SECURITY code

Secret Net Studio

Installation, Management, Monitoring and Audit

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

List of abbreviations **8**

Introduction **10**

General information **11**
- About 11
- Main functions 11
- Secret Net Studio components 12
  - Client 12
  - Security Server 12
  - Control Center 12
- Subsystem licensing 12

Client components **14**
- Client component groups 14
- Base protection 14
  - Core 15
  - Agent 15
  - Local Management Tools 15
  - Local Authentication Subsystem 15
  - Integrity control subsystem 15
  - Hardware support subsystem 16
  - Self-protection subsystem 16
- Additional components 16
  - Local Protection 16
  - Trusted Environment 16
  - Network Protection 16
  - Malware Protection 16

Client protection mechanisms **17**
- Secure logon 17
  - User identification and authentication 17
  - Computer lockout 17
  - Security tools 18
  - General information about Secret Net Studio and Sobol integration 18
- Functional control of subsystems 20
- Self-protection 20
- Event registration 20
- Integrity Control 21
- Discretionary Access Control 22
- Data Wipe 23
- Control of the connection and computer device change 24
- Device Control 24
- Application Execution Control 25
- Mandatory Access Control 25
- Print Control 27
- Shadow copying of output data 28
- Protection of information on local disks 28
- Full Disk Encryption 29
- Data encryption in encrypted containers 31
- Software Passport 32
- Trusted Environment 32
- Sandbox 33
- Firewall 33
- Network authentication 33

Setting up centralized system control **35**
- Interacting components 35

Security Server 35
Control Center 35
The Client in network operation mode 36
network structure 36
Security domains 36
Security domain forests 36
Federation 37
Network structure design features 38
Domain user management 38
Centralized data storage 38
About Secret Net Studio deployment 39
Secret Net Studio components 39
Hardware and software requirements 39
Client 39
Security Server 40
Control Center 41
System setup kit 41
Component installation options 42
Installation procedure for centralized management 43
Preparation 43
General procedure for component installation 43
Typical deployment scenario 43
Installing Secret Net Studio locally 45
Installing the Security Server 45
Creating a new security forest and domain 45
Creating a new security domain in an existing forest 50
Adding new Security Server to an existing security domain 50
Installing gateway software 51
Installing the Control Center 52
Installing the Client 53
Interactive installation 53
Installing the Client centrally 57
Installing under the control of the Security Server 57
Settings and control features panel 57
Managing the licenses for using security mechanisms 57
Creating a list of centrally installed software 60
Creating deployment tasks 61
Controlling task execution 64
Group policy-based Client installation 64
Configuring the OM structure 65
Creating files with a setup scenario 65
Creating a public network resource 70
Configuring Active Directory 71
SCCM-based installation 72
Configuring the OM structure 72
Creating files with a setup scenario 72
Creating a SCCM public network resource 74
Configuring SCCM 74
Updating and repairing Secret Net Studio 87
Updating 87
Centralized updating procedure 87
Updating the Security Server 87
Updating the Control Center 89
Updating the Client 89
Repairing 89
Repairing the Client 89
Repairing the Control Center 90
Uninstalling Secret Net Studio 91

Uninstallation procedure for network operation mode 91
Uninstalling the Client 91
Uninstalling the Control Center 91
Uninstalling the Security Server 92
Deleting gateway 92
Uninstalling Client subsystems 93
Uninstalling patches 94

Update server deployment 95
System requirements 95
Deployment options 96
Protected network with five or less workstations 96
Protected network with more than five workstations 96
Protected network without Internet connection 96
Server cascading 96
Installation, update and uninstallation 97
Install the update server 97
Updating the management program 98
Uninstalling the update server 98
Update server management program 99
View server information 99
View update information 100
Configure the update server 101
View the operation log 104

Secret Net Studio management 105
Organizing security system management 105
Central and local management 105
Using group policies 105
Delegating of administrative privileges 106
Management tools overview 106
Tools only for local management 106
Centralized and local management tools 109
User management program 110

About the Control Center 115
Starting the Control Center 115
The Control Center interface 115
Connection to the Security Server 117
Control Center settings 117

Centralized control structure 121
Diagram and list of control objects 121
Structure objects 122
Filtering objects 122
Import and export list of computers 124
Controlling the display of objects 125
OM structure after installation of Secret Net Studio components 127
Editing the OM structure 127
Adding objects to the OM structure 128
Managing the subordination ratio in the OM structure 131
Removing objects from the OM structure 132
Managing gateways 132

Configuring security settings 135
Lists of security settings 135
Saving changes 136
Configuring settings in the Policies and Event Registration sections 136
Policies section settings 136
Event Registration section settings 137
Applying settings on computers 137
Configuring settings in the Parameters section 137

Network connection settings 138
Settings of local log transfer 138
Server configuration 139
Settings for archiving centralized logs 140
Alert mailing settings 140
The Control Center user privileges 142
Alert filtering settings 143
Tracing settings 145
Security setting templates 145
Application 146
Creation 147
Comparison 149

Monitoring and operational management 151
General status of the system 151
Overview 151
Editing widget parameters 153
Adding and deleting widgets 154
Moving widgets 155
Configuring time parameters for displaying data 155
Monitoring groups 156
Viewing details 158
Object labels on the diagram 158
Details in the hierarchical list of control objects 159
Information about the state of objects 161
Details in the system events panel 162
Tracking alerts 163
Notifications about alerts 163
Alert acknowledgment 163
Resetting alert counters 164
Creating filtration rules based on alert notifications 164
Operational Management 165
Managing user sessions 165
Locking and unlocking computers 165
Restarting and shutting down computers 166
Updating group policies on computers 166
Approving changes to hardware configuration 166
Collecting local logs at the administrators command 167
Controlling the operation of security mechanisms on computers 167
Starting computer remote control 167
Generating reports 168
Programs and Components report 169
Security Settings report 170
Hardware Trusted Boot Module Report 171
Security tokens report 172

Using centralized logs 174
Centralized logs 174
Alert log 174
Combined computer log 174
Security Server log 174
Storing logs 175
Local storage of logs 175
Centralized storage 175
Log archives created by the Security Server 175
Panels to work with log entries 176
Loading log entries 178
Requests for the alert log 178
Requests for the stations log 179
Requests for the Security Server log 180
Requests for log archives 181
Configuring request settings 182
Controlling requests 184

Entry viewing options ... 184
Display event details modes ... 184
Acknowledgment alerts in the log ... 188
Sorting entries ... 189
Searching entries ... 189
Color coding of entries ... 189
Obtaining information about events from external knowledge bases ... 189
Printing entries ... 190
Exporting entries ... 191
Archiving centralized logs at the administrators command ... 192

Additional features of the local administration ... 193
Editing computer registration information ... 193
Local alert notifications ... 193
Local license management ... 193
Changing the client operation mode ... 195

Appendix ... 199
Required rights for installation and management ... 199
Installing and uninstalling components ... 199
Configuring mechanisms and managing object parameters ... 200
Using the Control Center ... 200
Assessing database size for the Security Server ... 201
Applying settings after configuration ... 203
Software for supported USB keys and smart cards ... 205
Client installation folder ... 205
Installing and configuring MS SQL DBMS ... 205
IIS changes during the Security Server installation ... 207
Changing connection settings between the Security Server and the DB ... 208
Changing credentials for connecting to DB ... 208
Changing DB connection settings ... 209
Creating a new DB ... 209
Updating DB ... 210
Specific features of the standby Security Server ... 210
Restoring an incorrectly uninstalled Security Server ... 210
Update server ... 214
Download updates from a network resource ... 214
Transfer updates manually ... 214
Update tool ... 214
Troubleshooting ... 215
Installing additional software manually ... 216
Networking settings ... 216
Color coding settings for log entries ... 218
Restoring logs from archives ... 220
Security Server DBMS maintenance recommendations ... 220
Defragmentation and rebuilding of indexes ... 220
Statistics update ... 222
Database backup ... 224
Archiving logs ... 226
Secret Net Studio integration with SIEM systems ... 227
Generating and installing the Security Server certificate ... 231
Configuring a secure connection to directory services ... 232
Registering events in the Security Server log ... 233

Documentation ... 246

List of abbreviations

AD	Active Directory
AEC	Application Execution Control
API	Application Programming Interface
ARP	Address Resolution Protocol
CC	Control Center
DB	Database
DBMS	Database Management System
DNS	Domain Name System
GUID	Globally Unique Identifier
FC	Functional Check
HC	Hardware configuration
HTTPS	HyperText Transfer Protocol Secure
IC	Integrity Check
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IIS	Intenet Information Services
LDAP	Lightweight Directory Access Protocol
LDS	Lightweight Directory Services
MBR	Master Boot Record
NTFS	New Technology File System
OM	Operational Management
OU	Organizational Unit
OS	Operating System
OSI	Open Systems Interconnection
PCI	Peripheral component interconnect
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
RDP	Remote Desktop Protocol
RFC	Request for Comments
SCCM	System Center Configuration Manager
SIEM	Security Information and Event Management
SMBIOS	System Management Basic Input/Output System
SSL	Secure Socket Layer
SQL	Structured Query Language
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Account Control
UEFI	Unified Extensible Firmware Interface
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus

XML	Extensible Markup Language

Introduction

This guide is intended for Secret Net Studio administrators. It contains the following information on:

- Secret Net Studio features and operation principles;
- instructions for Secret Net Studio installation, update and uninstallation;
- tools for local and central management of the security system;
- monitoring tools;
- working with centralized Secret Net Studio logs.

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 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.

Information sources

You can contact SECURITY CODE LLC representatives via email (info@securitycode.ru).

Chapter 1
General information

About Secret Net Studio

Secret Net Studio provides the security of information systems for Windows computers (MS Windows 10/8/7 OS, Windows Server 2019/2016/2012/2008 OS).

When using the respective subsystems, Secret Net Studio ensures:

- protection against unauthorized access to informational resources on computers;
- control of devices connected to computers;
- network traffic firewalling;
- network authentication;
- intrusion detection;
- antivirus protection.

You can manage Secret Net Studio in centralized or local mode.

Main functions

The Secret Net Studio main functions are as follows:

- user logon control (user identification and authentication);
- discretionary control of access to file resources, devices, printers;
- mandatory control of access to file resources, devices, printers, and network interfaces, including:
  - data flow control;
  - control of data copying to external drives;
- computer device status monitoring, with the following options:
  - computer lockout when the device status changes;
  - blocking the connection of an unauthorized device (devices from an unauthorized group);
- shadow copying of information transferred to external drives or being printed;
- automatic marking of documents being printed;
- integrity control of file objects and registry;
- providing application execution control for users (control over starting of executable modules, loading of dynamic libraries, execution of scripts using Active Scripts technology);
- RAM and external memory wiping at its reallocation;
- process isolation (executable programs) in RAM;
- protection of local hard disks, in case of unauthorized system startup;
- encryption of data on computer hard drives;
- creation of trusted environment (external control of the OS and installed security subsystems);
- antivirus protection;
- intrusion detection;
- network traffic firewalling;
- network authorization;
- Sobol management (user management, integrity check, security event transfer).
- functional control of key security subsystems;

- self- protection from unauthorized interaction with key subsystems of the security system;
- security event registration;
- centralized and local control of security mechanism parameters;
- centralized and local control of user work parameters;
- monitoring and operational management of protected computers;
- centralized collecting, storage and archiving of logs.

Secret Net Studio components

The Secret Net Studio components are as follows:

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

Client

The Client is designed to protect the computer where it is installed. The computer is protected by implementing security mechanisms that extend and enhance Windows security tools. Security mechanisms are a group of configurable tools included in the Client. These tools enable secure use of computer resources.

The Client can operate in the following modes:

- standalone mode allows to manage security mechanisms only locally;
- network mode allows to manage security mechanisms locally and centrally, to centrally obtain information about protected computers and change their state.

Operation mode is selected during the Client installation and can be changed later when using the Client (see p. **195**).

Security Server

The Security Server is used to centrally manage clients in network operation mode. This component allows to:

- store centralized management data;
- coordinate operation of other components during the centralized system management;
- obtain and process status information from protected computers;
- manage users and authorize network connections;
- centrally collect, store and archive logs.

Control Center

The Control Center is used to centrally manage security servers and clients in network operation mode. This component allows to:

- manage object settings;
- view status information about protected computers and alert-type events;
- load event logs;
- perform operative management on protected computers.

Subsystem licensing

To use Secret Net Studio security mechanisms , you need to purchase the licenses for the respective subsystems. You need licenses to work with the following mechanisms:

- basic protection mechanisms (mandatory license);
- discretionary access control;
- device control;

- data wipe;
- application execution control;
- mandatory access control;
- print control;
- disk protection and data encryption;
- full disk encryption;
- firewall;
- network authentication;
- detecting and preventing intrusions;
- antivirus;
- software passport;
- trusted environment;
- sandbox.

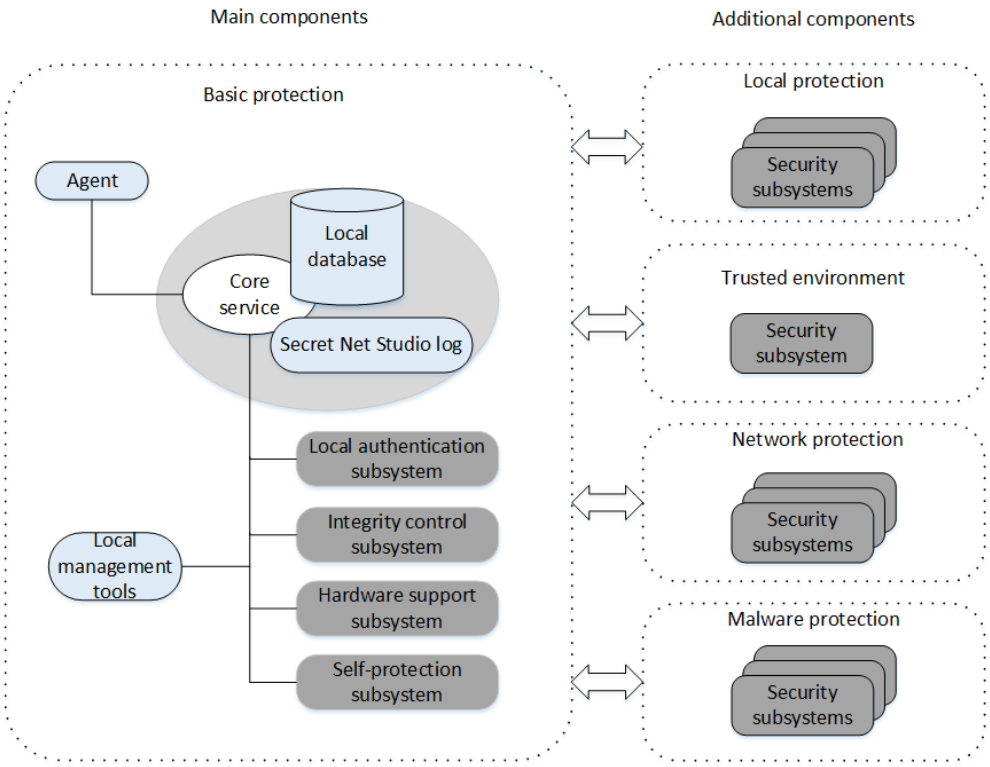
Chapter 2
Client components

Client component groups

The Client component groups are as follows:

- main components, which include basic program services, modules, security subsystems (base protection);
- additional components, which include:
  - Local Protection;
  - Trusted Environment;
  - Network Protection;
  - Malware Protection.

The Client structure is shown in the figure below.



Base protection

Base protection includes the following software services, modules and security subsystems:

- Core;
- Agent;
- Local Management Tools;
- Local Authentication Subsystem;
- Integrity Control Subsystem;
- Hardware Support Subsystem;
- Self-protection Subsystem.

Core

The Core starts automatically on a protected computer at system startup and is operating while the computer is turned on.

The core controls basic protection subsystems and ensures their interoperation. The core main functions are as follows:

- data exchange between the Client subsystems and command processing;
- remote access to information stored in the local database;
- system event processing and registration.

Secret Net Studio registration subsystem controls event logging. The events are registered in the Secret Net Studio log. The information about the events is provided by the monitoring subsystems. The security administrator specifies which Secret Net Studio events are to be logged.

The local database contains information about the security system settings necessary for a protected computer. The local database is stored in the Windows registry.

Agent

The Agent is a Client program module that ensures interaction with the Security Server. The agent receives commands from the Security Server and sends back computer status information.

The Agent operates only in network mode.

Local Management Tools

The Local Management Tools ensure:

- management of security objects (devices, files, folders);
- management of user parameters and security mechanisms;
- creation of integrity control tasks;
- viewing local logs.

Local Authentication Subsystem

The Local Authentication Subsystem is used in the logon security mechanism. Along with Windows OS the subsystem ensures:

- user logon possibility check;
- user notification about the information security measures and about the last logon to the system;
- notification of other modules about the user logon and logoff;
- user lockout;
- loading data from user security tokens;
- advanced logon authentication.

When processing a user logon, the user context is created: user privileges, access level, etc. Additionally, the logon module performs the functional check of the Secret Net Studio health.

Integrity control subsystem

The integrity control subsystem checks whether the following computer resources were modified: folders, files, keys and registry values. As part of the integrity control mechanism, the subsystem protects resources from substitution by comparing them with certain reference values. This subsystem does not perform control functions when the user works with resources. The control is performed only in case of the system events (loading, user logon, scheduled control).

Hardware support subsystem

The Hardware support subsystem operates as a part of the logon security mechanism that controls the hardware devices. The subsystem ensures the interaction of the Secret Net Studio with certain devices. The subsystem modules are as follows:

- the module providing a common interface for handling all supported devices;
- device modules (each module ensures operations with a specific device);
- hardware device drivers (if necessary).

Self-protection subsystem

This subsystem provides the Self-protection mechanism features (see p. **20**).

Additional components

Local Protection

Local Protection group includes subsystems that use the following security mechanisms:

- device control;
- print control;
- application execution control;
- mandatory access control;
- discretionary access control;
- local disk protection;
- data encryption in encrypted containers;
- data wipe;
- software passport.

Trusted Environment

This subsystem provides the Trusted Environment mechanism features.

Network Protection

Network Protection group includes the subsystems that use the following security mechanisms:

- network authentication;
- firewall.

Malware Protection

Malware Protection group includes the subsystems that use the following security mechanisms:

- intrusion detection and prevention;
- antivirus.

Chapter 3
Client protection mechanisms

Secure logon

Secure logon prevents unauthorized access to the system. The security logon mechanism includes:

- user identification and authentication tools;
- computer lockout tools;
- tools preventing OS startup using external drives.

User identification and authentication

User identification and authentication are performed at every logon. The standard Windows logon procedure involves entering a user name and password or using hardware tools supported by the operating system.

Secret Net Studio provides the following ways of user identification:

- By name – the user is to enter his/her credentials (name and password) or use hardware tools supported by the OS;
- Mixed – the user is to enter his/her credentials (name and password) or use a personal security token supported by Secret Net Studio;
- Only by security token – each user is to log on using his/her personal security token supported by Secret Net Studio.

Identification and authentication tools based on eToken, iKey, Rutoken, JaCarta and ESMART identifiers are used as SNS security tokens. These devices are to be registered (assigned to users) in the security system.

Advanced user authentication includes additional user password check by Secret Net Studio. Advanced authentication mode involves user password check against the current password policy of both the operating system and Secret Net Studio.

Computer protection can be improved using the following modes:

- interactive logon mode for domain users only. The attempts of local users (local accounts) to log on are blocked in this mode;
- secondary logon denial mode. It is impossible to run commands or establish network connections by entering other user credentials (who has not performed an interactive logon into the System) in this mode.

Computer lockout

Computer lockout tools are designed to prevent unauthorized use of a computer. Input devices (keyboard and mouse) and monitor screen are locked in this mode. In this mode, the current user session is blocked, only the administrator is allowed to log on.

Lockout due to unsuccessful logon attempts

You can set the limit of unsuccessful logon attempts for each user. When the advanced password- based authentication is enabled, the System controls unsuccessful logon attempts additionally to standard Windows features (account lockout after a certain number of wrong passwords). When repeatedly entering a password that is not saved in the SNS database, the System locks out the computer. Computers are unlocked by the administrator. The logon attempt count resets after successful user logon or after the computer is unlocked.

You can set up a temporary lockout when the limit of unsuccessful logon attempts is reached. In this case, the lockout is removed after the specified time has passed since the last unsuccessful logon attempt.

Temporary computer lockout

Temporary computer lockout is enabled when:

- the user performs an activity that provokes lockout;
- the preset computer inactivity interval has expired.

To enable lockout, the user may use the standard lockout method or diconnect the user security token from the computer. To enable computer lockout when disconnecting the security token, the administrator configures a response to the operation in the group policy using the Control Center. Lockout when removing the security token applies if the user logs on to the System using the security token.

When the preset inactivity interval expires, lockout takes effect automatically and applies to all computer users.

To disable temporary lockout, specify the current user password or provide the user security token.

Computer lockout by security subsystems

Computer lockout is also included in security system operation algorithms. This type of lockout is used when:

- the functional integrity of the Secret Net Studio system is violated;
- the computer hardware configuration is changed;
- the integrity of controlled objects is violated.

In these cases the computer is to be unlocked by the administrator.

Computer lockout by administrator

In network operation mode, a protected computer may be locked out and unlocked remotely via a command in the Control Center.

Security tools

Secret Net Studio supports the following security tools:

Security tools	Main tasks
Identification and authentication tools based on eToken, RuToken, JaCarta, Guardant ID, vdToken and ESMART security tokens	• Identification and authentication during user logon after the OS is loaded. • Identification and authentication during user logon from a remote computer. • Unlocking the computer. • Password and cryptographic key storage in the security token

The following tools can be applied for user identification and authentication:

- USB security tokens: eToken PRO, eToken PRO (Java), RuToken S, RuToken EDS, RuToken Lite, RuToken 2151, JaCarta PKI, JaCarta PKI Flash, JaCarta GOST, JaCarta GOST Flash, JaCarta-2 GOST, JaCarta-2 PKI/GOST, JaCarta-2 SE, JaCarta LT, JaCarta PRO, JaCarta PRO/GOST, JaCarta U2F, JaCarta WebPass, ESMART Token, ESMART Token GOST, ESMART Token GOST D, Guardant ID, vdToken ;
- smart cards: eToken PRO, eToken PRO (Java), RuToken EDS, RuToken Lite, RuToken 2151 SC, JaCarta PKI, JaCarta GOST, JaCarta PRO, JaCarta-2 PRO/GOST, ESMART Token SC, ESMART Token GOST SC, ESMART Token GOST D SC with any compatible USB readers.

General information about Secret Net Studio and Sobol integration

Secret Net Studio can work along with Sobol. Sobol provides additional protection against unauthorized access to information resources of the computer with Secret Net Studio system installed.

Note.
In Secret Net Studio version 8.4 and below, the integration with Sobol versions 3.x is implemented.
In Secret Net Studio version 8.5 and higher, the integration with Sobol version 4 is implemented. Sobol version 4 is a new generation of the Sobol product line, and its architecture and interface significantly differ from Sobol versions 3.x. The specifics of Secret Net Studio joint work with Sobol version 4 will be mentioned separately or in a note to the information contained in manuals.

In Sobol, a sharing mode of work is implemented for the Secret Net Studio integration. Sobol also can work by itself in stand-alone mode.

In stand-alone mode, Sobol performs its main functions before the start of the operating system regardless of Secret Net Studio. You can manage users and event registration log, configure general parameters by using complex administration tools without limitations.

In sharing mode of work (integration), a significant part of complex management functions is performed by using Secret Net Studio administration tools. The functions are listed in the following table.

Function	Description
Managing the Secret Net Studio user logon to the Sobol complex using an identifier which was initialized and assigned to the user in the Secret Net Studio system	The user is granted the privilege to automatically logon to the complex and then to the system upon presenting an identifier once. Also, a password written in the memory of a personal identifier can be used for logon
Managing the operation of Sobol integration control subsystem	For Sobol, you can create tasks for integrity control of hard disk files and registry objects by using Secret Net Studio administration tools
Transferring Sobol event log records to the Secret Net Studio log automatically	Records are transferred and transformed automatically when the Secret Net Studio hardware support subsystem is loaded.

For detailed information about performing these functions, see document [].

Attention!
- In the integration mode of the Secret Net Studio system and Sobol complex, the iButton DS1992 identifier is not used. We recommend using the DS1995 and DS1996 identifiers or USB keys and smart cards supported by Sobol.
- To use Secret Net Studio along with the Sobol complex, you need to install additional complex software (see the product documentation).

To ensure data protection in the process of centralized management of Sobol, a number of cryptographic transformations based on GOST 28147–89 and GOST R 34.10–2001 are implemented in Secret Net Studio. The encryption keys in use are listed in the following table.

Key name	Purpose	Storage location
Symmetric CM key	Encrypting authenticators[1] in the Secret Net Studio centralized management object storage. Calculation of MAC for the list of computers available to the user	Personal administrator identifier
Private CM key	Calculation of the session computer key when performing administration operations	Personal administrator identifier
Public CM key	Calculation of the session computer key when performing synchronization operations	Local database of the managed computer
Private computer key	Calculation of the session computer key when performing synchronization operations	Local database of the managed computer

[1]Authenticator is a data structure stored in the directory service which is used in the user authentication process along with the user's password.

Key name	Purpose	Storage location
Public computer key	Calculation of the session computer key when performing administration operations	Directory service
Session computer key	Encrypting information meant for the protected computer	Is not stored (calculated during work process)
Key for transforming the Sobol passwords	In Sobol versions 3.x — encrypting information in the closed board memory of Sobol. In Sobol versions 3.x and 4 — encrypting information stored in local database of the protected computer	In Sobol versions 3.x — closed board memory of Sobol. In Sobol version 4 — local database of the managed computer
Unique board number[2]	Decrypting information from the open board memory of Sobol. Signing external requests	Local database of the managed computer

Functional control of subsystems

The Functional Control is designed to ensure that all core security subsystems are loaded and operating when a user logs on (i.e. at system startup).

Successful completion of functional control is logged by Secret Net Studio.

The unsuccessful functional control is logged by Secret Net Studio stating the reasons (if the Secret Net Studio core is healthy). Only local administrators are allowed to log on to the System.

One of the main tasks of functional control is to ensure protection of computer resources at system startup in Safe Mode. Safe Mode is not considered a standard mode of the Secret Net Studio operations. However, the administrator can use it to fix problems, if necessary. Since some security functions are disabled in Safe Mode, functional control terminates with an error. As a result no user can log on to the System, except for administrators. In accordance with security policy rules, a standard user with no administrator privileges cannot access the computer resources bypassing security mechanisms.

Self-protection

Self-protection mechanism performs the following security actions:

- prevents unauthorized Secret Net Studio driver unloading and stopping of critical services and processes;
- protects Client modules and system registry keys necessary for Client operation from unauthorized modification and deletion;
- controls access of local administrators to the following Control Centers:
  - the Local Control Center;
  - the Application and Data Control Center;
  - the Application and Data Local Control Center;
  - the Mandatory Access Control Center additional configuration;
  - User management settings;
  - Client installation in deletion mode;
  - the Secret Net Studio Control dialog box on the Windows Control Panel.

Event registration

The security system events are logged while Secret Net Studio is running. All log entries are stored in a file on the system drive. The file data format is the same as in

[2] Only for integration with Sobol version 4.

the Windows security log.

You can configure the list of logged events and set the log storage parameters to provide the optimal amount of saved data matching the log size the system load.

Integrity Control

The mechanism ensures the integrity control of all selected objects. The objects are controlled automatically, in accordance with a predefined schedule.

Controlled objects include files, folders and system registry elements. Each object type has a set of controlled parameters. For example, files can be controlled for content integrity, access rights, attributes, as well as their existence, i.e. the availability of files for a specified path.

While using Secret Net Studio, you can set the control frequency by days or by the time during the day. The integrity control starts at the OS boot-start or when a user logs on to the System, or after the user logon.

Integrity Control can use various scenarios of system response to control jobs. You can configure registration of certain types of events (success or failure of an individual job or the whole set of jobs) and actions, in case of integrity is compromised (ignore the error, lock the computer or accept the new value as a reference).

All information about objects, methods, control schedules is contained in the data model. The data model is a hierarchical list of objects with a description of links between them, which is stored in the local database.

The hierarchical list includes the following categories of objects in ascending order:

- resources;
- groups of resources;
- tasks;
- jobs;
- control actors (computers, users, groups of computers and users).

The data model is common for the integrity control and application execution control mechanisms.

You can manage local data models on protected computers centrally (for clients in network operation mode). To provide centralized management, two data models are created in the Global Catalog (for 32-bit and 64-bit Windows OS), taking into account specific features of the software used on protected computers with various OS versions.

Each of the centralized data models is common for all protected computers with the respective Windows OS version (32-bit and 64-bit Windows OS). When centralized data model parameters are modified, the modifications are synchronized locally on the protected computer. New parameters are transferred from centralized storage to the computer and are included in the local data model to be used by security mechanisms afterward.

Synchronization is performed:

- at computer startup;
- at user logon;
- after logon (in background, while the user is working);
- periodically at predetermined time intervals;
- manually by the administrator;
- after changing the IC-AEC central database settings.

Features of centralized data model editing are as follows: only data model matching Windows OS version (32-bit and 64-bit) on the administrator's computer is editable. A data model with a different bitness is read-only (it is also possible to export data from that model to another one). If the System includes protected computers with different Windows OS versions (32-bit and 64-bit), the

administrator is to set up two workstations — one with a 32-bit Windows OS and one with a 64-bit Windows OS.

Discretionary Access Control

Secret Net Studio includes a mechanism of discretionary control of access to file system resources. The mechanism ensures:

- restriction of user access to folders and files on local disks based on an access matrix for actors (users, groups) regarding the accessory objects;
- object access control for local or network access, including access under system account name;
- denial of access to objects bypassing predefined access rights (if standard OS tools or application software without native drivers for operating with the file system are in use);
- operational independence from the Windows OS built-in mechanism of discretionary access control, meaning that the predefined Secret Net Studio file object access rights do not affect the similar ones of the Windows OS and vice versa.

Similarly to the Windows OS, the Secret Net Studio access matrix is a list of file objects in which accounts with access rights are defined. These rights permit or prohibit the execution of certain operations. The list of the access rights is presented in the table below.

Access right	Folder action	File action
Reading (R)	Permits or prohibits viewing file and subfolder names	Permits or prohibits data reading
	Permits or prohibits viewing file object attributes	
Writing (W)	Permits or prohibits the creation of subfolders and files	Permits or prohibits making changes
	Permits or prohibits changing file object attributes	
Execution (X)	Permits or prohibits moving files within the structure of subfolders	Permits or prohibits execution
Deletion (D)	Permits or prohibits file object deletion	
Access rights change (P)	Permits or prohibits changing rights to access a file object. A user with permission to change access rights to a resource is conventionally considered the resource administrator	

File object access rights can be assigned explicitly or inherited from a higher hierarchy element. Explicitly assigned rights have a higher priority than inherited ones. If the rights inheritance mode is disabled for an object, the access rights are considered to be explicitly assigned.

The privilege "Discretionary Access Control: Accounts with access rights management privilege" is aimed to manage the lists of access to any file objects. Users who have been granted this privilege can change access rights for all folders and files on local disks (irrespective of the predefined access rights for objects).

By default, the privilege to manage the access rights is granted to users included in the local administrators group. In addition, all these users have rights to access resources for reading, writing, execution and deletion purposes (RWXD). These rights are inherited from the root folders of logical partitions. To prevent an unintentional lockout of the OS due to incorrectly set rights to access resources, you are not able to change the access rights for the system disk (%SystemDrive%) root folder or the entire system folder (%SystemRoot%).

File object copying and moving

When copying a file object, the access rights inheritance mode is enabled, even if the access rights are explicitly assigned to the original object.

The explicitly assigned access rights of the file object are retained when the object is moved within its logical partition. If inheritance mode is enabled for the object, the rights of the folder to which the object has been moved come into effect. When moving the object to another logical partition, the rights inheritance mode is enabled.

Audit of file object operations

When the discretionary access control mechanism is enabled, the events of successful access to objects, access denial, or access rights change can be logged by Secret Net Studio. By default, successful access events are not logged, but access denial and rights change events are logged for all file objects. Logging such events is enabled and disabled by the security administrator when configuring group policy parameters.

You can detail file object audit according to the executable operations that require certain access rights. For example, you can enable successful access audit when writing to a file or deleting it. The operations audit can be enabled or disabled by the resource administrator when configuring additional parameters for a file object access rights.

Data Wipe

Wiping deleted information makes it impossible to recover and reuse data. Guaranteed data wiping is achieved by writing a sequence of random numbers instead of the removed information in the freed memory area.

Secret Net Studio provides the following data wipe options:

- wiping deleted information automatically on specific devices (local, removable drives, RAM), if data wipe is enabled in the Control Center;

  Note. Secret Net Studio provides exclusion of selected objects (files and folders) from processing when wiping data automatically on local and removable drives by creating an exception list.

- wiping selected file objects using the context menu;
- wiping all data using the Control Center command including a partition table, logical volumes, file objects, residual data on local drives (except for a system drive) and removable drives connected to a protected computer.

To improve the security level Secret Net Studio can perform several wipe cycles.

When configuring the mechanism, you can specify the number of data wipe cycles for the following items:

- local and removable drives;
- RAM;
- file objects to be deleted by using the context menu;
- data storage devices on which all data will be wiped.

Attention! A swap file wipe is performed using standard Windows tools, when you turn off the computer. If the Secret Net Studio RAM wipe mode is enabled, we recommend you to enable the standard Windows security parameter "On shutdown: clear the virtual memory paging file" (located in Computer Configuration\Windows Parameters\Security settings\Local policies\Security settings).

Files are not wiped while moving to the Recycle Bin, as they are not deleted from the drive. You can wipe the files by clearing the Recycle Bin.

To ensure the optimum load on your computer when deleting a large amount of data from local and removable drives, Secret Net Studio provides the delayed wiping mechanism. Residual data that is to be wiped is queued for processing. Data wipe is performed over queue with a time delay and completes before the computer is shut down.

Control of the connection and computer device change

The connection control and computer device change mechanism ensures:

- timely detection of computer hardware configuration changes, and response to these changes;
- updating computer device list that is used by the mechanism of disretionary access control to devices.

Hardware configuration changes are monitored by the security system for devices with the "device is always connected to the computer" control mode enabled.

Initial hardware configuration of the computer is set during the Secret Net Studio installation. Control parameter values are set by default. You can configure control policy individually for each device. The control policy parameters can be inherited from the device models, classes and groups and applied to the devices.

The following configuration control methods are used:

- Static configuration control. Each time the computer is started, the subsystem is informed about the actual hardware configuration and compares it with the reference one.
- Dynamic configuration control. When the computer is operating (also when the PC wakes up from sleep), the device filtering driver monitors device connections, disconnections, and parameter modifications. When changing the configuration, the filtering driver delivers the respective notification, and Secret Net Studio takes the appropriate action (for example, a computer lockout).

When changing the hardware configuration, Secret Net Studio is awaiting the security administrator to approve of the changes. A hardware configuration approval procedure is required to validate the identified modifications and accept the current hardware configuration as the reference one.

Device Control

User access to devices is based on device lists that are created by the device control mechanism (see p. **24**).

The Secret Net Studio device control ensures:

- permitting and restricting device operations;
- assigning confidentiality categories or user session confidentiality levels to restrict access using the mandatory access control mechanism.

Access control options depend on the device type. No full or partial isolation of access is applied to devices of specific use or ones required for the computer operation. For example, there are no access restrictions to the processing unit and RAM, but the options for discretionary access to input/output ports are restricted.

If control is disabled for a device, or no connections are allowed, the access is not restricted for assigned operation permissions or restrictions. User rights to access such devices are not controlled.

When installing the Client, access rights are set for all detected devices that support discretionary access. By default, full access is granted to three standard user groups: "System", "Administrators" and "All" meaning that initially unlimited access is granted to all users for all devices detected on the computer. Then, the security administrator restricts user access to certain devices, according to the security policy requirements. For this purpose, access rights can be configured directly for devices, or for the device classes and groups.

Configuring access rights for classes and groups ensures that the security system is prepared for the possible connection of new devices. Once connected, the new device is included in the respective group, class and model (if any). User access to such a device will be restricted automatically in accordance with the rules set for the device group, class or model.

User access to devices with assigned confidentiality levels or session confidentiality levels is controlled by the mandatory access control mechanism.

Application Execution Control

Application execution control makes it possible to create for any computer user an individual list of allowed software. The security system controls and prohibits the use of the following resources:

- program and library startup files that are not included in the list of ones allowed to run and do not meet certain criteria;
- scenarios that are not included in the list of ones allowed to run and not registered in the database.

Note. A scenario (also referred to as a "script") is a sequence of executable commands and/or activities in text format. Secret Net Studio controls the execution of scripts using the Active Scripts technology.

Attempts to start unauthorized resources are registered in the log as alerts.

During the mechanism configuration, a list of resources allowed to run and to be executed is created. The list can be created automatically, based on information about the programs installed on a computer, or on log records (security log, or Secret Net Studio log) containing information about started programs, libraries and scripts.

You can enable the integrity check for files included in the list (see p. 21). For this reason, the application execution and integrity control mechanisms use a uniform data model.

The application execution control mechanism does not block the start of programs, libraries and scripts in the following cases:

- if the user has the "Application execution control: Not active" privilege (by default, this privilege is granted to the computer administrator), the control over resources started by the user is not performed;
- if the application execution control operates in soft mode, the subsystem controls attempts to run programs, libraries and scripts but the use of any software is allowed. This mode is usually used when configuring the mechanism.

Process isolation

The Secret Net Studio process isolation mode is used to isolate processes preventing third party access to data of certain executable modules. The process isolation mode provides control of the following operations with the data exchanged by various processes:

- reading clipboard data;
- reading data in another process window;
- writing data to another process window;
- transferring data between processes using the drag-and-drop method.

A process is considered to be isolated if isolation is enabled for the executable file of the process. Data exchange with other processes is impossible for an isolated process. The clipboard can be used only when writing or reading data of the same process. Non-isolated processes exchange data without any restrictions.

Process isolation mode can be used when the application execution control mechanism is enabled (the mechanism driver must be functioning). Also, in order to avoid starting copies of executable files in a non-isolated environment, we recommend you to configure the AEC mechanism and enable the "hard" operation mode for the mechanism.

Mandatory Access Control

The mandatory access control mechanism ensures:

- control of user access to information with an assigned confidentiality category (confidential information);
- control of the connection and use of devices with assigned confidentiality categories;
- control of confidential information flows in the system;
- control of displaying confidential files in file managers;
- control of network interface use with assigned acceptable user session confidentiality levels;
- control of confidential document printing.

By default, the Secret Net Studio confidentiality categories are as follows: "Non-confidential" (for public information), "Confidential" and "Strictly confidential". If necessary, you may add more confidentiality categories and set their names in accordance with the standards adopted by your company. The maximum allowed categories is 16.

You can assign a confidentiality category to the following resources:

- local physical drives (except for drives with logical partitions) and any devices included in the following device groups: USB, PCMCIA, IEEE1394 or Secure Digital;
- folders and files on local physical drives.

Note. Files and folders stored on devices included in the USB, PCMCIA, IEEE1394, Secure Digital (external drives) device groups are not assigned a confidentiality category individually since it is inherited according to the device confidentiality category.

The user is granted access to confidential information based on respective access level. If the user access level is lower than the resource confidential category, Secret Net Studio blocks access to the resource. Once access to confidential information is granted, the program (process) confidentiality level is elevated to the resource confidentiality level. This is needed to avoid saving confidential data to files with lower confidentiality categories.

There is an operation mode of the mandatory access control mechanism, in which the user in various file managers see only those files which confidentiality category does not violate his/her access rights. Files from higher confidentiality categories are not shown to users. In flow control mode, user rights are determined by the session confidentiality level.

Mandatory access control for devices is ensured as follows. If a device is connected during a session of a user with a lower access level than the device category, Secret Net Studio will deny the device connection. If such a device is connected before starting the user session, the user is not be allowed to log on. In flow control mode, the user session confidentiality level must match the categories of all connected devices.

Device operation is allowed regardless of user access level, if the "Without category" mode is selected for the device. This mode is selected by default.

Access to confidential file content is granted to the user, if the file confidentiality category is not higher than the user access level. Moreover, the confidentiality category of the device containing the file is also taken into account. If the confidentiality category of a file or a folder is lower than the device confidentiality level, Secret Net Studio considers the file confidentiality category equal to the device one. If the file confidentiality category is higher than the device one, the state is considered to be incorrect, and access to the file is denied.

Flow control mode

When using the mechanism in confidential flow control mode, all data processes are assigned a common confidentiality level. The required confidentiality level is selected from a number of available to the user before starting the user session. This level cannot be changed before the session ends.

In flow control mode, information can be saved only with a category equal to the session confidentiality level. Access to data that has a category higher than the session confidentiality level is prohibited (even if the user access level allows access to such data). Thus, flow control mode ensures strict adherence to the principles of mandatory access control, and prevents unauthorized copying or transferring confidential data.

In flow control mode, the use of devices with a confidentiality category that differs from the session confidentiality level is prohibited. If the devices with different confidentiality categories are connected to the computer at the moment of the user logon, access is denied due to the conflict of connected devices. The use of devices with a confidentiality category higher than the user access level is restricted in the same way as when the flow control mode is disabled.

Flow control mode makes it possible to restrict the use of network interfaces. For each network interface, you can select the session confidentiality level, according to which the interface will be available to the user. If you start a session with another confidentiality level, the security system blocks the interface operation. It lets you organize the user work in various networks depending on the session confidentiality level.

The "Adapter is always available" mode is provided for network interfaces (enabled by default). In this mode, network interface operation is allowed regardless of the session confidentiality level.

Hiding confidential files

If the mode of hiding unavailable confidential files is enabled, the user will not see in the file managers the files which confidentiality category exceeds the current session confidentiality level.

Confidential information output

The mandatory access control mechanism controls the output of confidential information to external media. External media in the Secret Net Studio system are removable disks with the "irrespective of confidentiality category" access mode enabled. When copying or moving a confidential resource, its initial confidentiality category on such media may not be saved. Therefore, to output confidential information to external media in the flow control mode, the user must be granted the respective privilege.

Print control mode is to prevent the unauthorized output of confidential documents to local and network printers. The mechanism ensures the output of confidential documents for printing, only if the respective privilege is granted. Also, a special marker can be added to a printed document specifying the document confidentiality category. Print events are registered in the Secret Net Studio log.

Print Control

Print Control mechanism ensures:

- control of user access to printers;
- registration of the documents to be printed in Secret Net Studio log;
- printing out documents with a certain confidentiality category;
- automatic addition of markers to printers documents (document marking);
- shadow copying of printed documents.

In order to implement the marking and/or shadow copying functions for printed documents, "virtual printer" drivers are added to the system. Virtual printers correspond to real ones installed on the computer. The list of virtual printers is created automatically when the print control or shadow copying mode is enabled. In this case, printing is only possible to virtual printers.

When printing to a virtual printer, additional transformations are performed to obtain the XPS (abbr. XML Paper Specification) image of the printed document. The XPS document is further copied to the shadow copy storage (if shadow copying is

enabled for the printer), modified as required, and then sent to the respective printer.

Shadow copying of output data

The shadow copy mechanism ensures the creation of data duplicates in the System that are to be sent to external drives. Duplicates (copies) are saved in a repository that only authorized users may access. The mechanism is applied to devices for which the **saving of copies when information is being saved** mode is enabled.

When copy saving mode is enabled, the data output to external drives can be performed only if the data copies are created in the shadow copy repository. If it is not possible to create a duplicate for some reason, the data output operation is blocked.

Shadow copying is supported for the following types of devices:

- external removable disks;
- floppy disk drives;
- optical disk drives with enabled data writing;
- printers.

When the data output to an external removable disk (for example, a USB flash drive) is performed, the copies of files saved to the device during the data output operation, are created in the shadow copy repository. If a file is open for editing directly from the removable drive, when saving a new file version, its copy is created in the repository.

For optical disk devices with data writing, the shadow copy mechanism creates a disk image in the repository if the Image Mastering API (IMAPI) interface is used for writing. If the writing is performed in the Universal Disk Format (UDF) file system format, the file copies are created.

Attention! Some software packages with enabled optical disk writing use their own device control drivers. Such drivers may access the device bypassing the shadow copy mechanism. To ensure guaranteed control, disk writing should be performed by standard Windows tools only.

Shadow copying of printed documents is performed using the print control mechanism (see p. 27). An XPS (abbr. XML Paper Specification) image of a printed document is saved as a copy of the information to be printed. XPS is an open XML-based graphical fixed markup format developed by Microsoft.

Data output control using the shadow copying mechanism is one of the audit tasks. Data output events are registered in the Secret Net Studio log. You can access the copies in the shadow copy repository using the Local Control Center. The program provides the tools for searching the repository contents.

The administrator configures the operation of the shadow copy mechanism via the Control Center. When configuring, the shadow copy repository parameters are defined, and the mechanism is enabled or disabled for the devices or printers.

Protection of information on local disks

The data protection mechanism on the computer local disks (disk protection mechanism) is designed to block access to hard disks during an unauthorized start of the computer. A start is considered authorized if it is performed by the OS with the installed Client. All other methods of starting the OS are considered unauthorized (for example, loading from an external drive or the start of another OS installed on the computer).

The mechanism ensures the protection of information when attempting to access it using standard OS tools.

The operation of the disk protection mechanism is based on the modification of the boot sectors of logical partitions on the computer hard disks. The content of boot sectors is modified by encoding using a special key that is automatically generated when the mechanism is enabled. Part of the disk protection mechanism service data is saved in the System registry.

Modification makes it possible to hide information about logical partitions in case of an unauthorized start of the computer. The System considers partitions with modified boot sectors as unformatted or bad ones. In case of the authorized start of the computer, the content of boot sectors of protected logical partitions is decoded automatically if accessed.

The administrator selects the logical partitions for which the protection mode (i.e., the boot sector modification) is to be enabled.

The disk protection mechanism can be used, if the physical disk, from which the OS is loaded, is one of the following types:

- GUID partition disks (GUID Partition Table — GPT) on a UEFI computer (Unified Extensible Firmware Interface). When the mechanism is enabled, a special loader is being written to the Secret Net Studio disk in a hidden system UEFI partition, and gets registered in UEFI;
- MBR (Master Boot Record) disk. When the mechanism is enabled, the MBR and the zero disk track space are modified.

Attention! When using the MBR disk, the virus scanning is to be disabled in BIOS settings. To disable the virus scan function, set the Disabled value for the Boot Virus Detection parameter (the function availability and the parameter name may differ depending on the BIOS version).

The mechanism ensures the protection of up to 128 logical partitions for a total of 32 physical disks. Logical partitions with enabled protection mode must have the FAT, NTFS or ReFS file systems. Partitions may be the MBR disks or on the GUID partition disks. Disks with other types of logical partitions are not supported (for example, dynamic disks).

When using the disk protection mechanisms, only one OS is to be installed on the computer. If more than one operating system is installed, the stable operation of other OS is not guaranteed after the mechanism is enabled.

Full Disk Encryption

Secret Net Studio Full Disk Encryption mechanism allows you to encrypt data on drives to prevent unauthorized access attempts to confidential information stored on these drives.

Secret Net Studio supports encryption of system and non-system hard drive partitions with GPT layout and UEFI boot mode, as well as encryption of non-system hard drive partitions with MBR layout.

The maximum number of encrypted partitions on one hard drive is 32. The number of hard drives is not limited. The maximum total number of encrypted partitions on all hard drives is 66.

Note. These limitations apply also to partitions with enabled Secret Net Studio disk protection mechanism.

The encryption algorithm is AES-256. Key information is stored in an encrypted form on the unencrypted partition ESP (EFI Partition).

To gain access to encrypted disks, you need to have a password that was set when encrypting data. Several disks are encrypted with the same password.

Secret Net Studio Full Disk Encryption subsystem provides the following:

- **Local encryption by the user with storing recovery data locally.** This mode makes it possible to encrypt data on disks on a computer with Secret Net Studio in standalone or network mode. The user chooses disks and partitions, sets a password, saves recovery data.

  Only the user can decrypt and restore data.

  To grant the user the privilege to encrypt data on disks, the security administrator assign it to them in Secret Net Studio giving them a capability to save recovery data themselves.
- **Local encryption by the user with storing recovery data centrally.** This mode makes it possible to encrypt data on disks on a computer with Secret Net

Studio in network mode. The user chooses disks and partitions, sets a password. Recovery data are saved to Secret Net Studio centralized storage.

Both the user and the administrator can decrypt and restore data.

To grant the user the privilege to encrypt data on disks, the security administrator assign it to them in Secret Net Studio selecting that recovery data must be stored centrally.

- **Local encryption by the administrator.** This mode makes it possible to encrypt a given partition on a local hard drive on a computer with Secret Net Studio in standalone or network mode. The administrator chooses a partition, sets a temporary password, sets up the parameter for a password change after the first logon, and saves recovery data. The administrator gives the temporary password to the user. The user sets their password at the first logon.

  Only the administrator can decrypt and restore data.
- **Centralized encryption by the administrator.** This mode makes it possible to encrypt given drives or partitions on a group of computer with Secret Net Studio in network mode. The administrator chooses drives or the types of partitions (system, non-system or all). The user sets a password. Recovery data are saved to Secret Net Studio centralized storage.

  Only the administrator can decrypt and restore data.

When you enable the Full Disk Encryption subsystem, Secret Net Studio bootloader is installed on the computer. If there are encrypted disks on your computer, Secret Net Studio bootloader starts up and you are prompted to enter the password for the disks.

Secret Net Studio performs monitoring and audit of encryption processes. The administrator can look at the current state of the Full Disk Encryption subsystem in the Control Center or in the Local Control Center. Full Disk Encryption subsystem events are registered in the Secret Net Studio log. You can see notifications about the main encryption processes on a computer with this subsystem enabled.

The following tools are used to recover access in case of losing the password for encrypted disks or in case of computer failure:

- if the user has recovery data, they need to enter the recovery code and the password for the recovery code at logon, and then change the password for disks;
- if the user performed the encryption and recovery data are stored in a centralized storage, the administrators sends the recovery code to the user, and the user changes the password for disks;
- in case of failure of a computer with encrypted data, you can boot the computer from the emergency recovery disk to restore the configuration of the encrypted partitions and to decrypt the data.

Recovery data are encrypted with Secret Net Studio security domain key. The security domain key is created when the domain is created or the Security Server is updated. This key can be updated by the security domain administrator.

To use the Full Disk Encryption subsystem, a separate license is required. When the license has expired, you can still access encrypted data, as well as decrypt data and restore access.

Attention!

- You cannot protect an encrypted partition of a hard drive using Secret Net Studio disk protection mechanism. And vise versa, you cannot encrypt a protected partition of a hard drive with Secret Net Studio Full Disk Encryption mechanism.
- Simultaneous operation of the Full Disk Encryption and Trusted Environment mechanisms is not supported.
- Full Disk Encryption is not supported on a computer with several operating systems.
- Dynamic disk encryption is not supported.
- Changing the configuration of encrypted partitions of hard drives is not supported.
- Parallel operation of the Full Disk Encryption mechanism with other disk encryption systems (for example, Bitlocker) is not supported.

Data encryption in encrypted containers

Secret Net Studio ensures the encryption of the contents of file system objects (files and folders). Special repositories (encrypted containers) are used for encryption and decryption operations.

Physically, an encrypted container is a file that can be connected to the operating system as an additional drive. The encrypted container is a disk image but all encrypted container operations are performed by the encryption mechanism driver. The driver processes user data in containers, in "transparent encryption mode", meaning that the user, after connecting the encrypted container as a disk, may perform file operations on this disk as using any other drive. No additional operations are required to encrypt or decrypt files. All cryptographic file operations are performed automatically.

Encrypted container can be connected to the local disk system, external drives or network resources. The space available for saving data is specified when creating an encrypted container. The volume limit is determined on the basis of the available resource space and file system type. Minimum container size – 1 megabyte.

To restrict access to encrypted containers in Secret Net Studio, the following rights are provided:

- data reading – read-only access to files in the encrypted container;
- full data access – the right to read and write files to the encrypted container;
- encrypted container management – the right to read and write to files, as to manage the list of users that have access to the encrypted container.

The right to create encrypted containers is available to users with the respective privileges. This privilege is granted by default to accounts included in the local administrator group.

After creating an encrypted container, the user is able to manage it and grant the access rights to another user. If necessary, the creator of the encrypted container can be removed from the list of users with access rights, as long as at least one user with the right to manage the encrypted container remains in the list.

In order to work with encrypted resources, users must have encryption keys. The security administrator is to generate and issue the encryption keys. Key pairs are created for users; each consists of a public and a private key. Public keys are stored in a shared repository (the local Secret Net Studio database is used for local user keys, while a global catalog repository is used for domain users). Private keys are stored in key carriers assigned to users. Private keys (key information) can be stored on identifiers or external drives, such as memory sticks, USB drives and so on.

General information about the key scheme

To access the encrypted containers you may use certain key sets and additional values that are generated and calculated during cryptographic operations.

An encrypted container contains the following data groups:

- encrypted container control information – a structure of encrypted keys and values for accessing the encrypted container;
- encrypted user data – the files cryptographically transformed and encrypted by users.

Control information is generated when creating the encrypted container and contains the public key of the encrypted container creator along with other information. When creating the list of users with access to the container, the user public keys get included in the structure. The respective parts of the structure are encrypted using public keys.

Files inserted in the encrypted container by users are encrypted using the encryption keys and calculated on the basis of a generic encryption key, shared by all encrypted container users. The generic encryption key is generated when

creating the encrypted container and is calculated when accessing to the encrypted container using private key.

To provide additional security for the generic encryption key, you can use a special corporate key. The key is generated when creating an encrypted container, provided that the use corporate key parameter is enabled. The corporate key is stored in the system registry, and used for generic key encryption and decryption.

When using the corporate key, you can access the encrypted container, if the key is encrypted and stored in the system registry. To access an encrypted container located on another computer, the corporate key must be imported to the registry on that computer.

Key rollover

When using Secret Net Studio, you should regularly rotate user keys and generic encryption keys of encrypted containers.

The user key rollover is performed by the user or by the security administrator. The frequency of the user key rollover is controlled by Secret Net Studio. You can configure the key rollover frequency by setting a maximum or minimum key expiration period. When rotating user keys, two key pairs (current and previous) are stored in the system. The previous pair is required to re-encrypt the respective control information of the user encrypted containers using the new key. The re-encryption of the control information starts automatically after the key rollover.

Attention! The encrypted container must be available for the automatic re-encryption of control information. For example, if an encrypted container is not available over the network or is located on a currently disconnected external drive, re-encryption is not performed. In this case, after the keys have been rotated for the re-encryption of control information, the user is to perform any operation with the encrypted container (for example, to connect it) prior to the next key rollover. Otherwise, the previous key pair will be rotated at the next key rollover, and the user will not access the encrypted container due to the key mismatch. To regain the user access, you are to remove the user from the list of those with access to the encrypted container and add the user back to the list.

The user with the encrypted container management rights is able to rotate the generic key of the encrypted container. To rotate the generic key, the user is to initiate the container re-encryption procedure. As a result, all encrypted data in the container will be re-encrypted using the new generic key. When using a corporate key, it is rotated automatically when rotating the generic one.

Software Passport

The Software Passport mechanism is designed to control the integrity of software installed on protected computers. Software integrity control is performed by scanning executable files and calculating their checksums. The set of controlled files on computer drives represents software environment for gathering data and analyzing changes.

Executable files identification is performed using file name extensions. The set of file name extensions and search directories can be configured. The scan can be performed manually or according to a schedule.

The results of software environment scan (software passport) are uploaded to the Security Server and get the passport project status for a computer. The scan results are compared to the previous ones, which are kept as a confirmed passport. The changes are analyzed and, if necessary, the passport project is confirmed as the current passport of the protected computer.

Trusted Environment

Secret Net Studio Trusted Environment is a security mechanism that controls OS and Client operation. The mechanism performs the following security actions:

- controls Secret Net Studio module (driver, service, application) integrity;
- controls Secret Net Studio module (driver, service, application) start and operation;

- denies writing to the memory pages where Secret Net Studio modules are located;
- detects and prevents computer attacks or forces emergency OS shutdown if the attack cannot be prevented;
- registers events in TE log.

When Trusted Environment is enabled, you can only start the OS using a boot drive created in advance via the Client.

Note. Trusted Environment is available in Secret Net Studio version 8.5 and later.

Sandbox

Sandbox is a mechanism which protects computer resources from damage by running unknown software in an isolated environment. Unknown software can be run either by users or administrators.

When a user works with software being analyzed, Sandbox monitors and analyzes its behavior:

If the behavior of the software is abnormal, Sandbox force-quits the program, includes it into the list of prohibited programs (black list) and notifies the user about the actions performed.

If the behavior of the software is not suspicious and does not contradict the trust level indicated in Control Center, Sandbox includes it into the list of trusted programs.

If the user quits a program before the check is completed, Sandbox saves the context of the program analysis and uses it next time when the program is run via Sandbox.

Attention! Sandbox is compatible with Windows 10 version 1809 and later.

Firewall

The Secret Net Studio system ensures network traffic control on the network, transport and application layers based on the created filtration rules.

The Secret Net Studio Firewall subsystem main features are as follows:

- filtration on the network layer with independent decision-making for each packet;
- filtration of service protocol packets (ICMP, IGMP, etc.) required for diagnostics and management of network device operations;
- filtration considering the incoming and outgoing network interface, for the authentication of network addresses;
- filtration of requests for the establishment of virtual connections (TCP sessions) on the transport layer;
- filtration of requests for application services (filtering by character sequence in packets) on the application layer;
- filtration considering network packet fields;
- filtration considering date/time.

Filtration of network traffic is performed on Ethernet (IEEE 802.3) and Wi-Fi (IEEE 802.11b/g/n) interfaces. Firewall-related events are registered in the Secret Net Studio log.

Network authentication

If the network authentication mechanism is enabled, special service information is added to network packets, ensuring the authenticity and integrity of transferred data, as well as protection against Man in the Middle attacks.

The network authentication subsystem ensures:

- receiving the connection authorization rules from the authorization server included in the Security Server (the list of connection parameters to which service information is added);
- receiving the session data for adding special service information;
- adding special control information;
- analysis of special service information in incoming packets and transmission of information about the remote user context to the firewall subsystem for the rule-based filtration.

Network connections are authorized on Ethernet (IEEE 802.3) and Wi-Fi (IEEE 802.11b/g/n) interfaces.

Chapter 4
Setting up centralized system control

Interacting components

Security Server

The Security Server main functions are as follows:

- receive information from clients on protected computers about the current state of workstations and user sessions;
- receive and send information about alert events logged on protected computers in real-time;
- send control commands to protected computers;
- view information about the state of security subsystems on computers and send commands to change the security subsystem state;
- load and send group policy parameters specified in the Control Center to protected computers;
- validate licenses for the use of Secret Net Studio components;
- load logs from protected computers and send the log contents to the Security Server database;
- process database queries;
- archive and restore the log contents in the database;
- log the server queries.

The Security Server provides control and management of the protected computers, provided that the computers are subordinate to it. Computers with the Client installed and the OS Linux computers with Secret Net LSP installed (for these computers, some Security Server functions are unavailable) and other Security Servers can be subordinate to the Security Server.

MS SQL server-based database management system (DBMS) is required for the Security Server operation. The Security Server and the DBMS server can be installed on different computers (recommended) or on the same computer.

Authentication server

The Security Server includes the authentication server, which ensures the operation of firewall and network authentication mechanisms. The authentication server is installed and removed along with the Security Server.

Gateway

The Security Server software includes a separate component, the gateway. The Gateway is a service that provides a way for two Security Servers located in different and unrelated AD domain forests to communicate. One of them is parent or root to the other. The AD child domain server sends the data about agents performance to the root server and the root server sends security policy information to the AD domain child forest. It is also possible to manage agents on the root server from another AD forest.

Control Center

The Control Center installed on the administrator computers allows centralized management of the protected computers. To perform the required operations, the Control Center interacts with the Security Server.

The Client in network operation mode

To perform centralized control, the Client is to be installed on all protected computers in the network operation mode. These computers must be subordinated to the Security Server.

Secret Net Studio network structure

Security domains

Secret Net Studio uses security domains to implement the computer centralized control and the synchronization of security parameters. An Active Directory domain or organizational units (objects included in specific AD containers) form security domains. Like AD domains, several security domains (with their own Security Servers) may form a domain forest.

The first security domain in the AD domain is created when the first Security Server is installed.

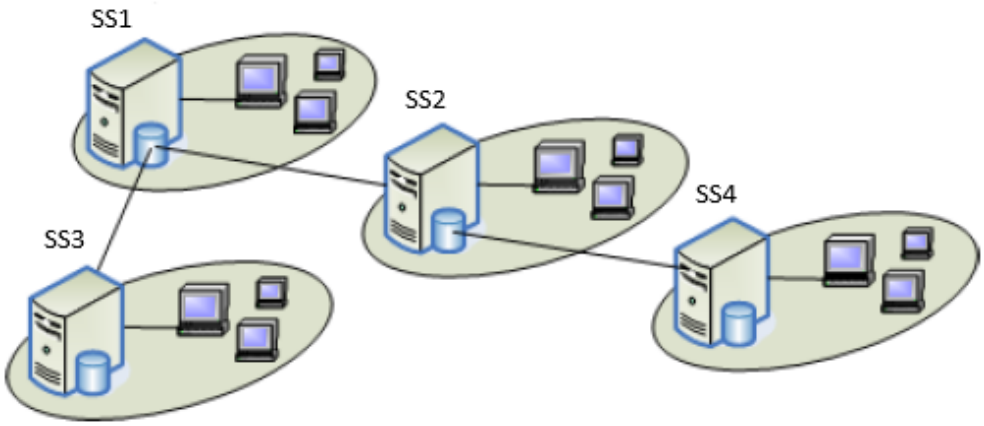
The Security Server uses Active Directory Lightweight Directory Services (AD LDS) to access the Active Directory folders. The security server controls the receipt and application of parameters for protected computers.

The security domain is created as part of the security domain forest structure. An administrator group, which includes users with privileges to create new security domains, is assigned to the security domain forest. When creating a security domain, the security domain administrator group is assigned to it.

Attention! For the continuous operation of protected computers, a permanently running standby Security Server in the security domain is required.

Security domain forests

Multiple security domains (with their own Security Servers) can build a domain forest in a similar way to Active Directory domains.
A group of users is assigned to the forest and the users are given the rights to create new security domains. This group is a group of security domain forest administrators.
Within a domain forest, it is possible to subordinate Security Servers hierarchically. However, the hierarchy of servers' subordination does not have to correspond to the structure of domains in the forest. In the picture below you can see an example of using multiple servers SS1 — SS4.



Each server controls its group of protected computers and has its own database. Moreover, some operations are also available for objects related to the subordinate servers. As can be seen from the picture, the Security Servers SS2 and SS3 are subordinate to SS1 and SS4 is subordinate to SS2.

Federation

Secret Net Studio allows organizing a hierarchical structure of security domain forests based on unrelated Windows AD domain forests. These are separate Windows AD domain forests with no trust relationship between them.

In this case, one of the Secret Net Studio security domain forests becomes the root or parent forest, and the rest become subordinate or child forests to it.

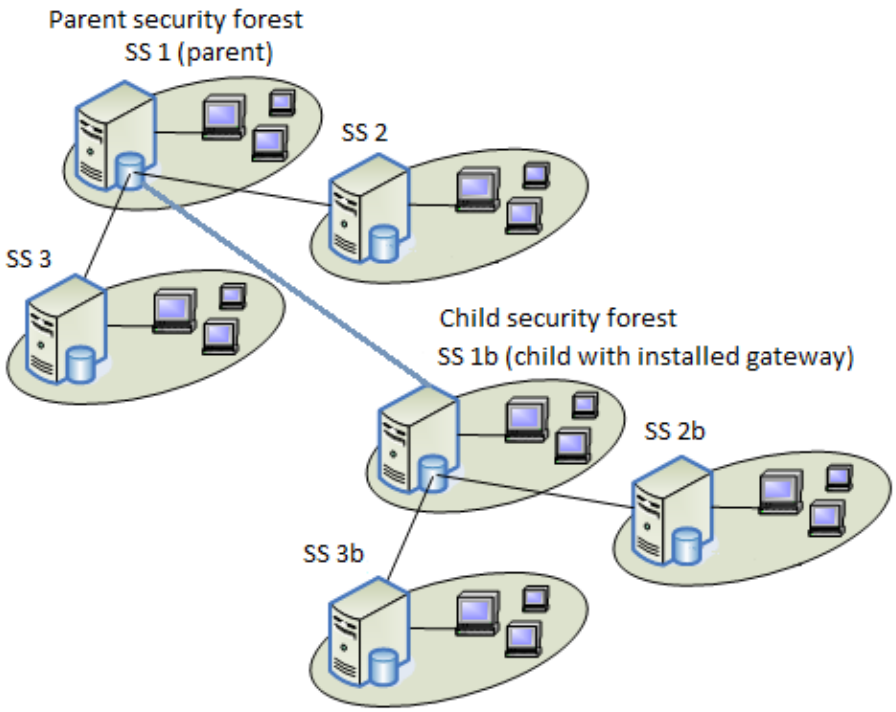
For security forests interaction a special gateway is used. The gateway is located in each of the child security forests. All of them are registered on the parent security server. All the security forests related to this server are united into a single entity called a federation.

To synchronize data between AD forests, a separate service is used. The synchronization service is installed on the child server. The service is deployed by a separate installer, which is built into the security server installation process.

After forests are united, an administrator working on the parent security server is able to do the following to operate protected computers from the child security forests:

- get updates on the protected computers status;
- send operational commands to protected computers;
- receive alerts and collect local logs from protected computers;
- manage the security settings of protected computers via group policies defined on the parent security server.

Within this network structure, it is possible to subordinate security forests hierarchically. On the picture below you can see an example that illustrates the subordination of one security forest to another.



Each forest has its own hierarchy of Security Servers. The SS 1b server has a gateway that connects this child server to the SS 1 parent server. When working on the SS1 parent server, the security administrator is able to control all servers and protected computers in the parent forest as well as all servers and protected computers in the child forest (within the limited range of possibilities listed above).

Restrictions

When planning and deploying this network structure, the following restrictions must be considered:

- only one gateway can be used for the interaction of two security forests. A second gateway cannot be installed between these two forests;
- there is only a two-tier hierarchy of security forests. This means that the child security forest cannot be subordinated to another child security forest.

Network structure design features

Secret Net Studio network structure is designed based on network features and distribution of administrator privileges. Granting privileges to security administrators is a key aspect of the Secret Net Studio network creation. To distribute the administrator privileges, create security domains based on organizational units. This allows distributing privileges to security administrators and Active Directory domain administrators to the extent required. Within an organizational unit, the security administrator can be granted all necessary privileges.

Data exchange between clients and the server is carried out in session mode. Data is transferred over the HTTPS protocol. A certificate must be installed on the server to protect the server connections.

Domain user management

Domain user parameters are configured in the Control Center. The program is part of the control tools and allows users to create and delete accounts, and to configure main user and group parameters.

It is recommended to use standard OS tools (user management tools) only for configuring the parameters not available in the Control Center. When creating or deleting accounts using standard tools, some control functions may be unavailable until the changes are synchronized with Secret Net Studio.

Centralized data storage

Secret Net Studio components use the following centralized data storage structures:

- Security Server database on the DBMS server – contains centralized logs and operational information for system monitoring;
- AD LDS service database – contains Secret Net Studio system parameters related to accounts, Security Server lists, security token lists, and other objects for the security system centralized management.

