trustedACCESS
by Security Code

Continent-RA
Version 4

Setup and Management

Administrator guide

Mailing address:	**Silicon Oasis HQ, Wing B, office # A-611, Dubai. UAE | P.O Box 341260**
Phone:	**+971 43 724 695** **+971 43 591 001**
Email:	**sales@trustedaccesstech.com**
Web:	**https://www.trustedaccesstech.com**

Table of contents

Introduction

This manual is designed for administrators of Continent-RA, Version 4 (hereinafter Continent-RA). It contains information about installation, setup and operation of Continent-RA on computers running Windows.

Web-site. Information about Trusted Access Technologies products can be found on https://www.trustedaccesstech.com/.

Technical support. You can contact 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 Trusted Access Technologies in authorized education centers. List of the centers and information about learning environment can be found on the web site: https://www.trustedaccesstech.com/. You can contact company representative for more information about organization of teaching process by email: education@securitycode.ru.

Chapter 1
Overview

Purpose and main functions

Continent-RA is designed to establish a secure connection and exchange encrypted data with the Access Server (AS) of Continent Enterprise Firewall, versions 3.7, 3.9 (available only in Russian Federation) and a Security Gateway (Continent, version 4) with the **Access Server** component enabled via public (unprotected) networks.

Continent-RA can perform the following:

- establish a secure connection and exchange of encrypted data with the Access Server;
- log operation events;
- manage a Public Key Infrastructure (PKI);
- control the integrity of software and transferred and stored information.

Continent-RA is used alongside Continent Enterprise Firewall and/or Continent 4.

Continent-RA comes in the following modifications:

- modification 1 — complies with the Federal Security Service of the Russian Federation requirements for KC1 cryptographic tools.
- modification 2 — complies with the Federal Security Service of the Russian Federation requirements for KC2 cryptographic tools. Operates alongside Sobol.
- modification 3 — complies with the Federal Security Service of the Russian Federation requirements for KC2 cryptographic tools. Operates alongside Sobol and CryptoPro CSP.

To install Continent-RA, a computer must meet the following system requirements:

Component	Requirement
Operating system	• Windows Server 2016 x64; • Windows Server 2012 R2 x64; • Windows Server 2012 x64; • Windows 10 x86/x64 (except Education, Home and Insider Preview editions); • Windows 8.1 x64/x86;
CPU, RAM	According to the requirements of the installed OS
HDD (free space)	150 MB
Additional hardware	DVD/CD-ROM drive
Additional software	• Sobol (for modifications 2, 3); • CryptoPro CSP (for modification 3)

Continent-RA is software installed on a user computer and operates alongside Continent Enterprise Firewall and/or Continent 4. To connect to the Access Server, the user establishes a secure connection according to the settings given by the administrator. Thus, all data during exchange is encrypted. Continent-RA can connect to the Access Server using protocols of versions 3.X and 4.X.

When a user connects using **3.X** protocol:

- **TCP** and **UDP** can be used for connection;
- user certificate authentication is performed.

When a user connects using 4.X protocol:

- **TCP** is used;
- user certificate authentication or password-based authentication can be performed.

To connect via VPN, there are IPS protections created for each user on the Access Server. To redirect all the traffic through the Access Server while the connection is established, the required metric of routes on the computer with Continent-RA must be not less than 276.

Note. Continent-RA cannot be used as a gateway passing all traffic.

While in operation, the Integrity check utility controls the integrity of Continent-RA and the Diagnostic information utility audits software performance.

Required certificates

Continent-RA requires the following certificates:

- certificate of a user certificate issuer;
- certificate of a server certificate issuer;

  Note. Certificate of an issuer is a root certificate of a certificate authority (CA).
- user certificate;
- server certificate.

Continent-RA enables you to check if certificates are on a Certificate Revocation List (CRL).

If a computer is directly connected to a CA, a CRL is automatically downloaded via HTTP. Otherwise, the user should download CRL certificates to Windows certificate store using Continent-RA software.

Attention! If a certificate issued by the AS is checked, disable CRL check.

Integrity check

Continent-RA Integrity check is a utility designed to monitor the Continent-RA software contents integrity and shipped along with the Continent-RA distribution kit.

It checks files and folders of the distribution kit or installed Continent-RA software and Windows files.

In the first case, integrity check is performed by calculating checksums for files stored on a disk copied from the distribution kit and then comparing results to the values stored in a special file of the Continent-RA distribution kit.

In the second case, it is performed by comparing current checksums to the reference values that were calculated during Continent-RA installation. Reference values can be recalculated only by a user with Windows administrator privileges.

A list of files for integrity check and their checksums are stored in a configuration file. This file is created during the installation.

Software integrity check is performed during Continent-RA startup and during an audit, the frequency of which is set in the Integrity check utility. Integrity check parameters can be configured only by users with Windows administrator privileges (see p. **37**).

If there is an error while the integrity check is performed, a user receives a message about an integrity violation.

If an integrity violation is detected during the audit and Continent-RA is in operation, all active sessions with protected resources remain active. New sessions cannot be created and the warning element will be added to the application icon in the Windows notification area. If an integrity violation is detected and Continent-RA is not in operation, the respective event is logged.

If an integrity violation is detected, a user receives a message prompting him or her to restore files:

- at Continent-RA startup;
- during an attempt to connect to the Access Server (if an integrity violation is detected during the audit and there is an active connection).

Integrity check events are registered in the Windows log.

Key carriers

A personal key carrier stores key information: a container with a private key and its password. It can also store a user certificate and its root certificate. The carriers are issued to users by an administrator.

The following types of hardware media can be used as key carriers:

- USB flash drives;
- USB-keys and smart cards — Rutoken S, Rutoken Lite, Rutoken ES 2.0, Rutoken ES 2.0 Flash, JaCarta PKI, JaCarta PKI/GOST, JaCarta GOST, JaCarta 2 GOST;
- DS1995, DS1996 security tokens.

Note. To use the hardware media, install all the required software and drivers (see p. 12).

Audit

Audit (gathering of diagnostics information) is a process of Continent-RA performance control. The audit is performed by the **Diagnostic Information Utility** that is a part of the Continent-RA distribution kit. The performance assessment is performed by analyzing events registered during the audit.

All events of Security Gateways, Continent-RA services and all system events that meet the minimum requirements of log storage are registered in the system log.

Chapter 2
Quick start and first run

To install, configure and start using Continent-RA, use the quick start procedure.

Before you start the installation, get the configuration profile (configuration file) and passwords to import the configuration profile and key container from your company's security administrator. Use any available carrier, e.g. USB-drive.

Attention! During the installation of Continent-RA, Security Code CSP will be installed.If you want to use Continent-RA with another cryptographic provider, install its software before Continent-RA installation.

To install, configure and run Continent-RA for the first time:

1. Insert the installation disk into DVD/CD-ROM, run **Continent-RA.exe** () and follow the instructions on the screen.

   Note. If the Windows security window prompting you to confirm the installation of Continent-RA appears, click **Yes** or **Install**.

   The Installation Wizard will diagnose the system and start the software installation. When the installation is completed, you receive a message prompting you to restart the operating system.

2. Click **Restart**.

   The operating system will be restarted.

   After that Continent-RA runs automatically. You receive a message prompting you to gather entropy for the RNG using human input.

   Note. If Continent-RA is installed by a user with the restricted rights, then after restarting the operating system Continent-RA does not run automatically.The user needs to run it by double clicking on the Continent-RA icon or selecting it from the **Start** menu.

3. Follow the instructions on the screen.

   After the entropy is gathered, you receive a message prompting you to register Continent-RA on the Security Code server.

4. Click **Continue without registration**.

   For detailed information about registration, see p. **14**.

   A dialog box prompting you to import the configuration file appears.

   Note. The configuration file contains all the necessary information to establish a secure connection.

5. Click **Yes**.

   The File Explorer appears.

6. Select the required configuration file and click **Open**.

   A dialog box prompting you to enter the configuration import password appears.

7. Enter the password of the configuration profile import that you received from the administrator and click **OK**.

   A dialog box prompting you to enter the key container password appears.

   Enter the key container password that you received from the administrator and click **OK**.

   Note. Select the **Remember password** check box if your company's security policy does not require you to set a new password after the first run of Continent-RA. If necessary, change the password following the instructions on the screen.

   A dialog box prompting you to select the key carrier for saving the configuration file appears.

8. Select the required key carrier and click **OK**.

   You receive a message about the successful import completion.

9. Click **OK**.

   You receive a message prompting you to connect using the imported profile.

10. To return to the main menu of Continent-RA, click **No**.

11. If you do not want to return to the main menu, click **Yes**.

    The connection establishment starts.

You receive the respective message after the remote connection is successfully established. In the notification area, the Continent-RA icon will change from gray to green.

Chapter 3
Installing, repairing and updating Continent-RA

Install Continent-RA

Security Code CSP is installed during the Continent-RA installation. If you need to use Continent-RA in combination with the CSP of another manufacturer, install the third-party software before installing Continent-RA.

If you want to use only Security Code CSP, run the installation process and click **Settings**, then clear the **Allow both Security Code CSP and a third party CSP installed** check box.

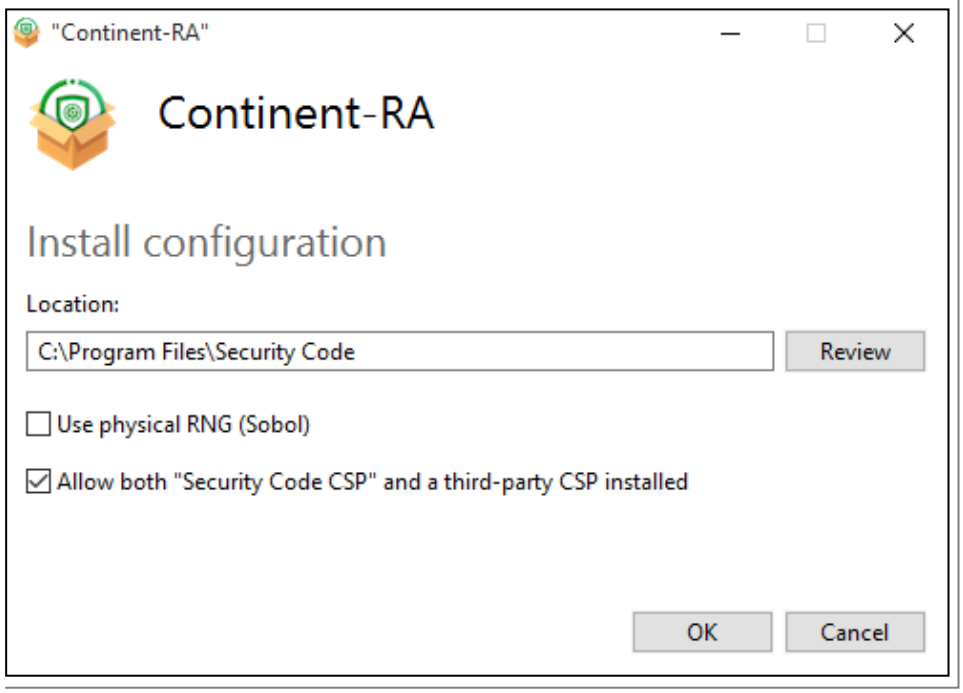
Attention! If a third-party CSP and TLS client version 2.0 are installed on your computer, you cannot install Security Code CSP when installing Continent-RA. The selected **Allow both Security Code CSP and a third party CSP installed** check box will be ignored.

To install the software:

1. Insert the installation disk and run **Continent-RA.exe** ().

   The Continent-RA installation dialog box appears on the screen. It contains the license agreement.

   Note. If you need to select a destination folder for the installation or select a physical RNG for Sobol, click **Settings** and follow the instructions that appear on the screen.



2. Read the agreement and click **I accept the terms of the license agreement**, then click **Install**.

   Note. If the **Windows Security** dialog box appears and asks you to confirm the installation, click either **Yes** or **Install**.

   The installation wizard performs the system diagnostics and starts the installation. After the installation is finished, a dialog box appears asking you to restart your computer.

3. Click **Restart**.

   Computer restarts.

After you install Continent-RA, the application shortcut appears on the desktop, and the Start menu contains the **Security Code** section.

