



Continent Enterprise Firewall Version 4

Authentication



© **SECURITY CODE LLC, 2024. All rights reserved.**

All rights to operation manuals are reserved.

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

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

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

Table of contents

List of abbreviations	4
Introduction	5
Overview	6
Authentication settings	7
How the Authentication Portal works	7
How Transparent Kerberos Authentication works	8
Identification Agent	9
How the Identification Agent works	9
Install the Identification Agent	9
Uninstall the Identification Agent	12
Run the Identification Agent	13
Configure the Identification Agent	13
Connect to the Security Gateway	14

List of abbreviations

AD	Active Directory
DNS	Domain Name System
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
SPNEGO	Simple and Protected GSS-API Negotiation Mechanism
TCP	Transmission Control Protocol
VPN	Virtual Private Network

Introduction

This manual is designed for users of Continent Enterprise Firewall, Version 4 (hereinafter — Continent). It contains information about the user authentication configuration.

See Continent Enterprise Firewall. Version 4. Administrator guide. Firewall before reading this guide.

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.

Overview

Secure operation of the Continent in the standard mode is provided by its correct configuration by the administrator (see Continent Enterprise Firewall. Version 4. Administrator guide. Authentication).

Continent 4 provides identification and authentication of users within a protected network by:

- the Authentication Portal (see p. 7);
- the Identification Agent on an end-user device (see p. 9);
- Transparent Kerberos (Single Sign-On) authentication (see p. 8).

You can create a user account using the Security Management Server local database or import it from AD.

User access to the Internet is granted to users or user groups after successful identification and authentication procedures through the interfaces of the Identification Agent or Authentication Portal.

The security settings of Continent are not available to the user.

Access is granted to groups of users by means of IP filtering.

The information about registered users and groups of users is stored in the Security Management Server database. The information about authenticated users is stored on a Security Gateway.

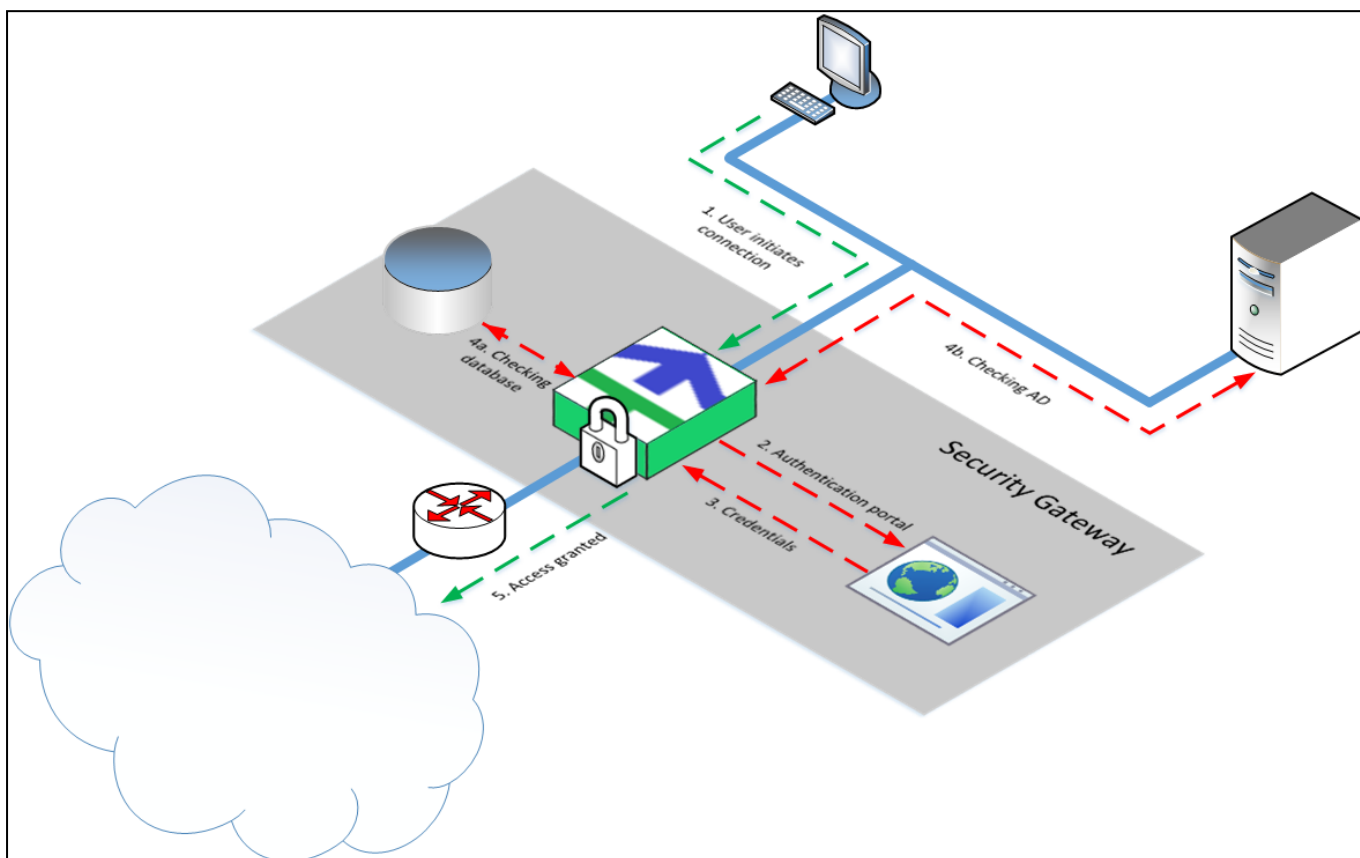
When connecting to the Firewall, a user is authenticated on the Security Gateway using non-cryptographic means via user credentials.

