SECURITY code

Continent Enterprise Firewall
Version 4

Installation and Update

Administrator guide

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

Table of contents

List of abbreviations

IP	Internet Protocol
NAT	Network Address Translation
RNG	Random Number Generator

Introduction

This manual is designed for administrators of Continent Enterprise Firewall. Version 4 (hereinafter — Continent). It contains information about the installation and update of Continent.

Additional information needed for the administrator can be found in [**1**], [**2**].

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.

Install the Configuration Manager

Only a member of the local administrator group can install or uninstall the Configuration Manager and Security Code CSP.

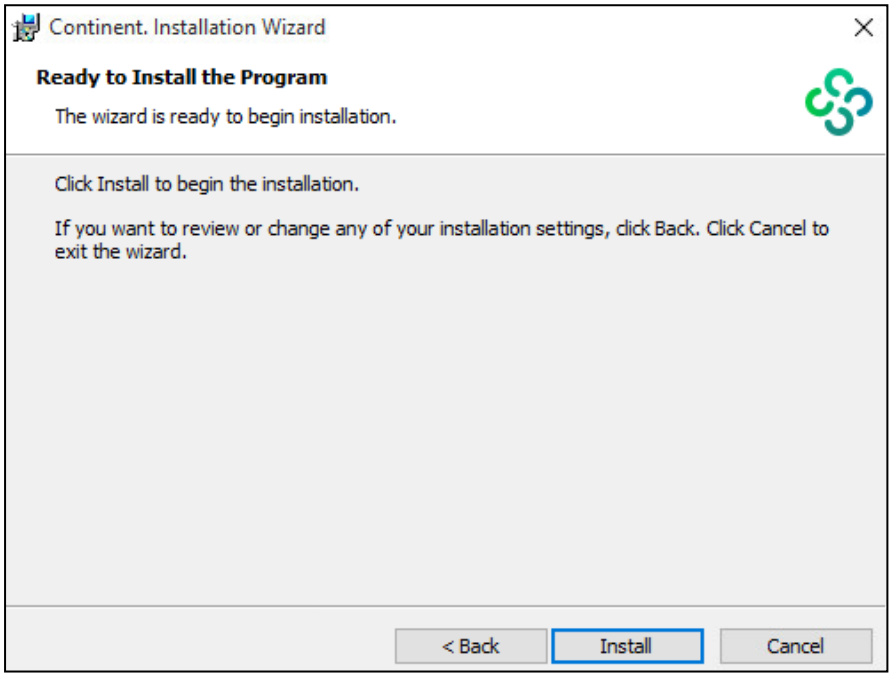
Close all applications before running the installation program.

During the **Configuration Manager** installation, disconnect the computer from the network or block Internet access.

To install the Configuration Manager:

1. Run **\Setup\Continent\MS\Rus\Setup.exe**.

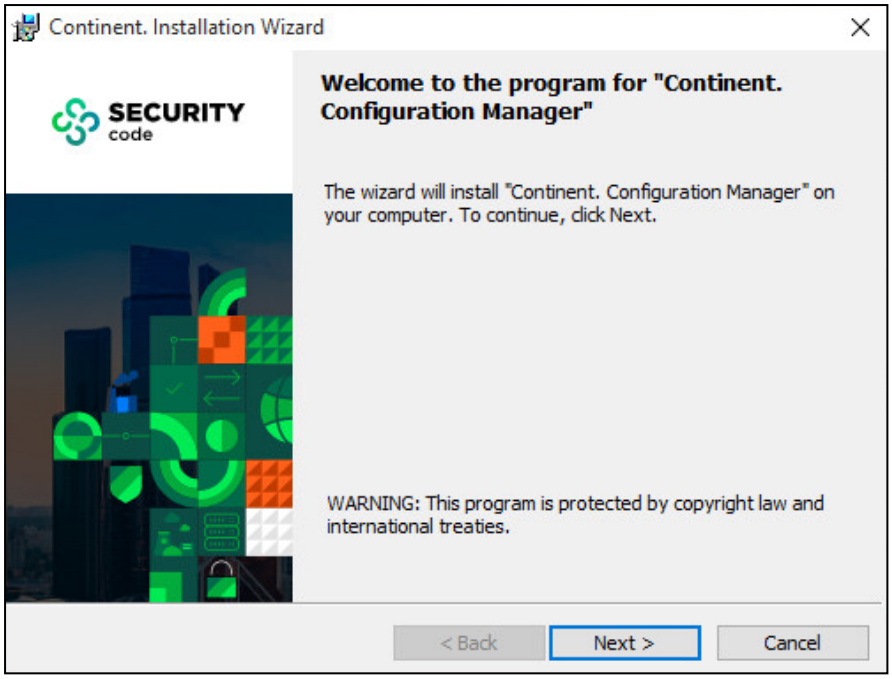
   The Installation Wizard appears. It contains the list of additional components required to be installed before the Configuration Management installation.



