SECURITY code

Continent TLS Server Version 2

Setup and Operation

Administrator guide

Mailing address:	**P.O. Box 66, Moscow, Russian Federation, 115127**
Phone:	**+7 495 982 30 20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Table of contents

Introduction

This manual is designed for administrators of Continent TLS Server. Version 2 (hereinafter — TLS Server). It contains information that administrators need in order to install, configure and use the Server.

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.

Chapter 1
Overview

Purpose and main functions

The TLS Server is designed to provide remote users with access to protected resources in a local network with traffic encryption between user workstations and the TLS Server.

The Server performs the following tasks:

- connect remote users and establish secure connections after successful two-way authentication using public-key cryptography;
- protect transferred data using certified cryptographic algorithms.

To this end, the TLS Server has the following capabilities:

- authentication of remote users using a public key infrastructure (X.509 v3 public key certificates are used);
- generation of session keys;
- HTTPS support;
- VLAN creation and management;
- control of the integrity of transferred data using hash functions and message authentication codes;
- deletion of the session information if a connection was lost;
- generation of a private key and creation of a public key using the private key as well as a request to obtain a certificate from a third-party certification authority;
- issue of certificates according to the requests created by the TLS Server own certification authority;
- verification of certificates against a CRL;
- receiving and processing remote users requests to access corporate network resources;
- translation of requests to web servers of a corporate network with the possibility of modifying the rules for translation of requests to endpoint resources as well as web server responses;
- access control using server certificates;
- synchronization of primary and subordinate server configurations;
- saving the resource and certificate settings;
- option to remotely restart a TLS cluster;
- registration of events connected to the TLS Server configuration and operation;
- control of the state of protected connections established with remote users;
- control of the TLS Server state;
- support of local and remote TLS Server management options;
- one-way authentication mode (does not require a Client certificate);
- automatic and manual upload of a TSL list;
- creation of an Application portal (hereinafter — the Portal) that provides a single entry point to access the web resources of a protected network.

The TLS Server operates with Client software (hereafter — the Client) installed on the computer of a remote user. The following software can be used as the Client (if it is certified against the requirements of the FSS of the Russian Federation):

- Continent TLS Client version 2 (using an encryption protocol);
- CryptoPro CSP version 4.0 or 5.0;
- Validata CSP version 6.0;

The TLS Server operates with the preinstalled Hardware Trusted Boot Module Sobol version 3.0, 3.1, 3.2 (hereinafter — Sobol) to prevent unauthorized access to the TLS Server resources.

Continent TLS Client version 2 allows you to obtain the configuration from the Server and use it to perform the automatic configuration of available resources.

Validata CSP cannot be used during the first TLS Server configuration because it does not support the establishment of TLS connections with the servers that provide self-signed certificates as Server certificates. If the administrator decides to use this software, the first TLS Server configuration must be performed using another software with the replacement of the management certificate and the default certificate with a certificate provided by a certification authority.

The TLS Server has its own certification authority to issue unqualified digital certificates.

The integrity check is performed once a day during the Server reboot. If an integrity violation is detected, the cluster is blocked.

To exclude the HTTP protocol usage in a browser while transferring data in the Server, the automatic user request redirection is provided for the HTTPS protocol usage. When the browser receives a redirection code, one more automatic user request is sent to the specified resource address over the HTTPS protocol. Automatic redirection is performed for every proxy resource configured on the Server except ones for which port 443 is used.

Operation principles

The TLS Server is located in a DMZ or directly separates the external data transmission environment and the protected segments of a corporate network. The client can be located on the computer of a remote user in a local network with Internet access or have direct access to the Internet.

The TLS Client interacts with the Server via the TLS protocol. During the connection establishment, two-way (default mode) or one-way (test mode) authentication of the parties is performed. X. 509v3 certificates are used for authentication.

The TLS Server has the cryptographic characteristics are shown in the table below.

Cryptographic algorithm
According to GOST 34.12-2018 (using the **Magma** and **Kuznyechik** algorithms) in the additive stream cipher mode according to GOST 34.13-2018 (with a key length – 256 bit)
Protection of data in transit from corruption
According to GOST 34.12-2018 (using the **Magma** and **Kuznyechik** algorithms) in the message authentication code mode according to GOST 34.13-2018
Hash function calculation
According to GOST R 34.11-2012 (with a key length – 256 bits)
Digital signature generation and verification
According to GOST R 34.10-2012 (based on the Edwards curves with a key length being 256 bits or 512 bits)

The TLS Server allows using non GOST TLS encryption suites and RSA digital signature algorithms to establish connections, issue/reissue a CA certificate, create internal requests for Server and user certificates.

A secure connection is considered established after the generation of a symmetric session key.

The TLS Server functions in the modes are shown in the table below.

HTTPS proxy
A secure HTTPS channel is created between the Client and the TLS server via TLS protocol. In HTTPS proxy mode, a separate Server certificate is used for each protected resource. To protect several web resources simultaneously, a wildcard certificate is used
TLS tunnel
The TLS tunnel mode creates a secure tunnel for applications using TCP including SSH
Application portal
One Server certificate and one entry point are used to access protected resources, access to which can be controlled via LDAP and LDPS. After performing authentication and authorization, a user is provided with a list of available protected resources to choose from. In other respects, the operation of the TLS server in Portal mode is similar to the HTTPS proxy mode

The Server forwards Client requests to the protected network and responds from the protected network to the Client. The redirection of requests is performed automatically according to translation rules specified by the administrator.

In HTTPS Proxy and Application portal modes, the administrator can add fields and edit HTTP headers in Client requests. Transmission of the original IP address of the Client in the HTTP request headers is supported. This IP address can also be used to identify the destination resource of the Client whose request is being broadcast.

To increase performance, individual servers can be combined into a cluster with the primary-subordinate architecture. The load distribution on cluster elements is performed using a third-party network load balancing server (hereinafter referred to as the load balancer). The load balancer must support the balancing based on TCP sessions.

The administrator manages the TLS Server. It is possible to manage the Server locally and remotely. Remote management is performed via a web interface. Administrator authentication at the start of a remote management session is performed based on public key certificates (a management certificate from the Server side and a user certificate from the Client side).

Access to the management tools depends on the TLS Server operation mode:

- default mode;
- local administrator mode.

You can enter the local administrator mode at the initial stage of the Server startup. Server switches to default mode automatically. To start the local administration mode, present the administrator ID of Sobol at the initial stage of the TLS Server startup.

Each time the Sobol Server is started, it searches for integrity control templates on all devices connected to the platform. Before starting or restarting the Server, all external disks must be disconnected.

Public key certificates

The following certificates are required for the TLS Server operation:

- one (or more) root certification authority certificate;
- one (or more) Server certificate;
- one (or more) Server administrator certificate.

Operation with certificates of the DER, PEM, P7B formats and containers of the PKCS7 format are supported.

The generation of a private key and creation of a public key certificate request is performed by the administrator via Client software and the administrator computer. The administrator uploads a root certificate and an administrator certificate provided by the certification authority to the TLS Server locally or remotely.

The administrator can create requests and upload the TLS server certificates locally or remotely too.

The validity of user and root certificates is checked by the Server using the lists of revoked certificates uploaded to its local database. The validity of the user certificate is checked during the authentication while accessing a protected resource.

If a user or root certificate is added to the lists of revoked certificates, the TLS Server finishes the authentication procedure with an error and the denial of access to the requested resource.

If the CRL verification is enabled for user certificates and a CRL certificate is missing, the certificate is considered not validated.

The TLS Server checks the local database and deletes the lists of revoked certificates that have expired. The check is performed during the loading of the Server configuration and if its parameters were changed.

The time of updating the lists of revoked certificates, the paths to which are specified in user certificates, can be selected by the administrator remotely. In addition, the update is performed each time a Server certificate or a root certificate is downloaded by means of remote management.

A Server certificate used for the TLS Server authentication when the administrator connects to it remotely is called a management certificate.

A self-signed technological certificate generated during the TLS Server initialization is used as a management certificate. This certificate is changed when the TLS Server is put into operation by means of the remote or local management tools.

The types of certificates to work with the TLS Server are shown in the table below.

Update server certificate
Used for the Server authentication while Client is establishing connection with the Server to update the Client software

Default certificate
Used as a Server certificate if it is impossible to determine the necessary certificate or the Client does not specify the resource name

Initially, as in the case of the management certificate, the self-signed technological certificate created while the TLS Server initialization is used. The certificate should be replaced with the one requested and received from an external certification authority when the Server is put into operation.

Event log

Events registered by the TLS Server are shown in the table below.

Log file	Purpose
syslog.log	System log
access.log	Event log related to access to http resources
sctunnel.log	Event log related to access to an encrypted tunnel
https_login.log	Authorization log
blacklist.log	Event log related to certificate blocking based on the data received from Continent WAF
limited_access_error.log	Event log related to the limited access by certificates fields
crl_errors.log	Event log related to TSL/CRL loading error

The following events are registered in the system log:

- system events;
- events related to Server management;
- events related to errors in application operation.

Server archives files automatically on a daily basis.

The system log is stored in the Server database. Viewing its records is performed via the local or remote management tools.

User HTTP requests are stored in the access log.

Events related to user attempts to connect to corporate resources are stored in the authorization log.

Viewing access events, including archived events, is performed via the local or remote management tools. It is possible to download access logs for later viewing.

Old records and archived files are deleted when the disk space allocated for the logs is full. There are some settings that make it possible to disable the logging of events related to user access via HTTPS proxy or enable the mode of sending logs to a remote syslog server to prevent the overflow of a hard disk with the log files.

There are several levels of event registration. The results of administrator actions are registered regardless of the specified settings. The number of registered events for an administrator to view depends on the level of event registration. If the detalization level has been changed, events will be shown according to the current level.

The TLS Server provides Sobol events registration. Sobol events registration is enabled by default.

Failover

The failover of the TLS Server is provided by clustering and creating backup copies of a configuration.

Clustering

Servers can be combined into clusters with load sharing between them by an external load balancer to ensure fault tolerance and higher performance. In this case, one Server becomes primary and the server management is performed via it. Other Servers remain subordinate. Only the parameters of the network interfaces and the IP address of the primary Server are configured locally, the other settings are taken from the settings of the primary Server. A dedicated network interface should be used for the primary - subordinate link.

Servers in a cluster exchange only service information. We recommend using an external load balancer or use the DNS balancing.

If the primary TLS Server breaks down, only the cluster management is lost. It does not affect the performance of all other servers. They operate in accordance with the configuration received from the Server before its failure.

Recovery of the primary Server after the failure is performed from a backup copy. If it is missing or outdated, a backup copy from any subordinate Server can be used.

The TLS Server allows you to shut down or restart cluster services or the whole cluster via the remote management tools. Remote cluster activation is impossible.

Note. We recommend you reinitialize the subordinate Server before putting it into operation if it has been shut down for a while.

Creating a backup copy

The following data is included in a backup copy:

- the settings of the TLS Server on which the backup copy was created;
- settings of the HTTPS proxy, TLS tunnel, Application portal;
- certificates of the TLS server own certification authority;
- installed Server root certificates, key containers for them and the administrator certificates.

The creation of a backup copy can be performed remotely or locally. The backup copy of the settings is saved to a file and can be exported to an external drive via the remote management tools. The backup copy is exported to an external drive via the local management tools.

The restoration of the settings from a backup copy can be performed via the local or remote management tools. The backup copy is imported from an external drive via the local management tools.

TLS Server users

TLS Server users can be:

- remote users using open channels of public networks as a transport environment to access web resources of a corporate environment;
- administrators performing the configuration and management of the Server.

A remote user sends a request to access corporate web resources from the computer or smart-phone using public network channels by entering the necessary URI in the browser search bar. The request is sent to the Server located at the perimeter of the protected corporate network.

User authentication is performed after the Server receives the request. The server establishes a secure connection with a remote user device and starts processing the request after the successful user authentication.

The external address of the web resource specified in the request is translated according to a set rule into the internal address of the web resource during the request processing. The request is sent to the protected network using the internal address.

The Server sends the received answer to the user.

The administrator installs Server software, configures it and controls the parameters during its operation. The administrator can create backup copies, restore Server operation configurations, view registered events and perform the monitoring if it is required.

User authentication and authorization

A secure connection when a user accesses resources of a corporate network is established as a result of authentication performed by the TLS Server based on the user request. Authentication is based on the TLSv1.0 and TLSv1.2 protocols using X.509v3 certificate.

There is a Server operation mode that does not require from a user to present a certificate to establish a secure connection.

There are the following types of user authentication while logging in to the Application portal.

Authentication by login and password on the LDAP Server
User enters authentication data which is sent to the LDAP Server. Then, the user is authenticated on the LDAP Server under the specified login
Authentication by name and password in the local database of users
User enters authentication data which is compared to the data stored in the local database of users. There is a group named **Local users of the TLS Server** which exists for local users to access applications

Authentication by certificate
Search in the specific part of the LDAP tree by the field identical to the specific LDAP attribute is performed. The field is taken from the user certificate and specified by the administrator. The set of attributes necessary for providing the uniqueness of the sample must be provided by the administrator

Authentication by login and password can be two-factor to make it more secure. The user has to enter a one-time password apart from the login and password if two-factor authentication is set.

User authorization to access to protected resources is performed after authentication. Each Application portal recourse has its own list of authorized LDAP groups. The list of the LDAP groups in which the user is included is the result of successful authentication.

Notification about TLS Server critical events via email

The administrator can not only view registered events but also receive notifications about the TLS Server critical events via email.

Data encryption

A cryptographic tool supported by the Client must be installed and configured on the computers of remote users to meet the requirements for secure connection (see p. 7).

TLS Server management

The administrator configures and manages the TLS-Server using the local and remote management tools.

Attention! Software downloading and the first initialization of the TLS-Server is performed only locally. The opportunity to connect remotely to the TLS Server for its further configuration and management is provided after the first initialization.

Local management is available only for the Sobol administrator.

The installed and configured Client (see p. 7) is required to perform remote management from the administrator computer. The web interface is used as a remote management tool. The administrator access it by providing a certificate. The Server also makes it possible to establish remote access via SSH.

Chapter 2
Deployment

Standalone Server deployment process

The deployment of a standalone Server consists of the following steps.

Preparation

1. Installation of the Client software on the administrator's workstation (see the corresponding documentation).
2. Generating an administrator private key and creating a request for a public key certificate on the administrator's workstation using the Client.
3. Sending a request to the certification authority and receiving an administrator certificate, a root certificate and a CRL.
4. Installation of a root certificate and an administrator certificate in the certificate storage on the administrator's workstation.

Note.
- When using CryptoPRO CSP, a CA certificate is installed in the certificate storage of the current user (**Certificates — current user** | **Trusted root certification authorities**).
- A user certificate is installed using CryptoPRO CSP.

Local configuration

1. Logon to the Server in administrator mode (see p. **14**).
2. Network parameters configuration (see p. **15**).
3. Master key generation (see p. **18**).
4. The Server initialization (see p. **19**).
5. Changing the OS bootloader code (see p. **20**).
6. Rebooting the TLS Server to exit the administrator mode (see p. **14**).

Remote configuration using the web interface

1. Connecting to the Server through the web-interface (see p. **24**).
2. Generating the Server keys and creating a request for a public key certificate (see p. **55**).

Note. Algorithms for generation of a digital signature in a Server certificate, an administrator certificate and a root certificate must be the same (GOST R 34.10-2012).

3. Sending a request to the certification authority and receiving the Server certificate.
4. Uploading the Server certificates (see p. **57**).
5. Replacing certificates of a management server, a default server and an update server with certificates received from the certification authority (see p. **31**).

Note. We recommend changing a management server certificate after changing a default server and an update server certificates.

6. Uploading an administrator certificate (see p. **57**).
7. HTTPS proxy configuration (see p. **60**).
8. Uploading a root certificate (see p. **57**).
9. Unlocking the Server (see p. **26**).

Server cluster deployment process

The deployment of a Server cluster consists of the following steps:

Preparation

The same steps as for deployment of the standalone Server, see p. **13**.

Local configuration of the primary Server

1. Local logon to the Server in management mode (see p. **14**).
2. Network configuration (see p. **15**).
3. Generating a master key and exporting it to the external drive (see p. **18**).
4. Initializing the Server as the primary one (see p. **19**).
5. Changing the OS bootloader code (see p. **20**).
6. Rebooting the Server to exit the management mode (see p. **14**).

Local configuration of the subordinate Servers

1. Local logon to the Server in management mode (see p. **14**).
2. Uploading a master key (see p. **18**).
3. Configuring the network parameters (see p. **15**).
4. Initializing the Server as a subordinate one (see p. **20**).
5. Changing the OS bootloader code (see p. **20**).
6. Rebooting the TLS Server to exit the management mode (see p. **23**).

Remote configuration using the web interface

1. Connecting the administrator to the primary Server using the web interface (see p. **24**).
2. Uploading a root certificate (see p. **57**).
3. Generating the Server keys and creating a request for a public key certificate (see p. **55**).

   Note. Algorithms for generation of a digital signature in Server certificates, in an administrator certificate and in a root certificate must be the same (GOST R 34.10-2012).
4. Sending the request to the certification authority and receiving the Server certificate.
5. Uploading the Server certificate (see p. **57**).
6. Replacing certificates of a management server, a default server and an update server with the certificates received from the certification authority (see p. **31**).
7. Uploading an administrator certificate (see p. **57**).
8. HTTPS proxy, TLS tunnel or Portal configuration (see p. **60**).
9. Unlocking the Server (see p. **26**).

Deployment and initial configuration

Server activation

Local management of the Server in management mode is available after the successful administrator authentication using Sobol during the hardware platform loading.

The Server loading without an administrator security token ensures its functioning in operational mode. Local management of its configuration is not available.

To load in management mode:

1. Connect a keyboard and a monitor to the Server system unit.
2. Turn on the Server and wait until the prompt for an administrator security token appears:

   ```
   Present your personal security token
   ```
3. Present the Sobol administrator security token not waiting for the automatic loading.

   The Sobol loading starts.
4. In the Sobol menu, select **Load OS** and press **<Enter>**.

   The system loading starts. The main menu will appear once the loading process has finished (see p. **23**).

Server reboot

To reboot and set the operational mode using the local menu:

1. In the local menu, select **Reboot** and press **<Enter>**.

2. In the respective dialog box, select **Yes** and press **<Enter>**.
   The Server loads in the operational mode automatically.

To reboot and set the operational mode remotely:

1. In the **Menu**, select **Status**.
   The window containing information about the available servers and the menu to manage their operation appears.

   Note. Only the button enabling you to update the information about servers in use is activated by default. If you select the Server from the list of available servers, all the other commands become available.

2. Select the required Server and click **Reboot**.
3. In the appeared dialog box, click **Next**.
   The Server loads in operational mode automatically.

To reboot and set the management mode:

1. In the local menu, select **Reboot** and press **<Enter>**.
2. Wait until the window prompting you to present an administrator security token appears:

   ```
   Present your personal security token
   ```

3. Present the Sobol administrator security token not waiting for the automatic loading.
4. The system loading starts. The Server local menu appears once the loading process has finished (see p. **23**).

Server power-off

To power off the Server locally:

1. In the local menu, select **Poweroff** and press **<Enter>**.
2. In the respective dialog box, select **Yes** and press **<Enter>**.
   The Server is powered off.

To power off the Server remotely:

1. In the Server control menu, select **Status**.
   The window containing information about the available servers and the menu to manage their work appears.

   Note. Only the button enabling you to update the information about servers in use is activated by default. If you select the Server from the list of available servers, all the other commands become available.

2. Choose the required Server and click **Poweroff**.
3. In the appeared dialog box, click **Next**.
   The Server is powered off.

Configuring network parameters

To configure the network parameters:

1. In the local menu, select **Network configuration** and press **<Enter>**.
   The **Network configuration** menu containing the items shown in the table below appears.

Menu item	Description
Show current network configuration	Information about the host name, the network interfaces configuration, the default gateway, DNS-servers and search domains
Network interfaces	The list of the current network interfaces. If you select one of them, you can set or change an IP address, a mask and MTU (in the range from 576 to 9000, the default value — 1500)
Default gateway	Configuring the IP address of the default gateway
Hostname	Configuring the Server network name. A random one is generated by default
DNS servers	Configuring IP addresses of the available DNS servers
Search domains	Configuring search domains (DNS suffixes)

Menu item	Description
Static routes	The list of static routes. To add a new route, press **<Enter>** and specify its parameters. To remove a route, select it in the list and press **<Del>**
VLAN	Adding, configuring and deleting a VLAN interface
Apply changes	Applying changes of this session (available after changes in configuration)

2. Select the required option and press **<Enter>**.

   The dialog box prompting you to configure the selected parameters appears.
3. Specify or edit the parameters.
4. Repeat steps **2, 3** if necessary.
5. To finish configuring and applying changes, select **Apply changes** in the network configuration menu and press **<Enter>**.

   The entered and edited parameters will be applied.

   Note. While applying changes, the Server is unavailable for a short period of time. That should be considered when changing network configuration on the Server.
6. To get back to the previous menu, press **<Esc>** or select **Back to previous menu** and press **<Enter>**.

Clustering

To create a Server cluster, you need to generate a master key (cluster key) on the main Server of the cluster.

You can use a master key for the following tasks:

- encrypting private keys of server certificates;
- signing the Server backup copies;
- configuring a secure connection between cluster elements.

All cluster Security Gateways use the same master key. A master key is valid for one year. After this period expires, an administrator needs to change the key in three months, otherwise the Server will be blocked. Five days before master key expiration, the respective notification starts to appear daily in the local menu. To resume the Server operation, you need to change or generate a master key, then create its backup copy and distribute the key to all subordinate Servers. Otherwise, remote access to the Server will be impossible. The TLS Server also allows you to configure automatic master key reissue.

The order of initial installation of a master key in a cluster is as follows:

- key generation on the primary Server;
- export of the cluster configuration to the removable media;
- import of the cluster configuration from the removable media to every subordinate Server.

You can use USB drive or Rutoken as removable media.

Note.

- During the replacement (generation) of a master key, it is distributed to all connected subordinate Servers in a cluster.
- Once the master key is generated, it is impossible to roll back to the previous software version. It is also impossible to make a recovery from a backup copy using the old private key. The master key is stored in Sobol and is not destroyed if the device firmware is changed.

You can manage the Server configurations and certificates in the cluster via the **Clustering** section of the local menu. Depending on the Server role, the **Clustering** section contains commands listed in the table below.

Primary Server	Subordinate Server
• View the cluster certificate list; • Reissue the root certificate; • Reissue the subordinate Server certificate; • Reissue the Server certificate; • Export configuration for the subordinate Server to the removable media; • Export configuration for the subordinate Server to the file system (only on VMs); • Import configuration for the subordinate Server from the removable media; • Import configuration for the subordinate Server from the file system (only on VMs)	• Reissue the Server certificate; • Import configuration of the subordinate Server from the removable media; • Import configuration of the subordinate Server from the file system (only on VMs)

View the certificate list of Servers in the cluster

To view the certificate list of the cluster of Servers, in the **Clustering** section, select **Cluster certificate list** and press **Enter**.

The list contains information about the name, type and expiration time of the certificates.

Reissue certificates of Servers in the cluster

To reissue certificates of Servers in the cluster:

1. In the local menu of the TLS Server, in the **Clustering** section, select a command for reissuing a certificate of the required type and press **Enter**.

   The message about the certificate reissue procedure appears, and if it is successfully completed, a respective message appears.
2. Press **Enter**.

   The message closes. You are returned to the **Clustering** section.

Export and import configuration of Servers in the cluster

You can export and import configuration for subordinate Servers to/from removable media or a file system (for virtual machines) via the local menu. During export, the configuration is saved as an archive with the **cluster_config.tar.gz** default name.

To export configuration to removable media:

1. In the local menu of the TLS Server, in the **Clustering** section, select **Export configuration for subordinate server to removable media** and press **Enter**.

   The message asking you to present removable media appears.
2. Present removable media and press **Enter**.

   Note. If provided removable media contains a previously exported configuration archive file with a default name, a prompt to replace the configuration on the media appears. Take one of the following actions:
   - to overwrite the configuration archive file on removable media, select **Yes** and press **Enter**;
   - to cancel the procedure and return to the **Clustering** section, select **No** and press **Enter**.

   A dialog box for setting the configuration access password appears.
3. Set a password and press **Enter**.

   After successful configuration export, the respective message appears.

To import configuration from removable media:

1. In the local menu of the TLS Server, in the **Clustering** section, select **Import configuration for subordinate server from removable media** and press **Enter**.

   The message asking you to present removable media appears.
2. Present removable media and press **Enter**.

   Note. For a successful configuration import, the archive file with the imported configuration must have the **cluster_config.tar.gz** default name. Otherwise, the message stating that the configuration could not be found on the presented removable media appears.

   A dialog box prompting you to enter the configuration access password appears.
3. Enter the configuration access password that you set during configuration export, then press **Enter**.

A confirmation dialog box with a message about replacement of the master key and cluster configuration as a result of the import appears.

Note. To cancel the import procedure, select **No** and press **Enter**.

4. Select **Yes** and press **Enter**.

   After successful configuration import, the respective message appears.

Master key management

To generate a master key:

1. In the local menu, select **Masterkey** and press **<Enter>**.

   The **Masterkey** menu appears.
2. Select **Generate masterkey** and press **<Enter>**.

   A warning of replacing the current master key appears.
3. Select **Yes** and press **<Enter>**.

   The new master key is generated and stored in the Sobol storage. When the certificate is created successfully, the respective message appears.
4. Export the master key to the key drive (see below) or exit the master key menu.

In case of the primary Security Gateway cluster failure, the key can be imported from the subordinate Server to the primary one.

To export the master key to the key drive:

1. In the main menu, select **Masterkey** and press **<Enter>**.

   The **Masterkey** menu appears.
2. Select **Masterkey export to key drive** and press **<Enter>**.

   Note. If there is no master key in Sobol, the **Masterkey export to key drive** command is unavailable.

   The dialog box prompting you to choose the external drive to write the key to appears.
3. Select the required drive type and press **<Enter>**.

   You are prompted to present the external drive.
4. Present the external drive and press **<Enter>**.

   You are prompted to enter a PIN code or a password to protect the contents of the external drive depending on the type of the presented external drive.
5. Specify a PIN code or a password and press **<Enter>**.

   Note. If a USB drive already contains the master key, you will be asked to choose another name for the key.

   The master key is written to the external drive and the respective message appears.
6. Remove the key drive and exit the master key menu.

To import the master key to the subordinate Server:

1. In the local menu of the subordinate Server, select **Masterkey** and press **<Enter>**.

   The **Masterkey** menu appears.
2. Select **Masterkey import from key drive** and press **<Enter>**.

