SECURITY CODE

Secret Net Studio

Administrator's manual

Installation and update

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

Table of contents

List of abbreviations 5

Introduction 6

About Secret Net Studio deployment 7

Components of the System 7

Hardware and software requirements 7

Client 7

Security Server 8

Control Center 8

System setup disk 9

Secret Net Studio installer 9

Component installation options 10

Installation procedure for centralized management 10

Preparation 10

General procedure for component installation 11

Typical deployment scenario 11

Installing Secret Net Studio locally 13

Installing the Security Server 13

Creating a new security forest and domain 13

Creating a security domain in an existing forest 16

Adding the Security Server to an existing security domain 17

Installing the Control Center 18

Installing the Client 18

Interactive installation 18

Installing the Client centrally 22

Creating a list of centrally installed software 22

Creating deployment tasks 23

Updating and restoring Secret Net Studio 25

Updating 25

Centralized updating procedure 25

Updating the Security Server 25

Updating the Control Center 27

Updating the Client 27

Restoring 27

Restoring the Client 28

Restoring the Control Center 28

Uninstalling Secret Net Studio 29

Uninstallation procedure for network operation mode 29

Uninstalling the Client 29

Uninstalling the Control Center 29

Uninstalling the Security Server 29

Uninstalling the Client subsystems 30

Appendix 31

Software for supported USB keys and smart cards 31

Registry changes during the Client installation 31

Client installation folder 31

Installing and configuring MS SQL DBMS 32

IIS changes during the Security Server installation 34

Settings change for the connection of the Security Server to the DBMS server 35

Account data 35

Connection string 35

Specific features of the standby Security Server 36

Options for restoring an incorrectly removed Security Server 37

Transfer of the LDAP schema master role to another Security Server 37

Documentation 38

List of abbreviations

AD	Active Directory
IIS	Internet Information Services
LDAP	Lightweight Directory Access Protocol
NTFS	New Technology File System
OID	Object Identifier
SID	Security Identifier
SP	Service Pack
USB	Universal Serial Bus
XML	Extensible Markup Language
DB	Database
IS	Information System
IC	Integrity control
OS	Operating System
PNR	Public Network Resource
OM	Operational Management
SW	Software
DBMS	Database Management System
CM	Centralized Management
eID	Electronic Identifier

Introduction

This manual is designed for Secret Net Studio administrators (hereinafter "Secret Net Studio, the System"). It contains information that administrators need in order to install, update, correct or remove the product's software. Before reading this manual, read the general information about Secret Net Studio, which can be found in the document [**1**].

Conventions

In order to highlight certain elements in the text, a series of conventions is used.

Internal links usually indicate the required page number.

Important and additional information in the document is presented as notes. Icons in the margins indicate the importance of the information they contain.

- This icon highlights additional information that may contain examples, links to other documents, or other parts of the manual.
- This icon highlights important information that must be taken into account.
- This icon highlights a warning.

Exceptions. Some notes may not have any icons. Apart from note icons, the margins may also contain other graphical elements, for example, buttons that are explained in adjacent paragraphs.

Other information sources

If you have Internet access, you can visit SECURITY CODE Ltd. website (https://www.securitycode.ru/) or contact a company's representatives via email (info@securitycode.ru).

Chapter 1
About Secret Net Studio deployment

The Secret Net Studio system has a module structure. For details of the Secret Net Studio system architecture, see document [**1**].

Components of the System

The Secret Net Studio system components are as follows:

1. "Secret Net Studio" (hereinafter – "the Client").
2. "Secret Net Studio — Security Server" (hereinafter – "the Security Server").
3. "Secret Net Studio — Control Center" (hereinafter – "the Control Center").

Hardware and software requirements

Client

The Client is installed on computers running the following operating systems (32-bit and 64-bit OS versions are supported with the following minimal update packages installed):

- Windows 10;
- Windows 8/8.1;
- Windows 7 SP1;
- Windows Vista SP2;
- Windows Server 2012/Server 2012 R2;
- Windows Server 2008 SP2/Server 2008 R2 SP1.

To install the Client in network operation mode, the computer must be included in the Active Directory domain.

The following table lists the hardware components that are required for the Client:

Requirement	Minimum value
Processor	According to OS requirements
RAM	2 GB
Disk space	4 GB

The Windows OS system catalog %SystemRoot% must be in an NTFS or NTFS5 file system volume.

To install the Client on a computer, the following software must be installed:

- Internet Explorer 8 or later.

If you want to use hardware security tools on a computer, we recommend you prepare these tools before installing the Client. The preparation of the tools is performed in accordance with product documentation. Software for supported USB keys and smart cards can be installed from the System setup disk. Setup files are located in the respective subfolders of the \Tools\ folder (information about file locations can be found in the Appendix on p. **31**).

The Client can be centrally installed in network operation mode under the Security Server control. In this case, if the firewall is enabled, you will need to authorize ports to share access to general resources: 137, 138, 139, 445. By default, these ports are closed by the firewall unless there are shared folders on the computer.

A restore point will be automatically created for the OS before installing the Client. The setup program automatically checks and, if necessary, installs the following Microsoft packages that are available for distribution:

- Microsoft C/C++ Runtime for Visual Studio 2013;

- Microsoft .NET Framework 4.5;
- Microsoft service packs: KB2117917, KB971512 and KB2462317;
- Microsoft Core XML Services (MSXML) 6.0;
- Microsoft XML Paper Specification Essentials Pack (XPS EP).

You may need to restart the computer after you install the updates.

Security Server

The Security Server is installed on computers included in the Active Directory domain and running the following OS:

- Windows Server 2012/Server 2012 R2;
- Windows Server 2008 R2 SP1.

The following table lists the hardware components that are required for the Security Server:

Requirement	Minimum value	Recommended value
Processor	According to the OS requirements	Intel Core i5/Xeon E3 or higher
RAM	8 GB	16 GB[1]
Disk space	150 GB High-speed HDDs are recommended	

[1] When deploying the SS and the DBMS server on the same computer.

You need to install a MS SQL server-based DBMS. The Security Server and the DBMS server can be installed on different computers (recommended) or on the same computer.

The following versions of the database server software that are compatible with the Security Server (32-bit and 64-bit OS versions are supported with the following minimal update packages installed):

- Microsoft SQL Server 2012 SP1, including SQL Server 2012 Express (MS SQL Server 2012 SP1 Express can be installed from the setup disk — see p. **32**);
- Microsoft SQL Server 2014, including SQL Server 2014 Express;
- Microsoft SQL Server 2008 R2 SP1, including SQL Server 2008 R2 Express.

Note.
Correct interaction between the security server and MS SQL DBMS is ensured by meeting the conditions specified in the Appendix on p. 32.

The computer must meet the following additional requirements:

- the computer must have free TCP ports 50000–50003. If these ports are used by other applications, we recommend you to assign other ports to the Security Server during installation;
- the Web server (ISS) role must be enabled on the computer.

The setup program automatically checks and, if necessary, installs the following Microsoft packages that are available for distribution:

- Microsoft C/C++ Runtime for Visual Studio 2013.

You may need to restart the computer after you install the updates.

Control Center

The Control Center is installed on computers included in the Active Directory domain running the following OS (32-bit and 64-bit OS versions are supported with the following minimal update packages installed):

- Windows 10;
- Windows 8/8.1;
- Windows 7 SP1;
- Windows Vista SP2;

- Windows Server 2012/Server 2012 R2;
- Windows Server 2008 SP2/Server 2008 R2 SP1.

The following table lists the hardware components that are required for the Control Center:

Requirement	Minimum value
Processor	According to OS requirements
RAM	2 GB[1]
Disk space	4 GB[2]

[1] This value is sufficient to display 1-1.5 million log entries. If you want to view archives larger than 80 MB increase this value or filter the log entries.

[2] This value is sufficient to unpack archives not larger than 80 MB (files are extracted from archives to the user's folder for temporary files) If you want to unpack archives larger than 80 MB increase this value. For example, to unpack 200-300 MB archives, you need at least 10 GB.

To install the Control Center, the following software must be installed:

- Internet Explorer 8 or later.

The setup program automatically checks and, if necessary, installs the following Microsoft package that is available for distribution:

- Microsoft .NET Framework 4.5.

System setup disk

The Secret Net Studio system software and operating instructions are supplied on a setup disk. The setup disk is an AutoRun-enabled disc. When the disk is inserted, AutoRun automatically runs Secret Net Studio installer.

The general structure of the disk's folders is described in the table below:

Folder	Content
\Setup\Server\	Security Server distribution kit
\Setup\Console\	Control Center distribution kits
\Setup\Client\	Client distribution kits
\Documentation\	Documentation
\Tools\	Additional tools and files for software installation and setup

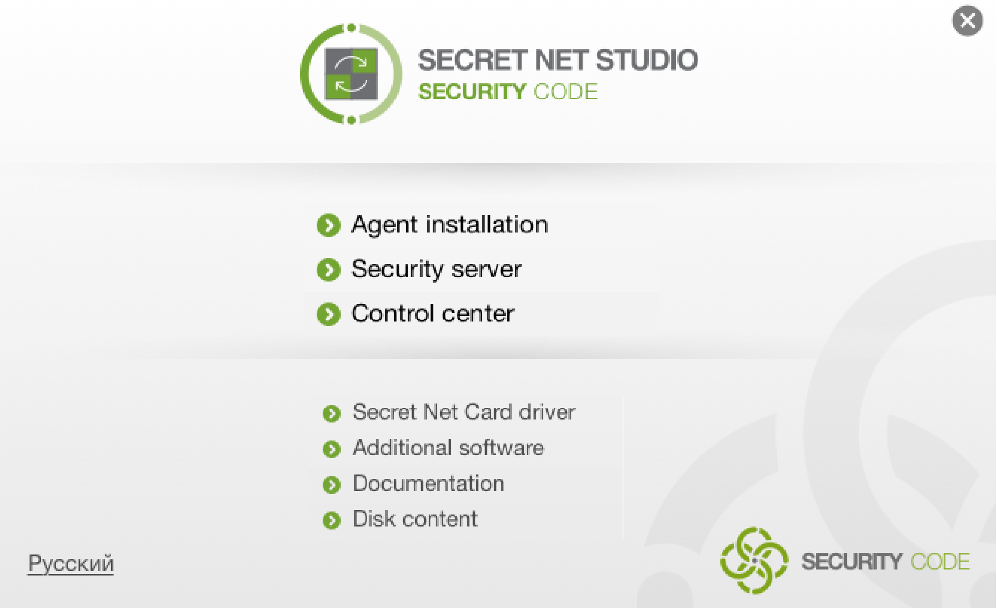
Secret Net Studio installer

Secret Net Studio installer makes it possible to perform the following operations:

- run the program for the installation of the Secret Net Studio system components;
- open disk catalogs in separate windows.

