

The background of the page is a dark blue color. Overlaid on this is a complex network diagram consisting of numerous small, light blue circular nodes connected by thin, light blue lines. The nodes are scattered across the page, with a higher density in the upper and middle sections, creating a web-like structure that suggests connectivity and data flow.

Log Analyzer 7.1.0 Administrator Guide

Table of Contents

- [Introduction](#)
 - [Introduction \(Description\)](#)
- [LogAn Licensing](#)
 - [LogAn Licensing \(Description\)](#)
- [Initial Configuration](#)
 - [Description](#)
 - [HSC Deployment](#)
 - [Virtual Appliance Deployment](#)
 - [Connecting to LogAn](#)
- [Offline Server Operations](#)
 - [Offline Server Operations \(Description\)](#)
- [LogAn Configuration](#)
 - [General Settings Section](#)
 - [Device management](#)
 - [Administrators](#)
 - [Certificate Management](#)
 - [Auth servers](#)
 - [Authentication Profiles](#)
 - [User Catalogs](#)
 - [Expanding the system partition](#)
- [Network Configuration](#)
 - [Zone Configuration](#)
 - [Network Interface Configuration](#)
 - [Routes](#)
 - [Gateway Configuration](#)
- [Users and Devices](#)
 - [User-ID agent](#)
 - [Redistribution Profiles](#)
- [Command Line Interface \(CLI\)](#)
 - [Command Line Interface — CLI \(Description\)](#)
- [Sensors](#)
 - [General information](#)
 - [UserGate Sensors](#)
 - [SNMP Sensors](#)
 - [SNMP MIB Management](#)
 - [WMI Sensors](#)
 - [Endpoint devices](#)
- [Log Collector](#)
 - [Description](#)
 - [Syslog](#)

- [Libraries](#)
 - [IP Addresses](#)
 - [Emails](#)
 - [Phones](#)
 - [Notification Profiles](#)
 - [Syslog Applications](#)
 - [Agent UserID Syslog Filters](#)
- [Dashboard](#)
 - [Dashboard \(Description\)](#)
- [Diagnostics and Monitoring](#)
 - [Routes](#)
 - [Ping](#)
 - [Traceroute](#)
 - [DNS Query](#)
 - [Notifications](#)
 - [Alerts](#)
 - [SNMP](#)
 - [SNMP Parameters](#)
 - [SNMP Security Profiles](#)
 - [Alert Rules](#)
 - [SNMP](#)
 - [SNMP Parameters](#)
 - [SNMP Security Profiles](#)
- [Logs and Reports](#)
 - [Logs](#)
 - [Description](#)
 - [Event Log](#)
 - [Web Access Log](#)
 - [DNS Log](#)
 - [Traffic Log](#)
 - [IDPS Log](#)
 - [SCADA Log](#)
 - [SSH inspection log](#)
 - [Search History](#)
 - [Endpoint Log](#)
 - [Syslog](#)
 - [Mail Security Log](#)
 - [UserID Log](#)
 - [Windows Active Directory log](#)
 - [Logs Export](#)
 - [Data Search and Filtering](#)
 - [Reports](#)
 - [General information](#)
 - [Templates](#)
 - [Custom Report Templates](#)

- [Report Rules](#)
 - [Generated reports](#)
- [Technical Support](#)
 - [Technical Support \(Description\)](#)
- [ADMIN](#)
 - [ADMIN \(description\)](#)
- [Favorites](#)
 - [Favorites \(Description\)](#)
- [Appendices](#)
 - [Appendix 1. Network environment requirements](#)
 - [Log format description](#)
 - [Logs Export in CEF Format](#)
 - [Export logs in JSON format](#)

INTRODUCTION

Introduction (Description)

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

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

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

LOGAN LICENSING

LogAn Licensing (Description)

LogAn 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 LogAn server.

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

The following modules can be additionally licensed:

Name	Description
Security Update (SU) Module	The SU module grants the right to receive LogAn software updates.

Name	Description
	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.

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: <ul style="list-style-type: none"> • Management: the first VM interface. • Trusted - The 2nd interface of the virtual machine.

Name	Description
Step 6. Perform factory reset.	Start the LogAn VM. During loading, select Support Menu and then Factory reset . This is a critical step. This step is used to configure network adapters and increase the partition size on the hard disk to the full size specified at Step 4.

Connecting to LogAn

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

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

Note

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

Other network interfaces are disabled and require further configuration.

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.

Name	Description
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.	<p>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:</p> <ul style="list-style-type: none"> • Management (management network), port0 interface. • Trusted (LAN). It is assumed that the Trusted zone will connect LogAn to the network that will be used by UserGate gateways to send logs to it and by LogAn to access the Internet. <p>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.</p>
Step 6. Configure the Internet gateway.	In the Gateways section, specify the IP address for the Internet gateway on an Internet-connected network interface. Usually, this is the Trusted zone. For more details on configuring Internet gateways, see the Gateway Configuration chapter.
Step 7. Specify the system DNS servers.	In the DNS section, specify the IP addresses of your provider's or corporate DNS servers. For more details on DNS management, see the chapter General Settings Section .
Step 8. Register the product, if it was not registered at Step 4.	Register the product using the PIN code. For a successful registration, LogAn must have Internet access, and the previous steps must be completed. For more details on product licensing, see the LogAn Licensing chapter.
Step 9. (Optional) Create additional administrators.	In the Administrators section, create additional system administrators and grant them the necessary rights (roles).

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

OFFLINE SERVER OPERATIONS

Offline 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.

Name	Description
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.

LOGAN CONFIGURATION

General Settings Section

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

Name	Description
Admin console settings	<p>LogAn interface settings:</p> <ul style="list-style-type: none"> • 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	<p>Configure the time synchronization settings:</p> <ul style="list-style-type: none"> • 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.

Name	Description
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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Off: diagnostics logs are disabled • Error: log only server errors

Name	Description
	<ul style="list-style-type: none"> • Warning: log only errors and warnings • Info: log only errors, warnings, and additional information • Debug: provide as much detail as possible <p>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.</p>
Diagnostics logs	<ul style="list-style-type: none"> • Download logs: download the diagnostic logs for sending them to UserGate support. • Clear logs: purge logs of content.
Remote assistance	<ul style="list-style-type: none"> • On/Off: enable/disable the remote assistance mode. Remote assistance allows a UserGate support engineer to connect securely to a LogAn server for troubleshooting using the known values of the Remote assistance ID and token. For a successful activation of remote assistance, LogAn must have SSH access to the UserGate remote assistance server. • Remote assistance ID: a randomly generated value that is unique for each remote assistance session. that is unique for each remote assistance session. • Remote assistance token: a randomly generated token value. that is unique for each remote assistance session.