   The dialog box prompting you to choose the key drive type appears.
3. Select the required key drive type and press **<Enter>**.

   A warning of replacing the current master key appears.
4. Select **Yes** and press **<Enter>**.

   You are prompted to present the key drive.
5. Present the key drive and press **<Enter>**.

   Note. In case of importing from the USB drive, you can choose the required master key file from the list.

   You are prompted to enter a PIN code or a password to protect the contents of the key drive appears depending on the type of the presented key drive.
6. Specify a secure PIN code or a password and press **<Enter>**.

   The master key is written to the Sobol storage and the respective message appears.

7. Remove the key drive and exit the **Masterkey** menu.

Replace the master key in a cluster

To replace the master key:

1. Prepare two empty external drive sets:
   - set №1 — USB drive_1;
   - set №2 — Rutoken e-signature_1 and Rutoken e-signature_2.

   Note. As a set, you can use one external drive if it is a USB drive. In this case, both the database backup and the master key are stored.
2. On the primary Server of a cluster, create a database backup on USB drive_1 (see p. **42**) and export the current master key to Rutoken e-signature_1 (see p. **18**).

   Store the set №1 according to the requirements for the procedure of creating and storing backups in your organization but not less than their validity period.

   Attention! The database recovery from backups can be performed using the master key that is valid at the time of backup creation.
3. Remove the network load on the Server.
4. Generate a new master key on the Server (see p. **18**).
5. Reboot the primary Server of the cluster and turn on the network load.
6. Make sure the Server is up and running. To do so, use the local statistics monitoring tools representing **http sessions data** (see p. **80**).
7. On the primary Server, create a database backup on USB drive_1 (see p. **42**) and export the new master key to Rutoken e-signature_2 (see p. **18**).
8. Turn off all the network cables from the interfaces on the subordinate Server.
9. Import the master key from Rutoken e-signature_2 on the subordinate Server (see p. **18**).
10. Restart the subordinate Server and turn on the network load.
11. Make sure the subordinate Server is displayed in the primary Server remote management web interface. Open the web page of the primary Server remote management and select **Status**.

    The statistics on the subordinate Server are displayed.
12. Make sure the subordinate Server is up and running (see step **6**).
13. Take steps **8 – 12** for other subordinate Servers.

Initialization

Initialization is required to prepare the Server for operation and activate the management web interface.

During the initialization:

- a new database is created (the existing one is removed);
- the Server initial configuration is performed;
- a self-signed technological certificate is created for the initial connection of the administrator to the web interface.

The initialization is performed using the local menu only.

Attention! Before the initialization, perform the network configuration, generate or upload the master key. In the network configuration, specify an IP address and a mask for a network interface.

Initializing standalone Server

To initialize the Server:

1. In the **Main menu**, select **Initialization** and press **<Enter>**.

   Note. If the network configuration is not performed and the master key is not uploaded, initialization is not available.

   A dialog box prompting you to confirm the Server initialization appears.
2. Select **Yes** and press **<Enter>**.

   In the dialog box, select the Server role — primary or subordinate.
3. Select **Primary** and press **<Enter>**.

   A list of network interfaces set during the network parameters configuration appears (see p. **15**).

4. Select the required interface and press **<Enter>**.

   The database initialization starts and the respective message appears. After the database initialization, the web management initialization starts and the respective message appears.

   The initialization process is displayed in the respective messages. During the initialization, a self-signed technological certificate is created and used as a default certificate. The initialization finishes and the **Success** message appears.

5. To finish the procedure, press **<Enter>** or **<Esc>**.

Initializing Server from a cluster

When initializing the Server in a cluster, specify its role — primary or subordinate.

The initialization of the primary Server is performed in the same way as for the standalone Server initialization (see p. 19).

Attention! Before the initialization of either the primary or the subordinate Servers, configure their network interfaces (see p. 15), generate or upload the master key (see p. 18) and TLS certificates..

To initialize the subordinate Server:

1. In the local menu, select **Initialization** and press **<Enter>**.

   The dialog box prompting you to confirm the initialization appears.

2. Select **Yes** and press **<Enter>**.

   The dialog box prompting you to select the Server role (primary or subordinate) appears.

3. Select **Subordinate** and press **<Enter>**.

   The dialog box prompting you to enter the primary Server IP address appears.

4. Enter the primary Server IP address and press **<Enter>**.

   Note. When entering an IP address, you can specify any IP address of the primary Server. The cluster synchronization is performed through the interface to which the selected address will be assigned. To ensure security, select the address that will make it impossible for intruders to monitor the cluster synchronization traffic.

   The NTP service of the primary Server availability check, creating and initializing a database and web management start. The initialization process is displayed in the respective messages.

   The initialization finishes and the **Success** message appears.

5. To continue working, press **<Enter>** or **<Esc>**.

Changing OS bootloader code

Entering the OS bootloader code enables changing the Server boot parameters. To learn more about the administrator rights while configuring the parameters, see p. 89.

When deploying the Server, change the factory bootloader code so that non-authorized users cannot change the Server bootloader parameters.

Changing the OS bootloader code is available using the local menu only.

To change the bootloader code:

1. In the **Main menu**, select **Change GRUB password** and press **<Enter>**.

   The dialog box prompting you to enter the current GRUB password appears.

2. Enter the current bootloader code and press **<Enter>**.

   Note. The factory bootloader code — **3.7TLSpw**.

   The dialog box prompting you to enter a new code appears.

3. Enter a new code twice and press **<Enter>**.

   The respective message appears.

4. To return to the **Main menu**, press **<Enter>**.

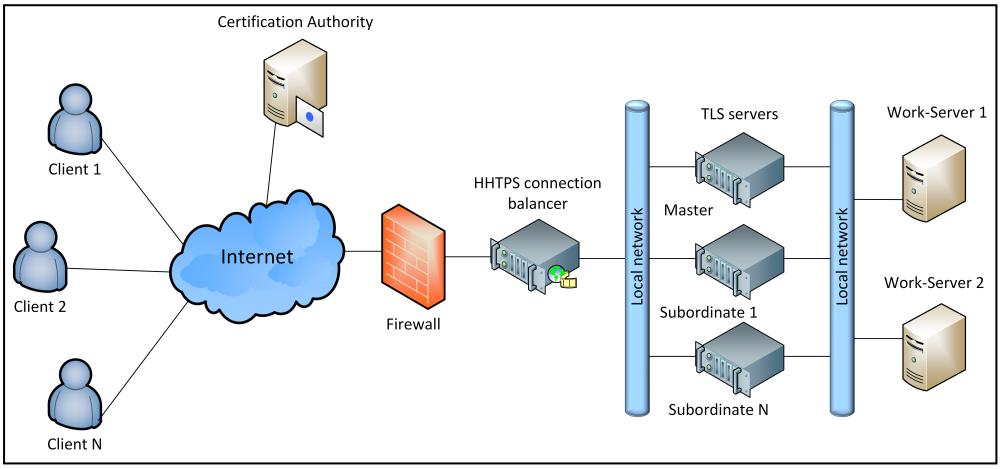
Attention! Remember the code. Loss of the bootloader code leads to the inability to change OS bootloader parameters.

Chapter 3
Configuration and operation

Server use scenarios

The Client access to the protected resources can be provided in different ways depending on the network configuration and the company's objectives.

Client access via a Server cluster



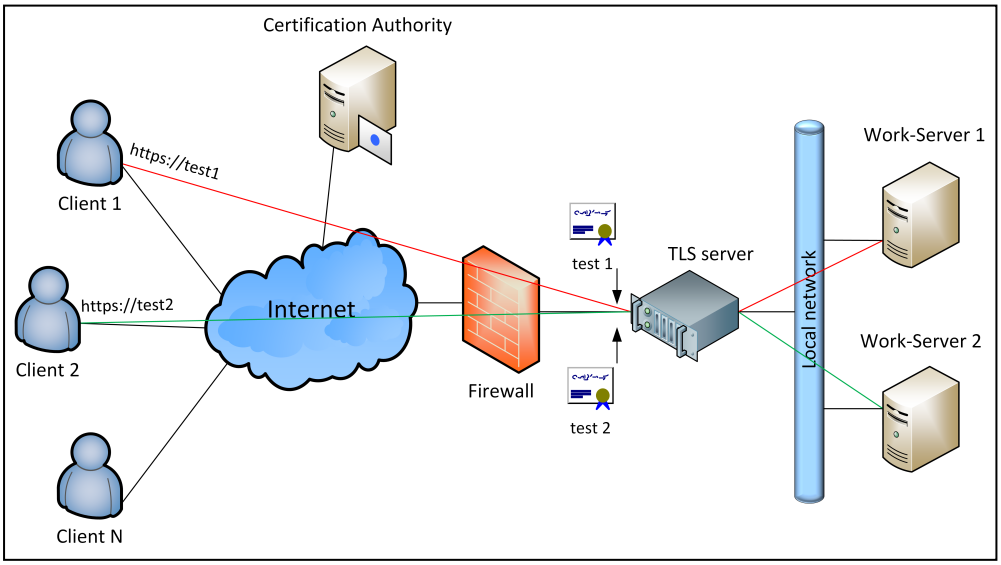
Problem:

To provide the Client access considering that the total traffic volume exceeds the maximum capacity of the Server.

Solution:

1. Configure the load balancer to distribute HTTPS connections through the Server cluster nodes.
2. Configure the Server cluster nodes according to this guide.
3. Configure HTTPS proxy on the Server according to this guide.

Client access to protected resources



Problem:

To provide the Client access to two protected resources located beyond the Server. To gain access to each of the protected resources, different certificates are used.

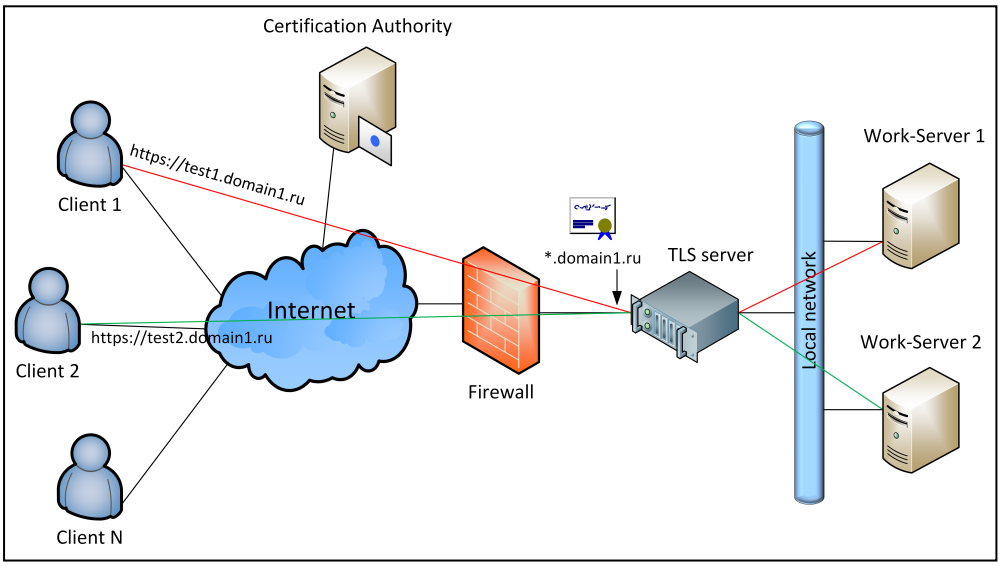
Solution:

1. Create two HTTPS proxy resources on the Server. Select the ***.domain1.ru** and ***.domain2.ru** certificates for HTTPS proxy resources.
2. For the first HTTPS proxy specify the **Work-Server 1** resource.
3. For the second HTTPS proxy specify the **Work-Server 2** resource.

   The Client addressing the **test1.domain1.ru** name gains access to the **Work-Server 1** resources. By addressing the **test2.domain1.ru** name, the Client gains access to the **Work-Server 2** resources.

Attention! In case of presenting an invalid certificate or denying that, the Server returns an error to the web browser. The respective massage appears. To learn more about the error, use the system log (see p. 48).

Client access to protected resources using a wildcard certificate



Problem:

To provide the Client access to two protected resources that are located beyond the Server. To gain access to both protected resources, the same wildcard certificate is used.

Solution:

1. Create two HTTPS proxy resources on the Server. Select the ***.domain1.ru** certificate for each of the HTTPS proxy resources.
2. For the first HTTPS proxy specify the **Work-Server 1** resource.
3. For the second HTTPS proxy specify the **Work-Server 2** resource.

   The Client addressing the **test1.domain1.ru** name gains access to the **Work-Server 1** resources. By addressing the **test2.domain1.ru** name, the Client gains access to the **Work-Server 2** resources.

An example of the Server configuration using this scenario is provided on p. **90**.

The Server management

Server configuration and management is performed by the administrator either locally or remotely. Local management is available for the administrator with the Sobol administrator rights. The Server remote management tool is a web console displayed in the web browser on the administrator's workstation on request.

Note. The Server provides remote access through the SSH protocol (see p. 35).

To get access to the remote management interface on the administrator's workstation, the following items must be installed:

- the Client (see p. **7**);

- a web browser with the enabled TLS protocol support;

  Note. In Internet Explorer 11, the TLS protocol support is enabled by default.

- an administrator certificate;
- a CA certificate.

  Note. The administrator certificate and the CA certificate are not required during the initial connection.

The administrator's workstation and the Server must be located in the same subnetwork or the routing must be configured between them. Port **443** must be open on the firewall.

To open the remote management web console for the first time insert the key storage containing the administrator keys, launch the web browser and enter the Server address in the address bar specified during the network configuration (see p. **15**). You should specify the address using the **https://** prefix.

Note. The key storage is not required for the initial configuration after the installation.

The startup page of the Server remote control appears (see p. **24**).

Local menu

The local menu appears after the OS loading and when the Server powers on (see p. **14**) or reboots (see p. **14**).

The command set of the local menu depends on the Server operation mode:

- The commands **Reboot** and **Poweroff** are available only in the operational mode;
- All the commands of the main menu are available in management mode. Some menu items become available after the Server initialization.

To change the operation mode, reboot the Server.

The main menu consists of the items shown in the table below.

Menu item	Purpose
Network configuration	View and edit the following network parameters: • network interfaces; • default gateway; • hostname; • search domains; • DNS servers; • static routes; • VLAN
Certificate (available after the Server initialization)	View and manage certificates: • administrator certificates; • server certificates; • CA certificates. Export certificates Create a request for the Server certificate and manage security certificates: view, import from an external USB drive, remove CA certificates, replace a control certificate
System time and date	Configure system time and connection to the NTP server
Clustering	View and reissue Server certificates in the cluster. Import and export of the cluster Server configuration
Entropy	Import and generate entropy using a keyboard
Masterkey	After the master key generation or its import from a key drive, the following operations are available: • display the master key expiration date; • export the master key to a key drive
Initialization (available after the master key generation/loading and specifying an interface IP address)	The Server preparatory work and web interface activation. Assign the Server role in a cluster. Delete a database (if any existed). Create a new database

Menu item	Purpose
Intrusion prevention system configuration (available only on the main node in cluster)	Configure the parameters of the Server temporary lockout that happens if the maximum number of the user's attempts to present the certificate within a limited period of time is exceeded. Default value — **ON**
Administrator server configuration	Choose a network interface, a port through which access to the management Server is provided. Activate the use of IP address in the management Server name
Diagnostics	Collect, display and save results of the Server audit. • status — display the current state of the Client connection with HTTPS proxy and the statistics on the Server (available after the Server initialization); • network diagnostics — launch and audit the results of the **tcpdump** (it enables to select the Server network interface to audit traffic), **ping** and **traceroute** commands and ARP cache content display (available after performing the network configuration); • network interfaces diagnostics — audit of the Server network interfaces; • creating a technological repository on an external USB drive; • audit of the Sobol checksum files; • nginx configuration
System backup and restore	Create a backup of the Server configuration on an external drive after the initialization. Restore the configuration from the external drive and their application (only for the primary Server)
Change GRUB password (available after the Server initialization)	Change the OS boot loader code while deploying the Server or if necessary
Lock server	The Server lockout. Only the management of the Server is available after the lockout
Logs (available after the Server initialization)	View access logs and system logs. The Server events log configuration: • power on/off event logs while getting access or authorizing; • the log drill-down configuration (debug, high, medium, low); • select the connection protocol; • send the logs to the remote syslog server; • configure the number of connection attempts; • configure the storage time and logs capacity
Access from the external devices	Configure the serial console. Configure access via SSH: • enable/disable access via SSH; • manage the access password; • remote access configuration; • choose the port of the Server remotely; • configure the IP address at which the connection is available
Change language	Change the interface language
Reboot	The OS reboot and the Server startup
Poweroff	The Server power-off

Remote management menu

In the top left corner, next to the Security Code logo, there is a button that hides or expands the menu. When you expand your web browser the Server menu appears. It displays a list of available sections.
A brief description of the menu items is shown below:

Menu item	Description
Status	View the Server statistics according to the current HTTPS proxy connections and processed requests (see p. **80**)
Logs	View, export, clear system messages and events logs (see p. **48**)
Certificates	View, import, export and delete security certificates (see p. **54**)
Resources	Configure parameters of protected resources (see p. **60**)

Menu item	Description
Settings	Manage lockout, connections to logs, network security, logs, certificates etc. (see p. **26**)
TSL/CRL Management	View a download address and a list of the installed certificates, issue and remove certificates, configure the TSL files update schedule (see p. **75**)
Network Management	Configure the network connection (see p. **77**)
Diagnostics	Launch and audit the **ping**, **traceroute** and **arp** commands (see p. **80**). Launch the extended logging
Certification Authority	Issue root, user and server certificates on the CRL requests. View information about the issued certificates (see p. **83**)
About	Software version information

In the top right corner, there is a button that displays the Server lockout state:

- open lock — the Server is enabled;
- closed lock — the Server is locked (available for the Server management).

The icon color informs you about the Server:

- green — the Server is operating;
- orange — the Master key validity period expires;
- red — the Server is locked.

The Server lockout reasons:

- no administrator certificate;
- no CA certificate;
- no required license;
- the issued certificates are compromised;
- the Master key validity period has expired.

On the right, there is a graphical icon that displays administrator notifications, the theme appearance and language.

On the left, there are buttons that allow you to control the Server. In the central part, there is a panel and a toolbar above it.

The **Status** section is loaded by default.

Configuring the Server parameters

To manage the Server efficiently, configure its parameters beforehand. To do so, select **Settings** in the local menu.

Attention! If the Server is locked, you cannot change the settings.

The Server configuration contains the following sections:

- Lock and unlock the Server (see p. **26**).
- Configure the management Server (see p. **26**).
- Configure user authorization using LDAP (see p. **27**).
- Configure intrusion prevention system (see p. **28**).
- Configure log parameters (see p. **26**).
- Manage security certificates (see p. **31**).
- Configure remote access (see p. **35**).
- Configure the date and time (see p. **37**).
- Configure the notification system (see p. **38**).
- Manage licenses (see p. **39**).
- Manage software updates (see p. **40**).

- Create a configuration backup and restore a configuration from a backup (see p. **41**).
- Synchronize with WAF (see p. **45**).
- Monitoring (see p. **51**).

Lock and unlock the Server

In case of the Server lockout, the current user connections will be lost. Establishing new connections will be unavailable.

Attention! Managing the Server lockout is available if the license is installed, the root and administrator certificates are loaded and there are no compromised certificates.

To lock/unlock the Server:

1. In the top right corner of the Server local menu, click the lock button.
   The dialog box prompting you to confirm the operation appears.
2. To switch the status, click **Lock/Unlock** and close the dialog box.
3. Refresh the web page.
   The color and the image of the icon will change (— the Server is unlocked; — the Server is locked).

Configure the management Server

To ensure the proper operation of the Server remote management, specify the access port and select the Server interface. All interfaces are allowed to be selected, the access to the Server is granted through port 443 by default.

A default Server hides the management Server and other HTTPS resources. If the Server name is not specified or specified incorrectly, all requests will be sent to the Server by default. An error will always be the result of the Server request. You can restore the administrator access to the web management in the local menu.

To configure the management Server parameters using the remote management tools:

1. In the **Menu**, go to **Settings | Management Server**.
   The **Management Server** settings appear.
2. To specify a new IP address of the Server, click **+** in the **Management certificate** field.
   The list of certificates appears.
3. Select the management certificate and click **Select**.

   Attention! Select a certificate with the signature algorithm GOST R 34.10-2012 with a key length in range from 256 to 512 bits.

   The address at which access to the management server will be granted is in the **Common name** field or in the **DNS altname** field if such an extension exists.

   Note. Using an IP address as a Server name is allowed by default.
4. To change the management interface port value, enter a new port number.
   The default Server has the same port on which the management Server resides.

   Note. To create a server on port **443**, select the respective check box. It is locked by default. After changing the port's value for the default Server, this parameter becomes available.
5. Select the respective interface from the list.
6. Configure the **TLSv1.2** usage mode (enabled by default).
7. After changing the configuration, click **Save** on the toolbar.

To change the management certificate created during the Server loading to the one received from the CA using the local menu:

1. In the local menu, select **Certificates** and press **<Enter>**.
   The **Certificates** menu appears.
2. Select **Server certificates** and press **<Enter>**.
   The **Server certificates** menu appears.
3. Select **Change management certificate** and press **<Enter>**.
   The **Certificates list** appears.

4. Select the required certificate and press **<Enter>**.

   The certificate will be changed and you will be returned to the list of certificates. Information about the current certificate will be updated.

To configure the management server parameters using the local menu:

1. In the local menu, select **Administration server configuration**.

   The **Administration server configuration** menu appears.
2. Select **Select control interface**.
3. In the dialog box, select the required interface and press **<Enter>**.

   The **Success** message appears.
4. To return to the **Settings** menu, press **<Enter>**.
5. To change an interface port, select **Select control port**, enter the required value and press **<Enter>**.
6. To return to the **Settings** menu, press **<Enter>**.

   In the **Settings** menu, the **Disable the default server on port 443** option appears. In case of the Server power-off the item's status changes to the opposite. When specifying the 443 management port, this item will be deleted after applying the changes.
7. To change the configuration that allows/prohibits you to use an IP address in the Server name, select **Permit\Prohibit IP in control certificate name** and press **<Enter>**.

   The **Success** message appears.
8. To return to the **Settings** menu, press **<Enter>**.

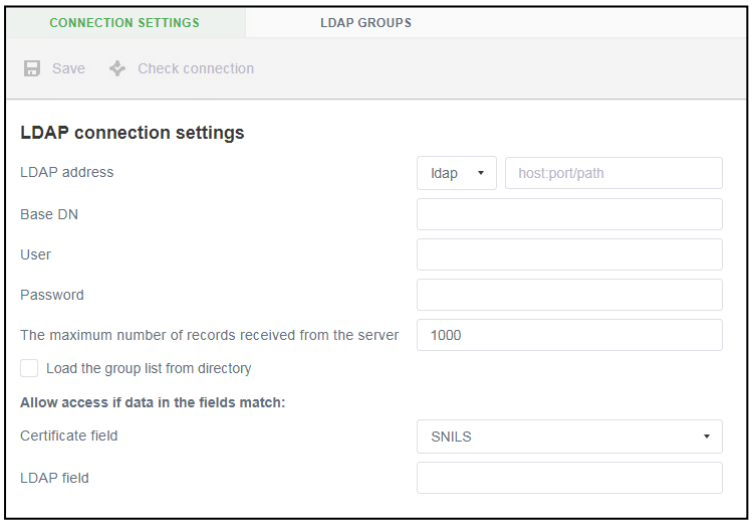
Configure user authorization using LDAP

On the Server, you can perform the user authorization using LDAP in TLS tunnel or an application portal mode.

To configure the user authorization using LDAP:

1. In the **Menu**, select **Settings | LDAP connection**.

   The **LDAP connection settings** menu appears.



2. Specify the required parameters:

Parameter	Description
LDAP address	LDAP/LDAPS protocol and domain controller address are specified. Protocol value by default — **ldap**
Base DN	LDAP directory where the data search starts
User	LDAP user account name
Password	LDAP user account password
The limited number of records received from the Server	The maximum number of records received from the Server Default value — **1000**

Parameter	Description
Load the group list from directory	LDAP group list refreshes automatically every 15 minutes if the respective check box is selected
Certificate field	The certificate field that contains information to compare it with LDAP directory attribute. Default value — **SNILS**
LDAP field	The LDAP directory attribute

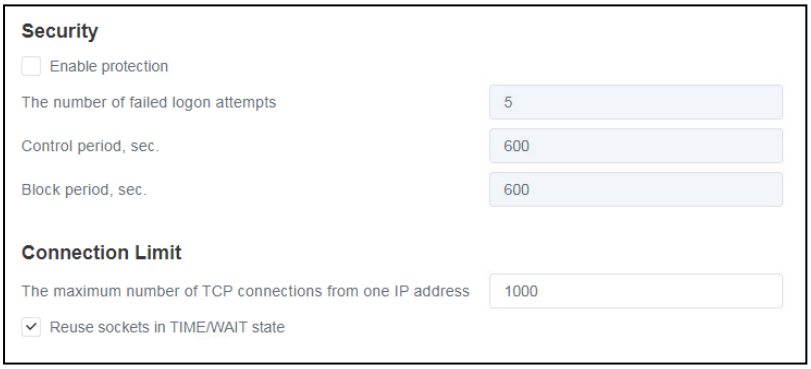
Note.
- To check the entered parameters, click **Check connection** on the toolbar. If all the parameters are specified correctly, the respective message appears.
- User search is performed by comparing the **Certificate** field value to the **LDAP** field value.
- Microsoft Active Directory has a limit of 1000 records in response to LDAP requires by default. If there are more than 1000 groups on the Server, you need to either change this parameter or limit the fetch using Base DN.

3. On the toolbar, click **Save**.

On the **LDAP groups** tab, you can find information about the LDAP groups. If necessary, you can update the information about the groups and select the required one by clicking the search button in the right corner.

Configure the intrusion prevention system

Continent TLS Server includes an intrusion prevention system designed to counter brute force attacks. This control blocks a user temporarily if the number of authentication attempts is exceeded during a certain period of time.



Before enabling the protection, specify the following parameters:
- number of failed logon attempts (for the Application Portal);
- time period during which the number of failed logon attempts is recorded;
- time period during which a user will be blocked;
- maximum number of TCP connections (connections to resources) from one IP address.

The intrusion prevention system is disabled by default. The following parameters become available by default when you enable the control:
- The number of failed logon attempts — 5.
- Control period, sec — 600 seconds.
- Block period, sec — 600 seconds.