Note.
If AutoRun is disabled on your computer, the installer cannot be run automatically. In this case, in order to run the installer, run the SnAutoRun.exe file in the disk's root folder.

The installer welcome window is shown in the figure below.



SECRET NET STUDIO
SECURITY CODE

- Agent installation
- Security server
- Control center

- Secret Net Card driver
- Additional software
- Documentation
- Disk content

In this window, you can run the following commands:

Command	Purpose
Agent installation	Runs the Client setup program
Security server	Runs the Security Server setup program
Control center	Runs the Control Center setup program
Additional software	Opens the \Tools\ catalog in a separate window
Documentation	Opens the \Documentation\ catalog in a separate window
Disk content	Opens the disk's root directory in a separate window

Certain run commands can be blocked if it is impossible to install components or if no installation is required. To view the reasons for blocking, hover the pointer over the command, and the respective clarifying pop-up message appears in 1-2 seconds.

Component installation options

Components of the Secret Net Studio system can be installed during a local or terminal computer session.

To install the Client in network operation mode, installation managed by the Security Server is provided for.

Installation procedure for centralized management

Preparation

Before the Secret Net Studio system components are installed for centralized management, you need to complete certain preparations to create security domains and a network structure. For information about security domains and the network infrastructure of the Secret Net Studio system, see[**1**].

Preparations:

1. If a security domain is to be created on the basis of organizational units, prepare the organizational units and include the required computers in them.
2. Create a group of users that will be specified as the forest administrators group for each security domain forest. The users included in the group of security domain forest administrators will have the privilege to create new security domains in the respective forest.
3. Create the groups of users who will be specified as security domain administrators.

General procedure for component installation

The Secret Net Studio system components are installed in the following order:

1. Do the following on the computer that will be used as the root Security Server (not subordinate to other servers):
   - include the group of administrators of the security domain forest and the group of administrators of the security domain in the local computer's group of administrators (based on which security domain a server will be related to);
   - install the Security Server (see p. **13**).
2. Complete the same steps as in p. **1** on the other computers that will be used as subordinate Security Servers.
3. On the Secret Net Studio administrators' computers install the Control Center (see p. **18**).
4. Install the Client in network operation mode (see p. **18**) on the Security Server computers first, and then on other computers.

Typical deployment scenario

Below is a typical scenario for the deployment of the Secret Net Studio system components when creating one security domain on the basis of an Active Directory organizational unit. All protected computers are subordinate to one Security Server.

1. Using the Active Directory object management tools, create an organizational unit and include in it all the computers where the Secret Net Studio system software will be installed.
2. Create domain user for administrators of the security domain forest and administrators of the security domain. Include the accounts that should be granted the respective privileges in these groups.

   Note.
   In this typical scenario, you can create one group of security administrators instead of creating two groups. This group can be selected both as the group of forest administrators and the group of security domain administrators. However, if you want to expand the system to several security domains, we recommend you to create an individual group of forest administrators and include different accounts in the new groups.

3. Do the following on the computer that will be used as the Security Server:
   - include the group of forest administrators and the group of security domain administrators in the local group of the computer's administrators;
   - install the Security Server (see p. **13**).

   Attention!
   To ensure the continuous operation of protected computers, you will need to install a standby server within the same security domain. The standby server is installed when the server is included in an existing security domain. Make the standby server subordinate to the main server of the security domain. For specific features of standby server, see the Appendix on p. 36

4. Install the Control Center on the security administrator's computer (see p. **18**).
5. Run the Control Center and establish a connection to the Security Server.

Note.
For more information about operating the Control Center, see [**4**].

6. Set up centralized installation of the Client on the computers of the organizational unit. To do this, add the Client setup files to the list of software installed centrally and create deployment tasks (see p. **22**).
7. Monitor the execution of tasks in the Control Center. After installing the Client and restarting the computers, they will appear in the management structure as objects subordinate to the Security Server.

Chapter 2
Installing Secret Net Studio locally

Secret Net Studio components can be installed in the local or terminal sessions. All components must be installed by a user included in the local group of computer administrators.

In order to centrally manage the Clients in network operation mode, you need to install the Security Server and Control Center. The Clients in autonomous mode can be managed only locally. Therefore, you do not need to install the above components.

Installing the Security Server

Before installing the Security Server, you need to install the MS SQL DBMS server software (for information about installation options, see p. **8**).

You may need special permissions to perform some the Security Server installation procedures. For example, the rights to administer the security domain forest. If the user installing the software does not have the necessary rights, the setup program asks for the account data of privileged users during certain stages.

Attention!

You will not be able to change the server computer name after the Security Server is installed. If the computer is renamed, the Security Server will stop working and become unavailable for connections to other components of the Secret Net Studio.

The options for installing the Security Server are as follows:

- installation with the creation of a new forest and security domain;
- installation with the creation of a new security domain in an existing forest of security domains;
- installation with the adding the Security Server to an existing security domain.

Creating a new security forest and domain

When installing the first Security Server, use the option that creates a new security domain forest and security domain. This option is also used to create a separate security domain forest.

To install the Security Server with the creation a new forest and security domain:

1. Insert the Secret Net Studio setup disk into the drive. Wait until the installer welcome window appears (see p. **9**) and click the "Security Server" command.

   Note.

   If AutoRun is disabled on your computer, the installer cannot be run automatically. In this case, in order to launch the installer, run the following file from the setup disk: \Setup\Server\x64\setup.en-US.exe.

   When the setup program starts the computer is checked for compliance with the software and hardware requirements for installing the component. The state of the built-in User Account Control (UAC) mechanism is checked during this stage.

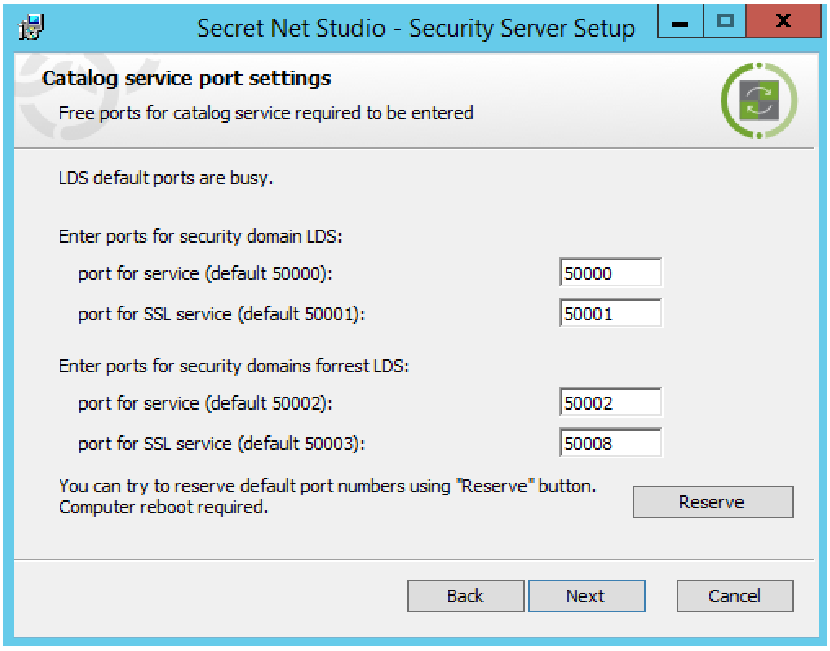
   Attention!

   If UAC is enabled, a dialog box appears asking you to temporary disable it. Click Yes to disable the mechanism, then restart the computer and start the Security Server installation procedure again.

   The setup program begins its preparations, and then the Setup Wizard dialog box appears.
2. To continue the installation, click Next.

   The license agreement dialog box appears.
3. Read the license agreement, and if you agree with all its terms, select the accept check box and then click Next.

If the computer ports designed for directory services are already in use (any port within the 50000–50003 range), the "Catalog service port settings" dialog box appears as in the figure below.



Secret Net Studio - Security Server Setup

Catalog service port settings

Free ports for catalog service required to be entered

LDS default ports are busy.

Enter ports for security domain LDS:

port for service (default 50000): 50000

port for SSL service (default 50001): 50001

Enter ports for security domains forrest LDS:

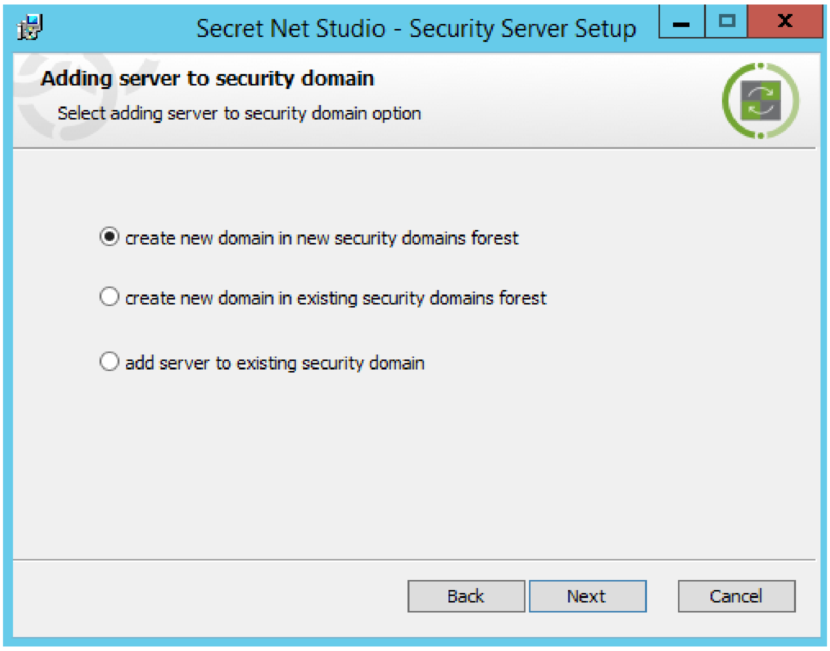
port for service (default 50002): 50002

port for SSL service (default 50003): 50008

You can try to reserve default port numbers using "Reserve" button. Computer reboot required.

