SECURITY
code

Continent Enterprise Firewall
Version 4

Deployment

Administrator guide

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

Mailing address: **115230, Russian Federation, Moscow,**
1st Nagatinsky proezd 10/1

Phone: **+7 (495) 982-30-20**

E-mail: **info@securitycode.ru**

Web: **www.securitycode.ru**

Table of contents

List of abbreviations

CSR	Certificate Signing Request
DB	Database
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
IPS	Intrusion Prevention System
OS	Operating System
RNG	Random Number Generator
USB	Universal Serial Bus
UTC	Coordinated Universal Time

Introduction

This manual is designed for administrators of Continent Enterprise Firewall, Version 4 (hereinafter — Continent). It contains information about deployment and configuration procedures.

This document contains links to documents [**1**] – [**4**].

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

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

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

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

Version 4.1.9 — Released on May 22nd, 2024.

Deployment procedures

The deployment of Continent consists of the following steps:

1. Deployment of the Security Management Server (see p. **7**).
2. Deployment of administrator workstations (see p. **13**).
3. Deployment of the Security Gateway with the standby Security Management Server (see p. **18**).
4. Deployment of additional Security Gateways (see p. **25**).

Note.
We recommend updating the software, the IPS protections and Web/FTP filters after deploying Continent (see [**4**]).

Chapter 1

Deployment of the Security Management Server

To deploy the Security Management Server, take the following steps:

1. Log on to the local menu (see below).

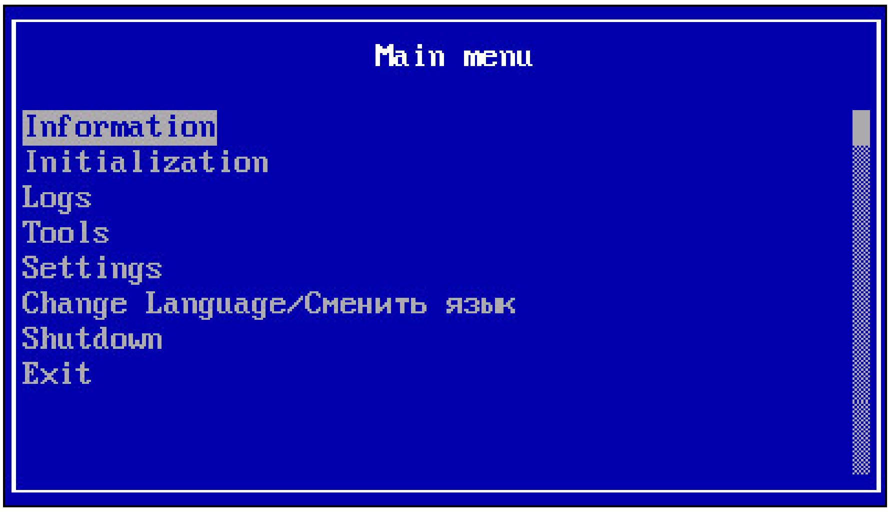
> **Note.**
> For security reasons, we recommend changing the BIOS password (see p. 44).

2. Initialize the Security Management Server (see p. 8).
3. Set up the system time (see p. 9).
4. Create a root certificate and a Security Management Server control channel certificate (see p. 9).
5. Configure the Security Management Server and install a local policy (see p. 11).

Log on to the local menu

To log on to the system:

1. Connect a keyboard and a monitor or a portable device (e.g., a laptop) to a Security Gateway (see p. 43).
2. Power on the Security Gateway.
   After loading the OS, the main menu of the Security Gateway appears as in the figure below.



Use the navigation keys to move through menu sections:

- <**Enter**> — to select the current menu section;
- <↑> — to move up;
- <↓> — to move down;
- <**Page Up**> — to move to the top;
- <**Page Down**> — to move to the bottom;
- <**Esc**> — to get back to the previous menu.

The following windows are available for an administrator:

Console	Combination
Local menu console	<**Alt**>+<**F1**>
Console with Security Gateway events	<**Alt**>+<**F6**>
Console with Security Management Server events	<**Alt**>+<**F8**>

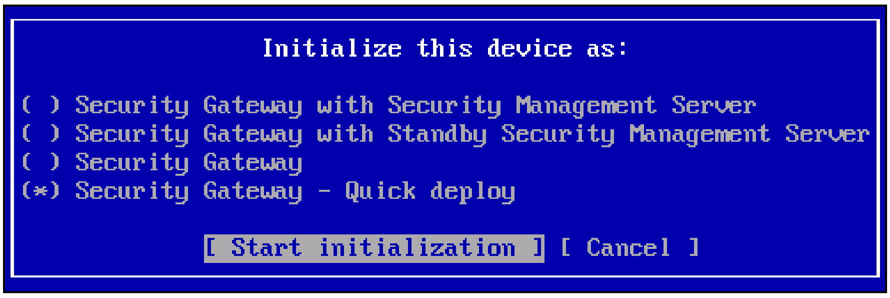
Note.
Consoles with events are available only after the Security Management Server initialization.

Initialize the Security Management Server

To initialize the Security Management Server:

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

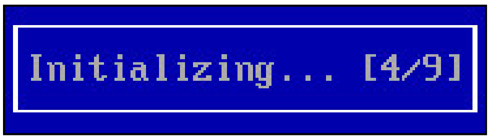
   The dialog box prompting you to select a component to be initialized appears as in the figure below.



```
                Initialize this device as:

( ) Security Gateway with Security Management Server
( ) Security Gateway with Standby Security Management Server
( ) Security Gateway
(*) Security Gateway - Quick deploy

              [ Start initialization ] [ Cancel ]
```

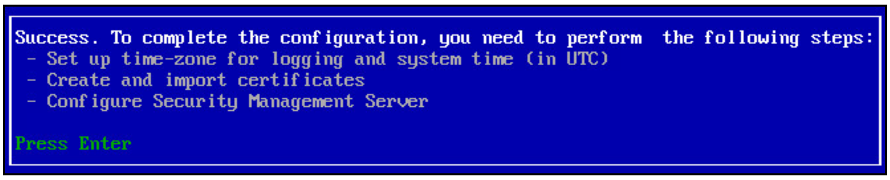
2. Select **Security Gateway with Security Management Server** and press <**Enter**>.

   The initialization of the Security Gateway starts.



```
Initializing... [4/9]
```

   Please wait until the initialization is completed with the respective message as in the figure below.

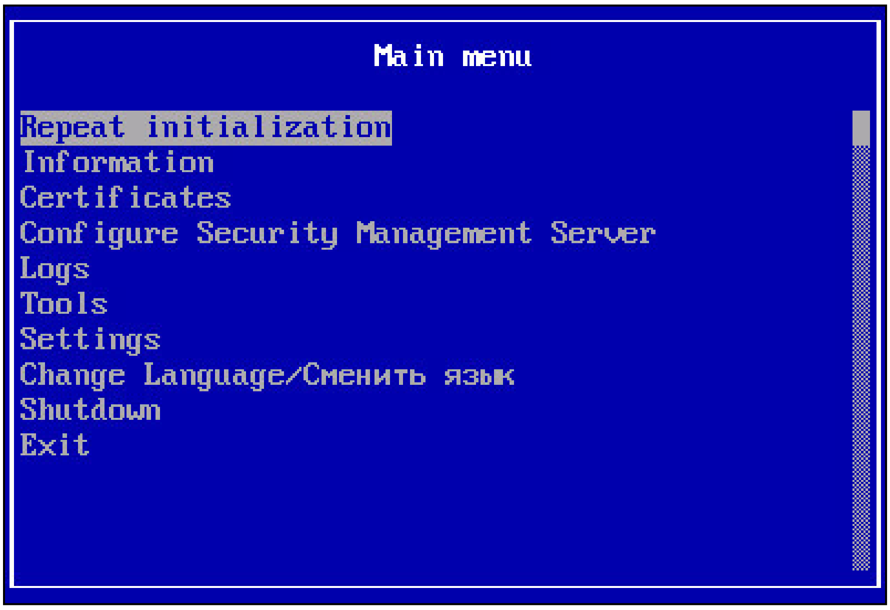


```
Success. To complete the configuration, you need to perform  the following steps:
 - Set up time-zone for logging and system time (in UTC)
 - Create and import certificates
 - Configure Security Management Server

Press Enter
```

Note.
If virtual interfaces have been added on a Security Gateway, after reinitialization or network card change, the following message might appear: **Udev rules for network interfaces are not compatible with the current equipment.** Press <**Enter**> in this case.

3. Press <**Enter**>.

   You will be returned to the main menu. When the initialization is completed, the contents of the menu will be changed.



Set up the system time

Before creating certificates, you must set up the system time. It enables the correct synchronization of Security Gateways (including Security Management Servers).

To set up the system time:

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

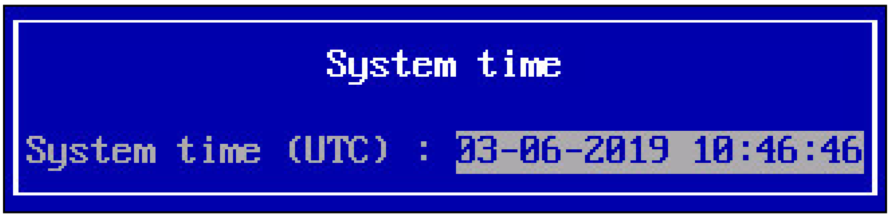
   The **Settings** menu appears.

2. Select **System time** and press <**Enter**>.

   The **Time settings** menu appears.

3. Select **Manual time setup** and press <**Enter**>.

   A window appears as in the figure below.



System time

System time (UTC) : 03-06-2019 10:46:46

4. Type the current time according to UTC+0 and press <**Enter**>.

   Note.
   For Abu Dhabi, you must set 6:05 instead of 12:05.

   The system time is set when the respective message appears.

5. Press <**Enter**>.

   You will be returned to the **System time** menu.

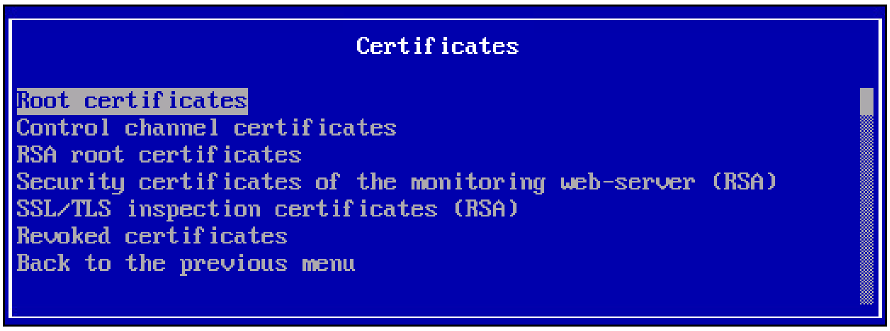
Create certificates

When deploying the Security Management Server a root certificate and a control channel certificate are created using the local menu.

To enter the Certificates menu:

- Select **Certificates** in the main menu and press **<Enter>**.

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



```
Certificates

Root certificates
Control channel certificates
RSA root certificates
Security certificates of the monitoring web-server (RSA)
SSL/TLS inspection certificates (RSA)
Revoked certificates
Back to the previous menu
```

To create a root certificate:

1. In the **Certificates** menu, select **Root certificates** and press <**Enter**>.

   The **Root certificates** menu appears.

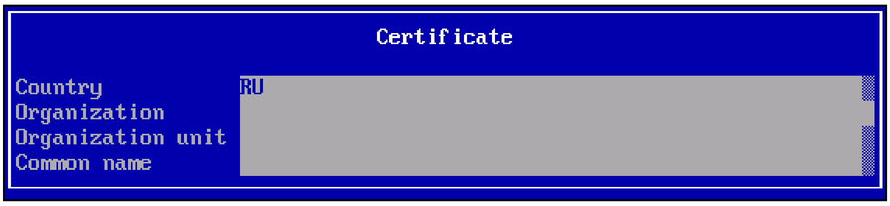
   Note.
   To work with the update server, there is a pre-installed **Trusted Publisher** root certificate. It cannot be used for other purposes.

2. To create a root certificate, press <**F2**>.

   The **Issue certificate** menu appears.

3. Select **Issue root certificate** and press <**Enter**>.

   The dialog box appears as in the figure below.



```
Certificate

Country              RU
Organization
Organization unit
Common name
```

4. Specify the required information in the respective fields and press <**Enter**>.

   Note.
   To move through the sections, use the following keys: <**↑**>, <**↓**>, <**Tab**>, <**Page Down**>, <**Page Up**>, <**Home**>, <**End**>.

   When the certificate is created, the respective message appears.

5. Press <**Enter**>.

   You will be returned to the **Issue certificate** menu.

6. Press <**Esc**>.

   You will be returned to the **Root certificates** menu. You can see the new certificate here.

7. Press <**Esc**>.

   You will be returned to the **Certificates** menu.

To create a control channel certificate:

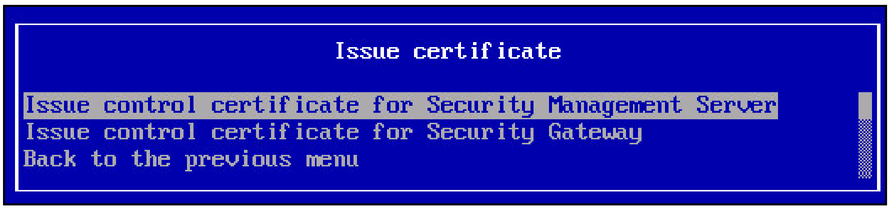
1. In the **Certificates** menu, select **Control channel certificates** and press <**Enter**>.

   The **Control channel certificates** menu appears.

   Note.
   If you create a certificate for the first time, the list of certificates is empty.

