

Continent Enterprise Firewall Version 4

Authentication

Administrator guide



© SECURITY CODE LLC, 2023. 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	
Issue authentication certificates	
Add a certificate to the Security Gateway	
Add users over LDAP	
Configure LDAP	
Create Firewall rules	
Authentication Portal	
Preconfigure the Security Gateway	
Authentication parameters configuration	
Authentication via the Authentication Portal	
Configure Transparent Kerberos Authentication	22
Identification Agent	
Install the Identification Agent	
Run 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
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 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 4.1.7 — Released on December 5th, 2023.

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 single sign-on with Kerberos (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 and network address translation. A group of users is connected to a specific network object. Access granted to this group is available only on computers related to this network object.

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 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.

The SPNEGO protocol is used to ensure the mechanism of browser transparent authentication in Continent. The whole authentication process looks as follows:



- **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. 25).

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. 10).
- 2. Issue an Authentication Portal certificate (see p. 10).
- 3. Issue an Authentication Portal certificate for redirection (see p. 11).

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]		
Organization: State: Email:		Organization Unit: Locality: Country:		
Key usage Digital signature Non-repudiation Key enciphement	☐ Data encipherment ☐ Key agreement ✔ Certificate signing	CRL signing		
Advanced Signature algorithm:	RSA (2048) 🔹	Valid to (UTC):	May /21/2024 09:34:25 *	

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.
- On the toolbar, click Certificate.
 The Certificate dialog box appears.

Certificate type: Auth	entication portal	-			
Certificate owner dat	inistrator				
Enter data for the ne	entication portal				
Common Name: Acce Secu Web	iss server rity gateway -monitoring				
Description:					
Organization:		Organization Unit:			
State:		Location:			
Email:		Country:	RU		
ey usage					
Digital signature	Data encipherment	CRL signing			
Non-repudiation	Key agreement	Encipher only			
Key enciphement	Certificate signing	Decipher only			
dvanced					
Root certificate:	root_certificate				-
Signature algorithm:	RSA (2048)	Valid to (U	JTC): 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 certificate name must be exactly the same as the fully qualified domain name (FQDN) of the Security Gateway stored in the DNS server.

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 certifica	ate	×
Certificate type: Certificate owner da Enter data for the	Authentication portal-redirect ata new certificate or load request data	•
Common Name:		
Description: Organization: State:		Prganization Unit:
Email:	C	Country:
Key usage		
🔽 Digital signatur	e Data encipherment	CRL signing
Non-repudiation	n Key agreement	Encipher only
Key encipherm	ent Certificate signing	Decipher only
Advanced		
Root certificate:	RSA	•
Signature algorithm	n: 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**.
- 2. In the display area, select the Security Gateway and click **Properties** on the toolbar.

The **Security Gateway** dialog box appears.

Security Gateway - SG-1			×
Security Gateway Certificates Interfacee	Server Certificates	ateway and its components:	
Titeraces Static Routes Dynamic Routes Multi-WAN Firewall ▲ Logs and Alerts Local Storage Databases	Name	Issued by Root_cert	Role Val Security gateway 18.
DNS DHCP SNMP LLDP NetRow Collectors Date and Time SSH Access	Root Certificates Trusted root certificates of t	he security gateway:	•
	Name	Issued by	Valid from
	Root_cert	Root_cert	18.01.2022 10:12 Image: Cancel

- 3. Go to Security Gateway | Certificates.
- 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 .

loot Certificates	es 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
E CN	CN	17.05.2023 13:13	15.05.2028 13:13
4			
		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
1	🕑 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 users over LDAP or creates new ones. 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 LDAPS.

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	ly .		
Servers				
Primary and second	lary LDAP servers:			0 🗪 🗙
Server		Address		Port
	1 No	items found.		
			ОК	Cancel

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

Note.

To enable AD, use the domain administrator account. We recommend creating a separate account for this purpose.

In the **Authentication** group box, enter the credentials of the domain administrator 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. Specify the AD server IP address and port for connection in the LDAP profile dialog box.

Attention! It is forbidde	en to use th	e following	character	s in the Al) server (divisions:							
«	»	#	*	()	=	+	١	;	"	>	<	,
Attention! The connec	tion to the	AD server i	s establisl	hed over L	DAPS.								
Note.							- (°			:u. u 0.	- C 1'		
To support AD server	the LDAPS	S protocol, p	ports with	the same	number	must be co	onfigured on	the work	station w	ith the Co	nfiguration	Manager a	nd o

Name.	testers.corp					
Domain						
Name:	testers.local					
Base DN:	DC=testers, DC=	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 **User Identification**.