Server operations

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

Name	Description
Server operations	<ul style="list-style-type: none"> • Reboot: reboot the LogAn server • Shutdown: shutdown the LogAn server
Updates channel	<p>Here you can select the update channel for LogAn software:</p> <ul style="list-style-type: none"> • Stable: check for stable software updates and download them (if any) • Beta: check for experimental updates and download them (if any)

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

To install updates, follow these steps:

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

System backup management

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

To create a backup, follow these actions:

Name	Description
Step 1. Create a backup	

Name	Description
	<p>Under Device management → System backup management, click Create backup. The system will save the current server settings in a file named:</p> <p>backup_PRODUCT_NODE-NAME_DATE.gpg, where <i>PRODUCT</i> is the product type: NGFW, LogAn, or MC; <i>NODE-NAME</i> is the UserGate node name; <i>DATE</i> is the date and time when the backup was created as YYYY-MM-DD-HH-MM. The time is in UTC time zone.</p> <p>To interrupt the backup process, press the Stop button. The backup record will be displayed in the device event log.</p>

To restore the device status, follow these steps:

Name	Description
Step 1. Restore the device state	<p>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.</p>

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	<p>In the Device management → System backup management, click Add and enter a name and description for the rule.</p>
Step 2. Specify the remote server parameters	<p>In the Remote server tab of the rule, specify the parameters for the remote server:</p> <ul style="list-style-type: none"> • 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 <p>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.</p> <p>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</p>

Name	Description
	<p>user keys directory <code>/home/user/.ssh/</code> in the <code>authorized_keys</code> file.</p> <p>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 <code>known_hosts</code>. The files are not sent without verification.</p> <p>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.</p>
<p>Step 3. Select the upload schedule</p>	<p>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:</p> <p>(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)</p> <p>Each of the first five fields can be defined using:</p> <ul style="list-style-type: none"> • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • The asterisk and dash are also used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*/2" in the "hours" field means "every two hours".

Exporting and importing settings

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

Note

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

To export the settings, follow these steps:

Name	Description
Step 1. Export the settings.	<p>Under Device management → Settings export and import, click Export and select Export all settings or Export network settings. The system will save:</p> <ul style="list-style-type: none"> • 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_YY YYMMDD_HHMMSS.bin <p>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.</p> <p>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.</p>

To apply the exported settings, follow these steps:

Name	Description
Step 1. Import the settings.	<p>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.</p>

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.	<p>Under Device management → Settings export and import, click Add and enter a name and description for the rule.</p>
Step 2. Specify the remote server parameters.	<p>In the Remote server tab of the rule, specify the parameters for the remote server:</p> <ul style="list-style-type: none"> • 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

Name	Description
	<ul style="list-style-type: none"> • Directory path: the path on the server where the settings will be uploaded
<p>Step 3. Select the upload schedule.</p>	<p>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:</p> <p>(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)</p> <p>Each of the first five fields can be defined using:</p> <ul style="list-style-type: none"> • 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
<p>Step 1. Create an administrator access profile.</p>	<p>In the Administrators → Administrator profiles section, click Add and enter the desired settings.</p>
<p>Step 2. Create an administrator account and assign it one of the</p>	

Name	Description
administrator profiles created earlier.	<p>In the Administrators section, click Add and select the desired option.</p> <ul style="list-style-type: none"> • Add local administrator: create a local user, set a password for the user, and assign them one of the access profiles created earlier. • Add LDAP user: add a user from an existing domain. This requires a correctly configured LDAP connector in the Auth servers section. When logging in to the administrative console, the username must be specified in the user@domain format. Assign this user a profile created earlier. • Add LDAP group: add a user group from an existing domain. This requires a correctly configured LDAP connector in the Auth servers section. When logging in to the administrative console, the username must be specified in the user@domain format. Assign this user a profile created earlier. • Add administrator with auth profile: create a user and assign them an administrator profile created earlier and an auth profile (this requires correctly configured auth servers).

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

Name	Description
Name	Profile name.
Description	Profile description.
Permissions	<p>The list of web console tree objects available for delegation. The following access options are available:</p> <ul style="list-style-type: none"> • No access • Read only • Read and write.

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

To configure the above settings, follow these steps:

Name	Description
Step 1. Configure the password policy.	In the Administrators → Administrators section, click Configure .
Step 2. Fill in the relevant fields.	<p>Provide values for these fields:</p> <ul style="list-style-type: none"> • Strong password: enables the additional password complexity settings presented below, such as Minimum length, Minimum uppercase letters, Minimum lowercase letters, Minimum digit letters, Minimum special characters, and Maximum characters repetition block. • Number of invalid auth attempts: the number of failed attempts to authenticate as an administrator after which the account is blocked for Block time. • Block time: the time for which the account is blocked.

The **Administrators → Administrator sessions** section displays all administrators who are logged in to the 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. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе [Настройка зон](#).

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.	<p>Provide values for these fields:</p> <ul style="list-style-type: none"> • Name: the name under which the certificate will be displayed in the certificate list. • Description: a description of the certificate. • Country: the country where the certificate is being issued. • State or province name: the state or province where the certificate is being issued. • Locality name: the city or town where the certificate is being issued. • Organization name: the name of the organization to which the certificate is being issued. • Common name: the certificate name. To ensure compatibility with the majority of browsers, we recommend using only Latin characters. • Email: your company's email.
Step 3. Specify the purpose of the certificate.	After creating the certificate, specify its intended role in LogAn. To do that, select the relevant certificate in the certificate list, click Edit , and specify the Web console SSL certificate type. After that, LogAn will restart the web console service and invite you to connect using the new certificate.

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

To export a certificate, follow these steps:

Name	Description
Step 1. Select a certificate for export.	Select the desired certificate in the certificate list.
Step 2. Export the certificate.	<p>Select the export type:</p> <ul style="list-style-type: none"> • 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.	<p>Provide values for these fields:</p> <ul style="list-style-type: none"> • Name: the name under which the certificate will be displayed in the certificate list. • Description: a description of the certificate. • Certificate file: the certificate data file. • Private key: the private key file for the certificate. • Passphrase: specify the private key passphrase (if required). • Certificate's chain: a file containing the upstream CA certificates used when creating this certificate.

Auth servers

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

LDAP Connector

An LDAP connector allows you to:

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

• Authorize LogAn administrators via Active Directory/FreeIPA domains.

