	Description
	• **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). For more on network availability requirements, see Appendix 1. Network Environment Requirements.
Step 4. (Optional) Configure the IP spoofing protection settings.	IP spoofing attacks allow a malicious actor to transmit a packet from one network, such as **Trusted**, to another, such as **Manage ment**. To do that, the attacker substitutes the source IP address with an assumed address of the relevant network. In this case, responses to this packet will be sent to the internal address. To protect against this kind of attack, the administrator can specify the source IP address ranges allowed in the selected zone. Network packets with source IP addresses other than those specified will be discarded. Using the Negate checkbox, the administrator can specify the source IP addresses from which packets may not be received on 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 and MTU size.
- Select the IP address assignment type: no address, a static IP address, or a dynamic IP address obtained using DHCP.

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

- VLAN
- Bond.

Bonding Network Interfaces

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

Name	Description
Enabled	Enables the bond.
Name	The bond name.
Zone	The zone to which the bond belongs.
Interfaces	One or more network interfaces that will be used to create the bond.
Aggregation mode	The aggregation mode must match the operating mode for the device to which the bond is connected. The options are: • **Round robin**. Packets are sent consecutively, starting from the first available slave and continuing to the last one. This policy is used to provide load balancing and high availability. • **Active backup**. Only one network interface in the bond will be active. Another slave interface can become active only if the currently active interface fails. With this policy, the MAC address of the bond interface is only visible externally through one network port to avoid problems with the switch. This policy is used for high availability. • **XOR**. Transmission is distributed between the slave interfaces using the formula: [(XOR) MOD]. This means that the same NIC sends packets to the same recipients. Optionally, the transmission allocation can also be based on the xmit_hash policy. The XOR policy is used to provide load balancing and high availability. • **Broadcast**. Transmits everything on all network interfaces. This policy is used for high availability. • **IEEE 802.3ad**. The default mode, supported by most network switches. Creates aggregated groups of NICs with identical speed and duplex settings. When combined like this, all links in the active aggregation participate in transmission as per IEEE 802.3ad. The

Name	Description
	choice of interface for packet transmission is determined by the policy. By default, the XOR policy is used, with the xmit_hash policy as a possible alternative. • **Adaptive transmit load balancing**. The outgoing traffic is distributed depending on the load on each slave interface (determined by the download speed). No additional configuration on the switch is required. The incoming traffic is received by the current network card. If this card fails, another card assumes the MAC address of the failed one. • **Adaptive load balancing**. Includes the previous policy plus incoming traffic balancing. No additional configuration on the switch is required. The incoming traffic is balanced through ARP negotiation. The driver intercepts ARP responses sent from the local NICs to the outside and overwrites the source MAC address with one of the unique MAC addresses of the NIC in the bond. Thus, different peers use different server MAC addresses. The incoming traffic is balanced sequentially (round-robin) among the interfaces.
MII monitoring period (msec)	Sets the MII monitoring period in milliseconds. Determines how often the link state will be checked for failures. The default value of 0 disables MII monitoring.
Down delay (msec)	Sets the delay in milliseconds before disabling the interface on a connection failure. This option is only valid for MII monitoring (miimon). The parameter value must be a multiple of miimon, otherwise it will be rounded to the nearest multiple. Default value: 0.
Up delay (msec)	Sets the delay in milliseconds before bringing up the link on discovering that it has been restored. This parameter is only valid with MII monitoring (miimon). The parameter value must be a multiple of miimon, otherwise it will be rounded to the nearest multiple. Default value: 0.
LACP rate	Determines the interval between LACPDU packets sent by the partner in the 802.3ad mode. Enumerated options: • **Slow**: requests that the partner send LACPDU packets every 30 seconds. • **Fast**: requests that the partner send LACPDU packets every second.
Failover MAC	Determines how MAC addresses will be assigned to the bonded slaves in the active-backup mode on switching

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

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.

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 **Ad d**. 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.

USERS AND DEVICES

User-ID agent

Description

The User'ID agent is designed to perform transparent authentication on selected UserGate devices. It uses Microsoft Active Directory logs (via the WMI protocol) and Syslog (via the standardized syslog protocol RFC 3164, RFC 5424, RFC 6587) as the source of the authentication data.

How it works

The UserID agent makes periodical queries to the database to search for user logon/logoff events. The search is performed only on the records obtained through UserID sources, i.e. other records (obtained through WMI sensors, endpoint devices, or log collectors) are ignored. Based on the obtained data, it searches for the user in the user catalogs of the log source. If the user is found, the user authorization data is sent to all NGFW devices specified in the source redistribution profile. Thus, the user is authorized on all the specified devices. It is similar in case of the user logout (except for Microsoft Active Directory, where user logout data is not processed at the moment). The information about logon/logoff/error is stored in the UserID log.

Note

Events received from sources are displayed in the UserID logs on the Logs and reports.

Settings

In general, to configure collecting information from sources, you follow these steps:

Name	Description
Step 1. Configure the UserID agent settings.	To do it, click **Configure agent** button under **Users and devices → UserID agent**.
Step 2. Configure the event source.	You can use Microsoft Active Directory or Syslog as sources.

When configuring the agent, you must fill in the following fields:

Name	Description
Polling interval (sec.)	Active Directory servers polling interval. The default value is 120 seconds.
Session expiration time (sec.)	The period of time after which the user's session will be forcibly terminated. The default value is 2700 seconds (45 minutes).
Syslog Monitoring Interval (sec.)	Database poll period to look for syslog-source user session start/end events.
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. You can create the list in the **Libraries → IP addresses** or when configuring the agent (**Create and add new object** button). For more details about how to create and configure IP address lists, see IP addresses. 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.

Note
When NGFW connects to the Log Analyzer, UserID agents configured on both devices can operate simultaneously. The device agents will run independently of each other. UserID agent log events received by NGFW, as well as other log events, will be sent to LogAn.

Microsoft Active Directory

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

Name	Description
Step 1. Configure the UserID agent settings for monitor Microsoft AD.	The UserID agent parameters were discussed earlier.
Step 3. Configure the event source.	Configure Microsoft Active Directory as the source. See below for more information on the source settings.

When using AD servers as event sources, UserGate performs WMI queries to search for successful logon events (event ID 4624), Kerberos events (event numbers: 4768, 4769, 4770) and group membership events (event ID 4627). The frequency of the queries execution is defined by the UserID agent settings (**Polling interval** parameter). The found events are displayed on the **Logs and reports**, under **Logs → Endpoint devices → Events**.

When adding an event source of Microsoft Active Directory type, you need to specify the following:

Name	Description
Enabled	Enable/disable receiving logs from the source.
Name	The source name.
Description	An optional description of the source.
Server address	Microsoft Active Directory address.
Protocol	AD access protocol (WMI).
Name	The username for connecting to AD.
Пароль	The user's password for connecting to AD.

Name	Description
Redistribution 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.
Каталоги пользователей	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

Note

For the UserID log collector to work properly, you must configure the Syslog server to send logs to the UserID agent address. For more details, see the Syslog documentation.

To configure the event source, follow these steps:

Name	Description
Step 1. Allow collecting information from remote devices using the Syslog protocol.	Under **Network→ Zones**, enable the **Log collector**service for the zone in which the Syslog servers are located.
Step 2. Configure the UserID agent settings to monitor the Syslog server.	The UserID agent parameters were discussed earlier.
Step 3. Configure the event source.	Configure the Syslog server as the source. See below for more information on the source settings.

When adding a source of Syslog type, you need to specify the following:

Name	Description
Enabled	Enable/disable receiving logs from the source.
Name	The source name.
Description	The source description.
Server address	The host address from which UserGate will receive syslog events.

Name	Description
Default domain	The name of the domain used to search for users found in syslog logs.
Timezone	The time zone set on the source.
Redistribution 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.
Фильтры	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.
User 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.

The found events are displayed on the **Logs and reports**, under **Logs → User-ID agent → Syslog**.

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 **Setti ngs**.

Note

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

COMMAND LINE INTERFACE (CLI)

Command Line Interface — CLI (Description)

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

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

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

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

Name	Description
Step 1. Connect a monitor and keyboard to the UserGate LogAn 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 name and password for a user with Full administrator permissions (the default is Admin).

Note

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

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

Name	Description
Step 1. Connect to the UserGate LogAn device.	Use a special serial cable or a USB-Serial adapter to connect your computer to the UserGate LogAn 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 name and password for a user with Full administrator permissions (the default is Admin). If the UserGate LogAn device has not undergone initial setup, use Admin as the login and utm as the password for accessing the CLI.

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

Name	Description
Step 1. Allow CLI (SSH) access for the selected zone.	Allow SSH access for the CLI protocol in the settings for the zone to which you want to connect for CLI management. The TCP port 2200 will be opened.
Step 2. Launch an SSH terminal.	Launch an SSH terminal on your computer, such as SSH for Linux or Putty for Windows. Specify UserGate LogAn's address as the IP address, 2200 as the connection port, and the login of a user with Full 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. If the UserGate LogAn device has not undergone initial setup, use Admin as the login and utm as the password for accessing the CLI.

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

help command

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

help iface

The full list of commands is presented below:

Name	Description
help	Lists the available commands.
exit quit Ctrl+D	Log out of the CLI.
date	View the current server time.
gateway	View or configure the gateway settings. For detailed information, see "gateway help".
iface	A set of commands used to view and configure network interface settings. For detailed information, see "iface help".
license	View the license information.
netcheck	Check the availability of a 3rd party HTTP/HTTPS server. **netcheck [-t TIMEOUT] [-d] URL** Options: -t: the maximum timeout for a server response. -d: request the website's content. Only headers are requested by default.
nslookup	Determine the IP address from a host name.
ping	Ping a specific host.
radmin	Enable or disable remote server access for UserGate LogAn technical support.
radmin_e	Enable or disable remote server access for UserGate LogAn technical support in case of a UserGate LogAn server freeze.
reboot	Reboot the UserGate LogAn server.
route	Create, modify, or delete a route.
shutdown	Shut down the UserGate LogAn server.
traceroute	Traceroute the connection to a specific host.
zone	A set of commands used to view and configure zone settings. For detailed information, see "zone help".

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 LogAn. A sensor can be NGFW, 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** 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** and **SN MP** services.
Step 2. On the UserGate node, copy the token to the clipboard.	On the UserGate node that you want to add as a sensor, go to the **General settings → Log Analyzer** section and copy the token value to the clipboard. It will be needed at Step 4.
Step 3. On LogAn, enable the Log Analyzer 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 Analyzer 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.

Name	Description
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 **General settings → Log Analyzer** section, the Log Analyzer server address has changed to the one specified during the creation of 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.

Name	Description
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.
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.

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.

Connectors

Connectors are used to connect the LogAn node to various security tools to collect information.

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

Name	Description
Name	Connector name.
Description	An optional description of the connector.
Server type	Select the server type: • **SSH** • **HTTP** • **HTTPS**
Server address	Type: • **IP** • **FQDN**
IP address	The server's IP address. Specify it if the **IP** server type is selected.
Port	The server's port. Specify it if the **IP** server type is selected.
FQDN	The server's FQDN. Specify it if the **FQDN** server type is selected.
URL path	Used to manage a device via API.
Login name	User login for connector authorization.
Password	Password to the user account required for connector authorization.
Command group	You can only specify a command group for a SSH server; see the Commands section for details.
HTTP headers	You can only specify headers for HTTP and HTTPS servers.

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

LOG COLLECTOR

Description

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

Syslog

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

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

To configure the server, go to the **Log collector → Syslog** section in the **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 • UDP.
Port	The port number used to collect syslog events. The default port is 514.

Name	Description
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	The rule's 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.
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.

Name	Description
	• **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 Syslog Applications section.

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`

Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.

Name	Description
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 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.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Step 5. Create an IP address list and specify an update URL for it.</td><td>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".
• 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".</td></tr>
</table>

Emails

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

To add a new email group, follow these steps:

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

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

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

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

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

Phones

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

To add a new phone group, follow these steps:

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

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

Name	Description
Step 1. Create a file with the relevant phone list.	Create a file named **list.txt** with the phone list.

