SECURITY code

Continent Enterprise Firewall
Version 4

Management

Administrator guide

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

Table of contents

List of abbreviations

CA	Certification authority
CSR	Certificate Signing Request
DNS	Domain Name System
FW	Firewall
GRUB	GRand Unified Bootloader
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
MMC	Microsoft Management Console
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
QAT	Quick Access Toolbar
RNG	Random number generator
USB	Universal Serial Bus
UTC	Coordinated Universal Time

Introduction

This manual is designed for administrators of Continent Enterprise Firewall (hereinafter — Continent). It contains information needed for work with Continent.

This document contains links to documents [**1**] – [**9**].

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 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.

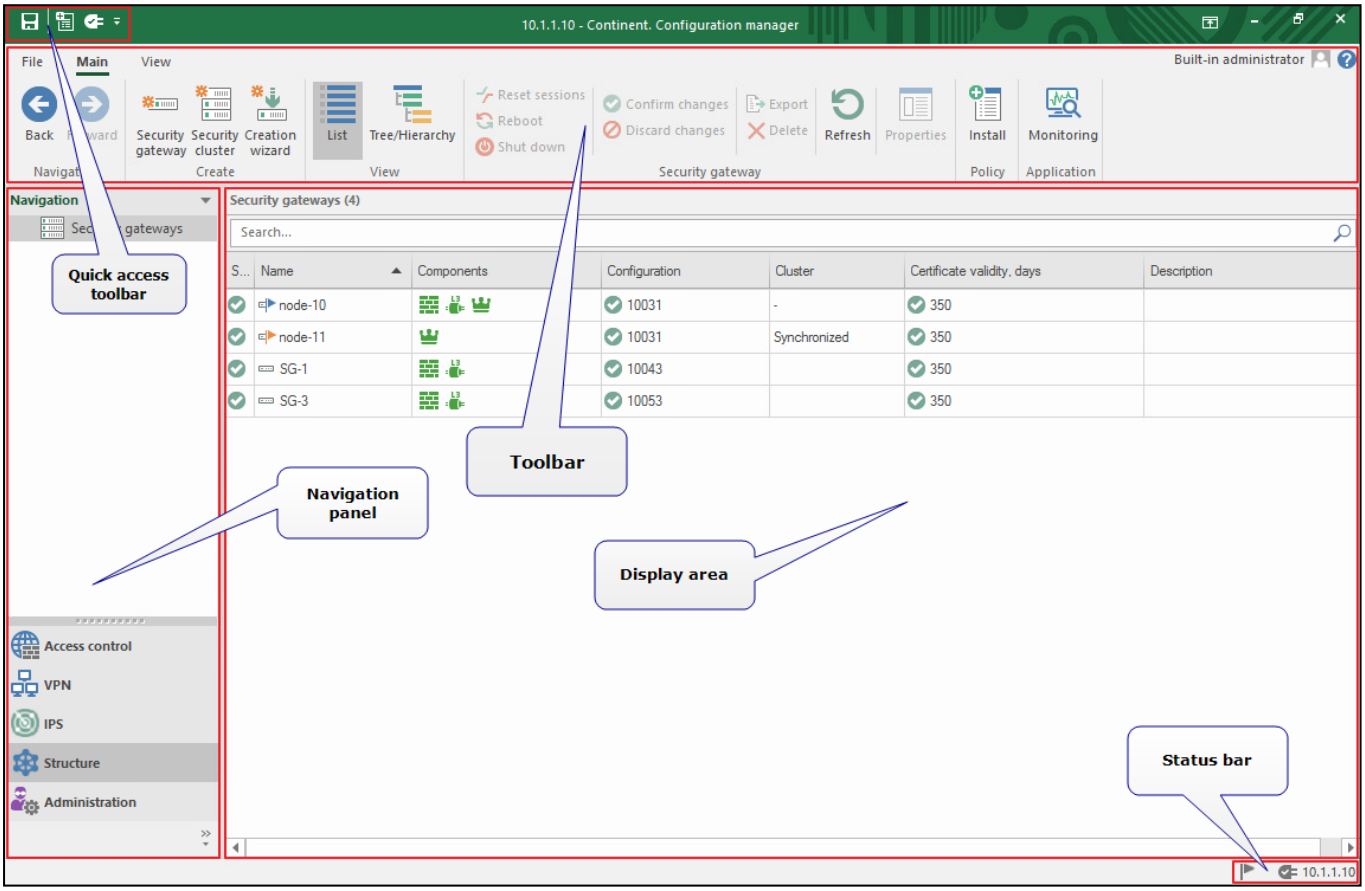
Version 4.1.7 — Released on December 5th, 2023.

Chapter 1
Administering Configuration Manager

The Configuration Manager is software for remote administration of the Security Management Server and other Continent Security Gateways. It is shipped along with the product kit and has a special graphic user interface.

Configuration Manager interface

After running the Configuration Manager and successful authentication (see [**1**]), the main window appears.



The Configuration Manager window has the following elements:

Interface element	Description
Toolbar	Contains a set of tools and two tabs: • **Main** — displays the toolbar; • **View** — allows to configure interface the Configuration Manager interface. Tools are buttons that you can use to launch frequently used commands. A set of tools depends on a section which you can select in 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	Provides quick access to the most frequently used commands. Contains the following buttons: • — save the current configuration; • — install a security policy; • — configure the Security Management Server connections; • — connect to the Security Management Server; • — configure Quick Access Toolbar

Navigation panel	Contains the following sections: • **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 section
Status bar	Contains the following data: • the number of currently running tasks and the button to open the notification center  where you can find the link to open the general task list (see **Administration**); • the icon that indicates the status of a connection to the Security Management Server (if there is a connection, this icon also displays a Security Management Server IP address, for example )

On the right, there is the display area. The display area may contain organized data displayed as lists, tables or pie charts as well as several functional elements (additional buttons, active fields, etc.). Table data mostly has its own right-click menu overlapping with the toolbar. You can view the properties of an element by double-clicking it or clicking **Properties** on the toolbar.

The display area may contain an additional area shown at the bottom by default. In its top right corner, there are the control buttons to configure the display of the area.

Button/ menu command	Description
	Menu drop-down list
Floating	If you select the respective section, the area is displayed as an additional window which you can move or resize with standard tools. In this case, the control buttons are hidden; to switch to the docking mode, double-click the window header or drag the window to the additional docking buttons displayed at the bottom or on the right of the display area.
Docking	If you select the respective section, the area is shown in the certain part of the display area. This mode is used by default.
 or Autohide	The area is not displayed and the additional tab panel appears. The location of the panel depends on the location of the area docking (right or bottom). This panel is displayed for each selected section. The respective area appears on mouseover.
 or Hide	The area is not displayed as long as you switch the active section.

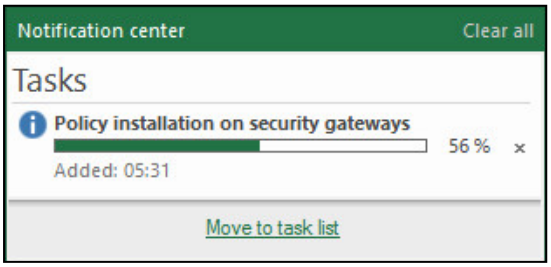
You can resize the list of sections using the mouse.

To operate organized data efficiently, use **Ctrl/Shift** with the cursor and drag selected objects.

To sort displayed data in ascending/descending order of a parameter, click the respective column header.

At the top of the display area, there is a status bar, containing the number of displayed elements, and the search bar.

In the bottom right corner, there is the **Notification center** icon  . The **Notification center** contains information about active task progress and the number of tasks (if they exist). On the right to the **Notification center**, there is the name of the administrator currently authorized in the Configuration Manager. You can configure these elements in the shortcut menu of the bottom bar.



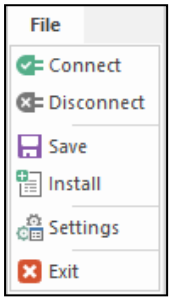
Configure the list of connections to Security Management Servers

You can create, delete and configure connections to several Security Management Servers in the Configuration Manager. The connection appears in the list after you connect to the Security Management Server at least once.

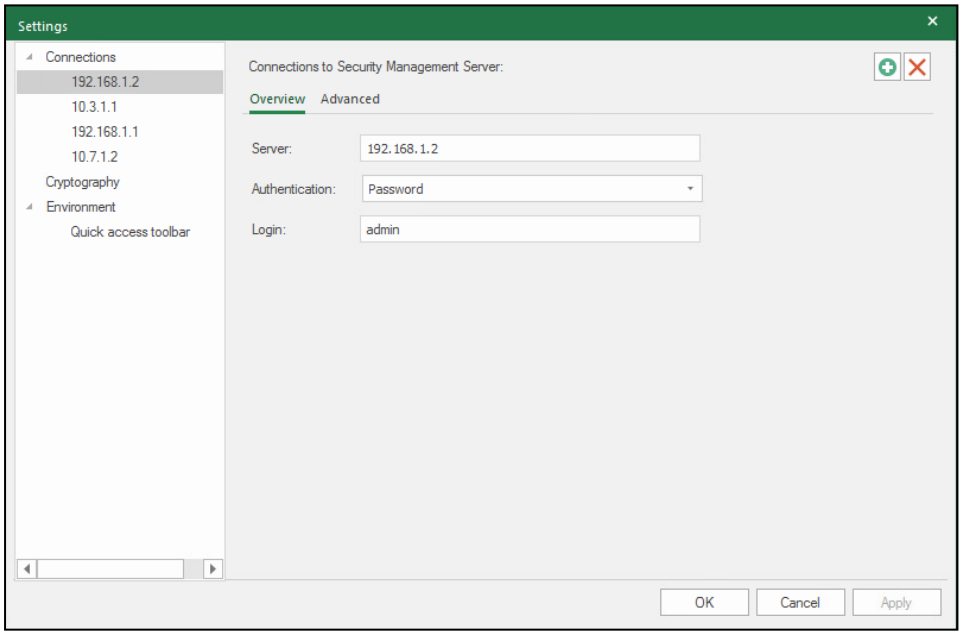
Note.
To prevent errors, we do not recommend using different versions of the Configuration Manager and the Security Management Server simultaneously.

To configure the connection list:

1. Run the Configuration Manager and close the **Administrator authentication** window.
2. On the ribbon, in the top left corner of the main window, click  and select **Options**.



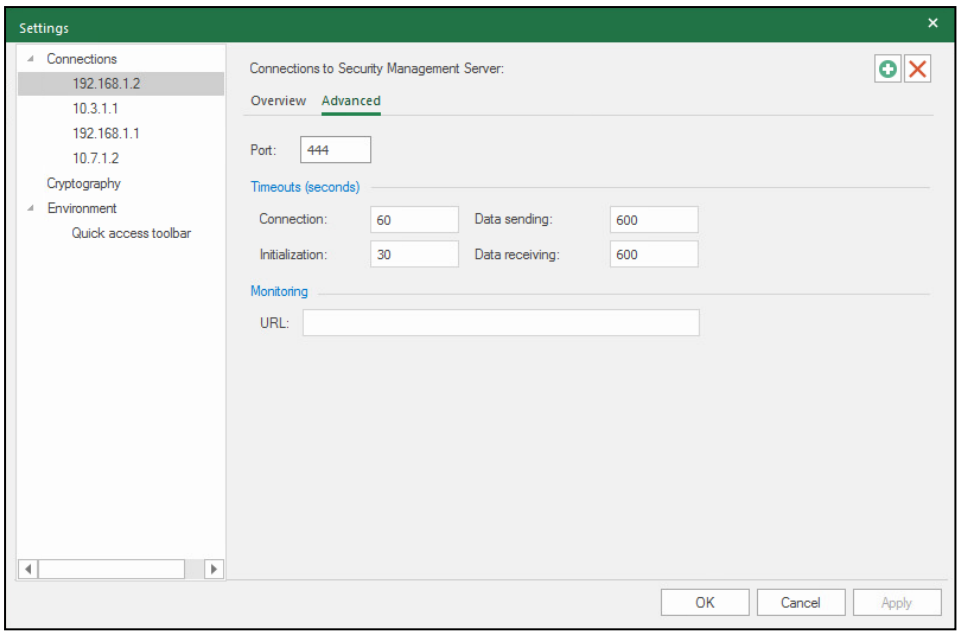
The dialog box appears as in the figure below.



On the left, there is the list of connections to the Security Management Server.

Note.
If you have never connected to the Security Management Server, the list of connections will be empty.

3. To create a connection, click  , specify the required parameters and go to the **Advanced** tab.



The tab shows additional parameters set by default for a new connection.

Parameter	Default value	Description
Port	444	Port used to connect the Configuration Manager to the Security Management Server
Timeouts (seconds)		
Connection	60	Connection timeout
Initialization	30	Initialization timeout
Data sending	600	Timeout for sending data to the Security Management Server
Data receiving	600	Timeout for receiving data
Monitoring		
URL		Name of a monitoring server

4. If necessary, change the additional parameters.
5. After you have specified the parameters, click **Apply**.
6. If you need to add a connection to another Security Management Server, click  and follow the instructions above.
7. To remove the connection that is not in use, select it in the list and click  .
8. Close the window or click **OK**.

Configure the Configuration Manager

Select a CSP

In the Configuration Manager, you can select a CSP that are already installed on the computer.

To select a CSP:

1. In the Main menu, click **Settings** and select **Cryptography**.
2. In the drop-down list, select a required CSP.

Configure view properties

To configure view properties:

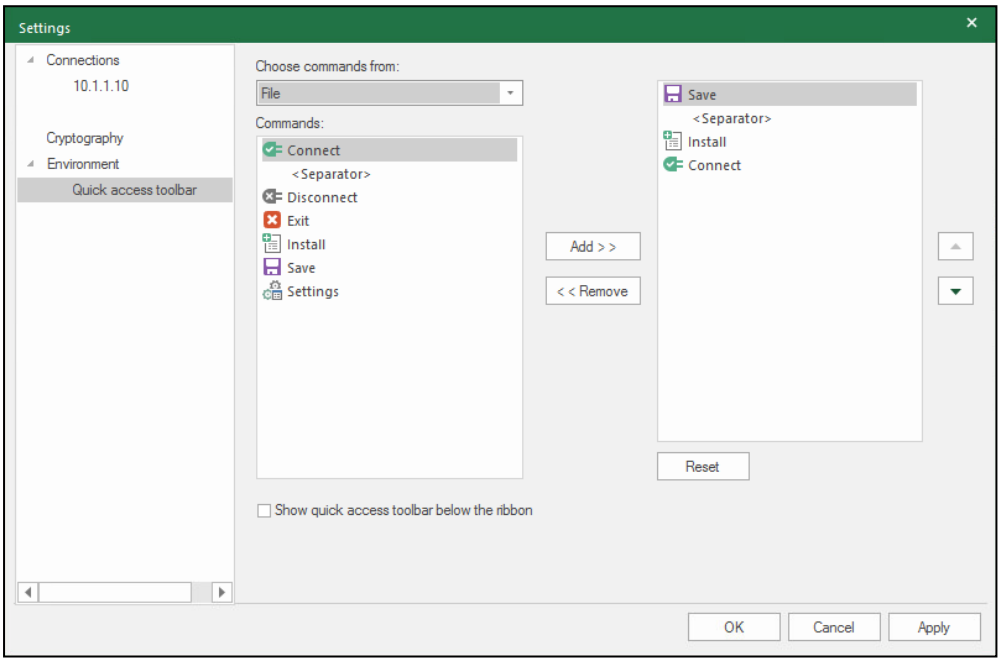
1. In the Main menu, click **Settings**, then click **Environment**.
2. To change the interface language, select the required one in the drop-down list.

3. In the **Visual presentation** area, select a visual schema and an accented color in the respective drop-down lists.
4. Click **OK**.

Configure the Quick Access Toolbar

You can call up the configuration window of the Quick Access Toolbar by clicking and selecting **More Commands**.

Note.
You can also call up the respective configuration window from the main menu. To do so, click the main menu button, select **Settings**, then select **Quick Access Toolbar** on the left.



In the **Commands** list, there are available commands of the Configuration Manager. On the right, there are commands displayed on the Quick Access Toolbar.

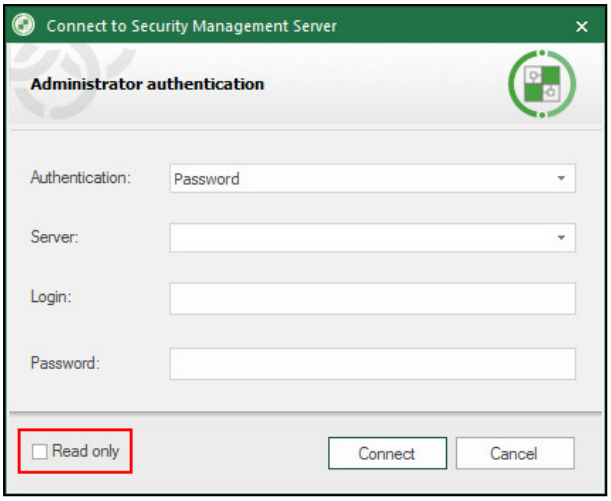
To configure the Quick Access Toolbar:

1. To clear the list of commands, click **Reset**.
2. To add a command to the Quick Access Toolbar, select it in the **Commands** list and click **Add >>**.
   The command appears at the bottom of the list.
3. To delete the command, select it in the list on the right and click **< <Remove**.
4. To move the command, select it in the list and click to move it one step up or to move it one step down.
5. To locate the Quick Access Toolbar below the ribbon, select the respective check box.
6. To apply changes, click **OK**.

Take over Security Management Server lock

There is a number of ways to take over the lock (using the Configuration Manager or the local menu of the Security Gateway with Security Management Server).

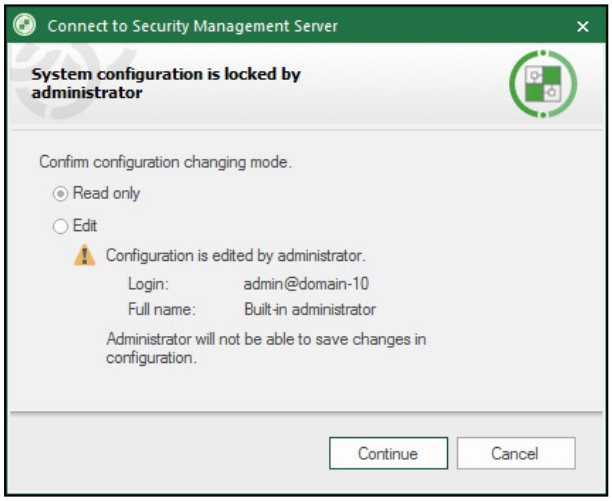
When you connect to the Security Management Server via the Configuration Manager, you can use the **Read only** mode available under any circumstances after the authentication. In this mode, you can only view information. All modifications are not allowed.



In the local menu, you can select the local changes mode (see below) available under any circumstances after the authentication. In this mode, you cannot apply changes in the Security Gateway as well as create Security Gateway and root certificates.

To take over the lock while administrating the Security Management Server using the Configuration Manager:

1. After an administrator is authenticated in the Configuration Manager, a dialog box containing the information about the lock appears as in the figure below.



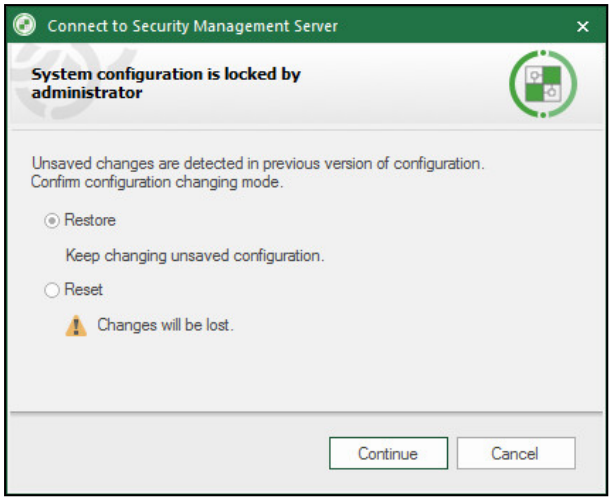
Note.
This dialog box also appears if the administrator has ended the previous Configuration Manager session incorrectly.

2. Select **Edit** and click **Continue**.

   If the administrator has enough privileges, the connection between the Configuration Manager and the Security Management Server is established.
3. If the administrator has not enough privileges, the respective dialog box appears. Click **Close**.

To connect to the Security Management Server after ending the previous Configuration Manager session incorrectly:

1. After an administrator who ended the previous Configuration Manager session incorrectly is authenticated in the Configuration Manager, the dialog box appears as in the figure below.



2. To restore the data of the previous session, select **Restore**, then click **Continue**.
3. To reset changes in the Security Management Server policy and load the previous version of its configuration, select **Reset**, then click **Continue**.

To take over the lock in the Security Management Server local menu:

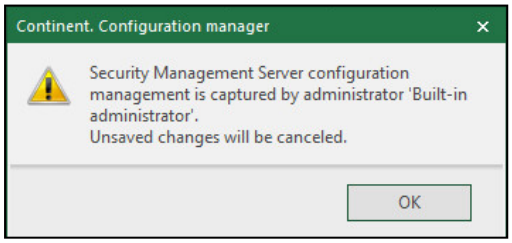
1. Log in to the Security Management Server local menu.

   A dialog box appears as in the figure below.

2. Select **Take over lock** and press **<Enter>**.

   Attention!
   Unsaved changes in the Configuration Manager will be lost.

   If the administrator has enough privileges to get access, the main menu appears. In the Configuration Manager, the information window appears as in the figure below.



   If the administrator has no rights to take over the lock, the message appears as in the figure below.

To switch control mode to the Security Management Server local menu (for one administrator):

1. Log in to the Security Management Server local menu.

   A dialog box appears as in the figure below.

2. Select **Take over lock** and press **<Enter>**.

Attention!
Unsaved changes in the Configuration Manager will be lost.

The main menu appears.

Uninstall the Configuration Manager

Only a member of a local administrators group can uninstall the Configuration Manager.

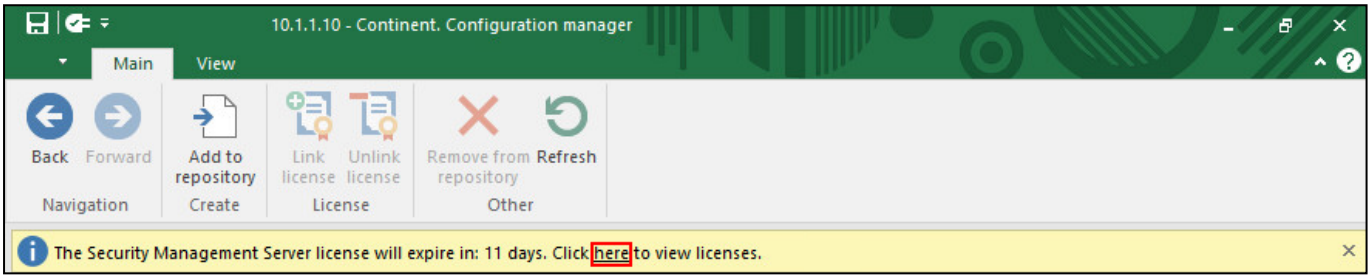
You can uninstall the Configuration Manager using Windows tools. To uninstall the Configuration Manager, take the following steps:

- shut down all user apps;
- uninstall the Configuration Manager;
- restart the OS.

Chapter 2
Licenses

The Security Gateway license determines which components of the Security Gateway are active. Without the license, you cannot apply policies (the procedure includes license check of the Security Management Server repository).

You can fully use the Security Management Server after its initialization. It is provided by a trial license that is created after the initialization by default and expires in 14 days. After this period, you cannot install a policy on the Security Gateway. If you save the configuration or log in to the system after the license has expired, the respective message appears.



The license unlinked from the Security Gateway remains in the repository. You can link it to another Security Gateway or remove it (see p. **16**).

View licenses

You can view Security Gateway licenses in the local menu or the Configuration Manager.

To view licenses in the local menu:

1. In the main menu, select **Information** and press **<Enter>**.
   The respective window appears.
2. Select **Licenses** and press <**Enter>**.
   The list of active Security Gateway licenses appears.

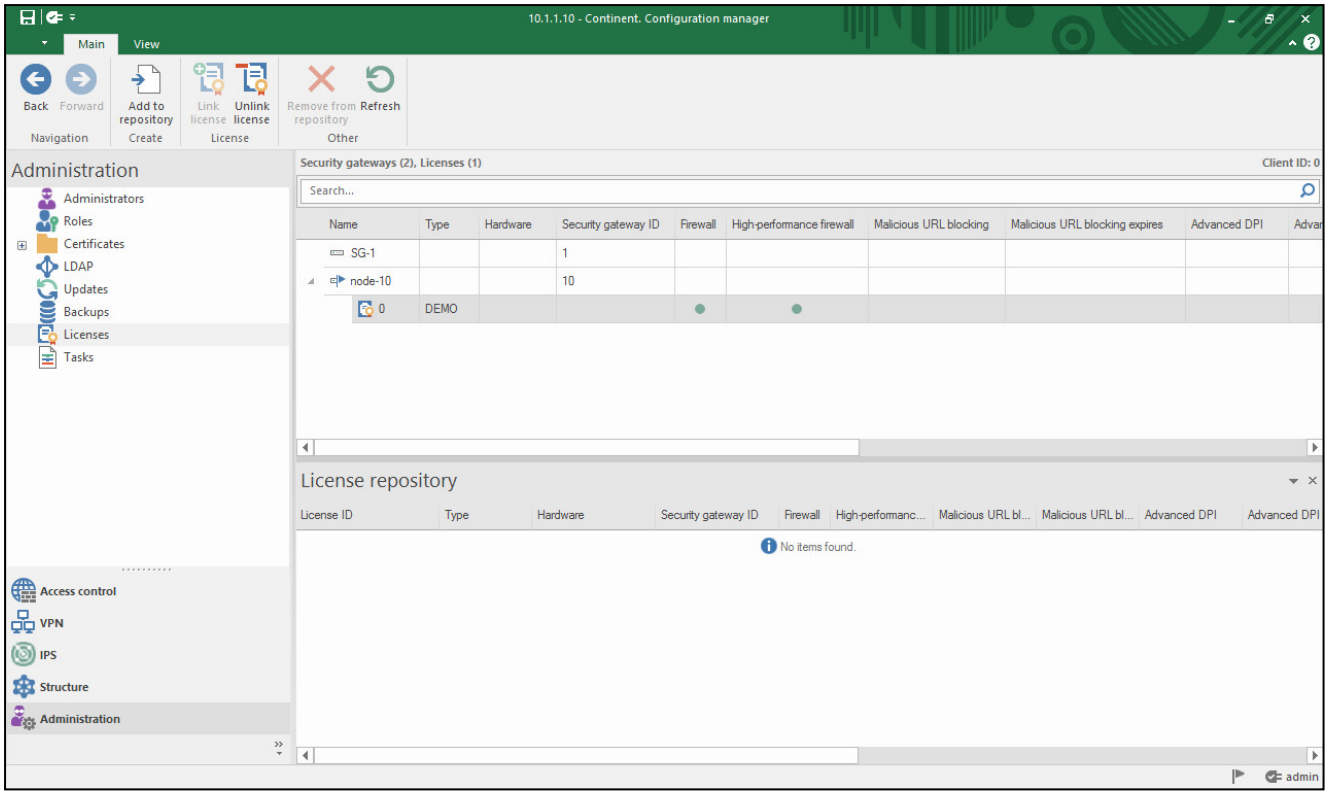
```
                                                    Licenses Information

============================================================

Common license information:
-----------------------------------
Client ID:   3
License ID:   10
License type:   SU
License host:
Host:   10
Platform:   DEFAULT_PLATFORM
Creation date:   2022-03-09 00:00:00
```

Attention!
Information about licenses appears only after the first installation of a policy on the Security Gateway with the Security Management Server.