The repository partition is the result of handling data specifics. Data handling is performed only by components with the respective privileges. Control and access restriction are performed by Secret Net Studio, therefore, no further action on the part of administrators is required to ensure the security of data handling.

Chapter 5
About Secret Net Studio deployment

The Secret Net Studio system has a module structure. For details of the Secret Net Studio system architecture, see the previous chapters of this document.

Secret Net Studio components

The Secret Net Studio components are as follows:

1. Secret Net Studio — Client (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 8.1 Rollup Update KB2919355;
- Windows 7 SP1 KB3033929;
- Windows Server 2019;
- Windows Server 2016;
- Windows Server 2012 R2 Rollup Update KB2919355;
- Windows Server 2012;
- Windows Server 2008 R2 SP1 KB3033929.

Attention! To avoid security tools conflicts, before installing Secret Net Studio, you need to make sure other antivirus tools, access security tools, firewalls are not installed on protected computers.

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

Attention! If you want to use Trusted Environment, the computer must meet the requirements specified in the document [**2**].
In order to use Full Disk Encryption, the UEFI boot mode must be enabled.

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.

Note. For correct operation of the antivirus, Internet Explorer version 11 or later is required..

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 Secret Net Studio 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. **205**).

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 Visual C/C++ 2015-2019 Redistributable 14.28.29325;
- Microsoft .NET Framework 4.5;
- Microsoft service pack 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 2019;
- Windows Server 2016;
- Windows Server 2012 R2 Rollup Update KB2919355;
- Windows Server 2012;
- Windows Server 2008 R2 KB3033929.

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 including free SQL Server Express):

- Microsoft SQL Server 2019;
- Microsoft SQL Server 2017;
- Microsoft SQL Server 2016;
- Microsoft SQL Server 2014;
- Microsoft SQL Server 2012 SP1or later;

Note. Correct interaction between the security server and MS SQL DBMS is ensured by meeting the conditions specified in the Appendix on p. **205**.

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 the installation.

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

- Microsoft Visual C++ 2015-2019 Redistributable.

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 8.1 Rollup Update KB2919355;
- Windows 7 SP1;
- Windows Server 2019;
- Windows Server 2016;
- Windows Server 2012 R2 Rollup Update KB2919355;
- Windows Server 2012;
- Windows 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 kit

The Secret Net Studio system software and operating instructions are supplied on a setup disk or in an electronic form. 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

Folder	Content
\Tools\	Additional tools and files for software installation and setup

Secret Net Studio AutoRun program

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 AutoPlay 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 disc root folder.

The installer welcome window is shown in the figure below.

In this window, you can run the following commands:

Command	Purpose
Security Components	Run the Client setup program
Security Server	Run the Security Server setup program
Control Center	Run the Control Center setup program
Update server	Run the Update server setup program
Additional software	Open the \Tools\ directory in a separate window
Documentation	Open the \Documentation\ directory in a separate window
RU|EN|ES	Switch installation language

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, centralized installation via the Security Server is provided.

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 p. 35.

Attention! We do not recommend installing the Security Server on the domain controller

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. 45).
2. Complete the same steps as in step **1** on other computers that will be used as subordinate Security Servers.
3. Install the Control Center on Secret Net Studio administrator computers (see p. 52).
4. Install the Client in network operation mode (see p. 53) 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.
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 Administrators group;
   - install the Security Server (see p. 45).

   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. 210.

4. Install the Control Center on the security administrator computer (see p. 52).
5. Run the Control Center and establish a connection to the Security Server.
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. 57).
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 6
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. 40).

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 you install the Security Server for the first time, use the option that creates a new security domain forest and a new 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 AutoRun dialog box appears (see p. 42) and click **Security Server**.

   Note. You may start the installation without using the AutoRun program. To do that, run the following file from the setup disk: \Setup\Server\x64\setup.en-US.exe.

   When you run the setup wizard, it checks the computer for meeting software and hardware requirements of the components. 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 run the Security Server installation again.

   When the system check is complete, a dialog box with the list of components to install appears. You may choose to additionally install the Synchronization service.

   Note. The Synchronization service may be installed on a security server to act as a gateway and allow interaction between this Security Server and the parent Security Server. The Synchronization service is installed by a separate setup wizard that is run automatically after the Security Server is installed (see p. 51).

2. If you need to install the synchronization service on this server, select **Synchronization service**. Click **Install**.

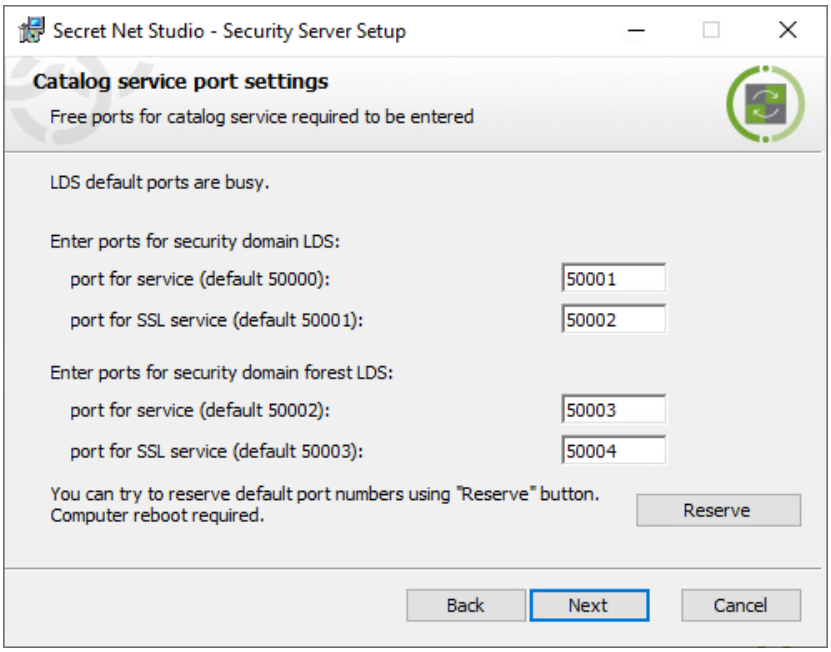
   The setup wizard begins its preparations, and then the welcome dialog box appears.

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

   The license agreement dialog box appears.

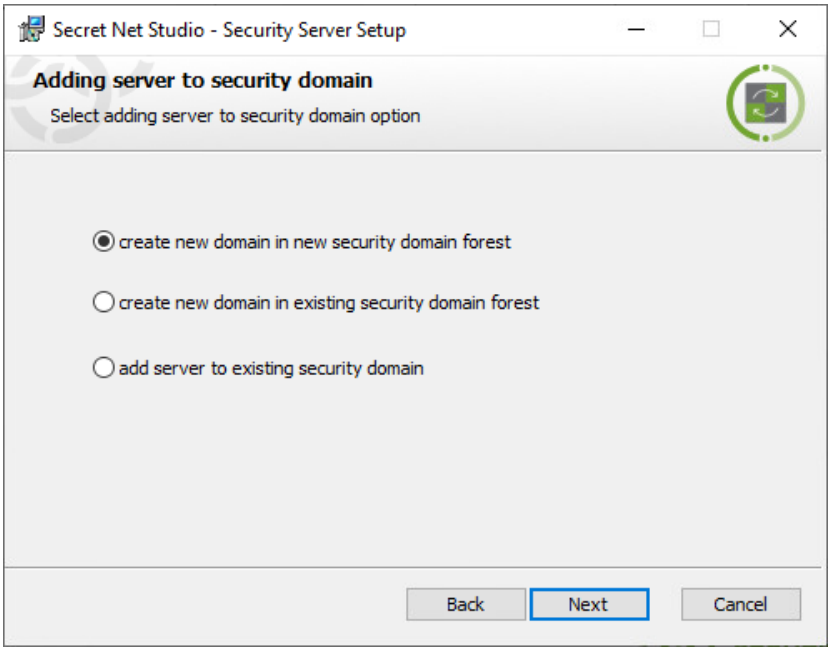
4. Read the license agreement, and if you agree with all its terms, select the accept check box and then click **Next**.

   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.



5. 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.



6. Select **create new domain in new security domains forest** 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.

7. 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 for adding new Security Servers 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.

8. In the drop-down list, select a container for creating 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).

9. Click **Next**.

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

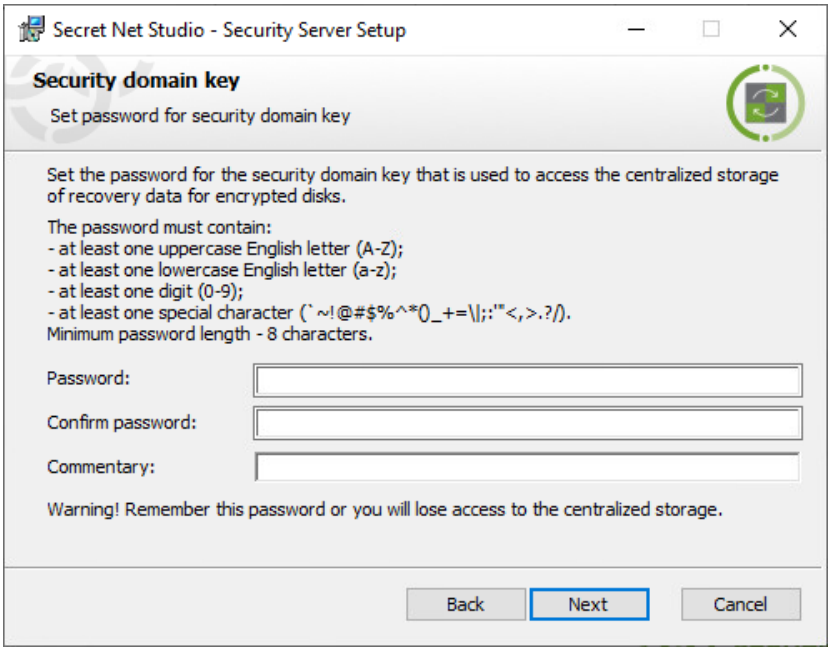
10. Select the user groups who you want to grant permissions to manage the security domain and security domain forest using the respective **Change** button. Click **Next**.

    Tip. For security purposes we recommend creating a new user group to use as security domain administrators. We do not recommend using the standard Domain Admins group.

    The **Folder settings** dialog box appears.

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

    The **Security domain key** dialog box appears as in the figure below.

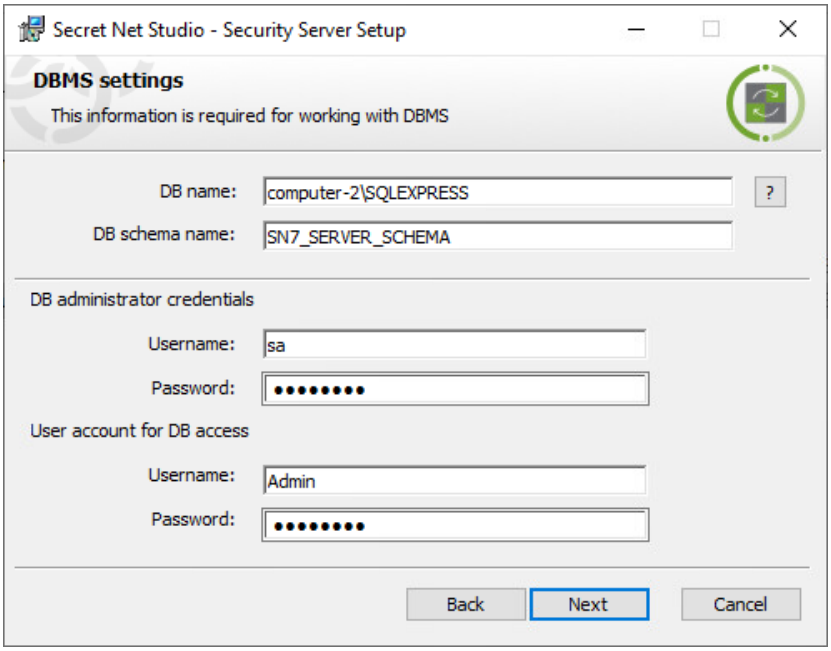


12. Set the password for the security domain key. The key and the password are required to access the centralized storage of recovery data for encrypted disks. The password must meet the requirements, specified in the dialog box.

Attention! Remember the password for the security domain key. Without the password you will lose access to the centralized storage of recovery data.

Confirm the password. If needed, enter the password commentary. Click **Next**.

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



13. 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 DB location, using the following format:
    <name_or_MS_SQL_server_IP_address>\<DB_instance_name>,<port>

Note.
- If the server containing DBMS is installed on a computer with the Security Server and the DBMS uses a standard MSSQLSERVER .instance, you may omit DBMS server name/IP address.
- If you use the default connection port, you do not need to specify it.

- in the **DB schema name** field, specify the name of the DB schema to be created;

Note. A separate DB schema is created for every Security Server.

- in the **DB administrator credentials** group of fields, specify the credentials of the DB administrator on the DBMS server;
- in the **User account for DB access** group of fields, specify the credentials that 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).
- Use English characters for credentials.

- Click **Next**.

14. 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 to create a new one. Select the needed option in this dialog box and click **Next**.

The **Organization name** dialog box appears.

15. 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.

16. 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 installation. Additional windows with service information may appear. These windows are closed automatically.

Note. If the user that runs Security Server installation is not a security domain administrator and/or a security domain forest administrator, the setup wizard requests the respective administrator credentials on this step.

If you chose to install the Synchronization service in step **2**, its setup wizard welcome dialog box appears. Perform the installation according to steps on p. **51**.

After the installation and setting are finished successfully, a window with the list of setup program operations appears. After all the operations are completed, you will be asked to restart the computer.

17. 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. We recommend you to wait for the synchronization to complete and not to perform any actions with the accounts, including the first logon on the protected computer. If the first logon 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 new 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 **1–5** of the Security Server installation procedure with the creation of a new forest and security domain (see p. **45**).
2. In the **Include Server in the Security Domain** dialog box, select **create new domain in existing security domains forest** 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**.

   Note. If the user that runs Security Server installation is not a security domain forest administrator, the setup wizard requests the respective administrator credentials in this step.

   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. **45**) starting from step **10**.

Adding new 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 and add it to an existing security domain:

1. Perform steps **1–5** of the Security Server installation procedure with the creation of a new forest and security domain (see p. **45**).
2. In the **Include Server in the Security Domain** dialog box, select **add server to existing security domain** 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**.

   A dialog box containing information about the security domain of the parent Security Server appears.

6. Click **Next**.

Note. If the user that runs Security Server installation is not a security domain administrator and a security domain forest administrator, the setup wizard requests both sets of administrator credentials in this step.

The **Directory Settings** dialog box appears. Next follow the installation procedure for creating new forest and new security domain (see p. 45) starting from step **11**.

Installing gateway software

Gateway software, the Synchronization service is a component of the Security Server and may be installed either during the Server installation or separately. The Synchronization service setup wizard is run by the Security Server setup wizard if you select the option to install it when you:

- install the Security Server;
- update the Security Server;
- run the setup wizard of the same version as the installed Security Server — use this option to install gateway software on an installed and operating Security Server.

Attention! Correct installation of the synchronization service requires the following:
- Registering a respective gateway on the parent Security Server via the Control Center;
- A special file with the gateway settings (.pav) on the computer with the installed child Security Server;
- The computer with the child Security Server must be able to establish a network connection with the computer with the parent Security Server using its full DNS name.

To install the synchronization service:

1. After performing the preparations a welcome dialog box of the setup wizard appears. Click **Next**.

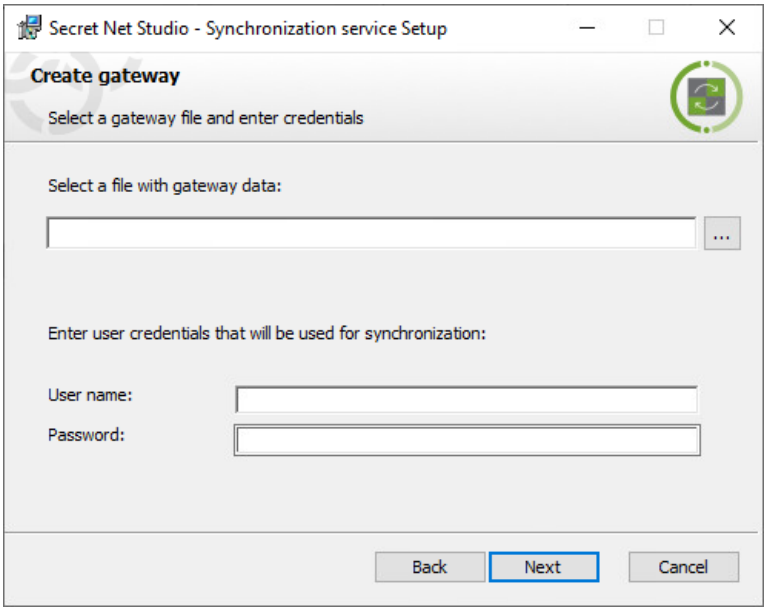
   The license agreement dialog box appears.

2. Read the license agreement, then select the **Accept** check box and click **Next**.

   The **Destination folder** dialog box appears.

3. Specify the required folder if necessary and click **Next**.

   A dialog box appears as in the figure below.



4. Enter the information necessary to create a gateway.
   - Click the **Browse** button and select the required gateway file.
   - Enter user credentials that were used to create the gateway in the root (parent) security domain forest.
   - Click **Next**.

   If the specified information is correct, a dialog box with information about the gateway appears.
5. Click **Next**.

   If the specified server is available, the **Ready to install** dialog box appears.
6. Click **Install**.

   The setup wizard begins to install the Synchronization service. A progress bar appears, showing the progress of the installation. When the installation successfully finishes, a dialog box with the respective message appears.
7. Click **Finish**.

   After the installation you will be returned to the Security Server setup wizard. Follow the wizard instructions, including computer restart.

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. 42) and click **Control Center**.

   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. **57**). In particular, if the Client is installed for use in the autonomous mode.

Interactive installation

To install the Client:

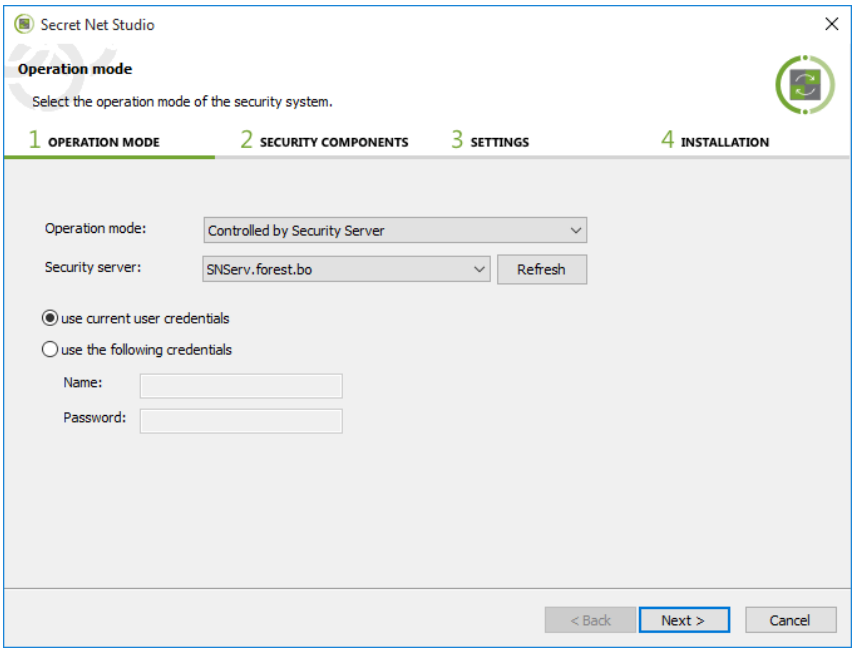
1. Insert the Secret Net Studio setup disk into the drive. Wait until the installer welcome window appears (see p. **42**) and click the **Security components** command.

   Note. If AutoRun is disabled on your computer, the installer cannot be run automatically. In this case, in order to launch the setup wizard, 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.

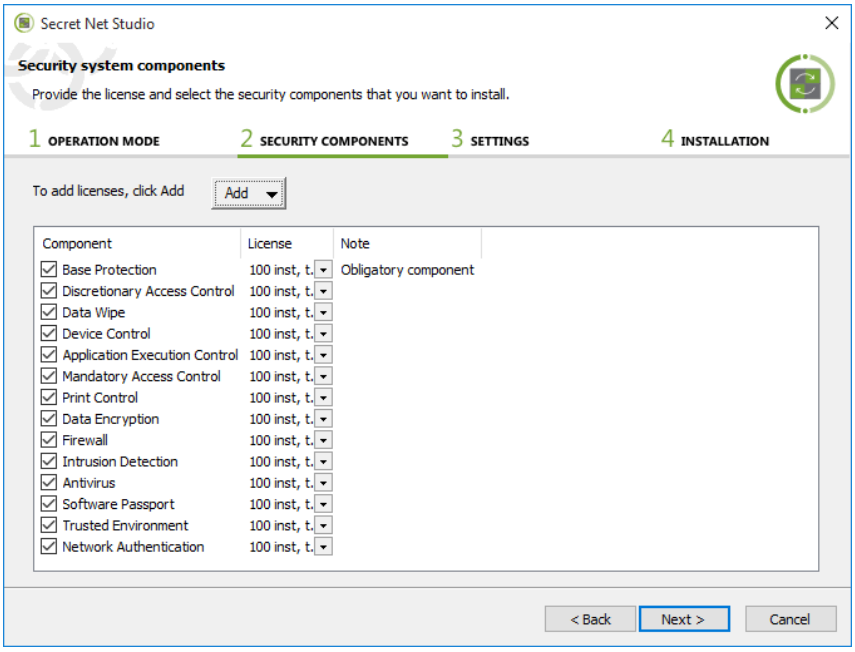


3. In the **Operation Mode** field, specify the required Client operation mode: autonomous (select **Standalone mode**) or network (select **Controlled by Security Server**). If you select the network operation mode, configure the settings of subordination to the Security Server:
   - Select the name of the Security Server this computer will be subordinate to (if the needed name is not present in the drop-down list, click **Refresh** to refresh the list).

- 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 these rights, select **use current user credentials**. Otherwise, select **use the following credentials** check box and enter the credentials 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.



5. Select the method of adding licenses:

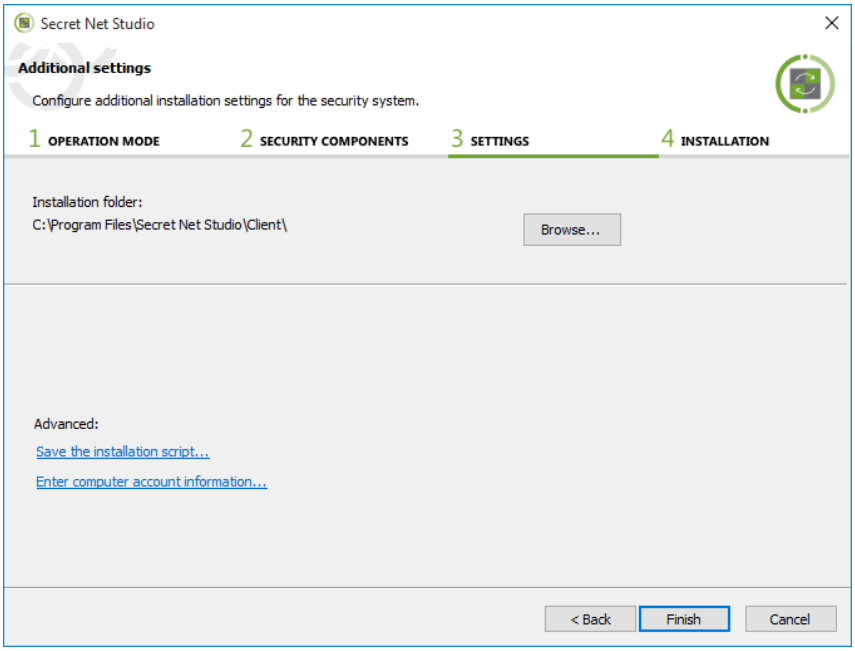
- To add licenses from the Security Server that will control this computer, click **Add** and click **From the Security Server**.
- To add licenses from a file (for example, if you need use the Client in standalone mode), click **Add** and click **From a file**, then select the required file in the appearing dialog box.

After the data is loaded, license information appears in the dialog box.

6. In the list, select the subsystems that will be installed and for which there are free licenses (the **Base Protection** subsystem cannot be disabled). If there are several license groups for the subsystem, you can select the relevant group from the drop-down list.

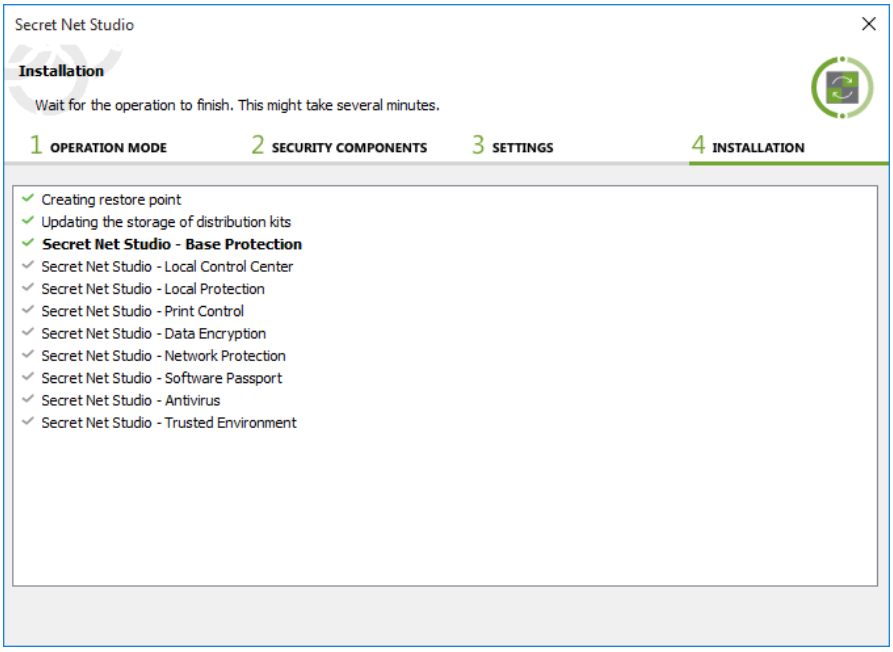
7. Click **Next**.

A dialog box appears as in the figure below.



8. In the **Installation folder** field, leave the default folder or specify another one to install the Client.
9. Use the links in the **Advanced** section to perform the following actions (if necessary):
   - To save specified installation settings to a file, click **Save the Installation Script**. Installation scripts can be used to automate the Client installation on other computers.
   - To enter information about the computer for registration purposes, click **Enter computer account information**.
   - To view and select patches that will be applied during installation, click **Select patches to install**.
10. After the configuration is complete, click **Finish**.

    The protection subsystems installation begins according to specified settings.



11. 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.

12. Check the list of devices connected to the computer. Disconnect the devices which usage should 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 must disconnect the devices that are to be prohibited before restarting the computer.

Tip. If necessary, use the links in the Information area to take the following actions:

- to view trace log records, click the **installation report** link;
- to collect all the files and data necessary for Secret Net Studio diagnostics if an error occurred during the installation, click the **diagnostics data** link.

13. Restart the computer.

Chapter 7
Installing the Client centrally

You can install the Client centrally from the Control Center. 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 receives 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. 39). 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.

Installing under the control of the Security Server

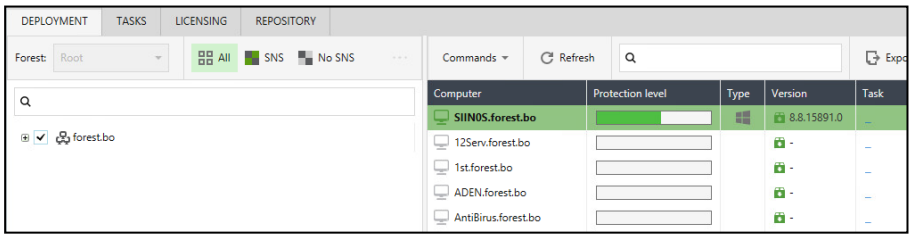
Centralized Client installation under the control of the Security Server is initiated via the Control Center. In the Control Center, you can select, what software to install and to create deployment tasks.

The Client will install automatically (in the background) on the client computers. The user will be notified about the start and the finish of the installation. Depending on the deployment settings, the computer will restart automatically or the user will be offered to restart the computer manually.

Attention! Before performing centralized installation, make sure that the client computers meet hardware and software requirements of the Client (see p. 39). In particular, resource sharing ports: 137, 138, 139, 445 must be opened. By default, these ports are closed by the Firewall if no network folders exist on the computer.

Settings and control features panel

Centralized software deployment is configured and controlled in the **Deployment** panel. The panel is shown in the figure below.



The following tabs in the panel are used for working with deployment settings and control features:

- **Deployment** displays the management structure (on the left) and the list of computers with details of existing software and status (on the right).
- **Tasks** displays deployment tasks (on the left) and task-related computers (on the right).
- **Licensing** is designed for viewing details of and managing registered licenses on the Security Server.
- **Repository** is designed for generating a list of centrally installed software.

To switch between the tabs, use the respective buttons at the top of the panel.

Managing the licenses for using security mechanisms

The Secret Net Studio system has license restrictions on the use of subsystems that implement the use of security mechanisms. Licenses are delivered in the form of files containing data for registration in the Secret Net Studio system.

Attention! If the license is expired, it cannot be used to install the client software. If the license is not activated, the Client can be installed interactively.

If the license for at least one operating subsystem is not activated or is expired, the client software enters a limited operation mode. In the limited operation mode you cannot configure the security system settings or run most of the security tools.

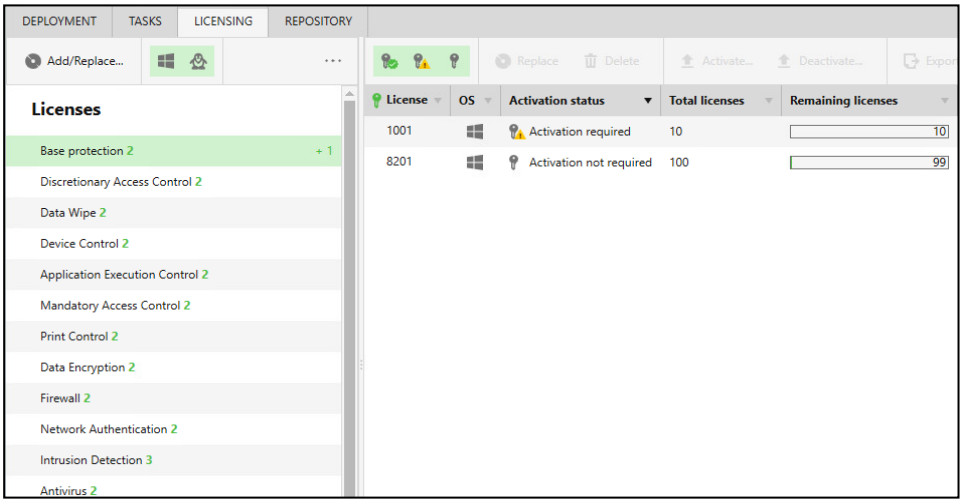
When creating software deployment tasks (see p. 61), you must specify the appropriate licenses. Licenses can be selected from the list of licenses registered on the Security Server or can be added separately for the deployment task.

To manage registered licenses, use the **Licensing** tab on the **Deployment** panel. The tab contains information about the licenses registered in the security domain of the connection server (the security server to which the program is connected):

- license assignment (for which subsystems the licenses are used);
- the type of operating system for which the licenses are intended (Windows/Linux);
- license activation status;
- total number and current number of unused (remaining) licenses;
- expiration time of licensed features;
- license types;
- information about the company that receives the license.

To register licenses:

1. On the **Deployment** panel, go to the **Licensing** tab.



2. At the top left of the panel, click **Add/Replace**.

   A dialog for selecting a file will appear on the screen.
3. Select the required license file and click **Apply**.
4. If the licenses are not activated, click **Next**. Select the required license activation option and click **Apply**.
5. When you select activation via your personal account, upload the request file to the activation page in your personal account, wait for the license activation and download the file with the activated licenses.

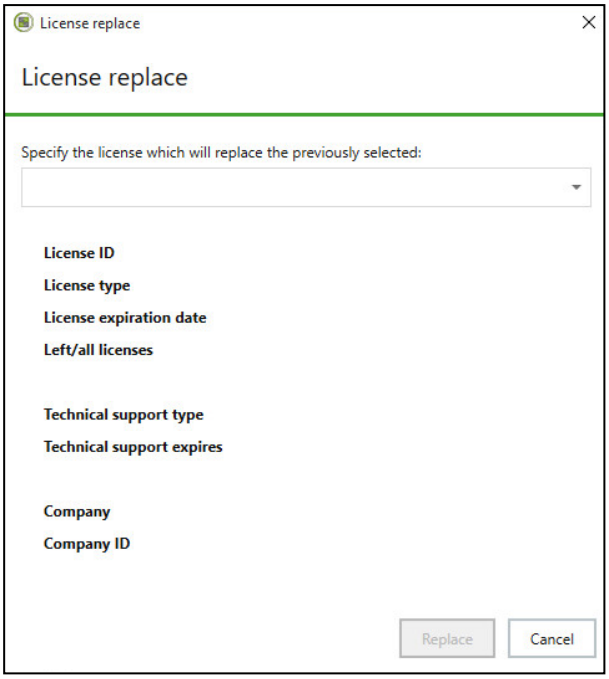
   Add the file with the activated licenses to the server and confirm the replacement operation.

To replace registered licenses:

1. On the **Deployment** panel, go to the **Licensing** tab.
2. On the **Licenses** list (on the left), select the subsystem that requires replacing licenses.
3. On the list of available licenses for using the subsystem (on the right), select licenses to replace.

4. Above the list of licenses, click **Replace**.

   The **License replace** dialog box appears as in the figure below.



5. Select a license from the drop-down list and click **Replace**.

To delete registered licenses:

1. On the **Deployment** panel, go to the **Licensing** tab.
2. On the **Licenses** list (on the left), select the subsystem that requires deleting licenses.
3. On the list of available licenses for using the subsystem (on the right), select the licenses to delete.

   Note. You cannot delete a license if it is used on at least one protected computer.

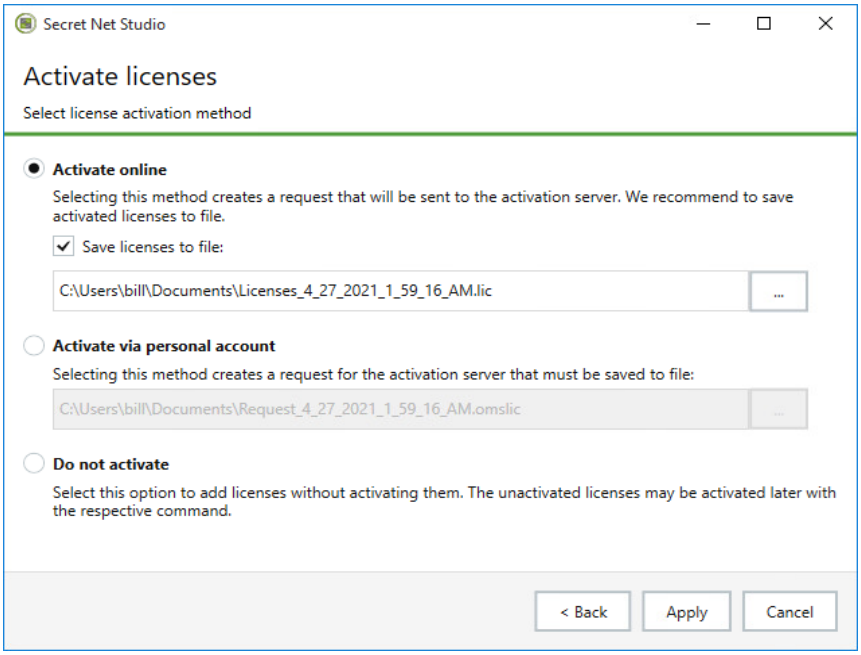
4. Above the list of licenses, click **Delete**.

   The prompt to continue the operation appears on the screen.
5. Click **Yes**.

To activate registered licenses:

1. On the **Deployment** panel, go to the **Licensing** tab.
2. On the **Licenses** list (on the left), select the subsystem that requires activating licenses.
3. On the list of available licenses (on the right), select the licenses to activate.
4. Above the list of licenses, click **Activate**.

   A dialog box appears as in the figure below.



5. Select the license activation option and click **Apply**.
6. When you select activation via your personal account, upload the request file to the activation page in your personal account, wait for the license activation and download the file with the activated licenses.

   Add the file with the activated licenses to the server and confirm the replacement operation.

To deactivate registered licenses:

1. On the **Deployment** panel, go to the **Licensing** tab.
2. On the **Licenses** list (on the left), select the subsystem that requires deactivating the licenses.
3. On the list of available licenses (on the right), select the licenses to deactivate.

   Note. The license cannot be deactivated if it is used on at least one protected computer.

4. Above the list of licenses, click **Deactivate**.

   The **Deactivate licenses** dialog box appears.
5. Select the option to deactivate the license and click **Apply**.

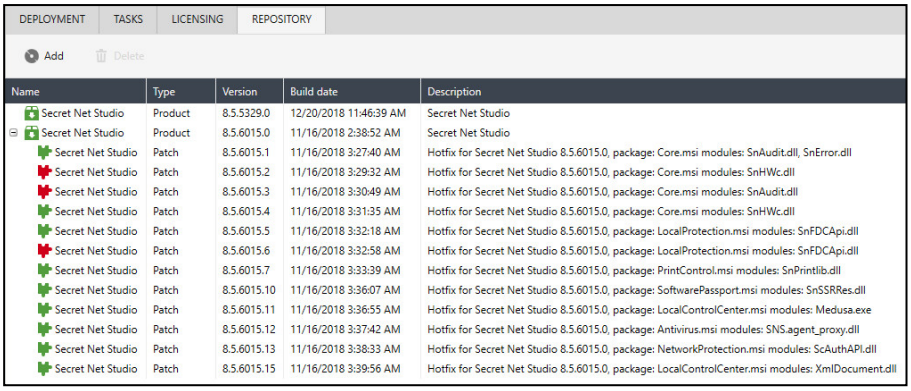
Creating a list of centrally installed software

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.

Attention! You need to place distribution kits to the **Repository** folder. It is created during the installation of the Security server in the **Server** installation folder and **Sharing** is configured. Do not change **Sharing** options to this folder, otherwise the centralized software installation will not be possible.

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

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



Comment. Patches with red icons are critical.

2. Click **Add** at the top of the **Repository** tab.

   The **Add** dialog box appears.

3. In the respective dialog box, click **Add**.

   The dialog box asking you to select the folder with the distribution kit appears.

4. In the **Folder** field, enter or select the path to the folder containing the distribution kit to create the installation package and click **Select Folder**. For example, if you want to use the Secret Net Studio system setup disk and a patch to create the installation package, select the root folder of the installation disk. If you want to create an installation package from a patch, select the patch's root folder from **\Tools\SecurityCode\Patches**.

   The patch will be added to the list of centrally installed software only if the Secret Net Studio setup disk was added to the repository earlier.

   Attention! The version of the Secret Net Studio distribution kit must match the version of the patch.

   In the **Add** dialog box, a new list item containing the information about the downloaded patch appears.

5. 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).

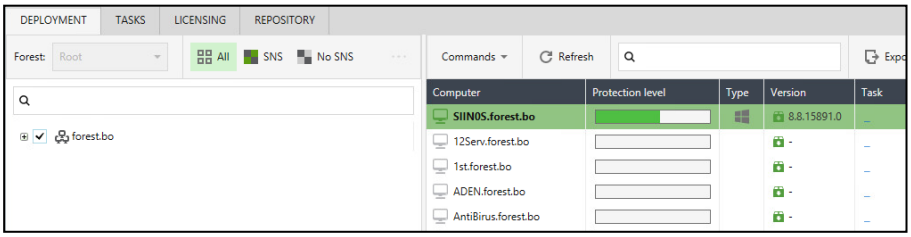
6. Click **Close**.
   When the process is completed, a new item appears in the list with information about the installation package.

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** panel, click **Deployment**.



2. If there are multiple forests, configure the structure display using the **Forest** drop-down list.

3. 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 (**SNS** or **No SNS** 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. The names of computers subordinate to the Security Server are highlighted in bold and their icons turn green.

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

Computers subordinate to the Security Server are indicated by the green icon and their names are written in bold.

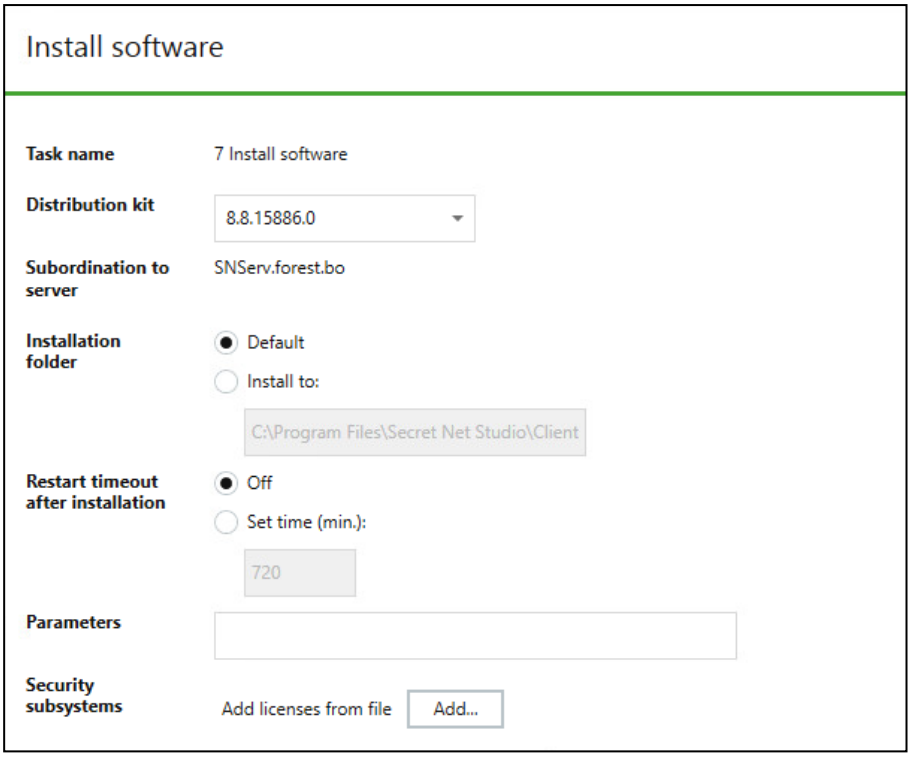
You can view additional information about computers by double-clicking a respective line or by clicking the upward arrow located in the bottom right corner of the **Deployment** panel.

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.

4. Right-click one of the selected computers and click the respective command. The list of commands:

Command	Description
Install software	Install the Client software (see detailed configuration description below)
Update software	Update the Client software version installed previously. In this case, the **Restart timeout after installation** parameter is configured for the task and the client version is specified for updating. Software update starts at a user logoff
Repair software	Repair the Client software installed previously. After clicking the command, the notification of an added task appears. The software repair starts on computer restart
Uninstall software	Uninstall the Client software installed previously. After clicking the command, the notification of an added task appears. The software uninstallation starts automatically on the selected computers
Install patch	Install update patches. In this case, in task parameters, you may select one or more patches uploaded to the repository previously. Patch installation starts on computer restart
Uninstall all patches	Uninstall all the patches installed previously. After clicking the command, the notification of an added task appears. Patch uninstallation on the selected computers begins on computer restart

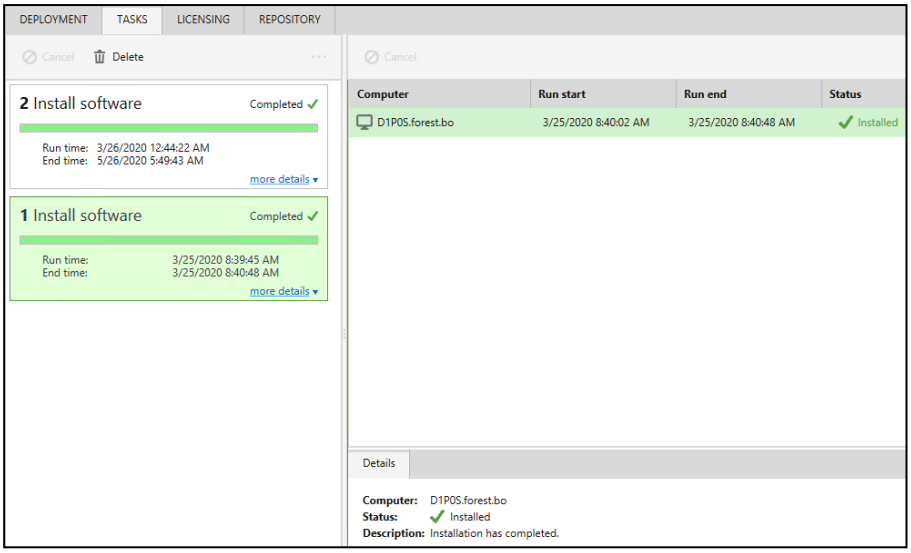
The task settings panel appears on the right of the window as in the figure below.



5. To configure the Client installation task, specify the following settings:
   - version of the software to be installed;
   - software installation folder;
   - restart timeout after installation — if **Off** is selected, the computer does not restart automatically after the software installation. To enable the automatic restart mode, select **Set time** and specify the number of minutes, after which the computer will be restarted;

     Tip. While configuring the software update task parameters, this parameter defines the timeout for the automatic computer restart after the computer receives the task. The timeout is specified in minutes. The software is updated at the computer restart.
   - parameters — determines the parameters of the command prompt that need to be applied to the installation (optional);
   - component licenses;
   - patches;
   - local administrator account data (a member of the local Administrators group on selected computers).

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

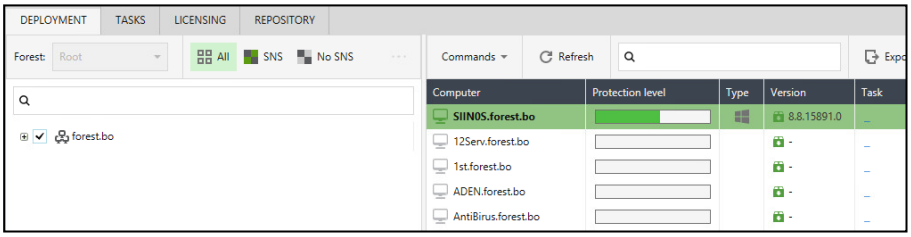


Controlling task execution

Created tasks are applied on computers based on respective settings. The administrator can use the **Tasks** list to control software deployment.

To control task execution:

1. Go to the **Tasks** tab in the **Deployment** panel.



   The time and status of process execution appear for tasks and computers.

2. To display additional details about a task, click **details** at the bottom of the information section. To view detailed information about the computer, enable the display of the information area using the button located on the right side of the line under the list of computers.

   Note. If the process does not start for a long time, check that the computer meets hardware and software requirements for installation of the Client (see p. 39). For example, a task can only be executed if the following ports, used to access shared resources, are enabled on the computer: 137, 138, 139, 445. By default, these ports are closed by the firewall if there are no shared folders on the computer. To permit the use of the above ports, modify firewall settings or create a folder and make it shared.

3. If you need to cancel a task:
   - To cancel execution on all computers, to which the task relates, select it and click **Cancel** above the tasks list in the **Task** section;
   - To cancel execution on individual computers, select them in the list and click **Cancel** above the list of computers in the **Computer** section.

   Attention! A task can be canceled only before its execution starts. If you click **Cancel** while the task execution is in progress, the task is displayed as a canceled one, but it is still being executed.

4. When the task is done, it can be removed from the list. To do this, select it and click **Delete** above the tasks list in the **Task** section.

Group policy-based Client installation

Group policy-based Client installation is performed by specifically configuring group policies on the computers of specific organizational units. The Client will be installed

or updated on each computer on restart. If the Client is not installed on the computer, it will be installed. If the Client is installed, it will be updated to the latest version.

System configuration for automatic installation and update consists of the following steps:

1. Configure the OM structure (see p. 65).
2. Create files with a setup scenario (see p. 65).
3. Create a public network resource (see p. 70).
4. Create OUs and move the required computers into them (see p. 71).
5. Create and configure group policies for the required OUs (see p. 71).

Configuring the OM structure

Before installing the Client automatically on the required computers, you need to add them to the OM structure. To do that, make each of them subordinate to the Security Server. For that, the system must contain the required structure of Security Servers and a Secret Net Studio administrator account.

Computers without the installed Client can be made subordinate to Security Servers via the Control Center.

Note. You do not have to make subordinate the computers where you want to use the Client in standalone mode.

Creating files with a setup scenario

An installation scenario is aimed at automating the installation process of the Client - it automatically inputs all the information, required by the Client Setup Wizard.

Scenario files are created in the INI file format and are the configuration files that contain the necessary data for installing Secret Net Studio Client. After creating the required scenario files, move them to the root folder of the previously created PNR (see p. 70).

You can create scenario files via the Client Setup Wizard (see p. 53) or manually.

Tip. For a scenario template, you may use a scenario file created via the Client Setup Wizard or an example specified below.

To create a scenario file manually:

- In a text editor, create a file SnInst.rsp, enter all the necessary information and save the file.

Scenario file structure

Scenario files must have the following structure:

[Section_1]

parameter_1 = parameter_value_1

parameter_2 = parameter_value_2

...

parameter_N = parameter_value_N

[Section_2]

parameter_1 = parameter_value_1

parameter_2 = parameter_value_2

...

parameter_N = parameter_value_N

[Section_N]

parameter_1 = parameter_value_1

parameter_2 = parameter_value_2

...

parameter_N = parameter_value_N

Every Section contains parameters and their values required by the Client Setup Wizard. The main sections and parameters are provided in the table below.

Parameter	Default value	Commentary
Section [Core]		
Action	install	Select the value for the **Base protection** component: • **install** – install the component; • **none** – do not install the component
Section [Console]		
Action	install	Select the value for the **Local Control Center** component: • **install** – install the component; • **none** – do not install the component
Section [Local]		
Action	none	Select the value for the **Local Protection** component group: • **install** – install the components; • **none** – do not install the components
ERASER	0	Select the value for the **Data Wipe** component: • **1** — enable after the installation; • **0** — disable after the installation
DC	0	Select the value for the **Device Control** component: • **1** — enable after the installation; • **0** — disable after the installation
FDC	0	Select the value for the **Discretionary Access Control** component: • **1** — enable after the installation; • **0** — disable after the installation
EXEQUOTA	0	Select the value for the **Application Execution Control** component: • **1** — enable after the installation; • **0** — disable after the installation
MC	0	Select the value for the **Mandatory Access Control** component: • **1** — enable after the installation; • **0** — disable after the installation
Section [Pc]		
Action	none	Select the value for the **Print Control** component: • **install** – install the component; • **none** – do not install the component
Section [Disk]		
Action	none	Select the value for the **Disk Protection and Data Encryption** component group: • **install** – install the components; • **none** – do not install the components
TBL	0	Select the value for the **Disk Protection** component: • **1** — enable after the installation; • **0** — disable after the installation

Parameter	Default value	Commentary
CRCONT	0	Select the value for the **Data Encryption** component: • **1** — enable after the installation; • **0** — disable after the installation
Section [Ta]		
Action	none	Select the value for the **Network Protection** component group: • **install** – install the components; • **none** – do not install the components
TA_Firewall	0	Select the value for the **Firewall** component: • **1** — enable after the installation; • **0** — disable after the installation
TA_IPSEC	0	Select the value for the **Network Authentication** component: • **1** — enable after the installation; • **0** — disable after the installation
TA_IDS	0	Select the value for the **Intrusion Detection** component: • **1** — enable after the installation; • **0** — disable after the installation
Section [Antivirus]		
Action	none	Select the value for the **Antivirus** component: • **install** – install the component; • **none** – do not install the component
Section [Common]		
Installdir	[ProgramFilesFolder]Secret Net Studio\Client	Select the folder where you want to install the Client
User	empty	Name of a user from Security Domain Administrators group
Password	empty	User password
Server	empty	Select the Client operation mode: • Security Server SID – network operation mode; • empty –stand-alone operation mode
Source *	empty	Enter the path to the Client installation file
Division	empty	Computer account information: Department name
SysName	empty	Computer account information: Information system name
Workplace	empty	Computer account information: Workstation
Id	empty	Computer account information: System unit number
LicenseFilePath *	empty	Path to a license file
Servername	empty	Security Server DNS name
locale **	empty	Select the language of the Client: • **ru-RU** – Russian; • **en-US** – English
RebootTimeOut	empty	Installation restart timeout in minutes
Section [Softpspt]		

Parameter	Default value	Commentary
Action	none	Select the value for the **Software Passport** component: • **install** – install the component; • **none** – do not install the component
Section [Patches]		
Count	empty	Number of normal patches to install
PatchN	empty	Path to the normal patch, where **N** is the patch sequence number
Section [Te]		
Action	none	Select the value for the **Trusted Environment** component: • **install** – install the component; • **none** – do not install the component

* Required parameter.

** Required and case-sensitive parameter

You may use environment variables to specify the path. Names of environment variables must be put in brackets and placed at the beginning of the parameter value. Applicable environment variables are provided in the table below.

Environment variables	Value example
WindowsVolume	C:\
WindowsFolder	C:\WINDOWS\
USERPROFILE	C:\Documents and Settings\Ivanov\
TemplateFolder	C:\Documents and Settings\All Users\Templates\
TempFolder	C:\Documents and Settings\Ivanov\Local Settings\Temp
SystemFolder	C:\WINDOWS\system32\
StartupFolder	C:\Documents and Settings\All Users\Start Menu\Programs\Startup\
StartMenuFolder	C:\Documents and Settings\All Users\Start Menu
SendToFolder	C:\Documents and Settings\Ivanov\SendTo\
ProgramMenuFolder	C:\Documents and Settings\All Users\Start Menu\Programs\
PrimaryVolumePath	C:\
PersonalFolder	C:\Documents and Settings\Ivanov\My Documents\
MyPicturesFolder	C:\Documents and Settings\Ivanov\My Documents\My Pictures\
LocalAppDataFolder	C:\Documents and Settings\Ivanov\Local Settings\Application Data\
FontsFolder	C:\WINDOWS\Fonts\
FavoritesFolder	C:\Documents and Settings\Ivanov\Favorites\
CommonFilesFolder	C:\Program Files\Common Files\
CommonAppDataFolder	C:\Documents and Settings\All Users\Application Data\
ProgramFilesFolder	C:\Program Files\
AppDataFolder	C:\Documents and Settings\Ivanov\Application Data
AdminToolsFolder	C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\
ALLUSERSPROFILE	C:\Documents and Settings\All Users

Scenario file contents example

Below you may find an example of scenario file contents to install the Client in standalone mode.

```
[core]
Action=install
[console]
Action=install
[local]
Action=install
ERASER=1
DC=1
FDC=1
EXEQUOTA=1
MC=1
[pc]
Action=none
[disk]
Action=install
TBL=1
CRCONT=1
[ta]
Action=install
TA_Firewall=1
TA_IPSEC=1
TA_IDS=1
[antivirus]
Action=install
[Common]
Installdir=C:\Program Files\Secret Net Studio\Client\
server=
Source=\\computer.TWinfo.local\OSR
LicenseFilePath=full_new
locale=en-US
[softpspt]
Action=none
[patches]
count=2
patch0=\\computer.TWinfo.local\OSR\tools\SecurityCode\Patches\8_ 5_ 5329_ 8_ Inc72574_Build5\
patch1=\\computer.TWinfo.local\OSR\tools\SecurityCode\Patches\8_ 5_ 5329_ 9_ Inc72994_Build6\
```

This example includes the following actions:

1. Install the **Base protection** component.
2. Install the **Local Control Center**.
3. Install the **Local Protection** component group:
   - Enable the **Data Wipe** component.
   - Enable the **Device Control** component.
   - Enable the **Discretionary Access Control** component.

- Enable the **Application Execution Control** component.
- Enable the **Mandatory Access Control** component.

4. Do not install the **Print Control** component.
5. Install the **Disk Protection and Data Encryption** component group.
   - Enable the **Disk Protection** component.
   - Enable the **Data Encryption** component.
6. Install the **Network protection** component group.
   - Enable the **Firewall** component.
   - Enable the **Network Authentication** component.
   - Enable the **Intrusion Detection** component.
7. Install the **Antivirus** component.
8. Install the Client to the following folder: System_drive\Program Files\Secret Net Studio\Client.
   - Security Identifier of the Security Server is empty - install the Client install the Client in standalone operation mode.
   - Source of the Client installation file:\\computer.TWinfo.local\OSR.
   - Use license file: **full_new**.
   - Install the English version of the Client.
9. Do not install the **Software Passport** component.
10. Install 2 normal patches. All critical patches are installed automatically.
    - Two patches with their paths.

Note. The scenario may contain only one type of antivirus mechanism, according to the selected license: Antivirus, Antivirus (ESET technology) or Antivirus (Kaspersky technology).

Creating a public network resource

In the AD domain, create a public network resource (PNR) that contains Client installation files, a license file and an installation scenario file.

Attention! If the AD domain contains multiple Security Servers, you must create a separate PNR with respective contents for each of them.

To create a PNR:

1. On one of the domain computers, create a new folder and, in its properties, enable sharing.

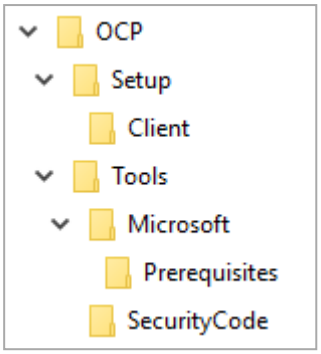
   Attention! Additionally grant permissions to **Read** the contents of that folder to all computer accounts where you plan to install the Client or to the **Domain Computers** group.

   Note. The computer must be available for network connections during the installation. We recommend creating the PNR on one of domain file servers.

2. Copy the contents of the required folders from the Secret Net Studio installation disk to the created PNR. The required folders with the required subfolders are provided in the table below.

Folder name	Role
\Setup\Client\	Contains Client distribution kits for 32-bit and 64-bit Windows versions
\Tools\Microsoft\Prerequisites	Contains installation files of the required Windows OS updates. If any of the files are missing, the installation will not be performed
\Tools\SecurityCode\	Contains additional tools and configuration files necessary for working with Secret Net Studio

PNR folder structure can be seen on the figure below.



3. Copy a Secret Net Studio license file to the created PNR.

   Tip. If you plan to use the Client in network operation mode, additionally add licenses from the Secret Net Studio license file to the Security Server.

4. Copy the scenario file to the created PNR.

Configuring Active Directory

Creating organizational units

To isolate specific domain computers to automatically install the Client, create OUs and move the required computers into them. You may also use existing OUs.

Creating OUs and moving computers requires standard administrative tools.

Creating and configuring group policies

After the OUs are ready, you need to create group policies for automatic installation of the Client. Separate group policies must be created for 32-bit and 64-bit Windows OS versions.

After the automatic Client installation is completed on all the required computers, you may delete the group policies.

To create a group policy on the Domain Controller:

1. Run **Group Policy Management**.
2. Right-click on the OU with the required computers, then click **Create a GPO in this domain and Link it here**. The **New GPO** dialog box appears.
3. Enter the name of the new policy and click **OK**.

   The new policy appears in the hierarchical list as a subobject of the OU.
4. Right-click on the policy and click **Edit**.

   The **Group Policy Management Editor** window appears.
5. Click **Computer Configuration > Policies > Software Settings** then right-click **Software installation** and click **New > Package**.

   Open dialog box appears.
6. Type the path to the required file in the **File name** field:
   - to apply the policy to computers with 32-bit Windows OS, type: *<network_path_to_the_PNR>*\Setup\Client\Win32\InstAgent.msi;
   - to apply the policy to computers with 64-bit Windows OS, type: *<network_path_to_the_PNR>*\Setup\Client\x64\InstAgent.msi.
7. Click **Open**.

   The **Deploy Software** window appears.
8. Click **OK**.

   Tip. For the created 32-bit distribution kit version, we recommend to clear the **Make this 32-bit X86 application available to Win64 machines** check box. To do that, in package properties, select the **Deployment** tab, then click **Advanced** and clear the check box.

Tip. If you use several OUs for automatic Client installation, you do not have to create a policy for every OU. You can create links to an existing policy. To do so, right-click the other OU and click **Link an Existing GPO**.

To apply the created group policy:

1. Restart the computer where you want to install the Client.
2. Log on as a user.

   After the successful logon, a message about started installation will appear above the Secret Net Studio icon in the notification area. Secret Net Studio component installation will begin after computer restart.

SCCM-based installation

You may centrally perform Secret Net Studio operations via a special Microsoft Windows tool for managing IT infrastructure — System Center Configuration Manager (SCCM).

Using SCCM tools you may:

- install, update, repair and uninstall Client software;
- install and uninstall patches.

System configuration procedure consists of the following steps:

1. Configure the OM structure (see p. 72).
2. Create files with a setup scenario (see p. 72).
3. Create a SCCM public network resource (see p. 74).
4. Configure SCCM (see p. 74).

Configuring the OM structure

Computers where you plan to perform central operations must be made subordinate to the Security Server. For that, the system must contain the required structure of Security Servers and a Secret Net Studio administrator account.

Computers without the installed Client can be made subordinate to Security Servers via the Control Center.

Note. You do not have to make subordinate the computers where you want to use the Client in standalone mode.

Creating files with a setup scenario

Scenario file creation for centrally installing Client software is performed the same way as during group policy-based installation (see p. 65).

Scenario file contents example

Below you may find an example of scenario file contents to install the Client in network mode.

```
[core]
Action=install
[console]
Action=install
[local]
Action=install
ERASER=1
DC=1
FDC=1
EXEQUOTA=1
MC=1
[pc]
Action=install
```

```
[disk]
Action=install
TBL=1
CRCONT=1
[Common]
Action=install
Installdir=C:\Program Files\Secret Net Studio\Client\
server=S-1-5-21-3534210826-639358159-2414785253-3826
Source=\\MSS2012\OSR\
LicenseFilePath=lic
servername=WIN-ATC89VIN2B9.testsn7.ru
locale=en-US
[ta]
Action=install
TA_Firewall=1
TA_IPSEC=1
TA_IDS=1
[softpspt]
Action=none
[te]
Action=none
[antivirus]
Action=install
[patches]
count=3
patch0=\\MSS2012\OSR\tools\SecurityCode\Patches\8_ 6_ 6186_ 11_ IncidentTest_LocalControlCentre_Client\
patch1=\\MSS2012\OSR\tools\SecurityCode\Patches\8_ 6_ 6186_ 14_ IncidentTest_AuthServer_Server\
patch2=\\MSS2012\OSR\tools\SecurityCode\Patches\8_ 6_ 6186_ 16_ IncidentTest5_Core_Client\
```

This example includes the following actions:

1. Install the **Base protection** component.
2. Install the **Local Control Center**.
3. Install the **Local Protection** component group.
   - Enable the **Data Wipe** component.
   - Enable the **Device Control** component.
   - Enable the **Discretionary Access Control** component.
   - Enable the **Application Execution Control** component.
   - Enable the **Mandatory Access Control** component.
4. Install the **Print Control** component.
5. Install the **Disk Protection and Data Encryption** component group.
   - Enable the **Disk Protection** component.
   - Enable the **Data Encryption** component.
6. Install the product to the following folder: System drive\ Secret Net Studio\Client
   - Security identifier of the Security Server: S- 1- 5- 21- 3534210826-639358159-2414785253-3826.
   - Source of the Client installation file: \\MSS2012\OSR.

- Use license file: **lic**.
- Security Server DNS name: WIN-ATC89VIN2B9.testsn7.ru.
- Install the English version of the Client.

7. Install the **Network protection** component group.
   - Enable the **Firewall** component.
   - Enable the **Network Authentication** component.
   - Enable the **Intrusion Detection** component.
8. Do not install the **Software Passport** component.
9. Do not install the **Trusted Environment** component.
10. Install the **Antivirus** component.
11. Install 3 normal patches. All critical patches are installed automatically.
    - Three patches with their paths.

Note. The scenario may contain only one type of antivirus mechanism, according to the selected license.

Creating a SCCM public network resource

In the AD domain, create a public network resource (PNR) that contains Client installation files, a license file and an installation scenario file.

Attention! If the AD domain contains multiple Security Servers, you must create a separate PNR with respective contents for each of them.

To create a PNR:

1. On one of the domain computers, create a new folder and, in its properties, enable sharing. Additionally, grant the **Read** permission to the accounts of computers where you plan to install the Client.

   Note. The computer must be available for network connections during the installation. We recommend creating the PNR on one of domain file servers.

2. Copy a Secret Net Studio license file to the created PNR.

   Tip. If you plan to use the Client in network operation mode, additionally add licenses from the Secret Net Studio license file to the Security Server.

3. Copy the scenario file to the created PNR.

   Note. To update, repair, uninstall the Client or uninstall patches you do not have to copy the license file or the scenario file to the PNR.

Configuring SCCM

There are the following ways to install the Client via the SCCM:

- installation package;
- application.

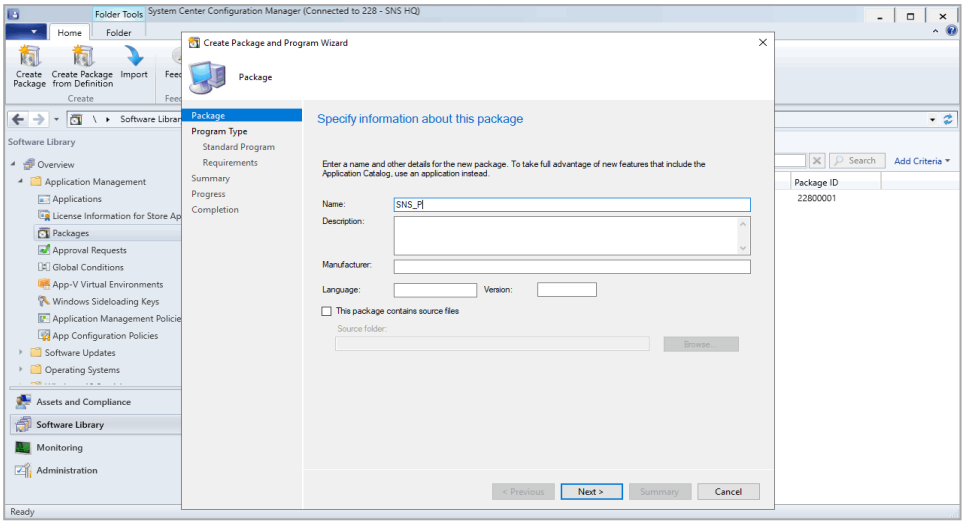
Deploying an installation package via SCCM

To centrally deploy the Client you need to create and install the installation package .

To create an installation package:

1. Run **System Center Configuration Manager**.
2. At the bottom left of the navigation panel (on the left of the main window), select **Software library**.
3. At the top of the navigation panel (on the left of the main window), expand **Application Management**.
4. Right-click the **Packages** item and click **Create Package**.

