

Continent Enterprise Firewall Version 4

Monitoring and Audit

Administrator guide



© SECURITY CODE LLC, 2024. All rights reserved.

All rights to operation manuals are reserved.

This document is shipped along with the product kit. It is covered by all terms of license agreement. You may not copy this document in printed or electronic form, in whole or part, or deliver it to third parties on commercial purpose without a special written consent of Security Code LLC.

Security Code LLC reserves the right to change the information contained herein without special notice.

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 a	bbreviations	. 5
Introdu	ction	. 6
Overvie		7
Overvie	Durposo and main functions	. /
	How monitoring works	. /
	How monitoring works	
		. /
	Groups of monitored objects	. /
	Pulos and tomplates	. /
	Object status	0 Q
	Run the Configuration Manager	. 0
Configu	re connection to the system	11
conngu	Configure connection using COST P 24 11 2012	
	Configure connection using GOSTR 34.11-2012	11
		.13
	Set up a configuration file of the Configuration Manager	15
Monitor	ing	.17
	Log on to the Monitoring and Audit system	.17
	Monitoring system main page	.17
	Monitoring dashboard	19
	Table widget	20
	Graph widget	. 21
	Structure widget	. 21
	Configure the monitoring dashboard	.21
	Statistics	24
	Widget management	.24
	View reports	25
	Prepare a report for printing	.25
	Monitoring modes	.27
	Structure	. 27
	Configure monitoring rules	. 28
	Domain	.31
	Security Gateway	. 32
	Security Gateway group	.40
	Cluster	.41
	Settings	.44
	Scheduled reports	. 45
	Configure e-mail notifications	.47
	Configure LLDP protocol	.49
	Restrict access to the Security Management Server	.49
Audit		51
	Log parameters	. 51
	Detalization level	52
	Store logs on an external syslog server	.52
	Configure automatic log clearing	.53
	Store logs in an external store	. 54
	View logs using the web interface	.57
	System log	. 57
	Network security log	. 58
	Management log	. 60
	Clear a log	. 60
	View logs using the local menu	61
	System log	. 61
	Network security log	. 64
	Management log	. 67
	Export logs	.70

Clear logs	71
Appendix	
Install a CRL certificate	
Configure widgets for VPN and Access Server	75
VPN widget	
Access Server widget	
Documentation	

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.

🖯 🗄 🗲 🗄		10.1.1.10 -	Continent. Configuration ma	anager		₽ ×
File Main View	urity Creation tser wizard	 ✓→ Reset sessions ◯ Reboot ◯ Shut down 	Confirm changes	Export Delete Refresh Pr	roperties Install Monitoring	Built-in administrator 🎮 🕜
Navigation Sec gateways	Security gateways (4) Search		Security gateway		Policy Application	م
Quick access toolbar	S Name ▲ Comp ♥ □ <td< td=""><td>onents</td><td>Configuration</td><td>Cluster - Synchronized</td><td>Certificate validity, days 350 350 350 350</td><td>Description</td></td<>	onents	Configuration	Cluster - Synchronized	Certificate validity, days 350 350 350 350	Description
	Navigation panel	Toolbar	Display area		350	
Access control CVPN CO IPS Structure Administration					(Status bar
*	•					▶ ₫ 10.1.1.10

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

The Configuration	Manager	window	contains t	he following	elements
The Configuration	manayer	window	contains ti	ne ionowing	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 (* 10.1.1.10) 				
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.

			10.1.1.10 - Continent	. Configuration manag	er		
Back Forward	Root certificate	Delete Refresh Properties Certificate					built-in administrator M
Navigation		▼ Certificates (2)					
👗 Adminis	trators	Search					Q
Roles	ites	Name	Issued by	Valid from	Valid to	Status	Description
Hoo	ot CAs			30.05.2017 13:34	30.05.2028 13:44	Valid	/O=??? ??? ???????????? /L=
🗐 🔂 Inte	ermediate CAs	Root_cert	Root_cert	18.01.2022 10:12	17.01.2027 10:12	Valid	/C=RU /O=SC /CN=Root_cert
LDAP Updates Backups Licenses Tasks Access contro UPN SIPS Structure Administratio	; ; ; ol	>>					
		* 4					
							C= 10.1.1.10

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.

- -						10.1.1.	10 - Continent.	Configuration man	lager				3 - 8 ×
File Mai	in View											Built-i	n administrator 🎮 🕜
Back Forw	vard Certificate	Request certificate	Import	∱ Export X Delete	9 Refresh	Properties							
Navigation		*	Certificate	es (4)	certificate								
👗 Adm	ninistrators		Search										م
Role	es tificates						Cer	tificate				Owner	
	Root CAs		Name			Issued I	ру	Valid from	Valid to	St	atus	Name	Source type
(Intermediate CAs		Control	l_cert		Root_ce	ert	18.01.2022 10:12	18.01.2023 1	0:12 Va	lid	📼 node-10	Security gateway
	Personal certifica	tes	Control	l_cert1		Root_ce	ert	18.01.2022 14:06	18.01.2023 1	4:06 Va	lid	🚥 node-11	Security gateway
Upd	lates		🕞 SG-1			Root_ce	ert	18.01.2022 14:38	18.01.2023 1	4:36 Va	ilid	🚥 SG-1	Security gateway
Back	kups		📑 SG-3			Root_ce	ert	18.01.2022 14:55	18.01.2023 1	4:54 Va	lid	📼 SG-3	Security gateway
Access of	ontrol												
ips 😥 Structure	e												
Administ	tration												
		*	4										
													▶ 🗲 10.1.1.10

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**.
- 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.

Root certificate			
Certificate owner data			
Common Name:			
Description:			
Organization:		Organization Unit:	
State:		Locality:	
Email:		Country:	RU
Key usage ———			
🔽 Digital signature	Data enciphement	CRL signing	
Non-repudiation	Key agreement	Encipher only	/
Key encipherment	Certificate signing	Decipher only	Y
Advanced			
Signature algorithm:	GOST 34.10-2012 (256) -	Valid to (UTC):	May /20/2024 12:30:34 *
		L	Create certificate Cancel

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.

ertificate				;
Certificate type: Secu	rity gateway	-		
Certificate owner dat Admin	nistrator			
User Enter data for the ne Author	antication portal			
Common Name: Acces	ss Server itv gateway			
Description: Web-	monitoring			
Organization:		Organization Unit:		
State:		Location:		
Email:		Country: RU		
Key usage				
Digital signature	Data enciphement	CRL signing		
Non-repudiation	🔽 Key agreement	Encipher only		
Key encipherment	Certificate signing	Decipher only		
Advanced				
Root certificate:	Root_cert			Ŧ
Signature algorithm:	GOST 34.10-2012 (256) 🔻	Valid to (UTC):	March /22/2023 15:17:55	5 -
Export to file:	SrvCert			
	Request file and key co	ntainer will be saved in the cer	tificate file directory	
		Crea	ate certificate Cance	

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**.

