SECURITY code

Continent Enterprise Firewall
Version 4

Authentication

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

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

Introduction

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

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

Users can access external resources upon their successful identification and authentication.

Continent 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. **8**);
- the Transparent Kerberos (Single Sign-On) authentication (see p. **9**).

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

Access is granted to groups of users by means of 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.

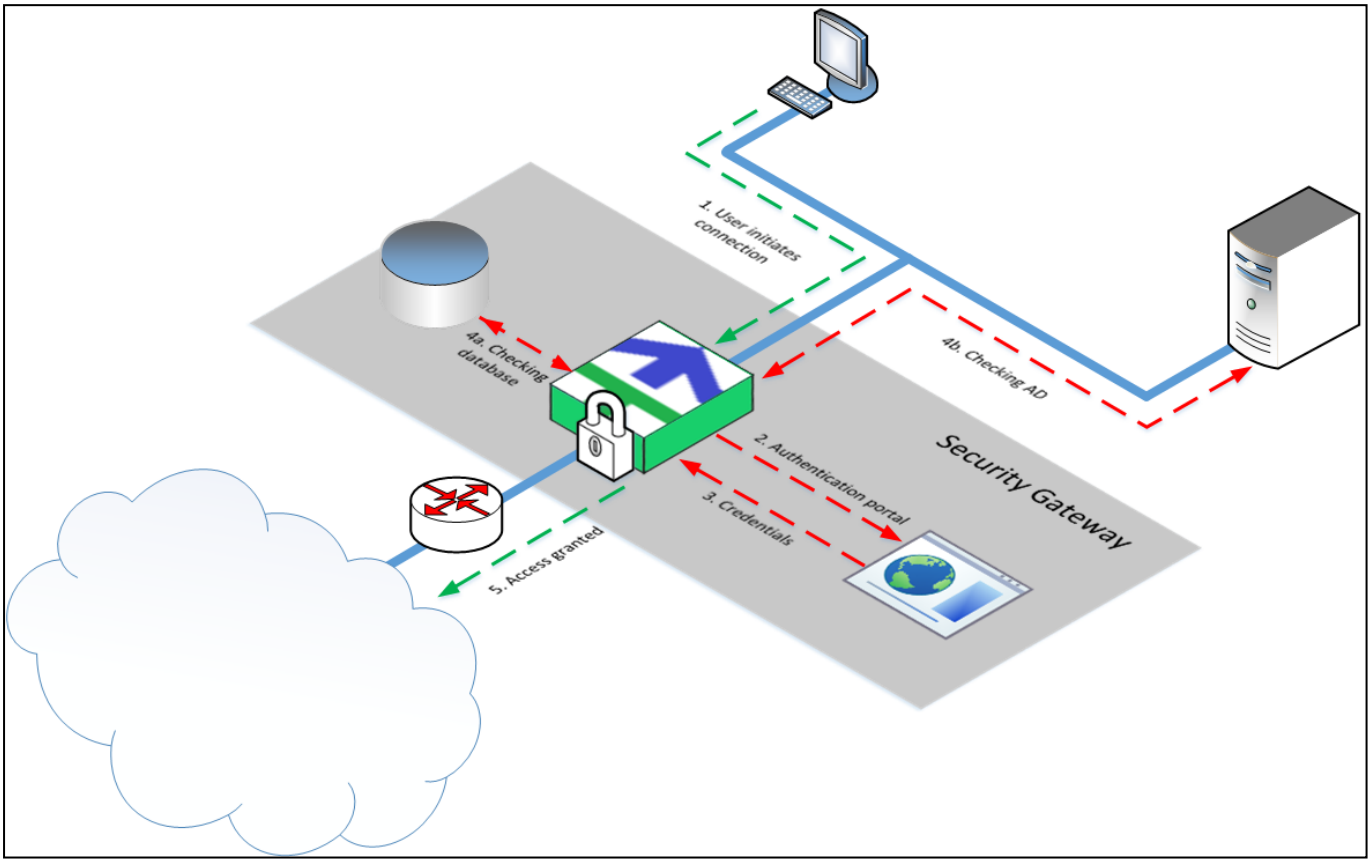
When connecting to the Firewall, a user is authenticated on the Security Gateway using non-cryptographic means via user credentials.

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

Configuration and use

How the Authentication Portal works

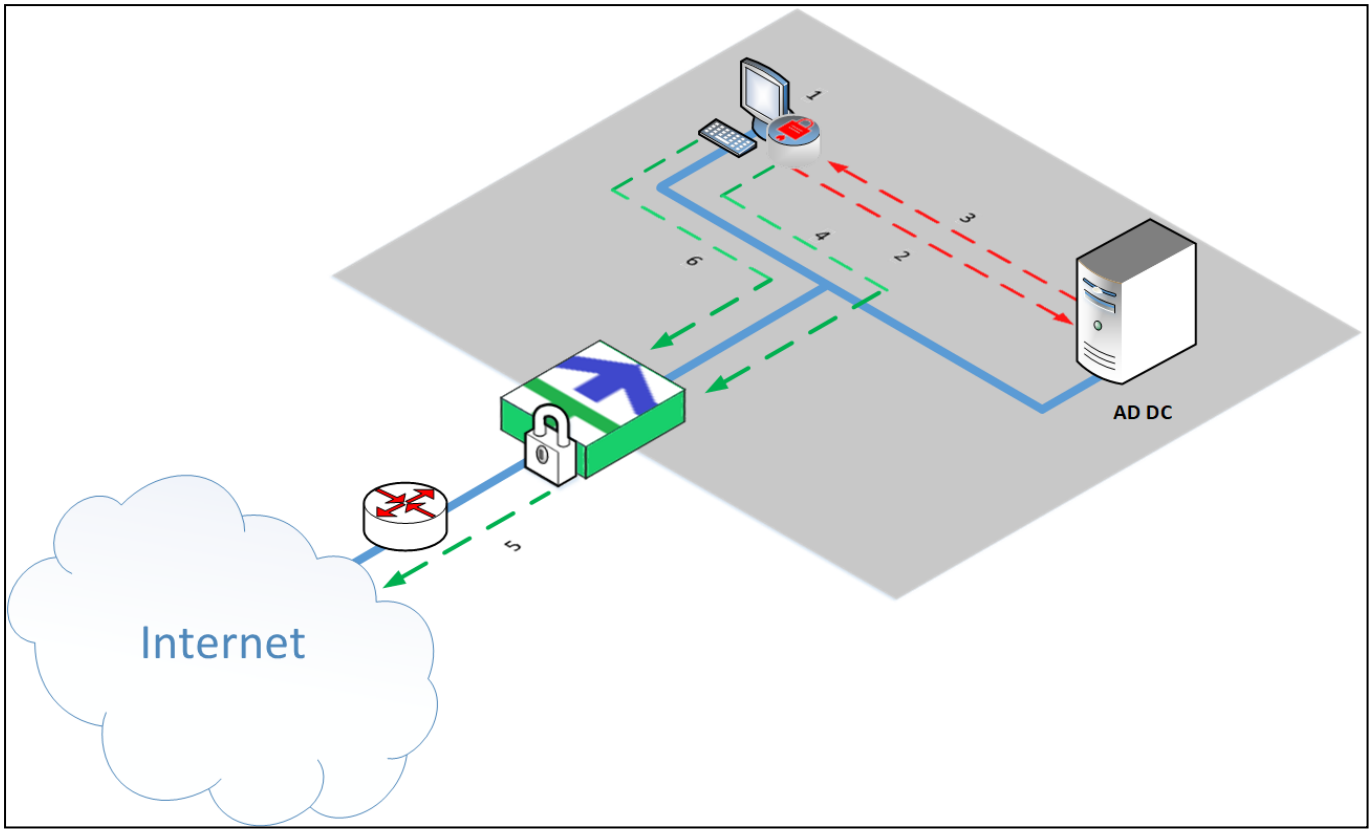
The Authentication Portal is one of the Security Gateway components that authenticates users through the web interface.



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 the Identification Agent works

The Identification Agent is 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.

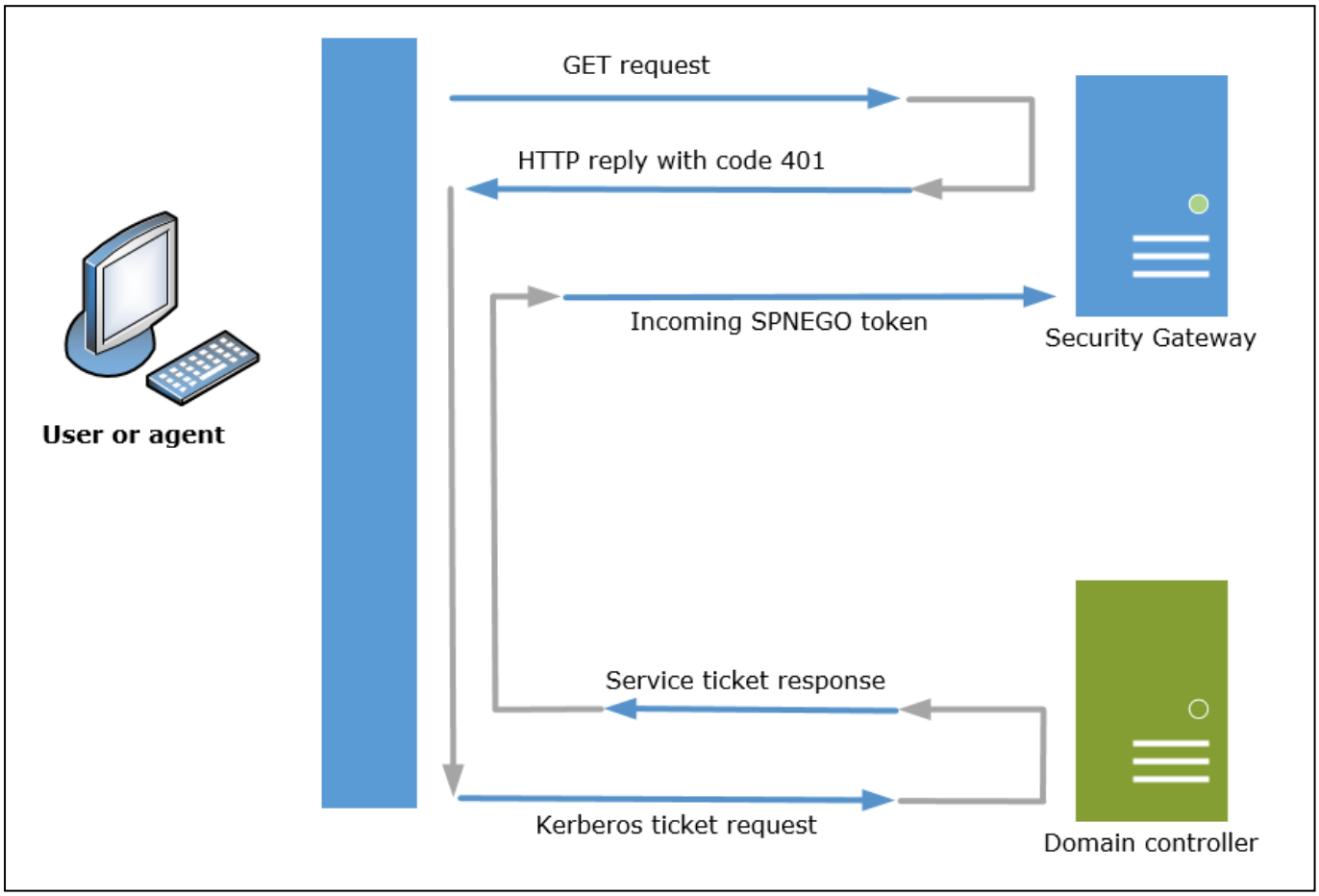
Note.
Identification Agent settings do not depend on Authentication Portal settings. Only a personal certificate connected in the Authentication Portal settings is used.

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. If you use the first scenario, the client browser has to be configured (see p. 24).

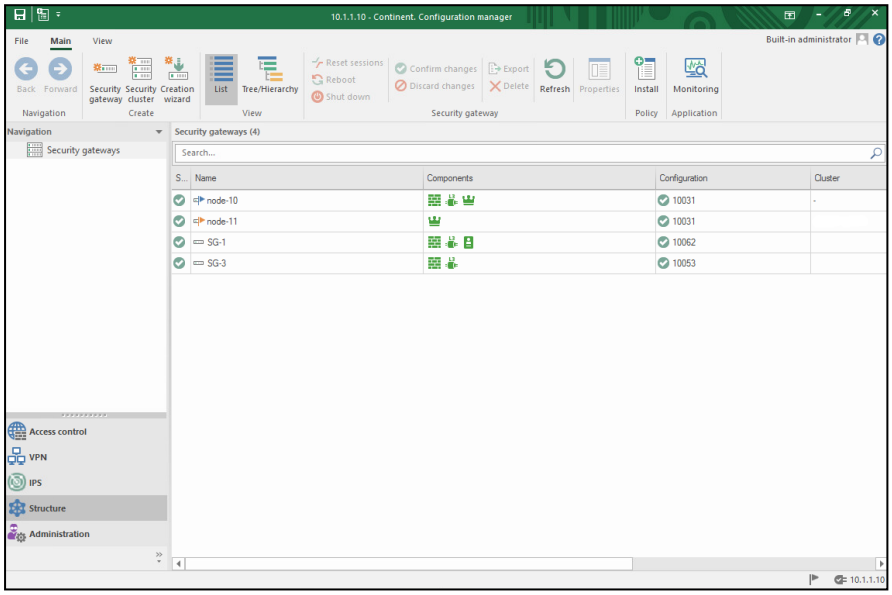
Preconfigure the Security Gateway

To preconfigure the Security Gateway, perform the following steps:

1. Activate the User Identification component on the Security Gateway.
2. Configure the DNS settings for the Security Gateway.
3. Configure the time and date (NTP) settings.

To preconfigure the Security Gateway:

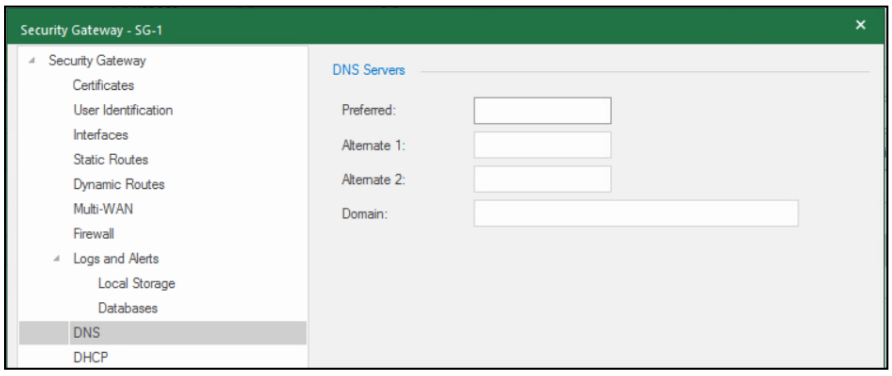
1. In the Configuration Manager, go to **Structure**.



2. Right-click the required Security Gateway and select **Properties**.
3. In the **Components** group box, select the **User Identification** check box and click **Apply**.

   The **User Identification** appears in the menu.