A Security Gateway and a connected workstation exchange data over HTTPS.

Authentication settings

How the Authentication Portal works

The Authentication Portal is one of the Security Gateway components that authenticates users through the web interface.



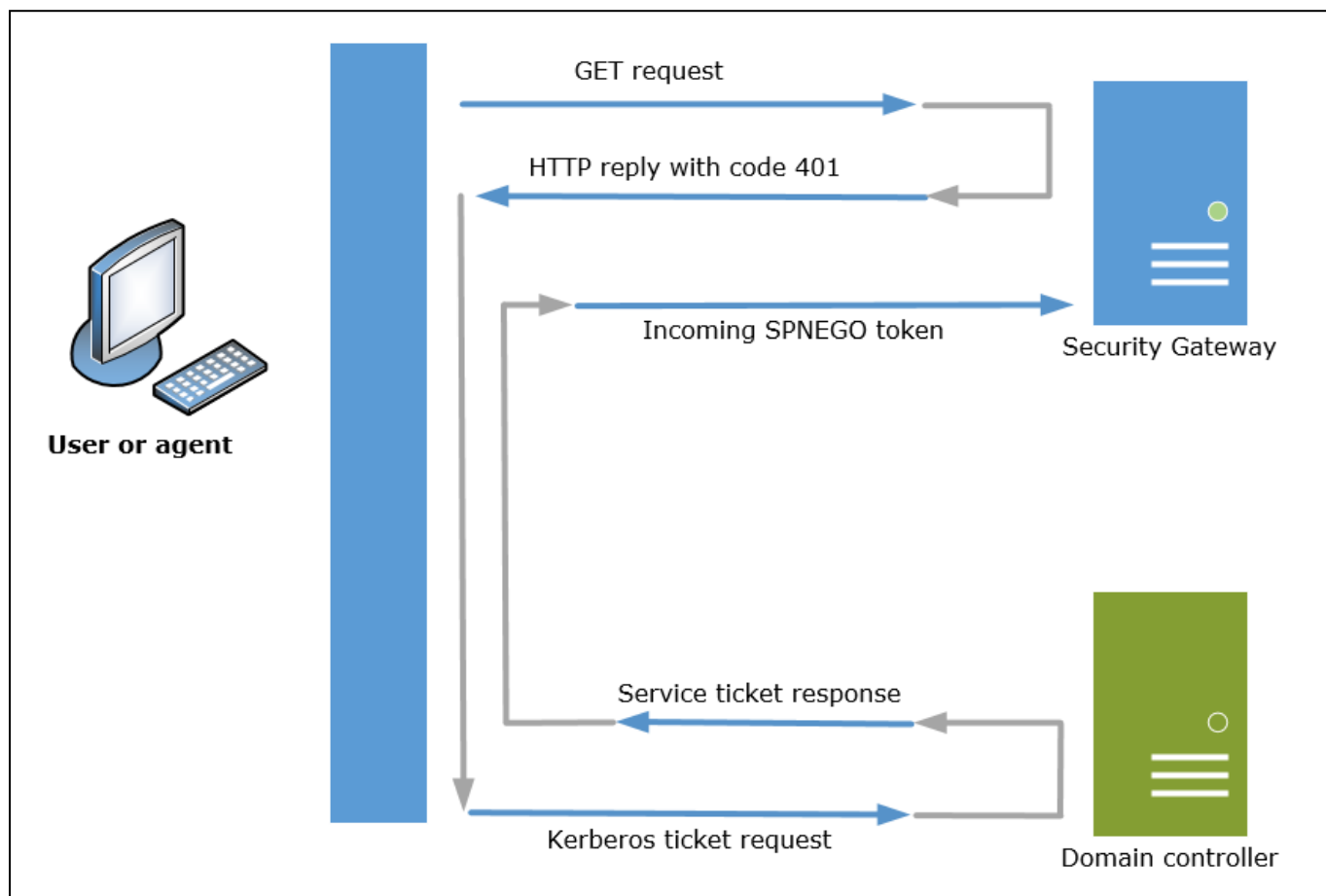
While sending an HTTP (TCP/80) or HTTPS (TCP/443) **[1]** request to a web page, a user is redirected to the Authentication Portal **[2]** if there are respective access control rules for the network from which users are redirected to the portal. If you open a web page over HTTPS, the intermediate certificate is required to establish a secure connection to a Security Gateway. The user enters his or her credentials. The credentials are sent to the Security Gateway **[3]**. The Security Gateway checks the Security Management Server local database for these credentials and if they are still valid **[4a]**. If the username looks like **username@domain**, the request is redirected to the AD server of the respective domain (for example, **usertst1@local.host**). The check procedure is repeated **[4b]**. If the match is found and the credentials are proved to be valid, then the respective data is sent to the Security Gateway, the respective temporary firewall rule is created and the user is granted access to the resource **[5]**.