This section contains the following applications:

Name	Description
Repair Continent-RA	Repair Continent-RA using the distribution kit
Continent-RA	Run Continent-RA
Continent-RA Integrity Check	Integrity check of the distribution kit and the installed software
Register Continent-RA	Register Continent-RA on the Registration server of Trusted Access Technologies
Collection of diagnostic information	Export the report of Continent-RA performance
Repair Security Code CSP	Repair Security Code CSP using the distribution kit
SECURITY CODE CSP	Run Security Code CSP

Uninstall Continent-RA

There are three ways to delete Continent-RA:

- using **Programs and Features** of Windows;

  Note. If you delete Continent-RA using Windows tools, custom settings are saved and can be used further if the software will be installed again.

- using the repair software tool;
- using the MSI packet on the setup disk.

  Note. If you delete Continent-RA using the repair tool or the MSI packet, you can also delete the custom settings.

Continent-RA and Security Code CSP can be deleted separately in any order.

Repair Continent-RA

To repair the software:

1. On the **Start** menu, in the list of applications, select **Security Code** folder and run the repair program for the respective software.

   The setup wizard appears on the screen.
2. Click **Next**.

   A dialog box for deleting or repairing software appears.
3. Click **Repair**, then click **Next**.

   A dialog box appears on the screen.
4. Click **Repair**.

   The procedure starts, when it is completed the respective dialog box appears.
5. Click **Finish**.

   A dialog box appears asking you to restart your computer.
6. Click **Restart**.

Update Continent-RA

To update Continent-RA, install the latest version on a computer that have an older one.

Attention! When you start updating Continent-RA, a dialog box appears asking you to confirm the update. To install the new version and migrate old settings, click **Yes**. To cancel installation, click **No**. Proxy settings will not be automatically migrated. You need to save them in advance.

The update procedure is similar to the installation procedure. (see p. **10**).

Install additional software

If you want to use Continent-RA with personal key carriers, install additional software.

Chapter 4
Setup and operation

Deployment

Get ready for operation

To deploy Continent-RA, take the following steps:

1. Install Continent-RA (see. p. **10**).
2. Register the software (see p. **14**).
3. Configure the connection profile (see p. **16**).
4. Get security certificates (see p. **22**).

> **Note.** Algorithms for digital signature generation used in the certificates must match (GOST R 34.10–2001 for CryptoPro CSP or GOST R 34.10–2012 for Security Code CSP).

5. Install root and user certificates (see p. **30**).
6. Install server certificates (see p. **31**).
7. Install a CRL (if you need to check certificates against a CRL, see p. **31**).
8. Configure Continent-RA operation parameters (see p. **33**).

Run Continent-RA

After the installation, Continent-RA runs automatically after OS startup. The program's window is minimized by default and its shortcut is displayed in the Notification area.

> **Attention!**
> - We do not recommend denying access to the public\continentvpnclient folder for Continent-RA appropriate operation.
> - A user with limited privileges should run the program manually. To do so, double-click **Continent-RA** shortcut or click it in the **Start** menu.

To run Continent-RA:

- Click **Start**, select **All applications | Security Code | Continent-RA** or double-click **Continent-RA** shortcut.

  The main window of Continent-RA appears. In the left corner of the Windows notification area, the program icon appears.

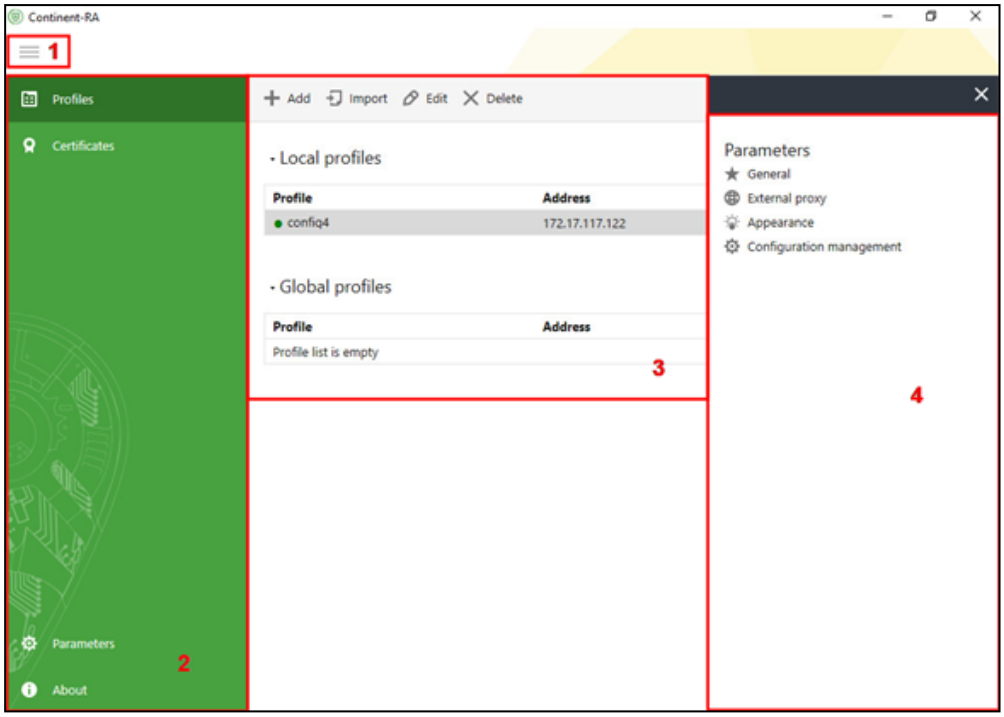
Right-click the Continent-RA icon in the notification area to perform the following:

- to connect with the default profile;
- to disconnect the current connection or establish a configured connection;
- to open software operating parameters configuration;
- to exit the application (the application closes, but the connection is not broken).

When you double-click the Continent-RA icon in the Windows notification area, the connection set by the default profile is established or ended.

> **Note.** To minimize the main window, you can use  and  in the top right corner. To exit Continent-RA, right-click its icon in the Windows notification area and click **Exit**.

Continent-RA main window

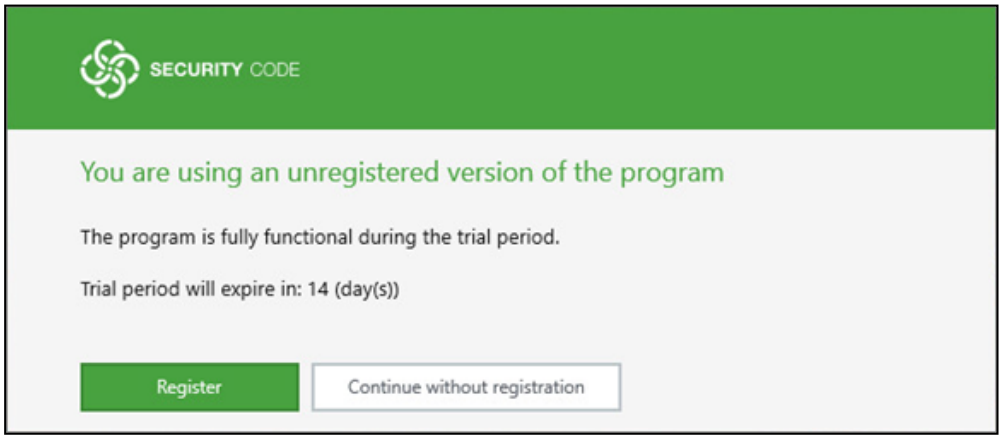


At the top of the main window, there is the menu button —  (1).

On the left of the main window, there is the navigation panel (2). In the display area, you can find details about the Continent-RA operating parameters configuration (3). On the right of the main window, there is the list of parameters (4). By default, the list of profiles appears.

Registering Continent-RA

If Continent-RA is not registered, when you run it, a dialog box prompting you to register it on the Security Code server appears. Both online and offline registration are available.

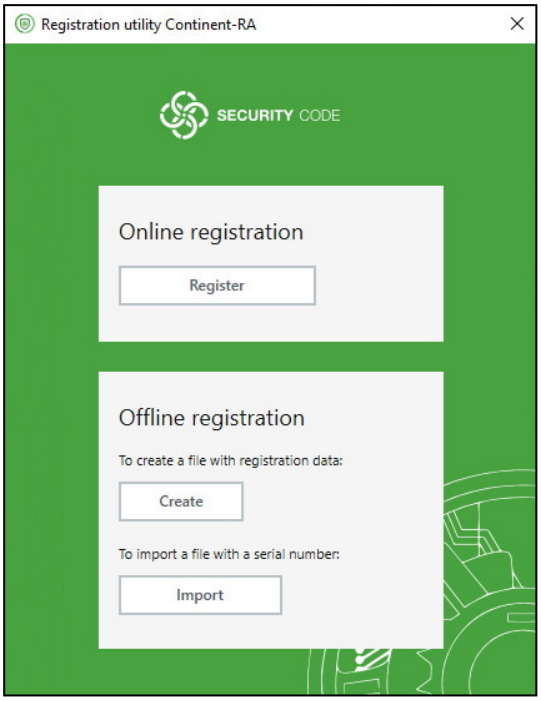


The trial version of Continent-RA will expire in 14 days after you have installed the software. The number of days left until the expiration date is displayed in the **About** section. If you do not register Continent-RA within this period, you will receive a message prompting you to register it every time you run the program. If you do not register Continent-RA, it will stop working.

To register Continent-RA online:

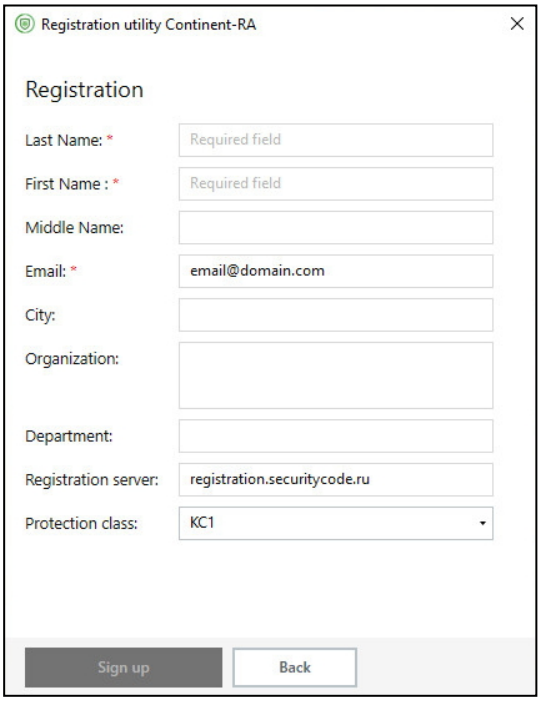
1. In the dialog box prompting you to register Continent-RA, click **Register** or select **All apps** | **Security code** | **Continent-RA** | **Register Continent-RA** in the Windows main menu.

   A dialog box appears as in the figure below.



2. Click **Register**.

   The **Registration** dialog box appears.



3. Specify the required information and click **Sign up**.

   The registration starts. The program attempts to connect to the specified server When the registration is completed, you will receive the respective message.

After the registration of Continent-RA, the program registration number appears in the **About** section.

To register Continent-RA offline:

1. If you do not have access to the registration server, click **Create** in the **Register Continent-RA**.

   The **Registration** dialog box appears.

   Note. If you have previously specified the information for online registration, it is saved automatically and you do not need to specify it again.

2. Specify the required information and click **Create file**.

   The File explorer appears.

3. Save the file and send it to the registration server to get the file with the serial number.
4. After you receive the file with the serial number, click **Import** in the **Register Continent-RA**.

   The **File explorer** dialog box appears.

5. Select the required file and click **Open**.

   When the registration is completed, you will receive the respective message.

Configuring connection profiles

Global and local profiles

To connect to the Access Server, you need to create and configure a connection profile or import an already created and configured profile from a configuration file created using the Access Server. In Continent-RA , there are two types of profiles: local and global.

Attention! All users can connect to the Access Server using a global profile (for detailed information about connecting to the Access Server, see p. 20.

To create a new profile, edit or delete an existing one and import a pre-configured one, use the toolbar.

Attention! To create and manage global profiles, you need to run Continent-RA as administrator.
Before you create a global profile, make sure the root certificate of the Access Server certificate and the user certificate are installed onto the Local Machine store.

