SECURITY code

Secret Net Studio

Getting Started

Administrator guide

© Security Code LLC, 2021. All rights reserved.

All rights to the operating instructions are reserved.

This document is part of the product package, and it is covered by all terms of the license agreement. Security Code LLC prohibits this content from being copied or distributed in any form for commercial purposes without a special written consent of the developer.

Security Code LLC reserves the right to change the information contained herein without special notice.

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

Table of contents

Introduction **4**

Installation **5**

Preparing for installation 5

Select computers 5

Create user groups 6

Install SQL Server 6

Installing the Security Server 7

Installing the Control Center 10

Installing the Client centrally 11

Start the Control Center 11

Create a list of software to install 11

Create deployment tasks 12

Secret Net Studio management **15**

Control Center interface 15

Monitoring and operative management 16

Configuring security settings 17

Operations with centralized logs 17

Documentation **19**

Introduction

This manual is intended for Secret Net Studio administrators. It contains basic information on how to install and manage the software.

This manual is designed Secret Net Studio administrators. It contains information that administrators need to use additional tools and configuration files (hereinafter additional tools) necessary to work with Secret Net Studio.

Conventions

We use conventions to highlight certain text elements.

Internal links refer to the page with the required information.

Notes in the manual contain important and additional information. Icons in the margins reflect the importance of the information the notes contain.

- Additional information (examples, links to other documents, or other parts of the manual).
- Important information.
- Attention.

Exceptions. Some notes may have no icons. Apart from note icons, the margins may also contain other graphical elements, for example, buttons that are explained in adjacent paragraphs.

Information sources

You can go to SECURITY CODE LLC website (https://www.securitycode.net/) or contact the company representatives via email (info@securitycode.ru).

Chapter 1
Installation

Secret Net Studio deployment in a single Active Directory domain containing a Security Server, an administrator workstation and several protected computers is a basic scenario for a quick reference of the product installation.
The installation can be performed in the following order:

1. Preparation for the installation (see below).
2. Installation of the Security Server (see p. **7**).
3. Installation of the Control Center (see p. **10**) on the administrator's workstation.
4. Centralized installation of the Clients (see p. **11**) on all protected computers.

Note.
Additionally Secret Net Studio supports hardware protection tools such as Sobol. This deployment scenario does not include its installation. For information on installing Sobol see document [].

Preparing for installation

Before starting the installation of Secret Net Studio components, perform a number of preparatory actions.

Select computers

Select computers for the Security Server, administrator workstation and Clients deployment in a single Active Directory domain or an organizational unit. Selected computers should comply with the recommended system requirements.

Tip. For detailed information about the system requirements, see document [1]

The Security Server

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

Requirement	Minimum value
CPU	Intel Core i5/Xeon E3 or later
RAM	16 GB
Disk space	150 GB. High-speed hard drive is recommended
Operating system and other software	Windows Server 2019/2016/2012/2012 R2 Rollup Update KB2919355/2008 R2 SP1 KB3033929

The additional requirements are the following:

- 50000–50003 TCP ports must be available on the computer. In case these ports are used by other applications, you will be requested to specify other available ports to be used by the directory service. Moreover, all TCP/UDP ports required for Windows components functioning in an Active Directory domain must be available;
- the English language should be specified as a system language that does not support Unicode;
- the Web server (ISS) role must be enabled on the computer.

The Client and the Control Center

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

Requirement	Minimum value
CPU	According to OS requirements[1]
RAM	2 GB
Disk space	4 GB
Operating system and other software	Windows 10/8.1 Rollup Update KB2919355/7 SP1 KB3033929 Windows Server 2019/2016/2012 R2 Rollup Update KB2919355/2008 R2 SP1 KB3033929 Internet Explorer version 8 or later

In this scenario, the Client is installed centrally under the Security Server control. In this case, if a firewall is enabled, you will need to authorize the following 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. Moreover, all TCP/UDP ports required for functioning of Windows components in an Active Directory domain must be available.

Create user groups

Create two global user groups in a single Active Directory domain using standard Windows administration tools:

- a group of security domain administrators;
- a group of administrators of a security domain forest (users of this group have privileges to create a security domain in the forest).

Required privileges are granted during the Security Server installation.

Include a domain user that will install and work with Secret Net Studio components in these groups.

Include these both groups in the group of local administrators on a computer with the Security Server. The group of security domain administrators must also be included in the group of local administrators on all computers selected for the Client to be installed.