How Transparent Kerberos Authentication works

Transparent authentication means that the domain user does not receive repeated requests for authentication when accessing network resources. In this case, a user specifies the domain login and password only once, when logging in to the operating system. When the user tries to access network resources, authentication is performed automatically.

You can use Kerberos authentication for both direct access and access via the Continent proxy server.

The SPNEGO protocol is used to ensure the mechanism of browser transparent authentication in Continent. You can see the whole authentication process in the figure below.



1. A user logs on to a Windows domain from the workstation and attempts to access the Internet using a web browser. The web browser sends an HTTP request which is intercepted by a Security Gateway.
2. The Security Gateway intercepts the client's request and sends back an HTTP response with a **401 (Unauthorized)** code and the **WWW-Authenticate: Negotiate** authorization header.
3. The web browser recognizes the **Negotiate** header. Then, a search for the Security Gateway name starts in the DNS, using which a service principal name (SPN) is found.
4. Using the SPN, the local system authentication service requests a Kerberos ticket from the key distribution center (KDC). It begins the Kerberos authentication sequence, an exchange of data between the client and the KDC. As a result, the client receives a service ticket (ST), based on which the Security Gateway will trust it.
5. The web browser resends the original HTTP request, but this time the authentication user data is contained in an encrypted Kerberos ticket encapsulated in a SPNEGO token, which is passed in the HTTP authorization header.
6. The Security Gateway identifies the incoming SPNEGO token in the request, then extracts the information from the Kerberos service ticket which contains all the information needed for authentication.
7. Transparent authentication can be used both with the browser authentication via the Authentication Portal page and separately.