Name	Description
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named **list.zip**.
Step 3. Create a version file for the list.	Create a file named **version.txt** and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.
Step 4. Upload the files to a web server.	Upload the **list.zip** and **version.txt** files to your website so that they can be downloaded.
Step 5. Create a phone list and specify an update URL for it.	On each UserGate server, create a phone list. When creating the list, select **Updatable** as the list type and enter the address for downloading updates. UserGate will check for a new version on your website according to the set update download schedule. The schedule can be configured in the list properties. The available options are: • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. With the Advanced option, a crontab-like format is used where the date/time string consists of six space-separated fields. The fields specify the time as follows: (minutes: 0-59) (hours: 0-23) (days of the month: 1-31) (month: 1-12) (days of the week: 0-6, where 0 is Sunday). Each of the first five fields can be defined using: • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

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

Commands

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

Provide the following settings to create a command group:

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

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

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

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

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

Notification Profiles

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

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

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

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

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

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

Triggered Alert Categories

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

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

External Enrichment Services

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

To use enrichment services, they need to be enabled. For some of the enrichment services, the user needs to register and provide an access key.

Name	Description
dnsgoogle	A web service by Google that provides public DNS servers. Detailed information: https://dns.google/. Types of observables: IP.
urlhaus	The abuse.ch project. The aim of this project is collecting, tracking, and exchanging malware URLs. Detailed information: https://urlhaus.abuse.ch/. Types of observables: Domain, Hash, Host name, IP, URL.

Name	Description
dshield	A system for correlating firewall logs collaboratively. The system collects firewall logs from volunteers all over the world and uses them to analyze attack trends. Detailed information: https://www.dshield.org/xml.html/. Types of observables: Domain, FQDN, IP.
cybercrime	The service provides information on threat levels presented by various objects. Detailed information: http://cybercrime-tracker.net/. Types of observables: Domain, FQDN, IP, URL, Other.
cyberprotect	The service provides information on threat levels presented by various objects. Detailed information: https://console.threatscore.cyberprotect.cloud/. Types of observables: Domain, Hash, IP, URL, Useragent.
unshorten	This service allows the target URL of any short URL to be previewed and checked for malicious links. The service does not use the external resource but rather analyzes the response for the requested URL. Types of observables: URL.
ipwhois	The service provides information on IP addresses. Detailed information: https://ipwhois.io/. Types of observables: IP.
ipinfo	A tool for identifying the owner, ISP, and location of a website, domain, or IP address. Detailed information: https://ipinfo.io/. Types of observables: IP. The service requires access credentials to be entered.
hashdd	The service provides a hash database of malicious files and offers various checks to get a thorough understanding of the threat. Detailed information: https://hashdd.com/. Types of observables: Hash. The service requires access credentials to be entered.
urlscan	A service providing information on suspicious, malicious, and phishing URLs. Detailed information: https://urlscan.io/. Types of observables: Domain, FQDN, Hash, IP, URL.

Name	Description
	The service requires access credentials to be entered.
emailrep	A system collecting data on email addresses, domains, and users. Detailed information: https://emailrep.io/. Types of observables: Mail. The service requires access credentials to be entered.
greynoise	The company focuses on analyzing the Internet's background noise (data packets destined to IP addresses or ports where there is no network device configured to receive them). This kind of filtering helps reduce false triggered events. Detailed information: https://www.greynoise.io/. Types of observables: IP. The service requires access credentials to be entered.
abuseip	A project that fights malicious activity on the Internet. Detailed information: https://www.abuseipdb.com/. Types of observables: IP. The service requires access credentials to be entered.
hybridanalysis	A service for checking files for malicious content. Detailed information: https://www.hybrid-analysis.com/. Types of observables: Hash. The service requires access credentials to be entered.

Syslog Applications

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

To add an application, follow these steps:

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

Agent UserID 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.
Unix PAM Authentication	A filter to track user logon/logoff events using **Pluggable Authentication Modules** (PAM) technology in syslog logs.

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 → Агент UserID → Syslog**.

DASHBOARD

Dashboard (Description)

This section allows you to view the current state of the Log Analyzer server and servers connected to it for sending logs as well as the servers' boot status, license status, and more.

Reports are presented as widgets, which can be customized by the system administrator as required. You can add, delete, move, and resize widgets on the **Dashboard** page. There are predefined pages with widgets for Log Analyzer (Log Analyzer server state), NOC (Network Operation Center), and SOC (Security Operation Center).

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

Name	Description
Name	Name of widget to display in the Dashboard.
Description	Optional widget description.
Number of records	Maximum number of records to display.
Group by	Data field by which to group the data.
Chart	Select how the data is presented. Available values: • Number • Pie chart • Column chart • Bar chart • Table • Line chart • World map
Filter query	SQL-like query string that allows you to limit the amount of information used to build a widget. To construct a query, use field names and values, keywords, and operators. For keywords and operators with examples of their use, see the Data Search and Filtering section.
Sensor	The sensor that provides data for this widget.

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 **S** 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.

Name	Description
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

Alerts

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, 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.
Version	Specify the version of the SNMP protocol used in the rule. Available options: SNMP v2c and SNMP v3.
Allow SNMP queries	When enabled, allows receiving and processing of SNMP requests from the SNMP manager.
Allow SNMP traps	When enabled, allows sending of SNMP traps to the server configured to receive notifications.
SNMP security profile name	For SNMP v3 only. For more details, see the SNMP Security Profiles section.
Events	Parameters the values of which the SNMP manager will be able to read. If trap sending is allowed, a trap is sent to the server when a critical parameter value is reached.

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.

The **Download MIBs** button allows you to download MIB files with UserGate monitoring parameters for later use in the SNMP manager. UserGate is assigned the unique **SNMP PEN** (Private Enterprise Number) **45741**.

You can download the following MIB files:

- UTM-TRAPS-MIB
- UTM-TRAPS-BINDINGS-MIB
- UTM-MIB
- UTM-INTERFACES-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.
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	Attack detected by IDPS.
trapChecksumFailed	Binary files checksum mismatch.
trapHighCPUUsage	High CPU usage.
trapLowMemory	Low memory.
trapLowLogdiskSpace	Not enough disk space to store logs.

Name	Description
trapRaidStatus	RAID status has been changed.
trapPowerSupply	The first power supply is off.
trapCableStatus	Cable has been connected or disconnected from the interface.
trapTrafficDrop	A firewall deny rule has been triggered.
trapLDAPServerDown	LDAP server unavailable.

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.
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: RAID 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
utmLDAPServerName	String	LDAP server name.
utmLDAPServerAddress	String	LDAP server IP address.

UTM-MIB

Name	Data type	Description
vcpuCount	Integer	Number of virtual CPUs in the system.
vcpuUsage	Integer	Virtual CPU load in the system (in %).
usersCounter	Integer	Current number of active users.

Name	Data type	Description
cpuLoad	Integer	System CPU load (in %).
memoryUsed	Integer	RAM usage (in %).
logDiskSpace	Integer	Disk space used for logs (in %).
Sys_power_supply1_status	String	State of the first power supply: • **no_power_supplies**. • **on** • **off**
Sys_power_supply2_status	String	State of the second power supply: • **no_power_supplies**. • **on** • **off**
Sys_raid_status	Integer	Current status of RAID (Redundant Array of Independent Disks): • **no_raid**. • **0**: optimal: the array is in its optimal state. • **1**: degraded: one drive has completely or partially failed. • **2**: rebuild: RAID rebuild in progress.

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.

Name	Data type	Description
ifDescr	String	Interface description.
ifType	Integer	Interface type determined according to the physical/link layer protocol: • **1**: other: unknown type. • **2**: regular1822: defined in BBN Report 1822. • **3**: hdh1822: defined in BBN Report 1822. • **4**: ddn-x25: defined in BBN Report 1822. • **5**: defined in the data link layer standard of the OSI X.25 network mode. • **6**: ethernet-csmacd: Ethernet-type network interface regardless of speed (defined in RFC 3635). • **7**: iso88023-csmacd: defined in IEEE 802.3. • **8**: iso88024-tokenBus: defined in IEEE 8802.4. • **9**: iso88025-tokenRing: network interface uses a Token Ring connection; defined in the IEEE 802.5 standard. • **10**: iso88026-man: defined in the ISO 88026 standard "MAN". • **11**: starLan: defined in the IEEE 802.3e standard. • **12**: proteon-10Mbit: Proteon 10 Mbit. • **13**: proteon-80Mbit: Proteon 80 Mbit. • **14**: hyperchannel: high-speed channel used in ISDN networks. • **15**: fddi: network interface uses FDDI

Name	Data type	Description
		(Fiber Distributed Data Interface) connection. FDDI is a set of standards for data transmission over fiber-optic lines in local networks. • **16**: lapb: data link layer protocol used to transmit X.25 standard packets. • **17**: sdlc: data link layer protocol for IBM system network architecture. • **18**: ds1: can handle 24 simultaneous connections at a total speed of 1.544Mbit/s; also called T1. • **19**: e1: European equivalent of T1. • **20**: basicISDN: used for communication between the subscriber's equipment and the ISDN station. • **21**: primaryISDN: used to connect to broadband backbones, connecting local and central PBX or network switches. • **22**: propPointToPointSerial: defined in RFC1213. • **23**: ppp: network interface uses PPP (Point-To-Point Protocol) connection. • **24**: softwareLoopback: network interface configured as a loopback adapter. These interfaces are often used for testing; they do not send traffic to the network.

Name	Data type	Description
		• **25**: eon: ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); defined in ISO/IEC 8473-1. • **26**: ethernet-3Mbit: network interface uses a 3Mbit/s Ethernet connection. This version of Ethernet is defined in the IETF standard RFC 895. • **27**: nsip, XNS over IP: intended for use in a variety of data transmission environments. • **28**: slip: network interface uses a SLIP (Serial Line Internet Protocol) connection. SLIP is defined in the IETF RFC 1055 standard. • **29**: ultra: ULTRA Technologies. • **30**: ds3: high-speed data interface multiplexing DS1 and DS2 signals; also know as T3. • **31**: sip: network interface uses a SLIP (Serial Line Internet Protocol) connection. SLIP is defined in the IETF RFC 1055 standard. • **32**: frame-relay: allows packet-switched data transmission across an interface between user devices and network equipment.
ifMtu	Integer	Maximum size of a network layer packet that can be sent over this interface.

Name	Data type	Description
ifSpeed	gauge32	Interface bandwidth in bits per second.
ifPhysAddress	String	Physical interface address (MAC address).
ifAdminStatus	Integer	Interface state assigned by the administrator: • **1**: up: ready to transmit packets • **2**: down: not working • **3**: testing: working in the test mode; cannot transmit work packets
ifOperStatus	Integer	Current operating status of the interface: • **1**: up: ready to transmit packets • **2**: down: interface cannot transmit data packets • **3**: testing: network interface is being tested; cannot transmit working packets • **4**: unknown: interface state is unknown • **5**: dormant: network interface cannot transmit data packets, it is waiting for an external event • **6**: notPresente: network interface cannot transmit data packets because a component, usually a piece of hardware, is missing • **7**: lowerLayerDown: network interface cannot transmit data packets because it is running on top of one or more other

Name	Data type	Description
		interfaces, and at least one of those "lower-layer" interfaces is down
ifLastChange	timeticks	SysUpTime value when the interface switches to this state.
ifInOctets	counter32	Number of bytes received by the interface, including service bytes.
ifInUcastPkts	counter32	Number of delivered unicast packets.
fInNUcastPkts	counter32	Number of delivered multicast and broadcast packets.
ifInDiscards	counter32	Number of incoming packets that were dropped, even if no errors were detected preventing the delivery. Buffer space release may be one of the reasons for dropping.
ifInErrors	counter32	Number of incoming packets that contain errors preventing the delivery.
ifInUnknownProtos	counter32	Number of packets that were received through the interface and dropped because an 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,

Name	Data type	Description
		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	Number of packets in the send queue.
ifInMulticastPkts	counter32	Number of delivered multicast packets.
ifInBroadcastPkts	counter32	Number of delivered broadcast packets.
ifOutMulticastPkts	counter32	Number of sent multicast packets, including packets that were dropped or not sent.
ifOutBroadcastPkts	counter32	Number of sent broadcast packets, including packets that were dropped or not sent.
ifHCInOctets	counter64	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 delivered multicast packets; uses a higher capacity counter.

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

Name	Data type	Description
		Promiscuous mode. Available values: • **1**: true: station receives all packets/frames regardless of the destination. • **2**: false: interface receives only packets/frames addressed to this station. The object value does not affect the reception of broadcast and multicast packets/frames.
ifAlias	String	Interface name assigned by the administrator.
ifCounterDiscontinuityTime	timeticks	SysUpTime value when the event occurred that caused one or more interface counters to fail.