The limit on the number of TCP connections (connections to resources) is always available. The maximum number of TCP connections from one IP address — 1000. If you specify the 0 value, the limitation will be removed.

Attention! If connection to resources is performed using NAT, disable the limitation.

To enable/disable the intrusion prevention system and configure its parameters using the remote management tools:

1. In the **Menu**, select **Settings | Security**.
   The **Security settings** menu appears.
2. To enable/disable the system, select/clear the **Enable protection** check box.
3. If necessary, change the protection parameter values (range from 0 to 2147483647).

4. On the toolbar, click **Save** after changing the parameters.

To enable/disable the intrusion prevention system and configure its parameters using the local menu:

1. In the local menu, select **Intrusion prevention system configuration**.
   The **Intrusion prevention system configuration** menu appears.
2. Select **Authentication errors processing control** and press **<Enter>**.
3. In the **Authentication errors processing control** dialog box, select the required option and press **<Enter>**.
4. To change protection parameters, select **Configure authentication error processing parameters**.
5. Set the required values (range from 0 to 2147483647) and press **<Enter>**.
   After changing the parameters, you will be returned to the **Main menu**.

Configuring log parameters

Configure event registration

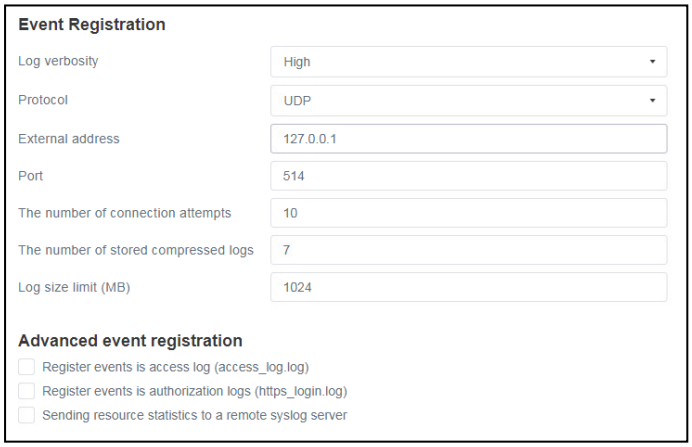
In the system log, the following events are registered by default:

- system events;
- events related to the Server management;
- events related to application failures;

Event registration can be activated in the authorization logs.

To configure event registration using the remote management tools:

1. In the **Menu**, select **Settings | Event Registration**.
   The **Event Registration** settings appear.



2. Specify the respective parameters in the **Event Registration** and **Advanced event registration** sections.
3. On the toolbar, click **Save**.

To configure event registration using the local menu:

1. In the local menu, select **Logs** and press **<Enter>**.
   The **Logs** menu appears.
2. Select **Configure TLS server event logging** and press **<Enter>**.
   The **TLS server events logging configuration** menu appears.
3. Select an event registration item in the required log and press **<Enter>**.
   The **Event logging configuration** menu appears.
4. Select **Enable/Disable event logging** and press **<Enter>**.
   You will be returned to the **Logs** menu.
5. After changing event logging parameters of the Server, select **Save configuration** and press **<Enter>**.
   The new parameters will be applied.

Configure log verbosity

You can configure the following levels of log verbosity:

- Debug — all events are registered including debug.
- High — all events are registered except debug.
- Medium — all errors, warnings and administrator actions are registered.
- Low — all errors and administrator actions are registered.

When changing the Debug level, all messages not corresponding to the level of log verbosity will not be registered in the system.

Note. Administrator activity and events related to storing key information are always registered but their presentation in the logs depends on the verbosity settings. When changing the log verbosity level, a user can notice the messages for the entire period since the previous system events log was cleared.

To configure log verbosity using the remote management tools:

1. In the **Menu**, select **Settings | Event Registration**.
   The **Event Registration** settings appear.
2. In the **Log verbosity** field, select the required level.
3. On the toolbar, click **Save**.

To configure log verbosity using the local menu:

1. In the local menu, select **Logs** and press **<Enter>**.
   The **Logs** menu appears.
2. Select **Configure TLS server event logging** and press **<Enter>**.
   The **TLS server events logging configuration** menu appears.
3. Select **Select logging level** and press **<Enter>**.
   The list of **Log verbosity** levels appears.
4. Select the required level and press **<Enter>**.
   You will be returned to the **TLS server events logging configuration** menu.
5. After changing event logging parameters of the Server select **Save configuration** and press **<Enter>**.
   The new parameters will be applied.

Send logs to a remote syslog server

After performing this configuration, system logs and access logs will be sent to the specified syslog server. All newly registered events will be stored locally on the Server.

Sending logs to a remote syslog server is disabled by default.

To enable sending logs to a remote syslog server using the remote management tools:

1. In the **Menu**, select **Settings | Event Registration**.
   The **Event Registration** settings appear.

   Attention! When the log sending is disabled, the default values are displayed:
   - The external IP server address for storing logs: **127.0.0.1**.
   - The server port for storing logs: **514**.
2. Enter the IP address and remote syslog server port to which the logs must be sent.
3. If necessary, change the transport protocol and the number of attempts
4. On the toolbar, click **Save**.

To cancel sending logs to the syslog server using the remote management tools, perform the procedure described above and restore the default values for the IP address and remote server port during the procedure.

To configure sending logs to the syslog server using the local menu:

1. In the local menu, select **Logs** and press **<Enter>**.
   The **Logs** menu appears.
2. Select **Configure TLS server event logging** and press **<Enter>**.

The **TLS server events logging configuration** menu appears.

3. Select **Configure remote syslog server**.
   Fields for entering an IP address and syslog server port appear.
4. To send logs to the remote syslog server, enter its IP address and port number. Then press **<Enter>**.
   To cancel sending logs, delete an IP address and port number. Then press **<Enter>**.
5. To specify the transport protocol, select **Select log protocol** and press **<Enter>**.
   The **Log protocol** menu appears.
6. Select the required protocol and press **<Enter>**.
7. To specify the limit of connection attempts, select **Configure limit of connection attempts** and press **<Enter>**.
   The **Number of connection attempts** dialog box appears.
8. Enter the required number of attempts and press **<Enter>**.
9. After changing the TLS event logging configuration select **Save configuration** and press **<Enter>**.
   The new parameters will be applied.

Manage log storing parameters

By default, the number of the logs stored on the Server is 7.

To configure the log storing parameters using the remote management tools:

1. In the **Menu**, select **Settings | Event Registration**.
   The **Event Registration** settings appear.
2. If necessary, change **Rotation frequency (days)**.
3. If necessary, change **Log size limit (MB)**.
4. On the toolbar, click **Save**.

To configure the log storing parameters using the local menu:

1. In the local menu, select **Logs** and press **<Enter>**.
   The **Logs** menu appears.
2. Select **Configure TLS server event logging** and press **<Enter>**.
   The **TLS server events logging configuration** menu appears.
3. To change the limits of the log storage size, select **Configure log size** and press **<Enter>**.
   A dialog box prompting you to enter the log storage size appears.
4. Enter the required value and press **<Enter>**.
   You will be returned to the **TLS server events logging configuration** menu.
5. After changing TLS server events logging configuration select **Save configuration** and press **<Enter>**.

Managing security certificates

You can manage certificates using the local or remote managing tools by:

- changing certificates;
- managing verification parameters and certificate use.

Change certificates

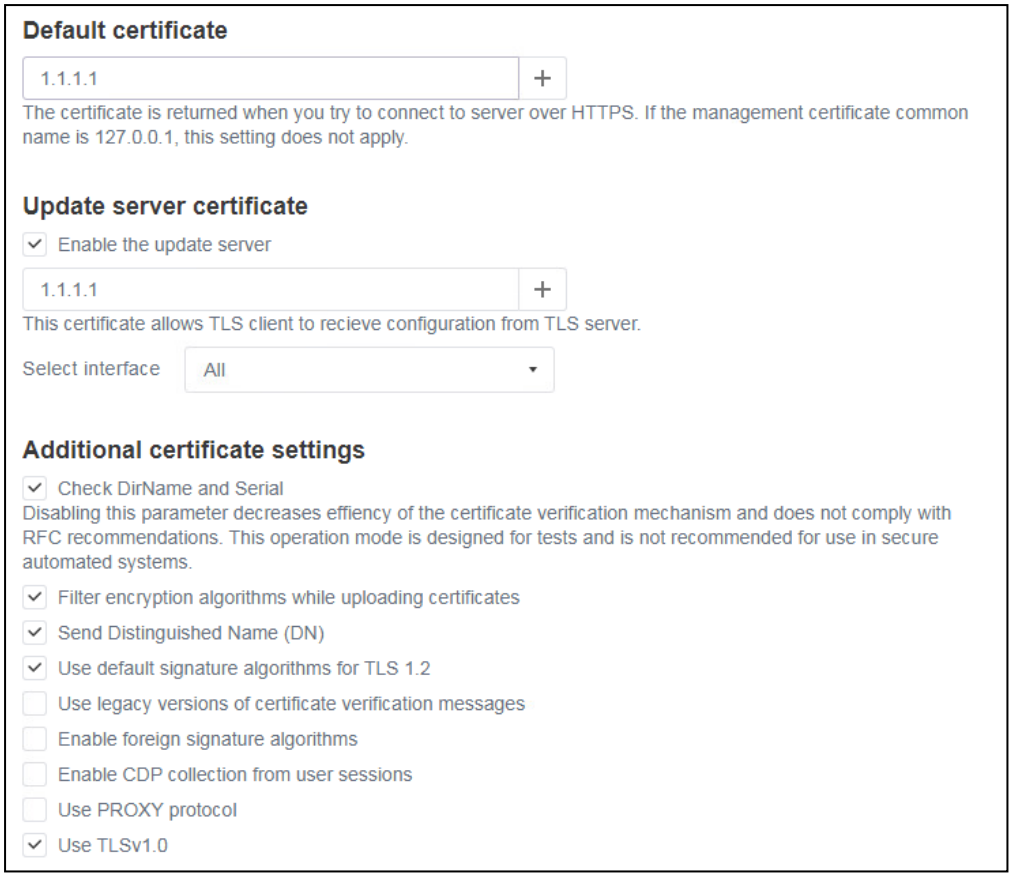
You may need to change certificates at one time or another. When the Client connects to the Server with a failure (for example, HTTPS failure, using an IP address instead of the Server name), a message denying access appears on the Client. The **Certificate failure** button appears in the address bar of the web browser. If you click the button, you can view information about the certificate use.

Attention! If you use a third-party CSP as the Client, specify the CA certificate as the default one because the third-party CSP does not interact with self-signed certificates.

To change the certificate using the remote management tools:

1. In the **Menu**, select **Settings | Certificates**.

The **Certificates** menu appears.



2. Click **+** in the respective certificate type.

   The **Certificates** dialog box appears.
3. Select the required certificate and click **Select**.

   The dialog box with the list of certificates closes. Parameters of the selected certificate appear.
4. On the toolbar, click **Save**.

   The certificate will be changed and the respective information will be updated.

Note. The default certificate and the Server update certificate can be changed using the remote management tools only. You can also choose the network interface for the Server update certificate to restrict the access to the TLS Client update server.

See more information about changing the certificate using the local menu on p. **26**.

Control certificate verification by DirName and Serial fields

To perform tests, you can disable certificate verification by the **DirName** and **Serial** fields in the **AKI** certificates extension. In this case the values of the specified fields are not verified during the chain creation.

The lack of this verification may cause a creation of several chains. Some chains can contain either revoked or invalid certificates, that can cause trust loss. The chain that trusts the certificate may exist at the same time. The chain is selected by chance. When disabling the certificate verification the chain creation is performed unambiguously.

Control certificates verification through the **DirName** and **Serial** fields is enabled by default.

To configure the certificate verification:

Attention! If you use a third-party CSP, the parameter must be disabled.

1. In the **Menu**, go to **Settings | Certificates**.
2. Select/clear the **Verify DirName and Serial** check box.
3. On the toolbar, click **Save**.

The web page will be updated. The certificate verification will be configured properly.

Filter cryptographic algorithms during certificates loading

During the certificates loading, the signature algorithms are verified and it is automatically prohibited to load certificates the signature algorithm of which are different from the issuer signature algorithm.

The algorithm filtration during the certificate loading is enabled by default. If necessary, you can disable it manually or enable it again.

To configure the algorithm filtration during the certificate loading:

Attention! If you use a third-party CSP, the parameter must be disabled.

1. In the **Menu**, go to **Settings | Certificates**.
2. Select the **Filter cryptoalgorithms during the certificate loading** option.
3. On the toolbar, click **Save**.

   The web page will be updated. Signature algorithms filtration during the certificates loading will be configured properly.

Sending Distinguished Name

When the number of the loaded CA certificates exceeds the threshold value (DN 32 KB), sending the CA certificates to the DN client is disabled automatically.

Sending the CA certificates to the DN client is enabled by default.

To configure the DN sending:

Attention! If you use a third-party CSP, the parameter must be disabled.

1. In the **Menu**, go to **Settings | Certificates**.
2. Select the **Send Distinguished Name** option.
3. On the toolbar, click **Save**.

   The DN sending will be configured properly.

Use standard signature algorithms for TLS 1.2

Enabling this parameter allows you to use the signature algorithms of the previous versions when working with a third-party CSP.

Using the standard signature algorithms for TLS 1.2 is enabled by default.

To configure the use of the standard signature algorithms for TLS 1.2:

1. In the **Menu**, select **Settings | Certificates**.
2. Select **Use standard signature algorithms with TLS 1.2** option.
3. On the toolbar, click **Save**.

   The web page will be updated. The use of the standard signature algorithms for TLS 1.2 will be configured properly.

Use legacy versions of certificate verification messages

Enabling this parameter allows you to use the old versions of the Server certificate verification messages to work with a third-party CSP.

Using the old versions of certificate verification messages is disabled by default.

To configure the use of the old versions of certificate verification messages:

1. In the **Menu**, go to **Settings | Certificates**.
2. Select **Use legacy versions of the certificate verification messages** option.
3. On the toolbar, click **Save**.

   The web page will be updated. The use of the old versions of certificate verification messages will be configured properly.

Use foreign signature algorithms

The TLS Server allows using foreign TLS cryptosuits and e-signature algorithms to provide compatibility with the Clients that do not have mechanisms which use algorithms and protocols compliant with GOST.

Using foreign algorithms is disabled by default.

Enabling this parameter allows using foreign TLS cryptosuits and e-signature algorithms to perform the following:

- establish a TLS connection;
- issue/reissue a CA root certificate;
- create an internal request for the Server certificate;
- issue the Server certificate and a user certificate by request.

Note. To provide data confidentiality, we recommend using the GOST signature algorithms and cryptosuits.

To manage the use of foreign signature algorithms:

Note. To use foreign signature algorithms for several resources, activate this parameter for each resource individually.

1. In the **Menu**, go to **Settings | Certificates**.
2. Specify the required value for the **Enable foreign signature algorithms** parameter.
3. On the toolbar, click **Save**.

   The web page will be updated. The use of foreign signature algorithms will be configured properly.

Collect CDP from user sessions

CDP collection from user sessions is enabled by default.

Note. When connecting a user with a certificate in which a new CDP is specified, this CDP is added to the general list. CRL loading for this CDP will be performed on schedule or may be initiated manually.

To configure CDP collection from user sessions:

1. In the **Menu**, go to **Settings | Certificates**.
2. Specify the required value for the **Enable CDP collection from user sessions** parameter.
3. On the toolbar, click **Save**.

   The web page will be updated. The CDP collection from user sessions will be configured properly.

Information about request source addresses after traffic leaves the balancer

The capability to receive information about request source addresses after traffic leaves the load balancer is provided by means of the proxy protocol. Information about the connection is determined and transferred in the header of the proxy protocol.

The Server supports two versions of proxy protocol that allow obtaining the headers of proxy protocols in two formats — standard and binary.

The standard format of the proxy protocol:

```
PROXY TCP4 192.168.0.1 192.168.0.11 56324 443\r\n
GET / HTTP/1.1\r\n
Host: 192.168.0.11\r\n
\r\n
```

The binary format of proxy protocol:

```
0d 0a 0d 0a 00 0d 0a 51  55 49 54 0a 21 11 00 0c  |.......QUIT.!...|
ac 13 00 01 ac 13 00 03  a6 52 00 50 47 45 54 20  |.........R.PGET |
2f 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74  |/ HTTP/1.1..Host|
3a 20 6c 6f 63 61 6c 68  6f 73 74 3a 38 30 38 30  |: localhost:8080|
0d 0a 0d 0a                                       |....|

<---------------     Bytes     ----------------> <----  ASCII ---->
```

To manage the proxy protocol operation:

1. In the **Menu**, go to **Settings | Certificates**.
2. Specify the **Use PROXY protocol** parameter.

   Note. In case of activating the parameter, proxy protocol is enabled for the entire Server.

   If enable the parameter, the following checks are conducted:
   - absence of protected resources on port 443;
   - connection port for every protected resource must differ from the Server management port (see p. **26**).
3. On the toolbar, click **Save**.

   The proxy port operation for transmitting information about request source addresses after traffic leaves the load balancer will be configured properly.

Attention! In case of enabling the parameter and values for the Server management port and protected resource ports match, the respective error message appears.

Remote access to Server

The Server makes it possible to provide remote access from external devices using the serial console or via SSH.

Configure the serial console

Connection to the TLS Server using the serial console is established via COM port providing access to the local menu.

To turn on/off the serial console:

1. In the **Main menu**, select **Remote access configuration** and press **<Enter>**.

   The **External access configuration** menu appears.
2. Select **Serial console configuration** and press **<Enter>**.
3. Select the respective option and press **<Enter>**.

   When the parameters are changed, the information dialog box appears.
4. To return to the **Serial console configuration** menu, press **<Enter>**.

Configure access via SSH

SSH is an application level protocol that makes it possible to encrypt data and passwords and also allows transferring any other protocol. An SSH tunnel is created for the secure use of SSH.

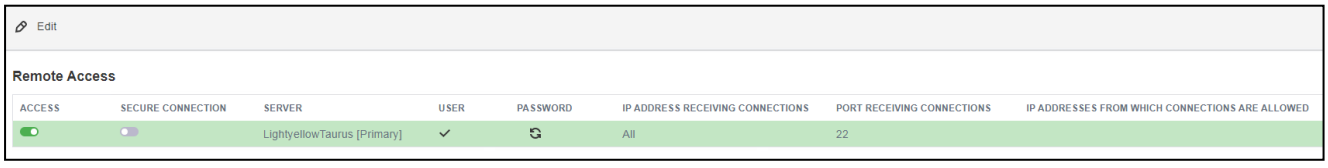
An SSH tunnel is a tunnel created using the SSH connection. It is used to secure traffic exchange on the Internet. During the transfer through an SSH tunnel, unencrypted traffic of any protocol is encrypted on one side of the SSH connection and decrypted on the other side.

Only the TLS Server administrator is granted access using the SSH protocol.

To configure access via the remote management tools:

1. In the **Menu**, go to **Setting | Remote Access**.

   The list of the Server clusters and their settings appears.



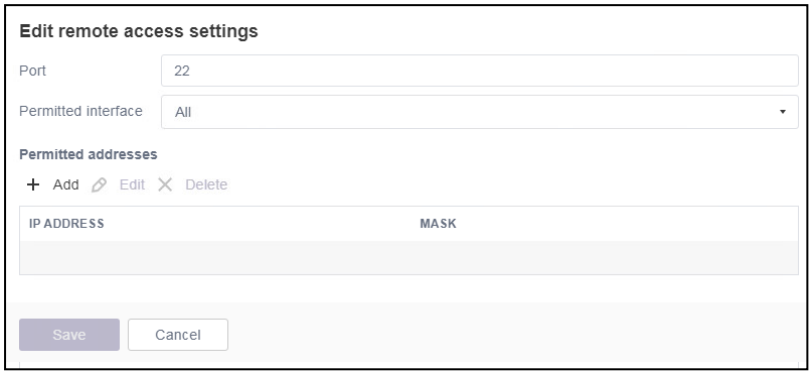
2. To enable/disable the remote access, turn on/off the **Access** toggle.

   Note. If remote access to the Server is enabled, an access password is generated automatically and a user cannot be changed.
3. To establish a secure connection via the TLS tunnel, turn on the **Secure connection** toggle (turned off by default).
4. Click **Configure** to go to the **Tunnel parameters** tab. If necessary, change the tunnel settings (see p. **65**).

Note. The secure connection configuration is possible only via a web interface with the TLS Client of version 2. SSH traffic is additionally encapsulated into the TLS protocol during the secure connection. An administrator certificate is required for access to the secured SSH tunnel.

5. To change the current password, click next to the respective password and click **Change password**.
6. To change other parameters, select the respective Server and click **Edit** on the toolbar.

   The **Edit remote access settings** page opens.



7. Specify the number of the used port.

Note. The 22 port of the TCP/IP protocol stack is assigned by the Internet Assigned Numbers Authority (IANA) for the SSH protocol.

8. Select the required interface from the **Permitted interface** drop-down list.
9. To make changes in the list of the allowed IP addresses, click **Add**, **Edit**, or **Change** on the toolbar. Click **Add** to add a new IP address. In the **Add permitted addresses** section, specify the IP address and mask. Click **Apply**.
10. Click **Save** at the bottom of the section to save the changes.

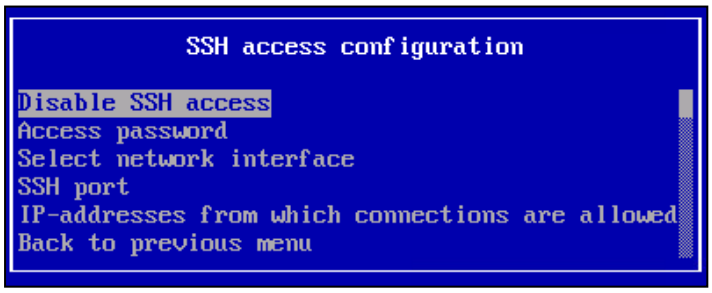
    The remote access configuration is now changed and information on the screen is updated automatically.

To configure access via the local menu:

1. In the **Main menu**, select **Remote access configuration** and press **<Enter>**.

   The **External access configuration** menu appears.
2. Select **SSH access configuration** and press **<Enter>**.

   The **SSH access configuration** menu appears.



3. To enable or disable SSH access, select the respective option.

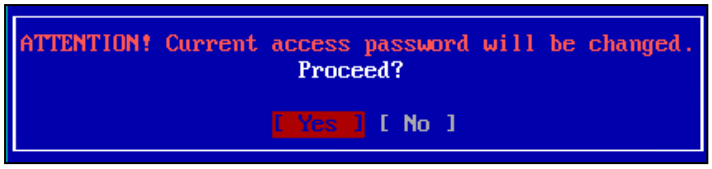
   The remote access configuration will change and the information message appears. To return to the **SSH access configuration** menu, press **<Enter>**.

To generate a new password via the local menu:

1. Select **Access password** and press **<Enter>**.

   The **Access password** menu appears.
2. Select **Generate new password** and press **<Enter>**.

   A warning message appears.



Note. To return to the previous menu without changing the current password, select **No** and press **<Enter>**.

3. To continue, press **<Enter>**.

   The password will be regenerated and the message **Remote access password successfully changed** appears.
4. To return to the previous menu, press **<Enter>**.

To view the current password using the local menu:

1. Select **Access password** and press **<Enter>**.

   The **Access password** menu appears.
2. Select **Show current password** and press **<Enter>**.

   The current access password is displayed.
3. To return to the previous menu, press **<Enter>**.

To select the network interface using the local menu:

1. In the **SSH access configuration** menu, select **Select network interface** and press **<Enter>**.

   The list of the configured network interfaces appears.
2. Select the required interface or **Enable all interfaces** and press **<Enter>**.

   The remote access configuration is changed.
3. To return to the **SSH access configuration** menu, press **<Enter>**.

To select the port for a remote connection using the local menu:

1. In the **SSH access configuration** menu, select **SSH port** and press **<Enter>**.

   The remote control server port number appears.
2. To change the port number, enter a new number and press **<Enter>**.

   Note. The 22 port of the TCP/IP protocol stack is assigned by the Internet Assigned Numbers Authority (IANA) for the SSH protocol.

   The remote access configuration is changed.
3. To return to the **SSH access configuration** menu, press **<Enter>**.

To specify the IP addresses from which connections are allowed using the local menu:

1. Select the IP addresses from which connections are allowed and press **<Enter>**.

   The list for entering the allowed IP addresses appears.
2. Select the required address in the list, and press **<Enter>**.

   A dialog box prompting you to enter the IP address and network mask appears.
3. Enter the IP address and press **<Enter>**.

Configure system time

The local and remote management tools are used for:

- setting the system time and date;
- configuring connection to the NTP server.

Attention! The Server does not support time zones. The Server time always matches UTC.

To change the system time using the remote management tools:

1. In the **Menu**, go to **Settings | Date and Time**.
2. For the forced configuration of the system date and time, specify the required parameters in the respective fields.

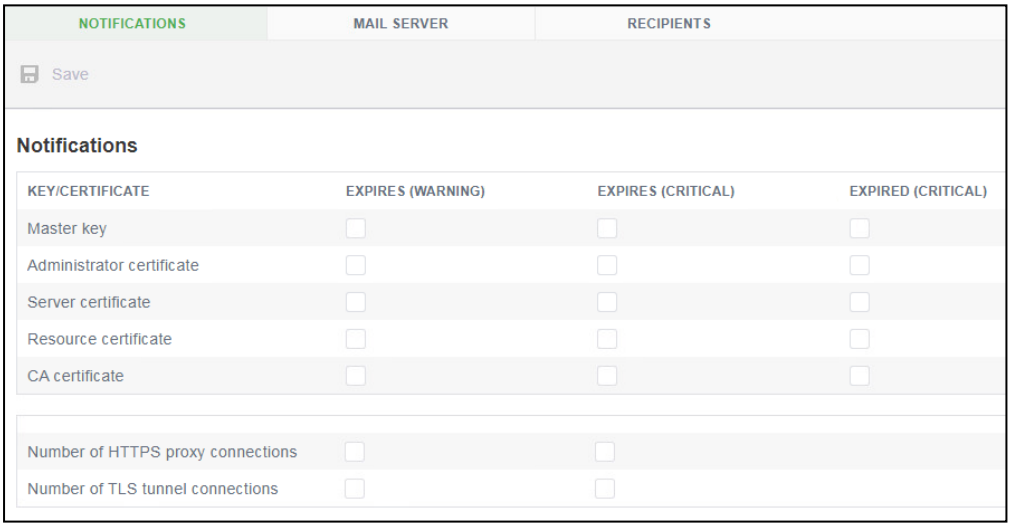
3. For automatic synchronization with the NTP server, in the **NTP server address** field, specify its IP address or name. Select the **Enable synchronization with the NTP server** check box, then click **Save** on the toolbar.