Note.
If a third-party cryptographic provider (CryptoPro CSP) is already installed on your computer, the installation program will not offer you to install Security Code CSP. You can choose a cryptographic provider after the Configuration Manager installation (see [**2**]).

2. Click **Install**.

   After the installation of additional components is completed, the Configuration Manager installation wizard appears.



3. Read the information in the start dialog box and click **Next** to continue the installation.

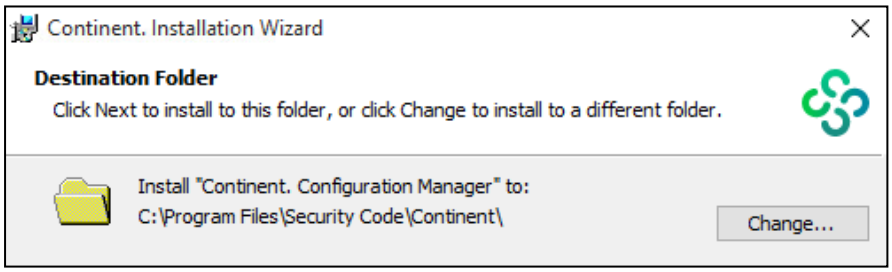
   The dialog box containing a license agreement appears.

4. Read the license agreement till the end. If you agree with the license agreement, select **I accept the terms of the License Agreement** check box and click **Next**.

   The dialog box where you can specify a destination folder for **Continent. Configuration Manger** appears.

5. If necessary, change the destination folder and click **Next**.

   Click **Change** to change the destination folder.



   By default, the installation wizard copies files to the system drive folder **..\Program Files\Security Code\Continent**.

6. Click **Next**.

   The final Installation Wizard dialog box appears.

   Note.
   To change the parameters, click **Back**.

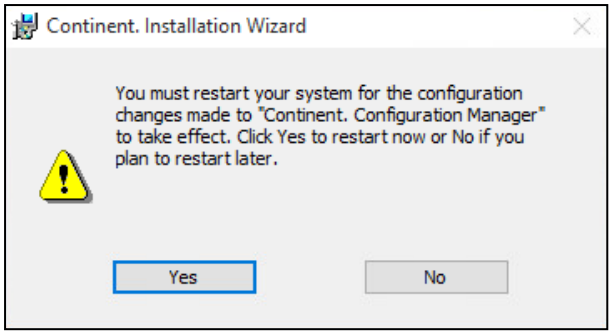
7. To start the program installation, click **Install**.

   The Installation Wizard starts to copy files to the system drive. The respective dialog box displays the progress of the operation.

   Note.
   If the installation program does not find files included in the package during the copying process, you recieve a warning message indicating the name of the missing file. Copy the files from the installation disk again and repeat the installation. If this does not lead to the required result, contact the Continent supplier.

   After the Configuration Manager installation is completed, the respective dialog box appears.

8. To finish the installation, click **Done**. The dialog box prompting you to restart the computer appears.



9. Restart the computer.

After the restart, the Configuration Manager shortcut appears on the desktop. The group **Security Code** appears in the **Start** menu. It contains **Configuration Manager**, **Security Code CSP**, **Restore Security Code CSP** and **Continent**.**Configuration Manager Integrity check**.

Update software and vendor rules

Manage the update repository

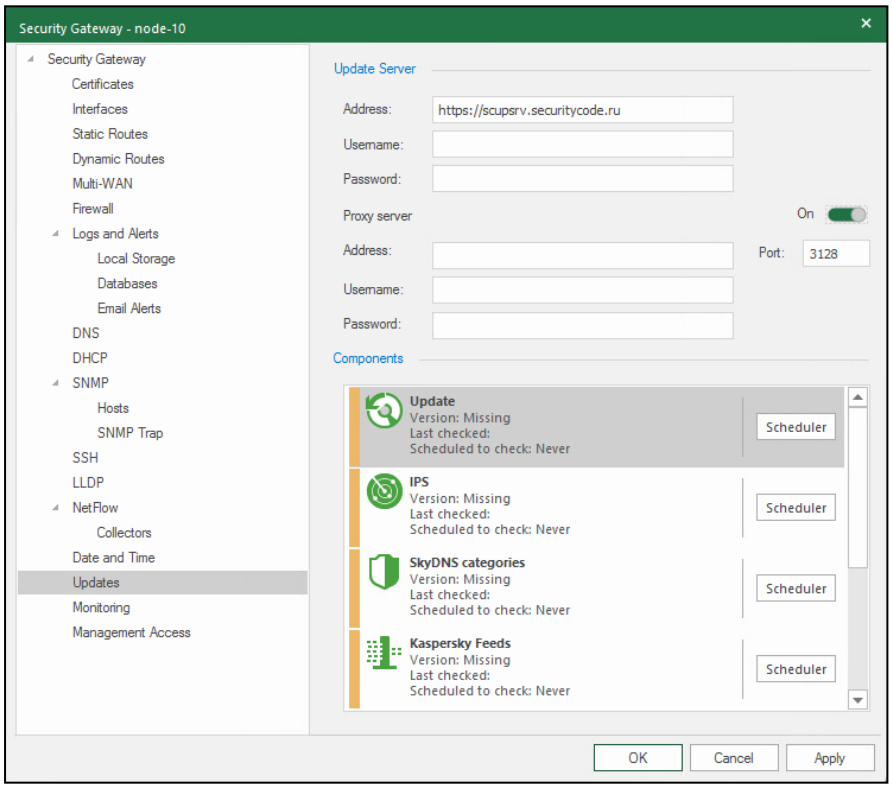
You can download update files to the repository:

