SECURITY code

Continent Enterprise Firewall
Version 4

Monitoring and Audit

Administrator guide

Mailing address:	**115230, Russian Federation, Moscow, 1st Nagatinsky proezd 10/1**
Phone:	**+7 (495) 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**www.securitycode.ru**

Table of contents

List of abbreviations

CPU	Central processing unit
CRL	Certificate Revocation List
IPS	Intrusion Prevention System
LLDP	Link Layer Discovery Protocol
RAM	Random Access Memory
RDP	Remote Desktop Protocol
SNMP	Simple Network Management Protocol
TLVS	Tag-Length Values

Introduction

This manual is designed for administrators of Continent Enterprise Firewall, Version 4 (hereinafter — Continent). It contains information about how to work with the Monitoring and Audit system.

This manual contains links to documents [**1**] – [**6**].

Website. Information about SECURITY CODE LLC products can be found on https://www.securitycode.ru.

Technical support. You can contact technical support by phone: +7 800 505 30 20 or by email: support@securitycode.ru.

Training. You can learn more about hardware and software products of SECURITY CODE LLC in authorized education centers. The list of the centers and information about the learning environment can be found on https://www.securitycode.ru/company/education/training-courses/.

You can contact a company's representative for more information about trainings by email: education@securitycode.ru.

Version 4.1.9 — Released on May 22nd, 2024.

Chapter 1
Overview

Purpose and main functions

The Monitoring and Audit system of Continent is software that performs the monitoring of the Security Gateway parameters. Its functions allow you to:

- register and perform an audit of security, management and system events;
- monitor Security Gateways state centrally.

Events of Security Gateway operation are registered in the Security Gateway logs and are sent to the Security Management Server. In Continent, you can use three log types: system log, network security log and management log. Each log allows you to search and filter log entries. The system log registers subsystem events, the network security log — events of IPS, Firewall and UA, the management log registers actions of users and administrators.

The Audit is performed by the audit administrator. The Audit allows you to:

- view logs regularly;
- configure parameters of the log storage;
- manage log contents (event records).

How monitoring works

Monitored objects

There following objects are monitored:

- Security Cluster;
- Security Gateway;
- Security Gateway group.

Groups of monitored objects

By default, all Security Gateways are shown as members of the Unsorted group, which is included in the root group of the domain.

Note.
The root group contains all Security Gateways and groups. You can create templates that affect all the Security Gateways and the groups within the structure. The root group contains a set of default monitoring rules. If necessary, you can modify the set (see p. 28).

A user that has access the Structure section (for more information, see [**3**]) can create new groups, add Security Gateways from the Unsorted group to them and move Security Gateways from one group to another.

Types and sources of displayed information

In the Monitoring and Audit system, the following data types are used:

- data;
- state;
- events.

The type and source of information are parameters used to display information about the state of monitoring objects in the system.

You can find sources for the information types in the table below:

Information type	Source
Data	Network interfaces Audit and monitoring Signature match

Information type	Source
State	Audit and monitoring
Events	Management Audit and monitoring Integrity check Access control Application control Firewall FTP Secure communications Intrusion detection Remote access Base platform VPN

Rules and templates

To display information about the object state in the system, create a monitoring rule for this object.

You can use the following types of monitoring rules:

- a Security Gateway rule — is applied to the required Security Gateway;
- a Security Cluster rule — is applied to the Security Gateways included in the cluster;
- a group rule — is applied to all the Security Gateways included in the group and its subgroups of any nesting level;
- a common rule — is applied to all the Security Gateways and Security Gateways groups.

A template is a rule or a group of rules applied to the Security Gateways or groups of Security Gateways and setting conditions for event counters reaction.

The priority of reaction depends on the rule type. The Security Gateway rule has the highest priority and precedes the cluster rule and the group rule. The common rule has the lowest priority.

Object status

Each object has its own status. You can find them in the table below:

Status	Description
Critical	An object has this status if an event of the critical level occurs. To change the status, you need to change the state of the parameter generated the event according to the security policy. Then, the event gets the **Closed** status
Warning	An object has this status if the event of the respective severity level occurs. An object has this status until it gets the **Closed** or **Critical** status
Info	An object has this status if the event of the information level occurs. An object has this status until the parameter state is changed

Note.
The monitoring rule generated an event defines the severity level of this event (see p. 28).

Each status has its own color:

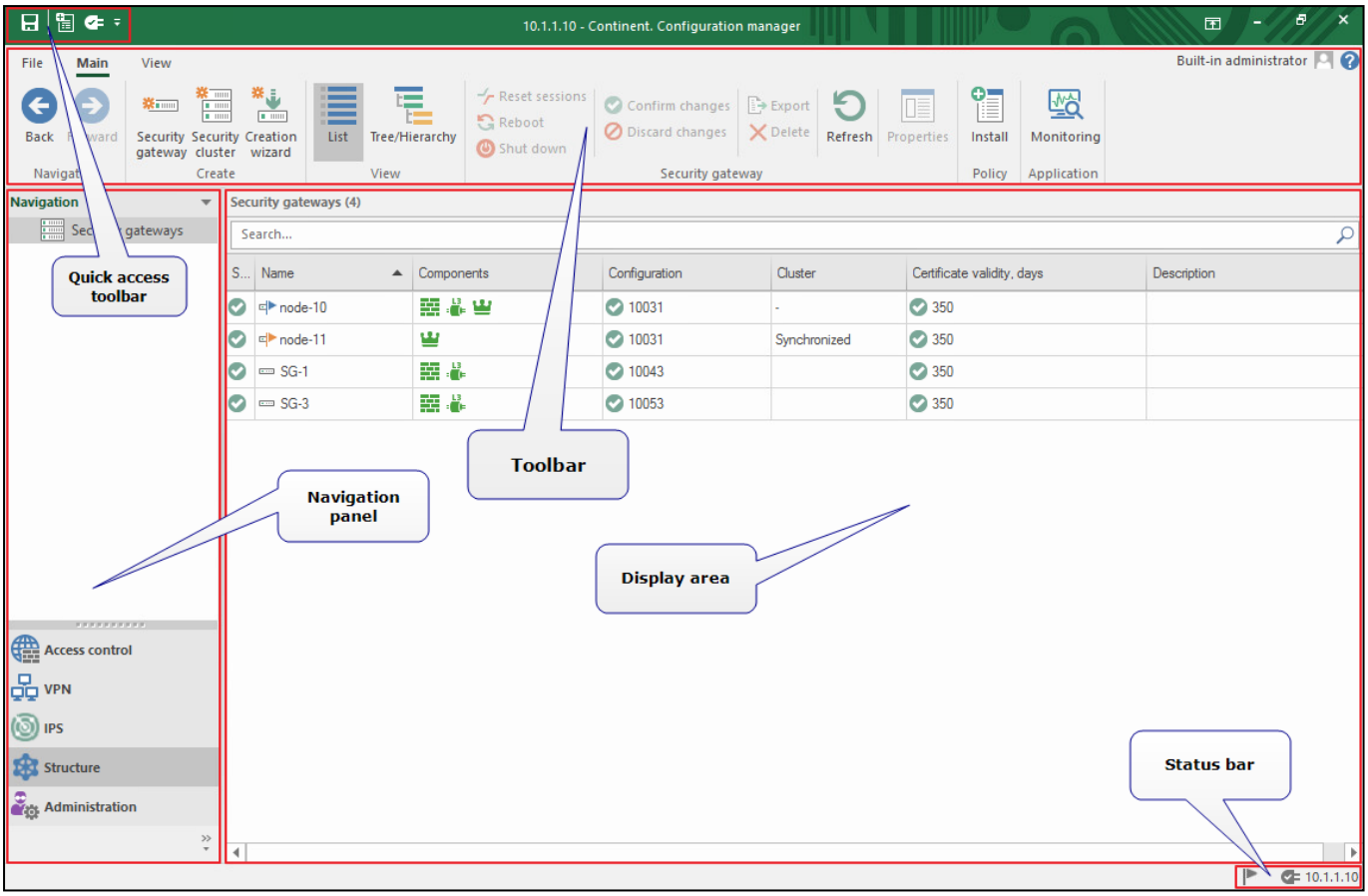
- red — critical;
- orange — warning;
- blue — info;
- green — no events with the mentioned statuses.

Run the Configuration Manager

To run the Configuration Manager:

- In the Start menu, select the **Security Code** group, then click **Configuration Manager** or double-click the **Configuration Manager** icon on the desktop.

After you run and log on to the Configuration Manager, the main window appears.



The Configuration Manager window contains the following elements:

Element of the interface	Description
Toolbar	Contains a set of tools and two tabs: • **Main** — displays the toolbar; • **View** — allows configuring the interface of the Configuration Manager. Tools are buttons that you can use to launch frequently used commands. A set of tools depends on a menu item which you can select on the navigation panel. Operating conditions determine which buttons are displayed and available. When you move the pointer over a button, a tooltip appears
Quick access toolbar	Allows quick access to the most frequently used buttons. Contains the following: • — save the current configuration; • — install a security policy; • — configure the Security Management Server connections; • — connect to the Security Management Server; • — configure Quick access toolbar; • — open Quick access toolbar
Navigation panel	Contains the following menu items: • **Access control** — to manage Firewall and NAT rules; • **VPN** — to create and configure VPN; • **IPS** — to configure IPS settings; • **Structure** — to manage Security Gateway settings; • **Administration** — to manage service functions (operations with certificates, backups, updates, licenses, etc.)
Display area	Displays information depending on the selected navigation panel menu item

Element of the interface	Description
Status bar	Contains the following: • the number of tasks currently being executed and the button to open the notification center  where you can find the link to open the general task list; • an icon that indicates the status of the connection to the Security Management Server (if there is a connection, this icon also displays a Security Management Server IP address, for example )
Authorized administrator	Displays information about the administrator account
 **About Configuration Manager**	Displays information about the program, its version and copyright

Chapter 2
Configure connection to the system

Before working with the system, establish secure data transfer between the Configuration Manager and the Security Management Server. You can establish a secure connection to the system using the following cryptographic algorithms:

- GOST R 34.11.-2012.

  You must install Continent TLS Client version 2 (hereinafter the TLS Client) in this case.
- RSA.

Configure connection using GOST R 34.11-2012

To configure connection using the TLS Client, perform the following procedures:

- Export and install security certificates and a CRL (see below).
- Install and configure the TLS Client.

  Attention!

  When installing the TLS Client, consider the following:
  - In case of using the TLS Client version 2, specify a new connection by the server certificate name used during the Security Management Server configuration (hereinafter — **monitoring_address**).
  - To ensure the compliance between the server certificate and the Security Management Server IP address, configure the DNS server or an additional **hosts** file.
- Set up a configuration file in the Configuration Manager (see p. **16**).

  During the procedure, the application launches through a secure connection by clicking **Monitoring** on the toolbar.
- System logon (see p. **17**).

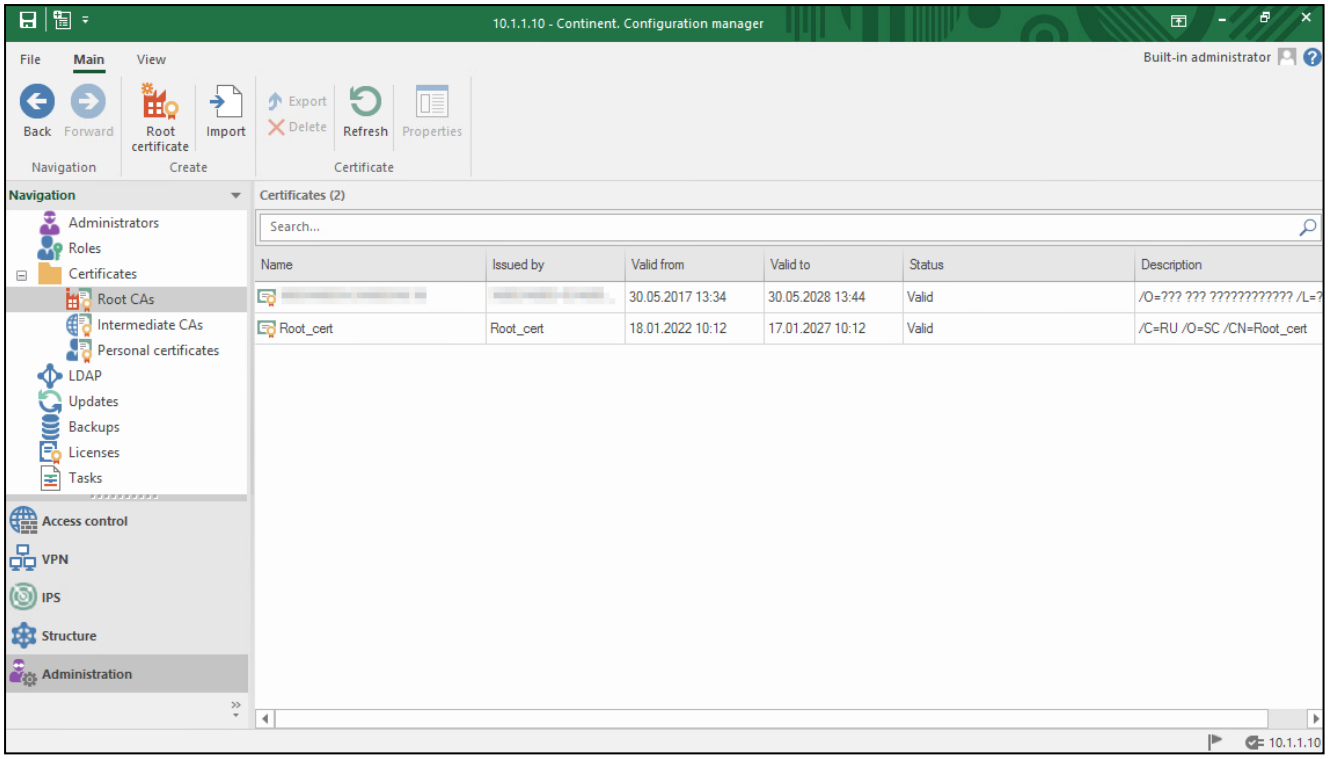
  Note.

  If a TLS Client connection error occurs, configure an additional network interface on the Security Management Server.

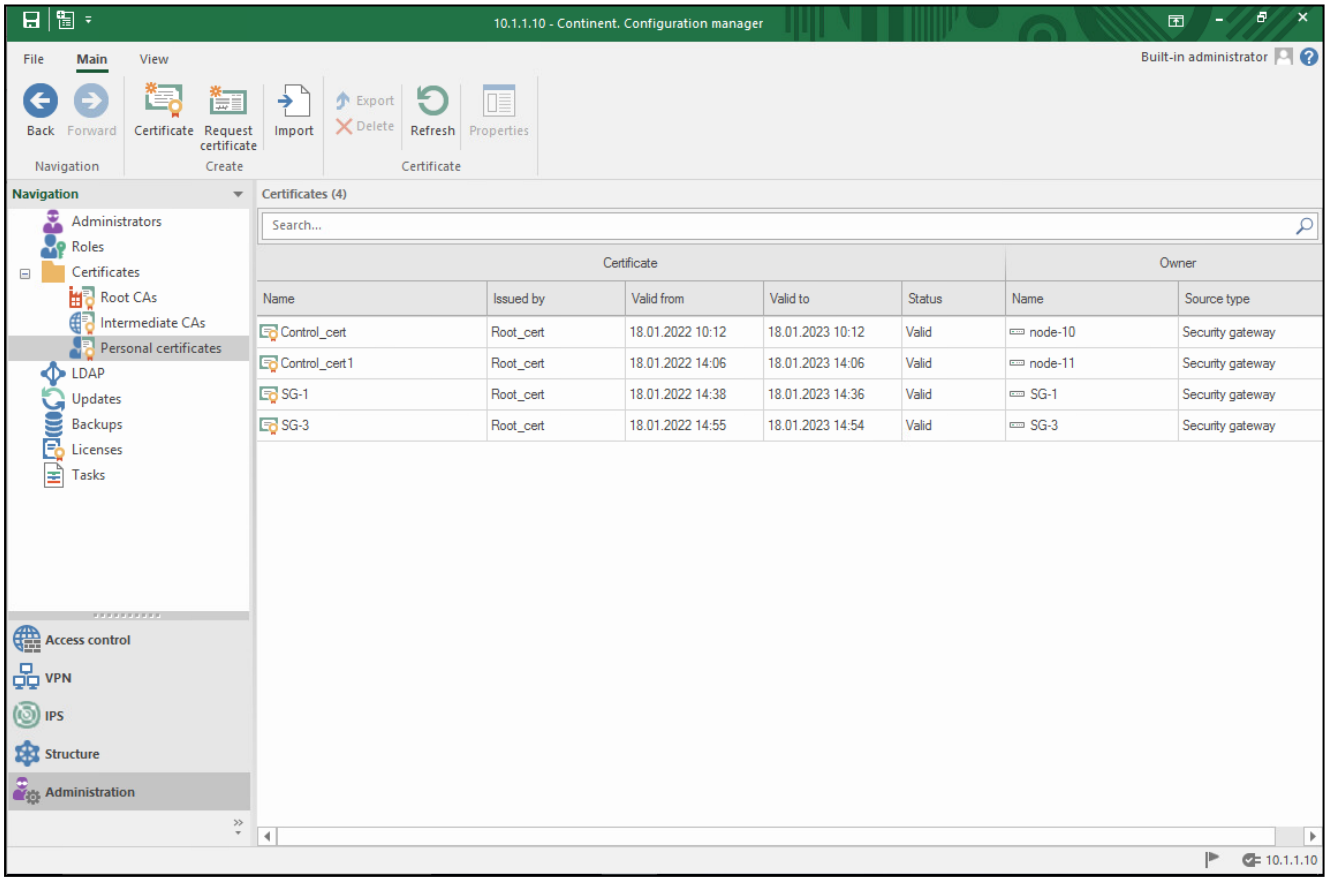
To export and install a certificate and CRL:

1. In the Configuration Manager, go to **Administration**.
2. In the list of certificates, select **Root CAs**.

   The list of installed root certificates appears on the right.



3. Right-click the active root certificate and select **Export**.
   The standard dialog box prompting you to save a file appears.
4. Select a storage to save the file, specify its name and type and click **Save**.
5. On the navigation panel, select **Personal certificates**.
   The list of installed personal certificates appears on the right.



6. Right-click the active Security Management Server certificate and select **Export**.

The standard dialog box prompting you to save a file appears.

7. Select a storage to save the file, specify its name and type and click **Save**.
8. Open the browser and download the CRL file from the **http://monitoring_address/cdc.crl** address. If the page does not open, change **monitoring_address** to the main or additional Security Management Server IP address.

Note.
If you cannot download a CRL file using the browser, then in the Security Management Server local menu, go to **Certificates | Revoked certificates | Export certificate revocation list** and specify the root certificate selected in step **3**.

9. Install the CRL file in the Windows certificate storage located on the local computer (see p. **73**).

Attention!
CRL file validity period — 1 month.

10. Install and configure the TLS Client.

Configure connection using RSA

To configure connection, take the following steps:

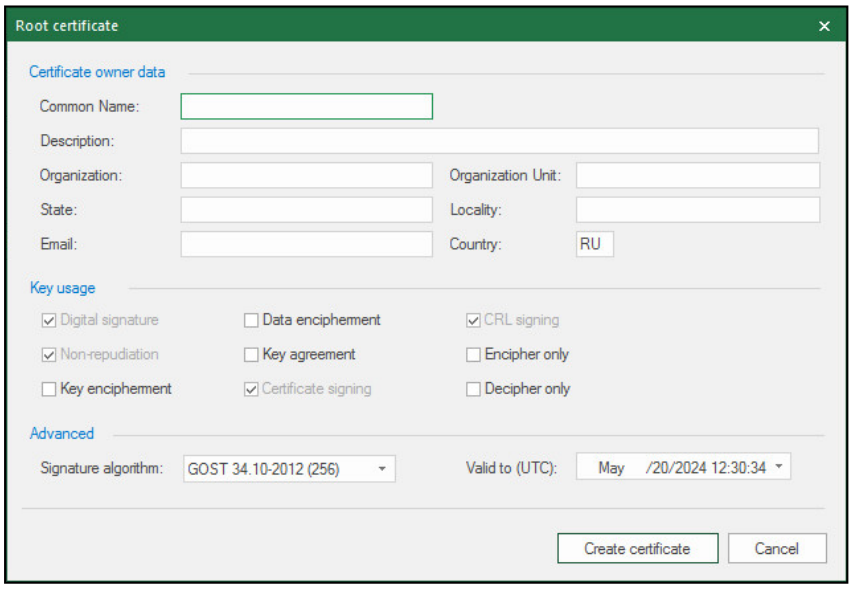
1. Issue a **Web-monitoring** certificate using the Configuration Manager (see p. **13**).
2. Set up a configuration file of the Configuration Manager (see p. **16**).
3. Run the Monitoring and Audit system (see p. **17**).

Attention!
Connection based on RSA is not protected from users with the right to access a workstation via RDP.

To issue a Web-monitoring certificate using the Configuration Manager:

1. On the navigation panel, go to **Administration** and select **Certificates**.
2. On the toolbar, click **Root certificate**.

   The **Root certificate** dialog box appears.

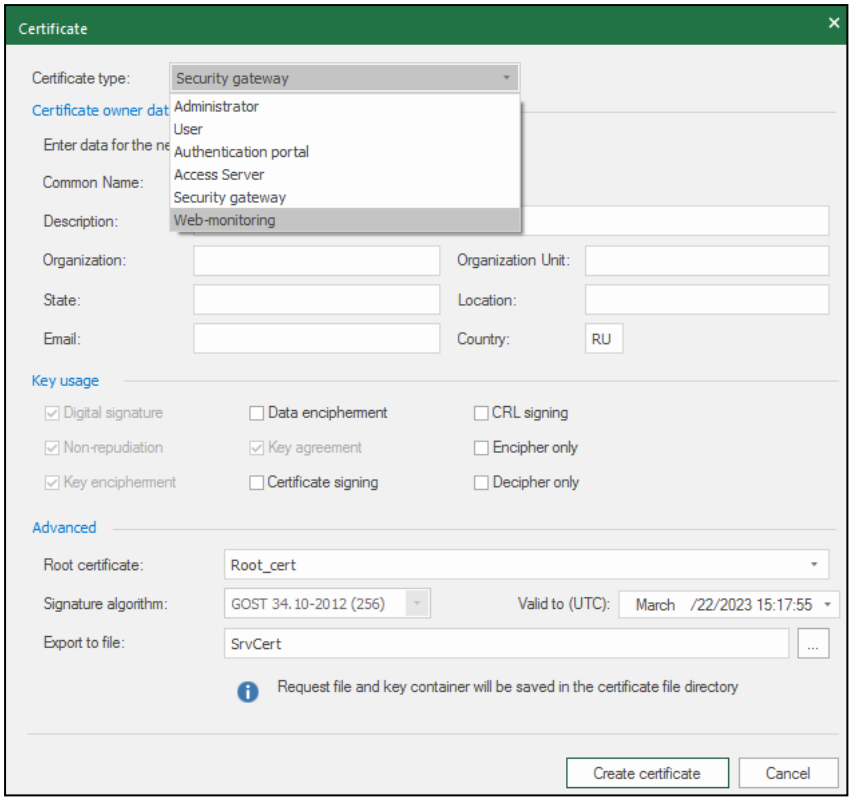


3. Specify the required information, select **RSA (2048)** as the signature algorithm and click **Create certificate**.

Note.
We recommend providing root and server certificates with names which are easy to remember.

4. On the navigation panel, click **Certificates**, then click **Personal certificates**.
5. On the toolbar, click **Certificate**.

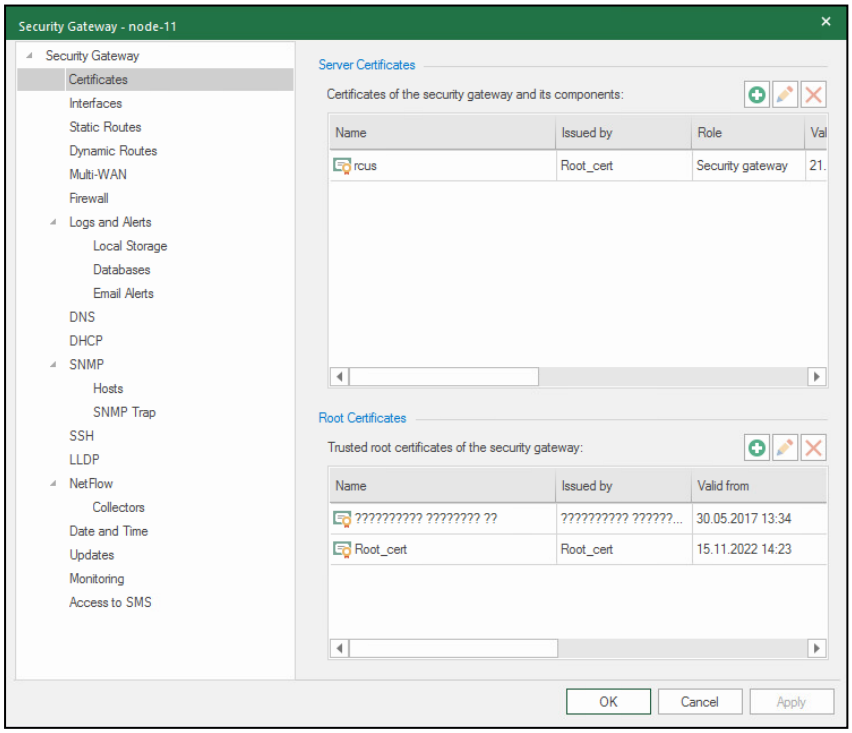
   The **Certificate** dialog box appears.



6. In the **Certificate type** drop-down list, select **Web-monitoring**. Specify all the required information and select the root certificate created in the step **3**.