To create a global profile:

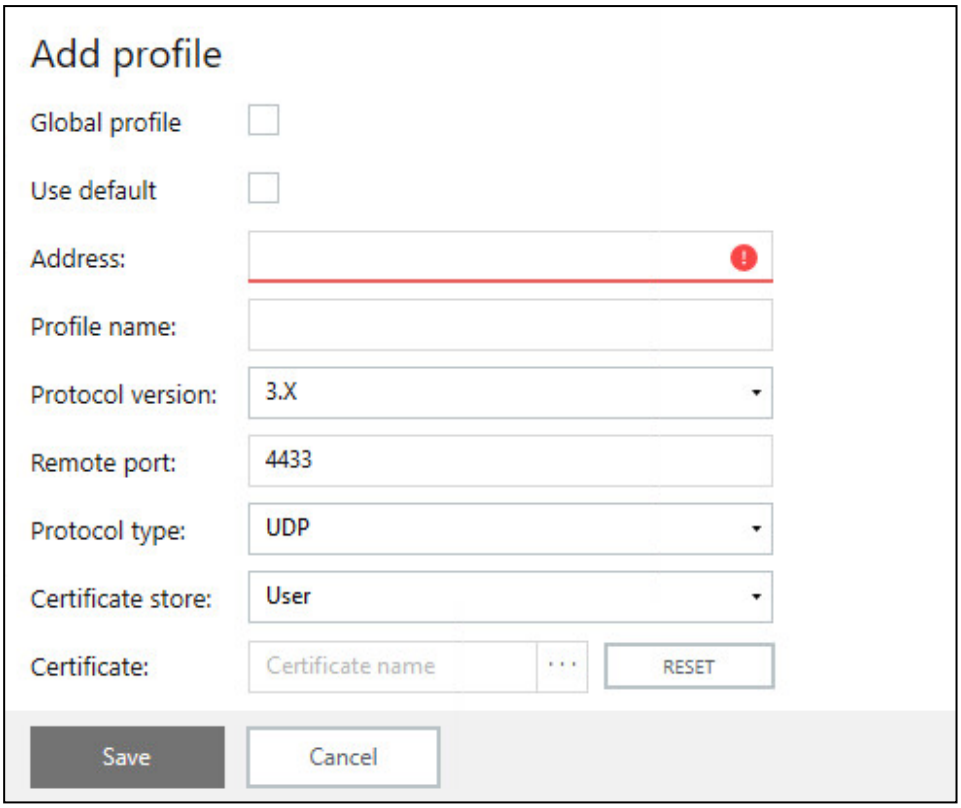
1. Run Continent-RA as administrator.
2. On the navigation panel, go to **Profiles**.

   In the display area, there is a list of the existing connection profiles. If a profile is configured correctly, it has a green indicator.

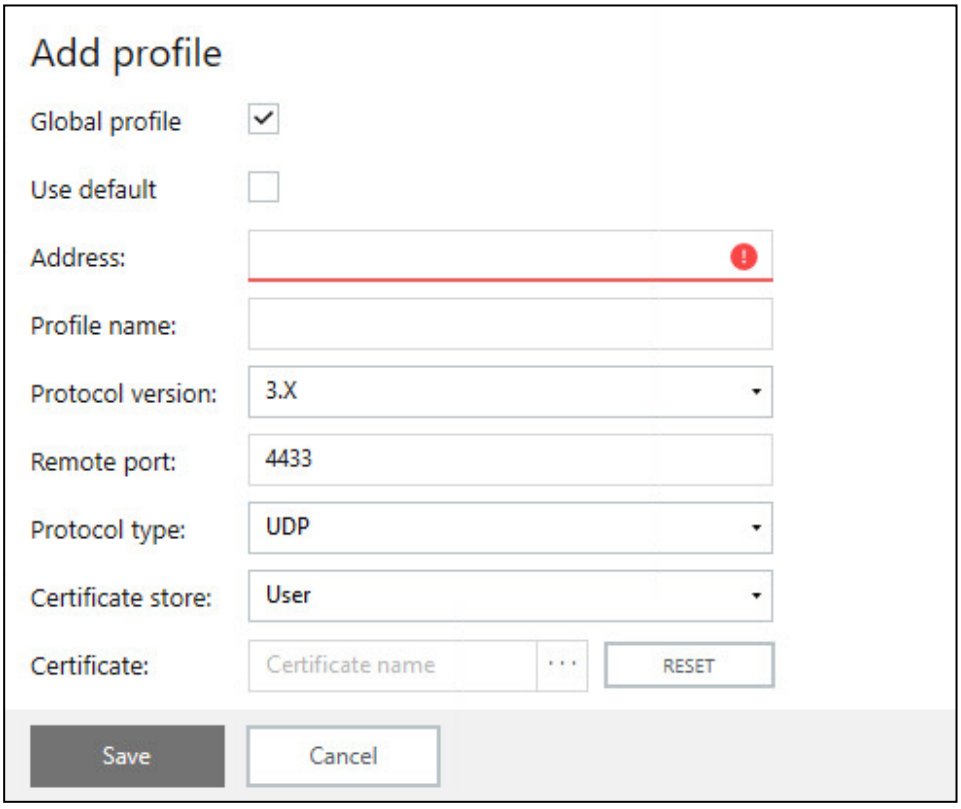
   Note. If a connection profile is configured incorrectly or not all the required information is specified,this profile has a red indicator and there is an error message in the **Status** column.

3. To add a new global connection profile, click Add on the toolbar.

The **Add profile** dialog box appears.



4. Select the **Global profile** check box.
The certificate store is selected automatically.



Note. If you want this profile to be a default connection profile, select the respective check box.

5. Specify the Access Server address, the profile name and the protocol version.

Attention! When you change the protocol version, the information in the **Remote port** field is changed automatically. If you have selected **4.X**, then in the **Address** field, you must specify the same value as in the **CommonName** field of the server certificate (the name must be an IP address or a domain name specified using Latin characters without spaces).

6. Specify the port if it differs from the default one.

Attention! If you need to change the port when connecting to the Access Server, version 4.0, clear the **Standard port** check box and specify the required value in the **Remote port** field. To roll back to the default value, select the **Standard port** check box.

7. If you have specified **3.X** protocol version, select the required protocol in the **Protocol type** drop-down list. If you have selected **4.X** protocol version, go to step **10**.
8. To authenticate using **3.X** protocol, click ... and select the required certificate.

Attention! If you do not want to use the selected certificate, click **Reset**.

The **Select the certificate** dialog box appears.

The list contains only valid certificates and certificates that comply with the algorithm of the used CSP.

9. Select the required certificate and click **OK**.

The name of the selected certificate appears in the **Certificate** field.

10. If you have selected **4.X** protocol, select the authentication type from the respective drop-down list:
    - authentication by user certificate;
    - authentication using user credentials.
11. If you have selected the first authentication type, go to step **9**.
12. Specify user credentials in the respective text boxes.
13. Click **Save**.

To create a local profile:

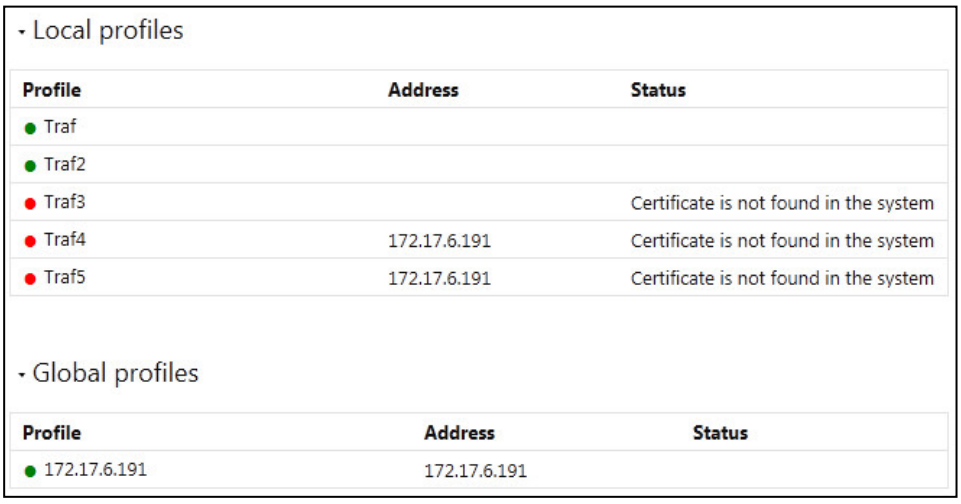
Attention! Only a user who has created such a profile can use it.

1. On the navigation panel, go to **Profiles**.

The list of profiles appears in the display area.

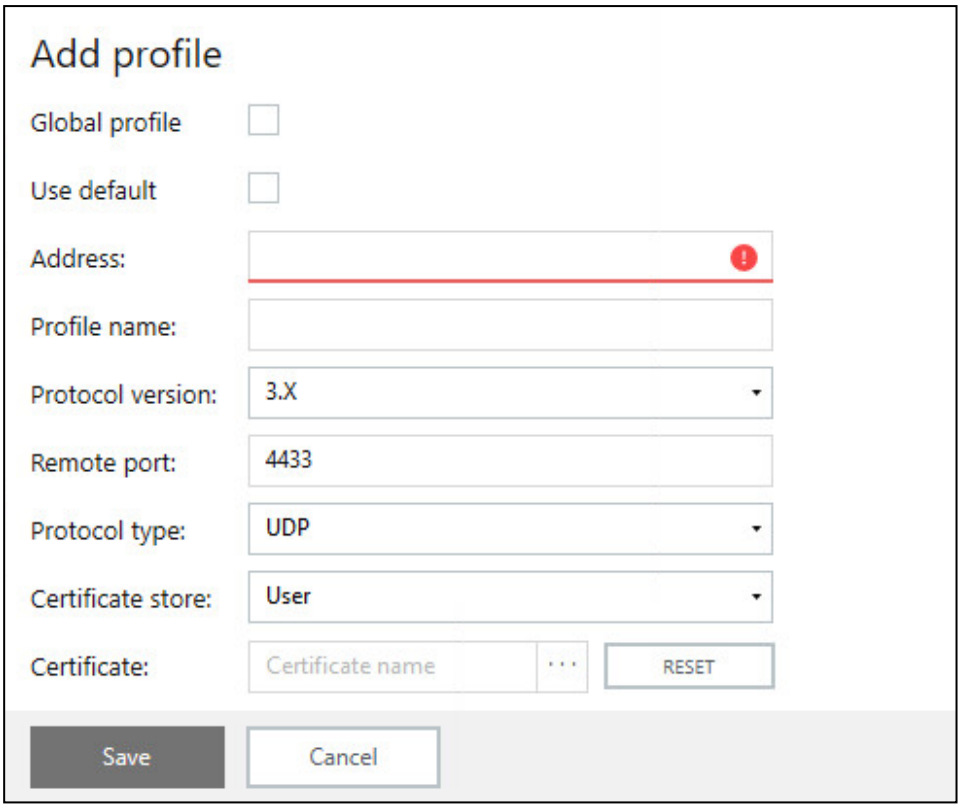
The green indicator means the profile is configured correctly.

Note. If the connection profile is configured incorrectly or not fully, the indicator of a profile is red and the **Status** column contains the error message.



2. To add a new connection profile, click Add.

The **Add profile** dialog box appears.



Note. If you want this profile to be a default connection profile, select the respective check box.

3. Specify the Access Server address, the profile name and the port (if necessary).

Attention! When you change the protocol version, the information in the **Remote port** field is changed automatically. If you have selected **4.X**, then in the **Address** field, you must specify the same value as in the **CommonName** field of the server certificate (the name must be an IP address or a domain name specified using Latin characters without spaces).

4. Specify the port if it differs from the default one.

Attention! If you need to change the port when connecting to the Access Server, version 4.0, clear the **Standard port** check box and specify the required value in the **Remote port** field. To roll back to the default value, select the **Standard port** check box.

5. If you have specified **3.X** protocol version, select the required protocol in the **Protocol type** drop-down list. If you have selected **4.X** protocol version, go to step **8**.

6. To authenticate using **3.X** protocol, click … and select the required certificate.

Attention! If you do not want to use the selected certificate, click **Reset**.

The **Select the certificate** dialog box appears.

The list contains only valid certificates and certificates that comply with the algorithm of the used CSP.

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

The name of the selected certificate appears in the **Certificate** field.

8. If you have selected **4.X** protocol, select the authentication type from the respective drop-down list:
   - authentication by user certificate;
   - authentication using user credentials.
9. If you have selected the first authentication type, go to step **9**.
10. Specify user credentials in the respective text boxes.
11. Click **Save**.