To manage the system time using the local menu:

1. In the **Main menu**, select **System time and date** and press **<Enter>**.
   The **System time and date** menu appears.
2. For the forced configuration, select **Set system time and date** and press **<Enter>**.
   The **Set system time and date** dialog box appears.
3. Enter the system time and date values and press **<Enter>**.
   The specified parameters are applied.
   A notification about the successful setting appears.
4. To set the automatic synchronization with the NTP server, select **Configure NTP** and press **<Enter>**.
   A dialog box prompting you to enter the NTP server address appears.
5. Enter the IP address of the NTP server and press **<Enter>**.
   The NTP operation is checked and the specified parameter is set. You are returned to the **System time and date** menu.

Configure notifications and connection to email server

Notifications and connection to the mail server configuration are available in the **Notifications** section.



The Server sends notifications about the expiration date of the master-key, administrator, Server, resources and CA certificates, the number of TLS tunnel and HTTPS proxy connections.

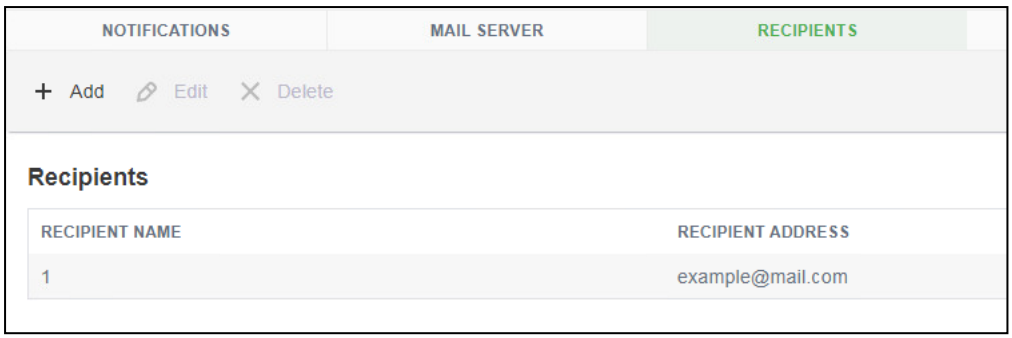
Attention! To receive notifications via email, it is necessary to establish the connection to a mail server.

The first warning notification is sent two weeks before the expiration date. Then, it is sent daily. The first critical notification is sent a week before the expiration date. Then, it is sent daily.

When reaching 70% or/and 90% of the active connections maximum number specified in the license, the Server automatically sends notifications on a daily basis using email.

To configure the notification system:

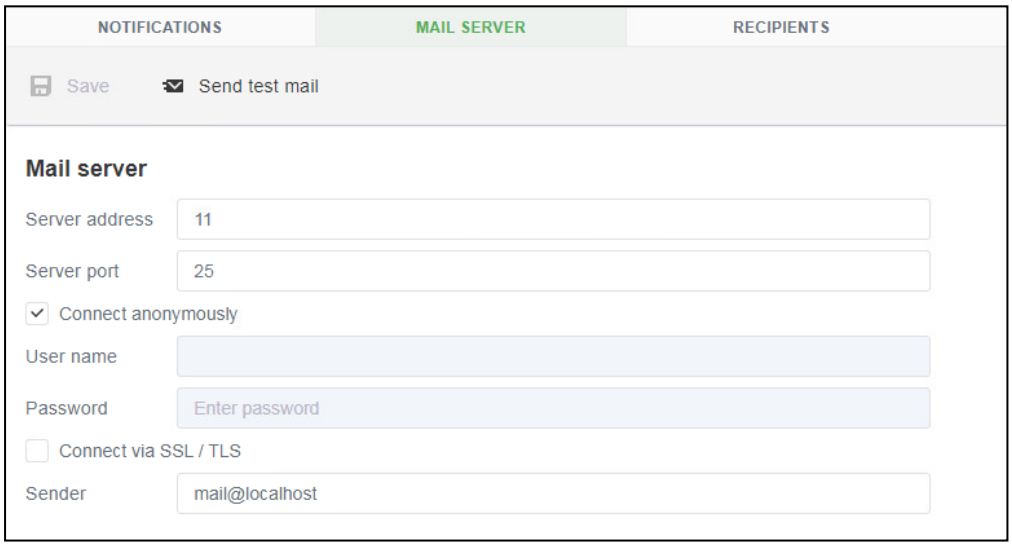
1. In the **Menu**, go to **Settings | Notifications**.
   The **Notifications** menu appears (see above).
2. Select the check boxes of events you want to receive notifications about, and click **Save** on the toolbar.
3. In the **Recipients** section, click **Add**.
4. In the **Add recipient** menu, specify the name and email address of the administrator and click **Save**.
   The new recipient appears in the **Recipients** list.



Note.
- To edit the existing recepient parameters, select a recipient in the list, click **Edit** on the toolbar, edit the required parameters and click **Save**.
- To delete a recipient from the list, select a recipient and click **Delete** on the toolbar.

To configure connection to a mail server:

1. Go to the **Mail server** section.
   The **Mail server** menu appears.



Attention! Entering the user name and password is forbidden by default. To enter the logon data, clear the **Connect anonymously** check box.

2. Enter the respective information.
   The standard mail server ports are specified in the RFC specification.

Protocol	Port	Port for the SSL/TLS
SMTP	25 (587)	465
POP3	110	995
IMAP	143	993
NNTP	119	563

3. On the toolbar, click **Save**.
4. A dialog box prompting you to confirm the procedure appears.
   Click **OK**.

Note. To check the connection to a mail server, click **Send test mail** on the toolbar. Specify the required parameters in the **Send test letter** section and click **Send**.

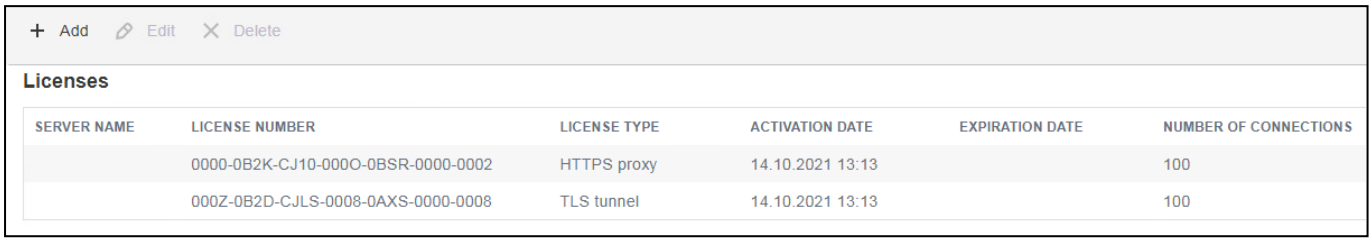
Licenses

You can view, add, edit and delete the installed licenses, which limit the number of client sessions, by means of remote management tools.

Attention! A user can edit the installed license only in the part of selecting the Server to which the license is added.

TLS Server requires the installing of certificates of two types. A specific type of license is required for the operation in proxy mode (HTTPS-proxy and Application portal) and TLS tunnel mode.

You can work with licenses in **Settings | Licenses**.



The **Number of connections** column contains the information about the total number of authorized HTTPS connections.

To add a license:

1. In the **Licenses** menu, click **Add** on the toolbar.

   A dialog box prompting you to enter the license parameters appears.
2. Enter a license number, select the required Server in the **Server** drop-down list and click **Save**.

   Note.
   - It is not necessary to specify the Server license number. In this case, the number of the connections is equally distributed among the active Servers of the cluster, the remainder of the division is assigned to a primary Server. It is possible to use this option for the clusters of similar hardware platforms.
   - No more than 65 535 connections can be assigned to a Server.

   The license appears in the list.

To edit a license:

1. In the **Licenses** menu, select the respective license and click **Edit** on the toolbar.

   A dialog box prompting you to enter the license parameters appears.
2. In the **Licenses** menu, select the Server to which you want add the license.
3. Click **Save**.

   A new Server name appears in the list.

To delete a license:

1. In the **Licenses** menu, select the license and click **Delete** on the toolbar.
2. In the appeared dialog box, click **Delete**.

   The license is deleted from the list.

Server and Client software update

The update is performed when the Server software is upgraded to a newer version. The update is stored on a compact disk or a USB flash drive. If necessary, you can store a disk image on a USB flash drive (see p. **90**).

Note. For more information on how to install the Server software, see p. 87.

The update procedure can be performed on a standalone Server as well as on the primary Server of a cluster. If the update is performed on the primary Server of a cluster, the update replication is performed on all subordinate Servers.

You can update the Server software by installing the firmware on a new version and uploading a backup copy.

To install an update using the local menu:

1. Save a master key to an external drive (see p. **18**).
2. Create and save a backup copy to the external drive (see p. **42**).
3. Install software of a newer version (see p. **87**).
4. Configure the Server network parameters (see p. **15**).
5. Import a master key to the updated Server (see p. **18**).

6. Initialize the updated Server (see p. **20**).
7. Restore the Server software from a backup copy (see p. **43**).

Note. You can view the results of the performed action in the list of the installed updates (see below).

View installed Server software updates

You can view installed Server software updates using the remote management tools in **Log** | **Settings** | **Server Update**.

The update log consists the following information:

- date and time of the update installation;
- version;
- Server name;
- status (successful or unsuccessful);
- operation (update or replication).

Server software backup and restoration

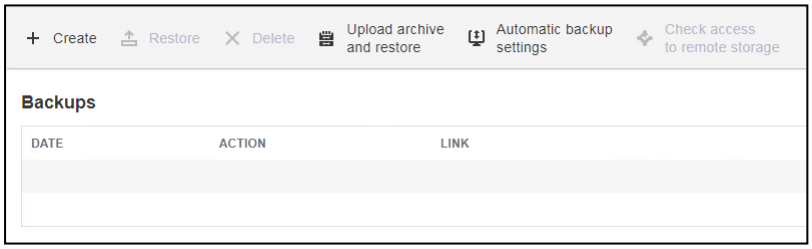
Create and delete a backup copy

We recommend exporting a master key to an external drive using the local menu before creating a backup copy (see p. **18**). A master key must be uploaded if it is necessary to initialize the Server applying the settings from a backup or the Server is restored from a backup after a master key was regenerated on it.

To create a backup by means of remote management:

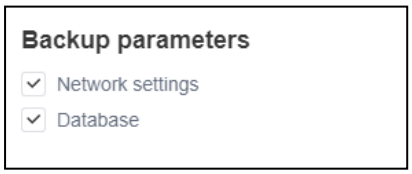
1. In the **Menu**, go to **Settings | Backups**.

   The list of created backup copies appears. If backup copies were not created before, the list is empty.



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

   A dialog box prompting you to specify the backup parameters appears (turned on by default).



3. In the **Backup parameters**, select the required parameters of the backup creation and click **Create**.

   The dialog box closes, the list of backup copies appears.

4. To get up-to-date information, refresh the web page.

   The information about the operation, the date of creation of the backup and a link to download the archived backup of the Server software appears. The message about the file location appears at the bottom of the screen.

5. If necessary, select the required backup in the list and save it to a hard drive or an external drive.

   Tip. If you use Internet Explorer, to save a file in a respective folder, select **Save As** from the save menu drop-down list (to the right of the **Save** button).

To delete a previously created backup

1. In the **Backups**, select the required backup from the list.
2. On the toolbar, click **Delete**.

The copy is deleted from the list.

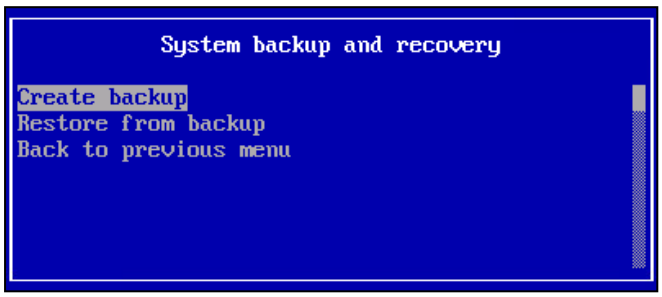
3. To get up-to-date information, refresh the web page.

To create a backup copy using the local menu:

Attention! The deletion of backup copies created earlier is possible only by means of remote management.

1. Insert the external drive into a USB port to save a backup copy.
2. In the **Main menu**, select **System backup and restore** and press **<Enter>**.

   The **System backup and recovery** menu appears.



3. Select **Create backup** and press **<Enter>**.

   The backup is saved to an external drive.

   A message about successful backup appears.
4. To return to the **Main menu**, press **<Enter>**.

Note. The backup copy can be created on any Server of the cluster using the local menu.

Restore from a backup copy

If the Server is initialized using backup settings or the second generation of the key was performed on the Server, upload the master key used in the creation of the backup copy and export it to a security token. The local management tools are used for uploading a master key from a token (see p. **18**).

The remote management tools allows you to restore from a software backup copy stored on a hard drive or an external drive.

To restore the settings from a backup copy stored on a hard drive using the remote management tools:

1. In the **Menu**, go to **Settings | Backups**.
2. In the list of backups, select the backup copy you need to restore and click **Restore**.

   The dialog box with the settings for restoring from a backup appears.
3. Specify the respective parameters and click **Restore**.

   A message that the backup copy has been used and the Server is temporarily unavailable appears.
4. Close the notification dialog box.

   The restoration of the Server settings continues. When the restoring is finished, the notification about the successful completion of the operation appears.

Attention! If the initial Server was changed with the other similar equipment with the same parameters or settings while restoring from a backup copy, it is necessary to register a license for the equipment after the restoration.

If the restoration is performed on equipment with a different software platform, we recommend checking its settings and if necessary, changing the network parameters after the restoring.

To restore the settings from a backup copy stored on an external drive using the remote management tools:

1. Insert the external drive with a backup copy into a USB port.
2. In the **Backups**, select **Upload archive and restore**.

   The dialog box prompting you to specify the settings for restoring from a backup and an archive selection dialog box appears.

3. Specify the restoration parameters.
4. To select an archive file, click **+**.

   A dialog box prompting you to select a file appears.
5. Select the required archive and click **Open**.

   Note. The default name of a backup file is **backup-YYYY_MM_DD__hh_mm.tar**, where **YYYY_MM_DD** and **hh_mm** — its date and time of creation.

   The file name appears.
6. Click **Restore**.

   A message notifying you that the backup has been applied and the Server is temporarily unavailable appears.
7. Close the notification dialog box.

   The restoration of the Server settings continues. When the restoration is finished, a notification about the successful completion of the operation appears.

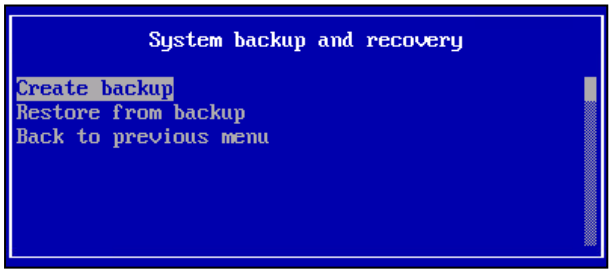
Attention! If the Server is replaced by another similar device with the same parameters and settings while restoring, you must register the license to the device again.

If the restoring is performed on a device with a different hardware platform, you should check and if necessary, change the network parameters after restoring.

To restore the settings using the local menu:

1. In the **Main menu**, select **System backup and restore** and press **<Enter>**.

   The **System backup and recovery** menu appears (see p. **42**).



2. Select **Restore from backup** and press **<Enter>**.

   A message that the settings will be changed and a prompt to continue the operation appears on the screen.
3. Select **Yes**, press **<Enter>**.

   The list of backup archives appears.
4. Select the required archive and press **<Enter>**.

   The restoring of the Server settings starts.

   A message about successful restoring appears.
5. Press **<Enter>**.

   The restored settings are applied. You are returned to the **System backup and recovery** menu.

   Note. Restoration of the settings from a backup copy using the local menu is only possible on the primary Server of a cluster.

Configure automatic backup

Automatic backup configuration is performed using the remote management tools only.

To configure automatic backup:

1. In the **Menu**, go to **Settings | Backups**.

the **Backups** menu appears.

2. On the toolbar, click **Automatic backup configuration**.
   The **Automatic backup configuration** menu appears.
3. Select the **Enable automatic backup** check box.
   The automatic backup parameters become available for editing.
4. Specify all the required parameters shown in the table below.

Parameter	Action
Include the following settings in an archive	
Network settings	Allows you to include network settings in a backup copy. Default value — **ON** To configure automatic backup, select at least one of the **Network settings** or **Database** check boxes
Database	Allows you to include a Server database in a backup copy. Default value — **ON** To configure automatic backup, select at least one of the **Network settings** or **Database** check boxes
Schedule	
Start time	Allows you to select the start time of the backup
Week days	Allows you to select the week days when the backup is performed
Remote storage settings	
Server address	Allows you to specify a remote storage address. In the drop-down list, select a remote server protocol, specify its address and port. Default protocol value — **ftp**
Folder	Allows you to specify a folder in which the backup copy is stored
Passive mode	Allows you to activate the passive mode. Default value — **OFF** The passive mode is available only if the **ftp** is selected in the **Server address** field
Use authentication	Allows you to authenticate users on a remote server. Default value — **OFF**
User name	Credentials for authentication on a remote server. If a user name is specified, the **Password** field cannot be empty. They are available for configuration only if authentication is enabled
Password	
Proxy server	
Use Proxy server	Allows you to use a proxy server. Default value — **OFF**.
Proxy server address	Allows you to specify the address of a required proxy server. In the drop-down list, select a proxy server protocol, specify its address and port. Default protocol value — **http**
Use authentication on a proxy server	Allows you to authenticate users on a proxy server. Default value — **OFF**
User name	Credentials for authentication on the server. If a user name is specified, the **Password** field cannot be empty. They are available for configuration only if authentication is enabled
User password	
Additionally	
Name	Allows you to specify the name of a backup copy. Default value: `backup_data_time` where **data** — backup copy creation date, **time** — creation time
Delete backups older than	Allows you to specify the number of the days after which the old backup copies are deleted. Default value — **5**

5. Click **Save**.
   Automatic backup settings are applied.

Checking access to the remote storage:

To check access to the remote storage in the **Backups** menu, click **Check access to remote storage**.

If the remote storage is available, the **Access established** message appears. Otherwise, the **Failed to establish access** message appears. The **Check the settings** message appears.

Synchronization with WAF

The blocking of sessions established using user certificates with suspicious activity is performed based on data received from Continent WAF (hereinafter — the WAF). This data contains the certificate number using which the session with suspicious activity is established.

After the detection of suspicious activity using data provided by the WAF, the following actions are performed:

1. The TLS Server searches for a session with a specified user certificate.
2. The certificate number is added to the list of blocked user certificates.
3. Session establishment using this certificate is terminated.

Note. Anonymous sessions are not processed.

If a certificate is blocked or an attempt to establish a session using a blocked certificate is detected, the Server redirects a user to the page with information about the reasons for blocking.

The blocking of the certificates is performed automatically based on the WAF criteria for suspicious activity.

A certificate can be deleted from the list of blocked user certificates in automatic or manual mode. A user certificate is automatically deleted from the list of blocked user certificates when its blocking time is over. An administrator can also delete a certificate from the list of blocked user certificates manually before its blocking time is over.

It is possible to add a certificate to the list of allowed user certificates. If a user certificate is added to the list of allowed user certificates and the WAF defines a session created using it to be suspicious, the session is not blocked.

Note. If a user certificate is deleted from the list of allowed user certificates and if suspicious activity is detected while establishing a session using it, the certificate is blocked.

The following certificates must be added to the Server base for the WAF identification:

- WAF client certificate;
- root certificate and/or root certificate chain.

The configuration of a user certificate filtration is possible only by means of remote management.

Attention! The configuration of a user certificate filtration is not possible without the WAF certificates.

To add a WAF certificate:

1. In the **Menu**, go to **Settings | WAF synchronization**.
   The **WAF settings** menu appears.
2. Go to the **WAF certificates** section.
   The sections for importing client and CA certificates appears.
3. Click **Import** in the section of the required certificate type.
   The dialog box prompting you to select a file appears.
4. Select a certificate file and click **Open**.
   The selected WAF certificate is added to the list of certificates.

Attention!

- If the WAF certificate you are adding does not pass the expiration check and/or the certificate chain is not trustworthy, the respective message appears. The WAF certificate is not added to the Server base.
- If the WAF certificate you are adding does not pass the CRL check, the certificate is added to the Server base and the check of a CRL state is performed.
- If the certificate successfully passes the checking, the certificate is added to the Server base with the **Valid** status.

To export a WAF certificate:

1. In the **WAF settings** menu, go to the **WAF certificates** section.
   A dialog box for importing the client and CA certificates appears.

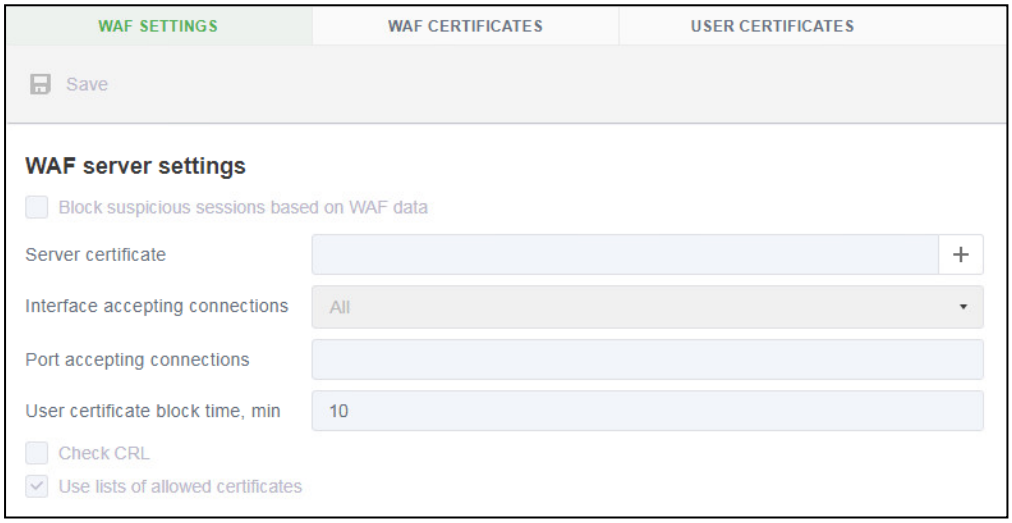
2. Select the WAF certificate to export.
3. Click **Export**.
   The WAF certificate will be saved on the administrator computer.

To delete a WAF certificate:

1. In the **WAF settings** menu, go to the **WAF certificates** section.
   The window for importing client and CA certificates appears.
2. Select the WAF certificate you want to delete.
3. Click **Delete**.
   The WAF certificate is deleted from the list.

To configure a WAF server:

1. In the **WAF settings** menu, go to the **Parameters** tab.
   The **WAF server settings** menu appears.



2. Click **+** in the **Server certificate** field.
3. Specify the required cerificate and click **Select**.
   The **Block suspicious sessions based on WAF data** toggle is turned on.
4. Turn on the **Block suspicious sessions based on WAF data** toggle.
   Parameters become available for specifying (see below).
5. If necessary, specify the following parameters:
   - **Interface accepting connections;**
   - **Port accepting connections;**
   - **User certificate block time;**
   - **Check CRL;**
   - **Use lists of allowed certificates.**
6. On the toolbar, click **Save**.
   The specified parameters are applied, as a result the blocking of suspicion sessions is performed automatically.

To delete a certificate from the list of blocked user certificates:

1. In the **WAF settings** menu, go to the **User certificates**.
   Sections with the lists of blocked or allowed user certificates appears.
2. In the blocked user certificates list, select the certificate number of the required certificate.
3. Click **Delete**.
   The certificate is deleted form the blocked user certificates list.

To edit the list of allowed user certificates:

1. In the **WAF settings** menu, go to the **User certificates**.

Sections with the lists of blocked or allowed user certificates appears.

2. To add a certificate to the list of allowed user certificates, perfprm the following steps:
   - in the **Allowed user certificate** menu, click **Add**;
   - in the **Serial number of the certificate** field, specify the certificate number;
   - click **Save** at the bottom of the screen.

   The certificate is added to the list of allowed user certificates.
3. To delete a certificate from the list of allowed user certificates, select its certificate number in the list and click **Delete**.

   The certificate is deleted form the list of allowed user certificates.

To add or delete a certificate, repeat steps **2** or **3** for each certificate.

Chapter 4
Monitoring and audit

Working with logs

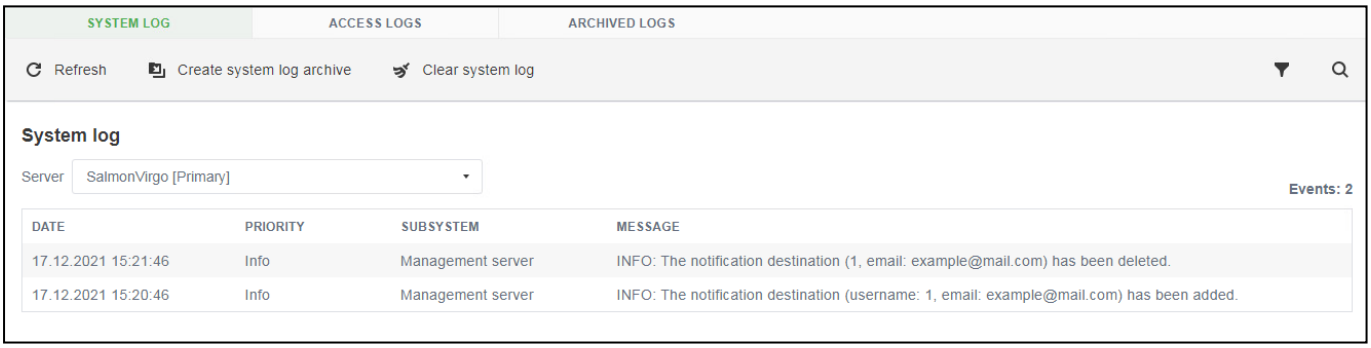
The **Logs** menu contains the following tabs:

- **System log** — allows you to configure registered events display settings, receive up-to-date information about events, export a log to the administrator's workstation and clear a log.
- **Access logs** — allows you to manage log export to the administrator's workstation.
- **Archived logs** — allows you to find information about the created archives. You can manage the storage export to the administrator's workstation and access logs removal.

Attention! Export to the administrator's workstation is available using the remote management tools by default. Only export to an external drive is available using the local menu.