Note.
The Web-monitoring certificate name must be unique.

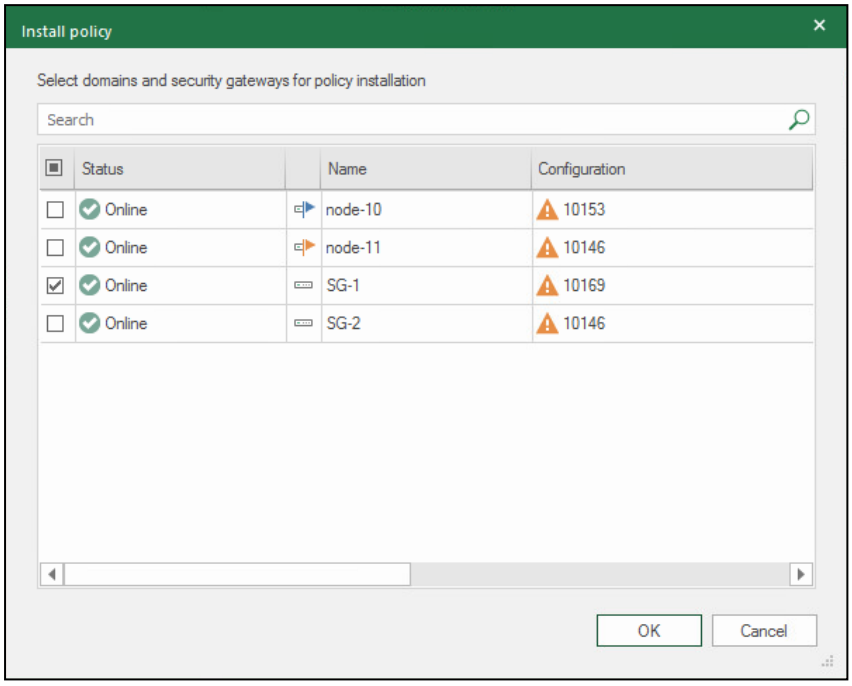
7. On the navigation panel, go to **Structure**.
8. In the display area, select the Security Gateway with the Security Management Server. On the toolbar, click **Properties**.



9. On the left, select **Certificates**.

10. In the **Server certificates** field, click to load a new certificate.
11. Click **OK**.
12. On the toolbar, click **Install**.

    The **Install policy** dialog box appears.



13. Select the required Security Gateway with the Security Management Server and click **OK**. The local changes will be sent to the Security Management Server.

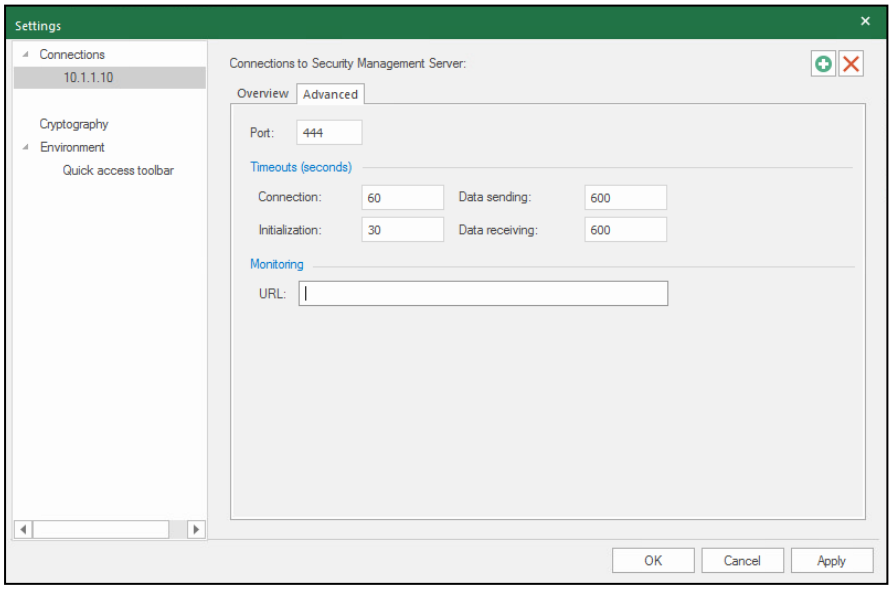
Attention!
To establish a new connection successfully, make sure the IP address of the Security Management Server corresponds to the domain name.

Set up a configuration file of the Configuration Manager

To set up a configuration file of the Configuration Manager:

1. On the quick access bar, click .

   The **Settings** dialog box appears.



2. Go to the **Advanced** tab.

3. In **Monitoring | URL**, specify a monitoring address in **https://"Web-monitoring_certificate_name** format.
4. Click **Apply** to save changes.
5. Restart the Configuration Manager to apply new configuration.

You can set up a configuration file of the Configuration Manager using the **Notepad** app if necessary.

To set up a configuration file of the Configuration Manager using Notepad:

1. Go to **C:\Users\%username%\AppData\Local\Continent\CCM** where **%username%** is the user account folder.
2. Open the **CCM.config** file using Notepad.
3. At the beginning of the file code, find **monitoring_url="monitoring_address"** (you can use the <**Ctrl**> + <**F**> to search) and enter the monitoring address.
4. In the **File** menu, click **Save**, then **Exit**.

Chapter 3
Monitoring

To configure monitoring, take the following steps:

1. Log on to the Monitoring and Audit system (see p. **17**).
2. Configure the Security Gateways, Security Gateway groups and monitoring rules in **Structure** (see p. **27**).
3. Configure the display area on **Monitoring dashboard** (see p. **19**).
4. Create a report in **Statistics** (see p. **24**).
5. Configure e-mail notifications in **Settings** (see p. **44**).
6. Configure e-mail notifications about policy installation in the Configuration Manager (see p. **47**).

Log on to the Monitoring and Audit system

To log on to the Monitoring and Audit system, use the Configuration Manager or open **https://mon-aes** where **mon-aes** is the server address.

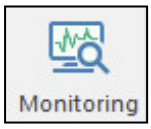
Note.
Use the Web-monitoring certificate name as a server address.

To log on to the system, use current versions of Internet browsers Yandex.Browser, Mozilla Firefox and Google Chrome.

Attention!
The system operates correctly only if you use **https**.
It is not possible to connect to the monitoring system using the administrator's certificate. Connection is possible only with the administrator login and password.

To log on to the Monitoring and Audit system:

1. In the Configuration Manager, go to **Structure**, then click **Monitoring** on the toolbar.

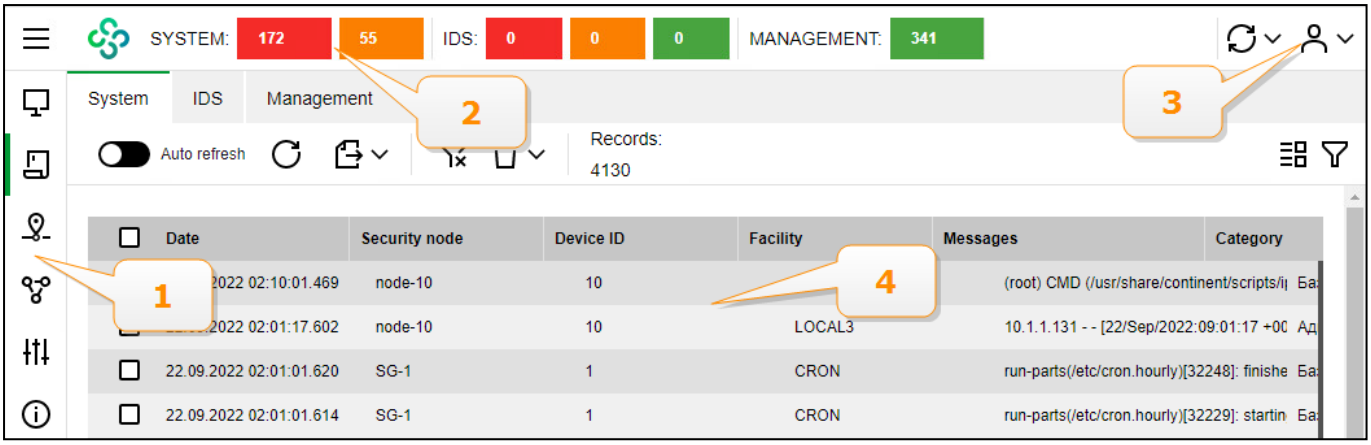
   The dialog box prompting you to enter administrator's credentials appears.
2. Enter the administrator's credentials and click **OK**.
   The main window of the Monitoring and Audit system appears.

Note.
To enter the system using the server certificate name, configure the DNS server.

Monitoring system main page

The main page contains the following elements:

1. Navigation panel.
2. Event counters.
3. **User profile** and **Reset counters** buttons.
4. Display area.

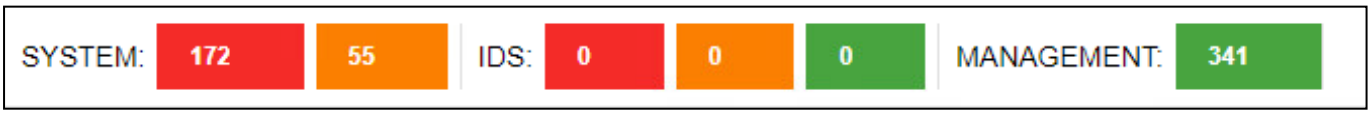


You can choose the required menu item of the Monitoring and Audit system using the navigation panel. You can find the description of the menu items in the table below:

Menu item	Description
Monitoring dashboard (see p. **19**)	Contains a set of custom widgets that display information about the state of the monitoring objects and the real-time logs
Logs (see p. **57**)	Allows you to view log records about all the Security Gateways of the controlled domain
Statistics (see p. **24**)	Allows you to create and view custom reports providing statistics for a required period of time in visual form
Structure (see p. **27**)	Allows you to: • configure the group and Security Gateways template; • control the administrator access to the monitoring of Security Gateways; • view active events on Security Gateways; • view information about the state of the software and hardware components and Security Gateways network interfaces; • view information about the persons responsible for the operation of individual Security Gateways and groups of them
Settings (see p. **44**)	Allows you to configure the server of outgoing emails SMTP, WhoIs and scheduled reports
About	Contains information about the version of Continent and contacts

An event counter displays the number of events currently registered. If you reset the event counters, they will display information about events starting from the reset moment.

Note.
Counters display information only about those Security Gateways a user can access.



- The left part displays system events. If you click one of the tiles, the system log with the severity filter will be opened.

Note.
The red tile displays the number of critical level events, the orange tile — the number of warning level events.

- The middle part displays network security events. If you click one of the tiles, the network security log with the severity filter will be opened.

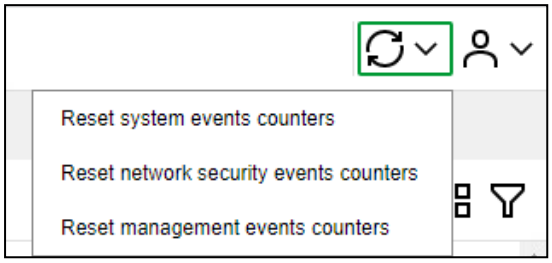
Note.
The red tile displays the number of events with the high severity level, the orange tile — events with the medium severity level, the green tile — events with the low severity level. Upon hovering the cursor over a tile, a label with the filter type appears.

- The right part displays management events. If you click the tiles, the management log with the informational filter will be opened.

Note.
The green tile displays the total number of system events.

To reset the event counters:

1. Click .
   A drop-down list appears as in the figure below.



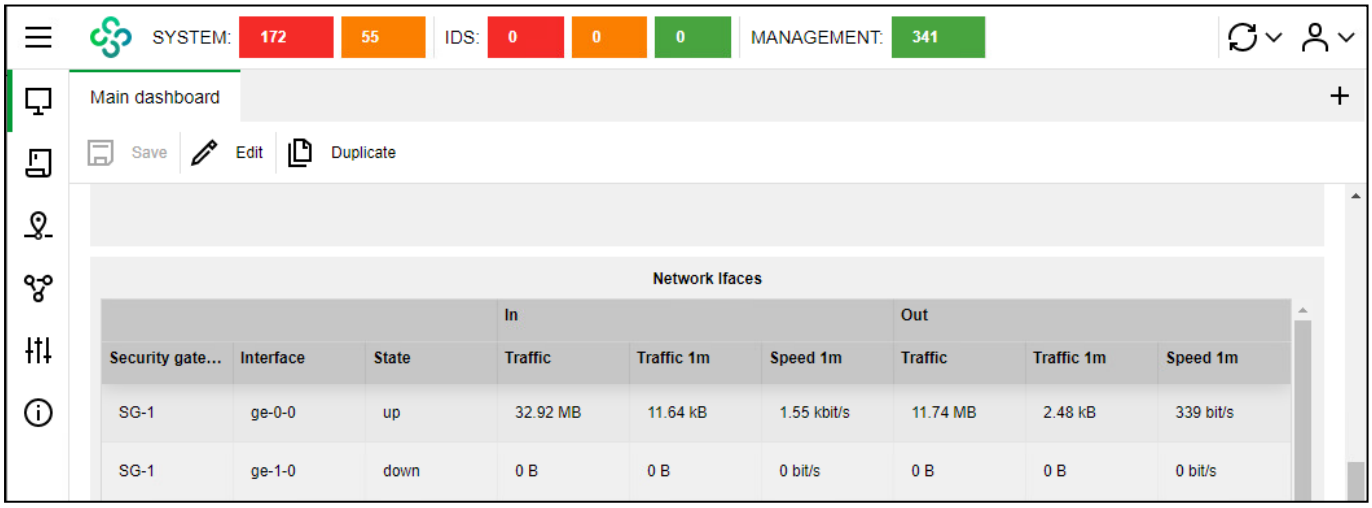
2. Select the event counters you want to reset.
3. To close the drop-down list, click .

To set up session parameters:

1. Click .
   In the drop-down list, select **Settings**.
2. The **User profile** properties sheet appears.
   The **Auto logout** option is enabled by default.
3. To change the time of inactivity before logout, select the required time period in the drop-down list.
4. Click **Save**.

Monitoring dashboard

The **Monitoring dashboard** section is a set of widgets. A widget is an element of the dashboard that displays information collected by the Monitoring and Audit system.



The monitoring dashboard displays a set of the following widgets:

- Structure;
- Access Server;
- VPN;
- Network interfaces;
- Network security log.

The monitoring dashboard displays a maximum of twelve widgets. You can use several tabs with sets of widgets.

There are the following types of widgets:

- Table;
- Graph;
- Structure.

Attention!
If the graph widgets are displayed incorrectly, refresh the page in the browser.

To add a new tab with a set of widgets:

1. In the top right corner of the **Monitoring dashboard**, click [+].
   The **Create new set of widgets** dialog box appears.
2. Specify a title of a set of widgets.
3. Click **Apply**.
   The tab appears in **Monitoring dashboard**.

To a set of widgets to a new tab:

1. Select the created tab.
   Two blank widgets are on the tab by default.

   Note.
   You can change the size of a widget window by holding and moving the bottom right corner.

2. Click **Edit**.
   The widgets become available for editing.
3. In the top right corner, click [ ] to start editing.
   To the Right of the widget, a group of parameters appears.
4. You can find the procedure for editing widgets on p. **21**.
5. Click **Save**.

Note.
To start editing the next widget, activate the link **Add widget** in the blank widget.

A set of widgets can be copied to a new tab.

To copy a set of widgets:

1. On the toolbar, click **Duplicate**.
2. In the appeared dialog box, specify a name of a new set of widgets and click **Save**.

To delete a widget, click [ ].

Table widget

The Table widget is a table with information.

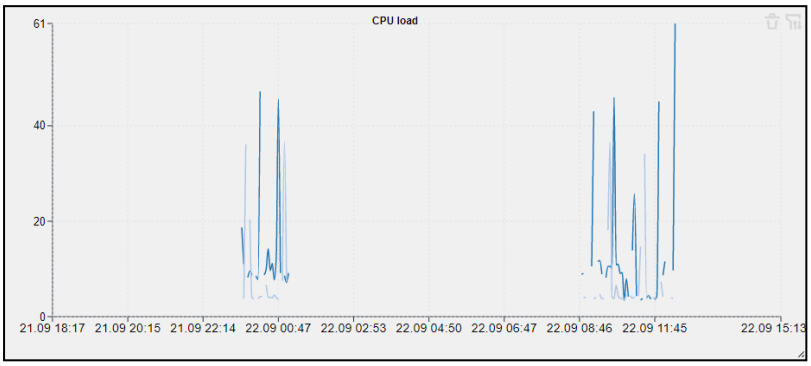
While configuring a widget, select the information type. It can be events or data. In the Monitoring and Audit System, there are the following sources of information:

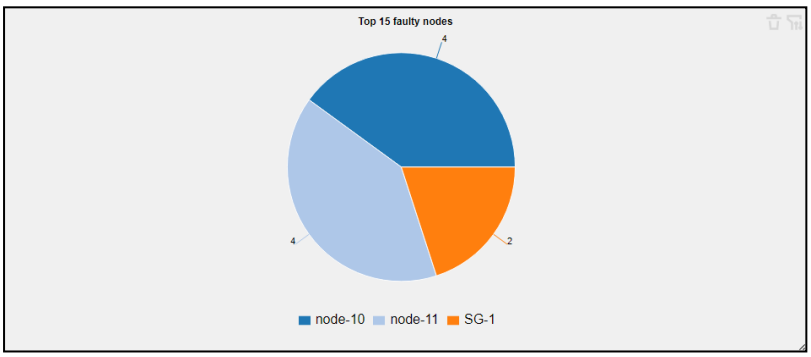
- Monitoring information;

- Domain VPN connection information;
- Domain Access Server information;
- Security Gateway network interface information.

Graph widget

The Graph widget is a graph or a pie chart.





The source of information for the widget is the data of Monitoring and Audit System.

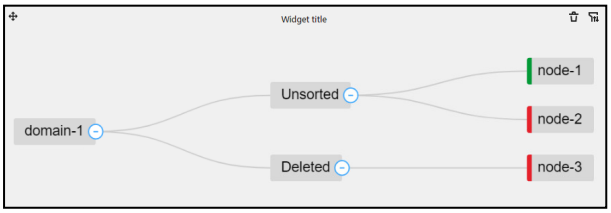
Structure widget

The **Structure** widget displays the structure of a monitoring object in the following sections:

- clusters — a list of clusters in the domain;
- groups — a list of groups in the domain;
- Security Gateways — a list of Security Gateways of the selected group.

You can configure the display of these sections.

Each section contains tiles that display the object names, the number of registered events and their severity level. The tile color indicates the maximum severity level of an event that occurred on this object or on one of the object groups.



Click the group tile to view included groups and Security Gateways. To return to higher levels of the structure, use the path at the top of the widget.

To go to the Security Gateway page, click the respective tile in **Structure**.

Configure the monitoring dashboard

Configuration of the monitoring dashboard allows you to:

- add new widgets to the dashboard;

- delete widgets from the dashboard;
- edit widgets;
- move widgets on the dashboard and change their size.

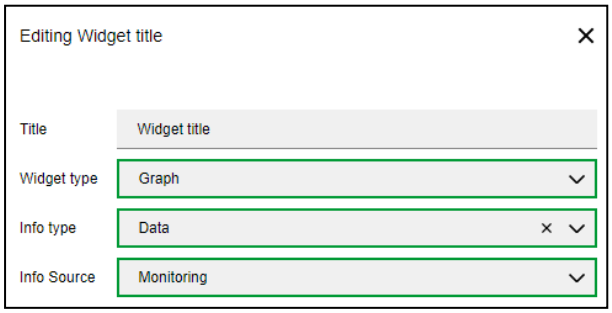
To create a new set of widgets:

1. At the top of the display area, click .
   The **Create new set of widgets** dialog box appears.

2. Enter a widget set name and click **Apply**.
   A new tab is created. The monitoring dashboard is in the **Edit** mode and you can configure a widget.

To configure a widget:

1. In the display area, click Edit.
   Now you can edit the dashboard elements.
2. To add a new widget, click on the **Add widget** tile.
   A widget template appears.
3. To configure a widget, click at the top right corner.
   The **Editing Widget title** dialog box appears.

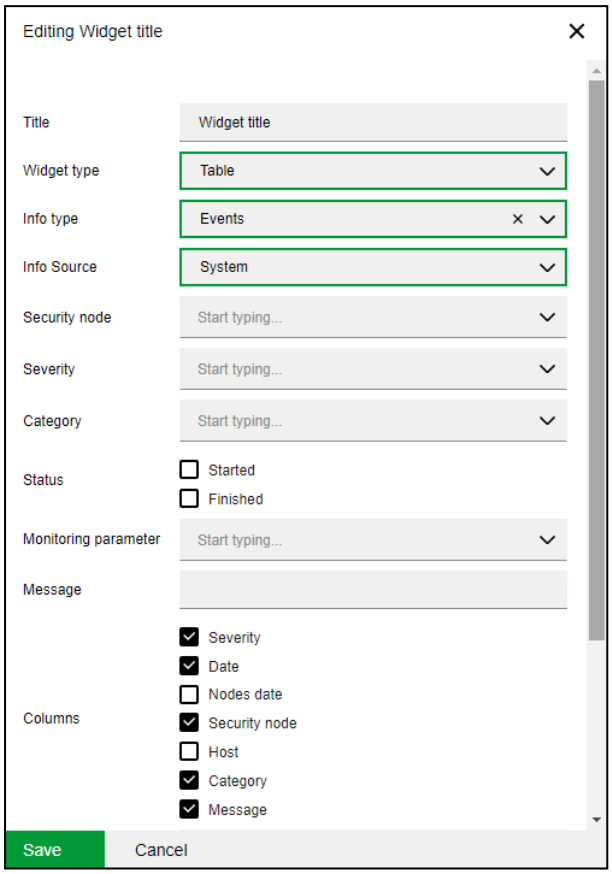


4. Enter the widget title and its type. It can be a table, a graph or a structure.

In the **Editing Widget title** dialog box, the **Info type** field appears. The following fields and steps of parameter configuration depend on the type of widget and information.

Example.

The figure below shows the fields of widget configuration when selecting the following parameters: **Widget type** — **Table**, **Info type** — **Event**, **Info Source**— **System**.



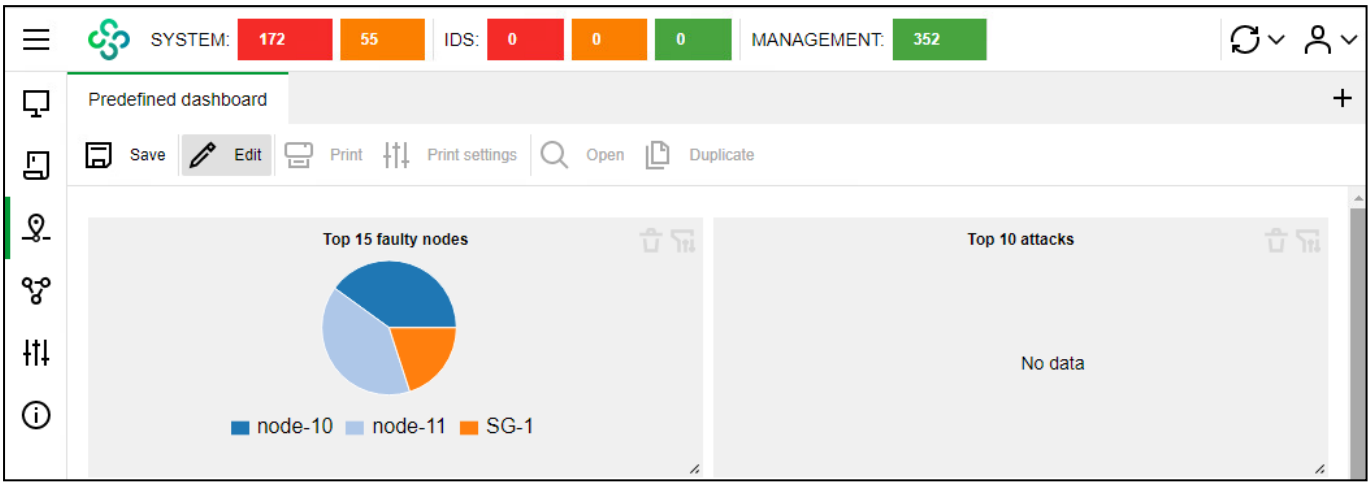
You can use the **Security Gateways/groups** filter while configuring widget parameters.

5. Configure the widget parameters and click **Apply**.

   A widget displays the values of the specified parameters.
6. To resize a widget, use in the bottom right corner.
7. To add another widget, repeat steps **3-6**.
8. To delete a widget, click in the top right corner.
9. To move a widget, select its title and drag it to an empty space of the display area.
10. To edit the widget parameters, click in the top right corner and specify the parameters in the **Settings** dialog box (see steps **5-6**).
11. To complete widget configuration, click **Save** at the bottom of the monitoring dashboard.

Statistics

In **Statistics**, you can create and view custom reports that provide statistics for a required period of time in the visual form.



Each report contains a set of table and graph widgets.

When you go to **Statistics**, the last selected report is displayed. If no reports have been created, the default report is displayed.

Attention!

Widgets included in the report are displayed in preview mode. Thus, table widget contain 1000 recent event records (40 pages, 25 lines per page) and the total number of them.

At the top of the page, you can find the buttons that allows you to:

- edit and save a widget;
- print a report;
- configure printing;
- open saved reports;
- duplicate widget sets.

Widget management

To edit widgets:

1. Click **Edit**.

   Widgets are in edit mode.
2. Take steps **3-12** (see p. **19**).