SNMP Parameters

This section allows to specify parameters of providing information over SNMP protocol by the SNMP agent.

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

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.

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.
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.

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, 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.
Version	Specify the version of the SNMP protocol used in the rule. Available options: SNMP v2c and SNMP v3.
Allow SNMP queries	When enabled, allows receiving and processing of SNMP requests from the SNMP manager.
Allow SNMP traps	When enabled, allows sending of SNMP traps to the server configured to receive notifications.
SNMP security profile name	For SNMP v3 only. Подробнее — в разделе Профили безопасности SNMP.
Events	Parameters the values of which the SNMP manager will be able to read. If trap sending is allowed, a trap is sent to the server when a critical parameter value is reached.

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.

Name	Description
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.
trapLowMemory	Low memory.
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.
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	

Name	Data type	Description
		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.
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

Name	Data type	Description
		• **1**: degraded: one drive has completely or partially failed. • **2**: rebuild: array rebuild in progress
utmBroadcomRaidStatus	Integer	Current status of RAID (Redundant Array of Independent Disks) built on the Broadcom controller: • **no_raid** • **0**: optimal: the array is in its optimal state • **1**: degraded: one drive has completely or partially failed. This 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.

Name	Data type	Description
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	Virtual CPU load in the system (in %).
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. (*)

Name	Data type	Description
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	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. (*)

Name	Data type	Description
dnsRequestRate	Integer	DNS requests per second. (*)
httpRequestCounter	Integer	Total HTTP requests. (*)
httpBlockedRequestCounter	Integer	Blocked HTTP requests. (*)
httpRequestRate	Integer	HTTP queries per second. (*)
dataPartitionFSStatus	String	File system status.
haStatus	Integer	The current state of the cluster node.
cpuLoad	Integer	System CPU load (in %).
memoryUsed	Integer	RAM usage (in %).
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

Name	Data type	Description
		• **1**: degraded: one drive has completely or partially failed. • **2**: rebuild: array rebuild in progress
diskIOUtilization	Integer	Current disk utilization (%).
diskIOUtilization60	Integer	Disk utilization (%). Average value for the last 60 seconds.
diskIOUtilization300	Integer	Disk utilization (%). Average value for the last 300 seconds.

Note

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

UTM-INTERFACES-MIB

Name	Data type	Description
ifNumber	Integer	Number of network interfaces.
ifIndex	Integer	The value is unique for each interface. Available values: from 1 to ifNumber.
ifDescr	String	Interface description.
ifType	Integer	Interface type determined according to the physical/link layer protocol: • **1**: other: unknown type • **2**: regular1822: defined in BBN Report 1822 • **3**: hdh1822: defined in BBN Report 1822 • **4**: ddn-x25: defined in BBN Report 1822

Name	Data type	Description
		• **5**: defined in the data link layer standard of the OSI X.25 network model • **6**: ethernet-csmacd: Ethernet-type network interface regardless of speed (defined in RFC 3635) • **7**: iso88023-csmacd: defined in IEEE 802.3 • **8**: iso88024-tokenBus: defined in IEEE 8802.4 • **9**: iso88025-tokenRing: network interface uses a Token Ring connection; defined in the IEEE 802.5 standard. • **10**: iso88026-man: defined in the ISO 88026 standard "MAN". • **11**: starLan: defined in the IEEE 802.3e standard. • **12** — proteon-10Mbit — Proteon 10 Mbit. • **13** — proteon-80Mbit — Proteon 80 Mbit. • **14**: hyperchannel: high-speed channel used in ISDN networks. • **15**: fddi: network interface uses FDDI (Fiber Distributed Data Interface) connection. FDDI is a set of standards for data transmission over fiber-optic lines in local networks. • **16**: lapb: data link layer protocol used to transmit X.25 standard packets. • **17**: sdlc: data link layer protocol for IBM system network architecture.

Name	Data type	Description
		• **18**: ds1: can handle 24 simultaneous connections at a total speed of 1.544Mbit/s; also called T1. • **19**: e1: European equivalent of T1. • **20**: basicISDN: used for communication between the subscriber's equipment and the ISDN station. • **21**: primaryISDN: used to connect to broadband backbones, connecting local and central PBX or network switches. • **22**: propPointToPointSerial: defined in RFC1213. • **23**: ppp: network interface uses PPP (Point-To-Point Protocol) connection. • **24**: softwareLoopback: network interface configured as a loopback adapter. These interfaces are often used for testing; they do not send traffic to the network. • **25**: eon: ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); defined in ISO/IEC 8473-1. • **26**: ethernet-3Mbit: network interface uses a 3Mbit/s Ethernet connection. This version of Ethernet is defined in the IETF standard RFC 895. • **27**: nsip, XNS over IP: intended for use in a

Name	Data type	Description
		variety of data transmission environments. • **28**: slip: network interface uses a SLIP (Serial Line Internet Protocol) connection. SLIP is defined in the IETF RFC 1055 standard. • **29** — ultra — ULTRA Technologies. • **30**: ds3: high-speed data interface multiplexing DS1 and DS2 signals; also know as T3. • **31**: sip: network interface uses a SLIP (Serial Line Internet Protocol) connection. SLIP is defined in the IETF RFC 1055 standard. • **32**: frame-relay: allows packet-switched data transmission across an interface between user devices and network equipment.
ifMtu	Integer	Maximum size of a network layer packet that can be sent over this interface.
ifSpeed	gauge32	Interface bandwidth in bits per second.
ifPhysAddress	String	Physical interface address (MAC address).

Name	Data type	Description
ifAdminStatus	Integer	Interface state assigned by the administrator: • **1**: up: ready to transmit packets • **2**: down: not working • **3**: testing: working in the test mode; cannot transmit work packets.
ifOperStatus	Integer	Current operating status of the interface: • **1**: up: ready to transmit packets • **2**: down: interface cannot transmit data packets • **3**: testing: network interface is being tested; cannot transmit working packets • **4**: unknown: interface state is unknown • **5**: dormant: network interface cannot transmit data packets, it is waiting for an external event • **6**: notPresente: network interface cannot transmit data packets because a component, usually a piece of hardware, is missing • **7**: lowerLayerDown: network interface cannot transmit data packets because it is running on top of one or more other interfaces, and at least one of those "lower-layer" interfaces is down

Name	Data type	Description
ifLastChange	timeticks	SysUpTime value when the interface switches to this state.
ifInOctets	counter32	Number of bytes received by the interface, including service bytes.
ifInUcastPkts	counter32	Number of delivered unicast packets.
fInNUcastPkts	counter32	Number of delivered multicast and broadcast packets.
ifInDiscards	counter32	Number of incoming packets that were dropped, even if no errors were detected preventing the delivery. Buffer space release may be one of the reasons for dropping.
ifInErrors	counter32	Number of incoming packets that contain errors preventing the delivery.
ifInUnknownProtos	counter32	Number of packets that were received through the interface and dropped because an 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

Name	Data type	Description
		preventing the transmission. Buffer space release may be one of the reasons for dropping.
ifOutErrors	counter32	The number of outgoing packets that could not be transmitted due to errors.
ifOutQLen	gauge32	The send queue length (number of packets).
ifInMulticastPkts	counter32	Number of delivered multicast packets.
ifInBroadcastPkts	counter32	Number of delivered broadcast packets.
ifOutMulticastPkts	counter32	Number of sent multicast packets, including packets that were dropped or not sent.
ifOutBroadcastPkts	counter32	Number of sent broadcast packets, including packets that were dropped or not sent.
ifHCInOctets	counter64	Identical to **ifInOctets**: number of bytes received by the interface, including service bytes; uses a higher capacity counter.
ifHCInUcastPkts	counter64	Identical to **ifInUcastPkts**: number of delivered unicast packets; uses a higher capacity counter.
ifHCInMulticastPkts	counter64	Identical to **ifInMulticastPkts**: number of delivered multicast packets; uses a higher capacity counter.
ifHCInBroadcastPkts	counter64	Identical to **ifInBroadcastPkts**: number of delivered broadcast packets; uses a higher capacity counter.

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

Name	Data type	Description
		The object value does not affect the reception of broadcast and multicast packets/frames.
ifAlias	String	Interface name assigned by the administrator.
ifCounterDiscontinuityTime	timeticks	SysUpTime value when the event occurred that caused one or more interface counters to fail.

UTM-TEMPERATURE-MIB

Name	Data type	Description
termNumber	Integer	Number of temperature sensors on this platform.
thermLowerThreshold	Integer	Lower operating temperature limit.
thermUpperThreshold	Integer	Upper operating temperature limit.
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**: 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**: shows events received from the devices that are controlled using the UserGate Endpoint software.
- **Endpoint rules**: trigger events for the endpoint firewall rules where logging is enabled in the settings.
- **Endpoint applications**: displays applications that were run on the devices.
- **Endpoint hardware**: contains information on the devices connected to end devices.
- **Syslog**: displays messages about events from remote Unix systems received using the Syslog protocol.

- **Mail traffic protection**: contains events triggered by mail traffic protection rules that have logging enabled in their settings.
- **UserID**: contains description of events reflecting the result of UserID agent's work.

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

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

Event log records are not rotated.

Endpoint Log

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

UserGate provides the following logs:

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

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

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

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

Syslog

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

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

UserID Log

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

Name	Description
Node	UserGate node where the event occurred.
Time	The time of the event.
Event details	Shows event details.
Action	The action applied to the event.
Log source	The source of the event received.

Name	Description
User	The UG user triggered the event.
IP address	The IP address of the node where the event occurred.
Information	The event description.

Windows Active Directory log

Windows Active Directory log contains events collected by the UserID agent from AD servers. The log contains successful logon events (event ID 4624), Kerberos events (event IDs: 4768, 4769, 4770) and group membership events (event ID 4627). The log contains the following information:

Name	Description
Node	UserGate node where the event occurred.
Time	The time of the event.
Endpoint event log record details	The link to the event.
Device/sensor	UserID connector.
Log level	The "Keywords" field from AD log.
Data	Event details from AD log.
Log event source	The "Source" field from AD log.
Log category	Incident category code (12554 Group Membership, 12544 Logon, 14337 Kerberos Service Ticket Operations etc.)
Incident category	The "Task type" field from AD log.
Computer name	windows node where the event took place.
User	The "User" field from AD log.
Log event code	The "Event code" field from AD log (EventCode).
Log event ID	The "Event ID" field from AD log (EventID).
Log event type	Windows log even type (System/Security/Application etc.)

Name	Description
Log file	Windows log file.

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. Для логгирования событий DNS на NGFW должна быть включена DNS-фильтрация в настройках DNS-прокси и разрешено журналирование в правилах контентной фильтрации, в которые будет попадать DNS трафик.

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.

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.

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.

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

- Endpoint hardware.

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

To send logs, you must first create log export configurations in the **Logs export** section.

When creating a configuration, provide the following parameters:

Name	Description
Rule name	The name of the log export rule.
Description	Optional field for rule description.
Logs to export	Select the log files to export: • DNS • Events • Web access • IDPS • SCADA • SSH inspection • Traffic • Endpoint events • Endpoint rules • Endpoint applications • Endpoint hardware. For each log, you can specify the export syntax: • CEF: Common Event Format (ArcSight) • JSON: JSON format • @CEE: JSON: CEE Log Syntax (CLS) Encoding JSON To select the desired log export format, refer to the documentation for the SIEM system you are using. Подробное описание форматов журналов читайте в Приложение 2. Description of Log Formats.
Server type	SSH (SFTP), FTP, Syslog.
Server address	IP address or domain name of the server.

Name	Description
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.
App-Name	Only for Syslog server type. Unique name of the application that sends data to the Syslog server.

Name	Description
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.

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
- Registry 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.