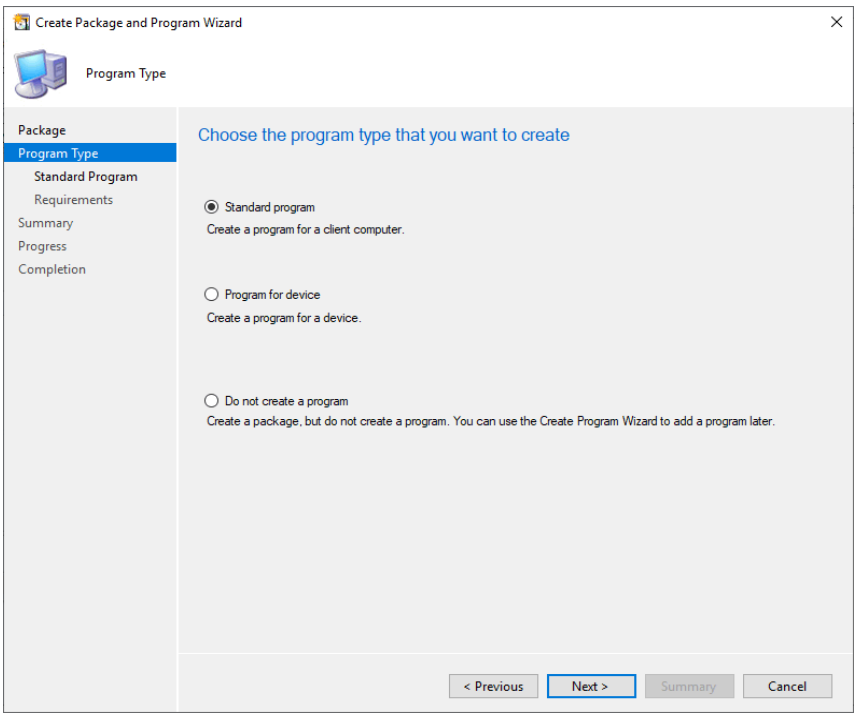
   A dialog box appears as in the figure below.



5. In the **Name** field, specify the name of the package and click **Next**.

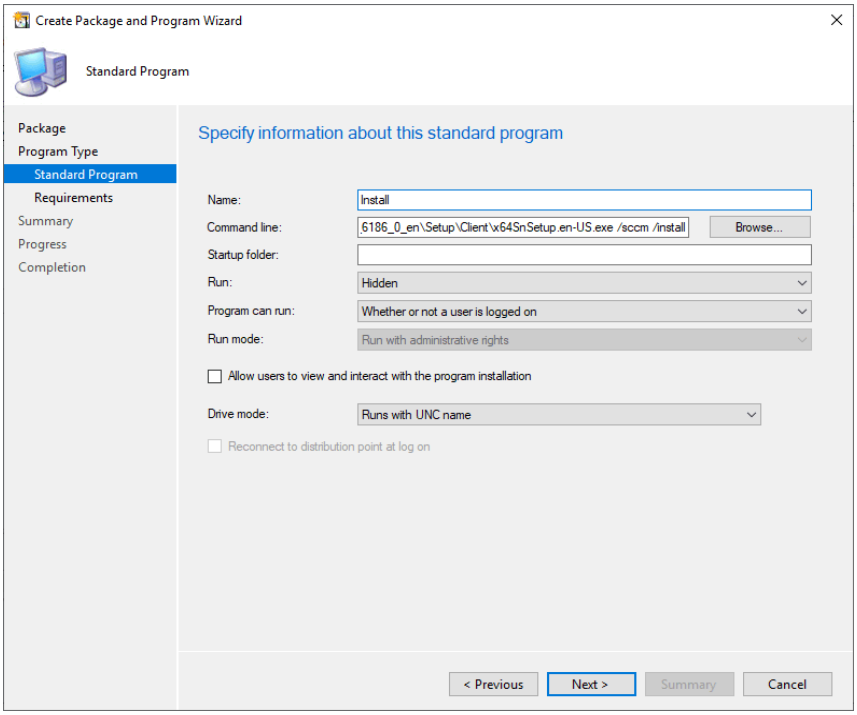
Note. If the distribution kit is located on the PNR, you do not have to select the **This package contains source files** check box.

A dialog box appears as in the figure below.



6. Select **Standard program** and click **Next**.

A dialog box appears as in the figure below.



7. Specify information:
   - in the **Name** field, specify the name of the standard program;
   - in the **Command line** field, specify the path to the distribution kit and the command in a required format (see below);
   - in the **Run** field, select **Hidden**;
   - in the **Program can run** field, select **Whether or not a user is logged on**.

   Click **Next**.

   A dialog box, containing requirement for the standard program appears.

   The **Command line** field has the following input format:

   ```
   <path to distribution kit> /sccm /<command>
   ```

   The descriptions of different commands are specified in the table below.

Command	Description
install [/timeout:x]	Install the Client
upgrade	Update the previously installed version of the Client to a new version
repair	Repair the previously installed Client
uninstall	Uninstall the previously installed Client
applypatch "path to the folder with the patch"	Install a patch
removeallpatches	Uninstall all previously installed patches

8. Click **Next**.

   A dialog box for confirming specified information appears.
9. Check the correctness of the specified information and click **Next**.

   The wizard starts creating the installation package.
10. When package creation is finished, click **Close**.

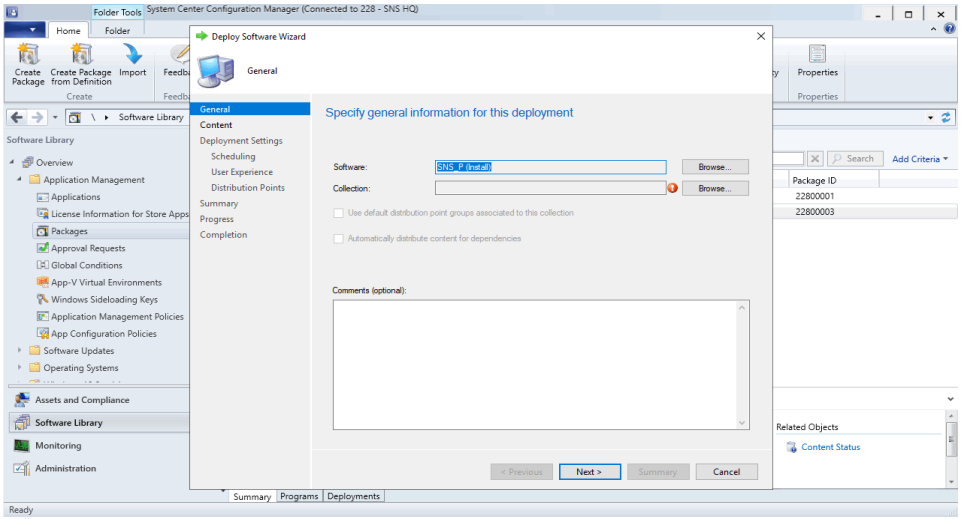
After you finish package installation, the new package with the specified information appears in the installation package list.

Note. New standard programs should be added to the installation package after it is created. To add a new standard program, right-click the created installation package then click **Create Program**, and follow steps **6–10**.

To install a standard program from a created installation package:

1. Run **System Center Configuration Manager**.
2. At the bottom of the navigation panel (on the left of the main window), select **Software Library**.
3. At the top of the navigation panel (on the left of the main window), expand **Application Management**.
4. Select **Packages**.
5. On the package list, select the previously created package.
6. At the bottom of the main window, select the **Programs** and select the previously created standard program.
7. Right-click the standard program and click **Deploy**.

   A dialog box appears as in the figure below.

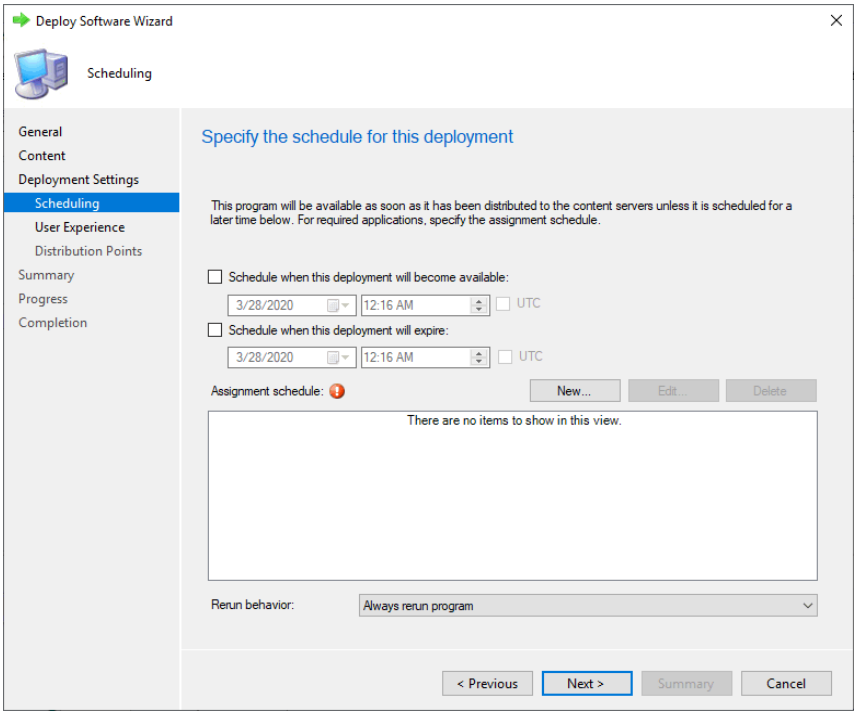


8. In the **Collection** field, click **Browse** and on the list, select the computer collection where you need to install the installation package and click **OK**.
9. Click **Next**.

   A dialog box for configuring content distribution appears.
10. Click **Next**.

    A dialog box for configuring software deployment settings appears.
11. In the **Purpose** field, select **Required** and click **Next**.

    A dialog box for configuring the deployment schedule appears.



12. Do the following:

- Click **New**:
  - Select **Assign immediately after the event**;
  - In the drop-down list, select **As soon as possible**.
- Click **OK**.

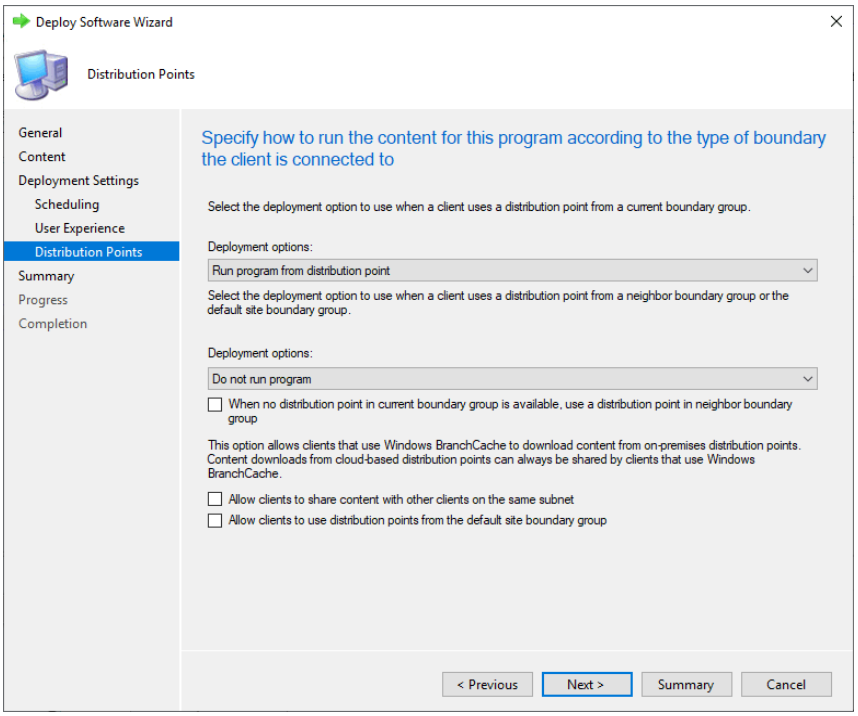
The new item will be added to the schedule list.

13. In the **Rerun behavior** list, select **Always rerun program** and click **Next**.

A dialog box for configuring user experience during the installation appears.

14. Click **Next**.

A dialog box appears as in the figure below.



15. In the **Deployment options** field, select **Run program from distribution point** and click **Next**.

    A dialog box for confirming deployment settings appears.

16. Check the correctness of the settings and click **Next**.

    The wizard begins installing the standard program.

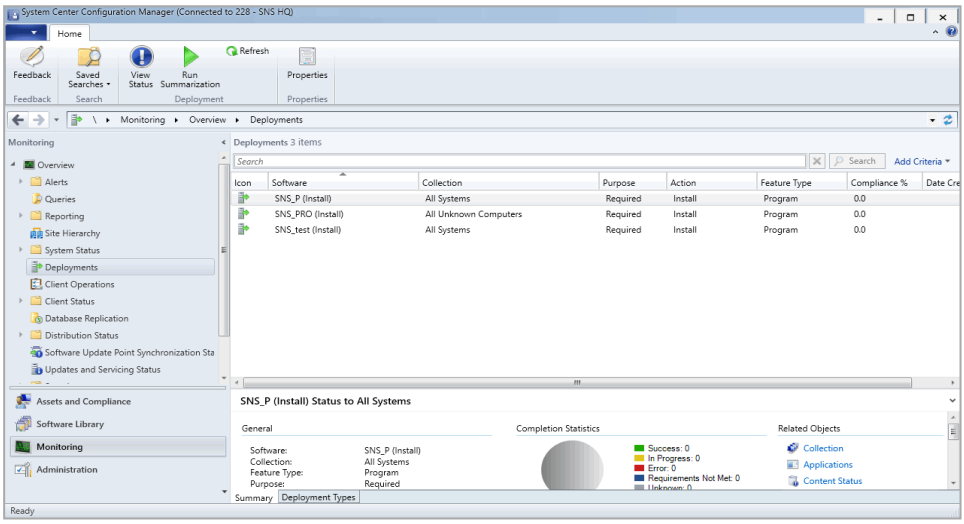
17. When the installation is finished, click **Close**.

Note. To install previously created programs from the installation package, follow steps **6–17**.

To monitor standard program deployment:

1. Run **System Center Configuration Manager**.
2. At the bottom of the navigation panel, select **Monitoring**.
3. At the top of the navigation panel, click **Deployments**.

   A dialog box appears as in the figure below.



4. On the software list, select the required standard program and view its status.

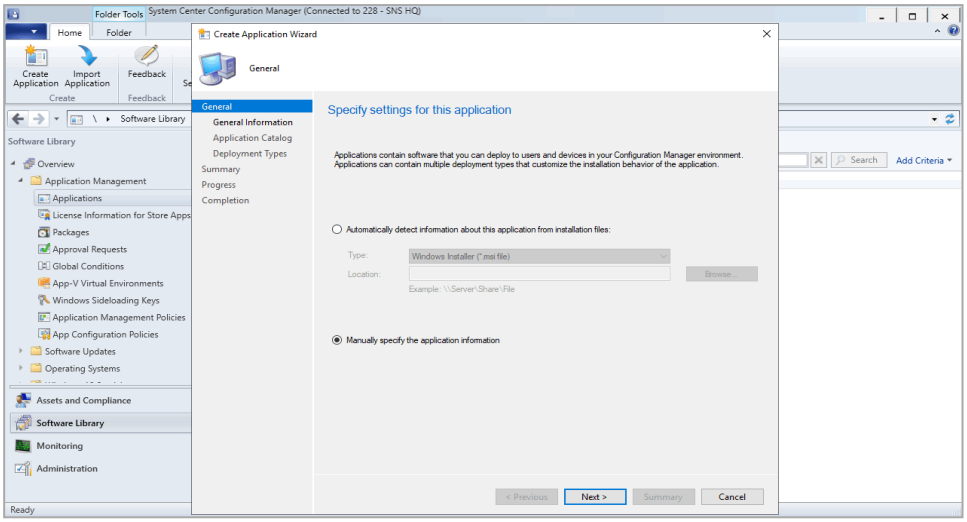
Deploying an application via SCCM

To centrally deploy the Client you must create and install an application.

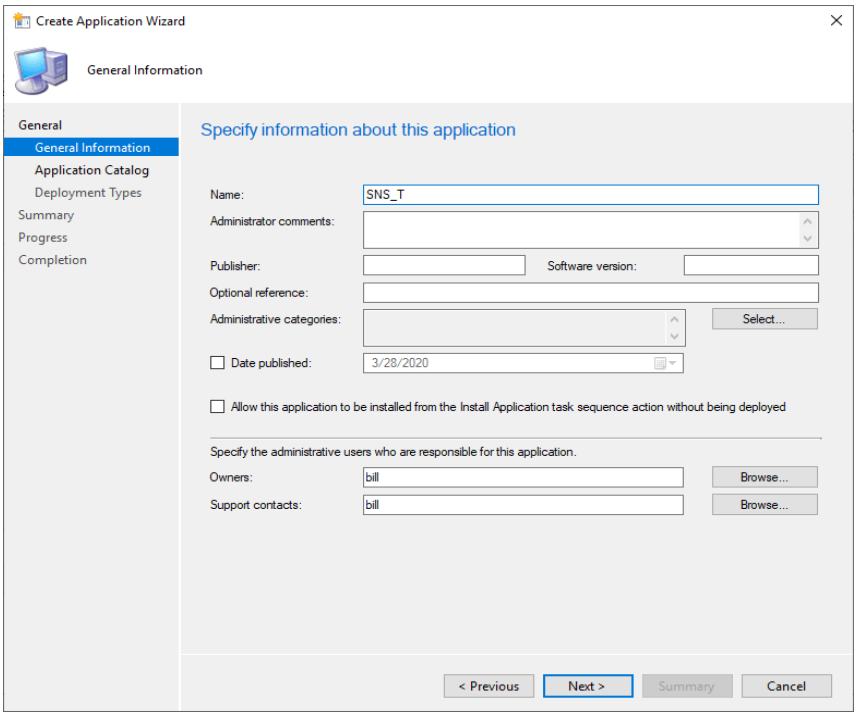
To create an application:

1. Run **System Center Configuration Manager**.
2. At the bottom of the navigation panel (on the left of the main window), select **Software Library**.
3. At the top of the navigation panel (on the left of the main window), expand **Application Management**.
4. Right-click **Applications** and click **Create application**.

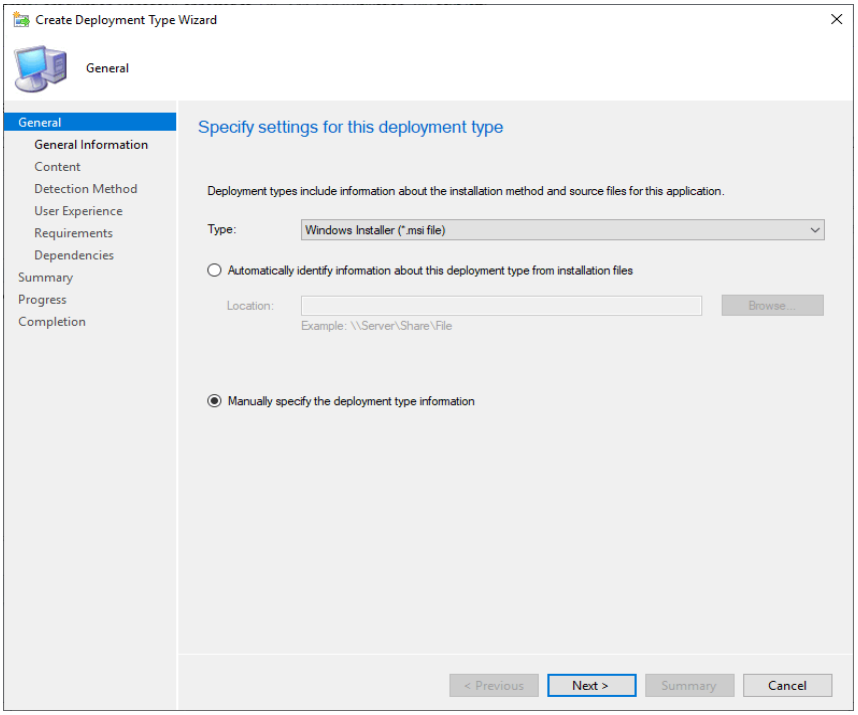
   A dialog box appears as in the figure below.



5. Select **Manually specify the application information** and click **Next**.
   A dialog box appears as in the figure below.

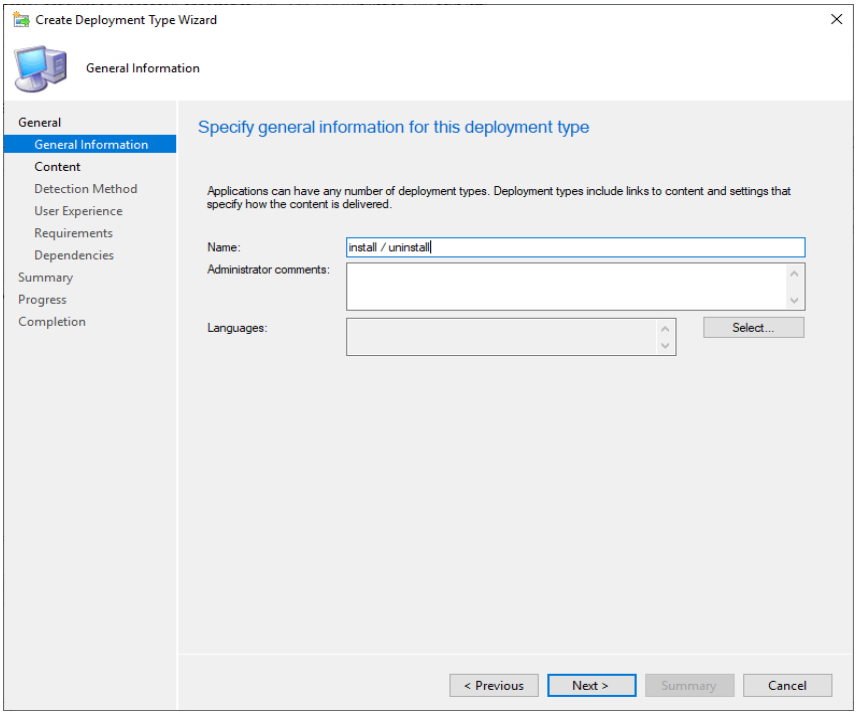


6. In the **Name** field, enter the application name and click **Next**.
   The **Application Catalog** dialog box appears.
7. Click **Next**.
   The **Deployment Types** dialog box appears.
8. Click **Add**.
   The **Deployment type creation wizard** dialog box appears.



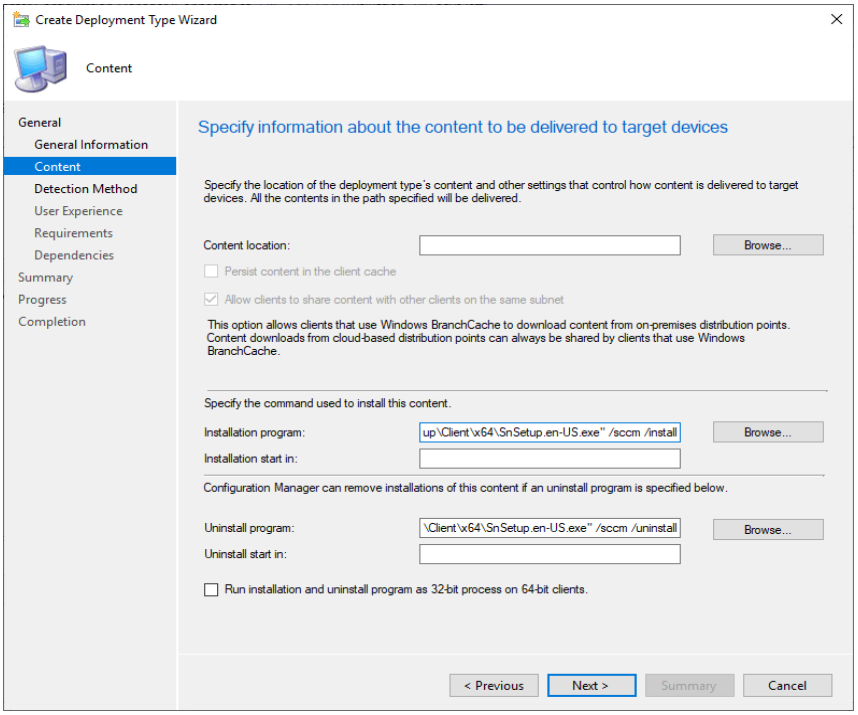
9. In the **Type** field, select **Windows Installer (*.msi file)**, then select **Manually specify the deployment type information** and click **Next**.

A dialog box appears as in the figure below.



10. In the **Name** field, enter the deployment type name and click **Next**.

The **Content** dialog box appears.



11. Enter required information:

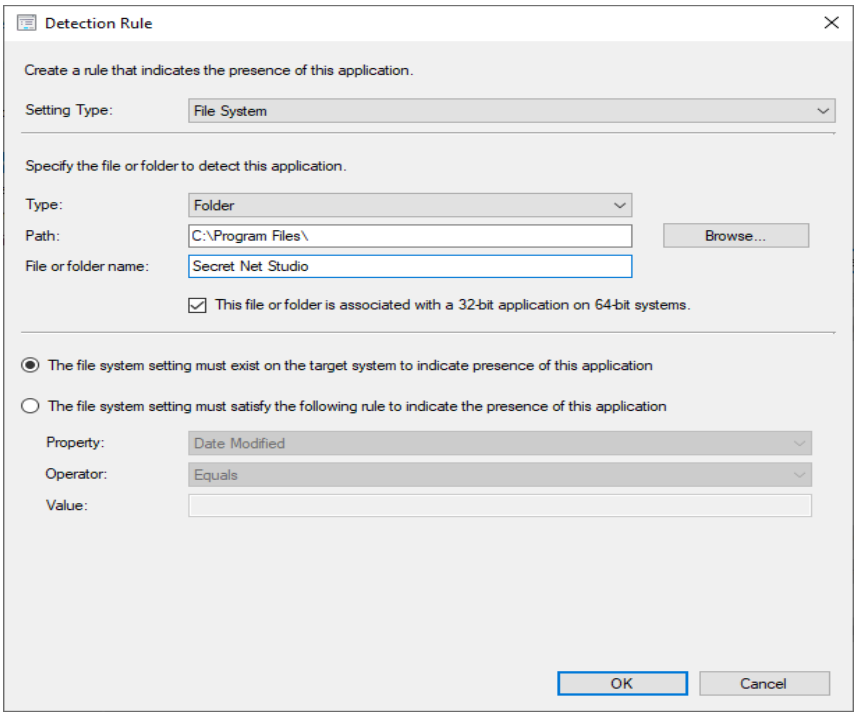
- in the **Installation program** field, enter the path to the distribution kit and the command (see p. **76**);
- in the **Uninstall program** field, enter the path to the distribution kit and the command (see p. **76**).

Click **Next**.

The **Detection Method** dialog box appears.

12. Click **Add Clause**.

The **Detection Rule** dialog box appears.



13. Enter required information:

- in the **Path** field, enter the path to the \Program Files folder;

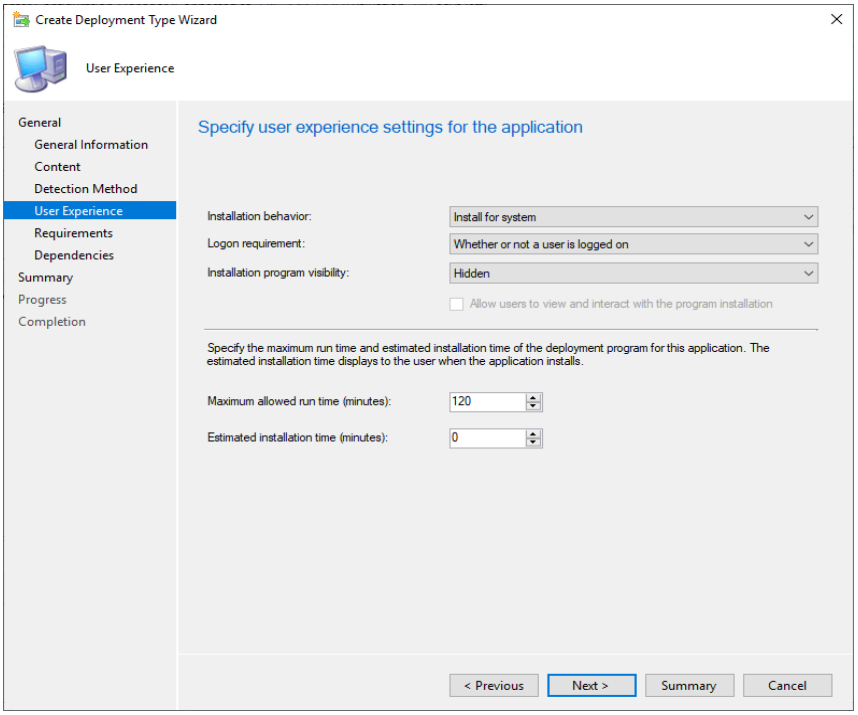
- in the **File of folder name** field, enter the path to the \Secret Net Studio folder.

Click **OK**.

The new rule is added to the detection rule list.

14. Click **Next**.

The **User Experience** dialog box appears.



15. Specify required information:

- In the **Installation behavior** field, select **Install for system**;
- In the **Logon requirement** field, select **Whether or not a user is logged on**;
- In the **Installation program visibility** field, select **Hidden**.

Click **Next**.

The **Requirements** dialog box appears.

16. Click **Next**.

The **Dependencies** dialog box appears.

17. Click **Next**.

A dialog box for confirming deployment settings appears.

18. Check the correctness of the specified settings and click **Next**.

The wizard begins creating the deployment type.

19. When the creation is finished, click **Next**.

The new element is added to the deployment type list.

20. Click **Next**.

A dialog box for confirming application settings appears.

21. Check the correctness of the specified settings and click **Next**.

The wizard begins creating the application.

22. When the creation is finished, click **Next**.

After the creation the new application is added to the list of applications.

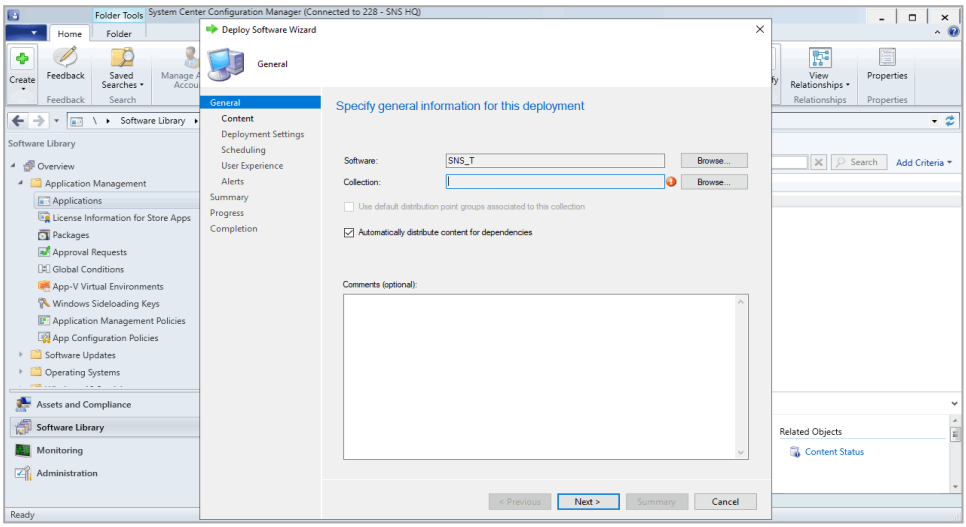
Note. Applications for installing and uninstalling patches are created in a similar manner.

To install the created application:

1. Run **System Center Configuration Manager**.

2. At the bottom of the navigation panel (on the left of the main window), select **Software library**.
3. At the top of the navigation panel (on the left of the main window), expand **Application Management**.
4. Select **Applications**.
5. In the list of applications, select the previously created application.
6. Right-click the application and click **Deploy**.

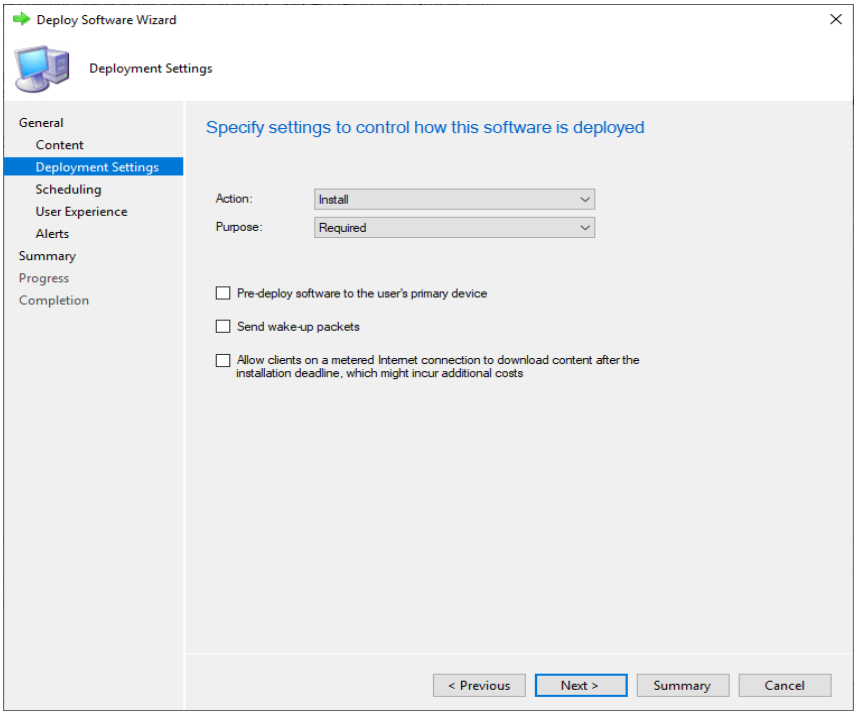
   A dialog box appears as in the figure below.



7. In the **Collection** field, click **Browse** and on the list select the required computer collection where you need to install the installation package and click **OK**.
8. Click **Next**.

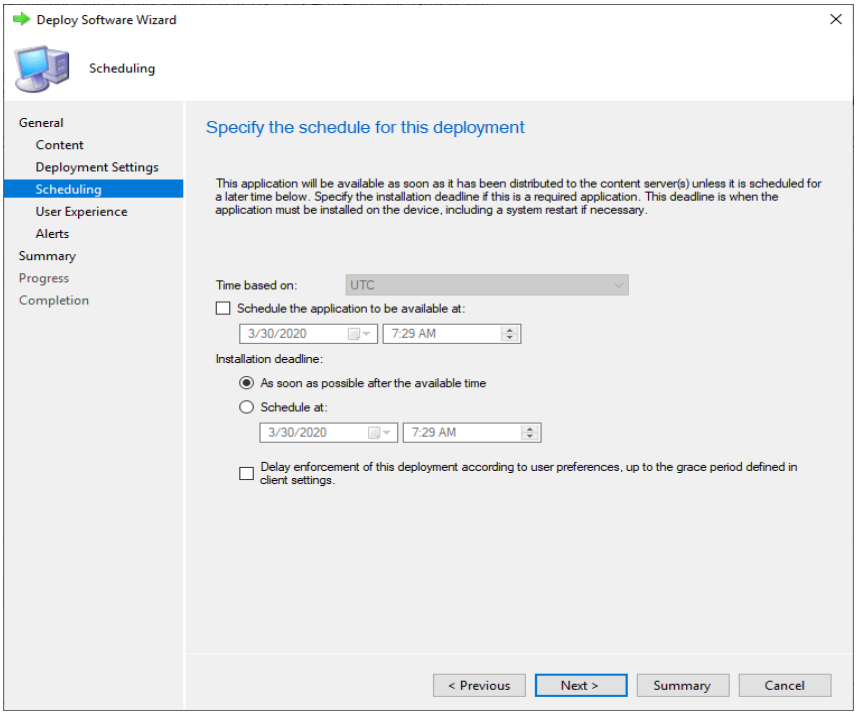
   A dialog box for configuring content distribution appears.
9. Click **Next**.

   A dialog box for configuring software deployment settings appears.



10. In the **Purpose** field, select **Required** and click **Next**.

    A dialog box for configuring deployment schedule appears.



Note. To perform uninstallation, in the **Action** field, select **Uninstall**. The **Purpose** field will be automatically set to **Required**.

11. Click **Next**.

A dialog box for configuring user experience during the installation appears.

12. Click **Next**.

A dialog box for configuring alert settings appears.

13. Click **Next**.

A dialog box for confirming deployment settings appears.

14. Check the correctness of the specified settings and click **Next**.

The wizard begins installing the application.

15. When the installation is finished, click **Close**.

Note. The application is not used for updating and repairing the Client.

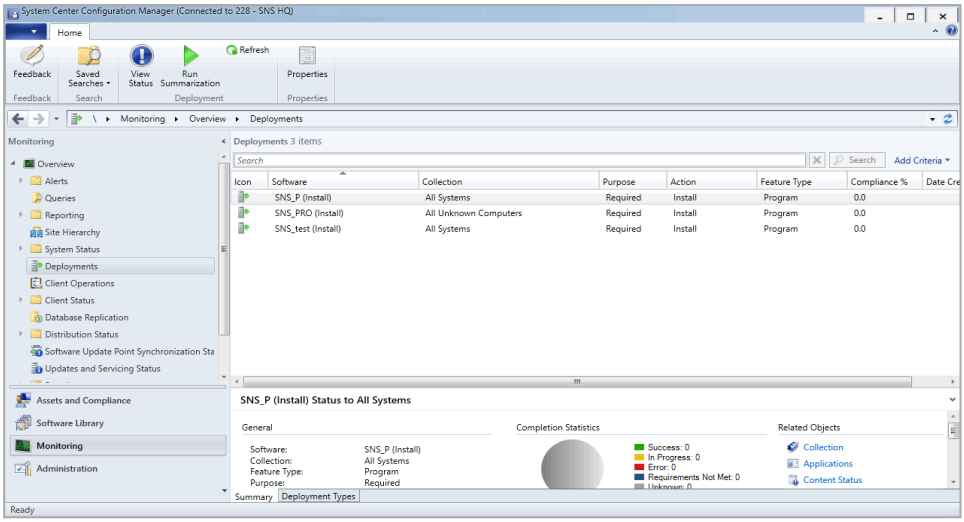
To monitor the application installation progress:

1. Run **System Center Configuration Manager**.

2. At the bottom of the navigation panel (on the left of the main window), select **Monitoring**.

3. At the top of the navigation panel (on the left of the main window), select **Deployments**.

A dialog box appears as in the figure below.



4. In the software list, select the required application and view its status.

Chapter 8
Updating and repairing 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. **87**). 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. **89**) on administrator computers.
4. Update the Client (see p. **89**) 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. 57).
5. Check and, if necessary, edit the operational management structure in the Control Center (see p. **127**).

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 cannot 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 healthy state;
- to update the Security Server in the domain forest for the 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. **42**) 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 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 successfully complete, a ready to update dialog box appears. You may additionally select to install the Synchronization service.

Note. The Synchronization service may be installed on a security server to act as a gateway and allow interaction between this Security Server and the parent Security Server. The Synchronization service is installed by a separate setup wizard that is automatically run after the Security Server is installed (see p. 51).

2. Click **Update** or select **Synchronization service** and click **Modify**.

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

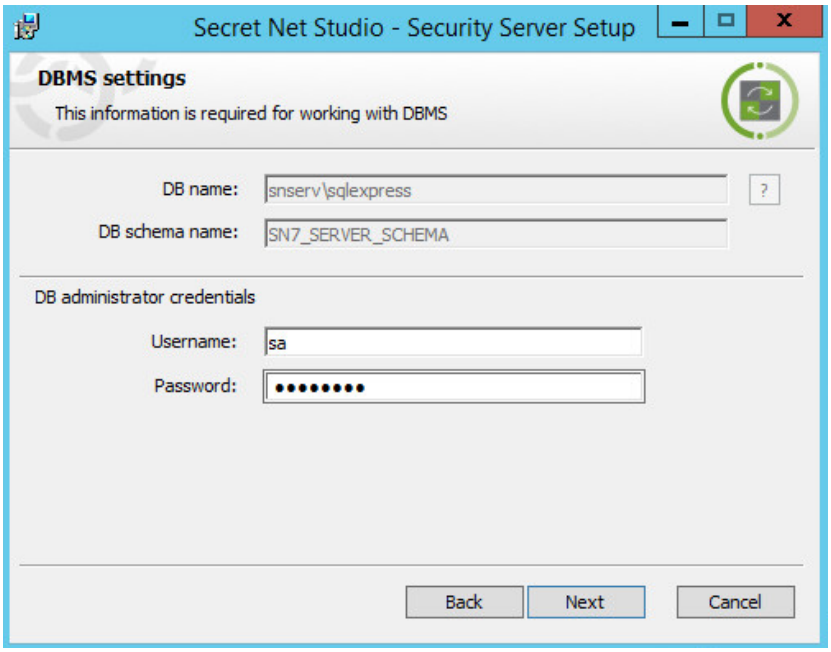
   Note. Before performing any further actions, close the AutoRun program by clicking **Exit**.

3. Click **Next**.

   The license agreement dialog box appears.

4. 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.



5. In the **DB administrator credentials** group of fields, enter the credentials of the database administrator and click **Next**.

   The **Preparation completed. Update can be started** dialog box appears.

6. Click **Update**.

   If you chose to install the Synchronization service in step **2**, its setup wizard welcome dialog box appears. Perform the installation according to steps on p. **51**.

   The update begins.

   Attention! If some software modules are in use at the moment, the dialog box prompting you to update files or services that can't be updated appears. To start the update, click **OK**.

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

7. Restart the computer.

Note. Information about the Security Server 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 information may appear a few minutes after updating the Security Server (this may take about 10-15 minutes).

Updating the Control Center

You must be included in the local Administrators group to update the Control Center. To perform the update, use the setup disk (see p. 52). 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. 42) and click **Security Components**.

   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, we recommend exiting the installer.To do so, click the **Close** button at the top right corner of the dialog box.

2. To view and select patches that will be applied during the software update, click **Patches**.

   Note. You may install patches separately from the Client update. To do that, on the installation disk, run the required patch file in folder Tools\SecurityCode\Patches\<patch_name>.

3. Click **Finish**.

   A dialog box asking you to restart your computer appears on the screen.

4. Click **Yes**.

   The security components update begins. When the update is complete, the computer is restarted. A message about successful update appears.

Repairing

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

You must be included in the local Administrators group to repair Secret Net Studio.

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

Repairing the Client

To repair the Client, follow the interactive Client installation procedure (see p. 53) or run the repair process of the Client 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 repair the Client:

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

   A dialog box asking you to restart your computer appears on the screen.

2. Click **Yes**.

   The repair process begins on the computer restart. When the repairs are complete, the computer is restarted. A message about successful repairing appears.

Repairing the Control Center

To repair the Control Center, follow the Client installation procedure (see p. 52). Wait for the welcome dialog box to appear and click the respective command.

To repair the Control Center:

1. In the dialog box, click **Repair**.

   A dialog box appears notifying you that the Setup Wizard is ready to repair the Control Center.

2. Click **Repair**.

   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 repair process.

   After the repair process is complete, the Installation Complete dialog box appears.

3. Click **Finish**, then click **Close** in the next dialog box.

Chapter 9
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 p. 57). To do this, create a software uninstallation tasks in the Control Center similar to deployment tasks.

The procedure for locally uninstalling 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. 53) or use the **Programs and Features** utility of Windows to uninstall 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 **Uninstall** and enter credentials of the security domain administrator.

   Comment. If current user has a permission to write to the centralized management object storage, proceed to the next step. Otherwise, select **use the following credentials** and enter credentials of a user that has the required permissions.
3. Click **Finish**.

   If **Administrative privilege control** is enabled, a dialog box appears requiring administrator PIN. To continue the uninstallation, enter the PIN and click **OK**.

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

   The uninstallation results dialog box prompting you to restart the computer appears.

   Tip. If necessary, use the links in the Information area to take the following actions:
   - to view trace log records, click the **installation report** link;
   - to collect all the files and data necessary Secret Net Studio for diagnostics if an error occurs during the installation, click the **diagnostics data** link.
5. Restart the computer.

Uninstalling the Control Center

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 the user performing 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 **Uninstall**.

   A confirmation dialog box appears.
2. Click **Yes**.

   The setup program checks the current state of the built-in 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.

Deleting gateway

If gateway software is installed on a Security Server, you may uninstall it separately from the Security Server. Before uninstalling gateway software, delete the gateway from the OM structure.

Attention! If you delete a configured and operating gateway, remember that the interaction between the parent security domain forest and the child security domain forest will be terminated. As a result, you will be unable to manage protected computers of the child forest via the Security Server on the parent forest.

We recommend performing this operation in the following order.

To delete gateway:

Step 1. Delete the gateway from the OM structure:

1. Run the **Control Center** and connect to the parent Security Server, where the gateway is registered.
2. At the bottom of the navigation panel, click the **Settings** button then select **Configuration**.

   A dialog box for selecting operation mode appears.
3. Select **Edit security forest hierarchy**.

A dialog box for editing the gateway list appears.

4. Select the required gateway then **Delete** and click **Yes**.

   The program begins deleting the gateway. The deletion takes some time. When the deletion is finished, a respective message will appear on **Events dialog box**. After the deletion is complete, the gateway is removed from the list. Additionally, the respective security forest will be deleted from the OM structure.

5. Click **Close**.

Step 2. Uninstall the gateway software:

1. On the computer with installed gateway software, run the Security Server setup wizard of the same version as the installed Security Server.

   The setup wizard checks UAC status. The following options are available:

   - if UAC is enabled, a dialog box appears asking you to temporarily disable UAC. Click **Yes**, then restart the computer and run the Security Server setup wizard again;
   - if UAC is disabled, the operation continues and the setup wizard dialog box appears containing the information about installed components.

2. Clear **Synchronization service** and click **Modify**.

   The wizard begins uninstalling the synchronization service. When the uninstallation is finished, a dialog box with a respective message appears.

3. Click **Close**.

Uninstalling 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:

- trusted environment;
- antivirus;
- software passport;
- network protection group and intrusion detection module;
- local disk protection and data encryption;
- print 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 Administrators group to uninstall subsystems.

To uninstall Client subsystems:

1. Run interactive client installation (see p. 53) 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 **Uninstall Components** and click **Next**.

   If **Administrative privilege control** is enabled, a dialog box appears requiring administrator PIN.

3. To continue the uninstallation, enter the PIN and click **OK**.

   A dialog box appears asking to select subsystems to uninstall.

4. Select the subsystems to uninstall and click **Finish**.

   The uninstallation process begins.

5. When the uninstallation is complete, click **Next**.

   The uninstallation results dialog box prompting you to restart the computer appears.

Tip. If necessary, use the links in the Information area to take the following actions:
- to view trace log records, click the **installation report** link;
- to collect all the files and data necessary Secret Net Studio for diagnostics if an error occurred during the installation, click the **diagnostics data** link.

6. Restart the computer.

Uninstalling patches

You can perform all patches uninstallation the same way you perform the interactive Client installation (see p. **53**) or via **Programs and Features** utility of Windows. The Setup wizard window appears.

To uninstall patches:

1. In the Setup wizard window select **Uninstall patches** and click **Next**.

   If **Administrative privilege control** is enabled, a dialog box appears requiring administrator PIN. To continue the uninstallation, enter the PIN and click **OK**.

   A dialog box prompting you to select patches to uninstall appears.
2. Select patches you want to uninstall. To select all patches, click **Select all**. Click **Finish**.

   The dialog box prompting you to restart the computer appears.
3. Click **Yes**.

   The computer restarts and the selected patches will be uninstalled. After a user has successfully logged on, the respective message will appear above the Secret Net Studio icon on the Windows taskbar.

Chapter 10
Update server deployment

The update server is designed to centrally update antivirus databases, decision rule bases and the dangerous website database of the intrusion detection tool. The following component databases can be updated:

- Antivirus;
- Antivirus (Kaspersky technology);
- Intrusion detection tool.

Attention! This version of the update server is only compatible with the Client versions 8.4 and later.

The update server architecture includes the following components:

- global update server — Security Code update server, located at https://updates.securitycode.ru, where you can download updates;
- local update server — update server installed in your company that downloads updates from the global update server;
- update server client — the component that downloads updates to a protected computer. The Update server client is included in the Client.

System requirements

The update server may be installed on computers with the following operating systems (32- and 64-bit systems with the following update packets or later):

- Windows 7 SP1;
- Windows 8.1 Rollup Update KB2919355;
- Windows 10;
- Windows Server 2008 R2 SP1;
- Windows Server 2012;
- Windows Server 2012 R2 Rollup Update KB2919355;
- Windows Server 2016;
- Windows Server 2019.

Attention!

- The update server can be installed on a computer only if your network contains 20 or less protected computers or for software learning process.
- The update server does not support Windows Server Core.

Additional software

The following software must be installed on the computers where you want to install the update server:

- Internet Information Services (IIS) 7.0 or higher;
- Microsoft Visual C++ Redistributable 2017;
- Microsoft .NET Framework 4.5.

If you start the update server installation using **SnAutoRun.exe** or **UpdateServer.exe**, these components will be installed automatically.

For correct operation, outgoing port 43444 must be available.

Deployment options

Depending on the size and configuration of your network, you can use different deployment options for the update server.

Protected network with five or less workstations

Update databases on protected computers directly from the Security Code server without using the update server. To do so, in the Control Center, configure the update parameters for each protected computer to update antivirus databases from the Security Code server.

Protected network with more than five workstations

Install the update server on a dedicated server in a protected network. The installed update server will download updates from the Security Code server and provide updates to the Clients in the network and other update servers used in cascading mode (without using any external traffic). In the Control Center, configure the update parameters to update antivirus databases from the local server.

Protected network without Internet connection

Install a separate server with Internet access. Install the update server on this server and on the server in the restricted access network.

The update server with Internet access will download the updates from the Security Code server and store them. Later, you will have to transfer the updates manually from that server to the server in the restricted access network.

In the Control Center, for each protected computer, configure the update settings to update antivirus databases from the local server and specify the address of the server in the restricted access network.

Server cascading

Create the following cascade of servers: one root server to download the updates from the Security Code server and several child servers to download updates from the root server and from other child servers.

Example 1

Install the primary update server that downloads updates from the Security Code website. Install an update server, configured to download updates from the primary server, in each subnet. Subnet workstations will download updates from these servers.

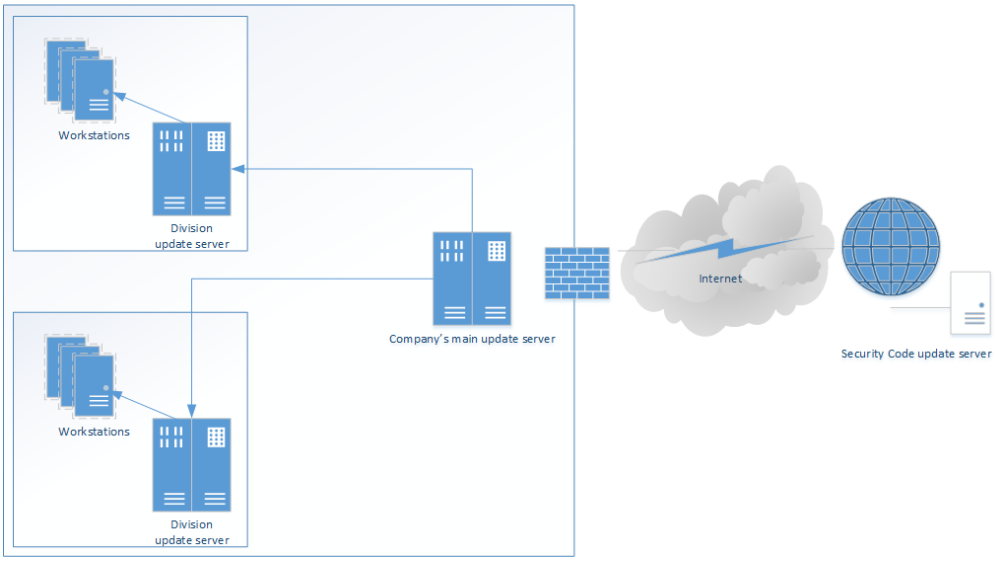


Fig.1 The company uses several subnets

Example 2

Install an update server in every sub-office. Each server will download available updates within the parent organization via the corporate network.

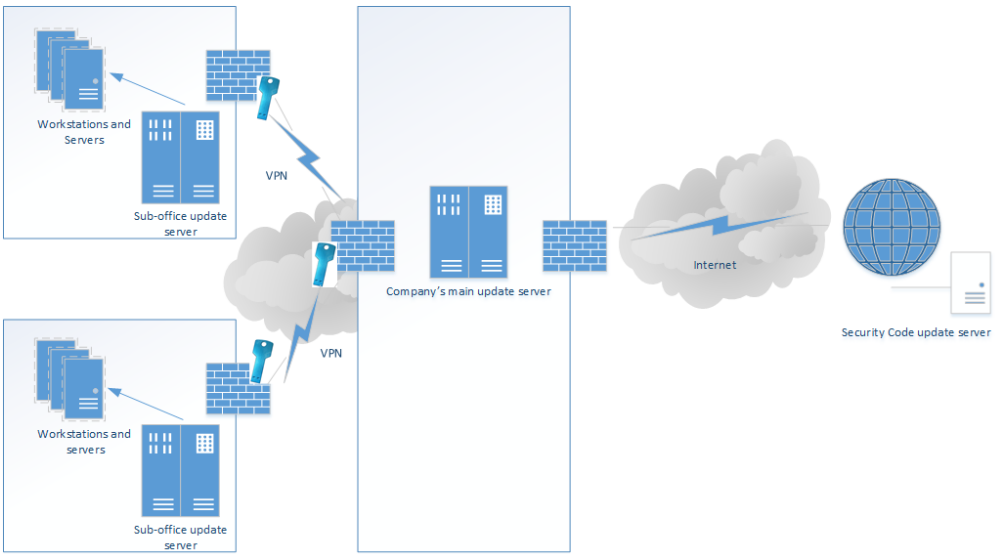


Fig.2 The company has several sub-offices

Installation, update and uninstallation

Install the update server

Before installing the update server, in the Windows Firewall, make the 43444 port available for the incoming connections.

To install the update server:

1. Insert the setup disk of Secret Net Studio and wait for the startup screen to appear.

   Note. If the startup screen does not appear, run **SnAutoRun.exe** that is located on the disk.
   To install the update server, you can also run **UpdateServer.exe** that is located either in \Tools\SecurityCode\Update Server\x64 or \Tools\SecurityCode\Update Server\Win32 (depending on the system) as administrator.

2. On the startup screen, activate the **Update server** link.

The Setup wizard begins preparations. Then the license agreement dialog box appears.

3. Read the license agreement, select **I accept the terms of the license agreement** and click **Install**.

   The system begins copying files to the hard drive and configuring installed components. This process is displayed on the progress bar on the Setup wizard dialog box.

   After installation and configuration have successfully finished, the respective dialog box appears.

4. Click **Close**.

Updating the management program

To update the management program:

1. On the computer with the installed update server, run the installation of a later version (see p. 97). The Setup wizard begins preparations. After all preparations are complete, the Setup wizard displays its welcome dialog box. Accept the terms of the license agreement. The Setup wizard updates the management program.
2. Update the databases of dangerous web-resources, antiviruses and decision rules on protected computers.

Uninstalling the update server

The Secret Net Studio Setup wizard helps to uninstall the update server from the computer.

Tip. You can also uninstall the update server via the Windows Control Panel.

Before starting the uninstallation, close the update server management program.

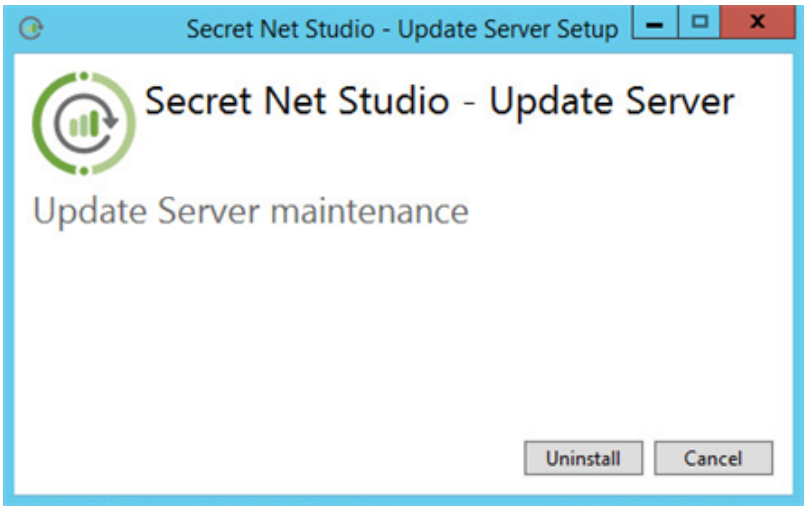
To uninstall the update server:

1. Insert the Secret Net Studio setup disk and wait until the startup screen appears.

   Note. If the autorun does not start, run **SnAutoRun.exe** that is located on the setup disk.

2. Activate the **Update Server** link.

   The Setup wizard begins preparations. After all preparations are complete, the Setup wizard displays its welcome dialog box.



3. Click **Uninstall**.

   The wizard begins uninstalling the update server components. After the uninstallation finishes, the information dialog box appears.

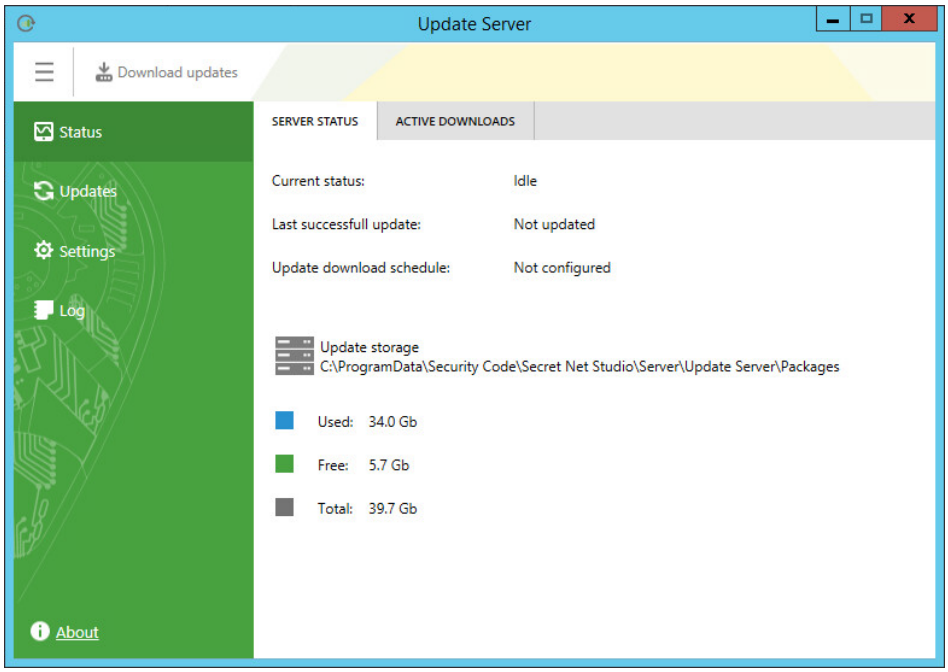
4. Click **Close**.

Update server management program

Installed update server is located in C:\Program Files\Secret Net Studio\Server\Update Server.

To run the update server management program, on the **Start** menu, click **Apps**, then click **Security Code** and click **Update server**.

The **Update Server** window opens.



Management program main menu contains the following control panels:

- **Status** (see p. **99**);
- **Updates** (see p. **100**);
- **Settings** (see p. **101**);
- **Log** (see p. **104**).

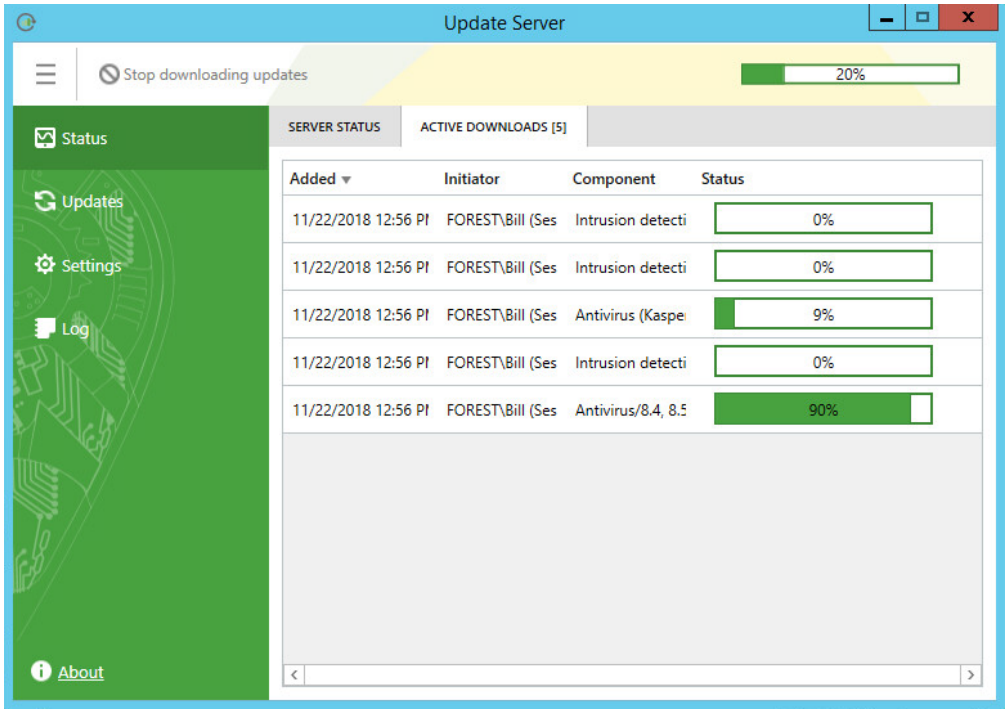
View server information

The **Server Status** tab on the **Status** panel contains information about current state of the update server and free capacity of the update packets repository folder.

The **Server Status** tab displays the following information:

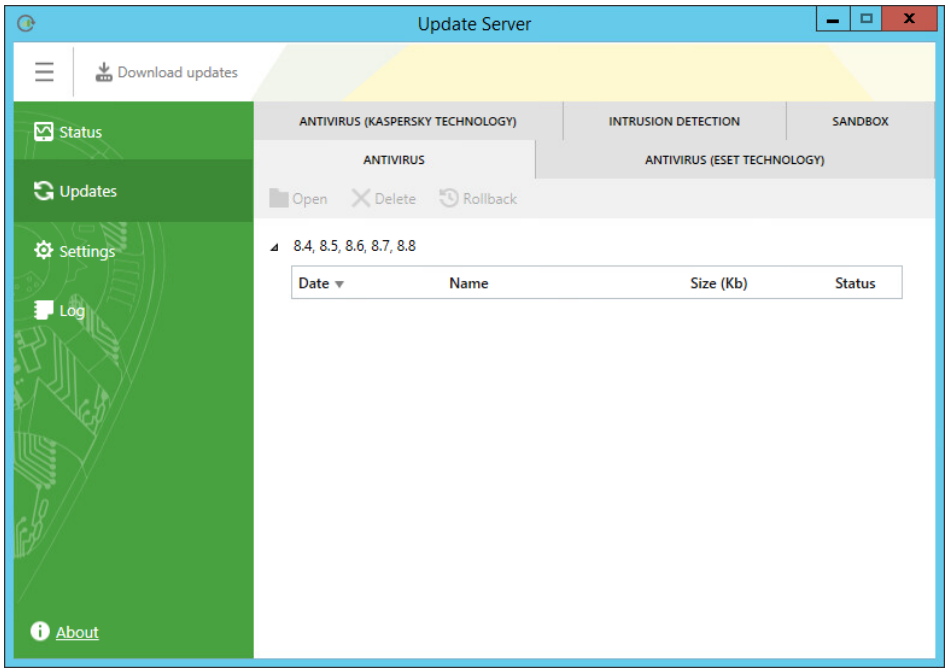
- current update download status;
- date and time of the last update;
- date and time of the scheduled update;
- path to update storage;
- amount of used disk space;
- amount of free disk space available for update storage;
- total storage size.

To view progress of the updates downloading, select the **Active downloads** tab.



View update information

Tabs **Antivirus (ESET technology)**, **Antivirus (Kaspersky technology)**, **Antivirus** and **Intrusion detection** on the **Updates** panel contain the lists of all the update packages for antivirus databases, databases of decision rules and databases of dangerous web-resources stored on the server.



For each update package the management program displays the information about its release date, name, size, Secret Net Studio version and current status. The **Status** field can display the following values:

- current version;
- backup version (a saved update file that can be disseminated);
- unavailable (for example, if the update file was deleted by means other than the update server management program).

You can perform the following actions with update packages.

Command	Action
Open	Select an update package and click **Open**, to open the folder with that update package
Delete	Select an update package and click **Delete** then confirm the deletion in the pop-up dialog box. This will delete all the files associated with that update package. Only backup and unavailable packages can be deleted
Rollback	Select an update package and click **Roll back** to restore the database to the selected version. You can roll back only to backup versions

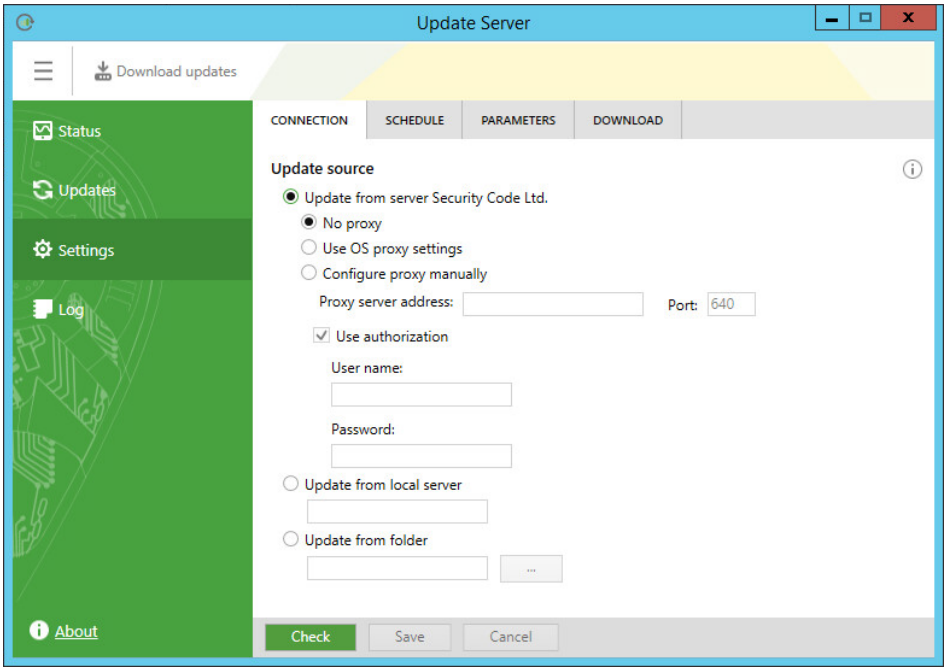
Configure the update server

Connect to an update source

For correct operation, the update server must be configured to connect to an update source.

To configure an update source:

1. On the **Settings** panel, select the **Connection** tab.



2. Select an update source.
   - **Update from Security Code Ltd. server** — select this option to download updates directly from the global server. Configure proxy settings if needed.

Option	Description
No proxy	Select this option to connect to the global server directly (without using a proxy server)
Use OS proxy settings	Proxy server settings will be configured automatically
Configure proxy manually	Select this option to manually configure proxy server settings. Type the proxy server address and port. If the proxy server requires authorization, type the user name and password

Note.
- The proxy server supports only NTLM authorization.
- We recommend allowing anonymous access to proxy servers for computers with installed update servers using MAC address verification.

- **Update from local server** — select this option, if you have a Secret Net Studio update server installed in your local network, and type the server address;
- **Update from folder** — select this option, if you store updates in a local or network folder. Click ... and select the folder or type its path.