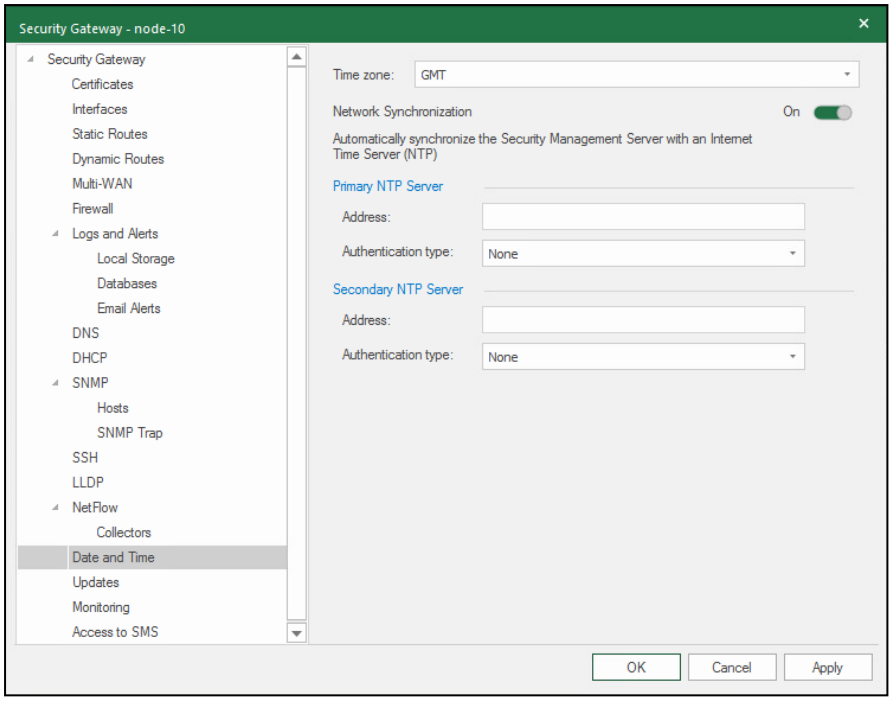
   The component is now activated. You can install policies regulating user identification and authentication.
4. On the left, select **DNS** and specify the preferred DNS server address in the **Preferred** text box. If necessary, specify alternative DNS addresses in the **Alternate 1** and **Alternate 2** fields.



Attention!

If the DNS server is available, but cannot allow the specific domain name, the Security Gateway will not try to get the IP address of this domain name via next DNS servers in the list.

5. Click **Apply**.
6. On the left, select **Date and Time**.



7. Turn on the **Network Synchronization** toggle. This enables the use of an NTP server.

   The **Primary NTP Server** and **Secondary NTP Server** groups of parameters become available for editing.
8. Specify the **Address** and **Authentication type** in the **Primary NTP Server** group.

> **Note.**
> If necessary, set authentication using a symmetric key and/or specify an additional NTP server.

9. On the toolbar, click **Install**, select the required Security Gateways and click **OK**.

For the authentication mechanisms (Authentication Portal, Kerberos authentication) to operate correctly, you need to go to the DNS server and create a record corresponding to the name of the Authentication Portal certificate.

To create a DNS record:

1. Run a DNS server snap-in.
2. Create a record of A type for the Authentication Portal:
   - In the **Node name** field, specify the Authentication Portal name without domain. The fully qualified domain name (FQDN) of a node will be specified automatically. For example, the domain is **TEST.LOCAL**, you need to create the type A record, for example, **auth**.

     The FQDN of this record will be **auth.testers.local**, and the Authentication Portal certificate must have the same name.
   - In the **IP address** field, specify the IP address of the internal interface of the Security Gateway or the virtual address of the Security Gateway cluster.
   - Select the **Create RTP record** check box.
3. Click **Add node**.

Issue authentication certificates

For the Authentication Portal operation and secure data exchange between the Security Management Server and user workstations, you need to issue authentication certificates.

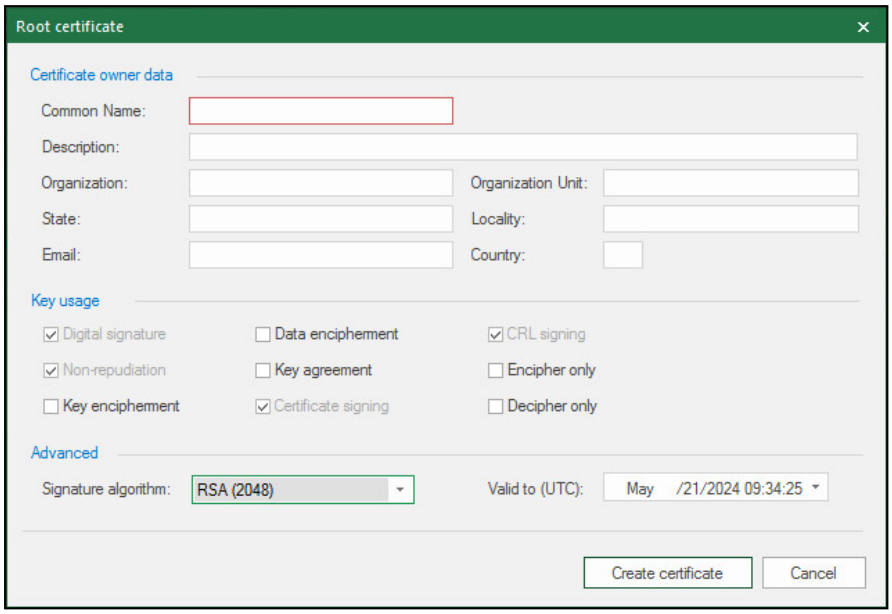
You need to issue the following certificates:

1. Issue a root RSA certificate (see p. **12**).
2. Issue an Authentication Portal certificate (see p. **12**).
3. Issue an Authentication Portal certificate for redirection (see p. **13**).

> **Attention!**
> In Continent, personal and intermediate certificates belong to the **Server certificates** group.

To issue a root RSA certificate:

1. In the Configuration Manager, go to **Administration | Certificates**
2. Click **Root certificate** on the toolbar.
   The **Root certificate** dialog box appears.

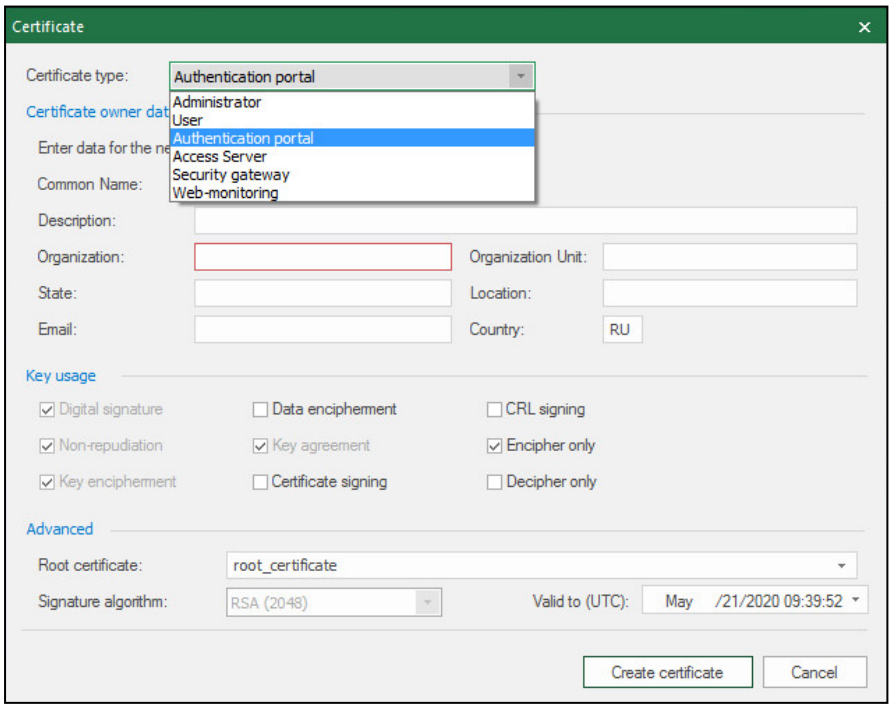


3. In the **Root certificate** dialog box, specify the required text boxes. Select the **RSA (2048)** signature algorithm and click **Create certificate**.

Note.
We recommend assigning understandable names to the root and server certificates.

To issue an Authentication portal certificate:

1. In the Configuration Manager, go to **Administration | Certificates** and select **Personal certificates**.
   The list of personal certificates appears in the display area.
2. On the toolbar, click **Certificate**.
   The **Certificate** dialog box appears.

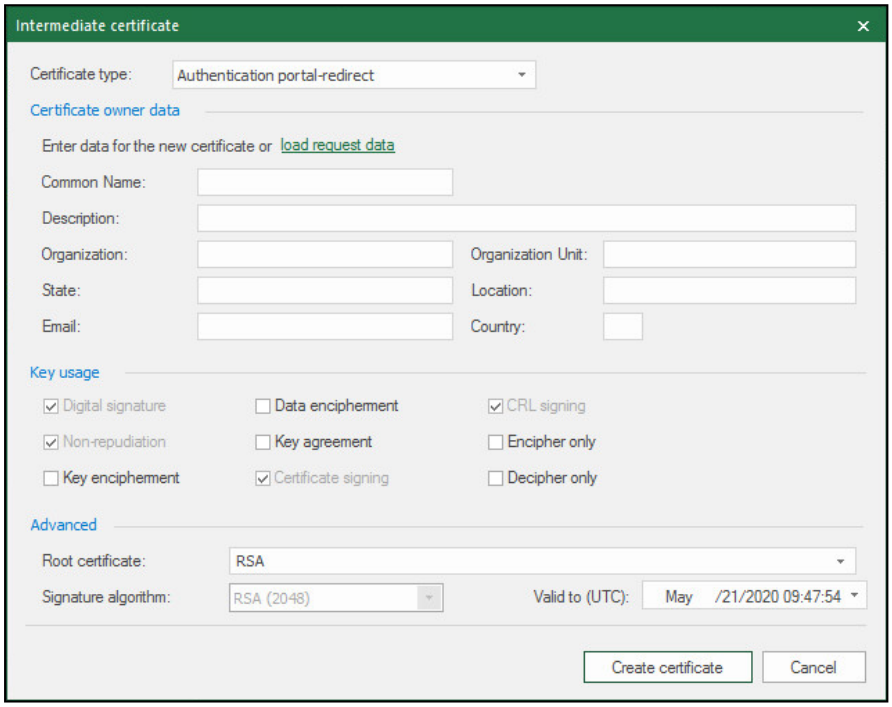


3. In the **Certificate** dialog box, select the **Authentication portal** certificate type. Specify the required parameters and choose the root certificate created during the previous procedure.

> **Attention!**
> The Authentication Portal certificate name must be exactly the same as the fully qualified domain name (FQDN) specified in the DNS server. An example of an Authentication Portal certificate name and DNS record in a domain looks as follows:
> **TESTERS.LOCAL: auth.testers.local**.

To issue an Authentication Portal-redirect certificate:

1. In the Configuration Manager, go to **Administration | Certificates** and select **Intermediate CAs**.
2. On the toolbar, click **Intermediate certificate**.
   The **Intermediate certificate** dialog box appears.



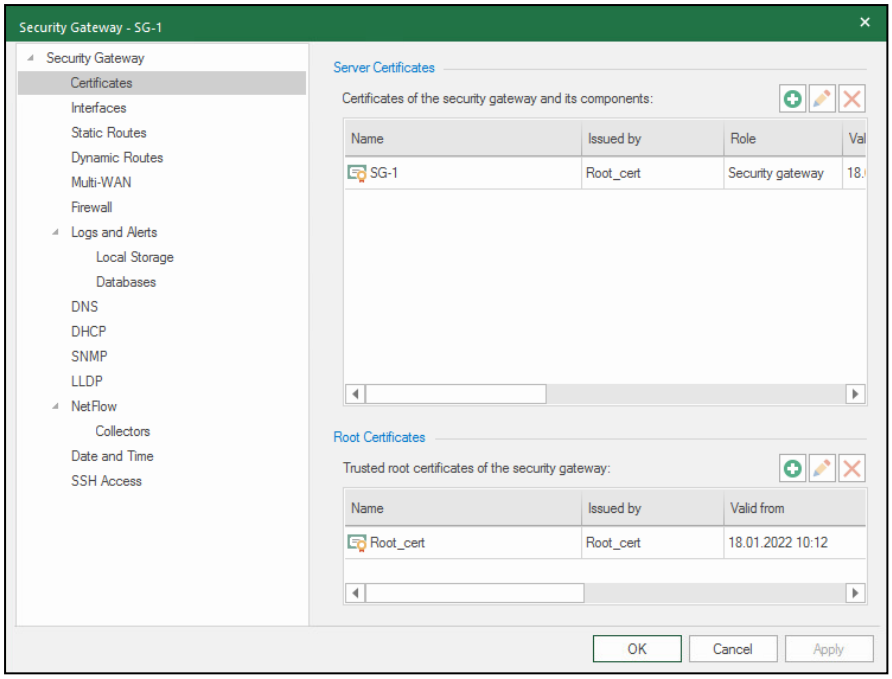
3. In the **Intermediate certificate** dialog box, specify the required text boxes, select the root certificate created for the Authentication Portal and click **Create certificate**.

Add a certificate to the Security Gateway

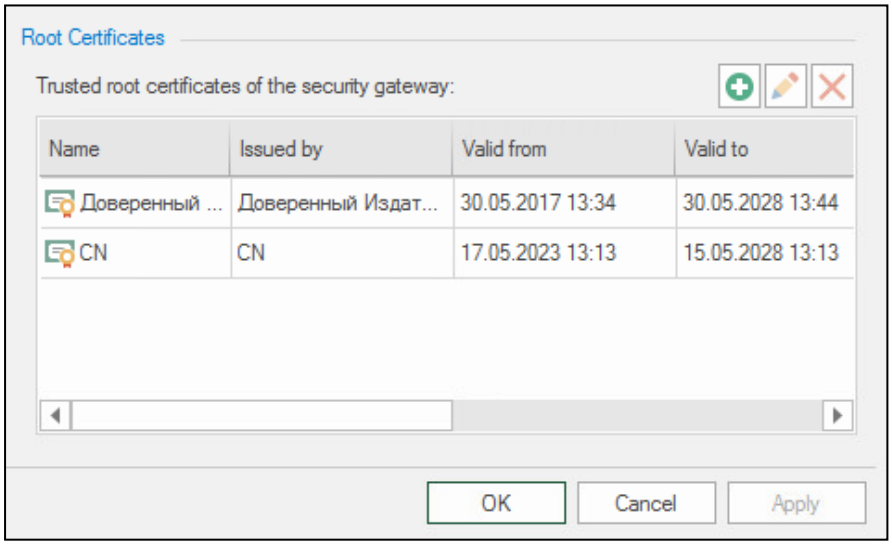
When Authentication Portal certificates are issued, it is necessary to add them to the Security Gateway.