Install SQL Server

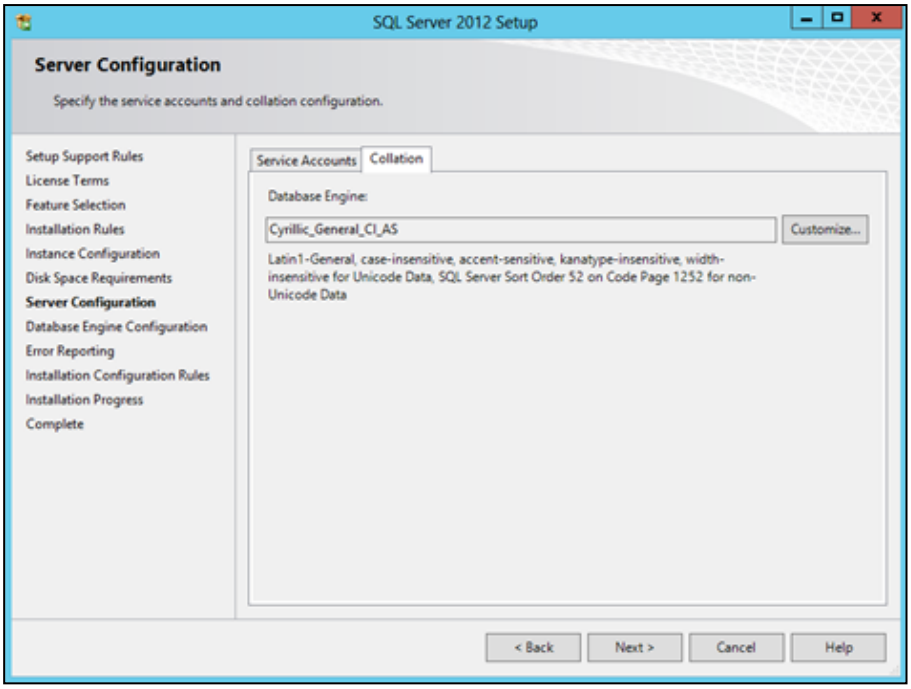
MS SQL is required for the Security Server operation. You can use a free version of MS SQL Server 2012 SP1 Express. In this deployment scenario, the Security Server and SQL Server are installed on the same computer.

Tip. If SQL Server was already installed, it can also be used. For more details, see document [**1**].

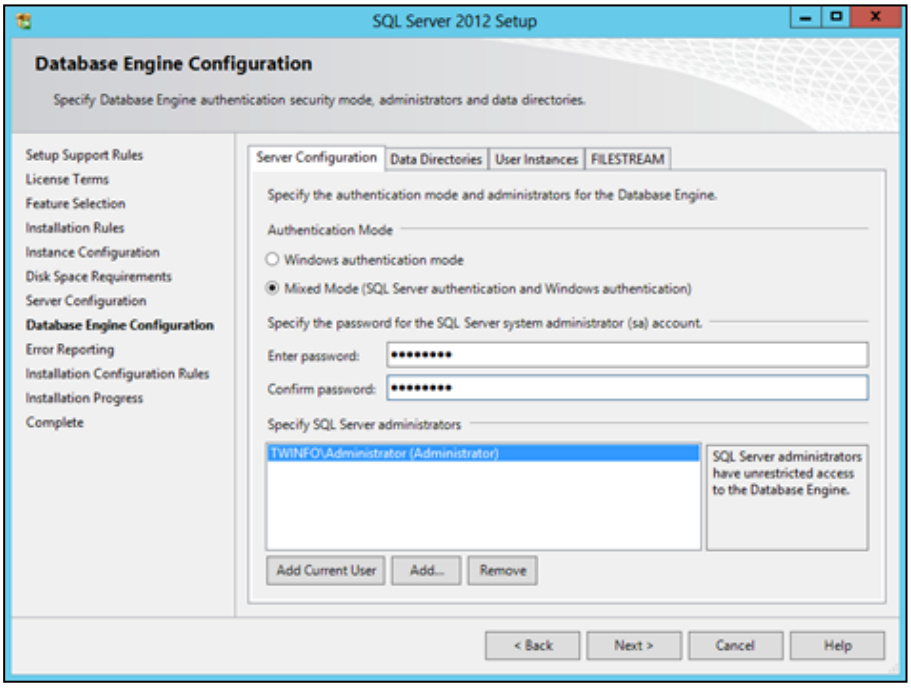
Before installing SQL Server, you must enable NET Framework 3.5 on Windows. On a computer running Windows Server 2008 R2, NET Framework 4.5 with a language pack is also required (installation files dotNetFx45_ Full_ x86_ x64.exe and dotNetFx45LP_ Full_ x86_ x64ru.exe are located in the \Tools\Microsoft\Prerequisites folder).

Install software using default parameters except the following ones that ensure correct interaction between the Security Server and SQL Server.

- To enable Cyrillic sorting support mode for the database instance, in the **Server Configuration** section, go to the **Collation** tab and, in the **Database Engine** text box, type **Cyrillic_General_CI_AS**.



- In the **Database Engine Configuration** section, go to the **Server Configuration** tab and, in the **Authentication mode** section, select **Mixed** mode. It ensures authentication for both SQL Server and Windows.



Tip. For detailed information about the installation and configuration procedures of MS SQL, see document [1].

Installing the Security Server

Log in as a domain user from the local group of administrators on a computer to be used as the Security Server.

To install the Security Server:

1. Insert the Secret Net Studio setup disk into the drive. Wait until the installer welcome window appears and click **Security Server**.

Note. If the autorun dialog box does not appear, you can launch the installation manually. To do so, run **\Setup\Server\x64\setup.en-En.exe** on the installation disk.

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 request to temporarily disable it appears. In this case, to disable UAC, click **Yes**, restart your computer and repeat the Security Server installation.

Upon the check completion, the dialog box displaying the list of components to be installed appears.