2. Press <**F2**>.

   The **Issue certificate** menu appears as in the figure below.



```
Issue certificate

Issue control certificate for Security Management Server
Issue control certificate for Security Gateway
Back to the previous menu
```

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

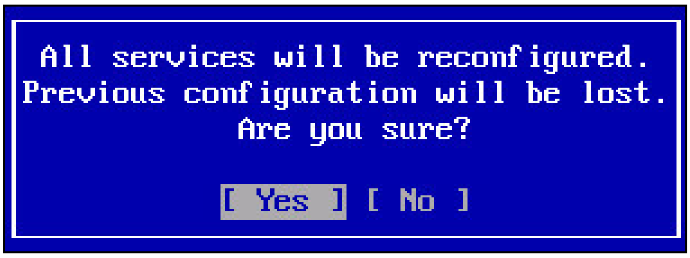
The **Certificate** menu appears.

4. Specify the required information in the respective fields and press <**Enter**>.
   The list of created root certificates appears.
5. Select a root certificate created in the previous procedure (see p. **10**) from the list and press <**Enter**>.
   When the certificate is created, the respective message appears.
6. Press <**Enter**>.
   You will be returned to the **Issue certificate** menu.
7. Press <**Esc**>.
   You will be returned to the **Control channel certificates** menu. You can see the new certificate here.
8. Press <**Esc**>.
   You will be returned to the **Certificates** menu.

Configure the Security Management Server

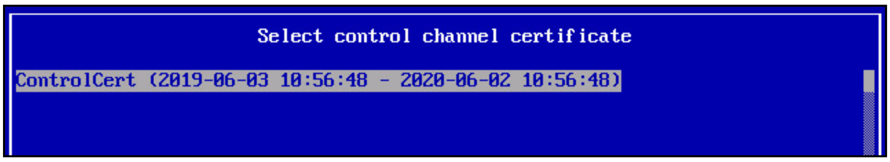
To configure the Security Management Server:

1. In the local menu, select **Configure Security Management Server** and press <**Enter**>.
   A warning message appears as in the figure below.



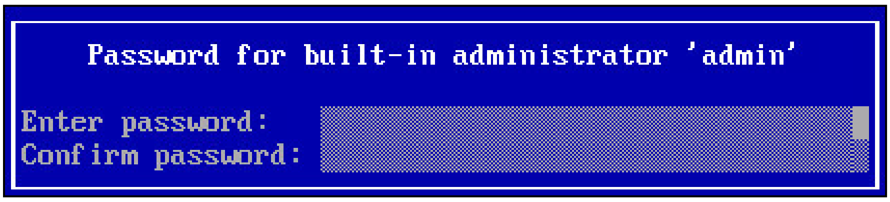
```
All services will be reconfigured.
Previous configuration will be lost.
Are you sure?
```

2. Select **Yes** and press <**Enter**>.
   The **Select control channel certificate** window appears as in the figure below.



```
Select control channel certificate

ControlCert (2019-06-03 10:56:48 - 2020-06-02 10:56:48)
```

3. Select the certificate of the Security Management Server (see p. **10**) and press <**Enter**>.
   The dialog box prompting you to type the main administrator password appears.
4. Type the password twice and press <**Enter**>.

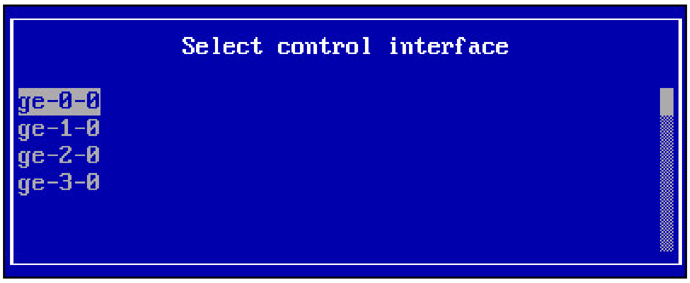


```
Password for built-in administrator 'admin'

Enter password:
Confirm password:
```

Note.
The password must contain at least 8 characters, one uppercase and one lowercase English letters, one base-10 digit and one of the following characters:

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

After you create the password, you can select a control interface.

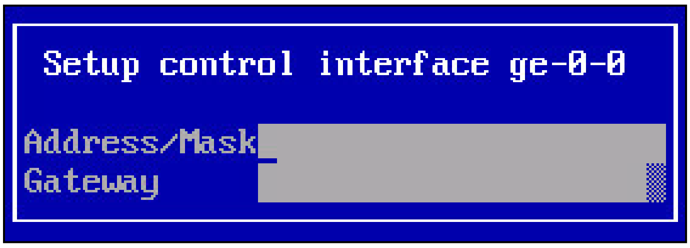


```
Select control interface

ge-0-0
ge-1-0
ge-2-0
ge-3-0
```

For more details about the interface syntax, see p. 45

5. Select the control interface connected to the administrator workstation and press <**Enter**>.

   The dialog box appears as in the figure below.



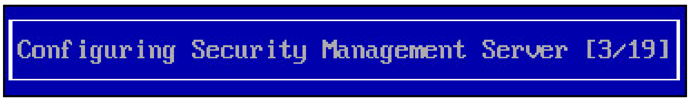
```
Setup control interface ge-0-0

Address/Mask
Gateway
```

6. Type the IP address of the Security Management Server specifying the mask prefix and IP address of a gateway (if necessary), press <**Enter**>.

   The dialog box prompting you to apply settings appears.

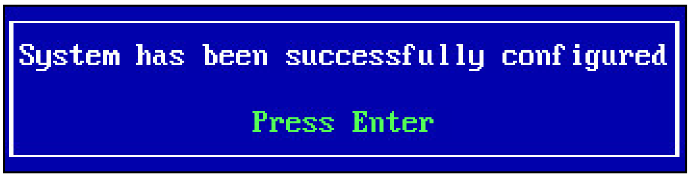
7. To apply the settings, select <**Yes**> and press <**Enter**>.

   The configuration of the Security Management Server starts.



```
Configuring Security Management Server [3/19]
```

When it is completed, you receive the respective message.



```
System has been successfully configured

Press Enter
```

8. Press <**Enter**>.

   After the configuration is completed, you will be returned to the main menu for user authentication.

Attention!

In case of a Security Management Server configuration failure, check the events in the system log.

After troubleshooting, perform re-initialization in the **Tools** menu, restart the Security Management Server, re-configure time settings and re-create certificates.

Note.

You can use main functions of Continent after the Security Management Server initialization. It is provided by a demo license with a null Client ID. The demo license does not allow you to use Advanced application control and Web/FTP filters. The number of connections to the Access Server is limited to 2. The demo license expires in 14 day and after that the functions will be limited. To resume using all the functions of Continent, install the Configuration Manager (see [**4**]) and upload new licenses to the Security Management Server repository (see **License management** in [**1**]).

Chapter 2

Deployment of administrator workstation

The Configuration Manager is software for remote control of the Security Management Server and other Security Gateways.

To perform the deployment of the administrator workstation, take the following steps:

1. Install the Configuration Manager and Security Code CSP (see [**4**]).
2. Run the Configuration Manager and connect it to the Security Management Server (see p. **13**).
3. Configure the Monitoring and Audit System (see [**2**]).

> **Note.**
> You can use the Monitoring and Audit System on any host in a protected network after you apply respective settings.

Configure an administrator workstation

To run the Configuration Manager for the first time, take the following steps:

1. Get ready to run the Configuration Manager (see below).
2. Run the Configuration Manager (see p. **14**).
3. Initialize an RNG using human input (see p. **14**).
4. Connect to the Security Management Server (see p. **15**).

> **Note.**
> Versions of the Configuration Manager and the Security Management Server must match.

When you run the Configuration Manager next time, the dialog box prompting you to connect to the Security Management Server appears. Its fields are automatically filled with the IP address or name of the Security Management Server to which the Configuration Manager connected last and the administrator account that was used during previous logon.

Get ready to run the Configuration Manager

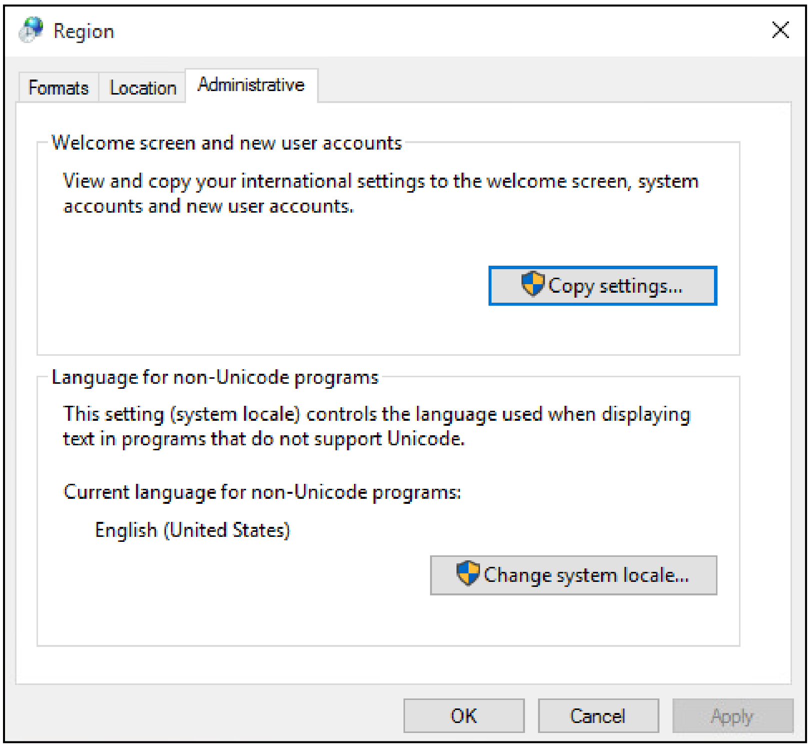
Check the regional OS settings and make sure that all programs in English support Unicode before running the Configuration Manager. Otherwise, you cannot connect to the Security Management Server and receive the respective error message.

To check the regional settings of OS:

1. Go to **Control panel | Region**.
2. On the **Administrative** tab, if **English** is not specified in **Languages that do not support Unicode**, click **Change system locale**.

   > **Note.**
   > If there is a request to enter or confirm an administrator password, specify the password in the respective field.

3. Select **English (United States)** and click **OK**.



View and copy your international settings to the welcome screen, system accounts and new user accounts.

This setting (system locale) controls the language used when displaying text in programs that do not support Unicode.

Current language for non-Unicode programs:

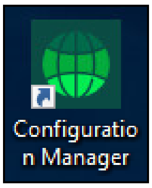
English (United States)

4. Restart your computer.

Run the Configuration Manager

To run the Configuration Manager:

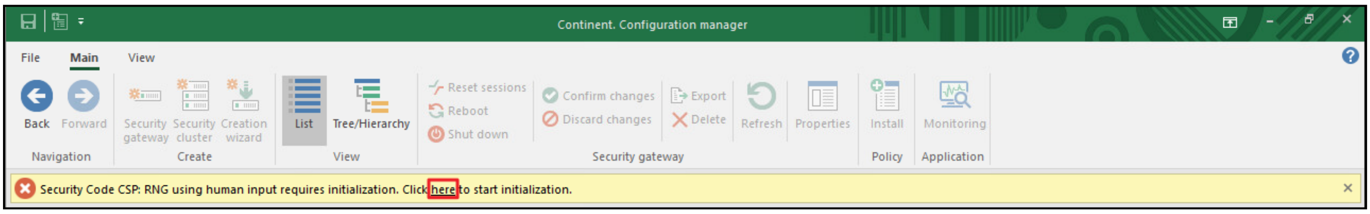
- Double-click the shortcut that is shown in the figure below.



The main window of the Configuration Manager and the **Administrator authentication** dialog box appear (see p. **16**).

Initialize the RNG using human input

If you run the Configuration Manager for the first time after the installation, you receive a message prompting you to initialize the RNG using human input as in the figure below.



Security Code CSP: RNG using human input requires initialization. Click here to start initialization.

To start the initialization of RNG using human input:

1. Click **Here** to start the RNG using human input initialization process and follow the instructions to gather entropy.

Attention!

If you miss the target, entropy may decrease.

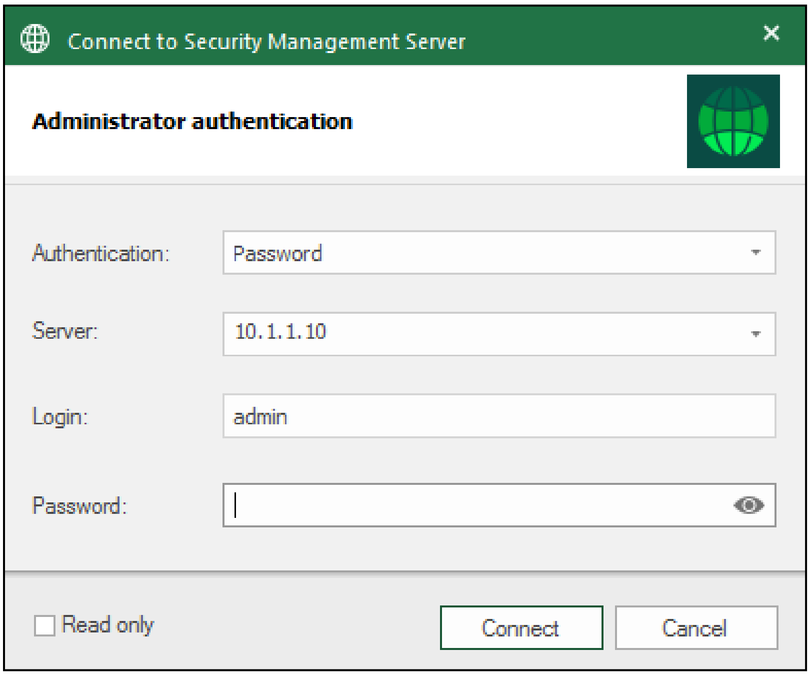
2. After the entropy is gathered, click ▾ in the upper left corner of the Configuration Manager, then click **Connect**.

Connect to the Security Management Server

To connect to the Security Management Server:

1. Run the Configuration Manager (see above).

   The **Administrator authentication** dialog box appears as in the figure below.