Custom log normalization

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

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

Log sources and their fields that can be further normalized:

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

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

SIEM database
node
userId
user
ruleId
rule
ipSource
portSource
portDest
macSource

SIEM database
macDest
natIpSource
natIpDest
natPortSource
natPortDest
applicationName
bytesSent
bytesRecv
packetsSent
packetsRecv
mime
httpMethod
referer
url
statusCode
userAgent
sensor
sensorId
processId
networkProtocol
status
error
counterId

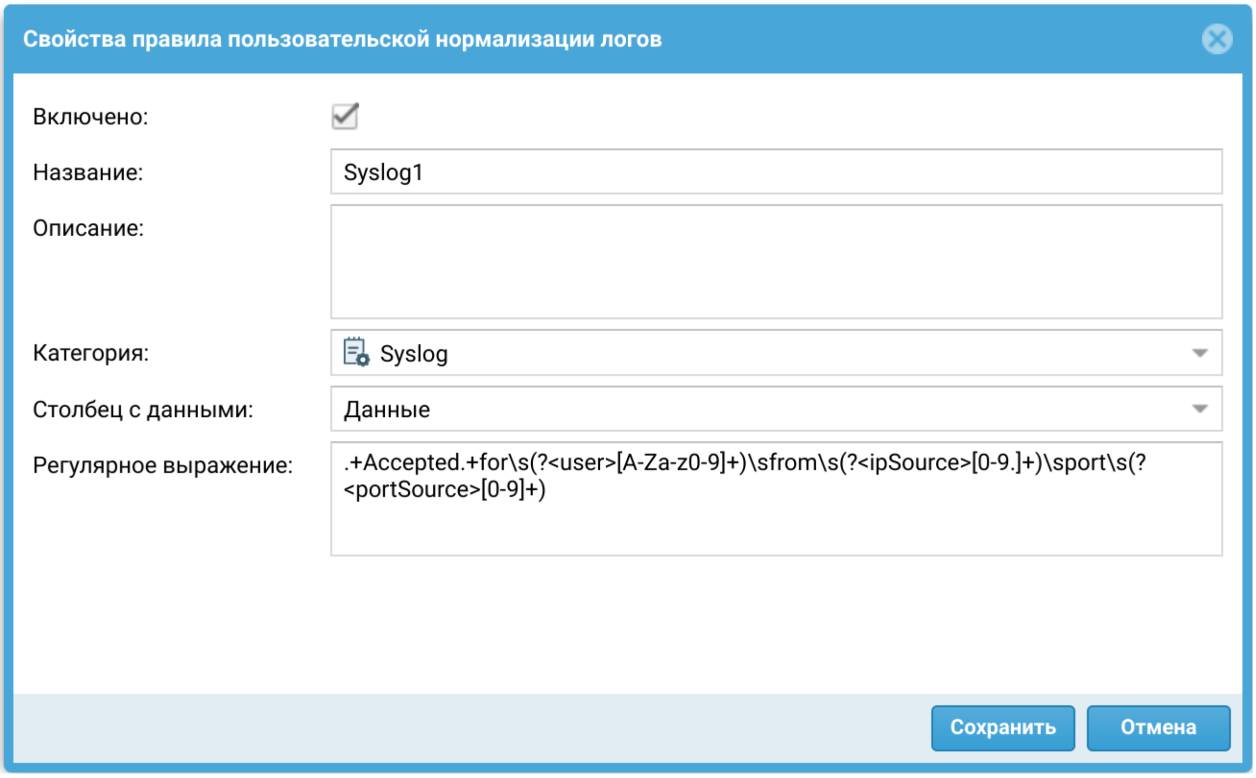
SIEM database
logCategory
taskCategory
computerName
logEventCode
logEventId
logEventType
logFile
severity
module
component
event
syslogFacility
syslogSeverity

To create a normalization rule, click the **Add** button under **Logs and Reports -> Logs -> Custom Log Normalization** and fill in the following fields in the window that opens:

Name	Description
Enabled	Enable/disable custom log normalization rule.
Name	Name of the custom log normalization rule.
Description	Description of the custom log normalization rule.
Category	Select the category (type) of the logs to which this rule is applied: • Endpoint events • Syslog
Data column	Select the column the data will be extracted from.

Name	Description
Regular Expression	A regular expression string with group names matching the columns to which the values will be written.

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



REPORTS

Templates

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

Here is the list of report templates by category:

- **Custom**: a group of templates for generalized statistics of report rule triggering.
- **Captive portal**: a group of templates for events related to user authentication using the Captive portal.

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

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

Custom Report Templates

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

Name	Description
Name	The name of the custom report template.

Name	Description
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. В качестве полей данных можно использовать столбцы, перечисленные ниже в поле **Столбцы.** Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных.
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.

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.

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

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>20 users who encountered errors authenticating in the web console.</td></tr>
<tr><td>Group by limit (if applicable)</td><td>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.</td></tr>
<tr><td>Users</td><td>Specify users or user groups for which the report will be created. If not specified, the report will be created for all users.</td></tr>
<tr><td>Templates</td><td>List of templates used to build the report. You need to add at least one template.</td></tr>
<tr><td>Schedule</td><td>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 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".</td></tr>
<tr><td>Delivery</td><td></td></tr>
</table>

Name	Description
	You can optionally send reports to recipients via the SMTP protocol. To do this, specify the following: • SMTP profile to use for sending reports. Подробно о настройке профилей SMTP смотрите в главе Профили оповещений. • From: email sender name. • Subject: email subject. • Body: email body. • Recipients: list of the email recipients. The recipients must be added to the lists of the **Emails** library.

Note

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

Note

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

Generated reports

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

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

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

INCIDENT REPORTS

Incident report templates

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

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

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

General information

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

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

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

Incident report rules

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

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

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

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

Generated incident reports

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

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

ANALYTICS

General information

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

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

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

The analytics settings are located in the **Analytics** tab where you can configure analytics rules, create response actions, and view the rule log and triggered alert details.

These features will be discussed in the next sections, Response Actions, Triggered Alerts, and Triggered Alert Details.

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

To create a rule, click **Add**. Then go to the **General** tab, and specify the rule's properties.

Name	Description
Enabled	Enables or disables applying the analytics rule in real time.
Name	The name of the analytics rule.
Description	A description of the analytics rule. This field is optional.
Threat level	The threat level that will be displayed when the rule is triggered. The following threat levels are defined: • **Very low**: the events present a very low threat level, and the administrator may choose not to take any action. • **Low**: the events present a low threat level, and the administrator may choose not to take any action. • **Medium**: the events require attention. • **High**: the events require investigation and response. • **Very high**: the events require investigation and urgent response.
Priority	The priority assigned to triggered alerts for this analytics rule: • **Low**: low response priority. • **Normal**: needs attention and may need response. • **Important**: needs attention and response. • **Critical**: requires urgent response. When the analytics rule is triggered, the priority will indicate the severity of the triggered alert.
Category	The category to which the triggered alert belongs. The following predefined categories are available: • **Security**: incidents that degrade the security of information systems. • **Availability**: incidents that degrade the availability of information systems. • **Performance**: incidents that degrade the performance of information systems.

Name	Description
	Additional triggered alert categories can be created in the **Libraries → Triggered alert categories** section of the **General settings** tab.
Timezone	The timezone that analytics rules will use (because the server can collect data from sources located in different timezones).

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

Name	Description
Name	The name of the analytics rule condition.
Description	A description of the analytics rule condition. This field is optional.
Limit condition time	Enable or disable the time limit for evaluating this condition. If the time limit is enabled, the analytics rule will be triggered only if the condition is matched the specified number of times within that time period.
Condition time, sec	The time period within which the condition must be matched the specified number of times for the analytics rule to be triggered. The time is set in seconds. This setting can be configured if the **Limit condition time** checkbox is set.
Use stop query	Enable/disable the use of a stop query in an analytics rule.
Stop query	An SQL-like stop search query is executed along with the condition query. To formulate a query, use field names, field values, keywords, and operators (set similarly to a filter query). If, when performing an analysis, at least one record is found that matches the specified stop query, before the specified number of events that match the condition of the analytics rule are found, then the analytics rule will not work, and the counter for the number of records found before the stop query is executed will be reset.
Filter query	An SQL-like condition search query against the log database. To formulate a query, use field names, field values, keywords, and operators. For the query syntax, refer to the section Data Search and Filtering.

Name	Description
	The query can also be written using the Google/RE2 syntax in a MATCH operator. **Example**. Search query: source = 'wmi log' and logFile = 'Microsoft-Windows-Sysmon/Operational' and logEventId = 1 and data MATCH 'ParentCommandLine:(.*)cmd.exe' and data ~ 'CertReq -Post -config'. This query will perform a search in the endpoint event log that gets data from the Microsoft-Windows-Sysmon/Operational log. When an event is found indicating the creation of a new process, a search is run for the parent process (i.e. the process that caused the new process to be created) and a certreq command invocation with parameters. The MATCH part of the query allows detection of the fact that certreq was invoked from cmd.exe (the command line). This identifies cmd.exe as the parent for the current process. More details on the use of Google/RE2 syntax with the MATCH operator can be found here: https://github.com/google/re2/wiki/Syntax.
Group by	The list of parameters by which rules can be grouped as a result of a triggered alert. The fields will be displayed when triggered alert details are viewed. The parameters that can be used for grouping are described in the Analytics Search section. When grouping categories are specified, the analytics rule will be triggered only if the condition is matched for this specific category the number of times specified in the **Pattern repeats** field.
Pattern repeats	How many times the condition must be matched for the rule to be triggered. This can be used with or without the **Limit condition time** setting.
Run now	Runs event analysis for a certain time range (historical mode). This option needs a time range to be specified. If the **Use time range** checkbox is not set, the analysis is run using the created analytics rule over the entire time span covered by the whole event database. When the analysis is completed, you can click **S how triggered alerts** in the **Analytics rule execution** window to open the alert log and view the triggered alert details for the rule. You can also run the rule without writing to the alert log — e.g., to check if the rule works correctly or just view the number of triggered alerts. To do that, set the **Test run** checkbox.

In the **Response actions** tab, you can add actions to be performed automatically when the analytics rule is triggered. Response actions can be created by clicking **Create and add new object** or added from the list of existing actions. For more details on response actions and how to configure them, see the section Response Actions.

To run the rule in real time, click **Enable**. To stop the execution of the selected analytics rule, click **Disable**.

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

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

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

Example of Analytics Rule Configuration

As an example, consider configuring an analytics rule that will detect brute force attack attempts.

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

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

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

  This condition performs a search of the endpoint event log for an event ID of 4625 corresponding to a failed account authorization attempt. The MATCH part of the condition specifies the reason for denied authorization as an invalid login or password.

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

- **source = 'endpoint events log' AND logEventId = 4672**

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

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

- **source = 'endpoint events log' AND logEventId = 4624**

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

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

Analytics Search

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Name in database	Name in search query	Description
		• **Security** (security log file): for audit system events. • **System** (system log file): for device driver events. • **CustomLog**: contains events logged by applications that create a custom log. The use of a custom log allows an application to control the log size or attach access control lists for security purposes without affecting other applications. Applicable to endpoint event log records.
Command	scadaCommand	The SCADA control command (e.g., read or write). Applicable to SCADA log records.
Registry address	scadaAddress	The address of the register on which the operation (read or write) should be performed. Applicable to SCADA log records.
ASDU number	scadaAsdu	The ASDU address (COA, or Common Object Address). Refers to the IEC-104 protocol. Applicable to SCADA log records.
Device ID	scadaDevice	The unique device number from the OPC server database. Used with the OPC UA protocol. Applicable to SCADA log records.
Variable name	scadaVarname	The name of the variable. Parameter is mainly used for real-time data exchange. Refers to the MMS protocol. Applicable to SCADA log records.

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

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

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

Response Actions

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

Notification and command variables

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

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

Name	Description
{ANALYTICS_RULE_NAME}	The name of the analytics rule.
{ANALYTICS_RULE_DESCRIPTION}	A description of the analytics rule.
{NAME}	The name of a specific triggered alert.
{TIME}	The time when the analytics rule was triggered.
{TRIGGERED_ALERTS_NUMBER}	The number of triggered alerts.
{FIRST_TRIGGERED_ALERT_TIME}	The time when the first triggered alert occurred.
{LAST_TRIGGERED_ALERT_TIME}	The time when the last triggered alert occurred.
{TRIGGERED_ALERTS_NAMES}	The list of triggered alert names if grouping is used.
{FIRST_EVENT_TIME}	The time of the first event included in the triggered alert for the analytics rule.
{LAST_EVENT_TIME}	The time of the last event included in the triggered alert for the analytics rule.
{THREAT_LEVEL}	The specified threat level.
{CATEGORY}	The category to which the triggered alert belongs.
{PRIORITY}	The priority of the triggered analytics rule alert.
{ADMINISTRATOR_NAME}	The name of the administrator who created the analytics rule.
{USER_NAME}	The username.
{SOURCE_ZONE}	Source zone
{DESTINATION_ZONE}	Destination zone
{SOURCE_COUNTRY}	The source country.
{DESTINATION_COUNTRY}	The destination country.
{SOURCE_IP}	Source IP address

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

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

Name	Description
Enabled	Enables or disables the response action.
Name	The name of the response action.
Description	A description of the response action. This field is optional.
Action	The action that should be taken when the analytics rule is triggered. Will be applied if specified in the analytics rule properties.