2. Do not modify the list and click **Install**.

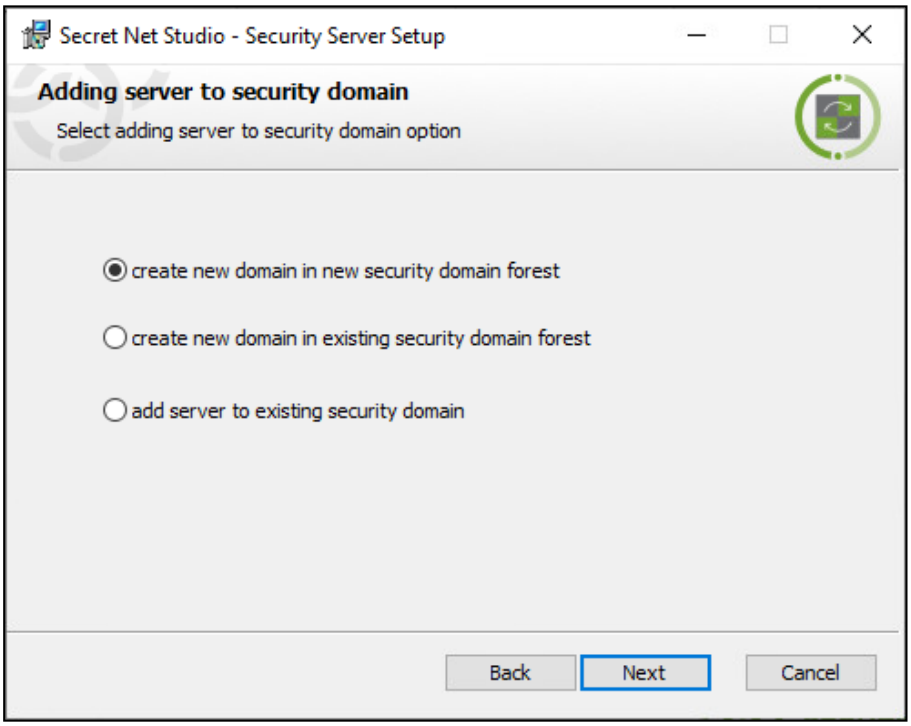
   The setup program begins its preparations and after that the **Setup Wizard** dialog box appears.

3. To continue the installation, click **Next**.

   The **License agreement** dialog box appears on the screen.

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

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



5. Select **create new domain in new security domain forest** and click **Next**.

   The **Authentication server configuration file** dialog box appears.

6. Do not change the parameters, click **Next**.

   The **Security domain configuration** dialog box appears.

7. Select a container to create a new security domain from the drop-down list. Use an organization unit that includes computers selected for the components to be installed on or use any upper unit (including entire AD domain). After you select the container, you can edit a name for the new security domain (if necessary).

8. Click **Next**.

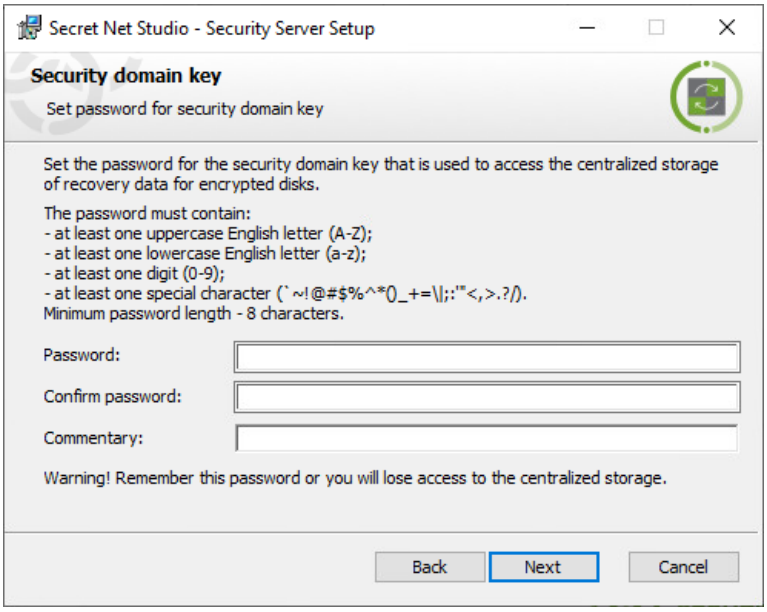
   The **Security administrators group** dialog box appears.

9. Select user groups to grant privileges to manage the security domain and the security domain forest. Click **Next**.

Tip. We do not recommend using the standard Domain Admins group as the group of security domain administrators. Otherwise, an error may occur during the connection to the Control Center server installed on the same computer. This error may occur because of insufficient user privileges.

The **Folder** settings dialog box appears.

10. Leave the default directory to install the Security Server and other destination folders. Click **Next**. The **Security domain key** dialog box appears.