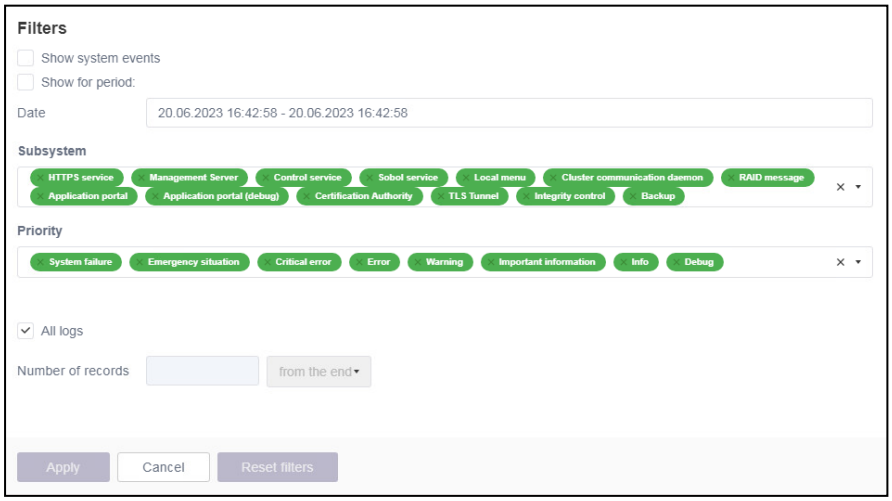
View logs

System events and the Server management events and application errors are stored in the Server database. You can view these events using the local menu or the remote management tools. The events are displayed according to the log verbosity level.



To view the system log using the remote management tools:

1. In the **Menu**, select **Logs**.
   The **System log** menu appears according to the filtering configuration.
2. Specify the Server name.
3. To configure filtering parameters, press  on the toolbar.
   The **Filters** dialog box appears.



4. To view the system events, select **Show system events**.

Note. If the check box is cleared, only the Server management events are displayed. Otherwise, the system events are displayed as well.

5. To view the system log for a certain period, perform the following steps:
   - select **Show for period**;
   - specify the start and finish dates as shown in the example.
6. In the **Subsystem**, select the necessary options for viewing events in the list.
   The selected items appear in the **Subsystem** section.
7. To delete an option, click on the left of the item.
8. In the **Priority** section, configure the parameters in the same way.
9. To apply changes, click **Apply**.

Note. To discard the filtering configuration, click **Reset filters**, then **Apply**.

10. To search for the events in the log, use **Search** on the toolbar.
11. To get the latest version of the logged events, click **Refresh** on the toolbar.

Attention! You can view only the system log using the remote management tools. Viewing access logs and log archives is available using the local menu only. Viewing access logs using the local menu is available only after exporting them to the administrator's workstation.

To view the system log using the local menu:

1. In the local menu, select **Logs** and press **<Enter>**.
   The **Logs** menu appears.
2. Select **Browse logs** and press **<Enter>**.
   The **Browse logs** menu appears.
3. To view all the events, select **Browse system log** and press **<Enter>**.
   The **System log browser** menu appears.

Note. To view the system events, press **<F2>**.

4. To view a certain log, select **Browse access logs** and press **<Enter>**.
   The list of access logs stored on the Server appears.
5. Select the required log and press **<Enter>**.
   The log contents appear.
6. After viewing the log, close it by pressing **<Esc>**.

Export logs to the administrator's workstation

To export the system log:

1. In the **Menu**, select **Logs**.
   The menu section appears.
2. Click .
   The **Filters** menu appears.
3. In the **Date** section, choose the period and click **OK**.
4. If necessary, specify the required parameters.
5. Click **Apply**.
   The **Filters** menu closes and the list of the events appears.
6. On the toolbar, click **Create system log archive**.
7. Go to **Archived logs**.
8. Select the required archive and click **Export** on the toolbar.

Attention! If the system log for the chosen period contains more than 700 000 records, specify another time period for which logs will be exported.

The process of saving files onto the administrator's workstation hard drive begins. The saved file will be available for further viewing in a text editor.

To export the access log:

1. In the **Logs**, go to **Access logs**.

   The list of the logs available for export appears.
2. Select the required log and click **Export** on the toolbar.

   The process of storing files onto the administrator's workstation hard drive begins. The saved file will be available for further viewing in a text editor.

To export log archives:

1. In the **Logs** section, go to **Archived logs**.

   The list of the archived logs available for export appears.
2. Select the required archive and click **Export** on the toolbar.

   The process of storing files onto the administrator's workstation hard drive begins. The saved file will be available for further viewing in a text editor.

Export logs to an external drive

To export the system log:

1. In the local menu, select **Logs** and press **<Enter>**.

   The **Logs** menu appears.
2. Select **Export logs** and press **<Enter>**.

   The **Export logs** menu appears.
3. Select **System log export** and press **<Enter>**.

   The message prompting you to insert a USB drive appears.
4. Insert an external drive and press **<Enter>**.

   The **Select storage** menu appears.
5. Select the required option and press **<Enter>**.

   The system log export to the external drive starts in the format of a **syslog-YYYYMMDDhhmm,** text file where **YYYYMMDDhhmm** is the export date and time. After the export, the **Success** message appears.

   Note. When exporting the log using the web management tools, the number of exported records is limited to 700 000.
6. To close the dialog box, press **<Enter>** or **<Esc>**.

To export access logs:

1. In the local menu, select **Logs** and press **<Enter>**.

   The **Logs** menu appears as in the figure below.
2. Select **Export logs** and press **<Enter>**.

   The **Export logs** menu appears.
3. Select **Access log** export and press **<Enter>**.

   The message prompting you to insert a USB drive appears.
4. Insert an external drive and press **<Enter>**.

   The log export to the external drive starts in the format of an archive **tls-log** file. After the export, the **Success** message appears.
5. To close the dialog box, press **<Enter>** or **<Esc>**.

Clear the system log

Attention! When clearing the system log, all the records about administrator's activity and key information events are deleted.

To clear the system log:

1. In the **Menu**, select **Logs**.

   The **System log** menu appears.
2. To delete the system log records, click **Clear system log** on the toolbar.

   The dialog box prompting you to confirm the operation appears.

3. Click **Clear logs**.
   The system log records will be deleted.

To delete log archives (available only via the remote management tools):

Note. To delete certain log archives, select the required archives, press **Delete** on the toolbar and confirm the operation.

1. In the **Logs** section, go to **Archived logs**.
   The list of the log archives appears.
2. On the toolbar, click **Delete all archives**.
   The dialog box prompting you to confirm the deletion appears.
3. Click **Delete all archives**.
   The archived records will be deleted.

To clear the system log using the local menu:

1. In the local menu, select **Logs** and press **<Enter>**.
   The **Logs** menu appears.
2. Select **Clear logs** and press **<Enter>**.
   The **Clear logs** menu appears.
3. Select **Clear system log** and press **<Enter>**.
   The dialog box prompting you to confirm the operation appears.
4. Select **Yes** and press **<Enter>**.
   The records will be deleted.

Monitoring

The **Monitoring** menu includes the following sections:

- SNMP;
- Collecting statistics.

SNMP management

SNMP is used for network device monitoring and notifying about the events that require the attention of the administrator.

The server state is checked every ten minutes. The result is saved to the syslog. An agent can request notifications about the status of certain parameters regarding the state of the server.

For the Continent TLS Server monitoring the default versions of SNMPv1 and SNMPv2 are enabled. SNMPv3 requires an additional configuration.

To configure the sending of notifications:

1. In the Menu, go to **Settings | SNMP**.
   The **Parameters** menu appears.
2. Turn on the **Enable SNMP server** toggle to enable the sending of notifications.
   The **SNMP domain name** and **Authorized network** fields become available for editing.
3. Specify the SNMP domain name and the authorized network.

   Note. The default SNMP domain is public. The domain and network configuration does not affect the SNMPv3 operation. We recommend using a network mask for security concerns. If the predetermined events occur on the device, the agent independently sends the data about them to the administrator.
4. Additionally, specify the Server location and the administrator email in the respective fields.
5. On the toolbar, click **Save**.
   A message about the successful change of settings appears.

To configure SNMPv3:

1. In the **Parameters** menu, go to **SNMPv3 settings** and turn on **SNMPv3**.
   The **SNMPv3 user name** and the **SNMPv3 user password** fields become available for editing.

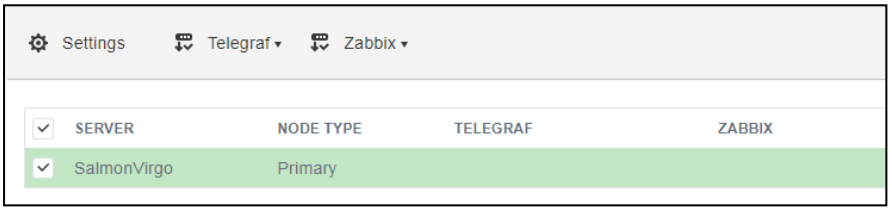
2. Enter the user name and password.
3. On the toolbar, click **Save**.
   A message about the successful change of the settings appears.

To configure SNMP notifications:

1. In the **Parameters** menu, go to **Access**.
   The list of the information sent in the SNMP notifications appears.
2. Turn on the toggles for the information you want to receive. To deny receiving, turn off the respective toggles.
3. On the toolbar, click **Save**.
   The settings are changed.

Collecting statistics

Monitoring and collecting statistics are performed using Telegraf and Zabbix. You can manage these utilities using the remote management tools.



Telegraf

After the Server initial installation and configuration, collecting statistics using Telegraf is enabled by default.

To manage the statistics collection using Telegraf:

1. In the **Menu**, go to **Settings | Monitoring**.
2. Click **Collecting statistics**.
   The **Collecting statistics** menu appears.
3. Select the Server or the Servers from the list for which you want to configure Telegraf to collect statistics.
4. On the toolbar, click **Telegraf**.
   In the drop-down list, select the respective option.
5. Specify the required value.

   Note. You can disable the statistics collection by Telegraf only if statistics collection by Zabbix-agent is turned on.

   The statistics collection for the specified Server or Servers by Telegraf is configured.

Zabbix-agent

Collecting statistics using Zabbix-agent is disabled by default.

To collect statistics using Zabbix-agent, install the **rpm** file on the Server and import the Zabbix-agent configuration.

To install Zabbix-agent using the local menu:

1. In the **Main menu**, select **Diagnostics** and press **<Enter>**.
   The **Diagnostics** menu appears.
2. Select **Install Zabbix-agent** and press **<Enter>**.
3. Select a USB flash drive and press **<Enter>**.
   A dialog box prompting you to insert a USB Flash drive appears.
4. Insert an external drive and press **<Enter>**.
   The utility will be installed on the Server.

To configure the statistics collection using Zabbix-agent:

1. In the **Collecting statistics** menu, select the required Server.
2. On the toolbar, select **Settings**.
   The **SalmonVirgo** menu appears.

3. Go to **Zabbix** section.
4. Click **Import configuration**.
   A dialog box prompting you to select a file appears.
5. Select Zabbix-agent configuration file and click **Open**.
   The imported file contents are displayed.
6. Click **Apply**.

To manage the statistics collection using Zabbix-agent:

1. Go to the **Collecting statistics** menu.
2. Select the Server or the Servers from the list for which you want to configure Zabbix-agent to collect statistics.
3. Click **Zabbix** on the toolbar.
   In the drop-down list, select the respective option.
4. Specify the required value.
   The statistics collection performed by Zabbix-agent for the specified Server or Servers is configured.

Chapter 5
Certificates

You can manage certificates using the local or the remote managing tools as follows:

- view the list of certificates (see below);
- create a request to issue a certificate (see p. **55**);
- upload an administrator certificate from the administrator's workstation or from a USB drive (see p. **57**);
- delete CA certificates (see p. **58**).

The Server remote management tools provide you with an extended list of opportunities to search, delete and export certificates, to export certificates to an external drive and configure additional parameters of certificate verification (see p. **32**).

View certificates

You can view the lists of:

- root and intermediate CA certificates;
- Server certificates;
- administrator certificates;
- revoked certificates (only via the remote management tools, see p. **75**);
- digital signature update file verification certificates (only via the local menu).

Certificates in the list are defined by the following parameters:

- issued to (IP address or subject name);
- issued by (IP address or issuer name);
- serial number;
- validity period and current status;
- certificate type (only for the Server certificates);
- CRL status (only for the CA certificates).

Note. To learn more about the certificate structure and parameters, see p. 87.

To view the certificates using the local menu:

1. In the local menu, select **Certificates** and press **<Enter>**.
   The **Certificates** menu appears.
2. Select the required certificate and press **<Enter>**.
   The **Certificates** menu appears.
3. Select **Show certificates** and press **<Enter>**.
   The **Certificates list** appears.
4. To exit, press **<Esc>**.

When viewing the certificate list using the remote management tools, you can search the required certificate, view the list of invalid certificates, remove selected certificates.

To view the list of certificates using the remote management tools:

- In the **Menu**, go to **Certificates**, then select the certificate category.

The **Certificate** toolbar contains items specified in the table below.

Button	Action
Import	Import a new certificate or a CRL from an external drive
Export	Export a certificate or request to the external drive
Delete	Delete the selected certificate or request from the list
Delete expired certificates	Delete expired certificates from the list (unavailable for the Server certificates)

Button	Action
Delete all	Delete all the certificates from the list (unavailable for the Server certificates)
Filter	Show only expired certificates
Search	Search in certificates by name or IP address

Server certificate request

In the **Server certificates** section, there is a tab informing about requests to create a Server certificate. When you select it, a list of submitted requests will be displayed in form of a table.

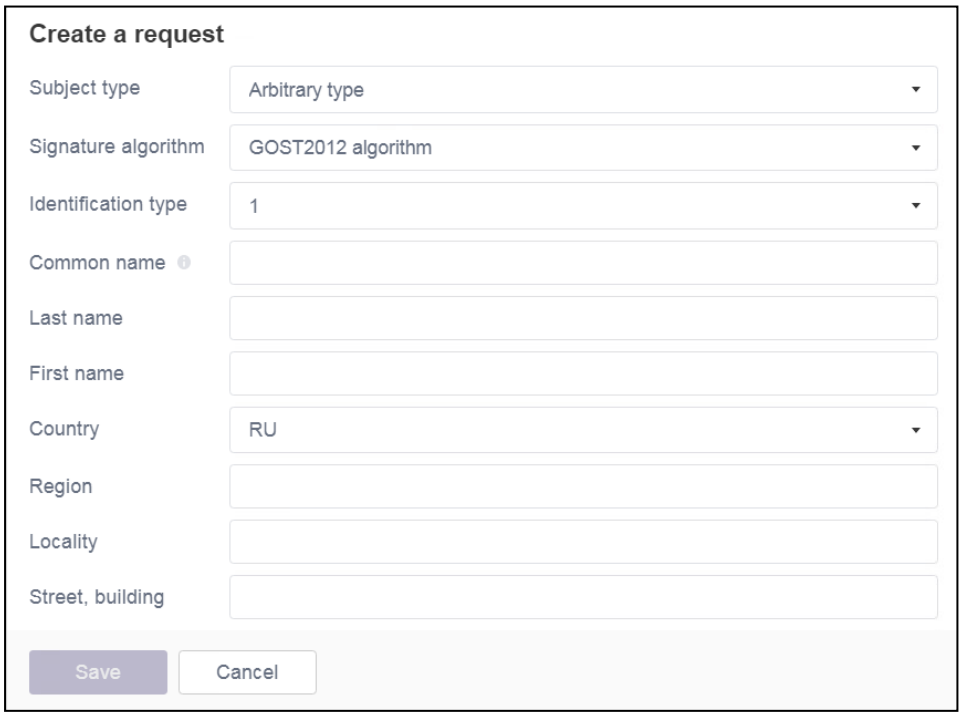
To receive the Server certificate, create a request and send it to the Certification Authority.

To create a request using the local menu:

1. Insert a USB drive to write a request onto it.
2. In the local menu, select **Certificates** and press **<Enter>**.
   The **Certificates** menu appears.
3. Select **Server certificates** and press **<Enter>**.
   The **Server certificates** menu appears.
4. Select **Create certificate request** and press **<Enter>**.
   The **Create a request** form appears.
5. Specify the fields using the arrows to move through the lines and press **<Enter>**.
   A dialog box prompting you to specify the GOST version appears.
6. Select the GOST version and press **<Enter>**.
   A request file will be written to the external drive. You will be returned to the **Certificates** menu.
7. Send the request file to the Certification Authority.

To create a request using the remote management tools:

1. In the **Menu**, go to **Certificates | Server**.
   The **Server certificates** menu appears.
2. Go to **Requests** and click **Create request** on the toolbar.
   The **Create a request** form appears.



   Fields required for filling, marked with the **i** sign.
3. Specify the **Subject type** by choosing it from the list:

- Arbitrary type;
- Individual;
- Entity;
- Individual (legal entity).

The **Create a request** form and its fields depend on the **Subject type** value. The required fields for every **Subject type** are shown in the table below and marked with the **+** sign.

Attribute	Arbitrary type	Individual	Individual (legal entity)	Entity
Common name	+	+	+	+
Last name	–	+	+	–
First name	–	+	+	–
Country	+	+	+	+
Region	–	–	+	+
Locality	–	–	+	+
Street, building	–	–	+	+
Organization	–	+	–	–
Department	–	–	–	–
Title	–	–	+	–
Email	–	–	–	–
INN	–	+	+	–
INNLE	–	–	–	+
SNILS	–	+	–	–
OGRN	–	–	+	+
OGRNIP	–	–	–	–

4. Specify the required values for the parameters described in the table below.

Name	Description
Signature algorithm	Select the signature algorithm type from the drop-down list
Identification type	Select the identification type from the drop-down list: • 0 — applicant's identification was performed in their presence; • 1 — applicant's identification was performed without their presence using the qualified digital signature with a valid certificate; • 2 — applicant's identification was performed without their presence using information technology; • 3 — applicant's identification was performed without their presence using information technology by providing information from the united identification and authentication system
Common name	Specify the Server domain name or the organization name that the Server belongs to. In case of specifying the name of the organization, it is necessary to specify the Server name in the **Alternative name** table (see below)
Last name, first name	Specify the last and the first name of the person who creates the request
Country	Select the country where the certificate will be valid in from the drop-down list
Region **Locality** **Street, building**	Specify the address where the subject creating a request resides at
Organization	Specify the organization name
Department	Specify the department to which the subject who creates the request belongs to

Name	Description
Title	Specify the title of the subject who creates the request
Email	Specify the email address of the subject who creates the request
INN, INNLE, OGRN, OGRNIP, SNILS	Specify the respective information
Alternative name	To type the Server name: **1.** Click **Add**. **2.** In the **Add alternative name** section, select the **Alternative name** type. **3.** Specify the **Alternative name** value and click **Apply**. To edit or delete the alternative name, use the **Edit** and **Delete** buttons

Note.
- In case of specifying the Server domain name, to receive a wildcard certificate, enter the Server name using the * sign instead of the host name. For example, **<domain name>.ru** or a part of the whole domain name.
- When specifying the Server name, it is allowed to use only lower case letters (a – z), numbers and the **. – *** signs.

4. Click **Save**.

   In the list of the Server certificates, the created request appears.
5. Select the required request line and click **Export**.

   The dialog box prompting you to save the file appears.
6. Save the request file and send it to the Certification Authority.

Upload certificates

Attention! When the number of the uploaded CA certificates exceeds the threshold value, sending the CA certificates to the DN (Distinguished Name) client is disabled automatically (see p. 33).

To upload a certificate using the remote management tools:

1. In the **Menu**, go to **Certificates** and select the respective certificate category.

   Note. To upload CA certificates used for update file verification, you can perform the same procedure by choosing **Certificates | Certification Authority | Import**.
2. On the toolbar, click **Import**.

   The dialog box prompting you to select a file appears.
3. Specify the certificate file and click **Open**.

   The specified certificate appears in the list of the uploaded certificates.

   Note. After uploading, the Server certificate will be displayed in the respective request line. The certificate type will be displayed as unlinked.

To upload certificates using the local menu:

1. Insert a USB drive with a certificate.
2. In the local menu, select **Certificates** and press **<Enter>**.

   The **Certificates** menu appears.
3. Select the required certificate category and press **<Enter>**.

   The **Certificates** menu appears.
4. Select **Certificate import** and press **<Enter>**.

   The list of certificates found in the drive root directory appears.
5. Select the required certificate and press **<Enter>**.

   The certificate uploading and installation start on the Server. The operation finishes with the respective message.

   Note. When processing **PKCS7** containers with root certificates, the container contents are analyzed. Only root certificates are available to be uploaded, the others are discarded.

   If a certificate cannot be uploaded for some reason, the respective short description is provided.
6. Press **<Enter>**.

Delete and disable revoked certificates

Deletion of the revoked certificates list is performed only for CRL download addresses added manually.

It is not allowed to delete a CRL list based on the information contained in the certificates. This list can be disabled only.

To delete a CRL added manually:

1. In the **Menu**, go to **TLS/CRL management | CRL**.
2. In the **CDP** list, select an address added manually and click **Delete**.
   The dialog box prompting you to confirm deletion appears.
3. Click **Yes**.
   The download address will be deleted from the list.

To disable a CRL:

1. In the **CRL distribution points**, select **CDP address** and click **Edit**.
   The **Edit CRL download address** dialog box appears.
2. In the **Update frequency** line, select **Off** value and click **Save**.
   In the **CRL distribution points** list, the respective value of **Update frequency** appears.

To disable CRL check when working with resources:

1. In the **Menu**, go to **Resources** and select the required resource (**HTTPS Proxy**, **TLS Tunnel** or **Application Portal**).
2. In the **HTTPS Proxy**, take the following steps:
   - select the required rule and click **Edit** on the toolbar;
   - in the **Edit proxy** menu, select **Check CRL**;
   - on the toolbar, click **Save**.
3. In the **Tunnel parameters**, perform the following steps:
   - select **Check CRL**;
   - on the toolbar, click **Save**.
4. In the **Application Portal connection** settings, perform the following steps:
   - in the **Certificate-based authentication** menu, click **Configure**;
   - in the **Certificate-based authentication** menu, select **Check CRL**;
   - on the toolbar, click **Save**.

   The certificate CRL check configuration will be changed.

User certificate verification

A certificate that has errors during the user authentication can be checked using the user certificate verification on the Server.

To check the certificate:

1. In the **Menu**, go to **Resources**.
2. Select the resource type that has errors during the connection.
3. On the toolbar, click **Verify user certificate**.
   The dialog box prompting you to select a file appears.
4. Specify the user certificate file and click **Open**.
   A report containing information about the certificate check appears.

Delete certificates

To delete a certificate using the remote management tools:

1. In the **Menu**, go to **Certificates** and select the respective certificate category.
2. Select the required certificate and click **Delete** on the toolbar.

3. In the dialog box, click **OK**.

Note. The buttons **Delete expired certificates** and **Delete all** are available when deleting administrator certificates.

To delete all root and intermediate certificates using the local menu:

1. In the local menu, select **Certificates** and press **<Enter>**.
   The **Certificates** menu appears.
2. Select **CA certificates** and press **<Enter>**.
   The **Certificates** menu appears.
3. Select **Remove all CA certificates** or **Remove all Expired CA certificates** and press **<Enter>**.
   The dialog box prompting you to confirm the removal appears.
4. Select **Yes** and press **<Enter>**.
   All root and intermediate certificates either valid or expired will be deleted.

Chapter 6
Configuring resources

HTTPS proxy configuration

You must set the translation rules of external Server addresses to the internal addresses of a protected corporate network resources to configure HTTPS proxy.

The protected web server must not redirect users to other resources of the corporate network. If absolute addressing is used on the web server, the automatic replacement of the URI or URL sent to the Client in response to the request must be configured.

When configuring the proxy, the external address of the Server is defined by the Server certificate. The external address is taken from the **Server Name** field specified when creating the request for obtaining the Server certificate (see p. 55).

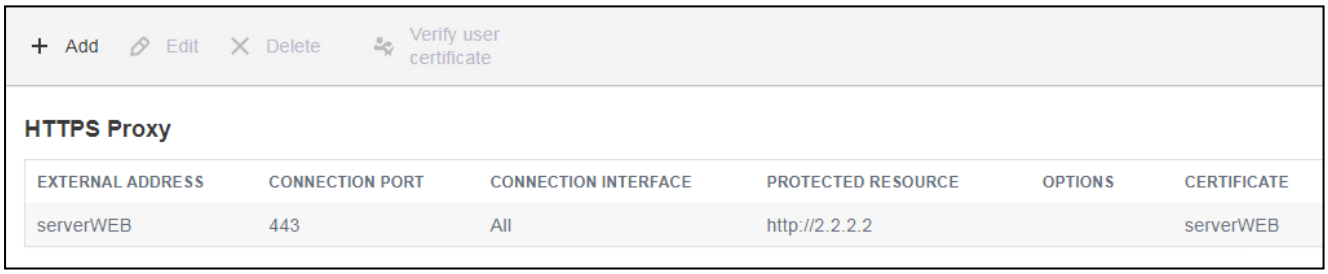
HTTPS proxy configuration is performed only via the remote management tools.

Attention! Before configuring HTTPS proxy, add the required license (see p. 39).

To add a proxy:

1. In the **Menu**, go to **Resources | HTTPS proxy**.

   The list of HTTPS proxies created by the administrator appears as in the figure below.



2. To add a new proxy, click **Add**.

   The **Add proxy** menu appears.