Connect to Security Management Server

Administrator authentication

Authentication: Password

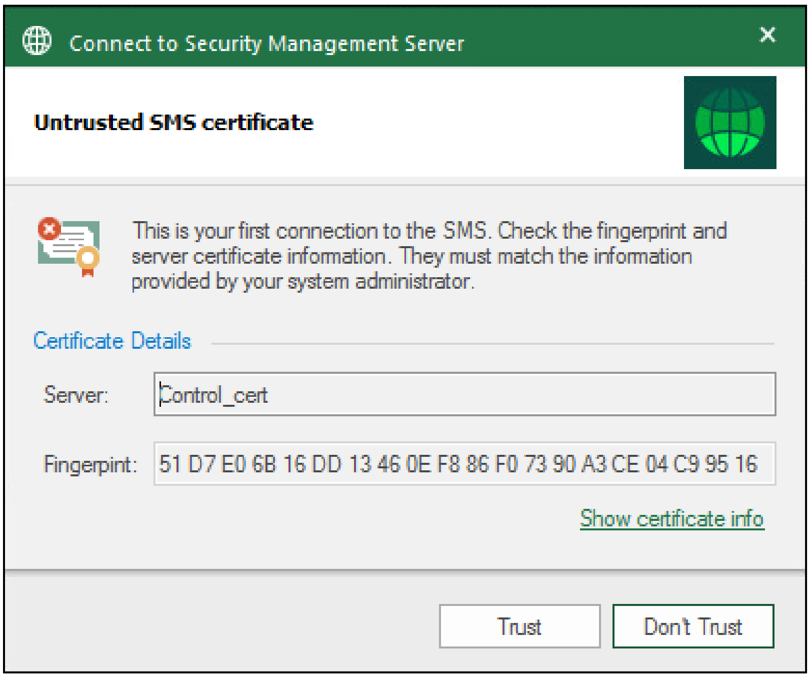
Server: 10.1.1.10

Login: admin

Password:

2. In the **Authentication** drop-down list, select **Password**. In the **Server** text box, specify the IP address of the Security Management Server to which you want to connect.
3. Enter the login and the password of the administrator in the respective text boxes, click **Connect**.

   The respective dialog box prompting you to verify the certificate appears. This dialog box appears during the first connection to the Security Management Server and after every update (automatic or manual) of the control channel certificate of the Security Management Server.



Connect to Security Management Server

Untrusted SMS certificate

This is your first connection to the SMS. Check the fingerprint and server certificate information. They must match the information provided by your system administrator.

Certificate Details

Server: Control_cert

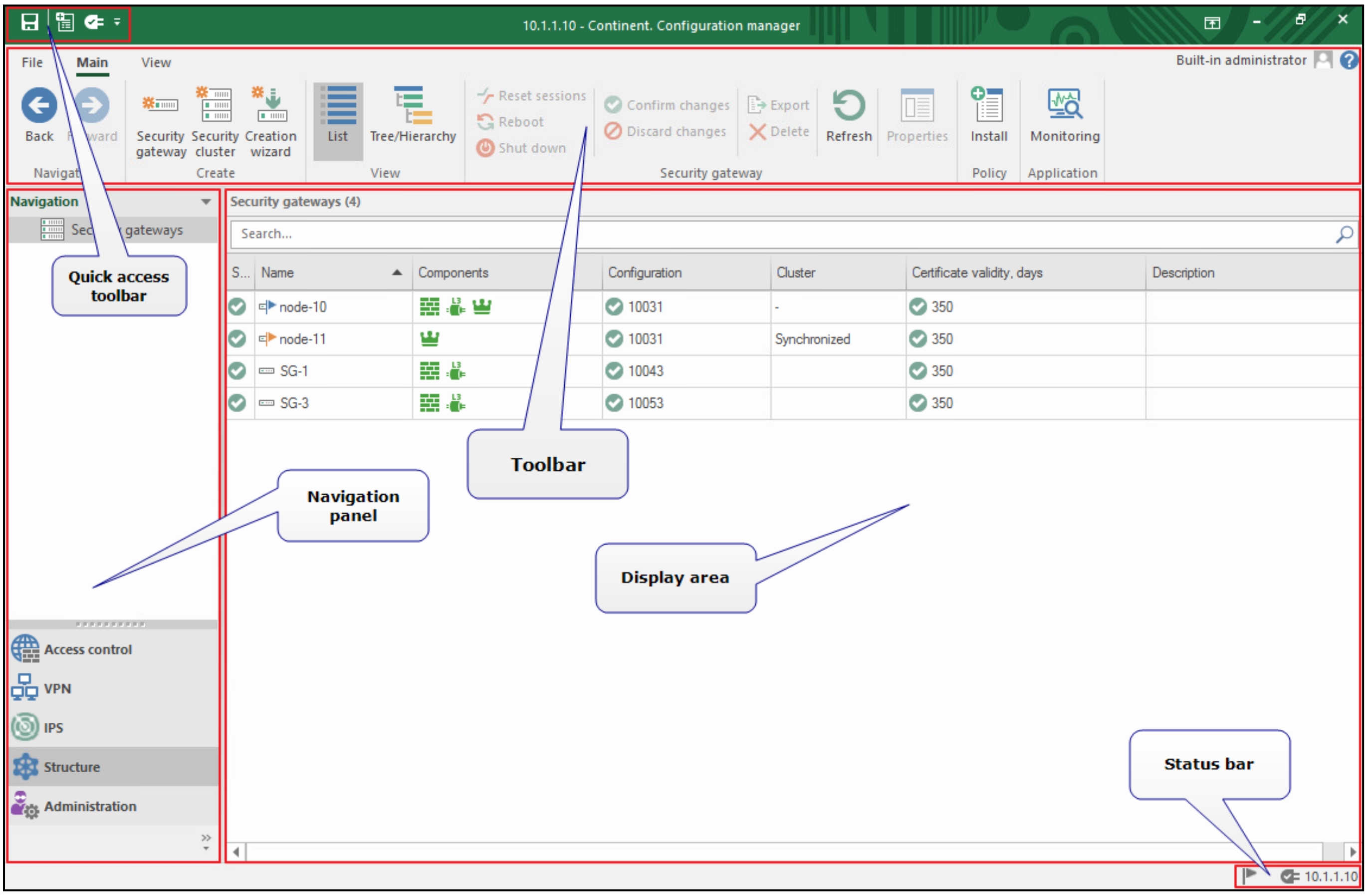
Fingerprint: 51 D7 E0 6B 16 DD 13 46 0E F8 86 F0 73 90 A3 CE 04 C9 95 16

4. Check the certificate parameters and click **Trust**.

If the Configuration Manager successfully connects to the Security Management Server, the main window appears. It contains information about the current status of Continent.

Interface of Configuration Manager

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



Security gateways (4)

S...	Name	Components	Configuration	Cluster	Certificate validity, days	Description
✓	node-10		✓ 10031	-	✓ 350	
✓	node-11		✓ 10031	Synchronized	✓ 350	
✓	SG-1		✓ 10043		✓ 350	
✓	SG-3		✓ 10053		✓ 350	

The Configuration Manager window contains the following elements:

Element of the interface	Description
Toolbar	Contains a set of tools and two tabs: • **Main** — displays the toolbar; • **View** — allows configuring the interface of the Configuration Manager. Tools are buttons that you can use to launch frequently used commands. A set of tools depends on a menu item which you can select on the navigation panel. Operating conditions determine which buttons are displayed and available. When you move the pointer over a button, a tooltip appears
Quick access toolbar	Allows quick access to the most frequently used buttons. Contains the following: • — save the current configuration; • — install a security policy; • — configure the Security Management Server connections; • — connect to the Security Management Server; • — configure Quick access toolbar; • — open Quick access toolbar

Element of the interface	Description
Navigation panel	Contains the following menu items: • **Access control** — to manage Firewall and NAT rules; • **VPN** — to create and configure VPN; • **IPS** — to configure IPS settings; • **Structure** — to manage Security Gateway settings; • **Administration** — to manage service functions (operations with certificates, backups, updates, licenses, etc.)
Display area	Displays information depending on the selected navigation panel menu item
Status bar	Contains the following: • the number of tasks currently being executed and the button to open the notification center ⚑ where you can find the link to open the general task list; • an icon that indicates the status of the connection to the Security Management Server (if there is a connection, this icon also displays a Security Management Server IP address, for example 10.1.1.10)
Authorized administrator	Displays information about the administrator account
? **About Configuration Manager**	Displays information about the program, its version and copyright

Chapter 3
Deployment of the Security Gateway with the standby Security Management Server

To deploy the Security Gateway with the standby Security Management Server, take the following steps:

Note.
For security reasons, we recommend changing the BIOS password (see p. 44).

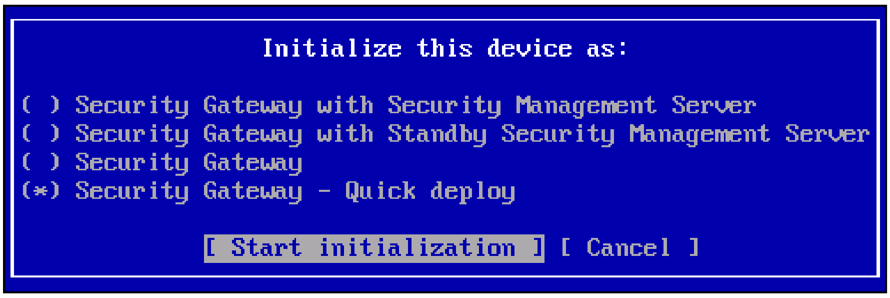
1. Initialize the standby Security Management Server using the local menu (see p. 18).
2. Set up the system time using the local menu (see p. 9).
3. Create a Security Management Server control channel certificate using the local menu and the standby Security Management Server (see p. 19).
4. Create a standby Security Management Server in the local menu of the active Security Management Server (see p. 21).
5. Connect the standby Security Management Server to the active Security Management Server using the local menu (see p. 21).
6. Confirm the configuration of the standby Security Management Server on the active Security Management Server and link a license to the standby Security Management Server using the Configuration Manager (see p. 22).
7. Synchronize the standby Security Management Server with the active Security Management Server using the Configuration Manager (see p. 23).
8. Export root certificates with private keys from the active Security Management Server.

Initialize the standby Security Management Server using the local menu

To initialize the standby Security Management Server:

1. In the main menu of the Security Gateway with the standby Security Management Server, select **Initialization** and press **<Enter>**.

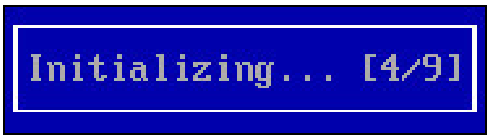
   The dialog box prompting you to select a component to be initialized appears as in the figure below.



```
              Initialize this device as:

( ) Security Gateway with Security Management Server
( ) Security Gateway with Standby Security Management Server
( ) Security Gateway
(*) Security Gateway - Quick deploy

         [ Start initialization ] [ Cancel ]
```

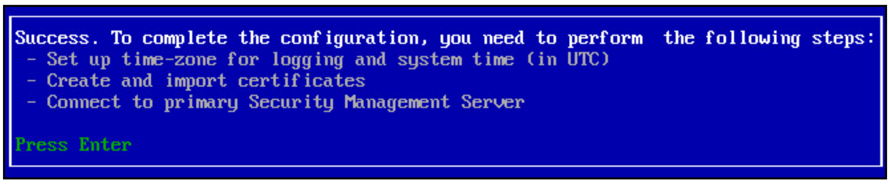
2. Select **Security Gateway with standby Security Management Server** and press **<Enter>**.

   The initialization of the Security Gateway starts.



```
Initializing... [4/9]
```

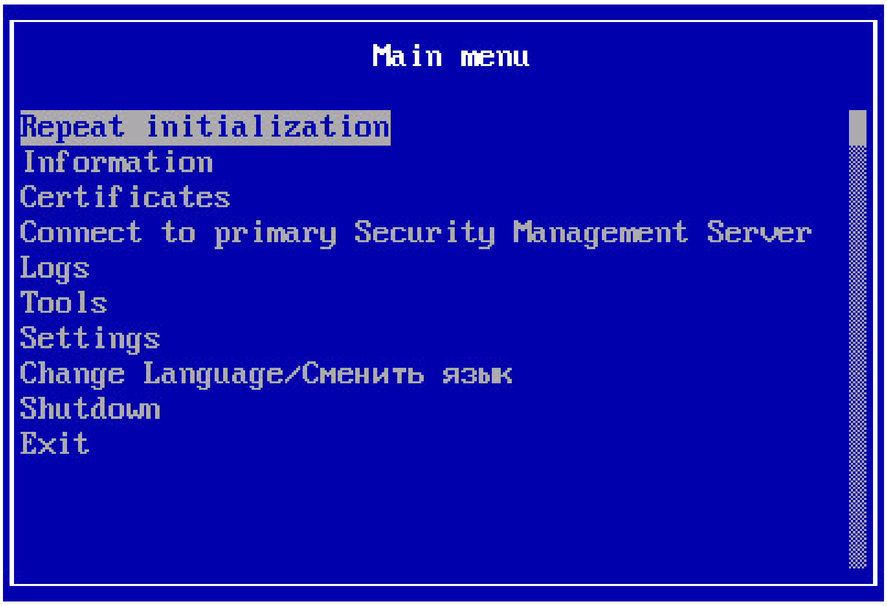
   Please wait until the initialization is completed with a respective message as in the figure below.



```
Success. To complete the configuration, you need to perform  the following steps:
 - Set up time-zone for logging and system time (in UTC)
 - Create and import certificates
 - Connect to primary Security Management Server

Press Enter
```

3. Press **<Enter>**.

   You will be returned to the main menu. When the initialization is completed, the contents of the menu will be changed.



```
                     Main menu

Repeat initialization
Information
Certificates
Connect to primary Security Management Server
Logs
Tools
Settings
Change Language/Сменить язык
Shutdown
Exit
```

Create a Security Management Server certificate using the local menu and the standby Security Management Server

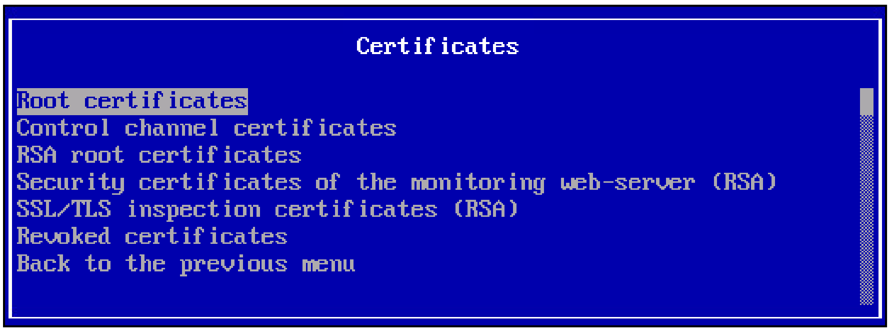
When deploying the Security Management Server via the local menu, only a control channel certificate is created.