Name	Description
	The following response actions are available: • **Send email**: send an email to the selected addresses. The procedure of configuring the **Send email** action will be discussed later in the Send Email Action section. • **Send message**: send a message to the specified phone numbers. The procedure of configuring the **Send message** action will be discussed later in the Send Message Action section. • **Webhook**: receive an alert on the rule trigger on the webpage whose address is specified in the action settings. The procedure of configuring the **Webhook** action will be discussed later in the Webhook Action section. • **Create incident**: automatically create an incident when the analytics rule is triggered. The procedure of configuring the **Create incident** action is described in the Incident Settings section. • **Send Command To Connector**: send a command to the selected connector. The procedure of configuring the Send Command To Connector action is described in the <0>Send Command To Connector Action section. • **Send Command To Endpoint** send a command to an endpoint with UserGate Client software installed. For more details, see Send Command To Endpoint Action.
Enable logging	Enables or disables the logging of response action triggers. The data is recorded in the SIEM event log that can be viewed in the **Logs and reports ➜ Logs ➜ Event log** tab.
Group similar triggered alerts	When configuring response actions, you can enable the grouping of triggered alerts for convenience. The following grouping options are available: • **Never**. • **For period of time**: the response action will be performed if at least one triggered alert occurs during the specified period of time. • **By number of triggered alerts**: the response action will be performed only after the specified number of triggered alerts.
Grouping time period (min.)	The grouping time period in minutes. This setting is available only when grouping for a period of time is selected.

Name	Description
Number of triggered events	The number of triggered alerts required for the grouping to happen. This setting is available only when grouping by the number of triggered alerts is selected.

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

Send Email Action

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

Name	Description
Notification profile	The SMTP notification profile to be used for sending emails. For more details on configuring SMTP profiles, see the Notificati on Profiles chapter.
From	The sender name.
Subject	The email subject.
Emails	The list of recipient email addresses. The recipients must be added to the lists under **Settings → Libraries → Emails**. For more details on adding emails, see the section Emails.
Template	The alert email template that can include the values of various variables related to the triggered alert. For more details, see the Alert Template and Notification and command variables sections.

Send Message Action

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

Name	Description
Notification profile	The SMPP notification profile to be used for sending messages. For more details on configuring SMPP profiles, see the Notificati on Profiles chapter.
From	The sender name.

Name	Description
Phones	The list of recipient phone numbers. The recipients must be added to the lists under **Settings → Libraries → Phones**. For more details on adding phone numbers, see the section Phone s.
Template	The message template that can include the values of various variables related to the triggered alert. For more details, see the Alert Template and Notification and command variables sections.

Webhook Action

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

Name	Description
URL	The URL of the website where notifications about rule triggers will be displayed.
Template	The alert template that can include the values of various variables related to the triggered alert. For more details, see the Alert Templateand Notification and command variables sections.

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

Send Command To Connector action

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

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

Name	Description
Connectors	Select the devices to which the command should be sent when an analytics rule is triggered. The connector must be added and configured in advance under **Sensors → Connectors** in the **Settings** tab in the UserGate SIEM web management interface (see Connectors for more information). **Important!** Only connectors with the same command group can be selected.

Name	Description
Command	Specify the command that will be sent to the connector for execution; the commands of the group specified for the selected connectors are available. If there are variables in the command, additional fields will be displayed where values should be specified. See Commands for more details on the commands.

Send Command To Endpoint action

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

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

Alert Template

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

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

Triggered Alerts

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

The following triggered alert details are shown.

Name	Description
Node	A unique code corresponding to the device.
Time	The date and time when the analytics rule was triggered.

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

Name	Description
Destination zone	The destination zone.
IP dest	The destination IP address.
Destination port	The destination port.

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

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

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

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

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

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

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

Triggered Alert Details

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

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

The following details about the triggered alert are displayed.

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

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

Endpoint processes

The **Endpoint processes** tab displays a list of processes of devices with UserGate Client software installed. Use it to trace the chain of process calls, understand startup parameters and view useful information about the file. The tab has two panels: **Process Log** and **Process**.

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

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

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

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

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

INCIDENTS

General information

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

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

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

Incident Settings

Incident investigation is a multi-stage process where the incident is assigned a certain **State** at each stage, e.g., **Open → Need more info → In progress → Closed**. Transition between states is possible based on certain rules set by the administrator

— e.g., a direct transition from **Open** to **Closed** is not allowed. The possible incident state transitions are defined in an **Incident schema**.

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

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

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

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

To create a new incident schema, follow these steps:

Name	Description
Step 1. Create the desired incident resolutions	Under **Incident settings → Incident resolutions**, click **Add**, provide a name and description for the resolution being created and click <0>Save.
Step 2. Create incident types	Under **Incident settings → Incident types**, click **Add**, provide a name and description for the incident type being created and click <0>Save.
Step 3. Create incident states	Under **Incident settings → Incident states**, click Add and provide the name, description, and group for the incident state being created. A state group determines the position of the state in the state schema. There are three types of group: • **Open**: assigned to incident states in which the work on the incident is not started yet or paused. Usually, these are initial incident states, such as "Created". All states from this group are marked blue in the web console. • **In Progress**: assigned to incident states in which the work on the incident is in progress but not completed yet. These are intermediate incident states, such as "In progress" or "Investigation". All states from this group are marked yellow in the web console. • **Closed**: assigned to incident states in which the work on the incident is completed. These are final incident states, such as "Completed" or "Closed". To transition to a state

Name	Description
	from this group, you need to provide a resolution for the incident, such as "False positive", "True positive", or "Completed". All states from this group are marked green in the web console. When you have defined all fields, click **Save**.
Step 4. Create incident schema	Under **Incident settings → Incident schema**, click Add and provide the following settings: • Set active: make this schema active. Only one schema can be active; if another schema was active before, this action will make it inactive, and all new and existing incidents will use the new schema. • Schema: the name of the schema. • Prefix: the prefix that will be used to assign IDs to incidents being created. An ID will have the format of -, e.g., INC-99. • Description: an optional description of the schema. • Workflow states: all states that the incident can take during its lifecycle. Add all incident states here that you created at the previous step. • Initial state: the state that an incident will take on creation. • Transitions: specify all possible state transitions here and give them names. For example, create a transition named **Activate** that will take the incident from an **Open** state to an **In Progress** state. An incident can be transitioned between states only if a transition is defined between them. • Incident resolutions: the list of the possible incident resolutions. A resolution is required when the ticket investigation is being completed, i.e. transitioned to a **Clo sed** state. Select all the required resolutions that you created earlier. • Incident types: the incident types that can be used with this schema.
Step 5. Activate the incident schema	After creating an incident schema, it needs to be activated. To do that, set the **Set active** checkbox in the incident schema settings.

Incident Dashboard

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

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

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

Incidents Log

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

Name in database	Name in search query	Description
Created	date	The date and time of incident creation.
Updated	updateDate	The date and time of the last update.
ID	incidentPrefix	The incident's prefix (INC-N, where N is the ordinal number of the incident, starting from 0).

Name in database	Name in search query	Description
Name	incidentName	The name of the incident.
Rule	rule	The name of the analytics rule the triggering of which caused the automatic creation of the incident as a result of the **Create incident** response action configured for the rule.
Status	status	The incident's state. There are three state groups that determine the position of the state in the state schema: • **Open**: assigned to incident states in which the work on the incident is not started yet or paused. Usually, these are initial incident states, such as "Created". All states from this group are marked blue in the web console. • **In Progress**: assigned to incident states in which the work on the incident is in progress but not completed yet. These are intermediate incident states, such as "In progress" or "Investigation". All states from this group are marked yellow in the web console. • **Closed**: assigned to incident states in which the work on the incident is completed. These are final incident states, such as "Completed" or "Closed". To transition to a state from this group, you need to provide a resolution for the incident, such as "False positive", "True

Name in database	Name in search query	Description
		positive", or "Completed". All states from this group are marked green in the web console. In UserGate, a schema named "Incident" is created by default that includes transitions between all possible states. Incident schemas can be added under **Settings → Incident settings → Incident schema**. Additional incident states can be defined in the **Settings → Incident settings → Incident states** tab. For more details, see the section Incident Settings.
Resolution	resolution	The resolution of the incident. The following predefined resolutions are available: • **False positive**: the incident is a false positive • **True positive**: the incident is a true positive • **Duplicate**: the problem is a duplicate of an existing one • **Won’t do**: the task cannot be accomplished • **Done**: the problem is resolved. Additional incident resolutions can be defined in the **Settings → Incident settings → Incident resolutions** tab. For more details, see the section Incident Settings.
Type	type	The incident type. By default, two incident types are

Name in database	Name in search query	Description
		available: a security incident and a task. Additional incident types can be defined in the **Settings → Incident settings → Incident types** section. For more details, see the section Incident Settings.
Priority	priority	The incident's priority: • Low • Normal • Important • Critical.
Reporter	reporter	The name of the administrator who created the incident.
Last change by	lastChangeBy	The name of the administrator who made the last change.
Assignee	assignee	The name of the administrator assigned to the incident.
Activity		The number of comments, triggered analytics rule alerts, and event logs added to the incident.

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

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

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

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

Creating Security Incidents

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

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

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

Incident Details

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

The **Triggered alerts** section shows the triggered analytics rule alerts added to the incident. For more details, see the section Triggered Alerts. To add triggered alerts to the incident, click **Add to incident**. and select the triggered alerts to be added to the incident. To view the details for a triggered alert for analytics rule, select it and click **Show details**. You can also view triggered alert details by clicking **Show**. To remove the triggered alert for analytics rule from the incident, click **Remove from incident**. By clicking **Export as CSV**, you can save the list of triggered analytics rule alerts added to incidents in a .csv file for subsequent analysis.

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

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

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

Name	Description
Observable type	Select one of the following observable types: • **Autonomous system**: a system of IP networks and routers under unified management • **Domain**: the name of an Internet website. • **File**: a file to collect information about. • **File name**: the name of a file to collect information about. • **FQDN**: a fully qualified domain name. • **Hash**: a hash of some file, e.g. a file added to the incident • **Host name**: the label of a device connected to a computer network and used for device identification. • **IP**: a unique address identifying the device in a computer network. • **Mail**: an email address. • **Mail subject**: the contents of the email's subject field. • **Registry**: a Microsoft Windows registry key is a directory where the settings and parameters of the operating system are stored.

Name	Description
	• **URI path**: a character sequence identifying an abstract or physical resource. • **URL**: the individual Internet address of the resource. • **Useragent**: an alphanumeric string identifying the software that sends a request to the server and at the same time requests access to a website. • **Other**.
Value	Specify the object to deal with, such as an IP address, domain, etc.
Attack type	Select one of the following attack types: • **BotNet**: a network of infected computers controlled remotely by malicious actors • **Phishing**: a type of Internet scam that aims to get access to confidential user data such as logins and passwords • **Malware**: any software that attempts to infect a computer or mobile device • **DDoS**: a method of bringing a website down by sending numerous requests to it that overwhelm the network • **Traffic hijack**: malicious redirection of traffic • **Network scanning**: scanning network nodes for vulnerabilities • **Brute force**: a method of cracking user accounts by guessing their passwords • **Compromised**: an actual or suspected case of unauthorized access to protected information • **Spam**: mass distribution of unsolicited email messages of commercial, political, or other nature using specialized software • **Other**.
TLP	A TLP (Traffic Light Protocol) marking of confidential information. The following TLP marks are possible: • **RED**: the information is highly confidential • **AMBER**: the information can be shared within the organization when necessary • **GREEN**: the information can be widely distributed within a certain community • **WHITE**: the information can be distributed freely and does not infringe copyright.

Name	Description
Is IoC?	Set this checkbox if the object is a potential indicator of compromise.
Services	The list of services used to obtain additional information on the observable objects. Displayed automatically after selecting the observable type. Available under **Settings ➔ Libraries ➔ External enrichment services** section. For more details, see the section External Enrichment Services.
Updated	The date and time when the service was last updated.

