

Continent Enterprise Firewall Version 4

Authentication

Administrator guide



© 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
Configuration and use	
How the Authentication Portal works	7
How the Identification Agent works	
How Transparent Kerberos Authentication works	
Preconfigure the Security Gateway	
Issue authentication certificates	
Add a certificate to the Security Gateway	
Add users over LDAP	
Configure LDAP	
Create Firewall rules	
Authentication parameters configuration	
Authentication via the Authentication Portal	
Configure Transparent Kerberos Authentication	21
Configure a browser for user authentication via the Authentication Portal	24
Configure authentication on the proxy server	
Negotiate (Kerberos) authentication	
Basic authentication	
Create proxy server rules	
Configure a proviser for user authentication via proxy server	tication via Kor-
heros	32
Install the Identification Agent	
Kun the Identification Agent	
Configure the Identification Agent	
Connect to the Security Gateway	
Uninstall the Identification Agent	

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
ТСР	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 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.

Security Gateway - SG-1		×
 Security Gateway Certificates User Identification Interfaces Static Routes Dynamic Routes Muti-WAN Firewall Logs and Alerts Local Storage Databases DNS DHCP 	DNS Servers Preferred: Alternate 1: Alternate 2: Domain:	

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.

Security Gateway	A	-	-				
Certificates		Time zone:	GMT				*
Interfaces		Network Syn	chronization				On
Static Routes		Automatically	synchronize	the Security Manag	ement Server with	an Internet	
Dynamic Routes		Time Server ((NTP)				
Multi-WAN		Primary NTP	Server				
Firewall		Address:					
 Logs and Alerts 							
Local Storage		Authenticat	ion type:	None			*
Databases		Secondary N	TP Server				
Email Alerts		Addresse					
DNS		Address.					
DHCP		Authenticat	ion type:	None			*
✓ SNMP							
Hosts							
SNMP Trap							
SSH							
LLDP							
⊿ NetFlow							
Collectors							
Date and Time							
Updates							
Monitoring							
Access to SMS	-						

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.

Root certificate				×
Certificate owner data —				
Common Name:				
Description:				
Organization:		Organization Unit:		
State:		Locality:		
Email:		Country:		
Key usage				
Digital signature	Data encipherment	CRL signing		
Non-repudiation	Key agreement	Encipher only		
Key encipherment	Certificate signing	Decipher only		
Advanced				
Signature algorithm: RS	A (2048)	Valid to (UTC):	May /21/2024 09	:34:25 *
			Create certificate	Cancel

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:

- 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.

Certificate			×
Certificate type: Aut Certificate owner dat Use Enter data for the ne Aut Common Name: Wet	hentication portal inistrator r hentication portal ess Server urity gateway o-monitoring	*	
Description: Organization: State: Email:		Organization Unit: Location: Country: RU	
Key usage ✓ Digital signature ✓ Non-repudiation ✓ Key encipherment	Data encipherment Key agreement Certificate signing	 □ CRL signing ✓ Encipher only □ Decipher only 	
Advanced Root certificate: Signature algorithm:	RSA (2048)	Valid to (UTC): May /21/2020 09:39	• 52 •

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.

Intermediate certificat	te ×
Certificate type: Certificate owner da	Authentication portal-redirect
Enter data for the n	ew certificate or load request data
Common Name:	
Description:	
Organization:	Organization Unit:
State:	Location:
Email:	Country:
Key usage	
☑ Digital signature	Data enciphement
Non-repudiation	☐ Key agreement ☐ Encipher only
Key encipherme	nt Certificate signing Decipher only
Advanced	
Root certificate:	RSA ×
Signature algorithm	RSA (2048) Valid to (UTC): May /21/2020 09:47:54 *
	Create certificate Cancel

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.
- In the display area, select the Security Gateway and click Properties on the toolbar. The Security Gateway dialog box appears.

ecurity Gateway	Server Certificates			
Certificates				
Interfaces	Certificates of the security gi	ateway and its components:	0 🧪	X
Static Routes	Name	Issued by	Role	V
ynamic Routes				
-WAN	Eg SG-1	Root_cert	Security gateway	18
vall				
s and Alerts				
Local Storage				
Databases				
Databases				
Databases S CP				
Databases S CP MP				
Databases S IP IP P				
Databases IS ICP IMP DP tRow	4			
Databases VS HCP DP tFlow Collectors	Boot Certificates			
Databases 5 5P AP P Row Collectors e and Time	Root Certificates			
Jatabases	Root Certificates Trusted root certificates of th	ie security gateway:	0/	
w ollectors und Time vccess	Root Certificates Trusted root certificates of th Name	ne security gateway:	Valid from	
latabases 5 5 5 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Image: Second control of the second	ne security gateway: Issued by Root_cert	Valid from 18.01.2022 10:12	
Databases ; ;P IP P P Collectors ; and Time Access	Image: Trusted root certificates of the second s	e security gateway: Issued by Root_cert	Valid from 18.01.2022 10:12	