3. To go back to the previous menu, press **<Esc>**.

To read licenses in the Configuration Manager:

- Run the Configuration Manager and select **Administration** on the navigation panel, then click **Licenses**.
  In the display area, the list of registered licenses grouped by Security Gateways appears. In columns, there are license parameters and components the license allows you to use. In the top right corner, there is a Client ID (null by default). At the bottom of the information panel, there is the License repository containing reserved licenses.



License management

You can add, link, unlink and remove Security Gateway licenses using the Configuration Manager.

To add a license:

1. In the Configuration Manager, go to **Administration** and select **Licenses**.
2. Click **Add to repository** on the toolbar.

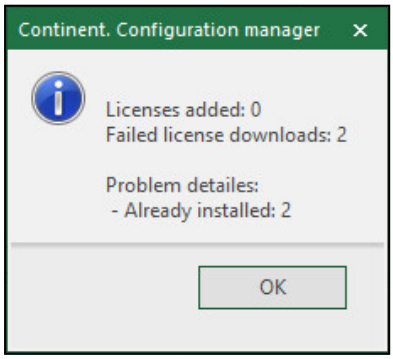
   The File Explorer dialog box appears.
3. Select the license file and click **Open**.

   Licenses are uploaded from the file if the following requirements are met:

   - Client ID in the license matches Client ID in the Security Management Server or the Security Management Server database contains only licenses with null Client ID.
   - The license has not expired.

     Note.
     If the update license for IPS protections has expired, it does not mean the Security Gateway license has also expired.
   - There is no license with the same ID in the Security Management Server database.

   After the import to the Security Management Server database has been finished, the message about added licenses, failed license downloads and the reasons for denying the latter will appear.



To link a license to the Security Gateway:

Attention!
You must link a license before exporting a configuration for the first time and connecting a Security Gateway to the Security Management Server.

1. If a demo license is linked to the Security Gateway, unlink it (see procedure below).
2. In the Configuration Manager, click **Update**.
3. In the Configuration Manager, go to **Administration** and select **Licenses**.
4. Select the Security Gateway in the list and click **Link license** on the toolbar.
   The window with licenses appears.
5. Select the license with the relevant purpose and expiration date and click **OK**.
   The license is linked to the Security Gateway and moved from the repository to the group of linked licenses under the following conditions:
   - The license has not expired.
   - The Security Gateway ID in the license (if specified) matches the ID of the linked Security Gateway.
   - The platform type of the license (if specified) matches the platform type of the linked Security Gateway.
6. Go to **Structure**, then click **Install** on the toolbar.
   The **Install policy** dialog box appears.
7. Select the required Security Gateway and click **OK**.

To unlink a license:

1. In the Configuration Manager, go to **Administration** and select **Licenses**.
2. Select the required license in the display area and click **Unlink license** on the toolbar.
   The dialog box prompting you to confirm the action appears.
3. Click **Yes**.

   Note.
   To unlink the license, we recommend dragging it from the Security Gateway to the repository.

   The license is unlinked from the Security Gateway and moved to the repository.

To remove a license:

Attention!
You cannot remove the linked license. First, unlink the license.

1. In the Configuration Manager, go to **Administration** and select **Licenses**.
2. Select the required license in the repository and click **Remove from repository** on the toolbar.
   The dialog box prompting you to confirm the action appears.
3. Click **Yes**.
   The license is removed from the repository.

Note.
You can reupload the removed license from the file to the Security Management Server database.

Chapter 3
Management of Continent

Administrators manage Continent according to assigned roles.

The first administrator account is created when initializing the Security Management Server and has all the possible permissions to manage the Security Management Server and Security Gateways of a domain.

There are two types of administrator roles:

- built-in — a role with the fixed set of permissions, cannot be modified or deleted;
- user — a role with a custom set of permissions, can be created and modified by the Configuration Manager administrator.

There are four built-in roles:

- Main administrator;
- Security administrator;
- Network administrator;
- Audit administrator.

You can assign a role to an administrator in the following ways:

- when creating or modifying an administrator account;
- when creating or modifying a role (to extend permissions for the administrator group).

You can assign either built-in or custom roles to the administrator. The administrator is granted a permission if any of the assigned roles include it.

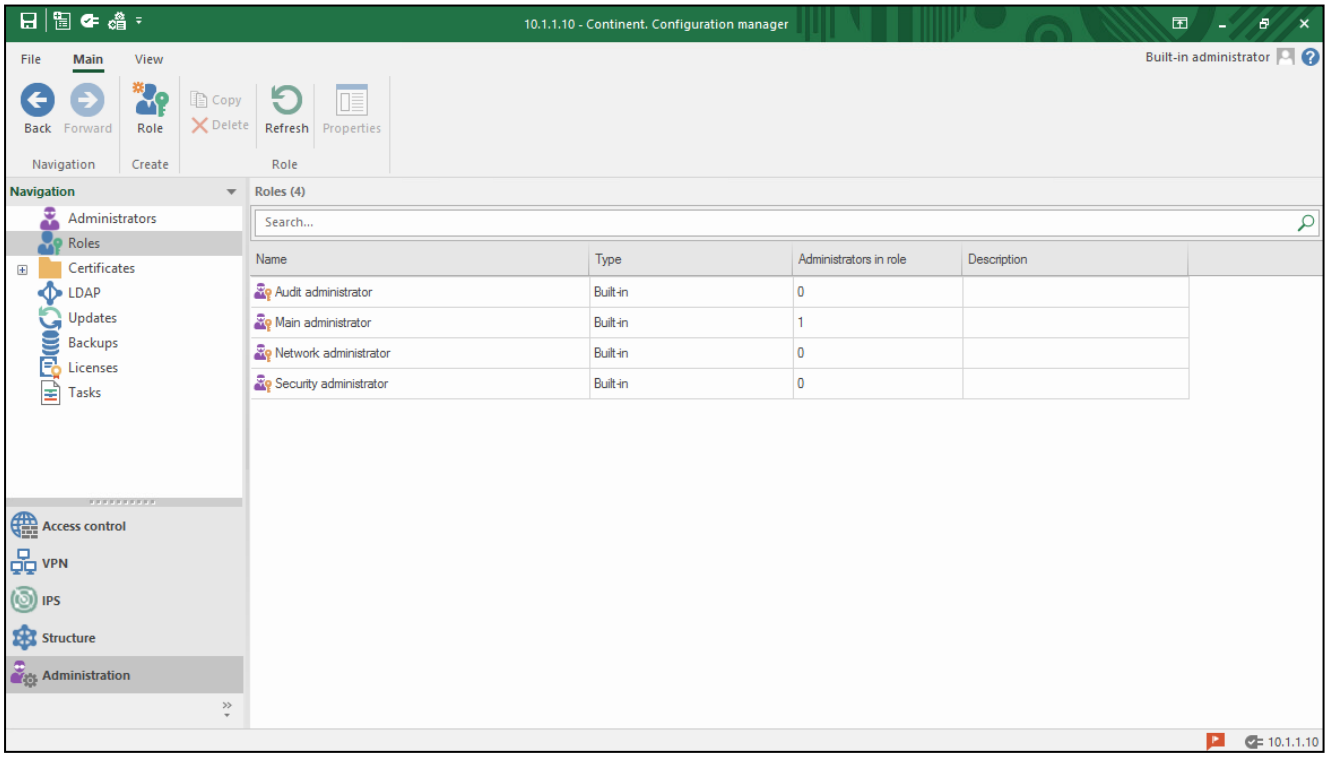
Manage administrator roles

View roles

To view a role:

1. In the Configuration Manager, go to **Administration** and select **Roles**.

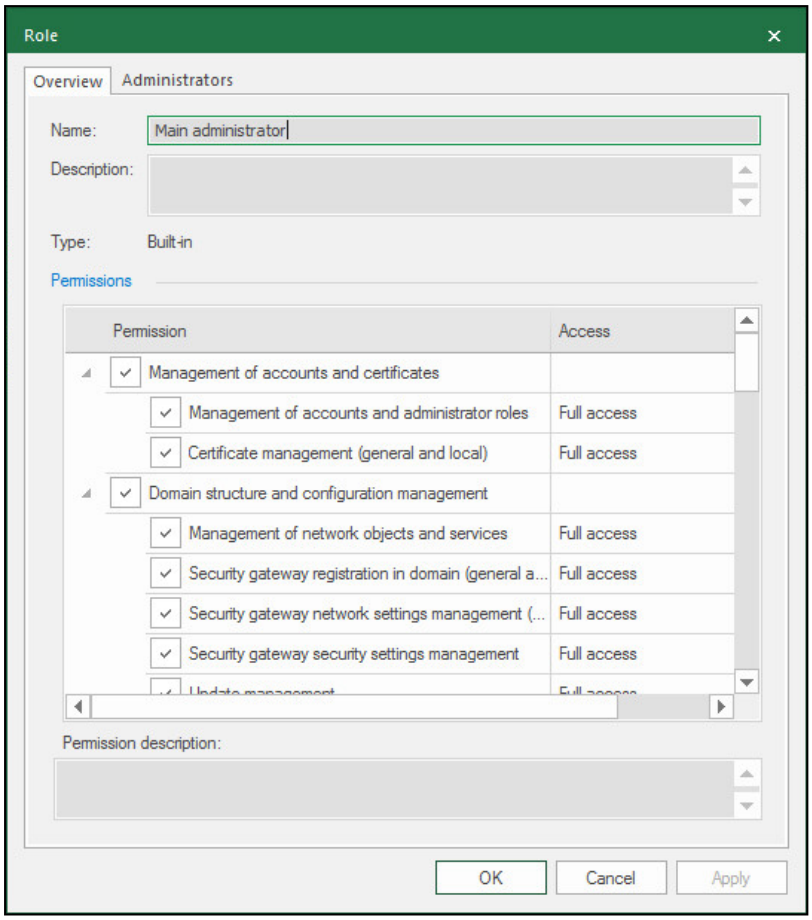
   In the display area, the list of roles appears.



   Every role has a type (built-in or custom) and the number of administrators to whom the role is assigned.

2. To view permissions of the role, select the role in the list and click **Properties** on the toolbar.

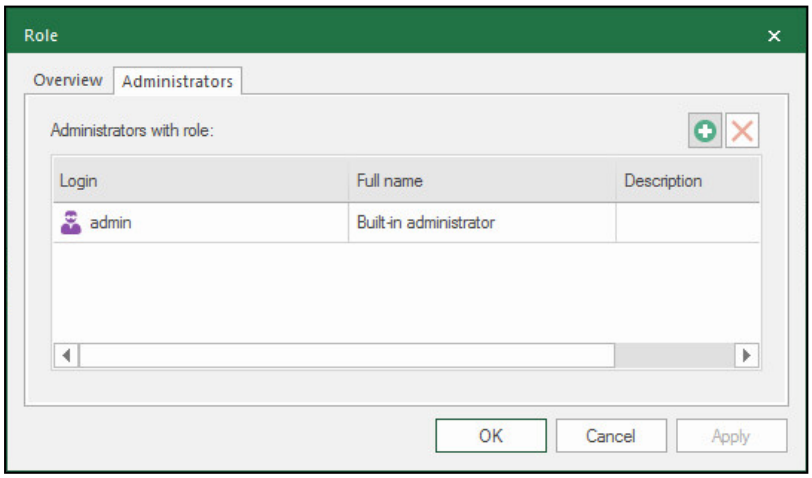
   The **Role** permissions with their description appear. The window contains two tabs: **Overview** and **Administrators**.



   On the **Overview** tab, you can view and modify permissions of the role.

Attention!
You can modify only custom roles (see p. 21).

3. To view the list of administrators to whom the role is assigned, select the **Administrators** tab.



   On the **Administrators** tab, you can assign the role to administrators.

4. After viewing information about the role, click **OK** or **Cancel**.

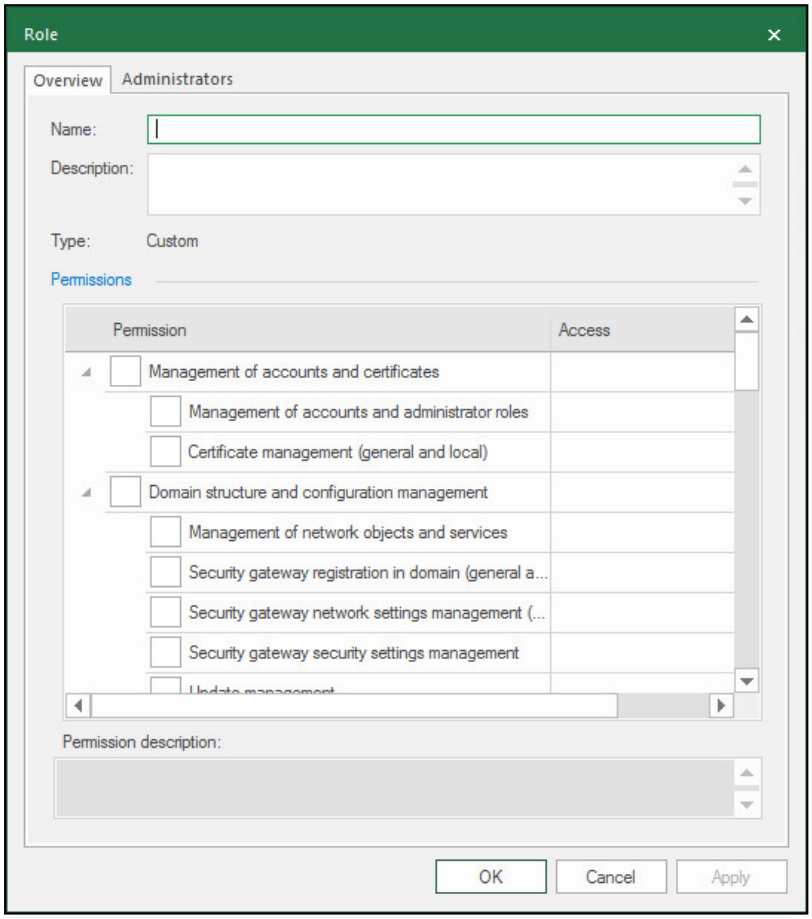
   The **Role** dialog box is closed.

Create roles

Attention!
When creating a role, we recommend saving the Security Management Server configuration before assigning the role to administrators (see p. 36).

To create a role:

1. Go to **Administration** and select **Roles**, then click **Role** on the toolbar.
   The **Role** dialog box appears.

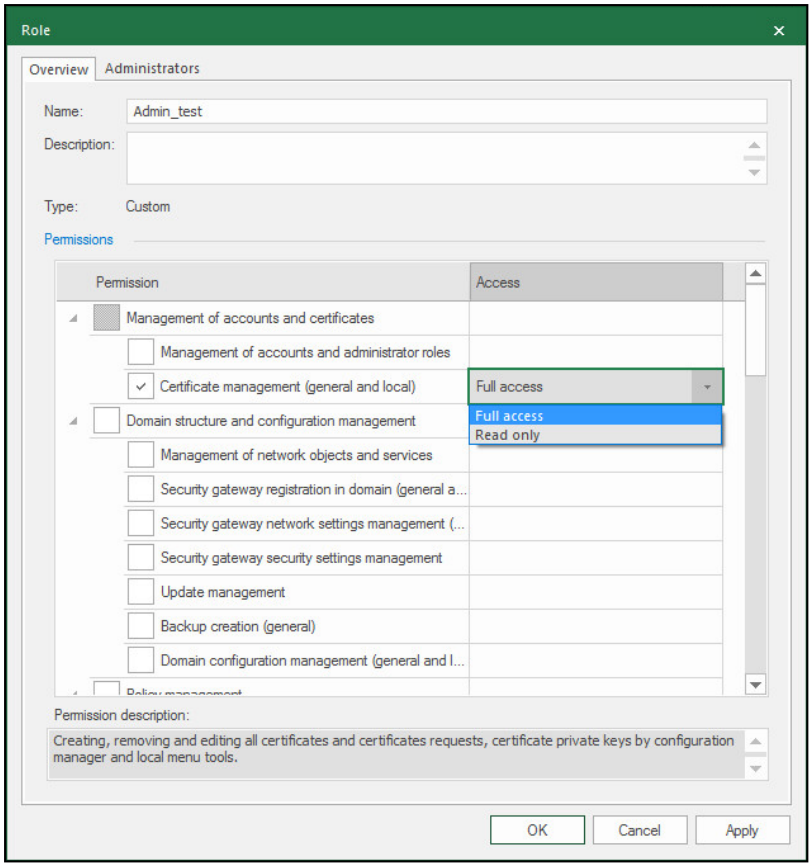


2. Specify the name and description of the created role in the respective fields.

   Note.
   The created role is custom by default.

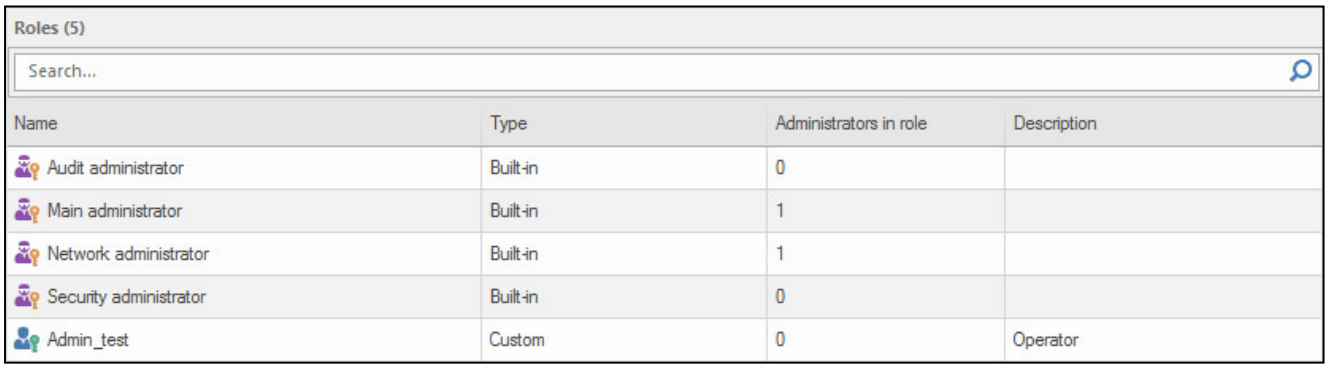
3. Select the required permissions, then select the required access type: full access or read-only.

   Note.
   For permissions of the **Local menu** and **Monitoring and diagnostic** groups, you can select only **Full access**.



4. Configure all the required permissions and click **Apply**.
5. Click **OK**.

   The **Role** dialog box is closed and the created role appears in the list.



6. To save changes of the Security Management Server configuration, click the respective icon in the top left corner of the Configuration Manager.

   The indeterminate progress bar appears. Wait for the operation to complete.
7. To apply the configuration, click **Install policy** on the toolbar, select the respective Security Gateways and click **OK**.

Modify and assign roles

Role modification means changing the set of permissions and their access type. You can modify only custom roles. Administrators can be assigned custom roles as well as built-in ones.

To modify a role:

1. In the Configuration Manager, go to **Administration**, select **Roles**, then select the required role in the list and click **Properties** on the toolbar.

   The **Role** dialog box appears.
2. Make the required changes (see p. **20**).
3. If you need to assign the role to an administrator, go to the **Administrators** tab and click  .

   Note.
   If the role was created recently, save the Security Management Server configuration before assigning it (see p. **36**).

   The list of administrator accounts appears.
4. Select the account to assign the role to.

   The account is added to the list of administrators whom the role is assigned to.
5. To assign the role to another administrator, repeat step **4.**
6. In the **Role** dialog box, click **OK**.

   The role properties are modified.
7. To apply the configuration, click **Install policy** on the toolbar, select the respective Security Gateways and click **OK**.

Delete roles

To delete a role:

1. In the **Administration** section of the Configuration Manager, go to **Roles**, select the required role and click **Delete** on the toolbar.

   The confirmation dialog box appears.
2. Click **Yes**.

   The selected role is deleted.
3. To apply the configuration, click **Install policy** on the toolbar, select the respective Security Gateways and click **OK**.

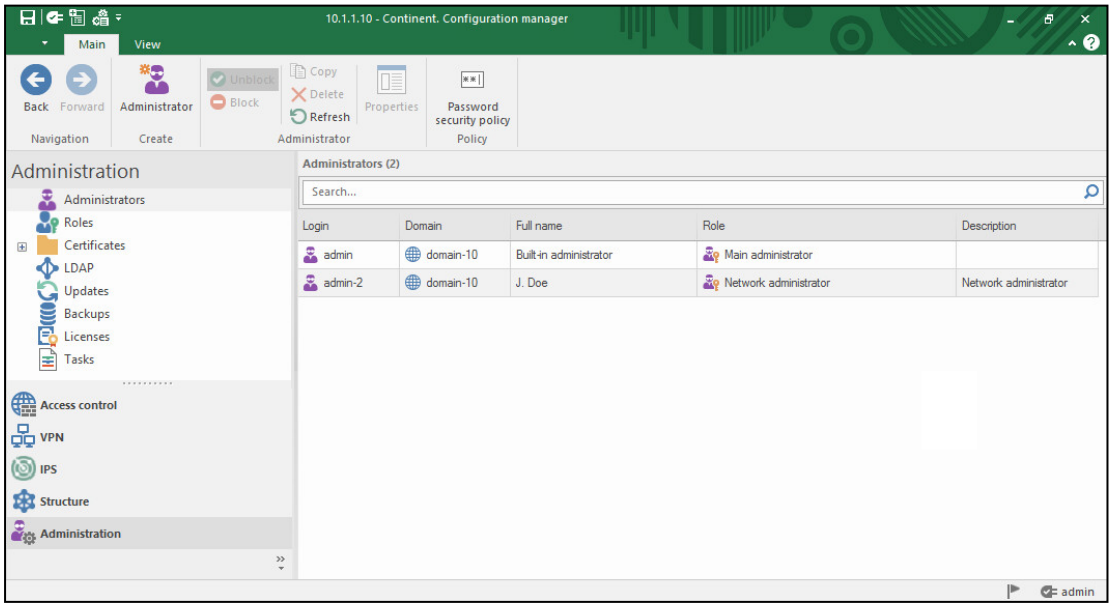
Manage accounts

View administrator accounts

To view account parameters:

1. In the Configuration Manager, go to **Administration** and select **Administrators**.

   In the display area, the list of administrators appears.



The list contains the following information:

- login;
- full name;
- role;
- description (not necessary).

2. To view information about the administrator account, select it and click **Properties** on the toolbar.

   The Administrator dialog box appears. It contains three tabs: **Overview**, **Authentication** and **Roles**.

Tab	Purpose
Overview	View and modify account parameters: • login; • full name; • description. Enable/disable account
Authentication	View and specify administrator authentication parameters: • authentication by a password; • authentication by a certificate
Roles	View and assign roles to an administrator

3. To view or modify parameters, go to the respective tab.

   You can view the description of possible parameter changes in the following sections.

4. After reading the information, click **OK** or **Cancel**.

   The **Administrator** dialog box is closed.

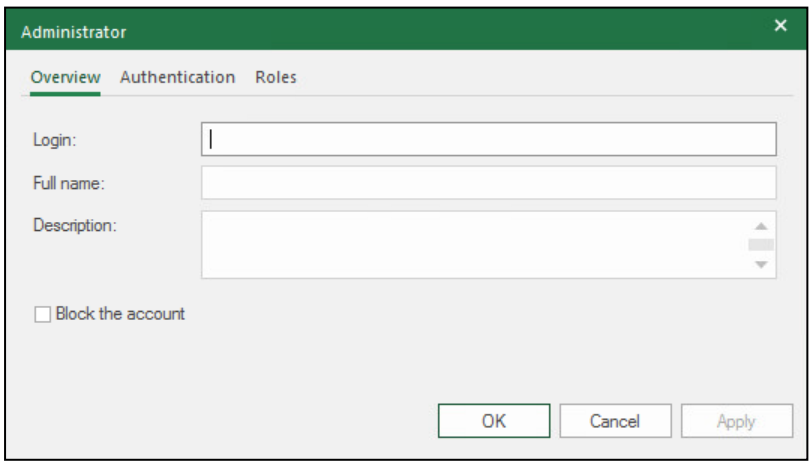
Create an administrator account

Attention!
To allow an administrator to authenticate by certificate, take the following steps:
1. Issue an administrator certificate (see p. **71**).
2. Install it to the administrator certificate store (see p. **71**).
3. Assign the previously created certificate to an administrator (see p. **24**).

To create an administrator account:

1. In the Configuration Manager, go to **Administration**, select **Administrators**, then click **Administrator** on the toolbar.

   The **Administrator** dialog box appears with the **Overview** tab open.

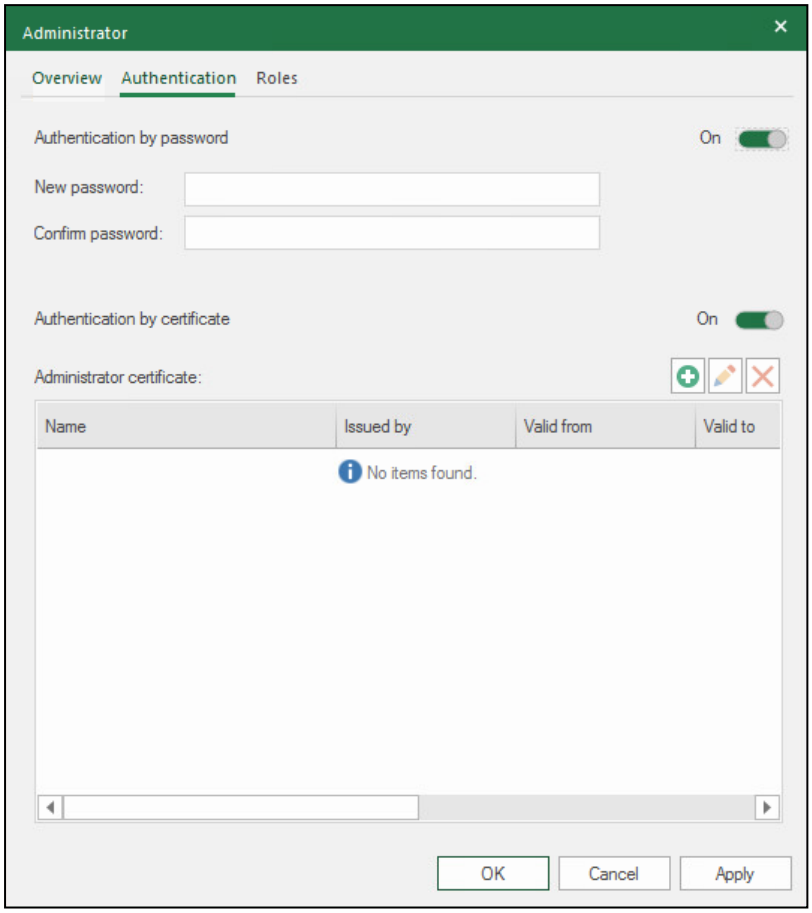


2. Specify the administrator account name, full name and brief description, then click **Apply**.

Note.
The account name can contain only Latin letters in lower case, numbers and "_-." symbols. The account name cannot be more than 32 symbols. The first symbol can be only a letter or "_".

Attention!
The following names are reserved for the operation needs: "adm", "bin", "daemon", "dhcpd", "ftp", "games", "gopher", "halt", "ips", "lp", "mail", "monit", "nginx", "nobody", "ntp", "nxlog", "operator", "postgres", "quagga", "root", "shutdown", "sshd", "sync", "tcpdump", "uucp", "vcsa", "djdb".

Then select the **Authentication** tab.



3. If an administrator must be authenticated by a password, select the respective check box, specify a password and click **Apply**.