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

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

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

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

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

ADMIN (description)

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

Name	Description
Change password	To change your password, enter your current password and then the new one twice.
Preferences	• Show items per page: number of lines to display in one dialog box, such as a list of firewall rules. • Night mode: set the dark theme for the UGOS GUI. • Favorite filters: rename or delete filters for various logs created by this user.
Logout	End the session in the web console of the device.

FAVORITES

Избранные (описание)

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.

APPENDICES

Appendix 1. 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.
DNS	UDP	53	Outbound (to DNS servers)	The service that resolves domain names into IP addresses.

Service	Protocol	Port	Outbound/ Inbound	Function
UserGate server registration	TCP	443	Outbound (to the registration server)	Access to the UserGate product registration server (reg2.entensys.com).
Update software and libraries	TCP	443	Outbound (to update servers)	Update software and library items: access to static.entensys.com, 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 the received keys.
	TCP			

Service	Protocol	Port	Outbound/ Inbound	Function
		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	Outbound (to a TACACS+ authenticatio n server)	User authenticatio n via the

Service	Protocol	Port	Outbound/ Inbound	Function
				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.

APPENDIX 2. LOG FORMAT DESCRIPTION

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	The severity of the event.	Available values: • 1: info • 4: warning • 7: error

Field type	Field name	Description	Example value
			• 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
	suser	The username.	Admin
	cat	Component where the event occurred.	console_auth
	act	Event type.	login_successful
	src	Source IPv4 address.	192.168.117.254
	cs1Label	This field is used for event details.	Attributes
	cs1	Event details in JSON format.	{"name":"MIME_BUI LTIN_COMPOSITE", "module":"nlist_imp ort"}

Web access log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	webaccess

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).	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}
	suser	The username.	user_example (Unknown, if the user is unknown)
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Default Allow
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.

Field type	Field name	Description	Example value
	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)
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	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
	app	Application layer protocol and its version.	HTTP/1.1
	requestMethod	Method used to access the URL address (POST, GET, etc.).	GET

Field type	Field name	Description	Example value
	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
	cn3Label	Specifies the server's original response.	Response
	cn3	Status code.	302
	flexString1Label	Refers to the content type.	Media type
	flexString1	The type of the content.	text/html
	flexString2Label	Indicates the category of the requested URL.	URL Categories
	flexString2	URL category.	Computers & Technology
	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	40

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

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
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1701085036026
	deviceExternalId	The unique name of the device that generated the event.	utmcore@ntoorereaeda

Field type	Field name	Description	Example value
	act	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}]}
	app	Application layer protocol	DNS
	suser	The username.	user1 (Unknown, if the user is unknown)
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Rule1
	dhost	The destination host name, whose address is determined using the DNS server.	google.com
	proto	Level 4 protocol used.	UDP
	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
	cs2Label	Indicates the source zone.	Source Zone
	cs2	Source zone name.	Trusted

Field type	Field name	Description	Example value
	cs3Label	Indicates the source country.	Source Country
	cs3	Source country name.	AE (a two-letter country code is displayed)
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535. Port 53 is normally used for DNS.
	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 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		URL Categories

Field type	Field name	Description	Example value
		Indicates the category of the requested URL.	
	flexString1	URL category.	Search Engines & Portals

Differences in the **CEF Compact** format:

- The following fields are missing:
  - cs3Label=Source Country; cs3=$src_country
  - cs5Label=Destination Country; cs5=$dst_country
- The following fields have been changed:
  - cs2Label=SrcZone
  - cs3Label=DstZone; cs3=$dst_zone_name
  - cs4Label=Data; cs4=$data
  - flexString1Label=URLCats
- 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.

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

Field type	Field name	Description	Example value
	Threat Level	Application threat level.	Available values: from 1 (if no application) to 10 (the set threat level multiplied by 2).
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
	suser	The username.	user_example (Unknown, if the user is unknown)
	act	Action taken by the device according to the configured policies.	accept
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Allow trusted to untrusted
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	cs2Label	Indicates the source zone.	Source Zone
	cs2	Source zone name.	Trusted
	cs3Label	Indicates the source country.	Source Country
	cs3		

Field type	Field name	Description	Example value
		Source country name.	AE (a two-letter country code is displayed)
	proto	Level 4 protocol used.	TCP or UDP
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	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)
	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)
	in	Number of transmitted	231

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

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

Field type	Field name	Description	Example value
	Signature	Name of the triggered IPS signature.	BlackSun Test
	Threat Level	Signature threat level.	Available values: from 2 to 10 (the set threat level multiplied by 2).
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
	suser	The username.	user_example (Unknown, if the user is unknown)
	act	Action taken by the device according to the configured policies.	accept
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	IDPS Rule Example
	msg	Signature threat level and name.	[2] BlackSun
	app	Application layer protocol	HTTP
	proto	Level 4 protocol used.	TCP or UDP
	src	Traffic source IPv4 address.	10.10.10.10

Field type	Field name	Description	Example value
	spt	Source port	Values: 0-65535.
	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)
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	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)
	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

SCADA log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	scada
	Name	Source type.	log
	PDU Severity	SCADA severity.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 5: very high
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that generated the event.	utmcore@erstheta tica
	act	Action taken by the device according to the configured policies.	accept
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	Scada Rule Example

Field type	Field name	Description	Example value
	src	Traffic source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	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)
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	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)
	app	Application layer protocol	Modbus
	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":

Field type	Field name	Description	Example value
			0,"mb_payload":"AAIAAA==", "mb_message":"response","mb_addr": 0}

SSH inspection log format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log name.	ssh
	Name	Source type.	log
	Threat Level	Application threat level.	Available values: from 1 (if no application) to 10 (the set threat level multiplied by 2).
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

Field type	Field name	Description	Example value
	suser	The username.	user_example (Unknown, if the user is unknown)
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	SSH inspection rule
	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
	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)
	dst	IPv4 address of the traffic destination.	194.226.127.130
	dpt	Destination port	Values: 0-65535.
	cs4Label	Indicates the destination zone.	Destination Zone
	cs4	Destination zone name.	Untrusted
	cs5Label	Indicates the destination country.	Destination Country

Field type	Field name	Description	Example value
	cs5	Destination country name.	AE (a two-letter country code is displayed)
	cs6Label	Refers to the command transmitted via SSH.	Command
	cs6	Command transmitted via SSH, in JSON format.	whoami

Mail Security Log Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	mailsecurity
	Name	Source type.	log
	Threat Level	Application threat level.	Available values: • 0: info • 6: warning • 8: error • 10: critical
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	The unique name of the device that	utmcore@einerson stal

Field type	Field name	Description	Example value
		generated the event.	
	act	Action taken by the device according to the configured policies.	mark
	suser	The username.	user_example (Unknown, if the user is unknown)
	cs1Label	Indicates the rule name.	Rule
	cs1	Name for the mail security rule.	Mail security rule
	src	Source IPv4 address.	10.10.10.10
	spt	Source port	Values: 0-65535.
	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)
	dst	Destination IPv4 address.	10.10.10.10
	dpt	Destination port	Values: 0-65535.
	cs4Label	Indicates the traffic destination zone.	Destination Zone
	cs4	Traffic destination zone name.	Untrusted

Field type	Field name	Description	Example value
	cs5Label	Indicates the country of the traffic destination.	Destination Country
	cs5	The destination country.	AE (a two-letter country code is displayed)
	app	Application layer protocol	SMTP
	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
	flexString1Label	Indicates the sender's address.	From
	flexString1	Sender's email.	sender@example.com
	cs6Label	Indicates the recipient's address.	To
	cs6	Recipient's email.	receiver@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

Field type	Field name	Description	Example value
	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

Endpoint Event Log Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	endpoint_log
	Name	Source type.	log
	Severity	The severity of the event.	Available values: • 0: info • 6: warning • 8: error • 10: critical
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	ID of the device generated this event.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	suser	The username.	Admin

Field type	Field name	Description	Example value
	msg	Detailed information about the event.	Windows Defender state successfully changed to SECURITY_PRODUCT_STATE_ON.
	cs1Label	Specifies the endpoint device ID.	endpointId
	cs1	Endpoint device or sensor ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Indicates the name of the endpoint device or the sensor.	endpointName
	cs2	Endpoint device or sensor name.	DESKTOP-0731NFQ
	cs3Label	Indicates the event type.	logLevel
	cs3	Event type.	Success audit, Warning, Details, Rejection audit, Error
	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

Field type	Field name	Description	Example value
	cs6Label	Indicates the log event source.	sourceName
	cs6	Log event source.	Microsoft-Windows-Security-Auditing
	flexString1Label	Indicates the insertion string.	insertionString
	flexString1	The insertion string is the EventData block of the Windows event data.	Windows DefenderSECURITY_PRODUCT_STATE_ON
	cn1Label	Indicates the log event code.	logEventCode
	cn1	Log event code.	1154
	cn2Label	Indicates the event ID.	logEventId
	cn2	Event ID.	10016
	cn3Label	Indicates the log event type.	logEventType
	cn3	Log event type.	1 (error), 2 (warning), 3 (information), 4 (audit success), 5 (audit failure).

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

Field type	Field name	Description	Example value
	Source	Log type.	endpoint_log
	Name	Source type.	log
	Threat Level	Threat level for the URL category.	Values: 1-10: • 6: very low • 6: low • 6: medium • 8: high • 10: very high
CEF [extension]	**rt**	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	ID of the device generated this event.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Action taken by the device according to the configured policies.	accept
	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
	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.
	shost	Hostname.	www.google.com
	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 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

Field type	Field name	Description	Example value
	Source	Log type.	endpoint_applicati ons
	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-4e ac-b05b-d01bc284c4e8
	act	Action (application start or stop).	start, stop
	suser	User	DESKTOP-0731NF Q\User
	filePath	Path to the file.	C:\\Windows\ \system32\ \cmd.exe
	cs1Label	Specifies the endpoint device ID.	endpointId
	cs1	The endpoint device ID.	35fb5820-74db-4e ac-b05b-d01bc284c4e8
	cs2Label	Specifies the endpoint device NetBIOS name.	endpointName
	cs2	Endpoint device NetBIOS name.	DESKTOP-0731NF Q
	spid	Process ID.	3860
	fileHash	The application hash.	B4979A9F9700298 89713D756C3F1236 43DDE73DA

Field type	Field name	Description	Example value
	cs3Label	Indicates the command line.	cmdLine
	cs3	Command line prompt.	C:\\Windows\\system32\\sc.exe start w32time task_started
	cs4Label	Indicates the Session ID.	sessionId
	cs4	Session ID.	1656395717

Endpoint Hardware Log Format

Field type	Field name	Description	Example value
CEF header	**CEF:Version**	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	Device Version	Product version.	7
	Source	Log type.	endpoint_hardware
	Name	Source type.	log
	Threat Level	Default value.	0
CEF [extension]	**rt**	Time when the event was received (in milliseconds 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
	cs1Label	Specifies the endpoint device ID.	endpointId

Field type	Field name	Description	Example value
	cs1	The endpoint device ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Specifies the endpoint device NetBIOS name.	endpointName
	cs2	Endpoint device NetBIOS name.	DESKTOP-0731NFQ
	sourceServiceName	A Windows driver that allows the computer to communicate with hardware/device.	USBHUB3
	cs3Label	Specifies the ID of the device being connected or removed.	deviceId
	cs3	Device ID.	USB\\VID_0E0F&PID_0002\\6&201153C1&0&8
	cs4Label	Indicates the device name.	deviceName
	cs4	The name of the device.	Kingston DataTraveler 2.0 USB Device

Windows Active Directory 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.	endpoint_log

Field type	Field name	Description	Example value
	Name	Source type.	log
	Threat Level	Threat level.	Available values: from 1 to 10 (the set threat level multiplied by 2).
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
	suser	The username.	user1.dep.local
	msg	The event description in the AD log.	Group membership information Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: S-1-5-21-3795870133-5220325-2125745684-1103 Account Name: user1 Account Domain: DEP Logon ID: 0xA57A446 Event in sequence: 1 of 1 Group Membership: %{S-1-5-21-3795870133-5220325-2125745684-513} %{S-1-1-0} %{S-1-5-32-544} %{S-1-5-32-555} %{S-1-5-32-545} %{S-1-5-32-554} %