To add certificates to the Security Gateway:

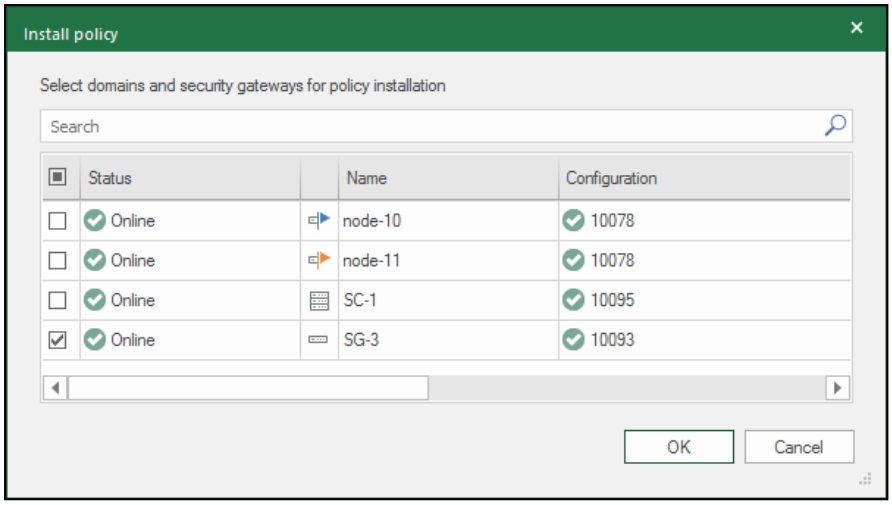
1. On the navigation panel, go to **Structure**.
2. In the display area, select the Security Gateway and click **Properties** on the toolbar.
   The **Security Gateway** dialog box appears.



3. Go to **Security Gateway | Certificates**.
4. Add the created Authentication Portal and Authentication portal-redirect certificates to the **Certificates of the security gateway and its components** list by clicking .
5. Add the created root RSA certificate to the **Trusted root certificates of the security gateway** list by clicking .



6. Click **OK**.
7. On the toolbar, click **Install**.
   The **Install policy** dialog box appears.



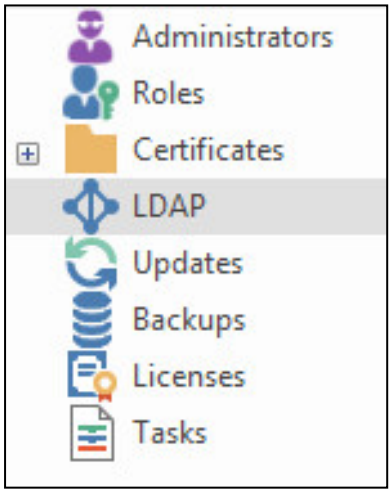
8. Select the required Security Gateways and click **OK**.
   The changes are sent to the Security Gateways.

Add users over LDAP

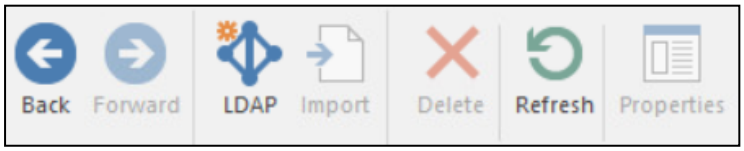
At this step, an administrator adds user groups over LDAP or creates new ones in the Security Management Server database. For more information about creating, deleting and editing user accounts, see Continent Enterprise Firewall. Version 4. Administrator Guide. Firewall. Continent supports user authentication using AD over LDAP.

Configure LDAP

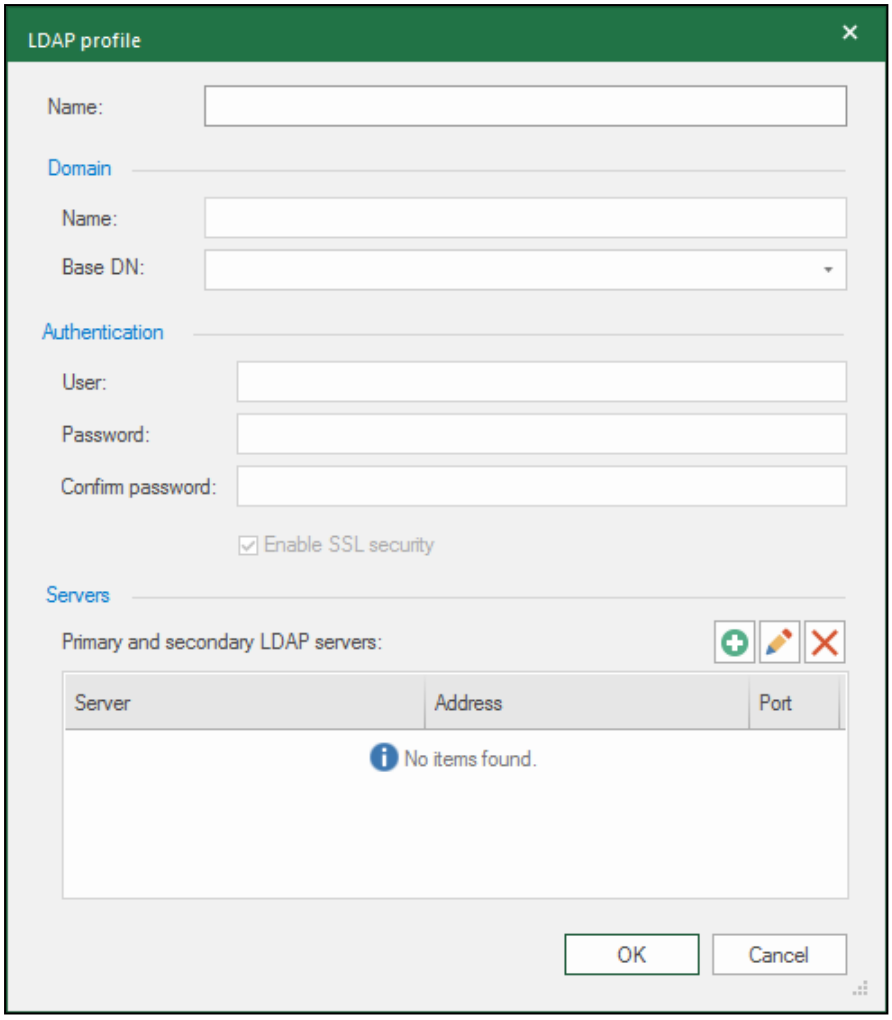
1. In the Configuration Manager, go to **Administration** and select **LDAP**.



2. On the toolbar, click **LDAP**.



   The **LDAP profile** dialog box appears.



3. Specify the required parameters in the respective text boxes.

Note.
To enable AD, we recommend creating a separate account that will have the rights to read groups and users.

In the **Authentication** group box, enter the user credentials in the **User** and **Password** text boxes.

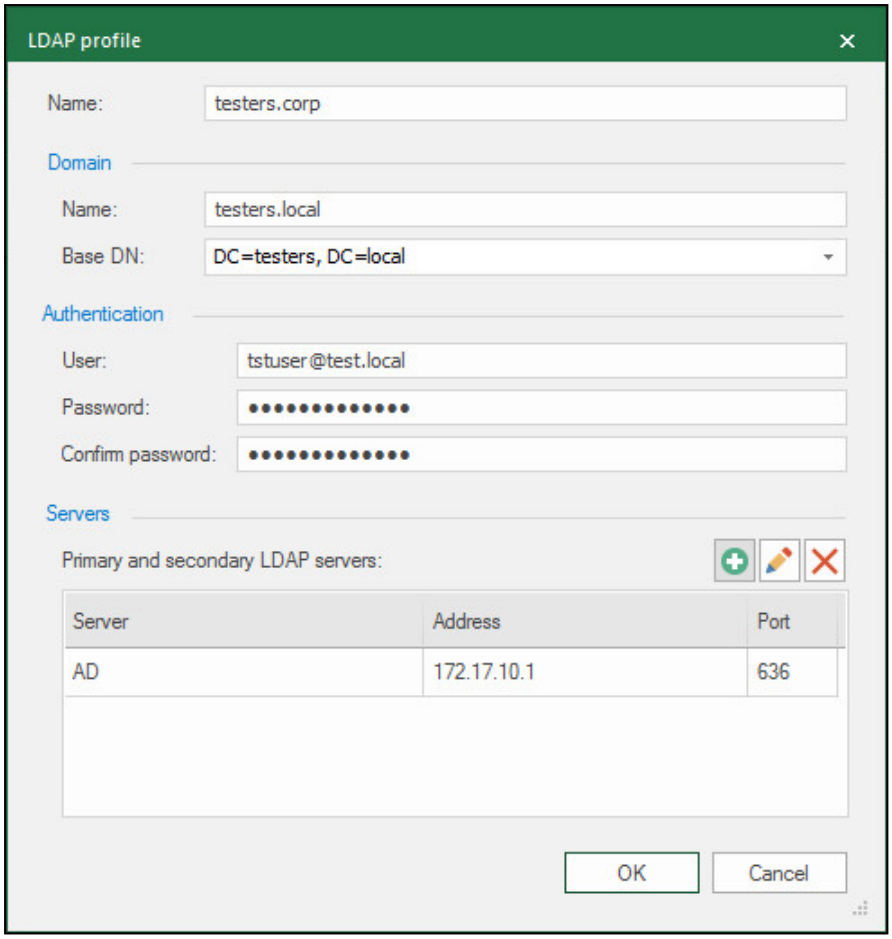
4. In the **Servers** group box, add the AD server IP address and a port by clicking . To edit the added server, click , to delete — .

5. In the **LDAP profile** dialog box, specify the AD server name in the **Server** field, then the AD server IP address or domain name in the **Address** field.

Attention!
It is forbidden to use the following characters in the AD server divisions:

«	»	#	*	(	)	=	+	\	;	"	>	<	,

Attention!
The connection to the AD server is established over LDAPS. To support the LDAP protocol, ports with the same number must be configured on the workstation with the Configuration Manager and on the AD server.



6. Click **OK**.

   The created LDAP profile appears in the display area.

7. On the navigation panel, go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.

   The respective dialog box appears.

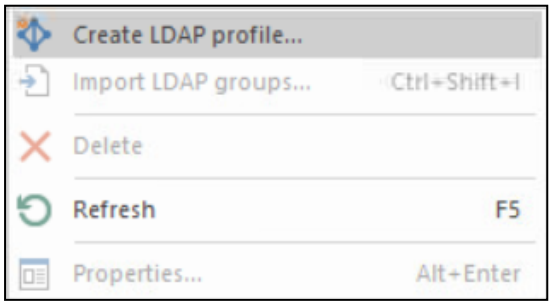
8. On the left, select **Authentification**.

   The respective parameters appear on the right.

9. In the **LDAP profile** drop-down list, select the profile created at step **5**.

10. Click **OK**.
11. On the toolbar, click **Install policy** and select the Security Gateway for which you specified the LDAP profile, then click **OK**.
12. Go back to **Administration** and select **LDAP**.

    The LDAP context menu appears.



13. Click **Import LDAP groups**.

Attention!
In Continent, only groups can be imported.

If AD is connected successfully, the **LDAP groups import** dialog box appears.

Note.
The Security Management Server creates a group import command for all Security Gateways to which the current profile is bound in the **User Identification** properties. You can import profiles that are not connected to any Security Gateway. After one of the Security Gateways responds, the Security Management Server saves imported groups in its configuration.

14. Select groups to import and click **Import**.

Attention!
The Configuration Manager starts to work slower if there are many AD groups. It is recommended to use Active Directory nested groups.

After the import is completed, you receive the respective message. Imported groups can be added to filtering and translation rules.

Note.
To delete a group in the list of Security Management Server objects, first delete it in AD and then import groups once again. If you delete a group in AD and do not import groups, the group remains in the Security Management Server database.
If a new group with the same name is created in AD, you must re-import the group from AD to update the ObjectGUID of the group in the Security Management Server database. If new groups are created in AD, you need to import them from AD to use them in Firewall rules.

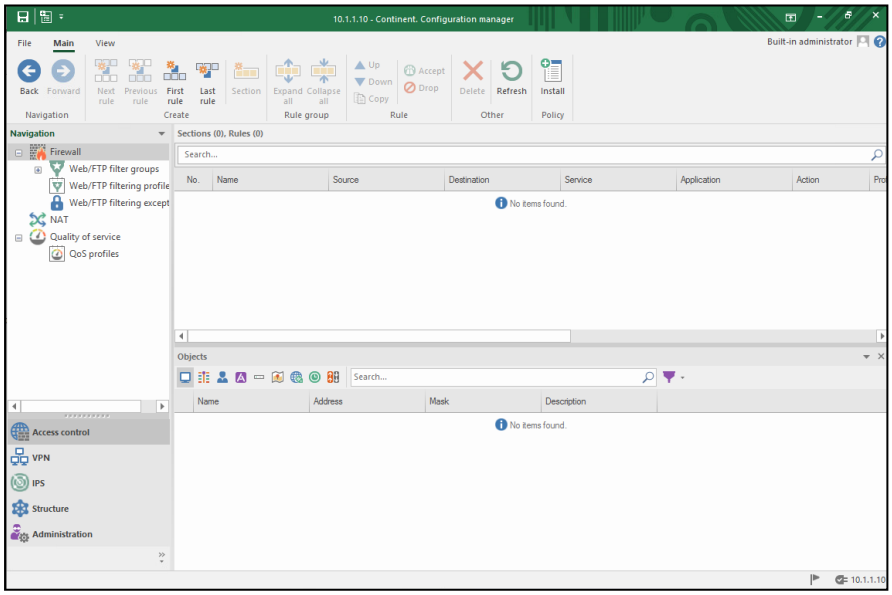
Create Firewall rules

To ensure correct operation of the Authentication Portal, traffic should pass through the DNS protocol from the client to the DNS server and the Security Gateway with the configured **Authentication Portal** component.

Note.
In case of difficulties while working in Access control, see Continent Enterprise Firewall. Version 4. Administrator guide. Firewall.

To create Firewall rules:

1. In the Configuration Manager, go to **Access control**.



2. Right-click the display area and click **Create first rule** or **Create last rule**.
   The created rule appears in the list.
3. Create access rules.
   For example, to create a permitting access rule for a user, specify the user account or user group in the **Source** box, type the name of a resource to which the user will be granted access in **Destination**, specify the protocols for user access in **Service**, in **Action** select **Accept**.
4. Click **Install** on the toolbar to install the policy.

Note.
Before you install the policy, make sure you enabled the **User Identification** component.