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.

Note.

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 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. C	onfiguration manager			H - //	ā ×
File Main View						Built-in administrate	or 🎮 😭
Back Forward Navigation	First Last rule Section all all Rule	Collapse all Copy Rule	rop Delete Refresh Other	Policy			
Navigation 👻	Sections (0), Rules (0)						
😑 🎆 Firewall	Search						Q
Web/FTP filter groups	No. Name	Source	Destination	Service	Application	Action	Pr
Web/FIP fittering except Web/FIP fittering except NAT Coulity of service C QoS profiles	 I Objects III ▲ △ □ ∅ € Name 	BB Search Address	No tem Mask:	a found.	₽ ▼.		
			1 No item	s found.			
Structure							
Administration							
- 346							

2. Right-click the display area and click Create first/last rule.

The created rule appears in the list.

3. Create access rules.

```
For example:
To create a permitting access rule for a user, type the user's account name 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 Drop.
```

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 Portal

Preconfigure the Security Gateway

To preconfigure the Security Gateway, perform the following steps:

- Activate the User Authentication component on the Security Gateway.
- Configure the DNS settings for the Security Gateway.
- Configure the time and date (NTP) settings.

To preconfigure the Security Gateway:

1. In the Configuration Manager, go to Structure.

🗄 🗄 Ŧ						10.1.1.10 - Cont	tinent. Config	guration manager				0		- 8
File Main	View			-									Built-in a	dministrator 🎮
Back Forward	Security gatewa	Security y cluster	Creatio wizard	n List	t Tree/Hierarchy	-∽ Reset sessions S Reboot Shut down	Confirm	changes Delet	e Refresh	Properties	Install	Monitoring		
Navigation		Create			View		Sec	curity gateway			Policy	Application		
avigation		1	Sec	urity gatewa	ays (4)									
Securit	y gateways		S	arch										
			S	Name			Com	ponents				Configuration		Cluster
			0	► node-10			55	÷ 🗉				10031		
			0	► node-11			<u>w</u>					10031		
			0	SG-1				ě 🛛				3 10062		
			0	- SG-3								10053		
Access cont	rol													
Structure	lion													
		2	*											
														I≥ #1-101

- 2. Right-click the required Security Gateway and select Properties.
- 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 **Alternative 1** and **Alternative 2** fields.

Security Gat	teway - SG-1		
Security Cert Use Inte Stat Dyn Muit Fire Z DN2 DN2 DH1	r Gateway trificates er Identification arfaces tric Routes namic Routes hti-WAN ewall gs and Alerts Local Storage Databases IS	DNS Servers Preferred: Atemate 1: Atemate 2: Domain:	

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

Security Gateway	A	T	-				
Certificates		Time zone:	GMT				Ť
Interfaces		Network Syn	chronization			On 🗨	D
Static Routes		Automatically	synchronize	the Security Managemer	t 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		Address:					
DNS		naaross.					
DHCP		Authenticat	ion type:	None		-	
✓ SNMP							
Hosts							
SNMP Trap							
SSH							
LLDP							
⊿ NetFlow							
Collectors							
Date and Time							
Updates							
Monitoring							
Access to SMS	-						

- Turn on the Network Synchronization toggle.
 The Primary NTP Server and Secondary NTP Server groups of parameters become available for editing.
- 8. Select the Use NTP server option.
- 9. 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.

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

Authentication parameters configuration

The authentication mechanism is implemented through the Authentication Portal and via Kerberos.

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

For correct operation of the authentication through the Authentication Portal mechanism, perform the following steps on the AD side:

- On the domain DNS server, create an account corresponding to the Security Gateway;
- Create an account for the LDAP profile in the AD domain.

To create an account corresponding to the Security Gateway:

- 1. Run a DNS server snap-in.
- **2.** Create an account of A type on the DNS server.
- **3.** Specify the following parameters:
 - In the Node name field, specify the Security Gateway name for which an account is being created.

The fully qualified domain name (FQDN) of a node will be specified automatically.

Note.

The FQDN of a node must be exactly the same as the Authentication Portal certificate name.

- In the IP address field, specify the IP address of the internal interface of the Security Gateway.
- Select the Create RTP record check box.
- 4. Click Add node.

To create an Active Directory user account:

- 1. Run the Active Directory snap-in.
- In the context menu of the Users section, click New | User. The New object - User dialog box appears.
- **3.** Specify the required parameters and click **Next**.

Note.

The value of the **User logon name** field will be used when the keytab file is created.