Note.
The administrator password must meet the following requirements:

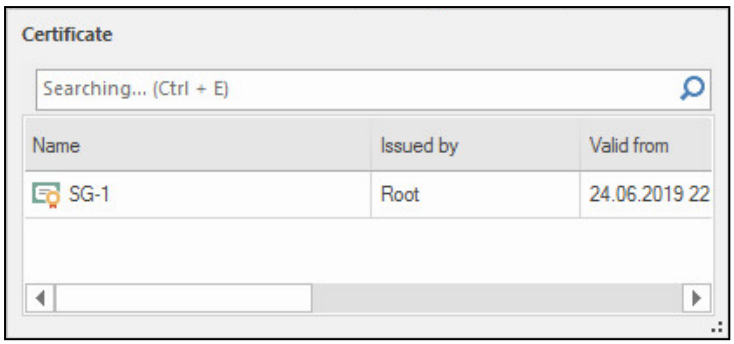
- contain numbers, Latin letters or the following special symbols:

!	@	#	$	%	^	&	*	(	)	_	-	+	;	:	.	,
[	]	{	}	=	\	|	/	?	>	<						

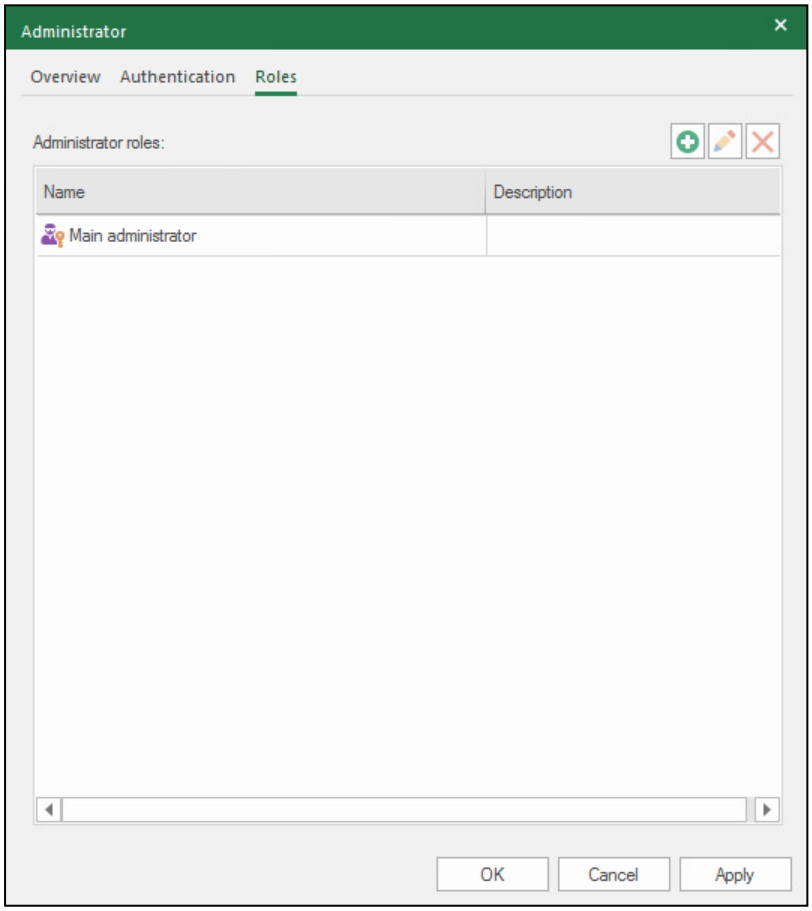
- follow the other rules set in the **Password security policy** (see the toolbar of **Administrators**). By default, it contains the following additional requirements for the password:
  - at least one number;
  - at least one lowercase letter;
  - do not contain more than 4 consecutive characters of the previous password;
  - the minimum length — 8 characters.

The password security policy can be modified (see p. 27).

4. If authentication by a certificate is not required for an administrator, go to **step 7**.
5. Select the **Authentication by certificate** check box, then click ⊕.
   The list of certificates appears.



6. Select the required certificate and click **Apply**.
7. Select the **Roles** tab.
8. To assign a role to the administrator, click .
   The list of roles appears.
9. Select the required role in the list.
   The selected role appears in the list on the **Roles** tab.



   Add other roles if necessary.
10. After adding the role, click **OK**.
    The **Administrator** dialog box closes and a new account appears in the list.
11. To apply the configuration, click **Install policy** on the toolbar, select the respective Security Gateways and click **OK**.

Delete an administrator account

To delete an administrator account:

1. In the Configuration Manager, go to the **Administration** section, select **Administrators**, then select the required administrator account and click **Delete** on the toolbar.

   The dialog box prompting you to confirm the deletion appears.
2. Click **Yes**.

   The selected account is deleted.
3. To apply the configuration, click **Install policy** on the toolbar, select the respective Security Gateways and click **OK**.

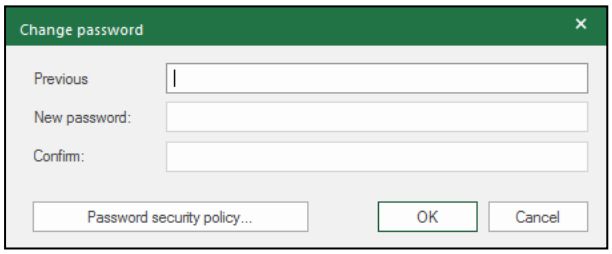
Change the password of the built-in administrator

To change the password of a built-in administrator in the Configuration Manager:

1. In the Configuration Manager, connect to the Security Management Server using the built-in administrator credentials.

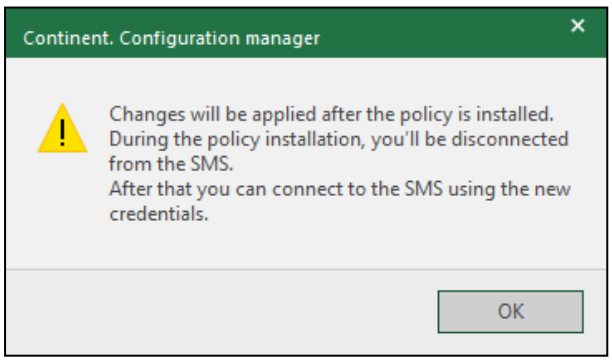
   The main window appears.
2. In the top right corner, click the built-in administrator name.
3. In the appeared dialog box, click **Change your password**.

   The Change password dialog box appears.



4. Specify the **Previous**, **New password** and **Confirm** fields.
5. Click **OK**.

   The confirmation window appears.



6. Click **OK**.
7. To apply the changes, install the policy on the required Security Gateways.

   Connection to the Security Management Server will be lost. Reconnect to the server using the new credentials.

Assign roles

You can assign a role to an administrator by:

- creating or modifying an administrator account (see p. **23**);
- creating or modifying a role.

To assign a role while modifying an account :

1. Go to the administrator list (see p. **22**), select the account and click **Properties** on the toolbar.

The **Administrator** dialog box appears.

2. Go to the **Roles** tab and add a role (see steps **4–5** of the administrator creation procedure on p. **23**).
3. After adding a role, click **Apply** in the **Administrator** dialog box.

To assign a role while modifying it:

Note.
If a role was created recently, you need to save the Security Management Server configuration before assigning (see p. **36**).

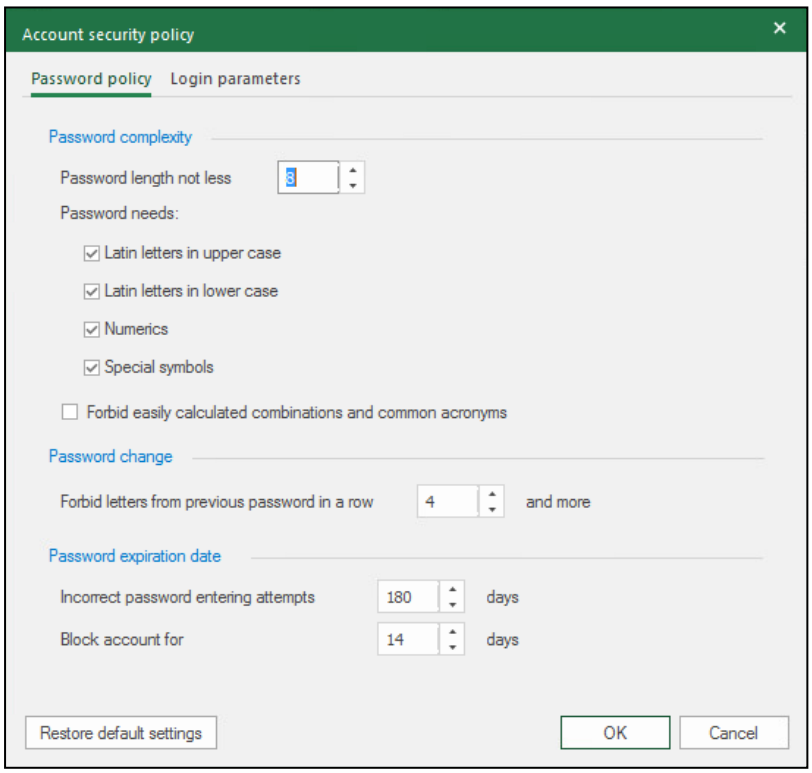
1. Go to **Roles** (see p. **18**), select the required role and click **Properties** on the toolbar.
   The **Role** dialog box appears.
2. Go to **Administrators** and click  .
   The list of administrators appears.
3. Select the account to assign the role to.
   The account is added to the list of administrators whom the role is assigned to.
4. In the **Role** dialog box, click **Apply**.
   The role is assigned to the administrator account.

Account security policy

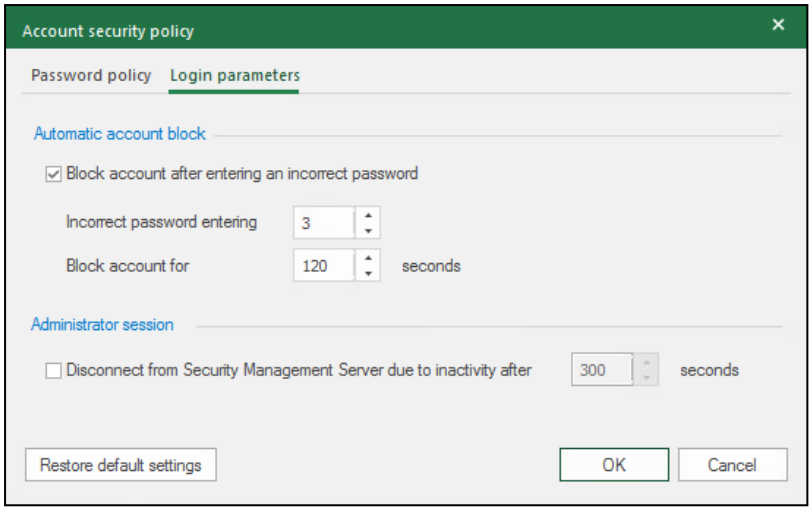
In Continent, you can set an account security policy.

To view a policy:

1. In the Configuration Manager, go to **Administration** and select **Administrators**.
   The list of administrators appears in the display area.
2. On the toolbar, click **Account security policy**.
   The respective dialog box appears.



3. Configure the account security policy according to your company's requirements.
4. Click **OK** to confirm the changes.
5. Go to the **Login parameters** tab.
   The respective dialog box appears.



6. Configure **Automatic account block** and **Administrator session** groups of parameters.
7. Click **OK** to apply parameters.

Chapter 4

Management of Security Gateways

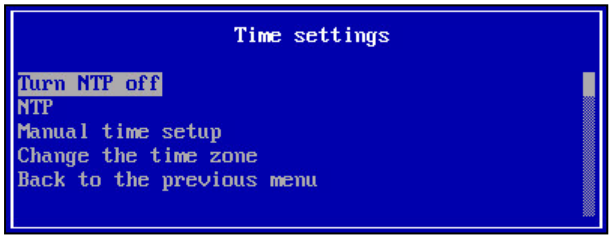
Configure the system time

You can configure the system time in the local menu. You can select a logging time zone and connect to the NTP server using the Security Management Server local menu and the Configuration Manager.

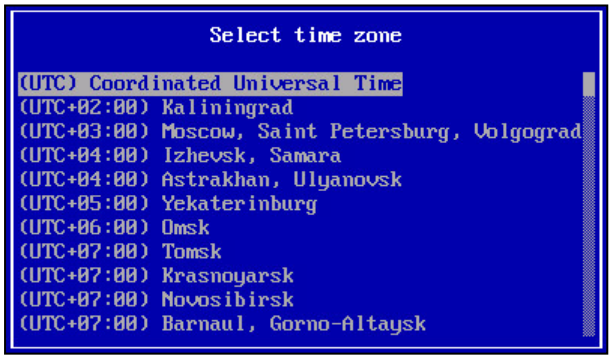
The synchronization using the NTP protocol between the system components is turned on (gateways automatically synchronize time with the Security Management Server) by default.

To configure the system time and a logging zone in the local menu:

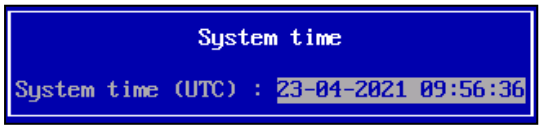
1. In the main menu, select **Settings**, then press **<Enter>**.
   The **Settings** menu appears.
2. Select **System time** and press **<Enter>**.
   The **Time settings** menu appears.



3. Select **Change the time zone** and press **<Enter>**.
   The **Select time zone** menu appears.



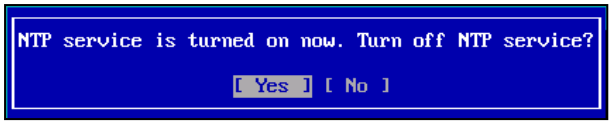
4. Select the required time zone and press **<Enter>**.
   You are returned to the **Time settings** menu.
5. Select **Manual time setup** and press **Enter**.
   The **System time** dialog box appears as in the figure below.



6. Enter the current time according to the UTC standard and press **Enter**.

   Example.
   For Abu Dhabi set 6:05 instead of 12:05.

   The time of the Security Gateway changes with a respective notification.
7. Press **<Enter>** to close the notification dialog box.
   While configuring the system time, an NTP service dialog box appears.



8. Choose the required option and press **<Enter>**.

   You are returned to the **Time settings** menu.

9. Press **<Esc>**.

   The window prompting you to save the changes appears.

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

    All the changes in the system time settings are applied to the automatic startup configuration of the Security Gateway with a respective notification.

11. Press **<Enter>**.

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

12. To apply the new configuration, select **Apply local policy** and press **<Enter>**.

    Wait for the operation to complete.

13. Confirm the changes of the Security Gateway configuration in the Security Management Server (see p. **39**).

To select a logging zone in the Configuration Manager:

1. Open the Configuration Manager and go to **Structure**.
2. Select the required Security Gateway in the list and click **Properties**.

   The **Security Gateway** dialog box appears.

3. On the left, select **Date and Time** section.
4. On the right, select the required time zone for logging in the drop-down list and click **OK**.
5. To apply the settings, click **Install policy** on the toolbar, select system components with modified parameters and click **OK**.

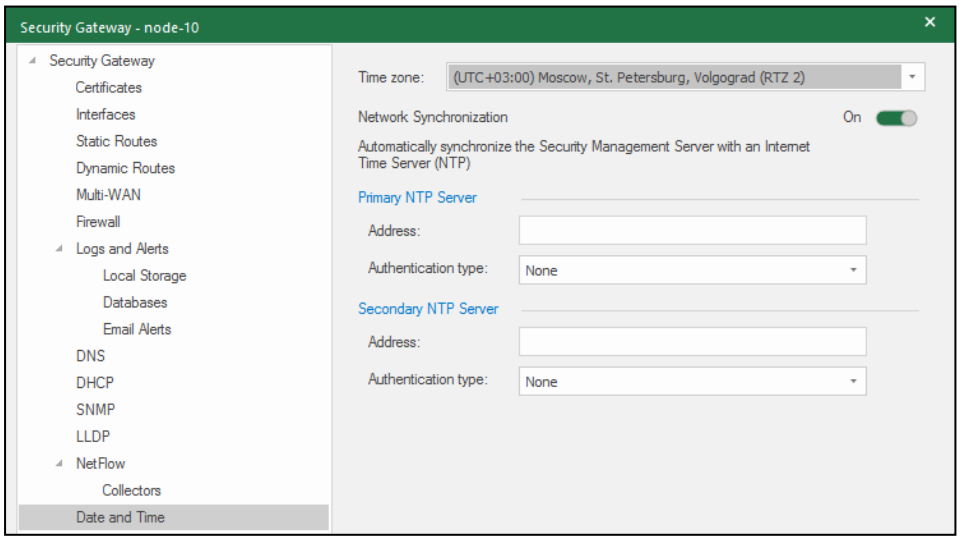
To configure the synchronization between a Security Management Server and the NTP server in the Configuration Manager:

1. In the Configuration Manager go to **Structure**, select the Security management Server and click **Properties**.

   The **Security Gateway** dialog box appears.

2. On the left, select the **Date and Time** section.

   On the right, the current settings of the Security Management Server synchronization via NTP appear.



3. Turn the **Network Synchronization** toggle on.

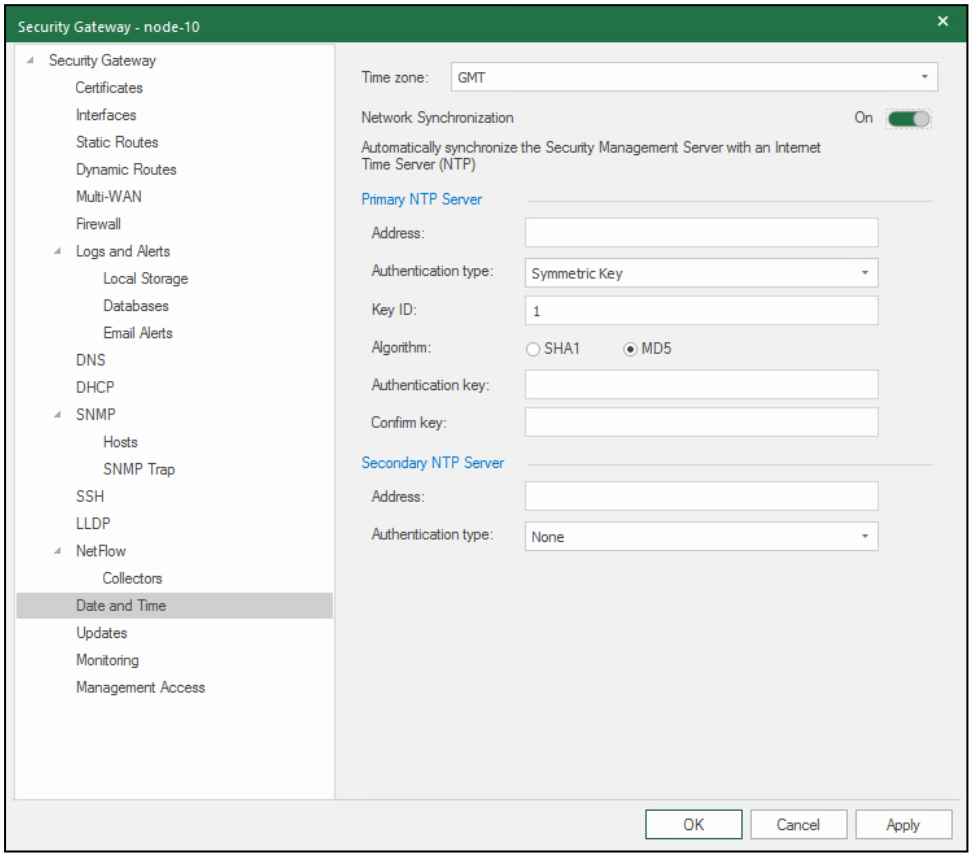
   Parameters of the primary and the secondary NTP server are available for editing.

4. Specify the required parameters.

Attention!
You must specify external NTP server addresses for the active and standby Security Management Server. The active Security Management Server cannot be used as NTP server for the standby Security Management Server and vice versa.

5. If the specified NTP server address uses authentication, in the **Authentication type** drop-down list select **Symmetric Key**. Otherwise, go to the step **7**.

   Additional authentication parameters appear.



6. Specify **Key ID**, **Authentication Key**, **Confirm Key** and select **Algorithm**.
7. Click **OK**.
8. To apply the settings, click **Install policy** on the toolbar, select system components with modified parameters and click **OK**.

To configure the synchronization between a Security Gateway and the NTP server in the Configuration Manager:

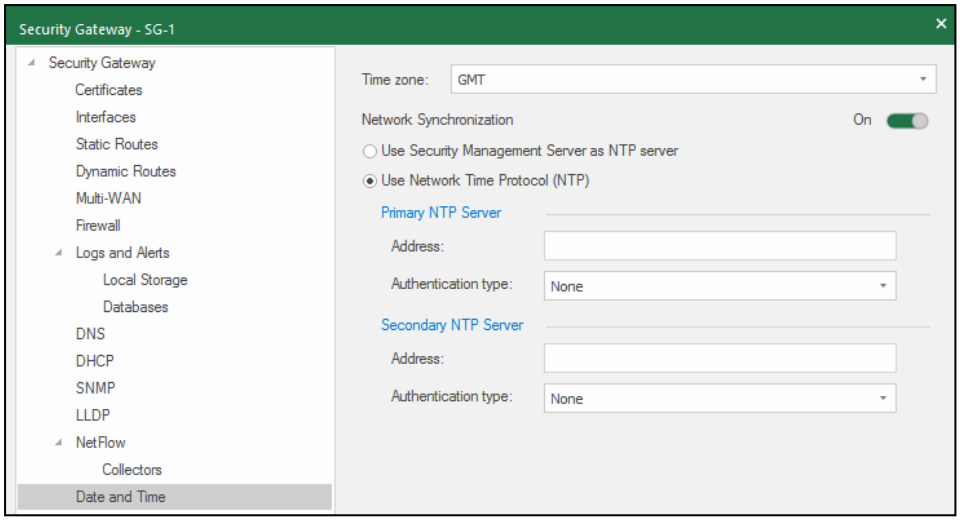
1. In the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Properties**.

   The **Security Gateway** properties dialog box appears.
2. On the left, select the **Date and Time** section.

   On the right, the current settings of the Security Gateway synchronization via NTP appear.
3. Turn the **Network Synchronization** toggle on.

   Options **Use Security Management Server as NTP server** and **Use Network Time Protocol (NTP)** are available.
4. Select **Use Security Management Server as NTP server** and go to the step **9** (optional).
5. Select **Use Network Time Protocol (NTP)** (optional).

   The **Primary** and **Secondary NTP Server** parameters are available for editing.



6. Specify the primary and the secondary NTP server addresses.
7. If the specified NTP server uses authentication, in the **Authentication type** drop-down list select **Symmetric Key**. Otherwise, go to step **9**.

   Additional authentication parameters appear.
8. Specify **Key ID**, **Authentication Key**, **Confirm Key** and select **Algorithm**.
9. Click **OK**.
10. To apply the settings, click **Install policy** on the toolbar, select system components with modified parameters and click **OK**.

To configure the system time via NTP in the Security Management Server local menu:

1. In the main menu, select **Settings** and press **<Enter>**.

   The **Settings** menu appears.
2. Select **System time** and press **<Enter>**.

   The **Time settings** menu appears.
3. Select **NTP** and press **<Enter>**.

   The **NTP settings** menu appears.
4. Select **Set up external NTP servers IP** and press **Enter**.

   NTP servers settings appear.

5. Type the IP addresses of NTP servers, press **<Enter>** and return to the previous menu.

Attention!
You should specify external NTP server addresses for the active and standby Security Management Server. The active Security Management Server cannot be used as NTP server for the standby Security Management Server and vice versa.

6. Press **<Esc>**.

   The window prompting you to save the changes appears.
7. Select **Yes** and press **<Enter>**.

   All the changes in the system time settings are applied to the automatic startup configuration of the Security Gateway with a respective notification.
8. Press **<Enter>**.

   You are returned to the **Settings menu**.
9. To apply the new configuration, select **Apply local policy** and press **<Enter>**.

   Wait for the operation to complete.

10. Confirm the changes of the Security Gateway configuration in the Security Management Server (see p. 39).

To configure the system time via NTP in the Security Gateway local menu:

1. In the main menu, select **Settings** and press **<Enter>**.

   The **Settings** menu appears.
2. Select **System time** and press **<Enter>**.

   The **Time settings** menu appears.
3. If the synchronization via NTP is turned off, select **Turn NTP on/off internal NTP server usage** and press **<Enter>**.

   The **Internal NTP server usage:** dialog box appears.
4. To use Security Management Server as NTP, select the respective option and press **<Enter>**.

   The **NTP settings** menu appears.
5. If you do not want to use the Security Management Server as the NTP server, select the respective option and press **<Enter>**.

   You are returned to the **NTP settings** menu.
6. Select **Set up external NTP servers IP** and press **<Enter>**.

   NTP server settings appear.

7. Enter the IP addresses of NTP servers, press **<Enter>** and return to the previous menu.

   Note.
   Use the arrows to navigate.
8. Press **<Esc>**.

   The window prompting you to save the changes appears.
9. Select **Yes** and press **<Enter>**.

   All the changes in the system time settings are applied to the automatic startup configuration of the Security Gateway with a respective notification.
10. Press **<Enter>**.

    You are returned to the **Settings menu**.
11. To apply the new configuration, select **Apply local policy** and press **<Enter>**.

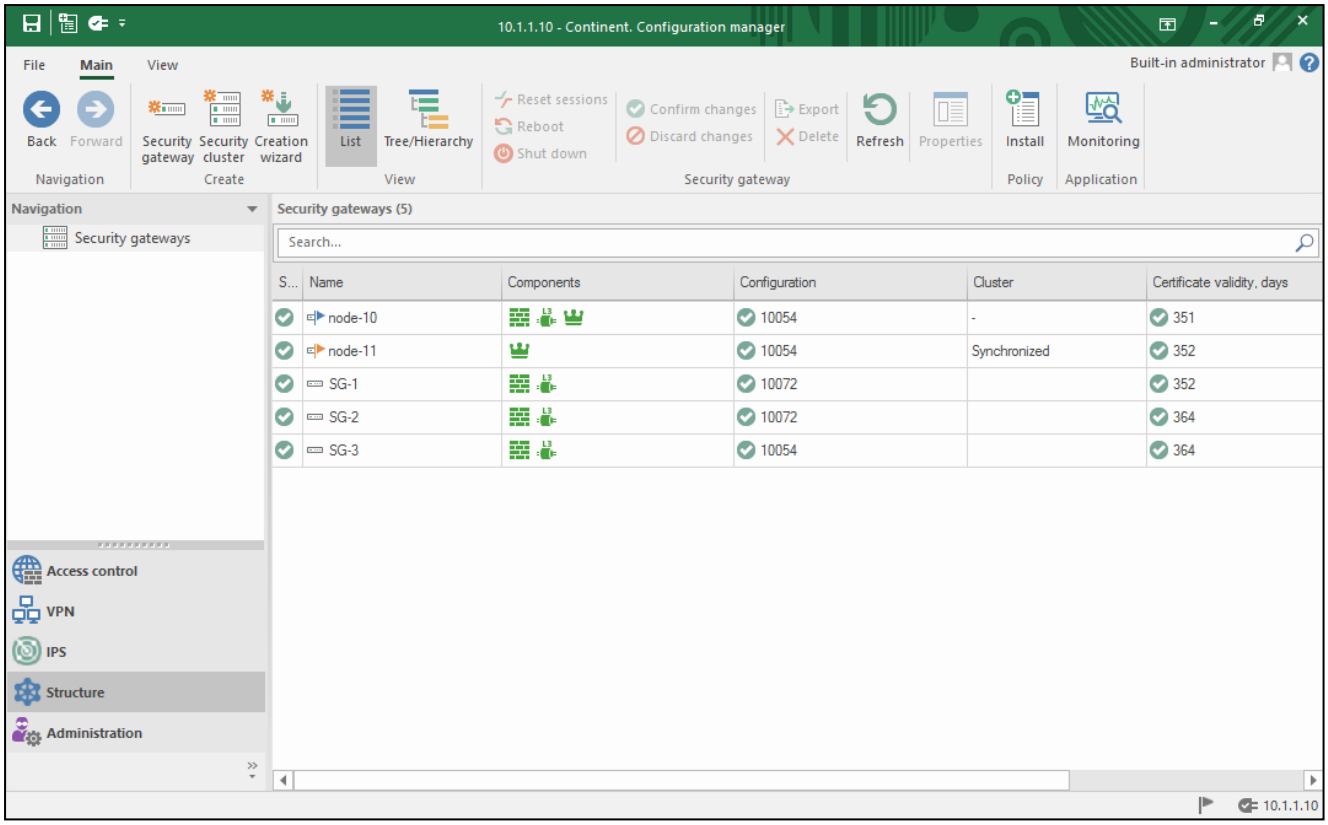
    Wait for the operation to complete.
12. Confirm the changes of the Security Gateway configuration in the Security Management Server (see p. 39).