- 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 **(**.

oot Certificates Trusted root certificate	s of the security gateway		0 🗡 🗙	
Name	Issued by	Valid from	Valid to	
🔄 Доверенный	Доверенный Издат	30.05.2017 13:34	30.05.2028 13:44	
🔁 CN	CN	17.05.2023 13:13	15.05.2028 13:13	
•			1	
	Γ	OK Cance	Apply	

- 6. Click OK.
- 7. On the toolbar, click Install.

The **Install policy** dialog box appears.

Sea	arch			
	Status		Name	Configuration
	Online	¢	node-10	10078
	🕗 Online	e ►	node-11	10078
	🕑 Online		SC-1	10095
V	🕑 Online		SG-3	10093
4				

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.

LDAP profile				×
Name:				
Domain				
Name:				
Base DN:				-
Authentication				
User:				
Password:				
Confirm password:				
	Enable SSL securit	у		
Servers				
Primary and second	lary LDAP servers:			0 🗡 🗙
Server		Address		Port
	1 No	items found.		<u> </u>
			OK	Cancel .:

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:

<i>"</i> » <i>"</i> * <i>(</i>) <i>– – – – – – – – – –</i>	"	/
\sim π $($ $)$ $ ($ $)$	-	· ·

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.

Name.	testers.corp		
Domain			
Name:	testers.local		
Base DN:	DC=testers, DC=	=local	
Authentication			
User:	tstuser@test	local	
Password:	•••••	••••	
Confirm passw	vord:	••••	
Servers			
Primary and se	econdary LDAP serve	ศร:	0 🗡 🗙
Server		Address	Port
AD		172.17.10.1	636

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.

		10.1.1.10 - Continent. Confi	guration manager			· -	ē ×
File Main View						Built-in admini	istrator 🎮 🕜
Back Forward Navigation	First Last Section rule rule Rule gr		t X Delete Refresh	nstall			
Navigation 👻	Sections (0), Rules (0)						
🕞 🎇 Firewall	Search						Q
Web/FTP filter groups Web/FTP filtering profile	e No. Name	Source	Destination	Service	Application	Action	Pro
Web/FP filtering except NAT Coulity of service Coulity of service Coc profiles	(Objects □ II & M □ @ @ () Name) 88 Search Address Man	No tems i sk	found.	▼-		* ×
Access control			🚹 No items	found.			
VPN SIPS Structure Administration							

- **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**.

Security Gateway	Authentication	Portal	Off
Certificates			
Interfaces	User session d	furation: 720 minutes	
Virtual Routing and Forwarding	Allow agent	t to work	
Static Routes	Client keep	palive timeout: 30 📫 minutes	
Dynamic Routes	Kerberos authe	entication	Off
Multi-WAN	Rasic settings		
Firewall	busic settings		
⊿ Logs and Alerts	Certificate:		.*.
Local Storage			
Databases	The address	of interfaces available for user identification	on: OX
Email Alerts	Address	Description	
 Authentification 		Description	
User Identification		(1) No items fo	ound.
HTTP proxy			
ARP			
DNS			
DHCP	Address rang	es redirected to the captive portal:	
⊿ SNMP			
Hosts	Search		٩
SNMP Trap	Name	Address/Mask	
SSH			
LLDP		1 No items fo	ound.
⊿ NetFlow			
Collectors			
Date and Time			
Updates			
Manhadan	Ŧ		

- 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.
- 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.

Security Gateway	Authentication Portal		00
Certificates	Automodulor Forda		
Interfaces	User session duration:	720 C minutes	
Virtual Routing and Forwarding	Allow agent to work		
Static Routes	Client keepalive timeout:	30 🗘 minutes	
Dynamic Routes	Kerberos authentication		Off
Multi-WAN	Dasia acttings		
Firewall	basic settings		
 Logs and Alerts 	Certificate: auth.teste	ers.local	-
Local Storage			
Databases	The address of interfaces ava	ilable for user identification:	\circ \times
Email Alerts	Address	Description	
 Authentification 	huureaa	beauption	
User Identification	10.24.42.1	ge-0-0	
HTTP proxy			
ARP			
DNS			
DHCP	Address ranges redirected to t	he captive portal:	0 2 X
⊿ SNMP			
Hosts	Search		ρ
SNMP Trap	Name	Address/Mask	
SSH	De Net Drivete 10.0.0.0/9	10.0.0.0/8	
LLDP	TT Net_Private_10.0.0/o	10.0.0/8	
⊿ NetFlow			
Collectors			
Date and Time			
Updates			

- 8. Specify addresses of the interfaces on which user identification will operate.
- 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.