Security Gateway - node-11			
✓ Security Gateway	Server Certificates		1
Certificates		1.2	
Interfaces	Certricates of the security gateway and	a its components:	
Static Routes	Name	Issued by	Role Val
Dynamic Routes		Past ast	Coourity antourny 21
Multi-WAN		Hoot_cert	Security gateway 21.
Firewall			
 Logs and Alerts 			
Local Storage			
Databases			
Email Alerts			
DNS			
DHCP			
✓ SNMP			Þ
Hosts			
SNMP Trap	Root Certificates		
SSH	Trusted root certificates of the security	gateway:	O 🧪 🗙
✓ NetFlow	Name	Issued by	Valid from
Collectors Date and Time	רי הההההה הההההה און איני איני איני איני איני איני איני אינ	······	30.05.2017 13:34
Updates	Root_cert	Root_cert	15.11.2022 14:23
Monitoring			
Access to SMS			
	4		•
		ок с	ancel Apply

9. On the left, select Certificates.

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

The Install policy dialog box appears.

Sea	arch)
	Status		Name	Configuration	
	Online	¢	node-10	A 10153	
	🕑 Online	e	node-11	A 10146	
~	🕑 Online		SG-1	10169	
	🕑 Online		SG-2	A 10146	

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.

Settings		×
 Connections 10.1.1.10 	Connections to Security Management Server: Overview Advanced	
Cryptography 4 Environment Quick access toolbar	Pot: 444 Timeouts (seconds) Connection: 60 Data sending: 600 Initialization: 30 Data receiving: 600 Monitoring URL:	
•		
	OK Cancel	Apply

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.

Ξ	SYSTEM: 172	55 IDS: 0	0 0	MANAGEMENT: 341		ପ~ ^~
ŋ	System IDS Managem	ent 2			3	
<u>[</u>]	Auto refresh	- ע אר י	Records: 4130			≣ 7
<u></u>	Date	Security node	Device ID	Facility	lessages	Category
ę مو	1 2022 02:10:01.469	node-10	10	4	(root) CMD (/usr/share/contir	nent/scripts/ij Ба
141	2022 02:01:17.602	node-10	10	LOCAL3	10.1.1.131 [22/Sep/2022:0	09:01:17 +00 Ад
TI+	22.09.2022 02:01:01.620	SG-1	1	CRON	run-parts(/etc/cron.hourly)[32	248]: finishe Ба:
í	22.09.2022 02:01:01.614	SG-1	1	CRON	run-parts(/etc/cron.hourly)[32	229]: startin Ea:

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.

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 $[\mathfrak{S}]$.

To set up session parameters:

1. Click ^{▲~}.

In the drop-down list, select **Settings**.

- 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.

≡	SYSTEM:	172	55 IDS:	0 0	0	MANAGEMENT:	341		Q~	ペ∽
Ð	Main dashboard									+
IJ	🗐 Save 🌈	Edit 🖸 Dup	blicate							
<u></u>										*
9 . 9					Network Iface	s				
				In			Out			•
łtł	Security gate	Interface	State	Traffic	Traffic 1m	Speed 1m	Traffic	Traffic 1m	Speed 1m	
í	SG-1	ge-0-0	up	32.92 MB	11.64 kB	1.55 kbit/s	11.74 MB	2.48 kB	339 bit/s	
	SG-1	ge-1-0	down	0 B	0 B	0 bit/s	0 B	0 B	0 bit/s	

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.

Ð	Main dashboard test 🖞 🖉		+
IJ	Save 🖍 Edit 🕒 Duplicate		
<u>_</u>	Widget title	Widget title	
970			
ŧti		Add widget	
í		Add widget	
			1.

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.

÷	Widget title	ជំ Ⴅ
	Unsorted	node-1
domain-1 🕞		node-2
	Deleted	node-3

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.

Create new set of widgets						
Title:						
Widgets set name						
Wrong widget group name						
	Cancel					

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.

모	Main dashboard test 🖞 🌈			+
5	Save 🖍 Edit 🕒 Duplicate			
<u></u>	Widget title		Widget title	
~~				
łţt				
(i)			Add widget	
		4		1.

To configure a widget:

- In the display area, click et al.
 Now you can edit the dashboard elements.
- 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.

Editing Widg	Editing Widget title				
Title	Widget title				
Widget type	Graph	~			
Info type	Data	×			
Info Source	Monitoring	~			

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.

Editing Widget title		×
Title	Widget title	
Widget type	Table	~
Info type	Events	×
Info Source	System	~
Security node	Start typing	~
Severity	Start typing	~
Category	Start typing	~
Status	Started Finished	
Monitoring parameter	Start typing	~
Message		
	 Severity Date Nodes date 	
Columns	Security node Host Category Message	
Save Canc	el	

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

Configure the widget parameters and click Apply.
 A widget displays the values of the specified parameters.

- **6.** To resize a widget, use *i* 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.

	SYSTEM: 172 55 IDS: 0 0	0 MANAGEMENT: 352	ር~ ዲ~
돠	Predefined dashboard		+
Ŀ	Save 🖍 Edit 🖸 Print 🕂 Print settings Q Oper		
<u></u>	Top 15 faulty nodes	Top 10 attacks	ት ፲ ፲
9 . 9			
łtł		No data	
í	■ node-10 ■ node-11 ■ SG-1		
		<i>^</i>	4

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.

Saved reports				
Predefined dashboard				
Widgets count: 3 Creation date: 21.04.2023 15:42:44				
✓ widget_set_1 Current				
Widgets count: 1 Creation date: 21.04.2023 15:45:46				
Save Cancel				

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.

Predefined dashboard	test 🖞 🖉	
🗔 Save 🥟 Edit	Print +++ Print settings Q Open	Duplicate

- 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 む.

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.

		×
Print settings		•
Logo		
Title page		
Show page	Add title page	
Title of report		
Show date and time	Add date and time of report generation	
Page header		
Show header	Add page header	
Header text		
	Show list of avaliable macros	5
Page footer		
Show footer	Add page footer	
Footer text		
1 obtor toxt	Show list of avaliable macros	5
Widgets		
	Top 15 faulty nodes	
Show widgets	Top 10 attacks by countries	
	Number of attacks for the week	
		-
Save Ca	incel	

- 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 powerdemanding and slows down the Monitoring and Audit system.

Structure

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

Search in structure	TEMPLATE ACCI	ESS					
Searching	🖍 Edit 🕂 Add	🖉 Edit 🕂 Add 🗙 Cancel					Save
Structure <u>Edit</u>	∧ Own rules						Î
▼ BG domain-10	Name	Condition	State	Reason	Actions		
▼ ☐ Unsorted SG-1 ☐ node-10	CPU Temperature: critical	For temperature if temperature.cpu.now >= 80	critical	Security gateway %host%. CPU temperature: %value (temperature.cpu.n			
년 node-11 한 Deleted	CPU Temperature: warning	For temperature if temperature.cpu.now >= 65 and temperature.cpu.now < 80	warning	Security gateway %host%. CPU temperature: %value (temperature.cpu.n			

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.

Structure	<u>Edit</u>
🕶 🈫 domain-10	
✓ ☐ Unsorted	
G SG-1	
node-10	
node-11	
Deleted	

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.

\leftarrow	STATE	DETAILS	TEMPLATE	SETTINGS	ACCESS	FAILOVER	NEIGHB \rightarrow
ß	Edit 🕂	Add					

- 3. Select the Rules tab.
- **4.** To create a rule, click **Add**.

The **New rule** dialog box appears.

Rule -	New rule	
Name	New rule	
if	Condition 1	
	=	
	~	
	Select	\sim
	Add one more condition	
	critical	~
Then	Send e-mail	
	Select	\sim
For	Select	~
	host condition	
Reason	Enter reason	
Save	Cancel	-

- **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.