Authentication parameters configuration

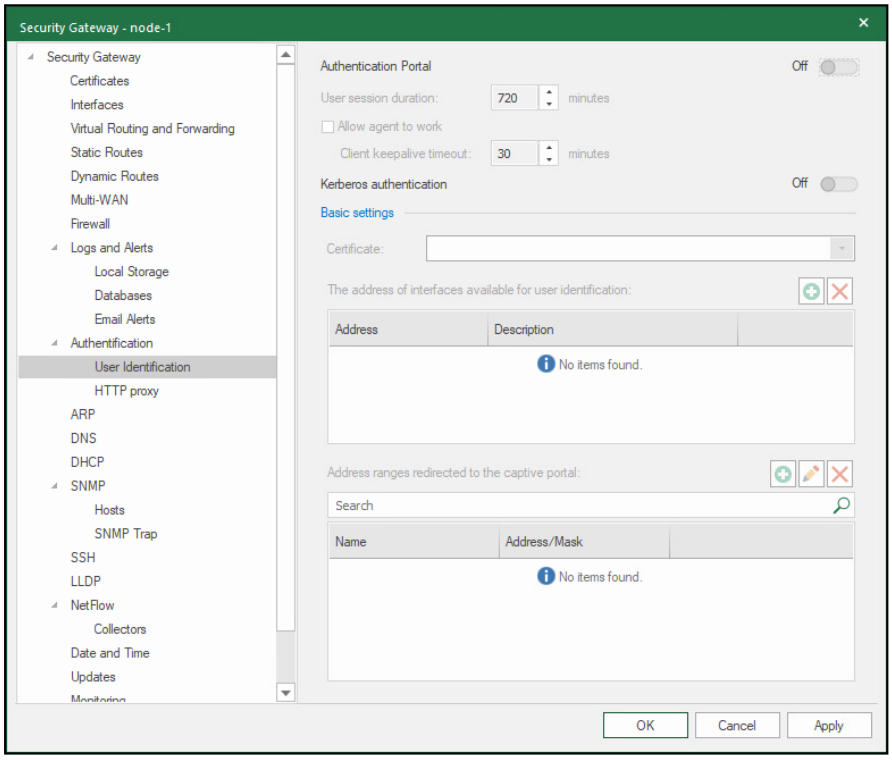
The authentication mechanism is implemented through the Authentication Portal and transparent authentication via Kerberos (SSO). Continent also contains a proxy server with several authentication methods.

To ensure correct operation of the Authentication Portal, it is necessary to configure the Security Gateway setting first. Then configure the Active Directory parameters depending on the required authentication method and the Security Gateway authentication settings.

Authentication via the Authentication Portal

To configure the Authentication Portal:

1. On the left, select **Authentification**.

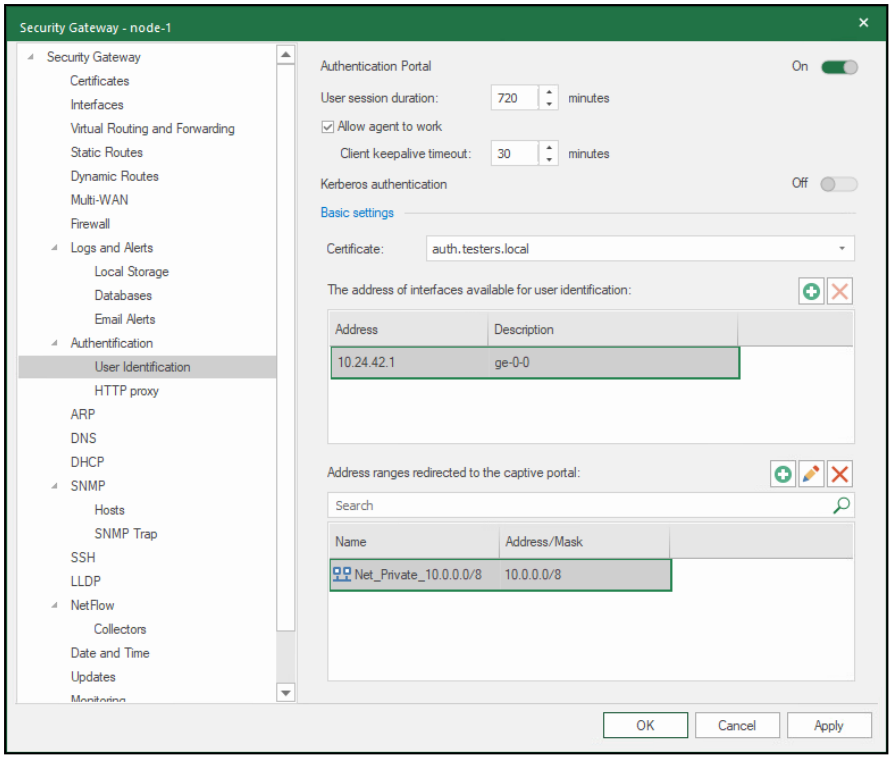


2. If it is necessary to add users, select a LDAP profile in the **LDAP profile** drop-down list (to create users, see **Add users over LDAP** on p. **15**).
3. Go to **User Identification**, turn on the **Authentication Portal** toggle and click **Apply**.

   The connection settings are now available for editing.
4. Specify the duration of a user session in minutes in the **User session duration** spin box.

   Note.
   The user session duration ranges from **5** to **1440** minutes.
5. Select the **Allow agent to work** check box to enable usage of the Identification Agent for authentication at the portal.
6. Specify the client keepalive timeout in the respective spin box.

   If access to the portal is maintained, the user will automatically reconnect at intervals equal to ½ of the set time.
7. In the **Certificate** drop-down list, select the Authentication Portal personal certificate.

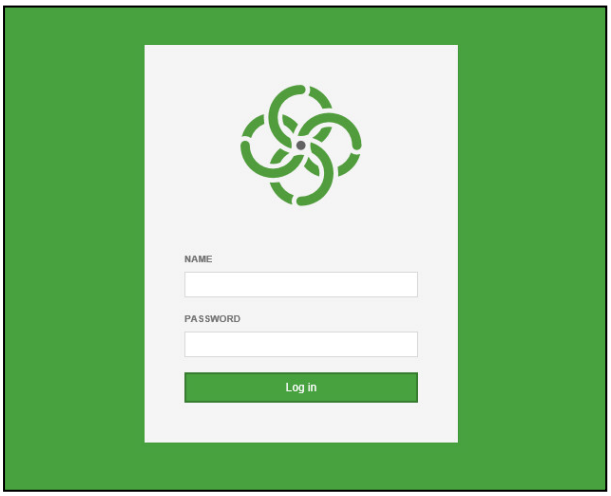


8. Specify addresses of the interfaces on which user identification will operate.
9. In the **Address ranges redirected to the captive portal** group, click .
   The list of available network objects appears.
10. Select the network objects that could be redirected to the Authentication Portal.

> **Note.**
> If it is necessary, create a new network object. To do so, click **Create**. In the appeared dialog box, specify the required parameters and click **OK**.

11. Click **OK** to save the changes.

If all the settings are correct, a user's browser is displayed as in the figure below.

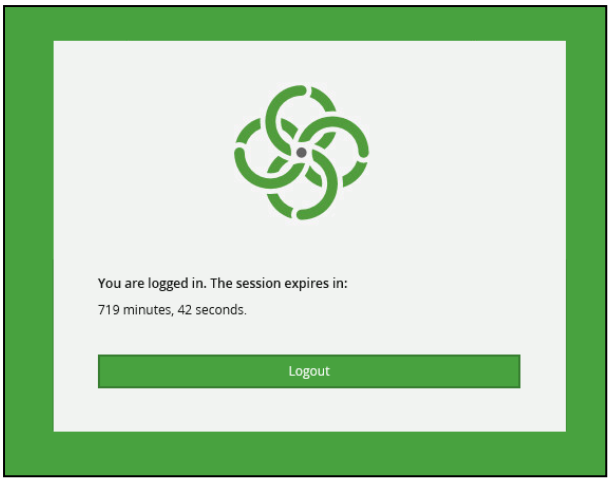


> **Note.**
> If you access the Authentication Portal directly, the name of the Authentication Portal personal certificate appears in the browser address bar.

To access the Internet, you need to enter user's credentials in the respective text boxes, then click **Login**. If the server checks a local database for the user's credentials, enter a username without a domain. In the case of using the AD server, specify a username and a domain, divided by **@** (for example, **usertst1@local.host**).

> **Note.**
> If a certificate warning appears when loading the portal page, add the root certificate used to generate the portal certificate to the root trusted certification authorities on the user's workstation.

If the authentication is successful, you receive the respective message.



To continue working on the Internet:

- open a new browser tab.

To end the session:

- click **Log out**.

Configure Transparent Kerberos Authentication

Transparent Kerberos or Single Sign-On (SSO) authentication allows users to access authorized resources without explicit authentication. The user is authenticated through Active Directory when logging in to the OS. When accessing resources, the Firewall verifies the authentication in Active Directory without asking the user for credentials again, i.e. authentication on the Firewall is automatic for the user.

SSO can operate either in parallel with the Authentication Portal and the proxy server or independently. However, SSO requires configuration to work in parallel with the Authentication Portal.

SSO functions correctly if the following requirements are met:

- Transparent Authentication works only for domain accounts, not for local accounts. A LDAP profile with the used domain must be added to the Configuration Manager.
- The system time on the Configuration Manager, Security Gateway, domain controller and user workstations must be synchronized with the current local time. We recommended using a corporate NTP server for synchronization.
- For user workstations and Security Gateways of Continent, network connectivity with the domain controller and DNS server must be provided.
- Configuration Manager, Security Gateway, domain controller, as well as user workstations must use the same DNS servers for name resolution.

SSO is configured in the following order:

1. Configure a LDAP profile on the Configuration Manager and import user groups from the domain controller (see p. **15**).

   This step is required so that the Configuration Manager can verify that the user authentication to the Active Directory.

   Note.
   If the required LDAP profile is already configured, no additional configuration is required.

2. Create Authentication portal and Authentication portal-redirect certificates and bind them to the Security Gateway (see p. **11**).

   Attention!
   If the Authentication Portal has already been configured, no additional configuration is required. In this case, you can use the DNS record of the Authentication Portal, which should already be created.

   The Authentication Portal certificate name must match its domain address assigned on the DNS server (see p. **11**), so you need to name the certificate accordingly (in the FQDN record format).

   For example, **auth.testers.local**.

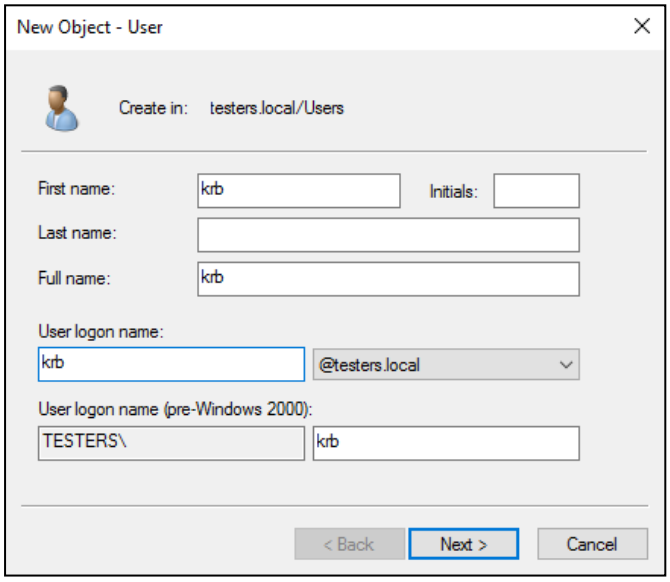
Note.
To configure the Authentication Portal on the cluster, you need to issue two certificates of the **Authentication Portal** type with the same name (one for each node). When you configure the cluster identification settings, the portal certificates are automatically defined and will not be displayed will not be displayed in the Configuration Manager.
When configuring a record on the DNS server, the virtual address of the cluster is specified.

3. Create and configure a user account in AD for Kerberos operation (see below).
4. Issue a keytab file (see p. **22**).
5. Configure Kerberos protocol authentication in the Configuration Manager.
6. Create Firewall rules for domain users (see p. **18**).
7. Configure browsers on user workstations (see p. **24**).

Attention!
After updating Continent from version 4.1.7, in order to avoid a warning when working with transparent authentication, you need to assign a keytab record for the Authentication Portal in the **Services and Kerberos Credentials** table on the **Authentification** tab of the Security Gateway properties.

To create and configure a user account for Kerberos operation:

1. Create an account in the **Users** section of the AD snap-in tool.



Attention!
If the password for the account based on which the keytab file was created changes, it is necessary to generate a keytab file again. We recommend setting a complex password for this account from the start so you will not need to change it.

2. In the account properties, select **Account** and, in account parameters, enable **This account supports 256-bit encryption**.
3. Specify the SPN for a user account in PowerShell by running the following command:

```
setspn –A HTTP/auth.testers.local krb
```

where **auth.testers.local** is the Authentication Portal address specified in the DNS server and Authentication Portal certificate name, **krb** is the user account name created on the previous step.

To issue a keytab file:

1. Run PowerShell on the domain controller as administrator and generate a keytab file using the following command:

Attention!
The command is case sensetive. You cannot use special characters in user names and names of organizational units.

```
ktpass /princ HTTP/auth.testers.local@TESTERS.LOCAL /mapuser krb@TESTERS.LOCAL
/crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL /pass * +dumpsalt /out C:\sso.keytab
```

where:

- **auth.testers.local** is the domain address of the Authentication Portal on the DNS server, as well as the Authentication Portal certificate name, followed by **@** and an uppercase domain address name (**TESTERS.LOCAL** in this example);
- **krb@TESTERS.LOCAL** is the **krb** account in the **TESTERS.LOCAL** domain, **/pass *** means that after entering the command, a user will be prompted to enter the password;
- **/crypto** specifies the encryption type;
- **/out** specifies the path for saving the keytab file.

```
PS C:\Users\Администратор.WIN-KIE0LPT41AL> ktpass /princ HTTP/SG01.testers.local@TESTERS.LOCAL /mapuser testers\krb /pas
s * /crypto ALL /ptype KRB5_NT_PRINCIPAL /out SG01.keytab
Targeting domain controller: TST-ADS01.testers.local
Successfully mapped HTTP/SG01.testers.local to KRB$.
```

2. Enter and confirm the password for the account. Confirm the password change.

You need to add the created keytab file to the Security Gateway in the Configuration Manager.

Attention!
If the root certificate was changed, generate a keytab file again and add it to the Security Gateway.