4. In the "Catalog service port settings" dialog box, you can specify other ports instead of those that are already in use or try to reassign the occupied ports (using the Reserve button) for the Security Server. Complete the required steps and click Next.

   The "Adding server to security domain" dialog box appears as in the figure below.



Secret Net Studio - Security Server Setup

Adding server to security domain

Select adding server to security domain option

● create new domain in new security domains forest

○ create new domain in existing security domains forest

○ add server to existing security domain

5. Select the "create new domain in new security domains forest" check box and click Next.

   The "File with Authentication Server Settings" dialog box appears. Use this dialog box to create a file with the settings of the authentication server connection in the new security domain.

6. In the dialog box, specify the location and name of the created file and click Next.

> **Attention!**
> The authentication server settings file contains the data required to access to the server. This data is necessary when the new Security Servers are added to the same security domain. Ensure the created file is securely stored and protected against any data compromising.

The "Security domain settings" dialog box appears.

7. In the drop-down list, select a container for creation the new security domain. You can select an organizational unit of the computer or any superior organizational unit as the container (including the entire AD domain). After the container is selected, edit the created security domain name(if necessary).
8. Click Next.

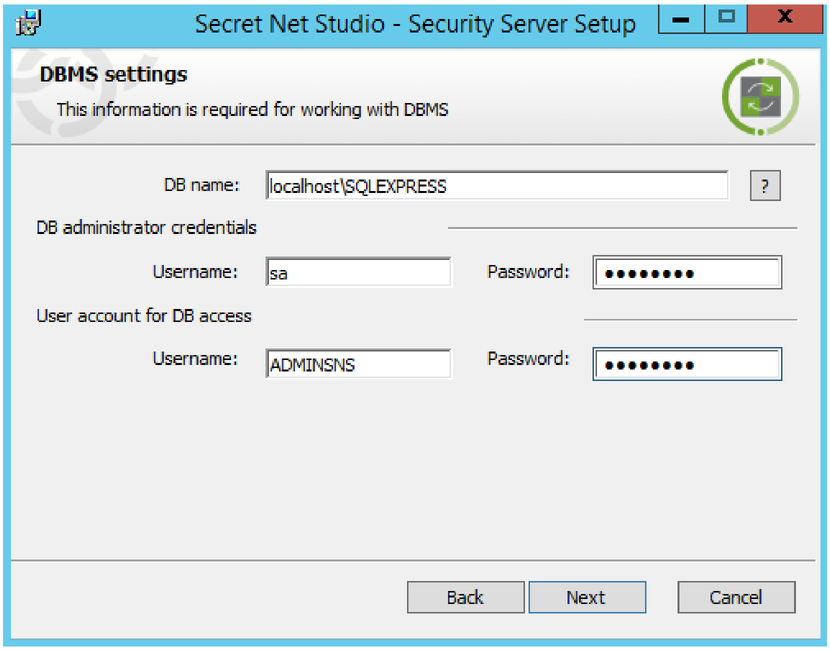
   The "Security administrator group" dialog box appears.
9. Select the user groups who you want to grant permissions to manage the security domain and security domain forest using the respective "Change" button. Click Next.

> **Note.**
> We recommend not to use the standard Domain Admins group as the group of security domain administrators. If User Account Control (UAC) mechanism is enabled, an error may occur during connecting to the Control Center server that installed on the same computer. This error may occur because of insufficient user privileges. In this case, connection is allowed only for the initial administrator account of the Windows domain. To start a program session with sufficient rights click the "Run As Administrator" command in the context menu of the Control Center icon.
> We recommend you to use a specifically created users group to be security domain administrators.

The "Folder settings" dialog box appears.

10. Leave the default folders to install the Security Server and copy the system files or specify other destination folders. Click Next.

    The "DBMS settings" dialog box appears as in the figure below.



Secret Net Studio - Security Server Setup

DBMS settings

This information is required for working with DBMS

DB name: localhost\SQLEXPRESS

DB administrator credentials

Username: sa   Password: ••••••••

User account for DB access

Username: ADMINSNS   Password: ••••••••

11. Perform the following actions for MS SQL DBMS:
    - Specify the connection settings for the DB to work with the Security Server:
      - in the "DB Name" field, specify the connection string: *<name_or_MS_SQL_server_IP_address>\<DB_instance_name>,<port>*

> **Note.**
> You do not need to specify the port number if the default port is used.

- in the "DB administrator credentials" group of fields, specify the account data of the DB administrator on the DBMS server;
- in the "User account for DB access" group of fields, specify the account data which the Security Server will use to connect to the DB (an account for connection will be created);

Note.
The Security Server does not support Windows authentication mode when it works with the DBMS server. Therefore, to connect to the DB, specify the account data of a database user (not a domain user).

- Click Next.

12. If a DB already exists (if it remains after a previously installed server), a dialog box with options of continuation appears: to use the existing DB or create a new one. Select the needed option in this dialog box and click Next.

The "Organization name" dialog box appears.

13. Specify the organization name and unit that will maintain the Security Server being installed and click Next.

Note.
This data will be used when the Security Server certificate is generated. The organization name and unit may be entered later or replaced during the execution of the "Generation and installation of the Security Server certificate" procedure.

A dialog box appears notifying you that everything is ready for installation.

14. Click Install.

The setup program begins copying files to the hard disk and registering the components in the Windows OS registry. A progress bar appears, showing the progress of the process. Additional windows with service information may appear. These windows are closed automatically.

After the installation and setting are finished successfully, the "Installation complete" dialog box appears.

15. Click Close.

A window with the list of setup program operations appears. After all the operations are completed, you will be asked to restart the computer.

16. Restart the computer.

Attention!
The new Security Server object may appear in the operational management structure with a slight delay (about 10-15 minutes if the Control Center is connected to another Security Server).
When the Security Server is run for the first time, domain users from the Active Directory are synchronized with the Security Server's database. Synchronization may take from a few minutes to one hour depending on the number of accounts. During synchronization, the Control Center cannot establish a connection to this server (you will see a message that synchronization is executed). We recommend you to wait for the synchronization to complete and not to perform any actions with the accounts, including the first login on the protected computer. If the first login occurs before the synchronization is completed, incorrect user information may be stored in the Security Server database. In particular, an invalid user password may be saved and you will have to change the password for this user in the Control Center.

Creating a security domain in an existing forest

You can create a new security domain and include it in a security domain forest that already exists.

To install the Security Server with the creation of a security domain in the existing forest:

1. Perform steps **1–4** of the Security Server installation procedure with the creation of a new forest and security domain (see p. **13**).
2. In the "Include Server in the Security Domain" dialog box, select the "Create new domain in existing security domains forest" check box and click Next.

The "Authentication Server Settings File" dialog appears, which is used to create a configuration file with settings of the authentication server connection in the new security domain.

3. In the dialog box, specify the location and name of the created file and click Next.

⚠

> **Attention!**
> The data from the Authentication Server Settings File is necessary, when new Security Servers are added to the same security domain. Ensure the created file is securely stored and protected against any data compromising.

The "Security server subordination" dialog box appears.

4. In the "Parent Server" drop-down list, select the name of the computer that will be the parent Security Server. In the Connection Settings field, specify the network settings template to be used to interact with the parent Security Server.

> **Comment.**
> The network settings template determines the timeout values in accordance with network speed parameters. You can correct the timeout values later during the Security Server setting in the Control Center.

5. Click Next.

   The "Security domain settings" dialog box appears.

6. In the drop-down list, select a container to create the new security domain. You can choose an organizational unit of the Security Server computer or any superior organizational unit as the container (including the entire AD domain). After the container is selected, edit the created security domain name (if necessary) and click Next.

   The "Groups of Security Administrators" dialog box appears.

7. In the dialog box, specify the group of users who will be granted the administration rights to the security domain. Click Next.

   The "Depository Settings" dialog box appears. Then you must complete the Security Server installation procedure by creating a new forest and security domain (see p. **13**) starting from step **10**.

Adding the Security Server to an existing security domain

If you have a security domain that was created, when you installed the first Security Server in this domain, you can include an additional Security Server to the existing domain.

To install the Security Server with its inclusion in the existing security domain:

1. Perform steps **1–4** of the Security Server installation procedure with the creation of a new forest and security domain (see p. **13**).

2. In the "Include Server in the Security Domain" dialog box, select "add server to existing security domain" check box and click Next.

   The "Authentication Server Settings File" dialog box appears, which is used to choose a configuration file with settings of the authentication server connection in the target security domain.

3. In the dialog box, specify the location and name of the file that was created during the first Security Server installation in the target security domain and click Next.

⚠

> **Attention!**
> Ensure the secure transfer of the Authentication Server Settings File to the target computer in order to prevent compromising this file.

The "Security server subordination" dialog box appears.

4. In the "Parent Server" drop-down list, select the name of the computer that will be the parent Security Server. In the "Connection Settings" field, specify the network settings template to be used to interact with the parent Security Server.

Comment.
The network settings template determines the timeout values in accordance with network speed parameters. You can correct the timeout values later during the Security Server setting in the Control Center.

5. Click Next.

   The "Security domain" dialog box appears.