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

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

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

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

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

RADIUS Authentication Server

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

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

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

To authorize users in UserGate's web interface using a RADIUS server, you need to configure an authentication profile. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации](#).

TACACS+ Authentication Server

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

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

Name	Description
Enabled	Enables or disables the use of this authentication server.
Name	The name of the TACACS+ authentication server.

Name	Description
Description	An optional description of the server.
Secret	Pre-shared key used by the TACACS+ protocol for authentication.
Address	The IP address for the TACACS+ server.
Port	The UDP port on which the TACACS+ server listens for authentication requests.
Use single TCP connection	Use a single TCP connection for communicating with the TACACS+ server.
Timeout (sec.)	The authentication timeout for the TACACS+ server. The default is 4 seconds.

To authorize users in UserGate’s web interface using a TACACS+ server, you need to configure an authentication profile. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации](#).

Authentication Profiles

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

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

User Catalogs

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

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

Name	Description
Enabled	Enables or disables this LDAP connector.
Name	The name of the LDAP connector.
Description	LDAP connector description.
SSL	This specifies whether SSL is required to connect to the LDAP server.
LDAP domain name or IP address	The IP address of the domain controller, the domain controller FQDN or the domain FQDN (e.g., test.local). If the domain controller FQDN is specified, UserGate will obtain the domain controller's address using a DNS request. If the domain FQDN is specified, UserGate will use a backup domain controller if the primary one fails.
Bind DN ("login")	The username for connecting to the LDAP server. Must be in the DOMAIN\username or username@domain format. This user must be already created in the domain.
Password	The user's password for connecting to the domain.
LDAP domains	The list of domains served by the specified domain controller, e.g., in case of a domain tree or an Active Directory domain forest.
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. 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.	<p>Configure the network flood protection settings for TCP (SYN-flood), UDP, and ICMP protocols in the zone:</p> <ul style="list-style-type: none"> • 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. <p>The recommended values are 300 requests per second for the alert threshold and 600 requests per second for the drop threshold.</p> <p>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.</p>
Step 3. (Optional) Configure the access control settings for the zone.	<p>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.</p> <p>The following services exist:</p> <ul style="list-style-type: none"> • 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).

Name	Description
	<ul style="list-style-type: none"> • CLI over SSH: provides server access for management using CLI (command line interface) (TCP port 2200). • Log Analyzer: the Log Analyzer service. Needs to be allowed in zones from which 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). <p>For more on network availability requirements, see Appendix 1. Network Environment Requirements.</p>
<p>Step 4. (Optional) Configure the IP spoofing protection settings.</p>	<p>IP spoofing attacks allow a malicious actor to transmit a packet from one network, such as Trusted, to another, such as Management. To do that, the attacker substitutes the source IP address with an assumed address of the relevant network. In this case, responses to this packet will be sent to the internal address.</p> <p>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.</p> <p>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.</p>

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	<p>The aggregation mode must match the operating mode for the device to which the bond is connected. The options are:</p> <ul style="list-style-type: none"> • 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: $[(XOR) \text{ MOD }]$. This means that the same NIC sends packets to the same recipients. Optionally, the transmission allocation can also be based on the xmit_hash policy. The XOR policy is used to provide load balancing and high availability. • Broadcast. Transmits everything on all network interfaces. This policy is used for high availability. • IEEE 802.3ad. The default mode, supported by most network switches. Creates aggregated groups of NICs

Name	Description
	<p>with identical speed and duplex settings. When combined like this, all links in the active aggregation participate in transmission as per IEEE 802.3ad. The choice of interface for packet transmission is determined by the policy. By default, the XOR policy is used, with the xmit_hash policy as a possible alternative.</p> <ul style="list-style-type: none"> • 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	<p>Determines the interval between LACPDU packets sent by the partner in the 802.3ad mode. Enumerated options:</p> <ul style="list-style-type: none"> • Slow: requests that the partner send LACPDU packets every 30 seconds. • Fast: requests that the partner send LACPDU packets every second.

Name	Description
Failover MAC	<p>Determines how MAC addresses will be assigned to the bonded slaves in the active-backup mode on switching between slaves. The normal behavior is to use the same MAC address on all slaves. Enumerated options:</p> <ul style="list-style-type: none"> • 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	<p>Determines the hash policy for packet transmission via bonded interfaces in the XOR or IEEE 802.3ad modes. Enumerated options:</p> <ul style="list-style-type: none"> • 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	<p>The IP address assignment method: no address, a static IP address, or a dynamic IP address obtained using DHCP.</p>

Routes

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

To add a route, follow these steps:

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

Gateway Configuration

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

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

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

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

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

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

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 Settings .

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: <code>ssh Admin@IPUserGateLogAn -p 2200</code>
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	<p>Check the availability of a 3rd party HTTP/HTTPS server.</p> <p>netcheck [-t TIMEOUT] [-d] URL</p> <p>Options:</p> <ul style="list-style-type: none"> -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 a LogAn server. A sensor can be a UserGate NGFW device, a UserGate Client endpoint, or any other network device that supports SNMP data transfer.

UserGate Sensors

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

Name	Description
Step 1. On the UserGate node, enable the Log Analyzer 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 SNMP 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	<p>The authentication mode. The available options are:</p> <ul style="list-style-type: none"> • No authentication; No encryption (noAuthNoPriv) • Authentication; No encryption (authNoPriv) • Authentication; Encryption (authPriv). <p>The authPriv mode is considered the most secure.</p>
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	<p>Specify all data here that LogAn should query from the network device. The counters can be selected from the MIBs uploaded to the device.</p> <p>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.</p>

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.

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: <ul style="list-style-type: none"> • TCP • UDP.
Port	The port number used to collect syslog events. The default port is 514.
Max session number	The maximum allowed number of concurrent devices connected for message sending.
Secure connection	Enable or disable data flow encryption.

Name	Description
	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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Emergency: a critical state that affects system health • Alert: a state that requires immediate intervention. • Critical: a state that requires immediate intervention or signals a fault in the system. • Error: messages about system faults • Warnings: warnings on potential errors that can occur if no action is taken.

Name	Description
	<ul style="list-style-type: none"> • Notice: events that relate to unusual system behavior but are not errors. • Info: informational alerts • Debug: information useful to developers for debugging applications
Object	<p>The event's category:</p> <ul style="list-style-type: none"> • 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	<p>The name of the application for which the collection of information should be allowed or blocked.</p> <p>Подробнее читайте в разделе Приложения syslog.</p>

Записи событий будут отображены в журнале **Syslog**, подробнее читайте в разделе [Системный журнал](#).

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: <pre style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">X.X.X.X Y.Y.Y.Y Z.Z.Z.Z</pre>
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.