View properties

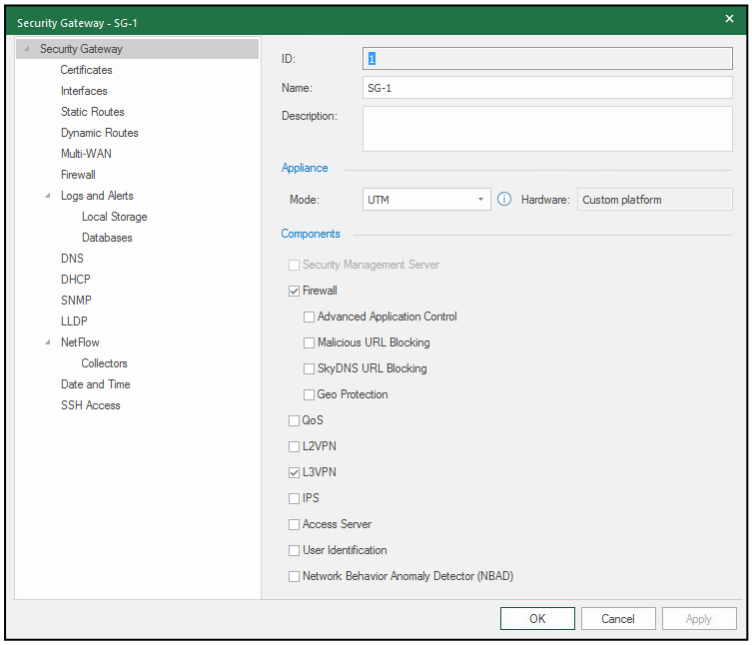
To view device properties using the Configuration Manager:

1. Go to **Structure**.

   The list of Security Gateways appears as in the figure below.



2. In the display area, select the required Security Gateway and click **Properties** on the toolbar.
   The **Security gateway** dialog box appears.



   The left side of the dialog box contains the sections of the Security Gateway settings. The right side contains the respective parameters.

3. To return to **Structure**, click **OK**.

To view device information in the local menu:

1. In the main menu, select **Information** and press **<Enter>**.
   The **Information** menu appears.

2. Select **Device** and press **<Enter>**.

   A menu that displays the device information appears.

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

Configure the Security Gateway

The Security Gateway configuration changes made in the local menu are saved in the local DB. Then, the configuration is confirmed by the administrator and becomes the active configuration of the Security Gateway. A notification about the changes is automatically sent to the Security Management Server while the Configuration Manager is displaying the active configuration as local one until it is confirmed by the administrator. The local configuration is active until new local changes are applied or the policy is installed using the Configuration Manager.

Transfer configuration changes

After you change settings of any Continent component (including the Security Management Server), take one of the following steps:

- in the Configuration Manager, save changes to the Security Management Server DB and install the policy on the Security Gateway with the changed configuration (see p. **37**);

  Note.
  If the Security Gateway has no connection to the Security Management Server, transfer a new configuration using a USB drive (see p. 36).

- in the local menu, save the new configuration in the local DB and send changes to the Security Management Server (see below), after that, the administrator should confirm changes on the Security Management Server (see p. **38**).

  Note.
  If the administrator discards the changes (see p. 38), the Security Gateway still has its local configuration. To roll back to the configuration of the Security Management Server, install the policy on the Security Gateway (see p. 37);

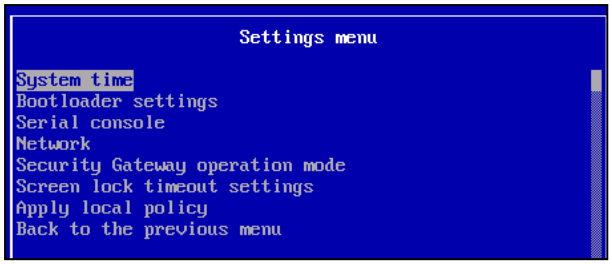
  The Security Gateway configuration changes made from the local menu are overwritten by the configuration changes from the Configuration Manager if the configuration is changed from both the local menu and the Configuration Manager at the same time. In the local menu, you can change addresses of Security Gateway interfaces, Security Management Server addresses, NTP settings, DNS settings and static routes. These changes are saved to the local database as an unconfirmed configuration. Then, the changed configuration is applied to the Security Gateway and, if no errors occur, the configuration becomes confirmed and is set as the active one for this Security Gateway. The active configuration is valid until you make new changes or install a policy in the Configuration Manager. The information about a new configuration is sent to the Security Management Server. The configuration becomes active in the Security Management Server database right after an administrator confirms it in the Configuration Manager.

  If the connection between the SG and the SMS is interrupted when local changes are being applied, than the local changes will be applied on the SG only and not be sent to the SMS. Before reboot, the message "There are not applied local changes" in the local menu of the SG. After connection recovery, you must send the information about the local changes to the SMS (see below).

To send configuration changes using the local menu:

1. In the main menu, select **Settings** and press **<Enter>**.

The **Settings menu** appears.



2. Select **Apply local policy** and press **<Enter>**.

   The Security Gateway configuration is saved to the local DB. A service data packet that contains the configuration changes is created and sent to a queue to be recorded in the Security Management Server DB with the respective sequence number.

   When the procedure is successfully finished, the respective message appears.

   Note.
   If the Security Management Server is not available when you apply a local policy, send local changes to the Security Management Server (select **Send local changes to the Security Management Server** in the **Tools menu**) when the connection is established.

3. Press **<Enter>**.

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

Transferring configuration changes without connection to the Security Management Server

If you want to change the Security Gateway configuration without connection to the Security Management Server, export the configuration file onto a USB drive using the local menu of the Security Management Server and then, import this configuration file to the Security Gateway.

To export the configuration file on a USB drive (only on the Security Management Server):

1. In the main menu, select **Tools** and press **<Enter>**.

   The **Tools menu** appears.

2. Select **Export node configuration to medium** and press **<Enter>**.

   The **Export policy** dialog box appears.

3. Insert a USB drive, type ID of the required Security Gateway and press **<Enter>**.

   Attention!
   The drive must be cleared before using.

   When the configuration file is saved on the drive as the **policy.json** file, the respective message appears.

To import the configuration from an external media:

1. In the main menu, select **Tools** and press **<Enter>**.

   The **Tools menu** appears.

2. Select **Import local policy from file**, insert the drive and press **<Enter>**.

   A dialog box where you should select the configuration file appears.

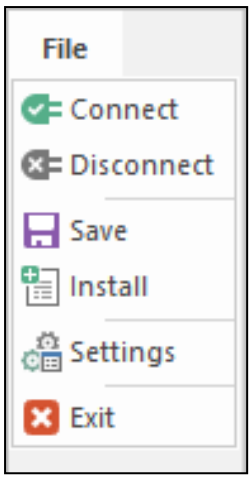
3. Select the required file and press **<Enter>**.

   When the policy is successfully installed, the respective message appears.

Save changes in the Security Management Server configuration

To save changes in the Security Management Server configuration:

- In the top left corner of the Configuration Manager, click  , then click **Save**.



Note.
You can also save changes as follows:
- press **Ctrl + S**;
- on the toolbar, click .

Install a policy

To apply changes to the Security Gateway configuration, install a policy on the Security Gateway. To install the policy, a task is created (see p. **39**). The progress of the task is displayed in the **Notification center**. The more changes to be applied, the more time is required to perform the task.

In the local menu, you can set timeouts for task execution. If they are exceeded, the policy installation task will fail, even if the policy is installed as a result. Default timeouts are the following:

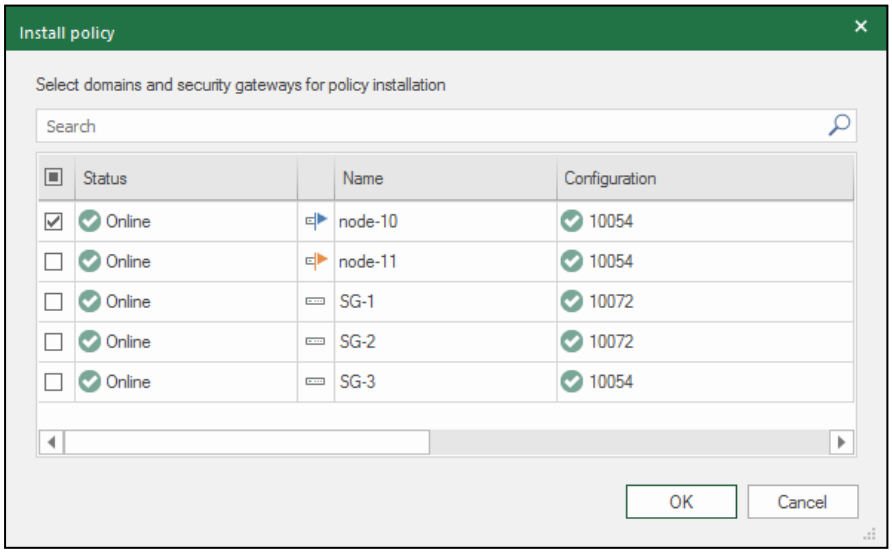
- 200 s — timeout for the task creation and initiation;
- 600 s — timeout for the task execution.

To install a policy:

1. Press <**Ctrl**>+<**I**>.

   Note.
   You can also open the **Install policy** dialog box in the **Access control**, **VPN** and **Structure** sections. To do so, on the toolbar, click **Install**.

   The **Install policy** dialog box appears.



2. Select the required Security Gateway and click **OK**.
   A policy installation task is created. A respective notification appears.
3. Click **OK**.

The notification closes.

The system starts to perform the new task if no other tasks are being performed. A number of current tasks in the queue is indicated by a numeral next to .

4. For detailed information about current tasks, click .

   The list is sorted by the time the tasks were added. When the task is completed, the respective icon appears. Then, the task is removed from the **Notification center**.

To configure the policy installation timeout:

1. In the local menu, select **Settings** and press **<Enter>**.

   The **Settings** menu appears.

2. Select **Settings of the policy install process** and press **<Enter>**.

   The **Policy installation settings** dialog box appears. It contains default timeout parameters.

3. Configure the required parameters and press **<Enter>**.
4. When the parameters are successfully changed, the respective message appears. Press **<Enter>**.

Manage the Security Gateway configuration

After you change the subordinate Security Gateway parameters and send local changes to the Security Management Server, appears in the **Configuration** column of the Security Gateway list. This icon indicates that the Security Gateway has local configuration that is not confirmed by the administrator.

The administrator can either confirm or discard changes of the Security Gateway parameters using the Configuration Manager.

The following icons indicate different states of the Security Gateway configuration:

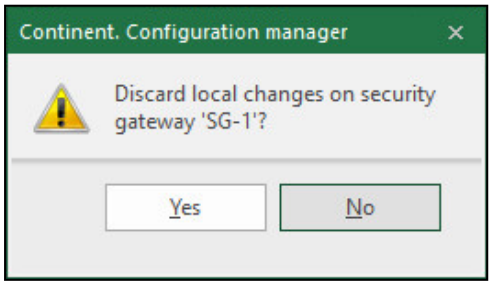
Icon	Configuration state	Note
	Not confirmed on the Security Management Server	Local changes of the Security Gateway configuration are to be confirmed
	Does not match the Security Management Server configuration	The Security Management Server DB contains the Security Gateway configuration changed in the Configuration Manager, the policy is not installed
	Confirmed on the Security Management Server	The Security Gateway configuration matches the configuration in the Security Management Server DB

To discard the Security Gateway configuration changes:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Discard changes** on the toolbar.

   The dialog box prompting you to confirm the action appears.

2. Click **Yes**.



   The configuration icon changes to .

3. To apply changes, install the policy on the Security Gateway (see p. **37**).

The icon changes a new numerical configuration value. The configuration sent from the Security Management Server is now active on the Security Gateway.

To confirm the Security Gateway configuration changes using the Configuration Manager:

1. In the Configuration Manager, on the navigation panel, click **Structure**.
2. In the list of the Security Gateway, select the required one and, on the toolbar, click **Confirm changes.** In the appeared dialog box, click **Yes**.

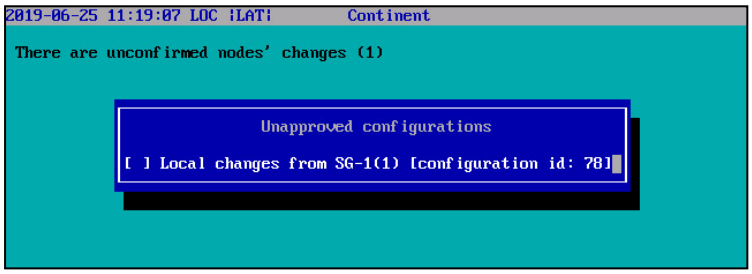
> **Note.**
> For detailed information about merge conflicts, see p. 35.

The icon in the **Configuration** column changes to the new numeral configuration value.

To confirm the Security Gateway configuration changes in the Security Management Server local menu:

1. In the **Tools menu**, select **Approve local changes for node** and press **<Enter>**.

   A dialog box appears as in the figure below.



2. Select the required option, press **<Space>**, then press **<Enter>**.

   A message appears as in the figure below.

3. Press **<Enter>**.

   The changes of the Security Gateway configuration are saved in the Security Management Server DB. You are returned to the **Tools menu**.
4. To return to the main menu, press **<Esc>**.

Task list

When you install a policy on the Security Gateway, the respective task is created. The Security Management Server starts performing the task if there are no tasks being performed at the moment. If there is a task being performed, the new task is registered in the system and moved to the queue.

Information about the tasks is stored on the Security Management Server as a list. The information contains the following:

- **Name**;
- **Owner** is a user who initialized the task;
- **Status** (**Done**, **Executing**, **Registered**, **Failure**, **Attention**);
- **Progress** (in percent);
- **Added**;
- **Started**;
- **Executing**.

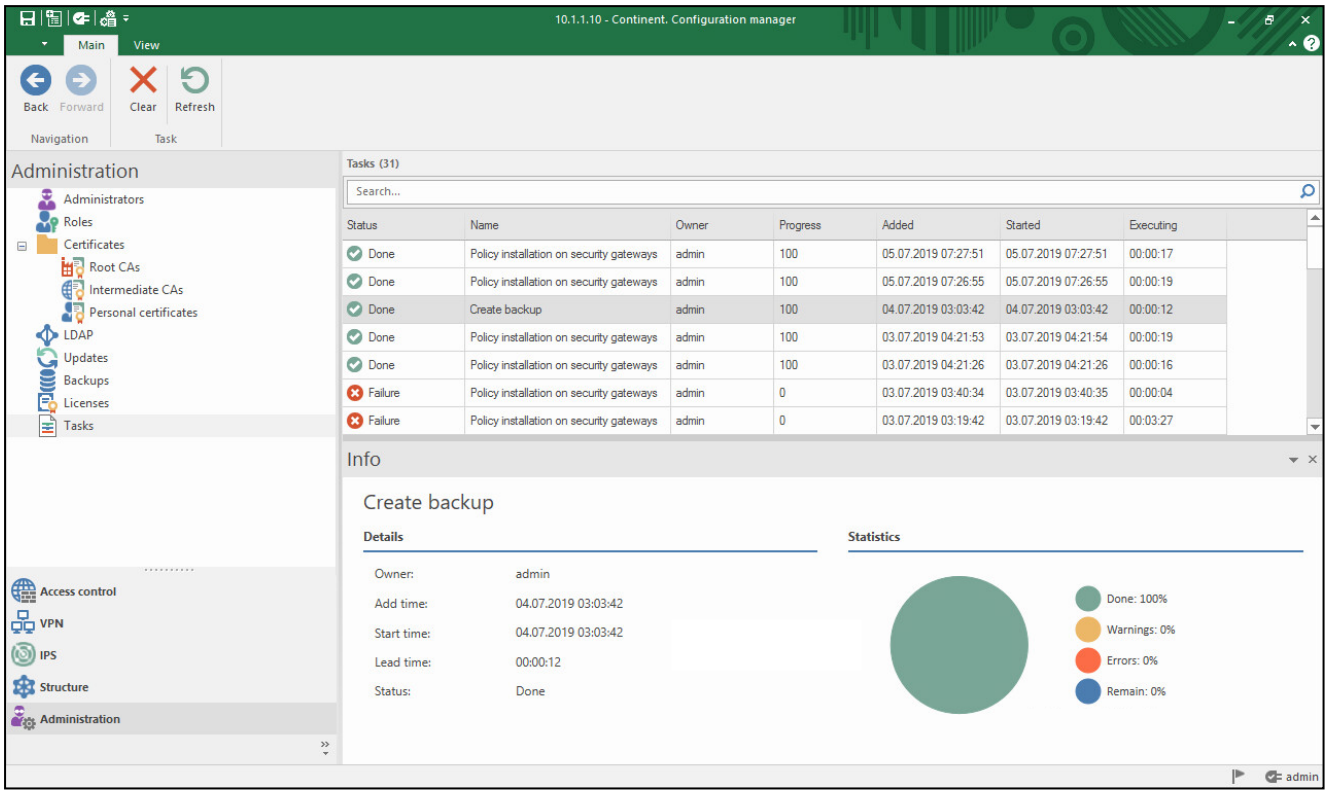
To view the task list:

1. Open the **Administration**, click **Tasks**.

   The list of tasks is shown on the display area.

Note.

You can open the task list from any section of the Configuration Manager. To do so, click , then, in the appeared **Notification center**, click the **Move to task list** link.



The following icons indicate the task status:

Icon	Status	Note
	Registered	In a queue
	Executing	Performing at the moment
	Done	Successfully finished
	Warning	Finished successfully but some errors occurred
	Failure	Finished with error

2. Select a required task in the list.

   Detailed information about the task being performed for each Security Gateway is shown in the **Info** dialog box.

3. To clear the list, on the toolbar, click **Clear**.

Attention!

This action is irreversible.

All the tasks but with the **Executing** and **Registered** status are deleted.

Operation diagnostics

To perform operation diagnostics:

1. In the local menu, select **Tools** and press **<Enter>**.

   The **Tools menu** appears.

2. Select **Diagnostics** and press **<Enter>**.

   A menu where you can select the required diagnostics type appears.

Option	Description
Network diagnostics	Performs diagnostics of network connection using the **ping**, **traceroute**, **arp** commands
View properties	View the list of network connections with the ability to control current connections
Command line	Enables switching to the console mode with a set of available commands is limited
RAID status	Checks RAID state
Technological report	Creates technological report that can be transmitted to software developers and exports it on a USB drive
Back to previous menu	Returns to the **Tools** menu

3. Select the required option and press **<Enter>**.

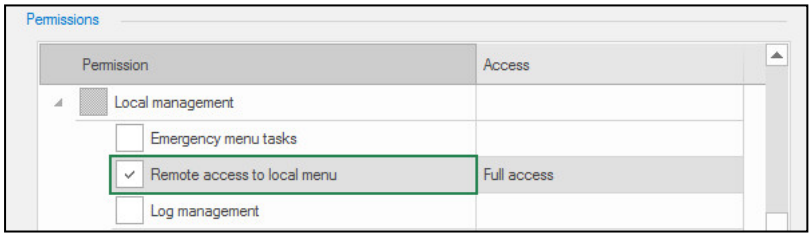
Configure remote access via SSH

To obtain access via SSH, configure the administrator account and add its remote IP to a list of allowed IP addresses. The maximum number of network objects that can be granted access through the SSH protocol — 10.

You can configure remote access in the local menu or in the Configuration Manager.

To grant remote access privileges to an administrator:

1. In the Configuration Manager, create a new role (see p. **20**) and, in the **Role** dialog box, in the **Permissions** section, select **Remote access to local menu** in the **Local management** group.



2. Save changes to the Security Management Server configuration (see p. **36**).
3. To add the created role, select the required administrator account or create a new one (see p. **23**).
4. In properties, go to the **Roles** tab, add the role created during step **1** and click **OK**.

To create a list of allowed IP addresses in the local menu:

1. In the local menu, select **Settings** and press **<Enter>**.

   The **Settings menu** appears.
2. Select **Network** and press **<Enter>**.

   The **Node network settings** menu appears.
3. Select **Set up SSH access** and press **<Enter>**.

   A dialog box appears as in the figure below.

4. Type the required IP address of a remote host in the form of **xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx** or a subnetwork with its prefix the following way: **xxx.xxx.xxx.xxx[/xx]**. Press <**Enter**>.

   A message appears asking you to wait until the operation is complete. When it is done, press <**Enter**>.

The **SSH settings** menu appears.

5. If you want to add another IP address to the list, repeat the procedure starting from step **3**.

> **Note.**
> To delete an IP address, select the required one, press <**Delete**> until the line is clear, then press <**Enter**>.

6. Select **Back to previous menu** and press <**Enter**>.

   The **Settings menu** appears.

7. Select **Apply local policy** and press <**Enter**>.
8. When the procedure is successfully finished, the respective message appears. Press <**Enter**>.
9. Confirm the Security Gateway configuration changes in the Configuration Manager or in the Security Management Server local menu (see p. **38**).

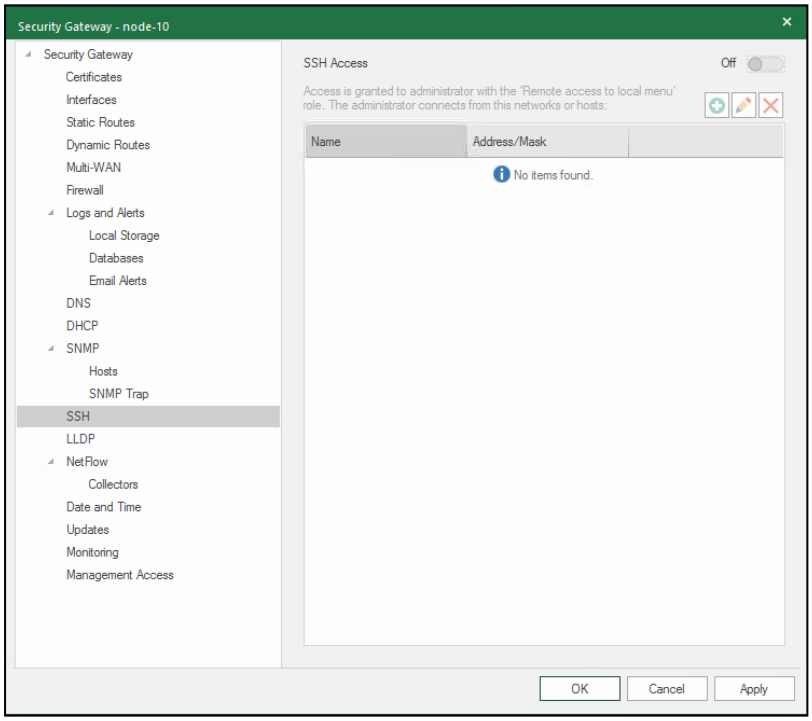
To create a list of allowed IP addresses in the Configuration Manager:

1. Select the required **Security Gateway** and click **Properties** on the toolbar.

   Security Gateway dialog box appears.

2. On the left, go to **SSH Access**.

   Respective parameters appear on the right.



Access settings contain the following:

- Enabling/disabling SSH access to the **Security Gateway**;
- Creating a list of the network objects that are granted SSH access to the **Security Gateway**.

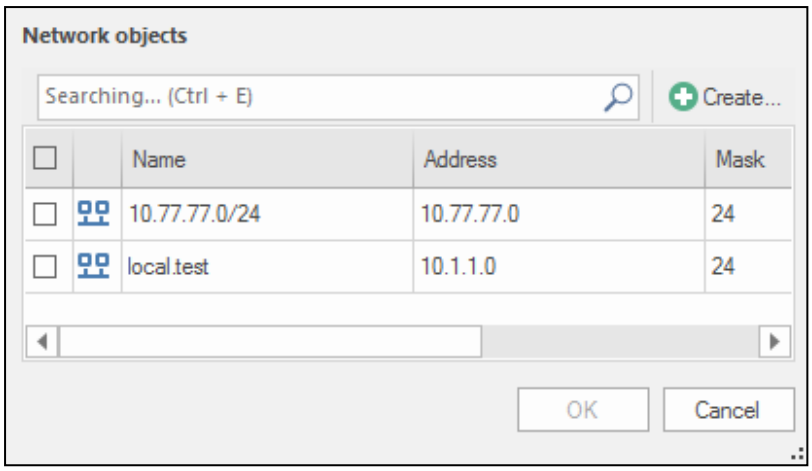
> **Attention!**
> After installing software, SSH access to the **Security Gateway** is disabled by default.

3. To enable SSH access and create a list of the network objects that are granted SSH access to the **Security Gateway**, select **Secure Shell Access**.

   The buttons used for creating a list of network objects that are granted SSH access to the **Security Gateway** become available:

4. To add a network object to the list, click  .

   A dialog box with a list of recorded network objects in the Security Management Server Database appears on the screen.

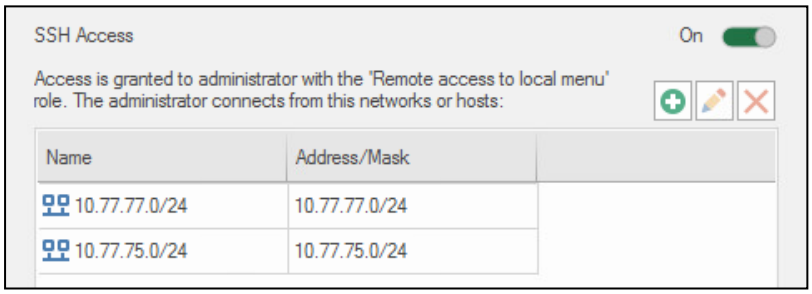


5. Select the objects that are to be granted SSH access to the **Security Gateway**.

Note.
You can create a new network object and add it to the list. To do this, click **Create** and specify the parameters of the new object.

6. Click **OK**.

   The selected network objects are added to the list of the network objects that are granted SSH access to the **Security Gateway**.



7. You can edit the list using the buttons:

8. Click **OK**.

   You are returned to the list of the Security Gateways.

9. Save the configuration in the Security Management Server Database and install the policy on this **Security Gateway**.