6. In the drop-down list, select a container to include the Security Server into a container-based security domain. The list shows containers associated with existing security domains. After selecting a container, click Next.

   The "Directory Settings" dialog box appears. Then you must complete the Security Server installation procedure by creating a new forest and security domain (see p. **13**) starting from step **10**.

Installing the Control Center

To install the Control Center:

1. Insert the Secret Net Studio setup disk into the drive. Wait until the installer welcome window appears (see p. **9**) and click the "Control Center" command.

   Note.
   If AutoRun is disabled on your computer, the installer cannot be run automatically. In this case, in order to launch the installer, run the following file from the setup disk:
   - on a computer running 64-bit Windows: \Setup\Console\x64\setup.en-US.exe;
   - on a computer running 32-bit Windows: \Setup\Console\Win32\setup.en-US.exe.

   The setup program begins its preparations and then the Setup Wizard dialog box appears.

2. To continue the installation, click Next.

   The license agreement dialog box appears.

3. Read the license agreement, and if you agree with all its terms, select the accept check box and then click Next.

   The "Destination Folder" dialog box appears.

4. Leave the default destination folder or specify another one and click Next.

   A dialog box appears notifying you that everything is ready for installation.

5. Click Install.

   The installation process begins. A progress bar appears, showing the progress of installation process. After the installation is finished with success the "Installation complete" dialog box appears.

6. Click Close.

Installing the Client

The Client is installed locally if its centralized installation is impossible or not advisable (see p. **22**). In particular, if the Client is installed for use in the autonomous mode.

Interactive installation

To install the Client:

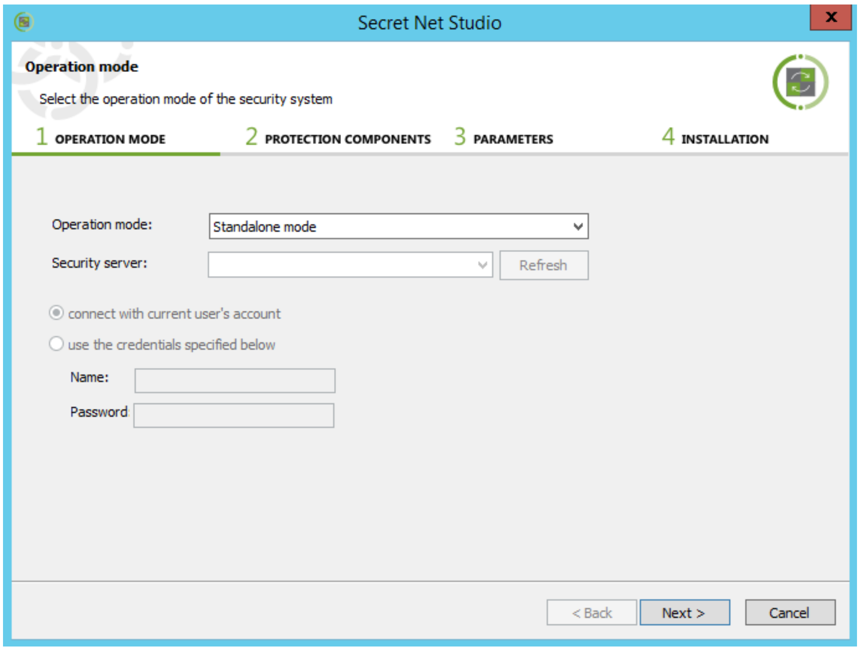
1. Insert the Secret Net Studio setup disk into the drive. Wait until the installer welcome window appears (see p. **9**) and click the "Agent installation" command.

   Note.
   If AutoRun is disabled on your computer, the installer cannot be run automatically. In this case, in order to launch the installer, run the following file from the setup disk:
   - on a computer running 64-bit Windows: \Setup\Client\x64\SnSetup.en-US.exe
   - on a computer running 32-bit Windows: \Setup\Client\Win32\SnSetup.en-US.exe.

   The license agreement dialog box appears.

2. Read the license agreement, and if you agree with all its terms, click Accept.

   A dialog box asking you to select the Client operation mode appears as in the figure below.



Secret Net Studio

Operation mode

Select the operation mode of the security system

Operation mode: Standalone mode

Security server:

● connect with current user's account

○ use the credentials specified below

Name:

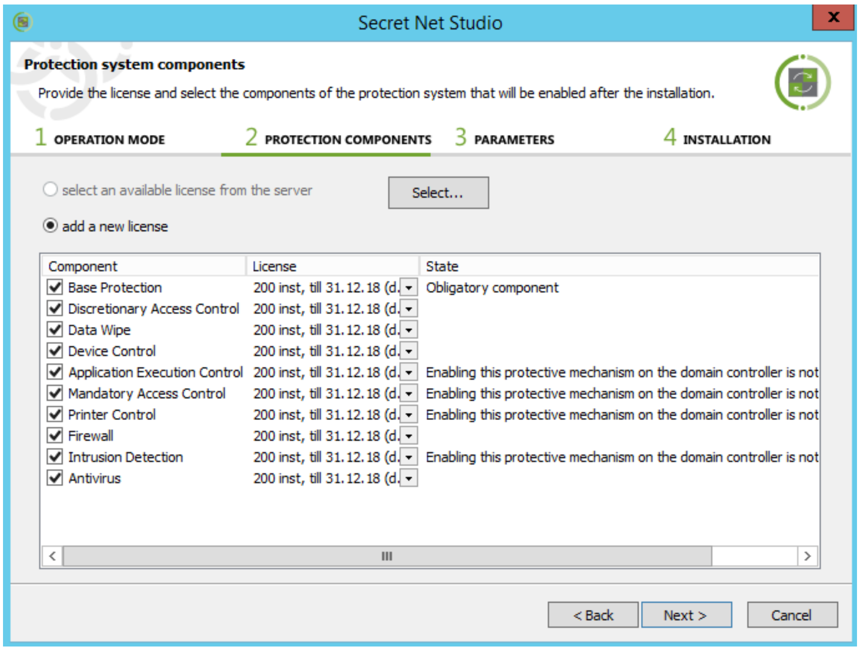
Password

3. In the "Operation Mode" field, specify the required Client operation mode: autonomous (select "standalone") or network (select "Controlled by Security Server"). If you select the network operation mode, configure the settings of subordination to the Security Server:

   - Select the name of the Security Server this computer will be subordinate to (if the needed name is not present in the drop-down list, click the Refresh button to reload).
   - To subordinate the computer, you need the administrative rights to the security domain the Security Server is related to. If the user installing the Client has such rights select the "connect with the current user's account" check box. Otherwise, select the "use the credentials specified below" check box and enter the account data of the user included in the group of the security domain administrators.

4. Click Next >.

   A dialog box appears asking you to select licenses and create a list of security subsystems to be installed.



Protection system components

Provide the license and select the components of the protection system that will be enabled after the installation.

○ select an available license from the server

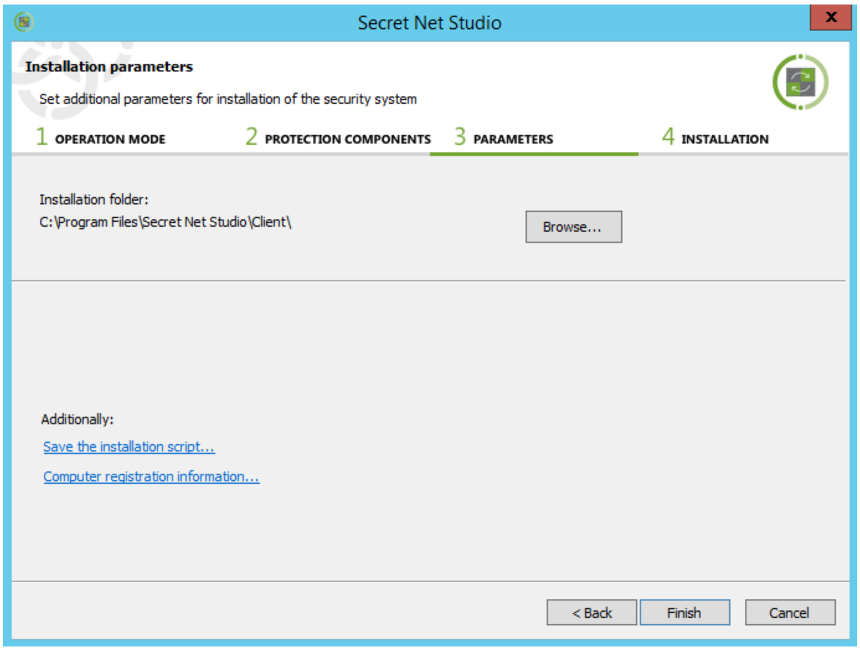
● add a new license

Component	License	State
☑ Base Protection	200 inst, till 31.12.18 (d.	Obligatory component
☑ Discretionary Access Control	200 inst, till 31.12.18 (d.	
☑ Data Wipe	200 inst, till 31.12.18 (d.	
☑ Device Control	200 inst, till 31.12.18 (d.	
☑ Application Execution Control	200 inst, till 31.12.18 (d.	Enabling this protective mechanism on the domain controller is not
☑ Mandatory Access Control	200 inst, till 31.12.18 (d.	Enabling this protective mechanism on the domain controller is not
☑ Printer Control	200 inst, till 31.12.18 (d.	Enabling this protective mechanism on the domain controller is not
☑ Firewall	200 inst, till 31.12.18 (d.	
☑ Intrusion Detection	200 inst, till 31.12.18 (d.	Enabling this protective mechanism on the domain controller is not
☑ Antivirus	200 inst, till 31.12.18 (d.	

5. In the dialog box, specify the method for obtaining licenses:
   - To get licenses from the Security Server that this computer will be subordinate to, select the "select an available licence from the server" check box.
   - To get licenses from a file (in particular, if the Client is installed for use in the autonomous mode), select the "add a new license" check box.
6. Click Select. If you selected the obtaining licenses from a file, specify the relevant file in the dialog box that appears.