Identification Agent

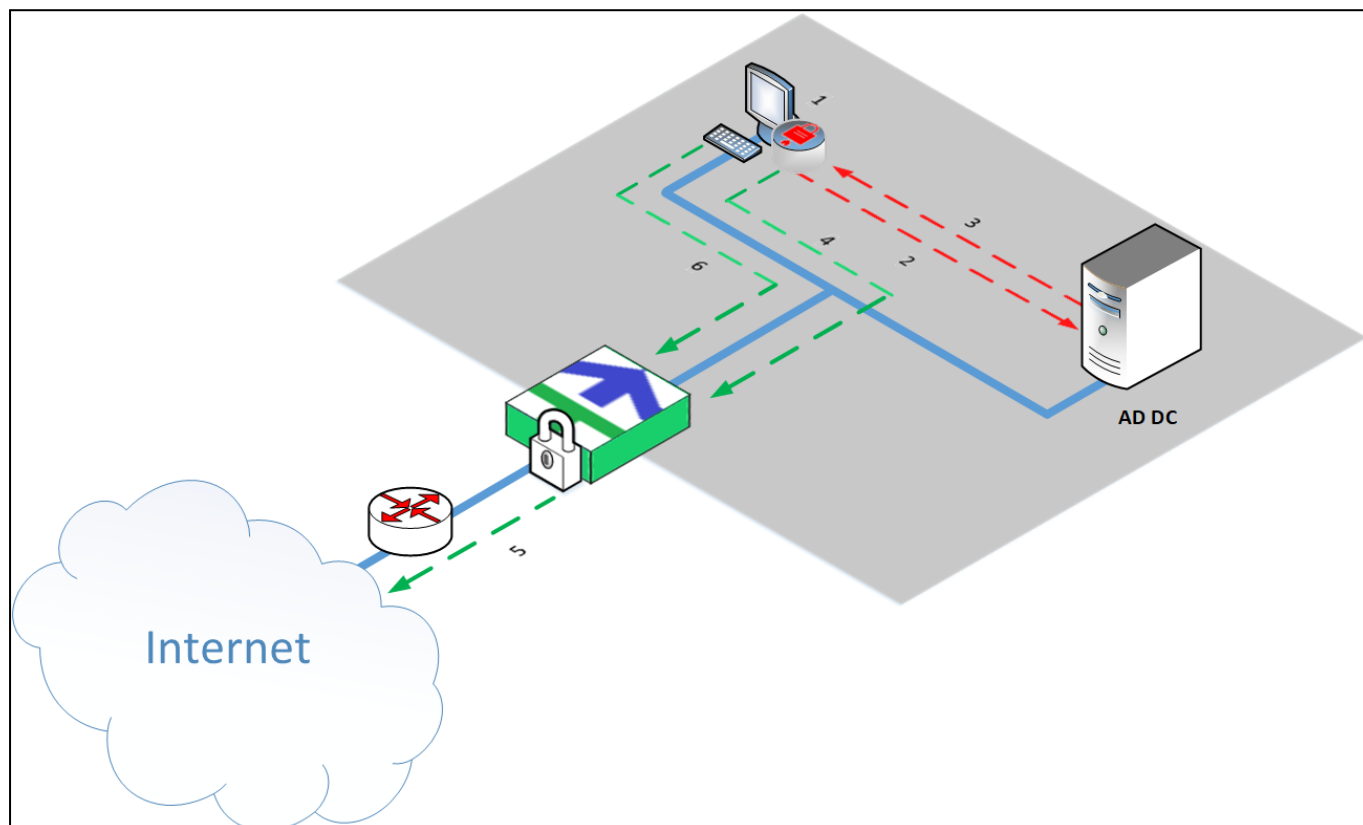
The Identification Agent is installed on a computer under the Windows OS.

Before enabling the Identification Agent, configure the Authentication Portal.

To enable the Identification Agent with AD, configure LDAP interconnection.

How the Identification Agent works

The Identification Agent is a software that is installed on workstations to connect to the Security Gateway and to verify user credentials.



To get access to the Internet, a user runs the Identification Agent and enters his or her credentials [1]. Then, the agent initiates the identification in AD [2]. The agent receives a confirmation for the identification [3]. When the user attempts to access the Internet [4] for the first time, the agent sends the confirmation to AD and receives a permission for connection. The user is granted access to the Internet according to the Security Gateway access control rules [5]. When the user attempts to access the Internet again [6], the agent checks the cache for a permission. If the permission has expired, the Identification Agent will request it from AD again.

A user within the protected network is granted access to the Internet and the local network resources if the following requirements are met:

- user's credentials are confirmed and valid;
- there are access control rules for this user.