To disable SSH access to the Security Gateway in the Configuration Manager:

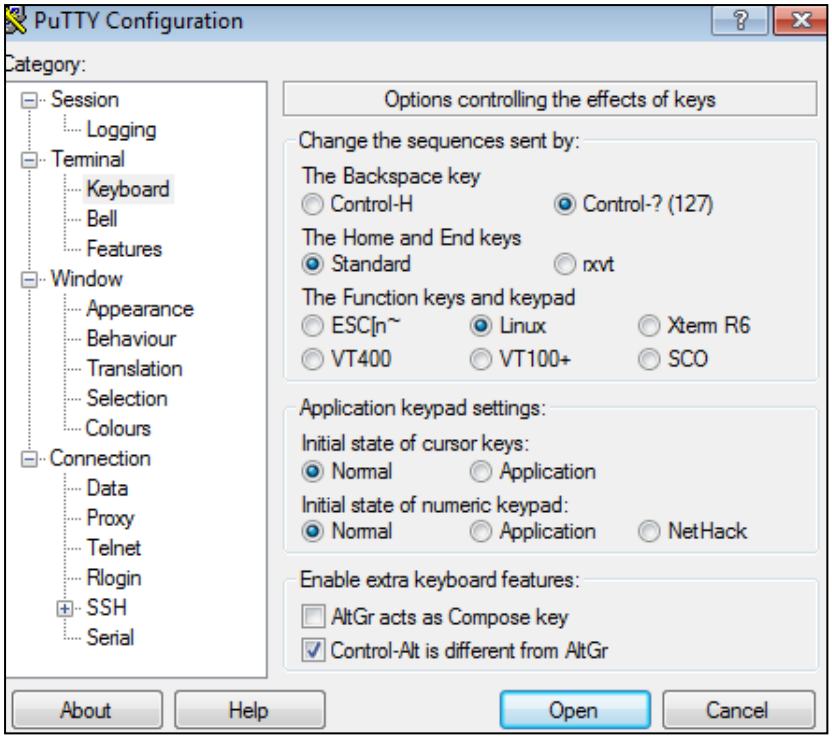
1. Select the required Security Gateway and click **Properties** on the toolbar.
2. On the left, go to the **SSH Access**.
3. Clear the **Secure Shell Access** check box and click **OK**.

   SSH access mode is disabled.
4. Save the configuration in the Security Management Server Database.

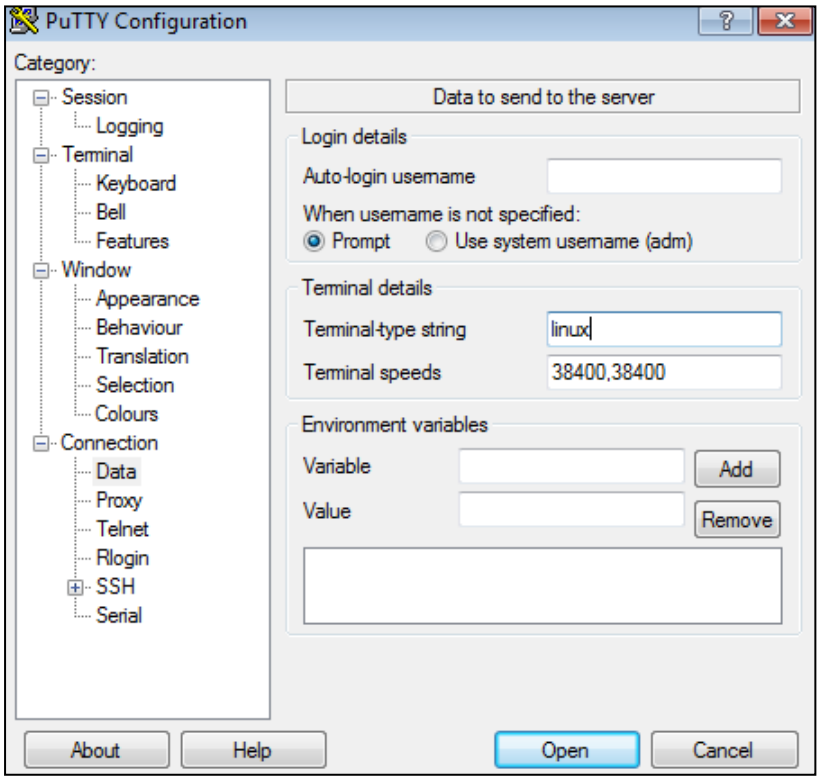
Configure the SSH client

To configure PuTTY:

1. Run the program.
2. On the left, select **Terminal** | **Keyboard**.



3. In the **The function keys and keypad** group box, select **Linux**.
4. On the left, select **Connection** | **Data**.



5. In the **Terminal-type string** text box of the **Terminal details** group box, enter **Linux**.

Control Security Gateways via SNMP

To control the Security Gateways using network object management tools via SNMP, you can use a module that enables SNMP service.

Attention!
SNMP module operates only in the mode that supports responding to **GetRequest**.

You can check the following parameters:

- the Security Gateway operation time since power-on;
- the number of received/sent packets;
- interfaces status (Up/Down), etc.

For detailed information about SNMP, see [**8**].

Connect portable devices to the Security Gateway

Attention!
You can connect a portable device only to the local menu.

To manage the Security Gateway, you can use a portable device (e.g. a laptop) connected through the console port.

You can connect the portable device using an RJ-45-DB-9 cable. A laptop must be equipped with a terminal emulator (e.g. PuTTY).

Attention!
A serial port can be disabled by default. You can enable it in the platform BIOS (in **Advanced** switch the **Serial Port** and **Serial Port Console Redirection** parameters to **Enabled**).

Connect one end of the cable to the 9 pin serial port connector of the laptop, then connect the other end of the cable to the RJ-45 connector on the front panel of the network device.

Run the terminal emulator on the laptop and specify the following parameters:

Parameter	Value
Port	Specify value from Device Manager of the laptop
Bits per second	115200
Connection type	serial
Data bits	8
Without parity check	Yes
Stop bits	1
Encoding	UTF-8
Function keys and keyboard	Linux

Connect to the serial port with the specified parameters. If the local menu has not appeared, press <**Esc**>, then press <**Enter**>.

Automatic logon timeout cannot be equal to 0. This parameter means the time after which the OS starts. "0" means that the automatic OS startup is disabled. The default value of the parameter is 5 seconds.

When connecting using the serial port, you need to log on Sobol as a user (without presenting a security token). The OS starts automatically when automatic logon timeout is over.

If you log on to Sobol as a user but **Automatic logon timeout** is 0, the OS will not start. You need to present a security token. When the RNG test is finished, Sobol shows invalid security token data. Press <**Enter**> to change the image on the screen, then press <**Enter**> again to start the OS.

If you log on Sobol as an administrator (by presenting a security token), the OS will not start. In this case, you need to press <**Enter**> to change the image on the screen, then press <**Enter**> again to start the OS.

Attention!
When you have finished working using the serial port, disable it in the platform BIOS (in **Advanced** switch the **Serial Port** and **Serial Port Console Redirection** parameters to **Disabled**).

To manage connections using the Security Gateway local menu:

1. In the **Main menu** of the Security Gateway, select **Settings** and press **<Enter>**.
   The **Settings** menu appears.
2. Select **Serial console** and press **<Enter>**.
   The **Serial console settings** dialog box appears.

3. To forbid the connection through the console port, select **Turn off serial console** and press **<Enter>**.

   You receive the message about the serial console shutdown.

4. Press **<Enter>**.

   The name of the option in the **Serial console settings** menu changes to the opposite.

5. To connect through the console port, select **Turn on serial console** and press **<Enter>**.

   You receive the message about the serial console initiation containing recommendations about the data transfer speed and data bits.

6. Press **<Enter>**.

   The name of the option in the **Serial console settings** menu changes to the opposite.

To manage connections in BIOS:

Note.
To navigate between tabs and options of BIOS, use the navigation keys to select the option or change its state, then press **<Enter>**.

1. Turn on the Security Gateway and enter BIOS.

   Note.
   Usually you can press **<Del>** to enter the menu, but on some platforms you can press **<F1>**, **<F2>**.

   The dialog box prompting a password appears.

2. To enter BIOS, type the current password (by default it is 123456) and press **<Enter>**.

   The BIOS setup menu appears. The kind and contents of the menu depends on the Security Gateway platform type and BIOS version. BIOS version LN010AISC.003 is described further. The menu of other BIOS versions can vary.

3. Go to advanced settings, select **Serial Port Console Redirection**.
4. To connect through the console port, **Console Redirection** must have the **Enable** value.
5. To forbid the connection through the console port, **Console Redirection** must have the **Disable** value.
6. To view the connection settings through the console port, select **Console Redirection Settings**.

   Note.
   We do not recommend changing the connection settings through the console port.

7. Save the changes and close the BIOS settings menu.

   The Security Gateway restarts.

Restart and shutdown

The main administrator can restart and shut down a Security Gateway.

To restart/shut down a Security Gateway in the Configuration Manager:

1. Select the required Security Gateway in the **Structure** and click **Reboot** or **Shut down** on the toolbar.

   The request to confirm the option appears.

2. Click **Yes**.

   According to the selected option, the Security Gateway restarts or shuts down.

To restart/shut down the Security Gateway in the local menu:

1. In the local menu, select **Power off** and press **<Enter>**.
   The request to select the option appears.

2. Select the required option and press **<Enter>**.
   According to the selected option, the Security Gateway reboots or shuts down.

Delete a Security Gateway

To delete a Security Gateway:

1. In the Configuration Manager, go to **Structure**.
   The list of Security Gateways appears .
2. To delete a Security Gateway, select it and click **Delete** on the toolbar.
   The request to confirm the deletion appears.
3. Click **Yes** in the dialog box, then save the Security Management Server configuration changes (see p. **36**).
4. To apply the configuration, install the policy on the Security Management Server (see p. **37**).
   The Security Gateway is deleted from the Security Management Server database.

Chapter 5
Backup and failover

Backup and restoration

In the local menu of a Security Gateway, you can create a backup of the Security Gateway database or restore it from a backup file.

Attention!
If you reinitialize the Security Gateway, you need to restore the database right after the reinitialization has been finished before creating the Security Gateway CSR.

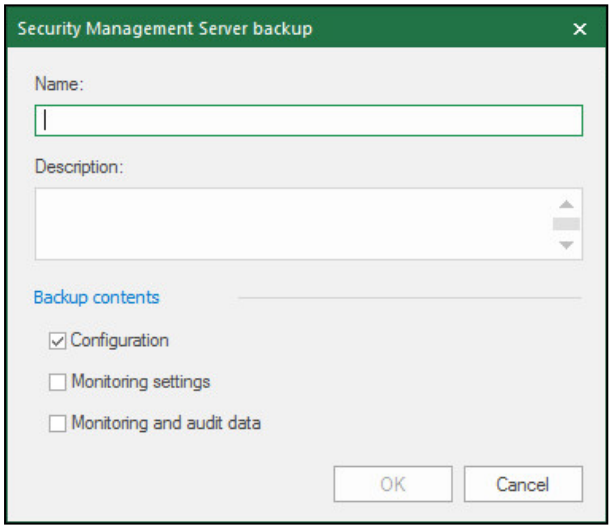
You can also manage the Security Management Server database backups via the Configuration Manager.

Create a backup

To create a Security Management Server database backup using the Configuration Manager:

1. In the Configuration Manager, go to **Administration** and select **Backups**.
2. On the toolbar, click **Backup**.

   The **Security Management Server backup** dialog box appears.

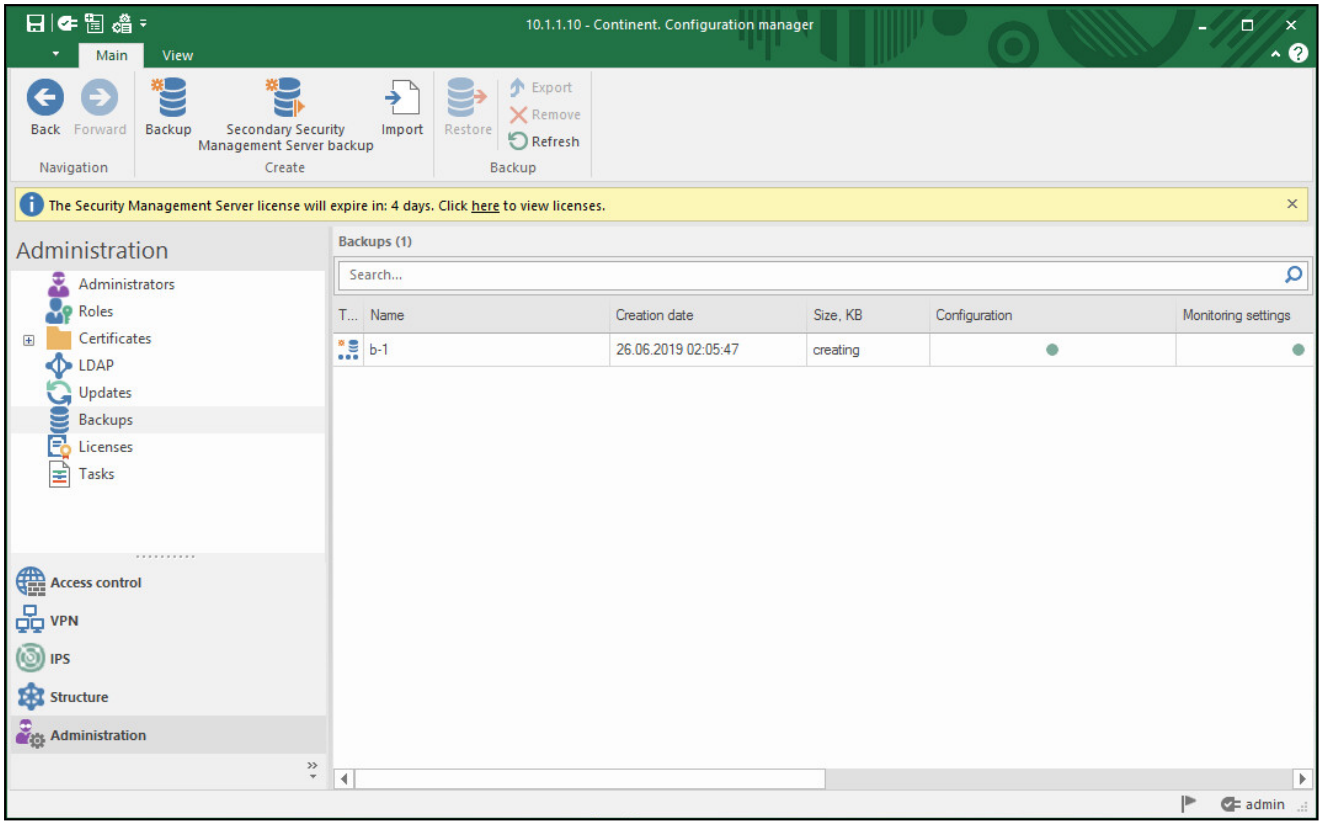


Note.
If there is an unsaved configuration of the Security Management Server, the dialog box prompting you to save changes appears.

3. Specify the name and description in the respective fields, select the content required to save and click **OK**.

   The system starts creating a backup and the respective position appears in the list of backups. During the backup creation the **Size** column shows **Creating** and a respective icon appears near the name of the backup.

Note.
To create a backup of a standby Security Management Server, click **Standby Security Management Server backup** on the toolbar. In the list, the icon of a standby Security Management Server backup is .



To create a backup in the local menu:

1. In the main menu, select **Tools** and press **<Enter>**.

   Tools menu appears.
2. Select **Backup and restore** and press **<Enter>**.

   The respective menu appears.
3. Select **Backup** and press **<Enter>**.

   The message prompting you to insert a USB drive appears.
4. Insert a USB drive and press **<Enter>**.

   The **Bases to create backup** dialog box appears.
5. Select the required options by pressing **<Space>** and **<Enter>**.
6. If you have selected **Monitoring and audit data**, the dialog box prompting to back up the search engine data will appear. Select the required option and press **<Enter>**.

   The backup is created and saved to the USB-drive. The message of the successful backup creation appears. The name of the file is **backup_ID_YYYYMMDD_HHMMSS.c4b**, where:
   - ID — the ID of the Security Gateway;
   - YYYYMMDD_HHMMSS — date and time of creation.

Restore from a backup

You must re-install a software update and vendor rules after the restoring from a backup (see [**9**]).

Attention!

When restoring the SMS from a backup copy that contains an expired update license, the component without a proper license will not operate until a valid license is added.

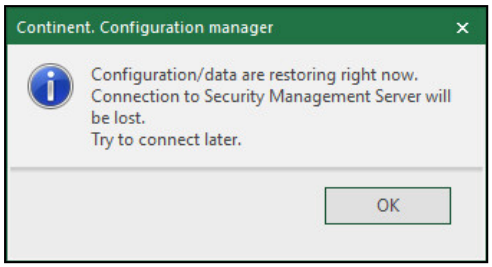
To restore components from the Security Management Server database backup using the Configuration Manager:

1. In the **Administration** of the Configuration Manager, select **Backups**.
2. Select a required backup and click **Restore** on the toolbar.

   The **Backup** dialog box appears.

3. Select the components required to restore and click **OK**.

   The system starts restoring the configuration and the respective message appears.



Note. Task list in the Configuration Manager is not restored.

To restore the Security Gateway configuration from the Security Management Server database backup:

Note.
This procedure is required in case of loss or compromising of Security Gateway key information.

1. If the Security Gateway is unavailable in the current Security Management Server configuration, restore a working Security Management Server configuration from its backup.
2. In the Configuration Manager, create a Security Gateway certificate, select it in the Security Gateway properties and export the Security Gateway configuration.
3. Reinitialize the Security Gateway in **Tools menu** and configure connection to the Security Management Server in the local menu. After the procedure has been finished, check whether the connection is established in the Configuration Manager.
4. In the Configuration Manager, delete the previous Security Gateway certificate and confirm local changes in the security gateway configuration (see p. **38**).
5. If you have restored the Security Management Server configuration in step **1**, install the policy on all the Security Gateways (see p. **37**).

Note.
After you have restored the security cluster configuration, we recommend creating a full backup of the Security Management Server configuration (see p. 48).

To restore the Security Gateway configuration from the backup in the local menu:

Attention!
The Security Management Server does not receive changes in the Security Gateway configuration after it has been restored from the backup on a Security Gateway. The Security Management Server will receive only local changes after it is restored from the backup on the Security Management Server.

1. In the main menu, select **Tools** and press **<Enter>**.

   Tools menu appears.
2. Select **Backup and restore** and press **<Enter>**.

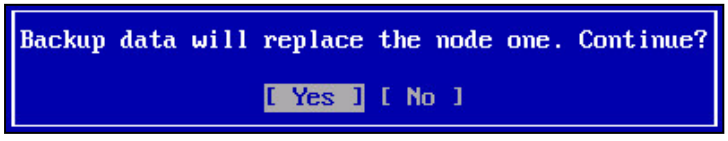
   Backup and restore appears.
3. Select **Restore from backup** and press **<Enter>**.

   The message prompting to insert a USB drive appears.
4. Insert a USB drive and press **<Enter>**.

   Select backup appears.
5. Select the required file and press **<Enter>**.

   Bases to restore appears.
6. Select databases required to restore by pressing **<Space>** and press **<Enter>**.

   The confirmation for replacing all data appears.



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

   The system restores the configuration from the backup stored in the USB drive. The message about the successful restoration from the backup appears.
8. If the IP address of the Security Management Server interface to which the Security Gateway was connected has been changed after the backup has been created, you must specify it as an alternate IP address and, if necessary, add it to the routing table.
9. If the Firewall operation mode of the Security Gateway has been changed in the restored configuration, restart the Security Gateway (see p. **46**).
10. If the IP address of the Security Management Server interface to which the Security Gateway was connected has not been changed while restoring from the backup, go to step **13**.
11. In the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.

    The properties of the required Security Gateway appear.
12. On the left, select the **Interfaces** section and specify the IP address to which the Security Gateway will be connected.
13. Click **OK**, then save the configuration by clicking in the top left corner of the Configuration Manager.
14. Install the policy on the Security Gateway with the restored configuration (see p. **37**).

Manage backups

To export a Security Management Server database backup:

1. In the Configuration Manager, go to **Administration** and select **Backups**.

   The list of backups appears in the display area.
2. Select a required backup in the list and click **Export** on the toolbar.

   The File Explorer dialog box appears.
3. Select the location and specify the name for the exported backup file, then click **Save**.

   The selected backup is successfully exported. The respective message appears.
4. Click **OK**.

To import a Security Management Server database backup:

1. In the Configuration Manager, go to **Administration** and select **Backups**.

   The list of backups appears in the display area.
2. Click **Import** on the toolbar.

   The File Explorer dialog box appears.
3. Select a required backup file and click **Open**.

   The backup is successfully uploaded and appears in the list. The respective message appears.
4. Click **OK**.

To delete a Security Management Server database backup:

1. In the Configuration Manager, go to **Administration** and select **Backups**.

   The list of backups appears in the display area.
2. Select a required backup in the list and click **Remove** on the toolbar.

   The dialog box prompting you to confirm the action appears.
3. Click **Yes**.

   The selected backup has been successfully deleted.

Security Management Server hardware redundancy

Attention!

A platform that can manage a number of Security Gateways connected to the Security Management Server must be used as a standby Security Management Server.

To provide Continent with Security Management Server hardware redundancy, you can deploy one or more standby Security Management Servers. In case of the active Security Management Server failover, the standby Security Management Server takes over network management functions of the active one.

Note.
While creating a personal or an intermediate certificate, only root certificates issued on the active Security Management Server are available for their signature.

For proper operation, each standby Security Management Server requires a license with Security Management Server privileges.

All the standby Security Management Server must have the same software version.

To provide Security Management Server replication, the active and standby Security Management Servers synchronize their databases and files in real time.

Note.
We recommend exporting root certificates with private keys beforehand (see p. 67) to ensure the possibility of restoring access to Continent if the primary SMS is out of order including scheduled maintenance and repair. The procedure for transferring the SMS to another SG (standby SMS) is given on p. 85.

The process of the standby Security Management Server deployment is described in [**1**].

You can perform management operations (install and modify a policy, edit user accounts and objects) only on the active Security Management Server.

There are two ways of using the standby Security Management Servers:

- The standby Security Management Server is on 24/7. The active and standby Security Management Server databases are synchronized by transferring changes.
- The standby Security Management Server is on only for database synchronization and set to active in case of the active Security Management Server failure.

There are the following synchronization types:

- **Full** — while deploying the standby Security Management Server. Databases of the active and standby Security Management Server are synchronized by transferring all the information to the standby Security Management Server database.

  After you have initialized the standby Security Management Server, you cannot perform synchronization of changes (see below). You can perform full synchronization in the two following ways:

  - by transferring the whole database of the active Security Management Server to the standby Security Management Server using the database synchronization channel;
  - by transferring the whole database using a USB drive.
- **Synchronization of changes** — after the deployment of the standby Security Management Server and full database synchronization.

You can synchronize databases in the two following ways:

- manually at any time (synchronously — the whole database at full synchronization, asynchronously — synchronization of changes);
- automatically when modifying the Security Management Server database (asynchronously — synchronization of changes).

The synchronization status indicates the Security Management Server state respectively to the Security Management Server the Configuration Manager is connected to.

When the Configuration Manager is connected to the active Security Management Server, the synchronization status can be:

- **Synchronized** — databases of the active and standby Security Management Servers contain the same information;
- **Unsynchronized** — infromation in the standby Security Management Server database differs from infromation in the active Security Management Server database;
- **Conflict** — the active Security Management Server database is newer than the standby one.

When the Configuration Manager is connected to the standby Security Management Server, the synchronization status can be:

- **Synchronized** — databases of the active and standby Security Management Servers contain the same information;

- **Synchronizing** — databases of the active and standby Security Management Servers are currently synchronizing;
- **Conflict** — the active Security Management Server database is older than the standby one.

When the Configuration Manager is connected to the standby Security Management Server, the synchronization statuses are not displayed.

When the Configuration Manager is connected to the active Security Management Server and the standby Security Management Server status cannot be defined, the synchronization status of the standby Security Management Server is set to **Undefined**.

When the Configuration Manager is connected to the standby Security Management Server and the active Security Management Server status cannot be defined, the synchronization status of the active Security Management Server is set to **Undefined**.

Manage Security Management Server redundancy

To manage the Security Management Server replication, in the Configuration Manager, go to **Structure**.

In the Configuration Manager, the following pictograms are used for managing the standby Security Management Server replication:

Pictogram	Description	State
	Active Security Management Server	-
	Standby Security Management Server	Synchronized

To synchronize the standby and active Security Management Servers:

1. In the Configuration Manager, go to **Structure**, right-click the standby Security Management Server and select **Replication | Synchronize**.

   This command is available only for the standby Security Management Server.

   The dialog box prompting you to confirm the action appears.

   Note.
   Use **<Ctrl>** for multiple choice.

2. Click **Yes**.
3. The synchronization starts and the progress bar appears.
4. When the operation is completed, the standby Security Management Server has the **Synchronized** state.

To make the active Security Management Server standby:

1. In the Configuration Manager, go to **Structure**, right-click the Security Management Server and select **Replication | Make standby**.

   This command is available only for the active Security Management Server.

   The dialog box prompting you to confirm the action appears.

2. Click **Yes**.

   The respective message appears.

3. The connection to the active Security Management Server will be lost.
4. After reconnecting to the Security Management Server, it has the **Standby** state.

To make the standby Security Management Server active:

1. In the Configuration Manager, go to **Structure**, right-click the required Security Management Server and select **Replication | Make active**.

   This command is available only for the standby Security Management Server if there are no active ones.

   The dialog box prompting you to confirm the action appears.

2. Click **Yes**.

   The respective message appears.

3. The connection to the active Security Management Server will be lost.

Note.
Changing the role can take several minutes. The role will not change if the logon to the Security Management Server was performed before changing the role. In this case, it is required to connected in several minutes.

4. After reconnecting to the Security Management Server, it has the **Active** role.

Troubleshooting

Synchronization network failure with operational Security Management Server

If the synchronization network Security Management Server is down and the control channel is up, the following situations may occur:

1. After you have connected from the Configuration Manager to the active Security Management Server, the standby Security Management Server state is **Disconnected**.
2. If the synchronization channel is restored but automatic synchronization of changes is not available and one or all the standby Security Management Servers are not synchronized, you should perform the full synchronization using the Configuration Manager.

   If the synchronization channel is not restored but you need the standby Security Management Server database, you should perform the full synchronization by exporting the active Security Management Server databases to the USB drive.
3. After you have connected from the Configuration Manager to the standby Security Management Server without making it active, the synchronization status of the active Security Management Server database is **Up-to-date**.

   After the synchronization channel has been restored, you should synchronize databases of the active and standby Security Management Servers.
4. After you have connected from the Configuration Manager to the standby Security Management Server with making it active, the state of the active Security Management Server is set to **Standby**.

   It may happen after making the active Security Management Server standby, but its database version is newer. In this case, the synchronization status of this Security Management Server is set to **Conflict**. An administrator should decide, which database version is more relevant and perform the full synchronization using the synchronization channel after the synchronization channel is restored or by transferring the database using a USB drive before the synchronization channel is restored.

Security Management Server failure

If the active Security Management Server fails to operate:

1. Connect from the Configuration Manager to the standby Security Management Server and make it active. Then, you should check the state of the other standby Security Management Server databases and perform the full synchronization if necessary.
2. After the active Security Management Server has been restored without initializing and connecting to the network, you should make the restored Security Management Server standby. Synchronization state is **Disconnected**. If the synchronization of changes is not available, you should perform the full synchronization.

Restoring Security Management Server databases from a backup

If you restore the active Security Management Server database from a backup, the standby Security Management Server database is more relevant. The synchronization status is **Conflict**. In this case, the synchronization of changes is unavailable. You should perform the full synchronization and export the database to all the standby Security Management Server.