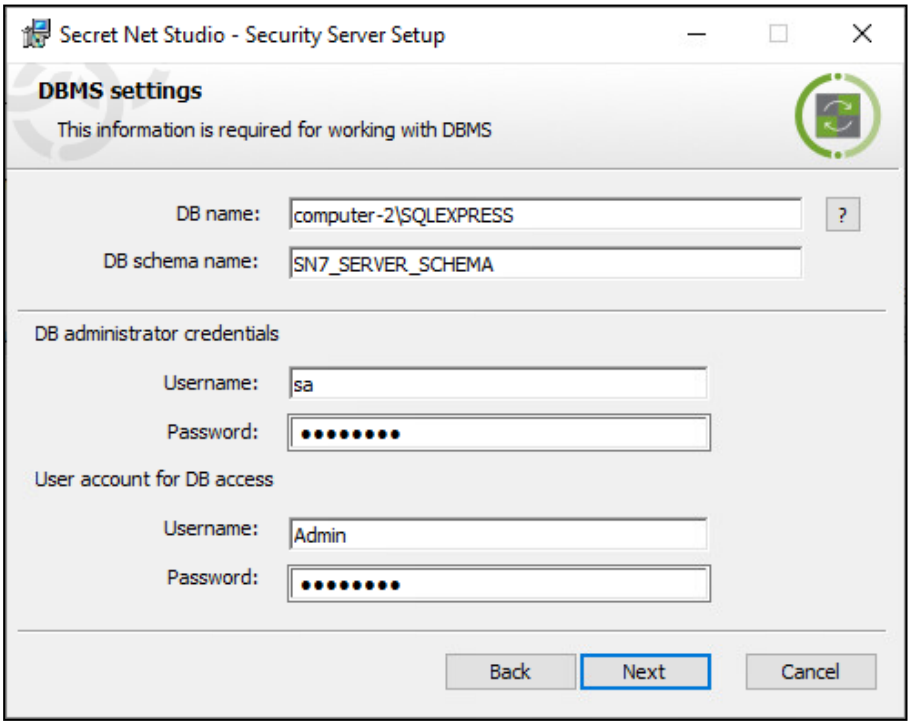


11. Set a password for the security domain key. The key and password are used to access the centralized storage of recovery data for encrypted disks. The password must meet the requirements specified in the dialog box.

Attention! Remember the password for the security domain key. Otherwise, access to the centralized storage of recovery data will be lost.

Confirm the password. If necessary, leave a comment to the password. Click **Next**.

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



12. Perform the following actions:
    - Specify the connection settings for the DB to work with the Security Server:
      - In the **DB name** text box, specify the connection string: **<computer name>\SQLEXPRESS**

        Note. In this scenario, SQL Server is installed with default parameters on a computer with the Security Server. For more details about the connection string, see the document [1].
      - in the **DB schema name** text box, specify the name of the DB schema;
      - in the **DB administrator credentials** group of fields, specify the account data of the DB administrator on the SQL server given during its installation;
      - 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).
    - Click **Next**.

    The **Organization name** dialog box appears on the screen.
13. Specify the organization name and unit that will maintain the Security Server being installed and click **Next**.
14. Click **Install**.

    The setup program begins copying files to the hard disk and registering the components in the **Windows registry**. A progress bar, showing the installation progress , appears.

    After the installation and setting are finished successfully, the **Installation complete** dialog box containing a list of performed operations appears. You will be prompted to restart the computer.
15. Click **Restart**.

Tip. For details about different ways of the Security Server installation, see the document [1] . If this Security Server is not to be used only for information purposes, but also to establish a security system, we recommend creating the second (reserve) Security Server in a created Secret Net Studio security domain.

Installing the Control Center

Log in to a computer selected as security administrator workstation. Use a domain user account included in a group of security domain administrators performing preparatory actions.

To install the Control Center:

1. Insert the Secret Net Studio setup disk into the drive. Wait until the installer welcome window appears and click **Control Center**.

   Tip. If **AutoRun** does not start, you should run the installation manually:
   - on a computer running 64-bit Windows — execute **\Setup\Console\x64\setup.en-US.exe**;
   - on a computer running 32-bit Windows — execute **\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 click **Next**.

   The **Destination Folder** dialog box appears.
4. Leave the default destination directory or specify another one and click **Next**.

   A dialog box notifying you that everything is ready for installation appears.
5. Click **Install**.

The installation process begins. A progress bar, showing the installation progress, appears. After the installation is finished successfully, the **Installation complete** dialog box appears.

6. Click **Finish**. In the appeared dialog box, click **Close**.

Attention! After installing the Control Center, you must install patch 8.5.5329.40 located on the installation disk in \Tools\SecurityCode\ManualPatches\8_5_5329_40_Inc76262_Build27. Without installing this patch the self-protection administrator PIN will work incorrectly and the new **administrative privilege control** feature will be unavailable.

Now you can start the installation of the Clients.

Installing the Client centrally

Centralized installation is controlled by the Security Server. The list of software to be installed along with deployment tasks are created in the Control Center.