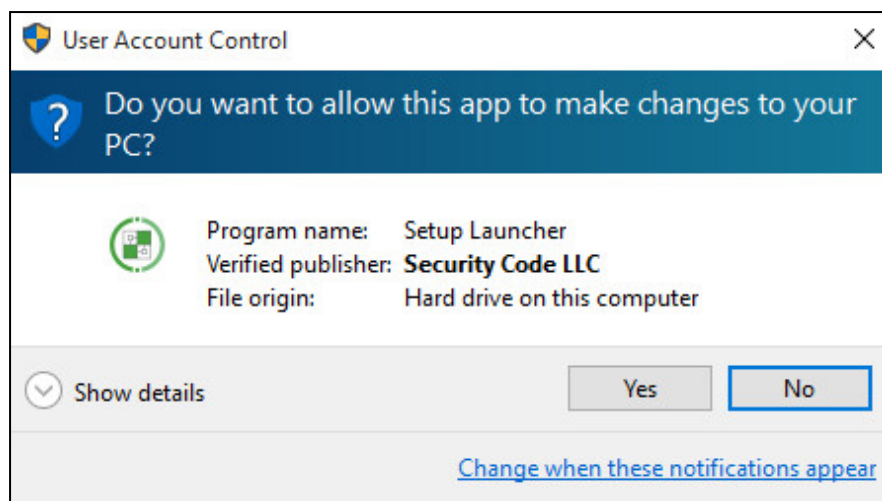
Note.

Identification Agent settings do not depend on Authentication Portal settings. Only a personal certificate connected in the Authentication Portal settings is used.

Install the Identification Agent

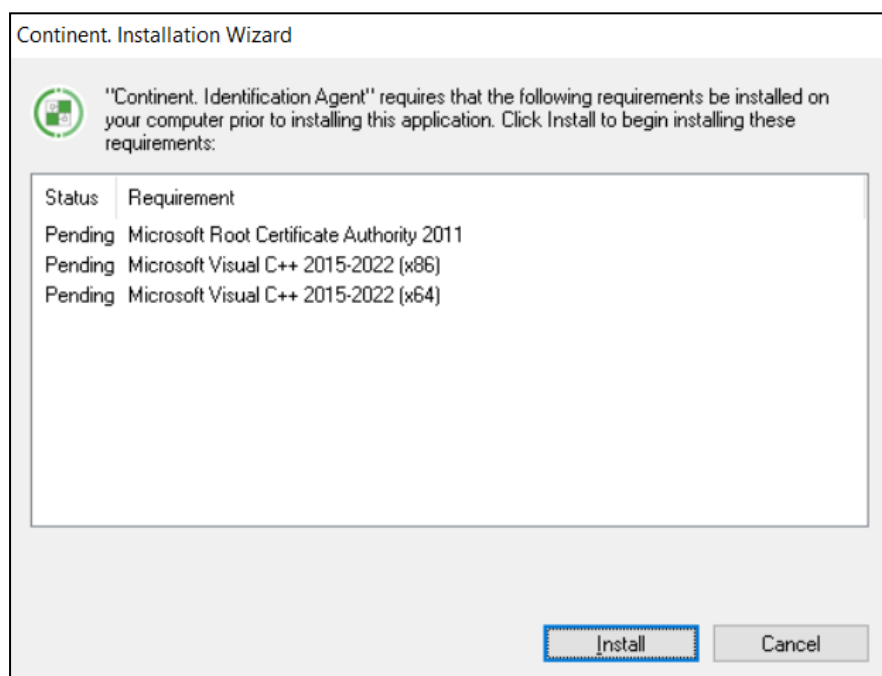
To install the software:

1. Log on to the system as an administrator.
2. Insert the installation disk in the disk drive and, in the distribution folder, run **setup.exe**. Allow the program to make changes to the computer if necessary.