Create a certificate signing request (CSR)

To enter the Certificates menu:

- In the main menu, select **Certificates** and click <**Enter**>.

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



```
                     Certificates

Root certificates
Control channel certificates
RSA root certificates
Security certificates of the monitoring web-server (RSA)
SSL/TLS inspection certificates (RSA)
Revoked certificates
Back to the previous menu
```

To create a certificate signing request of a control channel certificate:

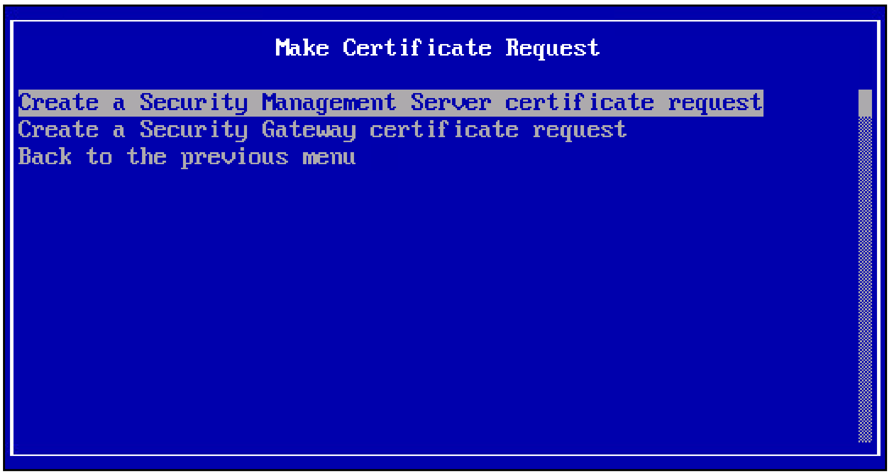
1. In the **Certificates** menu, select **Control channel certificates** and press <**Enter**>.

   The **Control channel certificates** menu appears.

> **Note.**
> If you create a certificate for the first time, the list of certificates is empty.

2. Press <**F4**>.

   The **Make Certificate Request** menu appears as in the figure below.



Make Certificate Request

Create a Security Management Server certificate request
Create a Security Gateway certificate request
Back to the previous menu

3. Select **Create a Security Management Server certificate request** and press <**Enter**>.

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

   The **Certificate** menu appears.
5. Specify the required information in the respective fields and press <**Enter**>.

   You receive the message about the successful export of the request to the USB drive.
6. Press <**Enter**>.

   You will be returned to the **Make certificate request** menu.
7. Press <**Esc**>.

   You will be returned to the **Control channel certificates** menu. The new request appears in the list.

Issue a standby Security Management Server control channel certificate on the active Security Management Server

To issue a certificate in the local menu:

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

   The **Certificates** menu appears.
2. Select **Control channel certificates** and press <**Enter**>.

   The **Control channel certificates** menu appears.
3. Press <**F2**>.

   The **Issue certificate** menu appears.
4. Select **Issue control certificate for Security Gateway** and press <**Enter**>.

   The dialog box prompting for a CSR appears.
5. Insert a USB drive, click **Yes** and press <**Enter**>.

   The list of files from the USB drive appears.

   Note.
   The request file default name is **continent-XX.req**, where **XX** is the Security Gateway ID.
6. Select the required request file and press <**Enter**>.

   The dialog box prompting you to select the root certificate appears.
7. Select the required root certificate and press <**Enter**>.

   When the standby Security Management Server control channel certificate is issued, the respective message appears.
8. Press <**Enter**>.

   You will be returned to the **Issue certificate** menu.
9. Select **Back to previous menu** and press <**Enter**>. You will be returned to the **Control channel certificates** menu. You can see the new certificate here.

Create a standby Security Management Server on the active Security Management Server in the local menu

To create a standby Security Management Server in the local menu of the active Security Management Server:

1. In the main menu of the active Security Management Server, select **Tools** and press <**Enter**>.

   The **Tools** menu appears.

2. Select **Create security gateway with standby Security Management Server** and press <**Enter**>.

   The dialog box prompting you to insert a USB drive appears (if it was not inserted earlier).

3. Insert the USB drive and press <**Enter**>.

   The dialog box prompting you to enter the ID of the Security Gateway with the standby Security Management Server appears.

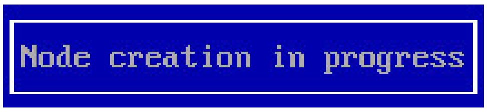
   > **Note.**
   > ID is the identifier of a hardware appliance shown on its case and specified in its datasheet.

4. Enter the ID and press <**Enter**>.

   The dialog box prompting you to select a control channel certificate for the standby Security Management Server appears.

5. Select the control channel certificate created earlier and press <**Enter**>.

   The process of standby Security Management Server creation starts.



```
Node creation in progress
```

   When the operation is completed, the respective message appears. The configuration file of the Security Gateway with the standby Security Management Server will be exported to the USB drive.

6. Press <**Enter**>.

   You will be returned to the **Tools** menu.

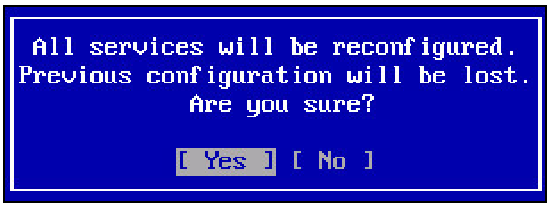
Connect the standby Security Management Server to the active Security Management Server in the local menu

Before starting the procedure, prepare a USB drive with the configuration file **gate-XX.json** (**XX** is the ID of a Security Gateway).

To connect the standby Security Management Server to the active Security Management Server:

1. In the main menu of the standby Security Management Server, select **Connect to active Security Management Server**.

   The warning message appears as in the figure below.



```
All services will be reconfigured.
Previous configuration will be lost.
Are you sure?
```

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

   The dialog box prompting you to insert a USB drive appears (if it was not inserted earlier).

3. Insert the USB drive with the configuration saved earlier and press <**Enter**>.

   The list of files from the USB drive appears.

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

   The window prompting you to select the Security Gateway control interface appears.

5. Select an interface that will be used for connection to the Security Management Server and press <**Enter**>.

The window prompting you to configure the Security Gateway control interface appears.

6. Type its IP address and mask, the IP address of the Security Gateway and press <**Enter**>.

   The window prompting you to confirm the new settings appears.

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

   The configuration of the Security Gateway starts. When the operation is completed, the respective message appears.

8. Press <**Enter**>.

Confirm the configuration and link a license to the standby Security Management Server

> **Note.**
> If you receive a message about the lock takeover in the Configuration Manager, you need to reconnect to the Security Management Server.

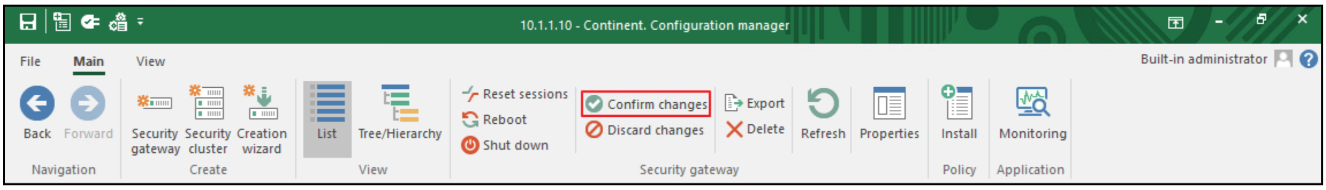
To confirm the Security Gateway configuration and link a license to the standby Security Management Server:

1. Open the Configuration Manager and go to **Structure**.

   In the display area, you can see a list of Security Gateways.

   > **Note.**
   > If you cannot see a local configuration version of the Security Gateway with the standby Security Management Server on the list, click **Refresh** on the toolbar.

2. Select the Security Gateway to be connected from the list. On the toolbar, click **Confirm changes**.



   The dialog box prompting you to confirm local changes appears.

3. Click **Yes**.

   When the system applies all the changes to the Security Management Server configuration and saves it to the DB, the respective message appears.

4. Click **OK**.

5. In the Configuration Manager, go to **Administration** and select **Licenses**.

6. In the list, select the standby Security Management Server and click **Link license** on the toolbar.

   The dialog box with available licenses under the following conditions appears:

   - The license has not expired.
   - The platform type of the license (if specified) matches the platform type of the linked Security Gateway.
   - The Security Gateway ID in the license (if specified) matches the ID of the linked Security Gateway.

   Adding licenses to the repository is described in [**1**], **Managing licenses**.

7. Select the required license and click **OK**.

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

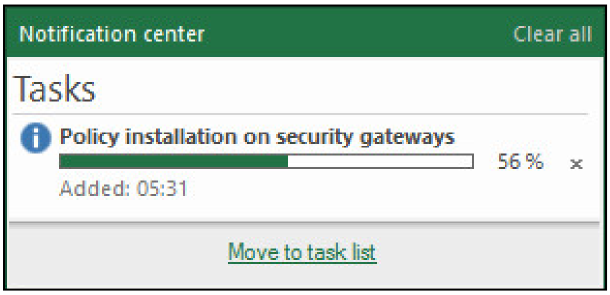
8. To save changes in the configuration, click the main menu button and then click 💾.

9. On the toolbar, click **Install**.

   A dialog box for applying policies to Security Gateways appears.

10. In the **Install policy** dialog box, select the required Security Gateway with the standby Security Management Server and click **OK**.

    The task to install the policy on the selected Security Gateway is created and appears in the notification center. The notification center displays the progress of tasks.



11. Wait for the operation to complete.

Synchronize the standby Security Management Server with the active Security Management Server

Synchronization of the standby Security Management Server with the active Security Management Server is performed automatically. If necessary, you can perform synchronization manually.

To synchronize the standby Security Management Server with the active one:

1. Open the Configuration Manager and go to **Structure**.

   In the display area, you can see a list of Security Gateways.
2. Right-click the Security Gateway and select **Replication — Synchronize Security Management Server**.

   The dialog box prompting you to confirm the Security Management Server synchronization appears.
3. Select **Yes** and press <**Enter**>.

   The synchronization starts. The notification center displays the progress of the task in real time.

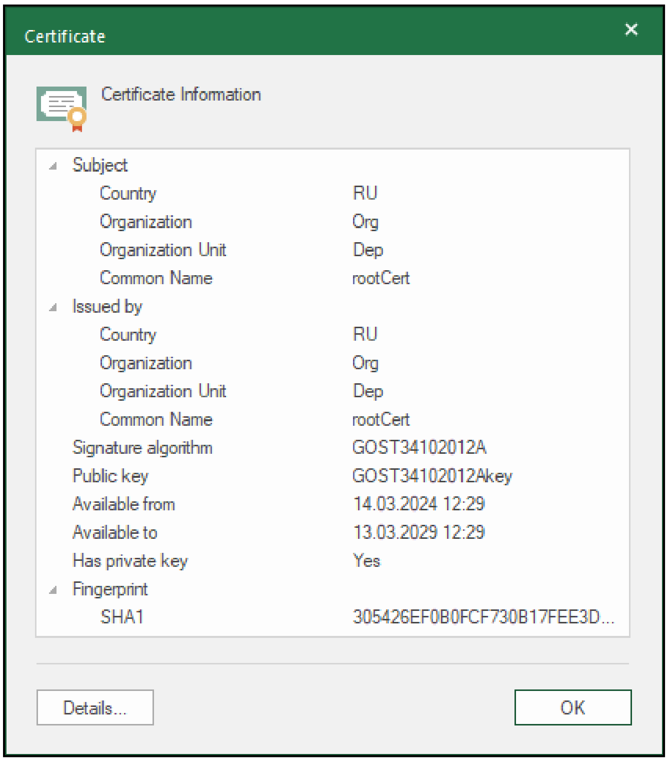
   When the operation is completed, the Security Gateway with the standby Security Management Server has the **Synchronized** status.

Export root certificates with private keys from the active Security Management Server

To export root certificates with private keys from the active Security Management Server:

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 the root certificates with private keys (see [**5**], the **Export certificates** section) without deleting the private key after a successful export.

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



Certificate

Certificate Information

Subject	
Country	RU
Organization	Org
Organization Unit	Dep
Common Name	rootCert
Issued by	
Country	RU
Organization	Org
Organization Unit	Dep
Common Name	rootCert
Signature algorithm	GOST34102012A
Public key	GOST34102012Akey
Available from	14.03.2024 12:29
Available to	13.03.2029 12:29
Has private key	Yes
Fingerprint	
SHA1	305426EF0B0FCF730B17FEE3D...

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

6. Make the standby Security Management Server the active one (see [**5**], the **Manage Security Management Server redundancy** section).

7. The Configuration Manager disconnects from the standby Security Management Server.

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

Check that after the reconnection, in the list of Security Gateways in **Structure**, this Security Gateway with the Security Management Server is displayed as the active Security Management Server.

8. Import the root certificates with private keys (see [**5**], the **Import certificates and security keys** section).

In the certificate properties, check that the private keys are imported.

9. Install the policy on all Security Gateways.

Chapter 4

Deployment of Security Gateway

To deploy a Security Gateway, we recommend taking the following steps:

1. Initialize the Security Gateway (see below).
2. Configure the system time (see p. **9**).
3. Connect Security Gateway to the Security Management Server (see p. **25**).