Name	Description
<p>Step 5. Create an IP address list and specify an update URL for it.</p>	<p>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.</p> <div data-bbox="587 450 1417 600" style="border: 1px solid #0056b3; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>Note The list URL format is <code>http://x.x.x.x/</code> or <code>ftp://x.x.x.x/</code>.</p> </div> <p>The schedule can be configured in the list properties. The available options are:</p> <ul style="list-style-type: none"> • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. <p>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:</p> <ul style="list-style-type: none"> • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "*" / 2 in the "hours" field means "every two hours".

Emails

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

To add a new email group, follow these steps:

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

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

Name	Description
Step 1. Create a file with the relevant email list.	Create a file named list.txt with the email list.
Step 2. Create an archive containing this file.	Put the file in a ZIP archive named list.zip .
Step 3. Create a version file for the list.	Create a file named version.txt and specify the list version number inside it, such as 3. On each update of the list, the version number must be incremented.
Step 4. Upload the files to a web server.	Upload the list.zip and version.txt files to your website so that they can be downloaded.
Step 5. Create an email list and specify an update URL for it.	<p>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:</p> <ul style="list-style-type: none"> • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced.

Name	Description
	<p>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:</p> <ul style="list-style-type: none"> • 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.	<p>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:</p> <ul style="list-style-type: none"> • Disabled: update checking will not be performed for the selected item • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. <p>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:</p> <ul style="list-style-type: none"> • An asterisk (*) denotes the entire range (from the first number to the last). • A dash (-) denotes a number range. For example, "5-7" means 5, 6, and 7. • Lists: comma-separated numbers or ranges. For example, "1,5,10,11" or "1-11,19-23". • An asterisk or range spacing: used for spacing out values in ranges. The increment is given after a slash. Examples: "2-10/2" means "2,4,6,8,10" while "* / 2" in the "hours" field means "every two hours".

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

Notification Profiles

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

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

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

Name	Description
Name	Profile name.
Description	Profile description.
Host	The IP address of the SMTP server that will be used for sending emails.
Port	The TCP port used by the SMTP server. Usually, SMTP uses port 25, and SMTP with SSL uses port 465. Consult your email server administrator regarding this value.
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.

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

Syslog Applications

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

To add an application, follow these steps:

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

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 → Agent 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.

Name	Description
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: <ul style="list-style-type: none"> • 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.
Use ICMP	Use ICMP to execute the traceroute command. If not specified, UDP is used.
Interface	Network interface from which to execute the command.

Name	Description
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.

Name	Description
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 SNMP 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	Contrack 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.
trapRaidStatus	RAID status has been changed.
trapPowerSupply	The first power supply is off.

Name	Description
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: <ul style="list-style-type: none"> • 0: master node • 1: slave node • 3: fault
utmHAStatusReason	Integer	Reason for the change of the HA cluster node status: <ul style="list-style-type: none"> • 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 %).

Name	Data type	Description
utmMemory	Integer	RAM usage (in %).
utmLogdiskSpace	Integer	Disk space used for logs (in %).
utmAdaptecRaidStatus	Integer	<p>Current status of RAID (Redundant Array of Independent Disks) built on the Adaptec controller:</p> <ul style="list-style-type: none"> • 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	<p>Current status of RAID (Redundant Array of Independent Disks) built on the Broadcom controller:</p> <ul style="list-style-type: none"> • 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	<p>Number of power supplies:</p> <ul style="list-style-type: none"> • 1: one power supply • 2: two power supplies

Name	Data type	Description
utmPowerSupplyStatus	Integer	State of the power supply: <ul style="list-style-type: none"> • no_power_supplies. • 0: off • 1: on
utmCSCIfName	String	The interface name.
utmCSCStatus	Integer	Status of the network adapter: <ul style="list-style-type: none"> • 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.
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: <ul style="list-style-type: none"> • no_power_supplies. • on • off
Sys_power_supply2_status	String	

Name	Data type	Description
		<p>State of the second power supply:</p> <ul style="list-style-type: none"> • no_power_supplies. • on • off
Sys_raid_status	Integer	<p>Current status of RAID (Redundant Array of Independent Disks):</p> <ul style="list-style-type: none"> • 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.
ifDescr	String	Interface description.
ifType	Integer	<p>Interface type determined according to the physical/link layer protocol:</p> <ul style="list-style-type: none"> • 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

Name	Data type	Description
		<p>the OSI X.25 network mode.</p> <ul style="list-style-type: none"> • 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. • 18: ds1: can handle 24 simultaneous

Name	Data type	Description
		<p>connections at a total speed of 1.544Mbit/s; also called T1.</p> <ul style="list-style-type: none"> • 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 variety of data

Name	Data type	Description
		<p>transmission environments.</p> <ul style="list-style-type: none"> • 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).
ifAdminStatus	Integer	<p>Interface state assigned by the administrator:</p> <ul style="list-style-type: none"> • 1: up: ready to transmit packets • 2: down: not working • 3: testing: working in the test mode; cannot transmit work packets

Name	Data type	Description
ifOperStatus	Integer	<p>Current operating status of the interface:</p> <ul style="list-style-type: none"> • 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
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.

Name	Data type	Description
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 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.

Name	Data type	Description
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.
ifHCInBroadcastPkts	counter64	Identical to ifInBroadcastPkts : number of broadcast packets delivered; a counter with the larger capacity is used.
ifHCOctets	counter64	Identical to ifOutOctets : number of bytes transmitted by this interface, including service bytes; a counter with the larger capacity is used.
ifHCOUcastPkts	counter64	Identical to ifOutUcastPkts : number of unicast packets sent; this includes packets

Name	Data type	Description
		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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 1: true: station receives all packets/frames regardless of the destination. • 2: false: interface receives only packets/frames addressed to this station. <p>The object value does not affect the reception of broadcast and multicast packets/frames.</p>
ifAlias	String	

Name	Data type	Description
		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	<p>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.</p> <p>The Engine ID can be generated in these formats:</p> <ul style="list-style-type: none"> • IPv4 (ip4) • IPv6 (ipv6) • MAC address (mac) • Text (text) • Octets (octets).
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	<p>Select an authentication mode for the SNMP manager. The available options are:</p> <ul style="list-style-type: none"> • No authentication; No encryption (noAuthNoPriv) • Authentication; No encryption (authNoPriv) • Authentication; Encryption (authPriv). <p>The authPriv mode is considered the most secure.</p>
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.

Name	Description
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.