The name sho	e 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	

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:

Dulo	CPUL critical	
Rule -		
Name	CPU_critical	
if	Condition 1	
	cpu.load.avg1 (%) >= 🗸 90	
	cpu 🗸 load 🗸 avg1 🗸	
	Add one more condition	
	critical V	
Then	Send e-mail	
	Select 🗸	
For	cpu 🗸	
_	host condition threshold (cpu.load.avg1) value (cpu.load.avg1)	
Reason	%host%%value (cpu.load.avg1)%	
Save	Cancel	-

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:

- 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:

- 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 \times ^{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.

Se	arch in structure	DETAILS	TEMPLATE	ACCESS					
S	earching	🜈 Edit -	🜈 Edit 🕂 Add 🗙 Cancel						ive
Str	ucture <u>Edit</u>	∧ Cor	nmon rules						•
•	domain-10	Name	Con	dition	State	Reason	Actions		
	▼ 🗋 Unsorted	CPU Tem critical	perature: For if	r temperature	critical	Security gateway %host%. CPU temperature: %value			1
	. SG-1		ten >=	mperature.cpu.now : 80		(temperature.cpu.n			1
	한 node-10 한 node-11 한 Deleted	CPU Tem warning	perature: For if ten >= ten < 8	or temperature mperature.cpu.now 65 and mperature.cpu.now 80	warning	Security gateway %host%. CPU temperature: %value (temperature.cpu.n			ļ

To add a new rule, click Add.
 The New rule dialog box appears.

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.

Contacts	Rules	Access	Users sessions	All sensors
🗗 Expor	t into .txt	+† ‡ Exp	oort settings	
All Sec Security	curity gatew gateway	vays Clust	ters	
> • n	ode-1			
> • n	ode-2			
Clusters				

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.

Security gateway						
All by default	×).					
Confirm	Cancel					

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.

Active events			
Severity	Duration	Reason	
 critical 	19:42:46	Security gateway node-11. CPU temperature: 100C	

- **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.

CPU and Memory						
13% ram		0% swap	3% CPU	0°C temperature		
RAM						
used	1.80	GB (47%)				
free	2.06	GB (53%)				
used-buffers-cached	525.	71 MB (13%)				
free+buffers+cached	3.34	GB (87%)				
buffers	160.	72 MB (4%)				
cache	1.13	GB (29%)				
Total	3.86	GB				

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

Up 3%			Subsystems
Firewall log	Up yslog	3% log	Up Firewall

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

Hard disk drives			
0			
sda			
Hard drives partiti	ons		
38%	3%	20%	0%
Boot	Data	System	Temporary

Network interfaces

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

• Information about the state and statistics of network interfaces.

Network interfaces							
Interface	IP-address	MAC address	State	Received	Transmitted	In errors	Out errors
● ge-0-0	10.1.1.1/24	00:50:56:a9:7b:cb	up	113.53 MB	49.99 MB	0	0
• ge-1-0		00:50:56:a9:1c:82	down	0 B	0 B	0	0
• ge-2-0		00:50:56:a9:6c:ba	down	0 B	0 B	0	0

• Active network connections.

Active network connections								
Source			Destinatio	n				
Host	IP-address	Port	Host	IP-address	Port	Protocol	Start date	Duration
SG-1.domain-10	10.1.1.1	56988	cdc	10.1.1.10	6666	tcp	20.09.2022 02:37:20	6 days, 22:0
SG-1.domain-10	10.1.1.1	123	cdc	10.1.1.10	123	udp	20.09.2022 02:39:22	6 days, 22:0
SG-1.domain-10	10.1.1.1	46760	cdc	10.1.1.10	8888	tcp	27.09.2022 00:34:51	00:09:12

• Active VPN connections.

	Received traffic	Received traffic			Transmitted traffic			Errors		
Channel	Bytes	Speed	Packets per second	Bytes	Speed	Packets per second	In errors	Out errors	Masking errors	
1001	22.84 MB	83.72 kbit/s	13	25.13 MB	91.16 kbit/s	8	0	0	0	
1003	78.63 kB	317 bit/s	9	1.55 MB	6.17 kbit/s	5	0	0	0	

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.



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.

Contacts	Rules	Access	Users sessions	All sensors			
🔲 Save	🗔 Save 🖉 Cancel						
> Cont	> Contact (person)						
> Phor	> Phone						
> Mob	> Mobile phone						
> Skyp	> Skype						
> E-ma	> E-mail ①						
> E-ma	> E-mail for notifications ①						
> Infor	> Information						

To add contact information:

- **1.** Click the required line.
- 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.

Node settings		
Node monitoring	\checkmark	
Statistic interval	5 minutes	\sim
Inactivity timeout	Turn off	\sim
	✓ swap	
	✓ Ildp	
	 network 	
	dns_resolv	
	 multiwan 	
List of monitoring parameters:	✓ syslog	
	firewall	
	 temperature 	
	 filesystem 	
	🗸 сри	
	yinl 🖌	
	🖌 ram	

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
сри	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.

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

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.

Automatic update					
Security gateway	Chassis ID	Port ID	Port description	System name	
				_	
					•

DNS names IP addresses

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

Auto refresh						
Host	DNS-name	IP-address	Last update time	•		
	No	data				
					-	
			Кол-і	BO:	5	\sim

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: Auto refresh . 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: Autorefresh . 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** \bigcirc .
- 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 T 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

Lease started from	茴
Lease started before	茴
Lease ends from	茴
Lease ends before	茴

- **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 μ ARP proxy records for objects of the **Cluster** type structure. It is available only for individual Security Gateways in a cluster.

Auto refresh C 🔀 🖉 ARP-records editing mode				
Interface GW $~~ \updownarrow ~~ \bigtriangledown$	Host 💠 🍸	IP address 🛛 🌲 🍸	MAC address $\ \diamondsuit$	Record type
te-1-0	node-1	11.11.11.11	00:50:56:96:e1:95	dynamic
< 1 > 2	5 / page \vee			

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.

ping V IP address	Execute	Clear
Continent \$		

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.

Auto refresh	С	Table	0	~		
Route type	\$ 7	Destination	\$ 7	Next Gateway	\$ 7	Network device
-		10.10.10.0/24		-		te-0-0
-		11.11.11.0/24		-		te-1-0
-		12.12.12.0/24		-		te-2-0
-		13.13.13.0/24		-		te-3-0
broadcast		10.10.10.0		-		te-0-0
local		10.10.10.10		5 		te-0-0

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.

0	Auto refresh C Display for last, мin: 15 ∨ Proxy SSL inspection
>	Top domains
>	Top users by domain: domain-1
>	Top domains by user: Choose user

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 Proxy SSL inspection

Security Gateway group

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

DETAILS	TEMPLATE	ACCESS
De Edit	$+$ Add \times C	ancel

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 ctp.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.

De Edit	X Canoel	
Access Select of	o objects jects to which access will be granted e security gateways in subgroups	
	Access object	Administrators
	cluster-hw	audit_admin
	cluster01	audit_admin
	node-1000	audit_admin
	node-1001	audit_admin
	node-1002	audit_admin
н 4	1 2) H	
Admini	strators	
Select ad	ministrators that will have access to objects	
Access	Account	Role
	All administators	
	audit_admin (audit)	Audit administrator

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 DETAILS TEMPLATE ACCESS

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.

Severity	Duration	Reason
warning	00:00:29	Cluster SC has critical state
Critical		

• **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.