   After the data is loaded, license information appears in the dialog box.
7. In the list, select the subsystems that will be installed and for which there are free licenses (the Basic Security subsystem can not be disabled). If there are several license groups for the subsystem, you can select the relevant group from the drop-down list.
8. Click Next >.

   A dialog box appears asking you to specify the installation folder for the Client and configure the connection parameters.



Installation parameters

Set additional parameters for installation of the security system

Installation folder:
C:\Program Files\Secret Net Studio\Client\

Additionally:

Save the installation script...

Computer registration information...

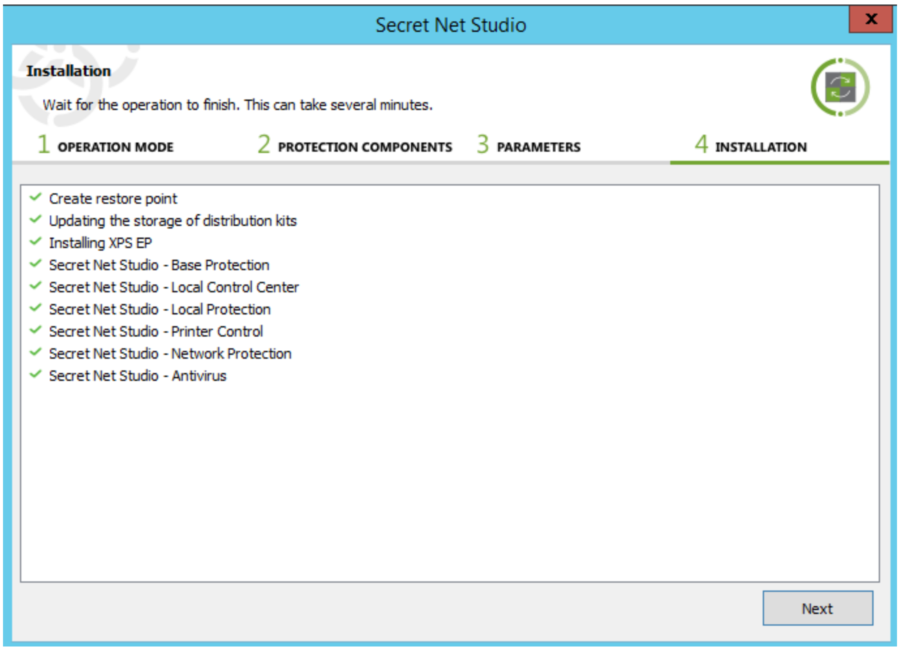
9. In the "Installation folder" field, leave the default folder or specify another one to install the Client.

10. Use the links in the "Additionally" section to perform the following actions (if necessary):

    - To save the specified installation parameters to a file, use the "Save the Installation Script" link. Installation scripts can be used to automate the Client installation on other computers.
    - To enter information about the computer for registration purposes, use the "Computer registration information" link.

11. After all parameters are complete, click Finish.

    The protection subsystems installation begins according to specified parameters.



✓ Create restore point
✓ Updating the storage of distribution kits
✓ Installing XPS EP
✓ Secret Net Studio - Base Protection
✓ Secret Net Studio - Local Control Center
✓ Secret Net Studio - Local Protection
✓ Secret Net Studio - Printer Control
✓ Secret Net Studio - Network Protection
✓ Secret Net Studio - Antivirus

12. After the installation is complete, click Next.

    The final dialog box with the information about the performed operations appears asking you to restart the computer.

13. Check the list of devices connected to the computer. Disconnect the devices that you want to be prohibited.

Attention!
When you first boot the computer with the newly installed Client, the current hardware configuration will automatically accepted as the reference configuration. Therefore, you should disconnect the devices that should be prohibited and then restart the computer.

14. Restart the computer.

Chapter 3
Installing the Client centrally

You can install the Client centrally from the Control Center (see [**4**]). The Control Center is used to create deployment tasks and lists of software to be installed.

Then the software is automatically installed on the Client computers in the background. The Client computer user recieves notifications about the start and the end of the installation process. When the process is complete, the user is asked to restart the computer.

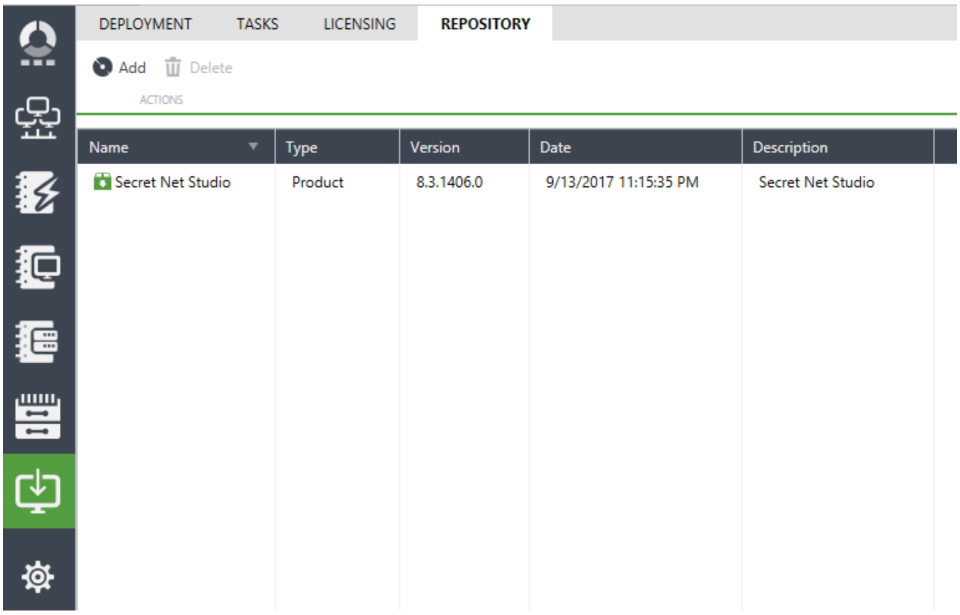
> ⚠ **Attention!**
> Before you start installing the Client, make sure computers meet the hardware and software requirements (see p. 7). In particular, the following ports must be allowed in order to access shared resources: 137, 138, 139, 445. By default, the firewall blocks these ports if there are no shared folders on the computer.

Creating a list of centrally installed software

By default, the list of centrally installed software is empty. You need to add a distribution kit to the list to configure the deployment task. A distribution kit can be added using the Secret Net Studio system setup disk or a special patch.

To add a distribution kit to the list of centrally installed software:

1. On the Deployment tab, click Repository.



Name	Type	Version	Date	Description
Secret Net Studio	Product	8.3.1406.0	9/13/2017 11:15:35 PM	Secret Net Studio

2. Right-click anywhere in the list and select Add.

   The Add dialog box appears.

3. In the Source Path field, enter or select the path to the folder containing the distribution kit to create the installation package. For example, if you want to use the Secret Net Studio system setup disk to create the installation package, select the installation disk's root folder.

   After analyzing the contents of the specified folder, the remaining fields in the Add dialog box will be automatically filled.

4. Click Add and wait until the installation package is created (it may take a while for the files to be sent to the Security Server).

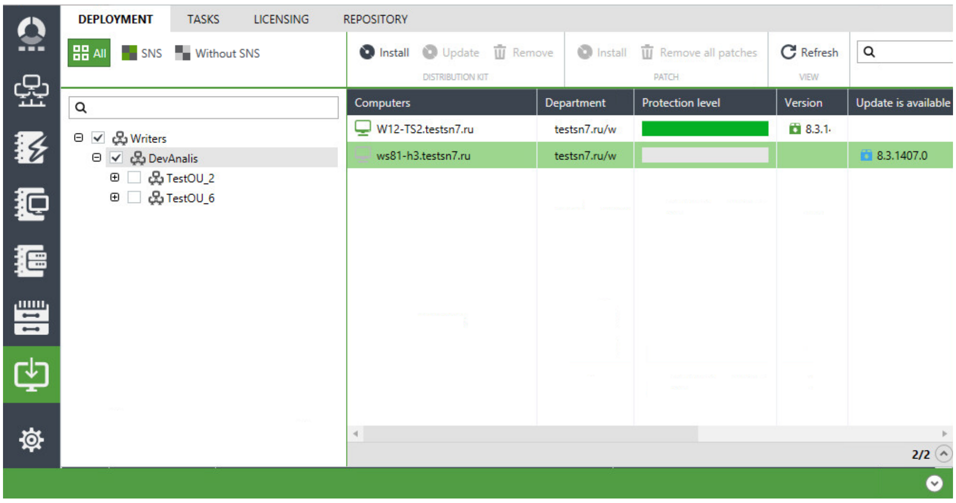
   When the process is complete, a new item appears in the list with information about the installation package.

Creating deployment tasks

You may add deployment tasks after creating the list of centrally installed software. Tasks define a list of computers where installation will be performed automatically.

To add a deployment task:

1. On the Deployment tab, click Deployment.



Computers	Department	Protection level	Version	Update is available
W12-TS2.testsn7.ru	testsn7.ru/w		8.3.1·	
ws81-h3.testsn7.ru	testsn7.ru/w			8.3.1407.0

2. Select computers the task should be created for. If necessary, use the program mechanisms to filter, sort or view information about computers.

   You may filter computers by installed client software ("DPS" or "Without DPS" buttons) or by using the Domain filter (select containers to highlight their child units), search bar (located above the AD container list and the computer list) or by using column headers.