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

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

You can download the following MIB files:

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

UTM-TRAPS-MIB

Name	Description
trapCoreCrush	Core crash.
trapStatDown	Statistics service (UserGate Log Analyzer) unavailable.
trapCoreBootstrapEnd	Server booting has finished successfully.
trapDefaultGatewayChanged	Default gateway has been changed.
trapHighSessionsCounter	Conntrack table 90% full.
trapHighUsersCounter	Number of active users has reached 90% of the license threshold.
trapDataPartitionFSStatus	File system status. The file system status changed to "not_clean".
trapStatusChanged	Status of the HA cluster node has been changed.
trapMemberUp	Status of the HA cluster node has been changed to "Connected".
trapMemberDown	HA cluster node has been disconnected.
trapAttackDetected	Detection of an attack by the IDPS.
trapChecksumFailed	Binary files checksum mismatch.
trapHighCPUUsage	High CPU usage.
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.
trapHighDiskIOUtilization	High disk load. An alert is sent when the load is $\geq 95\%$ 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	Maximum number of active users.
utmDataPartionFSStatus	Integer	File system status. <ul style="list-style-type: none"> • 0 — clean. • 1 — not clean.
utmHAStatus	Integer	Current status of the HA cluster node: <ul style="list-style-type: none"> • 0: master node • 1: slave node • 3 — fault.

Name	Data type	Description
utmHAStatusReason	Integer	Reason for the change of the HA cluster node status: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • no_raid. • 0: optimal: the array is in its optimal state • 1: degraded: one drive has completely or partially failed. • 2: rebuild: array rebuild in progress
utmBroadcomRaidStatus	Integer	Current status of RAID (Redundant Array of Independent Disks) built on the Broadcom controller: <ul style="list-style-type: none"> • 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
		<p>status occurs if 2 disks fail.</p> <ul style="list-style-type: none"> • 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	<p>Number of power supplies:</p> <ul style="list-style-type: none"> • 1: one power supply • 2: two power supplies
utmPowerSupplyStatus	Integer	<p>State of the power supply:</p> <ul style="list-style-type: none"> • no_power_supplies. • 0 — off. • 1 — on.
utmCSCIfName	String	The interface name.
utmCSCStatus	Integer	<p>Status of the network adapter:</p> <ul style="list-style-type: none"> • 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 UDP sessions. (*)
icmpSessionsCounter	Integer	Current number of active ICMP sessions. (*)
sessionsRate10	Integer	Number of new sessions per second. Average value for the last 10 seconds. (*)
sessionsRate60	Integer	Number of new sessions per second. Average value for the last 60 seconds. (*)
sessionsRate300	Integer	Number of new sessions per second. Average value for the last 300 seconds. (*)
tcpSessionsRate10	Integer	Number of new TCP sessions per second. Average value for the last 10 seconds. (*)
tcpSessionsRate60	Integer	Number of new TCP sessions per second. Average value for the last 60 seconds. (*)
tcpSessionsRate300	Integer	Number of new TCP sessions per second. Average value for the last 300 seconds. (*)
udpSessionsRate10	Integer	Number of new UDP sessions per second. Average value for the last 10 seconds. (*)

Name	Data type	Description
udpSessionsRate60	Integer	Number of new UDP sessions per second. Average value for the last 60 seconds. (*)
udpSessionsRate300	Integer	Number of new UDP sessions per second. Average value for the last 300 seconds. (*)
icmpSessionsRate10	Integer	Number of new ICMP sessions per second. Average value for the last 10 seconds. (*)
icmpSessionsRate60	Integer	Number of new ICMP sessions per second. Average value for the last 60 seconds. (*)
icmpSessionsRate300	Integer	Number of new ICMP sessions per second. Average value for the last 300 seconds. (*)
dnsRequestCounter	Integer	Total DNS requests. (*)
dnsBlockedRequestCounter	Integer	Blocked DNS requests. (*)
dnsRequestRate	Integer	DNS requests per second. (*)
httpRequestCounter	Integer	Total HTTP requests. (*)
httpBlockedRequestCounter	Integer	Blocked HTTP requests. (*)
httpRequestRate	Integer	HTTP queries per second. (*)
dataPartitionFSStatus	String	File system status.
haStatus	Integer	The current state of the cluster node.
cpuLoad	Integer	System CPU load (in %).
memoryUsed	Integer	RAM usage (in %).
logDiskSpace	Integer	Disk space used for logs (in %).
powerSupply1Status	String	

Name	Data type	Description
		State of the first power supply: <ul style="list-style-type: none"> • no_power_supplies. • on • off
powerSupply2Status	String	State of the second power supply: <ul style="list-style-type: none"> • no_power_supplies. • on • off
raidType	String	RAID array type.
raidStatus	String	Current status of RAID (Redundant Array of Independent Disks): <ul style="list-style-type: none"> • no_raid. • 0: optimal: the array is in its optimal state • 1: degraded: one drive has completely or partially failed. • 2: rebuild: array rebuild in progress
diskIOUtilization	Integer	Current disk utilization (%).
diskIOUtilization60	Integer	Disk utilization (%). Average value for the last 60 seconds.
diskIOUtilization300	Integer	Disk utilization (%). Average value for the last 300 seconds.

 **Note**

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

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	<p>Interface type determined according to the physical/link layer protocol:</p> <ul style="list-style-type: none"> • 1: other: unknown type • 2: regular1822: defined in BBN Report 1822 • 3: hdh1822: defined in BBN Report 1822 • 4: ddn-x25: defined in BBN Report 1822 • 5: defined in the data link layer standard of the OSI X.25 network model • 6: ethernet-csmacd: Ethernet-type network interface regardless of speed (defined in RFC 3635) • 7: iso88023-csmacd: defined in IEEE 802.3 • 8: iso88024-tokenBus: defined in IEEE 8802.4 • 9: iso88025-tokenRing: network interface uses a Token Ring connection; defined in the IEEE 802.5 standard. • 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.

Name	Data type	Description
		<ul style="list-style-type: none"> • 13 — proteon-80Mbit — Proteon 80 Mbit. • 14: hyperchannel: high-speed channel used in ISDN networks. • 15: fddi: network interface uses FDDI (Fiber Distributed Data Interface) connection. FDDI is a set of standards for data transmission over fiber-optic lines in local networks. • 16: lapb: data link layer protocol used to transmit X.25 standard packets. • 17: sdlc: data link layer protocol for IBM system network architecture. • 18: ds1: can handle 24 simultaneous connections at a total speed of 1.544Mbit/s; also called T1. • 19: e1: European equivalent of T1. • 20: basicISDN: used for communication between the subscriber's equipment and the ISDN station. • 21: primaryISDN: used to connect to broadband backbones, connecting local and central PBX or network switches. • 22: propPointToPointSerial: defined in RFC1213. • 23: ppp: network interface uses PPP (Point-To-Point Protocol) connection.