Example of keytab file generation

```
PS C:\Windows\system32> ktpass.exe /princ HTTP/auth.testers.local@TESTERS.LOCAL -mapuser squid@TESTERS.LOCAL -crypto AES
256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\proxy.keytab
Targeting domain controller: TST-ADS01.testers.local
Successfully mapped HTTP/auth.testers.local to squid.
Type the password for HTTP/auth.testers.local:
Type the password again to confirm:
Password successfully set!
Building salt with principalname HTTP/auth.testers.local and domain TESTERS.LOCAL (encryption type 18)...
Hashing password with salt "TESTERS.LOCALHTTPauth.testers.local".
Key created.
```

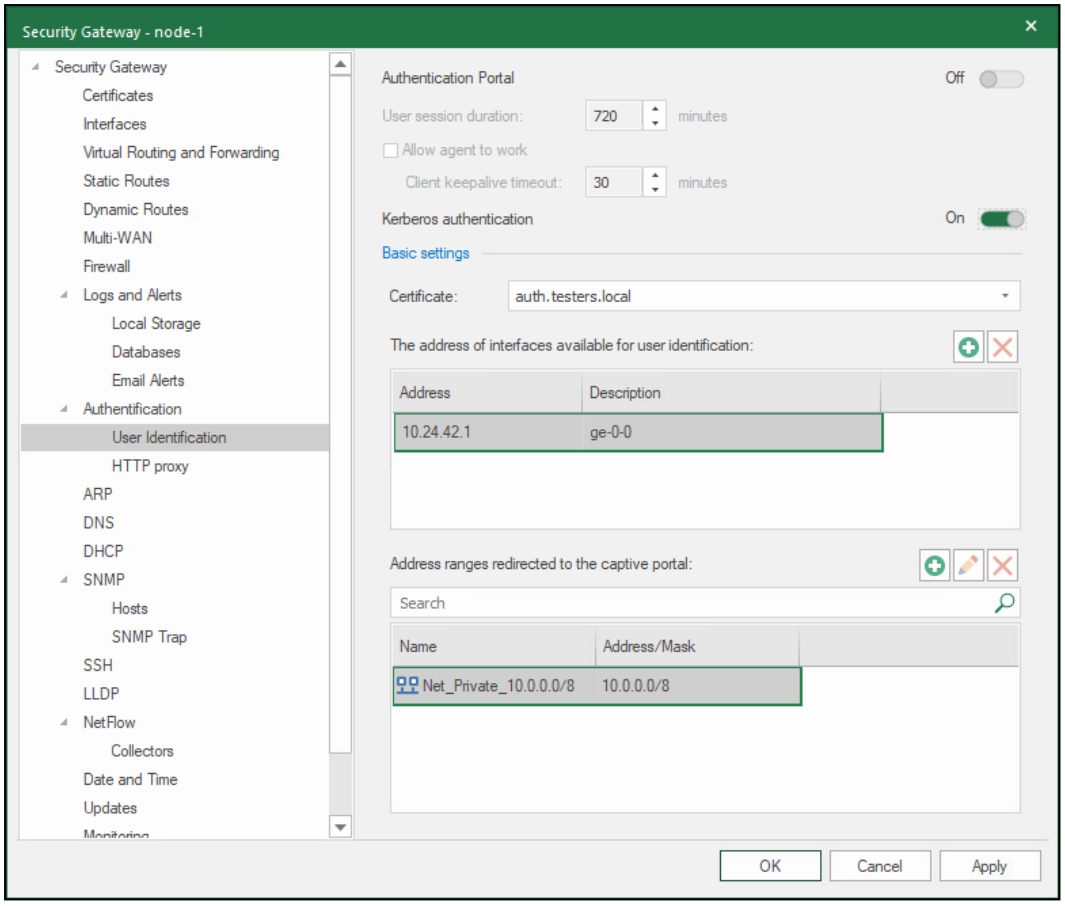
To configure authentication via Kerberos in the Configuration Manager:

1. Go to **Structure**, select the Security Gateway with the Authentication Portal and click **Properties** on the toolbar.

   The respective dialog box appears.
2. On the left, select **Authentification**.
3. In the **LDAP profile** drop-down list, select the created LDAP profile.
4. In the **Services and Kerberos Credentials** group of parameters, click  (**Import keytab file data**) and select the keytab file created earlier in the file explorer.

   Note.
   The keytab file is not displayed until the next step of the procedure is completed.
5. In the Services and Kerberos Credentials group of parameters, click  and assign **Authentication Portal** to the SPN service.
6. Specify the required user session duration in minutes.

   Note.
   The user session varies from **5** to **14440** minutes.
7. Go to **Authentification | User Identification**
8. Turn on the **Kerberos authentication** toggle.



The **Kerberos Authentication** group of parameters becomes available for editing.

9. In the **Certificate** drop-down list, select the Authentication Portal certificate.
10. In the **Address ranges redirected to the captive portal**, specify IP addresses of the users who can use transparent Kerberos authentication.

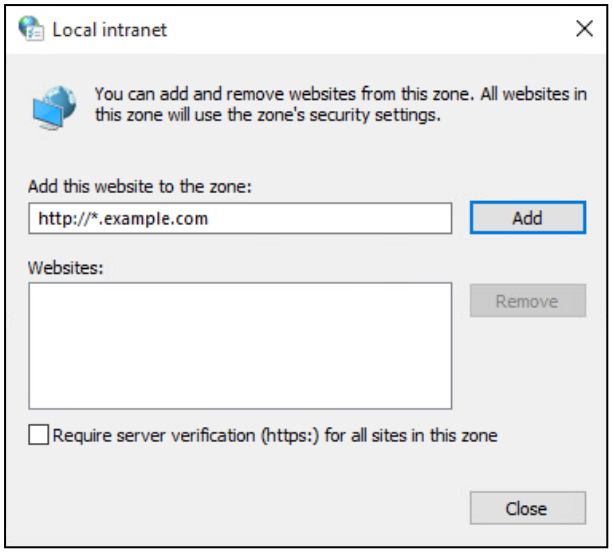
Note.
If it is necessary, create a new network object. To do so, click **Create**. In the appeared dialog box, specify the required parameters and click **OK**.

Configure a browser for user authentication via the Authentication Portal

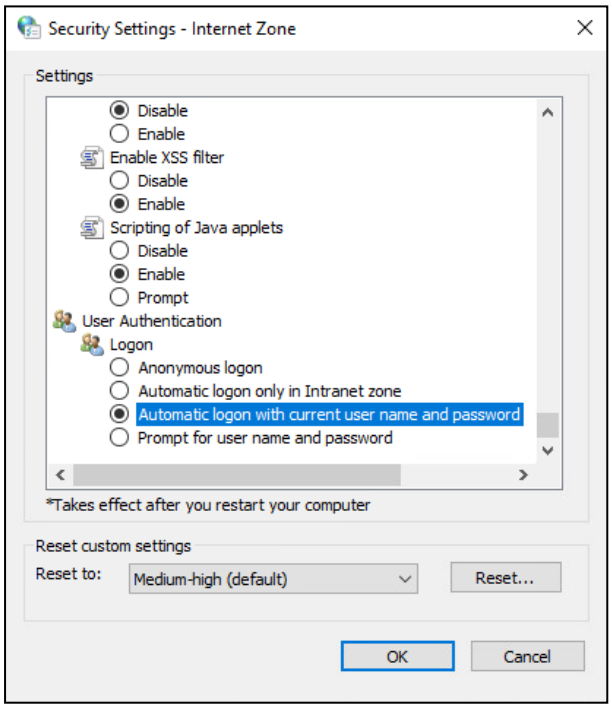
For correct user authentication using Kerberos via the Authentication Portal you need to configure the browser. We recommend using group policies to configure browsers on corporate workstations.

To configure Chrome, Yandex, Atom, Sputnik, Microsoft Edge, Internet Explorer:

1. In the control panel menu, select **Internet Options**.
   The **Internet properties** dialog box appears.
2. Go to the **Security** tab and select **Local intranet**.
3. Click **Sites**.
   The **Local intranet** dialog box appears.
4. In the **Local intranet** dialog box, click **Advanced**.
   The list of websites appears.
5. In the **Add this website to the zone** field, specify the domain of the Authentication Portal via the HTTPS protocol and click **Add**.



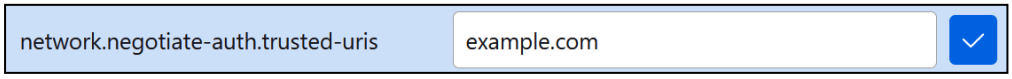
6. Click **Close** and then click **OK**.
7. Perform the following actions for each zone in the **Security** tab:
   - In the **Security level for this zone** group of parameters, click **Custom level**.
   - Go to **User Authentication | Logon** and select **Automatic logon with current user name and password**.
   - Click **OK**.



8. In the **Internet Properties** dialog box, click **Apply**.

To configure Firefox:

1. In the browser address bar, type **about:config**.
   The **Advanced Settings** window opens in the current tab.
2. In the search bar, type **network.negotiate**.
3. In the **network.negotiate-auth.trusted-uris** and **network.negotiate-auth.delegation-uris** parameter lines, click **Edit**, specify the Authentication Portal domain name and click **Save**.



Configure authentication on the proxy server

The proxy server can operate without authentication (anonymous proxy) or use two user authentication schemes:

- Negotiate (Kerberos);
- Basic.

Negotiate (Kerberos) authentication

Negotiate (Kerberos) authentication configuration is similar to a lot of settings for SSO. If SSO without a proxy is already configured, you need to configure only browsers on client computers. You do not need to issue certificates for the authentication portal and redirection to the authentication portal for this mode.

To configure Negotiate authentication, take the following steps:

1. Configure LDAP profile on the Security Management Server, import user groups from the domain controller (see p. **15**).

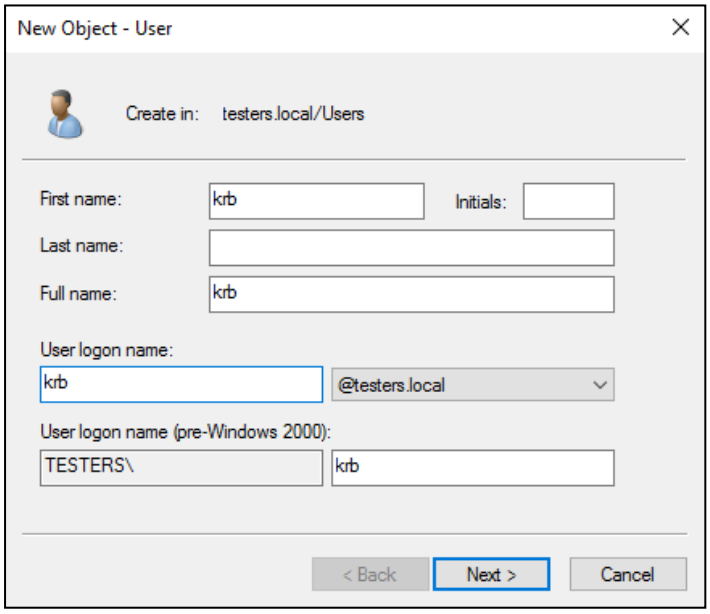
   This step is necessary for the Security Management Server to check whether the user is authenticated in AD.

   Note.
   If the required LDAP profile is already configured, no additional configuration is needed.

2. Create and configure the AD user account for Kerberos operation (see below).
3. Issue a keytab file (see p. **26**).
4. Configure the DNS server (see p. **11**).
5. Configure authentication via Kerberos in the Configuration Manager.
6. Create proxy server rules for domain user access (see p. **30**).
7. Configure browsers on client workstations (see p. **31**).

To create and configure a user account for Kerberos operation:

1. In the AD snap-in, go to the **Users** section and create an account.



2. In the account properties, select **Account** and, in account parameters, enable **This account supports 256-bit encryption**.
3. Determine the SPN for the account in PowerShell by running the following command:

   ```
   setspn –A HTTP/auth.testers.local krb
   ```

   where **auth.testers.local** is a DNS name for the address of the interface on which the proxy server is configured (to easily access it), **krb** is a name of the user account created during the previous step.

To issue a keytab file:

1. Run PowerShell on the domain controller as an administrator and generate a keytab file using the following command:

Attention!
The command is case sensitive. It is forbidden to use the special characters in user names and the names of organizational units.
If the password for the account based on which the keytab file was created changes, it is necessary to generate a keytab file again.
We recommend setting a complex password for this account from the start so you will not need to change it.

```
ktpass /princ HTTP/auth.testers.local@TESTERS.LOCAL /mapuser krb@TESTERS.LOCAL
/crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL /pass * +dumpsalt /out
C:\proxy.keytab
```

where:

- **auth.testers.local** is a DNS name of the proxy server interface followed by **@** and the domain address in upper case (**TESTERS.LOCAL** in this example);
  krb@TESTERS.LOCAL is the **krb** account in the **TESTERS.LOCAL** domain;
- **/pass *** means that after entering the command you will need to set the password;
- **/crypto** indicates the encryption type;
- **-dumpsalt** is used to reinforce encryption and keep the possibility of extending the keytab file in case of using the proxy server and SSO on different network interfaces;
- **/out** specifies the path for saving the keytab file.

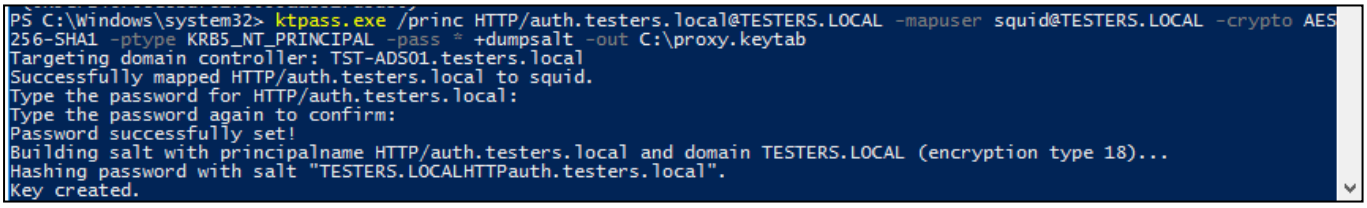
2. After entering the command, enter and confirm the password for the account, then confirm the password change.

Note.
We recommend using different service principal names (SPNs) if you configure authentication on separate Security Gateways.

After you receive the keytab file, you need to add it to the Security Gateway via the Configuration Manager.

Attention!
If the root certificate was changed, it is necessary to generate a keytab file again and add it to the Security Gateway.

Example of keytab file generation



To configure authentication via Kerberos in the Configuration Manager:

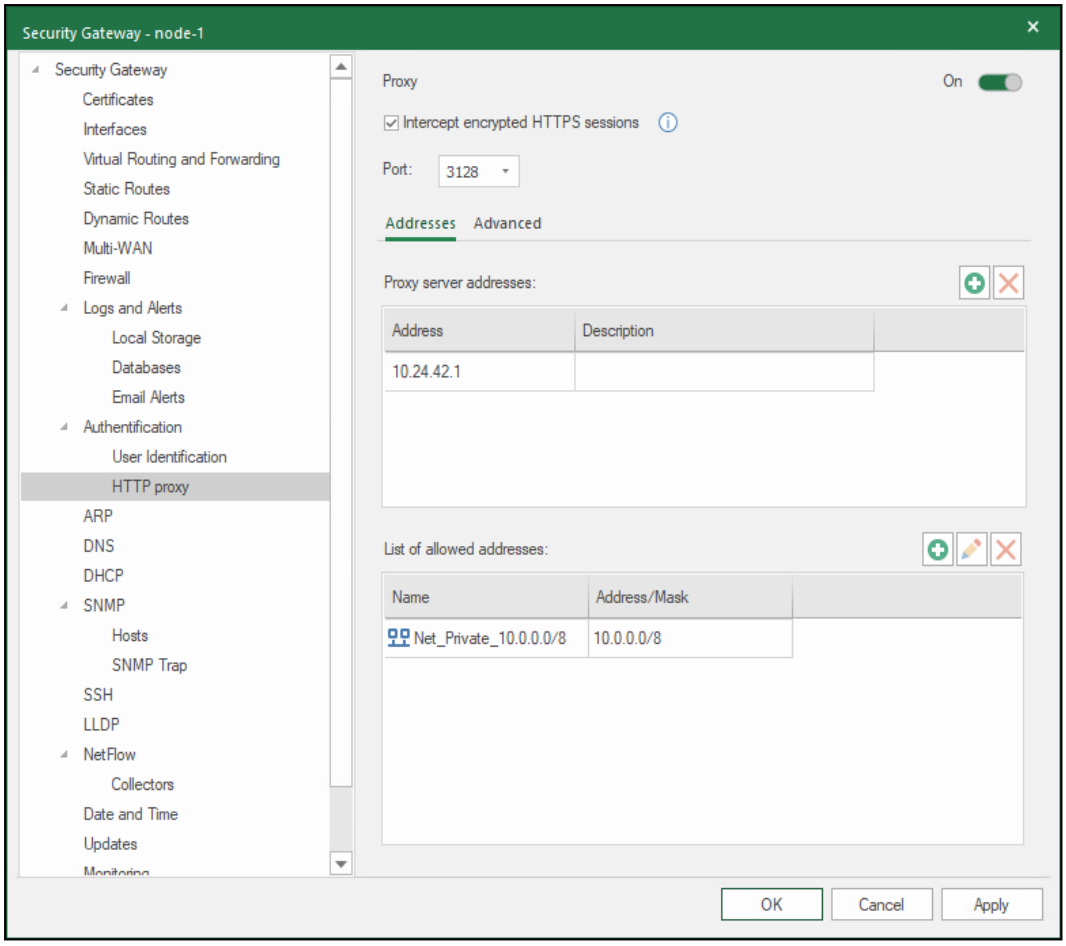
1. Go to **Structure**, select the Security Gateway and click **Properties** on the toolbar.
2. In the appeared dialog box, select **Authentication**.
3. In the **LDAP profile** drop-down list, select the LDAP profile created earlier.
4. In the **Services and Kerberos Credentials** group of parameters, click (**Import keytab file data**) and select the keytab file created earlier in the file explorer.