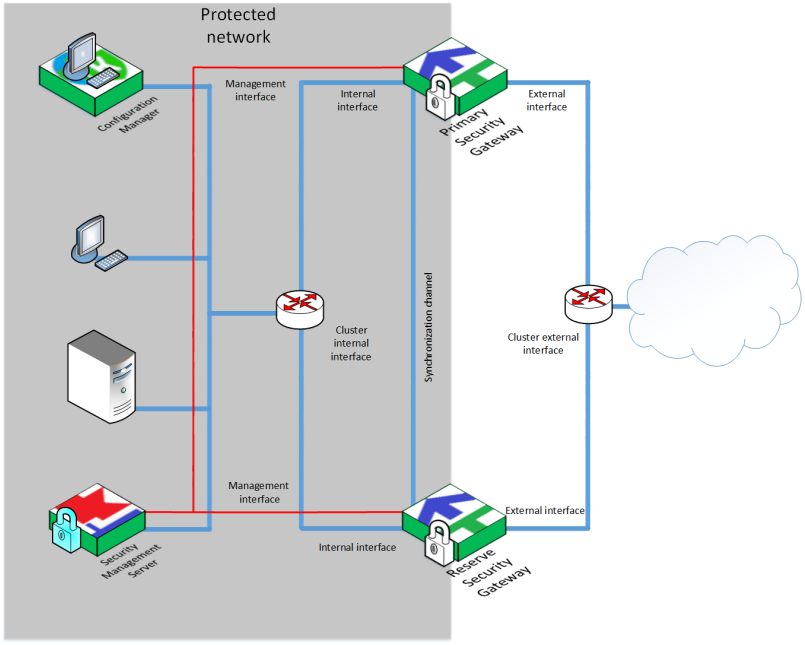
Manage a failover security cluster

Security cluster operating conditions

A failover security cluster provides hardware redundancy of the Security Gateway. If the active security cluster member loses its operability, the system switches to the standby Security Gateway and it automatically takes on functions of the active Security Gateway.

Note.
Hardware redundancy in IPS mode is not supported.

An example of a security cluster connection is in the figure below.



Cluster members have the following features:

- They have internal interfaces on which main IP addresses are assigned. In a cluster, a secondary IP address is assigned to the respective internal interface of an active SG for traffic in transit to pass.
- They have external interfaces on which main IP addresses are assigned. In a cluster, a secondary IP address is assigned to the respective external interface of an active SG for traffic in transit to pass.
- Each cluster member has its own IP address.

  Note.
  Secondary IP addresses are specified when creating a cluster. IP addresses of the cluster interface and its members must belong to one subnet.
- Every cluster member has its own MAC address.
- Members in a cluster can be **Active** or **Standby**.
- In the ARP cache of neighboring hosts, the IP address of the cluster corresponds to the MAC address of the cluster member in the **Active** state.

The proper operation of a security cluster requires the following:

- Security cluster members must have:
  - a license with the same set of components, including hardware redundancy (see p. **15**);
  - the same hardware platforms;
  - the same software versions;
  - the synchronized system time (see p. **29**).
- You cannot connect **1st sync** interfaces of both security cluster members to the both internal and external interfaces of these members. To connect **1st sync** interfaces, use a separate network.
- The communication channel between interfaces of security cluster members must support L2 framing.
- For a cluster to work in Web/FTP filtration mode, a SSL/TLS inspection certificate must be created for both cluster members (see [**2**]).

If a security cluster operates properly, the administrator can switch the status of a security cluster member to **Active**. This status means:

1. A security cluster member is operative (see p. **64**).
2. A active security cluster member has been selected automatically or by administrator (see p. **64**).
3. A higher position in the security cluster member list. The operative Security Gateway in the beginning of the list is the primary one. It is considered only if you have selected the **Auto-switch at primary Security Gateway recovery** check box.

Attention!
If you switch an active Security Gateway in a security cluster with **User identification** and **Access server** enabled, user sessions are not synchronized.

The active security cluster member is marked with  in the Security Gateway list of the Configuration Manager.

A security cluster member can have the following states:

- **OK** (in case of software update of a security cluster component — **updated OK**);
- **Attention** (an active Security Gateway that can process traffic but there are limitations or events the administrator must be informed about);
- **OK, not ready** (a Security Gateway cannot process traffic because of incorrect settings or inaccessible interfaces);
- **Problem**;
- **Down** (a deactivated security cluster Security Gateway that does not pass traffic but is currently working and can be configured);
- **Unavailable** (shut-down or disconnected from a communication channel);
- **Busy** (you cannot manage the security cluster in any way while a policy is being installed on it. Two security cluster members cannot be **Busy**).

See how failures and Security Gateway states correspond to each other on p. **83**.

A security cluster can operate in the following states:

- **OK**;
- **Attention** (both Security Gateways can process traffic);
- **Critical** (only one Security Gateway can process traffic);
- **Problem** (both Security Gateways cannot process traffic);
- **Offline** (both Security Gateways are down or unavailable).

See the table of security cluster states on p. **84**.

See the list of logged security cluster events on p. **85**.

Create a security cluster

To create a security cluster, take the following steps:

- Deploy the Security Gateways for the security cluster (see [**1**]).

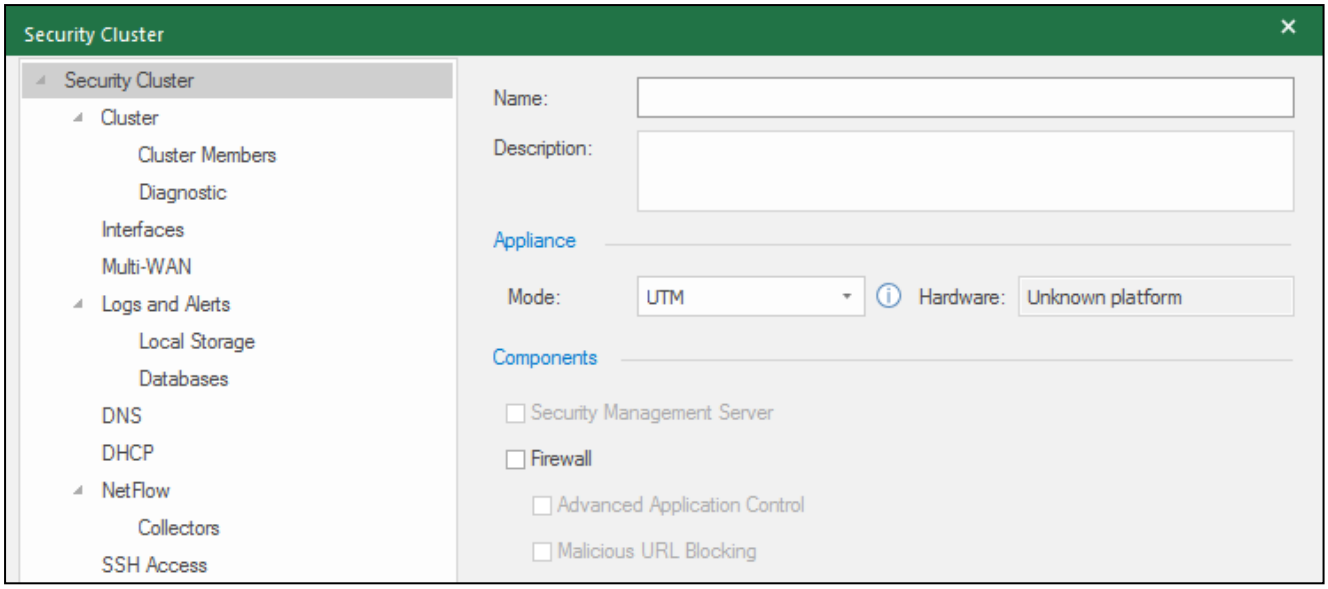
  Attention!
  Before you add a Security Gateway to a security cluster, make sure that **Access control** and **VPN** (L3 and RA) rules do not include this Security Gateway. You can add only two Security Gateways to a security cluster. LLDP is not supported on a cluster. To make LLDP work on the SG from a cluster, configure it on each SG separately.

- Register the security cluster (see below).
- Configure security cluster interfaces (see p. **58**).
- Configure synchronization of the security cluster elements (see p. **58**).
- Configure additional security cluster parameters (see p. **58**).
- Create and bind a SSL/TLS inspection certificate to work in Web/FTP filtration mode (see [**2**]).
- Install a policy on the security cluster and its members (see p. **37**).

After you have created a security cluster in the Configuration Manager, the member icons will switch to  and a cluster icon will be  .

To register a security cluster:

1. In the Configuration Manager, go to **Structure** and click **Security cluster** on the toolbar.
   The respective dialog box appears.



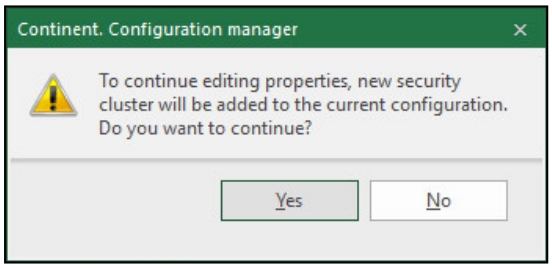
2. Specify the name and description in respective fields and select the time zone.

Attention!

- The **Name** can contain only Latin letters, numbers and "-". The length cannot exceed 32 symbols.
- All members of the security cluster require the same time zone for MAS to operate correctly.

3. On the left, select **Cluster**, then click **Cluster Members**.

The dialog box prompting you to save the current configuration appears.

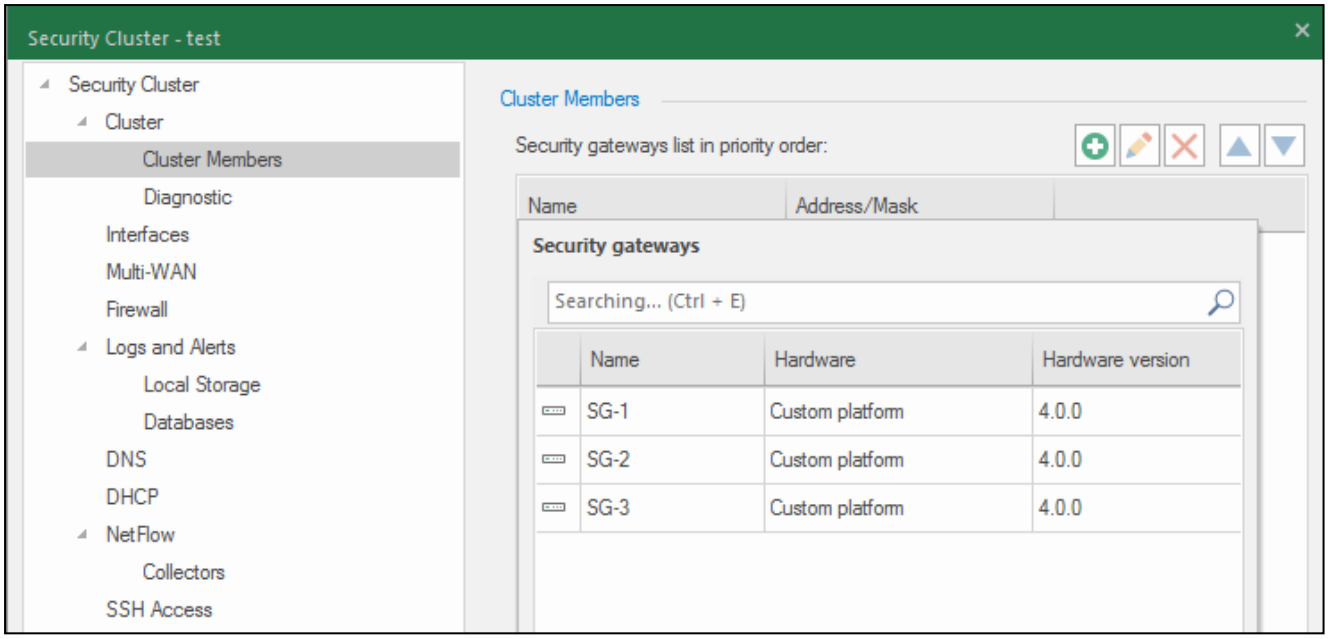


4. Click **Yes**.

The list of security cluster Security Gateways appears. It is empty by default.

5. To add a Security Gateway, click .

The list of existing Security Gateways registered in the Configuration Manager appears.

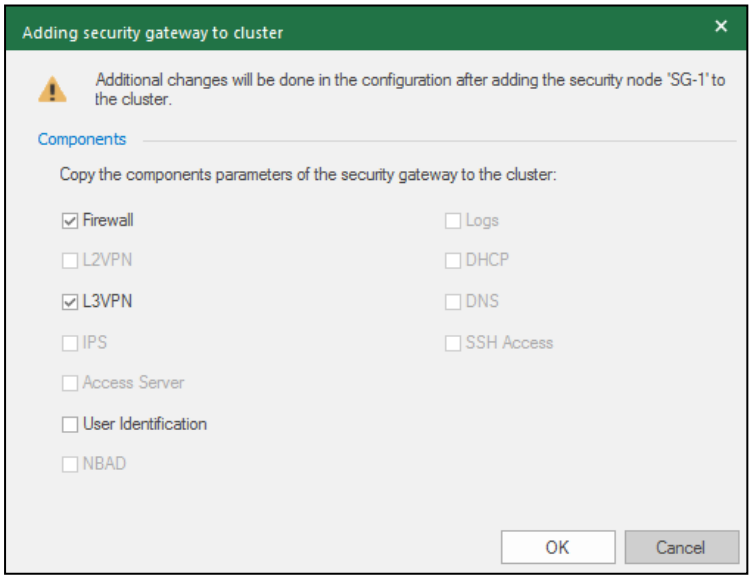


6. Select the required Security Gateway.

Note.
The Security Gateway placed on the top of the list is the primary security cluster member and gets the active status by default. To change the priority use  .

If the selected Security Gateway has certain settings not specified in security cluster settings before, the dialog box prompting you to transfer them to the security cluster configuration appears. Select required options and click **OK**.

Attention!
The Security Gateway settings different to the settings of the security cluster will be deleted without warning.



The selected Security Gateway appears in the list.

Note.
When transferring settings of DHCP server or relay, you need to select interfaces of its configuration again.

7. To add a reserve Security Gateway, repeat steps **5-6** and click **Apply**.

Make a security cluster member active

There are two ways for a security cluster member to become active:

- done automatically;
- done by user.

While operating, a security cluster automatically makes the security cluster member active according to the current device state (see below). At the same operability level of members, the administrator can also make a security cluster member active.

Note.
While changing active cluster with configured dynamic routing or Multi-WAN, the time of a traffic restoring is extended.

To make the security cluster member active:

1. In the Configuration Manager, go to **Structure**.
2. Right-click the required Security Gateway and click **Set active**.
   At the same operability level, the required Security Gateway becomes active.

Configure a security cluster

Note.
When configuring a cluster and external equipment to work with Security Cluster, take into consideration the fact that a Security Gateway in a cluster interacts with external services initiating its own queries from the Security Gateway address, not the cluster address.
For example, WEB/FTP filtering, where a DNS server must be configured. The administrator specifies the DNS server in the cluster settings but a module that performs WEB/FTP filtering intercepts a customer's query and initiates a new connection from the Security Gateway address, not the cluster address.

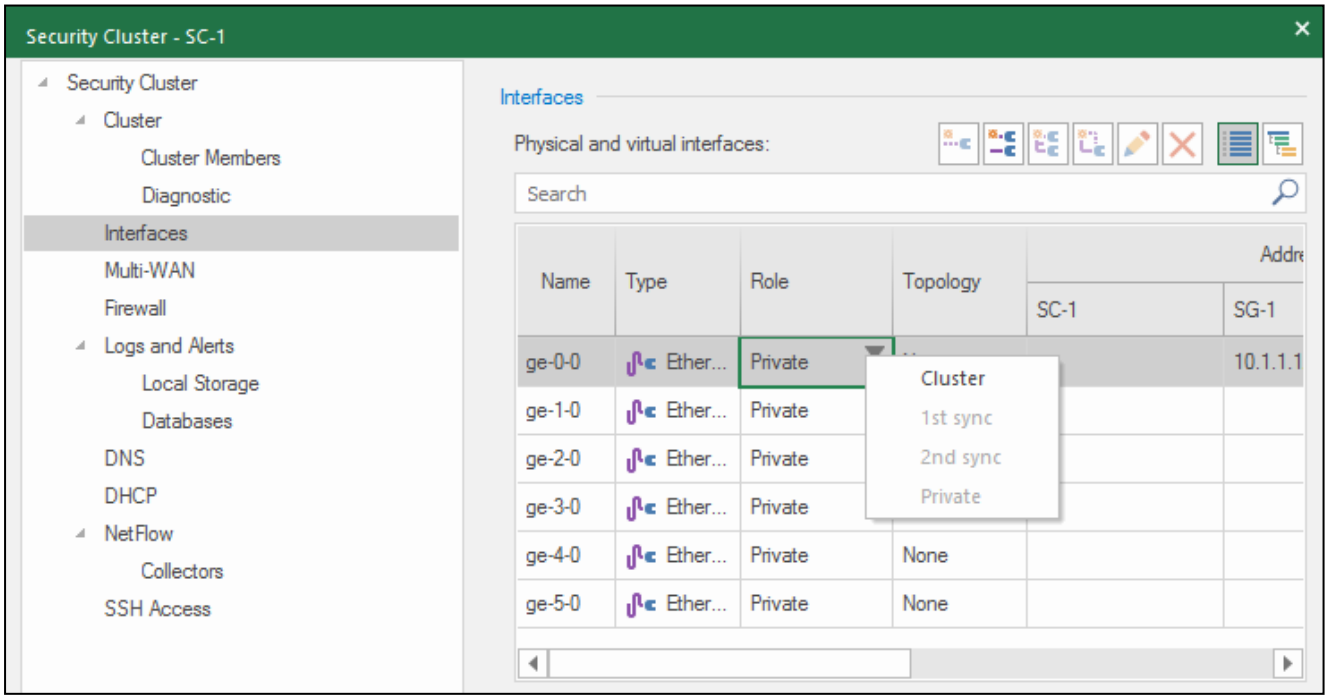
After you have modified the Security Management Server configuration, save it and install the policy on the security cluster (see p. **36**).

Configure security cluster interfaces

You can modify network parameters of security cluster Security Gateway interfaces with the **Private** role only in Security Gateway properties, network parameters of security cluster interfaces with the **Cluster** role — in security cluster properties.

To configure interfaces:

1. On the left, of the **Properties** dialog box, select **Interfaces**.
   The list of interfaces imported from Security Gateway parameters appears on the right.



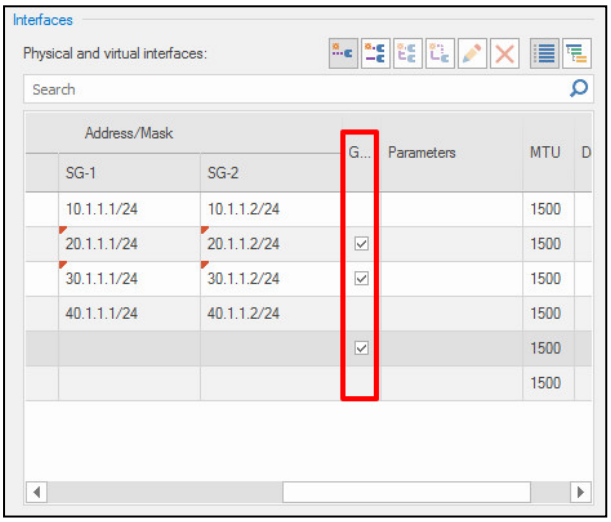
2. Select the role for each interface of the security cluster and modify the other parameters if necessary. Specify IP addresses for external and internal interfaces of the security cluster. IP addresses of the security cluster virtual interfaces and its members must be in the same subnet for each interface.

Note.
Empty required fields or incorrect ones are marked with in the top left corner. On mouseover, the tooltip appears.

Role	Description
Cluster	For the connection between the security cluster and a secure or external network
1st sync	For the synchronization between the security cluster members. You must use only physical interfaces (you cannot use VLAN and bond). It is not necessary to specify the IP addresses of the security cluster for the **1st sync** role but the **2nd sync** interfaces need the internal topology type and specified IP addresses to pass transit traffic. Subnets, which IP addresses are in use on the **1st sync** and **2nd sync** interfaces, cannot be used in NAT rules
2nd sync	
Private	For the connection between a Security Gateway and a secure or external network. This interface does not support synchronization

By default, the monitoring system controls the operability of security cluster interfaces. To turn off the monitoring, clear check boxes in the respective fields.

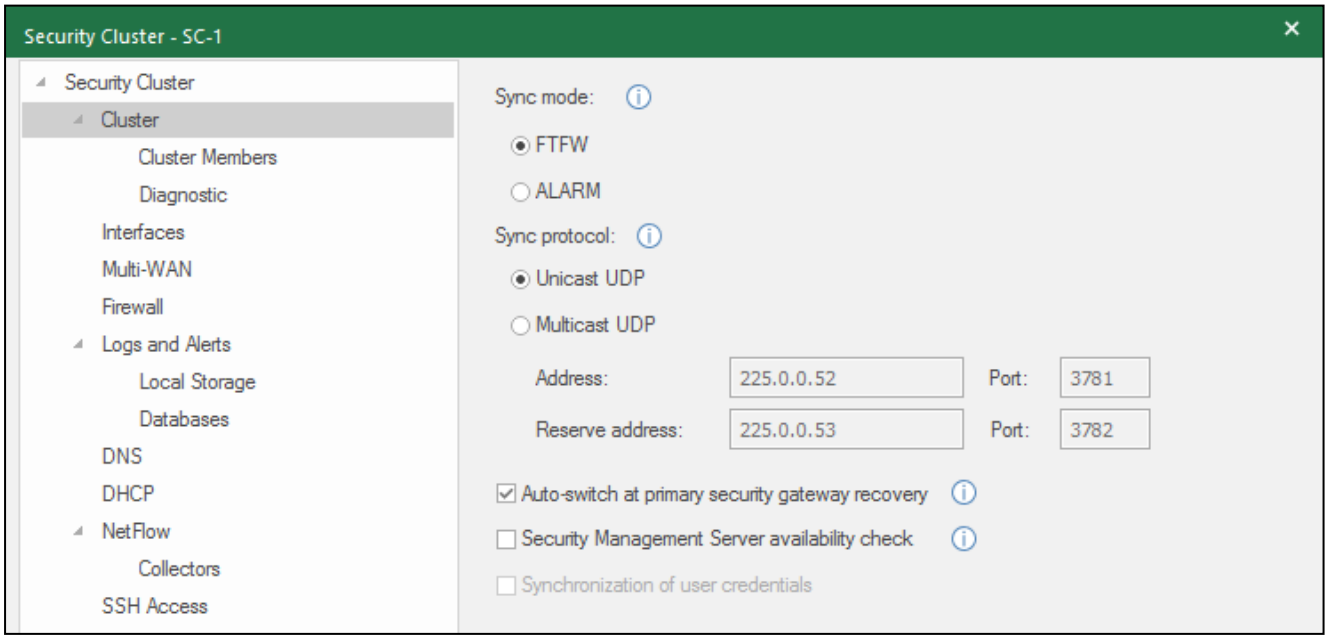
Note.
While monitoring a bond, you can monitor only either logical bonding interface or its components.



Configuring security cluster parameters

To configure security cluster parameters:

1. In the **Properties** dialog box of the security cluster, go to **Cluster**.



2. Specify the required parameters and click **Apply**.

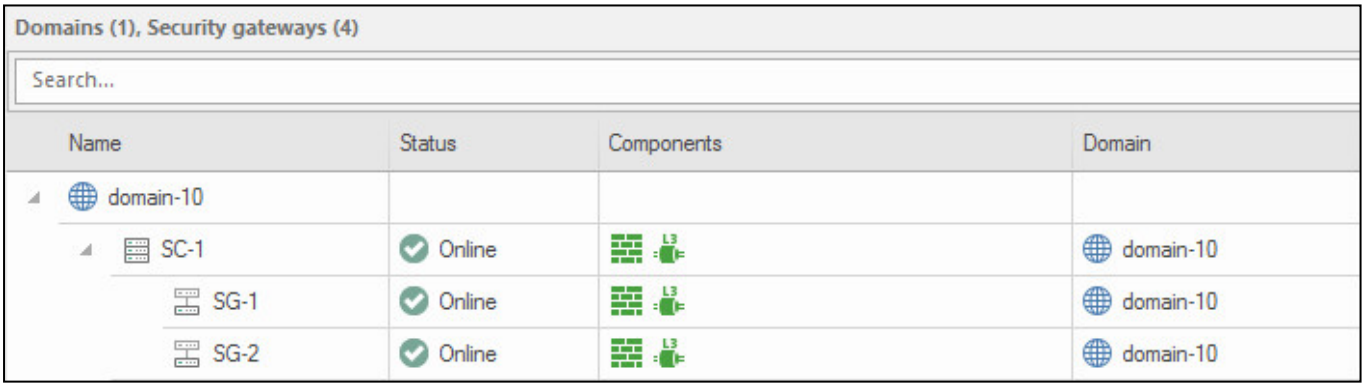
Parameter	Description
Synchronization mode	Select synchronization mode: • FTFW — the protocol with the sequence monitoring. Helps to avoid message loss. • ALARM — the protocol periodically sending messages with information about the state. Requires a wide bandwidth, works faster than FTFW
Data transmission protocol	Select protocol for data transmission in the security cluster synchronization network: • Unicast UDP — sending packets from point to point. • Multicast UDP — packet multicast
Auto-switch at primary Security Gateway recovery	When selected, the communication channel switches automatically from the reserve Security Gateway to the primary Security Gateway if the primary Security Gateway has recovered its operability which level is higher than the reserve Security Gateway (see p. **64**)
Security Management Server availability check	When selected, the system considers the Security Management Server availability when calculates the operability of a security cluster member (see p. **64**)

Attention!
If synchronization channels of several security clusters are in the same subnet and you have selected **Multicast UDP**, you must specify a unique IP address and port for each security cluster. Relevant information about reserved Multicast addresses is available on the IANA website https://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml

Configuring additional security cluster settings

In the Configuration Manager, a security cluster is a separate structure unit containing Security Gateways. You can configure common settings on the security cluster, other settings — on its elements.

Attention!
Settings configured in the local menu on cluster nodes are not synchronized in the cluster.



To configure a security cluster:

1. In the Configuration Manager, go to **Structure**.
   In the information panel, the list of Security Gateways appears.
2. Select the required security cluster and click **Properties** on the toolbar.
   The respective dialog box appears.
3. Configure required settings according to the following table.

Settings	Element	Note
Certificate assignment	Security Gateway	See [**1**]
DHCP configuration	Security Cluster	See [**7**]
DNS configuration	Security Cluster	See [**7**]
NTP configuration	Security Gateway	See p. **32**
Audit configuration	Security Cluster	See [**4**]
Configuration of access via SNMP	Security Gateway	See p. **41**
Configuration of synchronization	Security Cluster	See p. **56**

Settings	Element	Note
Routing configuration	Security Gateway	See [**7**]
Interface management*	Security Cluster	See p. **56**
	Security Gateway	See [**7**]
Access server configuration	Security Cluster	See [**6**]
Configuration of user identification	Security Cluster	See [**5**]

Note:

- You can modify network parameters of security cluster Security Gateway interfaces with the **Private** role only in Security Gateway properties, network parameters of a security cluster interfaces with the **Cluster** role — only in security cluster properties.
- You can change the role of an interface only in security cluster properties.
- If the security cluster member has no longer one of the cluster roles assigned, the respective interfaces of security cluster elements will inherit its parameters.
- If you use bonds when creating a security cluster, the security cluster IP address will be assigned to the first bond in the list.

4. Click **OK**.

Monitor a security cluster

You can view the information about the operability of a security cluster and its components in **Structure** of the Configuration Manager or in the Monitoring system of the Continent. A tile containing a status of a member (**Active**/**Standby**) is added to the cluster member state subsystems. It contains the monitoring data of the following parameters:

- state;
- synchronization network;
- integrity, identity and version of configuration;
- network interfaces;
- firewall;
- management subsystem.