Name	Data type	Description
		<ul style="list-style-type: none"> • 24: softwareLoopback: network interface configured as a loopback adapter. These interfaces are often used for testing; they do not send traffic to the network. • 25: eon: ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); defined in ISO/IEC 8473-1. • 26: ethernet-3Mbit: network interface uses a 3Mbit/s Ethernet connection. This version of Ethernet is defined in the IETF standard RFC 895. • 27: nsip, XNS over IP: intended for use in a variety of data transmission environments. • 28: slip: network interface uses a SLIP (Serial Line Internet Protocol) connection. SLIP is defined in the IETF RFC 1055 standard. • 29 — ultra — ULTRA Technologies. • 30: ds3: high-speed data interface multiplexing DS1 and DS2 signals; also know as T3. • 31: sip: network interface uses a SLIP (Serial Line Internet Protocol) connection. SLIP is defined in the IETF RFC 1055 standard. • 32: frame-relay: allows packet-switched data transmission across an

Name	Data type	Description
		interface between user devices and network equipment.
ifMtu	Integer	Maximum size of a network layer packet that can be sent over this interface.
ifSpeed	gauge32	Interface bandwidth in bits per second.
ifPhysAddress	String	Physical interface address (MAC address).
ifAdminStatus	Integer	<p>Interface state assigned by the administrator:</p> <ul style="list-style-type: none"> • 1: up: ready to transmit packets • 2: down: not working • 3: testing: working in the test mode; cannot transmit work packets.
ifOperStatus	Integer	<p>Current operating status of the interface:</p> <ul style="list-style-type: none"> • 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,

Name	Data type	Description
		usually a piece of hardware, is missing <ul style="list-style-type: none"> • 7: lowerLayerDown: network interface cannot transmit data packets because it is running on top of one or more other interfaces, and at least one of those "lower-layer" interfaces is down
ifLastChange	timeticks	SysUpTime value when the interface switches to this state.
ifInOctets	counter32	Number of bytes received by the interface, including service bytes.
ifInUcastPkts	counter32	Number of delivered unicast packets.
ifInNUcastPkts	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.

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

Name	Data type	Description
		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.
ifHCOctets	counter64	Identical to ifOutOctets : number of bytes transmitted by the interface, including service bytes; uses a higher capacity counter.
ifHCOUcastPkts	counter64	Identical to ifOutUcastPkts : number of sent unicast packets, including packets that were dropped or not sent; uses a higher capacity counter.
ifHCOmulticastPkts	counter64	Identical to ifOutMulticastPkts : number of sent multicast packets, including packets that were dropped or not sent; uses a higher capacity counter.
ifHCObroadcastPkts	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: <ul style="list-style-type: none"> • 1: enabled • 2: disabled
ifHighSpeed	gauge32	

Name	Data type	Description
		Current estimated interface bandwidth pool in bit/s, kbit/s, Mbit/s, or Gbit/s.
ifPromiscuousMode	Integer	<p>Promiscuous mode. Available values:</p> <ul style="list-style-type: none"> • 1: true: station receives all packets/frames regardless of the destination. • 2: false: interface receives only packets/frames addressed to this station. <p>The object value does not affect the reception of broadcast and multicast packets/frames.</p>
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	<p>A specific sensor info:</p> <ul style="list-style-type: none"> • thermName (string): sensor name.

Name	Data type	Description
		<ul style="list-style-type: none"> 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.

Name	Description
	<p>The Engine ID can be generated in these formats:</p> <ul style="list-style-type: none"> • 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	<p>Select an authentication mode for the SNMP manager. The available options are:</p> <ul style="list-style-type: none"> • No authentication; No encryption (noAuthNoPriv) • Authentication; No encryption (authNoPriv) • Authentication; Encryption (authPriv). <p>The authPriv mode is considered the most secure.</p>
Authentication algorithm	<p>The algorithm used for authentication. Possible to use:</p> <ul style="list-style-type: none"> • SHA1 • MD5 • SHA224 • SHA256

Name	Description
	<ul style="list-style-type: none"> • 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.

Event Log

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

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

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

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

Web Access Log

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

- UserGate node where the event occurred
- Event time
- User
- Actions
- Rule
- Reasons (if a site is blocked)
- Destination URL
- Source zone
- Source IP address
- Source port
- IP dest
- Destination port
- Categories
- Protocol (HTTP)
- Type (HTTP)
- Status code (HTTP)
- MIME (if present)
- Bytes sent/received
- Packets sent
- Referrer (if present)
- Operating system

- browser Useragent

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

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

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

DNS Log

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

The following information is displayed:

- Node
- Time
- User
- Rule
- Reasons
- Domain name
- Source zone
- Source IP address
- Source port
- Source MAC address.
- Destination zone
- Destination IP address
- Destination port

- Network protocol
- URL category.
- Information

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

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

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

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

Traffic Log

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

- UserGate node where the event occurred
- Event time
- User
- Action
- Rule
- Application
- Protocol
- Source zone
- Source address
- Source port
- IP dest
- Destination port

- NAT source IP (in case of a NAT rule)
- NAT source port (in case of a NAT rule)
- NAT destination IP (in case of a NAT rule)
- NAT destination port (in case of a NAT rule)
- Bytes sent/received
- Packets.

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

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

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

IDPS Log

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

- PCAP files
- NGFW node where the event occurred
- Time
- Event details
- User
- Action
- Rule
- Signatures
- Application
- Network protocol

- Source zone
- Source IP address
- Source port
- Source MAC address
- Destination zone
- Destination IP address
- Destination port
- Destination MAC address

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

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

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

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

SCADA Log

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

- NGFW node where the event occurred
- Time
- Action
- Rule
- Source zone
- Source IP address
- Destination IP address

- Destination port
- SCADA protocol.
- SCADA command
- 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.

SSH inspection log

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

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

- Destination IP address
- Destination port

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

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

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

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

Search History

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

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

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

Endpoint Log

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

Mail Security Log

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

- UserGate node where the event occurred
- Time triggered
- User
- Sender
- Recipient
- Rule
- Source zone
- Source IP address
- Source port
- Destination zone
- Destination IP address
- Destination port
- Application
- Application layer protocol
- Bytes sent/received
- Packets sent/received

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

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

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

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

UserID Log

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

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

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.

Name	Description
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.)
Log file	Windows log file.