3. Specify the following parameters from the table below.

Parameter	Description
General tab	
Certificate (required field)	Click **+**, select the required certificate in the drop-down list and click **Select**
External address (required field)	The field is filled in automatically when the certificate is selected. The field cannot be edited. If the selected certificate is a wildcard certificate, the field consists of two parts. The domain name specified in the certificate signing request is entered automatically in the right part of the field. Enter the missing subdomain name or the missing part of the fully qualified domain name in the left part
Connection port	Port number used for establishing a secure connection on the Server side. Default value — **443**
Interface	It allows you to select the preferred network interface. Default value — **All**
Protected resource (required field)	The protocol, domain name, IP address and port of the protected corporate network. Default protocol value — **http**. The Server supports adding several protected resources located behind a single HTTPS proxy. To add additional protected resources, click **+**. Incoming connections are distributed among the added protected resources. Maximum value — **16**

Parameter	Description
Require authentication	It is necessary to present a trusted certificate to use proxy if the option is enabled. If the option is disabled, authorization is performed on the web server. Default value — **ON**
Filter encryption algorithms	It forbids connection if the certificates are issued in accordance with GOSTs of different years. Default value — **ON**
Enable RSA ciphersuites	If necessary, select the check box to enable RSA ciphersuites. Default value — **OFF**
Check CRL	If it is necessary to check revoked user certificates, select the check box. If a CRL is missing for the user certificate, the certificate is considered to be unqualified. Default value — **ON**
Use GOST 89 algorithm	If necessary, select the check box to enable the GOST 89 encryption algorithm support. Default value — **ON**
Correct HTTP redirections	The HTTP redirection addresses in the response of the protected web server are replaced with the TLS server address. Default value — **ON**
Proxy UDP	If necessary, select the check box to proxy UDP. Default value — **OFF**
UDP Ports	The UDP ports or a port range which are used to proxy the traffic. It can be configured only if the **UDP port** check box is selected
Advanced connection settings	
Send timeout	If the time limit is exceeded, the Server terminates the connection and the error is saved to the system log. Default value — **120** (seconds)
Read timeout	If the time limit is exceeded, the Server terminates the connection and the error is saved to the system log. Default value — **120** (seconds)
Buffer size for reading request header	Buffer size for reading a Client request header. If the request and its header exceed the buffer size, the **Buffer size for reading large request header** parameter is configured. Default value — **1** (KB)
Buffer size for reading the response	Buffer size for reading the response headers. To specify the parameter, select the required value in the drop-down list. Default value — **32** (KB)
Buffer size for reading large request header	Buffer size for reading a large Client request header. A request must not exceed the buffer size or the 414 (**Request-URI Too Large**) error is returned to the Client. A request header must not exceed the buffer size or the 400 (**Bad Request**) error is returned to the Client. Default value — **8** (KB)
Request body type	The size of the buffer in which a Client request body is stored. If the value is exceeded, the 413 (**Request Entity Too Large**) error is returned to the Client. Default value — **1** (MB)
Connection timeout	The maximum allowed time for establishing connection to the protected resource. If the value is exceeded, the Server terminates the connection and the error is saved to the system log. Default value — **75** (seconds)
Inactive connection timeout	The maximum allowed time for an inactive connection. If the time limit is exceeded, the Server terminates the connection. Default value — **75** (seconds)
Event registration	

Parameter	Description
Register connection events	Select the event registration option for the connection: • **Off** — events are not saved to the logs; • **Errors only** — only events related to errors are saved to the logs. • **Errors and connections** — events related to errors and connections are saved to the logs • **All** — all events are saved to the logs. Default value — **OFF**
Start page	
Use start page	Selection of the user start page in HTTPS proxy mode. If necessary, upload the zip-archive of the start page or specify its address in the **Start page address** field. Default value — **OFF**
Connection processing tab	
Use NTLM authentication	Select the check box if the protected web server uses NTLM authentication of the Clients. Default value — **OFF**
Allow NTLMv1	If necessary, select the check box to use the **NTLMv1**. Default value — **OFF**
Change Host header	Select the check box to replace the Host header with the IP address of the protected Server (otherwise, it contains the TLS Server IP address). Default value — **OFF**
Autocorrection list	Template-based replacement list for responses from the protected web server. If the template text is found in the Server response, it is replaced with the respective text
Use WebSocket proxy	If necessary, select the check box to enable WebSocket proxying. Default value — **OFF**
URIs resources	The list of the URI resources for which WebSocket proxy is used. It can be configured only if the **WebSocket proxy** check box is selected
Data transfer tab	
Transfer data in HHTP headers	Transferring data in the certificates of authorized users. Default value — **OFF**
Delimiter	The selection of the delimiter between additional data in the HHTP headers. Default value — **Space**. It can be configured only if the **Transfer data in HHTP headers** check box is selected
HHTP headers	The HHTP header, transferred data and its sources are specified. It can be configured only if the **Transfer data** in **HHTP headers** check box is selected
Access control tab	
Enable access control	Select the check box if it is necessary to enable and configure access control to the resource based on the certificate parameters. If the parameter is enabled, user access to the resources is granted based on the parameters specified in the **Access control parameters** table (see below). Default value — **OFF**
Enable access control by certificates	Select the checkbox to enable and configure access to the resource based on the root certificates. If the parameter is enabled, user access to the resources is granted only to users who use the root certificates specified in the **Certificate** field (see below). Default value — **OFF**
Certificate	Click **+** to open the window to specify the root certificates to be used to connect to the resources. Otherwise, the connection is reset. It can be configured only if the **Enable access control by certificates** check box is selected

Parameter	Description
Access control parameters	Certificate parameter and its value are specified. The created access control parameter is added to the list. It can be configured only if the **Enable access control** check box is selected. To configure the list of access control parameters, the following is availale: • add, delete and edit access parameters; • import the list of access control parameters from the TXT-file; • export the list of access control parameters; • clear the list of access control parameters; For more information about managing access control parameters, see p. 63

4. Click **Save**.

   The created proxy is added to the list.

To view and edit HTTPS proxy:

1. In the **HTTPS Proxy** menu, select the required proxy and click **Edit** on the toolbar.

   The **Edit proxy** menu appears.
2. Specify the required parameters (see in the table above) and click **Save**.

To delete a proxy:

1. In the **HTTPS Proxy** menu, select the required proxy and click **Delete** on the toolbar.
2. Click **Continue** in the confirmation dialog box.

   The selected proxy is deleted.

HTTP header configuration

To add a HTTP header:

Attention! The **Transfer data in HTTP headers** check box must be selected.

1. Go to the **Data transfer** section and select **Transfer data in HTTP headers**.
2. In the **HTTP headers** section, click **Add**.

   The **Add HTTP** section appears.
3. Specify the header name and select the data source in the **Data source** drop-down list.
4. Enter the data you want to transfer (if a certificate is used as the source of the transferred data, select the required data in the **Data** drop-down list).

   Note.
   - The unique certificate number can contain the leading zeros. To transfer data in this format, use the value specified in the **Unique certificate number (raw)** field.
   - To transfer INNLE and OGRNIP, specify the respective OID values: OID INNLE — 1.2.643.100.4 OID OGRNIP — 1.2.643.100.5.
5. Click **Apply**.

   The created header is added to the **HTTP headers** table. If there are two headers with the same name, their values are combined into one header and the delimiter is inserted between them.

To edit/delete a HTTP header:

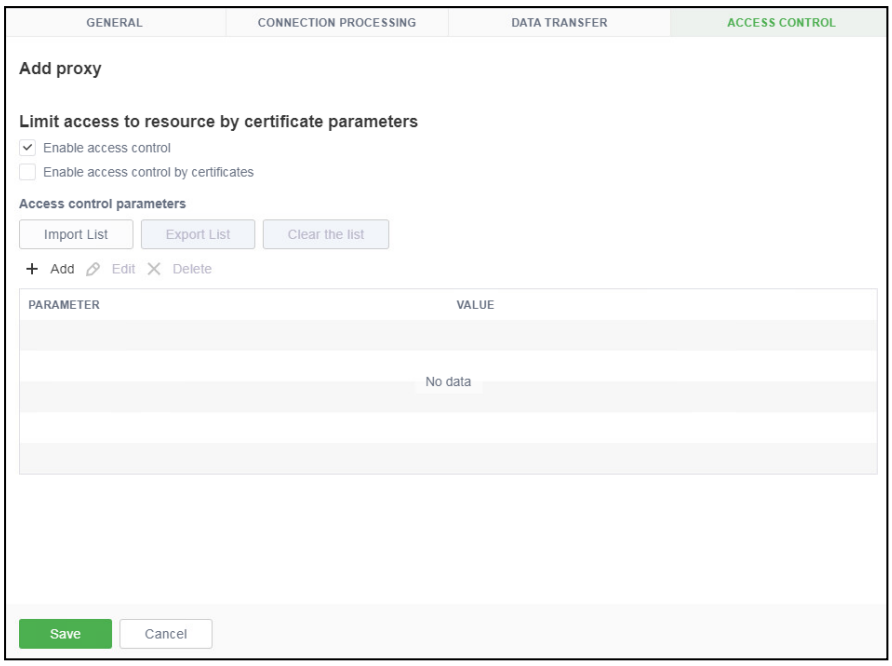
1. Go to the **Data transfer** section, select the required header and click the respective button.
2. If necessary, change the order of the headers using the **Down** and **Up** buttons.
3. When the required changes are made, click **Save**.

Access control by certificate parameters configuration

To add a new access control parameter:

Attention! The **Enable access control** check box must be selected.

1. Go to the **Access control** section and click **Add**.



The **Add access parameter** section appears.

2. Select the required certificate from the **Parameter** drop-down list.
3. In the **Value** field, specify the value of the required parameter on the basis of which the access to the resource is granted.
4. Click **Apply**.

   The created access parameter is added to the list.

Note. If there are several access parameters, the logical operator **OR** is used.

To edit access control parameters:

1. In the **Access control** section, select the required parameter in the list and click **Edit**.

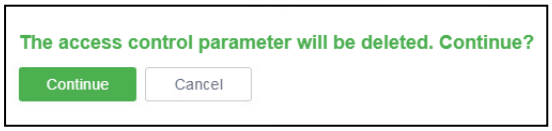
   The **Edit access parameter** menu appears.
2. In the **Parameter** drop-down list, select the required certificate parameter.
3. In the **Value** text box, specify the required parameter value on which basis the access to the resource will be granted.
4. Click **Apply**.

   The **Edit access parameter** menu closes. The edited access control parameter appears in the list with new configuration.

To delete access control parameters:

1. In the **Access control** section, select the required parameter and click **Delete**.

   The dialog box prompting you to confirm the operation appears.



2. Click **Continue**.

   The respective parameter will be deleted.

Import the list of access control parameters

When importing the list of access control parameters, the existing list of parameters will be overwritten by the imported one.

To import the list of access control parameters, create a **TXT** file containing certificate parameters and their values on which basis the access to the resource will be granted (see p. **92**).

To import the list of access control parameters:

1. In **Access control** section, click **Import list**.
   The standard dialog box prompting you to select a file appears.
2. Select the required **TXT** file and click **Open**.
   The list of parameters and their values specified in the **TXT** file appears.

Export the list of access control parameters

The procedure is performed in the **Access control** section using the **Export list** command. The list is saved in the form of a file named **proxy_X_ADDRESS.txt** where **X** — a resource serial number, **ADDRESS** — an external resource address.

If necessary, the exported **TXT** file can be used for importing the list of access control parameters on other HTTPS proxy resources.

Clear the list of access control parameters

The procedure allows deleting all access control parameters for a specific resource.

To clear the list of access control parameters:

1. In the **Access control** section, click **Clear the list**.
   The dialog box prompting you to confirm the operation appears.
2. Click **Continue**.
   All access control parameters will be deleted.

TLS Tunnel settings

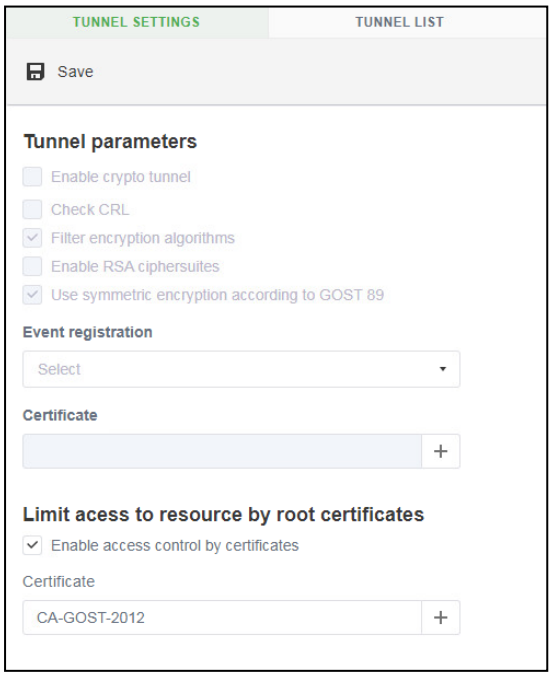
You must specify the Server certificate and the tunnel parameters for each protected network resource to configure the TLS tunnel.

The TLS tunnel configuration is performed only via the remote management tools.

Attention! Before the TLS tunnel configuration, add the required license (see p. 39).

For general tunneling settings:

1. In the **Menu**, go to **Resources | TLS tunnel**.
   The **Tunnel settings** menu with the tunnel parameters appears.



2. In the **Certificate** section, click **+**.
3. In the opened section, select the required certificate and click **Select**.

4. On the toolbar, click **Save**.
5. Specify parameters described in the table below.

Parameter	Description
Enable crypto tunnel	If the check box is selected, the TLS tunnel mode is enabled. Otherwise, the TLS tunnel mode is disabled. Default value — **OFF**
Check CRL	Select the check box if it is necessary to verify the user certificates against a CRL. If the CRL is missing for the user certificate, the certificate is considered to be unqualified. Default value — **OFF**
Filter encryption algorithms	It forbids connection if the certificates are issued in accordance with the GOSTs of different years. Default value — **ON**
Enable RSA ciphersuites	If necessary, select a check box to enable RSA ciphersuites. Default value — **OFF**
Use symmetric encryption according to GOST 89	If necessary, select the check box to use symmetric encryption according to GOST 89. Default value — **ON**
Event registration	Event registration configuration In the **Event registration** drop-down list, select the required parameters: • Register events in the system log; • Save logs to a file to save logs to **stunnel.log** file on the Server hard drive
Enable access control by certificates	Select the checkbox to enable and configure access to the resource based on the root certificates. If the parameter is enabled, user access to the resources is granted only to users who use the root certificates specified in the **Certificate** field (see below). Default value — **OFF**
Certificate	Click **+** to open the window to specify the root certificates to be used to connect to the resources. Otherwise, the connection is reset. It can be configured only if the **Enable access control by certificates** check box is selected

6. On the toolbar, click **Save**.

To create a tunnel and configure its parameters:

Attention! To create and configure a tunnel, unlock the Server (see p. 26) and add the respective license (see p. 39).

1. In the **Tunnel settings**, go to the **Tunnel list**.

   Note. If the configuration is performed for the first time, the list is empty.

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

   The **Add tunnel** section appears.

3. Specify parameters described in the table below.

Parameter	Description
General	
Anonymous connection	Default value — **OFF**
Tunnel name (required field)	The name of the TLS tunnel
Protected resource address (required field)	The address of a protected resource with which a secure connection will be established
Protected resource port (required field)	The number of the port used for establishing a secure connection on the resource side. Default value — **80**
Local port (required field)	The port number used for establishing a connection on the Server side

Parameter	Description
Connection timeout	If the specified value is exceeded when establishing a connection to the protected resource, the connection is terminated and the error is saved to the system log. Default value — **120** (seconds)
Interface	It allows you to select the preferred network interface. Default value — **All**
Access control	
Check LDAP groups	Certificate-based check (see p. **27**)
Groups that have access to resource	The groups of LDAP users which can use the tunnel. It can be configured only if the **Check LDAP groups** check box is selected

4. On the toolbar, click **Save**.

   The tunnel is added to the list.

To edit/delete a tunnel:

- Select the required tunnel, click the respective button on the toolbar.

  If you edit a tunnel, the **Tunnel configuration** section appears on the screen. If you delete a tunnel, a confirmation dialog box appears.

Application Portal configuration

The Application Portal (hereinafter — the Portal) provides a single entry point to web resources or applications (including external ones). After authentication, a user is directed to the Portal page containing the list of resources that they can access. Web resources are usually designed to work with the Client directly and their URIs are considered to be from the root domain of the resource.

There are the following methods to resolve a URI conflict.

The direct change of a URI in the Server traffic
The Server adds an additional prefix to the URIs of web resources when the Portal is running. The Server processes the traffic to the resource and performs an automatic or forced replacement of all URIs with the URIs containing an additional prefix and vice versa
Using sections
If the resource pages (or its section) look like **http://www.a.ru/path1/...**, it is possible to mount the path1 of the protected resource to the path1 on the Server. For example, **https://www.portal.ru/path1/1.html** is broadcast as **http://www.a.ru/path1/1.html**. In this case, an additional prefix is not added to the URI of the web resources

The algorithm for the Portal configuration is the following:

- Connection to the Portal configuration (see below).
- Portal applications creation (see p. **70**).
- Portal sections configuration (see p. **70**).
- Portal logon page configuration for each application (see p. **70**).
- Creation of the Portal users (if necessary, see p. **70**).
- Portal appearance(if necessary, see p. **70**).

Portal configuration is performed using the remote management tools only.

Configuring Application Portal parameters

To start working in Portal mode, you must configure its parameters.

User authentication

User authentication is an important parameter. It can be performed using a login and a password or using a certificate.

If a user is authenticated using a login and a password, the option of two-factor authentication via the **auth.as** service is available. In this case, a user must enter a one-time password in addition to a login and a password.

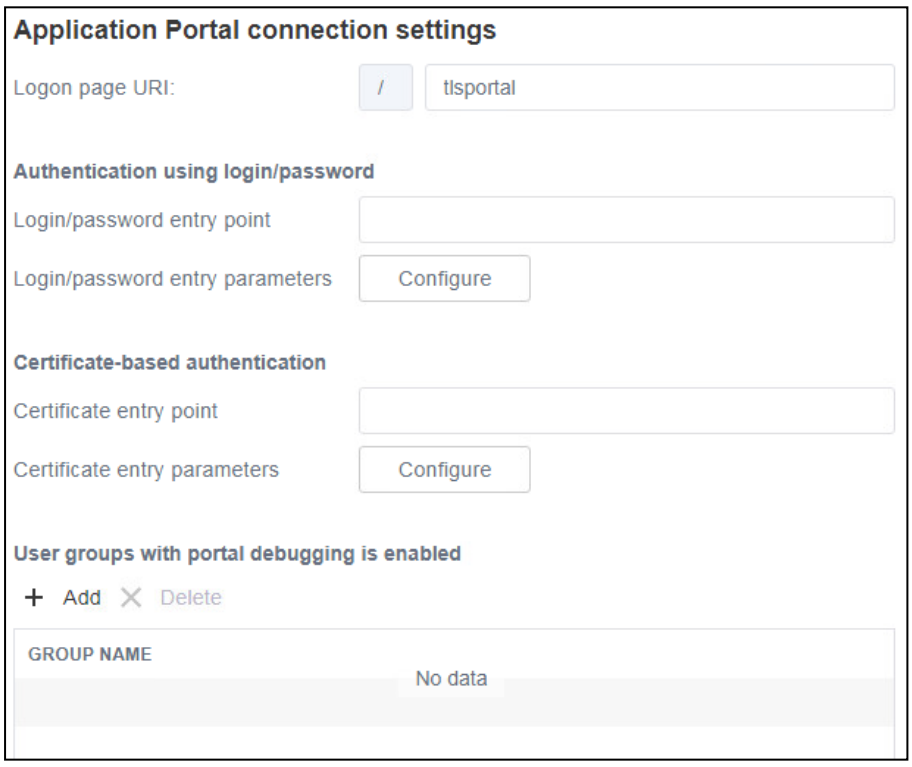
The one-time password is generated automatically and is sent to the user device. Its usage time is limited.

Application Portal connection settings

Attention! It is necessary to use the URL addresses with HTTPS to connect to the Portal.

To configure the general connection settings:

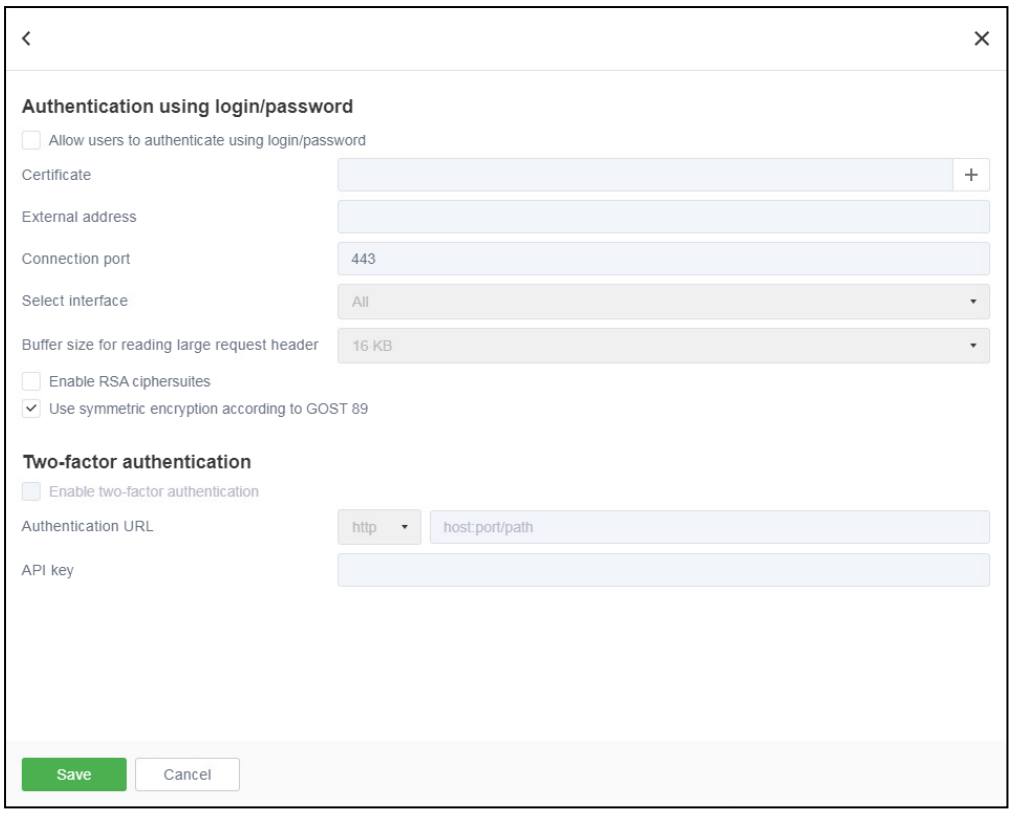
1. In the **Menu**, go to **Resources | Application Portal**.
   The **Application Portal connection settings** menu appears.



2. Specify the relative URI of the logon page in the respective field.
3. Specify the required parameter in the **Login/password entry point** or **Certificate entry point** fields depending on the type of authentication you need and click **Configure**.
4. In the opened section, specify the required authentication parameters and click **Save**.
5. To provide the group of users with debugging information while working with the Portal, in the **User groups with portal debugging enabled** section, click **Add**. Select a group from the list of LDAP groups created by the administrator.
6. On the toolbar, click **Save**.
   The parameter configuration will be saved.

To configure Authentication using a login and a password:

1. In the **Application Portal connection settings** menu, click **Configure**.
   The **Authentication using login/password** menu appears.



2. Select **Allow users to authenticate using login/password**.
3. Click **+** and specify the entry point certificate.
4. Select the required certificate and click **Select**.
   The section closes and the external address is filled in the respective field.
5. Specify the connection port in the respective field (by default — **443**).
6. Select the interface in the respective field (by default — **All**).
7. In the drop-down list, select the buffer size for reading large request headers.
8. If necessary, enable **RSA ciphersuites**.
9. If necessary, enable **USe symmetric encryption according to GOST 89**.
10. If necessary, select **Enable two-factor authentication**.
11. Specify the **Authentication URL** and the **API key** in the respective fields.
12. Click **Save**.
    The parameters are configured and you are returned to the **Connection** section.

Authentication by certificate:

1. Click **Configure** in the **Certificate-based authentication** section.
   In the opened section, specify the required parameters.
2. Select **Allow users to authenticate using certificate**.
3. Click **+** and specify the entry point certificate.
4. Select the required certificate and click **Select**.
   The section closes and the external address is filled in the respective field.
5. Specify the connection port in the respective field (by default — **443**).
6. Select the interface in the respective field (by default — **All**).
7. Select the buffer size for reading large request header in the drop-down list.
8. If necessary, enable **RSA ciphersuites**.
9. If necessary, enable **Use symmetric encryption according to GOST 89**.
10. Select **Check CRL** if it is necessary to verify the user certificates against a CRL.
11. If necessary, select **Add a connection port to the certificate authorization link** (enabled by default).

12. If necessary, enable a certificate- based acess control by selecting the **Enable access control by certificates** check box.

    If the parameter is enabled, user access to the resources is granted only to users who use the root certificates specified in the **Certificate** field (see below).

13. If necessary and if the **Enable acess control by certificates** check box is selected, in the **Certificate** field, click **+** and specify the root certificates to be used to provide access control.

14. Click **Select**.

    The specified certificates will appear in the **Certificate** field.

15. Click **Save**.

    The settings are configured and you are returned to the **Connection** section.

To configure the Portal appearance:

1. Go to the **Appearance** section.

   The current **Portal appearance parameters** appear. The parameters in the table below are available for configuration.

Logon page appearance	Resource list page appearance
• Background image; • header; • logon using login/password button; • link for certificate-based logon	• Header; • resource area; • resource view - its tile with the resource name and description

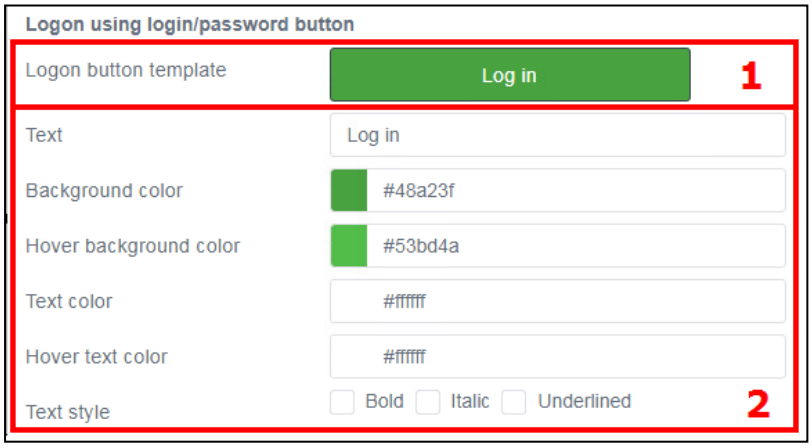
Note. A tile template is a rectangular area displayed on the Portal page representing a resource/application. When you click it, the resource/application is launched.

2. To change the background image, click **Change**.

   In the dialog box, select the required file and click **Open**.

   The thumbnail image of the background picture is changed according to the loaded file.

3. Specify other parameters (2) and view the changes of the parameters in the respective field of the corresponding template (1) in real time as in the figure below.



4. Click **Save** on the toolbar.

Portal application configuration

To create a Portal application:

1. In the **Menu**, go to **Resources | Application Portal**.
2. Go to **Applications**.

   The list of portal applications specified by the administrator appears.

Note. If the configuration is performed for the first time, the list of applications is empty.

3. To add a new application to the list, click **Add**.
4. In the **Add application** section, specify parameters described in the table below.