For widgets that have the parameters **Info type** — **Data**, **Info Source** — **Monitoring**, statistics sampling is performed automatically according to the table below:

Period of time	Percentage of saved data, %
24 hours	100
1-3 days	80
3-7 days	65
7-14 days	50
14 days - 1 month	35
1-6 months	15
6-12 months	5
More that 1 year	0

The following messages appear in the audit log:

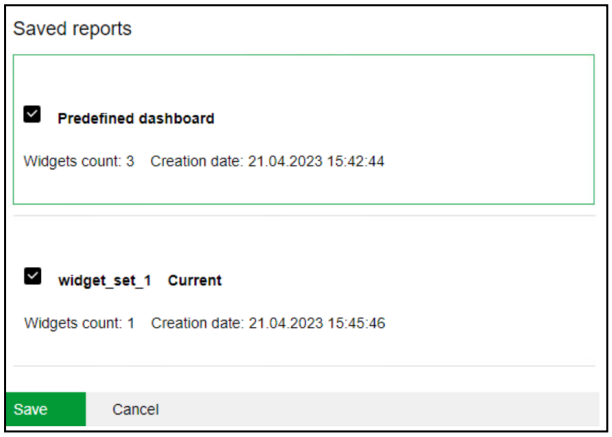
Message	Category
Administrator has opened management journal.	Audit and monitoring
Administrator has changed the profile	Audit and monitoring
Administrator has cleared network security events counters	Audit and monitoring

View reports

To view a report:

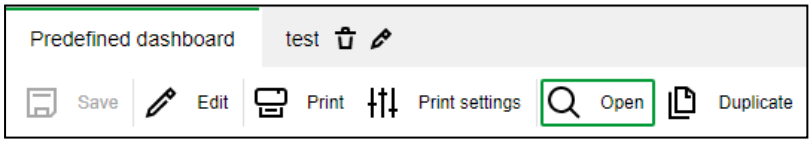
1. Click **Open**.

   The **Saved reports** dialog box with the list of reports sorted by creation time appears.



Note.
If no reports have been created, the list will contain one default report.

   To view a report, select the required check box. You can find all the selected reports in the display area. Use the tabs to navigate through them.



2. To copy a report, click Duplicate.
3. To delete a report from the display area, clear the respective check box.
4. To delete a report from Monitoring and Audit system, click .

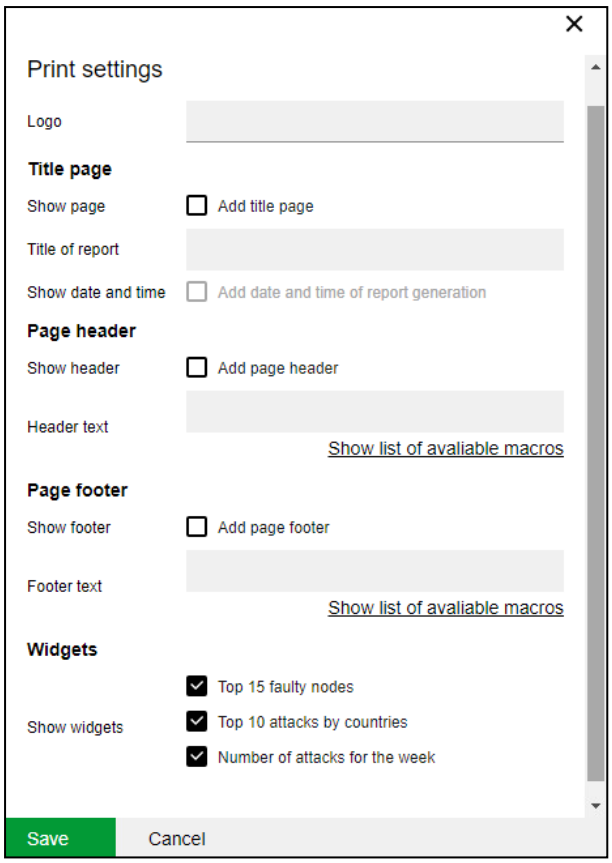
Attention!
The report list cannot be empty. If there is only one report in the list, you cannot delete it.

Prepare a report for printing

To configure report appearance:

1. Click **Print settings**.

   The **Print settings** dialog box appears.



2. To select a logo, click the **Logo** field. File Explorer dialog box appears. Select the required file. The file name appears in the **Logo** field.
3. To view the image, hover over the **Show logo** link.
4. To select another file or delete the selected file, delete its name.
5. Specify the other parameters.

> **Attention!**
> You can add headers and footers manually or using macros. To view the available macros, click the **Show list of available macros** link.

6. When printing selectively, clear the check boxes of the widgets that should not be included in the report. For table widgets you can limit a number of rows to print.
7. After configuring the report appearance, click **Save**.

To generate a report:

1. Click **Print**.

   You will receive a message that the report is being generated. When the report is generated, you will receive a message prompting you to download the PDF file.

> **Attention!**
> The report generation time is 30 minutes. If it is exceeded, we recommend reducing the number of widgets and repeat the procedure.

2. Save the PDF file and if necessary print it.

Monitoring modes

In the Monitoring and Audit system, there are two modes of data visualization: real time and for the selected period.

Monitoring for the selected period is used to collect and view reports in **Statistics** (see p. **24**). You can use this mode when the widget has the following settings:

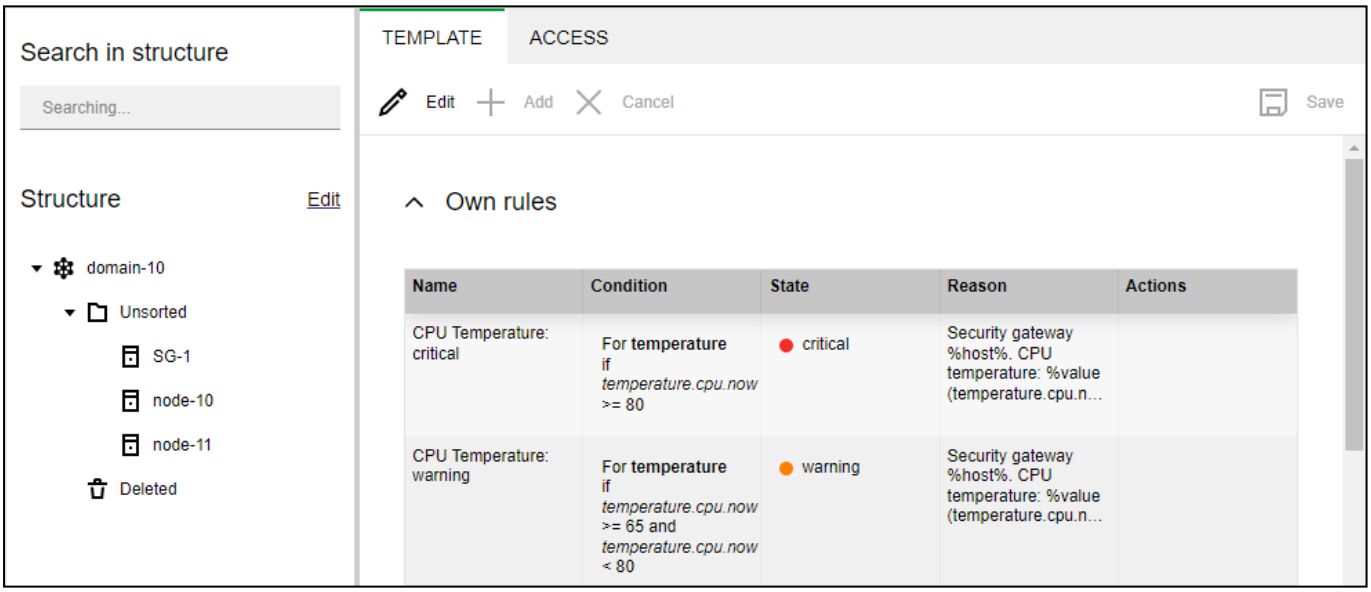
- in the **Widget type** drop-down list, select **Table**, in **Information type** — **Data**, in **Information source** — **Monitoring and Audit**;
- in the **Widget type** drop-down list, select **Graph**, in **Information type** — **Data**, in **Information source** — **Monitoring and Audit**.

The real time mode is available in **Structure** on the **State** tab of the required Security Gateway. You can also use it on the monitoring dashboard if a widget has the required settings. In this mode, parameter values are displayed in real time.

Note.
Real-time parameter values are updated every 5 seconds. We do not recommend using this mode on more than 20 Security Gateways as it is power-demanding and slows down the Monitoring and Audit system.

Structure

In **Structure**, you can view information about the status of monitoring objects and configure templates.

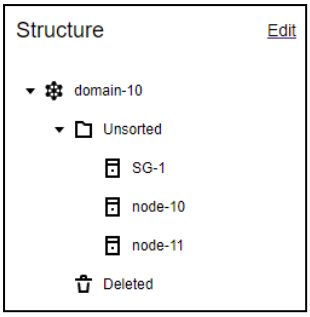


To navigate, use the object tree on the left of the page. The object tree contains the following elements:

- cluster;
- Security Gateways;
- Security Gateways groups;
- domain.

Note.
By default, **Structure** consists of two groups: **Unsorted** containing all registered Security Gateways and **Deleted** containing all Security Gateways deleted using the Configuration Manager.

To configure an element, select it in the object tree.



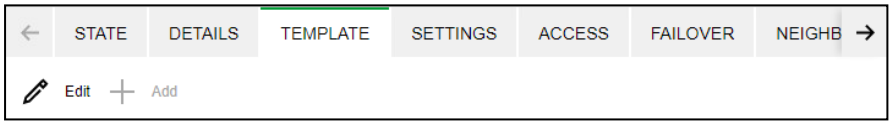
Note.
The root domain group contains all Security Gateways and groups of them. It allows you to create templates for the Security Gateways and groups of them. These groups contain a set of rules by default.

Configure monitoring rules

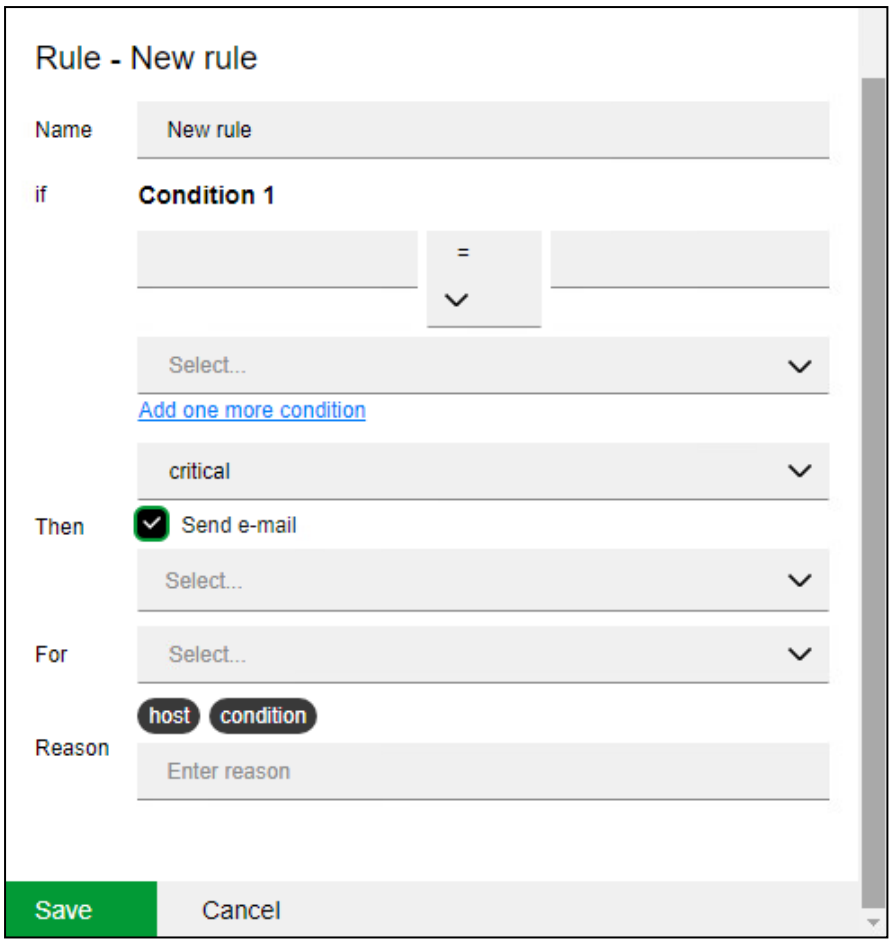
You can create, edit and delete rules.

To create a rule:

1. In the **Monitoring** section, select **Structure**.
2. In the **Structure** object tree, select the required Security Gateway or a group of them.
   A dialog box with the parameters of this object appears.



3. Select the **Rules** tab.
4. To create a rule, click **Add**.
   The **New rule** dialog box appears.



5. Specify the rule name and condition of its application. To do so, take the following steps:

- In the **Name** text box, enter the rule name.

Note.
The name should contain English uppercase and lowercase characters, base 10 digits or special characters:

(	)	[	]	_	-	*	?	!	%

- In the **If** group of text boxes, specify a system parameter, a logical condition and an operation threshold.

Note.
To select a system parameter, use the lower text box with a drop-down list.

- A rule may have several operation thresholds. To add an extra condition, click **Add**.

Note.
If you add an extra condition, the **Condition** text box appears. In the drop-down list, select an operation threshold if one or all conditions are met.

6. Specify the following parameters:

Parameter	Description
Then	A reaction to rule triggering. You can configure the event severity level and notifications
For	A subsystem to which the rule applies
Reason	A message describing an event. You can use macros for more accurate message. The following macros are supported for each of the conditions: • %host% — Security Gateway, where an event occurred; • %value% — current value of the parameter; • %condition% — text value of the condition (e.g. **>** — more than); • %threshold% — operation threshold. In the message, you can use the characters from the note (step **4**)

7. Click **Save**.

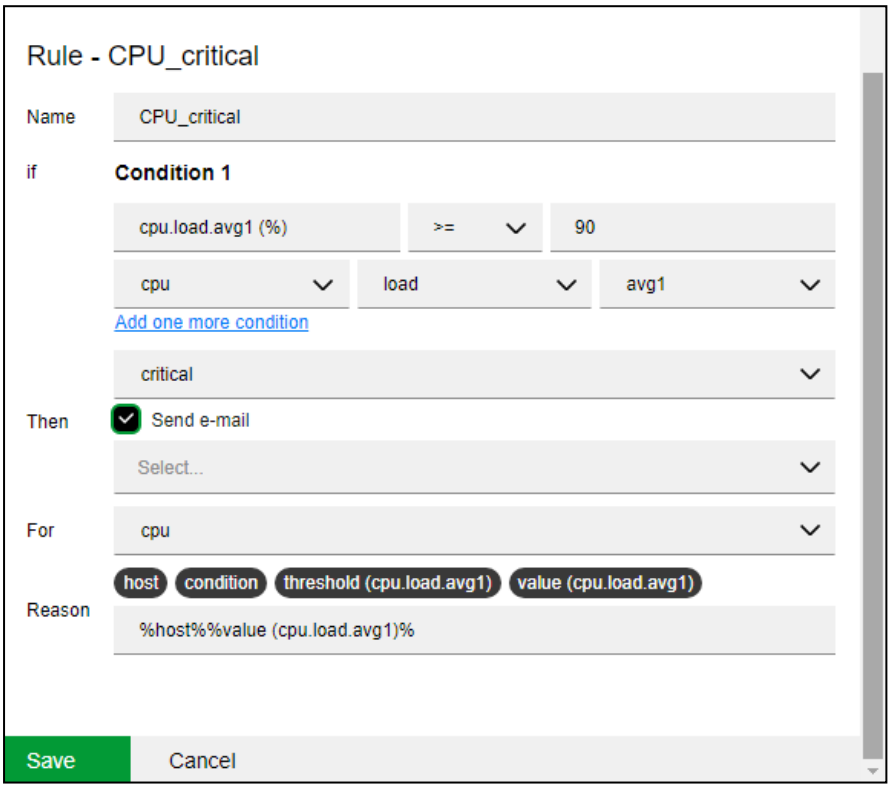
The saved rule appears in the Own rules list of the Security Gateway or a group of them.

Name	Condition	State	Reason	Actions
CPU Temperature: critical	For **temperature** if *temperature.cpu.nov* >= 80	critical	Security gateway %host%. CPU temperature: %value (temperature.cpu....	

Note.

Example of a monitoring rule:

To set the **If the average CPU load is equal or exceeds 90%, the warning event is registered** condition, specify the parameters in the following way:



Example of a message in the **Reason** text box: **If the average CPU load is equal or exceeds %threshold (cpu/load/avg1)%, the warning event is registered**.

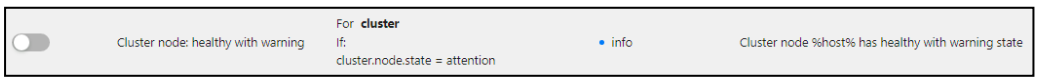
To edit a rule:

1. In the object tree, select the required Security Gateway or a group of them.
   A dialog box with the parameters of this object appears.
2. Select the **Rules** tab.
3. In the **Actions** column of the required rule, click .
4. Repeat steps **3**-**6** (see p. **28**).

You can temporarily disable a rule.

To disable a rule:

- turn off the rule toggle.



To delete a rule:

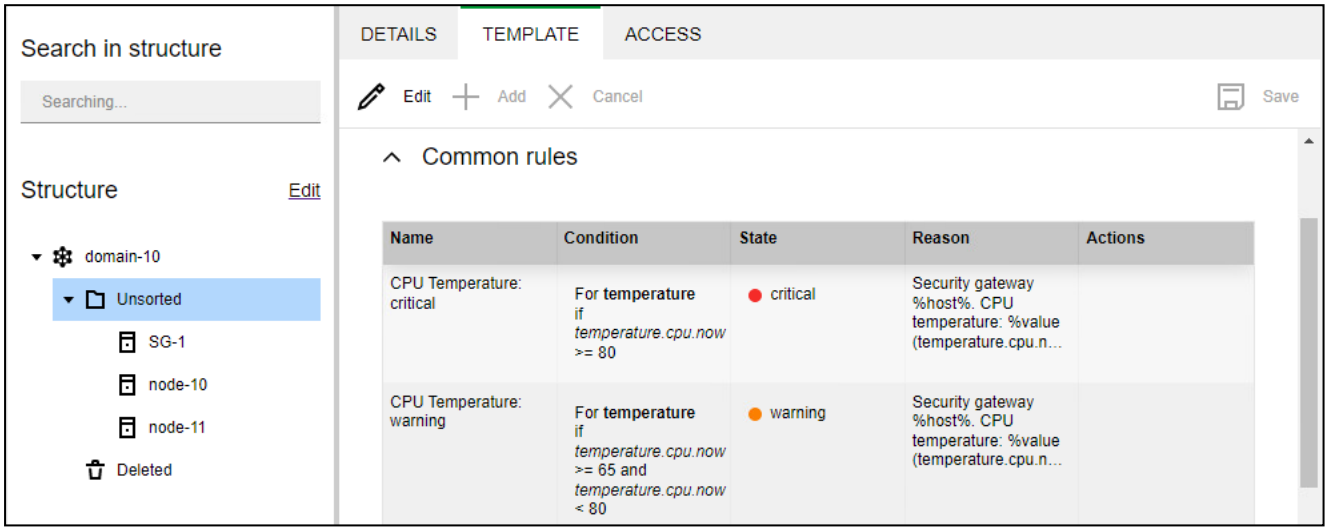
1. In the object tree, select the required Security Gateway or a group of them.
   A dialog box with the parameters of this object appears.
2. Select the **Rules** tab.

3. In the **Actions** column of the required rule, click .
4. To restore the rule, click Cancel.

To create common rules:

Note.
Common rules are applied to all Security Gateways and groups of them and have the lowest priority.

1. Go to **Structure** and select the top hierarchy level of the object tree.
   The list of common rules appears. By default, the Monitoring and Audit System has preset common rules.



2. To add a new rule, click **Add**.
   The **New rule** dialog box appears.
3. Configure the rule (see p. **28**) and save it.
   Add a new rule to the list if necessary.

Domain

The Domain page contains the following tabs:

- contacts;
- rules;
- access;
- user sessions;
- all sensors.

Contacts

The **Contacts** tab is used to configure information about people responsible for the operation of the Security Gateway group.

The procedure of configuring the **Contacts** tab parameters for the Security Gateway group is similar to the configuring the **Contacts** tab parameters for the Security Gateway. For more information, go to the Security Gateways section (see p. **32**).

Rules

The **Rules** tab is used to configure the Security Gateway monitoring rules. You can find a detailed description of the parameter configuration procedure in the Configure monitoring rules section (see p. **28**).

Access

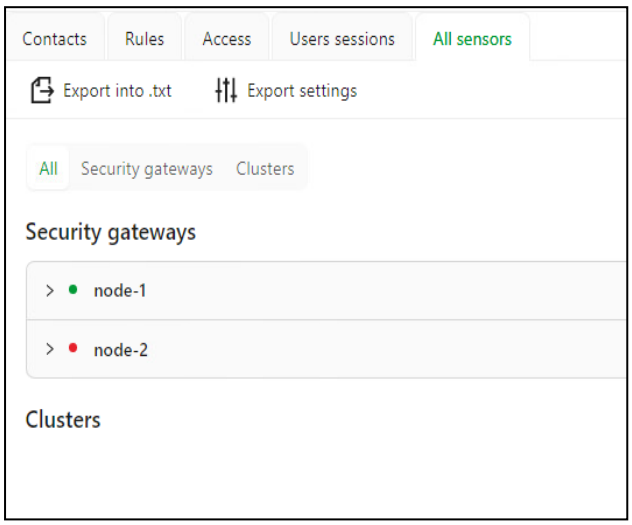
The tab is used to configure the access of system administrators to the Security Gateway monitoring in a domain. The configuration of the access to the Security Gateway is the same as the configuration of the access to the Security Gateway group (see p. **40**).

User sessions

The tab contains information about the DNS names of the Security Gateway. The information is the same as the information on the IP addresses of DNS names tab for the Security Gateway (p. 37), but it includes all the Security Gateways of a domain, regardless of groups.

All sensors

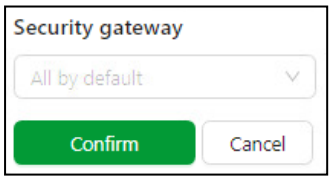
The **All sensors** tab contains a hierarchical list of all sensors for the Security Gateway and clusters, which are the data sources for widgets, rules and reports.



You can export data from sensors into a txt file. By default, data from all Security Gateways is included in the export.

To export data from sensors into a txt file:

1. Click **Export settings** on the toolbar of the **All sensors** tab.
   A window for selecting Security Gateways to include in the export opens.



2. In the drop-down list, select a Security Gateway or a Security Gateway group.
   The selected object appears in the box.
3. If you need to add another gateway or group, click the box with the selected Security Gateways and choose the new object in the drop-down list.
4. Click the **Export into .txt** button.
5. The file will be saved to the download folder specified in the browser settings.

Security Gateway

When you select a Security Gateway, there are the following tabs available:

- state;
- network state;
- contacts;
- rules;
- settings;
- access;
- neighboring network devices;
- IP/DNS;

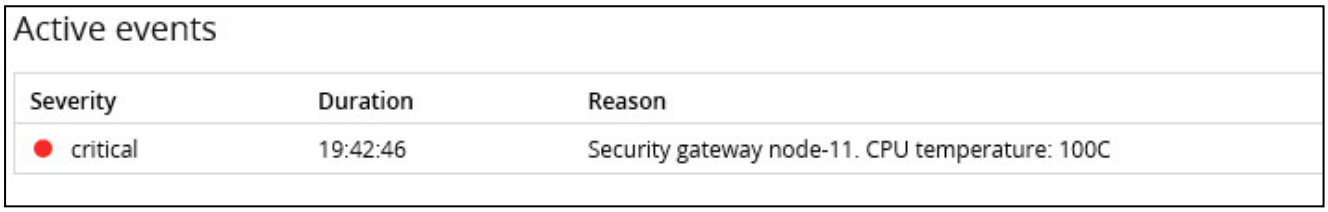
- user sessions;
- DHCP statistics;
- ARP records;
- remote command execution;
- routing;
- Web-resources;
- Web-resources statistics.

To navigate between tabs, scroll the mouse wheel. By default, not all sections are added to the list of tabs.

State

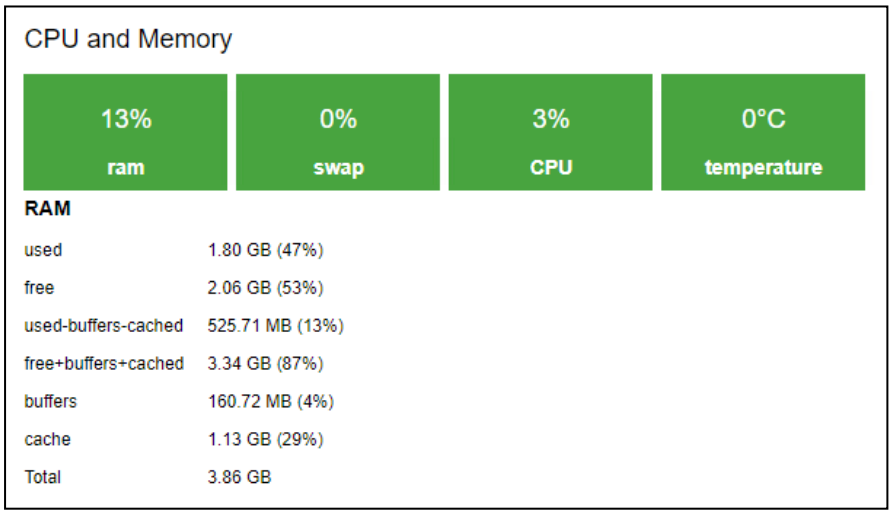
On the **State** tab, you can find the following information:

- **Active events** — the table containing the list of active events on the Security Gateways and the information about their severity level, duration and reason.