- automatically from the update server on schedule;
- from the update server on administrator command;
- by importing from a local source on administrator command.

In the Configuration Manager, you can configure access to the update server only for the Security Management Server.

To configure update server parameters:

1. In the Configuration Manager, go to **Structure**
2. Select the Security Management Server in the Security Gateway list and click **Properties** on the toolbar.
   The respective dialog box appears.
3. On the left, select **Updates**.
   The update parameters appear on the right.



4. To configure the connection to the update server, take the following steps:
   - Enter user credentials.

     Note.
     To get user credentials, contact the support (see p. 5).

   - If you want to use a proxy server, select the respective check box and specify its IP address and connection port.
5. Click **OK**.

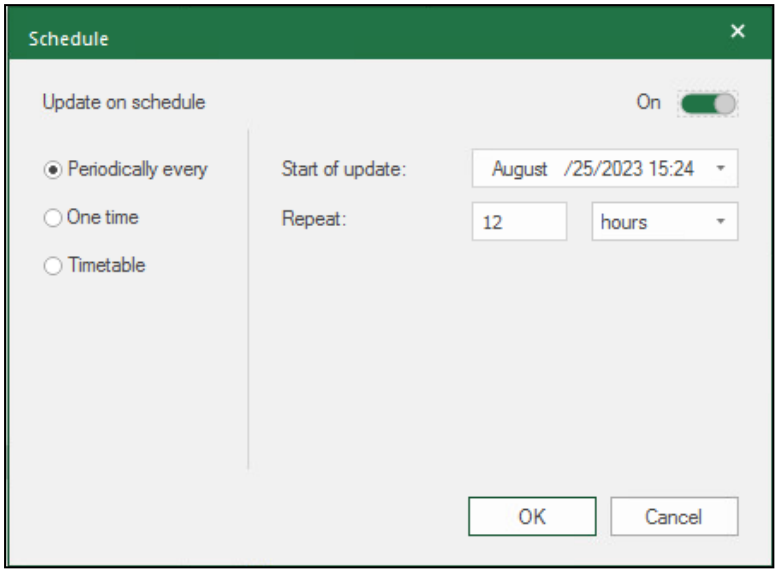
To enable automatic downloading of IPS protection updates and patches to the repository:

1. In the Configuration Manager, go to **Structure**.
2. Select the Security Management Server and click **Properties** on the toolbar.
   The Security Gateway dialog box appears.
3. On the left, go to **Updates**.

Update parameters appear.

4. Click **Scheduler** next to the required component.

   The **Schedule** dialog box appears.



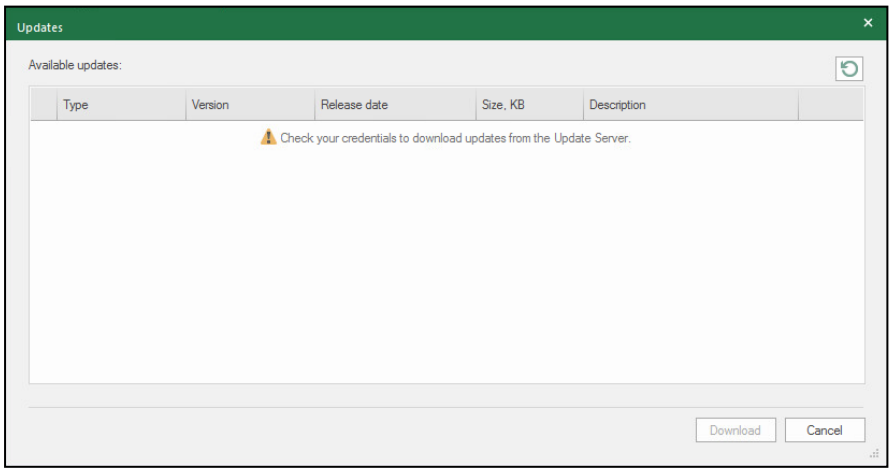
5. Turn on the **Update on schedule** toggle.
6. Select **Periodically every**, **One time** or **Timetable**.
7. For the **Periodically every** option specify **Start of update** and **Repeat** parameters, for **One time** — the **Start of update** parameter, for **Timetable** — the **On these days** parameter.
8. Click **OK**.
9. In the Security Gateway dialog box, click **OK**.
10. To apply the changes, click **Install policy** on the toolbar, select the Security Management Server and click **OK**.