Parameter	Description
General tab	
Protected resource (required field)	The data transfer protocol, address and port of a protected resource. Default protocol value — **http**
Proxy UDP	If necessary, select the check box to enable a UDP proxy. Default value — **OFF**
UDP ports	The UDP ports or a port range that are used to proxy the traffic. It can be configured only if the **Proxy UDP** check box is selected
Allow authentication access	The selection of the authentication type to access the resource. Default value — **By login/password and certificate**
Protected resource type	The selection of the protected resource type. Default value — **Others**
Show the Portal menu on the pages	The option to show the Portal menu on the resource pages. Default value — **ON**
Advanced connection settings	
Send timeout	The time available for transferring the user request to the protected resource. Default value — **120** (seconds). If the time limit is exceeded, the Server stops the session and registers the error in the system log
Read timeout	The time available for waiting for the response from a protected Server. Default value — **120** (seconds). If the time limit is exceeded, the Server stops the session and registers the error in the system log
Request body type	The size of the buffer in which a Client request body is stored. If the value is exceeded, a Client receives the **Error 413** message (**Request Entity Too Large**). Default value — **1** MB
Connection timeout	The maximum allowed time for establishing connection to the protected resource. Default value — **75** (seconds)
Keepalive timeout	The maximum allowed time of the inactive connection. If the time limit is exceeded, the connection is terminated by the Server. Default value — **75** (seconds)
Access control	
Groups that have access to resource	The list of LDP groups that have access to the resource
Connection processing tab	
Store cookies on TLS server	If necessary, select the check box to store the cookies on a TLS server. Default value — **OFF**
Allow NTLMv1	If necessary, select the check box to use NTLMv1. Default value — **OFF**
Change Host header	The option to change a Host header in the requests to the protected server. Default value — **ON**
Delete domain from cookie	If you do not need a domain from cookie, select the check box. Default value — **OFF**
Autocorrection list	The list of the automatically corrected content in the responses of the protected resource
Use WebSocket proxy	If necessary, select the check box to enable a WebSocket proxy. Default value — **OFF**
URIs resources	The list of the URI resources for which a WebSocket proxy is used. It can be configured only if the **Use WebSocket proxy** check box is selected
Data transfer tab	
Transfer data in HHTP headers	The transferring of the data concerning authorized certificates in the HTTP headers. Default value — **OFF**

Parameter	Description
Delimiter	The selection of the delimiter between additional data in the HTTP headers. Default value — **Space**. It can be configured only if the **Transfer data in HHTP headers** check box is selected
HHTP headers	The list of additional data in the HHTP headers. A header name, transferred data and its sources are specified. It can be configured only if the **Transfer data in HHTP headers** check box is selected
SSO tab	
Use logon data for SSO	Use the logon data used for authentication in the Portal for the authentication on the Server. Default value — **OFF**
Authentication type	The selection of the authentication type from the available ones on the resource. Default value — **None** The following parameters are available: • HTTPS Basic authentication — by login or password. A user login and password is transferred in the **Authorization** header in the unencoded format (base64-encoded). It is relatively secure when HTTPS is used. • NTLM pass-through authentication — NTLM authentication in which SSO is not used. • NTLM authentication

5. Click **Save**.

   A new data row is added to the **Portal applications** section.

To view and edit the Portal:

1. In **Applications**, select the required data row in the list of portal applications formed by the administrator.
2. On the toolbar, click **Edit**.

   The **Edit application** menu appears.
3. Specify the required parameters (see in the table above) and click **Save**.

To delete the Portal:

1. In the **Portal applications** menu, select the required portal.
2. On the toolbar, click **Delete**.

Additional Portal settings

To configure the Portal sections:

Note. The Portal sections are part of the URI that are transferred directly from the Portal to an application without any prefix.

1. In the **Menu**, go to **Resources | Application Portal**.
2. Go to **Sections**.

   The **Portal** menu specified by the administrator appears.

   Note. If the configuration is performed for the first time, the list is empty.
3. To add a new section, click **Add** on the toolbar.

   The **Add** section appears.
4. Specify the path and select the application from the list created by the administrator in the respective fields.
5. If necessary, select **Automatic response processing from protected resource**.
6. Click **Save**.

   A new data row is added to the **Portal sections** table.

To configure the Portal home page:

Note. Home page configuration is used to define the list of applications that a user sees when logging in to the Portal.

1. Go to the **User applications** section.

   The list of the home page applications specified by the administrator appears.

   Note. If the configuration is performed for the first time, the list is empty.

2. To add a new section, click **Add** on the toolbar.

   The **Add user application** menu appears.

3. Specify the resource logon page and its view in the Portal or select the resource address from the **Application** drop-down list.

   Note. The logon page address is a link (URL or URI).

   If the resource is a tunneled application, the logon page address must have the following format: **conttls://encoded_string_BASE64**. A string contains the following data:

   - protected resource address and its port;
   - launching applications with parameters that can be specified by the **%host% and %port%** variables.

   The string has the following format:

   ```
   address:port/application[parameters]
   ```

   The string must be encoded in UTF-16 LE (Windows) before encoding in BASE64.

   The example of the resource logon page for launching a tunneled application:

   ```
   conttls://dABlAHMAdAAtAHQAdQBuADIALgBzAGUAYwB1AHIAaQB0AHkAYwBvAGQAZQAuAHIAdQA6ADM
   AMwA4ADkALwBtAHMAdABzAGMALgBlAHgAZQAgAC8AdgA6ACUAaABvAHMAdAAlADoAJQBwAG8AcgB0ACUA
   ```

   where the string is the following:

   ```
   test-tun2.securitycode.ru:3389/mstsc.exe /v:%host%:%port%
   ```

   Note. TLS tunnel between the Server and a Client is created while working with an external application via the Portal. The Server launches the application and provides data exchange through the tunnel.

4. To change the resource icon, click **Change**.
5. In the file selection dialog box, select the required icon file.
6. To restore a standard resource icon, click **Default**.
7. Specify the header and its short description in the respective fields.
8. Click **Save**.

   A new data row is added to the **Users applications** table.

To add new Portal users:

Note. It is not necessary to create new users if LDAP authentication is used.

1. Go to the **Users** section.

   The list of Portal users appears.

   Note. If the configuration is performed for the first time, the list is empty.

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

   The **Add user** section appears.

3. Specify the user credentials and click **Save**.

   A new data row is added to the Add user table.

Attention! To provide the users from the Portal users list with access to the specific Portal application, you need to select **Local TLS server** users option while adding/editing this application in the **Applications** section.

Chapter 7
TSL/CRL management

In this section, you can find out how manage the settings of TLS and CRL files, including their update and the loading of a CRL using a proxy server.

TLS management

On the TLS page, you can download the lists of trusted CA certificates as a TLS file, configure their update frequency, as well as view details about the status of the update of earlier downloaded TLS files.

After downloading, a TLS file is installed in the certificate store. You can download a TLS file on demand or set a schedule for it. If necessary, you can download a TLS file manually using the **Update** button on the toolbar.

The integrity and authenticity of a TLS file are verified by building a chain from the certificate the private key of which was used to sign TLS to the TCA certificate. Therefore, you should download TLS files after you download TCA certificates used to verify TLS.

To perform any operation related to the downloading of TLS files, you should use the remote management tools.

To add an address for downloading TLS files:

Note. When downloading TLS files, CDPs will be imported for root certificates included in these TLS files.

1. In the Server management menu, select **TLS/CRL Management**, then select **TLS**.
   A list of addresses from which TLS files were downloaded appears.
2. On the toolbar, click **Add**.
   A dialog box prompting you to add an address appears.
3. Specify the TLS address and select the update frequency from the drop-down list.

   Note. The default value for the update frequency is set on the **TLS/CRL management** page.
4. Click **Save**.
   The URL will be added to the list. After the check, files downloaded from this URL will be installed in the storage.

To download a TLS file:

Note. When downloading TLS files, CDPs will be imported for root certificates included in these TLS files.

1. In the **TLS download addresses** menu, click **Import** on the toolbar.
   A dialog box to add a file appears.
2. Specify the path to the TLS file and click **Open**.
   The file will be downloaded to the Server. After the check, certificates from the file will be installed in the storage.

To edit a TLS download address:

1. In the **TLS download addresses** menu, select the required address and click **Edit** on the toolbar.
   A dialog box with parameters to edit an address appears.
2. Change the required parameters and click **Save**.

To delete a TLS download address:

1. In the **TLS download addresses** menu, select the required address and click **Delete** on the toolbar.
   A dialog box prompting you to confirm the operation appears.
2. Click **Delete**.
   The changes will be applied. An updated list of addresses will appear.

CRL management

You can download and update a CRL:

- manually;
- automatically by addresses specified by the administrator;
- by addresses received from the CDP of CA certificates.

To perform any operation related to the download and update of a CRL, you should use the Server web management.

To configure the automatic CRL loading:

1. In the Server management menu, select **TLS/CRL management**, then select **CRL**.
   A tab with the list of CDP files appear.
2. Select the **CRL download addresses** tab.
3. On the toolbar, click **Add**.
   The **Add CRL download address** dialog box appears.
4. Enter the URL to download the CRL and set the update frequency.

   Note. The default value for the update frequency is set on the **TLS/CRL Management** page.
5. Click **Save**.
   The CDP will be verified. If it has completed successfully, a new record will appear in the list. To edit the list of download addresses, use the buttons above the list.

In case you need to download the CRL through a proxy server, specify the respective parameters.

To edit a CRL download address:

1. On the **CRL** page, on the CDP list tab, select the required address in the list.
2. On the toolbar, click **Edit**.
   A dialog box allowing you to edit the address parameters appears.
3. Change the required parameters and click **Save**.
   Information about CRL download parameters appears.

To delete a CRL download address:

1. On the **CRL** page, on the **CDP list** tab, select the required address in the list.
2. On the toolbar, click **Delete**.
   A message prompting you to confirm the operation appears.
3. Click **Delete**.
   The changes will be applied. An updated list of addresses will appear.

To download a CRL manually:

1. On the **CRL** page, select the **CRL file list** tab.
2. Click **Import** above the CRL list.
   A standard dialog box to select a file appears.
3. Specify the path to the file and click **Open**.
   The CRL will be downloaded to the Server and added to the list.

   Note.
   - The selected CRL list can be deleted or downloaded to the computer from which you manage the Server. To download the CRL, click the Download the list button on the toolbar. If you want to delete it, click the Delete button.
   - To work with a large CRL list, you can use the respective option on the toolbar to search in the list. The search is performed by the contents of the Issuer parameter.

To delete a CRL file list:

1. On the **CRL** page, on the **CRL file list** tab, select the required address in the list.
2. On the toolbar, click **Delete**.
   A message prompting you to confirm the operation appears.

3. Click **Delete**.

   The changes will be applied. An updated list of files will appear.

To configure the parameters of a proxy server:

1. In the Server management menu, select **TLS/CRL management**, then select **TLS/CRL configuration**.

   The respective page opens.
2. Select the **Proxy connection** check box and specify the parameters of the proxy server.
3. If additional authentication is required, select the **Authentication required** check box and fill in the respective fields.
4. Click **Save**.

Note. You can disable the CRL update, even if the **Authentication required** check box is selected.

TCA certificates management

On the **Trusted Certification Authority** page, you can import, export and delete certificates.

To import a TCA certificate:

1. In the Server management menu, select **TLS/CRL management**, then select **Trusted Certification Authority**.

   The **TCA certificates** dialog box containing a list of certificates appears.
2. On the toolbar, click **Import**.

   A standard dialog box prompting you to select a file appears.
3. Specify the path to the file and click **Open**.

   The certificates appears in the list.

To export a TCA certificate:

- On the **TCA certificates** page, select the required certificate and click **Export**.

  The certificate will be saved to the default folder.

To delete a TCA certificate:

Note. To delete expired or all certificates, click **Delete the expired** or **Delete all** respectively.

- On the **TCA** page, select the required certificate and click **Delete** on the toolbar.

  The certificate will be removed from the list.

Chapter 8
Network settings

You can manage Server network settings using local and remote management tools. Using the **Network management** section, you can manage network settings remotely. The section menu contains the following tabs:

- **Common**;
- **Physical interfaces**;
- **Virtual interfaces**.

General network settings management

The **Common** tab contains information about the current Server network settings and allows you to manage the following parameters:

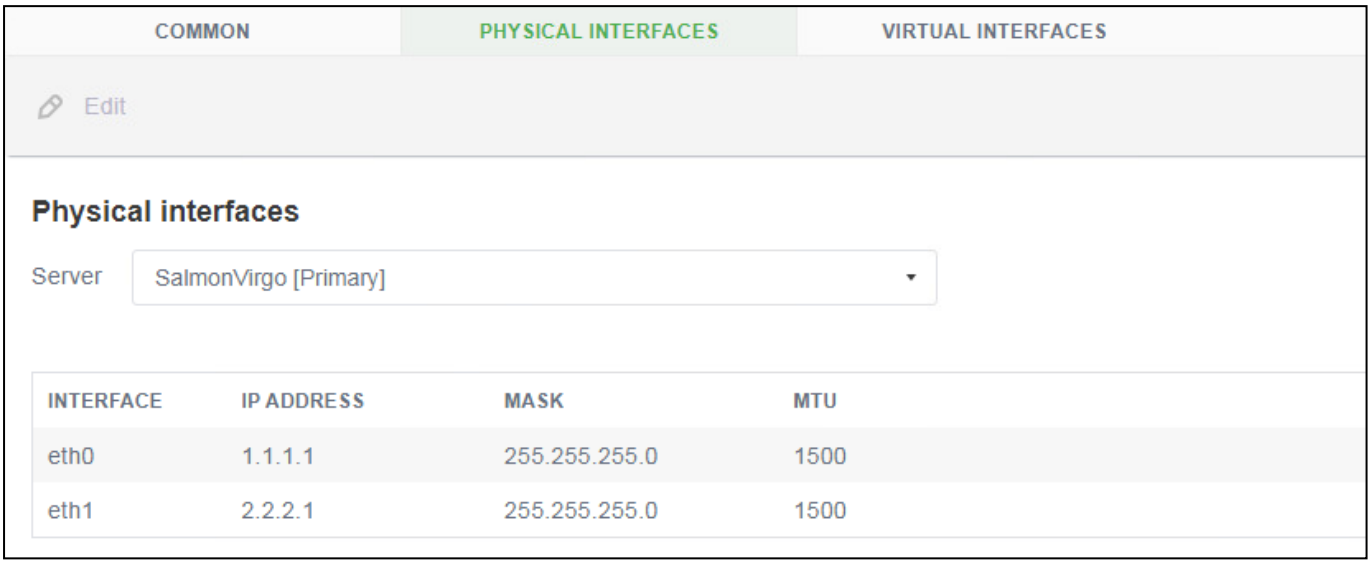
Parameter	Description
Server	A list of Servers to display and change the current parameters
Default gateway	Configuring the IP address of the default gateway
Server name	Configuring the Server name
DNS servers	Configuring the list of DNS servers
Search domains	Configuring the list of search domains (DNS suffixes)
Static routes	Configuring the list of static routes

To configure the network parameters using the remote management tools:

1. In the Server management menu, select **Network management**.
   The **Common** tab menu appears.
2. In the **Server** field, select the Server name from the drop-down list.
3. If necessary, specify the values for the **Default gateway** and **Server name** parameters.
4. If you need to edit the list of DNS servers, use the **Add**, **Edit**, **Delete** buttons:
   - to add a DNS server, click **Add**. In the appeared dialog box, specify the IP address for the required DNS server and click **Save**;
   - to change the IP address of the DNS server, click **Edit**. In the appeared dialog box, change its IP address and click **Save**;
   - to delete a DNS server, select the required one in the list and click **Delete**.
5. If you need to edit the list of search domains, use the **Add**, **Edit**, **Delete** buttons:
   - to add a search domain, click **Add**. In the appeared dialog box, specify the required DNS suffix and click **Save**;
   - to edit a search domain, click **Edit**. In the appeared dialog box, change the DNS suffix and click **Save**;
   - to delete a search domain, select the required DNS suffix and click **Delete**.
6. If you need to edit the list of static routes, use the **Add**, **Edit**, **Delete** buttons:
   - to add a static route, click **Add**. In the appeared dialog box, specify the parameters of the new route and click **Save**;
   - to edit a static route, click **Edit**. In the appeared dialog box, change the parameters of the required route and click **Save**;
   - to delete a static route, select the required one and click **Delete**.
7. To finish the configuration and apply the Server network parameters, click **Save** on the toolbar.
8. To edit the parameters of another Server, repeat steps **2–7**.

Physical interface settings management

The **Physical interfaces** tab in the **Network Management** section contains information about Server physical interfaces and allows you to edit the parameters of the existing physical interfaces.



To edit the parameters of physical interfaces using the remote management tools:

1. In the Server management menu, select **Network Management**.
   The section menu appears.
2. Select the **Physical interfaces** tab.
   A list of Server physical interfaces appears.

   Note. To display physical interfaces of another Server, select the required Server from the drop-down list.
3. Select the required physical interface and click **Edit** on the toolbar.
   The **Configure physical interface** dialog box appears.

4. Change the required parameters of the physical interface.

   Note. You must specify the **Subnet mask** and **MTU** parameters. If the **IP address** field is blank, the interface is only available for using in VLAN.
5. Click **Save**.

Virtual interface settings management

The **Virtual interfaces** tab in the **Network Management** section contains information about the existing virtual interfaces and allows you to edit the list of virtual interfaces.

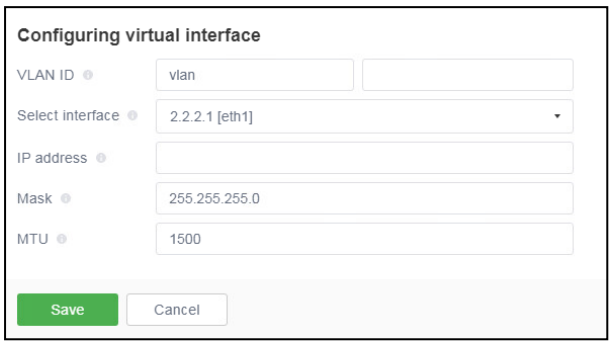
To create a virtual interface remotely:

1. In the Server management menu, select **Network management**.
   The **Common network settings** menu appears.
2. Go to the **Virtual interfaces** section.
   A list of Server virtual interfaces appears.

Note.
- If the configuration has not been performed yet, the list of virtual interfaces will be empty.
- To display virtual interfaces of another Server, select the required Server from the drop-down list.

3. On the toolbar, click **Add**.

   The **Configure virtual interface** dialog box appears.



4. Specify parameters described in the table below.

Parameter	Description
VLAN ID	Virtual interface identifier. Consists of the **vlan** prefix and the ordinal number given by the administrator. Takes the following values: • **2** – **1001**; • **1006** – **4094**
Interface	A drop-down list to select the existing physical interface
IP address	A field to enter the IP address
Subnet mask	A field to enter the subnet mask. Default value is **255.255.255.0**
MTU	A field to enter MTU. Default value is **1500**

5. Click **Save**.

   The **Configuring virtual interface** dialog box closes. The created interface appears in the list of virtual interfaces.

To edit the parameters of the existing virtual interface using the remote management tools:

1. In the **Network management** section, on the **Virtual interfaces** tab, select the required Server from the drop-down list.
2. In the list of virtual interfaces, select the required interface and click **Edit** on the toolbar.

   The **Configuring virtual interface** dialog box appears (see p. **79**).
3. Perform the required changes and click **Save**.

   The **Virtual interface settings** dialog box closes. The interface with the modified parameters appears in the list of Server virtual interfaces.

To delete a virtual interface remotely:

1. In the **Network management** section, on the **Virtual interfaces** tab, select the required Server from the drop-down list.
2. In the list of virtual interfaces, select the required interfaces and click **Delete** in the toolbar.

   The dialog box prompting you to confirm the deletion of the interfaces appears.
3. Click **Yes**.

   The selected interfaces will be deleted from the list of the virtual interfaces of the specified Server.

Chapter 9
Server diagnostics

The diagnostics include viewing Server operation statistics, checking its network interfaces and the network state.

Server operation monitoring

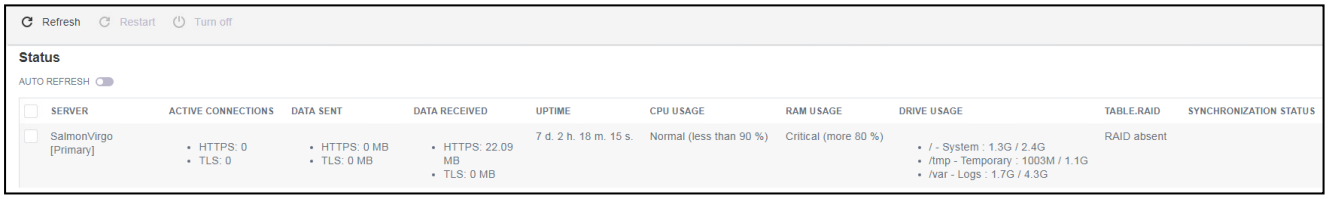
You can view the current state of the established connections of Clients with the HTTPS proxy server and obtain statistics about the Server operation.

You can view the following information about the Server operation using the remote management tools:

- Server name;
- the number of active connections;
- traffic volume;
- uptime;
- estimate of CPU and RAM usage;
- free/dedicated space for hard drive directories.

To view the information using the remote management tools:

- In the Server management menu, select **Status**.



To refresh the information on the page automatically, enable the status switch below the table. To refresh manually, click **Refresh** on the toolbar.

Note. If automatic refreshing is enabled, the **Refresh** button is not active.

To view the information using the local management tools:

1. In the local menu, select **Diagnostics** and press **<Enter>**.
   The **Diagnostics** menu appears.
2. In the **Main menu**, select **Status** and press **<Enter>**.
   An information window with the Server statistics appears.
3. To return to the **Main menu**, press **<Esc>**.

Network diagnostics

Network diagnostics allows you to run and check the execution of the **Ping**, **Traceroute**, **Arp** and **TCPdump** commands. You can run **Tcpdump** using the local management tools only.

To perform network diagnostics using the remote management tools:

1. In the Server management menu, select **Diagnostics**.
   The **Network diagnostics utilities** console appears.
2. Enter the IP address or the name of a remote host.

   Note. This parameter is not mandatory if you use the **Arp** command.
3. On the toolbar, click the button to run the required command.
   The command execution starts. The result of the command appears in the respective field.

To perform network diagnostics using the local management tools:

1. In the local menu, select **Diagnostics** and press **<Enter>**.
   The **Diagnostics** menu appears.

2. Select **Network diagnostics** and press **<Enter>**.

   The **Network diagnostics** menu appears.
3. Select the required command and press **<Enter>**.
4. When running the **Ping** and **Traceroute** commands, enter the IP address and press **<Enter>**.

   Note. This parameter is not mandatory if you use the **Arp** and **Tcpdump** commands.

   The result of the command appears.
5. To return to the **Network diagnostics** menu, press **<Enter>**.

Server network interfaces diagnostics

To perform the diagnostics of network interfaces, prepare the required number of patch cables for port commutation and a switch if necessary.

If the number of network interfaces is even, the number of patch cables is calculated given that one cable connects two interfaces. In this case, an additional switch is not required.

If the number of network interfaces is odd, the number of patch cables must be equal to the number of network interfaces. In this case, an additional switch is required to connect Server network interfaces to it.

The diagnostics of Server network interfaces is performed using only the local management tools.

To perform the diagnostics of the network interfaces:

1. In the local menu, select **Diagnostics** and press **<Enter>**.

   The **Diagnostics** menu appears.
2. Select **Network interfaces diagnostics** and press **<Enter>**.

   A message notifying you that the operation of the Server will be interrupted appears. You are prompted to perform the commutation of network interfaces.
3. Without closing this message window, perform the commutation according to one of the following schemes:
   - If the number of Server network ports is even, connect them pairwise: the first with the second, the third with the forth, and so on.
   - If the number of Server network ports is odd, connect each of them to a port of the switch.
4. In the following window, select **Yes** and press **<Enter>**.

   The Server services will be stopped. After that, the diagnostics of network interfaces starts. Then, you will see the results of the diagnostics.
5. Once you have finished viewing the results, return the Server network interfaces commutation to its initial state and press **<Esc>**.

   The network interface settings will be restored. The Server services will be loaded. You will be returned to the **Main menu**.

Extended logging and creating a logging report

A report about software errors or failures is designed to help developers find out the cause of a failure and fix it in further software releases. To do so, you need to enable extended logging so as to gather data about software operation and the current settings, generate a report based on it, archive the report and send it to the software vendor.

To enable extended logging using the remote management tools:

1. In the Server management menu, select **Diagnostics** and select the **Extended logging** tab.

   Information about Servers in use appears.
2. Choose the required Server and turn on the respective toggle. To enable extended logging for all Servers, use the toggle on the toolbar.

   Attention! This mode requires many resources and slows down the TLS server operation. We highly recommend you use this mode for a limited period of time and only in case of Server diagnostics.
3. In the appeared dialog box, click **Continue**.

   The process of enabling extended logging starts.
4. To get the current information, refresh the page.

   If the process is completed, a message about enabling extended logging appears. The toggle turns green.

You can save the results of extended logging as a report.

To create a report using the local management tools:

1. In the local menu, select **Diagnostics** and press **<Enter>**.
   The **Diagnostics** menu appears.
2. Select **Create a technological archive** and press **<Enter>**.
   The dialog box prompting you to plug in a USB flash drive appears.
3. Plug in an external drive and press **<Enter>**.
   The report creation, archiving and sending it to the external drive start. After that, a success message appears.

Note. As a result, a **tech_arc_YYYY-MM-DD_HH-MM-SS.tar** technological archive file will be created on the external drive, where **YYYY-MM-DD** is the archive creation date and **HH-MM-SS** is the archive creation time. Error 2 while creating a technological archive means that the archive does not contain all files, which is considered as normal situation and does not require fixing.

Nginx configuration

To configure resources:

1. In the local menu, select **Diagnostics** and press **<Enter>**.
   The **Diagnostics** menu appears.
2. Select **Nginx configuration** and press **<Enter>**.
3. Select **Resource configuration** and press **<Enter>**.
   A dialog box prompting you to enter the server name and resource address appears.
4. Specify the server name and the resource address in the respective fields.
5. Press **<Enter>**.

To configure the administration server:

1. In the local menu, select **Diagnostics** and press **<Enter>**.
   The **Diagnostics** menu appears.
2. Select **Nginx configuration** and press **<Enter>**.
3. Select **Administration server configuration** and press **<Enter>**.
   The **Administration server configuration** dialog box appears.
4. Perform the required actions to configure the Server.

Note. To view available commands, press **<F1>**. To return to the configuration dialog box, press **<Enter>**.

5. Press **<F2>** and **<F3>** to apply the changes and check the configuration respectively.
6. To return to the menu, press **<Enter>**.