- **4.** Set a password for the user account.
- 5. Select the Password never expires check box and click Next.
- **6.** The created account will be displayed in the directory tree of the Active Directory.

Attention!

When configuring the AD controller on the DNS server, the Security Gateway address and its DNS name must be specified as the IP address. To ensure proper operation, create the A record type, the CNAME record type cannot be used.

To configure the Authentication Portal:

1. On the left, select User Identification.

ecurity Gateway	LDAP profile; (no	ot selected)	
Certificates			
User Identification	Authentication Portal		Off 🥘
Interfaces			
Static Routes	Certificate:		
Dynamic Routes	Security gateway interf	aces that are open to authentication portal:	
Multi-WAN	O All		
Firewall	Internal		
Logs and Alerts	Addrees ranges radired	ted to the centive nortal-	
Local Storage	Address ranges redired	ted to the captive portai.	
Databases	Name	Address/Mask	
Email Alerts		No items found	
DNS		The licens round.	
DHCP			
51101			
SNMP			
SNMP Hosts			
SNMP Hosts SNMP Trap	User session duration:	720 * minutes	
SNMP Hosts SNMP Trap SSH	User session duration:	720 🗘 minutes	
SNMP Hosts SNMP Trap SSH LLDP	User session duration: Identification Agent	720 i minutes	
SNMP Hosts SNMP Trap SSH LLDP NetRow	User session duration : Identification Agent	720 C minutes	
SNMP Hosts SNMP Trap SSH LLDP NetFlow Collectors	User session duration: Identification Agent Allow agent to wo Client keepalive ti	720) minutes	
SNMP Hosts SNMP Trap SSH LLDP NetFlow Collectors Date and Time	User session duration: Identification Agent Allow agent to wo Client keepalive ti Kerberos authentication	720) minutes	
SNMP Hosts SNMP Trap SSH LLDP NetFlow Collectors Date and Time Updates	User session duration: Identification Agent Allow agent to wo Client keepalive ti Kerberos authentication Allow Single Sing	720 🗘 minutes	
SNMP Hosts SNMP Trap SSH LLDP NetRow Collectors Date and Time Updates Monitoring	User session duration: Identification Agent Allow agent to wo Client keepalive ti Kerberos authentication Allow Single Sing Unload Lentab All	720	
SNMP Hosts SNMP Trap SSH LLDP NetRow Collectors Date and Time Updates Monitoring Access to SMS	User session duration: Identification Agent Allow agent to wo Client keepalive ti Kerberos authentication Allow Single Sing Upload keytab-file	720 minutes rk meout: 30 minutes n On to connect LDAP users minutes	

- 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. 13).
- **3.** 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.
- 7. In the **Certificate** drop-down list, select the Authentication Portal personal certificate.

Security gateway inter All	faces that are open to authentication port	al:
 Internal Address ranges redired 	ted to the captive portal:	o≥×
Name	Address/Mask	
test_net	192.168.1.0/27	
	192 168 1 40	

8. Select interfaces that will be available to the Authentication Portal.

Note.

If you select **All**, then all interfaces are available to the Authentication Portal. If you select **Internal**, then only interfaces that are internal according to the topology are available to the Authentication Portal.

9. In the Address ranges redirected to the captive portal group, click 🖸.

The list of available network objects appears.

10. In the list of network objects, 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, enter user's credentials in the respective text boxes, then click **Login**. If the server is to check 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 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 server 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. 13).

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. **10**).

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 step **5**), so it is necessary to name the certificate accordingly (in the FQDN record format). For example, **SG01.DOMAIN.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 computer account in the Active Directory (see p. 16).
- 4. Issue a keytab file (see p. 23).
- 5. Configure a DNS server (see p. 24).
- **6.** Configure Kerberos protocol authentication in the Configuration Manager.
- 7. Create Firewall rules for domain users (see p. 16).
- **8.** Configure browsers on user workstations (see p. **25**).

To create and configure a computer account:

 Create a computer account in the **Computers** section of the Active Directory snap-in tool or using PowerShell by running the following command:

dsadd computer "CN=krb,CN=Computers,DC=testers,DC=local"

where \mathbf{krb} — computer account name, $\mathbf{Computers}$ — the AD membership, $\mathbf{testers}$ and \mathbf{local} — domain address.

PS C:\Users\Администратор.WIN-KIE0LPT41AL> <mark>dsadd</mark> computer "CN=krb,CN=Computers,DC=testers,DC=local" dsadd Успешно:CN=krb,CN=Computers,DC=testers,DC=local

2. Specify the SPN for a user account in PowerShell by running the following command:

setspn -A HTTP/sg01.testers.local krb

where **sg01.testers.local** — the domain address of a Security Gateway specified in the DNS server and Authentication Portal certificate name, **krb** — computer account name created on the previous step.