To import a connection profile:

1. To import an already created connection profile, click Import on the toolbar.

   Attention! Only a user with administrator privilegies can import a global profile (when working with the Access Server 4). To get administrator privilegies, run Continent-RA as administrator.

   The File Explorer appears.
2. Select the required configuration file and click **Open**.

   You receive a message prompting you to enter the configuration import password.
3. Enter the password of the configuration profile import that you received from the administrator and click **OK**.

   A dialog box prompting you to enter the key container password appears.

   Enter the key container password that you received from the administrator and click **OK**.

   Note. Select the **Remember password** check box if your company's security policy does not require you to set a new password after the first run of Continent-RA. If necessary, change the password following the instructions on the screen.

   The dialog box prompting you to select the key carrier for saving the configuration file appears.
4. Select the required key carrier and click **OK**.

   You receive a message about the successful import completion.
5. Click **OK**.

   You receive the message prompting you to connect using the imported profile.
6. To return to the **Profiles** section, click **No**.

To edit a connection profile:

1. To edit a profile, select it and click Edit on the toolbar.

   Attention! You can configure only the profile that is not connected at the moment. To edit a global profile, you must run Continent-RA as administrator. The global profile status cannot be edited.

   The **Add profile** dialog box appears.
2. Make the required changes and click **Save**.

To delete a connection profile:

1. To delete a profile, select the required profile and click Delete on the toolbar.
2. You receive a message asking you to confirm the deletion.

   Click **Yes**.

Connecting to the Access Server

You can connect to the Access Server:

- automatically at Continent-RA startup using a profile selected by default (for local and global profiles);
- manually (for local and global profiles);
- before Continent-RA logon (only for global profiles).

Configure automatic connection using a default profile

To configure automatic connection using a default profile:

1. Run Continent-RA as administrator.
2. Go to **Parameters** | **General** and select **Connect using a default profile** in the **Startup mode** group box.

3. If you have not selected a profile as default during its creation or import, select a profile from the list, click **Edit** on the toolbar and select **Use by default** (for detailed information, see p. 20).

   Attention! If you have selected **Connect using a default profile** but have not selected a default profile, Continent-RA does not connect to the Access Server at its next startup and you receive the message that the connection profile is not selected. To connect to the Access Server, take step **2**.

   At the next startup, Continent-RA automatically connects to the Access Server using the selected profile.

   Attention! An automatic connection using a default profile cannot be established if a user end the session without closing the connection. In this case, you receive the following message: **Connection using a default profile cannot be established if another connection was established earlier**. Close the connection and restart Continent-RA.

Connect to the Access Server manually

This connection method is applicable to both local and global profiles and is used when the company security policy prohibits an automatic connection to the Access Server at the OS startup.

If you have not set a default profile when importing profiles, select the required profile, click **Edit** on the toolbar and select **Use by default** (see p. 20).

To connect to the Access Server manually:

1. Run Continent-RA.

   If the default profile is selected in the Continent-RA settings, the connection process using the default profile will start.

2. If the default profile is not selected, right-click the Continent-RA icon on the Windows taskbar.
3. In the list, select **Connect**.Then, in the list of profiles, select the required profile.

   Note. When you select the profile by clicking **Connect**, you see only profile names but not their types.

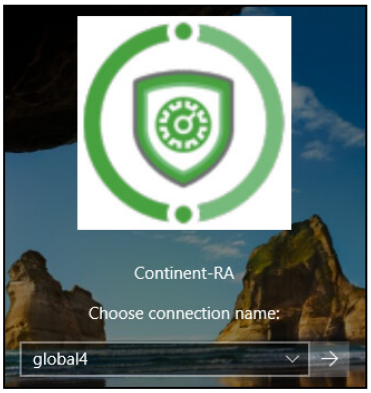
Connect to the Access Server before logon

You can connect to the Access Server before you log on to the system only using a global profile.

To connect to the Access Server before logon:

1. Run Continent-RA as an administrator.
2. Go to **Parameters | General** and select **Allow Continent-RA to connect before logon** in the **Startup mode** group box (by default, it is not selected). For details, see p. 34.
3. Make sure that the option is selected. To do so, log off the system. In the bottom right corner, the **Network logon** button  appears.
4. Click **Network logon**.

   The window appears as in the figure below.



5. In the drop-down list, select a global profile and click  .
6. You have connected to the Access Server. A dialog box prompting you to log on to the system appears. To continue working with the system, log on using your credentials.

Certificate management

Continent-RA allows you to install certificates into the store, create user certificate requests and save keys to a removable carrier or in the registry.

Initial configuration

To use Continent-RA, you need root certificates, user certificates and server certificates obtained according to the procedure established by a CA. For detailed information about creating a user certificate request, see p. **22**.

Note. You can use the valid unique user certificate issued by a CA earlier.

We recommend that you use removable carriers for the certificates.

Note. As a key carrier, you can use the following devices:

- USB drives;
- USB keys and smart-cards — Rutoken, Rutoken Lite, Rutoken S (versions 2.0 и 3.0), Rutoken Electronic Signature, JaCarta PKI, JaCarta GOST, JaCarta PKI Flash, JaCarta GOST Flash;
- DS1995 and DS1996 identifiers.

After you get the required certificates, install the certificates to the current user store using Continent-RA (see p. **30**), Windows tools or other CSPs:

Certificate	Cryptographic Service Provider	
	Security Code CSP	**Third-party**
Root	Windows or Continent-RA	Windows or Continent-RA
User	Continent-RA	CSP
Server, CRL Distribution Points (CDP)	Windows or Continent-RA	Windows or Continent-RA

Create a user certificate request

You can create a user certificate request via Continent-RA on the request of a security administrator. A user private key is generated by the CSP at the same time as the request.

The request is saved to a folder specified by a user. The key container with the private key is saved on a key carrier, specified in settings.

Advice. Before you create a request, prepare an empty formatted key carrier for the key container.

To create a certificate request:

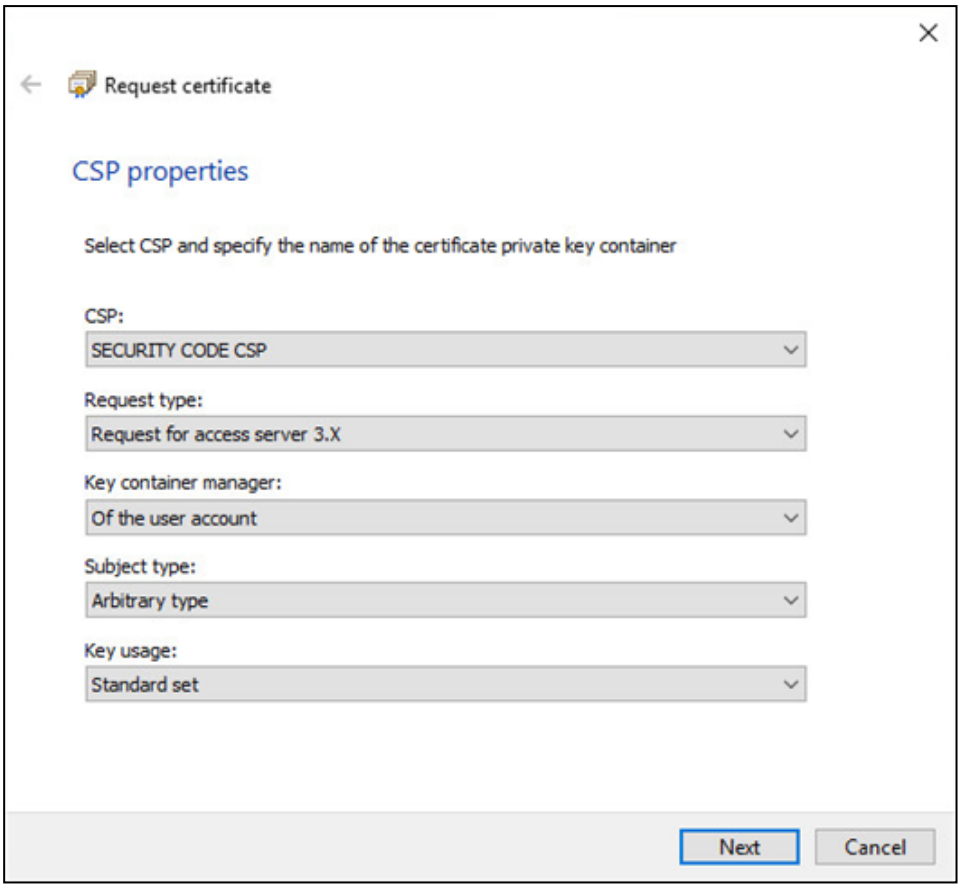
1. On the navigation panel, go to **Certificates**

   In the display area, the list of the installed certificates appears.

   Note. To view the installed certificates in the user account console, on the toolbar, click the **Open store** button.

2. On the toolbar, go to the **User certificates** tab and click the **Create request** button.

The **CSP properties** dialog box appears.

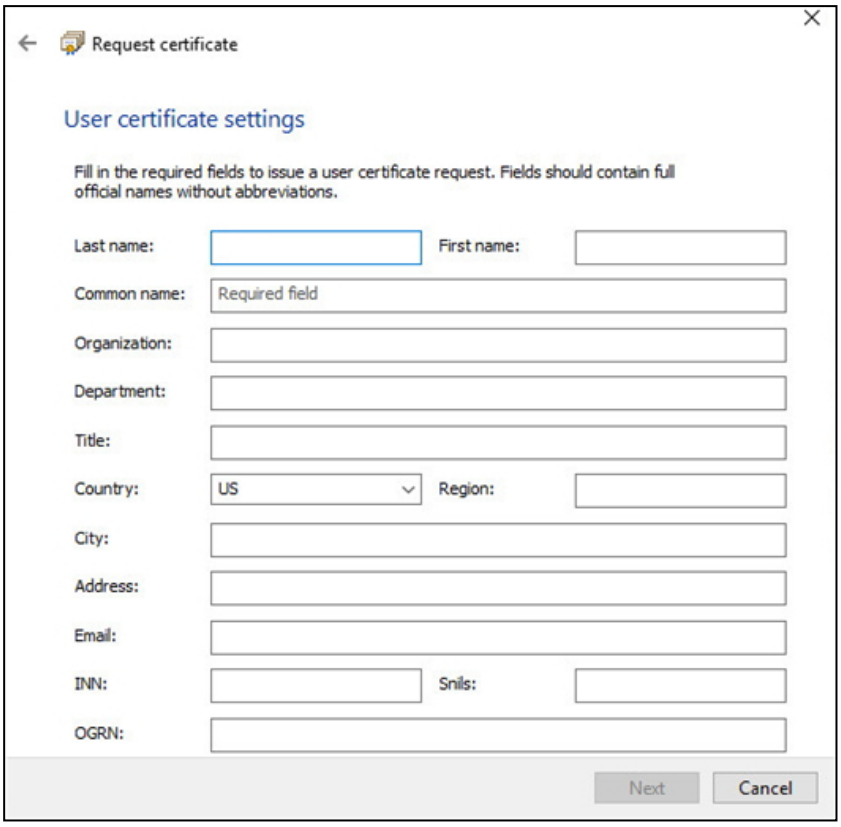


3. Select what is required:
   - in the **CSP** drop-down list, select the required CSP;
   - in the **Request type** drop-down list, select the request type:
     - **Request for access server 3.X** (by default) — the request format for the certificate created in the Configuration Manager;
     - **Request for access server 4.X or CA** — the request format for the certificate by the Configuration Manager of the Security Gateway or by a CA;

       Attention! Then you create a certificate request for a global profile, select **Local computer** as a storage type. For other certificates use the dfault storage.
     - **Request for CA CryptoPro** — the request format for the next processing by the CryptoPro CSP.
   - in the **Certificate store** drop-down list, select a key container store to save the user certificate private key;
   - in the **Subject type** drop-down list, select the user that creates the request:
     - **Arbitrary type** (by default);
     - **Individual**;
     - **An individual with power of attorney from a legal entity**;
     - **Individual entrepreneur**;
     - **Legal entity**;
   - in the **Key usage** drop-down list, select the key set:
     - **Standard set** (the minimum required parameters for the encryption key functioning);
     - **Extended set** (additional encryption key parameters; use if it is allowed according to the company's information security policy).
4. Click **Next**.