Note. Make sure that the selected user account has access to the contents of the selected folder.

Note. The network folder must be inside the domain. For correct operation, all authorized users and accounts of computers that require updating must have the permission to read the network folder.

3. To check the connection with the source, click **Check**.

   The **Connection check** window appears.
4. Click **Save**, to save the update server configuration.

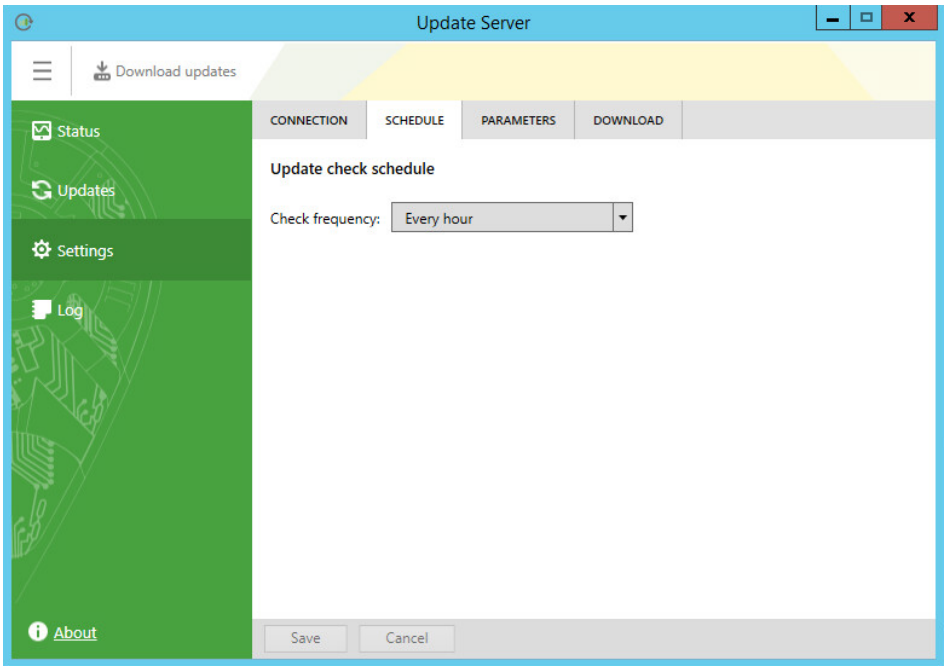
Note. To discard configuration changes, click **Cancel**.

Configure the update schedule

You can configure update check and download frequency via the management program.

To configure the update schedule:

1. On the **Settings** panel, select the **Schedule** tab.



2. Select the update check frequency from the drop-down list and configure the parameters of date and time.

Note. We recommend checking for database updates every hour.

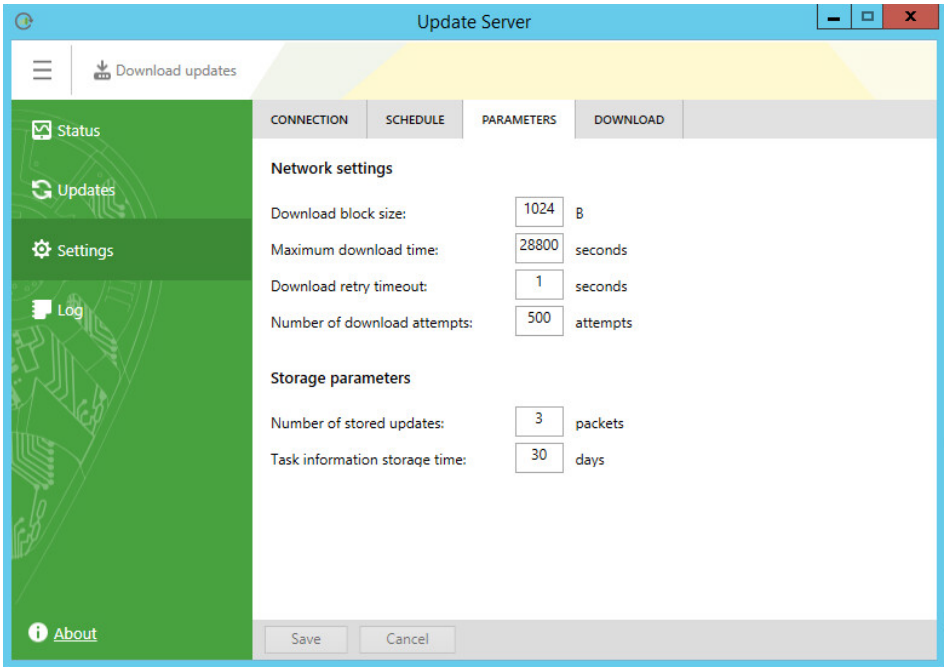
3. Click **Save** to apply changes.

Tip. To discard configuration changes, click **Cancel**.

Configure update download parameters

To configure download parameters:

1. On the **Settings** panel, select the **Parameters** tab.



2. Configure network parameters.

Parameter	Description
Download block size	Data block size when downloading via HTTPS (in bytes). Type a value between 1024 and 10485760
Maximum download time	Waiting time for an update to download (in seconds). Type a value between 100 and 36000
Download retry timeout	Waiting time between update download attempts (in seconds). Type a value between 1 and 100
Number of download attempts	Number of attempts to download an update. Type a value between 1 and 500

3. Configure update storage parameters.

Parameter	Description
Number of stored updates	Number of stored (backup) update packages. Type a value between 1 and 100
Task information storage time	Time period, during which information about finished update tasks is stored (in days). Type a value between 1 and 365

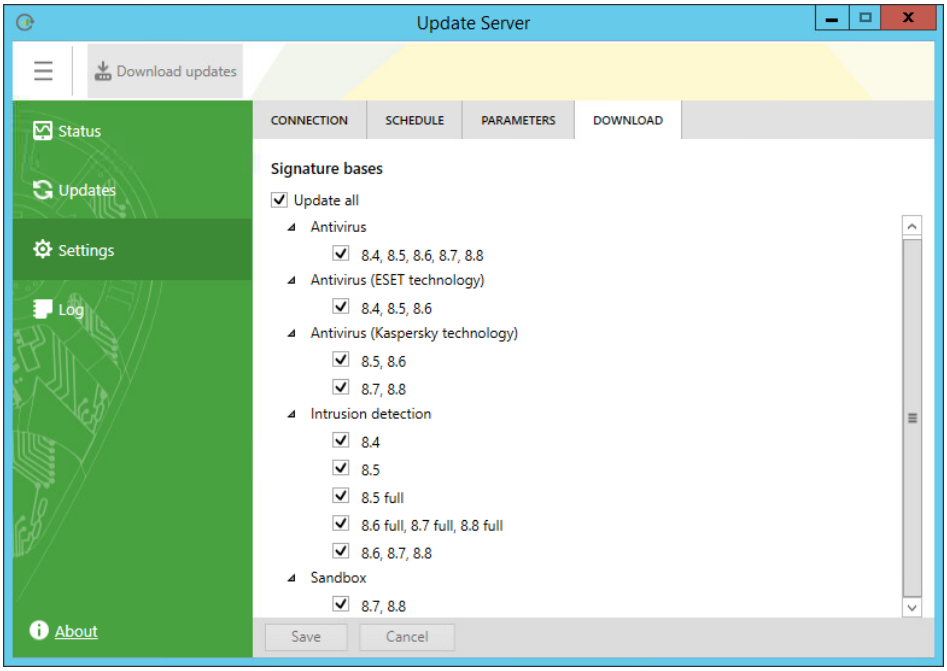
4. Click **Save**, to apply changes.

Note. To discard configuration changes, click **Cancel**.

Select components to update

To select components:

1. On the **Settings** panel, select the **Download** tab.



2. Select Secret Net Studio components that require their databases to be updated and click **Save**, to apply changes.

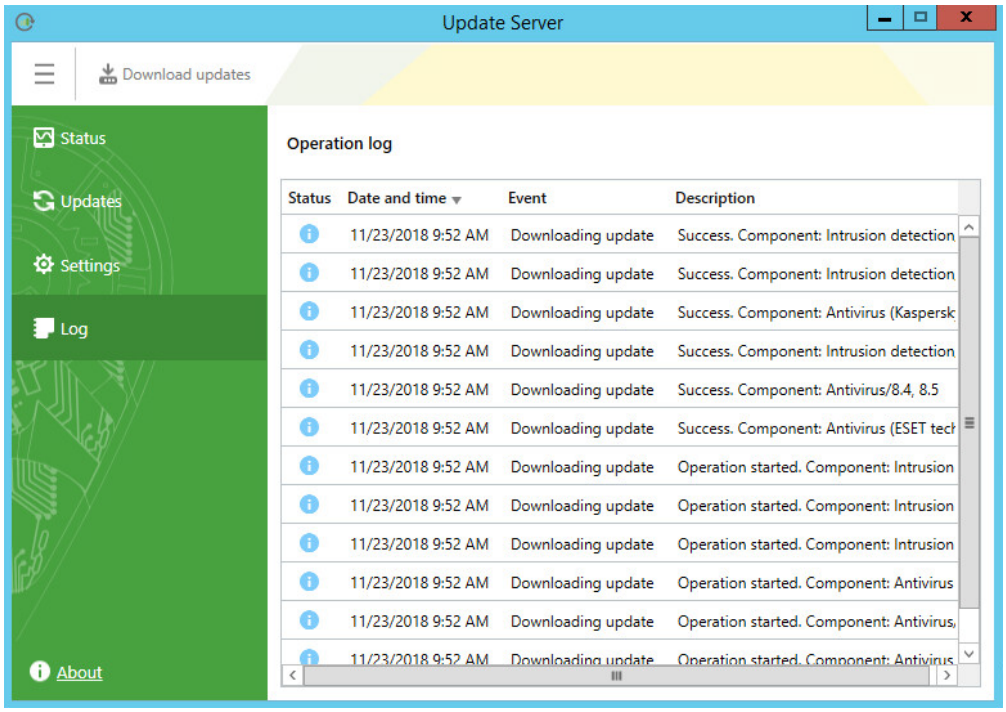
   Note. The **8.5 full** version for the **Intrusion detection** tool includes data update provided by Kaspersky.

3. A window appears, asking to download updates for selected components or to delete updates for those that are not selected. Click **Download** or **Delete** to do that.

   Note. To discard configuration changes, click **Cancel**.

View the operation log

The log contains information about operations, performed on the update server during the current session. To open the log, select the **Log** panel.



The log is automatically cleared every time you close the management program.

Chapter 11
Secret Net Studio management

Organizing security system management

Central and local management

Local management is the management of the security mechanisms of an individual computer, performed by the security administrator directly on the computer. Local management is used when central management for an individual computer is either unavailable or inappropriate. Software tools for local management are installed by default and can be used by users who are members of the local group of computer administrators.

Centralized control of Secret Net Studio parameters is carried out by the security administrator from a computer. For this purpose, any computer of the network with installed central management tools can be used.

Only local management capabilities are available for the Client in the standalone mode. In the network operation mode, management can be either central or local.

Attention! We recommend you to centrally manage computers with the Client in the network operation mode. Central management has priority over local management. For example, if certain parameters are set centrally in the group policy, they cannot be changed locally on the computer. Also, in case of disabling security subsystems by the local administrator in the local Control Center, an alert event is registered in the Secret Net Studio log.

Using group policies

Group policies are used to perform centralized configuration and apply security parameters on computers with the Client in the network operation mode. By default, the parameters are only set for the local policy which has lower priority.

In addition to local policy parameters, there are parameters that can be configured for domain policies, company units and the Security Servers. These parameters are applied on computers associated with respective domains, company units or the Security Servers regardless of the local policy values set for the computer.

The group policy parameters are applied in the following sequence:

- local policy;
- domain policy;
- company unit policy: applied on all computers associated with that unit;
- Security Server policy: applied on all computers linked to this Security Server.

If there is the Security Server hierarchy, the policy parameters are applied starting from the server governing computers directly, down to the root server of the hierarchy. Therefore, the root Security Server policy parameters have the highest priority rating.

Group policy parameters are configured using the Control Center.

Centralized parameter management is implemented using different group policies, taking into account various peculiarities. For example, you can configure general parameters for all computers within a domain policy range and, additionally, enter values for certain parameters for company unit policies. This will allow general parameters to be applied on computers of different company units and set specific values for computers of particular units.

Updating group policies

Group policy parameters on protected computers are automatically updated in accordance with the Windows OS policy application mechanism. The administrator can use special tools to force update policies in order to speed up the application

process for parameters configured on computers in the centralized mode.

Group policy force update can be executed using the following tools:

- the Control Center option to apply group policies;
- command prompt standard tools: gpupdate and secedit.

Once the policy update is complete, you need to restart the computer or end the current user session in order to apply parameter changes that are only valid upon OS startup or user login. There are special features available in both the Control Center (computer restart and shutdown options) and specified command prompt tools.

Delegating of administrative privileges

Delegation provides entrusting certain setup and control functions to users who are not members of the domain's administrator group.

By default, the security administrators have all required privileges to set the parameters for Secret Net Studio protection mechanisms. However, some object control features available to domain administrators may be also needed by security administrators to perform their duties. In particular, this may include the administrative change of user passwords, the creation or deletion of users and user groups, and configuration of the basic parameters for accounts. To provide security administrators with these capabilities, the domain administrator can delegate the respective tasks by using standard Windows tools.

The delegation procedure is carried out in **Active Directory** – **Users and Computers** tool set using a delegation control wizard. The wizard can be started for the respective AD container – the entire domain or a separate organizational unit (depending on what objects the security administrator is allowed to manage). In the delegation wizard, specify the account of the security administrator or group and then select the following items in the task list:

- Create, delete and manage user accounts;
- Reset user passwords and force password change at next logon;
- Create, delete and manage groups — this task is delegated for organizational units;
- Modify the membership of a group.

Management tools overview

You can manage Secret Net Studio using special tools installed when the security system is deployed. Management tools always provide the option for adjusting system parameters and for changing the state of objects, as well as for controlling the operation of protected computers. Management tools can contain individual programs or program elements embedded into other tools as additional solutions.

Tools only for local management

Local management tools are used when users and administrators are working on a protected computer. These tools make it possible to perform actions that are only available during local management (for example, setting the local resource access parameters), to view centrally parameters and to set the parameters that were not set centrally.

The following software tools are used only for local management:

- Secret Net Studio icon on the Windows taskbar;
- Secret Net Studio tab in the resource properties dialog box;
- Mandatory access control configuration program;
- Secret Net Studio management in the Windows **Control Panel**.

In addition, the following tools for central and local management can be used:

- Local Control Center (installed as a part of the Client);
- User management program (to set parameters for local users);

- Application and data control program.

Note. This section lists the commonly used control tools. To perform specific tasks additional software tools may be used. For information about how to use them, see the respective documents.

Secret Net Studio icon

After installing the Client, Secret Net Studio icon appears in the notification area of the taskbar. The icon is designed to notify the user about the availability of active security, to launch main user control commands and to receive data.

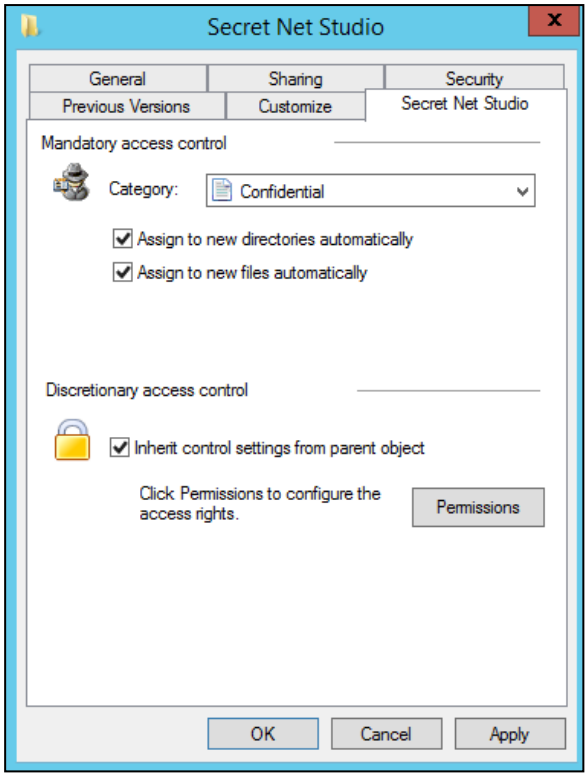
The commands are run from the shortcut menu of the icon. The available commands are shown in the following table.

Command	Description
About	General information about Secret Net Studio
Management (user mode)	Open the Local Control Center with the current user account permissions. If UAC is disabled, this command will not be available to the administrator
Management (administrator mode)	Open the Local Control Center with the built-in administrator account permissions. If UAC is disabled, this command will not be available to the user unless they are the administrator
Encryption	Open the **Full Disk Encryption** dialog box
Antivirus	Contains the command to show malware scan results, obtained by running the manual scan command in Explorer during the current session (see document [**2**])
Deleting data	Contains the command to permanently wipe all data from drives (see document [**2**])
User keys	Contains the commands to manage user key information located on key carriers (see document [**2**])
Reset alert state	Reset alert counts
Alert notifications	Enable/disable alert notifications

Secret Net Studio tab

The standard dialog box for setting the properties of a Windows OS resource (folder or file) contains the Secret Net Studio tab. The tab makes it possible to perform actions for changing the confidentiality category of resources for the mandatory access control mechanism or rights to access resources for the discretionary access control mechanism. Configuration can be performed by the security administrator or users who act as administrators of the selected resource.

The dialog box for setting the properties of the folder or file is called up using the Explorer. The Secret Net Studio tab is shown in the figure below.



Mandatory access control configuration program

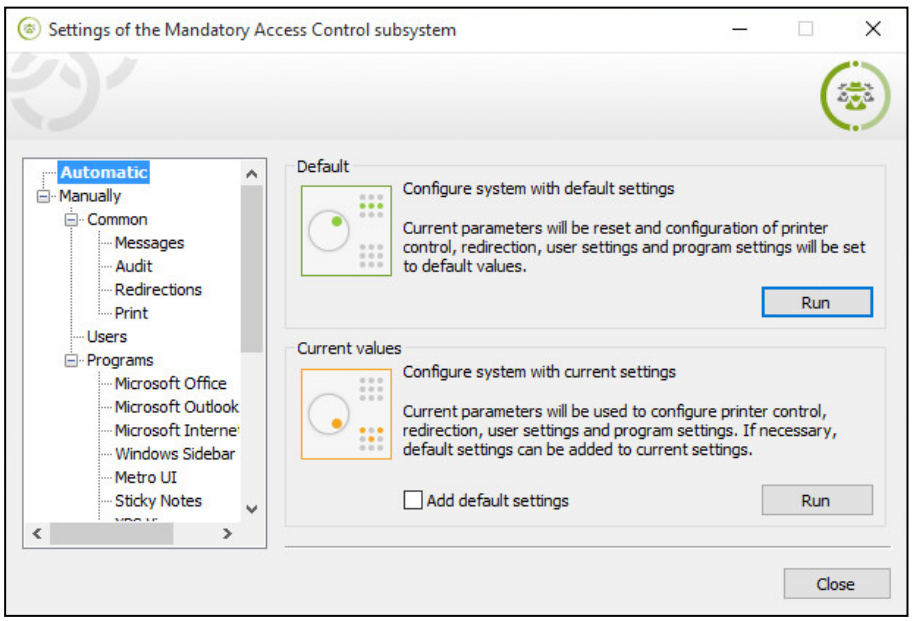
Mandatory access control configuration program is used for configuring additional system settings if the flow control mode is used. In addition, the program can be used to disable the output of warning messages and event registration when such notifications are not required.

To start the program, perform the following:

- on the **Start** menu, go to the **Security Code** submenu and click **Mandatory access control configuration**.

> **Attention!** If the administrative privilege control is enabled), a dialog box prompting you to enter an administrator PIN appears.
> - To start the program in administrator mode, type the security administrator PIN and click **OK**.
> - To start the program in limited functionality mode, click **Cancel** and close the dialog.

The program window is shown in the figure below.



The configuration of the mandatory access control is performed by the administrator.

Secret Net Studio management in the Windows Control Panel

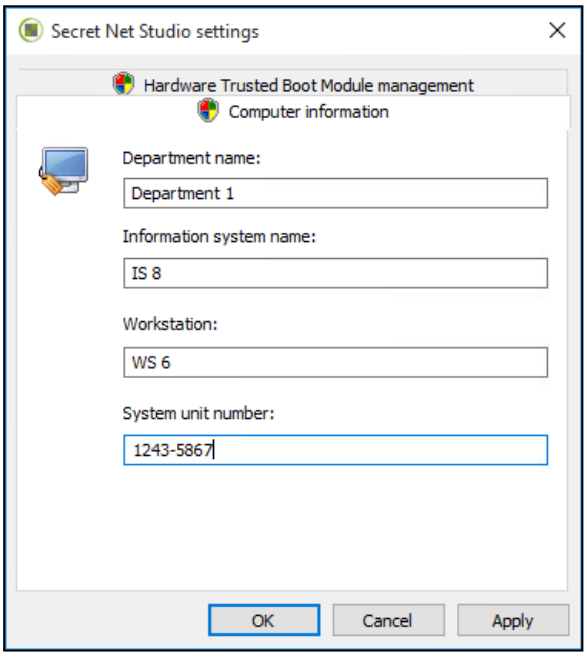
The Secret Net Studio settings dialog box allows you to view and edit general system data and manage local security mechanisms and hardware security tools.

To open the Secret Net Studio settings dialog box:

- On the **Control Panel**, go to **System and Security** and click **Secret Net Studio management**.

  Attention! If the administrative privilege control is enabled, a dialog box prompting you to enter an administrator PIN appears.
  - To start the program in administrator mode, type the security administrator PIN and click **OK**.
  - To start the program in limited functionality mode, click **Cancel** and close the dialog.

  The dialog box appears as in the figure below.



Centralized and local management tools

Centralized management tools are used on administrator computers for centralized configuration and control of protected computers. These tools can also be used for local management directly on the protected computers. For example, to manage a computer with the Client in the standalone mode.

Secret Net Studio contains the following centralized management tools:

- Control Center;
- User management program;
- Application and data control program.

Note. This section lists the commonly used management tools. To perform specific tasks, additional software tools may be used. For information on how to use them, see the respective documents.

Control Center

The Control Center is installed as a component of Secret Net Studio to work centrally. To work locally, use the Local Control Center which is installed as a part of the Client.

The Control Center makes it possible to manage computers from the security administrator workstation, monitor and view logs saved in the Security Server database. To work with the program, you need to establish a connection with the

Security Server. To work with logs that are saved as files, the connection is not required.

The Local Control Center allows you to manage a computer locally, view local logs and logs that are saved as files.

To start the Control Center:

- In the **Start** menu, go to **Security Code** and click **Control Center**.

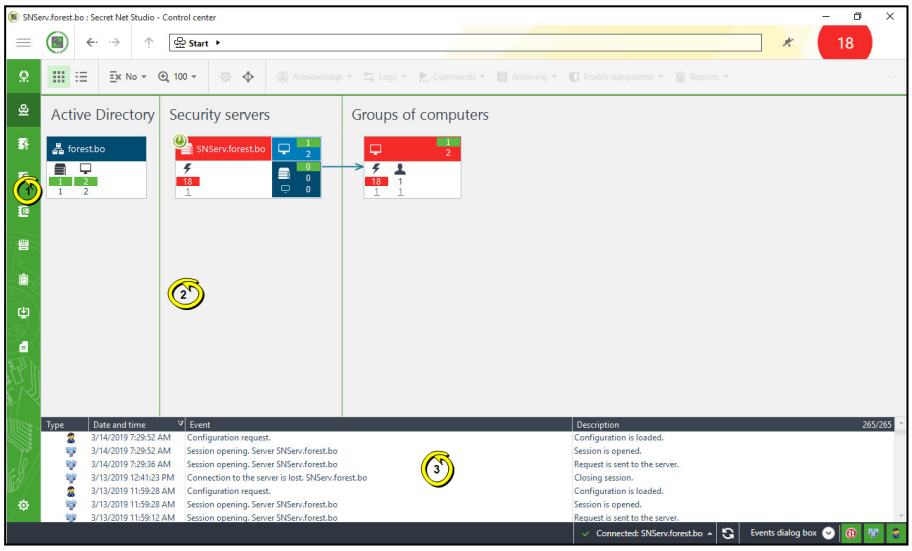
  Before you get started, a dialog box appears asking you to select the Security Server to which a connection will be established.

To start the Local Control Center:

- In the **Start menu**, go to **Security Code** and click **Local Control Center**.

> **Attention!** If the administrative privilege control is enabled, a dialog box prompting you to enter an administrator PIN appears.
> - To start the program in administrator mode, type the security administrator PIN and click **OK**.
> - To start the program in limited functionality mode, click **Cancel** and close the dialog box.

The Control Center main window is shown in the figure below.



User management program

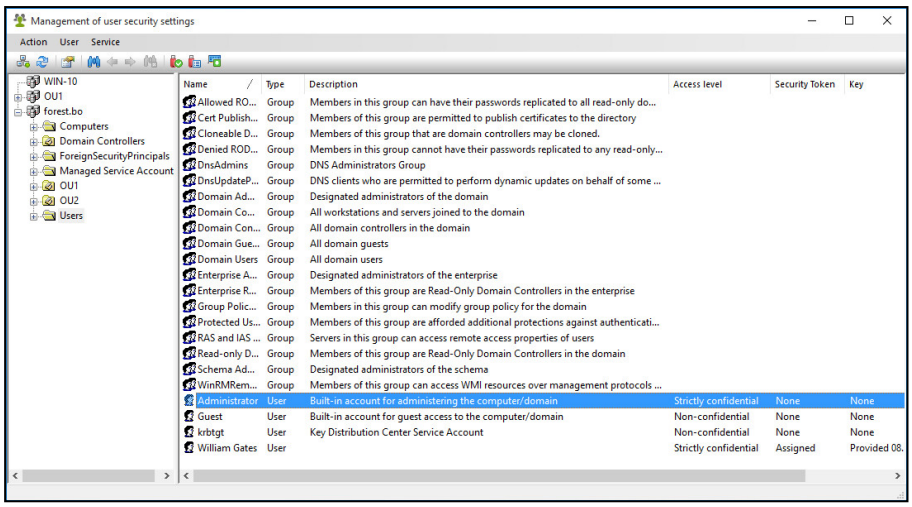
The user management program makes it possible to configure user operation parameters within the security system. Actions with both domain and local users can be performed using this program.

To run the program:

- On the **Start** menu, go to **Security Code** and click **User management**.

> **Attention!** If the administrative privilege control is enabled, a dialog box prompting you to enter an administrator PIN appears.
> - To start the program in administrator mode, type the security administrator PIN and click **OK**.
> - To start the program in limited functionality mode, click **Cancel** and close the dialog.

The user management program interface is shown in the figure below.



The program interface is similar to the standard interface of Active Directory – Users and Computers. The left part of the window displays a list of containers (the current computer and the structure of sections and organizational subdivisions of the domain), the right side displays the list of users in the selected container. The list of users is displayed as a table with data on user access levels, security tokens and cryptographic keys.

If the parameter **Enhanced authentication by password** is selected, in order to perform operations with users, select **Synchronize user data on the authentication server** at each operation or select **Trust Windows authentication** in the Control Center.

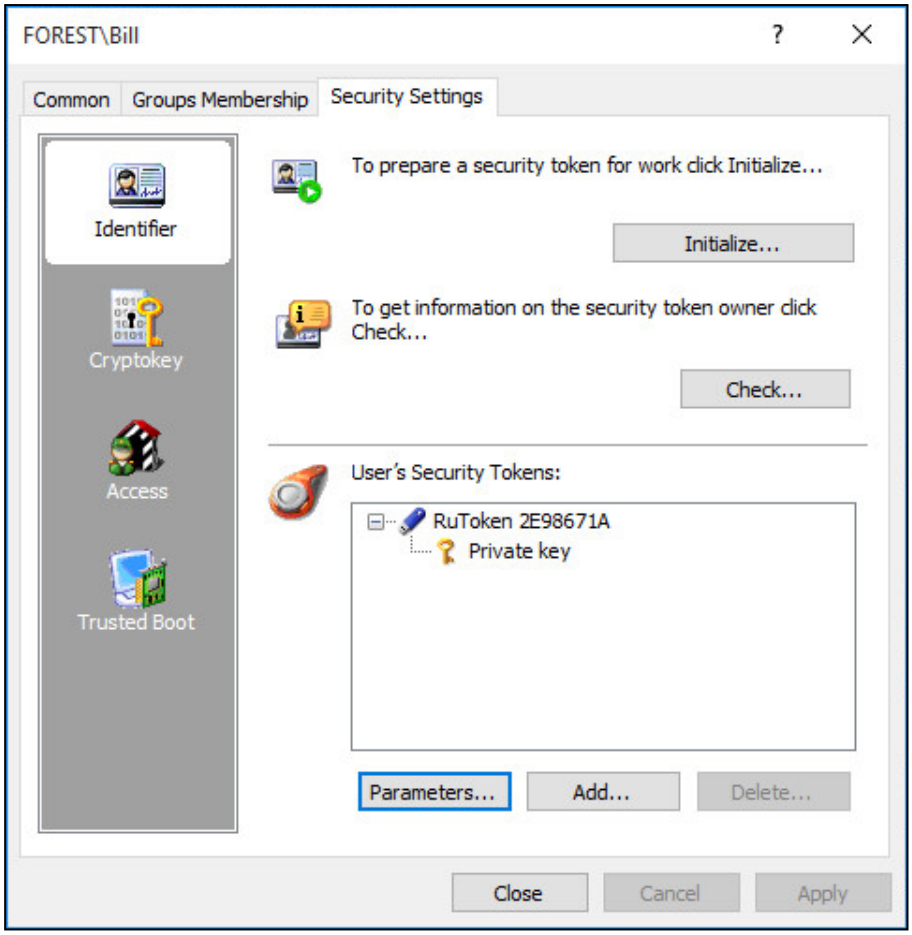
For the centralized management, the structure of the current domain is downloaded to the program by default. If necessary, the structures of other Active Directory domains can also be downloaded if it is possible to connect to these domains. To do so, in the **Action** menu, click **Connect to Active Directory Domain**.

Tip. Working with a large number of objects, use the sort and search functions. The sorting is performed using standard methods — by the contents of the table columns in the user list. The search can be performed based on various criteria. To configure the search parameters, select the Search command in the User menu and set the required criteria in the settings dialog box. The search results are displayed in the settings dialog box and also highlighted in the user lists after the dialog box is closed. To switch between the found objects, use the **Next** and **Previous** commands in the **User** menu.

You can delete from the authentication server databases user accounts deleted from AD but left in Secret Net Studio databases. To do so, in **Service**, select **Delete lost users**.

Tip. We do not recommend deleting lost users unless absolutely necessary, especially when it comes to a structure with several AD domains (to avoid deleting users from other domains).

User parameter management in Secret Net Studio is performed on the **Security Settings** tab as in the figure below.



Application and data control program

Application and data control program makes it possible to configure settings of IC and AEC mechanisms. During configuration, lists of controlled objects, control methods and schedules, and system reaction to the control results are determined for the integrity control mechanism. For the application execution control, lists of programs that the user permits to start, are determined. A data model containing a hierarchy of objects and description of connections between them is formed from this data.

You can work with the program in one of the following modes:

- local mode — for editing the local data model on the computer;
- centralized mode — for editing the centralized data model with descriptions of objects controlled on protected computers. The centralized data model is used on the Clients in the network operation mode along with local models, if they are set. Moreover, parameters of the centralized model have priority over parameters of the local model.

For centralized management, if computers with OS versions with different bit depth values are included in the system, two data models are generated — for computers with 32-bit versions and for computers with 64-bit operating system versions. Using the program, the administrator can only edit one centralized data model which bit depth value matches the OS bit depth on the administrator's computer. Therefore, when a centralized model of another bit depth value needs editing, the administrator needs to use a computer with an OS version of the same bit depth value.

To start the program in the centralized mode:

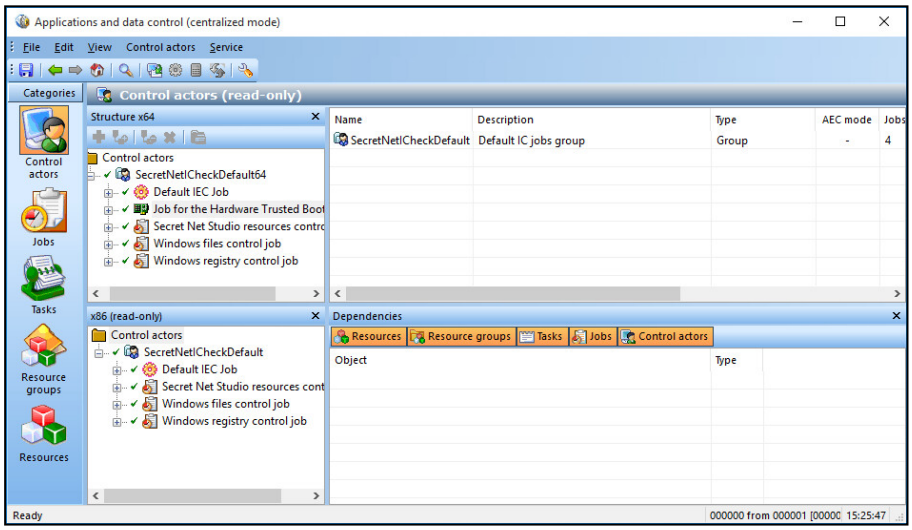
1. On the **Start** menu, go to **Security Code** and click **Application and data control (centralized mode)**.

During start, the program checks if full access is possible to the data model of corresponding bit depth value in the CDB of the IC-AEC. Full access is only available from one computer of the system.

2. If full access to the CDB is not possible (the management program of the IC-AEC is already working in the centralized mode on another computer with an OS of the same architecture), a message appears with a request to perform further actions. The following options are available:
   - cancel the program start (recommended) — click **Cancel**;
   - start the program in read-only mode — click **No**. In this case, the latest data model saved in the CDB will be uploaded to the program. The model cannot be edited;
   - start the program and receive full access to the CDB — click **Yes**. Any other user currently working with the IC-AEC on another computer will not be able to edit the CDB and save changes.

Attention! If the administrative privilege control is enabled, a dialog box prompting you to enter an administrator PIN appears.
- To start the program in administrator mode, type a security administrator PIN and click **OK**.
- To start the program in limited functionality mode, click **Cancel** and close the dialog box.

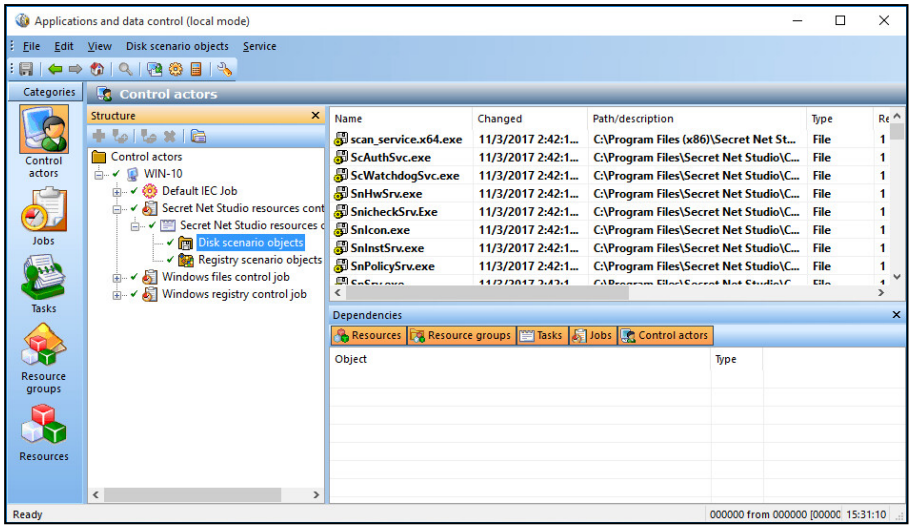
The program in the centralized mode is shown in the figure below.



To start the program in local mode:

- On the **Start** menu, go to **Security Code** and click **Application and data control (local mode)**.

  Attention! If the administrative privilege control is enabled, a dialog box prompting you to enter an administrator PIN appears.
  - To start the program in administrator mode, type a security administrator PIN and click **OK**.
  - To start the program in limited functionality mode, click **Cancel** and close the dialog box.


Applications and data control (local mode)
File
Edit
View
Disk scenario objects
Service
Categories
Control actors
Jobs
Tasks
Resource groups
Resources
Control actors
Structure
Control actors
WIN-10
Default IEC Job
Secret Net Studio resources cont
Secret Net Studio resources c
Disk scenario objects
Registry scenario objects
Windows files control job
Windows registry control job
Name
Changed
Path/description
Type
scan_service.x64.exe
ScAuthSvc.exe
ScWatchdogSvc.exe
SnHwSrv.exe
SnicheckSrv.Exe
SnIcon.exe
SnInstSrv.exe
SnPolicySrv.exe
11/3/2017 2:42:1...
C:\Program Files (x86)\Secret Net St...
C:\Program Files\Secret Net Studio\C...
File
Dependencies
Resources
Resource groups
Tasks
Jobs
Control actors
Object
Type
Ready
000000 from 000000 [00000 15:31:10

Chapter 12
About the Control Center

The Control Center is a component that is used for centralized control of computers. Using the Control Center you can:

- configure the security system;
- monitoring security system status;
- configure the network structure of the security system;
- manage centralized logs.

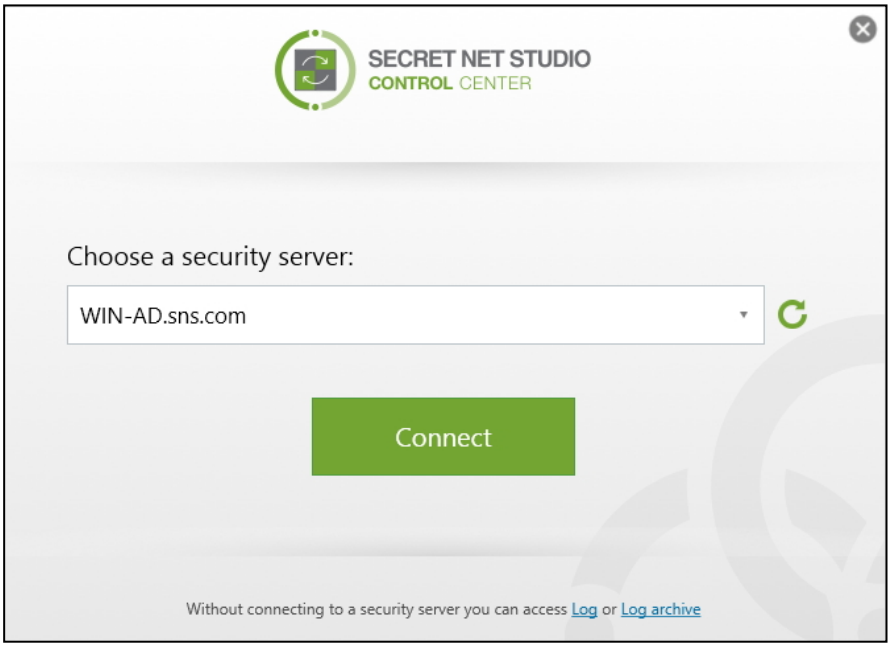
Note. The local version of the Control Center is installed on a computer as part of the Client. This version makes it possible to set up security settings, to control the Client subsystems, to view local logs of the computer, whereas centralized control features are not available.
This chapter describes how to use the Control Center for centralized control. You can perform same functions with the on-premises version similarly.

Starting the Control Center

To start the Control Center:

1. Click the **Start** button and click **Control Center** in the **Security Code** group of the program menu.

   The dialog box appears as in the figure below.



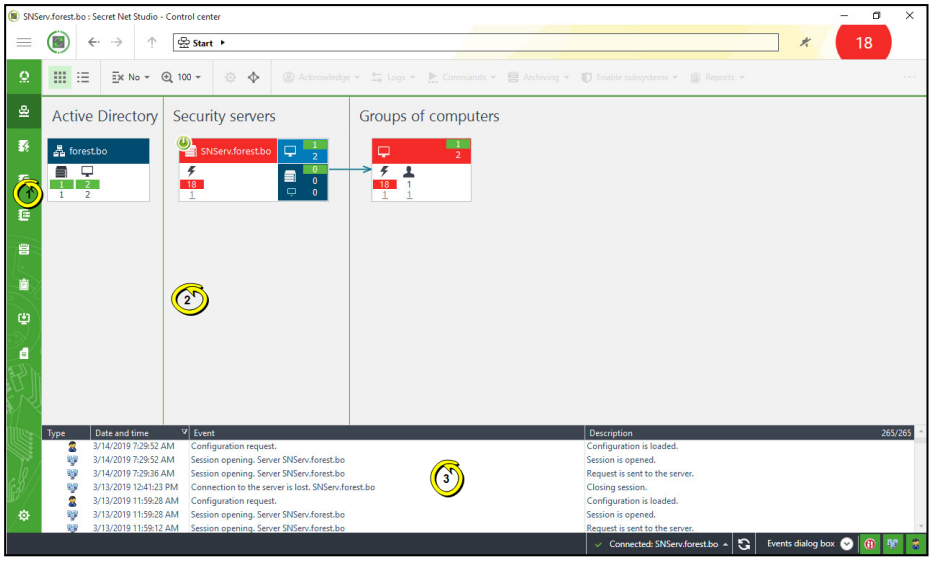
2. In the **Choose a security server** field, type or select the name of the Security Server for further connection. To get a list of all registered Security Servers, click the button to the right of the field (this operation may take a long time).
3. Click **Connect**.

Note. The Control Center supports starting without a connection to the Security Server to view the logs saved to files. To open the files, run the following commands at the bottom of the start dialog box:

- **Log** to load a log from a file;
- **Log archive** to load a log archive from a file.

The Control Center interface

The Control Center interface is shown in the figure below.



Note. The figure shows: 1 — the navigation panel; 2 — the Computers panel in Diagram mode; 3 — the Events dialog box; 4 — the OM navigation tools.

Interface elements

The Control Center interface consists of the following parts:

- the navigation panel is located on the left side of the Control Center window and contains shortcuts to control panels and the Control Center configuration tools;
- the control panels contain tools for viewing and configuring the software settings

The Control Center contains the following Control Panels:

Statistics
Contains information about the general system security status
Computers
Contains tools for administration and computer management
Alert logs
Contains tools for viewing alert log events
Station logs
Contains tools for viewing workstation log events
Server logs
Contains tools for viewing Security Server log events
Archives
Contains tools for viewing log archives
Reports
Contains tools for working with reports
Deployment
Contains tools for configuring automatic software installation and updating
Software passport
Contains tools for controlling content and integrity of the computer software

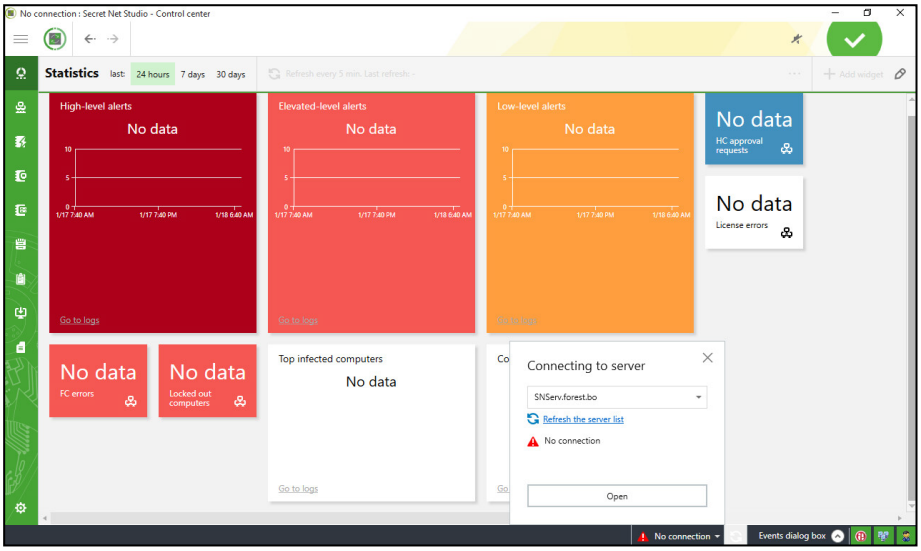
Connection to the Security Server

The Security Server connection starts when the session is open. If the session with the Security Server was not open at program launch or the Security Server connection was lost, connection to this Security Server can be established without restarting. If the connection to another Security Server is required, the existing session is closed and then a new session with the Security Server can be opened.

To open a session:

1. Click the button next to **No connection** at the bottom of the navigation panel.

   A panel with settings appears as in the figure below.



2. In the **Connecting to server** section, type or select the name of the Security Server to which a connection will be established. To view the list of all registered Security Servers, click the **Refresh the server list** button on the right.
3. Click **Open**.

   When a connection is established, configuration from the selected Security Server will be loaded into the Control Center.

The session is closed in a similar manner. The currently open session automatically closes when the Control Center is closed.

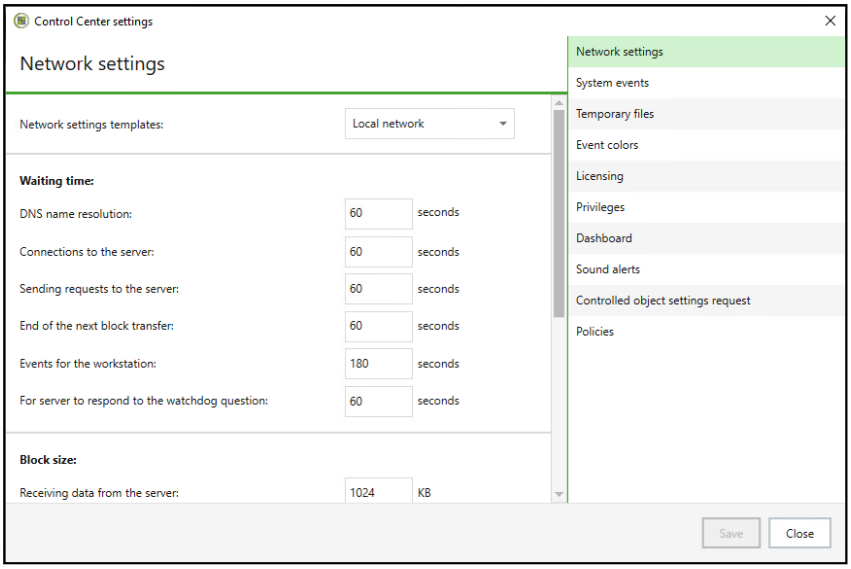
Control Center settings

To configure settings:

1. Click the **Settings** button at the bottom of the navigation panel.

   A panel with settings appears.
2. Click the **Control Center settings** link.

   A dialog box appears as in a figure below.



3. Select the required values for the settings. Settings are included in groups listed on the right of the dialog box. Click the name of the required group to view its settings. See below for the description of settings by groups.
4. Click **Save** after configuring the settings.

Note. Some settings take effect after the Control Center is restarted.

The Network settings group

Contains the settings for the program networking with the Security Server.

The Network settings templates field
Determines the template of network settings. Select the required template or configure settings manually in other groups. For settings description, see p. **216**.

The System events group

Contains settings for viewing information in the System events panel.

The Number of events in the System events window field
Determines the maximum number of notifications displayed on the **Events** dialog box. When the limit is reached, 80% of old notifications are deleted and 20% of the most recent notifications remain
The Event colors section
Fields in this section determine the color of the background of the table rows on the **Events** dialog box. The following types of notifications can appear in the events window: • **Network events** — notifications of changes in the condition of objects and the availability of communication with the Security Server; • **User actions** — notifications about the actions of the user in the Control Center; • **Alert events** — notifications of alert registration when working with the Control Center in centralized mode. You can specify a special color for each type of notification in the relevant cell by clicking the button in the right of the cell

The Temporary files group

Contains settings for the location and storage of temporary files created by the Control Center.

The Catalog for temporary files field
Shows the path to the directory where the Control Center temporary files are located. To specify another directory, type the full path to it or click the button on the right and select the required directory in the object selection dialog box. The path can be set explicitly or using environment variables
The Time period after which temporary files are deleted field
Determines the temporary file storage period in minutes starting at the time of the last call. Temporary files of loaded logs help accelerate a new call to these logs, without having to load data from the Security Server again. This setting applies during a user session of working with the Control Center. When work with the program is completed, temporary files from the most recent session are deleted, regardless of the configured storage period
The Path to PuTTY tool field
Determines the path to the PuTTY remote control program file used to connect to computers and to send control commands through Secure Shell (SSH). PuTTY is not shipped along with the Secret Net Studio product kit and should be installed separately. All the information about the program and links to download it can be found on the web-site of the developer: http://www.chiark.greenend.org.uk/~sgtatham/putty/ By default, the path to the Control Center setup directory is specified instead of the path to **putty.exe**. To select another directory, enter the full path to it or click **Browse** and select the required file in the appeared dialog box.

The Event colors group

Contains the settings for log entry color coding by sources of registration, categories or event codes. Formatting is based on rules that determine the conditions for the contents of fields in log entries. For a description of how settings are configured, see p. **218**.

The Privileges group

Contains the list of privileges for using the Control Center granted to the current user (including privileges the user has from groups).

The Dashboard group

Contains the field that determines time interval for updating the system security state on the Dashboard panel.

The Sound alerts group

Contains the settings of sound notifications to the program user about alerts as they occur. To control the sound notification mode, use the switch in the relevant section of the settings and configuration panel.

The Sound signal field
Determines the type of alert sound. A sound adapter should be installed on the computer to play the sound. This setting can have the following values: • **Alarm**, **Siren** — use the selected standard sound; • <***wav - file_name***> — use a sound from a specified file. To open the file selection dialog box, click **Choose**.
The Number of signal retries field
Determines the number of times the sound is repeated. To limit the number of repetitions, select the required numeric value. If **infinitely** is set, the sound will repeat until forced disable

The Retry interval field
Determines the pause between repetitions of the sound

The Controlled object settings request group

Contains a field determining the number of objects whose settings are stored in RAM after they are loaded.

The Policies group

Contains a parameter that allows you to configure a display of supported OS types for group policies. When enabled, each group policy has one of the following icons:

- — supported by Windows OS family;
- — supported by Linux OS family.

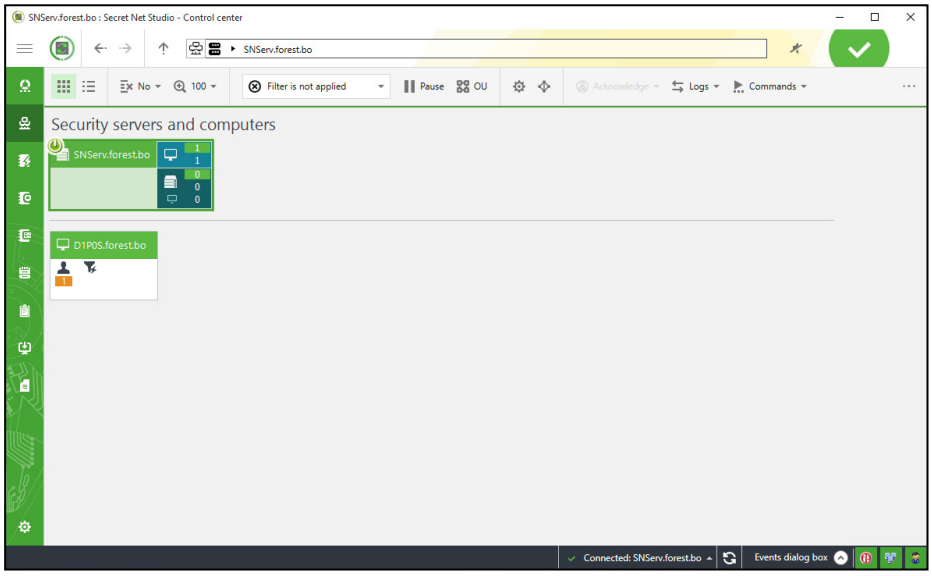
Chapter 13
Centralized control structure

Diagram and list of control objects

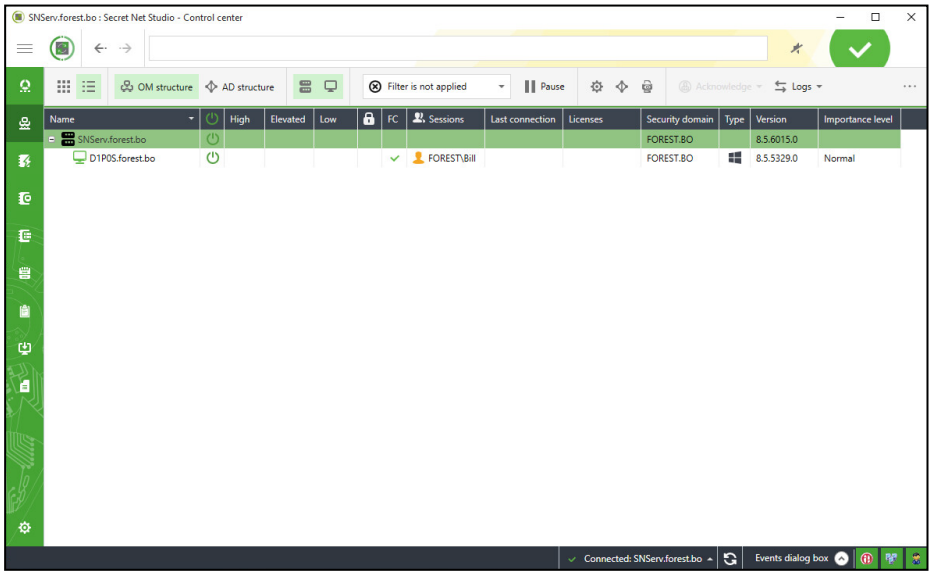
On the **Computers** panel, you can select the following modes for displaying control objects:

- **Diagram** is designed for graphical presentation of information about the structure of control objects;
- **Table** is designed for displaying the hierarchical list of control objects as a table.

The **Diagram** mode is shown in the figure below.



The **Table** mode is shown in the figure below.



To switch between display modes, on the **Computer** panel, on the **View** tab, click the **Diagram** or the **Table** button.

Structure objects

The structure is displayed on the diagram as a scheme of elements that correspond to security forests, business units, Security Servers and protected computers. The scheme is based on the structure of domains and business units in AD.

You can use the following main modes to view the scheme:

- the general original structure mode displays domains, business units, Security Servers, and groups of computers subordinated to Security Servers in respective business units;
- the computer lists mode displays the selected Security Server and the lists of directly subordinated computers.

In the general original structure mode, the diagram is split into two parts: the structure of security forests, AD domains and business units appear on the left, while Security Servers and groups of computers located on the level of AD objects that they are associated with appear on the right. Connections are drawn in each part between scheme elements from higher to lower elements, with the direction indicated by an arrow. An example of the diagram in the general original structure mode is shown in the figure on p. **115**.

To go to the computer lists mode, double-click the required Security Server or computer group. This enables an interface where the top of the diagram contains the selected Security Server with its subordinated servers, with computers directly subordinated to the selected server appearing below. An example of the diagram in this mode is shown in the figure on p. **121**. To return to the general original interface, use the navigation features at the top of the main window.

Object icons on the diagram are listed in the table below.

Icons	Description
	Security forest
	Domain or business unit
	Security Server
	Computer or computer group

Filtering objects

You can limit the number of displayed objects filtering them by:

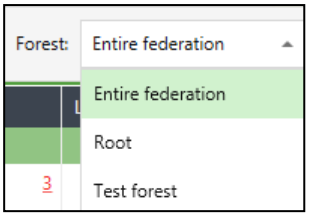
- association with security forests;
- association with domains and business units;
- their state;
- object types.

Filtering objects by association with security forests

In the general original structure mode, you can enable displaying of objects that belong to a specific security forest or to a whole federation.

To enable the display of objects of specific security forests:

- In the upper left corner of the **Computers** panel, in the drop-down list, select a security forest to display required objects.



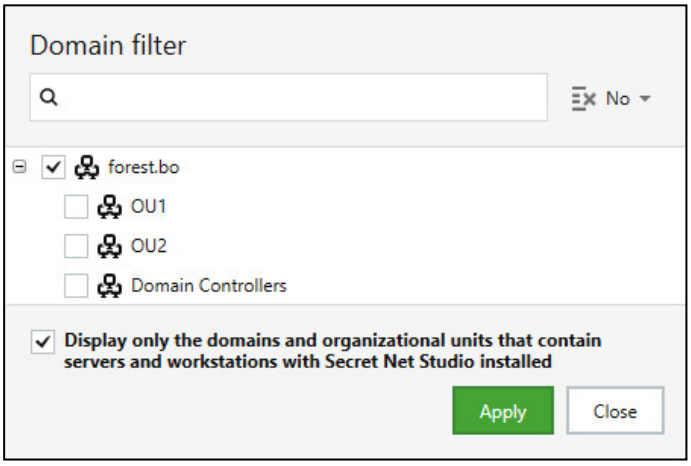
Filtering objects by association with domains and business units

Business units or domains whose objects do not need to be displayed in the Computers panel can be present in AD structure. For example, business units that have no protected computers. If necessary, you can use domain and business unit filtering to disable the display of unnecessary objects. Filtering applies both to the diagram and the table list of objects.

To enable the display of objects of specific domains and business units:

1. At the top of the Computers panel, click the **AD filter** button.

   The **Domain filter** dialog box appears where you can select domains and business units whose objects should be shown in the diagram as in the figure below.



2. If necessary, you can keep in the list only those domains and business units whose names contain a specific string of characters. To do this, type the desired string in the top field.
3. To manage the list of displayed objects, use the sorting button at the top of the dialog box.
4. Select the required list elements. To automatically select only the domains and business units that include computers with installed Secret Net Studio, select the respective at the bottom of the dialog box.
5. Click **Apply** and click **Close**.

   The diagram displays objects related to selected domains and business units.

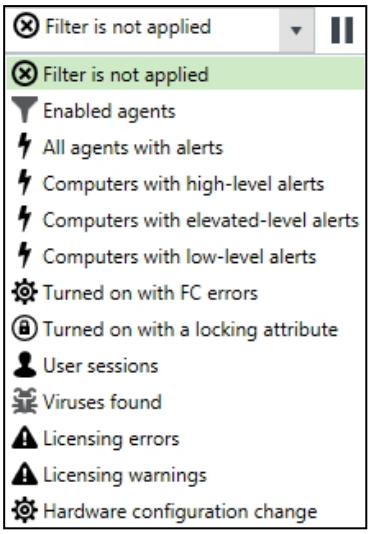
Filtering protected computers by their state

In the computer list mode (see p. 122), you can enable displaying of the objects that have a specific state, for example, computers with errors detected during a license verification or computers with an alert.

To enable the display of computers with a specific state:

1. Use navigation features to go to the required objects or point to the server/computer group and double-click it.
2. At the top of the **Computers** panel, select the feature for filtering from the drop-down list on the **Filter** tab.

A fragment of the panel with computer filtering tools is shown in the figure below.



Once filtering is enabled, the Security Server on the diagram is marked with a special icon of an active filter. This icon can be used as a button to disable filtering.

By default, filtering is performed dynamically: the list is automatically refreshed when the state of computers changes. If necessary, you can disable dynamic filtering to record the current list of computers.

To disable dynamic filtering:

- In the **Filter** section, click **Pause** next to the selected feature for which filtering is performed.

  Dynamic filtering is disabled and changes its appearance. To enable filtering again, click the button again.

Filtering by object types

When the object list is shown as a table, you can use the following buttons to filter objects:

- **OM structure** shows the object hierarchy as a tree of subordination of Security Servers and computers (the connection server is the root element of the hierarchy);
- **AD structure** shows the structure of AD domain made up of computers and business units;
- **View servers** enables and disables the display of Security Servers;
- **View computers** enables and disables the display of protected computers.

Import and export list of computers

Viewing the list of computers (see p. 122), you can export or import the names of workstations. Before importing the list of computers, it is necessary to export one or several computers.

To export a list of computers:

1. At the top of the **Computers** panel, select the Table mode of viewing objects.

   The list of root security servers and computers appears.
2. Select computers to export.
3. Click the **Export selected computer names to file** button.

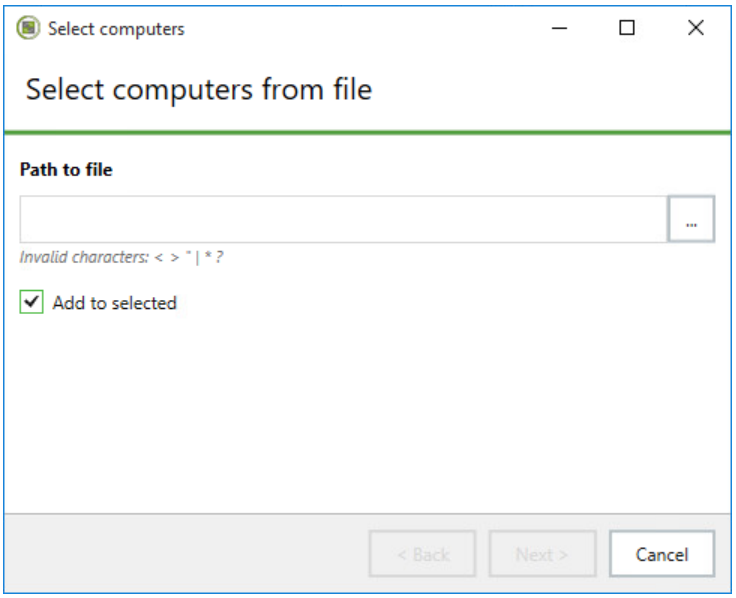
   In the system dialog, specify the file name and path.
4. Click **Save**.

   The file to be saved will have the .ws extension.

To import a list of computers:

1. At the top of the **Computers** panel, click the **Select computers from file** button.

   A window to select computers appears.



2. In the **Path to file** field, specify the file path.
3. In the dialog box, select the file with the list of computers.

   Files to be imported must have the txt, csv or ws extension.
4. Click **Open**.
5. Select the **Add to selected** check box to select computers from the file along with already selected computers. Clear the check box to select only computers from the file.
6. Click **Next**.

   If computers have been successfully added, the **Procedure has been successfully completed. Computers selected:** window will appear.
7. Click **Finish**.

Note. If some computers are not found, the **Selection results** window appears. The selected computers are displayed on the left; those not found in the list are displayed on the right.
In case of an error, the **No computers were found in the specified file** window appears.

Controlling the display of objects

The following general features are available to control how objects are displayed on the diagram:

- using navigation features to move about the OM structure;
- sorting objects;
- scaling the structure.

Objects can be additionally grouped by their association with business units in the computer lists mode (see p. 122).

Using navigation features to move about the OM structure

Navigation features at the top of the program main window (see p. 115) can be used to move about the OM structure and the search for the Security Servers and protected computers. You can move about the structure by selecting the required elements. Objects can be searched by their name when typing the required character string.

Navigation features are used like those in standard Windows OS applications such as Internet Explorer and File Explorer.

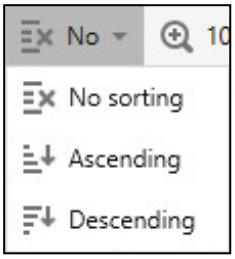
Sorting objects

Objects on the diagram can be sorted alphabetically. Their names can be sorted in descending or ascending order.

To sort objects:

1. In the **Computers** panel, on the **Diagram** tab click the **Sorting** menu.

   A menu appears as in the figure below where the sorting order can be selected.



2. Select the sorting order.

   Objects will be arranged in the selected order.

Using diagram scaling features

Scaling features are used to display elements on the diagram in the selected scale. This is useful to fit all the required elements onto the screen.

To modify the scale of display:

- Specify the required scale at the top of the main window of the program on the **Diagram** tab.

Grouping computers by association with organizational units

In computer lists mode, the general list of subordinated computers of the selected Security Server is displayed by default. If computers within different organizational units are subordinated to the Security Server, a grouping of computers can be enabled. When the grouping is enabled, the list of computers is split into blocks by different business units. Blocks are separated by horizontal lines, and key details are provided for each block.

Note. When the general original structure is displayed on the diagram, computers are always grouped into elements called computer groups. Each element brings together computers subordinated to one Security Server and associated with one business unit. To identify the server that computers in the group are subordinated to, find the parent element (that is linked to this group) in the diagram or point to the group element and double-click it to enable list mode.

To enable grouping of a computer list:

1. Enable the computer lists mode. Use navigation features to go to the required objects or point to the server/computer group and double-click it.
2. In the object display control panel, click **OU**.

   The list of computers will be split into blocks by organizational units. To disable grouping, click the button again.

OM structure after installation of Secret Net Studio components

Components of Secret Net Studio must be installed as described in the chapters 5–7 of this document. If the Security Servers and the Clients were subordinated to related Security Servers, computers with such components will be included in the operational management structure. The OM structure is considered to be adequately created if all protected computers are present in it and subordinated to the Security Servers.

Editing the OM structure

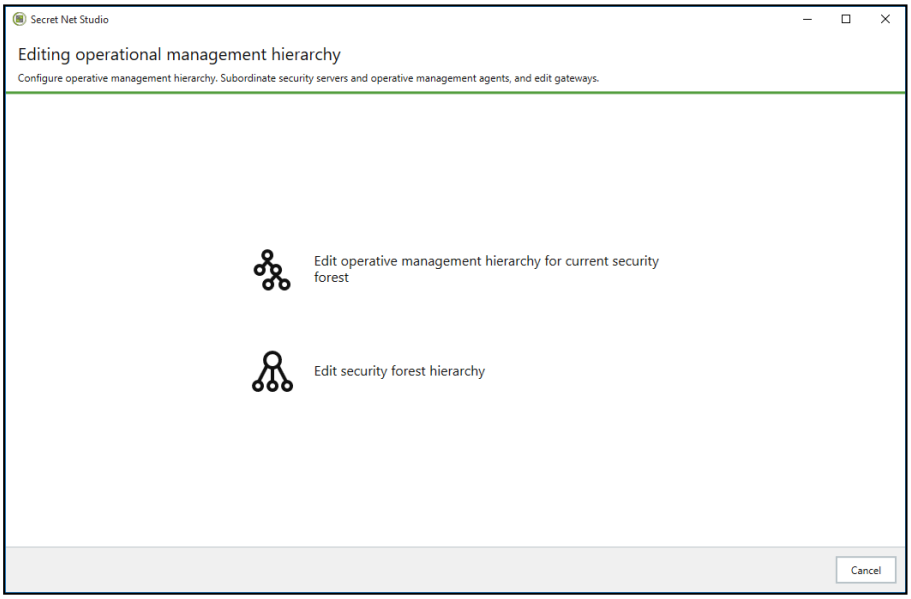
All available Security Servers and protected computers must be present to implement centralized control functions within the OM structure. Operations such as adding and removing objects to/from the OM structure can be performed automatically when installing or uninstalling Secret Net Studio on computers. If necessary, objects can be manually added or removed in the structure in the Control Center; for example, to implement automated installation of the Client, to make computers with Secret Net LSP subordinate to the Security Server or to register a gateway that provides interaction with a security domain child forest.