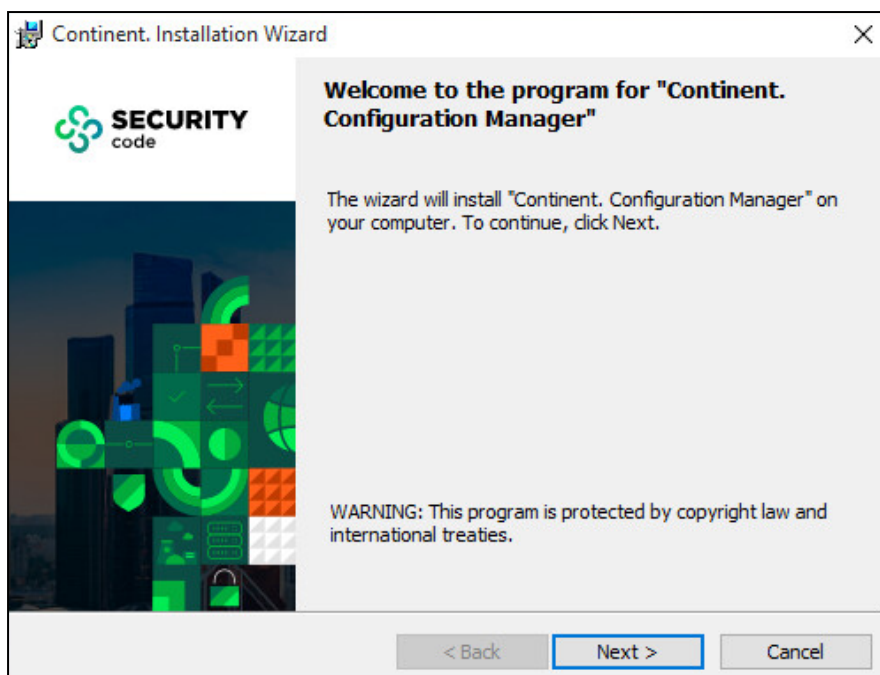


3. Before installing the Identification Agent, make sure the components that are required for its correct operation are installed.

The **Installation Wizard** appears as in the figure below.

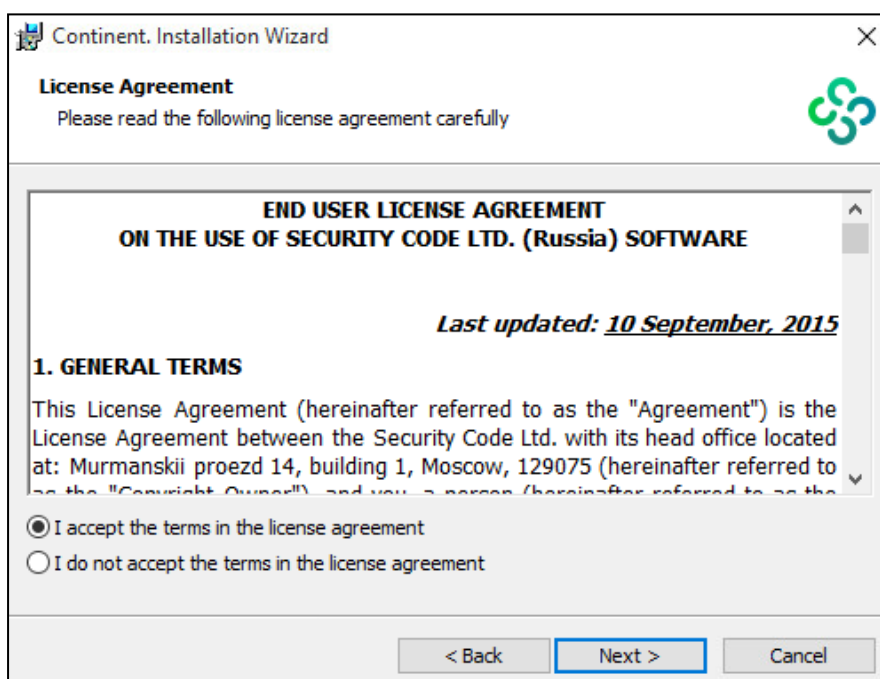


The **Continent. Installation Wizard** dialog box appears.



4. Click **Next** to continue.

The license agreement appears as in the figure below.



5. Read the license agreement. If you accept the terms, select the **I accept the terms in the license agreement** check box and click **Next**.