🔗 Edit	
Details	
Contact (person):	

To edit the information:

1. Click Edit.

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

Ø Edit	
Details	

- **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 \boxtimes .
- 6. Click Save.

Details		
Contact (person) -	Ivanov	×
Phone -	84995616364	×
E-mail for notifica	adminemail@com	×

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

Ţ	SMTP	WhoIs	Scheduled reports
Ŀ	🔲 Sav	e (2	Cancel Send test message
<u></u>			
Ŷ	Email S	Server S	Settings (SMTP)
+t+	Enable Em	nail Notific	tations
í	Server		182.12.12.12
	Port		587
	User		user@ourorg.ru
	Password		•••••
	Sender		usermail@ourorg.ru
	Security		No encryption Enable TLS

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 notifications 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.

× Scheduled report settings - New report

E-mail message settin	ngs
Message subject	
Recipients	user@domain.com
Send	Daily Weekly Monthly
	Time 12:00 (3)
Report settings	
Report name	New report O
Logo	+ Logo under 5 MB
Widgets	
	Widgets removed from Statistics will not be included in the report
Data	Last 24 hours
Page header	
	Available macros: page totalpages date datetime
Page footer	
	Available macros: page totalpages date datetime

- 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.

Security Gateway - node-10					×
 Security Gateway Certificates Interfaces Static Routes Dynamic Routes Multi-WAN 	Email Alerts Alert Policies Install policy Email Servers SMTP servers	ione: (i	<u> </u>		Off
Firewall Logs and Alerts Local Storage Databases	Server	Port	User	Sender	Connection security
Email Alerts DNS DHCP SNMP LLDP A NetFlow Collectors Date and Time Updates Monitoring SSH Access	Subscribers list: ①	Serve	er 1 No iten	Subject ns found.	Description
				ок	Cancel Apply

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.

Sender:		
Port:	587	
Connection security:	None *	
User:		
Password:		0

- 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 **O**.

The information about a destination appears.

Subscriber details		×
Email:		
SMTP Server:	smtp.gmail.com	Ŧ
Subject:		
Description:		
		OK Cancel

- 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.

Network Device Discovery		Off
Transmit interval:	30	seconds
Hold multiplier:	2	

The LLDP parameters become available for editing.

Security Gateway - SG-1			×
 Security Gateway Certificates 	Network Device Discover	/	On 🗮
Interfaces	Transmit interval:	30 seconds	
Static Routes Dynamic Routes	Hold multiplier:	2	
Multi-WAN	Event logging		
Firewall	Optional TLVS		
 Logs and Alerts Local Storage Databases DNS DHCP 	Port description System description Management address	✓ System name ✓ System capabilities	
SNMP			
LLDP	Specify interfaces for dis	covering network devices:	
⊿ NetFlow	Interface	Mode	
Collectors Date and Time SSH Access		1 No items found.	
		OK Ca	ncel Apply

- 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.
- 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.

urity Gateway - node-11			×
Security Gateway	Restricting access t	o the Security Management Server	On Con
Certificates	-		
Interfaces	The administrator co	onnects from this networks or hosts:	O 🗡 🗙
Static Routes			
Dynamic Routes	Name	Address/Mask	
Multi-WAN		 No items found. 	
Firewall			
Logs and Alerts			
Local Storage			
Databases			
Email Alerts			
DNS			
DHCP			
SNMP			
Hosts			
SNMP Trap			
SSH			
LLDP			
NetFlow			
Collectors			
Date and Time			
Updates			
Monitoring			
Access to SMS			
		ок	Cancel Apply

Access parameters become available for editing

4. Click **O**.

A dialog box for selecting network objects appears.

Netw	Network objects					
Se	Searching (Ctrl + E)					
		Name	Address	Mask	Description	
	₽	mk	192.168.1.40			
	뫄	test_net	192.168.1.0	27		
					OK Cancel	

- **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.
- Right-click the required Security Gateway and click Properties. The Security Gateway dialog box appears.
- 3. Go to Security Gateway | Logs and Alerts.

urity Gateway - node-10	_				
Security Gateway Certificates	Details				
Interfaces	Select log i	nfo detalization lev	el: High	• ①	
Static Routes	NAT data ti	meout.	E 1 00	anda	
Dynamic Routes		moode.	J * 50	contas	
Multi-WAN	External Logs	3			
Firewall					
 Logs and Alerts 	C 1		D .	D	
Local Storage	State	Address	Port	Protocol	Penod
Databases			🚹 No items fou	nd.	
Email Alerts					
DHCB					
SNMP					
LLDP					
✓ NetFlow					
Collectors					
Date and Time					1
Updates					
Monitoring					
SSH Access					
			OF	(Cancel	Apply

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.

				OX
State	Address	Port	Protocol	Period
	110.220.101.10	100	SYSLOG (TCP)	Always

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.

ame:					
escription					
ne					
et rule lifetime	ntervals: move pointe	er to appropriate day tim	e, press and hold left butt	on, then set interval.	
ou also can se	t time intervals using	keyboard in form startin	g time - ending time (some	intervals set using semico	lon ";"). Example:
):00-12:00; 15	:30-17:55				
0	6	12	18	24 Weekdays:	
Mo	<u> </u>	<u></u>		Monday	hh:mm - hh:mm
Ти				Tuesday	hh:mm - hh:mm
We				Wednesday	hh:mm - hh:mm
тh				Thursday	hh:mm - hh:mm
Fri				Friday	hh:mm - hh:mm
Sa				Saturday	hh:mm - hh:mm
Su				Sunday	hh:mm - hh:mm
me: 18:4	5				

- 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.

				OX
State	Address	Port	Protocol	Period
\checkmark	110.220.101.10	100	SYSLOG (TCP)	Always

- 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.

urity Gateway - node-11								
Security Gateway Certificates Interfaces Static Routes	Local Storage Store logs in th Daily log clear	ne local security gateway ning schedule:	database.					
Multi-WAN Firewall	Status 🔺	Log System	Start 23:00	Notify	Storage period (days) 365			
 Logs and Alerts 		Network security	23:00		365			
Local Storage		Management	23:00		365			
Email Alerts DNS DHCP SNMP Hosts SNMP Trap SSH LLDP NetFlow Collectors Date and Time Updates Monitoring Access to SMS	Start cleaning Save	when 50 * 10 *	% of logs	sk space is oc	ccupied			
						ОК	Cancel	Apply

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**.

Status	Log	Start	Notify	Storage period (days)
>	Management	23:00		365
\checkmark	System	23:00		365
	Network security	23:00		365

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.

- 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.

Security Gateway - node-10			×
✓ Security Gateway	Databases		On Con
Certificates			
Interfaces	Address:		Port: 5432
Static Routes	Database name:		
Dynamic Routes			
Multi-WAN	Usemame:		
Firewall	Password:		
⊿ Logs and Alerts			
Local Storage			
Databases			
Email Alerts			
DNS			
DHCP			
SNMP			
LLDP			
⊿ NetFlow			
Collectors			
Date and Time			
Updates			
Monitoring			
SSH Access			
		ОК	Cancel Apply

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.

Security Gateway	Databases	00
Certificates	Dalabases	
Interfaces	External Database	
Static Routes	Address:	Port: 5432
Dynamic Routes		
Multi-WAN	Database name:	
Firewall	Usemame:	
 Logs and Alerts 	Presward	
Local Storage	Fassword.	
Databases		
Email Alerts		
DNS		
DHCP		
SNMP		
LLDP		
⊿ NetFlow		
Collectors		
Date and Time		
Updates		
Monitoring		
SSH Access		

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**).