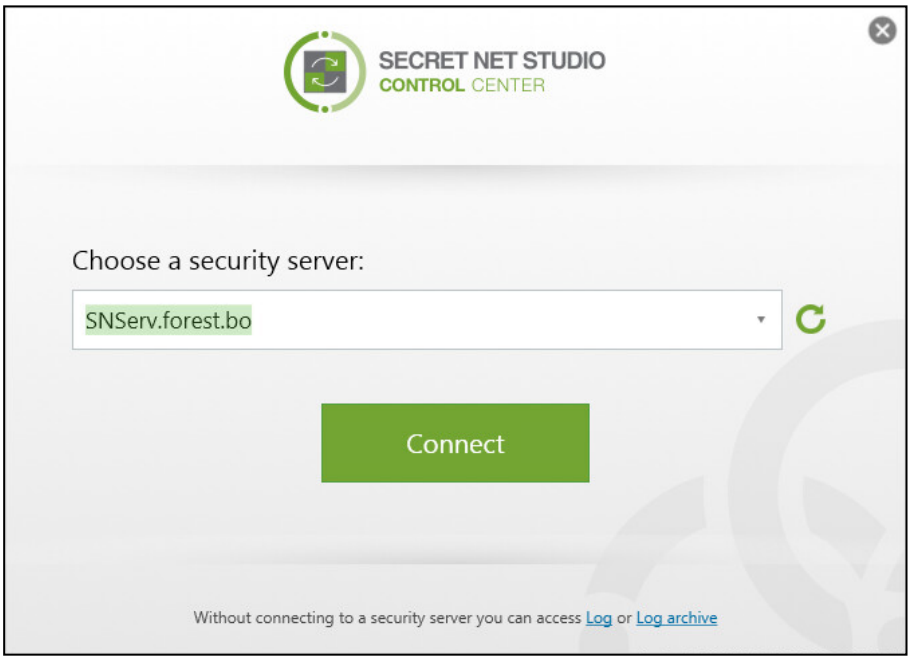
Attention! To successfully perform all procedures described below, a user should be included in a group of security domain administrators.

Start the Control Center

To start the Control Center:

1. In the **Start** menu, in the **Security Code** group, click **Control Center**.

   A dialog box appears as in the figure below.



2. In the **Choose a security server** text box, enter the name of an installed Security Server. To refresh the list of servers, click the respective button on the right.
3. Click **Connect**.

After that, the main window of the program appears.

Create a list of software to install

By default, a list of software to be installed centrally is empty. You can add a set of setup files to the list.

The first time you run the **Control Center**, a message box prompting you to start the system operation and proceed to the installation of the Clients appears.

To add a set of setup files:

1. Go to **Deployment**.

The **Deployment** panel and a message prompting you to add a Secret Net Studio distribution kit appear on the main window of the Control Center.

2. Click **Add**.

   The **Add distribution kits** dialog box appears.

3. Insert the Secret Net Studio setup disk into a drive, click **Add**. In the appeared dialog box, specify the root folder of the setup disk and click **Select Folder**.

   After processing contents of the specified folder, the information about the selected setup disk appears in the **Add distribution kits** dialog box.

4. Click **Apply**.
   The progress bar appears in a new dialog box. Wait until the process completes.

5. Click **Close**.

   On the **Repository** tab, a new element appears in the list. It contains information about the uploaded set of setup files.

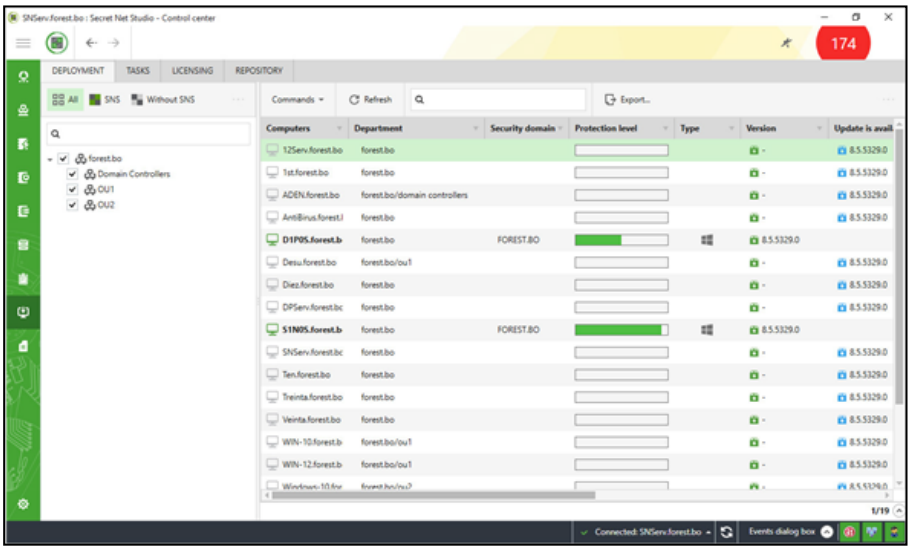
Create deployment tasks

After you create a list of software to be installed centrally, you should create a deployment task. The task defines a list of computers where the required actions are performed automatically.

Attention! For centralized installation of software on computers, a user should have local administrator privileges on these computers. While performing preparatory actions, a group of security domain administrators should be included into local groups of administrators. A domain user included in this group should have all needed privileges.