PS C:\Users\Администратор.WIN-KIEOLPT41AL> <mark>ktpass</mark> /princ HTTP/SGO1.testers.local@TESTERS.LOCAL /mapuser testers\krb /pas s * /crypto ALL /ptype KRB5_NT_PRINCIPAL /out C:\SGO1.keytab Targeting domain controller: TST-ADSO1.testers.local Successfully mapped HTTP/SGO1.testers.local to KRB\$.

To issue a keytab file:

1. Generate a keytab file by running 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/sg01.testers.local@TESTERS.LOCAL /mapuser testers\krb /pass *
/crypto ALL /ptype KRB5 NT PRINCIPAL /out C:\test.keytab

where **sg01.testers.local** is the domain address of Security Gateway specified on the DNS server, as well as the Authentication Portal certificate name, followed by **@** and an uppercase domain address name (in this case it is **TESTERS.LOCAL**), **testers\krb** is the **krb** account in the **testers** 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 to save the keytab file.

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

- 2. Enter and confirm the password for the computer account. Confirm the password change.
- **3.** The **krb** account is a computer account, not a user account. This choice is made for security reasons since a computer account does not allow logging in to the domain using its credentials, unlike a user account.

A keytab file will be generated according to the specified values and saved to the specified folder. For a Security Gateway cluster, a general keytab file is created. We recommend using different service principal names (SPNs) for the authentication on the independent nodes.

You must add the created keytab file to the Security Management Server in the Configuration Manager.

Attention!

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

Example:

Type the password for HTTP/SG01.testers.local: Type the password again to confirm: WARNING: Account KRB§ is not a user account (uacflags=0x1021). WARNING: Resetting KRB\$'s password may cause authentication problems if KRB\$ is being used as a server.
Reset KRB\$'s password [y/n]? y
Password successfully set!
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to C:\SG01.keytab:
Keytab version: 0x502
keysize_64_HTTP/SG01.testers.local@TESTERS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x1 (DES-CBC-CRC) keylength 8 (
0x61d629ef5bad235d)
keysize_64_HTTP/SG01.testers.local@TESTERS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (
0x61d629ef5bad235d)
keysize 72 HTTP/SG01.testers.local@TESTERS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength 16 (0
xe44def62f0fdb5b125210ce0bcb448d9)
keysize 88 HTTP/SG01.testers.local@TESTERS.LOCAL_ptype_1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x12 (AES256-SHA1) keylength 32
(0x252da628821454f6b461ace1fdafa6faeef313de814df24c71719126434fd6df)
keysize 72 HTTP/SGO1.testers.local@TESTERS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x11 (AES128-SHA1) keylength 16
(0x5c/246/08c8bdt61f3099aa831/d3d30)

To configure the DNS server:

- 1. Launch the DNS server snap-in.
- **2.** Create an account corresponding to the Authentication Portal certificate name.
- **3.** Specify the IP address of the internal Security Gateway interface as an IP address. If an IP address is specified for a cluster, enter the virtual address of the cluster internal interface.

SG01 - properties	2	Х
Node (A) Security		
Node (uses parent domain name if left blank):	() ()	-1
Fully qualified domain name (FQDN):		
SG01.testers.local		
IP address:		
10.13.95.5		
☑Update associated pointer (PTR) record		
OK Cancel	Ap	ply

4. Click OK.

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 User Identification.
- 3. In the LDAP profile drop-down list, select the created LDAP profile.
- 4. Turn on the Kerberos Authentication toggle.

Security Gateway	I DAP ample: (ast adapted)	
Certificates	LDAP profile: (not selected)	•
User Identification	Authentication Portal	On 💽
Access Server	User session duration: 720 🛟 minutes	
Interfaces	Allow agent to work	
Static Routes	Client keen slive timeout: 30 * minutes	
Dynamic Routes		
Multi-WAN	Kerberos Authentication	On 💽
Firewall	Unaversity densities and the state	
 Logs and Alerts 		
Local Storage	Keytab-file: Import	
Databases	Basic settings	
Email Alerts		
DNS	Certificate:	*
DHCP	Security gateway interfaces that are open to authentication portal:	
✓ SNMP	○ All	
Hosts	O lateral	
SNMP Trap	Internal	
SSH	Address ranges redirected to the captive portal:	0 🗡 🗙
LLDP	Search	Q
✓ NetFlow		
Collectors	Name Address/Mask	
Date and Time	 No items found. 	
Updates		
Monitoring		
Management Access		
ICMP Messaging		
IPS		
Parameters		

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

5. Specify the required user session duration in minutes.

Note.