To download updates to the repository manually:

Note.
Specify all the parameters to connect to the update server before the procedure.

1. In the Configuration Manager, go to **Administration** and select **Updates**.
2. Choose the necessary Security Gateway in the list and click **Download** on the toolbar.

   The **Updates** dialog box appears.



3. Click  to load the list of available updates.

   The system sends a request to the update server and, if updates are available, the list of software and vendor rules will be displayed (vendor IPS protections, SkyDNS categories, Threat Intelligence feeds, Kaspersky hash databases, Kaspersky Feeds, Web/FTP filtering exceptions and GEO/IP).

4. Choose the required vendor rules and software version and and click **Download**.

   After you download the file from the server to the repository, a new software version is displayed on the list.

To import a software update file from a local source:

1. In the Configuration Manager, go to **Administration**, select **Updates** and click **Import** on the toolbar.

   The Windows Explorer dialog box appears.
2. Specify an update file with the extension ***.tgz.signed** (if you import update files from the software installation disk, you can find them in the root directory) and click **Open**.

   The dialog box with an update type and date appears.
3. Click **Yes**.

   The Security Management Server starts to upload the update file to its database When the upload is completed successfully, the respective message appears.
4. Click **OK**.

   The update file with its type, version and size appears in the updates repository.

To delete an update file from the repository:

1. In the Configuration Manager, go to **Administration** and select **Updates**. On the display area, select unnecessary update files and click **Remove** on the toolbar.

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

   The update file is deleted from the repository.

Update Continent software

To update the software, take the following steps:

1. Download update files to the repository (see above).
2. Update the Security Management Server software (see p. **11**). For the update procedure of the Security Management Server software with the connected standby Security Management Server, see p. **12**.
3. Update the Configuration Manager (see p. **13**).

   Note.
   If you want to update the Security Management Server software with the connected standby Security Management Server, update the Configuration Manager before updating the standby Security Management Server software.
4. Update all the Security Gateways (see p. **11**). For the update procedure of the security cluster software, see p. **12**.

In case of failure while updating the Security Gateway software, the latest software version is automatically restored. Try to update the software for this Security Gateway again.

Install the latest updates of vendor rules after the Continent software update (see p. **9**).

Note.
To find information about the software versions in the Configuration manager, go to **Administration | Updates**.

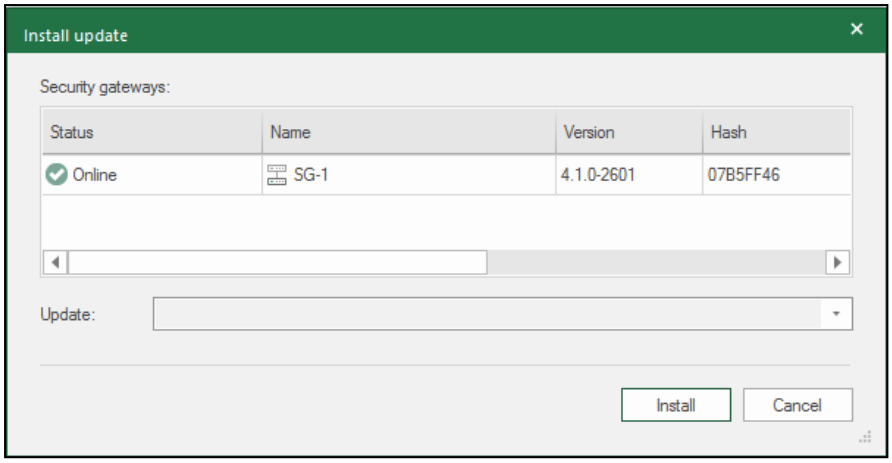
Update the Security Gateway software

Attention!
Before you update/roll back the software, we recommend creating a backup of the Security Gateway settings. If you update the Security Management Server software, create backups of its subordinate Security Gateways (see [**2**]).

To install a software update:

1. Restart the computer with the Configuration Manager.
2. In the Configuration Manager, go to **Administration** and select **Updates**.
3. In the list of Security Gateways, select the required one and click **Install update** on the toolbar.

   The **Install update** dialog box appears.



4. In the **Update** drop-down list, select the required software update and click **Install**.

   In the Notification center, the created task appears.