If you need to initialize a group of Security Gateways without connection to the Security Management Server, go to the Security Gateway creation wizard (see p. **40**).

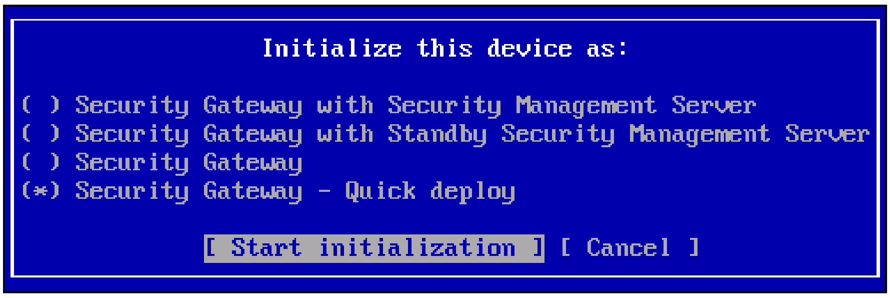
Initialize the Security Gateway

Note.
For security reasons, we recommend changing the BIOS password.

To initialize the Security Gateway:

1. In the main menu of the Security Gateway (see p. **7**), select **Initialization** and press <**Enter**>.

   The dialog box prompting you to select the component appears.

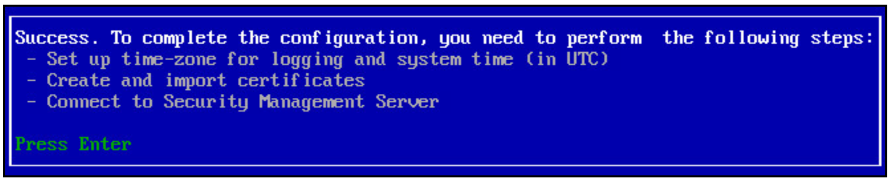


```
                  Initialize this device as:

( ) Security Gateway with Security Management Server
( ) Security Gateway with Standby Security Management Server
( ) Security Gateway
(*) Security Gateway - Quick deploy

          [ Start initialization ] [ Cancel ]
```

2. Select **Security gateway** and press <**Enter**>.

   The initialization of the Security Gateway starts.

   Please wait until the initialization is finished with the respective message as in the figure below.



```
Success. To complete the configuration, you need to perform  the following steps:
 - Set up time-zone for logging and system time (in UTC)
 - Create and import certificates
 - Connect to Security Management Server

Press Enter
```

3. Press <**Enter**>.

   You will be returned to the main menu.

Connect the Security Gateway to the Security Management Server

Find out the Security Gateway ID (it can be found on the case of the Security Gateway hardware appliance or in its datasheet) and prepare a USB drive before you start the procedure to export files onto it. The files are required to configure the connection between Security Gateway and Security Management Server.

Attention!
We do not recommend using a USB drive containing other private keys in order to avoid container confusion.

You can connect a Security Gateway to the Security Management Server in one of the following ways:

- Case 1. Connect a Security Gateway to the Security Management Server using a certificate issued in the Security Management Server local menu (see below).

- Case 2. Connect a Security Gateway to the Security Management Server using a certificate issued in the Security Management Server local menu by a request from the Security Gateway local menu (see p. **29**).
- Case 3. Connect a Security Gateway to the Security Management Server using a certificate issued in the Configuration Manager (see p. **31**).
- Case 4. Connect a Security Gateway to the Security Management Server using a certificate issued in the Configuration Manager by a request from the Security Gateway local menu (see p. **36**).

Attention!
Regardless of the case, we recommend installing the respective policy on the Security Management Server after connecting a new Security Gateway.

Case 1

To connect a Security Gateway to the Security Management Server, take the following steps:

1. Issue a Security Gateway certificate using the Security Management Server local menu (see below).
2. Create a Security Gateway using the Security Management Server local menu (see p. **26**).
3. Configure and connect the Security Gateway to the Security Management Server using the local menu (see p. **27**).
4. Confirm the Security Gateway configuration in the Configuration Manager (see p. **28**).
5. Link a license to the Security Gateway in the Configuration Manager (see p. **28**).

To issue a Security Gateway certificate using the local menu:

1. In the Security Management Server local menu, select **Certificates** and press <**Enter**>.

   The **Certificates** menu appears.
2. Select **Control channel certificates** and press <**Enter**>.

   The respective window appears.
3. Press <**F2**>.

   The **Issue certificate** dialog box appears.
4. Select **Issue control certificate for Security Gateway** and press <**Enter**>.

   The dialog box prompting for a CSR appears.
5. Select **No** and press <**Enter**>.

   The dialog box prompting you to enter identification attributes appears.
6. Specify the required information in the respective fields and press <**Enter**>.

   The dialog box prompting you to set the password for the key container appears.
7. Set the password and press <**Enter**>.

   The dialog box prompting for a key container name appears.
8. Set the name and press <**Enter**>.

   You receive the message about successful CSR saving.
9. Press <**Enter**>.

   The dialog box prompting you to select a root certificate appears.
10. Select the required root certificate and press <**Enter**>.

    You receive the message that the certificate has been successfully issued.
11. Press <**Enter**>.

    You will be returned to the **Issue certificate** menu.
12. Select **Back to previous menu** and press <**Enter**>.

    You will be returned to the **Control channel certificates** menu. You can see the new certificate in the list.

To create a Security Gateway using the Security Management Server local menu:

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

   The **Tools** menu appears.
2. Select **Create Security Gateway** and press <**Enter**>.

   The dialog box prompting you to insert a USB drive appears.
3. Insert a USB drive and press <**Enter**>.

   The dialog box prompting you to specify a Security Gateway ID appears.

> **Note.**
> The Security Gateway ID is an identifier shown on the Security Gateway hardware appliance case, in its datasheet, and in the local menu.

4. Enter the Security Gateway ID and press <**Enter**>.

The dialog box prompting you to specify a Security Gateway control certificate appears.

5. Select the certificate for the Security Gateway and press <**Enter**>.

The process of Security Gateway creation starts. When the operation is completed, the respective message appears. The configuration file of the Security Gateway will be exported to the USB drive.

6. Press <**Enter**>.

You will be returned to the **Tools** menu.

> **Note.**
> The configuration file name is **gate-XX.json**, where **XX** is the Security Gateway ID.

7. Remove the USB drive.

To configure the Security Gateway and connect it to the Security Management Server:

> **Note.**
> Prepare a USB drive with the configuration file **gate-XX.json** (**XX** is the Security Gateway ID).

1. Insert the USB drive.

2. In the main menu of the Security Gateway, select **Certificates | Control channel certificates** and press <**Enter**>.

The **Control channel certificates** window appears.

3. Press <**F5**>.

The window for selecting the request file appears.

4. Select the required file with the **.req** extension and press <**Enter**>.

The window for selecting the private key container appears.

5. Select the required private key container and press <**Enter**>.

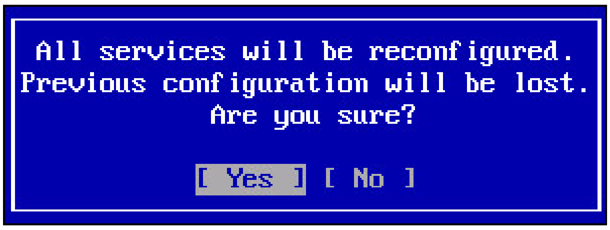
The password entry window appears.

6. Enter the password and press<**Enter**>.

The certificate request file and key information will be imported. When the operation is completed, you receive the respective message.

7. In the main menu of the Security Gateway, select **Connect to Security Management Server** and press <**Enter**>.

The warning message appears as in the figure below.



All services will be reconfigured.
Previous configuration will be lost.
Are you sure?

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

The list of files from the USD drive appears.

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

The window for selecting the Security Gateway management interface appears.

10. Select an interface that will be used for connection to the Security Management Server and press <**Enter**>.

The window for configuring the Security Gateway management interface appears.

11. Type its IP address and mask, the IP address of the gateway (if necessary) and press <**Enter**>.

The window prompting you to confirm the new settings appears.

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

When the operation is completed, you receive the respective message.

13. Press <**Enter**>.

To confirm the Security Gateway configuration:

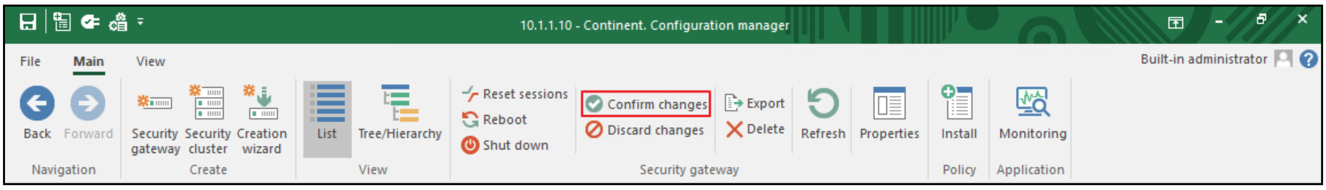
> **Note.**
> If you receive a message about the lock takeover in the Configuration Manager, reconnect the Security Management Server.

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

   The list of Security Gateways appears in the display area.

   > **Note.**
   > If you cannot see the local version of the Security Gateway configuration in the list, click **Refresh** on the toolbar.

2. Select the Security Gateway and click **Confirm changes** on the toolbar.



   The dialog box prompting you to confirm local changes appears.

3. Click **Yes**.

   When the system applies all changes to the Security Management Server configuration and saves it to the database, you receive the respective message.

   > **Note.**
   > It may take up to several minutes to send local changes to the Security Gateway configuration to the Security Management Server. If the configuration is not sent within **1–2** minutes, check the connection between the Security Management Server and the Security Gateway. If the connection between the Security Gateway and the Security Management Server is lost during the application of local changes, the local changes are applied only on the Security Gateway and are not sent to the Security Management Server. In this case, the message **There are unapplied local changes** appears until a restart. To send changes to the Security Management Server after the Security Gateway re-established connection between the Security Gateway and the Security Management Server, click **Confirm changes** in the Security Gateway local menu.

4. Click **OK**.

To link a license to the Security Gateway in the Configuration Manager:

1. Go to **Administration** and select **Licenses**.
2. Select the Security Gateway in the list and click **Link license** on the toolbar.

   The dialog box with all available licenses under the following conditions appears:

   - The license has not expired.
   - The platform type of the license (if specified) matches the platform type of the linked Security Gateway.
   - The Security Gateway ID in the license (if specified) matches the ID of the linked Security Gateway.

3. Select the required license and click **OK**.

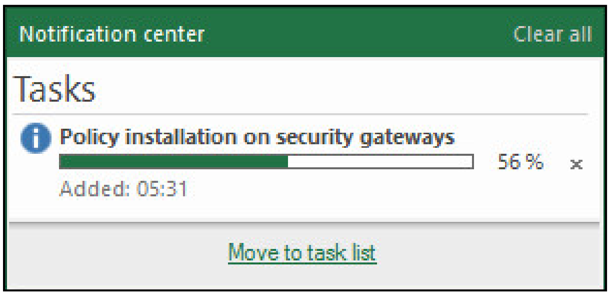
   The license is linked to the Security Gateway and moved from the repository to the linked license group

4. To save settings to the configuration, click the main menu button and then click **Save**.
5. On the toolbar, click **Install**.

   The dialog box for applying policies to the gateways appears.

6. In the **Install policy** dialog box, select the required Security Gateway and click **OK**.

   The task to install the policy on the selected Security Gateway is created and the notification center appears. It displays the progress of tasks.



Policy installation on security gateways
56 %
Added: 05:31

Case 2

To connect a Security Gateway to the Security Management Server, take the following steps:

1. Create a CSR using the local menu (see below).
2. Issue a certificate using the Security Management Server local menu (see p. **29**).
3. Create a Security Gateway using the Security Management Server local menu (see p. **30**).
4. Configure and connect the Security Gateway to the Security Management Server using the local menu (see p. **30**).
5. Confirm the Security Gateway configuration in the Configuration Manager (see p. **30**).
6. Link a license to a Security Gateway in the Configuration Manager (see p. **31**).

To create a request to issue a Security Gateway certificate:

1. In the local menu of the Security Gateway, select **Certificates** and press <**Enter**>.

   The **Certificates** menu appears.
2. Select **Certificate requests** and press <**Enter**>.

   The respective window appears.

   Note.
   If you create the first certificate, the list is empty.
3. Press <**F4**>.

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

   The **Certificate** dialog box appears.
5. Specify the required information in the respective fields and press <**Enter**>.

   The CSR will be successfully saved to the USB drive. You receive the respective message.
6. Press <**Enter**>.

   You will be returned to the **Issue certificate request** dialog box.
7. Press <**Esc**>.

   You will be returned to the **Control channel certificates** window. You can see the created CSR in the list.

To issue a certificate using the Security Management Server local menu:

1. Select **Certificates** and press <**Enter**>.

   The **Certificates** dialog box appears.
2. Select **Control channel certificates** and press <**Enter**>.

   The respective window appears.
3. Press <**F2**>.

   The **Issue certificate** dialog box appears.
4. Select **Issue control certificate for Security Gateway** and press <**Enter**>.

   The dialog box prompting for a CSR appears.
5. Select **Yes** and press <**Enter**>.

   The dialog box with the list of files detected on the USB drive appears.

   Note.
   By default, the CSR file name is **continent-XX.req** where **XX** is the Security Gateway ID.
6. Select the required file and press <**Enter**>.

   The dialog box prompting you to select a root certificate appears.
7. Select the required root certificate and press <**Enter**>.

   The control certificate file is successfully created. You will receive the respective message.
8. Press <**Enter**>.

   You will be returned to the **Issue certificate** menu.
9. Select **Back to previous menu** and press <**Enter**>.

   You will be returned to the **Control channel certificates** menu. The new certificate is displayed in the list.

To create a Security Gateway using the Security Management Server local menu:

1. Select **Tools** and press <**Enter**>.

   The **Tools** menu appears.

2. Select **Create** Security Gateway and press <**Enter**>.

   The dialog box prompting you to insert a USB drive appears.