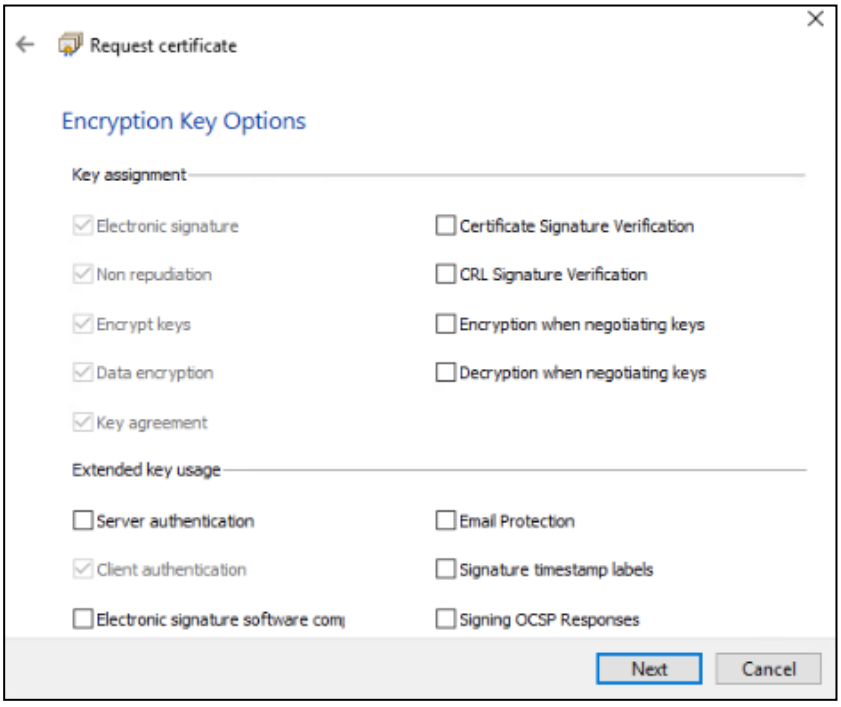
The **User certificate settings** dialog box appears.

Note. Each user type has its own list of parameters. In the figure below, you can see the list of parametrs for the **Arbitrary type**.



5. Fill in the text boxes and click **Next**.

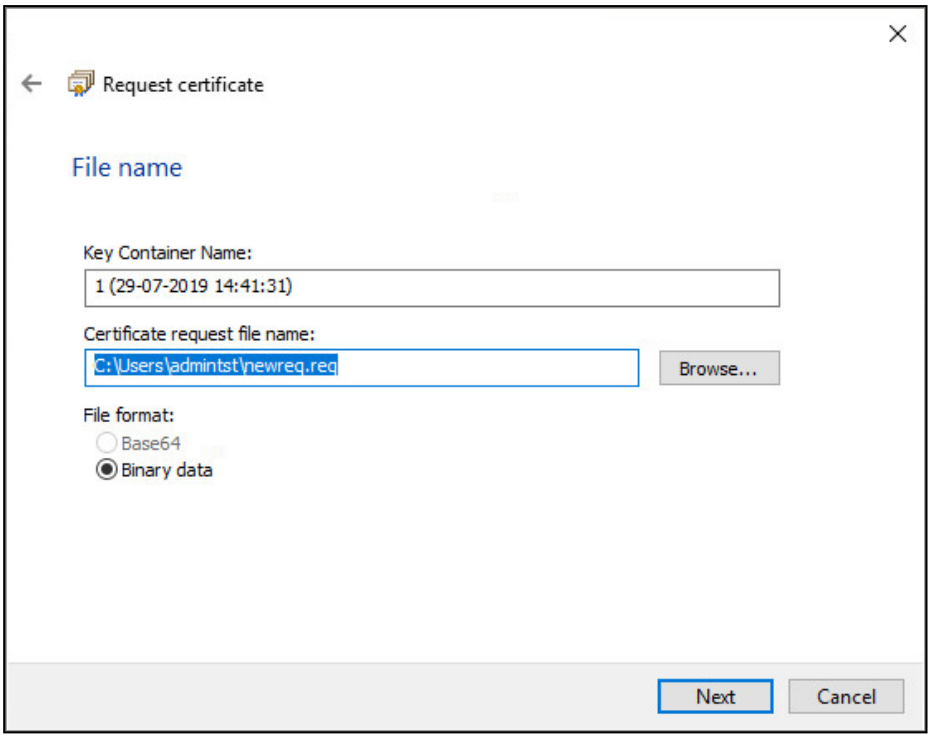
   If you have selected the **Extended set** in the **Key usage** box, the following dialog appears:



Note. If you have selected the **Standard set**, go to step **7**.

6. Specify the required parameters and click **Next**.

The **File name** dialog appears.



7. Specify the key container name.

Note. By default, the request is saved to a file with the **.req** extension and with the name containing the current Windows user's name and the current time and date.

To change the file destination, click **Browse** that is on the right of the respective field. In the File explorer, do the following:

- specify a drive (a folder) to save the file;
- type the request file name;
- click **Save**.

8. Click **Next**.

The **Completing the certificate request wizard** dialog box appears.

9. Click **Finish**.

The CSP generates the private key. Do the following:

- create a private key using a random number generator;
- select a key carrier;
- type the password for access to the key container.

Note. If you select the **Save password** check box, the password is saved to the computer's registry. After that, whenever you access the key container, the password is required.

The procedure depends on the CSP you use, the RNG and the key container for the key data. Follow the appearing instuctions.

For more information about the private key creation, see p. **26**.

After you finish the procedure, the finish message appears.

10. Click **OK** to finish the procedure.

Attention! If you selected the registry as the key container, we do not recommend that you perform any actions influencing the system software of your computer after creating the key data.

Transfer the created request file to the security administrator. To do this, you can use a public network, for example, to send the file via e-mail.

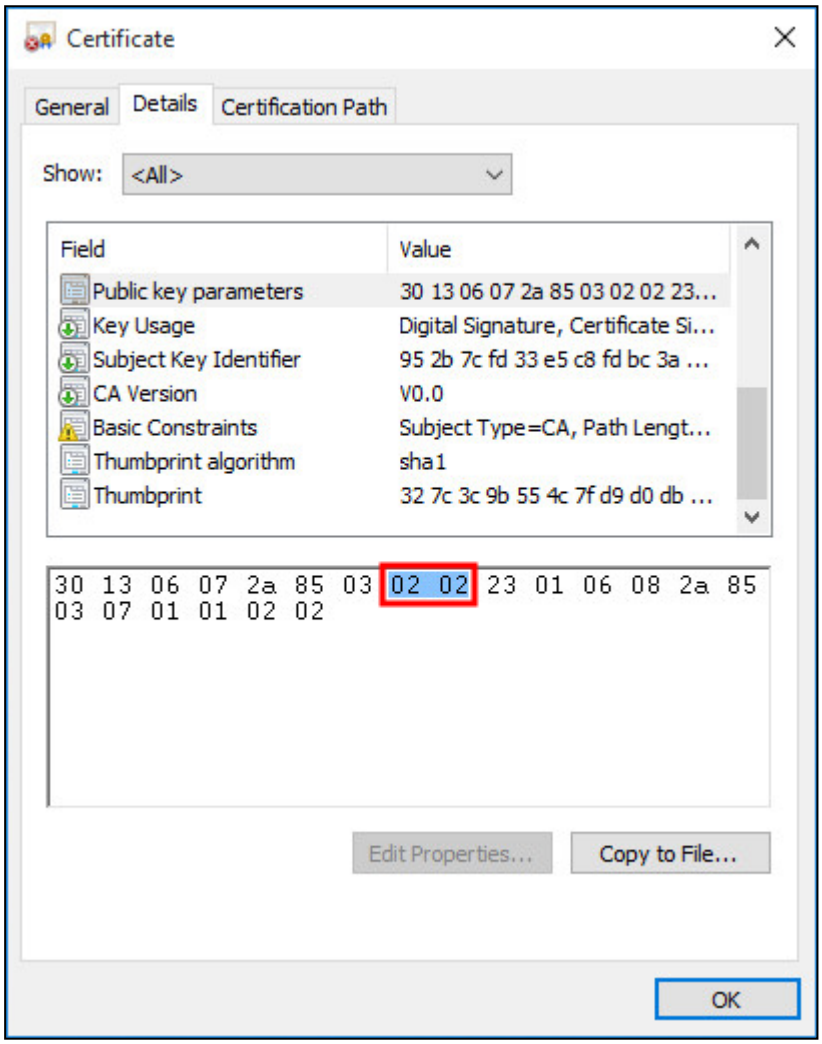
Note. If you want to send the request file using third-party CSP, open the request file using any text editor.

Ways to use CSP when generating a private key

You can find the procedures of user private key generation below (for more details, see p. **22**) as well as the ways to use the CryptoPro CSP and the Security Code CSP.

Attention! A certificate private key is valid for 1 year and 3 months by default. After the expiration date you cannot work using the old certificate. We recommend you to reissue the certificate.

When working with a third-party CSP, Continent-RA supports only keys created with the parameters 1.2.643.2.2.35.1, 1.2.643.2.2.35.2, 1.2.643.2.2.35.3, 1.2.643.2.2.36.0, 1.2.643.2.2.36.1. To verity the validity of a certificate, open the certificate store, find the required certificate and double-click it, then go to the **Details** tab and select **Public key parameters**. Make sure that the value of the eighth and ninth bytes is **02**.

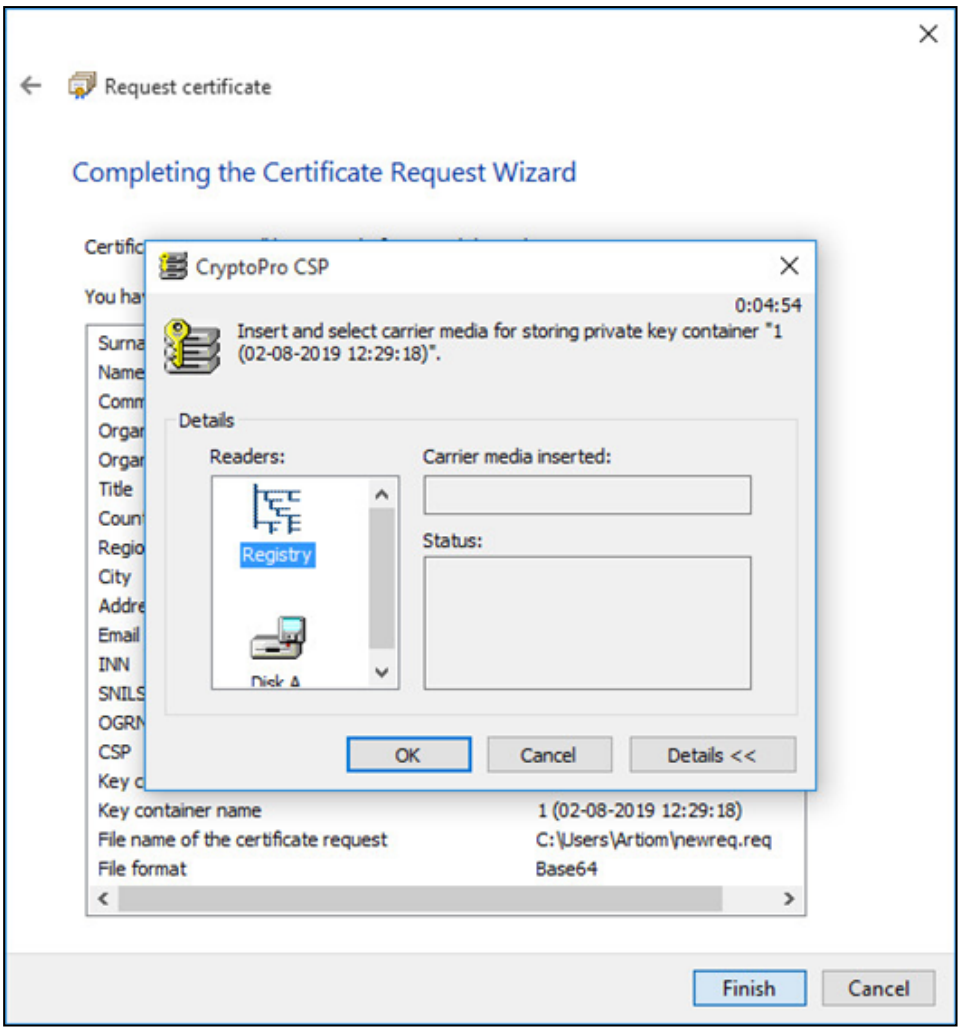


If the values are different, create a request for another certificate or get a new one from an external source.