> **Attention!**
> After you update the software, the Security Gateway automatically restarts. The first Security Gateway startup after the update may take a long time, do not interrupt this process and do not force the Security Gateway to restart. After the Security Management Server restarts, you need to re-establish the connection between the Configuration Manager and the Security Management Server.
> If you update the Security Management Server software, the Configuration Manager is disconnected. Wait for the update to install.

Update the Security Management Server with the connected standby Security Management Server

To update the Security Management Server with the connected standby Security Management Server:

1. Update the Security Management Server software (see p. **11**).

> **Note.**
> You cannot update the active and standby Security Management Servers simultaneously.

   The Security Management Server restarts automatically and becomes standby. The connection between Configuration Manager and Security Management Server will be lost.
2. Wait some time and try to reconnect to the Configuration Manager.
3. Go to **Structure**.
4. In the list of Security Gateways, right-click the updated Security Management Server, select **Replication** and click **Make active**.
5. Click **Yes** to confirm the operation.

   The respective message appears. The connection between the Configuration Manager and Security Management Server will be lost.
6. Wait some time and try to reconnect to the Configuration Manager.
7. Update the standby Security Management Server (see p. **11**).
8. After the software is updated, wait when the standby Security Management Server restarts.
9. Go to **Structure**.
10. Select the standby Security Management Server (use **<Ctrl>** for multiple choice).
11. Right-click the selected Security Gateway, select **Replication** and click **Synchronize**.
12. Click **Yes** to confirm the operation.

    The synchronization starts. The progress bar appears and closes once the procedure is complete.
13. The standby Security Management Server status becomes **Synchronized**.

Update the Security Gateway cluster software

To update the software of a failover security cluster, you need to take the following steps:

1. Update the cluster component software that has the **Standby** status.

2. Make the updated Security Gateway **Active**.
3. Update the cluster component software that has the **Standby** status.
4. Install the policy on the security cluster, then make the required Security Gateway **Active**.

Note.
The Security Gateway with the **Standby** status can change its state to **OK, not ready** right after the update. To finish the update, take the following steps:
- Install the policy on the security cluster. The policy will not be installed on a not updated (**Active**) Security Gateway. After the installation, the updated Security Gateway becomes **Active** automatically, whereas the not updated Security Gateway is assigned **Standby**.
- Update the standby Security Gateway software. After the update, it can be assigned **OK, not ready**.
- Install the policy on the cluster.

Update the Configuration Manager

To update the administrator's computer software:

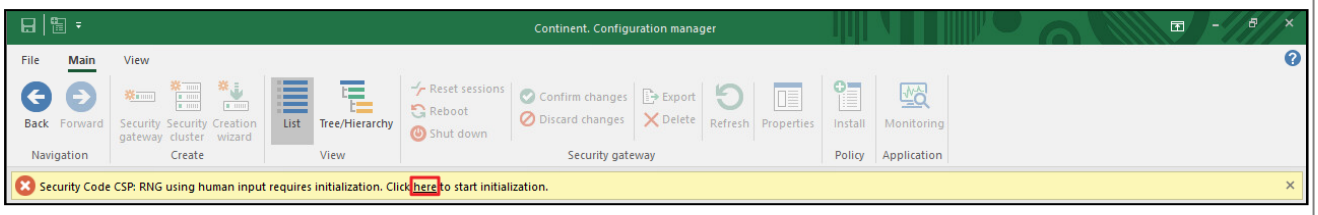
1. In the Windows Start menu, go to **Control Panel** | **Programs and Features**, select **Continent. Configuration Manger** and select **Modify**.
2. In the respective dialog box, click **Next**.
3. In the Installation Wizard, select **Uninstall** and click **Next**.
4. The uninstallation dialog box appears. Click **Delete**.
   Software uninstallation starts.
5. After the uninstallation is completed, click **Finish**.
   The dialog box prompting you to restart the computer appears.
6. Click **Yes**.
   The administrator's computer restarts to complete the uninstallation.
7. In **Control Panel**, go to **Programs and Features**, select **Security Code CSP** and click **Uninstall**.
   The respective dialog box appears.
8. Click **OK**.
   Software uninstallation starts.
   After the uninstallation is completed, the dialog box prompting you to restart the computer appears.
9. Click **Yes**.
   The administrator's computer restarts to complete the uninstallation.
10. Place the Configuration Manager distribution disk in the CD-ROM drive and go to the directory **\Setup\Continent\MS\En**, then select the directory with bitness matching bitness of the administrator workstation OS.

    Note.
    If you obtain the Configuration Manager distribution during the critical software update from the Internet, go to the directory containing the distribution file.

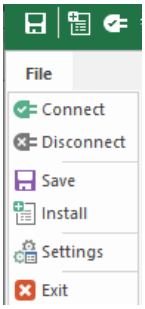
11. Install the Configuration Manager (see p. 6).