\equiv	SYSTEM: 176	59 IDS:	0 0	0 MANAGEMENT	405	ር~
Ţ	System IDS Manageme	ent				
<u> </u>	Auto refresh	∃~ \¥ ī	Records 8967	c.		≣ 7
8	Date	Security node	Device ID	Facility	Messages	Category
9 . 9	27.09.2022 05:52:21.753	node-10	10	LOCAL3	10.1.1.131 [27/Sep/2022:12:52:21 +	0000] "GET /ind
1+1	27.09.2022 05:52:21.533	node-10	10	LOCAL3	10.1.1.131 [27/Sep/2022:12:52:21 +	0000] "GET /ind
†I+	27.09.2022 05:52:21.529	node-10	10	LOCAL3	10.1.1.131 [27/Sep/2022:12:52:21 +	0000] "GET /ind
í	27.09.2022 05:52:01.943	node-10	10	LOCAL3	10.1.1.131 [27/Sep/2022:12:52:01 +	0000] "GET /ind

To create an event filter in a log:

- **1.** On the right, click \square .
- 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.

- 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.

Page size 25

To configure view of event parameters, click \blacksquare 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:

Тад	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.

Event details	
Security gateway (interface):	node-1065
Component:	AF
Last event date:	07.02.2019 12:45:10.844
Security gateway date:	07.02.2019 09:45:10.844 (UTC)
Source address:	192.168.10.2 : 49543
Destination port:	443
Destination domain:	site1.testers.com
Severity:	Notice
Details:	URL: https://site1.testers.com/favicon.ico HTTP method: GET MIME tipe: text/html
Action:	blocked
Alert counts:	1

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:

Тад	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:

Тад	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**.

ß	~	\x Ū~	
	(e)	Delete selected	
	V	Clear filtered	
	Q	Clear all	

All logs will be deleted.

To remove entries on request:

- **1.** Click T 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.

Logs	
<mark>View system log</mark> View network security log View management log Clean logs Back to the previous menu	

System log

To view a log:

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

The View system log dialog box appears.

2019-06-17 13:17:51	LOC LAT		Continent
		View	system log (records 1 - 1578)
Date∕time	l Node	l Host	Category and message
17.06.19 13:15:01	10	node-10.domai	[1] Base platform: (djdb) CMD (/usr/share/djdb/manage.py close_time
17.06.19 13:14:14	10	node-10.domai	[W] Administration: Local menu has been unlocked without authorizati
17.06.19 13:10:01	10	node-10.domai	[I] Base platform: (djdb) CMD (/usr/share/djdb/manage.py close_time
17.06.19 13:10:01	10	node-10.domai	[[]] Base platform: (root) CMD (/usr/share/continent/scripts/ip_conf
17.06.19 13:05:01	10	i node-10.domai	i III Base platform: (djdb) CMD (/usr/share/djdb/manage.py close_time
17.06.19 13:03:34	i 10	i node-10.doma1	i IWJ Management: Ionline_updateJ Failed to check available update
17.00.17 13:03:31	1 10	i node-10.domai	I IWI Management: Ionline_updated Countant download SSL exceptions
17.00.15 13.03.31	1 10	1 node-10.domai	1 III Management: [online_update.downloader] Cont downloading 'https://
17 06 19 13:01:02	10	: node-10 domai	[IF] Management: Failed to find hostname scupsru securitucode ru:
17.06.19 13:01:02	10	i node-10.domai	[[N] Base platform: run-parts(zetczcron.hourlu)[12272]; finished dh
17.86.19 13:81:81	10	1 node-10.domai	[N] Base platform: run-parts(/etc/cron.hourlu)[12756]; starting db
17.06.19 13:01:01	10	node-10.domai	[N] Base platform: run-parts(/etc/cron.hourlu)[12767]: finished Ban
17.06.19 13:01:01	10	node-10.domai	[[N] Base platform: run-parts(/etc/cron.hourly)[12756]: starting @an
17.06.19 13:01:01	10	node-10.domai	[1] Base platform: (ips) CMD (/usr/share/continent/scripts/check_fe
17.06.19 13:01:01	10	node-10.domai	[1] Base platform: (root) CMD (run-parts /etc/cron.hourly)
17.06.19 13:01:01	1 1	SG-1.domain-1	[N] Base platform: run-parts(/etc/cron.hourly)[27139]: finished db
17.06.19 13:01:01	1 1	SG-1.domain-1	I [N] Base platform: run-parts(/etc/cron.hourly)[27120]: starting db
17.06.19 13:01:01	1 1	SG-1.domain-1	I [N] Base platform: run-parts(/etc/cron.hourly)[27129]: finished @an
17.06.19 13:01:01	11	SG-1.domain-1	[N] Base platform: run-parts(/etc/cron.hourly)[27120]: starting @an
17.06.19 13:01:01	11	SG-1.domain-1	[I] Base platform: (root) CMD (run-parts /etc/cron.hourly)
17.06.19 13:00:01	10	node-10.domai	[[1] Base platform: (root) CMD (find /var/tmp/djmon_reports -not -ne
17.06.19 13:00:01	10	node-10.domai	IIII Base platform: (root) CMD (/usr/share/continent/scripts/mdadm_c
17.05.19 13:00:01	10	i node-10.domai	i III Base platform: (djdb) UMD (/usr/share/djdb/manage.py close_time
17.05.19 13:00:01	i 10	i node-10.doma1	i III Base platform: (root) UMD (rm -f /var/www/cdc*.cri aa cp -f /va
17.00.17 13:00:01	1 10	i node-10.domai	1 [1] Dase platform: (root) CrD (/usr/bln/makenasnair //aev/null 2/α]
17.00.15 13.00.01	1 10	SC 1 down in 1	III base platform: (rout) (ib (/usi/sin/r/continent/scripts/ip_cont
17.00.13 13.00.01	1 L 1 1	! SG-1 domain-1	<pre>1 [1] Dase platform: (root) CMD (/usr/bln/makenashulr //ucv/null 2/al ! [1] Base platform: (noot) CMD (/usr/blane/continent/scripts/in conf</pre>
17 86 19 13:80:81	! 1	: SG-1 domain-1	[1] Base platform: (root) CMD (rm -f /uar/umu/cdc* crl && cn -f /ua
17.06.19 13:00:01	i î	SG-1.domain-1	[1] Base platform: (root) CMD (/usr/share/continent/scripts/mdadm c
17.06.19 12:55:01	10	node-10.domai	[[1] Base platform: (didb) CMD (/usr/share/didb/manage.pu_close time
17.06.19 12:50:01	10	node-10.domai	[[1] Base platform: (root) CMD (/usr/share/continent/scripts/ip conf
17.06.19 12:50:01	10	node-10.domai	[1] Base platform: (djdb) CMD (/usr/share/djdb/manage.py close time
17.06.19 12:50:01	1	SG-1.domain-1	[1] Base platform: (root) CMD (/usr/share/continent/scripts/ip_conf
17.06.19 12:45:01	10	node-10.domai	[1] Base platform: (djdb) CMD (/usr/share/djdb/manage.py_close_time
17.06.19 12:40:01	10	node-10.domai	[1] Base platform: (djdb) CMD (/usr/share/djdb/manage.py close_time
17.06.19 12:40:01	10	node-10.domai	[1] Base platform: (root) CMD (/usr/share/continent/scripts/ip_conf
17.06.19 12:40:01	1 1	SG-1.domain-1	I []] Base platform: (root) CMD (/usr/share/continent/scripts/ip_conf
17.06.19 12:35:02	10	node-10.domai	[]] Base platform: (djdb) CMD (/usr/share/djdb/manage.py close_time
R2 (R2 (R4 0/14	DE Col DE	

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.