Field type	Field name	Description	Example value
			{S-1-5-2} % {S-1-5-11} % {S-1-5-15} % {S-1-5-21-3795870133-5220325-2125745684-512} % {S-1-5-21-3795870133-5220325-2125745684-572} % {S-1-5-64-10} % {S-1-16-12288} The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other

Field type	Field name	Description	Example value
			security audit events generated during this logon session.
	cn1Label	Indicates the event code in the AD log.	logEventCode
	cn1	Event code.	4627
	cn2Label	Indicates the event ID in the AD log.	logEventId
	cn2	Event ID.	4627
	cn3Label	Indicates the event type in the Windows log (System\Security\ Application, etc.).	logEventType
	cn3	Windows log event type.	4
	cs1Label	Indicates the ID of the endpoint — the source of the event.	endpointId
	cs1	The endpoint device ID.	16535060-5a1a-4e92-8331-239406ec34da
	cs2Label	Indicates the name of the endpoint — the source of the event (UserGate client, WMI sensor, etc.).	endpointName
	cs2	Endpoint device name.	dep.local
	cs3Label	Indicates the severity of the event in the AD log.	logLevel

Field type	Field name	Description	Example value
	cs3	Event severity level.	Audit Success
	cs4Label	Indicates the event category code (12554 Group Membership, 12544 Logon, 14337 Kerberos Service Ticket Operations, etc.).	logCategoryString
	cs4	The event's category.	Group Membership
	cs5Label	Indicates the Windows log file.	logFile
	cs5	Windows log file	Security
	cs6Label	Indicates the source of the AD log.	sourceName
	cs6	The source of the AD log.	Microsoft-Windows-Security-Auditing
	flexString1Label	Indicates the content of the event in the AD log.	insertionString
	flexString1	Parameters of the AD log event after message parsing.	['S-1-0-0', '-', '-', '0x0', 'S-1-5-21-3795870133-5220325-2125745684-1103', 'user1', 'DEP', '0x7a25a21', '3', '1', '1', '\\r\\n\\t\\t% {S-1-5-21-3795870133-5220325-2125745684-513}\\r\\n\\t\\t%{S-1-1-0}\\r\\n\\t\\t%{S-1-5-32-544}\\r\\n\\t\\t%{S-1-5-32-555}\\r\\n\\t\\t%

Field type	Field name	Description	Example value
			{S-1-5-32-545}\\r\\n\\t\\t%{S-1-5-32-554}\\r\\n\\t\\t%{S-1-5-2}\\r\\n\\t\\t%{S-1-5-11} \\r\\n\\t\\t%{S-1-5-15}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-512}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-572}\\r\\n\\t\\t%{S-1-5-64-10}\\r\\n\\t\\t%{S-1-16-12288}']

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: from 1 to 10 (the set threat level multiplied by 2).
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
	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
	cs2Label	Indicates the application that caused the event.	Tag
	cs2	The application that caused the event.	org.gnome.Shell.desktop

Field type	Field name	Description	Example value
	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

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
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-1-5-21-3795870133-5220325-21257

Field type	Field name	Description	Example value
			45684-513","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)
	cs1Label	Indicates that a rule was triggered.	Rule
	cs1	Name of the rule triggered to cause the event.	dev.local
	src	Traffic source IPv4 address.	10.10.0.11

Export logs in JSON format

Event log description

Field name	Description	Example value
user	The username.	Admin
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
ip_address	IPv4 address of the event source.	192.168.174.134
node	The unique name of the device that generated the event.	utmcore@ersthetatica
attributes	Event details in JSON format.	{"rule":{"logrotate":12,"attributes":

Field name	Description	Example value
		{"timezone":"Asia/Dubai"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}
event_type	Event type.	logexport_rule_updated
event_severity	The severity of the event.	info, warning, error, or critical
event_origin	Module where the event occurred.	core
event_component	Component where the event occurred.	console_auth

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
url_categories	**id**	ID of the category to which the URL belongs.	39
	threat_level	Threat level for the URL category.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	name	Name of the category to which the URL belongs.	Social Networking
bytes_sent		Number of bytes transmitted from the source to the destination.	52
node		The unique name of the device that generated the event.	utmcore@ersthetatica

Field name	Description	Example value
packets_recv	Number of bytes transmitted from the destination to the source.	5
request_method	Method used to access the URL address (POST, GET, etc.).	GET
url	Contains the URL of the requested resource and the protocol used.	http://www.secure.com
packets_sent	Number of packets transmitted from the source to the destination.	2
action	Action taken by the device according to the configured policies.	block
media_type	The type of the content.	application/json
host	Hostname.	www.google.com
session	Session ID.	a7a3cd49-8232-4f1a-962a-3659af89e96f (if System: 00000000-0000-0000-0000-000000000000)
app_protocol	Application layer protocol and its version.	HTTP/1.1
status_code	Status code.	302
bytes_recv	Number of packets transmitted from the destination to the source.	100
http_referer	Request source URL (HTTP referer).	https://www.google.com/
decrypted	Indicates if the content was decrypted.	true, false
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}]

Field name			Description	Example value
useragent			Browser useragent.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Source zone name.	Trusted
	country		Traffic source country.	AE (a two-letter country code is displayed)
	ip		Source IPv4 address.	10.10.10.10
	port		Source port	Values: 0-65535.
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.
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
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

<table>
<tr><th colspan="3">Field name</th><th>Description</th><th>Example value</th></tr>
<tr><td colspan="3">timestamp</td><td>Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.</td><td>2022-05-12T08:11:46.15869Z</td></tr>
<tr><td colspan="3">node</td><td>The unique name of the device that generated the event.</td><td>utmcore@ntoorereaeda</td></tr>
<tr><td colspan="3">proto</td><td>Level 4 protocol used.</td><td>UDP</td></tr>
<tr><td colspan="3">data</td><td>Indicates the data being transmitted.</td><td>{"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"}]}</td></tr>
<tr><td colspan="3">reasons</td><td>The reason why the event was created, e.g. the URL category on which the rule was triggered.</td><td>{"url_cats":[{"id":37,"name":"Search Engines & Portals","threat_level":1}]}</td></tr>
<tr><td rowspan="3">url_categories</td><td colspan="2">id</td><td>ID of the triggered URL category.</td><td>37</td></tr>
<tr><td colspan="2">threat_level</td><td>Threat level of the triggered category.</td><td>Available values:
• 1: very low
• 2: low
• 3: medium
• 4: high
• 5: very high</td></tr>
<tr><td colspan="2">name</td><td>Name of the triggered category.</td><td>Search Engines & Portals</td></tr>
<tr><td rowspan="2">source</td><td rowspan="2">zone</td><td>guid</td><td>Unique ID of the traffic source zone.</td><td>d0038912-0d8a-4583-a525-e63950b1da47</td></tr>
<tr><td>name</td><td>Traffic source zone name.</td><td>Trusted</td></tr>
</table>

<table>
<tr><th colspan="3">Field name</th><th>Description</th><th>Example value</th></tr>
<tr><td rowspan="3"></td><td colspan="2">country</td><td>Source country name.</td><td>AE (a two-letter country code is displayed)</td></tr>
<tr><td colspan="2">ip</td><td>IPv4 address of the traffic source.</td><td>10.10.10.10</td></tr>
<tr><td colspan="2">port</td><td>Source port</td><td>Values: 0-65535.</td></tr>
<tr><td rowspan="5">destination</td><td rowspan="2">zone</td><td>guid</td><td>Unique ID of the traffic destination zone.</td><td>3c0b1253-f069-4060-903b-5fec4f465db0</td></tr>
<tr><td>name</td><td>Traffic destination zone name.</td><td>Untrusted</td></tr>
<tr><td colspan="2">country</td><td>Destination country name.</td><td>AE (a two-letter country code is displayed)</td></tr>
<tr><td colspan="2">ip</td><td>IPv4 address of the traffic destination.</td><td>104.19.197.151</td></tr>
<tr><td colspan="2">port</td><td>Destination port</td><td>Values: 0-65535. Port 53 is normally used for DNS.</td></tr>
<tr><td rowspan="2">rule</td><td colspan="2">guid</td><td>Unique ID of the rule triggered to cause the event.</td><td>59e38e06-533a-4771-9664-031c3e8b2e1f</td></tr>
<tr><td colspan="2">name</td><td>Name of the rule triggered to cause the event.</td><td>Rule1</td></tr>
<tr><td rowspan="4">user</td><td colspan="2">guid</td><td>Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.</td><td>a7a3cd49-8232-4f1a-962a-3659af89e96f</td></tr>
<tr><td colspan="2">name</td><td>The username.</td><td>user1</td></tr>
<tr><td rowspan="2">groups</td><td>guid</td><td>Unique ID of the group the user is a member of.</td><td>919878b2-e882-49ed-3331-8ec72c3c79cb</td></tr>
<tr><td>name</td><td>Name of the group the user is a member of.</td><td>Default Group</td></tr>
</table>

Traffic log description

<table>
<tr><th colspan="2">Field name</th><th>Description</th><th>Example value</th></tr>
<tr><td colspan="2">timestamp</td><td>Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.</td><td>2022-05-12T08:11:46.15869Z</td></tr>
<tr><td colspan="2">bytes_sent</td><td>Number of bytes transmitted from the source to the destination.</td><td>100</td></tr>
<tr><td colspan="2">node</td><td>The unique name of the device that generated the event.</td><td>utmcore@ersthetatica</td></tr>
<tr><td colspan="2">packets_recv</td><td>Number of packets transmitted from the destination to the source.</td><td>1</td></tr>
<tr><td colspan="2">proto</td><td>Level 4 protocol used.</td><td>TCP or UDP</td></tr>
<tr><td colspan="2">packets_sent</td><td>Number of packets transmitted from the source to the destination.</td><td>1</td></tr>
<tr><td colspan="2">action</td><td>Action taken by the device according to the configured policies.</td><td>accept</td></tr>
<tr><td colspan="2">session</td><td>Session ID.</td><td>a7a3cd49-8232-4f1a-962a-3659af89e96f (if System: 00000000-0000-0000-0000-000000000000)</td></tr>
<tr><td colspan="2">bytes_recv</td><td>Number of bytes transmitted from the destination to the source.</td><td>6</td></tr>
<tr><td rowspan="2">signatures</td><td>id</td><td>ID of the triggered signature.</td><td>999999</td></tr>
<tr><td>threat_level</td><td>Threat level of the triggered signature.</td><td>Available values:
• 1: very low
• 2: low
• 3: medium
• 4: high
• 5: very high</td></tr>
</table>

Field name			Description	Example value
	name		Name of the triggered signature.	BlackSun Test
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
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.
nat	**source**	**ip**	Source address after reassignment (if NAT rules are configured).	192.168.117.85 (if NAT is not configured then **"nat":null**)

Field name			Description	Example value
		port	Source port after reassignment (if NAT rules are configured).	Values: 0-65535 (if NAT is not configured then **"nat":null**)
	destination	**ip**	Destination address after reassignment (if NAT rules are configured).	64.233.164.198 (if NAT is not configured then **"nat":null**)
		port	Source port after reassignment (if NAT rules are configured).	Values: 0-65535 (if NAT is not configured then **"nat":null**)
rule	**guid**		Unique ID of the rule triggered to cause the event.	59e38e06-533a-4771-9664-031c3e8b2e1f
	type		Rule type.	firewall
	name		Name of the rule triggered to cause the event.	Allow trusted to untrusted
user	**guid**		Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		The username.	Admin
	groups	**guid**	Unique ID of the group the user is a member of.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Name of the group the user is a member of.	Default Group

IDPS log description

Field name	Description	Example value
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Session ID.	a7a3cd49-8232-4f1a-962a-3659af89e96f (if System: 00000000-0000-0000-0000-000000000000)

<table>
<tr><th colspan="2">Field name</th><th>Description</th><th>Example value</th></tr>
<tr><td colspan="2">packets_sent</td><td>Number of packets transmitted from the source to the destination.</td><td>1</td></tr>
<tr><td colspan="2">packets_recv</td><td>Number of packets transmitted from the destination to the source.</td><td>1</td></tr>
<tr><td colspan="2">node</td><td>The unique name of the device that generated the event.</td><td>utmcore@ersthetatica</td></tr>
<tr><td colspan="2">proto</td><td>Level 4 protocol used.</td><td>TCP or UDP</td></tr>
<tr><td colspan="2">bytes_sent</td><td>Number of bytes transmitted from the source to the destination.</td><td>100</td></tr>
<tr><td colspan="2">bytes_recv</td><td>Number of bytes transmitted from the destination to the source.</td><td>6</td></tr>
<tr><td colspan="2">action</td><td>Action taken by the device according to the configured policies.</td><td>accept</td></tr>
<tr><td rowspan="3">application</td><td>id</td><td>Application ID.</td><td>195</td></tr>
<tr><td>threat_level</td><td>Application threat level.</td><td>Available values:
• 1: very low
• 2: low
• 3: medium
• 4: high
• 5: very high</td></tr>
<tr><td>name</td><td>Application name.</td><td>Youtube</td></tr>
<tr><td rowspan="2">user</td><td>guid</td><td>Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.</td><td>a7a3cd49-8232-4f1a-962a-3659af89e96f</td></tr>
<tr><td>name</td><td>The username.</td><td>Admin</td></tr>
</table>

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
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
signatures	**id**		ID of the triggered signature.	999999
	threat_level		Threat level of the triggered signature.	Available values: • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	name		Name of the triggered signature.	BlackSun Test
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Traffic source zone name.	Trusted
	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.	