To add a deployment task:

1. On the **Deployment** tab, click **Deployment**.

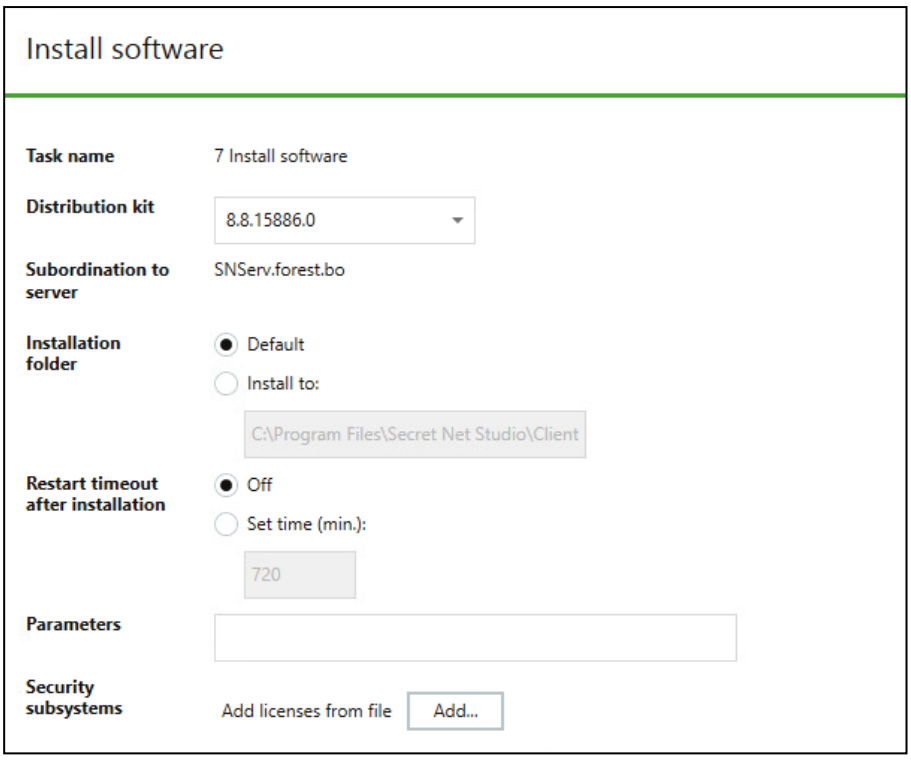


2. Select AD containers with the required computers from the list on the left. Select the computers where the Client should be installed from the list on the right.

   Tip. You can select several computers if you press **Ctrl** or **Shift**.

3. Right-click one of the computers, click **Install software**.

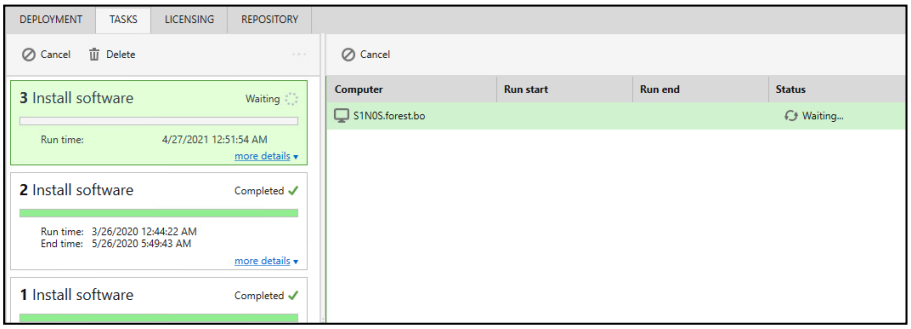
   The task settings panel appears on the right of the window as in the figure below.



4. To enable automatic restart mode, in the **Restart timeout after installation** group, select **Set time** and specify a timeout (in minutes) for automatic system restart.
5. To add product licenses, in the **Security subsystems** group, click **Browse** and select a file with the licenses provided by the supplier.

   After data is loaded, the respective license information appears in the group.
6. In the **Name** and **Password** text boxes, type credentials of a user account that has local administrator privileges on the selected computers.

   Tip. Use an account of a domain user included in a group of security domain administrators while performing preparatory actions.
7. Click **Install** at the bottom of the panel.
8. Go to the **Tasks** tab to see the progress of the task being performed.



   The data about progress and status of installation process is displayed on this tab.

   Tip. To view additional information about the task, click **more details** on the bottom of the information block. To view detailed information about all computers, click the button with an arrow on the right bottom of the computer list.

Software installation is performed automatically in a background mode on the protected computers. A user is notified about the start and the end of the installation.

After the Clients are installed successfully and computers restart, you can see them in the structure as objects subordinate to the Security Server.