	Details for selected event
Date/time:	17.06.19, 13:15:01.110
Security Gateway time:	17.06.19, 13:15:01.110 (UTC+00:00)
Host:	node-10.domain-10
Device ID:	10
Severity:	Information
Category:	Base platform
Source:	CROND
Repeat count:	1
(djdb) CMD (/usr/share/	′djdb/manage.py close_timeout_tasks 2>&1 > /dev/null)

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.

Search					
String					

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.

	Filter	
Date∕time Host Category Severity Message		
Apply Reset		

- 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 $<\uparrow >, <\downarrow >$.

• 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.

	Host
Name	

• 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.

01 02 11:33:11 10	-Thua1			CONTINENT		
View network security log (records 1 - 218)						
Date/time	Node	Componen	ti Source	Destination	Protocol	Action
N7.19 14:32:59 1	1070	I UPN	1192.168.50.71		IIDP	Detect(8)
N7.19 14:32:59	1979	I UPN	1192.168.59.71		LIDP	Detect
N7 19 14:27:00 1	1979	I FU	139 69 76 51	31 108 189 17	ICMP	1 Allow(3)
N7 19 14:27:00 1	1971	AnnCon	177 104 1 22	191 117 44 94	LINP	Alert(3)
07 19 14:27:00	1070	I IPN	193 191 9 124	1	TCP	: Redirect(4)
07 19 14:27:00	1965	I LIPN	139 69 76 51		TCMP	: Detect(8)
07 19 14 27 00 1	1972	1 LIPN	100.000.001		LIDP	! Block(10)
07 19 14 27 00 1	1070	1 102	102 101 0 124	1141 02 202 200	TCP	l Alent(6)
07 19 14·27·00	1971	1 105	139 69 76 54	131 108 189 17	ICMP	l Alert(6)
07 19 14·27·00 1	1070	1 FLI	177 104 1 22	191 117 44 94	IIDP	Redirect(4)
07 19 14 27 00 1	1965	! AnnCon	193 191 9 124	141 83 202 208	TCP	! Detect(3)
01.10 11.27.00	1003	г прреол	100 60 76 51	1111.03.202.200	TCMP	Plock(10)
07 40 44 27 00 1	1076		133.03.10.31	101 117 44 04		
07.13 14.27.00 1	1075	т нррсон	102 404 0 424	171.117.44.74	UUF	
07.13 14.27.00 1	1071	I FW	100.00.70.54	1141.03.202.200	ICF	
07.19 14:27:00 i	1070	i OPM	139.69.76.51	i 104 447 44 04	IUND	i Kedirect(9)
07.19 14:27:00 1	1000	i HppCon	102 404 0 424	131.117.44.34	UDP	i Detect(2)
07.13 14:27:00 1	1072	1 105	100.00.76.54	1141.03.202.200	ICF	i BIOCK(J)
07.13 14:27:00 1	1075	i Orn	137.07.70.31	104 447 44 04	ICFIF	
07.19 14:27:00 i	1071	i IW	i77.109.1.22	191.117.44.94	UUP	i Hiert(10)
.07.19 14:27:00 1	1070	i UPN	193.191.9.124		TUP	Redirect(9)
.07.19 14:27:00 1	1065	FW	139.69.76.51	131.108.189.17	ICHP	i Detect(2)
.07.19 14:27:00 1	1072	I UPN	177.104.1.22		UDP	Block(6)
.07.19 14:27:00 1	1079	i FW	193.191.9.124	1141.83.202.208	TCP	Allow(10)
.07.19 14:27:00 1	1071	l AppCon	139.69.76.51	131.108.189.17	ICMP	Alert(Z)
07.19 14:27:00	1070	i FW	177.104.1.22	191.117.44.94	UDP	Redirect(5)
07.19 14:27:00	1065	I IDS	193.191.9.124	1141.83.202.208	TCP	i Detect(3)
07.19 14:27:00	1072	IDS	139.69.76.51	131.108.189.17	ICMP	Block(9)
07.19 14:27:00	1079	l AppCon	177.104.1.22	191.117.44.94	UDP	Allow(6)
.07.19 14:27:00	1071	T UPN	193.191.9.124		TCP	Alert(4)
.07.19 14:27:00	1070	l AppCon	139.69.76.51	131.108.189.17	ICMP	Redirect(3)
07.19 14:27:00	1065	FW	177.104.1.22	191.117.44.94	UDP	l Detect
.07.19 14:27:00	1072	l AppCon	193.191.9.124	141.83.202.208	TCP	i Block(8)
07.19 14:27:00	1079	IDS	139.69.76.51	131.108.189.17	ICMP	Alert(6)
.07.19 14:27:00	1071	l AppCon	177.104.1.22	191.117.44.94	UDP	Alert(10)
.07.19 14:27:00	1070	I IDS	193.191.9.124	1141.83.202.208	TCP	Redirect(2)
.07.19 14:27:00	1065	I IDS	139.69.76.51	131.108.189.17	ICMP	Detect(4)
07.19 14:27:00	1072	I IDS	177.104.1.22	191.117.44.94	UDP	l Block
07.19 14:27:00	1079	I IDS	193.191.9.124	1141.83.202.208	TCP	Alert(1)
07.19 14:27:00	1071	l AppCon	139.69.76.51	131.108.189.17	ICMP	Alert(10)
07.19 14:27:00	1070	l AppCon	177.104.1.22	191.117.44.94	UDP	Redirect(10)

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.

Details for selected event			
Date/time:	02.07.19, 14:27:00.774		
Security Gateway time:	02.07.19, 14:27:00.774 (UTC+03:00)		
Node:	1070		
Action:	Redirect		
Source address:	77.104.1.22		
Source port:	6533		
Destination address:	91.117.44.94		
Destination port:	211		
Destination domain:	site1.testers.com		
Component:	FW		
Repeat count:	4		
Protocol:	UDP (Any)		
Rule:	18		

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.

Search				
String				

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.

- 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>.
- 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.

Filter	
<mark>Date∕time</mark> Node Component	•
Apply	

- 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 $<\uparrow >, <\downarrow >$.

• 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>**.

Component	
	I IDS I UPN I FW I AF I AppCon I NBA

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.