Field name		Description	Example value
			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.

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

Field name	Description	Example value
mb_value	Value to write (for Write Single Coil, Write Single Register commands).	322
mb_unit_id	Device address.	186
mb_read_quantity	Number of values to read (Read Write Register command).	658
mb_read_addr	Start registry address to read (Read Write Register command).	122
mb_quantity	Number of values to read.	875
mb_payload	Register values (for Read Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil commands).	75be5ecdc24f9883
mb_or_mask	OR mask value of the Mask Write Register command.	1024
mb_message	Modbus message.	exception
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	Registry 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

Field name			Description	Example value
	iec104_asdu		The ASDU address (COA, or Common Object Address). Refers to the IEC-104 protocol.	123
app_protocol			Application layer protocol	Modbus
action			Action taken by the device according to the configured policies.	pass
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Traffic source zone name.	Trusted
	country		Source country name.	AE (a two-letter country code is displayed)
	ip		IPv4 address of the traffic source.	10.10.10.10
	port		Source port	Values: 0-65535.
destination	**zone**	**guid**	Unique ID of the traffic destination zone.	3c0b1253-f069-4060-903b-5fec4f465db0
		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

<table>
<tr><th colspan="3">Field name</th><th>Description</th><th>Example value</th></tr>
<tr><td colspan="3">timestamp</td><td>Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.</td><td>2022-05-12T08:11:46.15869Z</td></tr>
<tr><td colspan="3">node</td><td>The unique name of the device that generated the event.</td><td>utmcore@ersthetatica</td></tr>
<tr><td colspan="3">command</td><td>Command sent via SSH.</td><td>whoami</td></tr>
<tr><td colspan="3">app_threat</td><td>Application threat level.</td><td>Available values: from 2 to 10 (set application threat level multiplied by 2)</td></tr>
<tr><td colspan="3">app_protocol</td><td>Application layer protocol</td><td>SSH or SFTP</td></tr>
<tr><td colspan="3">app_id</td><td>Application ID.</td><td>195</td></tr>
<tr><td colspan="3">action</td><td>Action taken by the device according to the configured policies.</td><td>block</td></tr>
<tr><td rowspan="6">source</td><td rowspan="2">zone</td><td>guid</td><td>Unique ID of the traffic source zone.</td><td>d0038912-0d8a-4583-a525-e63950b1da47</td></tr>
<tr><td>name</td><td>Traffic source zone name.</td><td>Trusted</td></tr>
<tr><td colspan="2">country</td><td>Source country name.</td><td>AE (a two-letter country code is displayed)</td></tr>
<tr><td colspan="2">ip</td><td>IPv4 address of the traffic source.</td><td>10.10.10.10</td></tr>
<tr><td colspan="2">port</td><td>Source port</td><td>Values: 0-65535.</td></tr>
<tr><td colspan="2">mac</td><td>Source MAC address.</td><td>FA:16:3E:65:1C:B4</td></tr>
<tr><td rowspan="3">destination</td><td rowspan="2">zone</td><td>guid</td><td>Unique ID of the traffic destination zone.</td><td>3c0b1253-f069-4060-903b-5fec4f465db0</td></tr>
<tr><td>name</td><td>Traffic destination zone name.</td><td>Untrusted</td></tr>
<tr><td colspan="2">country</td><td>Destination country name.</td><td>AE (a two-letter country code is displayed)</td></tr>
</table>

Field name			Description	Example value
	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.	SSH Rule Example
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
from			Sender email.	sender@example.com
to			Recipient email.	receiver@example.com
app_protocol			Application layer network protocol.	SMTP
source	**zone**	**guid**	Unique ID of the traffic source zone.	d0038912-0d8a-4583-a525-e63950b1da47

Field name			Description	Example value
		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.	10.10.10.10
	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.	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
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

Field name	Description	Example value
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

<table>
<tr><th colspan="2">Field name</th><th>Description</th><th>Example value</th></tr>
<tr><td rowspan="3">url_categories</td><td>id</td><td>ID of the category to which the URL belongs.</td><td>39</td></tr>
<tr><td>threat level</td><td>Threat level for the URL category.</td><td>Available values:
• 1: very low
• 2: low
• 3: medium
• 4: high
• 5: very high</td></tr>
<tr><td>name</td><td>Name of the category to which the URL belongs.</td><td>Social Networking</td></tr>
<tr><td colspan="2">timestamp</td><td>Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.</td><td>2022-05-12T08:11:46.15869Z</td></tr>
<tr><td colspan="2">endpoint_name</td><td>Endpoint device name.</td><td>DESKTOP-0731NFQ</td></tr>
<tr><td colspan="2">endpoint_id</td><td>The endpoint device ID.</td><td>35fb5820-74db-4eac-b05b-d01bc284c4e8</td></tr>
<tr><td colspan="2">media_type</td><td>The type of the content.</td><td>application/json</td></tr>
<tr><td colspan="2">ip_protocol</td><td>Number of the network protocol used.</td><td>4</td></tr>
</table>

<table>
<tr><th colspan="2">Field name</th><th>Description</th><th>Example value</th></tr>
<tr><td colspan="2">host</td><td>Hostname.</td><td>www.google.com</td></tr>
<tr><td colspan="2">app_name</td><td>Application to which the firewall rule was applied.</td><td>C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe</td></tr>
<tr><td colspan="2">action</td><td>Action taken by the device according to the configured policies.</td><td>drop, accept, nat</td></tr>
<tr><td rowspan="2">source</td><td>ip</td><td>Source IPv4 address.</td><td>10.10.10.10</td></tr>
<tr><td>port</td><td>Source port</td><td>Values: 0-65535.</td></tr>
<tr><td rowspan="2">destination</td><td>ip</td><td>Destination IPv4 address.</td><td>104.19.197.151</td></tr>
<tr><td>port</td><td>Destination port</td><td>Values: 0-65535.</td></tr>
<tr><td rowspan="2">rule</td><td>guid</td><td>Unique ID of the rule triggered to cause the event.</td><td>f93da24d-74f9-4f8c-9e9b-8e6d02346fb4</td></tr>
<tr><td>name</td><td>Name of the rule triggered to cause the event.</td><td>Default allow</td></tr>
</table>

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

Field name	Description	Example value
app_name	Application that was started/ stopped.	C:\\Program Files (x86)\ \Microsoft\\Edge\ \Application\\msedge.exe
action	Action (application start or stop).	start, stop
version	The application version.	6.2.19041.746
subject	Signature subject.	Microsoft Corporation
issuer	The issuer of the application's certificate.	Microsoft Windows Production PCA 2011
cmd_line	Command line prompt.	C:\\Windows\\system32\ \svchost.exe -k wsappx -p -s AppXSvc
session_id	Session ID.	1656038456

Endpoint Hardware Log Description

Field name	Description	Example value
timestamp	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

Windows Active Directory 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_name	A name that uniquely identifies the UserGate device generating this event.	utmcore@ntoorereaeda
endpoint_id	ID of the endpoint that is the source of the event.	16535060-5a1a-4e92-8331-239406ec34da
endpoint_name	Имя конечного устройства — источника события (UserGate клиента, сенсора WMI итд.).	dep.local
user_name	The "User" field from AD log.	user1.dep.local
log_level	The "Keywords" field from AD log.	Audit Success
log_category_string	Event category code in the AD log.	Group Membership
log_file	Windows log file.	Security
source_name	The "Source" field from AD log.	Microsoft-Windows-Security-Auditing
data	Event description in the AD log.	Group membership information.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\tAccount Name:\t\t-\r\n\tAccount Domain:\t\t-\r\n\tLogon ID:\t\t0x0\r\n\r\nLogon Type:\t\t\t3\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-21-3795870133-5220325-2125745684-1103\r\n\tAccount Name:\t\tuser1\r\n\tAccount Domain:\t\tDEP\r\n\tLogon ID:\t\t0x7A25A21\r\n\r\nEvent in sequence:\t\t1 of 1\r\n\r\nGroup Membership:

Field name	Description	Example value
		\t\t\t\r\n\t\t%{S-1-5-21-3795870133-5220325-2125745684-513}\r\n\t\t%{S-1-1-0}\r\n\t\t%{S-1-5-32-544}\r\n\t\t%{S-1-5-32-555}\r\n\t\t%{S-1-5-32-545}\r\n\t\t%{S-1-5-32-554}\r\n\t\t%{S-1-5-2}\r\n\t\t%{S-1-5-11}\r\n\t\t%{S-1-5-15}\r\n\t\t%{S-1-5-21-3795870133-5220325-2125745684-512}\r\n\t\t%{S-1-5-21-3795870133-5220325-2125745684-572}\r\n\t\t%{S-1-5-64-10}\r\n\t\t%{S-1-16-12288}\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThis event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.
computer_name	Windows node from the AD log where the event took place.	DC1.dep.local

Field name	Description	Example value
insertion_string	Parameters of the AD log event after message parsing.	['S-1-0-0', '-', '-', '0x0', 'S-1-5-21-3795870133-5220325-2125745684-1103', 'user1', 'DEP', '0x7a25a21', '3', '1', '1', '\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-513}\\r\\n\\t\\t%{S-1-1-0}\\r\\n\\t\\t%{S-1-5-32-544}\\r\\n\\t\\t%{S-1-5-32-555}\\r\\n\\t\\t%{S-1-5-32-545}\\r\\n\\t\\t%{S-1-5-32-554}\\r\\n\\t\\t%{S-1-5-2}\\r\\n\\t\\t%{S-1-5-11}\\r\\n\\t\\t%{S-1-5-15}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-512}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-572}\\r\\n\\t\\t%{S-1-5-64-10}\\r\\n\\t\\t%{S-1-16-12288}']
error	Error code from the AD log that occurred while receiving data.	0
status	Error description from the AD log that occurred while receiving data.	
counter_id	Counter ID of the WMI sensor.	login_logout
log_event_code	The "Event code" field from AD log.	4627
log_event_id	The "Event ID" field from AD log.	4627
log_event_type	Windows log even type (System/Security/Application etc.)	4

Syslog Description

Field name		Description	Example value
timestamp		Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		The unique name of the device that generated the event.	utmcore@ntoorereaeda
syslog_facility		Syslog event source type. Example: user-level messages. For more information about Syslog facility values, see RFC 5424.	1
syslog_severity		Syslog event severity level. Example: warning. For more information about Syslog severity values, see RF C 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

UserID log description

Field name			Description	Example value
timestamp			Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node			The unique name of the device that generated the event.	utmcore@ntoorereaeda
reasons			The reason why the event was created.	{\"user_groups_sids\":[\"S-1-5-21-3795870133-5220325-2125745684-513\",\"S-1-5-21-3795870133-5220325-2125745684-512\",\"S-1-5-21-3795870133-5220325-2125745684-572\"], \"user_sid\":\"S-1-5-21-3795870133-5220325-2125745684-1103\",\"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-4e92-8331-239406ec34da
	name		Name of the rule triggered to cause the event.	dev.local
user	**guid**		Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f
	name		The username.	user1
	groups	**guid**	Unique ID of the group the user is a member of.	aa218609-8716-9252-df20-88c43a0d0bf6

Field name			Description	Example value
		name	Name of the group the user is a member of.	CN=Domain Users,CN=Users,DC=dev,DC=local