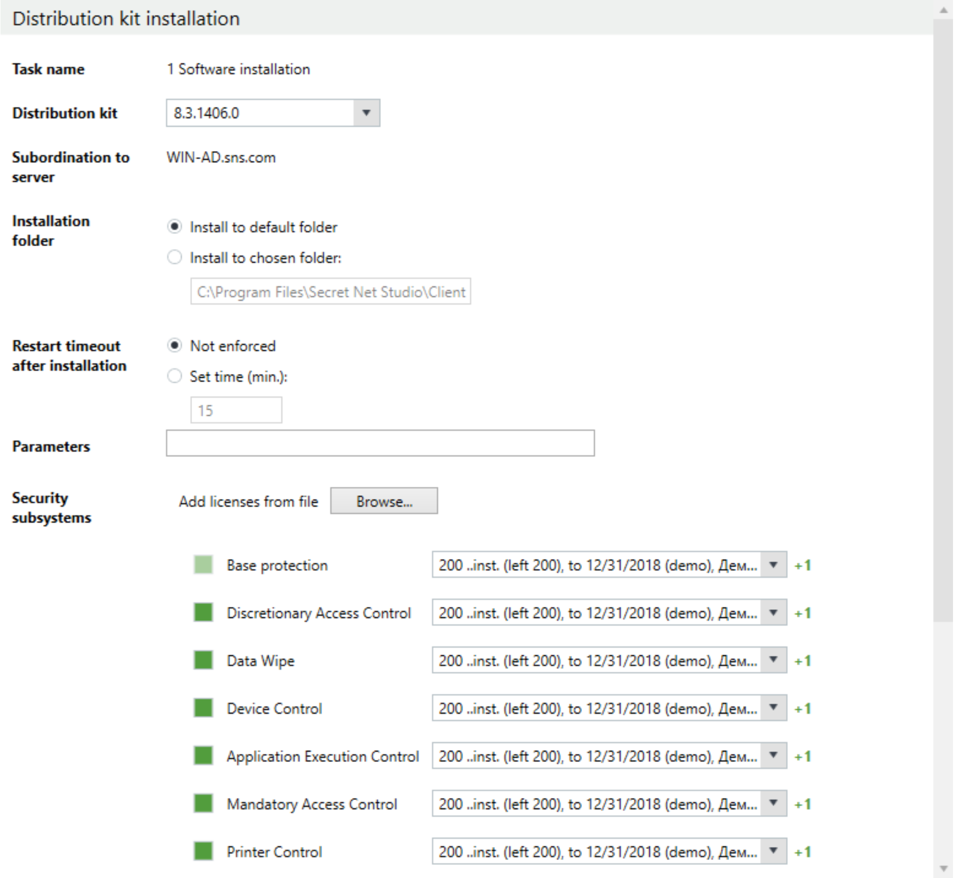
   You may change which columns are displayed on the panel and their order. To configure the columns, right-click on the header row, select Column Settings.

   You may view additional information about computers on the Detailed Panel by clicking on upward arrow located in the bottom right corner of the Deployment Tab.

   Note.
   The Control Center displays detailed information about the Client version and installed subsystems of the computers subordinate to the Security Server the Control Center is connected to. For other computers the Control Center only displays which of them contains the Client. Information about installed subsystems is unavailable in this case.

3. Right-click on one of the selected computers and click the respective command. For example, to install the Client, click Install Software.

   The task settings panel appears on the right of the window as in the figure below.



Distribution kit installation

Task name	1 Software installation
Distribution kit	8.3.1406.0 ▾
Subordination to server	WIN-AD.sns.com
Installation folder	● Install to default folder ○ Install to chosen folder: C:\Program Files\Secret Net Studio\Client
Restart timeout after installation	● Not enforced ○ Set time (min.): 15
Parameters	
Security subsystems	Add licenses from file Browse...

🟩 Base protection	200 ..inst. (left 200), to 12/31/2018 (demo), Дем... ▾	+1
🟩 Discretionary Access Control	200 ..inst. (left 200), to 12/31/2018 (demo), Дем... ▾	+1
🟩 Data Wipe	200 ..inst. (left 200), to 12/31/2018 (demo), Дем... ▾	+1
🟩 Device Control	200 ..inst. (left 200), to 12/31/2018 (demo), Дем... ▾	+1
🟩 Application Execution Control	200 ..inst. (left 200), to 12/31/2018 (demo), Дем... ▾	+1
🟩 Mandatory Access Control	200 ..inst. (left 200), to 12/31/2018 (demo), Дем... ▾	+1
🟩 Printer Control	200 ..inst. (left 200), to 12/31/2018 (demo), Дем... ▾	+1

4. To configure the Client installation task, specify the following settings:
   - version of the software to be installed;
   - software installation folder;
   - component licenses;
   - restart timeout after installation;
   - local administrator account data (a member of the Local Administrators group on selected computers).

   Click Install at the bottom of the panel.
5. After creating a task, on the Deployment panel, click the Tasks tab to check if the element was added.

Chapter 4
Updating and restoring Secret Net Studio

Updating

The Secret Net Studio system can be updated to the latest version. System settings will not be reset as a result of the update. However, some settings may be assigned default values if the previous values could not be saved.

System components are updated individually using the respective setup programs. The Client in network operation mode can be updated using the Security Server.

Centralized updating procedure

Perform the following tasks to successfully update centralized management components of Secret Net Studio:

1. Run all domain controllers.
2. Update the Security Server to the latest version (see p. **25**). If there are several Security Server computers in the security domain, start the update from the computer with the LDS schema master role. By default, this role is assigned to the first installed Security Server.
3. Update the Control Center (see p. **27**) on administrator computers.
4. Update the Client (see p. **27**) in the following order:
   - Security Server computers;
   - employee computers.

   Comment.
   If you need to install updates on a large number of computers, you can do it automatically by installing updates from the Security Server (see p. 22).
5. Check and, if necessary, edit the operational management structure in the Control Center (see [**4**]).

Updating the Security Server

Only a user who is included in the local Administrators group can update the Security Server.

Specific permissions may be required to perform some actions when updating the Security Server. For example, administrative rights may be required for the security domain forest and the security domain. If the user does not have the required permissions, the setup program may ask for the account data of a user with the required access rights during certain stages of the installation process.

Attention!
The update process must be completed without interruptions. If errors occur when replacing the modules and modifying the database structures (for example, when there are no permissions or services are not available), the Security Server can not be restored to the previous state (the state before the update). In this case, you need to manually restore the Security Server from a backup or reinstall the current version of the Security Server. The minimum prerequisites for a successful update are as follows:

- the previous version of the Security Server must be in working order;
- to update the Security Server in the domain forest for a first time, you must have security domain forest administrator permissions;
- you must have security domain administrator permissions.

To update the Security Server:

1. Insert the Secret Net Studio system setup disk into the disk drive. Wait until the installer welcome window appears (see p. **9**) and click the "Security Server" command.

Note.
You can start the update manually without using AutoRun. To do this, run the following file from the setup disk: \Setup\Server\x64\setup.en-US.exe.

When the setup program starts, the computer is checked for compliance with the software and hardware requirements for installing the component. The state of the built-in User Account Control (UAC) mechanism is checked during this stage.

Attention!
If UAC is enabled, a dialog box appears asking to temporary disable it. Click Yes to disable the mechanism, then restart the computer and start the Security Server update process again.

Once the check is complete, a dialog box appears, in which you can view the results of the check.

2. Click Update.

   A warning appears, in which you can view requirements for a successful update, and a request to continue the update.

3. Click Yes.

   The setup program begins its preparations and then a welcome dialog box appears.

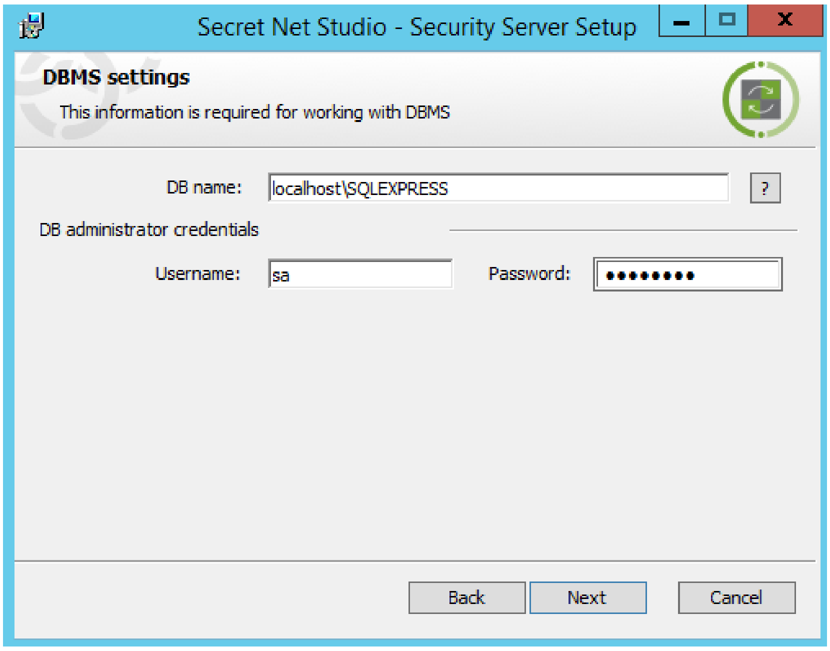
Note.
Before performing any further actions, exit the installer by clicking Exit.

4. Click Next.

   The license agreement dialog box appears.

5. Read the license agreement, and if you agree with all its terms, select the accept check box and then click Next.

   The "DBMS settings" window appears as in the figure below.



Secret Net Studio - Security Server Setup

DBMS settings

This information is required for working with DBMS

DB name: localhost\SQLEXPRESS

DB administrator credentials

Username: sa

Password: ●●●●●●●●

6. In the "Data administrator credentials" group of fields, enter the username and password of the database administrator and click Next.

   The "Preparation completed. Update can be started" dialog appears.

7. Click Update.

   The update begins.

   Once the update is complete, you will be asked to restart the computer.

8. Restart the computer.

Attention!
A new Security Server instance may appear in the operational management structure with a slight delay. In the Control Center that is connected to another Security Server, the updated structure with the new Security Server may appear a few minutes after installing the Security Server (this may take about 10-15 minutes).

Updating the Control Center

You must be included in the local Administrators group can to update the Control Center. To perform the update, use the setup disk (see p. **18**). Updates are performed as usual.

Updating the Client

You must be included in the local Administrators group to update the Client.