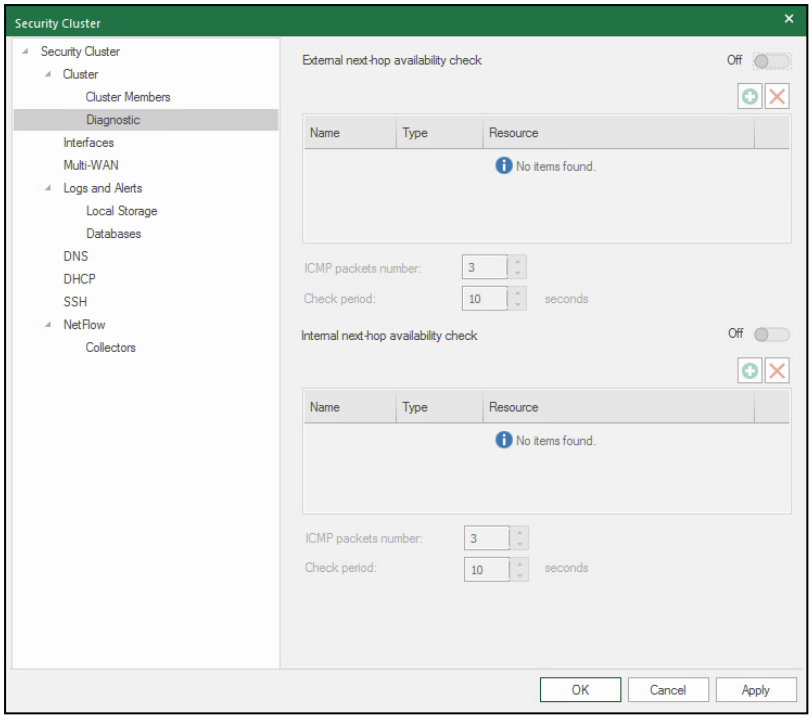
You can also monitor additional security cluster parameters:

- availability of internal next-hop;
- availability of external next-hop.

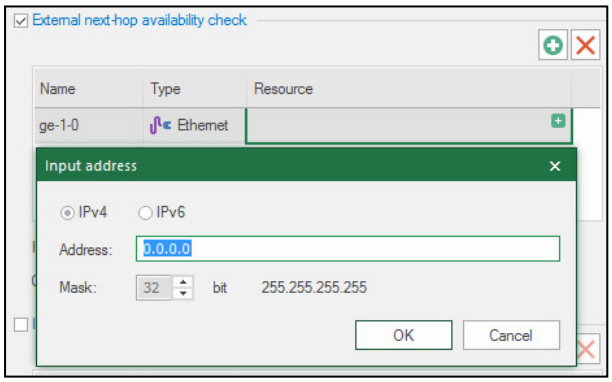
Attention!
Unavailability of additional cluster parameters during monitoring is considered a critical fault.

To check the availability of external next-hop:

1. On the left of the security cluster properties dialog box, select **Diagnostic**.
   Diagnostic parameters appear on the right.



2. Select **External next-hop availability check** and click .
   The list of external security cluster interfaces appears.
3. Select the interface that the required router is available through and click .
   The dialog box prompting the IP address of the router appears.



4. Specify the IP address and click **OK**.
5. Specify the number of test ICMP packets and the check period, then click **Apply**.

To check the availability of internal next-hop:

1. On the left of the security cluster properties dialog box, select **Diagnostic**.
   Diagnostic parameters appear on the right.
2. Select **Internal next-hop availability check** and click .
   The list of internal security cluster interfaces appears.
3. Select the interface that the required source is available through and click .
   The dialog box prompting the IP address of the source appears.
4. Specify the IP address and click **OK**.
5. Specify the number of test ICMP packets and the check period, then click **Apply**.

Operability of a security cluster member

A critical Security Gateway fault leads a Security Gateway to the **Problem** security cluster member status and makes a member with a higher operability level active.

There are four levels of faults:

Level	Description	Types
1	If the 1st level fault occurs, a Security Gateway gets the **Problem** or **OK, not ready** state. In this case, the security cluster performs the emergency switch	Failure of the only interface of a topology
		Failure of all the physical interfaces in a bond of any type if this bond is the only one in a security cluster (if the bond operability is being monitored)
		Failure of any number of physical interfaces in a bond of any type if this bond is the only one in a security cluster (if operability of bond components is being monitored)
		Unavailability of external next-hop
		Unavailability of internal next-hop
		Configuration integrity violation
2	If 2nd level fault occurs, a Security Gateway gets the **Attention** state. This means a failure of a critical device. A security cluster makes a decision whether to switch the active Security Gateway by comparing the number of 2nd level faults on both security cluster members. The **Active** status gets the Security Gateway with a fewer number of 2nd level faults. The 3rd level faults are taken into consideration when both active and reserve Security Gateways have the same number of 2nd level faults	Failure of a physical interface if there is another interface of the same topology
		Failure of any number of physical interfaces in a bond of any type if there is another bond of the same topology in this security cluster (if operability of bond components is being monitored)
		Failure of all the physical interfaces in a bond of any type if there is another bond of the same topology in a security cluster (if the bond operability is being monitored)
3	If the 3rd level fault occurs, a Security Gateway gets the **Attention** state. This means the failure that affects operability without causing a fault of a critical device. If both security cluster members have the same number of 2nd level faults or no 2nd level faults at all, the **Active** status gets the security cluster member that have a fewer number of 3rd level faults or no faults at all	Failure of a management subsystem (the Security Management Server is inaccessible)
		Failure of all physical interfaces in a bond operating in LACP or XOR (if the bond operability is being monitored)
4	If the 4th level fault occurs, a Security Gateway gets the **Attention** state. In this case, the security cluster does not perform the emergency switch	Failure of not the only **1st sync** interface
		Failure of one or more interfaces in an active-backup bond if it is the **1st sync** bond
		Failure of not all the physical interfaces in an active-backup bond (if the bond operability is being monitored)

If any of these faults occur, a security cluster member is in the **Attention** status. The system makes a security cluster member active according to the comparison of security cluster member faults: the Security Gateway with less number of 1st level faults (or no 1st level faults at all) becomes active. If there are the same number of 1st level faults, the Security Gateway with less number of 2nd level faults (or no 2nd level faults at all) becomes active.

Manage a security cluster backup

To create a security cluster backup:

1. In the local menu of the primary security cluster member, create a backup of its database (seep. **49**).
2. Repeat step **1** for the reserve security cluster member.

To restore a configuration, logs or both from the security cluster backup:

1. In the local menu of the primary security cluster member, restore its configuration from the backup (see p. 49). After the procedure has been finished, check if the Security Gateway is successfully connected.
2. Repeat step **1** for the reserve security cluster member.

To restore a configuration, logs or both from the Security Management Server backup:

Note.
This procedure is required if the critical information about a security cluster member is lost or compromised.

1. In the Configuration Manager, create a new Security Gateway certificate for the primary security cluster members, add it in the properties of the required Security Gateway, then export the Security Gateway configuration (see p. 69).
2. In the **Tools menu** of the primary security cluster member, reinitialize the Security Gateway and configure a connection to the Security Management Server in the local menu. After the procedure has been finished, check whether the connection is established in the Configuration Manager.

   Attention!
   You must not confirm changes of the security cluster in the Configuration Manager.
3. Repeat steps **2–3** for the reserve security cluster members.
4. Delete previous certificates of security cluster members and install the policy on all the Continent Security Gateways (see p. 37).

   Note.
   After you have restored the security cluster configuration, we recommend creating a full backup of the Security Management Server configuration (see p. 48).

To replace the SG (with the same ID) in a cluster:

1. In the local menu, create a backup copy of the database of the SG you want to change. (seep. 49).
2. Open the CM and go to **Structure**.
3. Right-click the SG from the cluster and click **Stop**. Repeat this for each SG in the cluster.
4. Right-click the SG from the cluster and click **Remove**. Repeat this for each SG in the cluster.
5. Select the SG you want to replace and click **Shut down** on the toolbar.
6. Replace the SG and restore its configuration from the backup copy (see p. 49).
7. Install the policy on all SGs removed from the cluster (see p. 37).
8. In **Properties** of the cluster, select **Cluster Members** on the left.

   A list of SGs included in the cluster appears.
9. Click  .

   A list of SGs appears..
10. Select the SGs removed from the cluster.
11. Configure the cluster (see p. 58).
12. Click **OK**.
13. Install the policy on the cluster (see p. 37).

Delete a security cluster

Attention!
Before deleting a security cluster, exclude all members from it.

To delete a security cluster:

1. In the Configuration Manager, go to **Structure**, select the required security cluster and click **Delete** on the toolbar.

   The dialog box prompting the confirmation appears.
2. Click **Yes**.

3. After you have finished configuring all the required settings, save the Security Management Server configuration and install the policy on the Security Management Server and Security Gateways with modified settings (see p. **36**).

Chapter 7
Security certificates

You can view the available certificates via any Continent component as well as import certificates, security keys and make requests to issue certificates.

The Security Management Server allows you to create and export the certificates listed in the table below.

Certificate type	Maximum service life	Signature algorithm	Note
Root CAs			
Root certificate	5 years	GOST R 34.10-2012	See p. **68**
RSA root certificate	5 years	RSA	See [**4**], **Configure the network connection**
Intermediate CAs			
Authentication portal-redirect	1 year	RSA	See [**5**], **Authentication Portal**
SSL/TLS inspection	1 year	RSA	See [**2**], **Initial configuration**
Personal certificates			
Security Management Server	1 year	GOST R 34.10-2012	
Administrator	1 year	GOST R 34.10-2012	See p. **71**
User	1 year	GOST R 34.10-2012	See [**6**], **Remote access**
Authentication Portal	1 year	RSA	See [**5**], **Authentication Portal**
Access Server	1 year	GOST R 34.10-2012	See [**6**], **Remote access**
Security Gateway	1 year	GOST R 34.10-2012	See p. **69**
Web-monitoring	1 year	RSA	See [**4**], **Configure the network connection**

View certificates

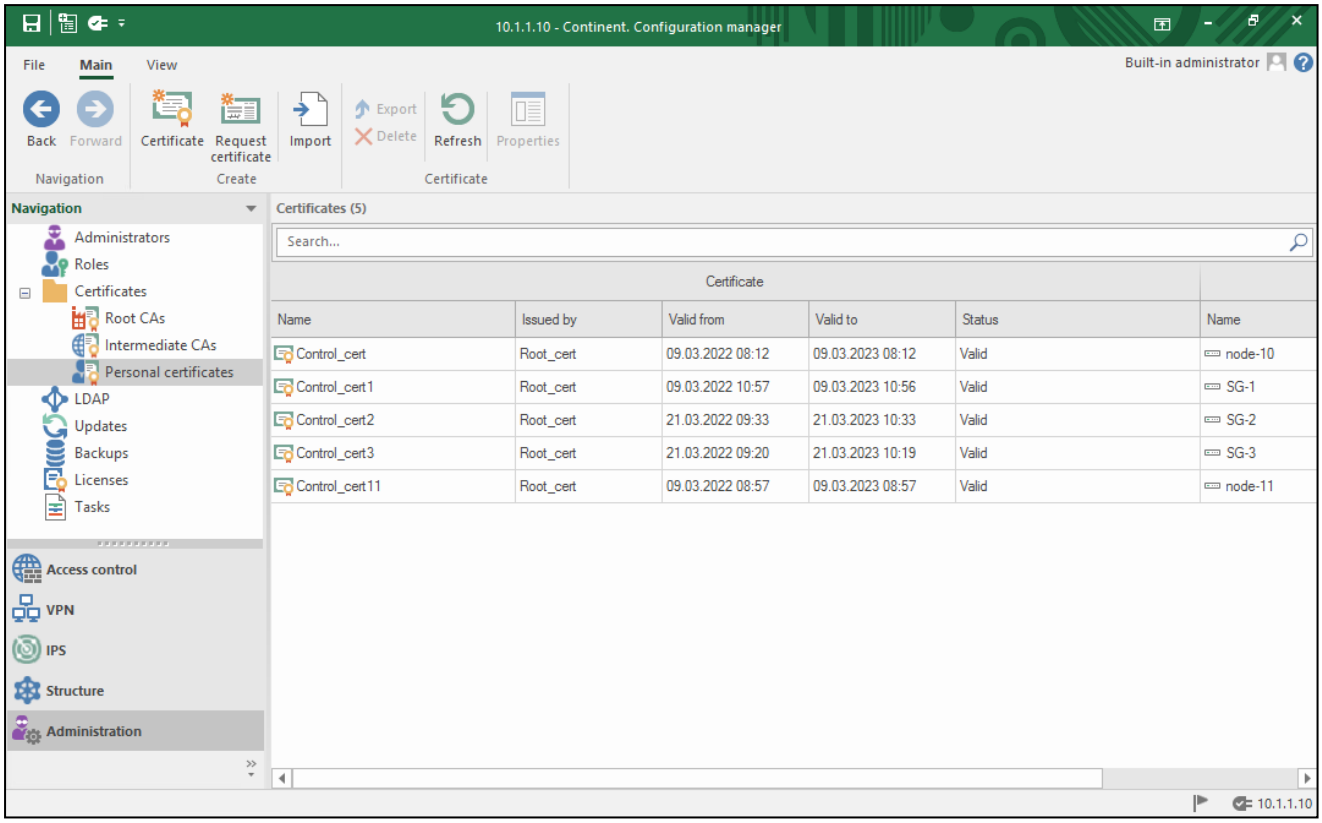
To view security certificates in the local menu:

1. In the main menu, select **Certificates** and press **<Enter>**.
   The **Certificates** menu appears.

2. Select the required certificate type and press **<Enter>**.
   A dialog box appears with the list of certificates of the respective type.
3. To view detailed information about a certificate, select the required one on the list and press **<Enter>**.
4. To return to the previous menu, press **<Esc>**.

To view security certificates using the Configuration Manager:

- In the Configuration Manager, go to **Administration**, expand **Certificates** and select the required type.



The list of installed certificates appears in the display area.

Create certificates

Create root certificates

To create a root certificate in the Security Management Server local menu:

1. In the main menu, select **Certificates** and press **<Enter>**.
   The **Certificates** menu appears.
2. Select **Root certificates** and press **<Enter>**.
   The **Root certificates** menu appears.

> **Note.**
> The pre-installed **Trusted Publisher** root certificate is a pre-installed certificate required for the software update. It cannot be used for other purposes.

3. To create root certificate, press **<F2>**.
   The **Issue certificate** menu appears.
4. Select **Issue root certificate** and press **<Enter>**.
   The **Certificate** dialog box appears.

5. Type the required information in the **Organization**, **Organization unit** and **Common name** text boxes and press **<Enter>**.

Note.
For navigation, use the following keys: **<↑>**, **<↓>**, **<Page Down>**, **<Page Up>**, **<Home>**.

A success message appears.

6. Press **<Enter>**.
   You are returned to the **Issue certificate** menu.
7. Press **<Esc>**.
   You are returned to the **Root certificates** menu. The created certificate is shown in the list.
8. Press **<Esc>.**
   You are returned to the **Certificates** menu.

To create a root certificate using the Configuration Manager:

1. In the Configuration Manager, go to **Administration**, expand **Certificates** and select **Root CAs**.
   The list of installed personal certificates appears in the display area.
2. On the toolbar, click **Root certificate**.
   The **Root certificate** dialog box appears.
3. Type the required information in the **Certificate owner data** section, configure the **Key usage** parameters, select the **Signature algorithm** and specify the expiration date. Click **Create certificate**.
   You are returned to the list where the new certificate is shown.

Create a control certificate for a Security Gateway

A Security Management Server certificate is created using the Security Management Server local menu (see below).

The Security Gateway certificate can be created in the following ways:

- in the local menu, create a CSR (see p. **70**) and issue this certificate on the Security Management Server (see p. **70**) on the created CSR;
- issue the certificate on the Security Management Server (see p. **69**) without a request.

Note.
In this case, a CSR is issued with the certificate itself. You should import the CSR file on the Security Gateway using the local menu (see Security certificates). The CSR file contains the private key container.

To create the Security Management Server control certificate:

1. In the local menu, select **Certificates** and press **<Enter>**.
2. In the **Certificates** menu, select **Control channel certificates** and press **<Enter>**.
   The **Control channel certificates** menu appears.

Note.
The list is empty before you create the first certificate.

3. Press **<F2>**.
   The **Issue certificate** menu appears.

4. Select **Issue control certificate for Security Management Server** and press **<Enter>**.
   The Certificate dialog box appears.
5. Specify the required information in the **Organization**, **Organization unit** and **Common name** text boxes, then press **<Enter>**.
   A list of the created root certificates appears.
6. Select the required one and press **<Enter>**.
   A success message appears.

7. Press **<Enter>**.
   You are returned to the **Issue certificate** menu.
8. Press **<Esc>**.
   You are returned to the **Control channel certificates** menu. The created certificate is shown in the list.
9. Press **<Esc>.**
   You are returned to the **Certificates** menu.

Create a CSR for a Security Gateway control certificate

To create a Security Gateway CSR using Security Gateway local menu:

1. In the **Certificates** menu, select **Control channel certificates** and press **<Enter>**.
   The **Control channel certificates** menu appears.
2. Insert a USB drive into a USB port. To export the CSR file, press **<F4>**.
   The **Make Certificate Request** menu appears.
3. Select **Create a control certificate request** and press **<Enter>**.
   A dialog box appears. It contains the identification attributes.
4. Specify the required information in the **Organization**, **Organization unit** and **Common name** text boxes, then press **<Enter>**.
   A dialog box prompting you to type the container password appears.
5. Type the password and press **<Enter>**.
   A dialog box prompting you to type the container name appears.
6. Type the name and press **<Enter>**.
   When the CSR file is saved on the USB drive, the respective message appears.
7. Press **<Esc>**.
8. You will be returned to the **Make Certificate Request** menu.
9. Press **<F5>**, select the CSR file (**continent-ID.req**, **ID** is the Security Gateway serial number) and press **<Enter>**.
   A dialog box prompting you to select a key container appears.
10. Select the required container and press **<Enter>**.
    A dialog box prompting you to type the key container password appears.
11. Type the password and press **<Enter>**.
    If the operation is successful, the respective message appears.
12. To return to the **Control channel certificates** menu, press **<Enter>**. Remove the drive and go to the Security Management Server or administrator workstation to issue the control certificate for the Security Gateway.

Issue control certificates for the Security Gateway

To issue a control certificate for the Security Gateway in the Security Management Server local menu:

1. In the **Certificates** menu, select **Control channel certificates** and press **<Enter>**.
   The **Control channel certificates** menu appears.
2. Insert a USB drive into a USB port for the CSR file import (see above) and press **<F2>**.
   The **Issue certificate** menu appears.
3. Select **Issue control certificate for Node** and press **<Enter>**.
   A dialog box asking you if you have the CSR appears.
4. Select **Yes** and press **<Enter>**.
   A dialog box with a list of the files detected on the USB drive appears.

   Note.
   The CSR file default name is **continent-XX.req**, where **XX** is the Security Gateway ID.

5. Select the CSR file and press **<Enter>**.
   A dialog box appears where you must select the root certificate.

6. Select the required certificate and press **<Enter>**.

   The control certificate file for the Security Gateway is created. Then you are returned to the **Issue certificate** menu.

7. Select **Back to previous menu** and press **<Enter>**.

   You are returned to the **Control channel certificate** menu where you can see the new certificate.

To issue the control certificate for the Security Gateway in the Configuration Manager:

1. In the Configuration Manager, go to the **Administration** section.
2. In the list of certificate type, click **Personal certificates**.

   A list of installed personal certificates appears.

3. On the toolbar, click **Certificate**.

   The Certificate dialog box appears.

4. In the **Certificate type** drop-down list, select **Security gateway**.
5. Click **load request data**, specify a path to the file and click **Open**.

   When the file is processed, all the data in the **Certificate owner data** and **Key usage** sections are specified.

6. In the **Advanced** section, select the root certificate created during the Security Management Server deployment and specify the expiration date.
7. Click **Create certificate**.

   The control certificate file is created and the certificate data is shown in the list.

Create administrator certificates

To create an administrator certificate:

1. In the Configuration Manager, go to **Administration**.
2. In the list of certificate type, select **Personal certificates**.

   The list of installed personal certificates appears.

3. On the toolbar, click **Certificate**.

   The **Certificate** dialog box appears.

4. In the **Certificate type** drop-down list, select **Administrator**.
5. In the **Certificate owner data** and **Key usage** section, type all the required information.
6. In the **Advanced** group box, select the root certificate created during the Security Management Server deployment and specify the expiration date.
7. Specify the key file and click **Create certificate**.

   The dialog box appears prompting you to reinitialize the RNG using human input.

8. Follow the instructions and wait until the process of gathering entropy is finished.

   A dialog box for password creation to access the key container appears.

9. Type the password and click **OK**.

   Attention!
   Do not lose this password, it is required in case of the certificate installation or administrator authentication by the certificate.

   A dialog box for selecting a drive for the key container appears.

10. Select the required key container, click **Refresh** if necessary, then click **OK**.

    The personal certificate and key container files are created and the certificate data is shown in the list.

Install an administrator certificate

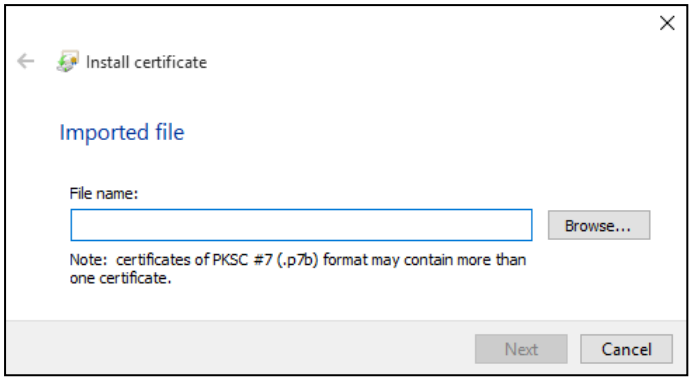
To log on as an administrator to the Configuration Manager using the certificate, you must install the certificate to the account repository. To do so, you can use **Security Code CSP** that is a part of the complex.

Attention!
You must not use third party CSPs.

To install an administrator certificate using Security Code CSP:

1. Run **Security Code CSP** (**All apps**/**Security code**/**Security Code CSP**) and go to the **Certificates** tab.

2. Click **Install certificate**.
   The installation wizard appears.



3. Insert a USB drive with the certificate file and click **Browse...**
   The File Explorer dialog box appears.
4. Select the required file and click **Open**. Then click **Next**.
   A dialog box for configuring the certificate storage appears.
5. In the **Certificate manager** drop-down list, select **Of the user account**. Click **Next**.
   A dialog box for selecting the private key container appears.

   Note.
   USB drive analysis may take some time. The list of available containers is updated as the data is processed.

6. Select the key container, click **Refresh** if necessary, then click **Next**.
   The **Ready for installation** dialog box appears.
7. Check the parameters and click **Finish**.
8. Follow the instructions on the screen and wait until entropy is gathered.
   A dialog box appears, where you must type a password for the key container.
9. Type the password and click **OK**.
   If the password is correct, the installation begins. When the installation is finished, the respective message appears.
10. Click **OK**.

Change certificates

To change the Security Management Server root certificate in the Configuration Manager:

1. In the Configuration Manager, create a root certificate (see p. 68).
2. On the navigation panel, go to **Structure**.
   The list of Security Gateways appears on the right.
3. Select the Security Management Server and click **Properties** on the toolbar.
   The Security Gateway properties dialog box appears on the screen.
4. On the left, select **Certificates**.
   The list of server and root certificates appears on the right.
5. In the **Root Certificates** group box, click  to add a new certificate.
   The **Certificates** dialog box appears on the screen.
6. Select the required certificate in the list.
   The certificate is displayed.
7. Click **OK**.
8. To save the Security Gateway configuration, press **<Ctrl>+<S>** or click  on the toolbar.

Note.
After changing the root certificate, you must change the Security Management Server control certificate in the local menu (see p. 74). Then, change security certificates and install policies on subordinate SGs.

If necessary, you can reissue Security Gateway control certificates using the Configuration Manager or the local menu.

Note.
Security Gateway control certificates are reissued automatically. When the validity period expires in 28 days, it is extended for another year.

To change the Security Management Server control certificate in the Configuration Manager:

1. In the Configuration Manager, go to **Administration**.
2. In the list of certificate type, select **Personal certificates**.
   The list of installed personal certificates appears.
3. On the toolbar, click **Certificate**.
   The **Certificate** dialog box appears.
4. In the **Certificate type** drop-down list, select **Security Gateway** and specify the required information in the **Certificate owner data** and **Key usage** group boxes.
5. In the **Advanced** group box, select the root certificate and specify the expiration date of the control certificate.
6. Click ..., select the root folder of the USB drive, specify the name and click **Save**.
7. Click **Create certificate**.
   The dialog box prompting you to enter and confirm the key container password appears.
8. Enter and confirm the password, then click **OK**.

   Note.
   Minimum password length is 6 characters.

   The control certificate file, the CSR file and the key container are saved to the USB drive and the certificate information appears in the display area.
9. In the local menu of the Security Management Server, go to **Certificates** and press <**Enter**>.
10. Select **Control channel certificates** and press <**Enter**>.
    The **Control channel certificates** window appears.
11. Insert the USB drive and press <**F5**> to import the CSR.
    The dialog box prompting you to select the CSR file appears.
12. Select the file with the **.req** extension and press <**Enter**>.
    The dialog box prompting you to select the key container appears.
13. Select the required key container and press <**Enter**>.
    The dialog box prompting you to type the password appears.
14. Type the password and press <**Enter**>.
    When the file and the key information is imported, the respective message appears.
15. Press <**Enter**>.
16. In the Configuration Manager, go to **Structure**.
    The list of Security Gateways appears in the display area.
17. Select the Security Management Server and click **Properties** on the toolbar.
18. On the right, select **Certificates**.
19. In the **Server certificates** group box, select an old certificate and click .
20. In the **Server certificates** group box, click and select the new control certificate.
    The selected server certificate appears in the list.
21. In the **Root certificates** group box, click and select the root certificate.
    The selected root certificate appears in the list.
22. Click **OK**.

23. Save changes by clicking on the toolbar.

To change the Security Management Server control certificate in the local menu:

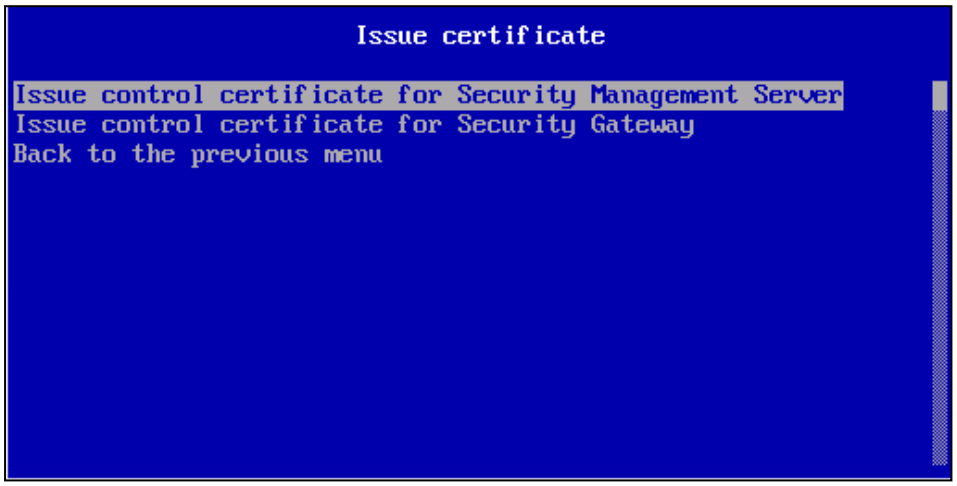
1. In the local menu, go to **Certificates | Control certificates** and click **Enter**.

The **Control channel certificates** dialog box appears.

> **Note.**
> When creating the first certificate. the list is empty.