3. Insert a USB drive and press <**Enter**>.

   The dialog box prompting for a Security Gateway ID appears.

   Note.
   The Security Gateway ID is an identifier shown on the Security Gateway hardware appliance case, in its datasheet, and in the local menu.

4. Enter the Security Gateway ID and press <**Enter**>.

   The dialog box prompting for a Security Gateway control certificate appears.

5. Select the certificate for the Security Gateway and press <**Enter**>.

   The process of Security Gateway creation starts. When the operation is completed, the respective message appears. The configuration file of the Security Gateway will be exported to the USB drive.

6. Press <**Enter**>.

   You will be returned to the **Tools** menu.

   Note.
   The configuration file name is **gate-XX.json**, where **XX** is the Security Gateway ID.

7. Remove the USB drive.

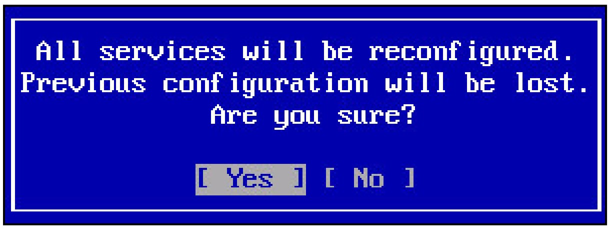
To configure and connect Security Gateway to the Security Management Server:

Note.
Prepare a USB drive with the configuration file **gate-XX.json** (**XX** is the Security Gateway ID).

1. Insert the prepared USB drive.

2. In the main menu of the Security Gateway, select **Connect to Security Management Server** and press <**Enter**>.

   The warning message appears as in the figure below.



All services will be reconfigured.
Previous configuration will be lost.
Are you sure?

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

   The list of files from the USD drive appears.

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

   The window for selecting the Security Gateway management interface appears.

5. Select an interface that will be used for connection to the Security Management Server and press <**Enter**>.

   The window for configuring the Security Gateway management interface appears.

6. Type its IP address and mask, the IP address of the gateway (if necessary) and press <**Enter**>.

   The window prompting you to confirm the new settings appears.

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

   When the operation is completed, you receive the respective message.

8. Press <**Enter**>.

To confirm the Security Gateway configuration:

Note.
If you receive a message about the lock takeover in the Configuration Manager, reconnect the Security Management Server.

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

The list of Security Gateways appears in the display area.

> **Note.**
> If you cannot see the local version of the Security Gateway configuration in the list, click **Refresh** on the toolbar.

2. Select the Security Gateway and click **Confirm changes** on the toolbar.

   The dialog box prompting you to confirm local changes appears.
3. Click **Yes**.

   When the system applies all changes to the Security Management Server configuration and saves it to the database, you receive the respective message.

> **Note.**
> It may take up to several minutes to send local changes to the Security Gateway configuration to the Security Management Server. If the configuration is not sent within **1–2** minutes, check the connection between the Security Management Server and the Security Gateway. If the connection between the Security Gateway and the Security Management Server is lost during the application of local changes, the local changes are applied only on the Security Gateway and are not sent to the Security Management Server. In this case, the message **There are unapplied local changes** appears until a restart. To send changes to the Security Management Server after the Security Gateway re-established connection between the Security Gateway and the Security Management Server, click **Confirm changes** in the Security Gateway local menu.

4. Click **OK**.

To link a license to a Security Gateway in the Configuration Manager:

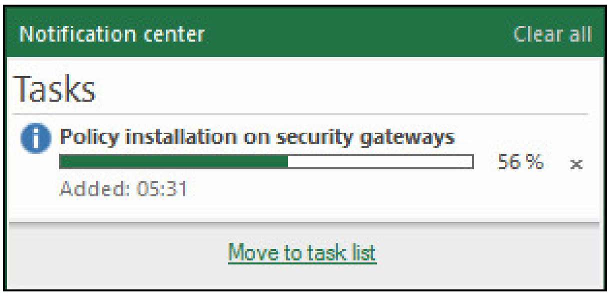
1. Go to **Administration** and select **Licenses**.
2. Select the Security Gateway in the list and click **Link license** on the toolbar.

   The dialog box with all available licenses under the following conditions appears:
   - The license has not expired;
   - The platform type of the license (if specified) matches the platform type of the linked Security Gateway;
   - The Security Gateway ID in the license (if specified) matches the ID of the linked Security Gateway.
3. Select the required license and click **OK**.

   The license will be linked to a Security Gateway and removed from the repository to the linked license group.
4. To save settings to the configuration, click the main menu button and then click **Save**.
5. On the toolbar, click **Install**.

   The dialog box for applying policies to the gateways appears.
6. In the **Install policy** dialog box, select the required Security Gateway and click **OK**.

   The task to install the policy on the selected Security Gateway is created and the notification center appears. It displays the progress of tasks.


Notification center
Clear all
Tasks
Policy installation on security gateways
56 %
Added: 05:31
Move to task list

Case 3

To connect a Security Gateway to the Security Management Server, take the following steps:

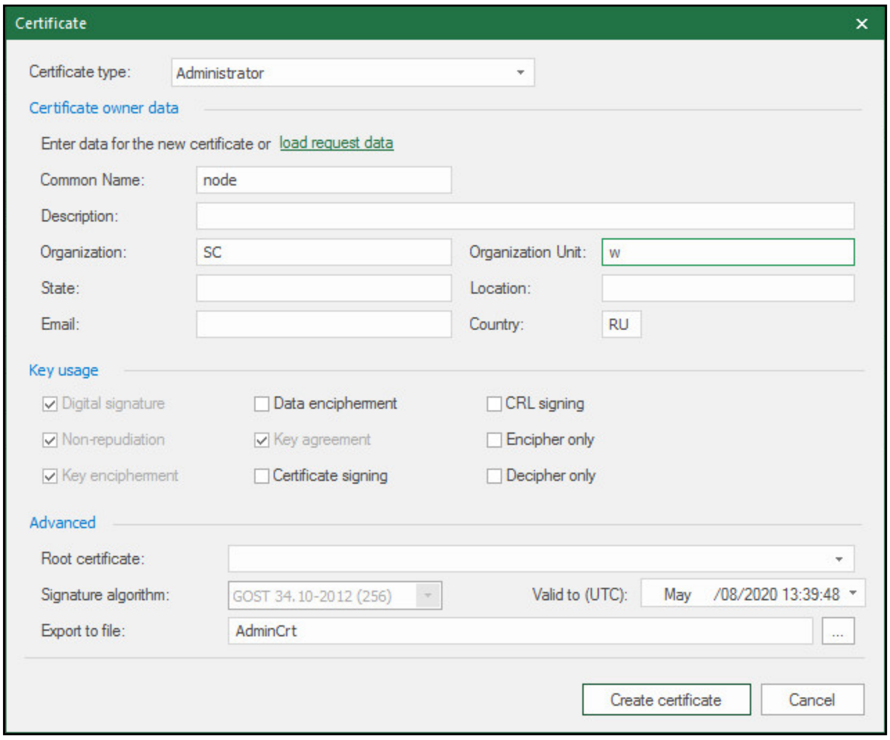
1. Issue a Security Gateway certificate in the Configuration Manager (see below).
2. Create a Security Gateway in the Configuration Manager (see p. **32**).
3. Export Security Gateway configuration in the Configuration Manager (see p. **34**).
4. Configure and connect Security Gateway to the Security Management Server using the local menu (see p. **34**).
5. Confirm Security Gateway configuration in the Configuration Manager (see p. **35**).
6. Link a license to a Security Gateway in the Configuration Manager (see p. **36**).

To issue a Security Gateway certificate in the Configuration Manager:

1. Go to the **Administration** section.
2. In the list of certificates, click **Personal certificates**.

   The list of installed personal certificates appears in the display area.
3. On the toolbar, click **Certificate**.

   The **Certificate** dialog box appears.



Certificate

Certificate type: Administrator

Certificate owner data

Enter data for the new certificate or load request data

Common Name: node

Description:

Organization: SC

Organization Unit: w

State:

Location:

Email:

Country: RU

Key usage

☑ Digital signature

☑ Non-repudiation

☑ Key encipherment

□ Data encipherment

☑ Key agreement

□ Certificate signing

□ CRL signing

□ Encipher only

□ Decipher only

Advanced

Root certificate:

Signature algorithm: GOST 34.10-2012 (256)

Valid to (UTC): May /08/2020 13:39:48

Export to file: AdminCrt

4. In the **Certificate type** drop-down list, select **Security gateway**. Specify all required parameters in the **Certificate owner data** and **Key usage** sections.
5. In the **Advanced** section, in the **Root certificate** drop-down list, select one that was created during the Security Management Server configuration. Specify an expiration date.
6. Click ..., select the destination folder of the USB drive, specify the name for the files and click **Save**.
7. Click **Create certificate**.

   The dialog box prompting you to enter a password for the container appears.
8. Enter the password and confirm it, click **OK**.

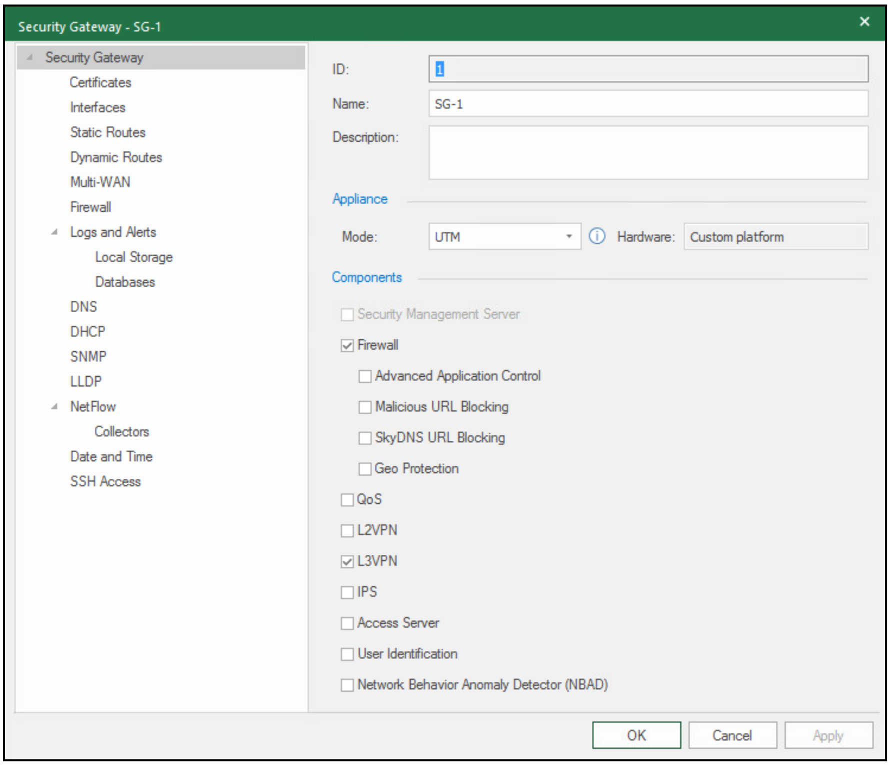
   The Security Gateway certificate file (***.cer**), the certificate request (***.req**) and the key container (in the **topsecretkey** folder) are created and exported to the USB drive. Then, the certificate data is displayed in the list.

To create a Security Gateway in the Configuration Manager:

Attention!
Before creating the Security Gateway, make sure that the Security Management Server is able to connect the Security Gateway.

1. In the Configuration Manager, go to the **Structure** section.
2. On the toolbar, click **Security gateway**.

   The **Security Gateway** dialog box appears.



ID: 1

Name: SG-1

Description:

Appliance

Mode: UTM Hardware: Custom platform

Components

□ Security Management Server
☑ Firewall
□ Advanced Application Control
□ Malicious URL Blocking
□ SkyDNS URL Blocking
□ Geo Protection
□ QoS
□ L2VPN
☑ L3VPN
□ IPS
□ Access Server
□ User Identification
□ Network Behavior Anomaly Detector (NBAD)

3. In the **ID** text box, type the Security Gateway ID; in the **Name** and **Description** text boxes, type the respective information.

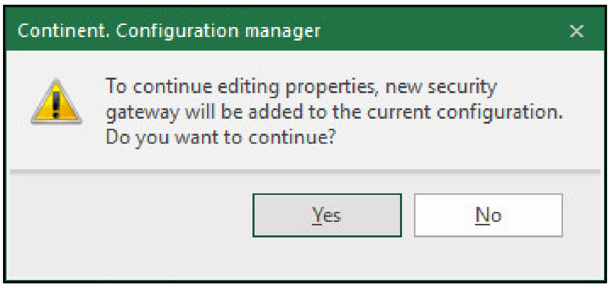
Attention!
- For the **Name** text box, you can use only English letters, digits and symbols, such as "**-**" and "**.**". The name length cannot be more than **32** characters.
- The Security Gateway ID is an identifier shown on the Security Gateway hardware appliance case, in its datasheet, and in the local menu.

4. In the **Hardware** section, select the platform from the drop-down list.

   When deploying a Security Gateway on the virtual machine, select **Custom platform** ang go to step **11**.

5. In the **Security gateway** section, select **Interfaces**.

   The dialog box prompting you to continue appears.



To continue editing properties, new security gateway will be added to the current configuration. Do you want to continue?

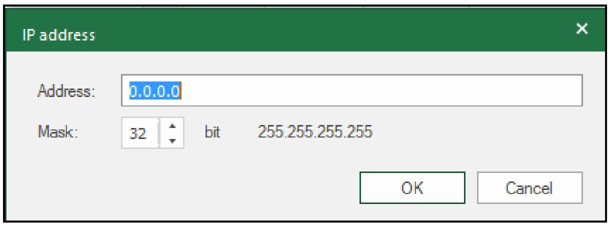
6. Select **Yes**.

   The list of interfaces appears.

7. Select an interfaces for managing Security Management Server. The interface numbers are mentioned in the device passport.

8. In the **Address/Mask** column, click ⊞.

   The **IP address** dialog box appears.