Note.

When you start the Configuration Manager for the first time after its update, the dialog box prompting you to initialize the RNG using human input may appear.



To initialize the RNG, click the link shown in the figure above and follow the instructions. Wait for the entropy collection process to complete, then click the **File** button in the upper-left corner of the MC and select **Connect** from the drop-down list.



Update vendor rules

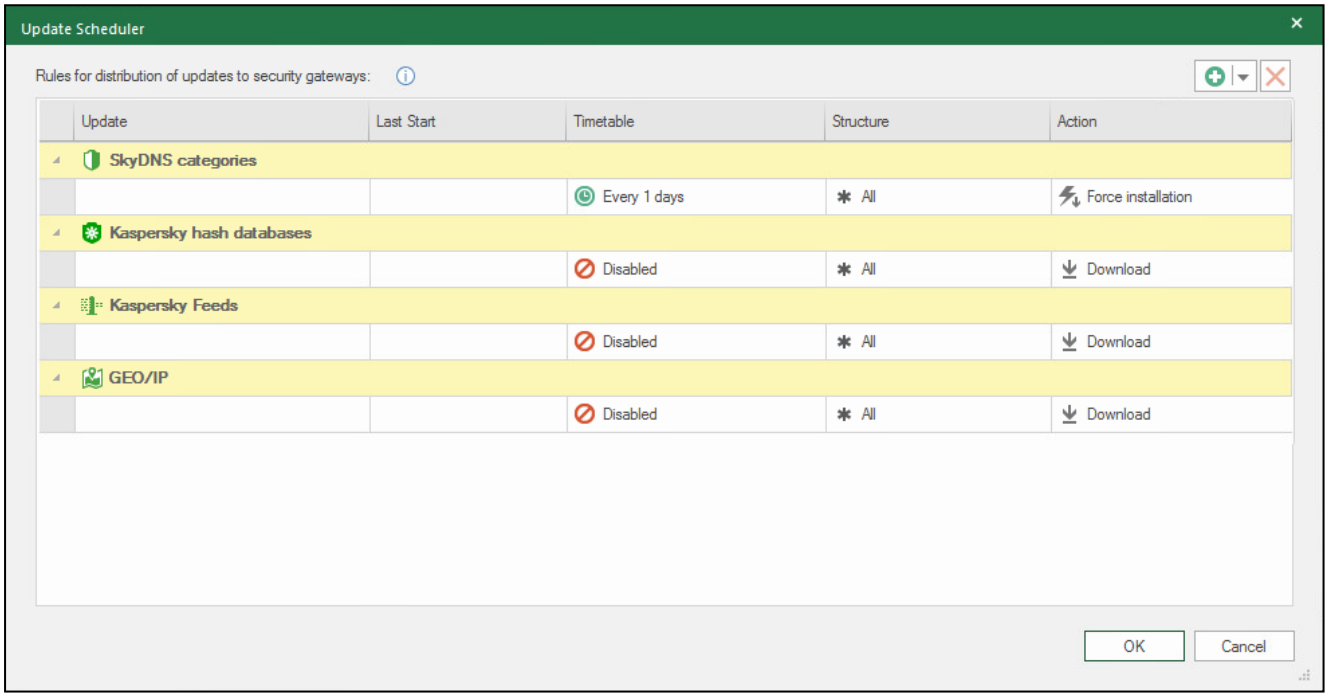
The distribution of vendor rule updates (IPS protections, SkyDNS categories, Threat Intelligence feeds, Kaspersky hash databases, Kaspersky Feeds, Web/FTP filtering exceptions and GEO/IP) is performed in two different ways:

- through the policy installation for IPS protections and Web/FTP filtering exceptions;
- through **Update Scheduler** for Sky/DNS categories, Threat Intelligence feeds, Kaspersky hash databases user hashes and GEO/IP.