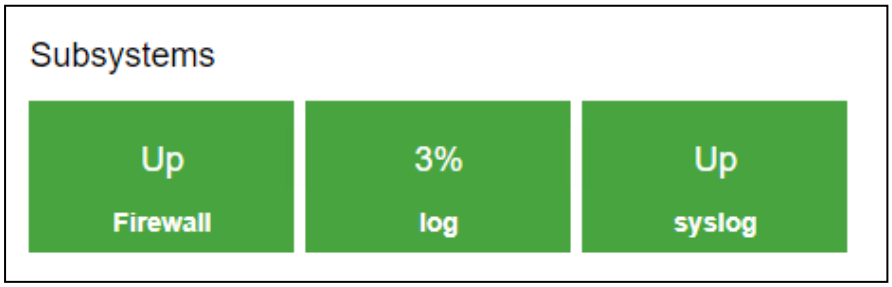


- **CPU and Memory** — information about CPU and RAM divided into subgroups of parameters:
  - RAM load;
  - SWAP use;
  - CPU load;
  - temperature of CPU, motherboard and disk subsystem.

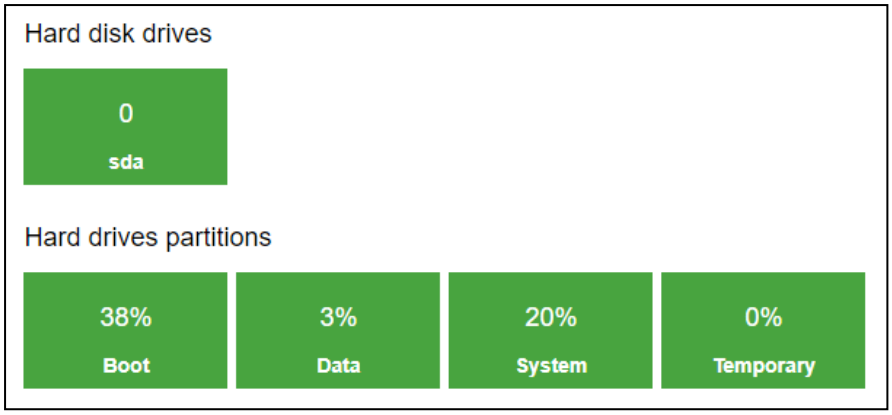
  To view parameters of each subgroup, click the respective tile.



- **Subsystems** — information about the state of IPS, Firewall, logs, VPN, a security cluster and the Access Server.



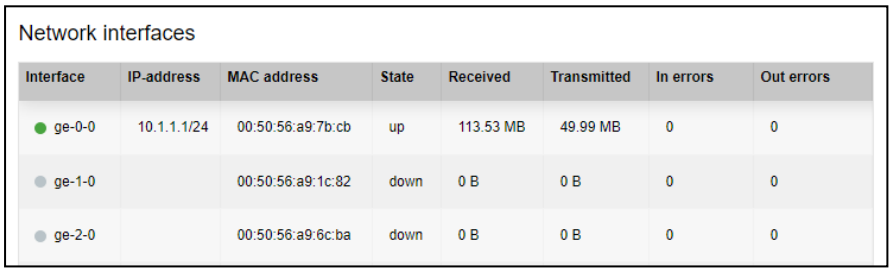
- **Hard disk drives** — information about hard drives and the state of their partitions.



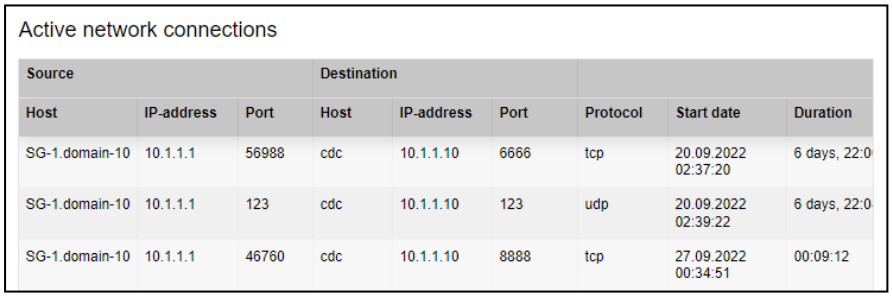
Network interfaces

On the Network interfaces tab, you can find the following information:

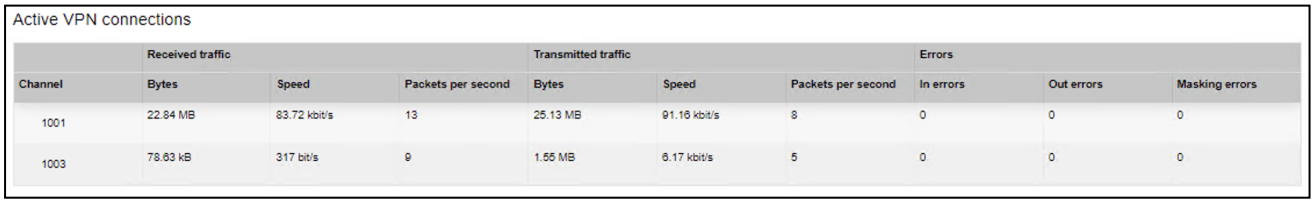
- Information about the state and statistics of network interfaces.



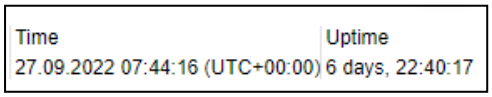
- Active network connections.



- Active VPN connections.



In the top right corner, you can find the time and the uptime of a Security Gateway.



In the top left corner, you can find the **All events** and **Generate report** buttons.

Note.
Report generation takes a long time after which will be saved to the folder according to the settings of the web browser.
Use **MonitoringReportDecoder.exe** included in the delivery set of Continent to work with reports .

Contacts

The **Contacts** tab allows you to configure and view information about the employees responsible for the Security Gateway operation:

- name;
- work phone number;
- mobile phone number;
- Skype account;
- e-mail address;

  Note.
  While creating a new monitoring rule, e-mail address is specified in the **Send email** field by default.

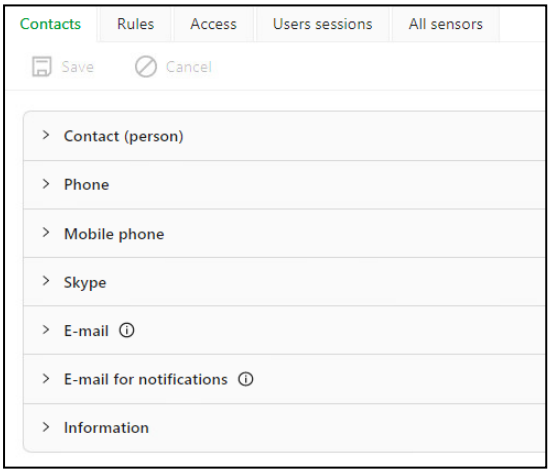
- e-mail address for notifications;

  Note.
  This e-mail address is used while creating an automatic notification about Security Gateway failure.

- information.

  Note.
  This information is displayed on the tile of the **Structure** widget on the Monitoring dashboard.

The initial form of the **Contacts** tab is shown in the figure below.



To add contact information:

1. Click the required line.
2. In the text box of the line, specify the necessary value and click **Add**.
   After you add one value, a new text box becomes available.
3. If necessary, add another value in the new text box and repeat step **2**.
4. Go to the next parameter and repeat steps **1, 2**.
5. Click **Save** to save the changes.

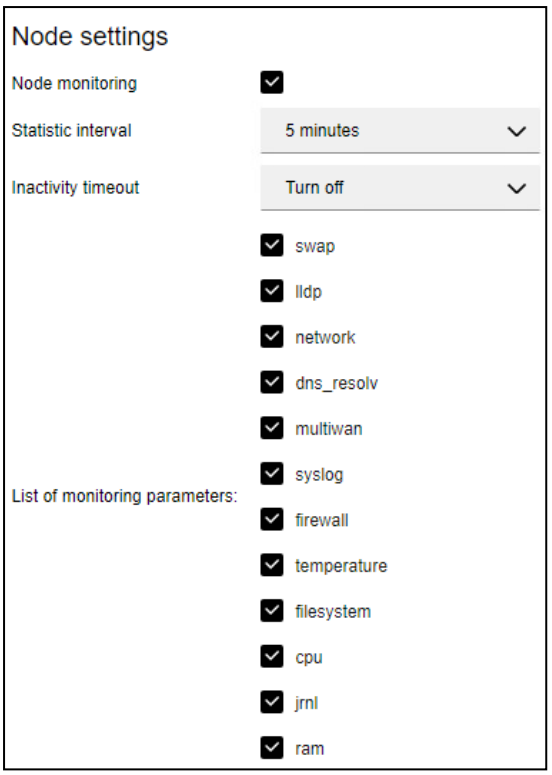
Rules

The **Template** tab allows you to configure monitoring rules of a Security Gateway. For more information about the monitoring rules configuration, see p. **28**.

Settings

The **Settings** tab allows you to select a statistics interval and Security Gateway parameters.

Security Gateways parameters are unavailable for editing by default.



To disable monitoring, click **Edit** and clear the **Node monitoring** check box. By default, Security Gateway monitoring is enabled.

Note.
After you disabled monitoring for a Security Gateway, the statistics for this Security Gateway is not saved to the database and not displayed. If SNMP is enabled in the Security Gateway settings, the system will send null values over SNMP for this Security Gateway.

To configure Security Gateway monitoring parameters:

1. In the drop-down list, select **Statistic interval**.
2. In the drop-down list, select **Inactivity timeout**.
3. To select other parameters, select the required check boxes and click **Save**.

Attention!
If you disable a parameter, statistics collection is stopped. Widgets and rules related to this parameter are disabled.

Parameter	Subgroup	Group
swap	SWAP	CPU and Memory
lldp	LLDP	Subsystems
network	Whole table	Network interfaces
dns_resolv	DNS Resolver	Subsystems
multiwan	Multi-WAN	Subsystems
syslog	SYSLOG	Subsystems
firewall	FIREWALL	Subsystems
temperature	TEMPERATURE	CPU and Memory
filesystem	SDA BOOT; DATA; SYSTEM; TEMPORARY	Hard disk drives Hard drives partitions
cpu	CPU	CPU and Memory
jrnl	Log	Subsystems
ram	RAM	CPU and Memory
as	Access Server	Subsystems

Parameter	Subgroup	Group
raid	RAID	Hard disk drives
cluster	Cluster	Subsystems
ips	IPS	Subsystems
vpn	VPN	VPN connections

Note.
When you go to the **State** tab, a slight delay may occur because of the settings update.

Access

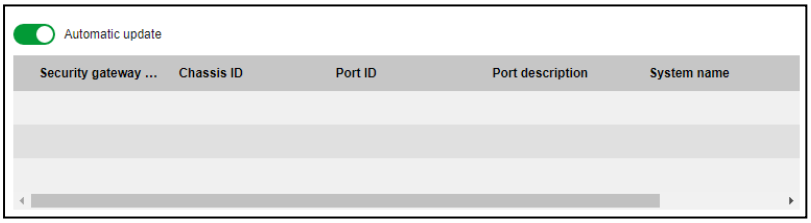
The **Access** tab allows you to configure administrators access to Security Gateway monitoring.

To block the administrator access, clear the required check box and click **Save**.

Note.
You can configure access only for an administrator with the restricted rights.

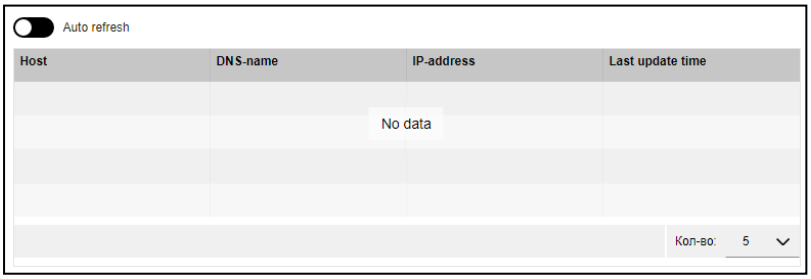
Neighboring network devices

The **Neighboring network devices** tab displays the information about the Security Gateways connected under the LLDP protocol.



DNS names IP addresses

The IP/DNS tab displays the information about Security Gateways DNS names.



DNS parameters are configured in the **Access control** or **VPN** section in the **Security Management Server objects** | **DNS**.

Manage user sessions

User Sessions tab in the **Security Gateway** section is available for viewing if the Access Server and/or User Identification components are enabled on the Security Gateway.

The tab displays information about users with access to the Security Gateway.

Click **Refresh** to update the information in the table.

To enable the automatic information updating mode for the **User Sessions** table, turn on the **Auto-refresh** toggle: 

. In the auto-refresh mode, the information in the table updates every 5 seconds.

The administrator can forcibly disconnect users from the monitoring system.

To disconnect users:

1. Turn on the **User disconnect mode** toggle.
2. Select the required users by selecting the respective check boxes.
3. Click **Disconnect selected users**.

> **Note.**
> To select all lines in the list, select the check box at the title of the list.

DHCP statistics

The **DHCP Statistics** tab displays the results of the DHCP operation (see [**4**]).

Click **Refresh** to update the information in the table.

To enable the automatic information updating mode for the **DHCP Statistics** table, turn on the **Auto-refresh** toggle: 

. In the auto-refresh mode, the information in the table updates every 5 seconds.

Continent provides an option for forced release of addresses assigned by the Security Management Server administrator.

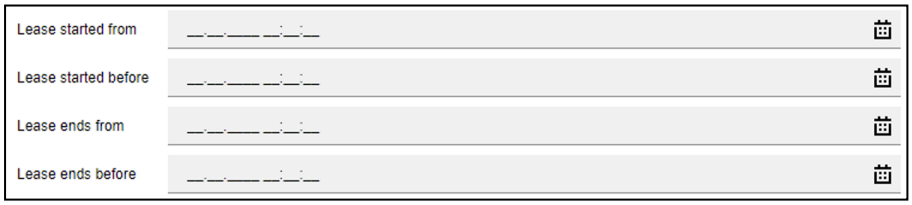
To forcibly release addresses:

1. Turn on the **Lease termination mode** toggle.
   The list of addresses assigned by the DHCP server becomes available for editing.
2. In the list, select the check boxes for addresses you want to release and click **Terminate lease**.
3. Turn off the **Lease termination mode** to finish releasing addresses and apply the changes.

To search for addresses, you can use a system for filtering the list of addresses.

To configure address list filters:

1. Click on the toolbar.
   The **Filter** parameter group appears.
2. Set the required values for filtering parameters.
3. To specify search intervals for the address lease duration, left-click the parameter line marked with .



4. In the appeared dialog box, select the date.
5. Click **Select time** to go to the section for filter time selection.

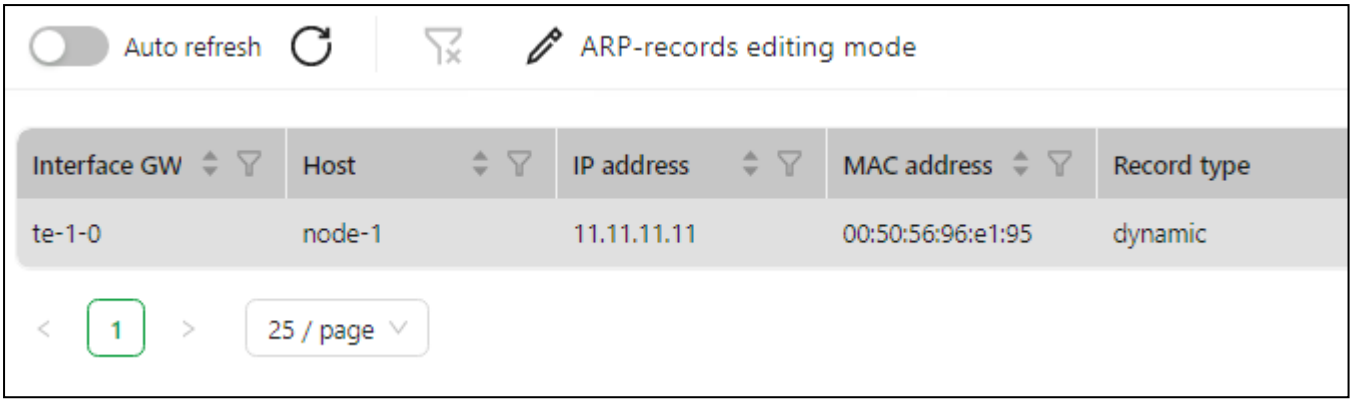
> **Note.**
> Clicking **Now** sets the current date and time.

6. To search for addresses with an expiring lease duration, specify the time in minutes for the **Expiration time from** and **Expiration time to** fields.
7. Click **Save**.

ARP-records

On the **ARP-records** tab, you can view, update and delete records in the ARP table (the IP address — the MAC address correspondence).

You cannot manage static ARP records и ARP proxy records for objects of the **Cluster** type structure. It is available only for individual Security Gateways in a cluster.

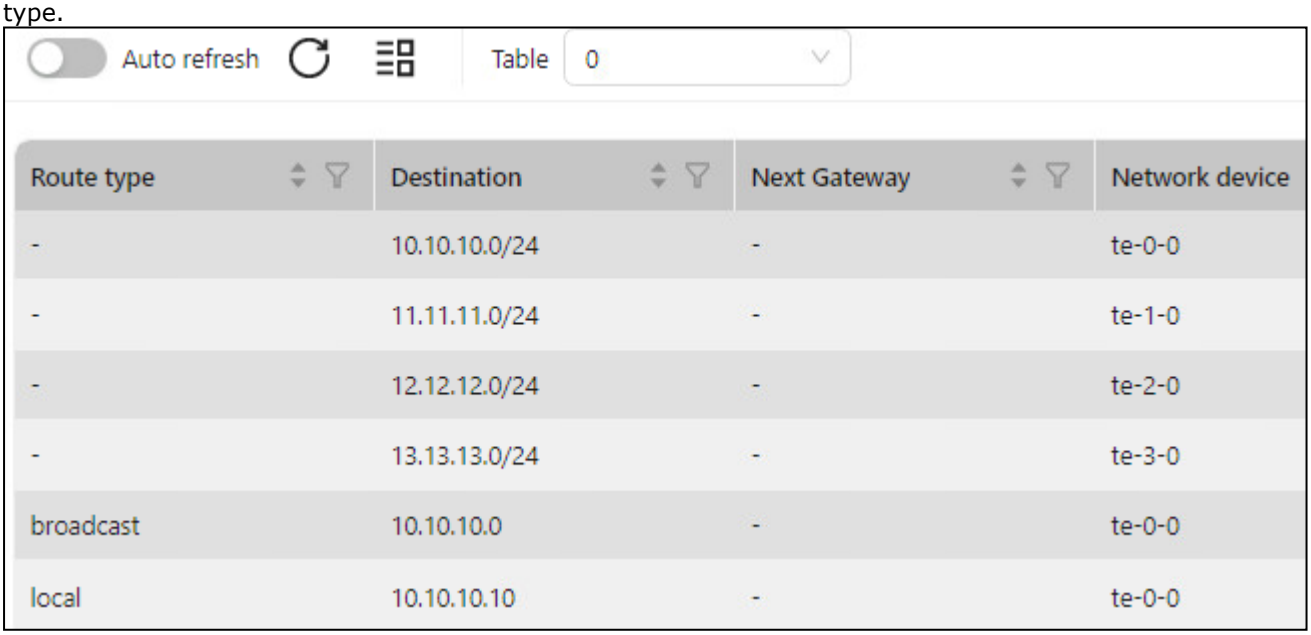


Remote command execution

On the **Remote command execution** tab, you can run the ping and traceroute commands for the Security Gateways that are seen in the monitoring. The results of command execution are displayed in the main area of the tab.

Routing

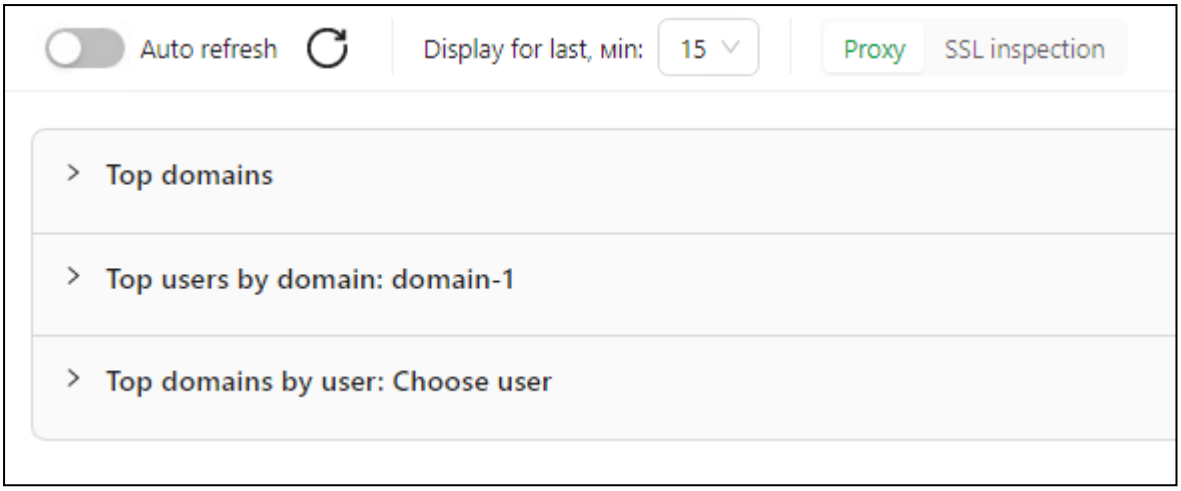
On the **Routing** tab, the table of routes created for the Security Gateway is displayed. Entries in the table can be filtered and sorted by route type, destination network, next gateway, network device, table type, and protocol type.



Web-resources and Web-resources statistics

On the **Web-resources** tab, proxy server user sessions are displayed (see [**5**]).

On the **Web-resources statistics** tab, statistics for these sessions are displayed.



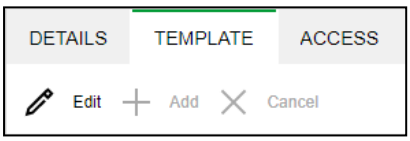
By default, the statistics sections are displayed in a closed view. To open the section, click the required line.

To switch between statistics sections, use 

.

Security Gateway group

When you select a Security Gateway group, there are the **Contacts**, **Rules**, **Access** and **IP addresses of DNS names** tabs available.



Contacts

The **Contacts** tab allows you to configure and view information about the employees responsible for Security Gateway group operation.

The procedure of configuring parameters of the Contacts tab is similar to configuring parameters of the Contacts tab for a Security Gateway. For more information, go to the **Security Gateways** section (see стр.**1**).

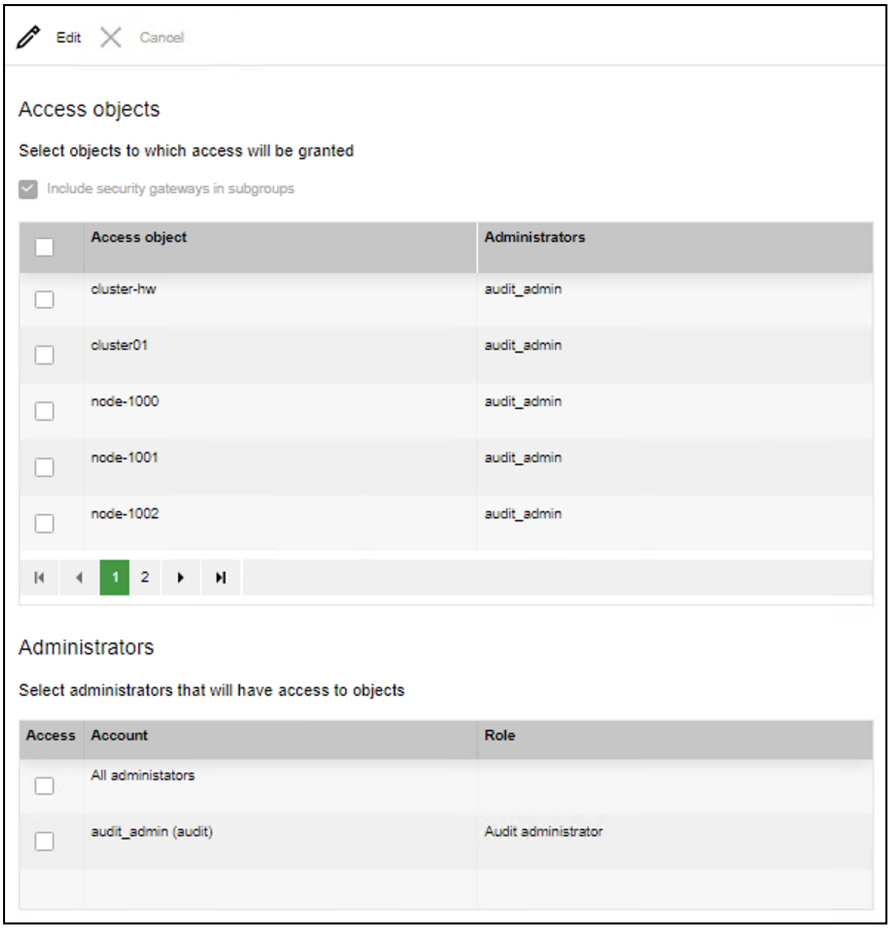
Rules

The **Template** tab allows you to configure monitoring rules of a Security Gateway. For more information about the monitoring rules configuration, see p. **28**.

Access

The **Access** tab allows you to configure administrators access to Security Gateway monitoring and consists of two areas:

- the **Access objects** area displays the Security Gateways of the group with the list of administrators who have access to them;
- the **Administrators** area contains the full list of Monitoring and Audit System administrators with the restricted rights.



In the **Access objects** area, select the Security Gateway. To select all the Security Gateways, select the **Access objects** check box.