To open the OM structure editing dialog box:

1. At the bottom of the navigation panel, click the **Settings** button.

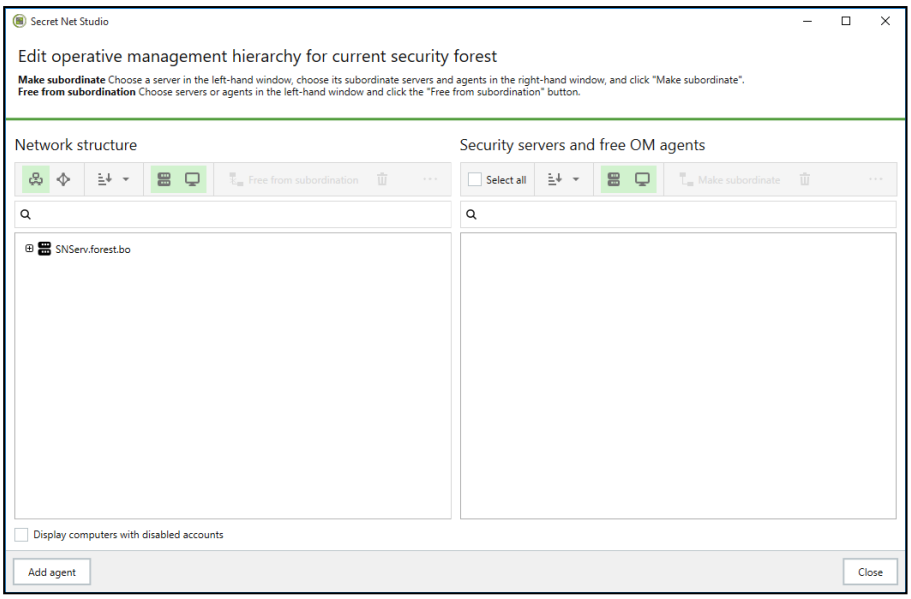
   A panel with settings and configuration features appears.
2. Click **Configuration**.

   A dialog box appears as in the figure below.



3. Select one of the following:
   - **Edit operative management hierarchy for current security forest** — if you need to edit the OM structure of a current security forest.

     A dialog box appears as in the figure below.



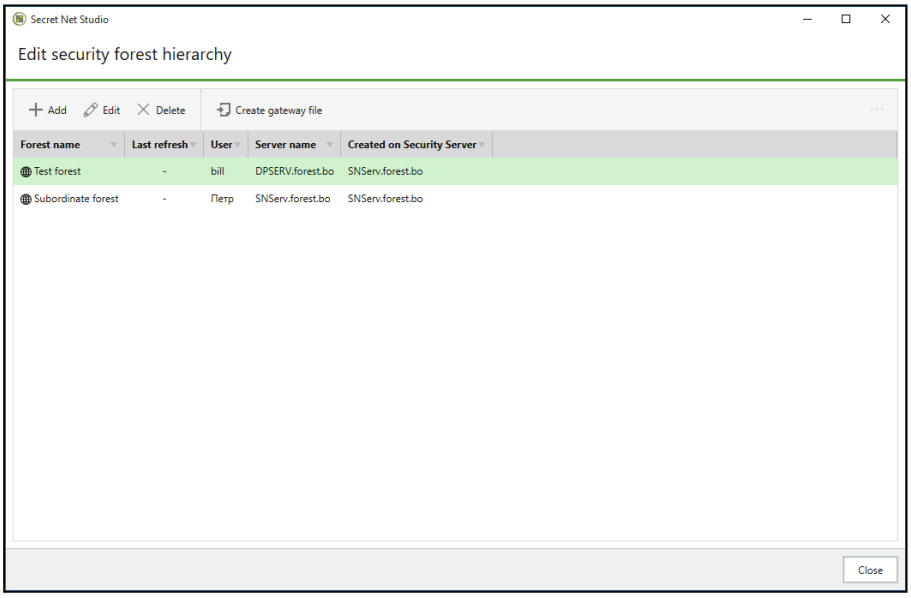
The current structure of the managed objects appears in the left part of the dialog box. In the right part, there is a list of protected computers and Security Servers available for subordination to the selected server.

Configure the object structure and click **Close**.

Note. If necessary, you may filter object lists by hiding objects of certain types. To filter the object lists, use the respective elements above them (buttons and search bars).

- **Edit security forest hierarchy** — to view and edit the gateway list for subordinate security forests connection.

  A dialog box appears as in the figure below.



The dialog box displays registered gateways. Parameters are specified for each gateway. Edit the list (see p. **132**) and click **Close**.

Adding objects to the OM structure

In the Control Center, any computer registered in Active Directory can be added as an OM structure object.

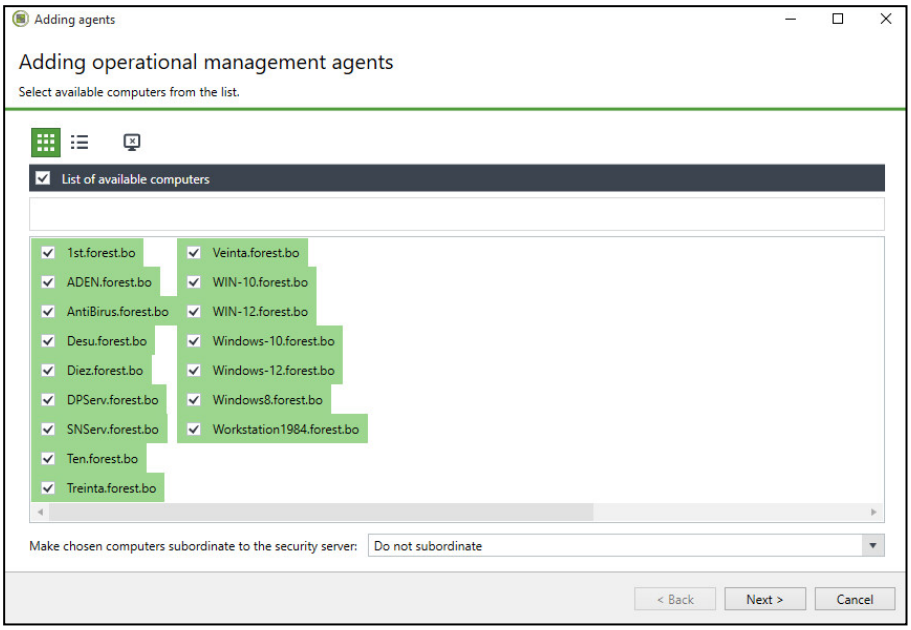
Note. Linux OS computers protected by Secret Net LSP can be registered (added to the domain) in Active Directory only when configuring remote control. See the description of the configuration sequence in Secret Net LSP documentation.

If the security domain is based on the embedded AD container (in the business unit), before being added to the OM structure, computers should be moved to this container by using standard AD administration features.

To add computers:

1. Open the OM structure editing dialog box (see p. **127**).
2. Click **Add Agent**.

   A dialog box appears as in the figure below.



   The dialog box contains a list of computers in the AD container that are not included in the OM structure (the security domain of the selected server is based on the displayed container).

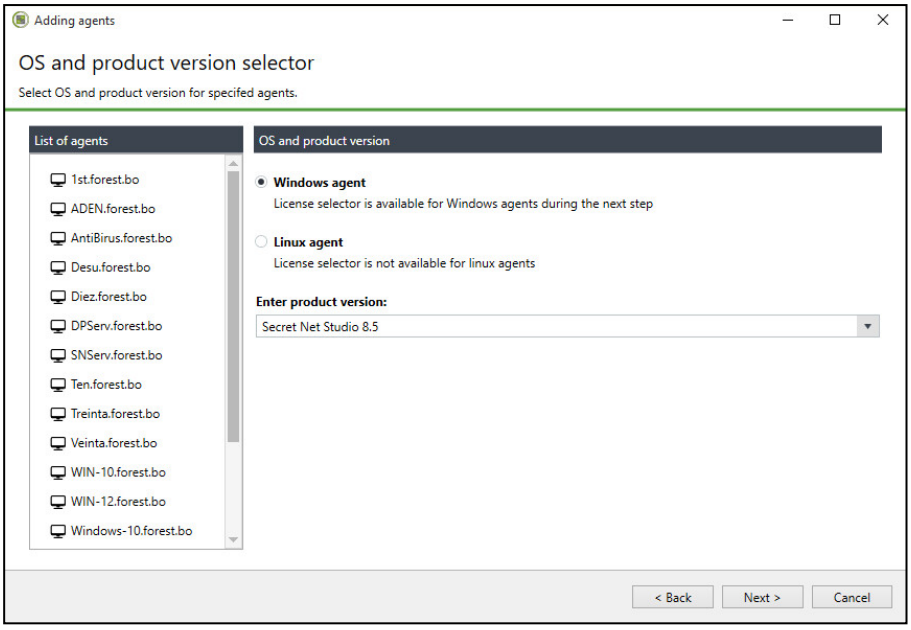
   Note. Available computers may be viewed as a list or as a table using the buttons above the display area. The list may be filtered by hiding disabled accounts and/or accounts with names that do not contain the given string of characters. To filter the list, select/clear the **Display computers with disabled accounts** check box.

3. In the list, select the computers that are to be added to the structure.
4. To subordinate computers to the Security Server, select the name of the required server in the **Make chosen computers subordinate to the security server** field.

   Note. Computers can be subordinated later (see p. 131).

5. Click **Next**.

   A dialog box appears as in the figure below where you can select the OS type and the product version.

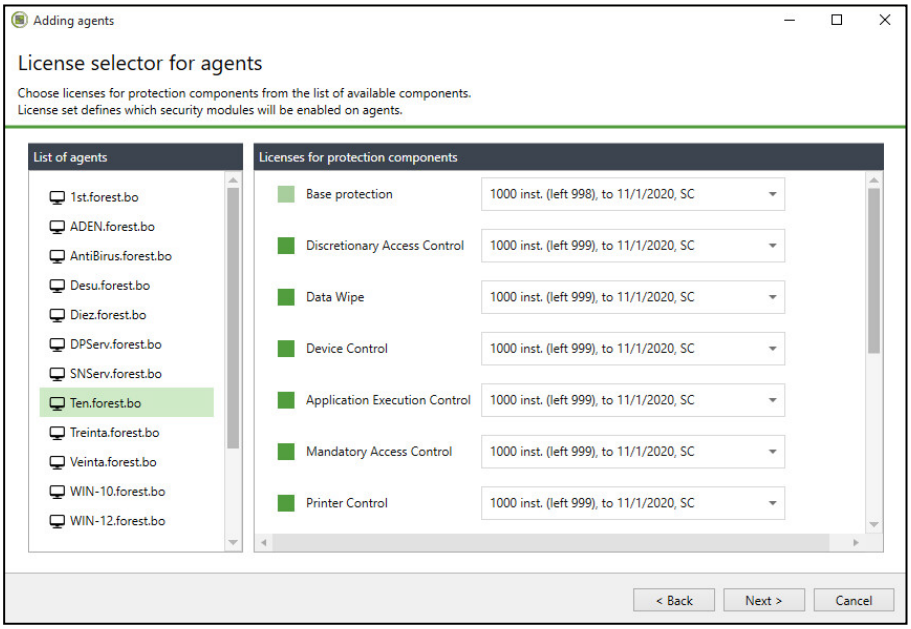


6. Select the respective OS type for the computers and enter the product version.

Attention! You must specify the product version for the computers correctly. Otherwise, the operation of the subordinated computers will be unstable. In this case, the OM structure objects require to be removed and then added once again.

7. Click **Next**.

If a Windows agent is specified, a dialog box appears as in the figure below where licenses to use the Secret Net Studio components (subsystems) on protected computers can be selected.

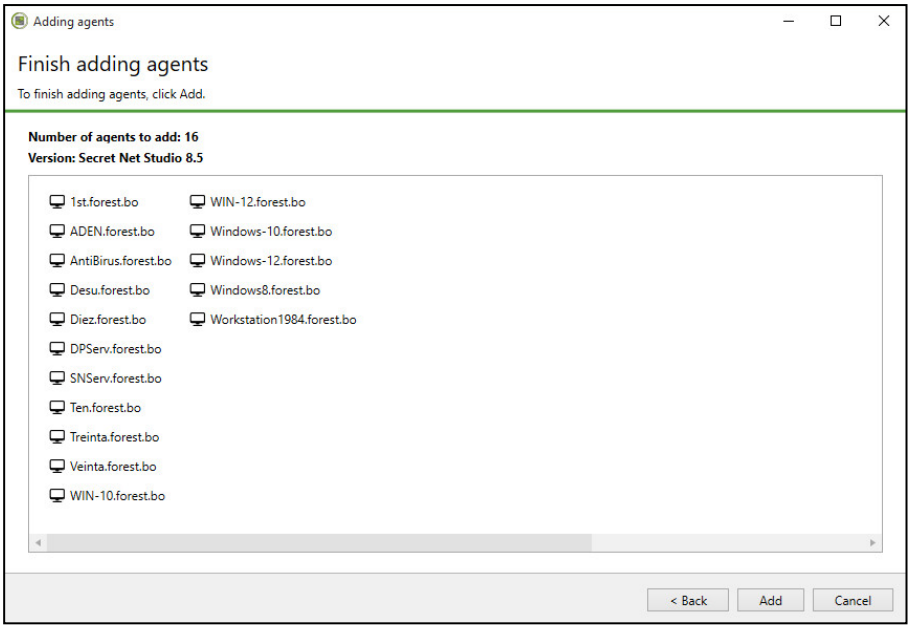


8. Select the subsystems that will be running. To manage subsystem activation (by enabling or disabling licenses), use the controls located to the left of the subsystem names. If there are different licenses registered on the Security Server for a subsystem, select the required license from the drop-down list.

Note. Base protection is enabled by default. Other subsystem can be enabled manually.

9. Click **Next**.

A dialog box appears as in the figure below to finish adding agents.



10. Click **Add**.

Selected computers are added to the current OM structure.

Managing the subordination ratio in the OM structure

The OM structure provides the option to change the ratio of subordination between the Security Servers or subordinating the protected computers to other servers. Resubordination of objects (for example, when the network structure is revised) requires that such objects should first be withdrawn from subordination to current Security Servers.

Withdrawing objects from subordination

An object that is withdrawn from subordination to the current Security Server becomes free. A free computer should be then subordinated to the respective Security Server. If the Security Server was withdrawn from subordination, this component can continue operating as an independent control object.

To withdraw objects from subordination:

1. Call up the OM structure editing dialog box (see p. **127**).
2. On the **Network Structure** list (on the left), select the objects to be withdrawn from subordination.
3. Click **Free from Subordination** and then confirm your operation in the dialog box that appears.

   The selected objects appear in the list of free objects when the Security Server is selected.

Subordination to the Security Server

New objects are subordinated to the Security Server from the free Security Servers and protected computers. If the required Security Server or protected computer is missing from the list of free objects, before subordination the object should be added to the structure (see p. **128**) or withdrawn from subordination to another Security Server (see above).

To subordinate objects:

1. Call up the OM structure editing dialog box (see p. **127**).
2. In the **Network Structure** list (on the left), select the Security Server that new objects need to be subordinate to.

A list of free Clients and root servers available in the OM structure appears in the right of the dialog box.

3. In the list of objects in the right of the dialog box, select computers to be subordinated to the selected Security Server. To select all elements in the list, select **Select all** located above the list.
4. Click **Make subordinate**.

Removing objects from the OM structure

Protected computers should only be removed from the OM structure in the Control Center if some components do not work on those computers. For example, due to incorrect Secret Net Studio uninstallation or when moving the computer from one security domain to another. If you need to exclude an object temporarily, first withdraw it from subordination to the Security Server (see p. **131**) and then reestablish the subordination ratio.

To remove objects:

1. Call up the OM structure editing dialog box (see p. **127**).
2. Select objects to remove.
3. Click **Remove the Operational Management Object** above the list with selected objects. Confirm your operation in the dialog box that appears.

Managing gateways

When the configuration wizard is in this mode, you can add gateways to the OM structure, edit their names, delete gateways and create gateway configuration files required to install gateway software in a child security forest.

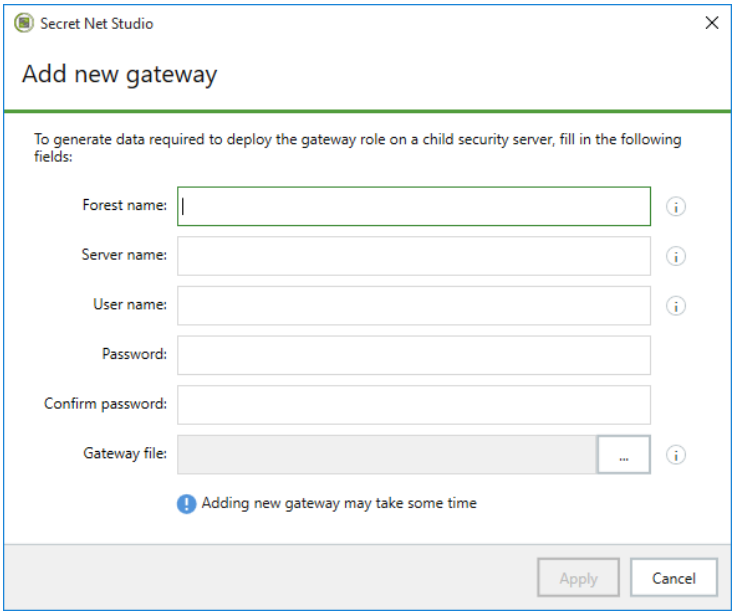
Adding a gateway

When a gateway is added, its essential parameters are set and a configuration file required for gateway software installation on the child Security Server is created.

To add a gateway:

1. Open the gateway list editing dialog box (see p. **127**).
2. Click **Add**.

   A dialog box appears as in the figure below.

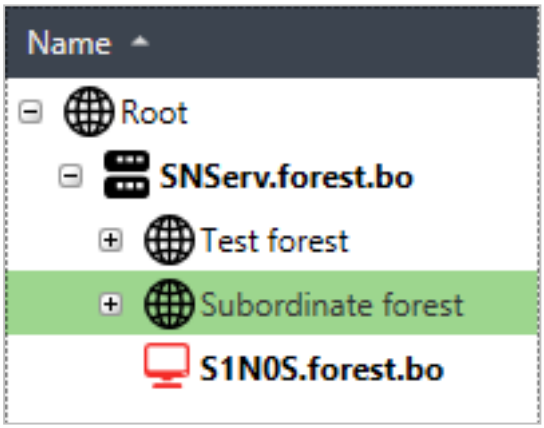


3. In the respective dialog fields, specify gateway parameters.

Parameter	Description
Forest name	The name of a root object in the OM structure, associated with the respective child security forest. You can change this name later
Server name	The DNS name of a gateway computer with a child security forest. It is necessary to specify a full DNS name including an AD domain name. For example, SecServer.SecondDomain
User name	The name of a user account used for an interaction between a gateway and the root Security Server. This user account is used automatically
Password/Confirm password	Enter the password for the specified user and then confirm it. Remember this password, because you will need it during gateway software installation on a child Security Server
Gateway file	Name of the file containing the gateway configuration. You will need this file to install gateway software on a child Security Server. To create the file, click the button to the right of the field, then enter the file name and its destination folder in the dialog box

4. Click **Apply**.

   The gateway adding process begins. For information on the process progress, see messages in the Events dialog box. Wait until the gateway is added. The new object appears on the gateway list. In the hierarchical OM list, the new object appears as in the figure below.



5. Click **Close**.

   Now you can install gateway software on a child Security Server and configure synchronization settings for the created gateway (see below).

Editing the gateway list

You can edit the gateway list using the following buttons:

Button	Description
Edit	Open the name editing dialog box for a selected gateway. Specify the required changes and click **Apply**. You can change other gateway parameters only by creating it again
Delete	Delete selected gateways from the list, the OM structure and a server database. After being deleted, the gateway cannot be used. To select multiple elements, use **Shift** and **Ctrl**
Create gateway file	Open the dialog box to create another gateway configuration file for a selected gateway. In the dialog box, click the button to the right of the field, then enter the file name and its destination folder

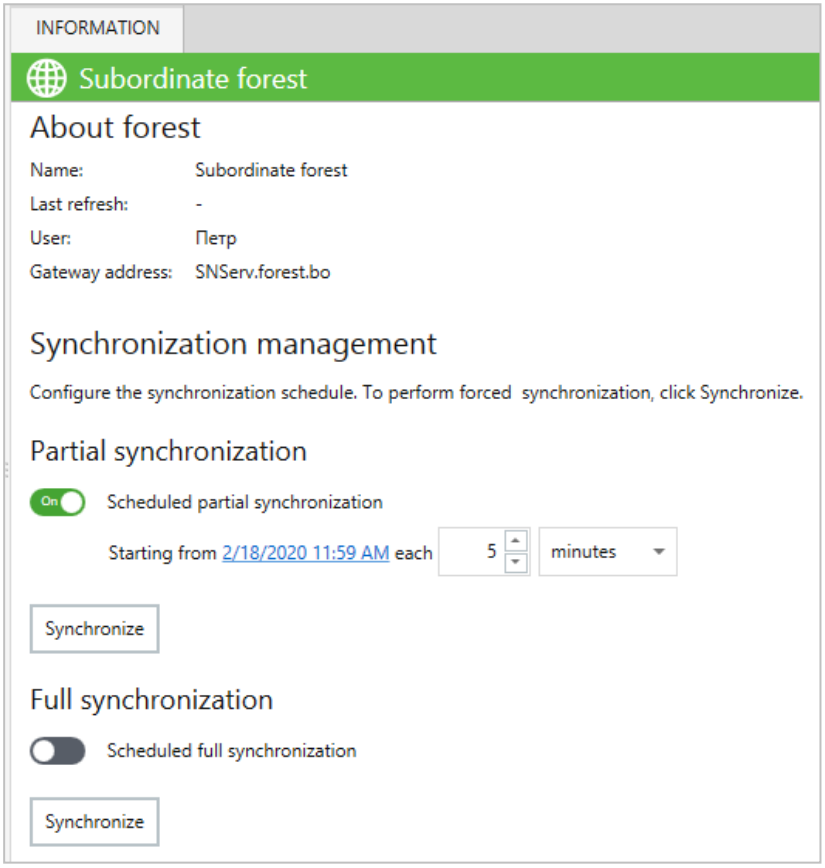
Configuring synchronization settings

Gateway synchronization settings determine synchronization frequency and the amount of information about the state of management objects sent from a child security server to the root server. There are two synchronization modes:

- Partial synchronization — synchronizes only the data modified after the last synchronization;
- Full synchronization — synchronizes all state data for management objects.

To configure synchronization settings:

1. In the Control Center, on the **Computers** panel, select an object related to the required child security forest (gateway). Right-click the object and click **Properties**. On the properties panel, the **Information** tab appears as in the figure below.



2. Turn on **Partial synchronization** and/or **Full synchronization** toggles in the respective group boxes.
3. For enabled modes, specify synchronization start date and time as well as frequency.
4. To apply changes, at the bottom on the **Information** tab, click **Apply**.

Tip. If you need immediate synchronization in one of the modes, click **Synchronize** in the respective group box. To force the synchronization, on the **Computers** panel, right-click the required child forest and select **Forest > Update configuration**.

Chapter 14
Configuring security settings

Secret Net Studio performs the following functions:

- manual configuration of security settings;
- import of security settings from a template;
- creation of security settings template using object settings;
- comparison of object security settings and template security settings.

Lists of security settings

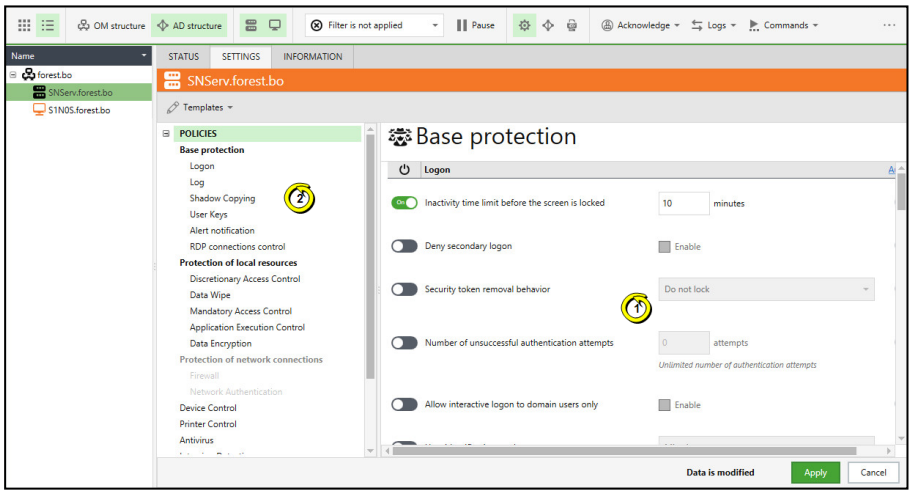
Security settings are managed on the **Computers** panel. Select an object and open its properties:

- on the toolbar, click **Properties**;
- right-click the required object and click **Properties**.

Go to the **Settings** tab.

To manage security settings of the selected object, go to the **Settings** tab and click **Load Settings**. The set of available settings depends on the type of selected object. After the settings are loaded, click **Refresh** at the top of the tab to update them.

An example of the **Settings** tab is shown in the figure below.



Note. The figure shows: 1 — the settings pane; 2 — the table of contents pane.

Purpose of elements:

Settings pane
For viewing and configuring object settings. Settings are distributed into groups. Groups with required settings can be selected in the table of contents pane
Table of contents pane
For selecting sections and groups for the settings pane. The table of contents contains the following higher level sections: • **Policies** brings together groups of settings used to configure the operation of security mechanisms on computers. • **Event registration** brings together groups of settings used to configure event registration in local logs. • **Parameters** brings together groups of parameters used to configure and maintain Security Servers and protected computers

Panes are separated by boundaries that can be moved. If necessary, you can hide any pane by moving its boundary. Individual scroll features are used to view data in each pane.

Saving changes

Changes made in the Control Center take effect after they are saved. Changes can be saved if the Security Server connection session is active. When using the program, you should regularly save your changes to avoid losing them if the connection with the Security Server is interrupted.

To save changes, click **Apply** at the bottom of the tab. The button appears if there are any unsaved changes.

A notification appears in the system events panel about the outcomes of the performed action.

Configuring settings in the Policies and Event Registration sections

The Policies and Event Registration sections of departments and the Security Servers contain settings applied on computers through group policies. These settings are designed for configuring the operation of security mechanisms and event registration in local logs.

Policies section settings

Note. This section contains the lists of parameters for the Clients of Windows OS family. Parameters for Linux OS family are different. You can configure a parameter for displaying the OSs supported by the group policies (see p. 120).

The **Policies** section includes the following groups of settings:

- **Base protection** groups (**Logon**, **Log**, **Shadow Copying**, **User Keys**, **Alert notification**, **RDP control**, **Security system administration**) contains settings for configuring basic Client security mechanisms;
- **Local protection** groups (**Discretionary Access Control**, **Data Wipe**, **Mandatory Access Control**, **Application Execution Control, Disk Protection and Data Encryption**) contain settings for configuring local Client security mechanisms;
- **Network protection** groups (**Network Authentication**, **Personal Firewall**) contains settings for configuring network Client security mechanisms;
- **Device Control** group contains settings for configuring device connection, modification control and device control mechanisms;
- **Print Control** group contains settings for configuring document marking, shadow copying, printer list and direct printing policies;
- **Antivirus** group contains settings for configuring real-time protection, different scan modes, exclusions and scan schedule;
- **Intrusion Detection** group contains settings for configuring network attack detectors and signature analyzers;
- **Update** group contains settings for configuring automatic checks for updating antivirus and intrusion detection databases;
- **Software Passport** group contains settings for configuring software passport generation schedule, folder properties and file extensions.

The details of mechanism configuration are provided in the related documents.

If event registration control is supported for a mechanism, you can go to the settings related to this mechanism in the **Event Registration** section. To go to the required group of registration settings, click the **Audit** link on the right of the group heading.

Event Registration section settings

Event Registration section settings are designed to enable and disable the registration of specific events in the Secret Net Studio log. Settings are distributed among groups by respective event categories.

Applying settings on computers

Settings configured in the **Policies** and **Event Registration** sections are applied on computers in the following order:

1. Settings made directly for the computer (local policy settings).
2. Settings made for domains and business units, — similar to the mechanism of Windows group policies, domain policy settings are applied first, followed by settings of policies for business units.
3. Settings made for Security Servers, — settings of the Security Server that computers are subordinated directly to are applied first followed by higher servers in the hierarchy.

Therefore, policy settings made for the root Security Server have the highest priority and are applied on all computers in direct or transitive subordination.

By default, settings are only configured in the local policy. For most of the local policy settings, values can be modified both centrally in the Control Center and locally on the protected computer. In this case, the value configured by a policy of another level cannot be modified in the local policy. Details of the policy that determines the value of the setting appear in the **Source** column of the local policy.

When several Security Servers are used, if the security domain structure is deployed on parent and nested AD containers (for example, one security domain represents the entire AD domain, and another, a nested business unit in this AD domain), the following policy settings features apply:

- policy settings of domains and business units set when connecting the program to the server in a parent security domain do not apply on protected computers subordinated to a server in another security domain in a nested Active Directory container. For these computers, policy settings of domains/business units should be configured when the program is connecting to the Security Server in a nested AD container. Individual sets of settings are used for domains/business units in each security domain;
- policy settings for the Security Server are unique within the forest of security domains and can be configured when the program is connecting either directly to this server or to any servers in other security domains (if the user has the required rights). Policy settings for the Security Server will be represented by one set regardless of how they were configured during connection to this server or to servers of other security domains.

Configuring settings in the Parameters section

The **Parameters** section includes groups of settings applied on the selected Security Server or protected computer.

Object settings may be present in the following groups:

- **Registration information** contains information about the computer used for registration;
- **Network Settings** contains network connection settings when the object interacts with the parent Security Server;
- **Log collection** contains settings for transferring local logs to the Security Server;
- **Server configuration** contains information about the Security Server certificate and the temporary files and archives location on the server;

- **Log Archiving** contains settings of automated archiving of logs stored in the Security Server database;
- **Alert Mailing List** contains settings of notification mailing when alerts are registered on subordinated computers;
- **User Privileges** contains a list of accounts with privileges for working with the Control Center;
- **Filter Of Alerts From Subordinate Servers** contains filtering settings for notifications about alerts arriving from Security Servers subordinated to the selected Security Server;
- **Windows Authentication** contains the setting the determines Windows authentication trust for the security domain;

  Attention! Windows Authentication is a global setting. If you change this setting for a security server, it will change for all servers inside the security domain

- **Tracing management** contains settings for tracing how the Secret Net Studio operates (service function).

Network connection settings

Network connection settings are managed in the **Network Settings** group. This group is available when selecting the Security Server or protected computer.

Settings are used when an object is establishing a network connection to the Security Server that the object is subordinated to. You do not need to configure these settings for the root.

The networking of Secret Net Studio components creates a certain load on communication channels. The stability of network connections and time for data transfer depend on the network capacity. If the capacity is low (for example, when connection is over a modem), connections can take long to establish, and even data transfer failures can occur.

To make sure the system operates normally on slow communication channels, the security administrator should check and, if necessary, adjust the settings of networking objects. These settings determine timeouts during the execution of network requests.

Note. There are other ways of reducing the load on communication channels, for example, by modifying the synchronization settings of integrity control jobs used by default on computers (see document [**2**]).

To configure network connection settings:

1. Select the required template in the **Network Settings Templates** to configure networking settings. Values of other fields change automatically based on the selected template. If necessary, you can edit the value manually (for a description of settings, see p. **216**).
2. Click **Apply** at the bottom of the **Settings** tab.

Settings of local log transfer

Settings of local log transfer are configured in the **Log Collection** group. This group is available when selecting the Security Server or protected computer.

Settings of local log collection configured for the Security Server apply to all computers subordinated to this server. In this case, settings can be customized on individual computers and will have a higher priority compared with settings configured on the Security Server.

The contents of local logs of a protected computer should be received in a timely manner by centralized logs in the Security Server database. Extended delays between transfers can cause an overflow of local logs or excessive load on the Security Server and communication channels as they receive large data volumes.

To avoid problems associated with untimely data transfer, the security administrator should check and, if necessary, adjust max Secret Net Studio log size and event overwrite settings (configured in the **Basic protection** section, **Log**

group), configure log collection settings and schedule (configured in the **Parameters** section, **Log collection** group). In these settings, you can configure conditions for transferring local logs to the Security Server and the schedule for starting the transfer. Settings should be configured in a manner that minimizes the load on network channels at peak times (for example, at the start of the working day or at a time scheduled for downloading software updates to computers), prevents logs from completely filling on protected computers (because user access to the computer can be restricted if the local log is full).

To configure log transfer settings:

1. Configure basic settings in the **Collect logs** tab:
   - If log collection must run every time computers are connected to the Security Server, select **When an agent connects to the security server**.
   - If logs that are almost full should be transferred to the Security Server, select **When filling the log 80% or more.**

     Note. Secret Net Studio monitors how full the local log on a computer and sends the log to the server when is the current log size reaches the 80% of the maximum log size. The log is transferred after the Security Servers confirms its readiness to receive the log. During the server's peak times, receipt of a full log is delayed.
2. If necessary, disable centralized collection of logs of certain types by clearing the relevant check boxes of the group **Enable collection of the following logs**. Centralized collection can only be disabled for standard Windows OS logs.
3. If copies of the contents of local logs should be kept on computers after their transfer to the Security Server, select **Save log copies on the protected computer**.

   Note. The copies of the contents of local logs are kept on the computer as EVT files in the directory **%ProgramData%\Security Code\Secret Net Studio\Client\OmsAgentEvtCopy**. These files are processed and deleted by the administrator.
   The log copying is used for troubleshooting. It must be disabled in normal operation mode.
4. If the transfer of local logs of connected computers must start at specific times, configure a log collection schedule by selecting the required mode in the drop-down list.

Periodically
Log transfer starts at even intervals. The interval is set in minutes, hours or days. The mode becomes active when a specific date and time are reached. To specify a different start time of the mode, select the link with the current date and time and specify the required values in the dialog box that appears
Weekly
Log transfer is performed at times specified in the schedule. The schedule is represented as a table. Table columns and rows list days of the week and hours, respectively. To choose the start time, select the required cell in the table. The schedule repeats on a weekly basis

   To disable a scheduled log transfer, select **Not Set** in the drop-down list. If the mode is disabled for a protected computer, schedule settings configured for the parent object will apply. To go to these settings, click **Go to the active schedule of the parent object**.

   Note. Schedule settings configured for the Security Server do not apply to computers with customized log transfer schedules.
5. Click **Apply** at the bottom of the **Settings** tab.

Server configuration

You can manage server settings in the **Server configuration** group. You can see the group while selecting a security server.

The server requires the certificate for the agent subordination. The link **Installed** appears in the **Servercertificate** field when there is the required certificate. With the help of the link **Installed**, you can call up the dialog box with the Security Server certificate details.

To place archives and temporary files created by the Security Server, there are local folders in the server software installation folder by default. You can specify other paths to place files in the **Files location on the server** field. After entering the path, click **Apply** at the bottom of the **Settings** tab.

Note. In case of using a network path, you should grant access to a folder for the Security Server computer account using built-in tools of the computer containing the network resource. Other user accounts should be limited in their rights to access. You can configure access right in the **Security** (permissions to access the folder) tab and **Sharing** (permissions of sharing) tab of the folder properties dialog box. You should add the security server computer account to the account list and select **Read** and **Write** check boxes if you configure permissions to access the folder, or select **Read** and **Modify** if you configure permissions of sharing.

Settings for archiving centralized logs

Settings for archiving centralized logs are managed in the **Log Archival** group. This group is available when selecting the Security Server.

Settings are used to create the schedule of automatic archiving centralized logs. Archiving applies to log entries received from subordinated protected computers and stored in the Security Server database.

The database should be archived regularly to ensure information integrity. Some DBMS versions impose limitations on the database volume. If the database exceeds the limit, new information cannot be received until the DB is cleaned.

In addition to information integrity, archiving helps remove irrelevant information from the database to reduce DB request execution time. If you need to view old entries about events, files of archive copies can be loaded to the Control Center.

Archiving can be performed on a set schedule for the Security Server or by running a special command available in the Control Center.

To configure archiving settings:

1. Select the required mode in the drop-down list:

Periodically
Archiving starts at equal intervals. The interval is set in minutes, hours or days. The mode becomes active when the preset date and time are reached. To specify a different start time of the mode, select the link with the current date and time and specify the required values in the dialog box that pops up.
Weekly
Archiving is performed at the times specified in the schedule. The schedule is represented as a table. Table columns and rows list days of the week and hours, respectively. To choose the start time, select the required cell in the table. The schedule repeats on a weekly basis

   To disable the automatic start of archiving, select **Not Set** in the drop-down list.

2. Click **Apply** at the bottom of the **Settings** tab.

Alert mailing settings

Settings for sending alert notifications are managed in the group **Alert Mailing List** This group is available when selecting the Security Server.

When registering alerts on protected computers subordinated to the Security Server or its subordinated servers, Secret Net Studio can automatically notify designated employees about this. Notifications are sent via email.

Mailing follows special rules that distribute notifications by sources of registration, categories or event codes. Based on preset rules, the Security Server will handle all registered alerts that it has received information about.

For example, you can configure notification mailing as follows:

- When an **Logon/logoff** category alert occurs, notifications are delivered to the system administrator.
- When an alert of any level occurs, notifications are delivered to the security administrator and the auditor.

To configure mailing settings:

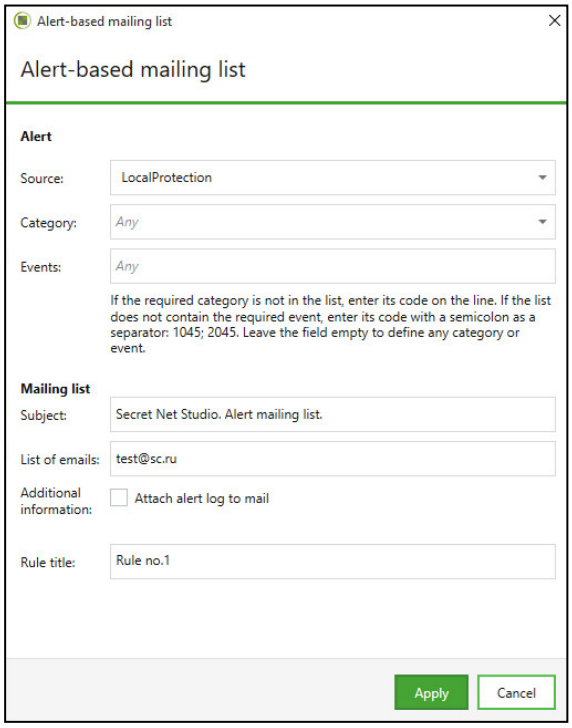
1. Create a list of mailing rules. To work with the list of rules, click the buttons under the list.

Button	Description
Edit	Opens a dialog box where you can configure the settings of the selected rule (see below)
Add	Adds a new rule to the list. Settings of the new rule are configured in the dialog box (see below)
Remove	Removes the selected element from the list

2. In the **Mail server** field, enter the name or IP-address of the mail server through which notifications will be sent. In the **Port** field, specify the number of the port for access to the server.
3. In the **From** field, enter, if required, the e-mail address to which notification recipients can send their responses. For example, the security administrator's e-mail address can be specified for these purposes.
4. If necessary, enter credentials for accessing the mail server. To do this, select the **Authentication** check box and enter the user name and password.
5. Click **Apply** at the bottom of the **Settings** tab.

Configuring mailing rule settings

An example of the mailing rule settings dialog box is shown in the figure below.



To configure the settings of a mailing rule:

1. In the **Ruletitle** field, edit the name for the element in the list of rules.

2. Configure event analysis settings in the **Alerts** group of fields:

Source
Contains the component or subsystem name specified at event registration as a source. Select the required source
Category
Contains a numeric code of the event category. Select the code of the required category from the drop-down list or enter the value manually. The list of categories available for selection depends on the specified source
Events
Contains numeric identifiers of events. Select identifiers of the required events from the drop-down list or enter the value manually. The list of events available for selection depends on the category specified. Identifiers are separated by **;**

Note. Details of events can be received when viewing alert log entries on the General tab (see p. 176). Sources, category codes and identifiers of events appear, respectively, in the following panes of the tab: Source, **Category** and **Events**.

3. In the **Mailing** group of fields, configure settings of notification mailing:

Subject
Contains a string that will appear in notifications as the e-mail subject
List of emails
Contains the list of e-mail addresses of notification recipients. Addresses are delimited by **;**
Additional information
If this check box is selected, notifications will contain additional information about alerts (in attached text files). This setting only applies to computers subordinated to this Security Server. Details are not added to notifications about alerts that occur on protected transitive subordination computers (associated with subordinated servers)

4. Click **Apply**.

The Control Center user privileges

The Control Center user privileges are managed in the **User Privileges** group. This group is available when selecting the Security Server.

Users and user groups can be assigned the following privileges:

- **View information** — the privilege for connecting to the Security Server and viewing information
- **Edit object hierarchy and parameters** — the privilege for editing object configuration and managing settings in the Settings section
- **Execute operational commands** — the privilege for running operational management commands
- **Edit policies** — the privilege for configuring the settings of the Policies and Event Registration sections
- **Acknowledge alert notifications** — the privilege for running alert acknowledgment commands
- **Collect logs on command** — the privilege for performing an unscheduled transfer of computers local logs
- **Archive/restore logs** — the privilege for archiving or restoring centralized logs
- **Load software passports from a file** — the privilege for uploading computer software passports to the Security Server database

- **Sign software passport** — the privilege for executing the command of passport draft signing as the current computer passport
- **Synchronize software passport database** — the privilege for executing the command of synchronizing passports stored on security server
- **Delete software passport**s — the privilege for deleting all the passports except the current one
- **Security system administration** — the privilege for configuring the self-protection settings.

By default, all privileges listed above are available to users that are members of the group of security domain administrators. If necessary, privileges can be assigned to other accounts, except for the **Edit object hierarchy and parameters** privilege, which is only available for the group of security domain administrators.

To grant privileges:

1. Create a list of users and groups that privileges should be granted to. Use the buttons under the list to add or remove accounts.
2. Grant required privileges to the accounts by selecting the account and the check box next to the name of the required privilege. To withdraw the privilege, clear the check box.

   Special features of granting privileges:
   - The **View information** privilege is automatically assigned to all accounts listed under **Users and Groups**.
   - The **Edit object hierarchy and parameters** privilege cannot be assigned to added accounts.
   - To edit the settings in the **Policies** section, the user should be granted **Editpolicies** and **Edit object hierarchy and parameters**. In this regard, these settings can only be modified by users from the group of security domain administrators.
3. Click **Apply** at the bottom of the **Settings** tab.

Alert filtering settings

In the **Filter of Alerts from Subordinate Servers** group, you can manage alert filtering to limit incoming notifications from protected computers of the following subordination levels (subordinate Security Servers). This group is available when selecting the Security Server.

Use the filter to reduce network traffic and only allow notifications about events critical for the administrator to be received.

Note. When configuring policy settings (see p. 136), you can configure the Alert **filter** settings in the **Alert notification** group. This setting limits **the** transfer of notifications directly on protected computers. Therefore, alert filtering controls can be used separately for protected computers and servers. This is useful, for example, for configuring different filtering settings for computers subordinated to a lower security server (in the **Policies** section) and a higher security server (in the **Settings** section). In such conditions, computer alert notifications will be filtered on a lower server with criteria different from those used for filtering events from the same computers on a higher server. The number of incoming notifications depends on the server that the connection is established to.

Below, we show how notifications are configured in the **Filter of Alerts from Subordinate Servers** group of the Settings section. Filtering is configured in the same way as in the **Policies** section (**Alert Notification** group).

Filtering is based on a list of rules. In the rules, you specify the conditions for the contents of fields in log entries.

The list of rules can be created as you work in the **Filter of Alerts from Subordinate Servers** group or by using controls in the **Events** panel (see p. 164).

To configure alert filtering:

1. Select the filter operating mode by selecting the respective check box:

- **Do not allow rule-regulated events to pass to the server** — the filter does not let through notifications of alerts that meet the conditions in the filtering rules;
- **Allow only rule-regulated events pass to the server** — the mode, where the filter only lets through notifications about alerts that meet rules in the list.

Attention! To not enable the latter mode when the list of rules is empty. Otherwise, the filter will not let through any alerts. The **Allow only rule-regulated events pass to the server** mode is recommended when incoming notifications of certain events should be let through and all others blocked. To do this, create rules to describe such events.

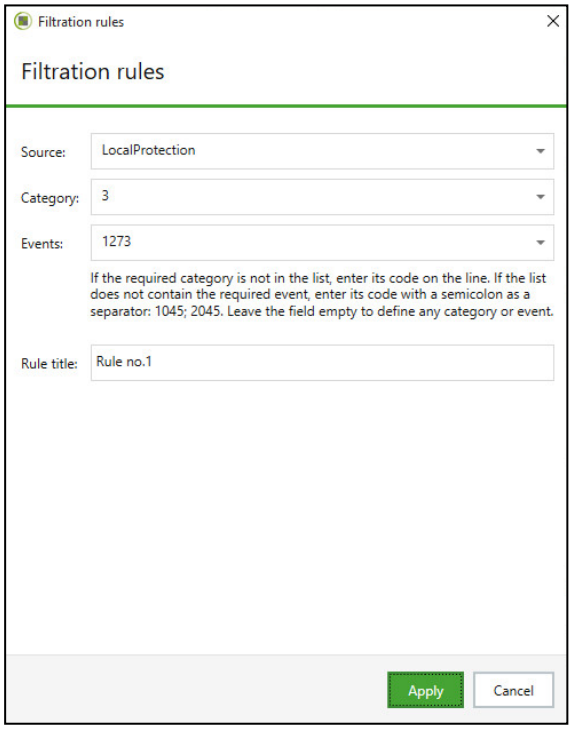
2. Create a list of filtering rules. To work with the list of rules, use the buttons under it.

Button	Description
Edit	Opens a dialog box where you can configure settings of the selected rule (see below)
Add	Adds a new rule to the list. Settings of the new rule are configured in the dialog box (see below)
Remove	Removes the selected element from the list

3. Click **Apply** at the bottom of the **Settings** tab.

Configuring filtration rule settings

The Filtration rules dialog box is shown in the figure below.



To configure filtering rule settings:

1. In the **Rule title** field, edit the name for the element in the list of rules.
2. Configure event analysis settings:

Source
Contains the component or subsystem name specified at event registration as a source. Select the required source
Category

Contains a numeric code of the event category. Select the code of the required category from the drop-down list or enter the value manually. The list of categories available for selection depends on the specified source
Events
Contains numeric identifiers of events. Select identifiers of the required events from the drop-down list or enter the value manually. The list of events available for selection depends on the category specified. Identifiers are delimited by ";"

Note. Details of events can be received when viewing alert log entries on the **General** tab (see p. 176). Sources, category codes and identifiers of events appear, respectively, in the following fields of the tab: **Source**, **Category** and **Events**.

3. Click **Apply** at the bottom of the **Settings** tab.

Tracing settings

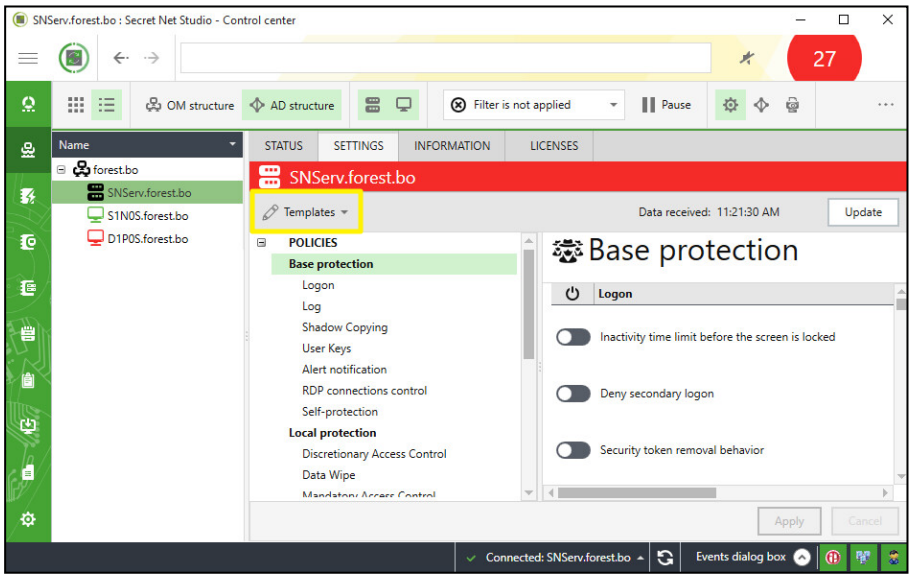
The Control Center makes it possible to centrally enable and configure tracing settings — a service function to gather information about the operation of Secret Net Studio. During tracing, service data about the functioning of program modules is written to special files. This data is required for troubleshooting failure or errors.

Tracing settings appear in the **Tracing Management** group. This group is available when the Security Server or computer is selected. To get information about action required for configuration, contact Technical Support.

Attention! We do not recommend enabling the tracing feature unless it is necessary. To avoid unnecessary load on the computer, this feature should be disabled in the standard operation mode of Secret Net Studio.

Security setting templates

You can find **Templates** menu in the Settings tab of the **Computers** panel like in the figure below.



Note. The Templates menu appears after downloading security parameters of the selected object from the Security Server. To display parameters in the respective field, click **Download settings**.

The Templates menu contains the following:

- **Create using control object parameters** — creation of a template with security parameters for a configured object;
- **Apply** — application of security parameters from existing templates;
- **Compare to** — comparison of object security parameters and template security parameters.

Note. You can apply templates to a similar objects group (clients under the control of the same OS subordinated to the same Security Server; security servers under the control of the same OS in the same security domain).
To apply and compare templates, the user should have permissions to edit policies.
In network mode of the local control center, clients cannot configure and apply network security policies.

Application

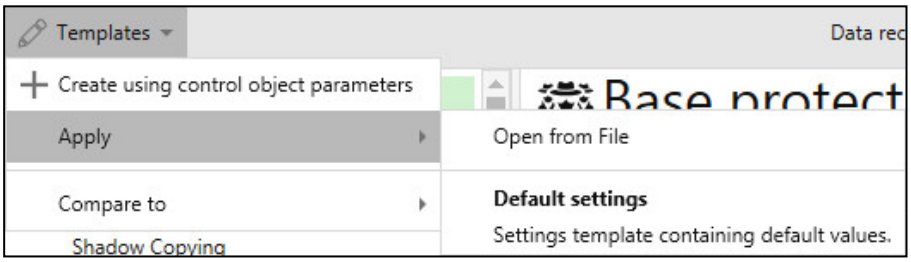
In Secret Net Studio you can apply the following templates:

- security parameter templates configured by default;
- templates created in Secret Net Studio by user.

Note. For computers with Secret Net LSP, you can apply templates created by user only.

To apply a template:

1. Select one or more computers and open their properties.
2. Go to the **Settings** tab and click **Load settings**.
3. Click **Apply** in the **Templates** menu.
   The list of templates appears as in the figure below.

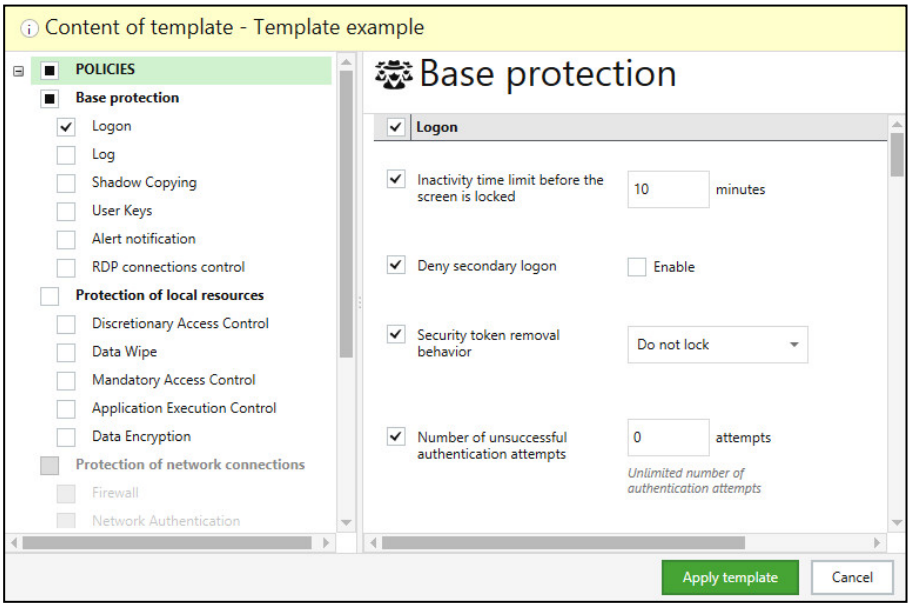


4. In the list, select a template required to apply:
   - **Open from File** — to apply the previously created template;

     Note. After selecting this option a general OS dialog box for opening a file appears. Select a security parameters' template which is to apply and click **Open**.

   - **Default settings** — to apply default security parameters' templates.

   The template content appears as in the figure below.



Tip. To read the help, click ⓘ.

5. Check parameter values to ensure compliance with information security requirements to an information system. Use the title field to select groups of parameters and information field to read parameter values of a selected group.

Comment.
- Parameter group check boxes take a respective form according to the presence/absence in the template:
  - ☐ — absent;
  - ■ — present partly (for the parameters' group only; means the template includes not all the parameters of the group);
  - ☑ — present.
- If you do not want to apply the parameter group or a template parameter, clear the respective check box. In this case, when applying template, group check box does not change its form.

6. Click **Apply template**.

Tip. If you do not want to apply, click **Cancel**.

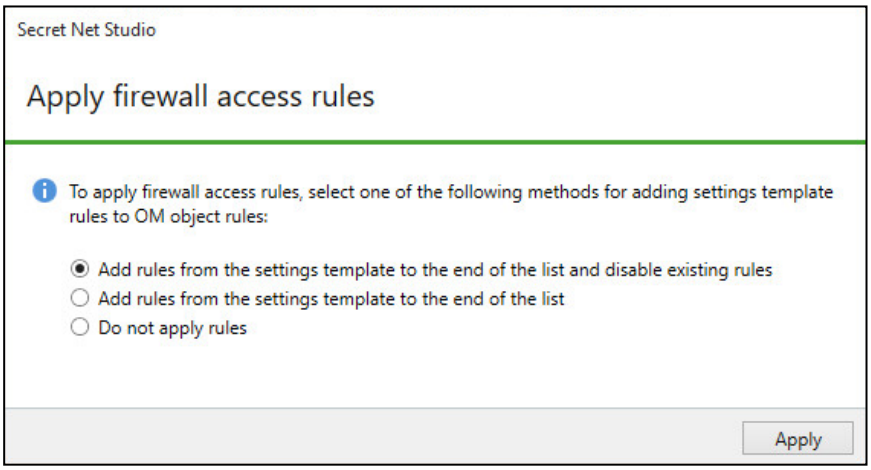
The system requests the confirmation.

7. Click **Yes**.

Tip.
- To cancel, click **No**.
- To return to reading and editing parameters, click **Cancel**.

The following system reaction is possible:

- When applying a template with FW rules to a client or a group of clients, a dialog box appears. In the dialog box you can select the way of applying template FW rules to an object:



  Select a required way to add settings and click **Apply**.

- When applying template to the group of clients with group policies, a dialog box appears. The dialog box informs you about group policies already applied to the client. In this case, when applying the template, the group policies do not change.

8. Wait for the system finishes applying security parameters.

Creation

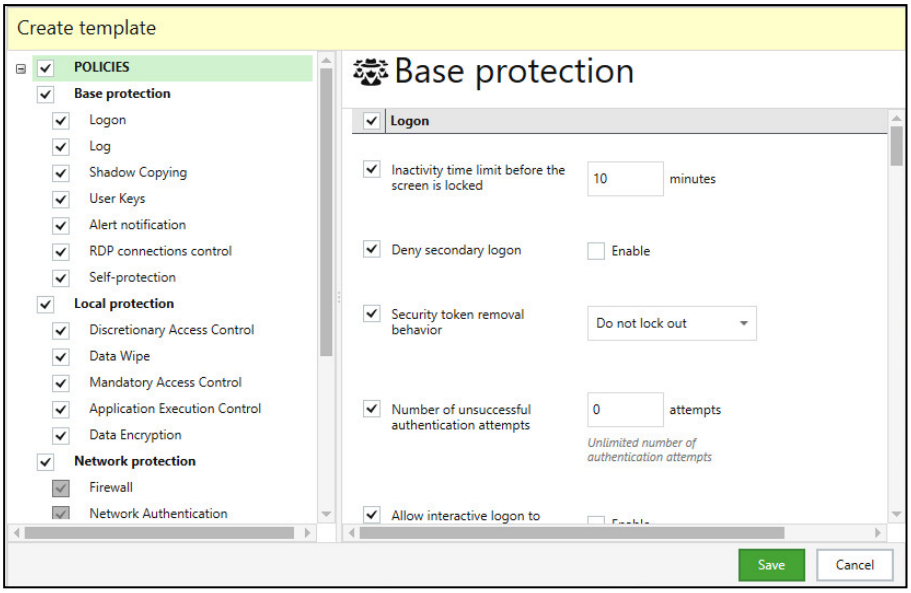
In Secret Net Studio you can save settings of object security parameters to a template for the further application of this template in other computers.

To create template:

1. Select one or more computers and open their properties.
2. Go to the Settings tab and click **Load settings**.

3. In **Templates** menu click **Create using control object parameters**.

   The window changes its view as in a figure below.



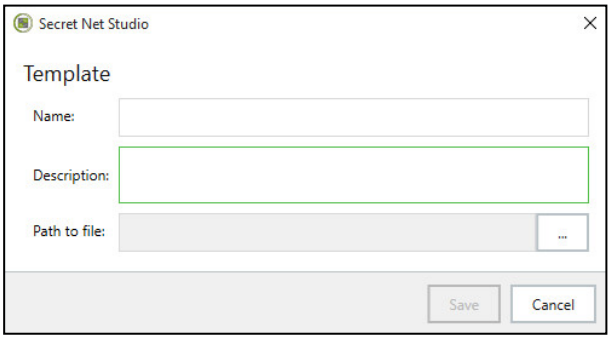
Comment.

- Parameter group check boxes take a respective form according to the presence/absence in the template:
  - — absent;
  - — present partly (for the parameters' group only; means the template includes not all the parameters of the group);
  - — present.
- When creating, a template includes all the parameters.

4. Exclude parameter or group of parameters from the template, clear the respective check box, if it is necessary.

5. Click **Save**.

   The dialog box appears as in the figure below.



6. Enter name, comment and path to file of the template. The template is saved in the selected file.

   Tip. To browse the file, click ... . The OS standard dialog box of file saving appears. Enter name and location of the file and click **Save**.

7. Click **Save**.

   The template saves to the file with .omstemplate extension.

Comparison

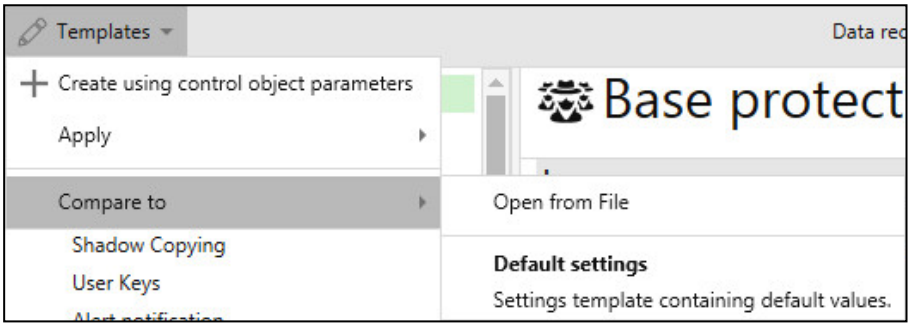
In Secret Net Studio you can compare object security parameters with template security parameters to check the settings compliance to information security requirements.

Note. For computers with Secret Net LSP, you can compare security parameters of templates created by user only.

To compare object security parameters to template security parameters:

1. Select one or more computers and open their properties.
2. Go to the **Settings** tab and click **Load settings**.
3. Click **Compare to** in the **Templates** menu.

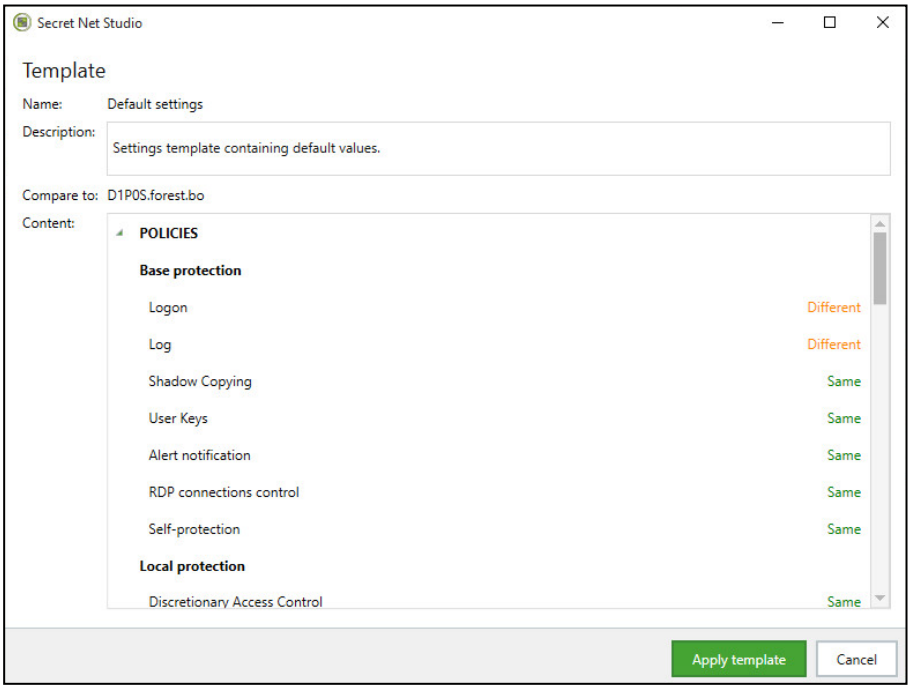
   The list of templates appears as in the figure below.



4. From the list, select the template to compare to object security parameters:
   - **Open from file** — to select previously created template;

     Note. After selecting this option, a general OS dialog box for opening a file appears. Select a template which is to compare to object security parameters and click **Open**.
   - **Default settings** — to select default security parameter templates.

   The dialog box with comparison results appears as in the figure below.



Comment. The following comparison results are possible:

- **Same** — the template parameter matches the object parameter;
- **Different** — the template parameter does not match the object parameter;
- **Missing from template** — the parameter is missing from the template;
- **Not supported** — the parameter is in the template but not supported by the object.

5. Read the comparison results.

Attention! If you applied the template and then compare applied settings to the same template, FW rules may be different (**Policies** → **Network protection** → **Firewall**). Template application do not delete previous FW rules. FW rules should be configured manually to match each other.

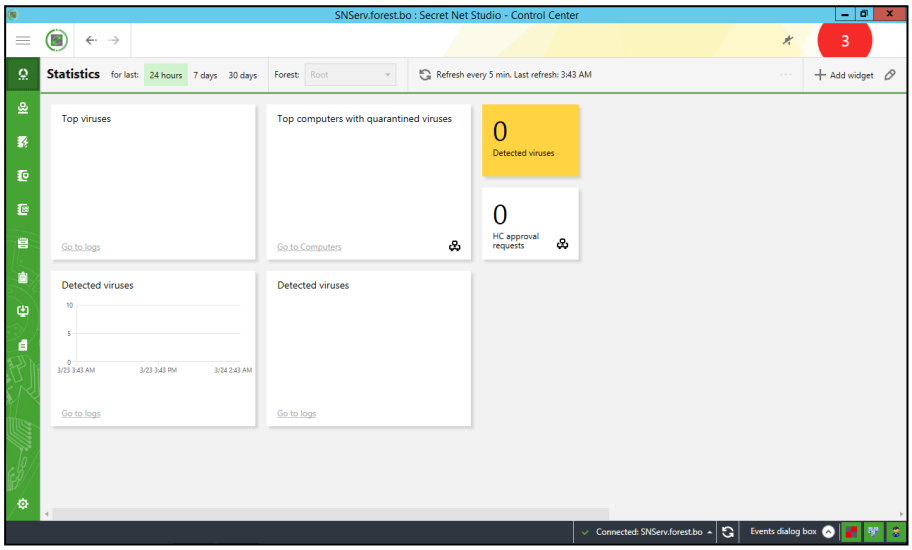
6. Select one of the following actions:
   - to apply the compared security parameters' template, click **Apply template**;
   - to return to editing parameters of the object, click **Cancel**.

Chapter 15
Monitoring and operational management

General status of the system

Overview

To read the system security status overview, click **Dashboard** at the top of the navigation panel. The respective window appears as in the figure below.



The **Dashboard** panel contains widgets. A widget is the graphical element of the program interface that displays a system parameter. The widget panel contains the following:

Element	Description
Name	Widget name
Show	May contain the following: • **Counter** – the relevant number of events. The number is a hyperlink to the log containing the information of the respective events; • **Histogram** – a graph with the number of system parameter events placed according to a time scale. The column of the graph is a hyperlink to the log containing information of the event; • **List** – the list of protected computer names. The name is a hyperlink to the protected computer information
Background	Color of the widget
Go to logs	Hyperlink to all the logged events related to the system parameter and all the subordinated objects

Widgets containing this icon show the information about all the computers subordinated to the Security Server including its subordinated servers.

By default the **Dashboard** panel contains fixed number of configured widgets. The list of widgets:

Name	Background	Contents
High-level alerts	Maroon	Counter, histogram, list
Elevated-level alerts	Red	Counter, histogram, list
Low-level alerts	Orange	Counter, histogram, list

Name	Background	Contents
HC approval requests	Blue	Counter
License errors	White	Counter
FC errors	Red	Counter
Locked out computers	Red	Counter
Most infected computers	White	Counter, list
Computers with integrity violations	White	Counter, list

The full list of widgets with their description:

Name	Description	Contents
Base protection		
Top denied-access computers	Computers with the largest number of registered **Logon denied**-type events	List
Top denied-access users	Users with the largest number of registered **Logon denied**-type events	List
High-level alerts	Number of unacknowledged high-level alerts	Counter, histogram, list
Elevated-level alerts	Number of unacknowledged elevated-level alerts	Counter, histogram, list
Low-level alerts	Number of unacknowledged low-level alerts	Counter, histogram, list
FC errors	Number of computers with functional check errors	Counter
HC approval requests	Number of computers with requests to approve hardware configuration	Counter
Locked out computers	Number of computers locked by the security system	Counter
Top computers with integrity violation	Computers with the largest number of registered **Integrity violation during task processing**-type events	Counter, histogram, list
Local protection		
Top computers with denied device connection	Computers with the largest number of registered **Device connection denied**-type events	Counter, histogram, list
Top computers denied to print	Computers with the largest number of registered printing denial events	Counter, histogram, list
Top users denied to print	Users with the largest number of registered printing denial events	Counter, histogram, list
Top computers with network attacks	Computers with the largest number of registered **IDS signature detected**-type events	Counter, histogram, list
Top attacking nodes	List of the most encountered attacking nodes in registered **IDS signature detected**-type events	List
Top infected computers	Computers with the largest number of registered **Virus detected**-type events	Counter, histogram, list

Name	Description	Contents
Top viruses	List of the most encountered viruses in registered **Virus detected**-type events	List
Top computers with quarantined viruses	List of computers with highlighted number of quarantined viruses	List
Additional widgets		
Free space in database	Percentage of free space in the DB of the connected server. Information about MS SQL Server (full version) only shows the free space in DB file regardless of dynamic memory management	Counter
Full logs	Number of computers with registered **Log is full**-type events	Counter
License errors	Number of computers with license policy violation or expired licenses	Counter

Note.
When adding a new widget to the **Dashboard** panel, the default widget background is white.