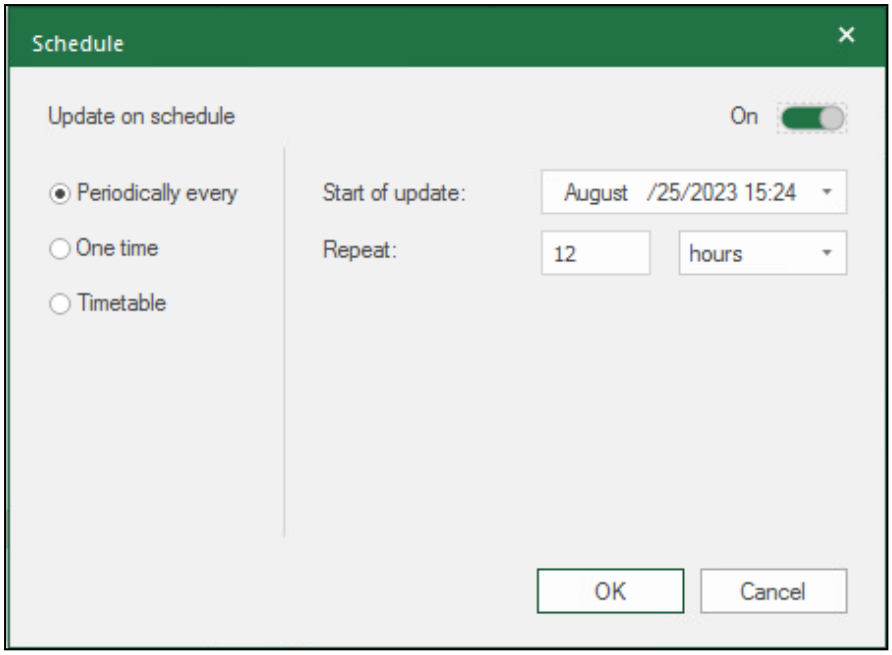
Note.
Information about vendor rule versions on Continent components is displayed in **Administration | Updates** section.

To configure the Update Scheduler:

1. In the Configuration Manager, go to **Administration | Updates** and click **Update Scheduler** on the toolbar.
   The **Update Scheduler** dialog box appears.

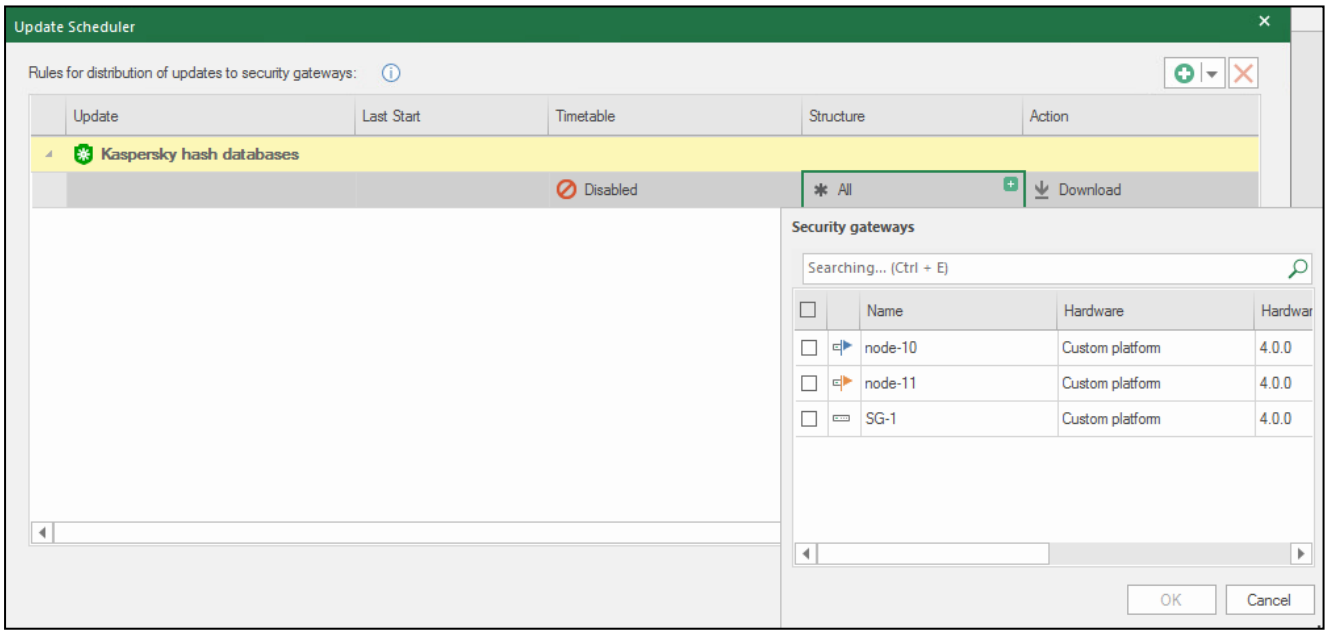


2. In the top right corner, click and in the drop-down list, select the required vendor rule category.
   The selected update profile appears. If the update repository contains the downloaded updates, their versions are displayed in the **Update** column.
3. In the **Timetable** column, click in the respective update profile.
   The **Schedule** dialog box appears.



4. Turn on the **Update on schedule** toggle.
5. Select the **Periodically every**/**One time**/**Timetable** option.
6. For the **Periodically every** option, specify the **Start of update** and **Repeat** parameters.
7. Click **OK**.
8. In the **Structure** column, click ⊞ in the respective update profile.

   The **Security Gateways** list appears.



9. Select the required Security Gateway and click **OK**.
10. In the **Action** column, click ▼ in the respective update profile.
11. In the drop-down list, select **Download** or **Force installation**.