Attention!
By default, the list of Security Gateways contains the Security Gateways that belong to subgroups of the selected group. To exclude them from the list, clear the **Include security gateways in subgroups** check box.

In the **Administrators** area, the list of administrators with the rights to access the selected Security Gateway appears. To configure the access of an administrator to the Security Gateways, select the check boxes in the **Access** column and click **Save**. To control the access of all the administrators, select the **All administrators** check box.

Attention!
To access the Security Gateway group, a user must have rights to access all the Security Gateways of this group.

DNS names IP addresses

The **DNS names IP addresses** tab allows you to view information about Security Gateway DNS names. The information is the same as the information on the **DNS names IP addresses** tab for a Security Gateway (p. **37**).

The parameters of DNS names are configured in the **Access control** or **VPN** sections in the **SMS objects | DNS-names** group.

Cluster

When you select a Security Gateway of a security cluster, there are the following tabs available:

State

On the **State** tab, you can find the following information:

- **Active events** — the table containing the list of active events on the Security Gateways and the cluster.

- **Primary Security Gateway** — the name of a primary Security Gateway and its state.

- **Reserve Security Gateway** — the name of a reserve Security Gateway and its state.

Details

The **Details** tab allows you to configure and view information about the employees responsible for Security Gateway operation:

- name;
- work phone number;
- mobile phone number;
- Skype account;
- e-mail address.

  Note.
  While creating a new monitoring rule, e-mail address is specified in the **Send email** field by default.

- e-mail address for notifications;

  Note.
  This e-mail address is used while creating an automatic notification about Security Gateway failure.

- information.

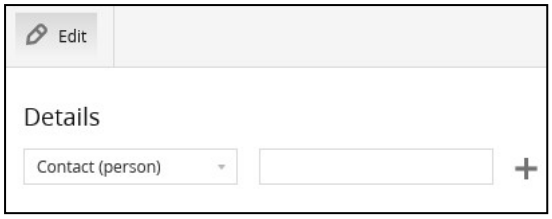
  Note.
  This information is displayed on the tile of the **Structure** widget on the Monitoring dashboard.

The initial form of the **Information** tab is shown in the figure below.

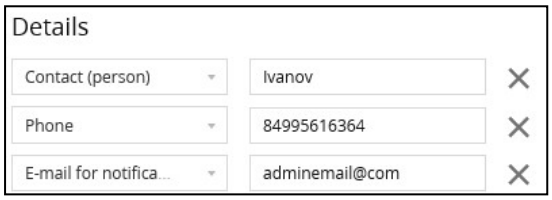
To edit the information:

1. Click **Edit**.

   The **Information** tab changes as in the figure below:



2. To add a new parameter, click **Add**.
   The field for a new parameter appears.
3. To change the parameter type, click and select the required type in the drop-down list.
4. In the right field, enter or change the parameter value.
5. To delete the parameter, click.
6. Click **Save**.



Template

The **Template** tab allows you to configure monitoring rules of a cluster. For more information about the monitoring rules configuration, see p. **28**

Access

The **Access** tab allows you to configure administrators access to Security Gateway monitoring.

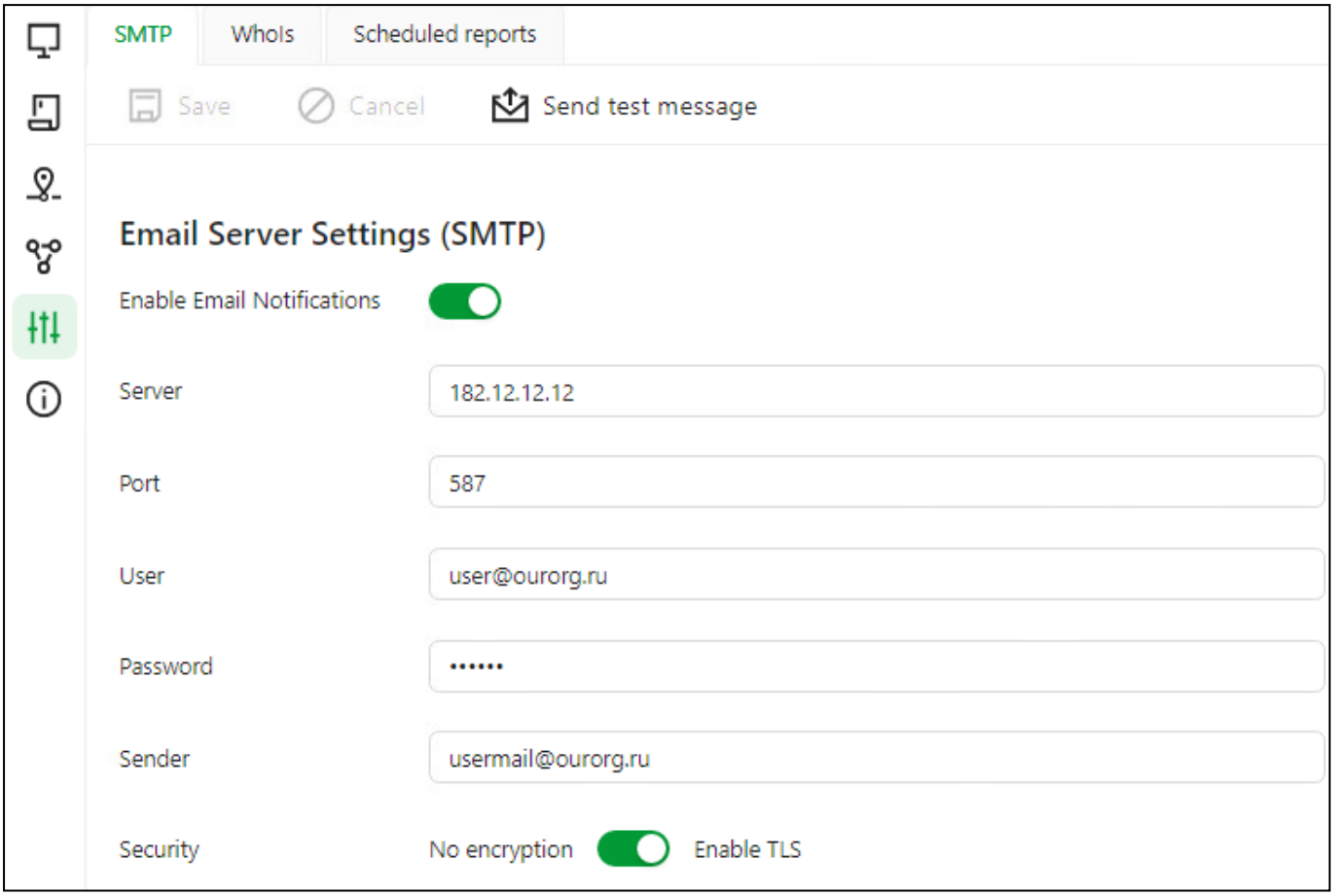
Account	Role	Access
All administrators		☑
asd (asdasd)	Security administrator	☑

To block an administrator access, clear the required check box and click **Save**.

Note.
You can configure access only for an administrator with the restricted rights.

Settings

You can see the **Settings** main window as follows.



In **Settings**, you can configure email notifications if a Security Gateway is unavailable.

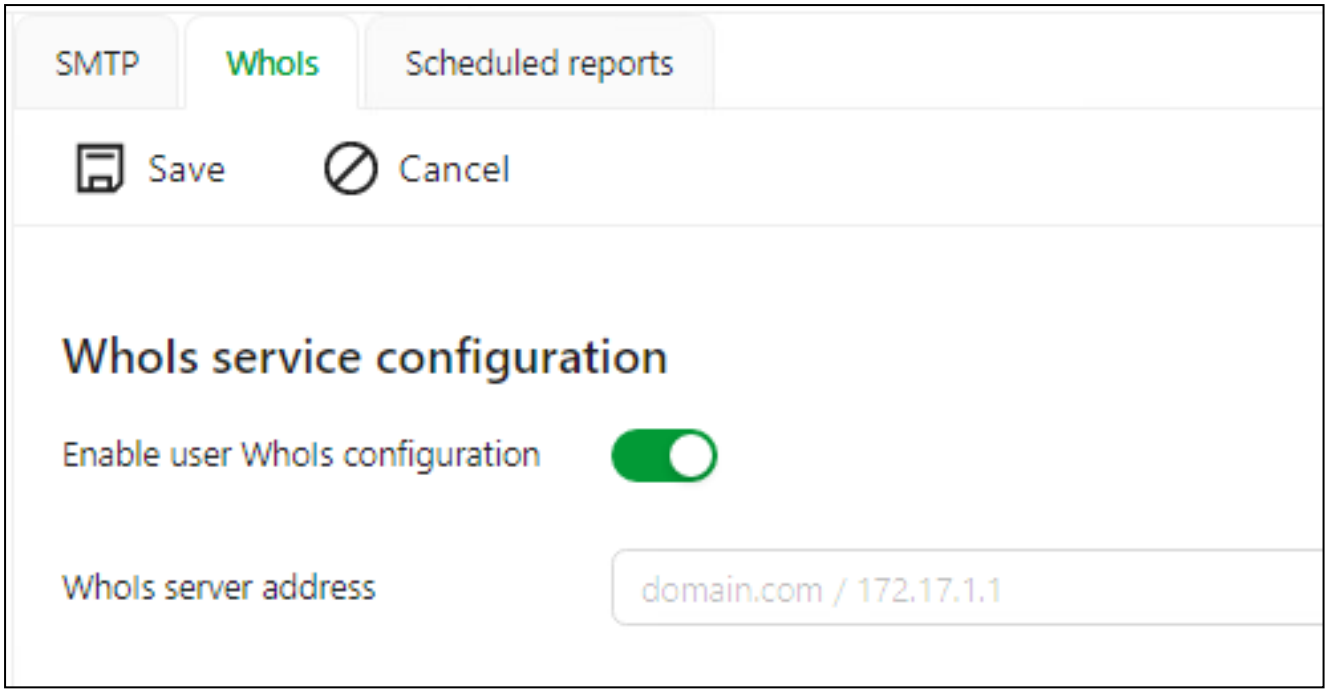
To configure e-mail notifications:

1. Go to the **SMTP** tab.
2. Select the **Enable Email Notifications** check box.
3. Specify the required information.
4. Turn on the **Enable TLS** toggle if necessary.
5. Click **Save**.
   The **Send text message** become available.
6. To check the setting, click **Send test message**.

The **WhoIs service configuration** section allows you to set the WhoIs server address.

To configure WhoIS protocol:

1. Go to the **WhoIs** tab.
2. Turn on the **Enable user WhoIs configuration** toggle.
   The **WhoIs server address** field becomes available for editing.



3. Specify **WhoIs server address** and click **Save**.

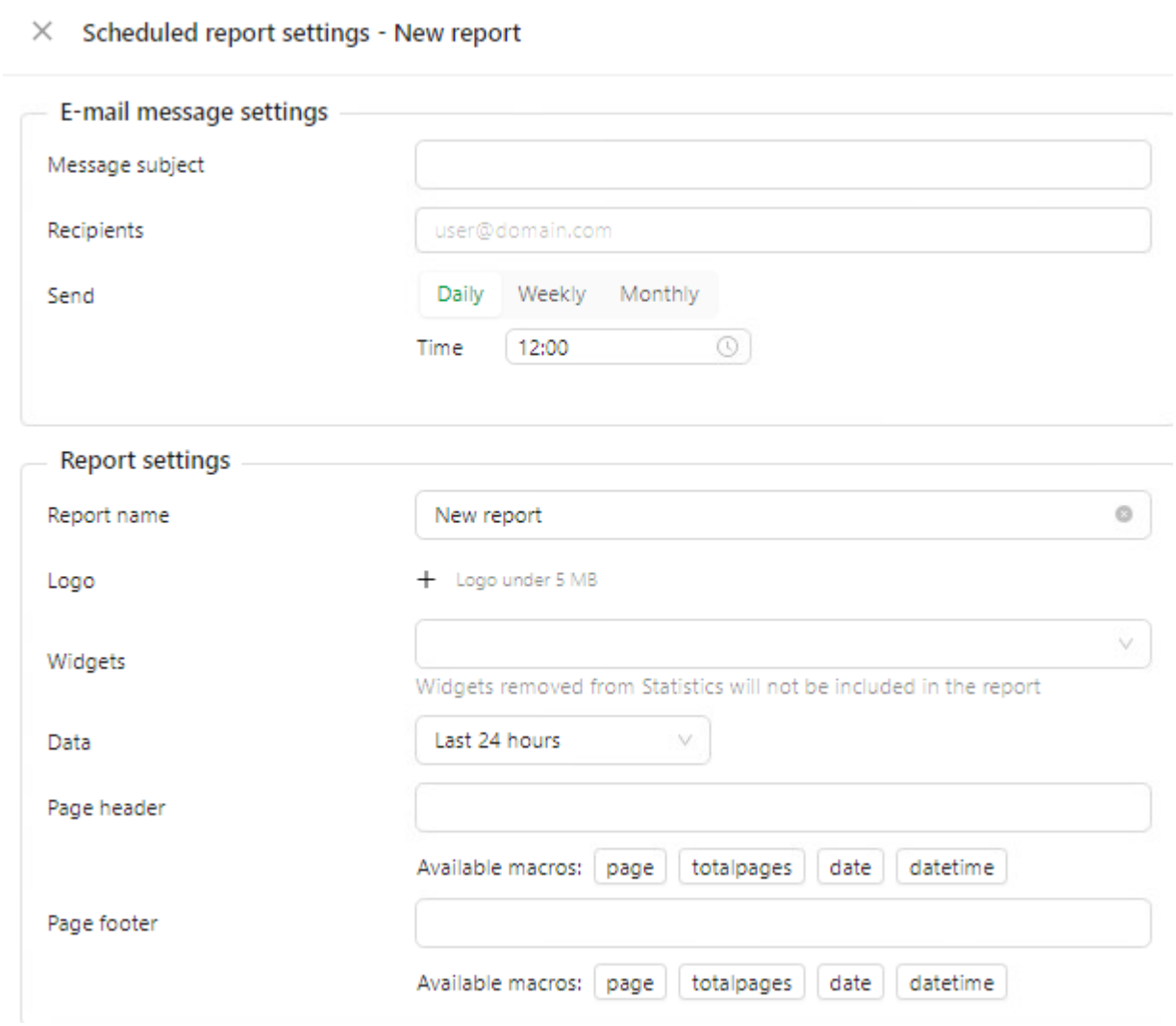
Scheduled reports

Continent makes it possible to send reports from the **Statistics** section of monitoring according to a specified schedule.

Attention! To send notifications about sent reports, you must enable the **Email notification**s parameter in the Security Gateway properties (see p. 1).

To configure scheduled reports:

1. In the **Settings** section, go to the **Scheduled reports** tab.
2. Click **Add report**. The following window appears.



3. In **Message subject**, specify the text that is to be displayed in the **Subject** field of an email.
4. In the **Recipients** list, add the email addresses of the recipients.
5. In **Send**, select the frequency and time of sending reports.
6. In the **Report settings parameter** group, specify the report name and add a logo if necessary.
7. In the **Widgets** drop-down list, check the widgets that must be included in the report.
8. If necessary, add macros to the page header and footer of the report.
9. Click **Save**.

The created report appears in the report list with the **State** toggle turned on.

To disable report sending:

- turn off the toggle of the selected report.

To edit a report:

1. Click ⋮ and select **Edit** in the context menu.
   A window with the parameters of the scheduled report opens.
2. Make the required changes and click **Save**.

To send a report out of turn:

1. Make sure that the report is active — the **State** toggle must be turned on.
2. Click **Send e-mail** in the context menu.

To delete a report:

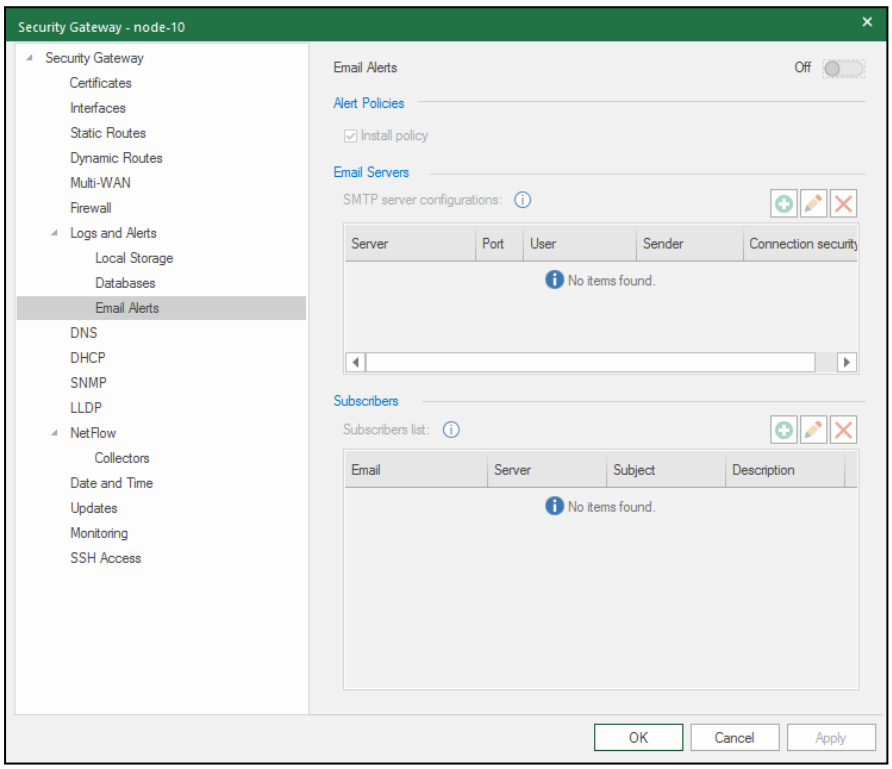
- select the required reports by selecting the checkbox in the row and click the **Delete selected reports** button.

Configure e-mail notifications

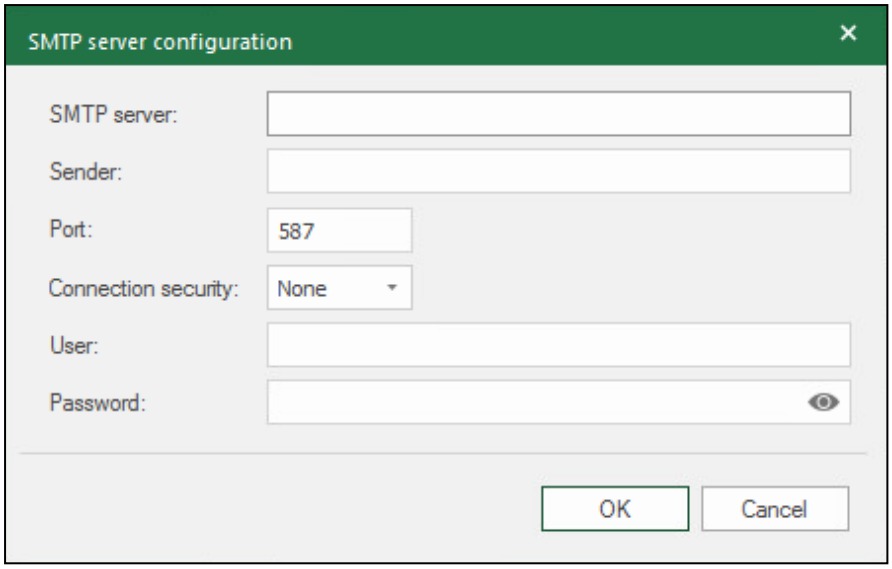
This parameter enables configuring email notifications about the results of the policy installation on a Security Gateway.

To configure e-mail notifications:

1. In the Configuration Manager, go to **Structure**.
2. Right-click the Security Management Server and select **Properties**.
3. In **Logs and Alerts**, select **Email Alerts**.
   The **Email Alerts** settings appear on the right.



4. Turn on the **Email Alerts** toggle.
   The **Email Alerts** parameters become available for editing.
5. Select the **Install policy** check box.
6. In the **Email Servers** section, click  .
   The **SMTP server configuration** dialog box appears.



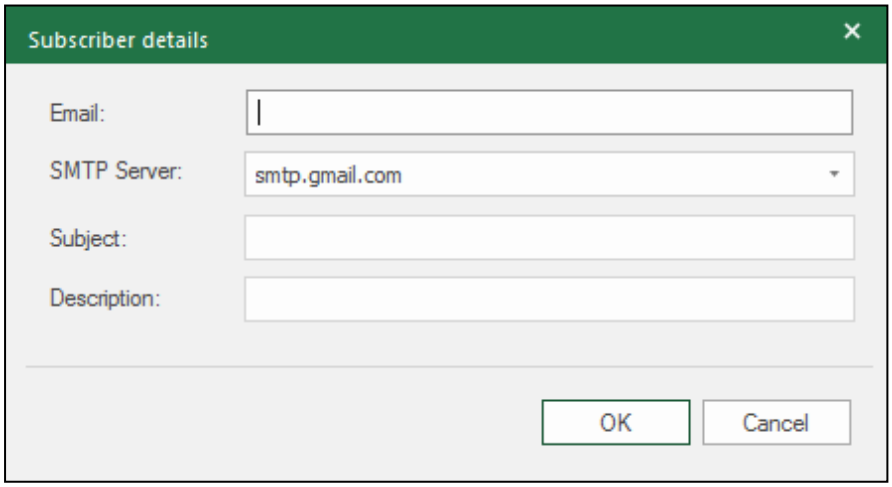
7. In **SMTP server**, specify the SMTP email server name in the form of an address or **smtp.gmail.com**.
8. In **Sender**, specify an email source name in the form of **user@domain.com**.
9. In **Port**, specify the SMTP server port.
10. In the **Connection security** drop-down list, select an encryption type.
11. If necessary, select the **Authentication** check box.

    The **User** and **Passwords** parameters become available for editing. Specify the SMTP server user name in the form of **user@domain.com** and a password.
12. Click **OK**.

    The added email server will appear in the **Email Servers** section.

    To add one more email server, perform steps **6** – **12**. The maximum number of email servers — 2.
13. In the **Subscribers** section, click .

    The information about a destination appears.



14. In **Email**, specify the subscriber email address.
15. In the **SMTP Server** drop-down list, select an email server configuration if necessary.
16. In **Subject**, specify the title of an email alert.
17. In necessary, specify **Description**.
18. Click **OK**.

    The added destination appears in the **Subscribers** section.

    To add other destinations, perform steps **13** – **18**.

    The maximum number of destinations — 32.

19. Click **OK**.

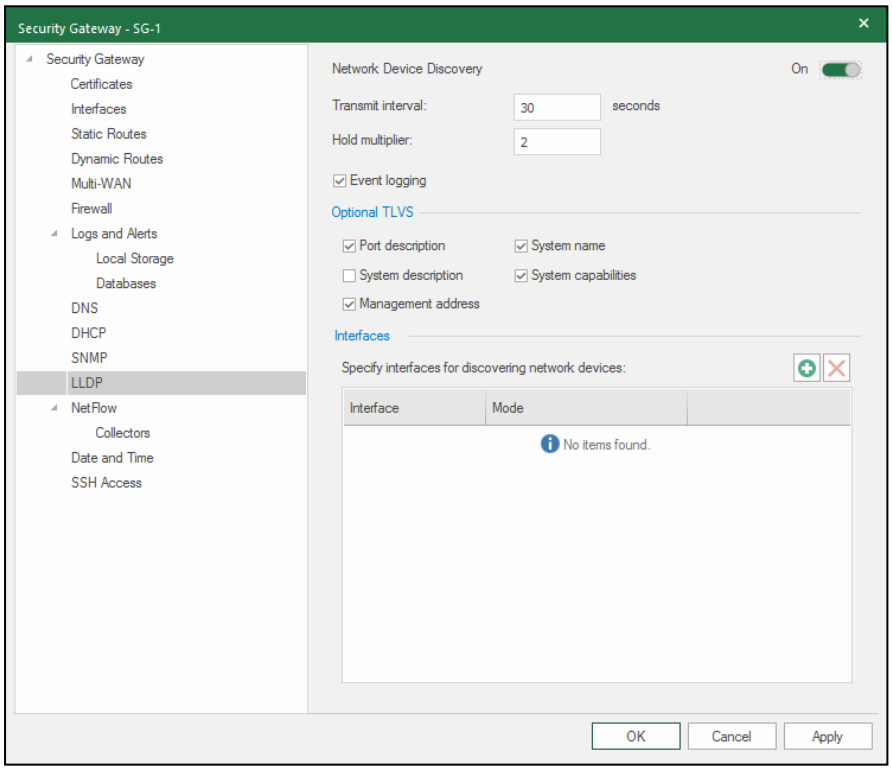
Configure LLDP protocol

Continent provides an opportunity to transfer Security Gateway information using network devices under the LLDP protocol.

To configure LLDP protocol:

1. In the Security Gateway properties, go to **LLDP**.
2. Turn on the **Network Device Discovery** toggle.

The LLDP parameters become available for editing.



3. Select **Event logging** to activate event logging between devices in the system log.
4. In the **Optional TLVS** group box, select the required options.
5. In the **Interfaces** section, specify the interfaces required to detect network devices. To add an interface, click and select the required interface.
6. Click **OK** to save the configuration and close the **Security Gateway** dialog box.