Specific permissions may be required to perform some actions when updating the Client. For example, administrative rights to the security domain may be required, if the Client is subordinate to the Security Server. If the user does not have the required permissions, the setup program may ask for the account data of a user with the required access rights during certain stages of the update.

To update the Client:

1. Insert the Secret Net Studio system setup disk into the disk drive. Wait until the installer welcome window appears (see p. **9**) and click the "Security Components" command.

   Note.
   You can start the update manually without using AutoRun. To do this, run the following file from the setup disk (depending on the OS):
   - on a computer running a 64-bit version of Windows: \Setup\Client\x64\SnSetup.en-US.exe;
   - on a computer running a 32-bit version of Windows: \Setup\Client\Win32\SnSetup.en-US.exe.

   The setup program begins its preparations and then a welcome dialog box appears.

   Note.
   Before performing any further actions, exit the installer by clicking Exit.

2. Click Finish.

   The update begins.

3. When the update is complete, click Next.

   The final dialog box appears providing information about the operations performed and asking to restart the computer.

4. Check the devices connected to the computer. Disconnect the devices that you want to be prohibited.

   Attention!
   When you first boot the computer with the newly installed Client, the current hardware configuration will automatically accepted as the reference configuration. Therefore, you should disconnect the devices that should be prohibited and then restart the computer.

5. Restart the computer.

Restoring

You can restore Secret Net Studio using the distribution kit of the same version as was installed on the computer.

You must be included in the local administrator group to restore Secret Net Studio.

Note.
The Security Server from the current release cannot be restored.

Restoring the Client

To restore the Client, follow the interactive Client installation procedure (see p. **18**) or reinstall the System from the Programs and Features utility of Windows. Wait for the setup program to start and click the respective command in the dialog box.

To restore the Client:

1. In the next dialog box, select the Repair check box and click Finish.

   The reinstallation process begins. A progress bar appears showing the progress of reinstallation process.
2. When the reinstallation is complete, click Next.

   The progress report appears.
3. Restart the computer.

Restoring the Control Center

To restore the Control Center, follow the Client installation procedure (see p. **18**). Wait for the welcome dialog box to appear and click the respective command.

To restore the Control Center:

1. In the dialog box, click Repair.

   A dialog appears notifying you that the System is ready to reinstall the Control Center.
2. Click Restore.

   The installer starts copying files to the hard disk and registering the components in the Windows registry. A progress bar appears showing the progress of re-installation process.

   After successful reinstallation, the Installation Complete dialog box appears.
3. Click Finish.

Chapter 5
Uninstalling Secret Net Studio

> **Warning!**
> If confidential or encrypted information is stored on protected computers, make sure it is secure and saved before uninstalling Secret Net Studio.

Uninstallation procedure for network operation mode

We recommend you to uninstall the Client in network operation mode and centralized management components in the following order:

1. Uninstall the Client from all computers.
2. Uninstall the Control Center from administrator computers.
3. Uninstall the Security Server.

Uninstalling the Client

The Client can be uninstalled locally or in a terminal session. The Client in network operation mode can be uninstalled centrally. Centralized uninstallation is performed using the Control Center (see [**4**]). To do this, create software uninstallation tasks in the Control Center similar to deployment tasks (see p. **23**).

The procedure for the local uninstallation of the Client is described below.

You must be included in the local administrator group to uninstall the Client.

To uninstall the Client:

1. Run the interactive Client installation (see p. **18**) or use Programs and Features utility of Windows to remove the Client.

   The setup program starts the preparation procedures, after which a dialog box appears asking you to select further options.
2. In the dialog box, select the Remove check box and enter the account data of the security domain administrator.

   > **Comment.**
   > If the current user has a permission to write to the centralized management object storage proceed to the next step. Otherwise, select the "use the following username and password" check box and enter the account data of a user who has the required permissions.
3. Click Finish.

   The uninstallation process begins.
4. When the uninstallation is complete, click Next.

   The progress report appears.
5. Restart the computer.

Uninstalling the Control Center

In order to uninstall the Control Center, use the Programs and Features utility of Windows.

Uninstalling the Security Server

When uninstalling the Security Server, keep in mind that all computers that were subordinate to this server will become free, i.e. they will not be subordinate to any server.

Specific permissions may be required to perform some actions when uninstalling the Security Server. For example, you may need the security domain administrator rights. If a user perfoming the uninstallation does not have the required permissions, the setup program will ask for the account data of a user with the required rights during certain stages of the process.

To uninstall the Security Server:

1. In the Programs and Features utility of Windows, select the Security Server and click Remove.

   A confirmation dialog box appears.
2. Click Yes.

   The setup program checks the current state of the built-in User Account Control (UAC) mechanism in Windows. The following scenarios are possible:

   - If UAC is enabled, a dialog box appears asking you to temporarily disable it. Click Yes to disable the mechanism, then restart the computer and run the Security Server uninstallation process again (see step **1**).
   - If UAC is disabled, the uninstallation process continues to run, and a dialog box appears providing information on the progress of the process. The "Database removal" dialog box appears during the stage of selecting actions concerning the Security Server database.
3. Choose an option:

   - Click Cancel if you do not want to delete the database.
   - To delete the database, enter the database administrator name and password in the respective fields and click OK.

   The uninstallation process continues. A confirmation dialog box asking whether you want to delete the certificate appears during the stage of selecting actions concerning the Security Server certificate.
4. To delete the Security Server certificate from the IIS, click Yes in the confirmation dialog box. To keep the certificate in the IIS, click No.
5. When the uninstallation is complete, restart the computer.

Uninstalling the Client subsystems

If some of the Client subsystems are not needed, they can be uninstalled locally or in a terminal session. The following subsystems can be uninstalled:

- antivirus;
- network protection group and intrusion detection module;
- local disk protection and data encryption;
- printer control;
- local protection group (with the exception of the above subsystems).

In addition, you can uninstall the local Control Center.

You must be included in the local administrator group to uninstall subsystems.

To uninstall the Client subsystems:

1. Run the interactive client installation (see p. **18**) or use the Programs and Features utility of Windows to uninstall a subsystem.

   The setup program starts the preparation procedures, after which a dialog box appears asking to select further options.
2. Select the Remove Components check box in the dialog box and click Next.

   A dialog box appears asking to select subsystems to be uninstalled.
3. Select the subsystems and click Finish.

   The uninstallation process begins.
4. When the uninstallation is complete, click Next.

   The progress report appears.
5. Restart the computer.

Appendix

Software for supported USB keys and smart cards

To use supported USB keys and smart cards in the Secret Net Studio system, you need to install additional software from respective device manufactures. The software can be installed from the Secret Net Studio system setup disk. Folders with the software setup files are listed in the table below.

Tool type	**Folders with setup files**
USB keys and smart cards	
Rutoken S, Rutoken EDS, Rutoken Lite	\Tools\Tokens\RuToken\
JaCarta PKI, JaCarta PKI Flash, JaCarta GOST, JaCarta GOST Flash	\Tools\Tokens\Aladdin\JaCartaUC\
eToken PRO (Java)*	\Tools\Tokens\Aladdin\JaCartaUC\ + \Tools\Tokens\Aladdin\eToken\
ESMART Token, ESMART Token GOST	\Tools\Tokens\eSmart\
Smart card readers	
Athena ASEDrive	\Tools\Tokens\Aladdin\Acedrv\

* To use eToken identifiers when working with standard Microsoft certificates, you need to additionally install the set of SafeNet Authentication Client drivers and utilities provided by the manufacturer.

Registry changes during the Client installation

The Client setup program makes the following changes in the standard settings of the registry:

Settings name	**Type**	**Value**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\		
NoDriveTypeAutoRun	DWORD	0xFF

Client installation folder

When installing the Client, the SNINSTALLDIR system variable is created, where the path to the client installation folder is written; this variable contains the path to the Client installation folder. Additionally, the access rights listed in the following table are defined for the Client installation folder.

Object Name	**Access Rights**
%SNINSTALLDIR%	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%SNINSTALLDIR%\icheck	Administrators: FullControl SYSTEM: FullControl

Installing and configuring MS SQL DBMS

MS SQL server must be installed in accordance with the manufacturer's requirements. The list of requirements is available on the following Microsoft webpages:

- http://technet.microsoft.com/ru-ru/library/ms143506%28v=sql.120%29.aspx (for SQL Server 2014);
- http://technet.microsoft.com/ru-ru/library/ms143506%28v=sql.110%29.aspx (for SQL Server 2012);
- http://technet.microsoft.com/ru-ru/library/ms143506%28v=sql.105%29.aspx (for SQL Server 2008 R2).

In particular, before installing the MS SQL server, the .NET Framework component of the respective version and the language pack for the component must be installed.