To view a list of patched resources:

1. In the local menu, select **Diagnostics** and press **<Enter>**.
   The **Diagnostics** menu appears.
2. Select **Nginx configuration** and press **<Enter>**.
3. Select **List of patched resources** and press **<Enter>**.
   A list of patched resources or the **No patches** message appears.
4. To return to the menu, press **<Enter>**.

To roll back patches:

Attention! If the nginx configuration is changed by the local management tools, the configuration using the remote management tools is impossible.

1. In the local menu, select **Diagnostics** and press **<Enter>**.
   The **Diagnostics** menu appears.
2. Select **Nginx configuration** and press **<Enter>**.
3. Select **Rollback patches** and press **<Enter>**.
   The patches will be rolled back or the **No patches** message will appear.
4. To return to the menu, press **<Enter>**.

Chapter 10
Certification authority

The **Certification Authority** section contains the following three tabs:

- **Root certificates** allows you to issue, reissue and export root certificates;
- **Issued certificates** allows you to sign requests, revoke and export issued certificates;
- **Revoked certificates** allows you to view, export and publish a CRL.

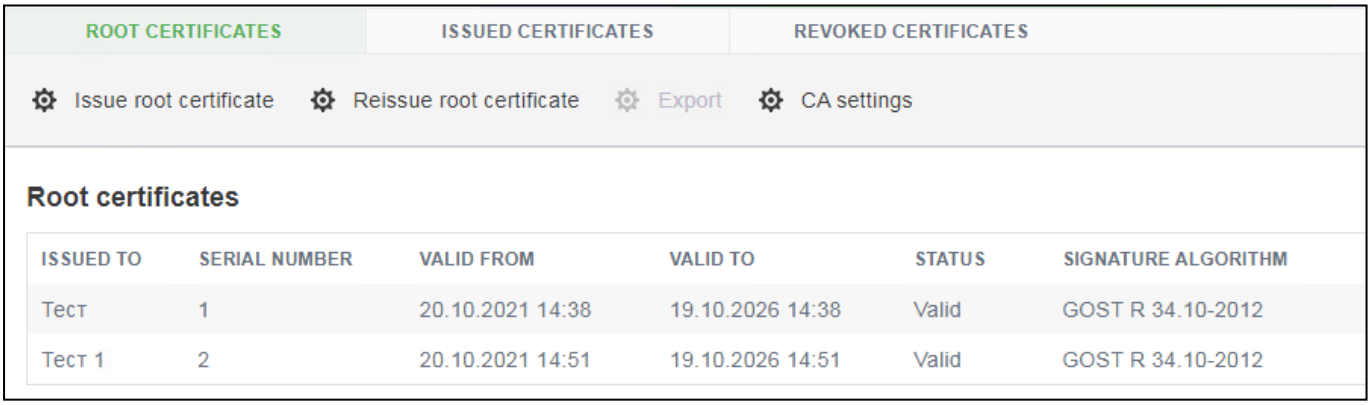
You can manage root, issued and revoked certificates, as well as configure the CA using only remote management tools.

To configure the CA:

1. In the Server management menu, select **Certification authority**.
   The **Root certificates** tab appears.
2. On the toolbar, select **CA settings**.
   A dialog box with CA settings appears.
3. Set a value for the **Allow automatic certificate import to the storage of the trusted** parameter.
4. Fill in the field **CRL distribution point** by specifying a CDP point.
5. Set a value for the parameter **CRL publication interval**.
   Below the value for this parameter, there is a hint with information about the next CRL update.
6. Click **Save**.
   New CA settings will be applied.

Root certificates management

The **Root certificates** tab of the **Certification authority** section contains information about root certificates.



To issue a root certificate:

Note. The **Issue root certificate** button is available only if the current root certificate is missing.

1. In the Server management menu, select **Certification authority**.
   The **Root certificates** tab opens.
2. On the toolbar, click **Issue root certificate**.
   The **Issue a root certificate** dialog box appears.
3. Specify the required parameters:
   - **Signature algorithm**;
   - **Common name**;
   - **Country**;
   - **Region**;
   - **Locality**;

- **Address**;
- **Organization**;
- **Organization unit**.

4. Set a value for the **Valid for** to field from the drop-down list.
5. Click **Issue**.

   The dialog box closes. On the **Root certificates** tab, information about the issued certificate appears.

To reissue a root certificate;

1. In the **Certification authority** section on the **Root certificates** tab on the toolbar, click **Reissue**.

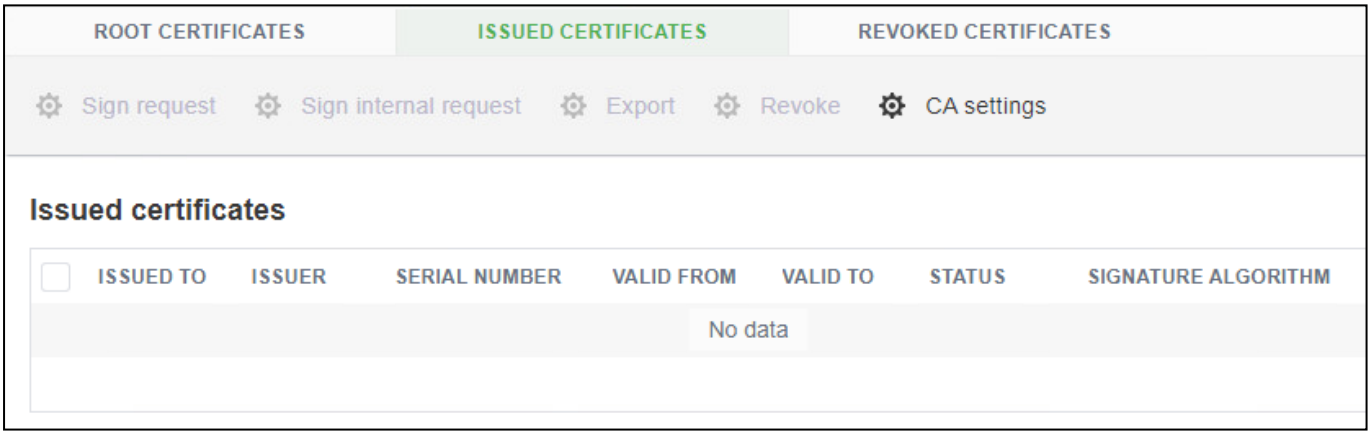
   The **Reissue a root certificate** dialog box appears.
2. Specify the required parameters.
3. Set a value for the **Valid for** to field from the drop-down list.
4. Click **Issue**.

   The dialog box closes. On the **Issued certificates** tab, information about the reissued certificate appears.

To export a root certificate in the **Certification authority** section, on the **Root certificates** tab, select a certificate, and on the toolbar, click **Export**.

Issued certificates management

The **Issued certificates** tab in the **Certification authority** section contains a list of certificates issued by the Server certification authority.



To sign a request for a certificate:

1. In the Server management menu, select **Certification authority**.

   The **Root certificates** tab opens.

   Attention! If a valid root certificate is missing, you cannot issue certificates by request.
2. Select the **Issued certificates** tab.
3. On the toolbar, click **Sign a request**.

   A standard dialog box prompting you to select a file appears.
4. Select the request file created using the Client (with the **req** or **P10** extension). Click **Open**.

   A new certificate appears in the **Issued certificates** table.

To sign an internal request for a certificate:

1. In the **Certification authority** section on the **Issued certificates** tab, click **Sign an internal request**.

   A dialog box containing requests for root certificates created using the Server appears.
2. Select one or several certificates and click **Apply**.

   A list of issued certificates with new ones appears. The names of issued certificates correspond to the names of signed requests.

To export an issued certificate:

1. In the **Certification authority** section on the **Issued certificates** tab, select the required certificate.

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

Attention!
- You cannot export several certificates at the same time. You need to repeat step **2** of this procedure for each certificate being exported.
- When exporting issued certificates, you cannot export a private key.

The process of saving a certificate file onto a hard drive starts.

To revoke one or several certificates:

1. In the **Certification authority** section on the **Issued certificates** tab, select one or several certificates.
2. On the toolbar, click **Revoke**.
   The dialog box prompting you to confirm the certificate revocation appears.
3. Click **Revoke**.
   The selected certificates will be revoked. For information about the state of certificates, see the **Issued certificates** table, the **Status** column.

Revoked certificates management

The **Revoked certificates** tab in the **Certification authority** section contains a list of revoked certificates.

To view a CRL:

1. In the Server management menu, go to **Certification authority | Revoked certificates**.
2. On the toolbar, click **View CRL**.
   The **CRL details** information box appears.
3. After viewing the information about CRL, click **Close**.

To export a CRL file:

1. In the **Certification authority** section, on the **Revoked certificates** tab, click **Export CRL** on the toolbar.
   The **CRL** dialog box appears.
2. Select the required CRL and click **Export**.
   The process of saving a CRL file onto a hard drive starts.

To publish a CRL:

1. In the **Certification authority** section, on the **Revoked certificates** tab, click **Publish CRL** on the toolbar.
   A notification informing you that the CRL has been published appears.
2. Click **Close**.

Appendix

Certificate requirements

The Server and user certificates must have a certain structure and meet a set of requirements.

The structure and contents of the Server certificate

To obtain the Server certificate, the administrator should create a request and send it to a certification authority. The parameters of the requested certificate are preset and specified automatically when creating the request.

Attention! The validity of the Server certificate is verified by the Client.

General characteristics of the Server certificates parameters are described in the table below.

№	Parameter	Description	Value
Basic certificate fields			
1.1	Version	Version	V3
1.3	Serial number	Serial number	Unique number of a certificate
1.3	Signature Algorithm	Signature algorithm	GOST R 34.10-2001 or GOST R 34.10-2012
1.4	Issuer	Certificate issuer, Vendor	CN = Certification center name. O = Organization. C = Country/Region. E = Email
1.5	Valid from	Certificate valid from	Valid from: dd.mm.yyyy hh:mm:ss GMT
1.6	Valid to	Certificate valid until	Valid to: dd.mm.yyyy hh:mm:ss GMT
1.7	Subject	Certificate owner	CN = Server name. OU = Organization unit. O = Organization. C = Country/Region (two English letters). E = Email
1.8	Public Key	Public key	Public key in accordance with the GOST R 34.10-2012 (512 bits) algorithm
Certificate extension			
2.1	Basic Constraints	Basic constraints	Subject type = End entity. Path length limit = no limit
2.2	Key Usage	Key usage	Key agreement or signature
2.3	Extended Key Usage	Extended Key	Server authentication (1.3.6.1.5.5.7.3.1)
2.4	CRL Distribution Point	CRL distribution point	URL = http://www.test.ru/test.crl

The structure and contents of the user certificate

The validity of the user certificate is verified by the Server.

General characteristics of the user certificates parameters are described in the table below

№	Parameter	Description	Value
Basic certificate fields			
1.1	Version	Version	V3
1.3	Serial Number	Serial number	Unique number of a certificate
1.3	Signature Algorithm	Signature algorithm	GOST R 34.10-2001 or GOST R 34.10-2012
1.4	Issuer	Certificate issuer. A vendor.	CN = Certification center name. O = Organization. C = Country/Region. E = Email
1.5	Valid from	Certificate valid from	Valid from: dd.mm.yyyy hh:mm:ss GMT
1.6	Valid to	Certificate valid until	Valid to: dd.mm.yyyy hh:mm:ss GMT
1.7	Subject	Certificate owner	CN = First name and last name. OU = Organization unit. O = Organization. C = Country/Region (two English letters). E = Email
1.8	Public Key	Public key	Public key in accordance with the GOST R 34.10-2001 (512 bits) or GOST R 34.10-2012 (512 bits) algorithm
Certificate extension			
2.1	Basic Constraints	Basic constraints	Subject type = End entity. Path length limit = no limit
2.2	Key Usage	Key usage	Key agreement or signature or key encryption
2.3	Extended Key Usage	Extended Key	Client authentication (1.3.6.1.5.5.7.3.2)
2.4	CRL Distribution Point	CRL distribution point	URL = http://www.test.ru/test.crl
2.5	Private Key Usage Period	Private key validity period	Hashed value of the private key expiration date

Firewall configuration

A firewall on the boundary of a DMZ that contains TLS Server must be configured in the following way:

1. To enable incoming connections, enable TCP port **443** as well as all ports of the created tunnels.

   Note If another port was specified in the HTTPS proxy settings instead of port 443, enable it in the settings for incoming connections.

2. Allow access from TLS Server to protected resources of an internal network.
3. Cluster nodes must be connected directly without the firewall in between. We recommend you isolate this network segment.
4. If you use a balancer, to make cluster nodes available, open port **80** by allowing it to be used in the firewall so that the balancer can access TLS Server.

Installing Server software

By default, the Server is delivered with the preinstalled software. Software is usually installed when updating the current version.

Server software can be delivered on the following media:

- CD-ROM;
- USB flash drive.

The server can be delivered in a case without a CD-ROM drive. In this case, all steps of the software installation are taken using a USB flash drive or an external USB CD/DVD drive.

When using a USB flash drive for the software installation, the drive must stay plugged in a USB port until the installation is complete, because the system boots from this very drive.

To install Server software:

1. Connect a keyboard and a monitor to the Server system unit.
2. Power on the Server and enter the BIOS menu.

   Note. Information on how to enter the BIOS menu is displayed on the monitor at the initial stage of the booting process. Generally, to enter the menu, you need to use the **<F1>**, **<F2>** or **<Del>** keys.

   Now you can see a list of settings. These settings vary depending on the BIOS model and version.
3. Specify the boot order taking into account the given drive.

Drive	Boot order
CD-ROM	**1.** CD-ROM. **2.** Hard drive
USB flash drive	**1.** USB flash drive. **2.** Hard drive

3. Set the system time according to the current GMT date and time. For example, if you are in Moscow time zone, set the time three hours earlier than the current Moscow time.
4. Insert the CD-ROM from the distribution kit into an optical disk drive or plug the USB flash drive in a USB port. Then, close the BIOS menu and save the changes.

   The computer restarts. The main Sobol window displaying a prompt for a security token appears similar to the following one:

   ```
   Present the security token
   ```
5. Do not wait until the Server is booted automatically and place the security token close to the reader.

   Tip. If the Server has been automatically boated, the software installation will not be possible. In this case, restart the Server and repeat the procedure.

   After the information from the security token is read successfully, you are prompted to enter the password.
6. Enter the administrator password created during the password change or specified in the Server data sheet.

   Note. If the administrator does hot have the default password, press **<Enter>**.

   A warning similar to following one appears.

   ```
   Attention! The parameters of the main boot disk have been changed. The boot may be performed from an external drive. Save the new parameters of the main boot disc? (Yes/No)
   ```

   Note. If the software boots from the USB flash drive and the logon to Sobol was performed not by the administrator but by a user for whom the OS boot from external drives is forbidden, the **The parameters of the main boot disk have been changed. The boot is forbidden** message appears. If you press any key, the **The computer is locked** message appears.
7. Enter **Yes** and press **<Enter>**.

   The administrator menu appears (for Sobol version 3.0).

   Attention!
   - In the administrator menu, select **General system parameters** and set **No** for **Standalone mode**.
   - For information about Sobol, see Sobol documentation.
8. Press **<Enter>**.

   The OS boot starts.

   Note. If an error occurs, the Server reboots in automatic emergency mode without any notifications. In this case, repeat the procedure from step 4. If the error occurs again, contact the technical support service of the manufacturer.
9. Select **Install Continent TLS XXXXXX**, where **XXXXXX** is a build number. Press **<Enter>**.

The list of platforms appears.

10. Select the required platform and press **<Enter>**.

    The list of products available for installation appears.

11. Select **TLS** and press **<Enter>**.

    The Server installation starts, during which the following operations are performed:

    - storage device check;
    - hard disk formatting;
    - dependencies check;
    - packages installation;
    - bootloader installation;
    - putting files under integrity control;
    - performing post-installation scenarios.

    After all the operations mentoned above are complete, the Server will be rebooted automatically. The Sobol main menu appears.

12. In the menu, select **Integrity check** and press **<Enter>**.

    A dialog box with integrity check parameters appears.

13. Check the path to the folder with IC templates. The right value is **C:/boot/sobol**.

14. Return to the Sobol main menu, select **General system parameters** and press **<Enter>**.

    A dialog box with general parameters appears.

15. Set a value in between 5 and 40 seconds for the **Automatic logon timeout** parameter.

16. Return to the Sobol main menu, select **OS boot** and press **<Enter>**.

    The boot starts. The main menu of the local management displaying the current version of the software appears.

Note. The availability of the main menu commands depends on the Server state (before and after initialization and network configuration) as well as its role in a cluster (primary or subordinate).

To prepare the Server for operation:

- configure network settings (see p. **15**);
- generate or upload a key if the Server is subordinate in a cluster (see p. **18**);
- perform the Server initialization (see p. **19**).

OS boot parameters modification

When powering on or rebooting the Server, you can modify the OS boot parameters, for example the OS kernel parameters or the monitor parameters.

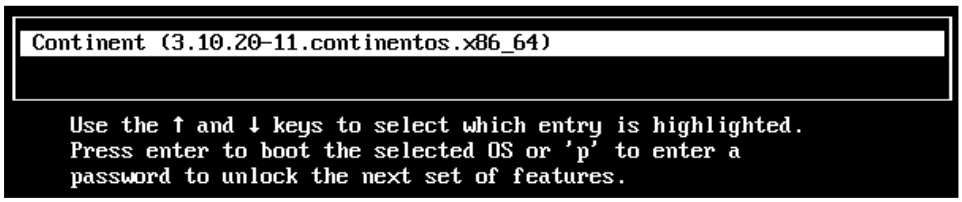
To modify the OS boot parameters:

1. Power on or reboot the Server. During its booting process and straight after the Sobol integrity checks, the following message appears:

Attention! The message is displayed for five seconds.

2. While the message is displayed, press any key.

   The bootloader menu appears.



3. Press **<P>** on the keyboard.

   You are prompted to enter the security code of the bootloader.

4. Enter the current code of the bootloader (see p. **20**) and press **<Enter>**. If the code has not been changed, enter the factory code.

   The modification of the boot parameters will be unlocked.

5. Press **<E>**.

   The menu item expands. The boot parameters will become available for editing.

6. Make the required changes in the boot parameters and press **<B>**.

   The OS starts booting according to the modified parameters.

Attention! The modified boot parameters will not be saved. During the next Server boot/reboot. if the procedure mentioned above is not performed, the default parameters will be applied.

Writing a disk image onto a USB flash drive

The distribution kit includes the **XXXXXX-release.iso** disk image file designed for the installation of Continent TLS Server from a USB flash drive, where **XXXXXX** is a build number.

To write the disk image onto a USB flash drive, use the **FlashGUI.exe** tool. This tool is located in the same folder as the disk image. The tool supports Windows 2000 or higher.

To write the disk image onto the USB flash drive in Windows:

1. Plug the USB flash drive in a USB port of your computer and wait until the drive has connected to the file system.

   After the connection, a new object named **Removable disk** appears in the **My computer** folder.

2. Run **FlashGUI.exe**.

3. In the tool window, enter the required data in the fields and click **Write**.

Parameter	Description
Select a disk to write the disk image onto	The name of a USB flash drive onto which you want to write the disk image. To refresh the list, click **Refresh**
Specify the image file	The full name of the disk image file. To select the file in the standard Windows dialog box, click **...**

   The tool starts writing the disk image onto the USB flash drive. The progress of this process can be seen in the respective field.

4. To finish work with the tool, click **Close**.

5. Remove the USB flah drive from the USB port.

To write the disk image onto the USB flash drive in Linux:

1. Plug the USB flash drive in a USB port of your computer and wait until the drive has appeared in the system.

2. Run the following command:

```
dd if=XXXXXX-release.iso of=/dev/sdb bs=512
```

   where **XXXXXX** is a build name and **sdb** is the name of the USB flash drive.

   The tool starts writing the disk image onto the USB flash drive. Wait until the success message appears.

Configuring access to protected resources using a wildcard certificate

To configure access to protected resources:

1. Create a certificate request (see p. **55**), filling in the values specified below.

Parameter	Value
Common name	***.<servername.ru>**
Additional name	
Additional name type	DNS name
Additional name value	***.<servername.ru>**

<servername.ru> is used to specify the Server domain name.

If necessary, specify other fields of the request (see p. **56**).

2. Sign the request (see p. **84**) and export the issued certificate (see p. **84**).
3. Create and configure two translation rules (see p. **60**) using the issued certificate. For each rule, specify the values shown below.

Parameter	Value
Certificate	Select the issued certificate
Outside address	In the field that contains *, specify the required host name (see p. **60**)

If necessary, fill in other fields (see p. **60**).

Putting the TLS Server into operation for installation on virtual machines

The TLS Server implementation corresponding to the **KS1** modification for installation on virtual machines is delivered as an individual distribution set with the **x.x.x.x-ks1.iso**file, where **x.x.x.x** is a software build number.

Putting the Server in this modification into operation consists of the same stages as for the Server in the hardware modification:

1. Preparation (see p. **13**).
2. Local configuration (see below)
3. Remote configuration using the web interface (see p. **13**).

After the Server software is installed on a virtual machine, then it is configured locally.

Local configuration of the Server installed on a virtual machine consists of the following stages:

1. Network settings configuration (see p. **15**).
2. Entropy file import (see below).
3. Master key generation (see p. **18**).
4. Server initialization (see p. **19**).

To generate entropy using a keyboard:

1. In the local menu, select **Entropy** and press **<Enter>**.
   The **Entropy import** menu appears.
2. Select **Generate entropy from keyboard** and press **<Enter>**.
   The dialog box prompting you to specify the number of long-term keys.
3. Specify the required value and press **<Enter>**.
   The confirmation dialog box appears.
4. Select **Yes** and press **<Enter>**.
   The process of entropy generation starts.
5. Follow the instructions till the progress bar displays **100%** value.
   When the procedure is finished, the **Entropy will now be moved to key drive** message appears.
6. Press **<Enter>**.
   The dialog box prompting you to specify the name for exported entropy file appears.
7. Specify the required name for exported entropy file and press **<Enter>**.
   The dialog box prompting you to insert a USB drive appears.
8. Insert a USB drive and press **<Enter>**.
   The entropy file will be recorded on the USB drive.

To import an entropy file:

Note. You cannot import the entropy file for the second time. You need to create a new entropy file on another administrator workstation using a biological RNG.

1. In the local menu, select **Entropy** and press **<Enter>**.
   The menu for entropy management appears.

2. Select **Import entropy from a key drive** and press **<Enter>**.
   The dialog box prompting you to present a key drive appears.
3. Present your key drive and press **<Enter>**.
   A dialog box prompting you to select the required file on the drive appears.
4. Select the required entropy file and press **<Enter>**.
   The entropy will be uploaded from this file. After that, a success message appears.
5. Remove the drive and exit the menu.

To delete an entropy file:

1. In the local menu, select **Entropy** and press **<Enter>**.
   The menu for entropy management appears.
2. Select **Delete entropy** and press **<Enter>**.
   A success message appears.
3. Press **<Enter>**.

After the local configuration, the Server management web interface will become available.

Create a file to import the list of access control parameters

To import the list of access control parameters, create a **TXT** file containing the list of certificate parameters and their values on which basis the access to the resource will be granted.

The format of a record in the list of parameters must be as follows:

```
PARAMETER VALUE
```

The access control parameters values are specified in the table below.

Parameter	Value	Available symbols
Common name	**commonName**	• lowercase and uppercase letters (A – Z, a– z); • numbers (0 – 9); • special characters: **' ; , - _**. Forbidden: • to use a space at the beginning and the end of a value; • to use more than one space between words. Maximum number of symbols — 128
E-Mail	**emailAddress**	Format of a record: `user@host.domain` Maximum number of symbols in a record — 128. For **user**: • lowercase and uppercase letters (A – Z, a– z); • numbers (0 – 9); • special characters: **- _ . * ! # $ % & ' + / = ? ^ ` { | } ~**; • minimum number of symbols — 1, maximum — 64; • a dot cannot be repeated more than once in a row and be the first or the last symbol. For **host.domain**: • lowercase and uppercase letters (A – Z, a– z); • numbers (0 – 9); • special characters: **- .** ; • minimum number of symbols — 1, maximum — 63; • a dot and a hyphen cannot be the first or the last symbol
Unique certificate number	**serial**	• lowercase and uppercase letters (A – F, a– f); • numbers (0 – 9); • a space cannot be the first or the last symbol. Maximum number of symbols — 128
INN	**inn**	• numbers (0 – 9); • a space cannot be the first or the last symbol. Maximum number of symbols — 12

Parameter	Value	Available symbols
INNLE	**innle**	• numbers (0 – 9); • a space cannot be the first or the last symbol. Maximum number of symbols — 10
OGRN	**ogrn**	• numbers (0 – 9); • a space cannot be the first or the last symbol. Maximum number of symbols — 13
SNILS	**snils**	• numbers (0 – 9); • a space cannot be the first or the last symbol. Maximum number of symbols — 11
Organization	**organization**	• lowercase and uppercase letters (A – Z, a– z); • numbers (0 – 9); • special characters: **" % & ' ( ) + , - : ; @ _ №**. Forbidden: • to use a space at the beginning and the end of a value; • to use more than one space between words. Maximum number of symbols — 128

Two-factor authentication on the Application portal using auth.as

When authenticating on the Application portal by login and password, two-factor authentication is available using the **auth.as** service. In case of two-factor authentication, besides entering a login and a password, you are to enter a one-time password additionally.

Attention! To authenticate using a one-time password, install and configure the **auth.as** app on your mobile device for one-time password generation.

To configure two-factor authentication:

1. In the **Menu**, go to **Resources | Application portal**.
   The **Application Portal connection settings** appears.
2. In the **Connection** tab, click **Configure** in the **Authentication using login/password** section.
   The **Authentication using login/password** menu appears.
3. In the **Two-factor authentication** section, select **Enable two-factor authentication**.
4. In **Authentication URL**, specify the required protocol and the address of the one-time password generation system.
5. In the **API key** text box, specify the required data.

   Note. To receive an API key, authorize in the one-time password generation system and copy the API key specified for the required domain name.
6. Click **Save**.
   The **Authentication using login/password** menu closes. A field for entering a one-time password appears in the Application portal web-page.

Entropy consumption

You can find the details about entropy consumption depending on the performed procedure in the table below.

Procedure	Entropy consumption
Initialization	160 bytes
Creating certificate request	40 bytes
Reissuing certificate of a Server in a cluster	40 bytes
Reissuing root certificate in a cluster	40 bytes

If the amount of entropy is less than 320 bytes, the administrator receives a respective notification.