Date/time I 7.86.19 13:36:51 I 7.86.19 13:32:59 I 7.86.19 13:22:59 I 7.86.19 13:22:59 I 7.86.19 13:22:59 I 7.86.19 13:22:58 I 7.86.19 13:22:54 I 7.86.19 13:22:24 I 7.86.19 13:22:24 I 7.86.19 13:22:36 I 7.86.19 13:22:36 I 7.86.19 13:22:44 I 7.86.19 13:22:46 I 7.86.19 13:22:46 I 7.86.19 13:22:46 I 7.86.19 13:22:41 I 7.86.19 13:22:41 I 7.86.19 13:22:43 I 7.86.19 13:22:43 I 7.86.19 13:22:43 I 7.86.19 13:22:12 I	Node 19 19 10 10 10 10 10 10 10 10	View management log i Host i Subject i node-18.domain superuser i mode-18.domain superuser i mode-18.domain superuser i mode-18.domain admin i mode-18.domain admin i mode-18.domain i admin	I Category and message I [1] Administration: View management log I [1] Administration: View metwork security log I [1] Administration: View system log I [1] [1] [1] [1] [1] [1] [1] [1] [1] [1]
Date×time I 7.06.19 13:36:51 1 7.06.19 13:38:40 1 7.06.19 13:28:59 1 7.06.19 13:25:59 1 7.06.19 13:25:55 1 7.06.19 13:25:55 1 7.06.19 13:25:54 1 7.06.19 13:25:26 1 7.06.19 13:25:28 1 7.06.19 13:25:28 1 7.06.19 13:23:40 1 7.06.19 13:23:44 1 7.06.19 13:23:44 1 7.06.19 13:23:44 1 7.06.19 13:23:44 1 7.06.19 13:23:44 1 7.06.19 13:23:41 1 7.06.19 13:22:41 1 7.06.19 13:22:43 1 7.06.19 13:22:43 1 7.06.19 13:22:43 1 7.06.19 13:22:43 1	Node 18 19 19 19 10 10 18 19 19 19	I Host I Subject I mode-10.domain i superuser I mode-10.domain i superuser I mode-10.domain i superuser I mode-10.domain i admin I mode-10.domain i admin I mode-10.domain i	i Category and message I [1] Administration: View management log I [1] Administration: View network security log I [1] Administration: View system log I [1] Management: Administrator executed login. Result
7, 86, 19, 13; 36; 51, 1 7, 86, 19, 13; 38; 48, 1 7, 86, 19, 13; 25; 59, 1 7, 86, 19, 13; 25; 59, 1 7, 86, 19, 13; 25; 59, 1 7, 86, 19, 13; 25; 54, 1 7, 86, 19, 13; 25; 24, 1 7, 86, 19, 13; 25; 24, 1 7, 86, 19, 13; 25; 24, 1 7, 86, 19, 13; 22; 24, 1 7, 86, 19, 13; 23; 34, 6 7, 86, 19, 13; 23; 34, 6 7, 86, 19, 13; 23; 34, 4 7, 86, 19, 13; 22; 34, 4 7, 86, 19, 14, 19, 14, 14, 14, 14, 14, 14, 14, 14, 14, 14	10 10 10 10 10 10 10 10 10	<pre>i node-18.domain; superuser i node-18.domain; superuser i node-18.domain; superuser i node-18.domain; admin i node-18.domain; admin i node-18.domain;</pre>	: [1] Administration: View management log [[1] Administration: View network security log [[1] Administration: View system log [[1] Management: Administrator executed login. Result
$\begin{array}{c} 7, 86, 19 \\ 31, 227; 12 \\ 7, 86, 19 \\ 31, 227; 12 \\ 7, 86, 19 \\ 31, 225; 59 \\ 7, 86, 19 \\ 31, 225; 58 \\ 7, 86, 19 \\ 31, 225; 58 \\ 7, 86, 19 \\ 31, 225; 36 \\ 7, 86, 19 \\ 31, 225; 36 \\ 7, 86, 19 \\ 31, 225; 36 \\ 7, 86, 19 \\ 31, 225; 36 \\ 7, 86, 19 \\ 31, 225; 36 \\ 7, 86, 19 \\ 31, 223; 36 \\ 16 \\ 7, 86, 19 \\ 31, 223; 36 \\ 16 \\ 7, 86, 19 \\ 31, 223; 46 \\ 16 \\ 7, 86, 19 \\ 31, 223; 46 \\ 16 \\ 7, 86, 19 \\ 31, 223; 46 \\ 16 \\ 7, 86, 19 \\ 31, 223; 44 \\ 17, 86, 19 \\ 31, 223; 44 \\ 17, 86, 19 \\ 31, 223; 41 \\ 18 \\ 18 \\ 18 \\ 18 \\ 18 \\ 18 \\ 18 \\$	10 10 10 10 10 10 10 10	I node-10.domain I superuser I node-10.domain I superuser I node-10.domain I admin I node-10.domain I admin I node-10.domain I	[1] Administration: View network security log [1] Administration: View system log [1] Management: Administrator executed login. Result
$\begin{array}{c} 7. \ 66. \ 19 \ 13:22:12 \\ 7. \ 66. \ 19 \ 13:25:59 \\ 7. \ 66. \ 19 \ 13:25:59 \\ 7. \ 66. \ 19 \ 13:25:59 \\ 7. \ 66. \ 19 \ 13:25:36 \\ 7. \ 66. \ 19 \ 13:25:36 \\ 7. \ 66. \ 19 \ 13:25:28 \\ 7. \ 66. \ 19 \ 13:25:28 \\ 7. \ 66. \ 19 \ 13:22:36 \\ 7. \ 66. \ 19 \ 13:22:36 \\ 7. \ 66. \ 19 \ 13:22:36 \\ 7. \ 66. \ 19 \ 13:22:36 \\ 7. \ 66. \ 19 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 10 \ 13:22:34 \\ 7. \ 66. \ 7. \ 7. \ 7. \ 7. \ 7. \ 7. $	10 10 10 10 10 10 10	i node-10.domain i superuser i node-10.domain i admin i node-10.domain i admin i node-10.domain i	[1] Administration: View system log [1] Management: Administrator executed login. Result
$\begin{array}{c} 7, 86, 19 \\ 3125; 59 \\ 7, 86, 19 \\ 3125; 55 \\ 7, 86, 19 \\ 3125; 55 \\ 7, 86, 19 \\ 3125; 54 \\ 7, 86, 19 \\ 3125; 54 \\ 7, 86, 19 \\ 3125; 22 \\ 10 \\ 10 \\ 10 \\ 10 \\ 10 \\ 10 \\ 10 \\$	10 10 10 10 10 10	node-10.domain admin node-10.domain admin node-10.domain	[1] Management: Administrator executed login. Result
7, 86, 19, 13;25;59, 7, 86, 19, 13;25;46, 7, 86, 19, 13;25;46, 7, 86, 19, 13;25;46, 7, 86, 19, 13;25;27, 7, 86, 19, 13;25;28, 7, 86, 19, 13;25;28, 7, 86, 19, 13;23;46, 7, 86, 19, 13;23;44, 7, 86, 19, 13;22;24, 7, 86, 19, 13;22;24, 7, 86, 19, 13;22;24, 7, 86, 19, 13;22;24,	10 10 10 10 10	node-10.domain admin node-10.domain	
7.46.19 13:25:58 + 7.46.19 13:25:44 + 7.46.19 13:25:44 + 7.46.19 13:25:28 + 7.46.19 13:25:28 + 7.46.19 13:25:28 + 7.46.19 13:23:58 + 7.46.19 13:23:44 + 7.46.19 13:23:44 + 7.46.19 13:23:44 + 7.46.19 13:23:43 + 7.46.19 13:22:42 + 7.46.19 13:22:42 +	10 10 10 10	node-10.domain	i III management: Administrator executed login. Result
7.86.19 13:25:46 7.86.19 13:25:44 7.86.19 13:25:28 7.86.19 13:25:28 7.86.19 13:23:28 7.86.19 13:23:46 7.86.19 13:23:44 7.86.19 13:23:44 7.86.19 13:23:44 7.86.19 13:23:42 7.86.19 13:22:42 7.86.19 13:22:42	10 10 10	1	[I] Administration: Log in
7.86.19 13:25:44 ; 7.86.19 13:25:28 ; 7.86.19 13:25:28 ; 7.86.19 13:25:28 ; 7.86.19 13:23:58 ; 7.86.19 13:23:46 ; 7.86.19 13:23:44 ; 7.86.19 13:23:44 ; 7.86.19 13:22:44 ; 7.86.19 13:22:21 ;	10 19	i node-10.domain i admin	[1] Management: Administrator executed Acquiring con
7.06.19 13:25:28 1 7.06.19 13:25:28 1 7.06.19 13:23:50 1 7.06.19 13:23:46 1 7.06.19 13:23:44 1 7.06.19 13:23:44 1 7.06.19 13:23:44 1 7.06.19 13:23:44 1 7.06.19 13:23:44 1 7.06.19 13:23:24 1 7.06.19 13:23:44 1 7.06.19 13:23:42 1 7.06.19 13:23:42 1 7.06.19 13:22:21 1	10	node-10.domain admin	[1] Management: Administrator executed login. Result
7.06.19 13:25:28 7.06.19 13:23:50 7.06.19 13:23:46 7.06.19 13:23:44 7.06.19 13:23:44 7.06.19 13:23:43 7.06.19 13:22:24 7.06.19 13:22:22		node-10.domain admin	[1] Management: Administrator executed login. Result
7.06.19 13:23:50 7.06.19 13:23:46 7.06.19 13:23:44 7.06.19 13:23:44 7.06.19 13:23:43 7.06.19 13:22:43 7.06.19 13:22:24 7.06.19 13:22:12	10	node-10.domain admin	[1] Management: Administrator executed logout, Resul
7.06.19 13:23:46 7.06.19 13:23:44 7.06.19 13:23:44 7.06.19 13:23:44 7.06.19 13:23:43 7.06.19 13:22:24 7.06.19 13:22:12	19	1 node-10.domain 1 superuser	[]] Administration: View sustem log
7.06.19 13:23:44 7.06.19 13:23:44 7.06.19 13:23:44 7.06.19 13:23:43 7.06.19 13:22:24 7.06.19 13:22:12	10	node-10 domain admin	[1] Management: Administrator executed Acquiring con
7.06.19 13:23:44 7.06.19 13:23:43 7.06.19 13:22:24 7.06.19 13:22:24 7.06.19 13:22:12	10	node-10.domain. admin	[1] Management: Administrator executed login. Result
7.06.19 13:23:43 7.06.19 13:22:24 7.06.19 13:22:12	10	node-10.domain admin	[[]] Management: Administrator executed login. Result
7.06.19 13:22:24 7.06.19 13:22:12	10	node-10 domain	[1] Administration: Log in
7.06.19 13:22:12	10	node-10 domain admin	[1] Management: Administrator executed Acquiring con
1.00.13 13.66.16 1	10	node-10 domain admin	III Management: Administrator executed login Result
7 86 19 13:21:52 1	10	pode-10 domain damin	! [1] Management: Administrator executed logout Resul
7 96 19 13 17 49	1	! SG-1 domain-10 ! superuser	! [1] Administration: Sustem time
7 96 19 13 17 37 1	1	SG-1 domain-10 superuser	! [1] Administration: Change node settings
7 96 19 12 17 24 1	10	hada 19 domain lounonucon	I III Administration: User suptem log
7 96 19 12 14 16 1	10	houe-10. domain ladmin	I III Huministration. View system by
7 06 49 42 44 44	10	i nuac-10.aumain i aamin	I III Management: Administrator executed legin Peould
7 06 10 12 13 14 14 1	10	i nuac-10.aumain i aamin	III Management: Administrator executed login. Result
7.00.13 13.11.11 1	10	i nuac-10.aumain i aamin	I III nanayement, naministrator executed login, nesult
7.00.17 13.14.12 1	10	i nuae-10.aumain i	i LIJ Haministration: Loy in
7.00.15 11.43.13 1	10	1 1000-10.00ma11 1 admin	1 III ranayement, Haministrator executed Hequiring con
7.06.19 11:43:11 i	10	i node-10.domain i admin	i III management: Haministrator executed login. Result
7.06.19 11:43:01 1	10	i node-10.domain i admin	i III management: Haministrator executed logout, Resul
7.06.19 11:43:01 1	10	i node-10.domain i admin	i III Management: Administrator executed Unlocking con
7.06.19 11:43:00 1	10	i node-10.domain i admin	i III Management: Administrator executed Creating modu
7.06.19 11:43:00 1	10	i node-10.domain i admin	i III Management: Administrator executed Saving config
7.06.19 11:42:59	10	i node-10.domain i admin	i III Management: Administrator added LDAP profile Use
7.06.19 11:42:59	10	i node-10.domain i admin	i III Management: Administrator added Firewall rule la
7.06.19 11:42:59	10	node-10.domain admin	III Management: Administrator added Firewall rule
7.06.19 11:42:59	10	node-10.domain admin	III Management: Administrator added Firewall rule
7.06.19 11:42:59	10	node-10.domain admin	[1] Management: Administrator added Firewall rule F
7.06.19 11:42:59	10	i node-10.domain i admin	i III Management: Administrator added Firewall rule F
7.06.19 11:42:59	10	i node-10.domain i admin	i III Management: Administrator added Firewall rule F
7.06.19 11:42:59	10	¦ node-10.domain ¦ admin	III Management: Administrator added Net object 1.1.1
7.06.19 11:42:59	10	node-10.domain admin	[1] Management: Administrator added Net object 30.1.
			The second