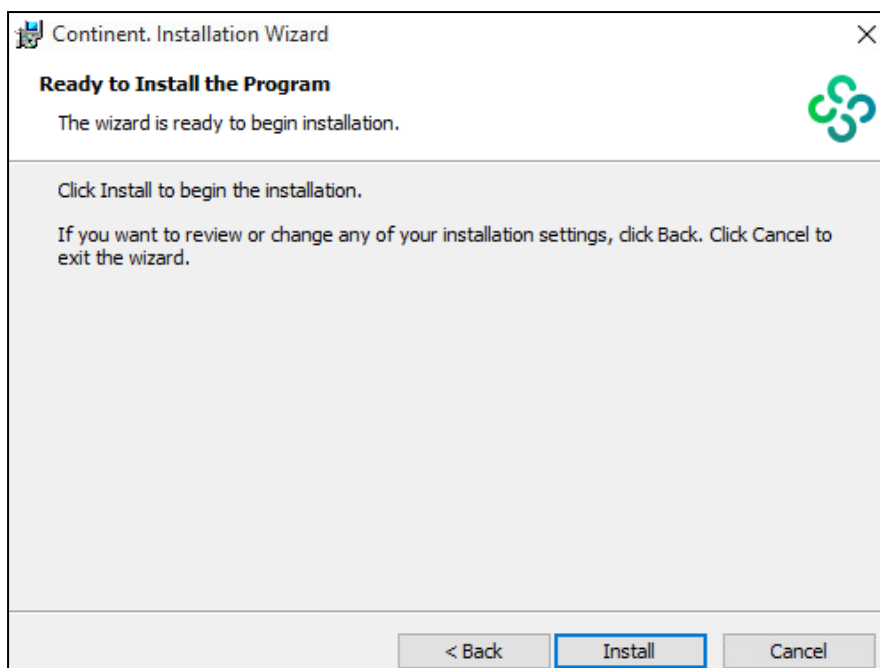
In the appeared dialog box, specify a destination folder for the program files.

Note.

By default, the installation wizard copies files to `\\Program files\\Security Code\\User authentication`. To install the program to another folder, click **Browse** and specify the required folder in the appeared dialog box.

6. Click **Next**.

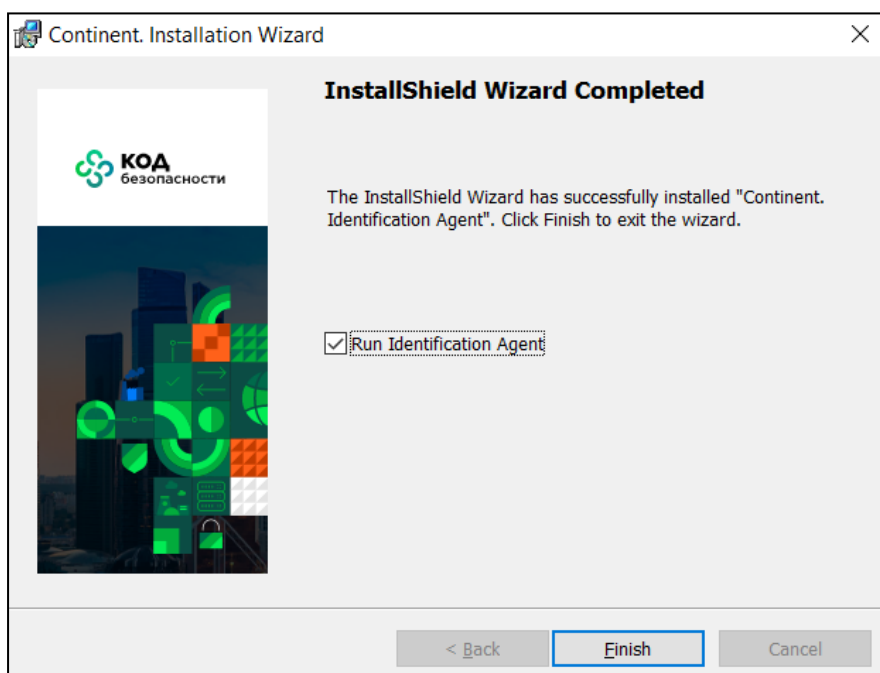
The **Ready to Install the Program** dialog box appears.




7. Click **Install.**

The installation wizard copies files to the destination folder. The appearing messages display information about the installation status.

After the successful installation, you receive the respective message.



8. If you want to start the program after the installation, select the **Run Identification Agent check box and click **Finish**.**

In the system control area, the following icon appears: .