Note.
The keytab file is not displayed until the next step of the procedure is completed.

5. Specify the user session duration in minutes.

Note.
The user session varies from **5** to **14440** minutes.

6. In the **Services and Kerberos Credentials** group of parameters, click and assign **Proxy server** to the SPN service.
7. In **Authentication**, go to **HTTP proxy** and turn on the **Proxy** toggle.

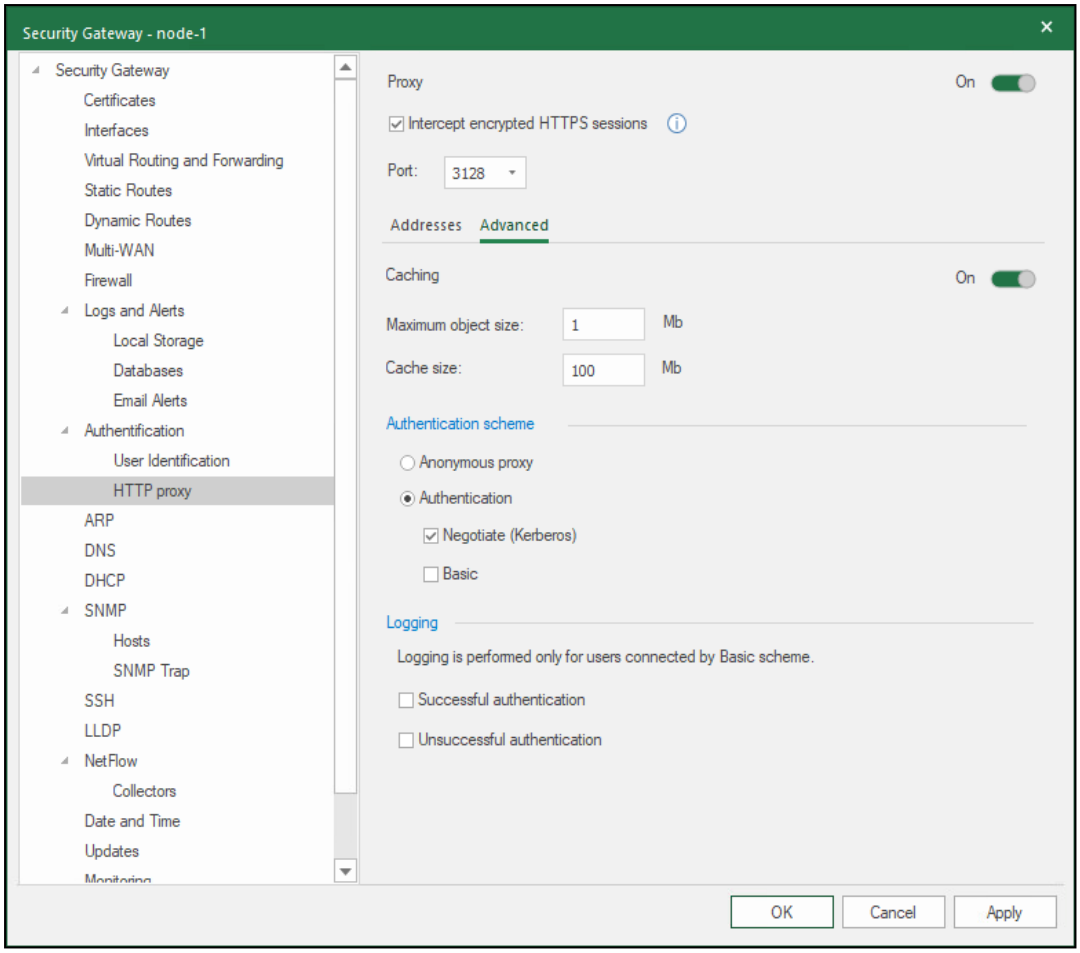


Parameters of authentication via proxy server become available for editing.

8. In the **Proxy server addresses** group of parameters, specify the IP address on which the proxy server will operate.
9. In the **List of allowed addresses** group of parameters, click .

   A dialog box with a list of available network objects appears.

   Note.
   Create a new network object, if necessary. To do so, click **Create**, specify the required parameter values and click **OK**.
10. Select objects that will be allowed access via the proxy server.
11. Go to **HTTP proxy | Advanced**.
12. In the **Authentication scheme** group of parameters, select **Authentication** and select the **Negotiate** check box.
13. Save and apply the policy.



14. Create rules for the proxy server in the **Access control** section (p. **30**).

15. Configure browsers on client workstations (p. **31**).

Basic authentication

To configure Basic authentication, take the following steps:

1. Configure LDAP profile on the Security Management Server, import user groups from the domain controller (see p. **15**).

This step is necessary for the Security Management Server to check whether the user is authenticated in AD.

Note.
If the required LDAP profile is already configured, no additional configuration is needed.

2. Configure the DNS server (see p. **11**).

3. Create proxy server rules for domain user access (see p. **30**).

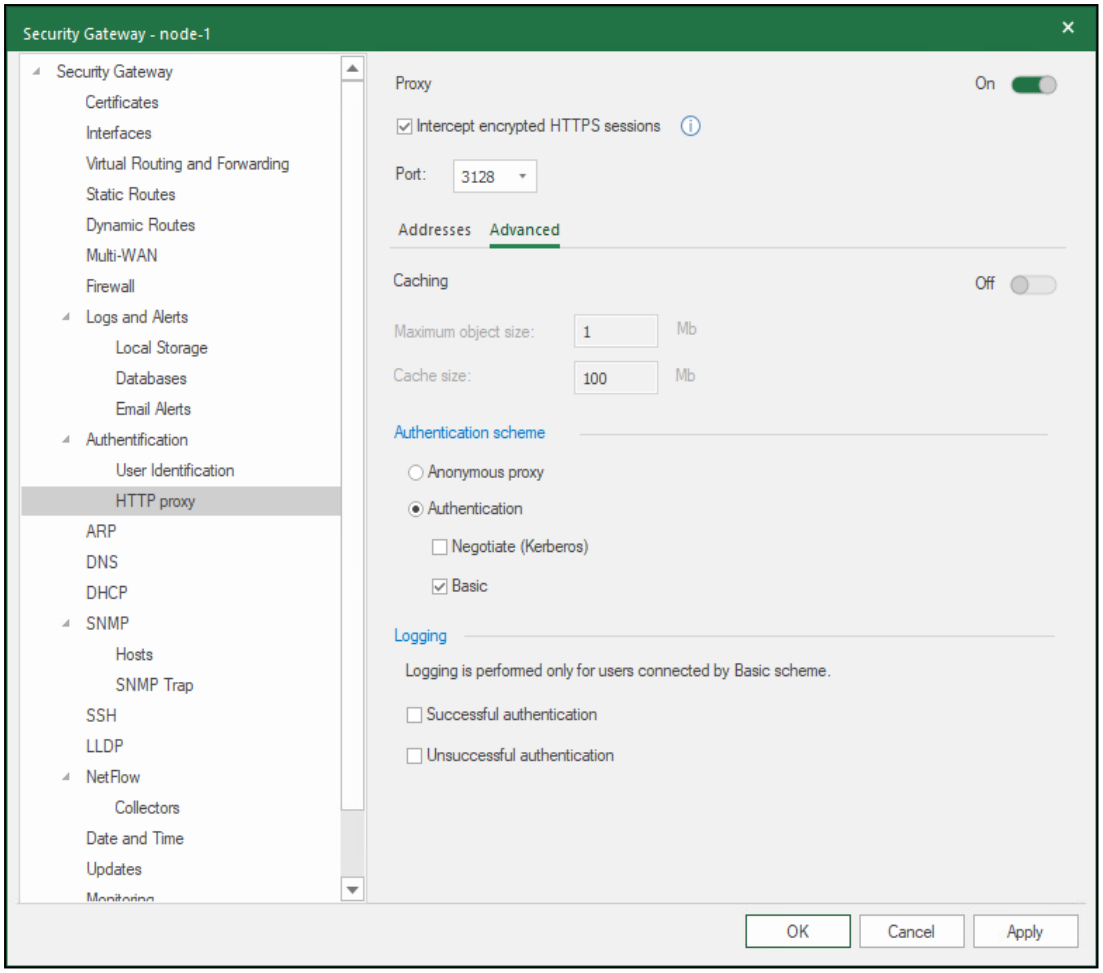
4. Select the authentication scheme (see p. **29**).

5. Configure browsers on client workstations (see p. **31**).

To select the authentication scheme:

1. In Security Gateway properties, go to **Authentication | HTTP proxy**.

2. In the **Authentication scheme** group of parameters, select **Authentication** and select the **Basic** check box.

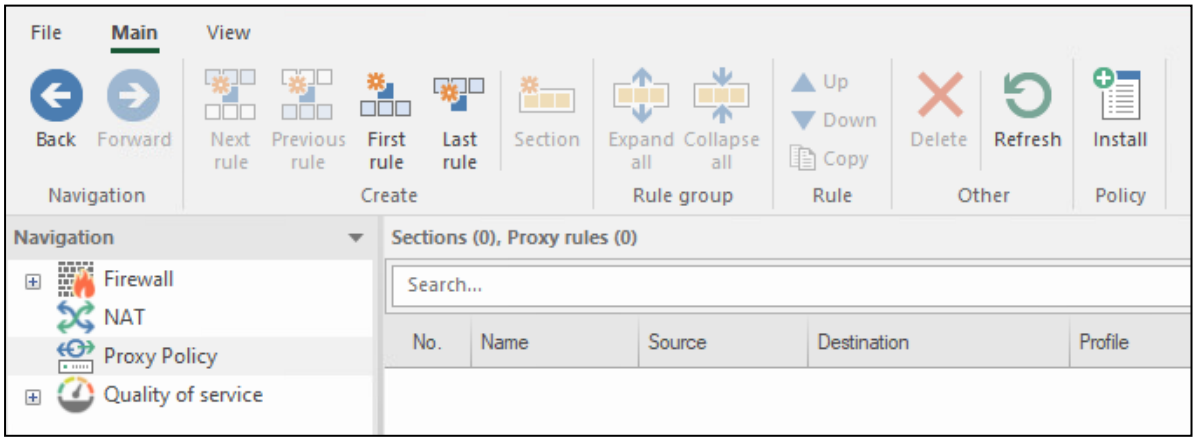


3. If necessary, select the check boxes in **Logging** to enable logging successful or unsuccessful authentication attempts.
4. Click **Apply** and install the policy on the Security Gateway.

Create proxy server rules

To create a proxy server rule:

1. In the Configuration Manager, go to **Access control | Proxy Policy**.



2. Right-click the information display area and select one of the prompts for creating a rule.
   If the rule list is empty, you can create only the first and the last rule.
   A row with a sequence number appears.
3. In the access rule row, specify its name.
4. For the **Source** and **Destination** fields, specify network objects or create new ones.

5. In the **Profile** drop-down list, select the Web/FTP filtering profile or create a new one.
6. In the **Log** drop-down list, select **Log** to enable logging of filtering profile triggers.

   Filtering profile triggers are displayed in the network security log.
7. To install the rule on the Security Gateway, in the **Install On** drop-down list, select the rows with Security Gateways that you need to install the rule on.
8. Install the policy.

Configure a browser for user authentication via proxy server

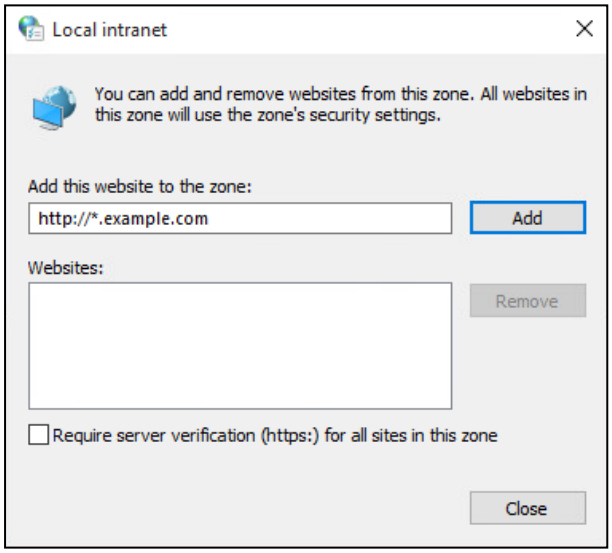
For correct user authentication using Kerberos via proxy, you need to configure browsers on client workstations. We recommend using group policies to configure browsers on corporate workstations.

To configure Chrome, Yandex, Atom, Sputnik, Edge, Internet Explorer:

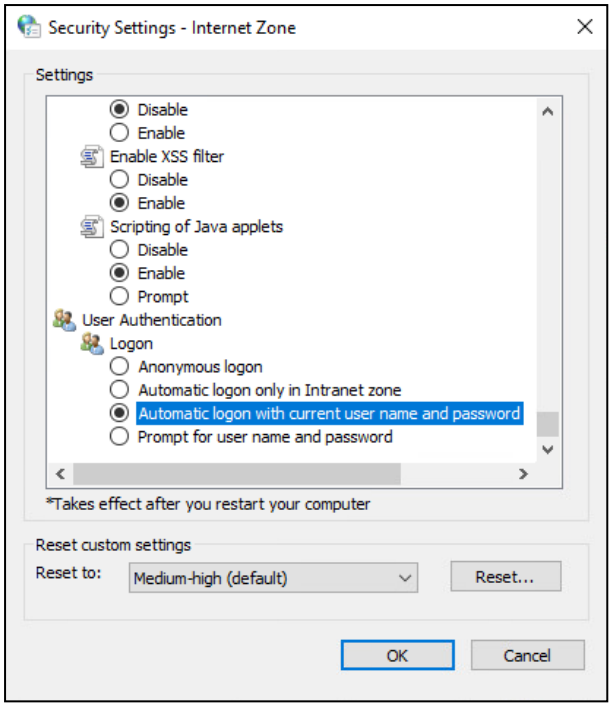
1. In the control panel menu, select **Internet Options**.
2. Go to the **Security** tab and select **Local intranet**.
3. Click **Sites**.

   The **Local intranet** dialog box appears.
4. Click **Advanced**.

   The new **Local intranet** dialog box appears. It contains a list of websites.
5. In the **Add this website to the zone** field, specify the Authentication Portal domain via the HTTPS protocol and click **Add**.