CryptoPro CSP

To generate a private key:

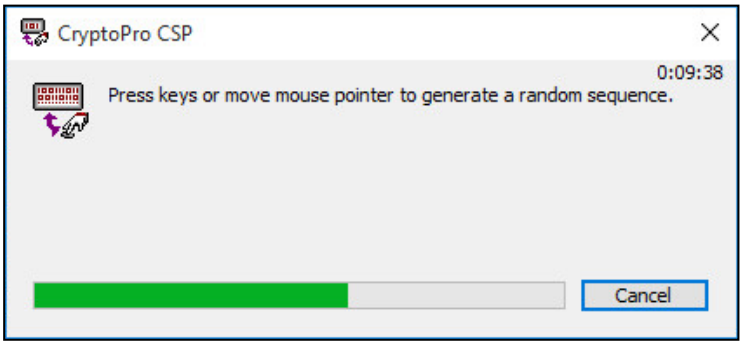
1. After you click **Finish** in the **Completing the Certificate Request Wizard** dialog box, the **CryptoPro** dialog box appears prompting you to select a carrier drive.



2. Insert an external drive, click **Details<<** and, in the **Readers** section, select the required carrier.
3. Click **OK**.

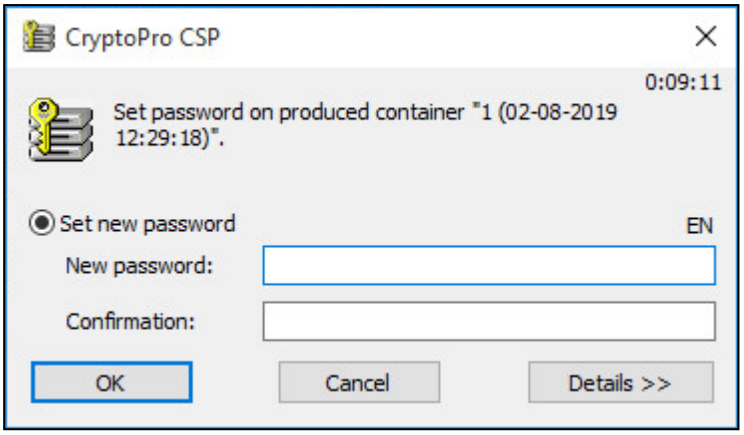
   A dialog box for gathering entropy appears as in the figure below.

Note. If Sobol RNG is configured for CryptoPro CSP, a dialog box for setting a password for a key container appears (see step **4**). Go to step **5**.



4. Follow the instructions on the screen and wait untill the key is generated.

   A dialog box for setting a password for a key container appears as in the figure below.



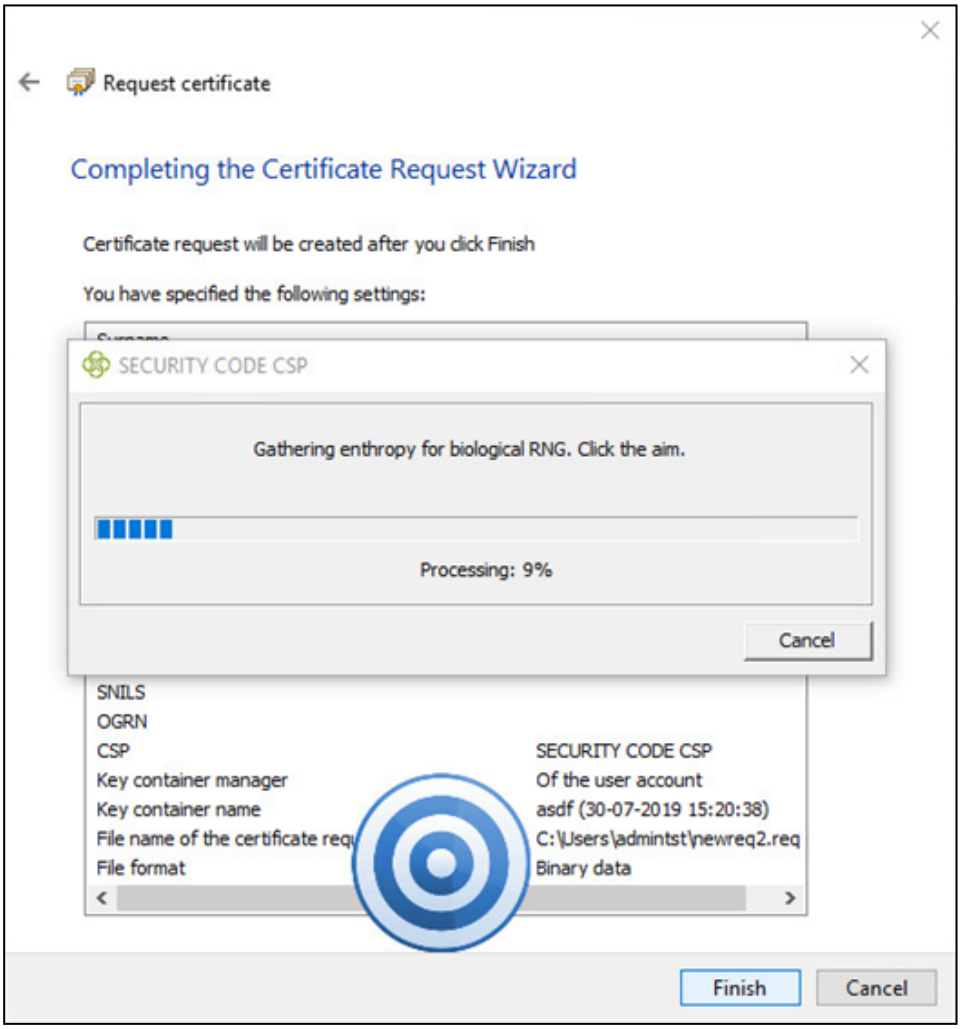
5. In the **New password** and **Confirmation** text boxes, enter a password for a key carrier. Click **OK**.

   A private key is being recorded to a key carrier. When the procedure is completed, you receive a message that the certificate request has been successfully created.

Security Code CSP

To generate a private key:

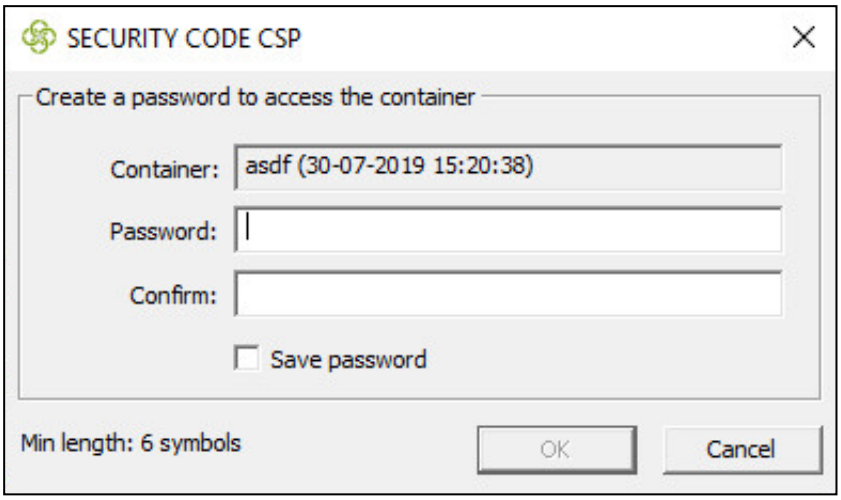
1. After you click **Finish** in the **Completing the Certificate Request Wizard** dialog box, the **Gathering entropy for RNG using human input** dialog box appears.



Note. If you use the Sobol physical RNG, entropy is gathered automatically, and the process is not displayed. Instead, the dialog box for creating a password appears. Proceed to step **3**.

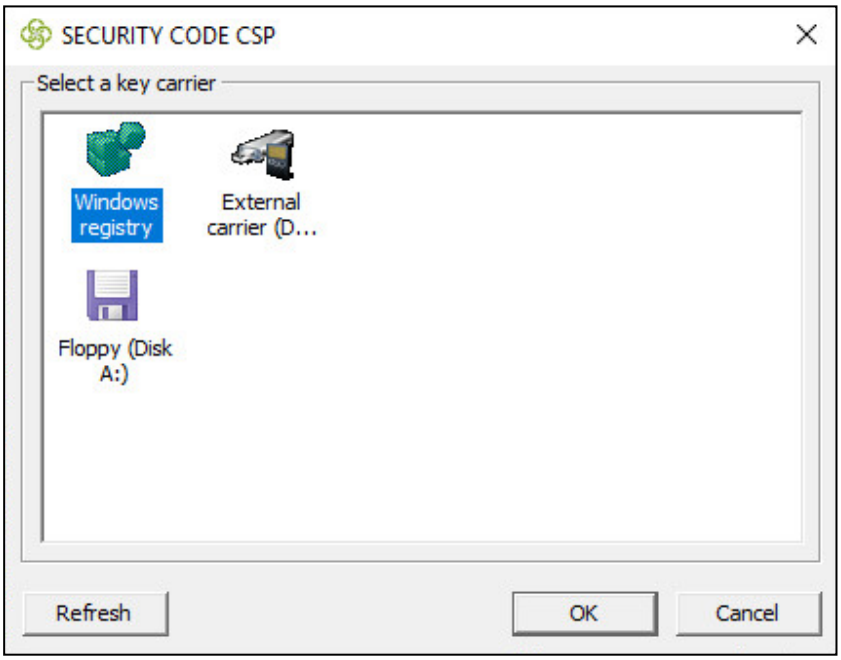
2. Follow the instructions and wait till entropy is gathered.

   After the procedure is finished, the **Create a password to access the container** dialog appears.



3. Type and confirm a password to access the key carrier and click **OK**.

   The **Select a key carrier** window appears.



4. Select the required key carrier and click **OK**.

Attention! If the names of the files stored on the removable drive you use match the names of the files you are to save onto the drive, then:

- files stored on the drive will be automatically renamed and saved;
- the files you are to save will be overwritten after you confirm the operation.

The request and the cryptographic container are being created. After the operation is completed, the respective message appears.

5. Click **OK** and remove the drive.

Note. If you need to send the contents of the file via a third-party CSP web interface, open the request file with any text editor.

Import certificates

To import a user certificate:

1. In the Continent-RA main menu, click **Certificates**, and then the **User certificates** tab.

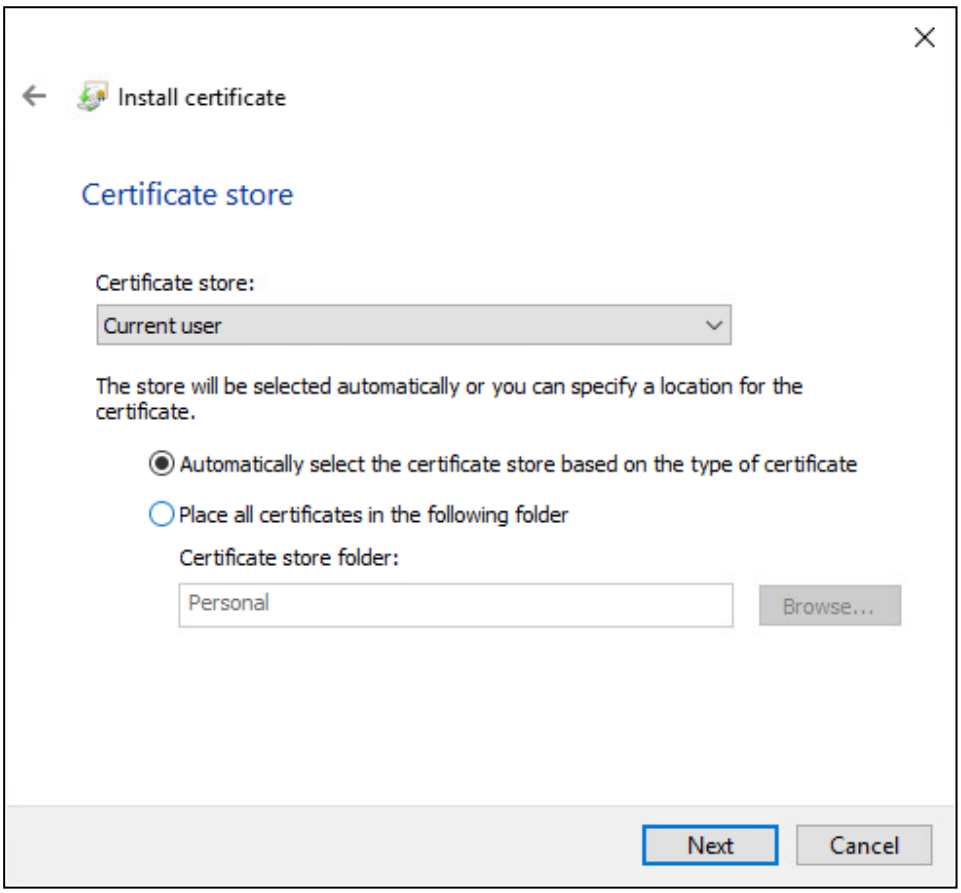
   In the display area, the list of the installed certificates appears.