Ś	
NAME	
PASSWORD	
Log in	

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.

 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.

ew Object - User			×
Create in:	testers.local/Users		
First name:	αb	Initials:	
Last name:			
Full name:	da		
User logon name:			
krb	@testers.lo	cal	\sim
User logon name (pre-V	/indows 2000):		
TESTERS\	krb		
-			

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 256bit 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> <mark>ktpas</mark>s /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 on 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.

Security Gateway		Autoritanting Ded				04
Certificates		Authentication Pon	a			Off Off
Interfaces		User session durati	ion:	720 🗘 minut	es	
Virtual Routing and Forwarding		Allow agent to v	vork			
Static Routes		Client keepaliv	e timeout:	30 🗘 minute	es	
Dynamic Routes		Kerberos authentic	ation			On Co
Multi-WAN			auon			
Firewall		Basic settings —				
✓ Logs and Alerts		Certificate:	auth.teste	rs.local		Ŧ
Local Storage						
Databases		The address of in	terfaces avai	lable for user identific	ation:	O ×
Email Alerts		Address		Description		
 Authentification 		Address		Description		
User Identification		10.24.42.1		ge-0-0		
HTTP proxy						
ARP						
DNS						
DHCP		Address ranges re	directed to t	ne cantive portal:		
✓ SNMP		i dareas ranges re		to captive portai.		
Hosts		Search				م
SNMP Trap		Name		Address/Mask		
SSH			10.0.0.0	10.0.0.0		
LLDP		Net_Private	_10.0.0.0/8	10.0.0/8		
⊿ NetFlow						
Collectors						
Date and Time						
Updates						
Monitoring	-					

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**.

here and the second sec	;
You can add and remove websites from this zone will use the zone's security se	n this zone. All websites ir ettings.
Add this website to the zone:	
http://*.example.com	Add
Websites:	Remove

- 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.

🏫 Security Settings - Internet Zone	Х
Settings	
Logon Anonymous logon Automatic logon only in Intranet zone Automatic logon with current user name and password Prompt for user name and password ✓ ✓ ✓	
*Takes effect after you restart your computer	
Reset custom settings	
Reset to: Medium-high (default) V Reset	
OK Cancel	

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

To configure Firefox:

- 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**.

network.negotiate-auth.trusted-uris	example.com	\checkmark	
-------------------------------------	-------------	--------------	--

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:

 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.

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.

New Object - User		\times
Create in:	testers.local/Users	
First name:	krb Initials:	
Last name:		
Full name:	krb	
User logon name:		
kıb	@testers.local ~	
User logon name (pre	-Windows 2000):	
TESTERS\	krb	
	< Back Next > Cance	el

- 2. In the account properties, select Account and, in account parameters, enable This account supports 256bit 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

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-ADSO1.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 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.

Security Gateway		Provid		0.
Certificates		ноху		
Interfaces		Intercept encrypted HTTPS	S sessions 🕧	
Virtual Routing and Forwarding		Port: 2129		
Static Routes		5126		
Dynamic Routes		Addresses Advanced		
Multi-WAN				
Firewall		Proxy server addresses:		0>
 Logs and Alerts 			-	
Local Storage		Address	Description	
Databases		10.24.42.1		
Email Alerts				
 Authentification 				
User Identification	_			
HTTP proxy				
ARP				
DNS		List of allowed addresses:		0 🖉 🔪
DHCP		Name	Address /Mask	
SNMP		Indilie	Address/ Mask	
Hosts		Private_10.0.0/8	10.0.0/8	
SNMP Trap				
SSH				
LLDP				
✓ NetFlow				
Collectors				
Date and Time				
Updates	-			

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:

 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.

Security Gateway		Deput,	0
Certificates		Froxy	
Interfaces		✓ Intercept encrypted HTTPS sessions ()	
Virtual Routing and Forwarding		Part: 2120 -	
Static Routes		10k. 3128 *	
Dynamic Routes		Addresses Advanced	
Multi-WAN			
Firewall		Caching	Off
✓ Logs and Alerts		Mb.	
Local Storage		Maximum object size: 1	
Databases		Cache size: 100 Mb	
Email Alerts			
 Authentification 		Authentication scheme	
User Identification		O Anonymous proxy	
HTTP proxy		Authentication	
ARP			
DNS		Negotiate (Kerberos)	
DHCP		✓ Basic	
✓ SNMP		l	
Hosts		Logging	
SNMP Trap		Logging is performed only for users connected by Basic scheme.	
SSH		Successful authentication	
LLDP			
⊿ NetFlow			
Collectors			
Date and Time			
Updates			
Monitoring	•		

- **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.