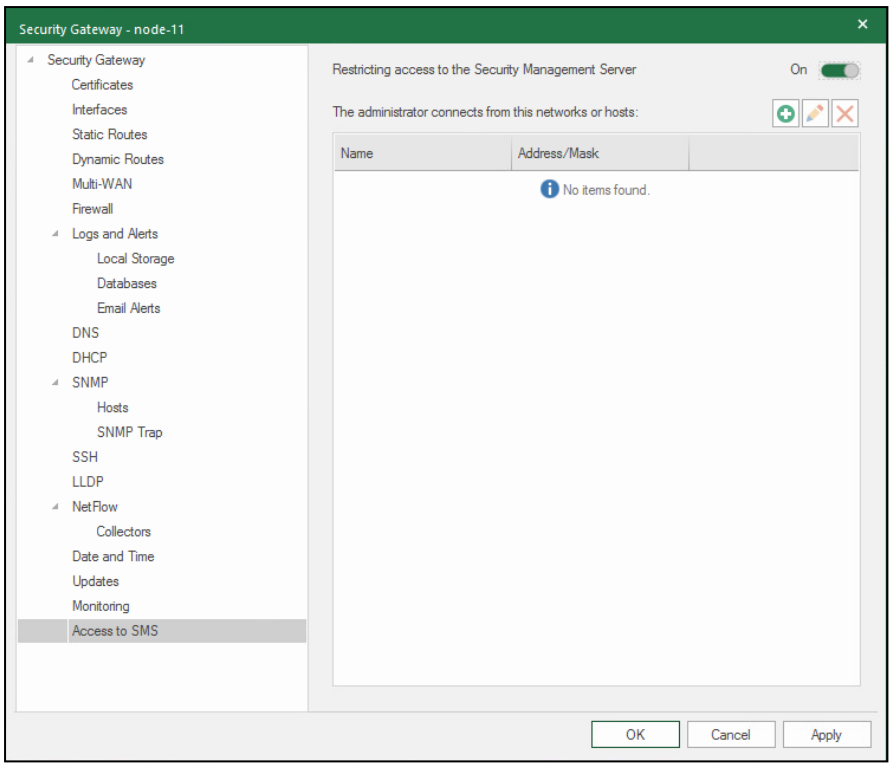
Restrict access to the Security Management Server

Continent provides an option to restrict access to the Security Management Server from any network object. By default, the Continent administrator is allowed access to the Security Management Server from any network object.

To restrict administrator access to the Security Management Server:

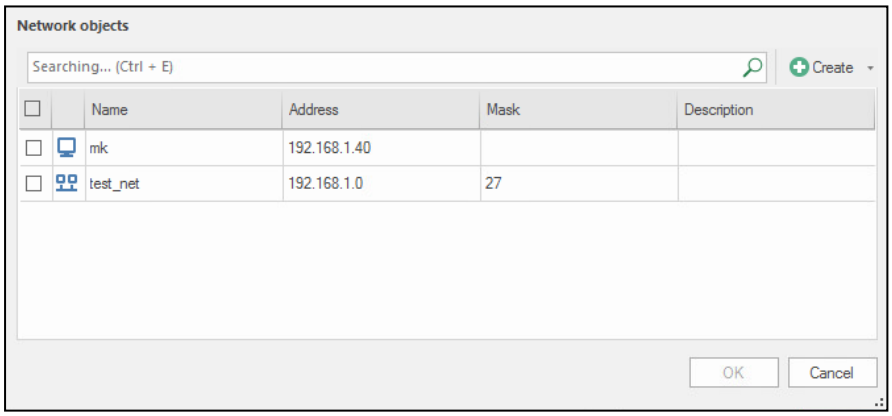
1. Right-click the Security Gateway and select **Properties**.
2. On the left, go to **Access to SMS**.
3. Turn on the **Restrict access to the Security Management Server** toggle.

Access parameters become available for editing.



4. Click  .

   A dialog box for selecting network objects appears.



5. In the list of network objects, select the ones from which the administrator is allowed access to the Security Management Server.
6. Create a new network object, if necessary. To do so, click **Create**, specify the required parameter values and click **OK**.
7. Click **OK** in the Security Gateway properties window to save the changes.

Chapter 4
Audit

To perform an audit, take the following steps:

- Configure log parameters (see below).
- View and analyze log entries using:
  - the Monitoring and Audit system tools (see p. **57**).
  - the local menu (see p. **61**).

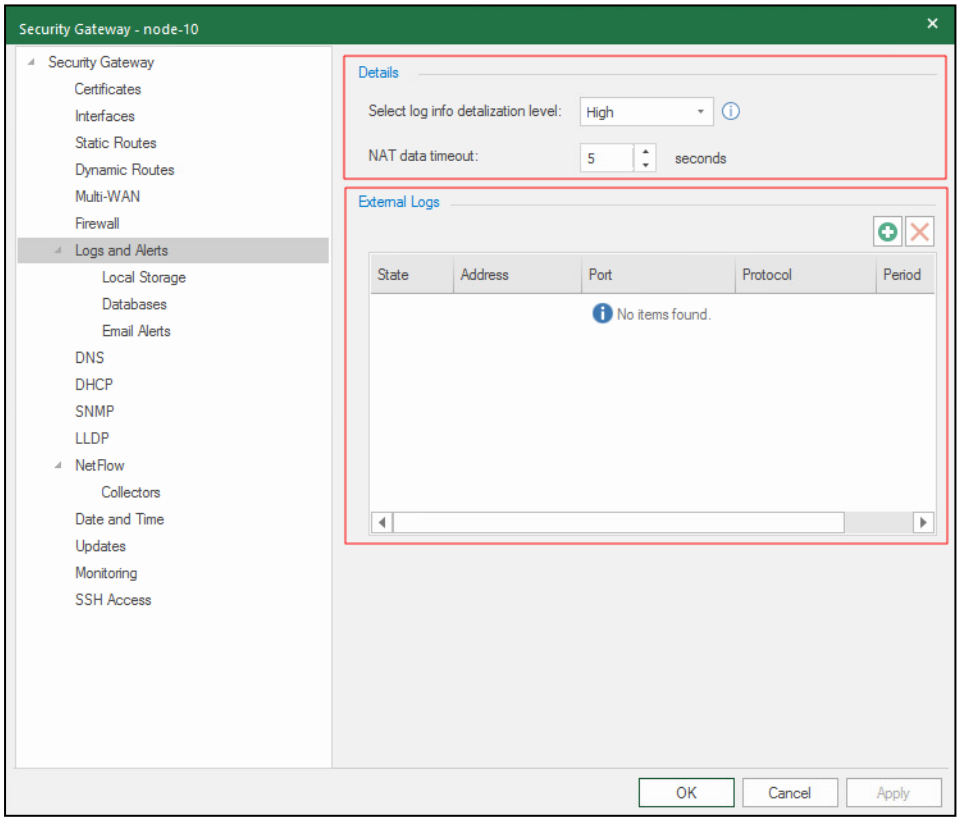
Log parameters

You can configure the following log parameters:

- detalization level for logs (see below);
- log storage on the external syslog server (see p. **52**);
- automatic log cleaning (see p. **53**);
- log storage on the external database (see p. **54**).

To view log parameters:

1. In the Configuration Manager, go to **Structure**.
2. Right-click the required Security Gateway and click **Properties**.
   The **Security Gateway** dialog box appears.
3. Go to **Security Gateway** | **Logs and Alerts**.



On the right, you can see current log parameters of the Security Gateway:

- **Details** — to configure detalization level for events registered in logs;
- **External logs** — to view and configure parameters of external system logs.

Detalization level

To set a detalization level for logs:

1. In the **Security Gateway** dialog box, go to **Security Gateway | Logs and Alerts**. In the **Details** group box, select the required detalization level from the respective drop-down list:

Detalization level	Severity level
Debugging	Debug (DEBUG)
High	Information (INFO)
Medium	Warning (WARNING)
Low	Critical error (CRIT)
Minimal	Alert (ALERT)

Attention!
Events are logged according to the selected (or higher) detalization level.

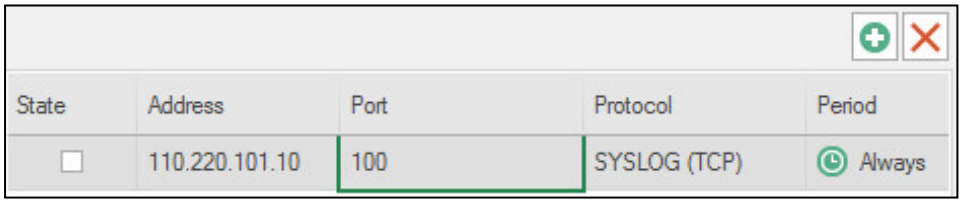
2. In the **Security Gateway** dialog box, click **OK**.
3. Save the changes and install the policy on the required Security Gateways.

Store logs on an external syslog server

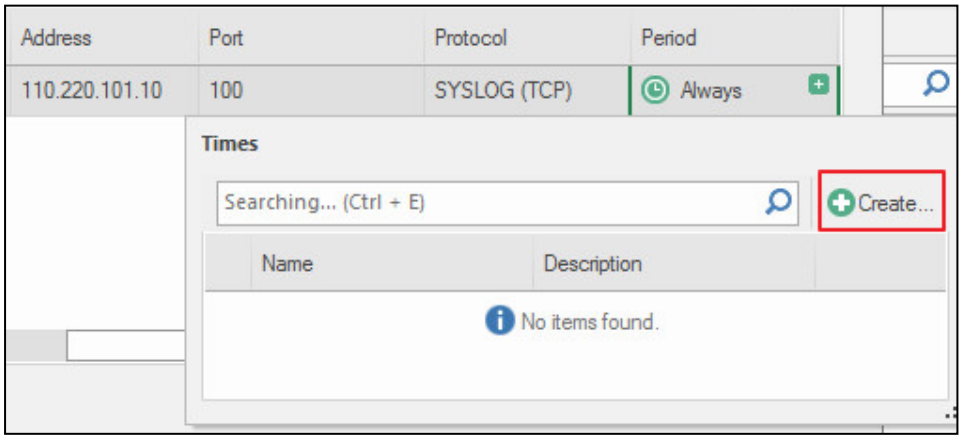
Attention!
A syslog server must support the event format RFC 5424.

To add a new syslog server:

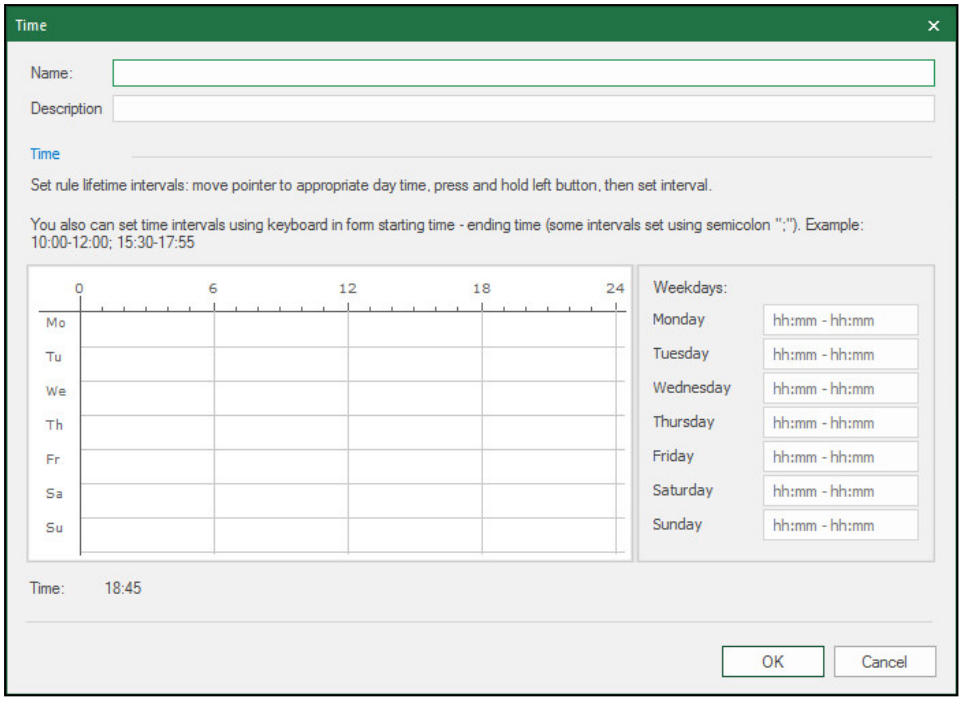
1. In the **Security Gateway** dialog box, go to **Security Gateway | Logs and Alerts**. In the **External Logs** group box, click .
   A new syslog server is added to the table.



2. Specify the required parameters of the syslog server.
   You can configure access to a syslog server at a specific time. To do so, in the **Period** column, set a required time interval. Hover your mouse over the respective cell, click . The **Times** dialog box appears.



3. In the **Times** dialog box, click **Create**.
   The dialog box appears as in the figure below.



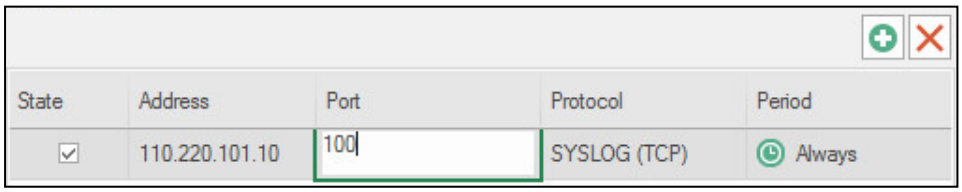
4. Follow the instructions on the screen and click **OK**.
5. In the **Security Gateway** dialog box, click **OK**.
6. To apply changes, on the toolbar, click **Install policy**. In the appeared dialog box, select the required **Security Gateway** and click **OK**.

Note.
The Security Management Server receives security cluster logs only during the Security Gateway logging process irrespective of a certain settings type. To get security cluster logs stored during time interval limitations, delete event information sending intervals and install the policy. The Security Management Server will receive logs stored on Security Gateways. If you do not need stored logs, delete them from the Security Gateway.

To configure syslog server parameters:

1. In the **Security Gateway** dialog box, go to **Security Gateway | Log Settings**. In the **External Logs** group box, select the required line.
2. Double-click the required cell and modify the information.

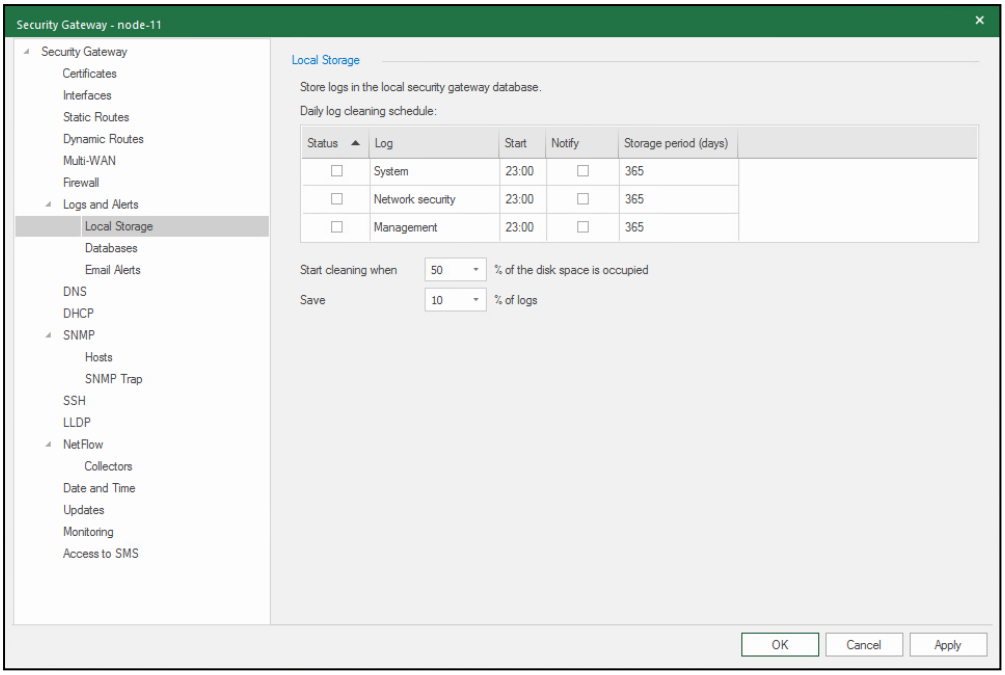
Note.
If **SYSLOG (UDP)** is selected as the transport protocol, the packet size must not exceed the set MTU value. Use the **SYSLOG (TCP)** protocol for packet fragmentation.



3. To disable log storing on the server, clear the **State** cell.
4. In the **Security Gateway** dialog box, click **OK**.
5. To apply changes, on the toolbar, click **Install policy**. In the appeared dialog box, select the required **Security Gateway** and click **OK**.

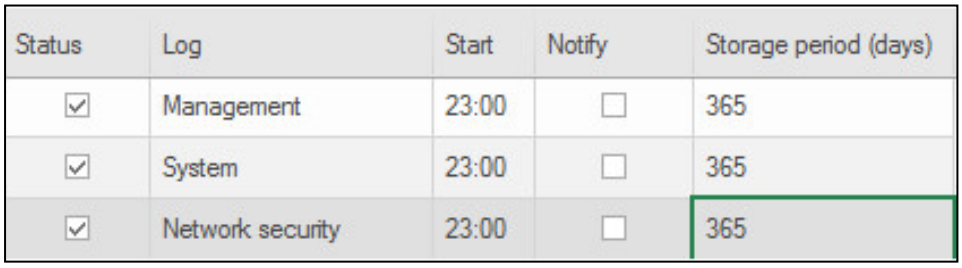
Configure automatic log clearing

- In the **Security Gateway** dialog box, go to **Security Gateway** | **Logs and Alerts** | **Local Storage**.



To clear logs on schedule:

1. In the **Daily log clearing schedule** table, select the required logs. To do so, in the **Status** column, select the respective check boxes.
2. To configure time for cleaning, double-click the **Start** cell and specify the time when the cleaning begins.
3. To receive emails when the cleaning is performed, in the **Notify** column, select the respective check boxes.
4. To configure a number of days for storing logs, double-click the **Storage period (days)** cell and specify the required information.
5. In the **Security Gateway** dialog box, click **OK**.
6. To apply changes, on the toolbar, click **Install policy**. In the appeared dialog box, select the required **Security Gateway** and click **OK**.



By default, logs are not cleared by expiration automatically. Logs are cleared automatically when used disk space matches the specified number (in percents) that displays rate of free and used disk space (available range is 50 – 80 percents). And a number of saved events (in percents) cannot be less than 10 percents (available range is 10 – 50 percents).

To clear logs automatically:

1. In the **Start cleaning when** and **Save** spin boxes, set the required values.
2. In the **Security Gateway** dialog box, click **OK**.
3. To apply changes, on the toolbar, click **Install policy**. In the appeared dialog box, select the required **Security Gateway** and click **OK**.

Store logs in an external store

Configure a server for external storage of logs

Storing network security logs, system logs and monitoring databases on an external database is turned off by default. To make this feature work, deploy a server with a Database Management System and search engine.

Note.
PostgreSQL is the only supported external storage.

Attention!
You must use local storage to send Security Gateway logs to the Security Management Server.

To configure PostgreSQL Server on the Windows Server:

1. In **PostgreSQL**, create a user that has privileges to manage databases for monitoring statistics storage and databases for logs storage.
2. Create a database for monitoring statistics storage and a database for logs storage.
3. Open the configuration file **pg_hba.conf** and add the following line:

```
host all all <subnet, used by Windows Server>/24 password
```

4. Open the configuration file **postgresql.conf** and set the following value for the listen_adresses parameter:

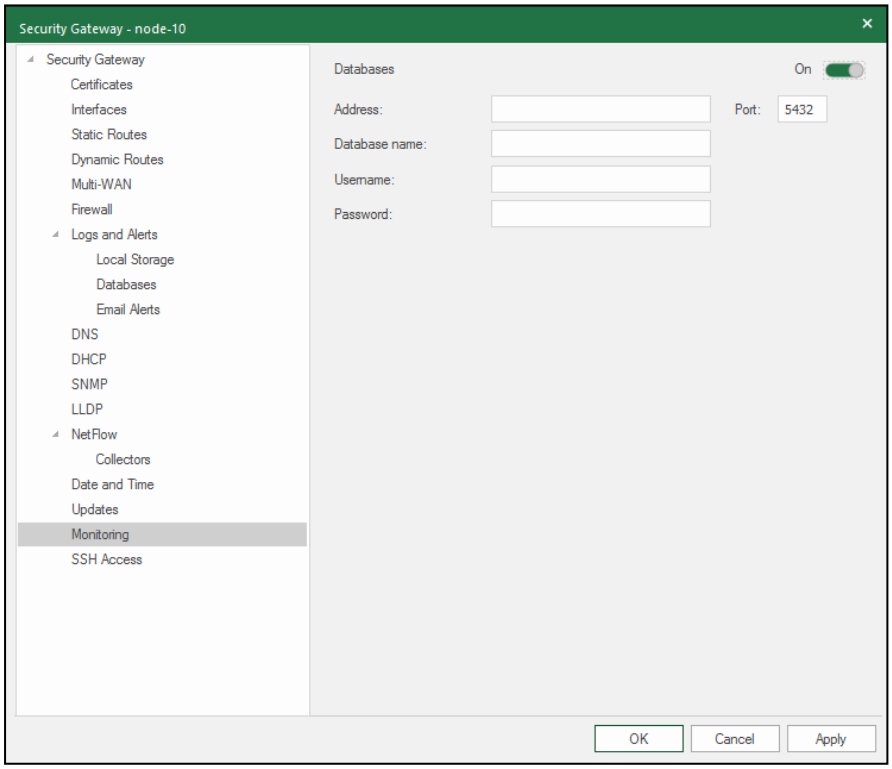
```
listen_addresses='*'
```

You can configure monitoring statistics storage and logs storage on an external database in the Configuration Manager.

To configure monitoring statistics storage in the Configuration Manager:

Note.
You can configure monitoring settings only on the Security Management Server.

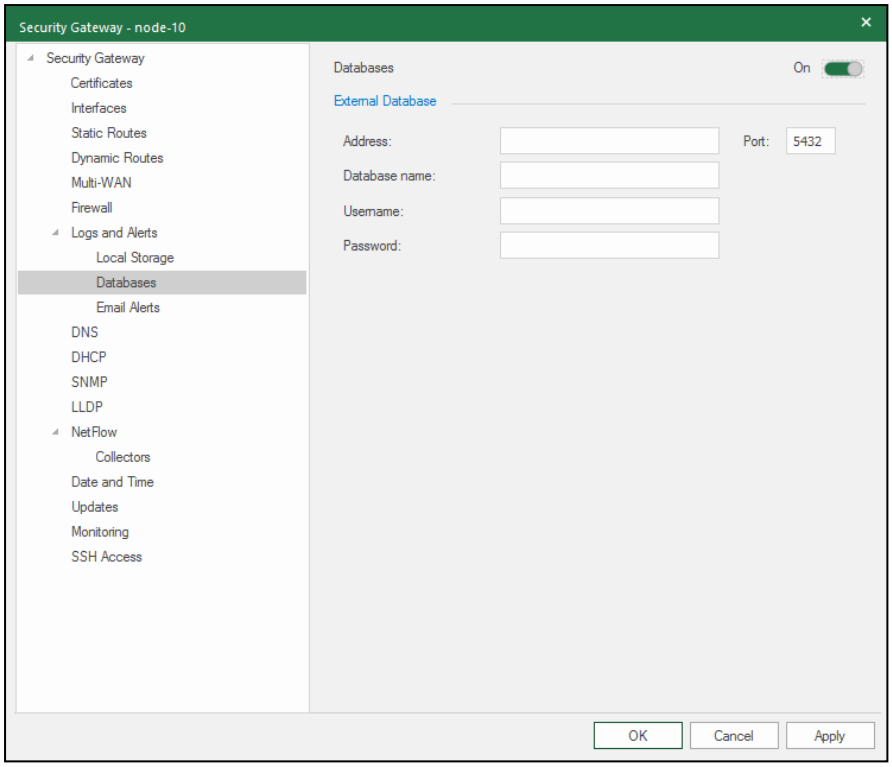
1. Go to **Structure**, select the Security Management Server and click **Properties** on the toolbar.
   The properties of the Security Management Server appear.
2. On the left, go to **Monitoring**.
   External database parameters appear on the right.



3. Turn the **Databases** toggle on.
   The external database parameters are available for editing.
4. Specify the required parameters in the respective text boxes and click **Apply**.

To configure logs storage on an external database in the Configuration Manager:

1. On the left, go to **Log Settings | Databases**.
   The respective settings of logs storage on an external database appear.



2. Turn the **Databases** toggle on.

   Text boxes for entering external database and search engine parameters become active.
3. Specify the required parameters in the **External Database** group box (see p. **55**).
4. Click **Apply**.

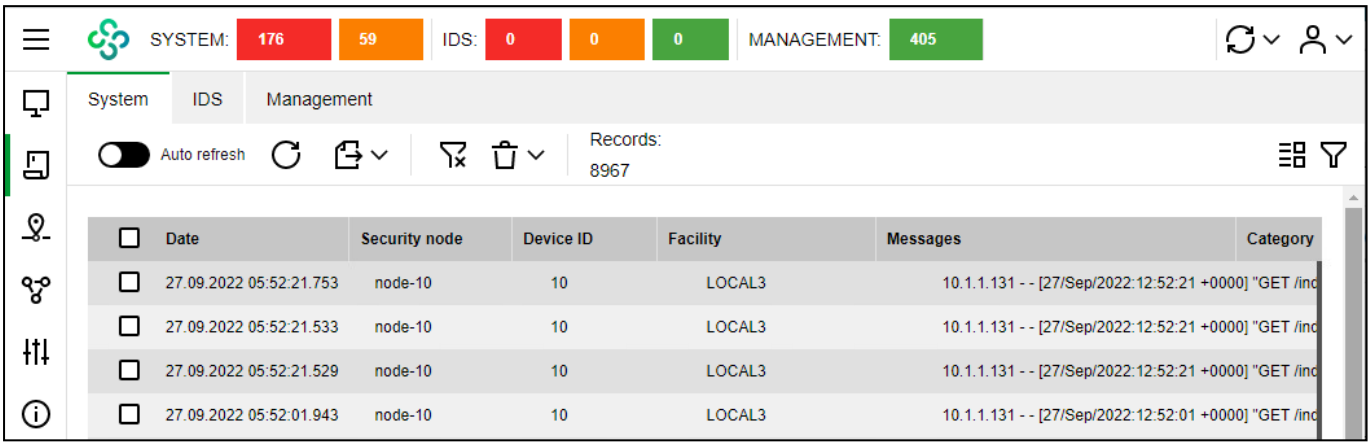
Attention!
The external database server must support the event format RFC 5424.