2. Click **Import**.

   The **Imported file** dialog box appears.

3. In the **File name** text box, specify the path to the certificate file and the name of the file with **.cer** or **.p7b** extension and click **Next**.

   The **Certificate store** dialog box appears as in the figure below.



4. Do the following:

   - In the **Certificate store** drop-down list, select **Current User**.

     Attention! When you use a certificate to create a global profile, select **Local Machine**. For other certificates, we recommend using the certificate store selected by default.

   - Then, select **Place all certificates in the following folder** and click **Browse** to specify the certificate store.
   - Click **Next**.

   When you import a user certificate, the certificate private key carrier is requested. In the respective window, select the required carrier and click **Next**.

   Note. To import certificates bound to key containers correctly, you must have rights to write or edit the registry branch:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\MY\Keys
   HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MY\Keys

   The finish dialog box appears.

5. Review all the specified parameters and click **Finish**.

When you import a user certificate, the **Enter password** window appears. Enter the password and click **OK**.

Note. If you saved the password when creating a certificate request, the password is not required when you import the respective certificate.

The certificate installation to the specified store begins. After the operation is successfully completed, the respective windows appears.

6. Click **OK**.

To import a root or server certificate:

1. In the Continent-RA main menu, click **Certificates** and then a tab of the required certificate type.

   In the display area, the list of the installed certificates appears.

2. Under the toolbar, click **Import**.

   The **Open** window appears.

   Note. If you import a root certificates using Windows tools, specify the **Trusted root CAs** as a store and **Local computer** as a store type.

3. Specify the certificate file and click **Open**.

   The certificate installation begins. After the operation is successfully completed, the respective windows appears.

4. Click **OK**.

   Attention! When you connect to the Access Server using the **4.X** protocol, the connection is esteblished using the server certificate name.To translate the server IP address to network address after certificate import, edit the **hosts** file. After editing **hosts**, restart Continent-RA or the computer.

View certificate information

To view certificate information using Windows tools along with Continent-RA:

1. On the navigation panel, go to **Certificates** and click **Open store**.

   The certificate manager appears.

2. Open the required folder and elect the certificate.
3. Double-click the respective certificate in the list to view certificate data.

   The respective window appears.

To view certificate information:

1. On the navigation panel, go to **Certificates**, then, in the toolbar, select the required certificate tab.

   In the display area, the list of installed certificates appears.

2. Double-click the respective certificate in the list to view certificate data.

   The respective window appears.

   Note. You can export a certificate using Windows tools. To do so, in the **Certificate** window, click **Details** and then **Copy to file**.

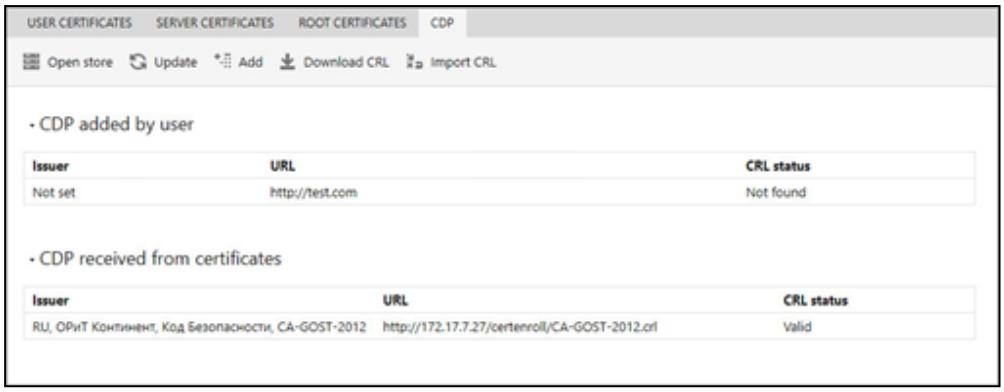
CRL management

Continent-RA allows you to get a CDP manually or automatically. Moreover, it automatically downloads a CRL to check the validity of certificates. You can also import a CRL manually.

Configure CDP

If certificates contain CDP data, Continent-RA parses it when importing a certificate. To download a CDP automatically, import a root or server certificate (see p. 31).

The following example illustrates the CDPs of root certificates imported to the system after installing CryptoPro CSP.



Note. For certificates issued on an Access Server/the Configuration Manager, the CRL is not required. To connect to an Access Server, disable CRL check in settings (see p. 34).

If imported certificates do not contain CDP, add the CDP list manually.

To configure the CDP list manually:

1. In Continent-RA settings, go to **Certificates**, and select the **CDP** tab.
   In the display area, the list of used CDP appears.
2. Click **Add** on the toolbar.
   The **Add CDP** dialog box appears.

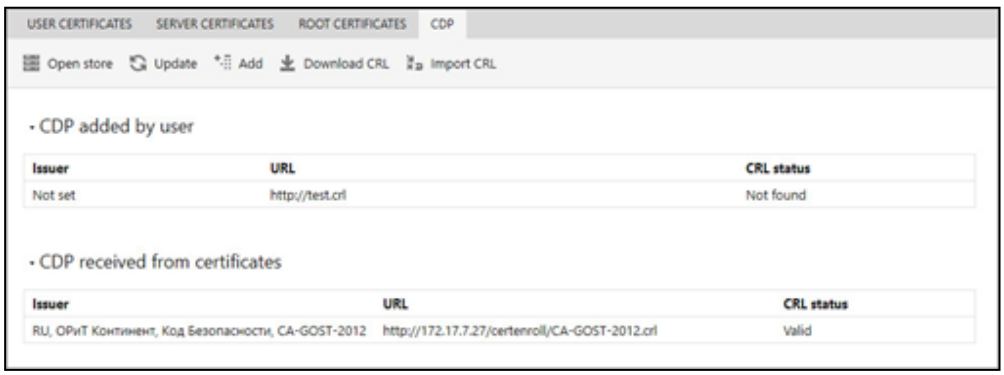
3. Enter the address of the required CDP and click **Save**.
   You will be returned to the CDP tab where you can see the added CDP with the respective parameters.
4. To edit or delete a CDP added by a user, select it in the list and click **Edit** or **Delete** on the toolbar.

Adding CRL

A CRL can be downloaded automatically in the following ways:

- by adding a CDP after importing certificates;
- according to a schedule set in Continent-RA settings (see p. **34**).

You can also add a CRL manually by importing a CRL file. If you could not upload a CRL or it was removed from the Continent-RA, the CDP table will display the CRL status.



To import a CRL file:

1. In Continent-RA, go to **Certificates**, and select the **CDP** tab.
   The CDP list appears.
2. Click **Import CRL** on the toolbar.
   The File Explorer appears.
3. Select the required CRL file and click **Open**.
   The uploading starts. After the successful uploading, the respective message appears.
4. Click **OK**.

To download a CRL file manually:

1. In Continent-RA, go to **Certificates** and select the **CDP** tab on the toolbar.
   The CDP list appears.

   Note. If the installed certificate has no CDP or a user did not download it earlier, add CDP to the list (see p. 32).
2. On the toolbar, click **Download CRL**.
   When the CRL is successfully downloaded, the respective message appears.
3. Click **OK**.

Continent-RA operation parameters

Continent-RA allows you:

- to configure software parameters;
- to create, edit and delete connection profiles in order to establish a secure connection and exchange encrypted data with an Access Server.

Continent-RA uses a two-way authentication to establish a connection. An Access Server checks a user certificate, whereas Continent-RA checks an Access Server certificate that must be previously imported to the system.

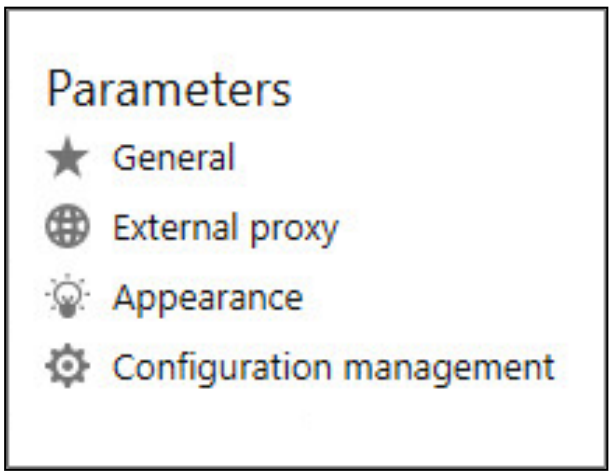
The authentication can be configured in two ways:

- automatically after a user imports a configuration file containing all required settings;
- by configuring parameters in connection profile settings manually.

There are two ways of configuring manual authentication mode:

- full configuration (strict trust mode);
- partial configuration (issuer trust mode).

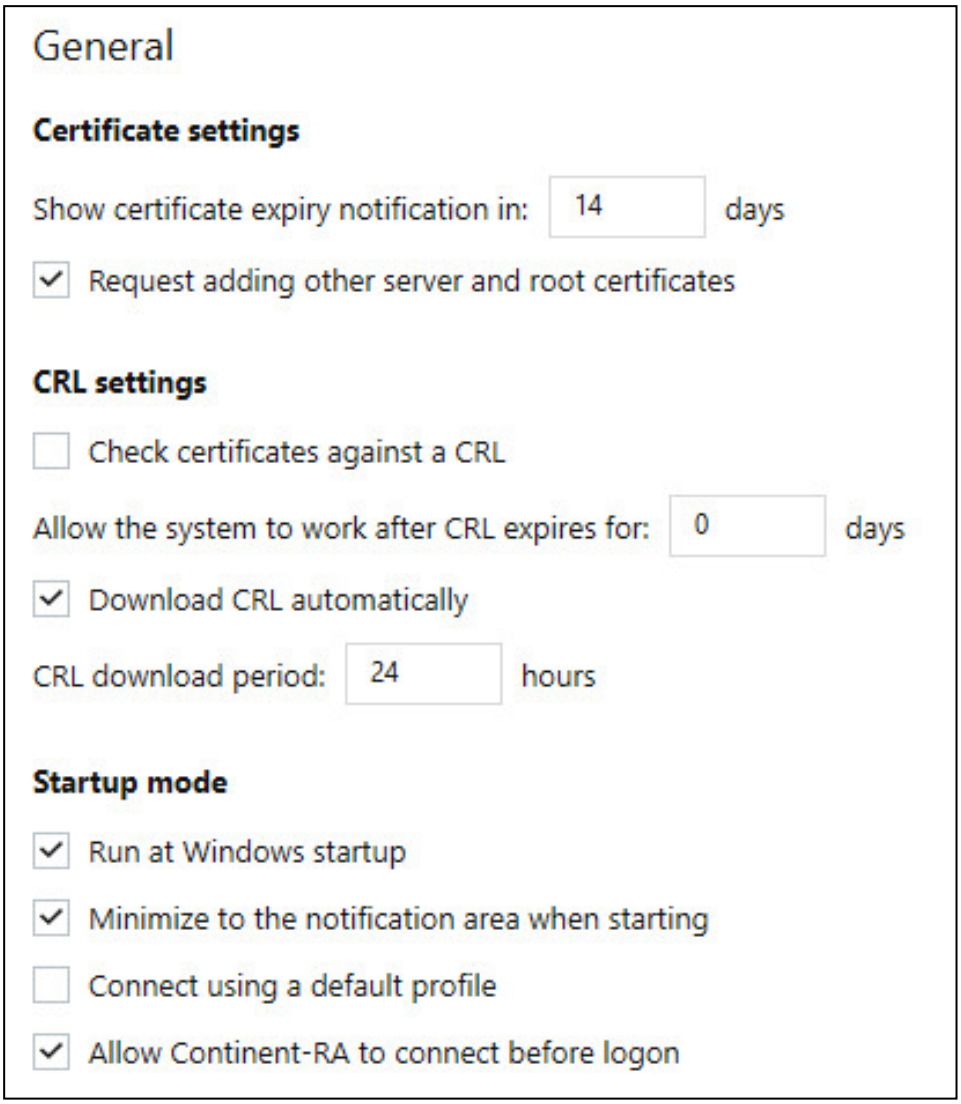
If you want to configure settings of Continent-RA, go to **Parameters** on the navigation panel. The list of parameter groups appears on the right.