Editing widget parameters

You can edit the following widget parameters:

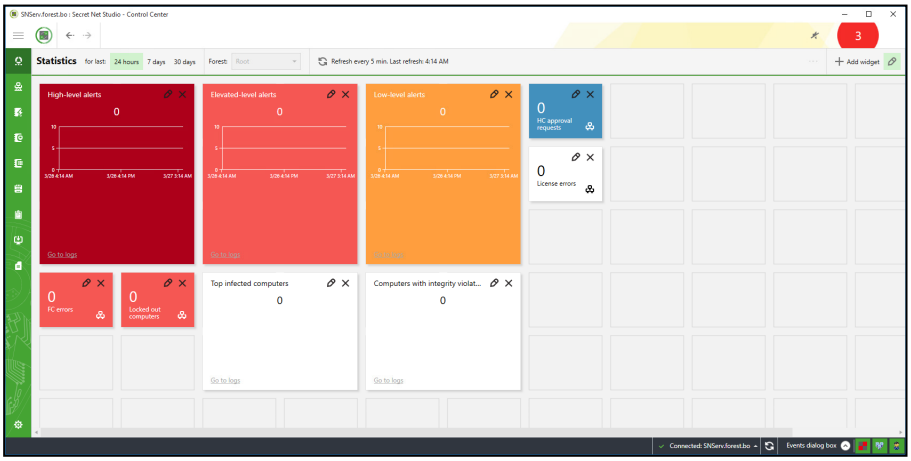
- **name**;
- **show**;
- **background**.

Widget editing is performed in a respective dialog box.

To edit a widget:

1. Click **Edit** widgets at the top right corner of the navigation panel.

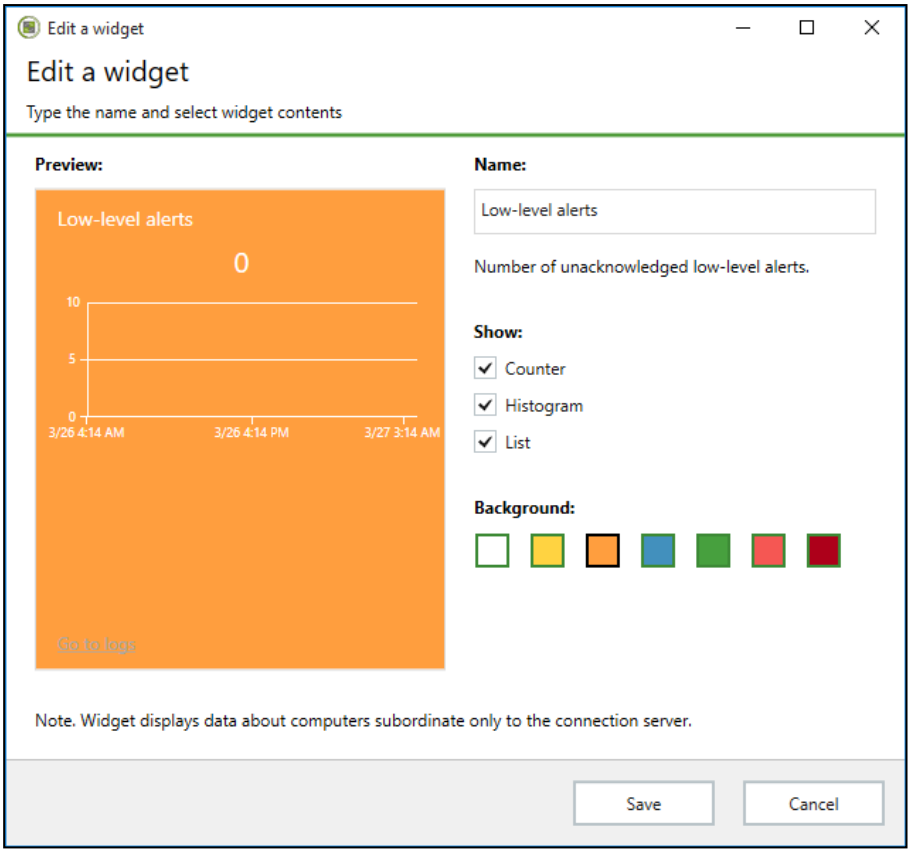
   Edit and **Delete** icons appear on all the widgets on the **Dashboard** panel. The **Edit widgets** icon turns green and free widget cells appear as in the figure below.



Tip. To delete a widget from the **Dashboard** panel, click the **Delete** button on the widget.

2. Click **Edit** on the appropriate widget.

   The dialog box appears as in the figure below.



3. Edit the widget parameters and click **Save**:
   - In the **Name** text box, enter the widget name.
   - In the **Show** group box, select the additional parameters to be displayed.
   - In the **Background** group box, select the widget panel color.
4. At the top right corner of the navigation panel, click **Edit widgets** again.

   Active **Edit** and **Delete** buttons disappear from all the widgets of the **Dashboard** panel. The **Edit widgets** button changes its color and free cells for widgets disappear.

Adding and deleting widgets

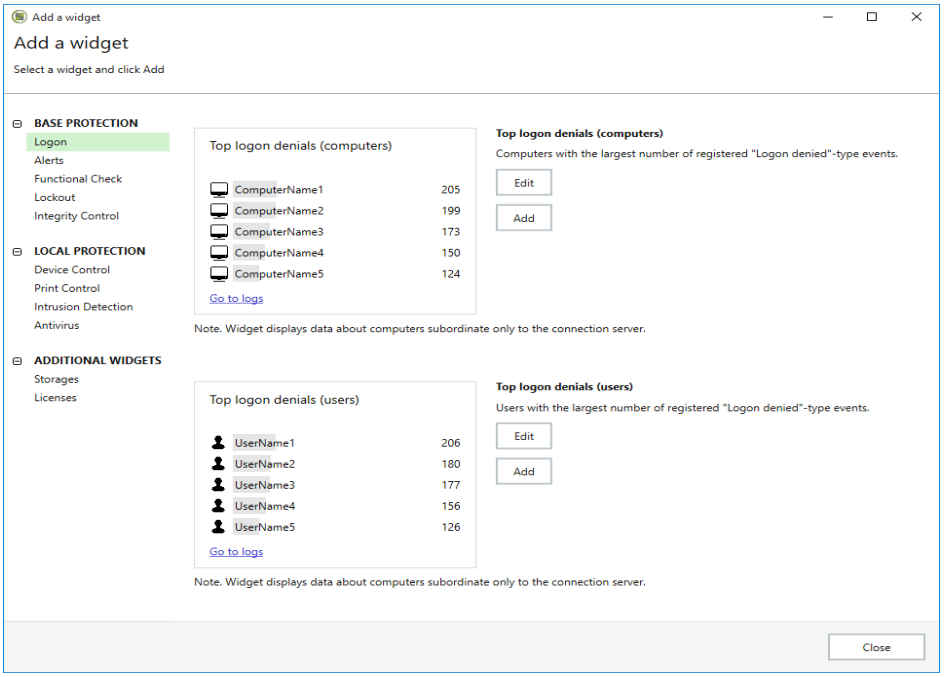
You can add and delete widgets on the **Dashboard** panel.

Adding widgets

To add a widget:

1. At the top right corner of the navigation panel, click **Add widget**.

   The **Add a widget** dialog box appears.



2. Select the required widget from the list and click **Add**.

   The selected widget appears on the **Dashboard** panel.

   Tip. To edit the available parameters of the selected widget, click **Edit**. The editing procedure is described below.

3. Click **Close**.

Deleting widgets

To delete a widget:

1. In the top-right corner of the **Dashboard** panel click **Edit widgets**.

   Edit and **Delete** buttons appear on all the widgets on the **Dashboard** panel. The **Edit widgets** button turns green and free widget cells appear.

2. To delete the required widget, click the **Delete** button in the top-right corner of the widget cell.

   The widget is deleted from the **Dashboard** panel.

3. At the top of the navigation panel, click **Edit widgets** again.

Moving widgets

You can move widgets on the **Dashboard** panel.

To move a widget:

1. Click **Edit widgets** at the top right corner of the **Dashboard** panel.

   Edit and **Delete** buttons appear on all the widgets on the **Dashboard** panel. The **Edit widgets** button turns green and free widget cells appear.

2. Drag the widget using the left mouse button.

   The widget moves to the free cell of the **Dashboard** panel.

3. Click **Edit widgets** once again.

Configuring time parameters for displaying data

The parameters include the period of data displaying and the period of refreshing the displayed data.

Data displaying period

You can select the data displaying period on the navigation panel. There are three time parameters:

- **24 hours**;
- **7 days**;
- **30 days**.

To configure the data displaying period:

- At the top of the navigation panel, select the data displaying period for the widget panel histograms.

  Data displaying periods change according to the selected time parameter.

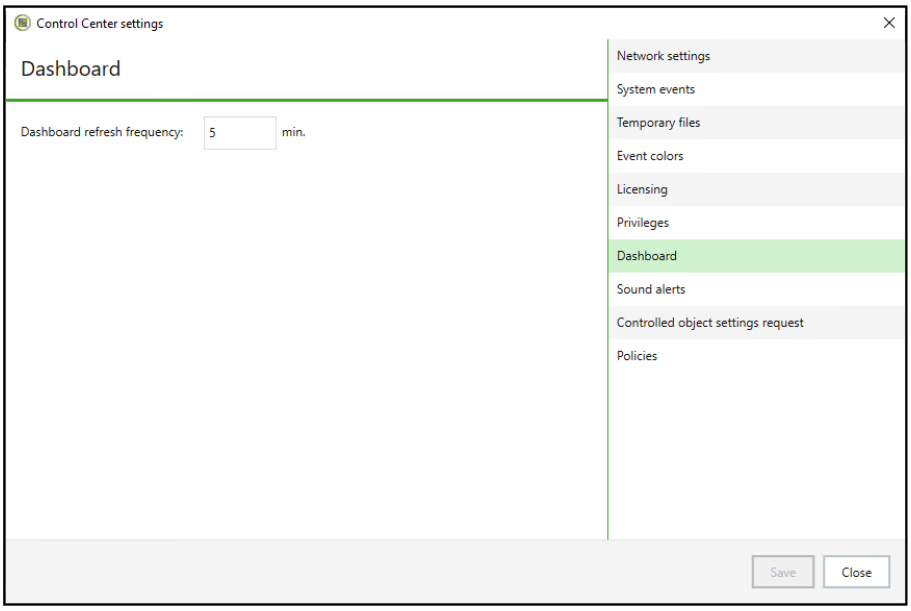
Data refreshing period

The frequency of data refreshing is displayed on the navigation panel. There are two types of data refreshing:

- **manual refreshing** — when you click the respective button;
- **automatic refreshing** — according to the refresh schedule (can be modified).

To configure the data refreshing period:

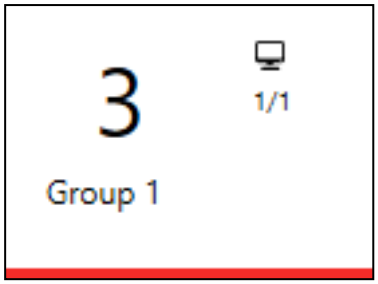
1. Click **Settings** at the bottom of the navigation panel. Then click **Control Center settings**.
2. Click **Dashboard** and configure the **Dashboard refresh frequency** parameter.



3. Click **Save** and close the **Control Center settings** dialog box.

Monitoring groups

A monitoring group contains overview of the system general alert level status. To perform operative monitoring, it is necessary to generate monitoring groups consisting of computers. The monitoring group is the widget on the **Dashboard** panel.



The monitoring group widget contains the following parameters:

- counter — the total number of level alerts of all the monitoring group computers;

  Tip. On mouseover, the data on the number of alerts is displayed according to the alert level. The total number of computers and the number of computers with alerts are displayed.

- name — the monitoring group name;
- the computer icon — indicates the number of computers with alerts and the number of computers in a group.

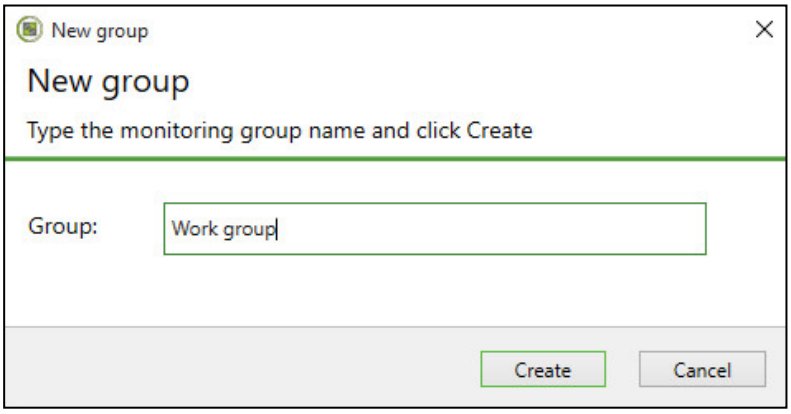
If you right-click such widget you can perform the following actions:

- **Go to computers** — to go the list of computers in the **Computers** panel;
- **Acknowledge** — to acknowledge all the alerts or according to the alert level;
- **Log** — to go to the alert log displaying all the registered alerts or selectively according to the alert level;
- **Delete group** — to delete the monitoring group.

To create a monitoring group:

1. On the **Computers** panel, select the **Diagram** view mode and select the computers to be included to the monitoring group.
2. Right-click a required computer and click **Monitoring > Create**.

   The **New group** dialog box appears as in the figure below.



3. In the **Group** field, enter the monitoring group name and click **Create**.
4. After the monitoring group is created, go to the **Dashboard** panel.

   The created widget appears on the **Dashboard** panel.

To add computers to an existing monitoring group:

1. On the **Computers** panel, select the **Diagram** view mode and select the required computers.
2. Right-click one of the selected computers and click **Monitoring > Add to > *Group name***.

To delete computers from an existing monitoring group:

1. On the **Computers** panel, select the **Diagram** view mode and select the required computers.
2. Right-click one of the selected computers and click **Monitoring > Delete from > *Group name***.

Viewing details

Object labels on the diagram

Elements of the diagram show key details about the state of objects. Details appear as icons and numeric data next to them (for example, the number of alerts on a protected computer or the number of open user sessions).

An example of the diagram with displayed details is shown in the figure on p. **121**.

The Security Server with an established connection is labeled with a special icon.

Numeric data is provided in two or more lines for Security Servers and computer groups: the upper line includes the total number of events/indications on all subordinated computers (for example, the aggregate number of alerts or the number of running computers), while lines under it display the number of computers or subordinated Security Servers with computers. Some numeric data is links that can be used to filter the lists of computers, for example, to display only computers with alert features in the chart.

Additional details of objects are shown in pop-up windows that appear when the cursor is pointed at objects.

The icons are listed in the table below.

Icon	Description
	The computer/s is/are locked. The number corresponds to the number of reasons for locking. In this example, there is one reason
	A virus was detected on the computer(s). The number represents a counter of registered virus detections
	Alerts were registered on the computer(s). The number represents a counter of registered highest alerts. The maximum numeric value of the counter is 999 events. If this is exceeded, the counter shows 99+
	Errors (the icon is red) or warnings (yellow) were detected on the computer (s) during the check of licenses for Secret Net Studio components. The number is an event counter for license errors of enabled subsystems.
	A change in hardware configuration was registered on the computer(s)
	User sessions are open on the computer(s). The number corresponds to the number of open sessions. The color background shows the local administrator session. The question mark shows that user rights are not defined
	An alert filter is active on the computer(s)
	Errors (the icon is red) or warnings (yellow) were detected on computers subordinated to the Security Server during the check of licenses for Secret Net Studio components
	The Security Server database is full

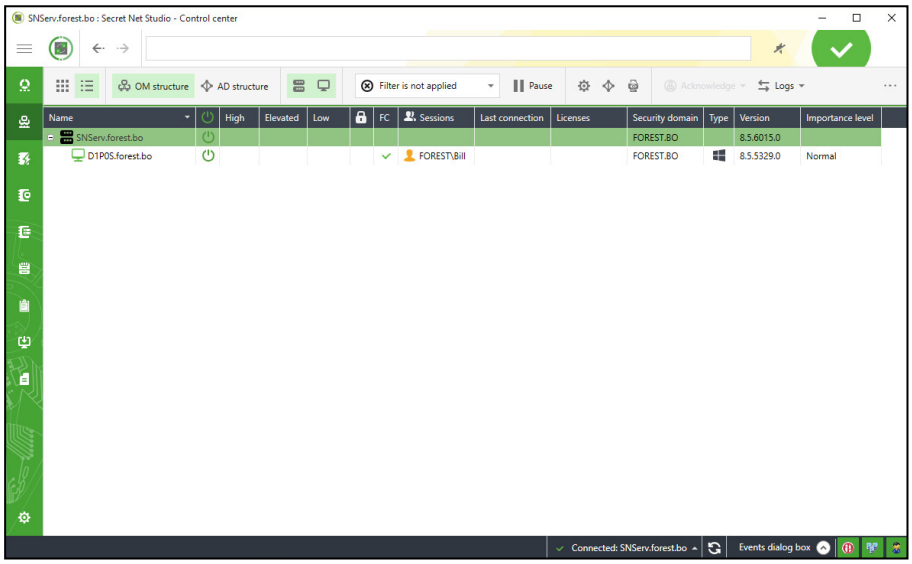
Icon	Description
	The computer's account is disabled

Icons are arranged in order of descending priority of display. Icons with a higher priority appear first in diagram elements. If an element doesn't have enough area allocated for displaying all icons, the least significant ones are excluded.

Details in the hierarchical list of control objects

Details about the state of objects are presented as a table in the **Computers** panel when the list of control objects is displayed. To enable the table display mode in the **Computers** panel, click the **Table** button.

An example of a control objects list is shown in the figure below.



Information about computers and Security Servers is displayed in columns:

Power on icon
Shows the icon if the computer or server is on. Additionally, the name of an enabled computer is highlighted in bold. Its icon turns green if there are no alerts or hardware configuration confirmation requests
High, Elevated, Low
Shows the number of alerts that occurred on the protected computer and are awaiting acknowledgment (confirmation of receipt) by the security administrator. The **High** column indicates the number of critical alerts (with the high level of alert). The other columns indicate the number of less significant alerts (with elevated and low levels of alert). Additionally, in the **Name** column, the computer icon color changes and displays the high-level alert that awaits acknowledgment (confirmation of receipt)
Lockout icon
Shows the enabled lockout icon if the computer is locked out. To get more information about the reason of the lockout, hover the cursor over the cell and information will be displayed in a message box next to the cursor
Functional Check (FC)
Shows an icon that corresponds to the result of functional check. To get more information, hover the cursor over the cell, and information will be displayed in a message box next to the cursor

Sessions
Shows brief information about active sessions or the name of a user who opened session. To get more information, hover the cursor over the cell, and information will be displayed in a message box next to the cursor
Last connection
Shows the time of the last connection to the Security Server for a computer that is off
Licenses
Shows icons if errors (red icon) or warnings (yellow) were detected during the check of licenses for Secret Net Studio components. The number of errors or warnings is shown next to the icon.
Security domain
Shows the name of the security domain that the object belongs to
Type
Shows the icon of the OS installed on the computer
Version
Shows the version number of the installed Secret Net Studio software (the Security Server or the Client)
Importance level
Shows the general importance level of the computer

Managing the display of control object list information

You can sort the information about the state of control objects by table column contents. You can sort in the standard way by using the column headings.

If necessary, you can also change the composition of displayed columns and their order. To configure the columns, call up the context menu in the header row, then click **Column settings** and use the dialog box to generate the list of displayed columns.

Printing and exporting information about computers

The program makes it possible to send for printing and/or save (export) information about computers displayed in the objects list.

The information is exported in RTF format. To load the contents of RTF files, use applications that support these files, such as, Microsoft Word.

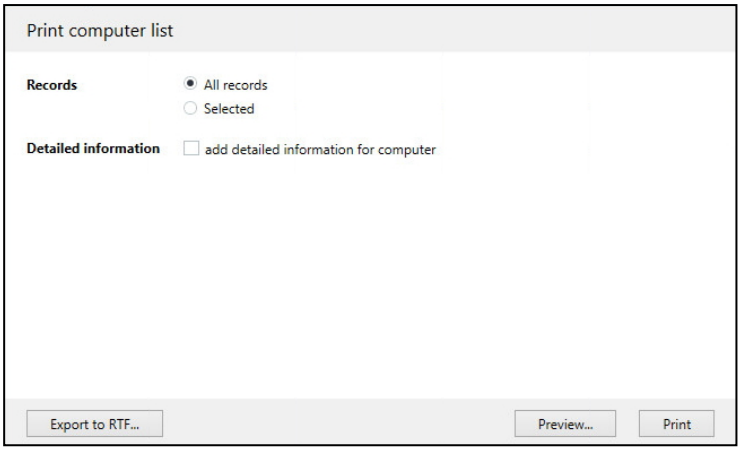
Attention! We do not recommend loading the file into Windows WordPad editor, because this editor may distort the formatting. If you do not have Microsoft Word, you can use Word Viewer to view and print RTF files. This application is free and available for download on the Microsoft web site.

To print or export information:

1. Prepare a table with an object list for data output: Configure the display of information (if necessary) and do not disable the display of servers and computers in the table.
2. If you want to print or save information about specific computers included in the table, select the required computers in the table.

3. At the top of the Computers panel, click Print.

   The settings panel appears as in the figure below.



4. Configure the information output settings.

Records group of fields
This specifies which records will be printed or saved: • **All records** — the operation is performed for all computers in the list; • **Selected** — the operation is only performed for those computers that are selected in the table
Detailed information field
If the check box is selected, Secret Net Studio will additionally provide the information that is not explicitly indicated in the table (for example, the reason for locking) to computers

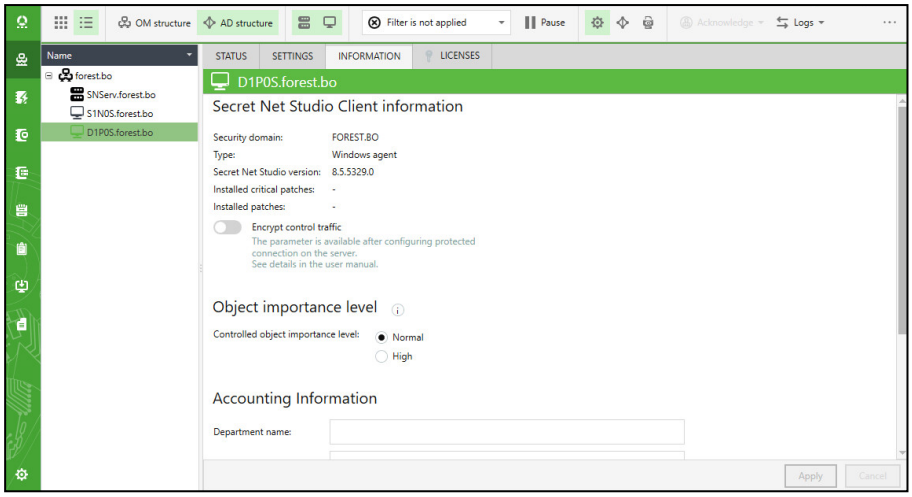
5. To open the preview page, click **Preview...** at the bottom of the **Print computer list** panel.

Note. The preview window makes it possible to send a document for printing by using the standard button on the toolbar.

6. Click the respective button at the bottom of the panel:
   - To start printing, click **Print** and specify the general printing options (selected printer, number of copies, etc.) in the Windows configuration dialog box.
   - To save the information in a file, click **Export to RTF...** and specify the file in the Windows file saving dialog box.

Information about the state of objects

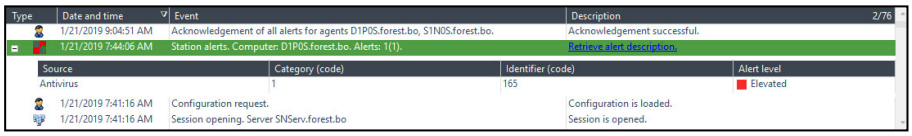
Information about the state of objects is displayed in the **Computers** panel on the Information tab. When information display is enabled, the **Computers** panel looks like in the figure below.



Key information about the object and the security domain that it belongs to is in the **Information** tab. Control tools for the object are available in the **Status** tab.

Details in the system events panel

The system events panel can be used to receive details of changes in the state of protected computers. An example of panel is shown in the figure below.



Details of the following types can be displayed in the system events panel:

- **Network events** are notifications about changes in the state of monitored objects, their configuration and connection with the Security Server (for example, ***<computer_name>* is locked**, **Connection with the server lost...**, etc.);
- **User actions** are notifications about users actions (for example, **Alert acknowledgment for agents...**, etc.);
- **Alerts** are notifications of alert registration on protected computers (for example, **Stationalerts**).

If no colors are customized for notifications, details received during the current session with the program are shown on a white background. Details of other sessions are on a gray background.

You can change the data display settings in the event panel (see p. **117**).

Viewing detailed information about events

The system events panel can display detailed information about events, for example, in notifications about events such as changes in the device control policy or alerts. Detailed information is displayed as a table block. To display it, click the button for expanding the hierarchy in the left part of the line.

The table block of the notification on changes in policies includes lists of policies and their modified values. Key details received in notifications are shown for alerts. To load all alert details in the block, click the **Get Alert Description** link, and details will be loaded to the block as log entries with a description of events. When viewing entries, you can use the same display configuration options as in the main table with log entries (sorting, grouping, column selection, etc.).

Additional details of an event can also be displayed. To do this, call the context menu of the event entry and click the **Detailed** command, and a panel with a detailed description opens in the right part of the system events panel. If details of an event include information about any device, this information can be copied to the clipboard so that the device is later added with these settings to the group policy.

To perform this action, run the **Copy Device** command in the context menu of the detailed description panel.

Automatic display of recent details

New notifications about events are put at the end of the list. To make it easier to view up-to-date information, the list has a mode for automatically scrolling to the most recently added element.

To enable this mode, right-click anywhere in the system events panel and click the **Automatic scroll** command.

Exporting details

The program supports saving (exporting) details that are displayed in the system events panel to files. The export is performed to XML files.

To export, run context menu commands, such as **Export...** and **Export All...**. The **Export...** command is used to export individual selected lines of the details table. To export the entire table, right-click anywhere in the system events panel and click the **Export All** command.

Tracking alerts

The Control Center notifies about events requiring the attention of the security administrator (alerts). Such events are registered on protected computers in the Secret Net Studio log or a standard OS security log, and their type is **Audit Failure** or **Errors**.

Alerts vary by the degree of significance of the events themselves and the importance of the object affected by them. Critical events may raise a **high** alert for objects of great importance or an **elevated** alert for objects of usual importance. Less significant events raise an **elevated** or low alert corresponding to the importance of objects.

The Security Server accumulates alert details in a separate log. The alert log is updated from notifications delivered by protected computers to the Security Server.

Notifications about alerts

The Control Center immediately notifies the user about alerts as soon as it receives notifications about their occurrence. A notification involves giving different visual signals. For example, relevant elements of the control chart become highlighted in red. Sound signals can be also be used for notification.

The notification is disabled and the object resumes its usual appearance after alerts are acknowledged.

Statistics of unacknowledged alerts are shown as lists, indicators and event distribution histograms on the **Dashboard** panel.

Attention! Alerts should be acknowledged before the alert log is archived. If entries that were not acknowledged are put in the archive, the value of the alert counter is reduced, and the security administrator can miss information about unauthorized access. In this case, to acknowledge events, the alert log should be restored from the archive to the Security Server database, and then information can be processed in the usual manner.

Alert acknowledgment

The alert acknowledgment is a confirmation that the security administrators received the information and describes the actions taken. Every alert requires an explanation for its occurrence and that urgent action is taken to ensure the security of the information system. After the security administrator has taken note of and analyzed the circumstances for the alert emerged, the acknowledgment procedure is performed to confirm that the information was received.

To acknowledge, the administrator enters a text comment describing the reasons and action taken, and the comment is saved in by Secret Net Studio along with an

indication that the event was acknowledged. Information about the alert itself is not deleted from the log. In the future, the alert log can be used to find out who responded to events that occurred, how, and when. After all events received from the computer are acknowledged, this object returns to its normal display.

Note. In addition to alert acknowledgments, where the security administrator must enter a comment, the program supports resetting event counters (see below). Resetting counters is only intended for situations that involve configuring Secret Net Studio and should not be used in the standard mode of operation.

Alerts are acknowledged when you work with the alert log on the **Alert Logs** panel (see p. **188**).

Resetting alert counters

When notifications of registered alerts are received, event counters and modified object icons are displayed until the values of the counters for these objects are reset to zero.

Counter values are reduced as alerts are acknowledged (see above). If Secret Net Studio operates normally, counters should be reset to zero only through event acknowledgment, because the acknowledgment procedure involves viewing information about events and adding more specific comments by the security administrator.

When configuring Secret Net Studio settings during test operation, you can reset alert counter values to promptly return to the normal display of objects. When counters are reset, Secret Net Studio treats as noted all the alerts that occurred on the protected computer(s) as of the receipt of the command. However, unlike the acknowledgment procedure, the security administrator is not prompted for a more specific comment when counters are reset. Secret Net Studio saves information about how and when values were reset to zero, together with information about alerts.

To reset alert counters:

1. Select the required objects in the diagram or objects list.
2. Right-click one of the selected objects, expand the **Acknowledge** submenu, and click the required command:
   - **All alerts** is used to acknowledge all events regardless of alert levels;
   - **High alerts** is only used to acknowledge **high** level alerts;
   - **Elevated alerts** is only used to acknowledge **elevated** level alerts;
   - **Low alerts** is only used to acknowledge **low** level alerts.
3. Confirm the operation.

   Objects return to their normal display. A notification about the outcomes of the performed action appears in the system events panel.

Creating filtration rules based on alert notifications

To selectively track events, you can configure a filter to determine alert notifications that should be delivered to the Security Server. The alerts filter runs independently from the event registration policy in local logs, allowing important changes in the system to be controlled without reducing the scope of information stored in local logs. The filter can be applied when transferring notifications from protected computers to the Security Server (configured in the **Alert Notifications** group of the **Policies** section of the object properties panel) and when transferring notifications received by subordinated Security Servers (configured in the **Settings** section).

Filtration rules are automatically added to newly created rules on the basis of selected details. Rule creation in the event panel is designed for alert notifications received during the current session of working with the program.

To add a rule in the system event panel:

1. In the system event panel, go to the alert notification and expand the block with detailed information about events. To do this, hover the cursor over the notification line and double left-click or click the button to expand the hierarchy in the left part of the line.

   Note. For a description of the system event panel and features for controlling information display, see p. 162.

2. In the block with detailed information, call up the context menu and expand the **Add event filtration rule** submenu.
3. Click the command to add the rule to the required filter. The alert filter can be set up in group policies (if policies are not read-only) or in the Security Server settings.

   After the command is run in the **Computer** panel, the respective group of settings opens, and the new rule appears in the list of rules. If the rule to be added can affect the application of preexisting settings, you will be prompted to confirm the action before it is added. In this case, you should check the settings you made before continuing the operation.

Operational Management

Commands are used to carry out operational management of protected computers. Operational management commands can apply to computers of the connection server itself (the Security Server that the program is connected to) and subordinated servers. In this case, the computer selected for management should be running.

Note. If any operational command cannot be currently run, it is either missing in the menu or inactive.

Managing user sessions

You may view information about current user sessions, as well as terminate selected sessions on running computers.

To terminate user sessions:

1. On the diagram or on the object list, select the required computer.
2. Right-click the selected computer and click **Properties**. On the properties panel, click the **Status** tab and click the **Logon** tile.

   The information about this computer and user session list appears.
3. Select user sessions to terminate. To select multiple sessions, use **Shift** or **Ctrl**. Click **Terminate session**.

Locking and unlocking computers

Computers can be remotely locked or unlocked. Commands apply to individual computers, the Security Servers and groups of computers. If the Security Server or group is selected, local logs are collected from all computers subordinated to the Security Server or included in the group.

When the command to lock is received, a message appears, and the current users session is interrupted. At the same time, the event **Workstation is locked by the security system**, which is an alert, is registered in the Secret Net Studio log. Only a member of the local group of administrators can unlock the computer.

If the computer is locked by Secret Net Studio, icons of affected objects in the Control Center appear modified (see p. 158). The unlock command can be applied to this computer. When the command to unlock is received, a message appears, and the user can resume their work.

To lock computers:

1. On the diagram or in the object list, select the required object (computer, group, the Security Server) or select multiple objects.
2. Right-click the selected object (one of the selected objects), point to the **Commands** submenu and click **Lock**. When you are prompted to continue, confirm the operation.

To unlock computers:

1. On the diagram or in the object list, select the required object (computer, group, the Security Server) or select multiple objects.
2. Right-click the selected object (one of the selected objects), point to the **Commands** submenu and click **Unlock**. When you are prompted to continue, confirm the operation.

Note. You can also lock/unlock a computer in its properties, on the Status tab. Select the **Lockout** tile and click either **Lock** or **Unlock** depending on the current state.

Restarting and shutting down computers

You can remotely initiate the restart or shutdown of running computers. Commands apply to individual computers, Security Servers and groups of computers. If the Security Server or group is selected, the corresponding action (restart or shut down) will be performed for all computers subordinated to that server.

The computer is restarted or shut down regardless of the number of open applications and unsaved documents. When the command is received, a message appears, and the computer user can save open documents during 15 seconds after the message appears.

To restart or shut down computers:

1. On the diagram or in the object list, select the required object (computer, group, Security Server) or select multiple objects.
2. Right-click one of the selected objects, point to the **Commands** submenu, and click the **Restart** or **Shut Down** command to restart or shut down the computer. When you are prompted to continue, confirm the operation.

Updating group policies on computers

An update of group policies can be initiated remotely for running computers. The command applies to individual computers, Security Servers, and groups of computers. If the Security Server or group is selected, group policies are updated on all Windows OS computers subordinated to the Security Server or included in the group.

A forced update accelerates the application of centrally imposed group policies on computers.

To update group policies on computers:

1. On the diagram or in the object list, select the required object (computer, group, the Security Server) or select multiple objects.
2. Right-click the selected object (one of the selected objects), point to the **Commands** submenu and click **Apply Group Policies**.

Approving changes to hardware configuration

Changes to hardware configuration can be approved remotely for running computers.

The computer where a change to hardware configuration was recorded is marked on the diagram with a special icon (see p. **158**).

To approve hardware configuration of a computer:

1. Right-click the computer with the modified hardware configuration and click the **Approve Hardware Configuration** command.

   A dialog box appears with a list of devices different from those in the standard hardware configuration of the computer.

2. To register changes in the standard hardware configuration of the computer, click **Approve**.

> **Note.** Hardware configuration can be approved in the following ways:
> - right-click the required computer and click **Properties**, go to the **Status** tab and select the **Device Control** cell, click **Confirm** hardware configuration.
> - on the **Dashboard** panel, right-click the notification about hardware configuration modification and click **Confirm** hardware configuration.

Collecting local logs at the administrators command

Local logs of protected computers are transferred to the Security Server DB regularly in accordance with current settings (see p. 138).

An unscheduled transfer of local logs can be started for running computers. Commands apply to individual computers, Security Servers and groups of computers. If the Security Server or group is selected, local logs are collected from all computers subordinated to the Security Server or included in the group.

To start the transfer of local logs:

1. On the diagram or in the object list, select the required objects.
2. Right-click one of the selected objects and expand the **Collect logs from computer** from the **Logs** submenu.
3. Click the command with the name of the required log or **All** if all local logs need to be transferred to the Security Server DB.

   A notification appears in the system events panel that the collection of local logs has started. Progress status is displayed in the **Description** column.

Controlling the operation of security mechanisms on computers

For running computers, you can use operational configuration features of the operation of security mechanisms.

To configure the operation of security mechanisms on computers:

1. On the diagram or in the object list, select the required objects.
2. Enable the display of object settings (by running the **Properties...** command in the context menu) and go to the **Status** tab (see p. 161).
3. Click the button of the required mechanism (for example, **Data Wipe**).

   A dialog box with information about the mechanism appears at the right side of the button.

4. To enable or disable the security mechanism, move the switch on the left of the dialog box heading to the required position. When you are prompted to continue, confirm the operation.

> **Note.** The security mechanism can be enabled if there is a valid license for the mechanism. The switch is present in the dialog box heading if the license for this mechanism is active. The list of licenses is managed on the **Licenses** tab.

5. If there are additional settings for the mechanism, use controls in the dialog box to perform the required actions.

Starting computer remote control

With the help of PuTTY remote control you can connect Linux OS computers with installed Secret Net LSP and to send control commands through Secure Shell

(SSH). You can enter control commands in the command prompt of the PuTTY window.

To use the program, computers should have the following software components:

- on the administrator workstation — the PuTTY SSH client. If putty.exe is not in the PuTTY control folder, you should specify the path to the file in program parameters;
- on the protected computer — the server for incoming SSH connections. On the computer with Linux OS and installed Secret Net LSP, SSH server components are included by default. On the computer with Windows OS, SSH server is not installed by default. To connect, you should install server software (for example, Bitvise SSH Server).

To start the PuTTY remote control:

1. Right-click the computer with Linux OS and installed Secret Net LSP and select **Enable PuTTY remote control**.

   The dialog box for specifying the login and the password of the user obtaining remote control rights appears.
2. Specify the login and the password of the user (for example, a local computer administrator) and click **Enable**.

   The PuTTY window appears on the screen. After it connects to the computer, the **Command Prompt** appears.
3. Enter the required command. All the actions in PuTTY window are the same to the **Command Prompt** console.

Generating reports

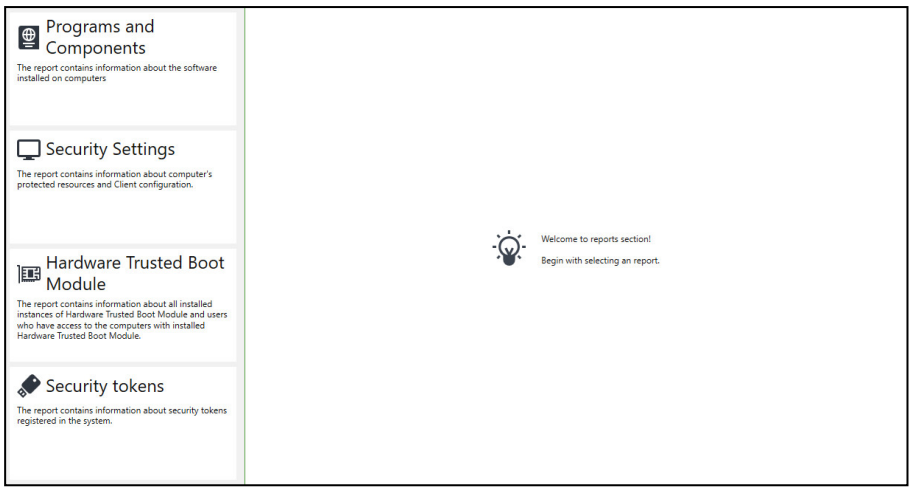
You can generate the following reports via the Control Center:

Name	Description
Programs and Components	Contains information about computers and software installed on them
Security Settings	Contains information about computers and detailed information about settings of the security system installed on them
Hardware Trusted Boot Module	Contains information about installed instances of **Hardware Trusted Boot Module** and a list of users that have access to computers with installed **Hardware Trusted Boot Module**
Security Tokens	Contains information about security tokens registered in Secret Net Studio

Note. Local Control Center allows to generate only **Programs and Components** and **Security Settings** reports.

To generate a report, on the navigation panel, click **Reports**. You can generate reports only for computers with Windows.

By default, the **Reports** panel looks like in the figure below.



You may configure the following report settings: name and logo of the organization as well as page numbering.

Report are saved in RTF format. To view an RTF file, use an application that can work with such files, e.g. Microsoft Word or Word Viewer.

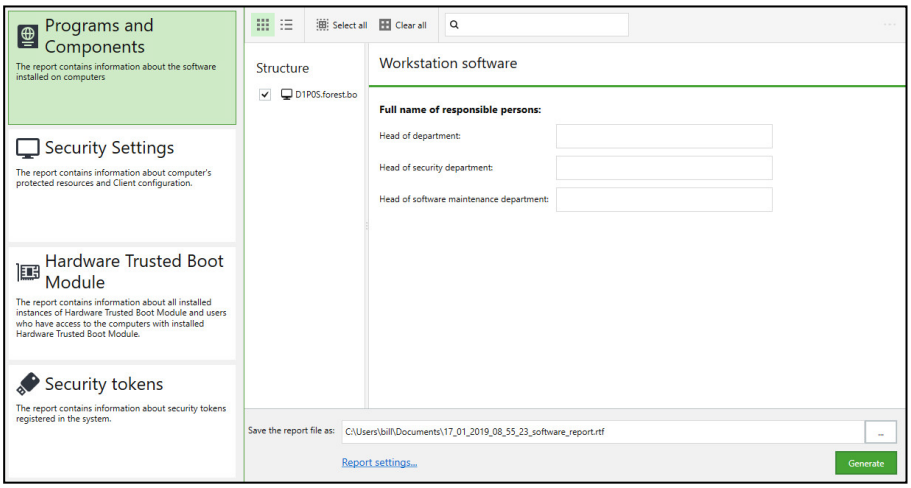
Programs and Components report

Only powered-on computers can be added to the report.

To generate the report:

1. In the **Reports** panel, click **Programs and Components**.

   The panel view changes as in the figure below.



   The **Structure** list contains computers that are available to be added to the report. Only powered-on computers can be added to the report.

   Tip.
   - The list has 2 modes of view: simple list and AD structure. To switch between the modes, click on the respective buttons above the list.
   - You may also filter the list by object names. To filter the list, enter the required name in the search bar.

2. Select the computers to add to the report.

   Tip.
   - To select or clear the selection on all the computers, click the respective button in the toolbar above the list.
   - You may also select computers to add to the report in the **Computers** panel: select the required computers, then right-click one of them and click **Reports** > **Programs and Components.**

3. On the right side of the **Reports** panel, type full names of the employees in charge of operating the selected computers.
4. In the **Save the report file as** field, enter the full name of the report file or click ... to specify the location to save the file.
5. Configure report settings: name and logo of the organization as well as page numbering, if necessary. To configure report settings, click **Report settings**, fill the respective fields and click **OK**.
6. Click **Generate**.

   The Control Center starts to retrieve and process data. When the report is ready, a respective message appears. To view the generated report, click **View**.

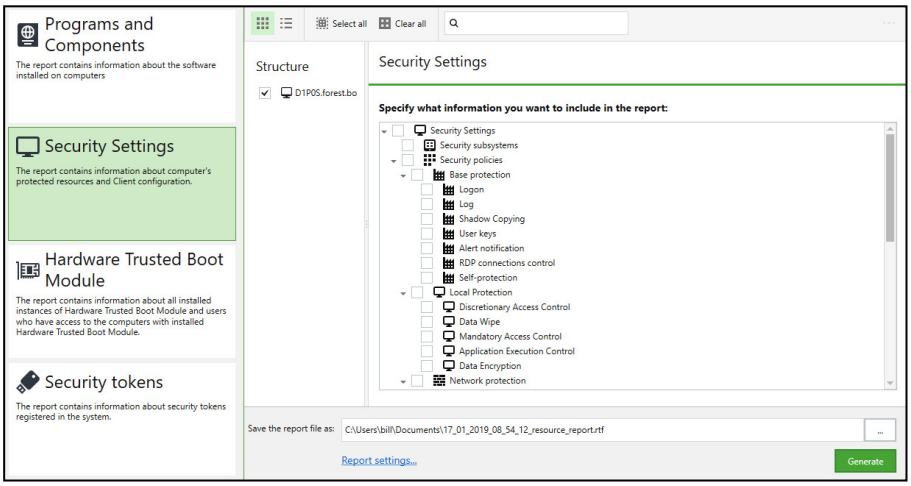
Security Settings report

Only powered-on computers can be added to the report.

To generate the report:

1. In the **Reports** panel, click **Security** Settings.

   The panel view changes as in the figure below.



   The Structure list contains computers that are available to be added to the report. Only powered-on computers can be added to the report.

   Tip.
   - The list has 2 modes of view: simple list and AD structure. To switch between the modes, click on the respective buttons above the list.
   - You may also filter the list by object names. To filter the list, enter the required name in the search bar.

2. Select the computers to add to the report.

   Tip.
   - To select or clear the selection on all the computers, click the respective button in the toolbar above the list.
   - You may also select computers to add to the report in the **Computers** panel: select the required computers, then right-click one of them and click **Reports** > **Programs and Components**.

3. On the right side of the **Reports** panel, type full names of the employees in charge of operating the selected computers.

Name	Description
Security subsystems	This section contains the list of Secret Net Studio security subsystems. Every subsystem is listed with information about its license and status
Security policies	This section contains information about policy configuration. To add specific information to the report, select only the required elements

Name	Description
Event registration	This section contains the list of events and their registration settings
Parameters	This section contains information about network settings and log collecting settings
Local users	This section contains information about local users of the computer
Local user groups	This section contains information about local user groups
Domain users that logged on the computer	This section contains information about domain users that previously logged on to the computer
Integrity Check jobs	This section contains information about **Integrity Check** jobs existing on the computer and their resource groups
Application Execution Control jobs	This section contains information about Application **Execution Control** jobs existing on the computer and their resource groups
Discretionary Access Control	This section contains information about resources controlled by the **DAC** mechanism and their security settings
Mandatory Access Control resources	This section contains the list of confidential resources with their security settings
Encrypted data resources	This section contains the list of encrypted containers existing on the computer with their settings

4. In the **Save the report file as** field, enter the full name of the report file or click ... to specify the location to save the file.
5. Configure report settings: name and logo of the organization as well as page numbering, if necessary. To configure report settings, click **Report settings**, fill the respective fields and click **OK**.
6. Click **Generate**.

   The Control Center starts to retrieve and process data. When the report is ready, a respective message appears. To view the generated report, click **View**.

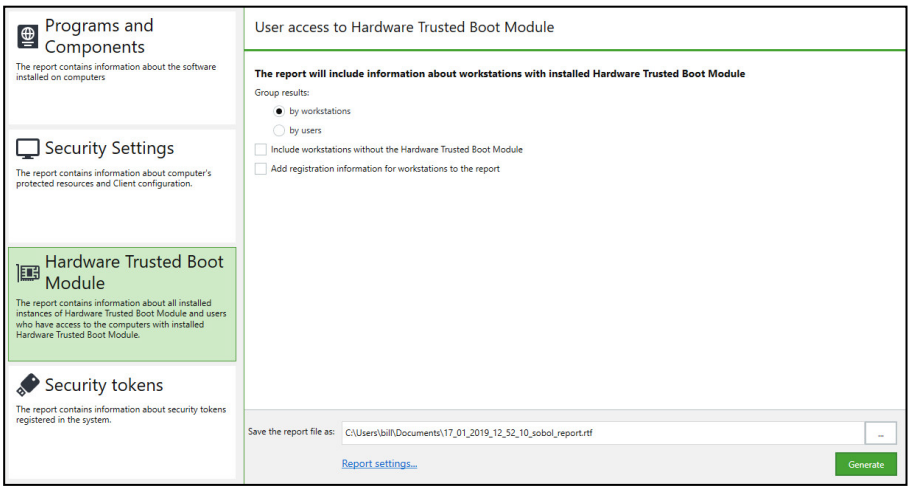
Hardware Trusted Boot Module Report

The report is generated based on the information stored on the Security Server.

To generate the report:

1. In the **Reports** panel, click **Hardware Trusted Boot Module**.

   The panel view changes as in the figure below.



Tip. To generate the **Hardware Trusted Boot Module** report, select the objects to add to the report in the **Computer** panel, then right-click one of them and click **Reports** > **Hardware Trusted Boot Module**.

2. Select an option for grouping results in the report. The information can be grouped by workstations or by users. To select the grouping option, click **by workstations** or **by users**.
3. To add the information about the computers without Hardware Trusted Boot Module, select **Include workstations without the Hardware Trusted Boot Module**.
4. To add account information for each computer (information about the workstation, system unit number, etc.), select **Add registration information for workstations to the report**.
5. In the **Save the report file as** field, enter the full name of the report file or click ... to specify the location to save the file.
6. Configure general report settings: organization name, logo and page numbering options, if necessary. To configure report settings, click **Report settings**, fill the respective fields and click **OK**.
7. Click **Generate**.

   The Control Center starts to retrieve and process data. When the report is ready, a respective message appears. To view the generated report, click **View**.

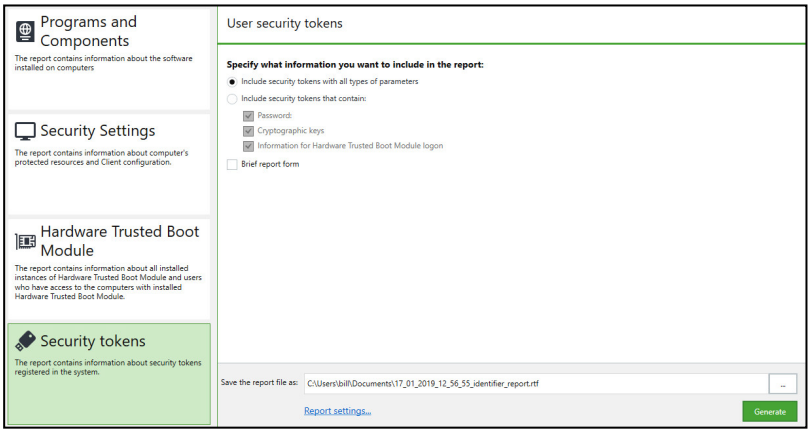
Security tokens report

The report is generated based on the information stored on the Security Server.

To generate the report:

1. In the **Reports** panel, click **Security tokens**.

   The panel view changes as in the figure below.



Tip. To generate the **Security tokens** report, select the objects to add to the report in the **Computer** panel, then right-click one of them and click **Reports** > **Security tokens**.

2. To add the security tokens with all types of parameters to the report, click **Include security tokens with all types of parameters**.
3. To filter security tokens depending on the data contained (passwords, cryptographic keys or information for Hardware Trusted Boot Module logon), click **Include security tokens that contain** and select the required options.
4. By default, the report contains a list of all types of data that can be written on each security token. To add only information about the existing data to the report, select **Brief report form**.
5. In the **Save the report file as** field, enter the full name of the report file or click ... to specify the location to save the file.

6. Configure general report settings: organization name, logo and page numbering options, if necessary. To configure report settings, click **Report settings**, fill the respective fields and click **OK**.
7. Click **Generate**.

   The Control Center starts to retrieve and process data. When the report is ready, a respective message appears. To view the generated report, click **View**.

Chapter 16
Using centralized logs

Centralized logs can be loaded from the Security Server database if the program is connected to the server. Entries can be loaded from files when the program is connected to the Security Server or runs in the on-premises mode.

Centralized logs

The Security Server database accumulates the following logs:

- the alert log that combines all entries for alerts from all controlled computers;
- the event log that combines the Secret Net Studio log and standard Windows OS logs from all controlled computers;
- the Security Server log.

Information from these logs can be imported in full or in part to the Control Center.

Alert log

The alert log is the centralized storage of information about alerts occurring on protected computers. An alert is an event registered locally in the Secret Net Studio log or a standard OS security log, and its type is **Audit Failure** or **Errors**. The alert log is updated from alert notifications delivered to the Security Server.

The security administrator can use details in the alert log to promptly receive the most important information about attempted unauthorized access to the system. Details of an alert are registered in the respective local log and are delivered to the Security Server that saves them to the alert log. As a result, the security system duplicates details of the event to reduce the risk of loss of information.

An alert filter, determining criteria for selective event tracking, may be enabled for computers. If filtering rules are not set, the alert log receives information about every alert on the computer.

Information about events is logged as entries. Each entry includes a set of fields with data from the local log, as well as fields with additional data (type of local log, agent information, threat level, acknowledgment and other parameters).

Combined computer log

The combined computer log (also called the station log) is the centralized storage of the contents of local logs from protected computers. Local logs include the Secret Net Studio log and standard Windows OS logs (applications log, system log and security log). For a description of the use of local logs, see document [**2**].

Local logs are delivered for centralized storage to the Security Server database in accordance with the preconfigured settings (see p. **138**).

Details received from local logs are saved in full in the combined log. Together with these details, the security system records additional information (type of local log, agent information, threat level and other parameters).

Security Server log

The Security Server maintains a log of access sessions to the server opened by the Secret Net Studio components and programs, including internal sessions of the Security Server.

Information about sessions is logged in the form of entries. Each entry includes a set of fields containing the following information:

- General information about the session: computer name, session opening initiators (component and user), time the session was opened and closed;

- Basic information about actions performed during the session: time of each action, result, description of the action;
- Additional information with a detailed description of events (object identifiers, coded designations of results and other parameters).

Storing logs

Logs with event entries can be stored in the following storages:

- local storages on computers where events were registered (local logs);
- the centralized log storage in the Security Server DB;
- archive files created by the Security Server.

Logs stored in the centralized storage or archive files can be viewed in the Control Center. Before the current contents of local logs can be viewed in the program, logs should first be transferred for storage to the Security Server DB.

Local storage of logs

When events are registered, related entries are placed into relevant local logs and stored on the protected computer. As long as entries are kept in the local storage, they can be loaded locally on the computer.

Local logs are stored until transferred to the centralized storage on the Security Server. After entries are transferred, the contents of local logs are cleared.

Attention! When handling local logs, the user with required rights can clear logs before they are transferred to the Security Server. To avoid unauthorized deletion of information, local log control rights should only be granted to trusted users.

Centralized storage

The centralized log storage is kept in the Security Server DB. Details of events registered in the alert log or the Security Server log are received directly by the centralized storage, without being kept intermediately in other storages. The integrated log of computers keeps the contents of local logs as they are transferred from local storages to the Security Server DB. The transfer of local logs from protected computers starts:

- At times specified in the settings for automated log transfer (see p. **138**);
- On the command of the Control Center user (see p. **167**).

Note. Entry transfer to a centralized storage can be disabled for standard Windows OS logs. If centralized collection is disabled for a log, it is ignored during local log requests and its contents remain in the local storage.

Log entries are deleted from the centralized storage as logs are archived.

Entries of logs stored in the Security Server DB can only be viewed and managed in the Control Center.

Log archives created by the Security Server

To reduce the volume of the Security Server database, there is a feature for archiving the contents of centralized logs. This archives all log entries in the Security Server DB from the start of the archiving process (for the Security Server log, it archives details of ended sessions). Entries placed in an archive are removed from the centralized storage.

Archiving starts:

- At times specified in the settings for automated log archiving (see p. **140**);
- On the command of the Control Center user (see p. **192**).

Archived log entries are stored in files. A separate file is created for each archive. By default, the subfolder **\Archive** located in the Security Server setup folder is used for keeping archives.

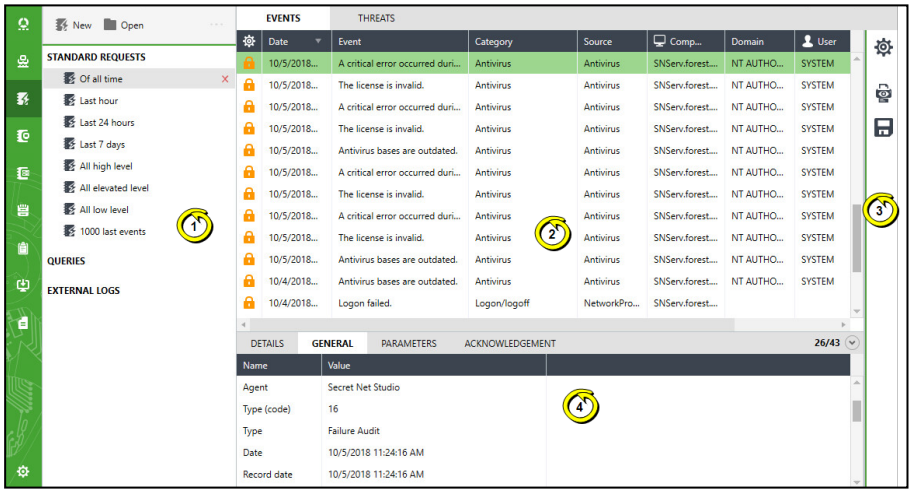
Panels to work with log entries

Entries of centralized logs are displayed in the following panels:

- **Alert logs** panel. To go to the log panel when using the program, click the **Alert Logs** link in the navigation panel or the **Log Received** shortcut in the notification in the log request in the system events panel;
- **Station log** panel. To go to the log panel when using the program, click the **Station Logs** link in the navigation panel or the **Log Received** shortcut in the notification in the event log request in the system events panel;
- **Server log** panel. To go to the log panel when using the program, click the **Server Logs** link in the navigation panel or the **Log Received** shortcut in the notification in the server log request in the system events panel;
- The log archives panel opens by default if the command to start in standalone mode **Logs Archive** is selected, and the archive file is specified for loading in the mode selection dialog box when the Control Center is launched. When working with the program, you can go to the archives panel by clicking on the **Archives** icon in the navigation panel.

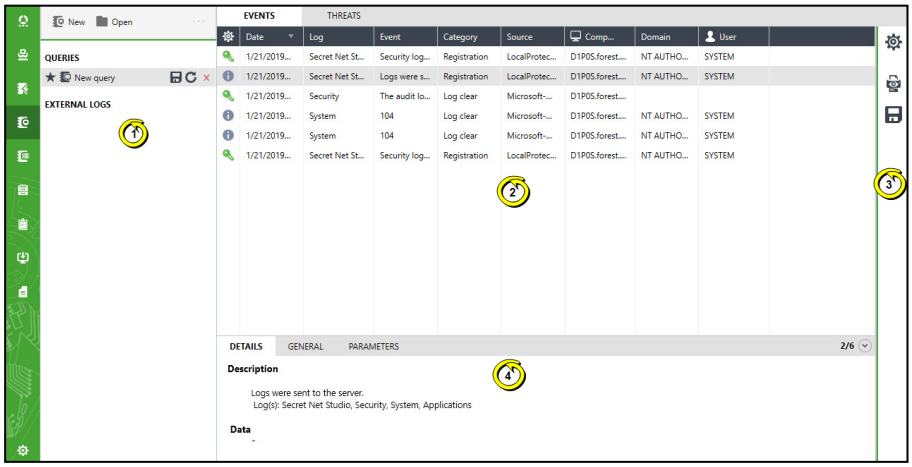
A tab called **request** is created in the panel for loading entries. Several requests at a time can be handled in the panel. To switch between them, select the required request in the request control panel.

The **Alert logs** panel is shown in the figure below.



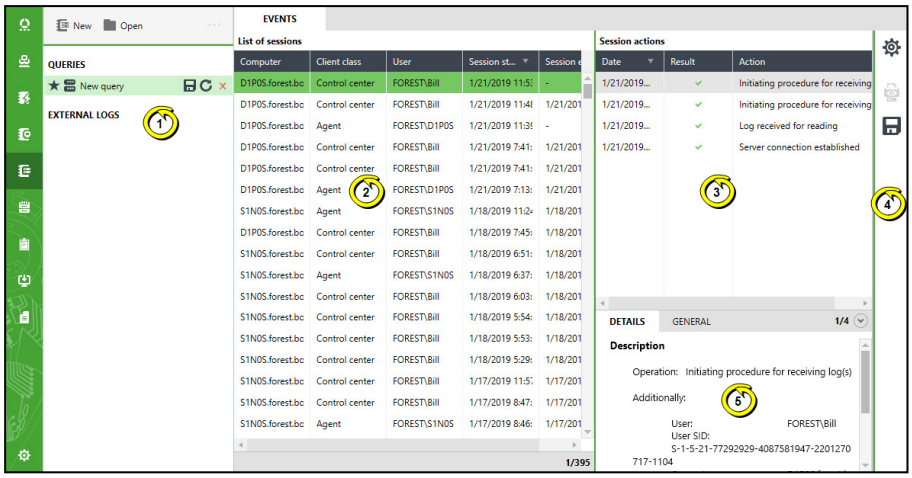
Comment. The figure shows: 1 — the request control panel; 2 — the information pane; 3 — the panel for information display configuration; 4 — the event description pane.

The **Station logs** panel is shown in the figure below.



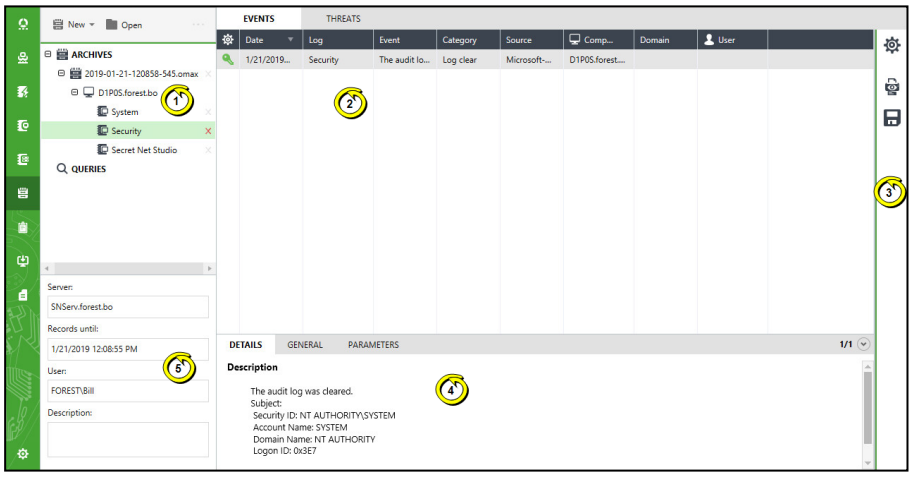
Comment. The figure shows: 1 — the request control panel; 2 — the information pane; 3 — the entry management panel; 4 — the event description pane.

The **Server logs** panel is shown in the figure below.



Comment. The figure shows: 1 — the request control panel; 2 — the session list pane; 3 — the information pane of the selected session; 4 — the panel for information display configuration ; 5 — the event description pane.

The panel of logs archives is shown in the figure below.



Comment. The figure shows: 1 — the request control panel; 2 — the information pane; 3 — the panel for information display configuration; 4 — the event description pane; 5 — the pane with key information about the archive.

Key interface elements:

Request control panel
Contains lists of requests for loading entries. Requests are grouped in the following sections: • **Standard requests** are requests with predefined criteria for picking entries loaded from the log (only for an alert log) • **Requests** are requests created by the user to load entries from a log • **External logs** are requests created as entries when loading from files • **Archives** are requests generated as a result of analysis of the contents of loaded archives
Information pane
Contains information about events in the log in the form of a table with a list of entries
Panel for information display configuration
Contains buttons for calling configuration controls for requests, printing, and entry export

Event description pane
Contains detailed information about the selected event. Information about events is grouped in the following tabs: • **Details** — contains a detailed description and received data. If details of an event include information about any device, this information can be copied to the clipboard so that the device is later added with these settings to the group policy; • **General** — contains the full list of fields and their values in the entry about a registered event. The list is provided as a table; • **Parameters** — contains the list of Secret Net Studio settings received from a detailed description of the event. The list is provided as a table; • **Acknowledgment** — contains details about who and when acknowledgment (confirmation of receipt) was performed for the selected entry and a text comment with a description of actions. The tab shows only for the alert log when an entry with an indication of acknowledgment is selected. To enable or disable the event description pane, click the **Detailed** command in the context menu of the event entry or click the button on the right in the bottom line of the information pane

Loading log entries

Requests for the alert log

The program allows requests for loading alert log entries to be created as follows:

- Creating statistics-based requests
- Context creation of requests for objects
- Creating requests with predefined selection criteria
- Creating requests with arbitrary selection criteria
- Creating requests for loading log entries from files

Creating statistics-based requests

Statistics about alerts are provided on the **Dashboard** panel. The system condition indicator, with the total number of alerts (if there are any unacknowledged events), appears in the top right corner of the main Control Center window.

Alert counters on the **Dashboard** panel and in the system state indicator can be used to create requests for loading alert log entries. To create a new request, select the value of the required counter. A new request where entries will be imported automatically appears in the alert log panel.

Context creation of requests for objects

Requests for loading alert log entries can be created for objects selected in the control chart panel or in the objects list. Rules for selecting and filtering by the context of selected objects and commands are automatically created for such requests.

For context creation of a request:

1. Select the required objects in the control chart or objects list.

   Note. Event counters displayed next to objects notify about registered alerts, if any, waiting for acknowledgment (confirmation of receipt) by the security administrator (see p. 158 and p. 159).

2. Right-click one of selected objects, expand the **Logs/Alert** Log submenu and click the required command:
   - **All alerts** is used to get details of events of all alert levels.
   - **High-level alerts**, **Elevated-level alerts** and **Low-level alerts** are used to get details of only events with the required alert level.

Creating requests with predefined selection criteria

You can use requests with predefined selection criteria to promptly import unacknowledged entries into the program about alerts registered within a specified

period or those with a specific alert level.

Requests with predefined selection criteria are created in the log panel. We recommend you to create such requests when there are unacknowledged alert entries in the system.

To create a request with predefined selection criteria:

- In the Standard Requests section of the request control panel, hover the cursor over the list element that corresponds to the required period or importance of events, and double-click it.

  A new request will be created in the log panel with the corresponding settings, and the export of entries from the log is automatically initiated. After entries are loaded, a notification with a link to the new request appears in the system event panel that the log was received.

Creating requests with arbitrary selection criteria

Requests with arbitrary entry selection criteria are created to subsequently configure settings and start the import of entries manually.

Requests are created in the alert log panel.

To create a request:

1. Click **New** in the request control panel.

   A new request is created in the log panel and a panel appears on the right to configure its settings.
2. Configure settings of the new request (see p. **182**) and click **Query the DB** at the bottom of the settings panel.

   This initiates the import of entries from the log. After entries are loaded, a notification with a link to the new request appears in the system event panel that the log has been received.

Creating requests for loading alert log entries from files

Alert log entries can be stored in special format ***.snua** files. Entries from such files are imported to the alert log panel by creating individual requests for each file.

The file to be loaded can be specified when the program starts in on-premises mode (see p. **115**), or when the program is used in the alert log panel.

To create a request to import entries from the file in the alert log panel:

1. Click **Open** in the request control panel.

   A dialog box appears.
2. Select the required file.

   A new request where entries from the file will be imported is created in the log panel.

Requests for the stations log

The program allows requests for loading stations log entries to be created as follows:

- Context creation of requests for objects
- Creating requests with arbitrary selection criteria
- Creating requests for loading stations log entries or local logs from files

Context creation of requests for objects

Requests for loading stations log entries can be created for objects selected in the control chart panel or in the objects list. Rules for selecting and filtering by the context of selected objects and commands are automatically created for such requests.

For context creation of a request:

1. Select the required objects in the control chart or objects list.

2. Right-click one of the selected objects, expand the **Logs/Computer** Logs from the **DB** submenu and click the command in line with the required entry selection criteria. You can load event entries that have arrived from specific local logs separately or from the Secret Net Studio log together with the security log. The **Create Request** command is used to create a request and then to go to the **Stations** Log panel to configure request settings (see p. 182).

   After the command to load event entries received from specific local logs is run, the import of entries from the stations log is initiated automatically. After entries are loaded, a notification appears in the system event panel that the log has been received. To go to log entries, click the **Log Received** link in the notification.

Creating requests with arbitrary selection criteria

Requests with arbitrary entry selection criteria are created to subsequently configure settings and start the import of entries manually.

Requests for loading stations log entries are created in the **Stations Logs** panel.

To create a request:

1. Click **New** in the request control panel.

   A new request is created in the **Stations Logs** panel, and a panel appears on the right to configure its settings.

2. Configure settings of the new request (see p. 182) and click **Query the DB** at the bottom of request settings panel.

   This initiates the import of entries from the log. After entries are loaded, a notification with a link to the new request appears in the system event panel that the log was received.

Creating requests for loading stations log entries or local logs from files

Stations log entries can be stored in special format *.snlog files. Entries from such files are imported to the Stations Logs panel by creating individual requests for each file.