5. Click **OK** in the **Security Gateway** dialog box.
6. To apply changes, click **Install policy** on the toolbar, select the required Security Gateways and click **OK** in **Install policy** dialog box.

View logs using the web interface

To view logs in the Monitoring and Audit system, on the navigation panel, select **Logs**.

Display area elements of the **Logs** section change in accordance to the selected **Source**. The display area of the **Logs** section is shown in the figure below (when **Source** set to **System**).



To create an event filter in a log:

1. On the right, click .
2. In the **Journals** group box, specify the **Filter title** and if necessary the **Date from** and **Date to** parameters.

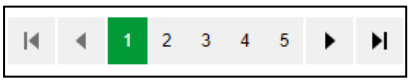
   Attention! When you filter by the **Date** parameter, the time is specified according to the time zone of the computer on which the browser with the monitoring and audit system is running.
3. If necessary, select **Save filter**. The saved filter will be available for choosing in the **Saved filters** drop-down list.
4. In the **Parameters** group box, specify the required parameters for filtering criteria.

   Note.
   For search criterion with a drop-down list, you can choose several filtering criteria.
5. Click **Apply**.

To apply the created filter:

1. In the **Saved filters** drop-down list, select a filter.
2. Click **Apply**.

To move through the table, use buttons shown in the figure below.



A number of shown messages is defined by the **Page size** parameter.

To configure view of event parameters, click and select the required parameters.

System log

System log contains the following information:

- **Date** — date and time of a message. An administrator of the Monitoring and Audit system set a required time zone.
- **Security Gateway** — the Security Gateway on which the message was generated.
- **Device ID** — a device identifier specified during the deployment.
- **Object** — an object type.
- **Category** — an event category.

- **Message**— information about an event.
- **Message severity** — information about message severity level.
- **Severity level** — a numerical indicator of a message severity.
- **Security Gateway date** — date and time of a message specified in a time zone of the respective Security Gateway.
- **Host** — a name of a Security Gateway specified as a host.

To filter events, use the following tags:

Tag	Description
severity:"level"	Filter messages by the required severity level
category:"text"	Filter messages by the required category
state:" "	Filter messages by the required state
monitoring_parameter:"subsystem"	Filter messages by the monitoring events on the required subsystem
security_gateway:"name"	Filter messages by the events on the required Security Gateway
message:"text"	Filter messages by the required text
repeat_count:"numeral"	Filter messages by the required number of events
hostname:"name"	Filter messages by the events on the required host

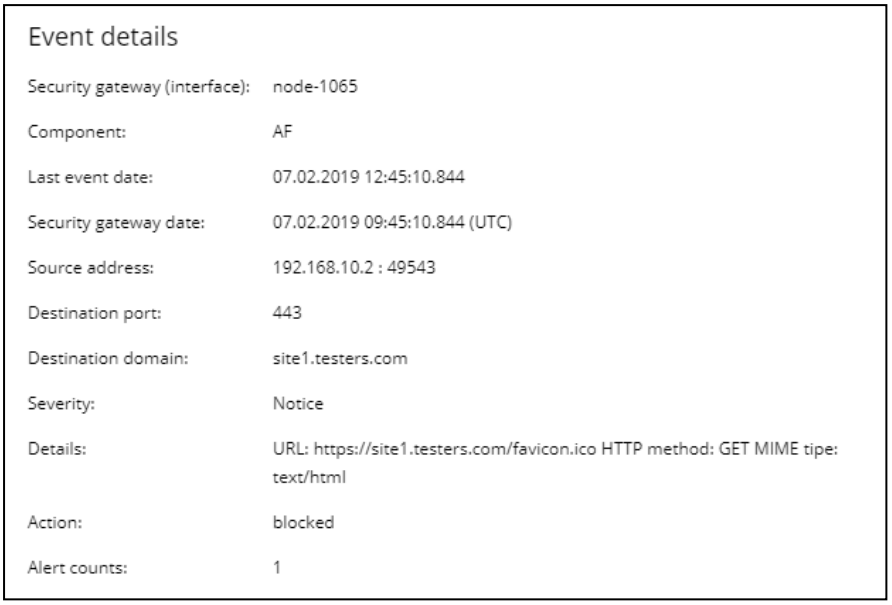
Note.
A hostname contains a name of the Security Gateway and a domain with a period (.) between them.

Network security log

Network security log contains the following information:

- **Date** — date and time of a message. The administrator of the Monitoring and Audit system set a required time zone.
- **Action** — action performed for a traffic.
- **Security Gateway** — Security Gateway on which the message was generated.
- **Source address** — address where an attack is generated.
- **Source country** — code of a source country.
- **Destination address** — address on which an attack is generated.
- **Destination country** — code of a destination country.
- **Destination domain** — domain on which an attack is performed.
- **Protocol** — protocol by which an attack is performed.
- **Destination port** — ports of a destination.
- **Source port** — ports of a source.
- **Signature/rule** — text of a message with the alert count.
- **SID** — unique signature number.
- **Component** — subsystem that recorded the event.
- **Category** — event category.
- **Severity** — information about message severity level.
- **Security Gateway date** — date and time of a message specified in a time zone of the respective Security Gateway.
- **Event type** — a type of event.
- **Host** — a name of a Security Gateway specified as a host.
- **Interface** — network interface of the IPS component where an attack is detected.
- **Alert count** — the number of event alerts.

When you select the network security event, a panel appears that contains the event details. Detailed information includes the first and the last date of the event displayed in the Security Gateway time zone, the IP address and source port of the attack and the destination address and port.



To view the full text of a message in the CSV format:

1. On the navigation panel, select **Logs**, and the **NETWORK SECURITY** tab on the top.

   Respective filters and log records appear in the display area.

   Events can be grouped by their parameters. The main section contains the last message from each group, signature description and a number of messages in a group.

   Messages are sorted by the alert count (descending). The maximum number of grouped messages to be displayed is 10000 events.

2. To filter events, use the following tags:

Tag	Description
source_address:"IP address"	Filter messages by an IP address where an attack is generated
destination_address:"IP address"	Filter messages by IP address which is attacked
severity:"level"	Filter messages by the required severity level
action:"alert/allowed/blocked/detect/redirect"	Filter messages by the required action performed for traffic
destination_domain:"domain name"	Filter messages by the required domain
severity	Filter messages by the required severity level
action:"alert/allowed/blocked/detect/redirect"	Filter messages by the required action performed for traffic
category:"text"	Filter messages by the required text in the **Category** field
component:"subsystem"	Filter messages by the required subsystem
protocol:"protocol"	Filter messages by the required protocol
source_country:"country code"	Filter messages by the IP addresses sent from the required countries
destination_country:"country code"	Filter messages by the attacked IP addresses of the required countries
security_gateway:"name"	Filter messages by the events on the required Security Gateway
source_address:"IP address"	Filter messages by the IP addresses sent from the required addresses
destination_address:"IP address"	Filter messages by the IP addresses sent from the required addresses
source_port:"port number"	Filter messages by the port where an attack is generated
destination_port:"port number"	Filter messages by the port which is attacked
destination_domain:"domain name"	Filter messages by the required domain

Tag	Description
signature:"text"	Filter messages by the required text in the **Signature** field
signature_id:"SID"	Filter messages by the signature with the required ID
interface:"text"	Filter messages by the required interface
revision:"text"	Filter messages by the signature with the required version
repeat_count:"numeral"	Filter messages by the required number of events

Example:
To find messages about an attack from the 1.1.1.1 Security Gateway to the 2.2.2.2 Security Gateway and the **ge-1-1** interface, in the **Query** text box, enter the following:
source_address:1.1.1.1 and destination_address:2.2.2.2 and interface: ge-1-1

3. Click **Apply**.
   The log displays records according to the specified parameters.
4. Click  .
   The log file in the ***.csv** extension is saved to the Windows **Downloads** folder.

Management log

This log contains events collected from all the Security Gateways in the domain controlled by the Security Management Server.

The log contains the following information:

- **Date** — date and time of a message. The administrator of the Monitoring and Audit system set a required time zone.
- **Security Gateway** — Security Gateway on which the message was generated.
- **Device ID** — network device identifier.
- **Subject** — administrator who performed an action.
- **Message** — text of a message with the alert count.
- **Category** — event category.
- **Severity** — information about severity level of a message that is displayed by a respective icon.
- **Severity level** — a numerical indicator of a message severity.
- **Security Gateway date** — date and time of a message specified in the time zone of a Security Gateway.
- **Host** — Security Gateway name.
- **Repeat Count**— how many times an event triggered.

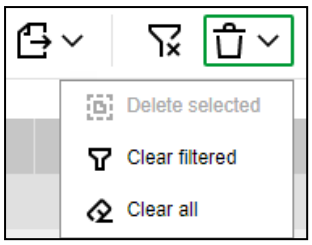
To filter events, use the following tags:

Tag	Description
severity:"level"	Filter messages by the required severity level
category:"text"	Filter messages by the required category
message:"text"	Filter messages by the required text
repeat_count:"numeral"	Filter messages by the required number of events
subject:"administrator"	Filter messages by the actions of the required administrator
hostname:"name"	Filter messages by the events on the required host
security_gateway:"name"	Filter messages by the events on the required Security Gateway

Clear a log

To clear a log:

1. Go to **Journals** and select the required log.
2. In the **Delete logs** drop-down list, select **Clear all**.



All logs will be deleted.

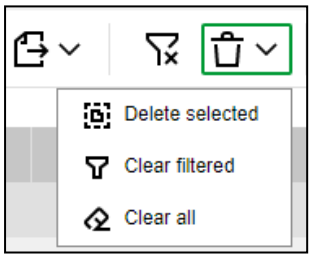
To remove entries on request:

1. Click to open the **Journals** menu.
2. Select the saved filter or create a new one with the required parameters.
3. In the **Delete logs** drop-down list, select **Clear filtered**.
4. The respective entries will be removed.

Note.
A log displays all entries by default. If no filter is applied, the **Clear filtered** command removes all entries in the log.

To remove selected entries:

1. Select the required entries.
2. Open the **Delete logs** drop-down-list.
   The **Delete selected** item becomes available.



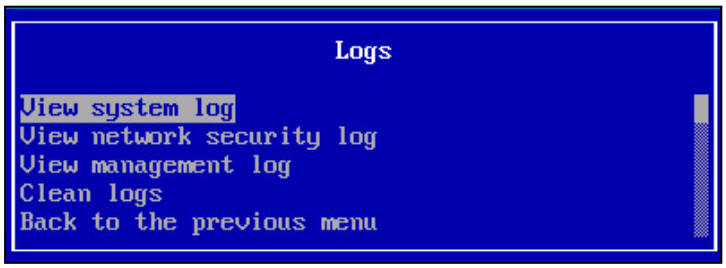
3. Select **Delete selected**.
   The selected entries will be removed.

Note.
To select all entries in the log, select an empty field in the table title.

View logs using the local menu

To work with logs in the local menu:

- In the **Main menu** of the local menu, select **Logs** and press **<Enter>**.
  The **Logs** menu appears as in the figure below.

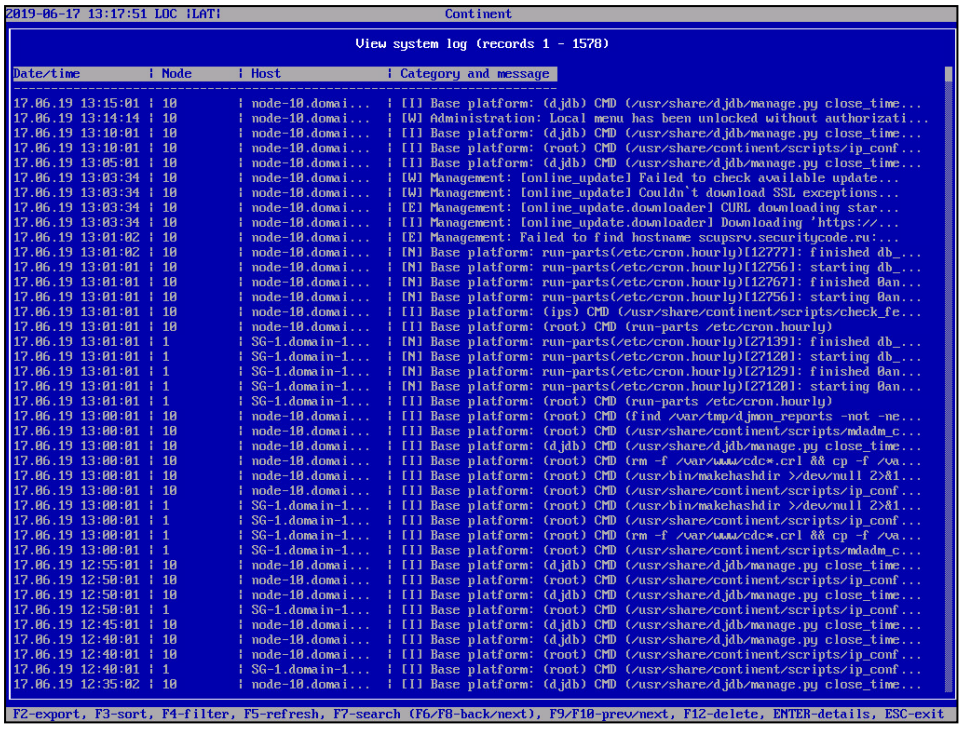


System log

To view a log:

- In the **Logs** menu, select **View system log** and press **<Enter>**.

The **View system log** dialog box appears.



This dialog box contains the list of all events saved in the log.

Each event has the following parameters:

- Date/time;
- Security Gateway
- Host;
- Event category and a message.

To move through the list, use the following keys: **<↑ >**, **<↓ >**, **<Page Down>**, **<Page up>**, **<Home>**.

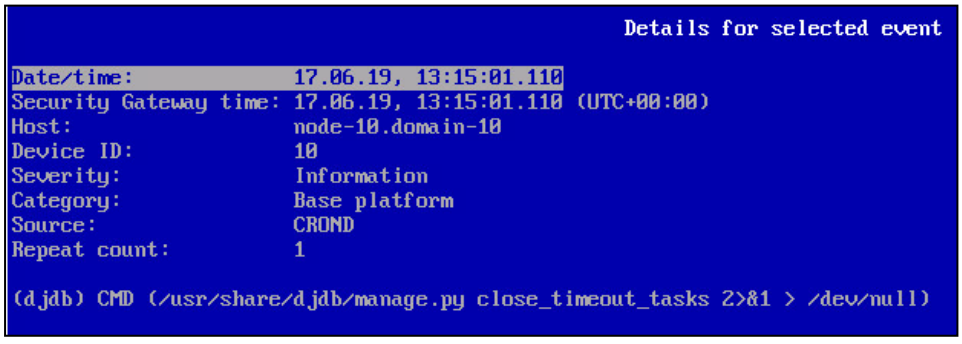
To refresh the list, press **<F5>**.

To return to the **Logs** menu, press **<Esc>**.

To view detailed information about an event:

1. Select the required event and press **<Enter>**.

   The **Details for selected event** menu appears.



   The detailed information includes the following:

   - Device ID;
   - Severity;
   - Source;
   - Full text of a message.

2. To return to the **View system log** dialog box, press **<Esc>**.

To search an event by text:

1. Press **<F7>**.

   The **Search** dialog box appears as in the figure below.

   Enter the required text and press **<Enter>**.

   The search by the required text starts. The search is performed down the list starting from the selected string.

   The first event that matches the searched text will be selected.

2. To continue searching for events with the specified text, press **<F8>**. You can also return to the previously found event. To do so, press **<F6>**.
3. To change the searched text, press **<F7>**, enter the new text and press **<Enter>**.

   The search begins down the list starting from the selected string.

   To change the search direction, press **<F6>**.

Filter the system log

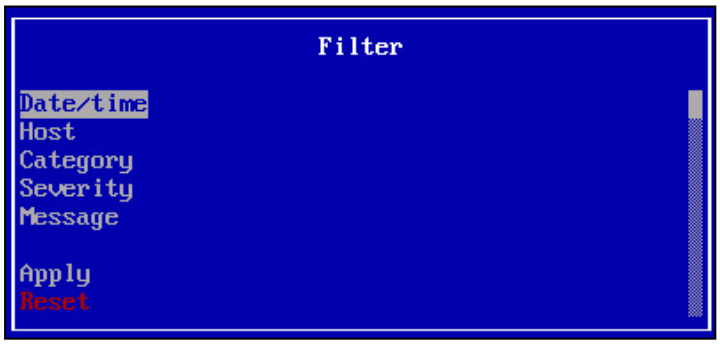
If you want to see only neccessary events in the **View system log** dialog box, use a filter that can be configured using the following parameters:

- Date/time;
- Host — event source;
- Category;
- Severity;
- Message.

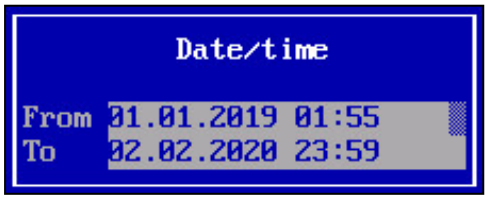
To configure a filter:

1. In the **View system log** dialog box, press **<F4>**.

   The **Filter** menu appears as in the figure below.

2. Select the required parameter, press **<Enter>** and set the required value.
   - To configure filtering by date and time, set the start and end of a time period as in the figure below.

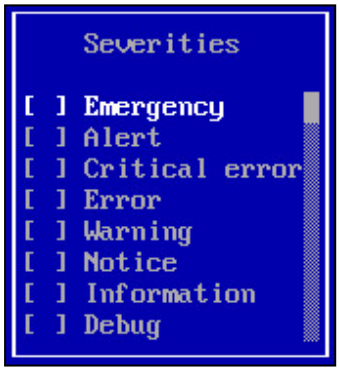
     

     Note.
     To move through text boxes, use <↑ >, <↓ >.

   - To configure filtering by hostname, enter the hostname or its part. You can use this filter to view Security Management Server logs that contain events from different Security Gateways.

- To configure filtering by category, select the required categories by pressing **<Space>**.

- To configure filtering by severity, select the required severity levels by pressing **<Space>**.



3. Press **<Enter>**.
   You are returned to the **Filter** menu.

> **Note.**
> After you configure filtering by one parameter, you can also configure it by another one. To do so, repeat steps **2** and **3**.

4. Select **Apply** and press **<Enter>**.
   The list of events contains only those messages that match the filtering parameters.
5. To resfresh the list, press **<F5>**.

> **Attention!**
> To disable filtering, reset filtering parameters.

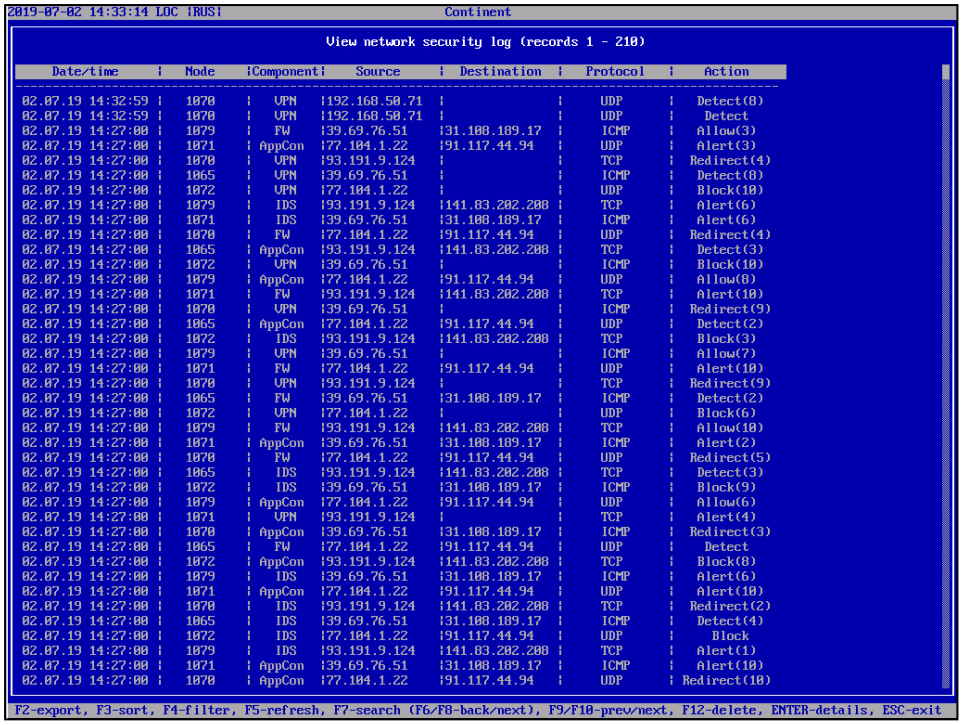
To reset filtering parameters:

1. In the **Filter** menu, select **Reset**.
2. Press **<Enter>**.

Network security log

To view a log:

- In the **Logs** menu, select **View network security log** and press **<Enter>**.
  The **View network security log** dialog box appears as in the figure below.



This dialog box contains the list of all events saved in the log.

The table heading contains a number of events per a certain time period (default time period is 10 seconds). Same events logged at the same time are displayed as one record.

Each event has the following parameters:

- Date/time;
- Node;
- Component;
- Source;
- Destination;
- Protocol;
- Action.

To move through the list, use the following keys: **<↑ >**, **<↓ >**, **<Page Down>**, **<Page up>**, **<Home>**.

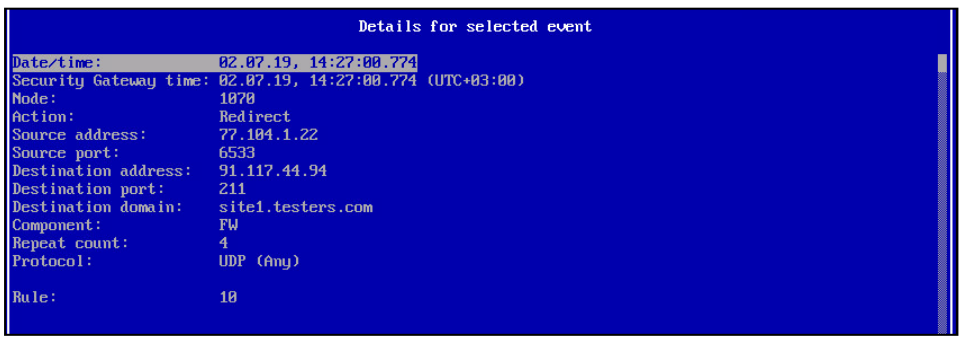
To refresh the list, press **<F5>**.

To return to the **Logs** menu, press **<Esc>**.

To view detailed information about an event:

1. Select the required event and press **<Enter>**.

   The **Details for selected event** menu appears.



   The detailed information includes the following:

   - Source address;
   - Source port;

- Destination address;
- Destination port;
- Protocol;
- Class;
- Signature ID;
- Signature description.

2. To return to the **View network security** log dialog box, press either **<Enter>** or **<Esc>**.

To search an event by signature:

1. Press **<F7>**.

   The **Search** dialog box appears as in the figure below.

   Enter the required signature text and press **<Enter>**.

   The search by the required signature text starts. The search is performed down the list starting from the selected string.

   The first event that matches the searched text will be selected.

2. To continue searching for events with the specified signature text, press **<F8>**. You can also return to the previously found event. To do so, press **<F6>**.
3. To change the searched text, press **<F7>**, enter the new signature text and press **<Enter>**.

   The search begins down the list starting from the selected string.

   To change the search direction, press **<F8>**.

Filter the network security log

To see required events in the **View system log** dialog box, use a filter that can be configured using the following parameters:

- Date/time;
- Security Gateway ID;
- Component.

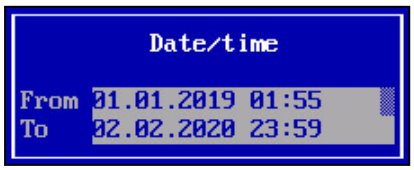
Note.
We recommend you use filtering by Security Gateway ID to view the Security Management Server log.

To configure a filter:

1. In the **View network security log** dialog box, press **<F4>**.

   The **Filter** menu appears as in the figure below.

2. Select the required parameter, press **<Enter>** and set the required value.
   - To configure filtering by date and time, set the start and the end of a time period as in the figure below.



Note.
To move through text boxes, use <↑ >, <↓ >.

- To configure filtering by Security Gateway ID, enter the ID or several IDs using comma (**,**).

- To configure filtering by Security Gateway components, select the required subsystems in the list by pressing **<Space>**.

3. Press **<Enter>**.
   You are returned to the **Filter** menu.

Note.
After you configure filtering by one parameter, you can also configure another. To do so, repeat steps **2** and **3**.

4. Select **Apply** and press **<Enter>**.
   The list of events contains only those messages that match the filtering parameters.
5. To refresh the list, press **<F5>**.

Attention!
To disable filtering, reset filtering parameters.