														_
File	Main	View												
Back	Forward	Next rule	Previous rule	¥ □I Fi	irst Las	t Section	Expa all	nd Collapse all		Up Down Copy	X Delete	9 Refresh	Install	
Navi	gation			Cr	eate		Ru	ile group	R	Rule	Ot	her	Policy	
Navigati	ion			Ŧ	Sections	(0), Proxy rul	es (0)							
±	Firewall				Search									
X O		liev			No.	Name	:	Source	[Destinatio	n		Profile	
		hicy			- C.									_
± 🍊	Quality o	of service												

- 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.

😪 Local intranet	×
You can add and remove websites from this zone. All v this zone will use the zone's security settings.	vebsites in
Add this website to the zone:	
http://*.example.com	Add
Websites:	emove
Require server verification (https:) for all sites in this zone	
	Close

- 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:

- 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**.

network.negotiate-auth.trusted-uris	example.com	~	
-------------------------------------	-------------	---	--

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.





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).

- 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.

🔮 Use	er Accour	nt Control	×
?	Do yo PC?	u want to allow	this app to make changes to your
		Program name: Verified publisher: File origin:	Setup Launcher Security Code LLC Hard drive on this computer
⊘ sł	now detai	ls	Yes No
			Change when these notifications appear

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.

Continent. Installation Wizard
"Continent. Identification Agent" requires that the following requirements be installed on your computer prior to installing this application. Click Install to begin installing these requirements:
Status Requirement Pending Microsoft Root Certificate Authority 2011 Pending Microsoft Visual C++ 2015-2022 (x86) Pending Microsoft Visual C++ 2015-2022 (x64)
<u>I</u> nstall Cancel

The Continent. Installation Wizard dialog box appears.



4. Click Next to continue.

The license agreement appears as in the figure below.

😸 Continent. Installation Wizard			×
License Agreement Please read the following license agreen	nent carefully		ංදිං
END USER LI ON THE USE OF SECURITY	CENSE AGREE CODE LTD. (F	MENT Russia) SOFTWA	RE
	Last upd	ated: <u>10 Septen</u>	<u>ıber, 2015</u>
1. GENERAL TERMS			
This License Agreement (hereinaft License Agreement between the Se at: Murmanskii proezd 14, building	er referred to curity Code Lt 1, Moscow, 12	as the "Agreeme d. with its head of 9075 (hereinafter	ent") is the fice located referred to
• I accept the terms in the license agreem	ent		
\bigcirc I do not accept the terms in the license a	agreement		
	< Back	Next >	Cancel

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.

Continent. Installation Wizard			×
Ready to Install the Program			<u>.</u> C.
The wizard is ready to begin installation	on.		్య
Click Install to begin the installation.			
If you want to review or change any exit the wizard.	of your installatior	ı settings, dick Back.	Click Cancel to
	< Back	Install	Cancel

7. Click Install.

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

🕼 Continent. Installation Wi	zard	\times
	InstallShield Wizard Completed	
	The InstallShield Wizard has successfully installed "Continent. Identification Agent". Click Finish to exit the wizard.	
	< Back Einish Cancel	

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:

- 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.
- Set the Client keepalive timeout value (maximum wait time 120 minutes, minimum wait time 5 minutes).

Authentication Portal		On	
User session duration:	720 🗘 minutes		
Allow agent to work			
Client keepalive timeout:	30 🌲 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.

💮 Settings				×
Preferences				
Connect on setup	up			
Auto reconnect af	er failure			
Block connections	to untrusted gateways			
Server				
Gateway:	node-10.domain-10			
	Example: access-server.lo	ocal		
Connection timeout in	seconds:		10	
Connection retry atter	nts:		2	
Delay between retries	in seconds:		10	
Options				
Taskbar: Sho	w icon and notifications		*	
Start automatically	agent			
	ОК		Cancel]

- **3.** In the **Gateway** text box, enter the domain name of the required AD server.
- 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:

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

Gonnect to server		×
Identification	Agent	
User name:	admin	
Password:	•••••	۲
	Remember my password	
	Connect	Cancel

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 \blacksquare 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: \blacksquare .

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.
- 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.