In addition, individual requests, similar to requests for loading the stations log, can be created for *.evt* files, a standard format of the Windows OS event log.

The file to be loaded can be specified when the program starts in on-premises mode (see p. 115) or when the program is used in the Stations Log panel.

To create a request to import entries from the file in the Station Log panel:

1. Click **Open** in the request control panel.

   A dialog box appears.

2. Select the required file.

   A new request where entries from the file will be imported is created in the **Stations Logs** panel.

Requests for the Security Server log

The program allows requests for loading Security Server log entries to be created as follows:

- Context creation of requests
- Creating requests with arbitrary selection criteria
- Creating requests for loading security server log entries from files.

Context creation of requests

Requests for loading the Security Server log entries can be created when using the control chart panel or the objects list. Rules for selecting and filtering by the context of selected commands can be automatically created for such requests.

For context creation of a request:

1. In the control chart or the objects list, right-click the Security Server whose log needs to be loaded. In the context menu, expand the **Logs/Server** Logs submenu.
2. Select the command that corresponds to the required entry selection criteria. You can load entries about events registered over the past hour, 24 hours, or all entries. The **Create Request** command is used to create a request and then to go to the **Server Logs** panel to configure request settings (see p. **182**).

   The export of entries from the Security Server log is automatically initiated after the command is selected for the loading of entries about events registered over the past hour, 24 hours, or all entries. After entries are loaded, a notification appears in the system event panel that the log was received. To go to log entries, select the **Log Received** link in the notification.

Creating requests with arbitrary selection criteria

Requests with arbitrary entry selection criteria are created to subsequently configure settings and start the import of entries manually.

Requests for loading Security Server log entries are created in the **Server Logs** panel.

To create a general request:

1. Click **New** in the request control panel.

   A new request is created in the Server Logs panel and a panel appears on the right to configure its settings.
2. Configure the settings of the new request (see p. **182**) and click **Query the DB** at the bottom of request settings panel.

   This initiates the import of entries from the log. After entries are loaded, a notification with a link to the new request appears in the system event panel that the log was received.

Creating requests for loading the Security Server log entries from files

The Security Server log entries can be stored in special format *.snsrv files. Entries from such files are imported to the Server Log panel by creating individual requests for each file.

The file to be loaded can be specified when the program starts in the on-premises mode (see p. **115**), or when the program is used in the **Server Logs** panel.

To create a request to import entries from the file in the Server Logs panel:

1. Click **Open** in the request control panel.

   A dialog box appears.
2. Select the required file.

   A new request where entries from the file will be imported is created in the **Server Logs** panel.

Requests for log archives

To view entries from archived logs, load the files of the required archives to the program.

Attention! To load the archives, the disk that will be used for the temporary files must have sufficient free space, (unarchiving is performed in the user's temporary files folder). To load files of up to 80-100 MB, you need about 4 GB of free space. Working with files of 200-300 MB requires at least 10 GB.

After the archives are loaded, create requests for selecting the required entries. Requests are created in the **Archives** panel. The program supports the following methods for creating requests:

- Creating a request for selecting entries in an individual log in a loaded archive
- Creating requests for selecting alert log or stations log entries in loaded archives

Loading archive files

The Security Server creates log archives in special format files *.omax.

Archive files to be loaded can be specified when the program starts in the on-premises mode (see p. 115), or when the program is used in the Archive panel.

Note. The Control Center supports the loading of archive files created by the Secret Net Studio 7.0 Security Server and above.

To load archive files in the Archives panel:

1. Click **Open** in the request control panel.

   A dialog box appears.
2. Select the required files.

   New subsections will be created in the **Archive** panel, and their number and names correspond to selected archive files. Subsections contain hierarchical lists of computers and logs whose entries were received from archives. Key details of loaded archives appear in the information pane under the request control panel.

Creating a request to select entries from an individual log in a loaded archive

In the loaded archive, you can create requests for selecting entries from separate logs included in the archives hierarchical list. Such requests only relate to the selected log of the relevant computer and do not allow other entries stored in the archive to be loaded.

To create a request for selecting entries from a separate log:

1. In the **Archive** section of the request control panel, expand the subsection list with the name of the required archive.
2. Point the cursor at the log line and double-click it.

   A new request showing details from the selected log is created in the **Archives** panel.

Creating a request to select alert log or stations log entries in loaded archives

In loaded archives, you can make a sampling from all entries of alert logs or stations logs stored in archives. The request for selecting entries from these logs is used to receive entries originated by different computers and can apply to several selected archives.

To create a request for selecting alert log or stations log entries:

1. In the request control panel, click **New** and select the required type of request in the menu that opens:
   - **Find in alert logs** creates a request for selecting entries from alert logs.
   - **Find in station logs** creates a request for selecting entries from stations logs.

   A new request is created in the **Archives** panel, and a panel appears on the right to configure its settings.
2. Configure settings of the new request (see p. 182) and click **Find in Archives**.

   This initiates importing entries from the selected archives.

Configuring request settings

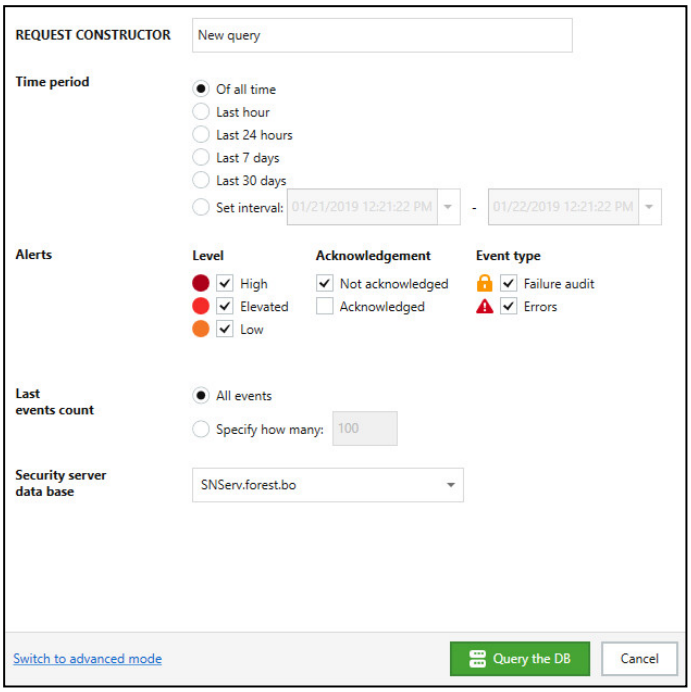
To get required information in a log query, you can modify entry loading and filtration settings. Settings can be configured in a special settings panel.

To configure entry request settings:

1. Enable the display of the request settings panel. To show or hide the panel, click **Query** in the information display configuration panel (on the right of the information pane).

   Note. The panel information display configuration panel is shown by default for a newly created request with arbitrary selection criteria.

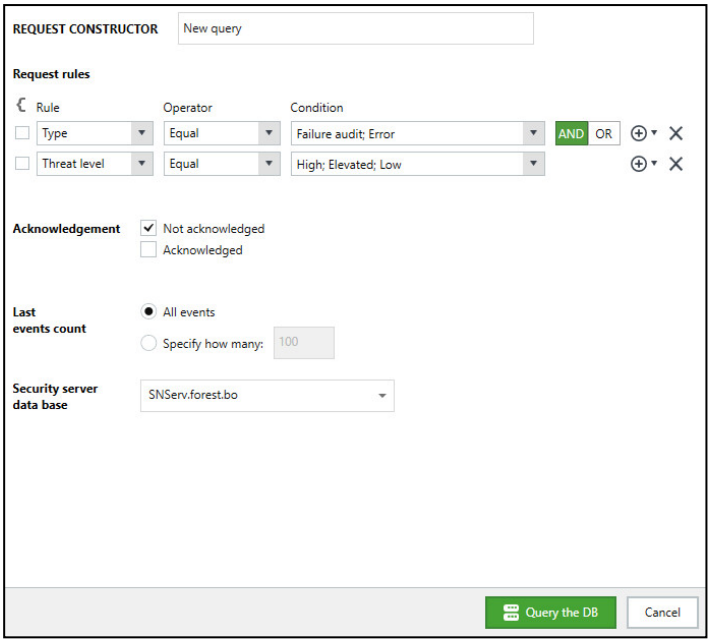
   An example of the contents of the alert log panel is shown in the figure below.



2. Enter the name of the request and configure entry selection settings in the relevant fields. The content of configured settings depends on the source of information, log types and the current settings panel mode.

   For a request created with arbitrary selection criteria, the panel by default is shown in simplified mode where you can specify key entry selection criteria (see the figure above). If you need detailed settings, enable the advanced settings mode by clicking the **Switch to advanced mode** link at the bottom of the panel.

   An example of the contents of the panel in advanced mode is shown in the figure below.



3. To apply new settings, click the respective button at the bottom of the settings panel:
   - To make a new sampling of log entries from the Security Server database, click **Query the DB**.
   - To quit the request settings configuration, click **Cancel**.

Controlling requests

The panes **Alert logs**, **Station logs**, and **Server logs** provide the following request control features (other than for requests with predefined selection criteria and requests for import from files):

- Enabling and disabling the automatic request loading mode;
- Saving request settings to a file;
- Loading request settings from a file;
- Reloading entries from the security server DB.

Use buttons in the request control panel to perform request control operations. Controls are listed in the table below.

Button	Description
	Enables and disables the automatic request loading mode in the next sessions of working with the program. When the mode is enabled, the button is highlighted
	Saves the selected request to a file. Saving is performed to a *.snreq file
	Starts a new loading of entries based on current request settings
Open	Calls up the **Open File** dialog box to load the request. To load a request that was previously saved, specify **Request** (*.snreq) as the file type. When loaded, the request is added to the Requests section of the relevant panel of logs (to the panel of the log for which the request was created)

To close the request, click **Close** to the right of its name.

Entry viewing options

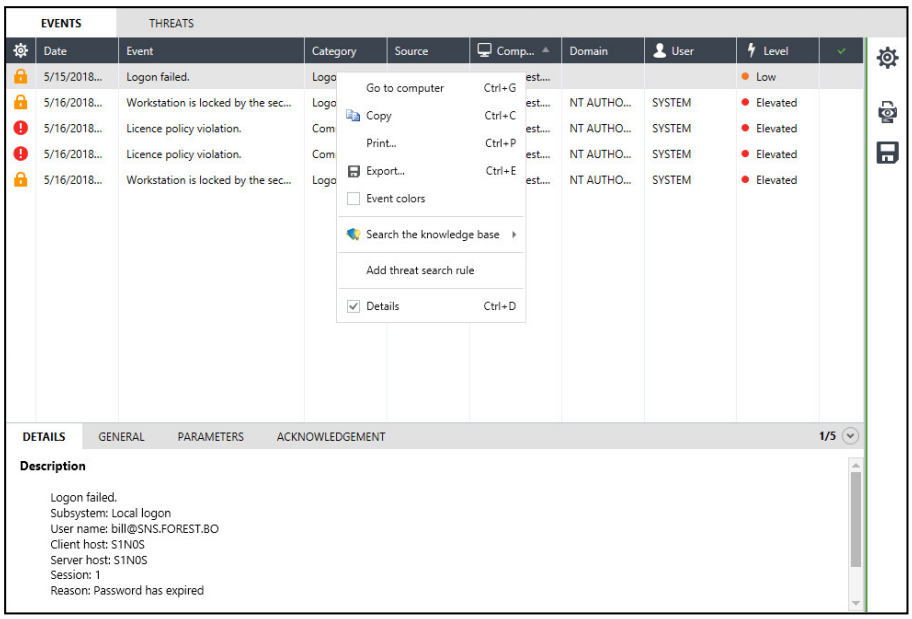
Display event details modes

Loaded information about events is displayed in the information pane of the respective panel (see p. 176). There are different displaying details modes for

analysis of log contents (other than for the Security Server log). Apart from displaying information as a usual list of entries, the program supports viewing information as a list of threat events.

Events mode

The **Events** mode displays the list of loaded log entries in a table format. This is the main and most feature-rich mode for viewing and working with entries. An example of the contents of the window with the entry table is shown in the figure below.

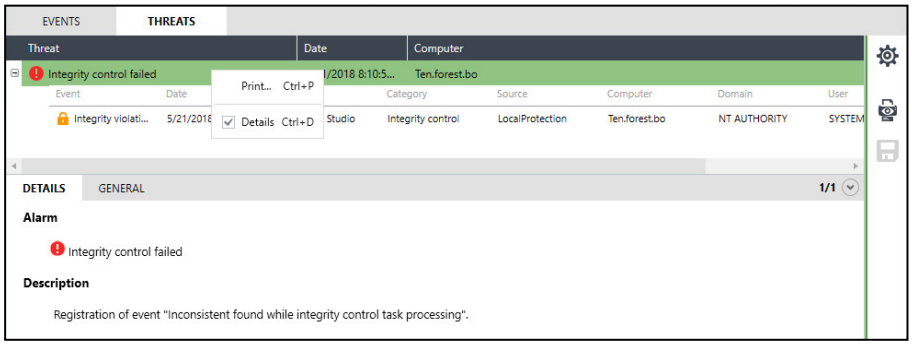


You can use the context menu of entries to perform necessary actions such as copying, printing, saving, etc.

There is an entry counter on the right of the line under the table: <**number of the selected entry**>/<**quantity of selected entries**>/<**total quantity of loaded entries**>.

Threats mode

The **Threats** mode displays a list of threat events generated through analysis of loaded entries. Threat events are compressed or clarifying information about registered events (for example, a threat with indications of password guessing). The mode is designed to provide the administrator or auditor with information most relevant for them from the logs. An example of the contents of the window with the generated list is shown in the figure below.



Information is displayed in a table format where lists of registered events related to threat events can be expanded. When viewing table blocks with log entries, you can use the same display configuration options as in the main table with log entries.

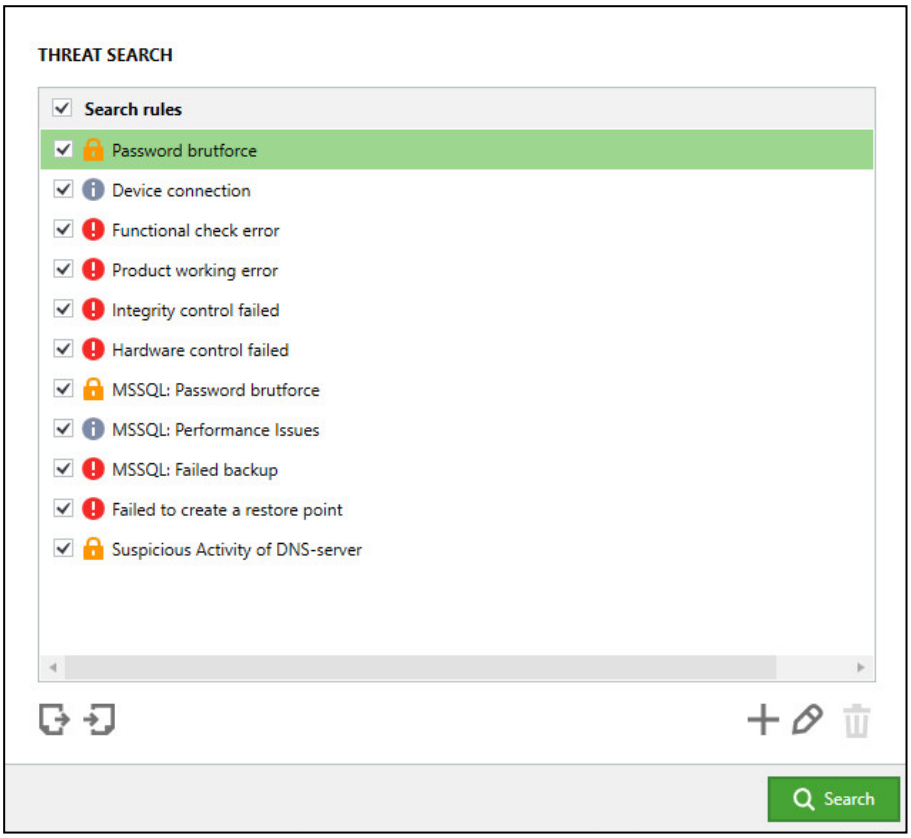
Commands of the context menu of threat events (this menu is shown in the figure) can be used to send the list for print or enable/disable displaying the event description pane.

There is a threat counter on the right of the line under the table: <**number of the selected event**>/<**total number of events**>.

To configure entry analysis and threat events search:

1. Load log entries.
2. Click the button at the top of the pane to enable the **Threats** mode of the information pane.
3. Click **Request** in the information display configuration panel (to the right of the information pane).

   The threat search settings panel appears as in the figure below.

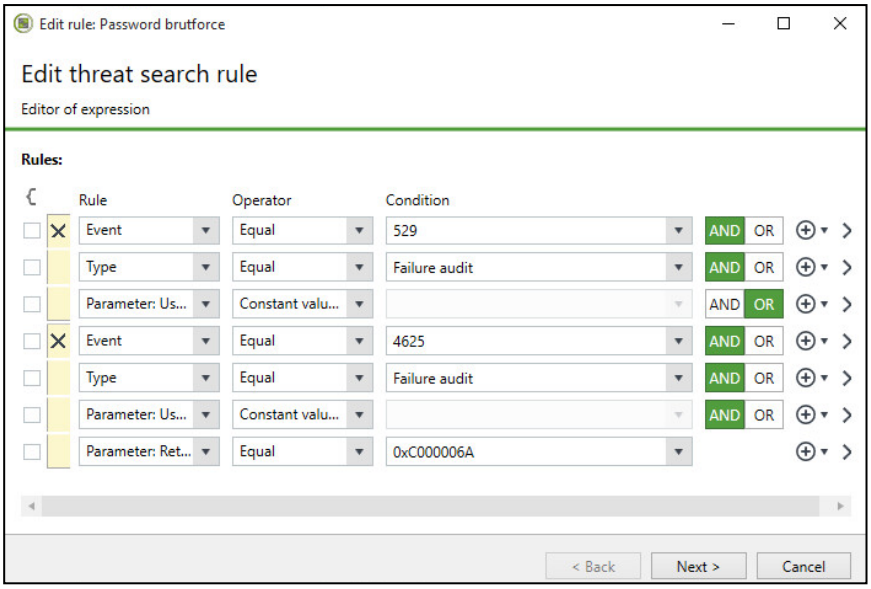


   Rules for searching threat events in loaded log entries appear in the list. By default, the list contains preset search rules of a general nature. These search rules cannot be removed from the list.

4. Generate a list of threat events search rules. To work with rules, use the buttons under the list. The following features are available for generating a list:
   - adding and deleting a threat search rule (use buttons **Add Threat Rule** and **Delete Threat Rule** under the list of rules on the right);
   - copying the rules of the threat list (to create an editable copy of the selected rule, click **Copy**);
   - loading a list or rules saved to a file (use the button **Import Threat Rule** under the list of rules on the left).
5. Configure threat events search settings. A wizard is used to configure settings for each rule individually. When a new rule is created, the wizard starts automatically. To configure the settings of an existing rule, either select it from the list and click **Edit Threat Rule** under the list of rules on the right or double-click the required rule.

   Note. Standard Secret Net Studio rules cannot be edited. The wizard can be used only to view the rules.

   Dialog boxes of the rule settings wizard:
   - The **Editor of expression** dialog box, which is shown in the figure below.



Draw up a list of conditions that entries should meet to qualify as this threat event. Conditions determine the contents of fields in event entries or settings in event descriptions. To control the contents of the field or an option on the list, there should be an expression where valid values are set. For example, the **Audit Failure** value can be set to the **Type** field so that event entries of only this type are taken into account during analysis.

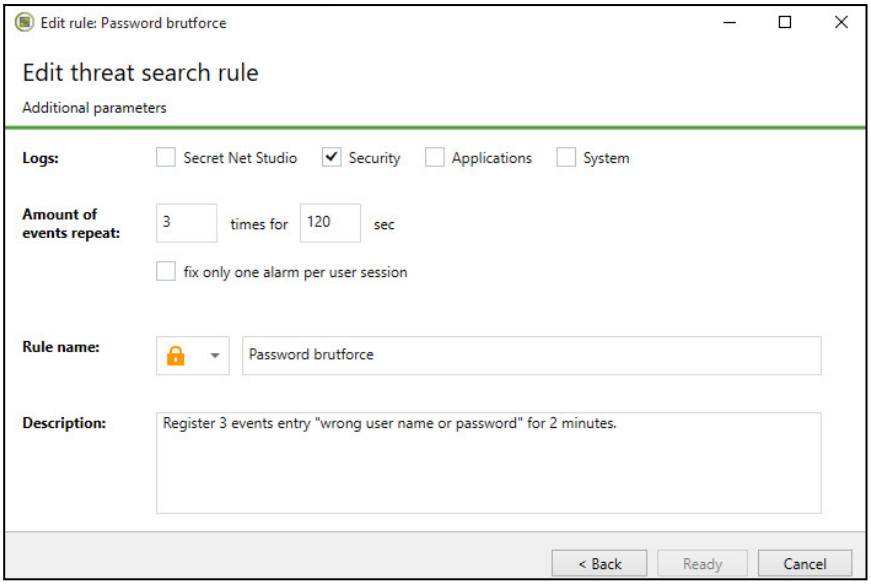
Several expressions are logically bound together. Logical connectives **AND** and **OR** can be used, and expressions can be grouped. For example, you can set a condition that the preset values for fields **Type**, **Source** and **Computer** must match, so that entries where at least one value in the specified fields does not match the preset value are not taken into account during analysis.

To create a list of conditions, use the following controls:

- Expression grouping features (on the left) — to bring into a group, select the required expressions and click the button with a curly bracket under the list. To undo the grouping, click the cross button in the grouping area;
- Features for determining conditions for the contents of a field or setting (in the center) — to set a condition, specify the name of the required field or setting and its value in drop-down lists;
- Features for selecting a logical operation with the subsequent expression or group (buttons **AND** / **OR**) — to enable a logical connective, click its button (the active logical operator is highlighted in green);
- Features for adding and deleting expressions (on the right).

After creating the list of conditions, click **Next** to move to the next dialog box.

- **Additional parameters** dialog box.



Check the logs whose entries will be taken into account during analysis for matching the given threat event.

In the **Amount of events repeats** group of fields, specify settings for tracking several entries that meet the preset conditions. If repetitive events, which occurred over a certain period (for example, to track password guessing attempts), need to be tracked, specify the required number of repetitions and the interval in seconds.

If necessary, you can enable the compression mode into one threat when analysis reveals several such events during one session of the user that the entries are related to. This helps reduce the list of threat events. This mode should be used if the sequence of threat events within one session is not important. To enable the compression mode, select **fix only one alarm per user session**.

In the fields of groups **Rule Name** and **Description**, specify the icon for the threat, its name and additional information.

To apply settings you made, click **Ready** in the rule settings wizard dialog box.

6. Once threat event search rules is configured, if necessary, save the list of rules to a file for future use. To do this, click **Export Threat Rule** under the list of rules on the left.
7. On the list, select the threat events to be searched and click **Search** at the bottom of the threat search settings panel.

   After loaded entries are analyzed, a list appears with resulting threat events.

Note. Threat search rules can be created directly when using log entries. To do this, select the required entries, call up the context menu and click the **Add Threat Rule** command. Then configure the rule settings in the dialog boxes of the configuration wizard (in a similar manner to the procedure described above).

Acknowledgment alerts in the log

To acknowledge a request with alert log entries:

1. Load alert log entries from the Security Server DB (see p. 178).
2. In the list of log entries, select the entries about events that must be acknowledged.
3. Right-click one of the selected entries and click the **Acknowledge Alerts** command.

   A dialog box appears.

4. Enter your text comment describing the reasons and action taken regarding events that occurred, and click **Acknowledge**.

   A notification appears in the system event panel saying that alerts were acknowledged, and the acknowledgment feature will be assigned to selected entries.

Sorting entries

Displayed entries are sorted by values contained in specific columns of the entries table. Standard features are used to sort the entries table. To sort by the column's contents, hover the cursor over its heading and click it.

Searching entries

The program can be used to search entries matching your criteria or containing a text string. The search is only performed on entries displayed in the current request.

To search entries based on your criteria:

1. Load log entries and configure request (see p. 178).
2. Click **Apply request locally**.

   All entries matching your criteria in the request are highlighted in the table of entries.

Color coding of entries

To visualize information, color coding is provided for the displayed entries (other than the Security Server log).

When the color coding mode is enabled, entries are highlighted with preset colors. To learn how to configure color coding settings, see p. 218.

To enable the color coding mode:

1. Load log entries (see p. 178).
2. Right-click any entry and click **Event colors**.

   Entries will be highlighted in colors corresponding to the characteristics of the event.

   The color coding mode can be disabled in a similar manner.

Obtaining information about events from external knowledge bases

If additional information about a registered event needs to be received, the program supports requesting information from external knowledge bases available on the Internet. External knowledge bases can contain useful information about reasons behind specific events and recommendations for users. The provision of information in external knowledge bases is regulated by the owners of such information resources.

Information related to Security Server log entries cannot be received from external knowledge bases.

To download information, the computer should have Internet access.

To generate an information request to the external knowledge base:

1. Load log entries (see p. 178).
2. Right-click the entry for the event that you need information about, point to the **Search in Knowledge Bases** submenu and click the required command:
   - Microsoft Knowledge Base is used to search the knowledge base at http://www.microsoft.com.
   - Event ID Database is used to search the knowledge base at http://www.eventid.net.

A browser window appears where a page with knowledge base search results opens.

Printing entries

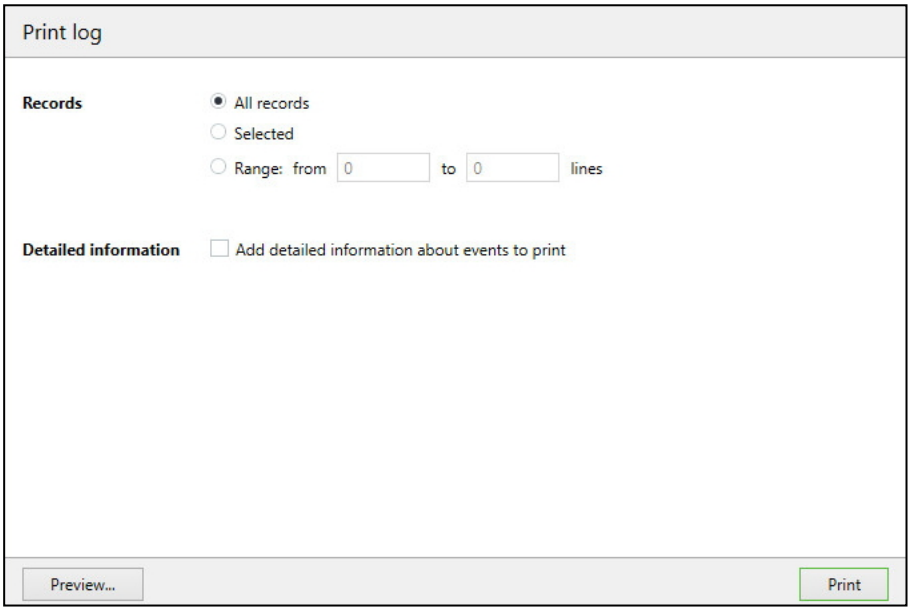
The program supports sending current request for printing. Settings can be configured in a special settings panel.

The Security Server log cannot be printed.

To print entries:

1. Load log entries (see p. **178**).
2. To print part of loaded entries, select the required entries in the table.
3. Click **Print Log** in the information display configuration panel (to the right of the information panel).

   The print settings panel appears as in the figure below.



4. Configure print settings.

Records group of fields
Determines entries to be printed: • **All records** will export the entries displayed in accordance with the current filtering settings; • **Selected** will only print the entries selected in the table; • **Range** allows you specify the range of entries to print in their sequence order in the table (according to current sorting settings). Range boundaries are specified in the fields **from** and **to**. The first and last entries in the range will also be printed
Detailed information check box
If this check box is selected, the contents of fields with a detailed description of events will be printed

5. To open the preview page, click **Preview...**. After the preview, start the process by clicking the **Print document** button on the toolbar of the preview window.

   Note. Printing can start without opening the preview window. To do this, click **Print** at the bottom of the print settings panel.

   A **Windows** dialog box appears where the printer can be selected, and general printer settings can be configured.
6. Select the printer and click **Print**.

Exporting entries

The program supports saving (exporting) entries in the current request to files. Settings can be configured in a special settings panel.

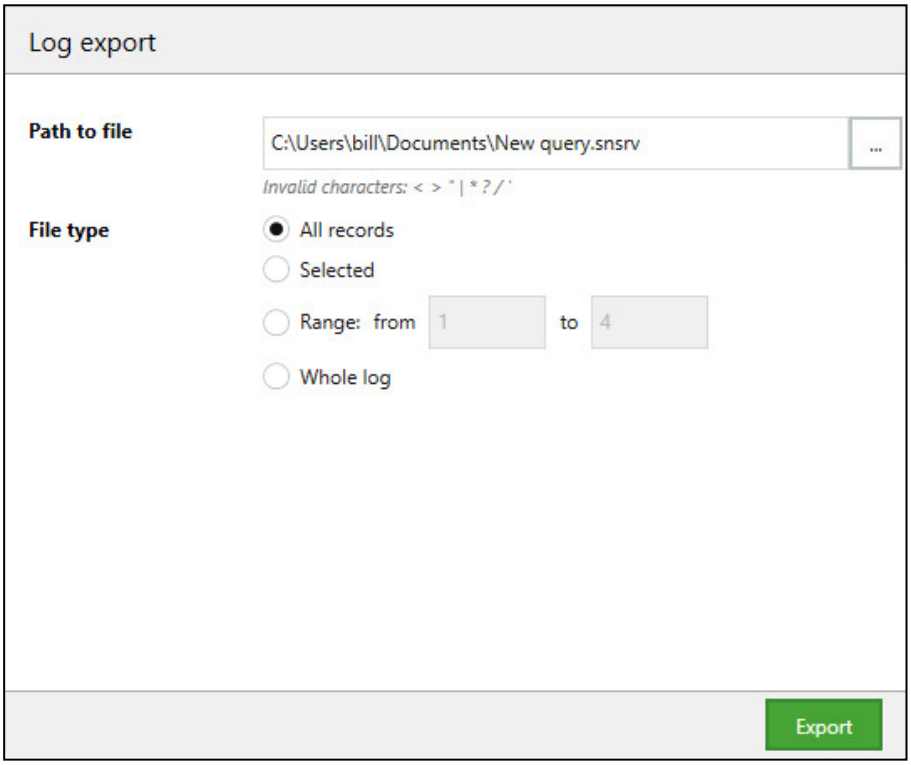
Export is performed to special file formats:

- **Alert logs** entries are exported to *.snua files
- **Station log** entries are exported to *.snlog files
- **Server log** entries are exported to *.snsrv files

To export entries:

1. Load log entries (see p. **178**).
2. To export part of loaded entries, select the required entries in the table.
3. Click **Log Export** in the information display configuration panel (to the right of the information panel).

   The export settings panel appears as in the figure below.



4. To specify the file for saving, click the button in the right part of the **Path to File** field and select the location in the Windows OS file saving dialog box.
5. Configure export settings.

File type group of fields
Determines the entries to be exported: • **All records** will export the entries displayed in accordance with the current filtering settings; • **Selected** will export only the entries selected in the table; • **Range** allows you specify the range of entries to export in their sequence order in the table (according to current sorting settings). Range boundaries are specified in the fields **from** and **to**. The first and last entries in the range will also be exported; • **Whole log** allows you to export all entries loaded in the request (including those that do not match current filtering settings)

6. Click **Export**.

Archiving centralized logs at the administrators command

Centralized logs stored in the Security Server DB are archived regularly in accordance with the Security Server's current settings (see p. 140).

You can start unscheduled archiving of centralized logs. The archiving command applies to the Security Server that the program established a connection to.

To start log archiving:

1. On the diagram or in the object list, right-click the Security Server, point to the **Archiving** submenu, and click the **Create the log archive** command.

   A dialog box appears where archiving settings can be configured.

2. Configure the archiving settings is shown below. Then click **Archive**.

Events until field
These fields determine the time interval. Entries registered until this time will be placed in the archive
Logs field
This field determines the types of logs whose entries should be archived
Comment field
Enter a brief description of the newly created archive in this field

Chapter 17
Additional features of the local administration

Editing computer registration information

The computer registration information may indicate the following details:

- name of the department where the computer is used;
- name of the company information system;
- the computer location;
- system unit number.

You can enter the registration information when installing the Client software or later. The options for editing the accounting information are provided in the Control Center (see p. 161), as well as in the Secret Net Studio settings dialog box.

To edit the registration information in the Secret Net Studio settings dialog box:

1. In the Windows **Control Panel**, select Secret Net Studio management.

   If the administrative privilege control is enabled, a dialog box prompting you to enter an administrator PIN appears.
2. In the **Administrator PIN** field, type the administrator PIN and click **OK**.

   The Secret Net Studio settings dialog box appears.
3. Select the **Computer information** tab.
4. Enter the computer information in the respective fields.
5. Click **Apply** or **OK**.

Local alert notifications

An alert is an event registered in the Secret Net Studio log or a standard OS security log, and its type is Audit Failure or Errors. When such events occur, the Secret Net Studio may locally notify the current computer user of this fact.

The mode for local alert notification can be enabled and disabled for all users of the computer (computers), or users can be provided the option to manage the mode independently.

For the description of the centralized setup procedure at the administrator's workplace in the Control Center see p. 109. Local setup is performed in the same way in the local Control Center.

To manage the local alert notification mode:

1. In the **Control Center**, click the **Computers** panel and select the object you want to configure. Right-click the object and click **Properties**. In the properties panel, select the Settings tab and click **Load Settings**
2. In the **Policies** section, select the **Alert Notification** group of parameters.
3. For the **Local alert notification** parameter, specify the mode of operation or select **User-defined**.

   Note. The user switches the local notification mode using the **Alert Notification** command in the context menu of Secret Net Studio icon located in the Windows taskbar.
4. Click **Apply**.

Local license management

The security system has license restrictions on the use of a number of subsystems that allow using security mechanisms. Licenses are managed by using special files.

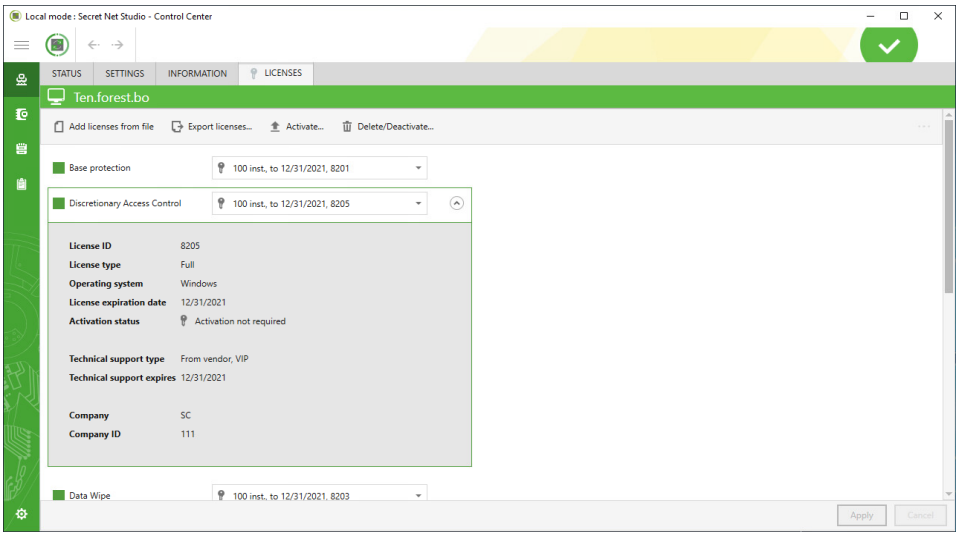
For Secret Net Studio Clients in network mode, license operations are performed on the Security Server. When a Client connects to the server, the license conditions are checked, and the corresponding client license is downloaded from the security server to the Client local storage. Licenses on the Security Server are managed via the Control Center in centralized mode.

The security system also supports local license management on protected computers. Local management may be required for Clients in standalone mode as well as in network mode if the continuous connection to the Security Server is not available.

Attention! If the license for at least one running subsystem is not activated, is missing, or has expired, the Client enters the limited operation mode. In limited operation mode, you cannot configure security system settings, and run most of the security tools.

To register licenses locally:

1. In the Local Control Center, open the **Computer** panel and go to the **Licenses** tab.



   The tab contains a list of licensed subsystems and information about the current status of licenses. Activated subsystems (with valid licenses) have green marks to the left of their names. To display detailed information about the license for a subsystem, hover your mouse over the line with the subsystem name and click the button that appears in the highlighted line on the right.

2. If you have a file with the licenses that you want to register, click **Add licenses from file**. In the file selection dialog box, select the required file with licenses.

   After processing the data, the list of licenses is updated.

3. To control the activation of subsystems (enable and disable licenses), use the controls located to the left of the names of subsystems. When you disable the license, the field with the license information for the subsystem becomes empty and a message about deleting the license is displayed below.

4. To save the current license configuration, click **Apply** at the bottom of the tab.

To export licenses locally:

1. In the Local Control Center, open the **Computer** panel and go to the **Licenses** tab.

2. Click **Export Licenses**. In the dialog box, specify the path to export the file with licenses.

To activate licenses locally:

1. In the Local Control Center, open the **Computer** panel and go to the **Licenses** tab.

2. Click **Activate** above the list of licensed subsystems. In the file selection dialog box, select the subsystems to activate licenses, and click **Next**.
3. Select the required license activation option and click **Apply**.
4. If you choose to activate via your personal account, upload the request file to the activation page in your personal account, wait for licenses to activate and download the file with the activated licenses.

   Click **Add licenses from file**. In the file selection dialog box, select the file with the activated licenses.

To delete licenses locally:

1. In the Local Control Center, open the **Computer** panel and go to the **Licenses** tab.
2. Click **Delete/Deactivate** above the list of licensed subsystems. In the dialog box, select the licenses that you want to remove from the client and click **Apply**.

To deactivate licenses locally:

1. In the Local Control Center, open the **Computer** panel and go to the **Licenses** tab.
2. Click **Delete/Deactivate** above the list of licensed subsystems. In the dialog box that appears, select the licenses that you want to remove from the client.
3. Check the box **Deactivate licenses on deletion** and click **Next**.
4. Select the option to deactivate licenses and click **Apply**.

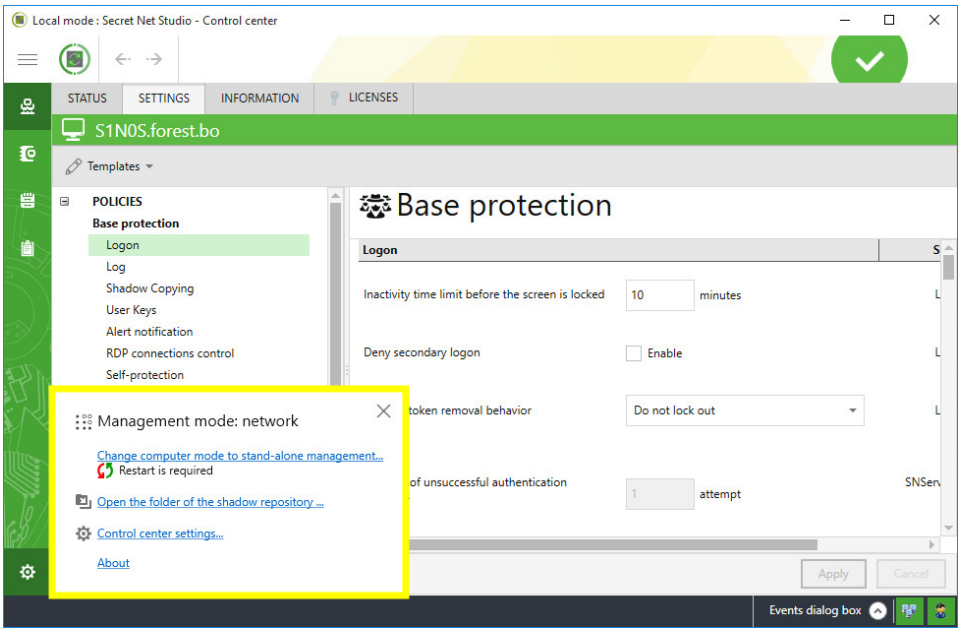
Attention! To deactivate the license for the Base Protection subsystem, you must first deactivate the licenses for all other subsystems.

Changing the client operation mode

Secret Net Studio client can operate in standalone and network modes. The current client operation mode is displayed in the Local Control Center. You can switch between the modes in the Local Control Center and using the command line.

To view information about the current client operation mode:

- In the Local Control Center, at the bottom of the navigation bar, click the **Settings** button. The configuration tools panel appears.



At the top of the configuration tools panel, the client operation mode is displayed:

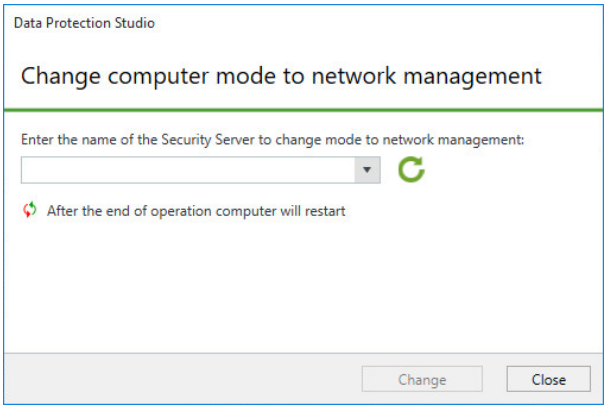
- Operation mode: **standalone** — when the client operates in standalone mode;
- Operation mode: **network** — when the client operates in network mode;
- Operation mode: the mode is being defined — when performing the mode definition process;
- Operation mode: **not defined** — if errors occur during the mode definition process;

Note. If the Client operation mode is not defined, restart the computer.

To switch the Client from standalone to network mode:

1. In the Local Control Center, at the bottom of the navigation bar, click the **Settings** button and select **Change computer mode to network management**.

   A dialog box requesting Security Server credentials appears.



2. Enter the name of the Security Server to control the Client, using one of the following methods:
   - click to search for available Security Servers and select the required server from the list;
   - enter the name of the Security Server manually.
3. Click **Next**.

   Note. To cancel the switch to network mode, click **Close**.

   The process of verifying the Security Server credentials begins. The following errors may occur:
   - Incorrect Security Server name. In this case, the system displays an error message. Click **Close** and try again;

     Note. If the name of the Security Server is incorrect, the **Error. The input parameter has a null value. Server not found** event is logged.
   - You do not have the permission to connect to the Security Server. In this case, the system displays an error message. Click **OK** and repeat the procedure with the security domain administrator privileges.
4. Select the licenses on the Security Server or on this computer and click **Next**.
5. Select the deactivation method for the licenses that were used in the standalone mode of the client, and click **Change**.

   Attention! To use these licenses on another local client, you must deactivate them.

   The configuration process begins.

Note. When switching a client from standalone to network mode, the Secret Net Studio does the following:
- creates a client account in the centralized management structure;
- creates an entry about the Security Server in the client registry;
- enters the client license key;
- connects the client to the security domain;
- switches the client protection mechanisms to the network mode.

After the configuration is completed, the notification to restart the computer appears.

6. Click **Restart**.

   The client is switched to network mode. The client license is validated. If a licensing error occurs, the system will display a corresponding message. In this case, adjust the licenses in the centralized management program.

Note. To switch the Client from standalone to network mode, go to the Client installation directory via the command prompt and run the command:

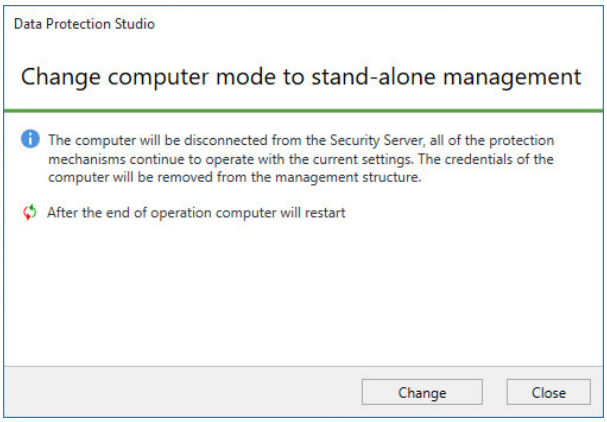
```
medusa.exe /switchmode=network /omserverName=<SERVERNAME>
/omserverPort=<PORT>
```

where:
- <SERVERNAME> — the name of the Security Server that the client is connected to;
- <PORT> — port of the Security Server; If this parameter is not defined, port **443** is used.

To switch the client from network to standalone mode:

1. In the **Local Control Center**, at the bottom of the navigation bar, click **Settings** and select **Change computer mode to standalone management**.

   The warning message appears.



Note. When switching a client from network to standalone mode, the Secret Net Studio does the following:
- deletes client credentials from the centralized management structure;
- switches the client protection mechanisms in standalone mode with the current settings saved, but without saving the license;
- deletes the Security Server credentials from the local client database.

2. Click **Next**.

   Note. To cancel the switch to standalone mode, click **Close**.

   Select the license file to be used by the client in standalone mode and click **Change**.

   Attention! You can switch the client to standalone mode with licenses that are not activated or without licenses. In this case, the Client is in limited mode, in which you cannot edit the security system settings, as well as run most of the security utilities. Licenses can be added and activated later through the Local Control Center.

   The configuration process begins.

   After the configuration is completed, the notification to restart the computer appears.

Note. After the client is switched to standalone mode, the client credentials may not be automatically deleted from the management structure. In this case, the system issues the corresponding warning message. After the client is switched to standalone mode, delete the credentials manually.

3. Click **Restart**.

   The client is switched to standalone mode.

Note. To switch the client from network to standalone mode, go to the Client installation directory at the command prompt and run the command:

```
medusa.exe /switchmode=standalone
```

Appendix

Required rights for installation and management

Secret Net Studio ensures logon and operational capabilities for any registered users, based on the user permissions within the OS and security mechanisms. To install and manage Secret Net Studio components, the users must be granted specific administrative privileges. Administrative rights and privileges depend on the executed operations.

Users included in the local administrator group are able to install the Client and manage the System in standalone mode. Some functions (e.g., Secret Net Studio log management) may be available for other users if they are granted the respective privileges.

The main Secret Net Studio operations available in network mode are listed below. The accounts with the privilege to execute operations are specified for each operation. The user account categories are as follows:

- **Security domain forest administrators** — users included in security domain forest administrators group. The user group is specified as security domain forest administrators when installing the Security Server if creating a domain in the new security domain forest is selected;
- **Security domain administrators** — users included in the security domain administrators group. The user group is specified as security domain administrators when installing the Security Server if creating a new security domain is selected;
- **Administrators** — users included in the standard local administrator group (Administrators);
- **Privilege <*privilege_name*>** — users with assigned specific privilege.

Installing and uninstalling components

The following tables contain the main operations for installing and uninstalling Secret Net Studio components.

Tab.1 Install and uninstall the Security Server

Operation	User accounts with execution rights
Create user groups for security domain forest administrators and security domain administrators	Users with permissions to create AD domain groups and to include users in groups
Install and create a domain in a new security domain forest	Administrators (domain user) + Security domain administrators
Install and create a new domain in an existing security domain forest	Administrators + Security domain forest administrators + Security domain administrators
Install and add the Security Server to an existing security domain	Administrators + Security domain forest administrators + Security domain administrators
Uninstall the Security Server and delete data from the OM structure	Administrators + Security domain administrators
Uninstall the Security Server without modifying the OM structure [1]	Administrators

[1] The Security Server will be uninstalled from the computer, but the server data will be retained in the OM structure. You can delete the Security Server data from the OM structure via the Control Center (see p. 200). This option is available if at least one Security Server is available for connection. When uninstalling the last domain server in the security domain forest without modifying the OM structure, the security forest data is deleted.

Tab.2 Install and uninstall the Client

Operation	User accounts with execution rights
Install and connect the Client to the Security Server	Administrators + Security domain administrators
Install the Client without connecting to the Security Server [1]	Administrators
Uninstall the Client and delete data from the OM structure	Administrators + Security domain administrators
Uninstall the Client without modifying the OM structure [2]	Administrators

[1]The Client will be installed on the computer without connecting to the Security Server within the OM structure. You can add the Client to the OM structure and subordinate it to the Security Server via the Control Center (see p. 200).

[2]The Client will be uninstalled from the computer, but the server information will be retained in the OM structure. You can remove the Client from the OM structure via the Control Center. (see p. 200).

Tab.3 Install and uninstall the Control Center

Operation	User accounts with execution rights
Install	Administrators
Uninstall	Administrators

Configuring mechanisms and managing object parameters

The following table contains the main operations for configuring Secret Net Studio security mechanisms and editing object (user, computer) parameters.

Tab.4 Configuring mechanisms and management of object parameters

Operation	User accounts with execution rights
Create and delete user groups	Users with permissions to create and delete AD domain accounts + Administrators
Create and delete users	Users with permissions to create and delete AD domain accounts + Security domain administrators + Administrators
Manage user parameters, assign and configure ID tokens	Security domain administrators + Administrators
Locally manage computer parameters, edit account information	Security domain administrators + Administrators
Manage Integrity Control and Application Execution Control parameters	Security domain administrators + Administrators

Using the Control Center

The following table contains the main operations in the Control Center.

Tab.5 Using the Control Center

Operation	User accounts with execution rights
Connect to the Security Server and view information	**View information** privilege for the connection server

Operation	User accounts with execution rights
Configure agents (add to the OM structure, remove, subordinate and set up parameters in configuration mode)	Security domain administrators
Configure the Security Server (add to the OM structure, remove, make subordinate and set up parameters in configuration mode)	Security domain administrators
Correct the OM structure after an abnormal uninstallation of the Security Server: the Server uninstallation when connecting to another domain within the same security forest[1]	Security domain administrators (in the connection server domain) + Security domain administrators (in the uninstalled server domain)
Configure group policy parameters for domains and organizational units	Security domain administrators + "Edit policies" privilege for the connection server. Configuring **Security system administration** settings group requires the "Security system administration" privilege on the connection server
Remotely configure local Secret Net Studio configuration: local security policy settings, hardware configuration, security mechanism status	**Edit policies** + **Execute operational commands** privileges for the connection server. Configuring **Security system administration** settings group requires the **Security system administration** privilege on the connection server
Execute operational management commands: lock, restart, update policies	**Execute operational commands** privilege for the connection server
Collect logs from protected computers	**Collect logs on command** privilege for the connection server
Archive logs in the Security Server database	**Archive/restore logs** privilege for the connection server
Acknowledge alert events (confirm receiving information)	**Acknowledge alert notifications** privilege for the connection server

[1]The operation is performed if the Security Server was abnormally uninstalled without modifying the OM structure (see p. 199) and the Security Server in another domain within the same security forest is available for connecting the program. If another Security Server in the same domain is available for connection, removing the object from the OM structure requires the same privileges as configuring the Security Servers (see above).

Assessing database size for the Security Server

To install and operate the Security Server you must install the DBMS server. To ensure better performance and the required data storage time, you must assess the future database size and the required disk space on the DBMS server computer. Based on the assessment results, you should choose database server edition (free versions have limited database size) and hardware configuration.

Main assessment criteria:

- Event flow rate is a number of registered events for a certain time period. Base value is estimated in Events Per Second (EPS) and includes the events registered in OS logs and in the Secret Net Studio log. Keep in mind that the event flow considerably depends on the computer role in the system (server, workstation) and on the working and registration parameters set in the subsystems.
- Event record size — the amount of event information stored in log entries. Record size depends on filled in empty fields: with information regarding event description, sources, objects, and other relevant data. Event record size may vary widely, hence we recommend to assess its average value.
- Log store age — determines the period of time the logs are stored in the database and archives. The logs must be available to quickly obtain information

about incidents and security policy violations, to perform audit and identify potential threats. Log store age should be sufficient to provide a retrospective analysis of system status.

Note. To ensure the database server health and reduce database maintenance costs, you should regularly back up logs. By default, backups are stored in the \Archive subfolder of the Security Server installation folder. If necessary you can upload backups to the database to analyze the log contents.

An example of calculation for a typical AS with 1G protection class, consisting of 1 Security Server and 100 Client computers is given below. A computer running Windows Server 2012 is used for the Security Server and the computers running Windows 8 are used for the Client.

Tab.6 Event flow and average record size for the Security Server

Logs	Average events per second (EPS)	Average record size (bytes)
Standard OS logs	3	1000
Secret Net Studio log	0.05	800

Tab.7 Event flow and average record size for the Client

Logs	Average events per second (EPS)	Average record size (bytes)
Standard OS logs	1	1000
Secret Net Studio log	0.05	800

Tab.8 Log volume

Log	Events Per Day	DB population per day (MB) [1]	DB log volume per 7 days (MB) [2]	Archive log volume per year (MB) [3]
Security Server, 1 computer				
Standard OS logs	259,200	259.2	1,814.4	2,365
Secret Net Studio log	4,320	3.5	24.2	31.5
Secret Net Studio client, 100 computers				
Standard OS logs	8,640,000	8,640	60,480	78,840
Secret Net Studio log	432,000	345.6	2,419.2	3,153
Total				
		9,248.3	**64,737.8**	**84,390**

[1] Specified values refer to the size of tables containing event logs. The total size of the database depends on the sizes of transaction logs and database compressing/compacting operations.

[2] When using MS SQL Express 2012 (with 10 GB database size limit) the number of data sources is to be minimized by reducing the number of subordinate computers down to 10 or by disabling OS log collection in local log transfer settings.

[3] Based on archive compression with a rate of 40:1.

Attention! To maintain total DB size and performance level, you should regularly back up database server logs and optimize DB structure to delete blank pages and defragment DB entries. In case of DB overflow (free DBs have limited size) you must perform DB cleaning procedures described in the Release Notes.

Applying settings after configuration

Not all changes in security mechanism settings take effect immediately after they are saved. Some settings apply on protected computers at certain moments.

Settings listed below take effect after computer restart or on next logon. The remaining settings apply immediately after changes are saved.

Tab.9 Control Center settings

Setting	Takes effect
Status tab — enable/disable security mechanisms	
Discretionary Access Control	After restart
Data Wipe	After restart
Device Control	After restart
Application Execution Control	After restart
Mandatory Access Control	After restart
Print Control	After restart
Disk protection and data encryption	After restart
Settings tab, Policies section — Logon group	
Inactivity time limit before the screen is locked	On next logon
Deny secondary logon	After restart
Security token removal behavior	On next logon
Number of unsuccessful authentication attempts	On next logon
User identification mode	On next logon
User authentication mode	On next logon
Password policy	On next logon
Settings tab, Policies section — Log group	
Maximum size of the security system log	If increased — immediately. If decreased — after clearing the log
Accounts with the privilege to view security system log	On next logon
Settings tab, Policies section — User Keys group	
All configurable settings in the group	On next logon
Settings tab, Policies section — RDP connections control group	
Device redirection in RDP connections	On next terminal logon
Redirection of clipboard in RDP connections	On next terminal logon
Redirection of printers in RDP connections	On next terminal logon
Settings tab, Policies section — Security system administration group	
Product self-protection	After restart
Product self-protection: Control of administrative privileges	After restart
Settings tab, Policies section — Discretionary Access Control group	
Accounts with access rights management privilege	On next logon
Settings tab, Policies section — Mandatory Access Control group	
Hide mode: Hide inaccessible confidential files	After restart
Hide mode: Show inaccessible confidential files	After restart
Operation mode: Disable flow control	After restart

Setting	Takes effect
Operation mode: Enable flow control	After restart
Operation mode: Strictly control terminal connections	On next logon
Operation mode: Automatically select maximum session level	On next logon
Settings tab, Policies section — Application Execution Control group	
Accounts excluded from Application Execution Control rules	On next logon
Settings tab, Policies section — Disk Protection and Data Encryption group	
Accounts with privileges to create encrypted file containers	On next logon
Settings tab, Policies section — Print Control group	
Document Marking	On next logon
Shadow copy	On next logon
Settings tab, Policies section — Traffic Encryption group	
Accounts with privileges to manage settings of access server connections	On next logon
Settings tab, Parameters section — Tracing Management group	
All configurable settings in the group	After restart
Settings tab, Event registration section — Antivirus group	
Registration level	After restart

Tab.10 Application and data control settings

Setting	Takes effect
List of resources in an AEC task	On next logon *
Control actor properties window, Modes tab	
AEC mode enabled	On next logon*
Process isolation enabled	On next logon*

*To force changes on controlled objects in centralized mode right-click an object/objects, select Commands and click Apply group policies.

Tab.11 User management settings

Setting	Takes effect
Account operations: delete, block, change password	On next logon
User properties configuration window, Security Settings tab — Identifier group	
User security tokens	On next logon
User properties configuration window, Security Settings tab — Access group	
All Mandatory Access Control settings	On next logon

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.

Client installation folder

When installing the Client, the following four system environment variables are created: LocalProtectionDir, NeworkProtectionDir, AntivirusDIr and LocalControlCenterDir. Every variable contains paths to the installation folders of the Client and its main subsystems.

Access permissions to the Client installation folder are inherited from the parent object.

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 Microsoft webpage.

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 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).

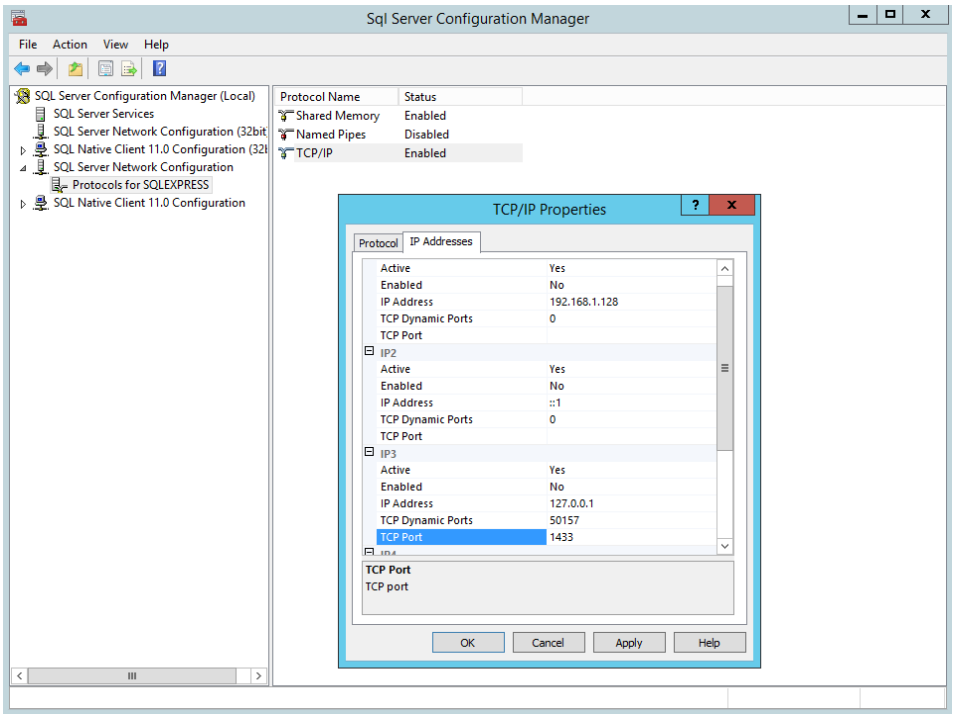
Correct interaction between the Security Server and MS SQL DBMS is ensured by enabling authentication mode to authenticate the SQL Server and Windows. For this purpose, enable mixed authentication mode on the MS SQL server.

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.



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 by default: 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 SecretNetStudioPool:

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

Changing connection settings between the Security Server and the DB

The Security Server connects to the database specified during the Security Server installation. If necessary, you may create a new DB and change connection settings between the Security Server and the DB without reinstalling the Security Server.

Changing credentials for connecting to DB

If the name and/or password of the account used for connecting to DB were changed via DBMS tools, the new credentials must be specified in the Security Server configuration file. This procedure is performed on the computer where the Security Server is installed.

To change credentials:

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

   A dialog box appears as in the figure below.

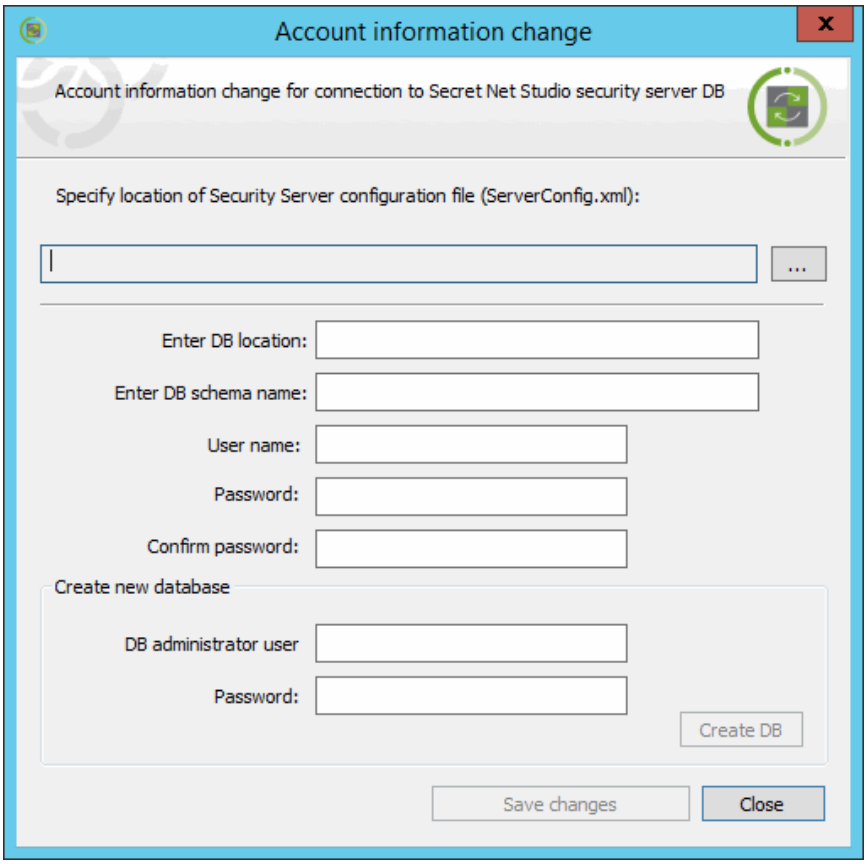


Fig.3 OmsDBPasswordChange.exe dialog box

2. Click the **Browse** button and specify the location of the **ServerConfig.xml** configuration file.

   Fields **DB location**, **DB schema name** and **User name** will be filled automatically.

3. Enter new credentials in the fields **User name**, **Password** and **Confirm password**.
4. Click **Save changes**.
5. Restart the computer.

Changing DB connection settings

If necessary, you may change the following connection settings between the Security Server and the DB:

- name or IP address of the computer, where DBMS server is located;
- DB instance name of that server;
- port for connecting the Security Server to DB.

Note. You may need to change connection settings if the DB is moved to another DBMS server. In that case, on the new server, create an account for connecting the Security Server to the DB. If the credentials of the new account do not match the credentials of the previous account, change credentials for connecting to the DB (see above).

To change connection settings:

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

   The tool dialog box appears as in p. 208.
2. Click the **Browse** button and specify the location of the **ServerConfig.xml** configuration file.

   Fields **DB location**, **DB schema name** and **User name** will be filled automatically.
3. In the **DB location** field, enter the new location in the following format:

   <name_or_IP_address_of_MS_SQL_server>\<DB_instance_name>,<port>

   Note.
   - If the server containing DBMS is installed on a computer with the Security Server and the DBMS uses a standard MSSQLSERVER .instance, you may omit DBMS server name/IP address.
   - If you use the default connection port, you do not need to specify it.
4. Enter and confirm the password.
5. Click **Save changes**.
6. Restart the computer.

Creating a new DB

You may use **OmsDBPasswordChange.exe** to create a new DB for Secret Net Studio based on a DB from the DBMS server.

To create a DB:

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

   The tool dialog box appears as in p. 208.
2. Click the **Browse** button and specify the location of the **ServerConfig.xml** configuration file.

   Fields **DB location**, **DB schema name** and **User name** will be filled automatically.
3. In the **DB location** field, enter the new location in the following format:

   <name_or_IP_address_of_MS_SQL_server>\<DB_instance_name>,<port>

   Note.
   - If the server containing DBMS is installed on a computer with the Security Server and the DBMS uses a standard MSSQLSERVER .instance, you may omit DBMS server name/IP address.
   - If you use the default connection port, you do not need to specify it.
4. Enter the name of Secret Net Studio DB schema to create.
5. Enter and confirm the credentials for connecting the Security Server to DB.
6. In the **Create new database** group, enter administrator credentials for the DB from the DBMS server.
7. Click **Create DB**.

The Secret Net Studio DB schema and the account for connecting to DB will be created in the specified DB.

8. Click **Save changes**.
9. Restart the computer.

Updating DB

You may need to update DB if you update Secret Net Studio from version 8.4 earlier.

Attention! We recommend creating a DB backup via DBMS tools before updating the DB.

To update DB:

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

   The tool dialog box appears as in p. 208.
2. Click the **Browse** button and specify the location of the **ServerConfig.xml** configuration file.

   Fields **DB location**, **DB schema name** and **User name** will be filled automatically.
3. Enter and confirm the credentials for connecting the Security Server to DB.

   Note. In this step, you may create a new account for connecting the Security Server to DB.
4. In the **Create new database** group, enter administrator credentials for current DB.
5. Click **Create DB**.

   The **The database will be updated to the latest version. We recommend creating a database backup before the update.** message appears.
6. Click **OK**.

   The database will be updated and the new account for connecting the Security Server to DB will be created.
7. 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. 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.

Restoring an incorrectly uninstalled Security Server

The Security Server uses two LDAP catalogs: global catalog and domain catalog. Those catalogs are synchronized but beside that they act independent of each other.

A single global catalog is used for the entire security forest while a separate domain catalog is created for each security domain of that forest. Each security server

corresponds to the single global catalog and to a domain catalog depending on its security domain.

Transferring schema master role and naming master role to a different Security Server

Every LDAP catalog (global or local) contains servers with special roles that allow to perform different operations inside the catalog, namely schema master role and naming master role. By default, both roles are assigned to the first server in the catalog (in case of global catalog it is the first server in the security forest. in case of domain catalog it is the first server in the domain).

If for some reason the computer that was assigned the roles is unavailable, some operations will be impossible.

To deal with this issue, you must restore the availability of the server or transfer both roles to a different Security Server.

Note. Generally in a LDAP catalog the two roles may be assigned to different servers (one server being a schema master and the other being the naming master). However, for correct operation of security servers, both roles must be assigned to a single security server in the global catalog and the domain catalog. When you transfer roles, make sure that inside the security forest a single security server is both a schema master and a naming master of the global catalog. Inside every security domain a single security server must be a schema master and a naming master of the domain catalog.

Further operations are described considering that both roles are assigned to a single server.