Address: 0.0.0.0

Mask: 32 bit 255.255.255.255

9. Specify an IP address, a mask prefix and click **OK**.
10. If necessary, specify a default route. To do so, select **Static routes** on the left of the **Security Gateway** section and click ✳.

    In the respective dialog box, specify a destination IP address and the next node in the route, then click **OK**.
11. In the **Security gateway** section, select **Date and Time**.

    The dialog box prompting you to confirm changes appears.
12. Specify the time zone.

    > **Attention!**
    > The time zone must be the same for all the Security Gateways (including Security Management Servers). It is required for correct logging and audit.
13. In the **Security gateway** section, select **Certificates**.

    A list of certificates appears.
14. In the **Server certificates** field, click ⊕ to load a new certificate.

    The **Certificate** dialog box appears.
15. Select the control channel certificate that was created during the previous procedure.

    The Security Gateway certificate is displayed on the list.
16. In the **Root certificates** field, click ⊕ to add a new certificate.

    The **Certificate** dialog box appears.
17. Select the root certificate from the list (see [**1**]) and click **OK**.

    > **Note.**
    > To update the software, use the pre-installed **Trusted Publisher** certificate. It cannot be used for other purposes.

    The created Security Gateway certificate appears on the list.
18. Click **OK**.

    The created Security Gateway appears on the list.
19. Save the changes by selecting **Save** from the drop-down menu in the upper left corner.

To export the Security Gateway configuration file in the Configuration Manager:

1. Insert the USB drive to save the configuration file onto it.
2. Go to **Structure**, select the Security Gateway in the list and click **Export** on the toolbar.

    The configuration is saved automatically and the File Explorer appears.
3. Specify the path to the USB drive root folder and click **Save**.

    > **Note.**
    > By default, the configuration file name is **gate-XX.json** (**XX** is the Security Gateway ID).

    When the Security Gateway configuration file is created, the respective message appears.
4. Click **OK**.

To configure the Security Gateway and connect it to the Security Management Server:

> **Note.**
> Prepare a USB drive with the configuration file **gate-XX.json** (**XX** is the Security Gateway ID).

1. Insert the USB drive.
2. In the main menu of the Security Gateway, select **Certificates | Control channel certificates** and press <**Enter**>.

The **Control channel certificates** window appears.

3. Press <**F5**>.

   The window for selecting the request file appears.

4. Select the required file with the **.req** extension and press <**Enter**>.

   The window for selecting the private key container appears.

5. Select the required private key container and press <**Enter**>.

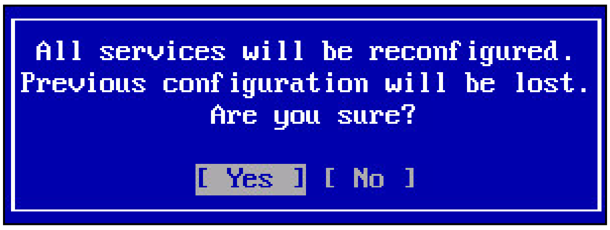
   The password entry window appears.

6. Enter the password and press<**Enter**>.

   The certificate request file and key information will be imported. When the operation is completed, you receive the respective message.

7. In the main menu of the Security Gateway, select **Connect to Security Management Server** and press <**Enter**>.

   The warning message appears as in the figure below.



All services will be reconfigured.
Previous configuration will be lost.
Are you sure?

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

   The list of files from the USB drive appears.

9. The following actions depend on the type of a platform:

   For platforms of the **Unknown type**, perform the following steps:

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

     The window for selecting the Security Gateway management interface appears.
   - Select an interface that will be used for connection to the Security Management Server and press <**Enter**>.

     The window for configuring the Security Gateway management interface appears.
   - Type its IP address and mask, the IP address of the gateway (if necessary) and press <**Enter**>.

     The window prompting you to confirm the new settings appears.
   - Select **Yes** and press <**Enter**>.

     The Security Gateway configuration will start. When the operation is completed, you receive the respective message.

   For platforms of the type different from **Unknown type**, take the following step:

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

     The Security Gateway configuration will start. When the operation is completed, you receive the respective message.

10. Press <**Enter**>.

To confirm the Security Gateway configuration:

Note.
If you receive a message about the lock takeover in the Configuration Manager, reconnect the Security Management Server.

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

   The list of Security Gateways appears in the display area.

   Note.
   If you cannot see the local version of the Security Gateway configuration in the list, click **Refresh** on the toolbar.

2. Select the Security Gateway and click **Confirm changes** on the toolbar.

   The dialog box prompting you to confirm local changes appears.

3. Click **Yes**.

When the system applies all changes to the Security Management Server configuration and saves it to the database, you receive the respective message.

Note.
It may take up to several minutes to send local changes to the Security Gateway configuration to the Security Management Server. If the configuration is not sent within **1–2** minutes, check the connection between the Security Management Server and the Security Gateway. If the connection between the Security Gateway and the Security Management Server is lost during the application of local changes, the local changes are applied only on the Security Gateway and are not sent to the Security Management Server. In this case, the message **There are unapplied local changes** appears until a restart. To send changes to the Security Management Server after the Security Gateway re-established connection between the Security Gateway and the Security Management Server, click **Confirm changes** in the Security Gateway local menu.

4. Click **OK**.

To link a Security Gateway license in the Configuration Manager:

1. Go to **Administration** and select **Licenses**.
2. Select the Security Gateway in the list and click **Link license** on the toolbar.

   The dialog box with all available licenses under the following conditions appears:

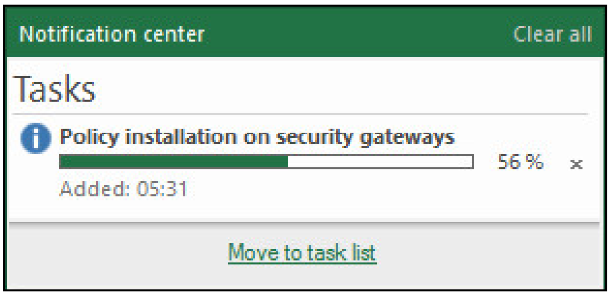
   - The license has not expired.
   - The platform type of the license (if specified) matches the platform type of the linked Security Gateway.
   - The Security Gateway ID in the license (if specified) matches the ID of the linked Security Gateway.

   For adding licenses to the repository, see [**1**], the **License management** section.
3. Select the required license and click **OK**.

   The license will be linked to a Security Gateway and removed from the repository to the linked license group.
4. To save the settings to the configuration, click the main menu button and then click **Save**.
5. On the toolbar, click **Install**.

   The dialog box for applying policies to Security Gateways appears.
6. In the **Install policy** dialog box, select the required Security Gateway and click **OK**.

   The task to install the policy on the selected Security Gateway is created and the notification center appears. It displays the progress of tasks.



Case 4

To connect the Security Gateway to the Security Management Server, take the following steps:

1. Create a Security Gateway CSR using the local menu (see below).
2. Issue a certificate in the Configuration Manager (see p. **37**).
3. Create a Security Gateway in the Configuration Manager (see p. **38**).
4. Export the Security Gateway configuration in the Configuration Manager (see p. **36**).
5. Configure the Security Gateway and connect it to the Security Management Server using the local menu of the Security Gateway (see p. **39**).
6. Confirm the Security Gateway configuration in the Configuration Manager (see p. **40**).
7. Link a license to the Security Gateway in the Configuration Manager (see p. **40**).

To create a Security Gateway CSR:

1. In the Security Gateway local menu, select **Certificates** and press <**Enter**>.

   The respective dialog box appears.
2. Select **Certificate requests** and press <**Enter**>.

   The respective window appears.

> **Note.**
> If you create the first certificate, the list is empty.

3. Press <**F4**>.

The dialog box prompting you to insert a USB drive appears.

4. Insert a USB drive and press <**Enter**>.

The **Certificate** dialog box appears.

5. Specify the required information in the respective fields and press <**Enter**>.

The CSR will be successfully saved to the USB drive. You receive the respective message.

6. Press <**Enter**>.

You will be returned to the **Issue certificate request** dialog box.

7. Press <**Esc**>.

You will be returned to the **Control channel certificates** window. You can see the created CSR in the list.

To issue a certificate in the Configuration Manager:

1. Go to the **Administration** section.

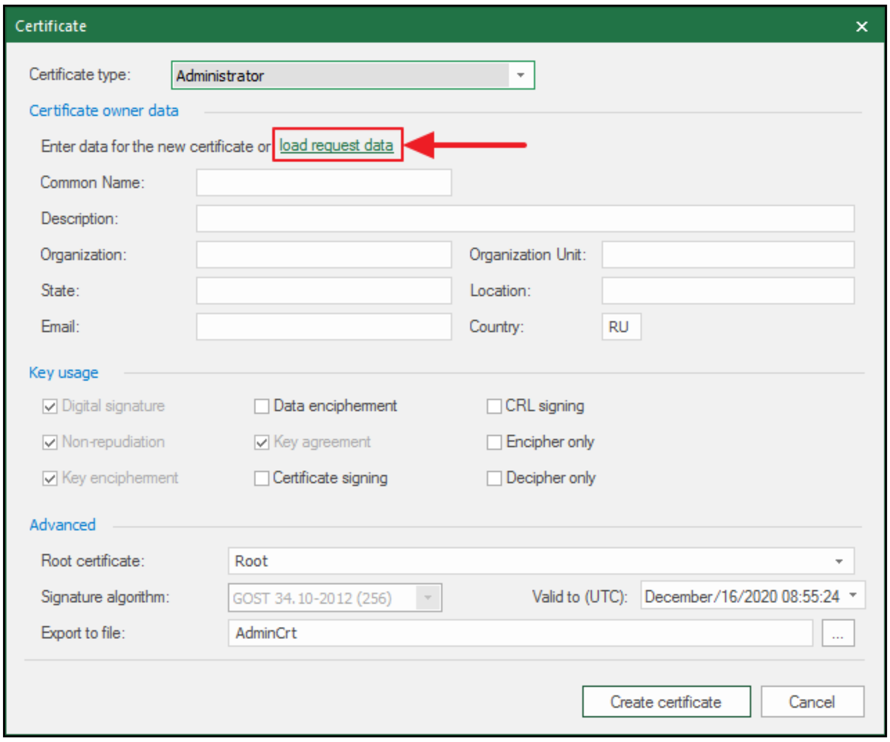
2. In the list of certificates, click **Personal certificates**.

The list of installed personal certificates appears in the display area.

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

The respective dialog box appears.

4. Load request data from the CSR file by clicking the respective link.



Certificate type: Administrator

Country: RU

☑ Digital signature
☑ Non-repudiation
☑ Key encipherment
☐ Data encipherment
☑ Key agreement
☐ Certificate signing
☐ CRL signing
☐ Encipher only
☐ Decipher only

Root certificate: Root

Signature algorithm: GOST 34.10-2012 (256)

Valid to (UTC): December/16/2020 08:55:24

Export to file: AdminCrt

The File Explorer appears.

5. Insert the USB drive, select the required CSR file with ***.req** extension that is stored in the root folder of the USB drive and click **Open**.

The required information will be specified in the respective fields automatically from the CSR file.

6. In the **Advanced** section, in the **Root certificate** drop-down list, select one that was created during the Security Management Server configuration and specify the expiration date.

7. Click **Create certificate**.

The certificate appears in the list.

To create a Security Gateway in the Configuration Manager:

Attention!
Before creating a Security Gateway, make sure that the Security Management Server can connect the Security Gateway.

1. Go to the **Structure** section.
2. On the toolbar, click **Security gateway**.

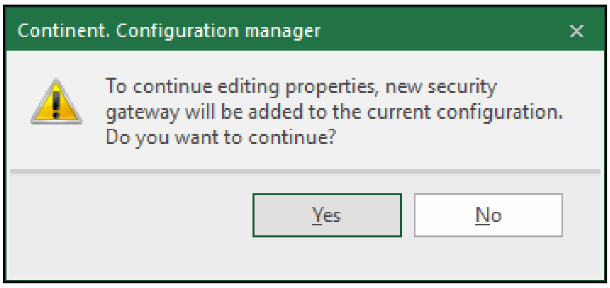
   The dialog box appears as in the figure below.
3. In the **ID** text box, type the Security Gateway ID; in the **Name** and **Description** text boxes, type the respective information.

Attention!
- For the **Name** text box, you can use only English letters, digits and symbols, such as "-" and ".". The length cannot be more than 32 characters.
- The Security Gateway ID is an identifier shown on the Security Gateway hardware appliance case, in its datasheet, and in the local menu.

4. In the **Hardware** section, select the platform from the drop-down list.

   When deploying a Security Gateway on the virtual machine, select **Custom platform** and go to step **11**.
5. In the **Security Gateway** section, select **Interfaces**.

   The dialog box prompting you to confirm changes appears.

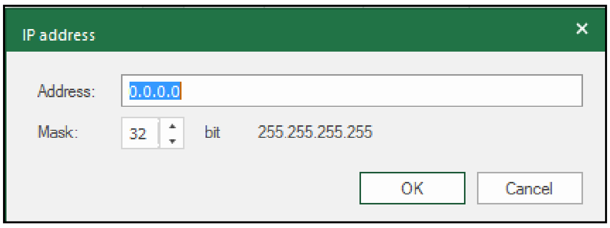

Continent. Configuration manager

To continue editing properties, new security gateway will be added to the current configuration. Do you want to continue?

6. Select **Yes**.

   The list of interfaces appears.
7. Select an interface for managing Security Management Server. The interface numbers are mentioned in the device passport.
8. In the **Address/Mask** column, click ⊞.

   The **IP address** dialog box appears.


IP address

Address: 0.0.0.0

Mask: 32 bit 255.255.255.255

9. Specify an IP address, a mask prefix and click **OK**.
10. If necessary, specify a default route. To do so, select **Static routes** on the left of the **Security Gateway** section and click ✱.

    In the respective dialog box, specify a destination IP address and the next node in the route, then click **OK**.
11. In the **Security Gateway** section, select **Date and Time**.

    You can see settings for the Security Gateway time on the right.
12. Specify the time zone.

    Attention!
    The time zone must be the same for all the Security Gateways (including Security Management Servers). It is required for correct logging and audit.
13. In the **Security Gateway** section, select **Certificates**.