General settings

To configure Continent-RA:

1. In **Parameters**, select **General**.
   The respective submenu appears in the display area.



2. Set a time period for receiving a warning message about user certificate expiration.
3. If an certificate issuer is trusted, select the **Request adding other server and root certificates** check box to add an Access Server to the list of trusted resources when you connect to it for the first time.

   Attention! For proper operation of Continent-RA, you need to import an issuer (a root certificate) of a server certificate.

4. If the information security policy of the company stipulates a strict trust mode, clear the **Request adding other server and root certificates** check box.
5. To check certificates against a CRL, select the respective check box.
6. To configure automatic download period for a CRL certificate, select **Download CRL automatically** and specify the required period in the respective text box.

   Attention! To edit CRL settings, you must run Continent-RA as an administrator. A user with administrator rights in Windows Server 2016 can edit settings once.

7. If necessary, select **Run at Windows startup** (selected by default) to run Continent-RA at Windows startup.

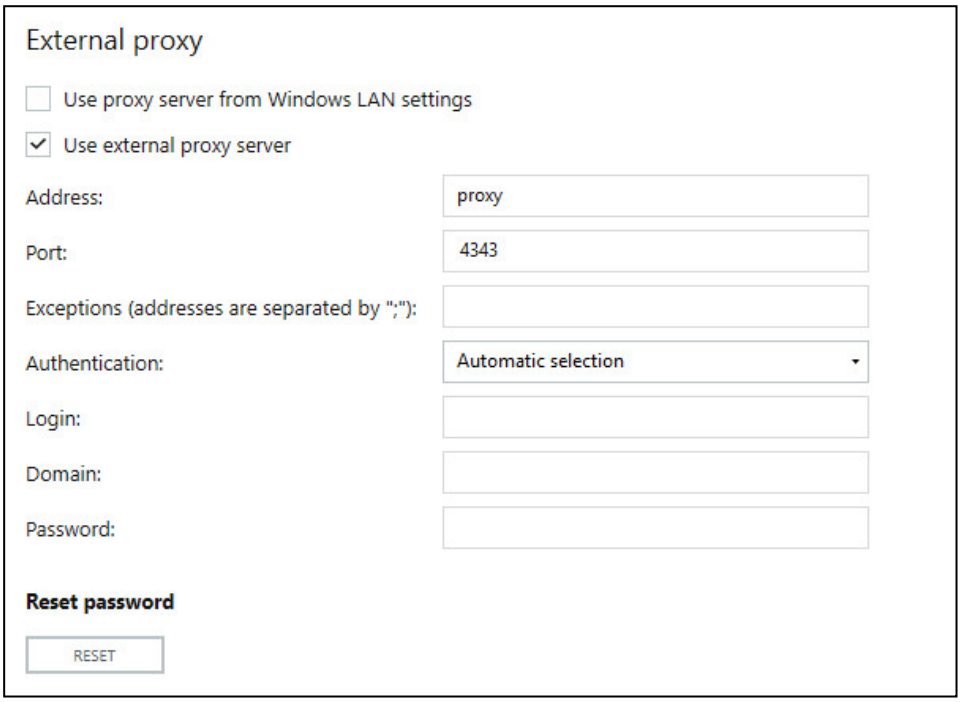
8. Select **Minimize to the notification area when starting** (in the Windows notification area default).
9. To automatically connect using a default profile, select the respective check box. If you want to select a profile manually, clear the check box.

External proxy

To configure the Internet connection using an external proxy server manually:

1. In **Settings**, select **External proxy**.

   The respective parameters appear.



2. Select **Use external proxy server**.
3. In the **Address** text box, enter the IP address or the domain name of a proxy server, in the **Port** text box — its port.

   Note. You need to restart Continent-RA for the configuration changes to be applied.

4. If necessary, specify exceptions (the list of IP addresses or domain names separated by semicolon **;**) in the respective text box.
5. Select the **Authentication** type and specify the required information.
6. To finish configuring external proxy and apply edited parameters click **Save**.

To configure the Internet connection using an external proxy server automatically:

1. In **Settings**, go to **External proxy**.

   The respective parameters appear.

2. Select **Use proxy server from Windows LAN settings**.

   Note. This parameter is selected by default. Select it again if you have configured the connection using an external proxy server manually.

   The fields are disabled and cannot be edited. Continent-RA will automaticlly apply the default system parameters to configure proxy server parameters.

   Note. If you change the DNS server address, Continent-RA will apply changes only after you restart the program. If you change proxy server settings, changes will be applied after you restart the program.

3. To apply changes, click **Save**.

Appearance

To configure the Continent-RA appearance:

1. In **Settings**, select **Appearance**.
   The respective settings appear.
2. Select the required color theme by clicking the respective option buttons.

Configuration management

You can import/export a configuration using Continent-RA

Attention! Root, server and user certificates are not migrated during configuration import/export. If necessary, import/export them manually. Exporting a global profile configuration, export the respective user certificate.

To export Continent-RA configuration:

1. In **Settings,** select **Configuration management** and click **Export configuration**.
   The **Save as** dialog box appears.
2. Select the requried destination folder and click **Save**.
   You receive a message about successful configuration export.
3. Click **OK**. You are returned to **Settings**.

To import Continent-RA configuration:

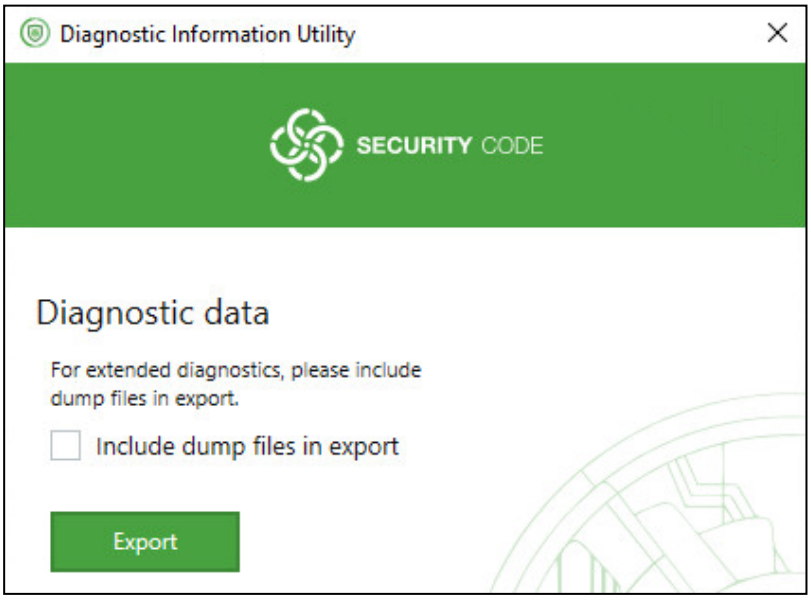
1. In **Settings** , select **Configuration management** and click **Import configuration**.
   The **Open** dialog box appears.
2. Select the requried file and click **Open**.
   You receive a message about successful configuration import.
3. Click **OK**. You are returned to **Settings**.

Attention! To import/export a global profile configuration, run Continent-RA as administrator.

Audit

To collect diagnostic information:

1. Open the **Start** menu, go to **All Apps** | **SECURITY CODE** | **Continent-RA** | **Collection of diagnostic information**.
   The respective dialog box appears.



Note. If you also want dump files to be collected, select the respective check box.
If you include dump files to the export file, it takes more time.

2. Click **Export**.
   The File Explorer appears.
3. Specify the file path and click **Save**.
   If the file is exported successfully, you receive the respective message.

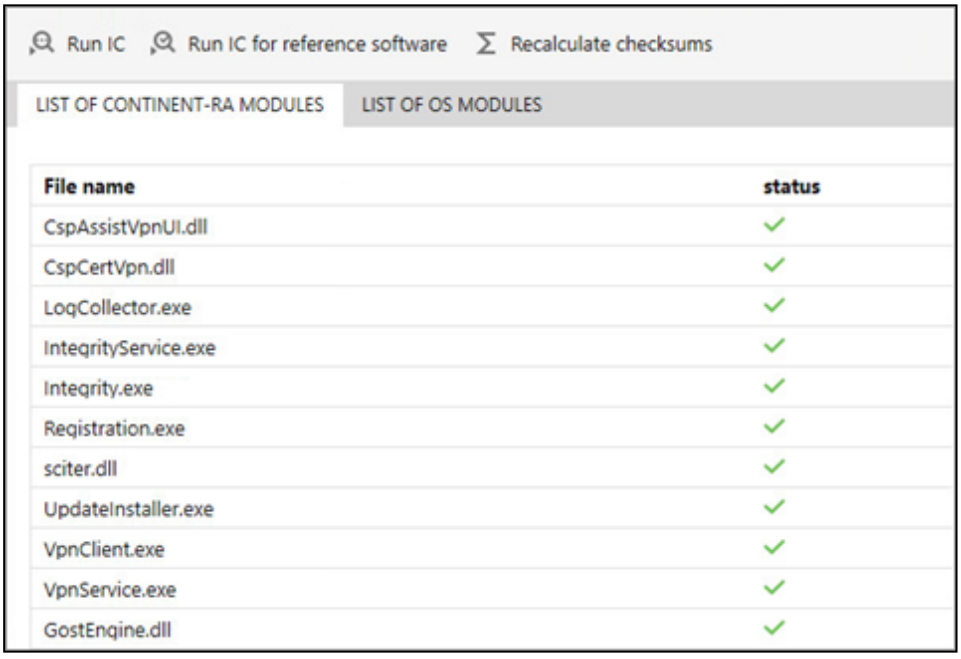
Integrity check

The integrity check is performed at the first start of Continent-RA according to the schedule in the configuration file or using the **Continent-RA Integrity Check** utility.

Attention! To edit the integrity check settings, run the utility as administrator.

To run Continent-RA Integrity Check:

- In the **Start** menu, go to **All Apps** | **SECURITY CODE** | **Continent-RA** and run **Continent-RA Integrity Check**.
  The integrity check will start automatically. The dialog box with integrity check results appears.



To check the integrity of the Continent-RA system files:

1. In the main window of **Continent-RA Integrity Check**, click **Run IC** on the toolbar.

   Attention! To recalculate checksums, you must run **Continent-RA Integrity Check** as administrator.
2. Click **Yes**.
   The system will check each file from the module list of Continent-RA and the operating system. The checked files will be marked with ☑. After the integrity check is successfully finished, you will receive the respective message.

If an error appears during the integrity check, the incorrect file will be marked with the respective icon ( ). To repair software, use the distribution kit (see p. **11**).

To check the integrity of the Continent-RA distribution kit files:

1. In the main window of **Continent-RA Integrity Check**, click **Run IC for reference software** on the toolbar.

   The dialog box prompting you to specify the path to the distribution kit folder appears.

2. Click [...] and specify the path.

   The system will check each file from the distribution kit. After the integrity check is successfully finished, you will receive the respective message.

After you have updated the program and restarted the operating system, you will receive an error message. The system will prompt you to recalculate checksums of the system files and resume working. If you confirm the action, **Continent-RA Integrity Check** automatically recalculates checksums and starts the Continent-RA. If you do not confirm the action, Continent-RA does not start and you cannot continue working.

To recalculate system file checksums of the Windows operating system:

1. In the main window of **Continent-RA Integrity Check**, click **Recalculate checksums** on the toolbar.

   Attention! To recalculate checksums, you must run **Continent-RA Integrity Check** as administrator.

   The dialog box prompting you to confirm the action.

2. Click **Yes**.

   The system will check each file from the module list of Continent-RA and the operating system. The checked files will be marked with ☑. After the integrity check is successfully finished, you will receive the respective message.