2. Press **<F2>**.

The **Issue certificate** menu appears.



3. Select **Issue control certificate for Security Management Server** and press **Enter**.

The **Certificate** dialog box appears.

4. Specify the required parameters **Organization**, **Organization unit** and **Common name**.

The list of created root certificates appears.

5. Select the root certificate and press **Enter**.

The message **Successful** appears.

6. Press **Enter** to go back to the **Issue certificate** menu.

7. Press **Esc** to go back to **Control channel certificates**.

The created certificate for Security Management Server appears in the list.

8. Press **Esc** to go back to the **Certificates** menu.

9. Press **Esc** to go back to the local menu.

10. Go to **Tools | Export node configuration to medium** and press **Enter**.

The **Export policy** dialog box appears.

11. Enter Security Management Server ID and press **<Enter>**.

Recording to the medium starts. When the configuration is successfully saved, you receive the respective message.

12. Press **Enter** to go to the **Tools** menu.

13. Select **Import local policy** from file and press **<Enter>**.

The list of available files appears on the screen.

14. Select the required configuration file with the .**json** extension and press **<Enter>**.

> **Note.**
> The name of the configuration file recorded to the medium: **policy-XX.json**, where **XX** is Security Gateway ID, specified earlier.

Confirmation of local changes starts. When the changes are successfully confirmed, you receive the respective message.

15. Press **Enter** to go back to the **Tools** menu.

To change the Security Gateway root certificate in the Configuration Manager:

1. In the Configuration Manager, go to **Structure**.

2. Select the required Security Gateway and click **Properties** on the toolbar.
   The Security Gateway properties dialog box appears on the screen.
3. On the left, select **Certificates**.
   The list of server and root certificates appears on the right.
4. In the Root Certificates group box, select an old certificate and click  .
   The certificate is deleted from the list.
5. In the **Root Certificates** group box, click  to add a new certificate.
   The **Certificates** dialog box appears.
6. Select the required certificate in the list.
   The certificate is displayed.
7. Click **OK**.

To change the Security Gateway control certificate in the Configuration Manager:

1. In the Configuration Manager, go to **Administration**.
2. In the list of certificate type, select **Personal certificates**.
   The list of installed personal certificates appears.
3. On the toolbar, click **Certificate**.
   The **Certificate** dialog box appears.
4. In the **Certificate type** drop-down list, select **Security Gateway** and specify the required information in the **Certificate owner data** and **Key usage** group boxes.
5. In the **Advanced** group box, select the root certificate and specify the expiration date of the control certificate. Connect an external USB drive.
6. Click  , select the root folder of the USB drive, specify the name and click **Save**.
7. Click **Create certificate**.
   The dialog box prompting you to enter and confirm the key container password appears.
8. Enter and confirm the password, then click **OK**.

   Note.
   Minimum password length is 6 characters.

   The control certificate file, the CSR file and the key container are saved to the USB drive and the certificate information appears in the display area.
9. To save the Security Gateway configuration, press **<Ctrl>+<S>** or click  on the toolbar.
10. In the local menu of the Security Gateway, go to **Certificates** and press <**Enter**>.
11. Select **Control channel certificates** and press <**Enter**>.
    The **Control channel certificates** window appears.
12. Insert the USB drive and press <**F5**> to import the CSR.
    The dialog box prompting you to select the CSR file appears.
13. Select the file with the **.req** extension and press **<Enter>**.
    The dialog box prompting you to select the key container appears.
14. Select the required key container and press **<Enter>**.
    The dialog box prompting you to type the password appears.
15. Type the password and press **<Enter>**.
    When the file and the key information is imported, the respective message appears.
16. Press **<Enter>**.
17. In the Configuration Manager, go to **Structure**.
    The list of Security Gateways appears in the display area.
18. Select the Security Management Server and click **Properties** on the toolbar.
19. On the right, select **Certificates**.
20. In the **Server certificates** group box, click  and select the new control certificate.

The selected server certificate appears in the list.

21. In the **Root certificates** group box, click and select the root certificate.
    The selected root certificate appears in the list.
22. Click **OK**.
23. Save the configuration and install the policy on the Security Gateway.

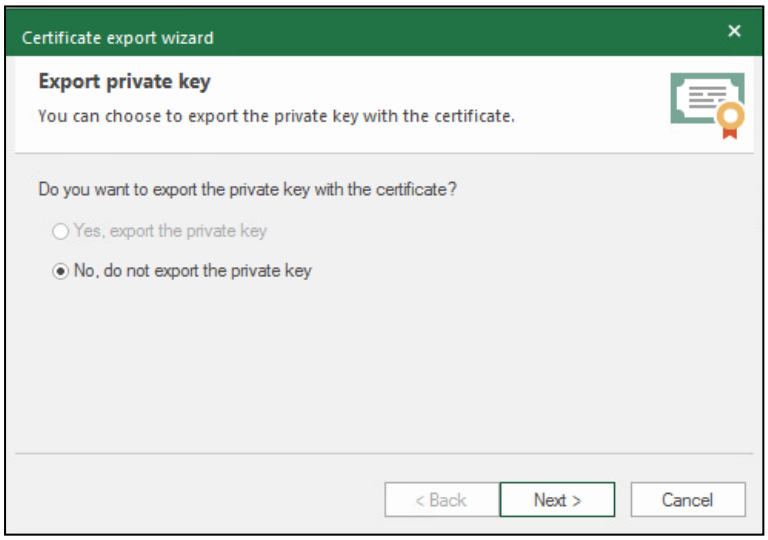
To remove a root or control certificate:

1. In the Configuration Manager, go to **Structure**.
2. Select the required Security Gateway and click **Properties** on the toolbar.
   The **Security Gateway** dialog box appears.
3. On the left, select **Certificates**.
4. In the **Server Certificates** or **Root Certificates**, select the one required to be replaced and click .
   The certificate will be removed from the list.

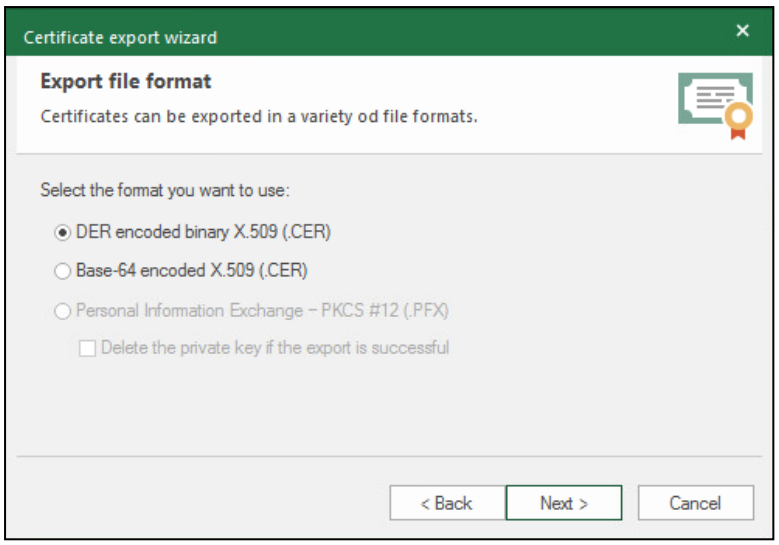
Export certificates

To export a root certificate via the Configuration Manager:

1. In the Configuration Manager, go to **Administration**.
2. Expand **Certificates** and select **Root CAs**.
   The list of installed certificates appears in the display area.
3. Right-click the required certificate and click **Export**.
   The **Export private key** window of the certificate export wizard appears.



4. Specify whether you need to export the private key with the certificate and click **Next**.
   The **Export file format** window appears.



5. When exporting a certificate without a private key, select **DER** or **Base-64** coding.

   When exporting a certificate with a private key, the file is saved in the .**PFX** format. If you need to delete the private key after the successful export, select the respective check box.
6. Click **Next**.

   The **File to export** window appears.
7. Click ... .

   The standard **Save as** dialog box appears.
8. Specify the destination folder, name and type of the file, then click **Save**.

   When exporting a certificate with a private key, the **Security** window appears. Specify a password according to the password policy and confirm it. Click **Next**.

   The **Completing the certificate export wizard** window appears.
9. Click **Finish**.

   After the successful export of the certificate, the respective message appears.
10. Click **OK**.

    After the certificate file export, you are returned to the list of certificates.

To export root certificates via the local menu:

1. Go to **Certificates**, select **Root certificates** and press **Enter**.
2. Insert an external drive into a USB port to export files to it.
3. Select the root certificate you need to export and press **F6**.

   A dialog box prompting you to confirm the deletion of the private key after the certificate export appears.
4. Select whether you need to delete the private key and press **Enter**.

   A dialog box prompting you to enter a password for the certificate container appears.
5. Set a password according to the password policy and confirm it. Press **Enter**.

   A dialog box prompting you to confirm the certificate export appears.
6. Select **Yes** and press **Enter**.

   A message notifying you about the successful completion of the operation appears.
7. Press **Enter**.

To export an intermediate or personal certificate:

1. In the Configuration Manager, go to **Administration**.
2. Expand **Certificates** and select the required type.

   The list of installed certificates appears in the display area.
3. Right-click the required certificate and click **Export**.

   The standard **Save as** dialog box appears.

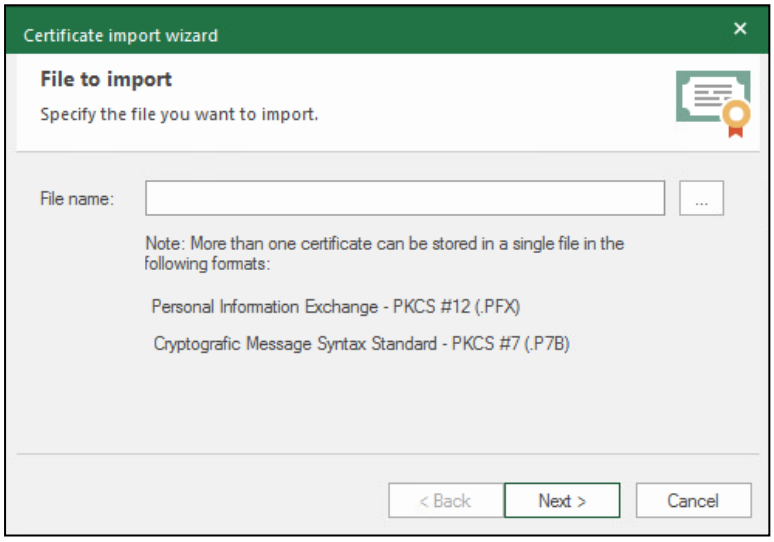
4. Specify the destination folder, name and type of the file, then click **Save**.
   After the certificate file export, you are returned to the list of certificates.

Import certificates and security keys

Attention!
The subject name in the certificate must not match the names in the previously installed certificates.

To import root certificates via the Configuration Manager:

1. In the Configuration Manager, go to **Administration**.
2. Expand **Certificates** and select **Root CAs**.
   The list of installed certificates appears in the display area.
3. On the toolbar, click **Import**.
   The **File to import** window of the certificate import wizard appears.



4. Click ... .
   File Explorer appears.
5. Select the required file and click **Open**.
6. In the certificate import wizard window, click **Next**.
   When importing a root certificate with a private key, the **Password protection of the private key** window appears. Enter a password and click **Next**.
   The **Completing the certificate import wizard** window appears.
7. Click **Finish**.
   After the successful import of the certificate, the respective message appears.
8. Click **OK**.
   The list of installed certificates updates.

To import intermediate and personal certificates via the Configuration Manager:

1. In the Configuration Manager, go to **Administration**.
2. Expand **Certificates** and select the required type.
   The list of installed certificates appears in the display area.
3. On the toolbar, click **Import**.
   File Explorer appears.
4. Select the required file and click **Open**.
   The list of installed certificates updates.

To import root certificates with a private key via the local menu:

1. Go to **Certificates**, select **Root certificates** and press **Enter**.

2. Insert an external drive into a USB port to import files from it and press **F7**.
   A dialog box prompting you to select a file appears.
3. Select the certificate file (***.pfx**) and press **Enter**.
   A dialog box prompting you to enter a password for the certificate container appears.
4. Enter a password and press **Enter**.
   A message notifying you about the successful completion of the operation appears.
5. Press **Enter**.

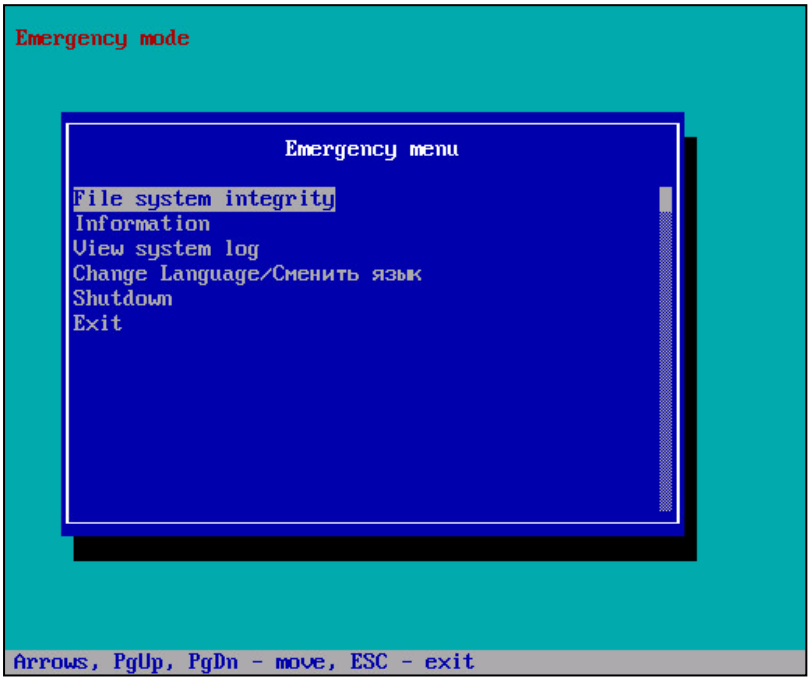
To import root certificates without a private key and the Security Gateway via the local menu:

1. Go to **Certificates**, select the required certificate type and press **Enter**.
2. Insert an external drive into a USB port to import files from it and press **F3**.
   A dialog box prompting you to select a file appears.
3. Select the certificate file (***.cer**) and press **Enter**.
   A message notifying you about the successful completion of the operation appears.
4. Press **Enter**.

Appendix

Software integrity check

If the Continent software integrity is violated, a Security Gateway is started in emergency mode. In the Configuration Manager, the Security Gateway is unavailable, in the local menu, in the top left corner, there is the respective warning. In this mode, there is the emergency menu listing the limited set of functions, unlike the main menu.



To check the file system integrity:

1. In emergency mode, select **File system integrity** and press **<Enter>**.
   The respective menu appears.
2. Select **Check FS integrity** and press **<Enter>**.
   The dialog box prompting you to confirm the procedure appears.
3. Select **Yes** and press **<Enter>**.
   After the procedure is complete, a window appears. The window contains check results with the detailed information about the software integrity and Security Gateway configuration.
4. To go back to the **File system integrity**, press **<Esc>**.

To check the configuration integrity:

1. In emergency mode, select **File system integrity** and press **<Enter>**.
   The respective menu appears.
2. Select **Configuration integrity** and press **<Enter>**.
   The dialog box prompting you to confirm the procedure appears.
3. Select **Yes** and press **<Enter>**.
   If the integrity of active configuration was violated, the following message appears:
   If the active configuration was not violated, the following message appears:
4. To go back to the **File system integrity**, press **<Esc>**.

> **Note.**
> If the active configuration integrity was violated after the Security Gateway restart, the Security Gateway does not switch to emergency mode.

To exit the emergency mode:

1. In emergency mode, select **File system integrity** and press **<Enter>**.
   The respective message appears.

2. Select **Rebuild FS integrity database** and press **<Enter>**.
   The dialog box prompting confirmation appears.
3. Select **Yes** and press **<Enter>**.
   After the procedure is complete, the **File system integrity** menu appears.
4. Go back to **Emergency menu**, select **Shutdown** and press **<Enter>**.
5. Select **Reboot** and press **<Enter>**.

Built-in administrator role permissions

Built-in administrator roles:

- MA —main administrator;
- NA — network administrator;
- SA — security administrator;
- AA — audit administrator.

You can find the built-in administrator role permissions in the table below.

Permission	MA	NA	SA	AA
Management of accounts and certificates				
Management of accounts and administrator roles	+	0	0	0
Certificate management (general and local)	+	0	+	0
Domain structure and configuration management				
Management of objects and services	+	+	0	0
Security gateway registration in a domain (general and local)	+	+	+	-
Security gateway network settings management (general and local)	+	+	+	0
Security gateway security settings management	+	0	+	0
Update management	+	+	0	0
Backup creation (general)	+	+	+	+
Domain configuration management (general and local)	+	-	-	-
Policy management				
Policy installation (general and local)	+	+	+	-
Management of IPS policies	+	0	+	0
Management of firewall policies	+	0	+	0
Hierarchy management				
Creating domain hierarchy (general and local)	+	0	+	0
Local management				
Emergency menu tasks	+	-	+	-
Remote access to the local menu	-	-	-	-
Log management	+	-	+	-
View logs	+	+	+	+
Security gateway diagnostic	+	+	-	-
Local policies management	+	+	+	-
Administrator password change	+	-	-	-
Reinitialization	+	-	-	-
Security gateway shutdown	+	+	+	-
Monitoring and diagnostic. System pages				

Permission	MA	NA	SA	AA
Monitoring panel	+	+	+	+
System log	+	+	+	+
Network Security log	+	-	+	-
Management log	+	+	+	-
Statistics	+	+	+	+
Structure (monitoring and parameters settings)	+	+	+	-
Structure (monitoring and access settings)	+	-	+	-
Group management	+	-	+	-
Available dashboard and statistics widgets				
Monitoring	+	+	+	-
Network interfaces	+	+	-	-
IPS signature triggering	+	-	+	-
Top failed security gateways	+	+	+	+
Number of attacks	+	-	+	+
Top signatures	+	-	+	+
Top attack sources	+	-	+	+
Top attack victims	+	-	+	+

+ — full access;

- — not available;

0 — read only.

Manage the network traffic dump

In Continent, you can manage the network traffic dump using the local menu of a Security Gateway.

To start recording network traffic:

1. Connect a USB drive to a Security Gateway.
2. In the local menu of the Security Gateway, go to **Tools** | **Manage network traffic dump**.
   The **Manage network traffic dump** menu appears.
3. Select **Start recording network traffic** and press <**Enter**>.
   The list of available USB drives appears.
4. Select the USB drive required to record network traffic and press <**Enter**>.
   The list of network interfaces appears.
5. Select the monitoring or inline IPS interface receiving traffic that is required to dump and press <**Enter**>.
   The **File rotation interval** dialog box appears.
6. Set the file rotation interval.

   Note.
   The file rotation interval is a period of time for saving traffic to a dump file. When the interval times out, traffic is being saved to another dump file. Takes on values from 60 to 3600. Default value — 900.

   Press <**Enter**>.
   You will receive the message about the successful start.
7. Press <**Enter**>.

To start recording network traffic:

1. In the local menu of the Security Gateway, go to **Tools** | **Manage network traffic dump**.
   The **Manage network traffic dump** menu appears.
2. Select **Stop recording network traffic** and press <**Enter**>.

The dialog box prompting you to confirm the action appears.

3. Select **Yes** and press <**Enter**>.
   You will receive the message about the successful stop.
4. Press <**Enter**>.

To view the status of network traffic recording:

1. In the local menu of the Security Gateway, go to **Tools** | **Manage network traffic dump**.
   The **Manage network traffic dump** menu appears.
2. Select **Status** and press <**Enter**>.
   You will receive the message about the current status of the recording procedure.
3. Press <**Enter**> to return to the previous menu.

Set the screen lock timeout

In Continent, you can set the screen lock timeout.

To set the screen lock timeout:

1. In the local menu, go to **Settings** | **Screen lock timeout settings**.
   The **Screen lock timeout** dialog box appears.
2. Set the required value in seconds.

   Note.
   Takes on values from 10 to 3600. Default value — 300.

   Press <**Enter**>.
   The screen lock timeout will take on the specified value and you will be returned to the previous menu.

Security cluster operability monitoring in the Configuration Manager

In **Structure**, there is the **Cluster** column to monitor status of a security cluster. It indicates the status of a security cluster and its components in real time.

Table of security cluster member states

The following correspondence table presents possible accidents in different Configuration Manager states of a security cluster and its components.

Fault	Security cluster member state					
	OK	Attention	Down	Problem	OK, not ready	Unavailable
Fault of network interface						
Fault of all network interfaces						
Fault of all internal interfaces						
Fault of synchronization network		**If a Security Gateway is active**	**If a Security Gateway is standby**			
External interface is not available						
Internal interface is not available						
Configuration integrity violation						
Router is not available						

Fault	Security cluster member state					
	OK	Attention	Down	Problem	OK, not ready	Unavailable
Internal source is not available						
Security Gateway is shutdown or disconnected						

Table of security cluster states

The following table shows the correspondence between a failover security cluster and its components.

Security Gateways		Security cluster state
First Security Gateway state	Second Security Gateway state	
OK	OK	OK
Busy	OK	OK
Attention	Attention	Attention
OK	Attention	Attention
Busy	Attention	Attention
OK	Problem	Critical
OK	OK, not ready	Critical
OK	Down	Critical
Attention	Problem	Critical
OK, not ready	OK, not ready	Critical
Attention	Down	Critical
OK	Unavailable	Critical
Attention	OK, not ready	Critical
Busy	OK, not ready	Critical
Busy	Problem	Critical
Busy	Down	Critical
Busy	Unavailable	Critical
Problem	Down	Problem
Problem	OK, not ready	Problem
OK, not ready	Down	Problem
OK, not ready	OK, not ready	Problem
Problem	Problem	Problem
OK, not ready	Unavailable	Problem
Problem	Unavailable	Problem
Unavailable	Unavailable	Offline
Down	Down	Offline
Down	Unavailable	Offline

List of logged security cluster events

Event	Note
Cluster has been created, #security cluster name	
Cluster has been deleted, #security cluster name	
Security Gateway has been added to cluster, #Security Gateway, #security cluster	
Security Gateway has been removed from cluster, #Security Gateway, #security cluster	
Security Gateway status has been changed in cluster, #Security Gateway, #status, #reason of change	
Security Gateway state has been changed in cluster, #previous state, #current state, #reason	
Interface fault, #Security Gateway, #interface name	
Interface not available, #Security Gateway, #interface name	
Cluster settings have been changed, #parameter name, #previous value, #current value	
Router not available, #router IP address	
Internal source not available, #source IP address	
Conntrack errors	

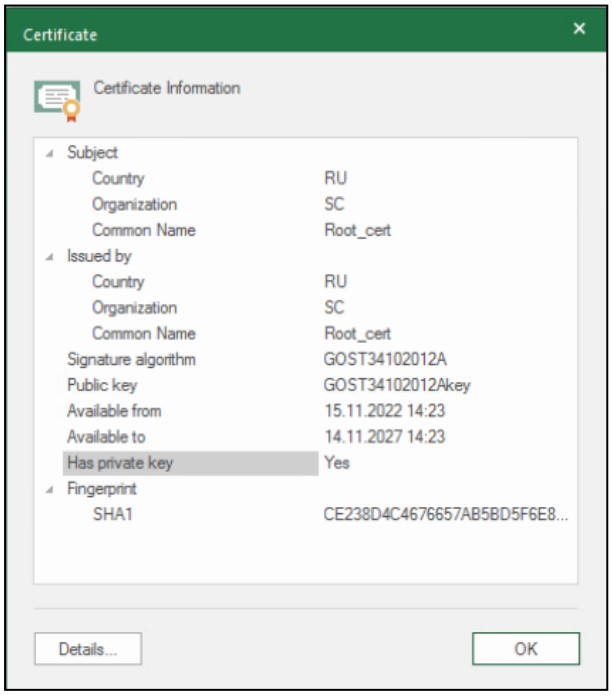
Transfer the Security Management Server to another Security Gateway

Before transferring the Security Management Server to another Security Gateway (hardware platform), you need to deploy the standby Security Management Server on a new Security Gateway. For more information about the standby Security Management Server deployment process, see [**1**].

To transfer the Security Management Server to another Security Gateway:

1. Run the Configuration Manager and connect to the Security Management Server.
2. Go to **Administration**.
3. Expand **Certificates** and select **Root CAs**.
4. Export root certificates with a private key (see p. **67**) and select the private key deletion after the successful export.

   The presence of a private key will be displayed in the certificate properties.



5. Disconnect from the Security Management Server and connect to the standby Security Management Server.

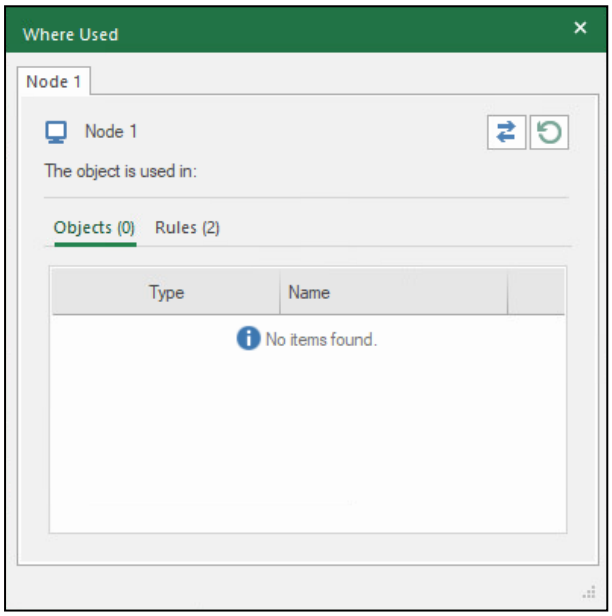
6. Make the standby Security Management Server active (see p. **53**).
7. The Configuration Manager disconnects from the standby Security Management Server.

   Note.
   Switching the role may take some time. The Security Management Server role will not change if the Security Management Server logon is performed before the role switch. In this case, you need to connect after a few minutes.

   After the reconnection, in the list of Security Gateways in **Structure**, check that the Security Gateway with the Security Management Server is displayed as the active Security Management Server.
8. Import the root certificates with private keys (see p. **67**).

   In the certificate properties, check that the private keys are imported.
9. Install the policy on all Security Gateways.
10. Go to **Access control** and select Security Gateways in the list of Security Management Server objects.
11. Right-click the replaced Security Management Server and select **Where Used...**

    The **Where Used** dialog box appears.



12. Click **Replace mode** and go to **Rules**.
13. Select the check box next to the rules and, in the **Replace with** field, open the drop-down list of objects.
14. Select the new Security Management Server and click **Replace**.

    A dialog box prompting you to confirm the replacement operation appears.
15. Click **Yes** and close the dialog box.
16. Go to **Structure**, select the replaced Security Management Server and click **Delete**.

    A dialog box prompting you to confirm the deletion appears.
17. Click **Yes**.

    After the Security Management Server is deleted, the linked license appears in the license repository.
18. Install the policy on all Security Gateways.

Documentation

1. Continent Enterprise Firewall. Version 4. Administrator guide. Deployment.
2. Continent Enterprise Firewall. Version 4. Administrator guide. Firewall.
3. Continent Enterprise Firewall. Version 4. Administrator guide. Intrusion Prevention System.
4. Continent Enterprise Firewall. Version 4. Administrator guide. Monitoring and Audit.
5. Continent Enterprise Firewall. Version 4. Administrator guide. User Authentication.
6. Continent Enterprise Firewall. Version 4. Administrator guide. VPN.
7. Continent Enterprise Firewall. Version 4. Administrator guide. Networking functions.
8. Continent Enterprise Firewall. Version 4. Administrator guide. SNMP.
9. Continent Enterprise Firewall. Version 4. Administrator guide. Installation and Update.