Chapter 2
Secret Net Studio management

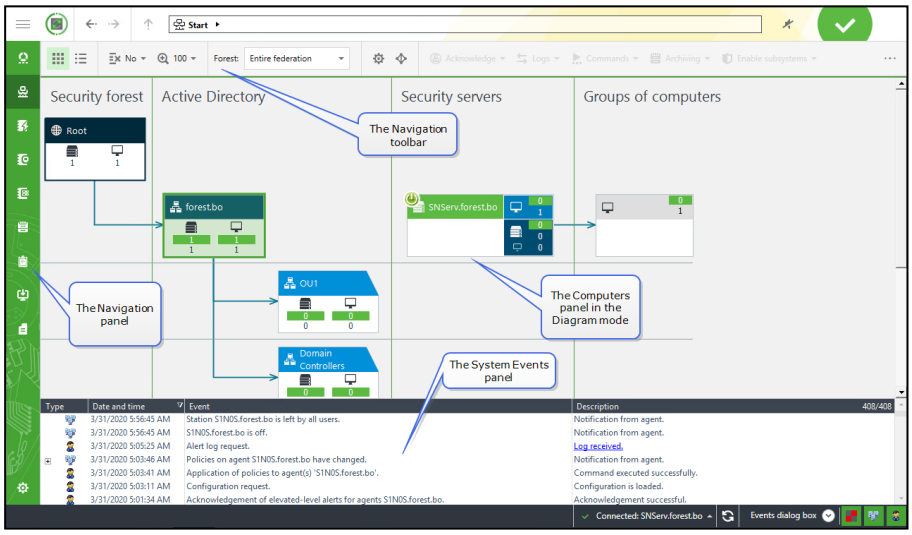
The Control Center is used for centralized management of protected computers (for more details about running the Control Center, see p. 11). It provides the following options:

- configuration of security parameters and management of computers;
- monitoring of system status;
- configuration of Secret Net Studio network structure;
- operations with centralized logs.

Note. The Local Control Center is installed on a computer as a part of the Client. This mode provides local configuration of security parameters, management of mechanisms and viewing local logs of the computer. Centralized management is not available in this mode.

Control Center interface

The Control Center interface is shown in the figure below.



The Control Center interface contains the following parts:

- the navigation panel is on the left of the main window and contains shortcuts to control panels and the Control Center configuration tools;
- the **Computers** panel displays a network structure and provides objects management;
- the **System events** panel displays the list of events registered by Secret Net Studio;
- the navigation toolbar contains buttons for configuring network structure display and other commands.

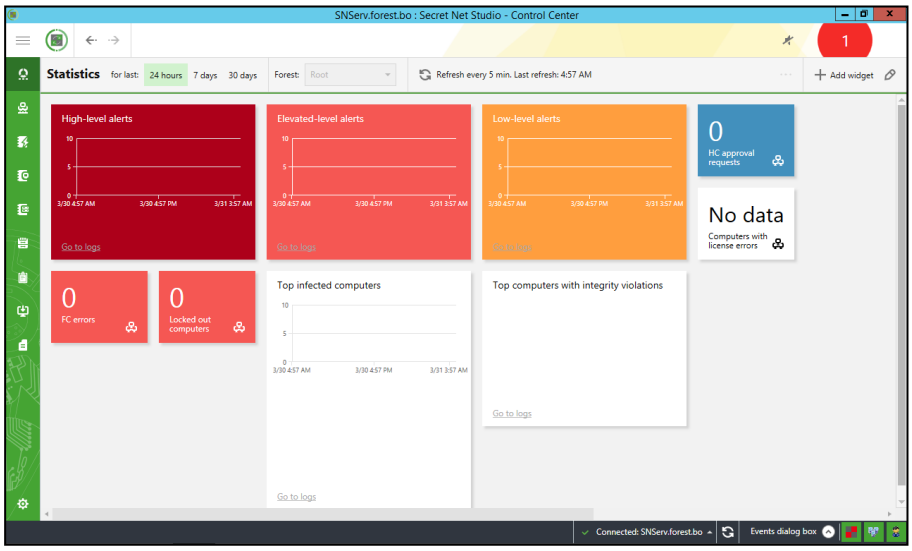
The Control Center contains the following control panels:

Control panel	Description
Dashboard	Contains widgets. A widget is an interface element that displays the status of a system parameter
Computers	Contains tools for computer management. It is a diagram that contains the elements respectively to their domains, organization units, the Security Servers and protected computers
Alert logs	Contains information about alerts on protected computers. Created from alert notifications sent to the Security Server
Station logs	Contains information about events registered in local logs on protected computers
Server logs	Contains information about access sessions to the Security Server opened by Secret Net Studio components including internal sessions of the server
Archives	Contains tools to work with log archives
Reports	Contains tools to work with reports
Deployment	Contains tools to configure software installation and updates
Software passport	Contains tools to configure the Software passport mechanism
System events	Contains information about changes in the state of system objects

Tip. For more details about operations with control panels, see the document [**1**].

Monitoring and operative management

Data about the general state of system security is displayed in the **Dashboard** panel. For example, see the figure below. To view this information, click **Dashboard** at the top of the navigation panel.

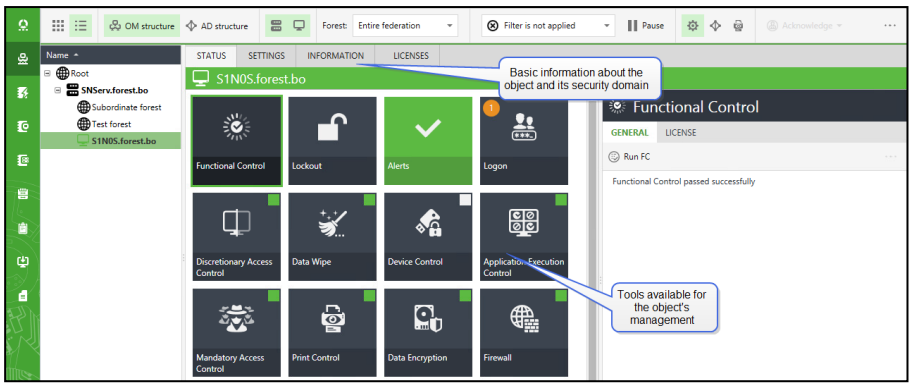


The panel contains widgets. A widget is an interface element that displays the status of a system parameter. By default, the panel contains a fixed set of widgets with the configured display parameters.