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.

	Details for selected event
Date/time:	17.06.19, 13:25:59.698
Security Gateway time:	17.06.19, 13:25:59.698 (UTC+00:00)
Host:	node-10.domain-10
Device ID:	10
Severity:	Information
Subject:	admin
Category:	Management
Administrator executed	login. Result: successfully. Source: 127.0.0.1.

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>**.

 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.

	Filter	
Date∕time Host Subject Category Severity Action		
Apply Reset		

- 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 $<\uparrow>$, $<\downarrow>$.

• 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.

Host				
Name				

• 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.



- Select the required format and press <Enter>.
 You receive the Insert USB Flash drive message.
- 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.

Choose log to clear	
<mark>System log</mark> NS log Management log Back to the previous menu	

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.

ilable shap-ins;	Veedee			Selected snap-ins:	Edit Extensions
iap-in	veridor				Luit Extensions
ActiveX Control	Microsoft Cor			Add >	Remove
Authorization Manager	Microsoft Cor				
^P Certificates	Microsoft Cor				the second se
Component Services	Microsoft Cor				Move Up
Computer Managem	Microsoft Cor				Move Down
Device Manager	Microsoft Cor		Add >		101000111
Disk Management	Microsoft and				
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor				
Link to Web Address	Microsoft Cor	~			Advanced
cription:					

4. In the list of available snap-ins, select **Certificates** and click **Add**.

The **Certificates snap-in** dialog box appears.

Certificates snap-in			×
This snap-in will always manage certificates for:			
O My user account			
O Service account			
Computer account			
			_
	< Back	Next >	Cancel

- 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.

Continent Enterprise Firewall. Version 4. Administrator guide. Monitoring and Audit

- 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.

Widget title	ជិ ក្រ
	1.

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

Editing Widg	et title	×
Title	Widget title	
Widget type	Select	~

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.

- 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.