    The **Download** parameter will be activated only after the policy installation. If the **Force installation** parameter is selected, the system initializes component restart to apply the update.
12. Click **OK**.
13. To apply changes, click **Install policy** on the toolbar, select the Security Management Server and the subordinate Security Gateways and click **OK**.

To update IPS protections and Web/FTP filtering exceptions:

1. Download updates to the repository manually (see p. **10**) or wait for the update download on schedule to complete.
2. Click **Install policy** on the toolbar, select the Security Management Server and the subordinate Security Gateways and click **OK**.

Roll back the latest software update

In Continent, you can roll back the latest update of the following components:

- Security Gateway software, SkyDNS categories, Threat Intelligence feeds, Kaspersky hash databases, user hashes and GEO/IP (see below).
- Configuration Manager. A rollback is performed identically to the update installation (see p. **13**).
- Security Gateway cluster software (see p. **17**).

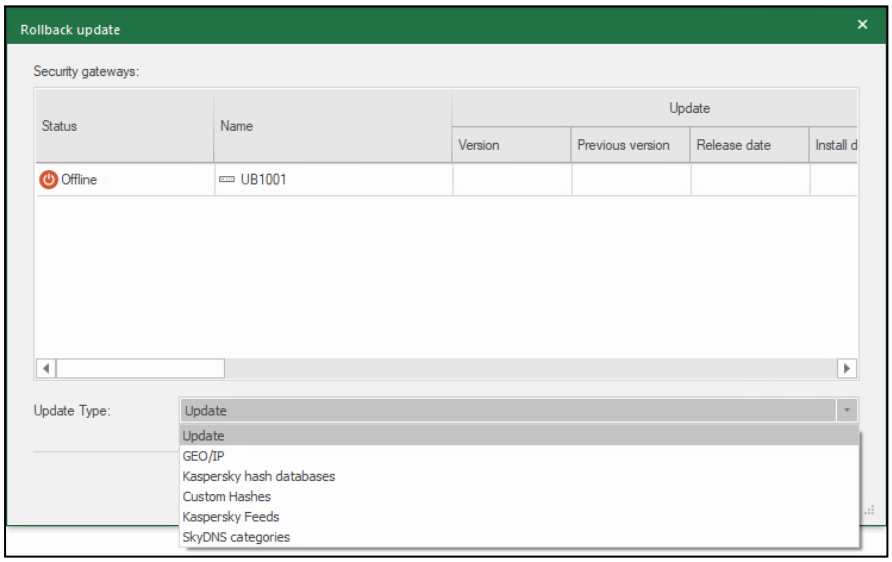
After rolling back the latest software update, the current updates of vendor rules must be reinstalled.

To roll back the latest software update of the Security Gateway software, SkyDNS categories, Threat Intelligence feeds, Kaspersky hash databases, user hashes and GEO/IP:

1. In the Configuration Manager, go to **Administration** and select **Updates**.
2. In the list, select the required Security Gateways and click **Roll back latest update** on the toolbar.

   The **Roll back latest update** command is available for several Security Gateways if the Security Management Server is not included in the list.

   The **Rollback update** dialog box appears.



3. In the **Update Type** drop-down list, select the update type required to be rolled back. Click **OK**.

   The previous software version is restored and the respective message appears.
4. Click **OK**.

   After the rollback of the Security Management Server software update, the created task appears in the Notification center. The connection with the Configuration Manager and Security Management Server will be lost. Roll back the latest Configuration Manager software update (see p. **13**). Then, restart the Security Management Server and try to re-establish the connection between the Configuration Manager and the Security Management Server.

> **Note.**
> When you roll back the latest Security Management Server software update, the SMS database will be restored from the latest snapshot. Thus, all the changes made after this snapshot was taken will be discarded.

To roll back the latest Security Gateway cluster software update:

1. Roll back the latest update of the Security Gateway software with the **Standby** status.
2. Wait until the Security Gateway restarts and the respective task appears in the Notification center.

   The state of the cluster component will be changed to **OK, Not ready**.

3. Right-click the active Security Gateway from the cluster. In the drop-down menu, click **Stop**.
4. Roll back the latest software update of the stopped Security Gateway.
5. Wait until the Security Gateway restarts and the respective task appears in the Notification center.
   The states of the cluster components will change to **OK**.
6. Roll back the latest Security Management Server software update (see p. **17**).
7. Install the policy on the Security Gateway.

In case of failure during the rollback of the latest software update, you can restore from a backup (see [**2**]). You need to take into account that restoring from a backup is performed for the software version for which the backup was created.

Documentation

1. Continent Enterprise Firewall. Version 4. Administrator guide. Deployment.
2. Continent Enterprise Firewall. Version 4. Administrator guide. Management.