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	<p>Select the log files to export:</p> <ul style="list-style-type: none"> • DNS • Events • Web access • IDPS • SCADA • SSH inspection • Traffic • Endpoint events • Endpoint rules • Endpoint applications • Endpoint hardware. <p>For each log, you can specify the export syntax:</p> <ul style="list-style-type: none"> • CEF: Common Event Format (ArcSight) • JSON: JSON format • @CEE: JSON: CEE Log Syntax (CLS) Encoding JSON <p>To select the desired log export format, refer to the documentation for the SIEM system you are using.</p> <p>For a detailed description of log formats, see Appendix 2. Description of Log Formats.</p>

Name	Description
Server type	SSH (SFTP), FTP, Syslog.
Server address	IP address or domain name of the server.
Transport	TCP or UDP; applicable only to Syslog servers.
Port	The server port to which the data should be sent.
Protocol	RFC5424 or BSD syslog RFC 3164; applicable only to Syslog servers. Select the protocol compatible with your SIEM system.
Severity	<p>Only for Syslog server type. Optional field; consult the documentation for your SIEM system. Available values:</p> <ul style="list-style-type: none"> • 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	<p>Only for Syslog server type. Optional field; consult the documentation for your SIEM system. Available values:</p> <ul style="list-style-type: none"> • 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	

Name	Description
	Only for Syslog server type. A unique host name identifying the server that sends data to the Syslog server in the FQDN (Fully Qualified Domain Name) format.
App-Name	Only for Syslog server type. Unique name of the application that sends data to the Syslog server.
Login name	The account name for connecting to the remote server. Not applicable to the Syslog export method.
Password	Account password for connecting to the remote server. Not applicable to the Syslog export method.
Repeat password	Confirm the account password for connecting to the remote server. Not applicable to the Syslog export method.
Directory path	Server directory to copy log files to. Not applicable to the Syslog export method.
Schedule	<p>Select schedule for sending logs. Not applicable to the Syslog export method. The available options are:</p> <ul style="list-style-type: none"> • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. <p>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:</p> <ul style="list-style-type: none"> • 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, <i>ip=172.16.31.1</i> 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, <i>ip!=172.16.31</i> 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: <i>date <= '2019-03-28T20:59:59' AND statusCode=303</i> .
>=	

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

Name	Description
	<p>details NOT MATCH "\"module\": \"threats\""</p> <p>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.</p>

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.

REPORTS

General information

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

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

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

Note

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

Templates

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

Here is the list of report templates by category:

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

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

Custom Report Templates

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

Name	Description
Name	The name of the custom report template.
Description	An optional description of the custom report template.
Category	Select the data source for the template. Available values: <ul style="list-style-type: none"> • Events • Traffic • Web access • IDPS • SSH inspection • Triggered alerts • Endpoint events • Endpoint rules • Endpoint applications
Filter query	An SQL-like query string that allows you to limit the amount of information used to generate a report based on this template. To construct a query, use field names and values, keywords, and operators. The data fields can be the columns listed below in the Columns field. For keywords and operators with examples of their use, see the Data Search and Filtering section.
Sort by	Specify the data field to sort the data by. The sorting can be in the ascending or descending order.
Group by	Specify the data field to group the data by.
Columns	The list of columns available for the specific data source.

Name	Description
Selected	The list of columns selected for display in the report.

Report Rules

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

Name	Description
Enabled	Enable or disable the report.
Name	The name of the rule.
Description	Optional field for rule description.
Report language	Language to use in the report.
Time range	Time range for preparation of the report.
Report format	Format (PDF, HTML, XML, CSV) of the report. Important! Creating reports in PDF results in a high load on the processor and memory. The larger the report, the higher the load. Do not use the PDF format for custom report templates. The Detailed list of all visited URLs and Detailed list of all visited sites reports use CSV format, regardless of the format you select.
Number of records	Set a limit on the number of records displayed in reports that have a limit on the number of top records, for example, the top 20 users who encountered errors authenticating in the web console.
Group by limit (if applicable)	Set a limit on the number of records displayed in reports that have a limit on the number of grouped records, for example, the top 10 users by category: a maximum of 10 users will be listed for each category. This restriction applies only to report templates that contain grouping.
Users	Specify users or user groups for which the report will be created. If not specified, the report will be created for all users.
Templates	List of templates used to build the report. You need to add at least one template.

Name	Description
<p>Schedule</p>	<p>Select a schedule to generate reports. The available options are:</p> <ul style="list-style-type: none"> • Daily • Weekly • Monthly • Every ... hours • Every ... minutes • Advanced. <p>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:</p> <ul style="list-style-type: none"> • 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".
<p>Delivery</p>	<p>You can optionally send reports to recipients via the SMTP protocol. To do this, specify the following:</p> <ul style="list-style-type: none"> • 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.



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.

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	<ul style="list-style-type: none"> • Show items per page: number of lines to display in one dialog box, such as a list of firewall rules. • Night mode: set the dark theme for the UGOS GUI. • Favorite filters: rename or delete filters for various logs created by this user.
Logout	End the session in the web console of the device.

FAVORITES

Favorites (Description)

The web interface allows you to filter the displayed sections by adding them to favorites and search for sections by their name. You can use filtering to hide unused sections. Displaying only the favorite sections does not affect the device functionality or configuration. To add a section to favorites, click the asterisk next to the section name. To customize the display, use the **Favorites Only** switch at the bottom of the panel.

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)	<p>Remote access to a technical support server.</p> <p>Access to servers:</p> <ul style="list-style-type: none"> • 93.91.17 1.46; • 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 authentication server)	User authentication via the RADIUS protocol.
TACACS+	TCP	49	Outbound (to a TACACS+ authentication server)	User authentication 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.