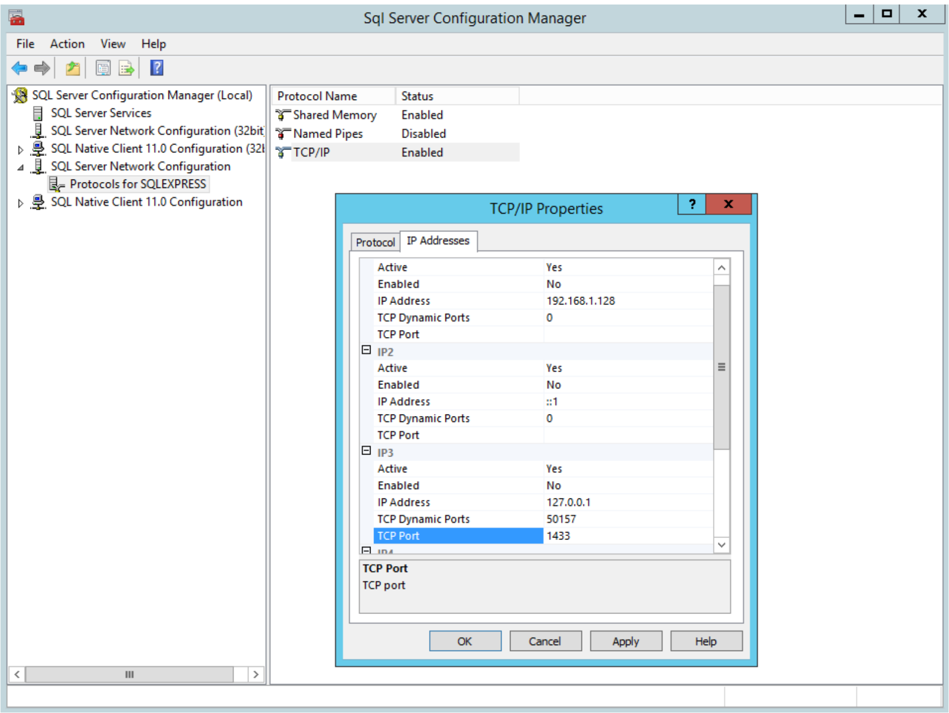
The setup disk contains the installation tools of MS SQL Server 2012 SP1 Express. The general procedure for installing the MS SQL server using the tools is as follows (using Windows Server 2008 R2 as an example):

1. Enable .NET Framework 3.5 in the OS.
2. Install .NET Framework 4.5. To do this, run the dotNetFx45_Full_x86_x64.exe file from the following folder: \Tools\Microsoft\Prerequisites.
3. Install the language package for .NET Framework 4.5. To do this, run the dotNetFx45LP_Full_x86_x64ru.exe file from the same folder.
4. Install MS SQL server. To do this, run the SQLEXPRWT_x64_ENU.exe or SQLEXPRWT_x86_ENU.exe file (depending on the OS bitness) from the following folder: \Tools\-Microsoft\SQL Server 2012 SP1 Express.

Correct interaction between the Security Server and MS SQL DBMS is ensured by enabling authentication mode to authenticate the SQL Server and Windows. For this purpose, enable mixed authentication mode on the MS SQL server.

If MS SQL server is installed on a separate computer (not on the Security Server computer), the following conditions must be met:

- if the MS SQL server is installed on a separate computer, then you can use port 1433 for DBMS connection in the firewall (if enabled). Moreover, the port on the MS SQL server must be opened for incoming connections; on the Security Server, the port must be opened for outgoing connections.
- TCP/IP must be enabled. Default mode is disabled when using SQL Server Express. This mode is managed by the SQL Server Configuration Manager included in the MS SQL Server software package. To enable this mode, go to the SQL Server Network Configuration / Protocols for <*database_instance_name*> section and open the setup window for "TCP/IP" element properties. In the "Protocol" dialog box, select "Yes" for the "Enabled" parameter; in the "IP Addresses" dialog box, check the values of "TCP Dynamic Ports" and "TCP Ports" parameters for all IP addresses: the parameters must be assigned an empty value and "1433", respectively. The "TCP/IP Properties" window is shown in the figure below.


Sql Server Configuration Manager
File Action View Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32l
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 11.0 Configuration
TCP/IP Properties
Protocol
IP Addresses
OK
Cancel
Apply
Help

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled

Active	Yes
Enabled	No
IP Address	192.168.1.128
TCP Dynamic Ports	0
TCP Port	
IP2	
Active	Yes
Enabled	No
IP Address	::1
TCP Dynamic Ports	0
TCP Port	
IP3	
Active	Yes
Enabled	No
IP Address	127.0.0.1
TCP Dynamic Ports	50157
TCP Port	1433

TCP Port
TCP port

Note.
If tracing is used, information about the interaction with the DBMS is stored in SnTrace.log and SB.txt log files which are in the following folder: C:\logs. These files can be used to troubleshoot connection problems.

IIS changes during the Security Server installation

During the Security Server installation, some settings of IIS components are changed. Settings are assigned the values required for the correct operation of the Security Server.

The special website SecretNetStudioSite is created in IIS. The following operations are performed on this website:

- organization of SSL access;
- binding the "https" protocol to "*:443:" addresses.

Note.
The binding is performed during the Security Server installation as well as when generating a new certificate for the Security Server.
Port 443 is required for the Security Server to function properly, so when a new binding is added, all existing bindings to this port on other IIS sites deployed on this computer are deleted. In this regard, other sites and applications that use IIS and port 443 may not function correctly.

Values for the following setting are set in the SecretNetStudioAppPool:

Settings name	**Value**
Section (general)	
queueLength	10000
Section: processModel	
identityType	ApplicationPoolIdentity
idleTimeout	0.00:00:00
pingingEnabled	false
Section: recycling	
periodicRestart.memory	0
periodicRestart.privateMemory	0
periodicRestart.time	0.00:00:00
periodicRestart.requests	0
periodicRestart.schedule	disabled

Values for the following settings are set in the website sections:

Settings name	**Value**
Section of the system.webServer/serverRuntime site	
appConcurrentRequestLimit	100000
uploadReadAheadSize	104857600
Site section: windowsAuthentication	
enabled	true
Site section: anonymousAuthentication	
enabled	false
Section of the handlers site	
accessPolicy	Read, Execute

Settings change for the connection of the Security Server to the DBMS server

The Security Server connects to the database on the DBMS server using the account data specified when the Security Server was installed. If necessary, these settings can be edited without reinstalling the Security Server.

Account data

If the name and/or password of the account were changed by DBMS tools, new account data must be synchronized in the Security Server configuration file in order to ensure access to the database. This new account data entry procedure is performed on the Security Server computer.

To change the account data used by the Security Server:

1. In the Security Server installation folder, run the OmsDBPasswordChange.exe file.

   The account data change program dialog box appears.

   The program will automatically define the location of the configuration file that is used by the Security Server and will display the full path to the file.
2. If necessary, specify another location for the configuration file (for example, edit the backup copy of the main file). To do this, click the button on the right-hand side from the current path line and specify the file in the Windows file selection dialog box.
3. Enter the new name and password in the respective fields: Username (by default contains the name retrieved from the configuration file), Password and Confirm Password.
4. Click Save Changes.
5. Restart the computer after updating the main configuration file used by the Security Server.

Connection string

The connection string used for a database connection contains the name or IP address of the DBMS as well as the name of the database instance on this server and the port to connect to that instance. If necessary, edit connection settings in the Security Server's configuration file. For example, if the database has been moved to another DBMS server.

Note.
Once the database is migrated to another DBMS server, you can use the DBMS tools to create an account on the new server to connect the Security Server to the database. Once the account is created you can edit the account data in case of the name and/or password of the new account differ from the name and password of previous account (see above).

To edit the connection settings:

1. In the Security Server setup folder, open the ServerConfig.xml file.
2. Find the DB element containing the dataSource attribute.
3. Edit the dataSource attribute. The connection string has the following format: dataSource="< *name_ or_ IP_ of_ the_ MS_ SQL_ server* >\< *name_ of_ the_ database_ instance*>,<*port*>"

   Note.
   You do not need to specify the port number if the default port is used.
4. Save the changes, close the configuration file and restart the computer.

Specific features of the standby Security Server

To ensure the continuous operation of protected computers that are subordinate to the Security Server, you need to provide for a standby Security Server within the same security domain. The standby Security Server must always be available for regular synchronization with the main server.

In case of the main Security Server failure, computers do not get reassigned automatically to the standby Security Server. Assignment to the standby Security Server can be performed in the Control Center(see [**4**]). To do this, unassign computers from the previous Security Server and assign them to the standby Security Server.

After the reassignment, computers may fail to detect the new Security Server. This may be a result of the unavailability of the Security Server or the absence of information about it in local storage. For example, if the standby Security Server is installed, and the main Security Server fails while the Client's computer is not connected. In this case, the agent on the computer will not be able to detect the new Security Server. Therefore, it will not operate correctly. In particular, login problems may occur in advanced authentication mode and in other security mechanisms.

Options for restoring an incorrectly removed Security Server

If the Security Server was removed incorrectly, the standard installation of a new Security Server may be impossible due to errors. Also, errors may occur if the con-figuration of the operational management structure changes.

Causes of the incorrect deletion of the Security Server may vary. For example, it may happen due to an error when the setup program is running in removal mode or if there is a hard disk failure on the Security Server computer. In order to ensure normal operations, extra measures are required for the restoration of the system state you need.

Transfer of the LDAP schema master role to another Security Server

One of the servers must be assigned the LDAP schema master role for the directory service. By default, this role is assigned the first installed Security Server.

If the schema master was deleted incorrectly, you cannot install new Security Servers in the system or perform other configuration procedures that require synchronization between the Security Servers.

To fix the problem, you need to make the Security Server available again or transfer the LDAP schema master role to another Security Server. The role is transferred by means of the Dsmgmt tool, which is part of Windows.

Attention!
Once the schema master role is transferred to another computer, you cannot use the previous computer in this role. Therefore, the role should be transferred only if it is impossible to restore the Security Server.

To transfer the LDAP schema master role:

1. On the Security Server computer that will be used as the schema master run the command prompt (cmd.exe) as an administrator.
2. Enter the utility start command:

   dsmgmt
3. In the dsmgmt line that appears, enter the management command:

   roles
4. In the fsmo maintenance line that appears, enter the management command:

   connections
5. In the server connections line that appears, enter the management command:

   connect to server <*computer_name*>:<*port_number*>

   Specify the full DNS name in the command parameters of the Security Server computer that will be used as the schema master (or "localhost") and port number 50002.
6. Once connection to the chosen computer is established, in the server con-nections line, enter the following command:

   quit
7. In the fsmo maintenance line, enter the management command:

   seize schema master
8. Once the schema master role has been assigned, close the utility using the quit command.

Documentation

1.	Secret Net Studio. Administrator's manual. Development principles
2.	Secret Net Studio. Administrator's manual. Installation and update
3.	Secret Net Studio. Administrator's manual. Setup and operation
4.	Secret Net Studio. Administrator's manual. Centralized management, monitoring and audit
5.	Secret Net Studio. Administrator's manual. Setup and operation. Local protection
6.	Secret Net Studio. Administrator's manual. Setup and operation. Network protection
7.	Secret Net Studio. Administrator's manual. Setup and operation. Antivirus and intrusion detection tool
8.	Secret Net Studio. User manual