A set of displayed widgets, their parameters and location can be changed.

Tip. For detailed information about the operations with the **Dashboard** panel, see the document [**1**].

You can view information about computer statuses on the **Computers** panel, on the **Status** tab as shown in the figure below.



To enable or disable the properties panel, right-click the required object and click **Properties**.

Operative management of the protected computers can be performed using commands of the shortcut menu. Operative management commands can be applied only to connected computers.

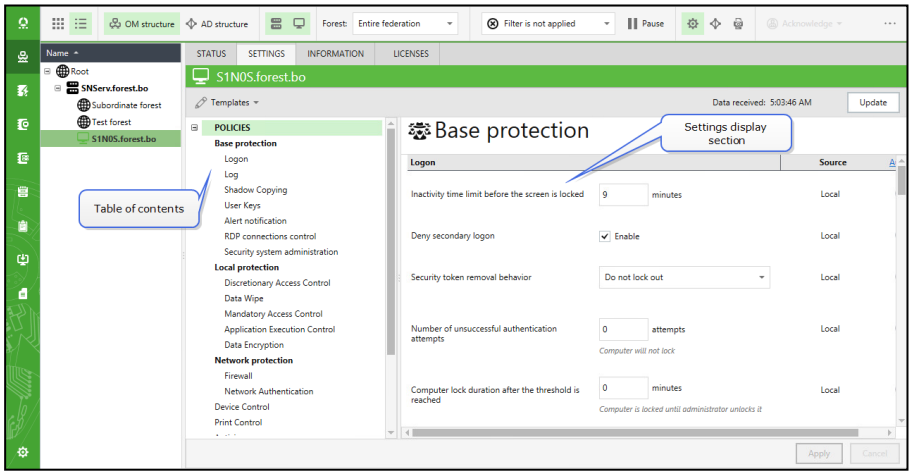
Tip. For detailed information about monitoring and operative management, see the document [1].

Configuring security settings

Security parameters can be configured in the **Computers** panel, on the **Settings** tab. To enable or disable display of the properties panel, right-click the required object and click **Properties**.

To configure security parameters of the selected objects, you must download the parameters from the Security Server. To do so, go to the **Settings** tab and click **Load settings**. A set of available parameters depends on the type of the selected object. After the parameters are loaded, to refresh them, click **Update**.

The **Settings** tab is shown in the figure below.



The interface is divided by the movable borders. You can hide any panel, if necessary.

Changes will apply you save them. To save changes, click **Apply**.

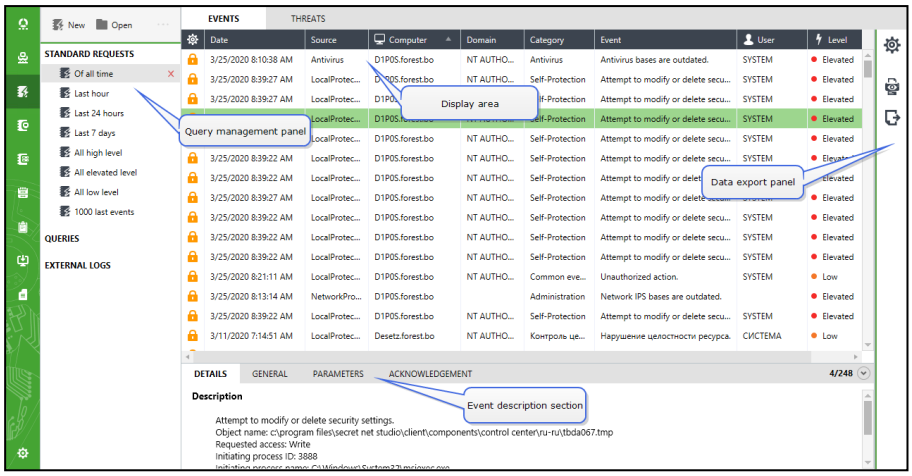
Tip. For detailed information about configuring security parameters, see the document [1].

Operations with centralized logs

The Security Server database contains the following logs:

- alert logs;
- event logs;
- the Security Server log.

The alert log is shown in the figure below.



Displaying and managing logs stored in the Security Server database is only possible using the Control Center. To load records use the **Request** section.

Downloaded information is displayed in the respective panel. To analyze the contents of the logs, there are different display modes.

A list of downloaded records in a table mode is displayed using the **Events** mode. This is the main mode to view and manage records.

A list of threat events received as a result of records analysis is displayed in the **Threats** tab. The threat log is short or detailed information about registered events. This mode is designed to provide an administrator or an auditor with the most critical information from the logs.

Tip. For more details about operations with logs, see document [**1**].

Documentation

1.	Secret Net Studio. Administrator guide. Installation, Management, Monitoring and Audit
2.	Secret Net Studio. Administrator guide. Setup and Operation
3.	Secret Net Studio. User guide. Operation Principles