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: <ul style="list-style-type: none"> • 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@ersthetica
	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_BUILTIN_COMPOSITE", "module":"nlist_import"}

Web access log format

Field type	Field name	Description	Example value
CEF header	CEF:Version	CEF version.	CEF:0
	Device Vendor	Product vendor.	UserGate
	Device Product	Product type.	NGFW
	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@ersthetatica
	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@ntoorere aeda

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.	<pre>{ "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" }] }</pre>
	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@ersthetatica
	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@ersthetatica
	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: <ul style="list-style-type: none"> • 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@ersthetatica
	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.	<pre>{"protocol":"modbus","pdu_severity":0,"pdu_func":"3","pdu_address":0,"mb_value":0,"mb_quantity":</pre>

Field type	Field name	Description	Example value
			0,"mb_payload":"A AIAAA==", "mb_message":"res ponse","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@ersthetatica
	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: <ul style="list-style-type: none"> • 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@einersonstal

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: <ul style="list-style-type: none"> • 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_STAT E_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: <ul style="list-style-type: none"> • 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_applications
	Name	Source type.	log
	Threat Level	Default value.	0
CEF [extension]	rt	Time when the event was received (in milliseconds since January 1, 1970).	1652344423822
	deviceExternalId	ID of the device generated this event.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Action (application start or stop).	start, stop
	suser	User	DESKTOP-0731NFQ\User
	filePath	Path to the file.	C:\\Windows\\system32\\cmd.exe
	cs1Label	Specifies the endpoint device ID.	endpointId
	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
	spid	Process ID.	3860
	fileHash	The application hash.	B4979A9F970029889713D756C3F123643DDE73DA

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@ntoorere aeda
	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-1-5-21-379587013 3-5220325-2125745 684-1103 Account Name: user1 Account Domain: DEP Logon ID: 0xA57A446 Event in sequence: 1 of 1 Group Membership: % {S-1-5-21-37958701 33-5220325-21257 45684-513} % {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
			<p>{S-1-5-2} % {S-1-5-11} % {S-1-5-15} % {S-1-5-21-37958701 33-5220325-21257 45684-512} % {S-1-5-21-37958701 33-5220325-21257 45684-572} % {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</p>

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-1-5-21-37958701 33-5220325-21257 45684-512}\\r\\n\\ \\t\\t% {S-1-5-21-37958701 33-5220325-21257 45684-572}\\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@ntoorere aeda
	msg	The event description.	[3603:3603:1128/17 5000.938565: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.de sktop

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@ntoorere aeda
	act	Action taken by the device according to the configured policies.	login
	reason	The reason why the event was created.	{"user_groups_sids": ["S-1-5-21-3795870 133-5220325-21257

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
		<code>{"timezone":"Asia/Dubai"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}</code>
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: <ul style="list-style-type: none"> • 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_rcv	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_rcv	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

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
proto		Level 4 protocol used.	UDP
data		Indicates the data being transmitted.	<pre>{"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"}]}</pre>
reasons		The reason why the event was created, e.g. the URL category on which the rule was triggered.	<pre>{"url_cats": [{"id": 37, "name": "Search Engines & Portals", "threat_level": 1}]}</pre>
url_cat egories	id	ID of the triggered URL category.	37
	threat_level	Threat level of the triggered category.	Available values: <ul style="list-style-type: none"> • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	name	Name of the triggered category.	Search Engines & Portals
source	zone	guid	Unique ID of the traffic source zone. d0038912-0d8a-4583-a525-e63950b1da47
		name	Traffic source zone name. Trusted

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

Traffic log description

Field name		Description	Example value
timestamp		Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
bytes_sent		Number of bytes transmitted from the source to the destination.	100
node		The unique name of the device that generated the event.	utmcore@ersthetatica
packets_rcv		Number of packets transmitted from the destination to the source.	1
proto		Level 4 protocol used.	TCP or UDP
packets_sent		Number of packets transmitted from the source to the destination.	1
action		Action taken by the device according to the configured policies.	accept
session		Session ID.	a7a3cd49-8232-4f1a-962a-3659af89e96f (if System: 00000000-0000-0000-0000-000000000000)
bytes_rcv		Number of bytes transmitted from the destination to the source.	6
signatures	id	ID of the triggered signature.	999999
	threat_level	Threat level of the triggered signature.	Available values: <ul style="list-style-type: none"> • 1: very low • 2: low • 3: medium • 4: high • 5: very high

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: <ul style="list-style-type: none"> • 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).	
		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)

Field name		Description	Example value
packets_sent		Number of packets transmitted from the source to the destination.	1
packets_recv		Number of packets transmitted from the destination to the source.	1
node		The unique name of the device that generated the event.	utmcore@ersthetatica
proto		Level 4 protocol used.	TCP or UDP
bytes_sent		Number of bytes transmitted from the source to the destination.	100
bytes_recv		Number of bytes transmitted from the destination to the source.	6
action		Action taken by the device according to the configured policies.	accept
application	id	Application ID.	195
	threat_level	Application threat level.	Available values: <ul style="list-style-type: none"> • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	name	Application name.	Youtube
user	guid	Unique ID of the user. If the user type is Unknown then the ID: 00000000-0000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name	The username.	Admin

Field name		Description	Example value
	groups	guid	Unique ID of the group the user is a member of.
		name	Name of the group the user is a member of.
rule	guid	Unique ID of the rule triggered to cause the event.	919878b2-e882-49ed-3331-8ec72c3c79cb
	name	Name of the rule triggered to cause the event.	Default Group
signature	id	ID of the triggered signature.	999999
	threat_level	Threat level of the triggered signature.	Available values: <ul style="list-style-type: none"> • 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.
		name	Traffic source zone name.
	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.
		name	Traffic destination zone name.
	country	Destination country name.	Untrusted

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

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

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_PRODUC T_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

Field name	Description	Example value	
url_categories	id	ID of the category to which the URL belongs.	39
	threat level	Threat level for the URL category.	Available values: <ul style="list-style-type: none"> • 1: very low • 2: low • 3: medium • 4: high • 5: very high
	name	Name of the category to which the URL belongs.	Social Networking
timestamp	Time when the event was received. Format: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z	
endpoint_name	Endpoint device name.	DESKTOP-0731NFQ	
endpoint_id	The endpoint device ID.	35fb5820-74db-4eac-b05b-d01bc284c4e8	
media_type	The type of the content.	application/json	
ip_protocol	Number of the network protocol used.	4	

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

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	Name of the endpoint that is the source of the event (UserGate client, WMI sensor, etc.).	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\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
		<p> \t\t\t\r\n\t\t% {S-1-5-21-3795870133-522032 5-2125745684-513}\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-1-5-21-3795870133-522032 5-2125745684-512}\r\n\t\t% {S-1-5-21-3795870133-522032 5-2125745684-572}\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. </p>
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.	<pre>['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}']</pre>
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 RFC 5424 .	4
computer_name		The name of the device where the event occurred.	node1
app_name		Application triggering the event.	org.gnome.Shell.desktop
process_id		PID of the process triggering the event.	3036
data		The event description.	[3603:3603:1130/125201.838651:ERROR:CONSOLE(6)] \"console.assert\", source: devtools://devtools/bundled/ devtools-frontend/front_end/ panels/console/console.js (6)
rule	guid	Unique ID of the rule triggered to cause the event.	16535060-5a1a-4e92-8331-239406ec34da
	name	Name of the rule triggered to cause the event.	Example - Allow user-level messages

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.

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