The user session varies from 5 to 14440 minutes.

- **6.** In the **Kerberos Authentication** group of parameters, click **Import**.
- The standard file explorer appears.
- 7. Select the created keytab file.
- 8. In the Certificate drop-down list, select the Authentication Portal certificate.
- **9.** Select interfaces that will be available for the Authentication Portal.

Note.

If the **All** check box is selected, the authentication is performed on each interface. If the **Internal** check box is selected, then authentication is performed on internal interfaces.

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 the browser to authenticate users through the Authentication Portal

The browsers have to be configured to correctly authenticate users via the Authentication Portal when Kerberos authentication is enabled. To configure the browsers centrally, it is recommended to use group policies.

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

1. In the Control Panel menu, click Manage browser add-ons.

The Internet properties dialog box appears.

2. Go to the Security tab and click 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**.

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

- 6. Click Close and then click OK.
- 7. On the **Security** tab, specify the following parameters:
 - In the Security level for this zone group, click Custom level.
 - In the User Authentication | Logon group, select the Automatic logon with current user name and password option.
 - Click OK.



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

To configure the Firefox browser:

1. In the browser address bar, type **about:config**.

The Advanced Settings window opens in the current tab.

- 2. In the search box, type **network.negotiate**.
- 3. In the network.negotiate-auth.trusted-uris and network.negotiate-auth.delegation-uris, click Edit.
- 4. Specify the domain name of the Authentication Portal and click Save.

network.negotiate-auth.trusted-uris

example.com



Identification Agent

Install the Identification Agent on a computer with Windows OS. Before enabling the Identification Agent, configure the Authentication Portal (see p. **18**). To enable the Identification Agent with AD, configure LDAP interconnection (see p. **13**).

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 mak	e chan	ges to your
		Program name: Verified publisher: File origin:	Setup Launcher Security Code LLC Hard drive on this co	omputer	
⊗ si	now detai	ils		Yes	No
			Change when t	these not	ifications 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
y ('Continent. Identification Agent'' requires that the following requirements be installed on our computer prior to installing this application. Click Install to begin installing these equirements:
Status	Requirement
Pending	Microsoft Root Certificate Authority 2011
Pending	Microsoft Visual C++ 2015-2022 (x86)
Pending	Microsoft Visual C++ 2015-2022 (x64)
	Install 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	ent carefully		ංදිං
END USER LI ON THE USE OF SECURITY	CENSE AGREEN CODE LTD. (Ru	1ENT Jssia) SOFTWAI	RE
	Last updat	ted: <u>10 Septem</u>	<u>ıber, 2015</u>
1. GENERAL TERMS			
This License Agreement (hereinafter referred to as the "Agreement") is the License Agreement between the Security Code Ltd. with its head office located at: Murmanskii proezd 14, building 1, Moscow, 129075 (hereinafter referred to			
• I accept the terms in the license agreem	ent		
\bigcirc I do not accept the terms in the license 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 a 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>
The wizard is ready to begin installatio	n.		635
Click Install to begin the installation.			
If you want to review or change any o exit the wizard.	of your installation s	ettings, click 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 Wiz	ard	\times
	InstallShield Wizard Completed	
<image/>	The InstallShield Wizard has successfully installed "Continent. Identification Agent". Click Finish to exit the wizard.	
	< <u>B</u> ack <u>Finish</u> 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 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, select User Identification, then select the Identification Agent check box.
- 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:

 In the Windows tray, right-click the Identification Agent icon and click Settings. The respective dialog box appears as in the figure below.

💭 Settings		×	
Preferences			
Connect on setup-	φ		
Auto reconnect after	er failure		
Block connections	to untrusted gateways		
Server			
Gateway:	node-10.domain-10		
	Example: access-server.local		
Connection timeout in seconds: 10		10	
Connection retry attem	ts:	2	
Delay between retries	in seconds:	10	
Options			
Taskbar: Sho	w icon and notifications	Ŧ	
Start automatically	agent		
	ОК	Cancel	

2. In the Gateway text box, enter the domain name of the required AD server.

3. Select the required check boxes and specify other text boxes.

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.

4. Click **OK** to save the settings.

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.

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.

📟 Connect to se	rver	×
Identification A	gent 🚺	
User name:	admin	
Password:	•••••	>
	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 2 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: 2.

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 uninstall 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.