    A list of certificates appears.
14. In the **Server certificates** field, click ⊕ to load a new certificate.

The **Certificate** dialog box appears.

15. Select the control channel certificate that was created during the previous procedure.

    The Security Gateway certificate is displayed on the list.

16. In the **Root certificates** field, click ⊕ to add a new certificate.

    The **Certificate** dialog box appears.

17. Select the root certificate from the list (see p. 10) and click **OK**.

    > **Note.**
    > To update the software, use the pre-installed **Trusted Publisher** certificate. It cannot be used for other purposes.

    The created Security Gateway certificate appears on the list.

18. Click **OK**.

    The created Security Gateway appears on the list.

19. Save the changes by clicking 🖫.

To export the Security Gateway configuration file in the Configuration Manager:

1. Insert the USB drive to save the configuration file onto it.
2. Go to **Structure**, select the Security Gateway in the list and click **Export** on the toolbar.

   The configuration is saved automatically and the File Explorer appears.

3. Specify the path to the USB drive root folder and click **Save**.

   > **Note.**
   > By default, the configuration file name is **gate-XX.json** (**XX** is the Security Gateway ID).

   When the Security Gateway configuration file is created, the respective message appears.

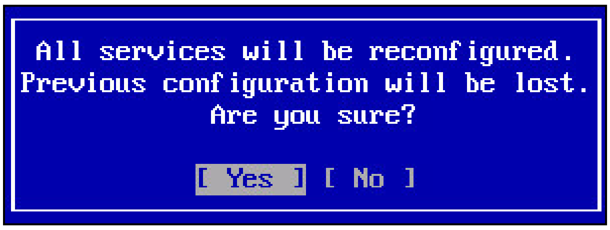
4. Click **OK**.

To configure the Security Gateway and connect it to the Security Management Server:

> **Note.**
> Prepare a USB drive with the configuration file **gate-XX.json** (**XX** is the Security Gateway ID).

1. Insert the USB drive.
2. In the main menu of the Security Gateway, select **Connect to Security Management Server** and press <**Enter**>.

   The warning message appears as in the figure below.



```
    All services will be reconfigured.
  Previous configuration will be lost.
             Are you sure?
```

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

   The list of files from the USB drive appears.

4. The following actions depend on the type of a platform.

   For platforms of the **Unknown type**, take the following steps:

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

     The window for selecting the Security Gateway management interface appears.

   - Select an interface that will be used for connection to the Security Management Server and press <**Enter**>.

     The window for configuring the Security Gateway management interface appears.

   - Type its IP address and mask, the IP address of the gateway (if necessary) and press <**Enter**>.

     The window prompting you to confirm the new settings appears.

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

The Security Gateway configuration will start. When the operation is completed, you receive the respective message.

For platforms of the different from the **Unknown type** type, perform the following steps:

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

  The Security Gateway configuration will start. When the operation is completed, you receive the respective message.

5. Press <**Enter**>.

To confirm the Security Gateway configuration:

> **Note.**
> If you receive a message about the lock takeover in the Configuration Manager, reconnect the Security Management Server.

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

   The list of Security Gateways appears in the display area.

   > **Note.**
   > If you cannot see the local version of the Security Gateway configuration in the list, click **Refresh** on the toolbar.

2. Select the Security Gateway and click **Confirm changes** on the toolbar.

   The dialog box prompting you to confirm local changes appears.

3. Click **Yes**.

   When the system applies all changes to the Security Management Server configuration and saves it to the database, you receive the respective message.

4. Click **OK**.

To link a Security Gateway license in the Configuration Manager:

1. Go to **Administration** and select **Licenses**.
2. Select the Security Gateway in the list and click **Link license** on the toolbar.

   The dialog box with all available licenses under the following conditions appears:

   - The license has not expired.
   - The platform type of the license (if specified) matches the platform type of the linked Security Gateway.
   - The Security Gateway ID in the license (if specified) matches the ID of the linked Security Gateway.

3. Select the required license and click **OK**.

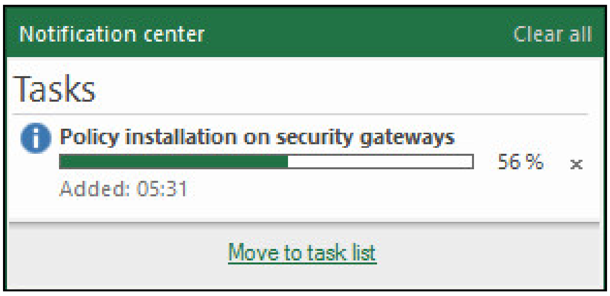
   The license will be linked to a Security Gateway and removed from the repository to the linked license group.

4. To save the settings to the configuration, click the main menu button and then click **Save**.
5. On the toolbar, click **Install**.

   The dialog box for applying policies to the gateways appears.

6. In the **Install policy** dialog box, select the required Security Gateway and click **OK**.

   The task to install the policy on the selected Security Gateway is created and the notification center appears. It displays the progress of tasks.



Policy installation on security gateways

56 %

Added: 05:31

Security Gateway creation wizard

You need to prepare a USB drive to export extended containers with information for the Security Gateway initialization, certificates and configuration files. You can initialize the Security Gateway using the local menu and the extended container without connection to the Security Management Server.

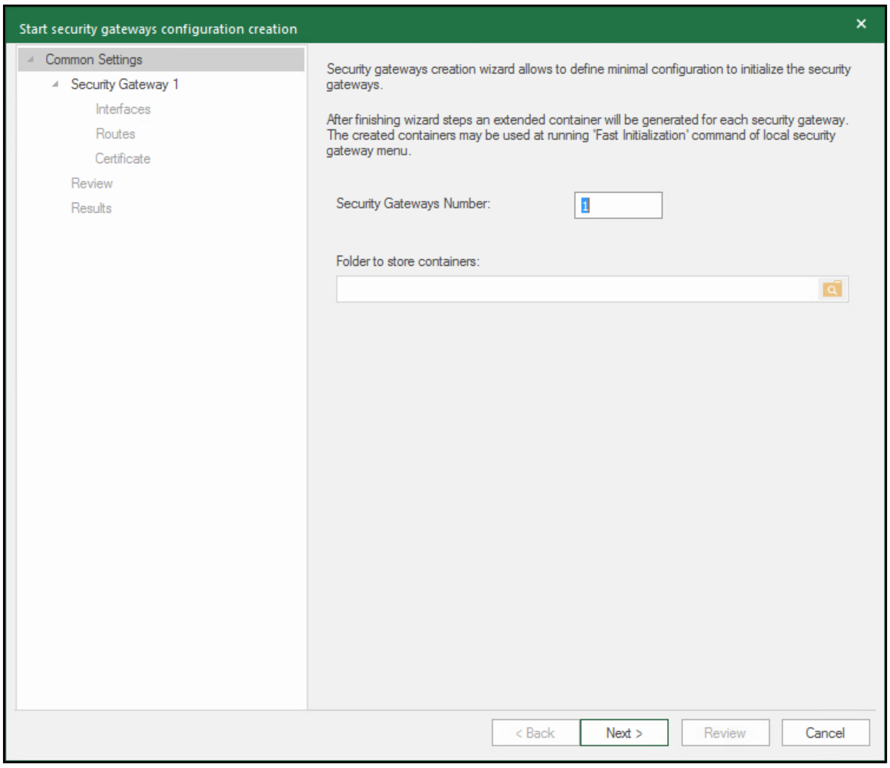
To deploy a group of Security Gateways:

1. Create a group of Security Gateways and generate extended containers using the Configuration Manager (see below).
2. Initialize each Security Gateway using the local menu and the extended container (see p. **42**).

To create a group of Security Gateways and generate containers using the Configuration Manager:

1. In the Configuration Manager, go to **Structure**.
2. Click **Creation wizard** on the toolbar.

   The **Start security gateways configuration creation** dialog box appears.



Security gateways creation wizard allows to define minimal configuration to initialize the security gateways.

After finishing wizard steps an extended container will be generated for each security gateway. The created containers may be used at running 'Fast Initialization' command of local security gateway menu.

Security Gateways Number: 1

Folder to store containers:

3. Specify the required value in the **Security Gateways Number** text box (from **1** to **50**), select the USB flash drive for saving containers and click **Next**.

   The **Security Gateway 1** tab opens.
4. Enter the Security Gateway ID in the ID text box and the Security Gateway name and description in the respective text boxes.

> **Note.**
> The Security Gateway ID is an identifier shown on the Security Gateway hardware appliance case, in its datasheet, and in the local menu. In the **Name** text box you can use only Latin letters, digits and the "**-**" symbol. The length cannot exceed **32** symbols.

5. Select the platform from the **Hardware** drop-down list and click **Next**.

   The **Interfaces** tab opens.
6. Configure the required network interfaces of the Security Gateway (see [**6**]) and click **Next**.

   The **Routes** tab opens.
7. To add a new static route, click ✱.

   In the opened dialog box, specify the destination IP address, next gateway and **Metric** cell (see [**6**]). Click **OK**.
8. After adding all required static routes click **OK**.

   The **Certificate** tab opens.
9. Fill in the **Organization** and **Password** text boxes. Click **Next**.

   A tab with the overview of the next Security Gateway opens.
10. Repeat steps **4**–**8** for every Security Gateway.

    The **Review** tab opens.
11. Check the specified data and click **Export**.

    The **Results** tab opens.

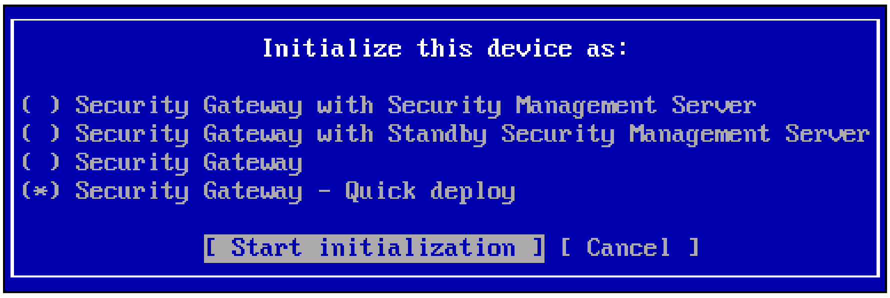
12. Wait for the **Completed** status for all Security Gateways and click **Finish**.

    The created Security Gateways are added to **Structure**, extended containers — to the USB flash drive.

To initialize the Security Gateway using the extended container:

1. In the Security Gateway local menu (see p. 7), select **Initialization** and press <**Enter**>.

   The dialog box where you can select the initialization type appears.



```
              Initialize this device as:

( ) Security Gateway with Security Management Server
( ) Security Gateway with Standby Security Management Server
( ) Security Gateway
(*) Security Gateway - Quick deploy

             [ Start initialization ] [ Cancel ]
```

2. Insert the USB drive with extended containers in the USB port.
3. Select **Security Gateway – Quick deploy** and press <**Enter**>.
4. Select the required extended container file in the opened dialog box.

   The dialog box prompting you to enter the password appears.
5. Enter the password and press <**Enter**>.

   The system time dialog box appears.
6. Specify date and time in UTC+0 format and press <**Enter**>.

   The Security Gateway applies system time and the respective notification appears.
7. Press <**Enter**>.

   The Security Gateway initialization starts. When initialization is completed, you receive the respective message.
8. Press <**Enter**>.

Note.
The policies are applied to the Security Gateway only if a license is added (see [1], **Licenses**).

Appendix

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. If the laptop does not have this connector, you can use a converter (for example, MOXA).

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	115,200
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 to 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>**.

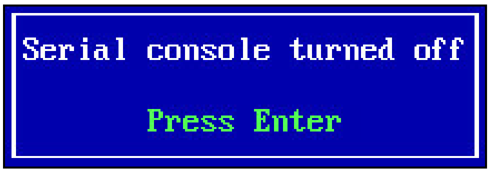
   The **Settings** menu appears.

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.



Serial console turned off

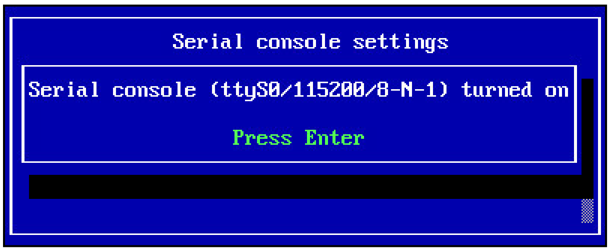
Press Enter

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.



Serial console settings

Serial console (ttyS0/115200/8-N-1) turned on

Press Enter

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>** or **<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.

Change the password to enter BIOS

To change the password:

1. Connect a keyboard and a monitor to the Security Gateway.
2. 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>** or **<F2>**.

   The dialog box prompting a password appears.

3. 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 depend on the platform type of the network device.

4. Go to the change password tab (usually it is **Security**), select **Administrator Password** and press **<Enter>**.

   The dialog box prompting the current password appears.

5. Type the current password and press **<Enter>**.

   The dialog box prompting a new password appears.

6. Type the new password and press **<Enter>**.

   The dialog box prompting the password confirmation appears.

7. Confirm the password and press **<Enter>**.

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

   The Security Gateway restarts.

Network interface syntax

In Continent, a network interface has the following structure:

```
<bandwidth>-<bus>-<interface>
```

- **<bandwidth>** is a prefix showing the maximum bandwidth of the interface. See the following table:

Prefix	Bandwidth
ge	1 Gbit/s
te	10 Gbit/s
qe	40 Gbit/s

- **<bus>** is the device address on the motherboard (0, 1, 2,...);
- **<interface>** is the interface number in the module (0–3) if it contains several interfaces.

```
Examples:
te-0-0
ge-1-1
```

Documentation

1. Continent Enterprise Firewall. Version 4. Administrator guide. Management.
2. Continent Enterprise Firewall. Version 4. Administrator guide. Monitoring and Audit.
3. Continent Enterprise Firewall. Version 4. Administrator guide. Networking functions.
4. Continent Enterprise Firewall. Version 4. Administrator guide. Installation and Update.