6. Click **Close**, then **OK**.
7. Perform the following actions for each zone in the **Security** tab:
   - In the **Security level for this zone** group of parameters, click **Custom level**.
   - Go to **User Authentication | Logon** and select **Automatic logon with current user name and password**.
   - Click **OK**.

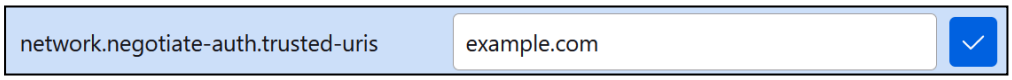


8. In the **Internet Properties** dialog box, click **Apply**.

To configure Firefox:

1. In the address bar, enter **about:config**.

   The **Advanced Settings** window opens in the current tab.
2. In the search bar, enter **network.negotiate**.
3. In the **network.negotiate-auth.trusted-uris** and **network.negotiate-auth.delegation-uris** parameter lines, click **Edit**, specify the Authentication Portal domain name and click **Save**.

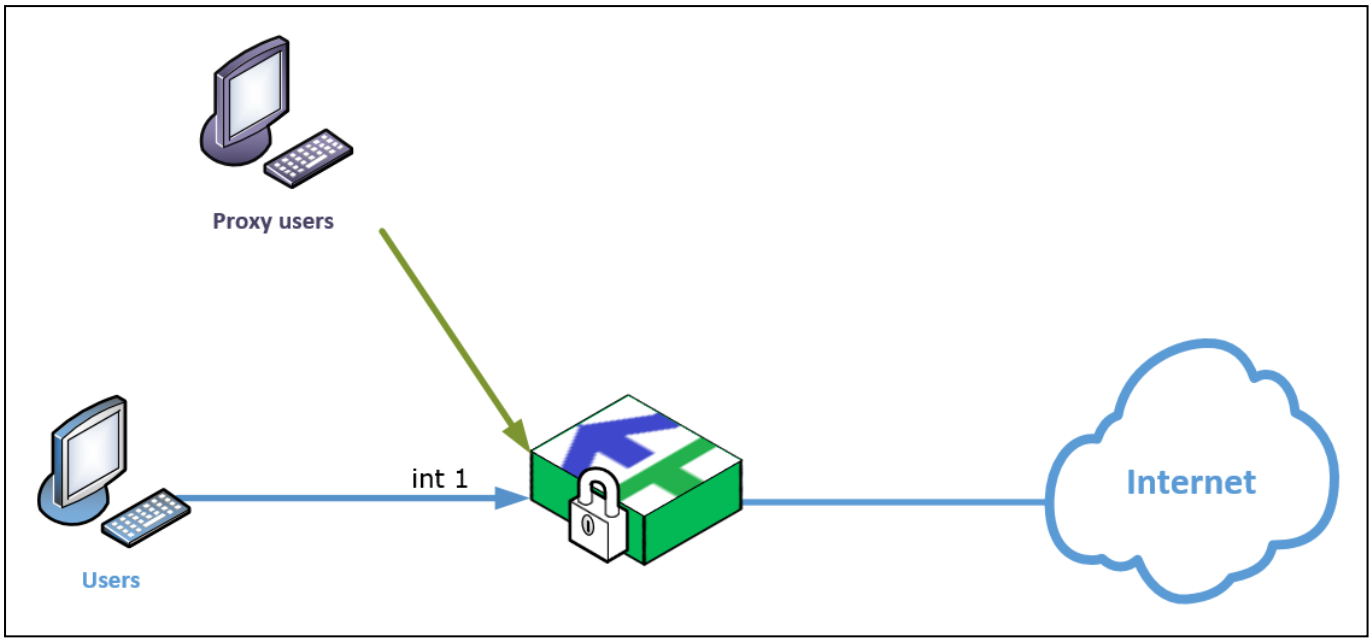


Interoperation between Transparent Kerberos Authentication and proxy server authentication via Kerberos

Below you can see configuration scenarios for interoperation between proxy with Kerberos and SSO.

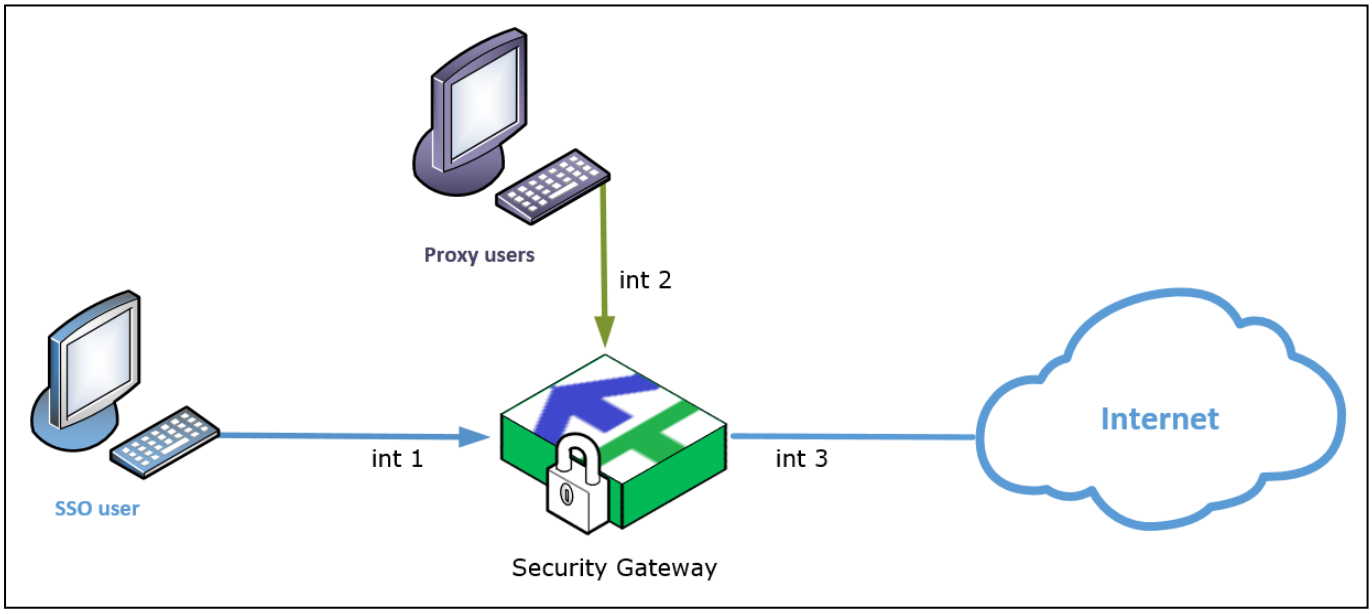
Such configuration implies that some users access the Internet via a proxy server with transparent authentication while the others access the Internet directly, but also using transparent authentication (SSO).

Scenario 1. A single network interface of the Security Gateway is specified as both the proxy interface and the SSO interface. All users access it from within the network.



For example, SSO users and proxy users access the Internet via the **int1** network interface. Both proxy server and transparent authentication (SSO) are configured on this interface. In this case, all you need to do is configure SSO according to the manual and generate the keytab file once. The proxy server address and the portal address (certificate name) will be the same.

Scenario 2. The same interface is specified as the proxy interface and the SSO interface, but users access it from different Security Gateway network interfaces.

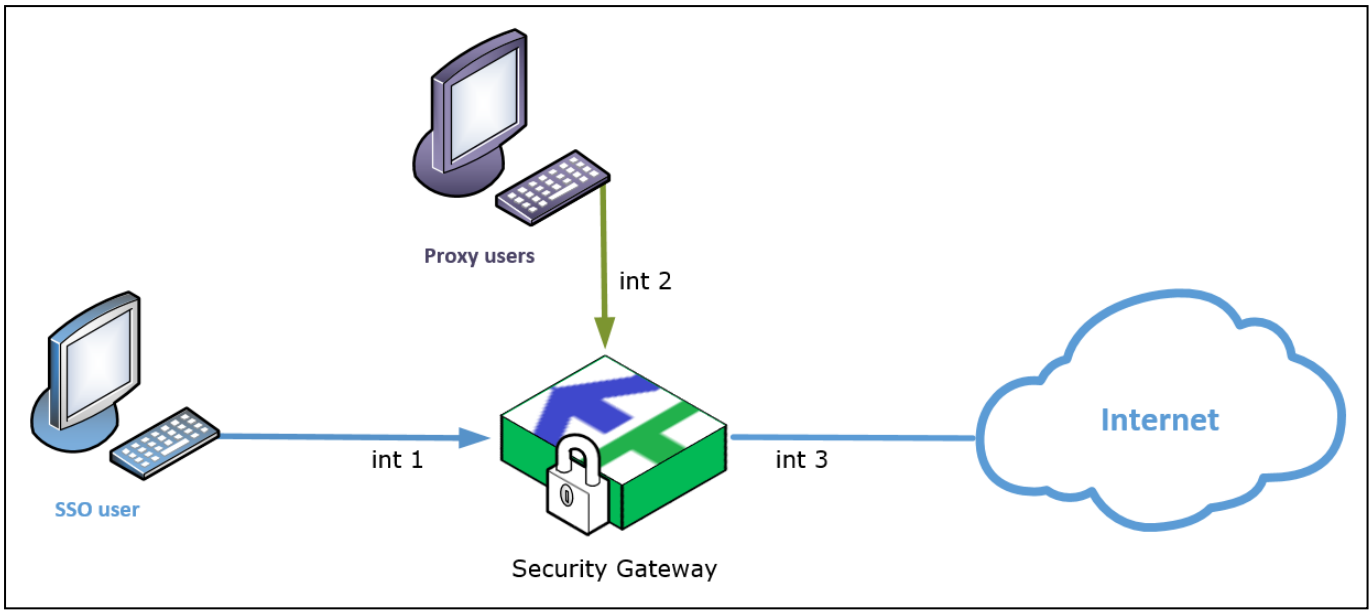


For example, the SSO user accesses the Internet via the **int1** interface while the proxy user gains access via the **int2** interface. Both proxy and SSO are configured on **int1**.

The configuration is the same as the one in scenario 1. You need to generate the keytab file for SSO once and configure settings according to the manual.

Attention!
You need to make sure that internal addresses are not translated when passing through the Security Gateway, i. e. the respective NAT rule with the **Do not translate** translation type is created.

Scenario 3. SSO authentication is configured on one interface while the proxy server is configured on the other.



For example, SSO is configured on the **int1** interface and SSO users access the Internet using the same interface. The proxy server is configured on **int2** and proxy users access the Internet using the same interface.

In this case you need to create a keytab file with two principals. The keytab file with the principal for SSO is always generated first, then the principal for the proxy is added to it.

To generate a keytab file in PowerShell on the AD server:

1. Configure the SPN for the account by running the following command:

   ```
   setspn -A HTTP/auth.testers.local krb
   ```

   where:

   - **auth.testers.local** is the name of the authentication portal certificate and the portal domain name;
   - **krb** is the name of the account in AD created for the keytab file generation and configured accordingly.

   Then, you need to generate the keytab file for the transparent authentication (SSO).

2. During the file generation, the salt is specified. If you already have the SSO keytab file, but the salt (**+dumpsalt**) was not specified from the start, you will not be able to use it in step **3**. In this case we recommend you to regenerate the keytab file.

3. Then, generate the keytab file by running the following command:

   ```
   ktpass /princ HTTP/auth.testers.local@TESTERS.LOCAL /mapuser krb@TESTERS.LOCAL
   /crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL /pass * +dumpsalt /out C:\sso.keytab
   ```

   where:

   - **auth.testers.local** is the DNS name for the IP address of the interface on which SSO operates (must be the same as the name of the authentication portal certificate), followed by **@** and the domain name in upper case (**TESTERS.LOCAL** in this example);
   - **krb@TESTERS.LOCAL** is the Kerberos account in the **TESTERS.LOCAL** domain;
   - **/pass *** means that after entering the command you will need to set the password;
   - **/crypto** indicates the encryption type;
   - **+dumpsalt** means that the salt algorithm used for the key generation will be displayed. The command output is required for extending the keytab file;
   - **/out** specifies the path for saving the keytab file.

   Attention!
   To add the second principal to the keytab file, you need to save the output of this command, specifically **Hashing password with salt "....."**, where you need to specify the hash value in quotes.

4. To add the second principal to the previously generated keytab file, run the following command:

```
ktpass /princ HTTP/proxy.testers.local@TESTERS.LOCAL /mapuser krb@TESTERS.LOCAL
/crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL /pass * /in C:\sso.keytab /out
C:\proxysso.keytab /setupn /setpass/rawsalt"TESTERS.LOCALHTTPauth.testers.local"
```

where:

- **proxy.testers.local** is the DNS name for the IP address of the interface on which the proxy server operates, followed by **@**, the domain address in upper case (**TESTERS.LOCAL** in this example) and values for parameters specified below.
- **krb@TESTERS.LOCAL** is the Kerberos account in the **TESTERS.LOCAL** domain with preconfigured parameters, it was used in the keytab file generation in the previous step;
- **/pass *** means that after entering the command you will need to set the password;
- **/crypto** indicates the encryption type;
- **/in** is the path to the keytab file acquired during the previous step;
- **/out** specifies the path for saving the new keytab file.
- **/setupn** sets the user principal name (UPN) in addition to the service principal name (SPN);
- **/setpass** sets the user password when specified;
- **/rawsalt "..."** uses the hash acquired during the keytab creation in step **3** — the output of the **Hashing password with salt** option.

5. You need to bind the acquired keytab file to the Security Gateway and configure authentication according to the procedure on p. **23**.

Identification Agent

Install the Identification Agent on a computer with Windows OS.

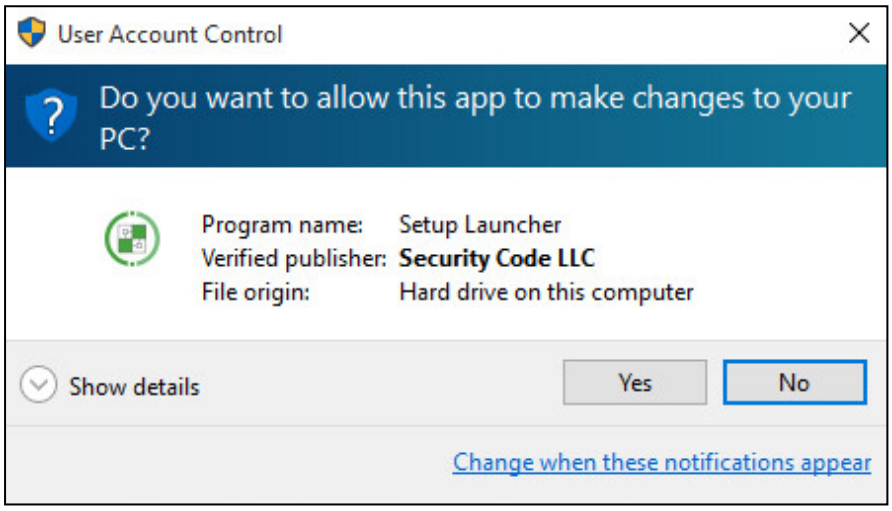
Before enabling the Identification Agent, configure the Authentication Portal (see p. **10**).

To enable the Identification Agent with AD, configure LDAP interconnection (see p. **15**).