Uninstall the Identification Agent

To uninstall the software:

1. In the Windows Start menu, go to **Control panel** and select **Programs and Features**.
2. Select **Continent. Identification Agent** and then click **Uninstall**.

After performing preparatory actions, the uninstallation dialog box appears.

3. Click **Next.**

The uninstallation confirmation dialog box appears.

4. Click **Uninstall.**

The program deletes files. After the successful uninstallation, you receive the respective message.

5. Click **Finish.**

Run the Identification Agent

To run the software manually:

- Go to the Windows Start menu, select **All apps**, expand the **Security Code** folder and select **Identification Agent**.

As the program runs, the icon of the program appears in the Windows tray.

To make the software run at startup:

- In the Windows tray, right-click the **Identification Agent** icon and select **Settings**.

The respective dialog box appears.

- Select the **Start automatically agent** check box and click **OK**.

Configure the Identification Agent

To configure connection on a user's workstation:

- In the Windows tray, right-click the **Identification Agent** icon.

- Click **Settings**.

The respective dialog box appears as in the figure below.

Note.

An untrusted server means:

- the server certificate is signed with an untrusted root certificate;
- the certificate is expired;
- the certificate is not a server certificate.

Settings

Preferences

- ☒ Connect on setup-up
- ☒ Auto reconnect after failure
- ☒ Block connections to untrusted gateways

Server

Gateway:
Example: access-server.local

Connection timeout in seconds:

Connection retry attempts:

Delay between retries in seconds:

Options

Taskbar:

☒ Start automatically agent

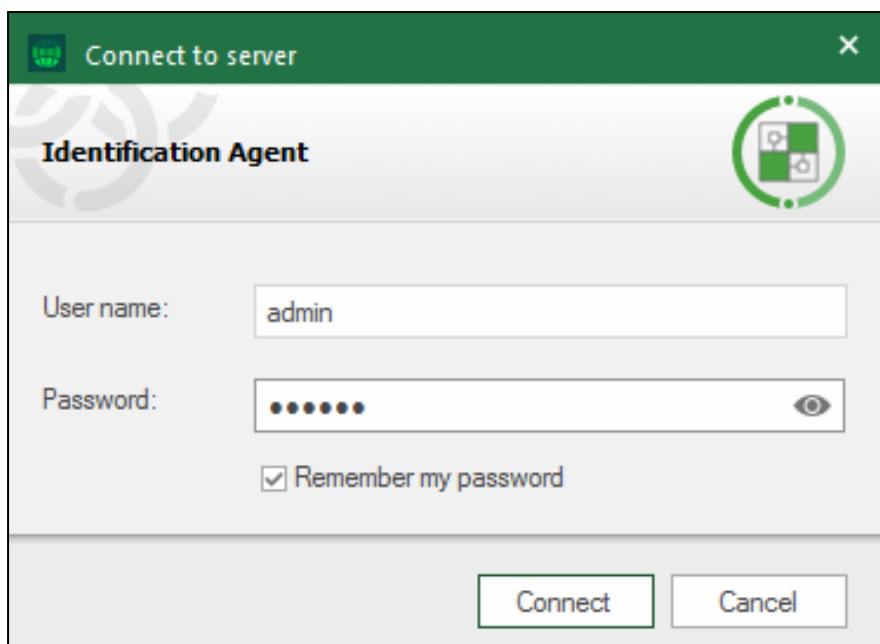
OK **Cancel**

3. In the **Gateway** text box, enter the domain name of the required AD server.
4. Select the required check boxes and specify the required parameters. The connection timeout value can be between **5** and **60**, the number of connection retry attempts is between **1** and **5**, the delay between retries is between **1** and **60**.
5. Click **OK** to save the settings.

Connect to the Security Gateway

To connect to the Security Gateway:

1. Right-click the **Identification Agent** icon in the Windows tray and select **Connect**.
The dialog box appears as in the figure below.





2. Enter the credentials and select the **Remember my password** check box if necessary.

Note.

To verify user credentials on the AD server, specify the user name and domain separated by @ (for example, **usertst1@local.host**).

3. Click **Connect**.

During the connection, the color of the  icon indicator switches from red to green and flickers. As soon as the connection is established, the indicator stops flickering, and the icon turns green: .

If all procedures are performed correctly, a user is granted access to the resources beyond the Firewall.