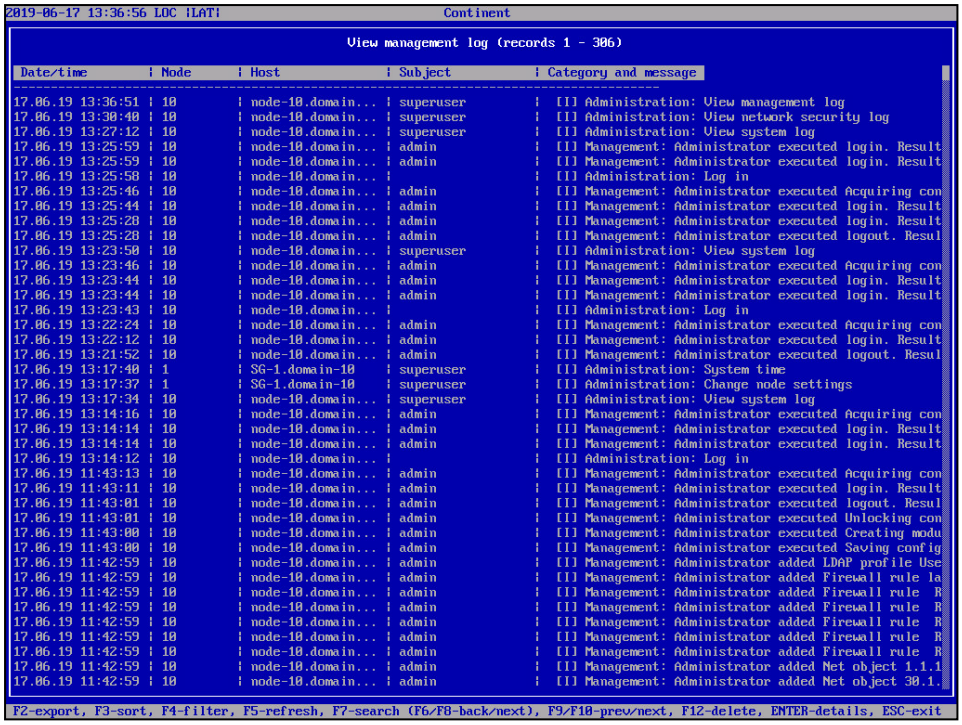
To reset filtering parameters:

1. In the **Filter** menu, select **Reset**.
2. Press **<Enter>**.

Management log

To view a log:

- In the **Logs** menu, select **View management log** and press **<Enter>**.
  The **View management log** dialog box appears.



This dialog box contains the list of all events saved in the log.

Each event has the following parameters:

- Date/time;
- Security Gateway;
- Host;
- Subject;
- Category and message.

To move through the list, use the following keys: **<↑ >**, **<↓ >**, **<Page Down>**, **<Page up>**, **<Home>**.

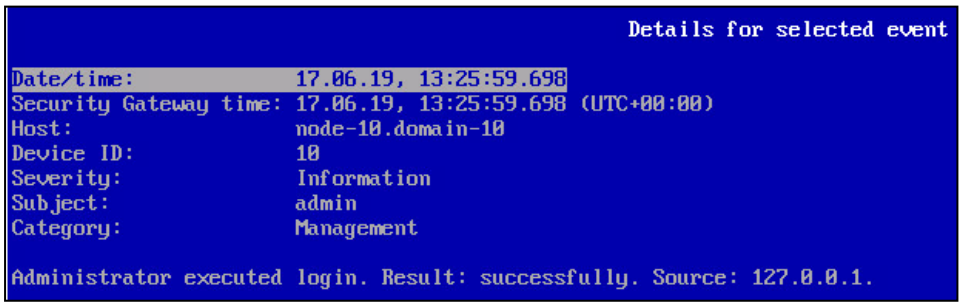
To refresh the list, press **<F5>**.

To return to the **Logs** menu, press **<Esc>**.

To view detailed information about an event:

1. Select the required event and press **<Enter>**.

   The **Details for selected event** menu appears.



   The detailed information includes the following:

   - Device ID;
   - Severity;
   - Full text of a message.

2. To return to the **View management log** dialog box, press **<Esc>**.

To search an event by text:

1. Press **<F7>**.

The **Search** dialog box appears as in the figure below.

Enter the required text and press **<Enter>**.

The search by the required text starts. The search is performed down the list starting from the selected string.

The first event that matches the searched text will be selected.

2. To continue searching for events with the specified text, press **<F8>**. You can also return to the previously found event. To do so, press **<F6>**.
3. To change the searched text, press **<F7>**, enter the new text and press **<Enter>**.

   The search begins down the list starting from the selected string.

   To change the search direction, press **<F8>**.

Filter the management log

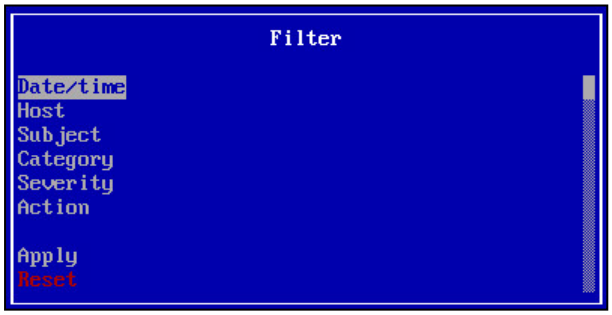
To see required events in the **View management log** dialog box, use a filter that can be configured using the following parameters:

- Date/time;
- Host — event source;
- Subject;
- Category;
- Severity;
- Message.

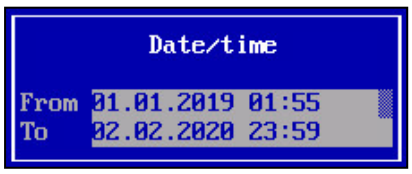
To configure a filter:

1. In the **View management log** dialog box, press **<F4>**.

   The **Filter** menu appears as in the figure below.



2. Select the required parameter, press **<Enter>** and set the required value.
   - To configure filtering by date and time, set the start and the end of a time period as in the figure below.



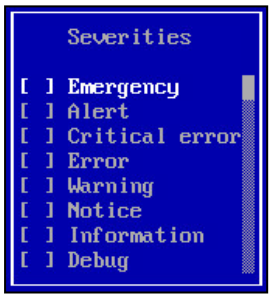
Note.
To move through text boxes, use <↑>, <↓>.

   - To configure filtering by hostname, enter the hostname or its part. You can use this filter to view Security Management Server logs that contain events from different Security Gateways.

- To configure filtering by hostname, enter the subject name or its part.

- To configure filtering by category, select the required categories by pressing **<Space>**.

- To configure filtering by severity, select the required severity levels by pressing **<Space>**.



3. Press **<Enter>**

   You are returned to the **Filter** menu.

> **Note.**
> After you configure filtering by one parameter, you can also configure another. To do so, repeat steps **2** and **3**.

4. Select **Apply** and press **<Enter>**.

   The list of events contains only those messages that match the filtering parameters.

5. To refresh the list, press **<F5>**.

> **Attention!**
> To disable filtering, reset filtering parameters.

To reset filtering parameters:

1. In the **Filter** menu, select **Reset**.
2. Press **<Enter>**.

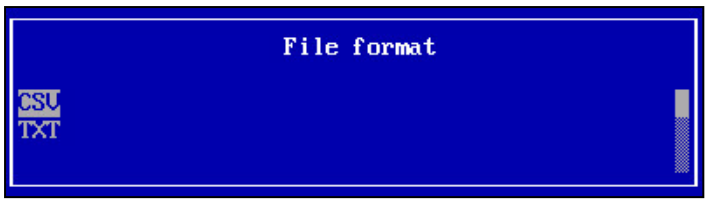
Export logs

You can export logs to an external drive using the local menu. Logs are saved to a USB drive in the **TXT** and **CSV** formats.

To export a log:

1. In the **Logs** menu, select the required log and press **<Enter>**.
2. If necessary, use log filtering.
3. Press **<F2>**.

   The **File format** dialog box appears as in the figure below.



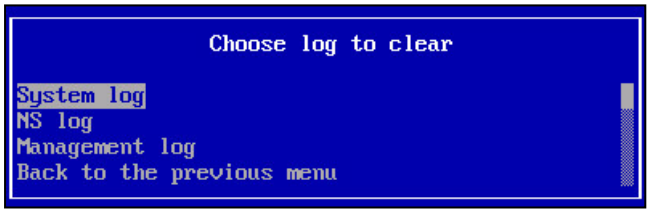
4. Select the required format and press **<Enter>**.
   You receive the **Insert USB Flash drive** message.
5. Insert an external drive and press **<Enter>**.
   Logs are exporting to the external drive. When the procedure is finished, you receive the **Success** message.
6. Remove the external drive and press **<Enter>**.
   You are returned to the list of events.

Clear logs

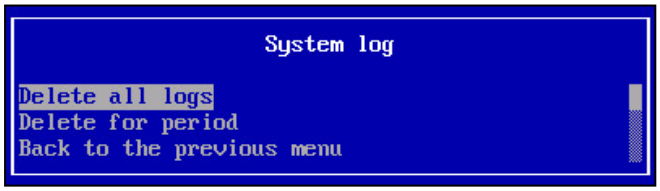
Logs can be cleared automatically, on schedule, fully, or by a specified time period. Automatic and scheduled clearing is configured using the Configuration Manager (see p. **53**). To clear logs fully or by a specified time period, use the local menu (see below).

To clear a log:

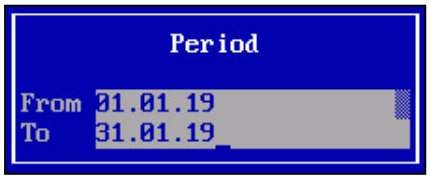
1. In the **Logs** menu, select **Clear logs** and press **<Enter>**.
   The **Choose log to clear** menu appears as in the figure below.



2. Select the required log and press **<Enter>**.
   The menu appears as in the figure below.

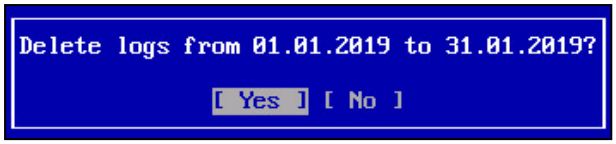


3. Select the required command and press **<Enter>**.
   - If you select **Delete all logs**, a dialog box asking you to confirm the procedure appears. Select **Yes** and press **<Enter>**.
   - Log clearing starts. When the procedure is finished, you receive the **Success** message.
   - If you select **Delete for period**, a dialog box appears as in the figure below.



   - set the start and the end of a time period and press **<Enter>**.

   The dialog box prompting you to confirm the procedure appears as in the figure below.



- Select **Yes** and press **<Enter>**.

Log clearing starts. When the procedure is finished, you receive the **Success** message.

4. Press **<Enter>**.

   You are returned to the **Choose log to clear** menu.

Note.
To delete filtered events, go to the required logs, apply the required filter, and press **<F12>**.

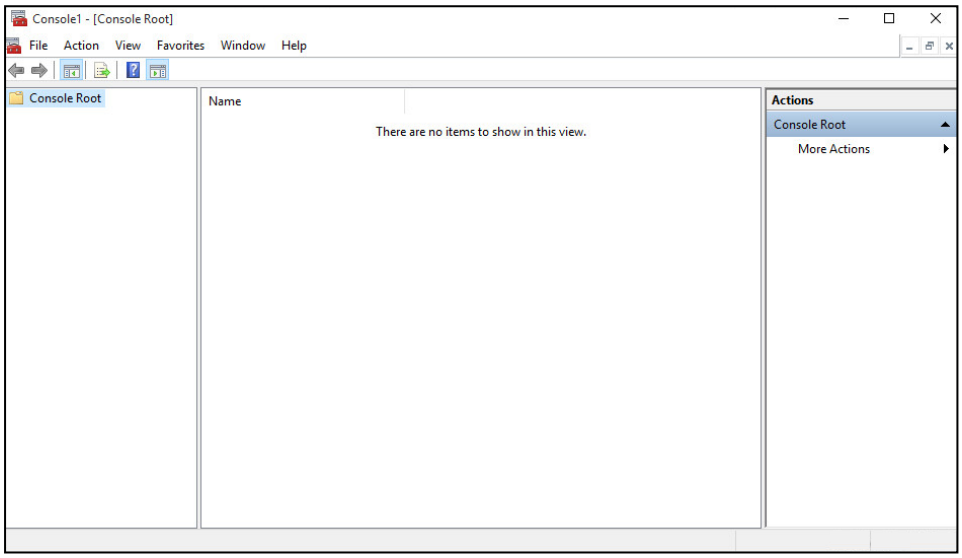
Appendix

Install a CRL certificate

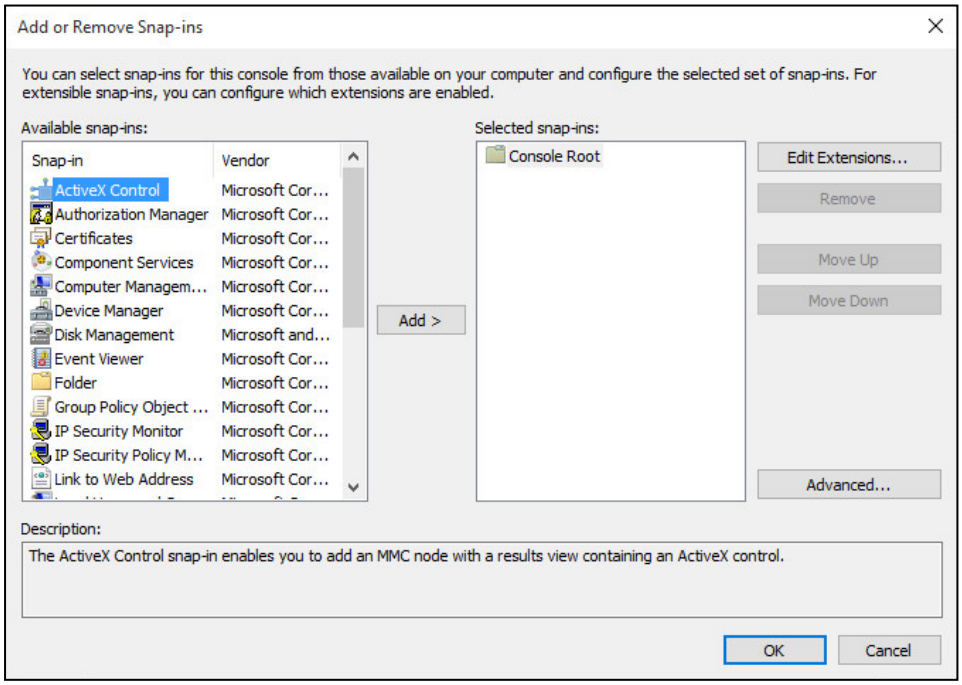
To install a CRL certificate on the Windows certificate store of the local computer, add the required snap-in and import a CRL file to trusted root certification authorities.

To add the Certificates snap-in using Microsoft Management Console:

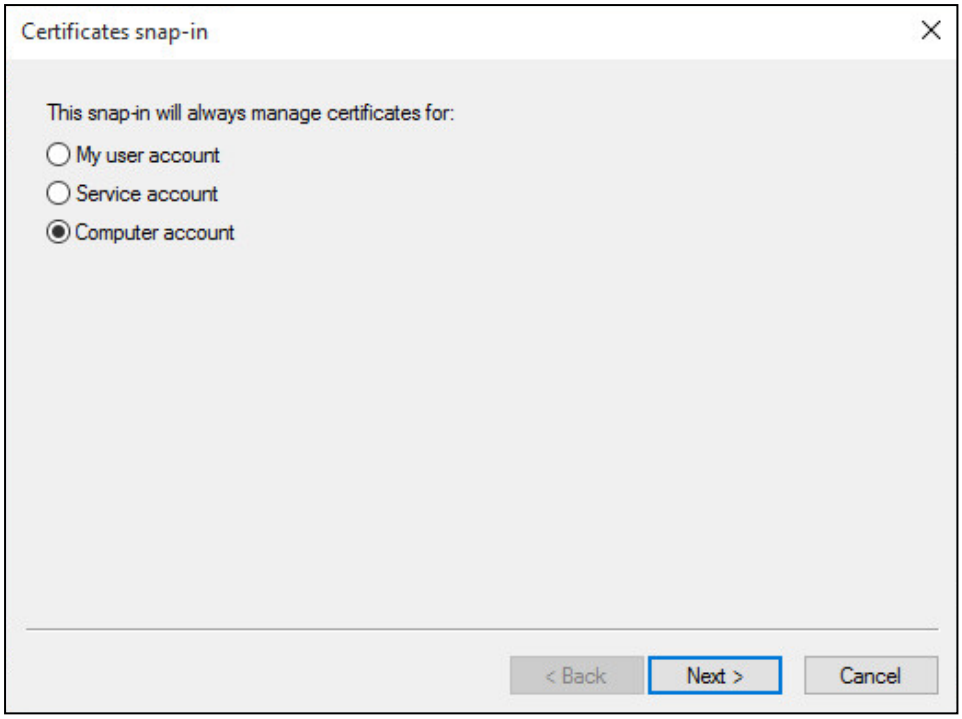
1. Click <**Win**>+<**R**>.
   The Windows **Run** dialog box appears.
2. Enter **mmc** and press <**Enter**>.
   Console Root appears as in the figure below.



3. On the toolbar, click **File** and select **Add/Remove Snap-in**.
   The **Add or Remove Snap-ins** dialog box appears.



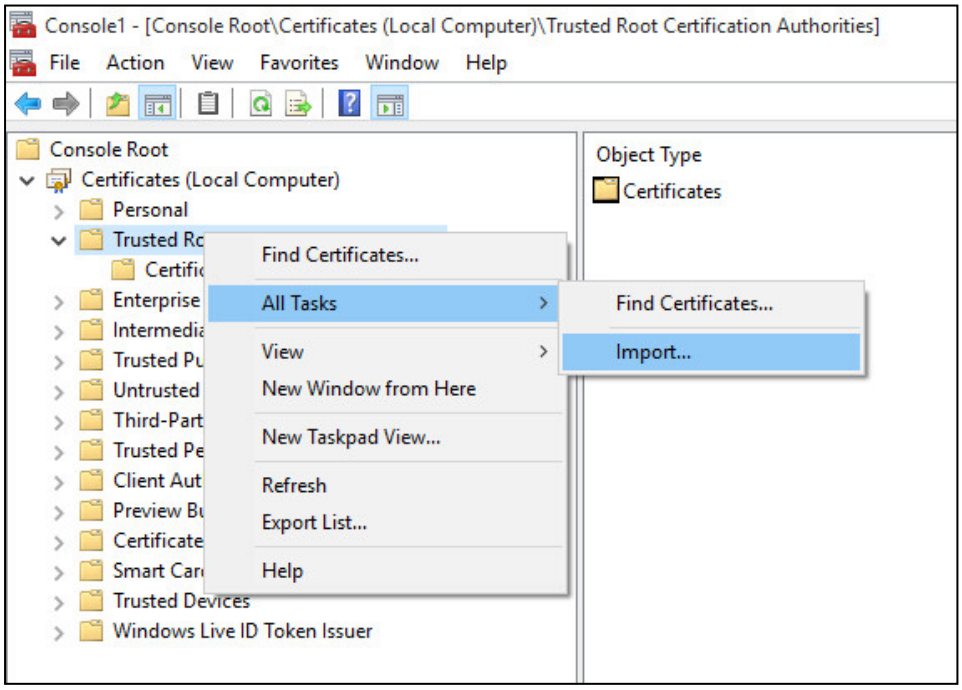
4. In the list of available snap-ins, select **Certificates** and click **Add**.
   The **Certificates snap-in** dialog box appears.



5. In the **Certificates snap-ins** dialog box, select **Computer account** and click **Next**.
6. In the **Select computer** dialog box, click **Finish**.
7. In the **Add or Remove Snap-ins** dialog box, click **OK**.
8. To view the certificate stores of the computer, double-click **Certificates (Local Computer)** in **Console Root**.
9. In the **File** menu, select **Save as**, specify the directory to save other CRL files imports and click **Save**.

To import a CRL file:

1. Open **Console Root** and expand the **Certificates** tree of the computer.
2. Right-click **Trusted Root Certification Authorities**.



3. Select **All tasks**, then click **Import**.
   The Certificate Import Wizard appears.

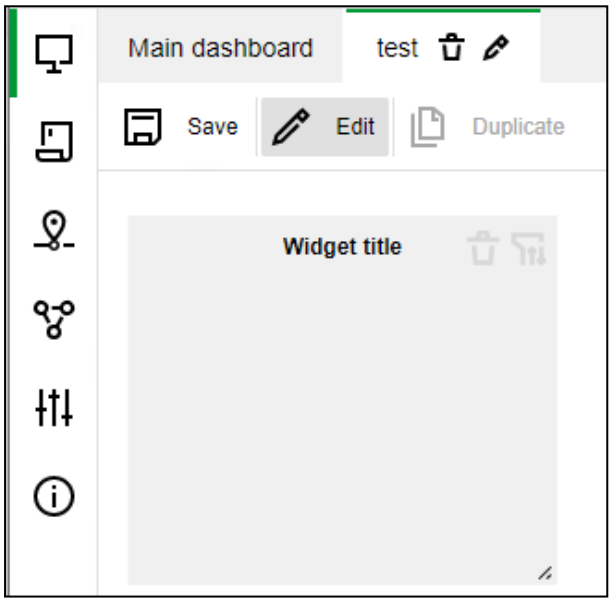
4. Click **Next**, then click **Browse...**.
5. In File Explorer, specify a file type and a path to the file.
6. Select the required file and click **Open**.
7. In the Certificate Import Wizard, click **Next**.
8. In the **Certificate Store** dialog box of the Certificate Import Wizard, select **Trusted Root Certification Authorities** and click **Next**.
9. In the Certificate Import Wizard, click **Finish**.

Configure widgets for VPN and Access Server

Widgets for VPN and Access Server display the state of the respective components on the Security Gateway.

To add a widget:

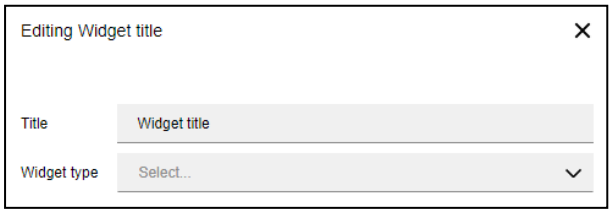
1. On the main page, on the navigation panel, click **Monitoring dashboard**.
2. Select the required tab or create one.
3. At the top of the **Main dashboard** page, click **Edit**.



The monitoring dashboard is in the **Edit** mode.

4. To add a new widget, click **Add widget**.
   A widget template appears as in the figure below.

5. To configure a widget, click in the top right corner.
   The **Editing Widget title** dialog box appears.



6. In the **Editing Widget title** dialog box, specify the following parameters:

Parameter	Contents
Title	Widget title. It is specified by a user and is displayed in the top left corner of the widget
Widget type	Table
Info type	Data
Info source	VPN or Access Server
Page size	The number of rows displayed on a single widget page. By default, it is 25

7. Select the required tunnels. To select all the tunnels and Access Servers, select the check box next to the search bar. To find the required tunnel, use the search bar.

Note.
If you select the check box net to the search bar, all the tunnels and Access Servers added will be automatically displayed in the widget.

8. For the **Access Server** widget in the **Show** drop-down list, select the required value. If you select **All servers**, all the Access Servers are displayed; if you select **Active only**, only active Access Servers are displayed.
9. To save widget configuration, click **Apply**.
10. When you have added all the required widgets, click **Save**.

    The dashboard configuration is saved.
11. To exit the **Edit** mode, click **Edit** again.

VPN widget

The **VPN** widget is a table with the list of tunnels selected in **Settings**. The table columns display the following information:

Parameter	Description
Tunnel state	Displays a tunnel state via green or red indicators. The green indicator — a tunnel is active, the red one — a tunnel is not available
Tunnel name	A tunnel name is formed from IDs of the Security Gateways connected by this tunnel
Tunnel counter	The counter of active and unavailable tunnels. The green part displays the number of active tunnels, the gray one — the number of unavailable ones
Download speed	In bits per second. It is the lowest value of the download speed on one Security Gateway and the upload speed on another Security Gateway
Upload speed	In bits per second. It is the lowest value of the upload speed on one Security Gateway and the download speed on another Security Gateway

Access Server widget

The Access Server widget consists of a table with the list of Access Servers and the **User sessions** button. The columns of the table display the following information:

Parameter	Description
Access Server state	Displays an Access Server state via green or red indicators. The green indicator — a server is active, the red one — a server is not available
Access Server name	The name of Security Gateway with an Access Server
Access Server counter	The counter of active and unavailable Access Servers. The green part displays the number of active Access Servers, the gray one — the number of unavailable ones
Connected	Displays active user sessions on an Access Server. The total number of user sessions for all the Access Servers selected while widget configuration is displayed next to the column header
Total	Displays the number of available licenses for an Access Server. The total number of available licenses for all Access Servers is displayed next to the column header

To view details about user sessions:

- Click the **User sessions** button.

  The **User sessions** dialog box contains the following information:

Parameter	Description
Show	A user session is displayed in two modes: **All servers** and **Servers of the widget**. In **Servers of the widget** mode, only user sessions selected while widget configuration are displayed. In **All servers** mode, all user sessions are displayed
Auto refresh	Allows you to automatically refresh the list of user sessions. The list of user sessions is refreshed once per five seconds
Force refresh	Allows you to manually refresh the list of user sessions. This parameter is not available if **Auto refresh** is enabled
Total	Counts active user sessions according to the filter configuration
Page size	The number of rows displayed on a single widget page. By default, it is 25
User	Displays the name of the user who initiated a connection to the Access Server. Allows you to filter the list of users
Access Server	The name of the Access Server to which a connection is initiated. To filter the list of Access Servers, use the search bar
Session	Contains the date, time of the user connection and the duration of sessions. The duration is specified in minutes

Documentation

1. Continent Enterprise Firewall. Version 4. Administrator guide. Basics.
2. Continent Enterprise Firewall. Version 4. Administrator guide. Deployment.
3. Continent Enterprise Firewall. Version 4. Administrator guide. Management.
4. Continent Enterprise Firewall. Version 4. Administrator guide. User Authentication.
5. Continent Enterprise Firewall. Version 4. Administrator guide. Networking functions.
6. Continent TLS Client. Setup and Operation.