Install the Identification Agent

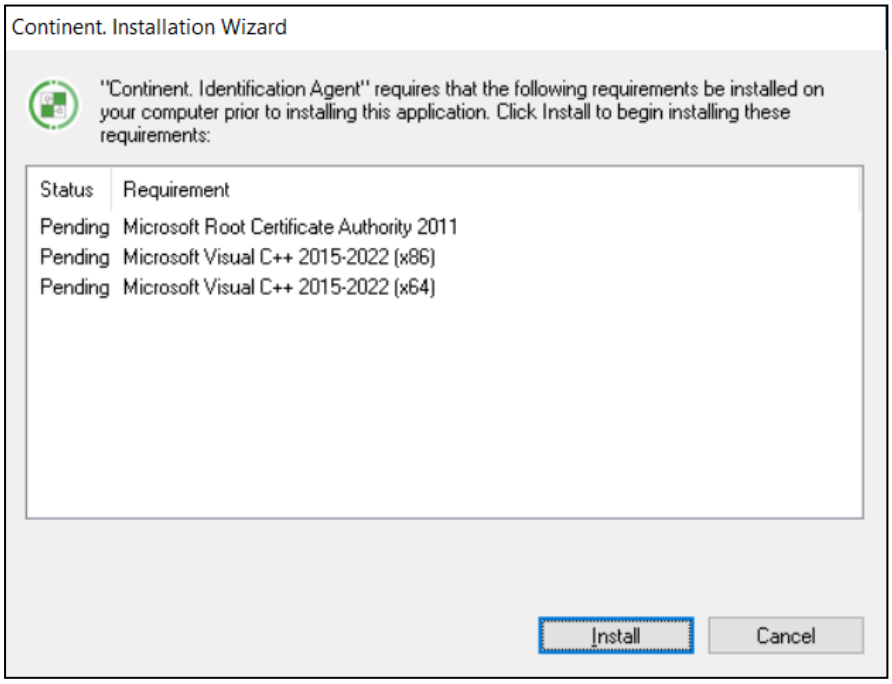
To install the program:

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.

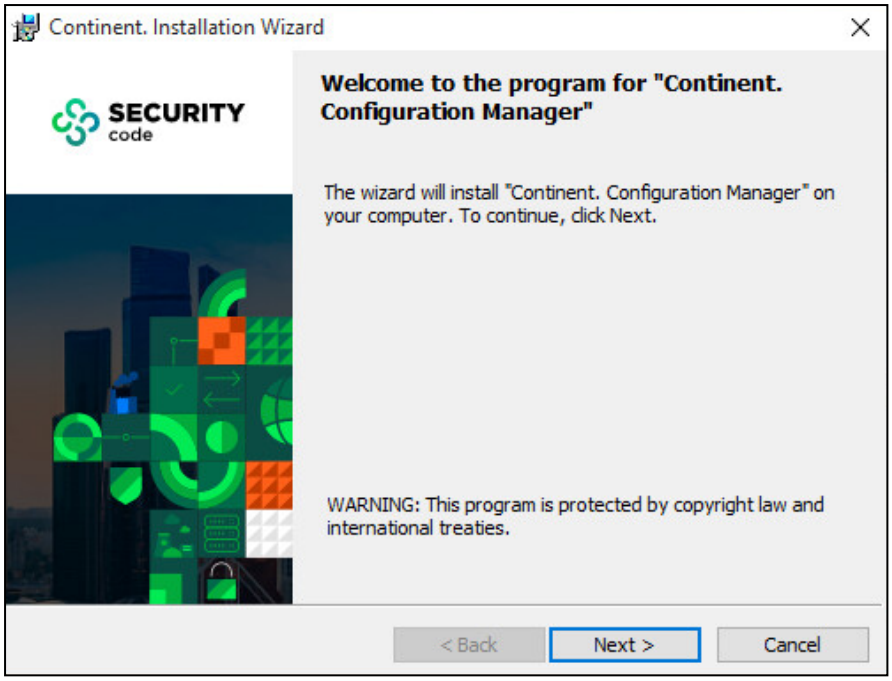


3. Before installing the Identification Agent, make sure the components that are required for its correct operation are installed.

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

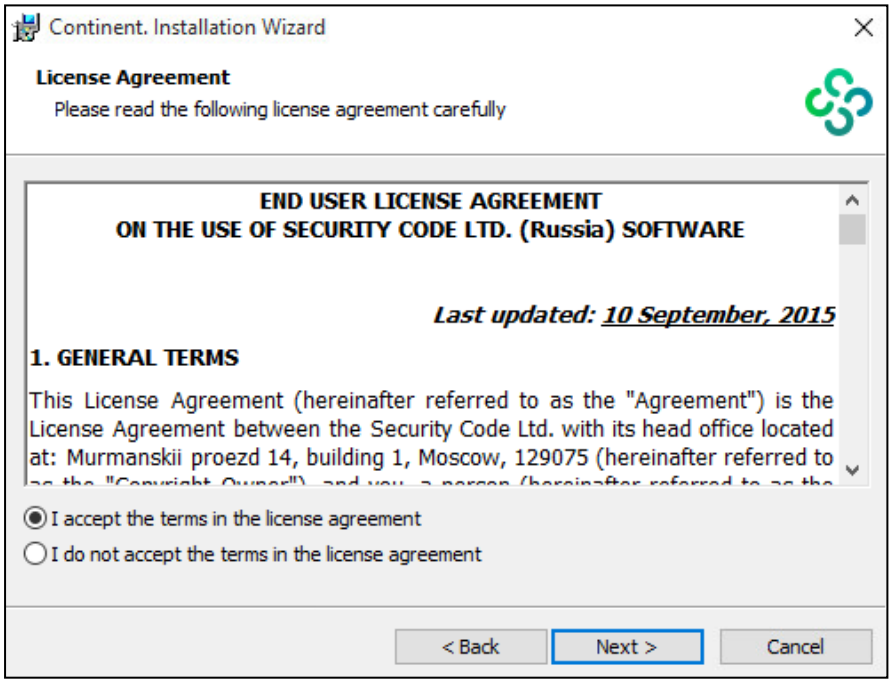


   The **Continent. Installation Wizard** dialog box appears.



4. Click **Next** to continue.

The license agreement appears as in the figure below.



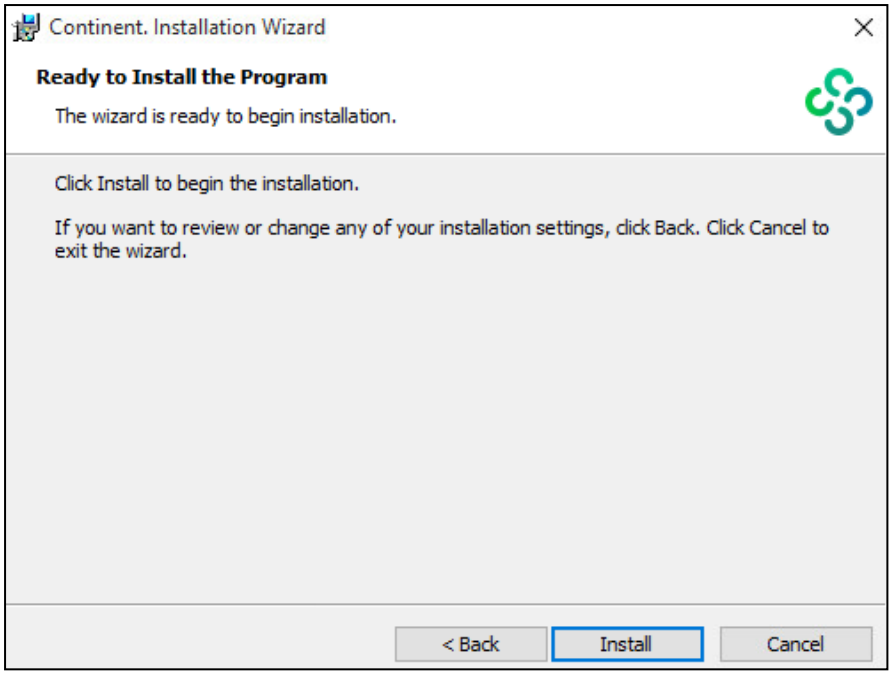
5. Read the license agreement. If you accept the terms, select the **I accept the terms in the license agreement** check box and click **Next**.

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**.

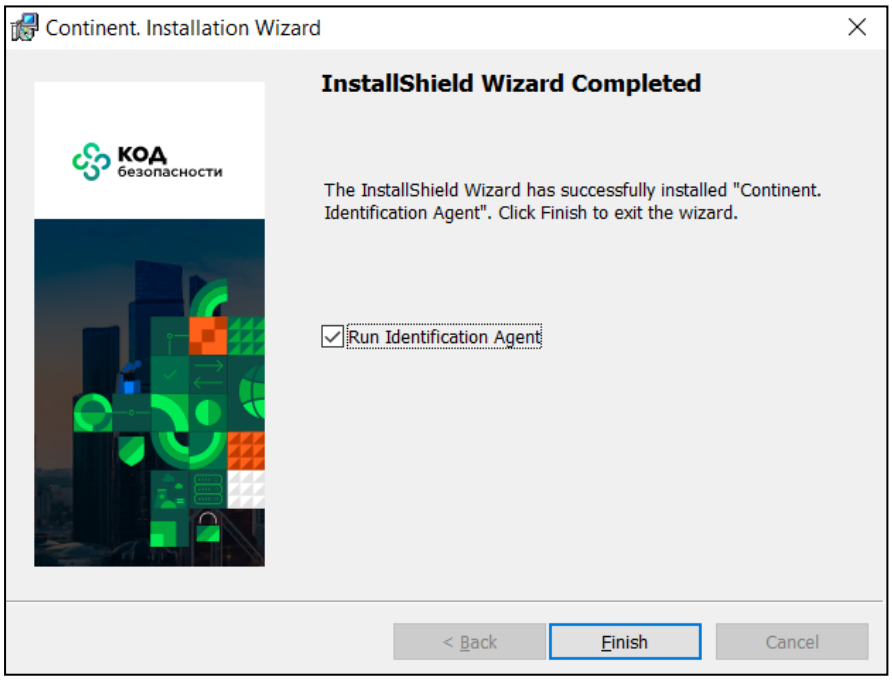
The **Ready to Install the Program** dialog box appears.



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:  .

Run the Identification Agent

To run the program 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 program run at startup:

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

   The respective dialog box appears.
2. Select the **Start automatically agent** check box and click **OK**.

Configure the Identification Agent

To configure the connection using the Configuration Manager:

1. Go to **Structure**, select the Security Gateway with the Authentication Portal and click **Properties** on the toolbar.

   The respective dialog box appears.
2. On the left, go to **Authentification | User Identification**, then turn on the **Authentication Portal** toggle and select the **Allow agent to work** check box.
3. Set the **Client keepalive timeout** value (maximum wait time — **120** minutes, minimum wait time — **5** minutes).

4. Click **OK**.
5. Click **Apply** to save the configuration.

To configure the connection on a user's workstation:

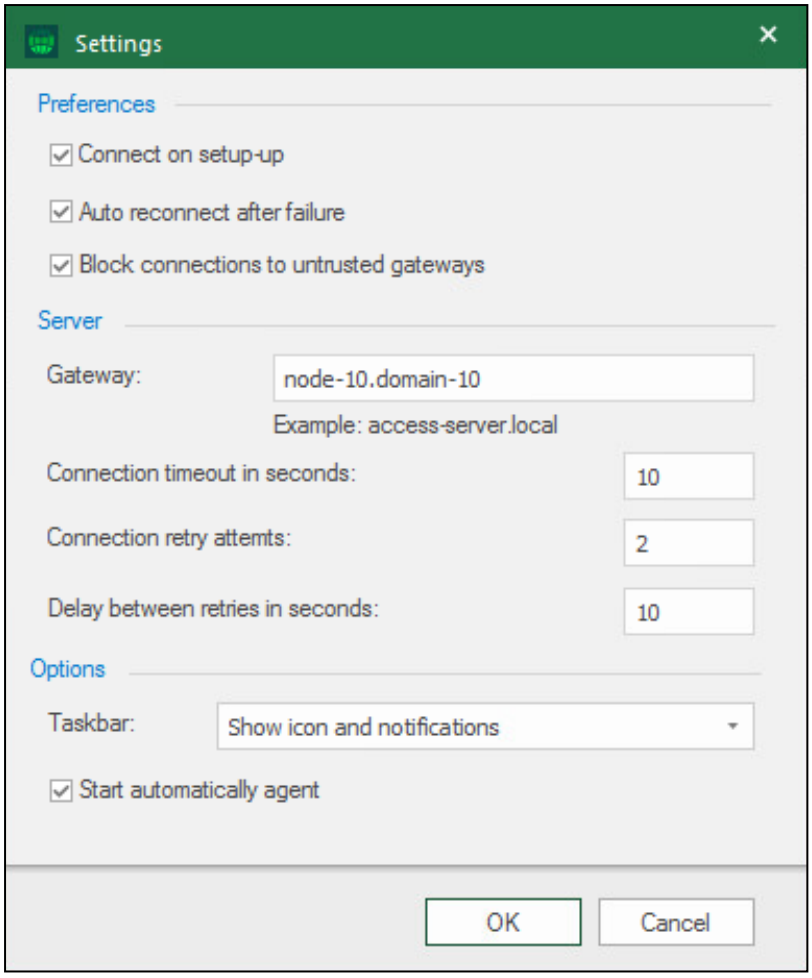
1. In the Windows tray, right-click the **Identification Agent** icon.
2. Click **Settings**.

   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.

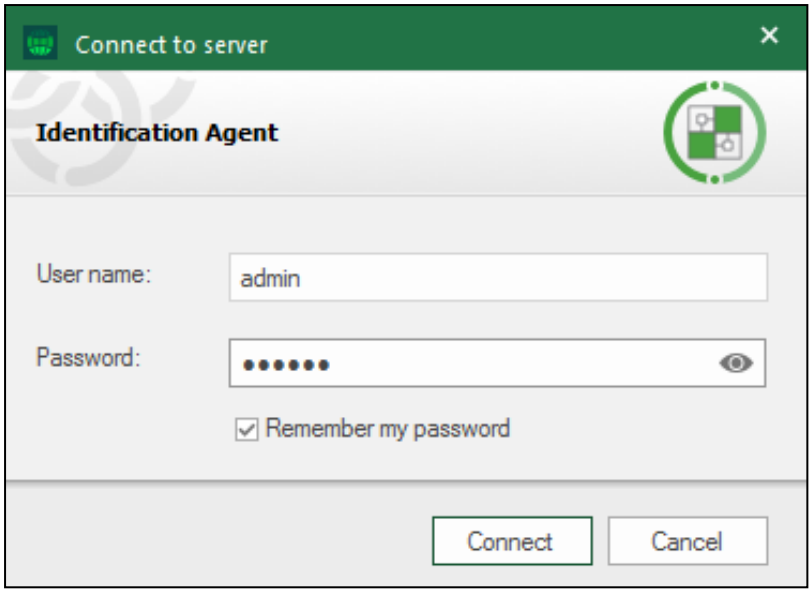


3. In the **Gateway** text box, enter the domain name of the required AD server.
4. Select the required check boxes and specify the required parameters. The connection timeout value can be between **5** and **60**, the number of connection retry attempts is between **1** and **5**, the delay between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

Uninstall the Identification Agent

To uninstall the program:

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 a successful uninstallation, you receive the respective message.
5. Click **Finish**.