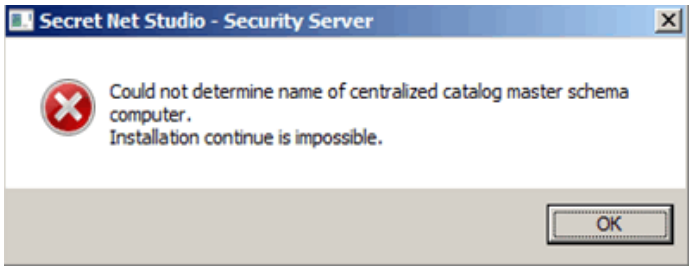
Possible causes of schema master unavailability

There are two main causes for schema master unavailability in a global catalog or in a local catalog:

1. The schema master security server was uninstalled from the security forest or from the security domain. By default, the schema master role of the global catalog is assigned to the first security server in the security forest. Similarly, the schema master role of the local catalog is assigned to the first security server in the security domain. If the first server in the forest (domain) is uninstalled, the forest (domain) will lose its schema master of the global (domain) catalog.
2. The schema master security server was lost (for example, the workstation was tuned off but was never turned back on), or it was uninstalled incorrectly (without entering the credentials of the security domain administrator and the security domain forest administrator, which led to its information remaining in the catalog). After some time the catalog will notice that the schema master has not been online for a long time and consider the schema master to be unavailable.

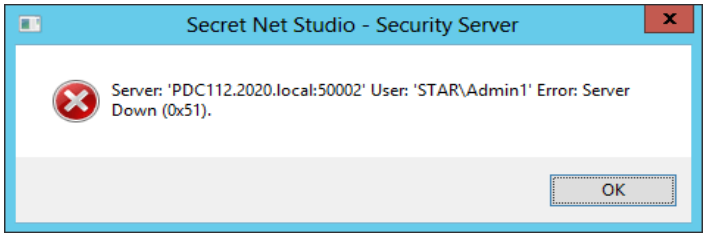
Issues caused by schema master unavailability

If the schema master of the global catalog was uninstalled, you may encounter the following error when you install new security servers:



Similarly, if schema master of the domain catalog is uninstalled in a security domain, you may also encounter the aforementioned error.

If schema master of the global catalog or of a domain catalog is lost (does not exist or was uninstalled incorrectly) you will encounter the following error when you install new security servers:



Viewing roles in the global catalog and the domain catalog

To determine, which server is assigned with schema master role and naming master role, you may use Dsmgmt, a Windows tool:

To view roles in catalogs:

1. On the computer with a server-type Windows, run cmd.exe as security forest administrator (to view roles in the global catalog) or as security domain administrator (to view roles in a domain catalog)
2. Enter the following command to run the tool:

   ```
   dsmgmt
   ```

3. On the **dsmgmt:**line, enter the following command:

   ```
   roles
   ```

4. On the **fsmo maintenance:** line, enter the following command:

   ```
   connections
   ```

5. On the **server connections:** line, enter the following command:

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

6. In command parameters, specify full DNS name of the computer with the Security Server from the required security domain forest (or from the required security domain to view the roles in the domain catalog) and port number (by default, port number is set to 50002 for global catalog, and to 50000 for domain catalog).
7. After connecting to the specified computer, on the **server connections:** line, enter the following command:

   ```
   quit
   ```

8. On the **fsmo maintenance:** line, enter the following command:

   ```
   select operation target
   ```

9. On line **select operation target:** line, enter the following command:

   ```
   list roles for connected server
   ```

As a result, a similar message appears:

```
Server "pdc:50002" knows about 2 roles
Schema - CN=NTDS Settings\0ADEL:98e3bb5c-8645-400f-8436-
8905e8c53b54,CN=2016FD$SecretNet-GC\0ADEL:8098b33f-16ec-44fa-
85d9-ff74aacea953,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,CN={00D201E5-F194-489D-9A9C-
6B28E33C2ADE}
Naming Master - CN=NTDS Settings\0ADEL:98e3bb5c-8645-400f-
8436-8905e8c53b54,CN=2016FD$SecretNet-GC\0ADEL:8098b33f-16ec-
44fa-85d9-ff74aacea953,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,CN={00D201E5-F194-489D-9A9C-
6B28E33C2ADE}
```

This message contains the DEL prefix and server name. This means that the server was deleted.

In ADAM system log (Secretnet-GC) the following message is registered:

```
Event ID 2091: Ownership of the following FSMO role is set to
a server which is deleted or does not exist. Operations which
require contacting a FSMO operation master will fail until
this condition is corrected.
```

If schema master was not uninstalled or was lost (with its information remaining in the system) the output of the **list roles for connected server** command will be similar to the following example:

```
Server "pdc:50002" knows about 2 roles
Schema - CN=NTDS Settings,CN=BOSS$SecretNet-
GC,CN=Servers,CN=Default-First-Site-N
ame,CN=Sites,CN=Configuration,CN={20256F81-63B0-46B4-991C-
74AC57F17622}
Naming Master - CN=NTDS Settings,CN=BOSS$SecretNet-
GC,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,CN={20256F81-63B0-
46B4-991C-74AC57F176
22}
```

This message does not contain the DEL prefix nex to server names of the schema master and the naming master.

Transferring roles

To transfer roles, use **Dsmgmt**, a Windows tool:.

Attention! After you transfer roles to a different computer, you will lose the option to use the previous computer as schema master and naming master. That is why you should transfer roles only in case you cannot restore the operation of the current role master. If the security server, that you transfer roles from (while it was unavailable), appears in the security domain forest (security domain) again, it will damage the respective catalog, because the LDAP catalog will contain more than one role master

To transfer schema master role and naming master role:

1. On the computer with the Security Server that you want to use as the new role master, run **cmd.exe** as security domain forest administrator (for global catalog) or as security domain administrator (for domain catalog).
2. Enter the following command to run the tool:

   ```
   dsmgmt
   ```

3. On the **dsmgmt:** line, enter the following command:

   ```
   roles
   ```

4. On the **fsmo maintenance:** line, enter the following command:

   ```
   connections
   ```

5. On the **server connections:** line, enter the following command:

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

   In command parameters, specify full DNS name of the computer with the Security Server, that you want to use as the new role master (or **localhost**), and port number (by default, port number is set to 50002 for global catalog, and to 50000 for domain catalog).
6. After connecting to the specified computer,on the **server connections:** line, enter the following command:

   ```
   quit
   ```

7. On the **fsmo maintenance:** line, enter the following command:

   ```
   seize schema master
   ```

8. View the operation result information and make sure that the schema master role was assigned to the required Security Server.
9. On the **fsmo maintenance:** line, enter the following command:

```
seize naming master
```

10. View the operation result information and make sure that the naming master role was assigned to the required Security Server.
11. After assigning both roles, enter the **quit** command to close the tool.

Update server

This chapter contains additional information about the Secret Net Studio Update server.

Download updates from a network resource

To download updates from a network resource:

1. Install the update server on a protected computer with Internet access.
2. Select **Update from SECURITY CODE LLC server** (see p. 101) and make sure that the connection is successful.
3. Create a network resource and give access to it for authorized users.
4. Configure the Secret Net Studio Clients or the cascade update servers to update from the created network resource.
5. Configure the synchronization of the C:\ProgramData\Security Code\Secret Net Studio\Server\Update Server\Packages folder with the required network resource. The folder is located on the installed update server.

Note. You can configure data synchronization using any folder replication tool, for example, Robocopy (included in Windows Vista and later versions).

Transfer updates manually

To transfer updates manually, copy the contents of the C:\ProgramData\Security Code\Secret Net Studio\Server\Update Server\Packages folder or a folder synchronized with it (see *Download updates from a network resource*) on an external drive and move it to the server in the restricted access network in the similar folder.

Update tool

Secret Net Studio contains a tool to update antivirus databases. When running the update tool, the antivirus databases are checked for updates. If necessary, latest updates are installed from the update tool.

When installing updates, the contents of the downloaded archive is checked if they are compatible with the product version that was installed on a protected computer. Verification and integrity check are also performed.

You can download the update tool from a website or from a local update server.

To download and run the update tool:

1. Follow the link https://updates.securitycode.ru:43444.
2. To download the tool, click the following:
   - **Update package for an antivirus database**;
   - **Update package for an antivirus database (ESET technology)**;
   - **Update package for an antivirus database (Kaspersky technology)**.

   Note. The file name contains the version number of an antivirus database from the tool.
3. Run the downloaded file on a protected computer. A dialog box notifying about the results of the update appears.

Note. If a hard drive does not have enough free space, the updates will not be installed.

If a failure occurs while applying updates, antivirus databases will be rolled back to the previous version. Otherwise, you can roll back the databases to previous versions using **av_cli.exe** (see document *Setup and operation. Antivirus and intrusion detection tool*) or the update server management program (see p. **99**).

Troubleshooting

If you encounter errors during the operation of Secret Net Studio update server, please check the event log of the Client (installed on your computer), Windows (if the Client is not installed) or the update server.

If necessary, you can repair the update server software.

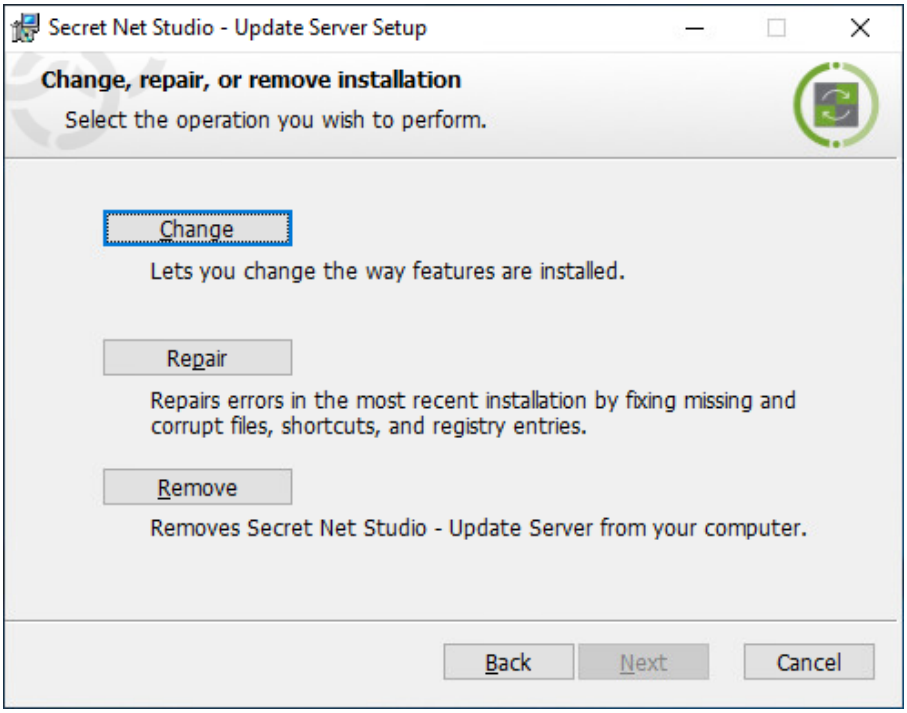
To repair the update server:

1. Run **UpdateServer.msi** that is located on the setup disk in \Tools\SecurityCode\Update Server\x64 or \Tools\SecurityCode\Update Server\Win32 (depending on Windows version).

   The program begins preparations and the welcome dialog box appears.

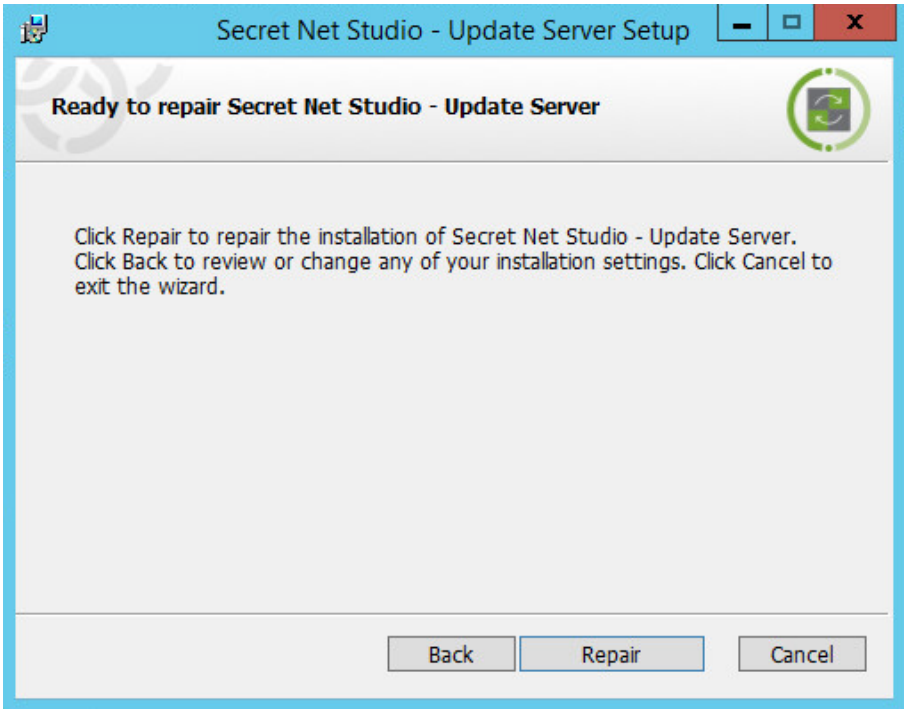
2. Click **Next**.

   A dialog box appears as in the figure below.



3. Click **Repair**.

   The following dialog box appears.



4. Click **Repair**, to start the update server repairing process. When the procedure finishes, the respective dialog box appears on the screen.
5. Click **Finish**.

Installing additional software manually

If necessary, it is possible to manually configure the computer before installing the update server.

Note. If you start the update server installation using SnAutoRun.exe or UpdateServer.exe, additional components will be installed automatically.

To install additional software:

1. Install Microsoft Visual C++ Redistributable 2017. To do this, run the vcredist_x64 or vcredist_x86 file (depending on the version of the Windows operating system installed on your computer) from the setup disk at \Tools\Microsoft\Prerequisites and follow the instructions of the Setup wizard.
2. Install the Internet Information Services (IIS) server 7.0 or higher.

   Note. The SSL certificate installed for the IIS server is self-signed.
3. Install Microsoft .NET Framework 4.5.

Networking settings

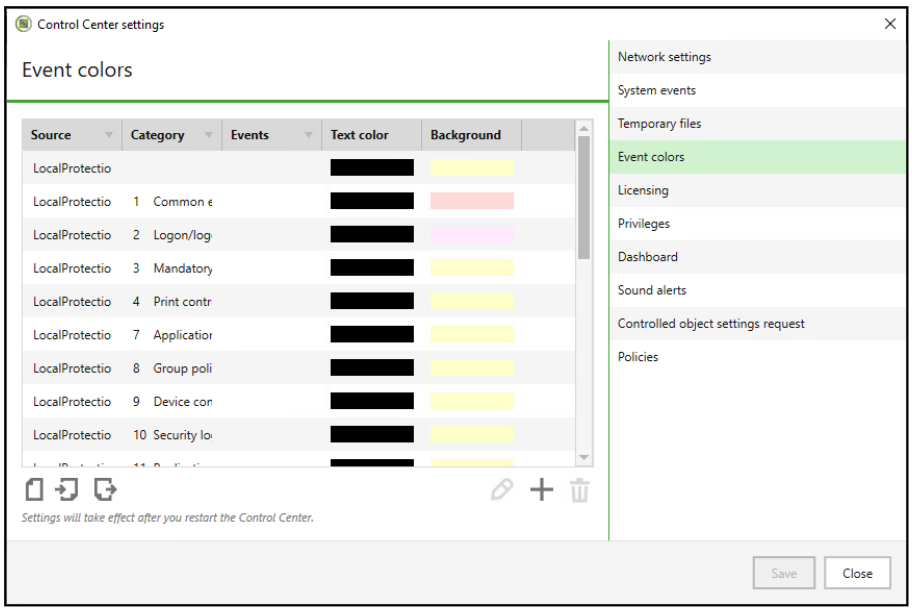
Description	Range
Waiting time	
DNS name resolution	30 – 1000 sec
Connections to the server	30 – 1000 sec
Sending requests to the server	30 – 1000 sec

Description	Range
End of the next block transfer Determines the interval during which block delivery confirmation or failed block delivery message is expected. The setting is designed for appropriate tracking of the **time to live** of operations associated with data streaming over the network. Depends on the network capacity: the higher the capacity, the shorter the interval can be. If the setting falls below an acceptable level, this can compromise the operation of the transport subsystem. This setting cannot accelerate the operation of the transport subsystem	30 – 1000 sec
Events for the workstation Determines the interval after which the server sends a watchdog request. This setting is designed for connection control. Control is based on the principle of periodically sending a service request and getting a response to it. The connection is treated as operational if the appropriate response is received. If an incorrect response is received, or the response timeout expires (see the next setting), the connection is treated as disabled. Increasing the value of this setting undermines the efficiency of getting accurate information about the state of the connection	30 – 1000 sec
For server to respond to the watchdog question Determines the maximum time for waiting for a response to the sent watchdog request. This setting is designed for controlling an established connection	30 – 1000 sec
Block size	
Receiving data from the server Determines the size of the cache of the transport subsystem for receiving a data stream. This setting is designed for optimizing data streaming over the network. Its value depends on the network capacity: the higher the capacity, the larger the cache can be	48–10240 KB
Transferring data to the server This setting is designed for optimizing data streaming over the network. Its value depends on the network capacity: the higher the capacity, the larger the block size can be	48–10240 KB
Reconnection	
Enable reconnection	On/Off
Timeout between reconnection attempts	30 – 1000 sec
Configuration update	
Takes on the following values: • **Manual. On clicking Update configuration**; • **Automatic. On registering Configuration change event**.	

Color coding settings for log entries

When configuring program settings (see p. **117**), you can create a list of rules to define the color of text and the background of displayed log entries depending on preset conditions. The list of rules appears in the **Event colors** group of the program settings dialog box.

The list of rules is shown in the figure below.

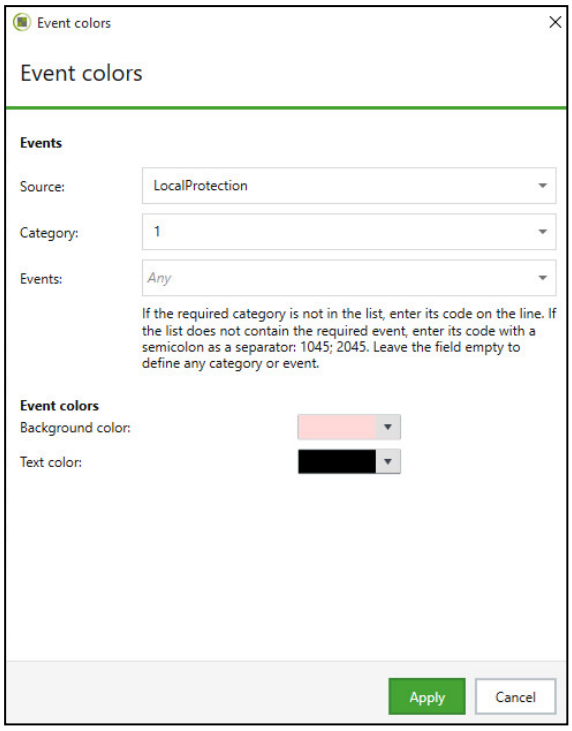


To work with the list of rules, use the buttons below the list:

Button	Description
Get default value	Returns the original list of rules used by default
Import	Loads a list of rules saved to a file
Export	Saves the current list of rules to a file
Edit	Opens a dialog box where you can configure settings of the selected rule (see below)
Add	Adds a new rule to the list. New rule settings are configured in the dialog box (see below)
Remove	Removes the selected element from the list

Configuring filtration rule settings

The filtration rule settings dialog box is shown in the figure below.



To configure rule settings:

1. Configure event analysis settings in the **Events** group of fields:

Source
Contains the component or subsystem name specified at event registration as a source. Select the required source
Category
Contains a numeric code of the event category. Select the code of the required category from the drop-down list or enter the value manually. The list of categories available for selection depends on the specified source
Events
Contains numeric identifiers of events. Select identifiers of the required events from the drop-down list or enter the value manually. The list of events available for selection depends on the category specified. Identifiers are delimited by ";"

Note. Details of events can be obtained when viewing the log entries on the General tab (see p. 176). Sources, categories, and identifiers of events appear, respectively, in the following tab fields: **Source**, **Category** and **Events**.

2. In the **Event Colors** group of fields, configure color coding settings for the background and text of lines in the table of entries. To call up color editing tools, click the button on the right of the field.
3. Click **Apply**.

Restoring logs from archives

Centralized log entries, placed into an archive from the Security Server DB, can be restored in the server database with the help of the Control Center. Restored entries can be loaded for view in the same way as for other entries stored in the DB.

Attention! Archives may only be restored by a user with the privilege to **Archive/restore logs**.

To recover entries from an archive:

1. On the diagram or in the objects list, right-click the Security Server, point to the Archiving submenu and click the **Restore the log archive** command.

   A dialog box appears with a list of archives that can be restored.
2. Select the required archive, logs (for an archive that contains several logs) and click **Restore**.

Security Server DBMS maintenance recommendations

The main reason of reducing the Security Server performance is the incorrect or untimely execution of appropriate DBMS MS SQL server procedures. The Security Server operates with a load and maintain a large number of clients at once. Configured SQL automatic actions are not enough to work effectively.

To enhance security server productivity, you should automate the execution of appropriate procedures with the help of SQL server tools.

We recommend executing and controlling the following procedures:

- defragmentation and rebuilding of indexes;
- statistics update;
- DB backup;
- log archiving.

Defragmentation and rebuilding of indexes

To speed up the processing of requests to the Security Server database on the SQL server, the security system automatically creates indexes. The indexes include information for searching across the data arrays in the database.

The content of the database changes during the operation of the Security Server. The largest changes in the database are usually associated with processing centralized logs. In particular, part of the allocated memory is released in the database after archiving the logs. Over time, these changes may eventually lead to data fragmentation which affects server performance.

To maintain a normal database operation, we recommend regularly running the procedure of index defragmentation/rebuilding in the SQL server (on average, once a week). The procedure for index defragmentation/rebuilding does not require stopping the server; however, for optimal performance, we recommend running the command at times of minimum load.

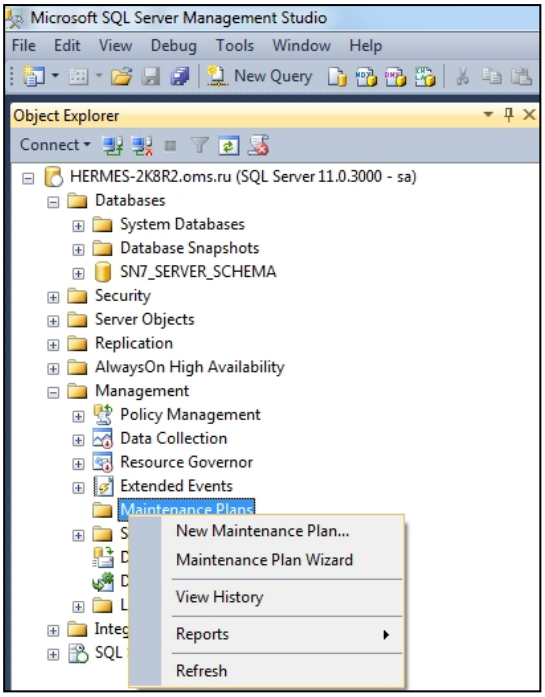
To run the index defragmentation/rebuilding, you can use batch files provided on the setup disk of Secret Net Studio distribution kit. Before using the files, follow these steps:

1. On the SQL server, create a folder on the local disk.
2. Copy the contents of \Tools\SecurityCode\ClearMSSQL\ to it from the setup disk.

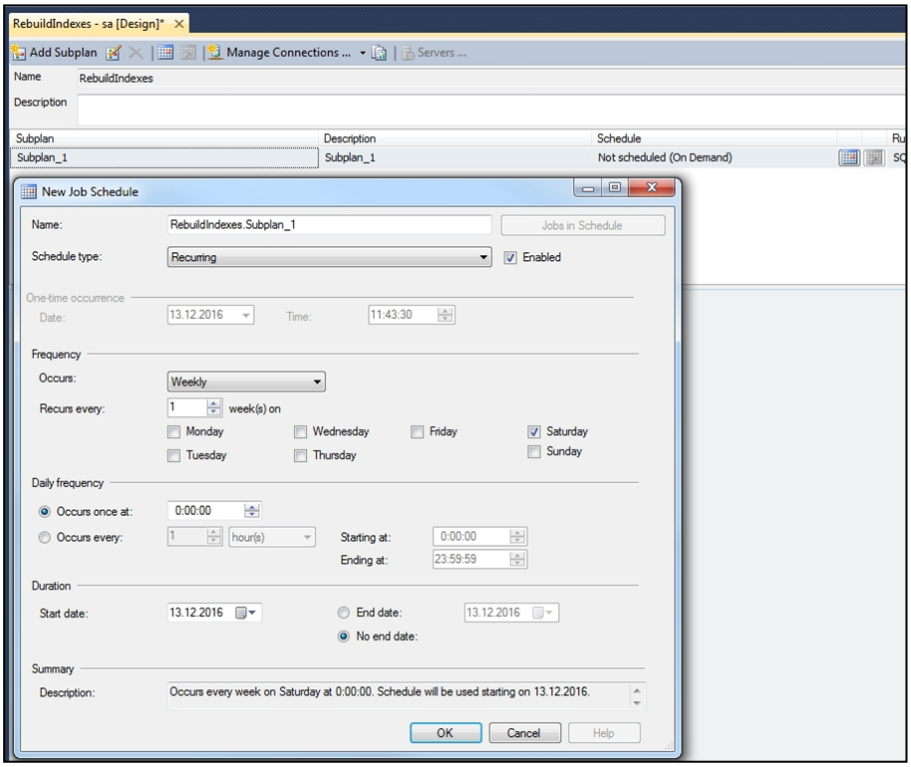
Next, run the **rebuild_index.sql** file at a time of minimum load for the SQL server. You can use the Windows Task Scheduler to run the file at a specific time.

To create a maintenance plan:

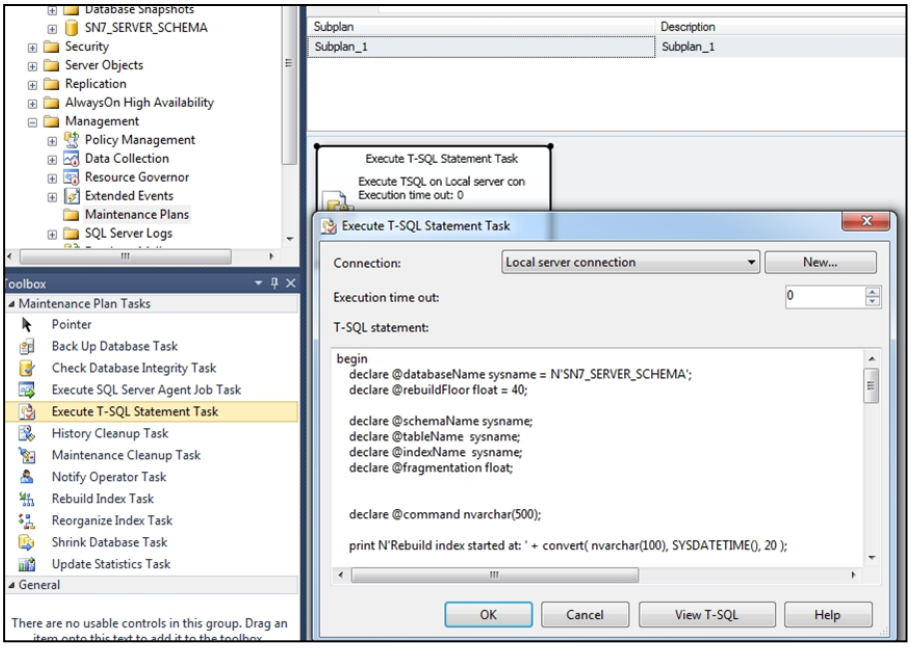
1. Open MS SQL Server Management Studio.
2. Select **Management**.
3. Right-click **Maintenance Plans** and select **New Maintenance Plan...**.



4. Set up a maintenance plan schedule.



5. Drag the **Execute T-SQL Statement Task** element from Toolbox and configure it copying the contents of the **rebuild_index.sql** to the **T-SQL Statement:** field.



6. To save changes, click **OK**.

When using SQL server of Express build, you should create the periodical task to run the command sequence with the following contents:

```
osql.exe -d [DB schema name] -i rebuild_index.sql
```

where [DB schema name] is a name of the Secret Net Studio DB schema.

Example:

```
osql.exe -d SN7_SERVER_SCHEMA -i rebuild_index.sql
```

Note. You should run the task as a SQL server administrator.

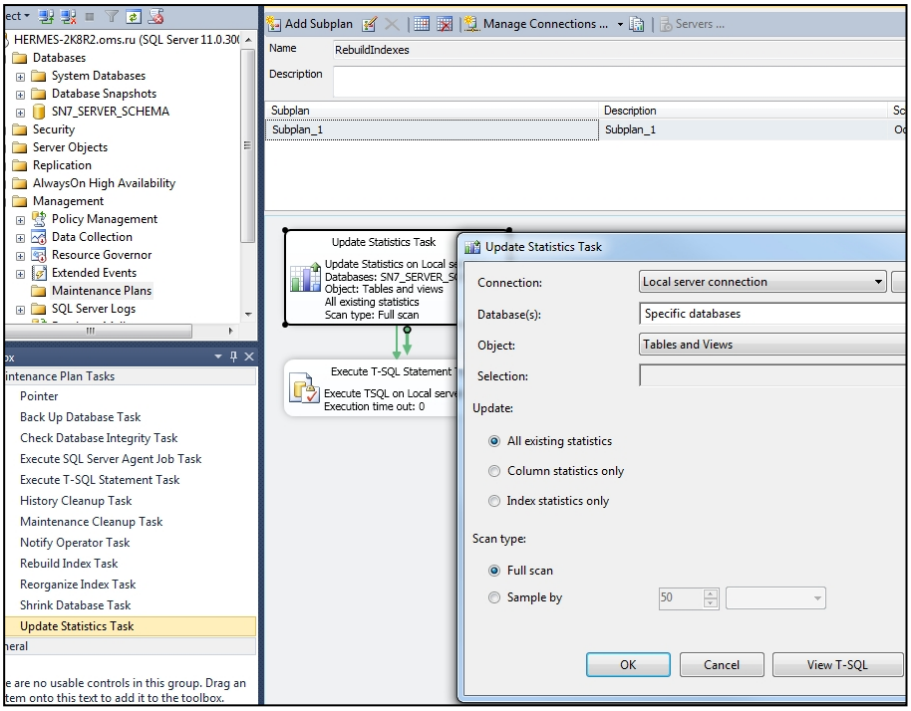
Statistics update

SQL server creates a request task based on statistics information about distribution of values in indexes and tables. Statistics information is collected on the basis of a data template. Automatic update operates when changing the data template. Sometimes, it is not enough for the SQL server to create an optimal task for execution of all the requests.

We recommend running DB statistics update procedure (usually, once per day) to guarantee the correct SQL server operation. DB statistics update procedure do not need the server to stop operating. However, we recommend running the command at times of minimum load.

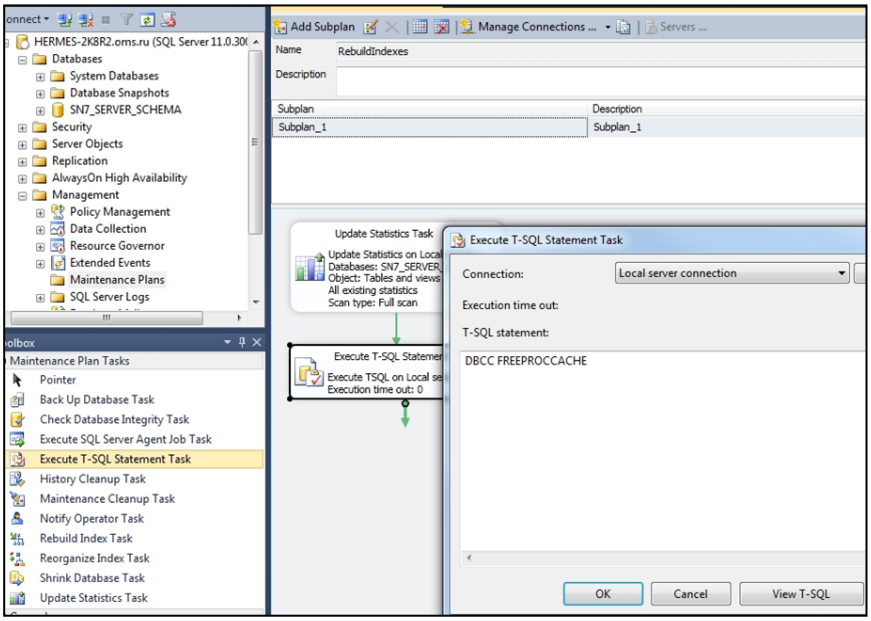
To create the statistics update task:

1. Open MS SQL Server Management Studio.
2. In the structure window, click **Management**.
3. Right-click **Maintenance Plans** and select **New Maintenance Plan...**.
4. Configure program startup schedule: once per day at midnight.
5. Drag the **Update Statistics Task** element from **Toolbox** and configure it.



6. Add the database cache clearing task:

- drag the **Execute T-SQL Statement Task** element from **Toolbox**;
- enter the **DBCC FREEPROCCACHE** command into the **T-SQL Statement** field as in the figure below.



7. To apply changes, click **OK**.

When using SQL server of Express build, you should create the periodical task to run the command sequence with the following contents:

```
osql.exe -d SN7_SERVER_SCHEMA -i update_statistic.sql
```

The contents of the **update_statistics.sql** should contain the following:

```
USE SN7_SERVER_SCHEMA;
EXEC sp_msforeachtable N'UPDATE STATISTICS ? WITH FULLSCAN';
GO
DBCC FREEPROCCACHE;
GO
```

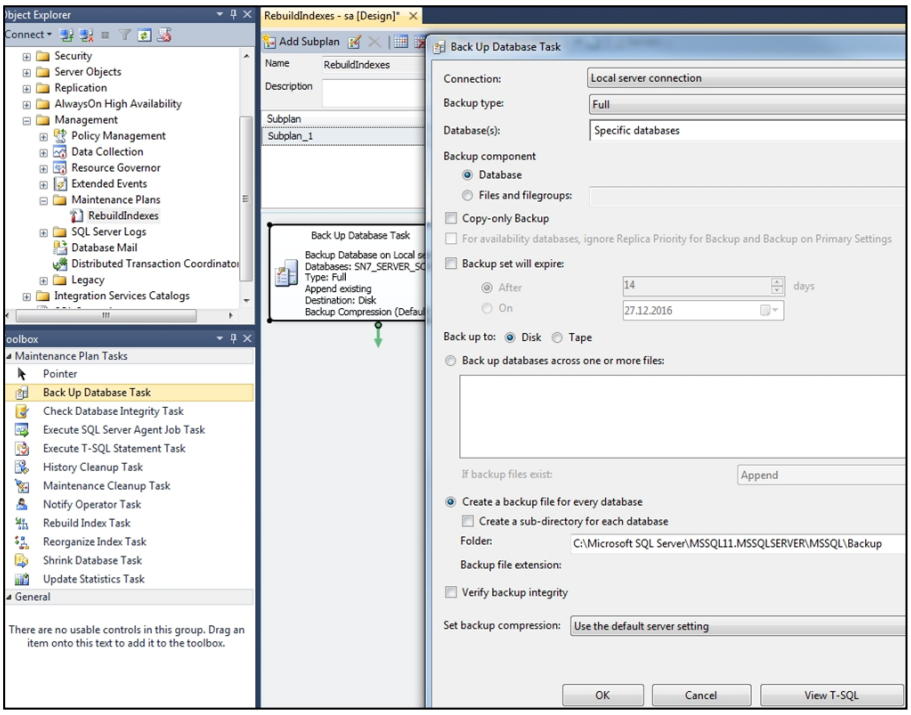
Note. You should run the task as a SQL server administrator.

Database backup

You should create the backup task to backup the database in case of failure. We recommend creating a full-type backup task for the database (usually once per week) and for **Transaction log** (usually, once per day).

To create a database full-type backup task:

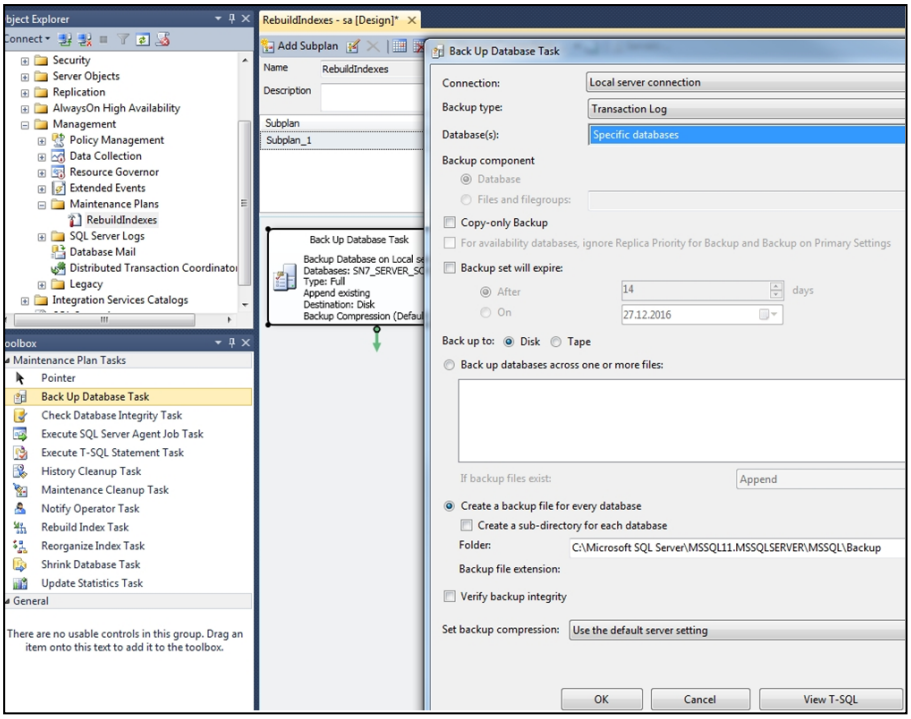
1. Open MS SQL Server Management Studio.
2. Click **Management**.
3. Right-click **Maintenance Plans** and select the **New Maintenance Plan...** command.
4. Configure the program startup schedule: once per week.
5. Drag **Back Up Database Task** from **Toolbox**.
6. Configure it selecting the **Full** backup type and **SN7_SERVER_SCHEMA** base as in the figure below.



7. To apply changes, click **OK**.

To create a transaction log backup task:

1. Open MS SQL Server Management Studio.
2. Click **Management**.
3. Right-click **Maintenance Plans** and select the **New Maintenance Plan...** command.
4. Configure the program startup schedule: once per week.
5. Drag **Back Up Database Task** from **Toolbox**.
6. Configure it selecting the **Transaction log** backup type and **SN7_SERVER_SCHEMA** base as in the figure below.



7. To apply changes, click **OK**.

When using SQL server of Express build, you should create two periodical tasks to back up the full database and transaction log. To make full-type backup of the database, the command sequence should contain the following:

```
osql.exe -d SN7_SERVER_SCHEMA -q BACKUP DATABASE SN7_SERVER_
SCHEMA TO DISK='C:\SN7_SERVER_Data.bak'
```

You should replace the **C:\SN7_SERVER_Data.bak** file path with the real backup file path.

To make backup of the transaction log, the command sequence should contain the following:

```
osql.exe -d SN7_SERVER_SCHEMA -q BACKUP LOG SN7_SERVER_SCHEMA
TO DISK='C:\SN7_SERVER_Log.bak'
```

You should replace the **C:\SN7_SERVER_Log.bak** file path with the real backup file path.

Note. You should run the task as a SQL server administrator.

The regular database maintenance task completeness control helps to enhance security server performance.

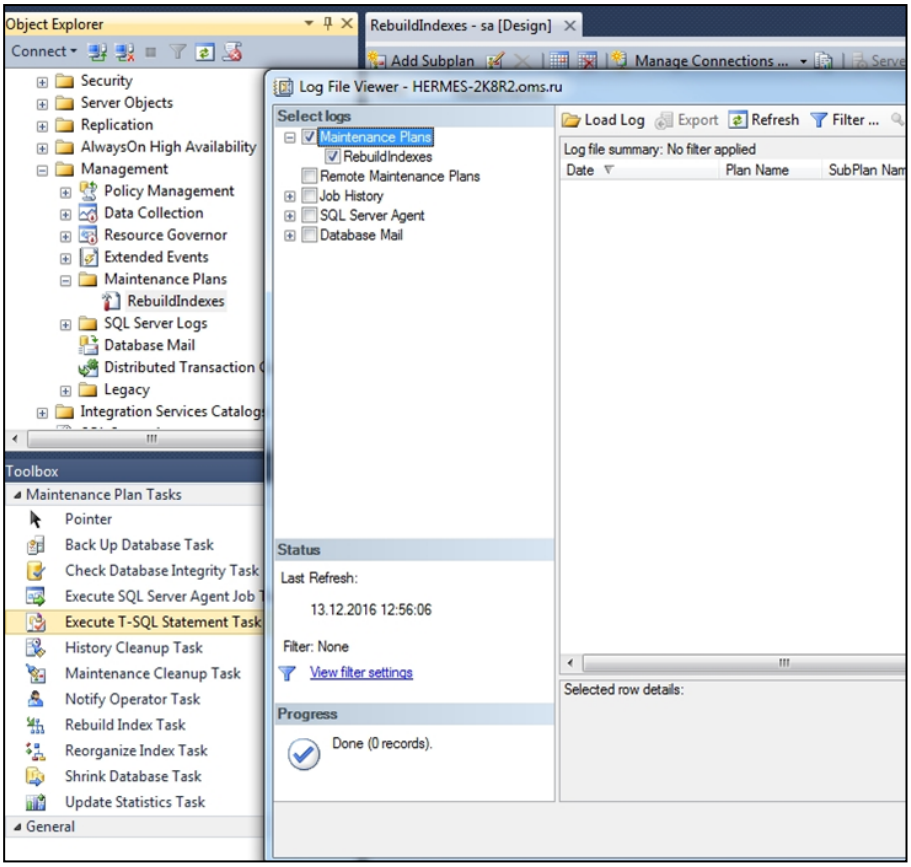
To check the created database maintenance task completeness:

1. Open MS SQL Server Management Studio.

2. Click **Management**.

3. Right-click **Maintenance Plans** and select the **View History** command.

The **Log File Viewer** window appears as in the figure below,



4. Click **Close**.

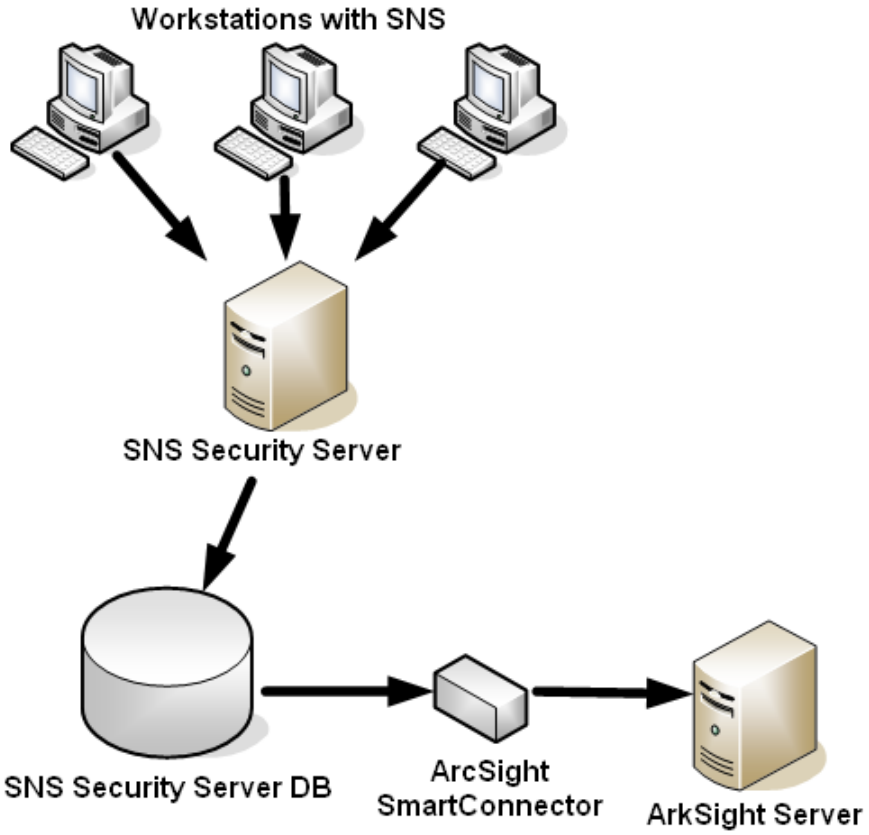
Archiving logs

The log archiving procedure is relevant for SQL server of Express build. When the database capacity limit exceeds, the Security Server fails. A log archiving schedule is configured 100 MB per one client a day. The database capacity for one client depends on the number of alert events and the log collecting frequency.

Secret Net Studio integration with SIEM systems

You can integrate Secret Net Studio with SIEM systems. Logs, collected from protected computers, can be transferred to a SIEM system from a database that is managed by MS SQL Server DBMS.

You can see the data flow after the integration of ArcSight SIEM system in the figure below.



To integrate Secret Net Studio with SIEM systems, do the following:

- configure log reading in MS SQL database for Secret Net Studio (you can use the data view below);
- configure connection, adapter or notifications for SIEM system.

Note. Consult with SIEM documentation to configure connection.

To configure log reading in MS SQL database for Secret Net Studio:

1. Create a view using the following SQL script.

```
/*
your DB name instead of "SN7_SERVER_SCHEMA"
*/

USE [SN7_SERVER_SCHEMA]
GO

EXEC sp_configure 'clr enabled' , '1';
RECONFIGURE;
GO
/*
creates stored function and view
```

```
*/

/*
load dll
*/

/*
Beware!
drops function and assembly if it exists to avoid name collision
*/

IF OBJECT_ID('dbo.GetDescription') IS NOT NULL
        DROP FUNCTION dbo.GetDescription;
GO

IF (select top 1 count(x.[name]) from
(select
        a.[name]
        from sys.assembly_files f
full outer join sys.assemblies a
        on f.assembly_id=a.assembly_id
full outer join sys.assembly_modules m
        on a.assembly_id=m.assembly_id
) as x where [name] like '%ByteDataToDeviceInfoConverterAsm') = 1
DROP ASSEMBLY ByteDataToDeviceInfoConverterAsm
GO

IF EXISTS (SELECT 1
        FROM SYSOBJECTS
        WHERE ID = OBJECT_ID('SECRETNETLOG')
        AND TYPE = 'V')
DROP VIEW SECRETNETLOG
GO

CREATE ASSEMBLY ByteDataToDeviceInfoConverterAsm
        FROM 'C:\CLRDeviceInfoConverter\DBConverter.dll';
GO

/*
create function from assembly
*/

CREATE FUNCTION dbo.GetDescription (@data varbinary (max), @eventid
int,@eventmessage nvarchar(max), @locale nvarchar(5))
RETURNS nvarchar(max)
AS EXTERNAL NAME [ByteDataToDeviceInfoConverterAsm].
[ByteDataToDeviceInfoConverter.CLRConverter].[GetDescription];
GO
```

```
/****** Object: View [dbo].[SERVICEEVENTLOGS] Script Date: 13.11.2018 11:24:41 ******/
SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO
/*==================================================================*/
/* View: SECRETNETLOG
don't forget to set locale at dbo.GetDescription(E.DATA, E.EVENTID, "ru-RU");
possible locales are: en-US, ru-RU, es-ES;
*/

/*==================================================================*/

CREATE VIEW SECRETNETLOG ( ID, TIMEWRITTEN, STATION, CATEGORY, EVENTID, EVENTMESSAGE, TYPE, COMPUTER, USERSID, USERDOMAINNAME, USERNAME )
AS
SELECT T.EVENTLOGRECID,
        T.TIMEWRITTEN,
        C.MNAME,
        CAST (T.CATEGORYMESSAGE as nvarchar(512)),
        T.EVENTID,
        CAST (dbo.GetDescription(T.DATA, T.EVENTID, T.EVENTMESSAGE ,'ru-RU') as nvarchar(MAX)),
        T.TYPEDESCRIPTION,
        T.COMPUTERNAME,
        T.USERSID,
        T.USERDOMAINNAME,
        T.USERNAME

FROM EVENTLOGREC T, EVENTLOG T1, SERVICE T2, SERVICEPROVIDER T3
WHERE T1.LOGTYPE=4 AND T.EVENTLOGRECID > 0 AND
        T.EVENTLOGID = T1.EVENTLOGID AND T1.SERVICEID = T2.SERVICEID AND T2.PROVIDERID = T3.PROVIDERID
GO
```

2. Specify the path to the supplied DBConverter.dll file in the block:

   CREATE ASSEMBLY ByteDataToDeviceInfoConverterAsm FROM 'C:\CLRDeviceInfoConverter\DBConverter.dll';

   GO

3. Specify the required localization:

   CAST (dbo.GetDescription(T.DATA, T.EVENTID, 'ru-RU') as nvarchar(1024))

Information about the columns of the created view is shown in the table below.

Column name	Type	Max size	Purpose
ID	Int	–	Service event ID

Column name	Type	Max size	Purpose
TIMEWRITTEN	Date/time	–	Event occurrence time
STATION	Line	255	Name of the computer from which the log was received
CATEGORY	Line	512	Event category
EVENTID	Int	–	Event ID
EVENTMESSAGE	Line	2 Gb	Event description
TYPE	Line	255	Event type
COMPUTER	Line	128	The computer that caused the event to occur (matches the Computer field in the standard LogViewer)
USERSID	Line	128	User SID
USERDOMAINNAME	Line	128	User domain name
USERNAME	Line	128	User name

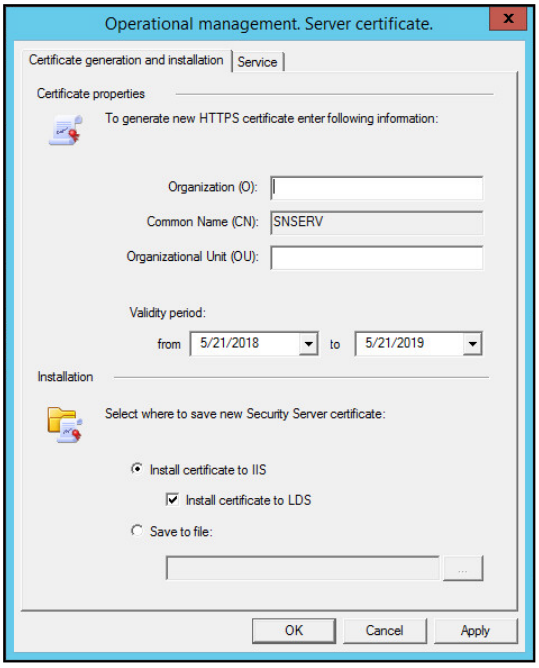
Generating and installing the Security Server certificate

This procedure is run on the Security Server computer.

To generate and install the Security Server certificate:

1. Click **Start** and select **Certificates** in the **Security Code** group:

   A configuration dialog box appears as in the figure below.



2. In the **Certificate Properties** field group, enter the required values.

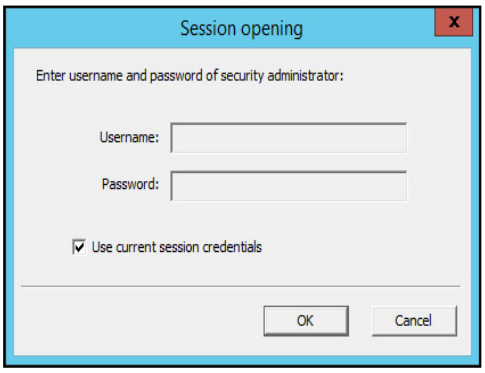
   Note. Organization and **Organizational Unit** are optional fields.

3. In the **Installation** field group, enter the certificate location and click **Apply**.

   If the IIS has a previously installed certificate, the system will display a request to continue writing the new certificate.

4. When prompted, click **OK**.

   The following dialog box appears as in the figure below.



5. Enter credentials of the user with the right to write in the storage of centralized control objects and click **OK**.

   Comments. If the current user has rights to write, select the **Use current session credentials** check box. If such rights are not granted, enter the details of the respective account. By default, rights to write to the storage are available to users that are members of the group of security domain administrators.

   After the new certificate is installed, a message appears.

Configuring a secure connection to directory services

Secret Net Studio supports enforced security of access to the storage of centralized control objects of Secret Net Studio. In this mode, network calls to AD LDS services made by components of Secret Net Studio are carried out over Secure Socket Layer/Transport Layer Security (SSL/TLS) protocols. These protocols involve authentication of the computer on which the directory service (Security Server) is deployed and support the functions of establishing a secure connection with certificates.

For the enforced security mode to be used, a public key infrastructure (PKI) should be arranged and configured in the system. PKI implementation can be guaranteed by standard Windows OS features or third-party software. See the section below for general details of how standard OS features are used to arrange and configure PKI.

Secure communication with AD LDS

To provide secure communication with AD LDS services, PKI is configured as follows:

1. Request a certificate for the Security Server from the Certification Authority (CA). For the certificate, specify the full domain name of the Security Server computer and the Server Authentication method. Save the received certificate in the computer context storage, in the **Personal** section.

   Note. If the system doesn't have a CA, a self-signed certificate created on the Security Server can be used to organize secure connections. This certificate is used in the future as both the computer certificate and the CA certificate.

2. Install the received certificate in IIS by launching IIS Manager and depending on the OS version perform the actions below:
   - In the hierarchical list, expand the section of websites, call the **SecretNetStudioSite** context menu and select the **Edit Bindings** command.
   - In the website bindings list that appears, call the dialog for configuring the https element and select the received certificate in the list of SSL certificates.
   - After the certificate is installed, use the respective control in the context menu of **SecretNetStudioSite** to restart IIS.
3. Grant required permissions to access the certificate key file. To do this, in File Explorer, go to the default directory where the keys are stored. Path to the directory in Windows Server 2012: %ProgramData%\Microsoft\Crypto\RSA\MachineKeys. In other OS versions: %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\MachineKeys. In the directory, call the window for configuring the certificate key file properties (the required file can be identified by its creation date and time), go to the Security tab, and add the required account with default permissions to the list. The name of the account to be added depends on the computer the security server is installed on:
   - If Security Server is installed on a domain controller, the account name includes OMS_LDS_xxx$.
   - If Security Server is installed on any other computer, the account name includes NETWORK SERVICE.
4. Put the server certificate on the Security Server computer in the **Personal storage** section in the context of **SecretNet** and **SecretNet-GC** service instances. To do this, load the Certificates snap-in in the managing computer certificates mode and in the managing certificates mode of each service (i.e., three snapins are loaded). Export the server certificate together with the private key from the **Personal** section of the snap-in with computer certificates and then import snap- ins with service certificates to sections ADAM_ SecretNet\Personal and ADAM_SecretNet-GC\Personal of snap-ins with service

certificates. Then grant permissions to access the files of imported certificate keys (see Step **3**).

5. If there is another Security Server, apply the above steps to that server as well.
6. Start the Security Server certificate control program and synchronize the certificate installed in IIS with the Security Server certificate. To do this, go to the **Service** tab in the configuration dialog box and click **Synchronize**.
7. Open the configuration file ServerConfig.xml in the Security Server setup folder. Find the **UseSSLConnection** parameter and change it from false to true. In the **Name** parameter (below) modify the value to the full domain name of the Security Server computer. Save the changes and restart the computer.
8. To enable encryption on the computers subordinate to the Security Server, install the Security Server certificate and root certificates on those computers:
   - the Security Server certificate — to the **Personal storage**;
   - the root certificate — to the **Trusted root certification authorities storage**.
9. Enable enforced traffic security on trusted computers. To do this, select the required objects in the Computers panel of the Control Center, go to the **Status** tab, and enable **Encrypt control network traffic**. This setting takes effect after the computers are restarted.

Registering events in the Security Server log

Name	ID	Description
Server connection established	1	The connection between the user computer and the Security Server established. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • session ID
Server connection terminated	2	The connection between the user computer and the Security Server terminated. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • session ID
Connection attempt denied	3	The connection between the user computer and the Security Server was denied. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • session ID; • reason of failure
Requesting configuration of operational management	4	The request to receive the OM configuration was sent
Error obtaining configuration of operational management	6	An error while obtaining OM configuration. Description of the error is in the "Details" field

Name	ID	Description
Modifying configuration of operational management	7	The OM configuration was changed. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • objects created; • objects modified; • objects deleted; • conf. updated firewall; • deleting conf firewall; • configuration changed: (collecting logs: <user SID>,archiving: <user SID>, alert mailing : <user SID>, network configuration: <user SID>)
Error modifying configuration of operational management	8	An error while changing the OM configuration. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • objects created; • objects modified; • objects deleted; • conf. updated firewall; • deleting conf firewall; • configuration changed: (collecting logs: <user SID>,archiving: <user SID>, alert mailing : <user SID>, network configuration: <user SID>); • error description
Executing command	10	The command execution process was launched. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • command; • agents
Command execution error	12	An error while executing the command. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • command; • agents; • error description
Request for log archiving	13	Request for log archiving in the Security Server database was sent. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • log types; • description; • temporary closing

Name	ID	Description
Request for log archiving executed	14	The request for log archiving in the Security Server database has been successfully executed. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • log types; • description; • temporary closing
Error archiving logs	15	An error while archiving logs in the Security Server database. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • log types; • description; • temporary closing; • error description
Scheduled log archiving started	16	The scheduled log content archiving process started. The following information is specified in the "Details" tab: • log types; • description; • temporary closing
Scheduled log archiving executed	17	The scheduled log content archiving process has been successfully executed. The following information is specified in the "Details" tab: • log types; • description; • temporary closing
Error during scheduled log archiving	18	An error while scheduled log archiving in the Security Server database. The following information is specified in the "Details" tab: • log types; • description; • temporary closing; • error description
Request for logs to be restored from the archive	19	The request for restoring logs from the Security Server database was sent. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • log types
Request for logs to be restored from the archive executed	20	The request for restoring logs from the Security Server database has been successfully executed. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • log types

Name	ID	Description
Error restoring from the archive	21	An error while restoring logs from the Security Server database. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • log types; • error description
Alert notifications successfully loaded to the server	23	Alert notifications have been successfully uploaded to the server. The following information is specified in the "Details" tab: • computer; • computer SID; • UAID (ID of the unauthorised access block saved in the DBMS); • number of notifications
Error loading alert notifications to the server	24	An error while uploading alert notifications to the server. The following information is specified in the "Details" tab: • computer; • computer SID; • UAID (ID of the unauthorised access block saved in the DBMS); • number of notifications • error description
Log received from the workstation	25	the Security Server database received the log from the workstation. The following information is specified in the "Details" tab: • computer; • computer SID; • log types
Error receiving log from the workstation	26	An error while sending the log from the workstation to the Security Server database. The following information is specified in the "Details" tab: • computer; • computer SID; • log types; • error description
Log received for reading	27	the Security Server database received the log for reading. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • log types; • query
Error receiving log for reading	28	An error while uploading the log to the Security Server database for reading. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • log types; • query; • error description

Name	ID	Description
Initiating procedure for receiving log(s)	29	Starting the automatic procedure of uploading log(s) to the Security Server database. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • log types; • query
Starting log collection	30	Starting log collection in the Security Server database. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • agents; • log types
Log collection successfully completed	31	The started process of log collection to the Security Server database has been successfully executed. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • agents; • log types
Error collecting logs	32	An error while collecting logs in the Security Server database. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • agents; • log types; • error description
Scheduled log collection started	33	Scheduled log collection in the Security Server database started. The following information is specified in the "Details" tab: • computer; • computer SID; • agents; • log types
Scheduled log collection successfully completed	34	The started process of scheduled log collection in the Security Server database has been successfully executed. The following information is specified in the "Details" tab: • computer; • computer SID; • agents; • log types
Error during scheduled log collection	35	An error while processing the scheduled log collection in the Security Server database. The following information is specified in the "Details" tab: • computer; • computer SID; • agents; • log types; • error description

Name	ID	Description
Modifying configuration of operational management	36	The configuration of operational management was modified. The following information is specified in the "Details" tab: • computer; • computer SID; • list of modified management objects identifiers: agents and servers
Error modifying configuration of operational management	37	An error while modifying the configuration of operational management. The following information is specified in the "Details" tab: • computer; • computer SID; • list of modified management objects identifiers: agents and servers; • error description
Alert acknowledgment	38	Alert acknowledgment. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • acknowledging; • alert level: (low | elevated | high) or identifiers: <list of acknowledged alerts identifiers>; • comments
Error acknowledging alerts	39	An error while acknowledging alerts. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • acknowledging; • alert level: (low | elevated | high) or identifiers: <list of acknowledged alerts identifiers>; • comments; • error description
Error connecting to a higher hierarchy server	40	An error while connecting to a higher hierarchy server. The following information is specified in the "Details" tab: • connection address; • server SID; • session ID; • error description
Report generation started	280	The process of generating report started. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • type; • agents
Error starting report generation	281	An error while generating the report. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • type; • agents; • error description

Name	ID	Description
Report generation successfully completed	282	Report generation has been successfully completed. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • type; • agents
Error generating the report	283	An error while generating the report. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • type; • agents; • error description
Canceling report generation	290	Canceling the process of report generation. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • type; • agents
Error canceling report generation	291	An error while canceling the process of report generation. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • type; • agents; • error description
Obtaining more information about OM agent	300	The process of obtaining more information about operational management agent started. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • agent name; • agent ID; • agent type; • agent class
Error obtaining more information about OM agent	301	An error while obtaining more information about the operational management agent. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • agent name; • agent ID; • agent type; • agent class; • error description

Name	ID	Description
Modifying the license	400	Modifying the license for using the Secret Net Studio components. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • licenses (added | deleted | modified)
Error modifying the license	401	An error while modifying the license for using the Secret Net Studio components. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • licenses (added | deleted | modified); • error description
Modifying server settings	500	Modifying the Security Server settings. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • option
Error modifying server settings	501	An error while modifying the Security Server settings. The following information is specified in the "Details" tab: • user; • user SID; • computer; • computer SID; • option; • error description
Modifying group policies of the security domain	502	Modifying group policies of the security domain. The following information is specified in the "Details" tab: • user; • user SID; • computer name; • computer SID; • group policies modified for objects
Error modifying group policies of the security domain	503	An error while modifying group policies of the security domain. The following information is specified in the "Details" tab: • user; • user SID; • computer name; • computer SID; • group policies modified for objects; • error description
Requesting group policies of the security domain	504	The request for the security domain group policies. The following information is specified in the "Details" tab: • computer name; • computer SID; • group policies
Error requesting group policies of the security domain	505	An error while requesting group policies of the security domain. The following information is specified in the "Details" tab: • computer name; • computer SID; • group policies; • error description

Name	ID	Description
Agent notification of changes in group policies of the security domain started	506	The process of notifying the agents of changing the security domain group policies started. The following information is specified in the "Details" tab: • servers; • AD containers
Error starting agent notification of changes in group policies of the security domain	507	An error while starting the agent notification of changing the security domain group policies. The following information is specified in the "Details" tab: • servers; • AD containers; • error description
Agent notification of changes in group policies of the security domain successfully completed	508	The process of notifying the agents of changing the security domain group policies succeeded. The following information is specified in the "Details" tab: • servers; • AD containers
Error notifying agents of changes in group policies of the security domain	509	An error while notifying the agents of changing the security domain group policies. The following information is specified in the "Details" tab: • servers; • AD containers; • error description
Notifying of changes in parent server settings	510	Notifying of changes in the parent the Security Server settings. The following information is specified in the "Details" tab: • server SID; • option
Error notifying of changes in parent server settings	511	An error while notifying of changes in the parent the Security Server settings. The following information is specified in the "Details" tab: • server SID; • option; • error description
Modifying the operational management job	512	Modifying the operational management job. The following information is specified in the "Details" tab: • user; • user SID; • action; • job ID; • category; • number; • command; • SW version; • number of computers
Error modifying the operational management job	513	An error while modifying the operational management job. The following information is specified in the "Details" tab: • user; • user SID; • action; • job ID; • category; • number; • command; • SW version; • number of computers; • error description

Name	ID	Description
Change in repository	514	A change in repository. The following information is specified in the "Details" tab: • user; • user SID; • action; • SW version; • SW category
Error handling the repository	515	An error while handling the repository. The following information is specified in the "Details" tab: • user; • user SID; • action; • SW version; • SW category; • error description
Change in the firewall configuration	516	A change in the firewall configuration. The user is specified in Details.
Error handling the firewall configuration	517	An error while handling the firewall configuration. The following information is specified in the "Details" tab: • user; • error description
SW deployment started	518	The software deployment started. The following information is specified in the "Details" tab: • computer name; • computer SID; • SW version; • job ID
SW deployment completed	519	The software deployment has been successfully completed. The following information is specified in the "Details" tab: • computer name; • computer SID; • SW version; • job ID
Error deploying SW	520	An error while deploying the software on the workstation. The following information is specified in the "Details" tab: • computer name; • computer SID; • SW version; • job ID; • error description
SW uninstallation started	525	The software uninstallation from the workstation started. The following information is specified in the "Details" tab: • computer name; • computer SID; • SW version; • job ID
SW uninstallation completed	526	The software uninstallation from the workstation has been successfully completed. The following information is specified in the "Details" tab: • computer name; • computer SID; • SW version; • job ID
JaCarta control command	527	JaCarta control command was launched

Name	ID	Description
JaCarta control command error	528	An error while executing JaCarta control command. JaCarta control command launched The descripion of the error is in Details
New corruptions in configuration found after replication	600	A new corruption in the configuration found after replication. The following information is specified in the "Details" tab: • lost agents; • duplicated agent; • lost servers; • duplicated servers
Corruptions in configuration were not found after replication	601	Corruptions in the configuration were not found after replication. The following information is specified in the "Details" tab: • lost agents; • duplicated agent; • lost servers; • duplicated servers
Command to remove corrupted entry from LDS	602	A command to remove a corrupted entry from LDS. The removed LDS objects are specified in Details
Replication of OM configuration	603	Replication of the operational management configuration. The following information is specified in the "Details" tab: • computer; • computer SID; • list of modified management objects identifiers: agents and servers
Error in replication of OU configuration	604	An error while replicating the operational management configuration. The following information is specified in the "Details" tab: • computer; • computer SID; • list of modified management objects identifiers: agents and servers; • error description
Software Passport was approved	605	The Software Passport of the workstation was approved. The following information is specified in the "Details" tab: • user; • user SID; • object(s)
Error in approving of Software Passport	606	An error while approving the Software Passport of the workstation. The following information is specified in the "Details" tab: • user; • user SID; • object(s); • error description
Software Passport was removed	607	The Software Passport was removed from the workstation. The following information is specified in the "Details" tab: • user; • user SID; • object(s)
Error in removing of Software Passport	608	An error while removing Software Passport from the workstation. The following information is specified in the "Details" tab: • user; • user SID; • object(s); • error description
Loading of Software Passport project	609	Uploading the Software Passport project to the workstation. The following information is specified in the "Details" tab: • user; • user SID; • object(s)

Name	ID	Description
Error in loading of Software Passport project	610	An error while loading the Software Passport project to the workstation. The following information is specified in the "Details" tab: • user; • user SID; • object(s); • error description
Synchronization of Software Passport	611	Synchronizing the Software Passports of the workstation. The following information is specified in the "Details" tab: • user; • user SID
Error in synchronization of Software Passport	612	An error while synchronizing the Software Passports of the workstation. The following information is specified in the "Details" tab: • user; • user SID; • error description
Software state data collection was started	613	Software state data collection started. The following information is specified in the "Details" tab: • user; • user SID; • computer(s)
Software state data collection was finished	614	Software state data collection finished. The following information is specified in the "Details" tab: • user; • user SID; • object(s)
Error in data collecting	615	An error while collecting software state data. The following information is specified in the "Details" tab: • user; • user SID; • computer; • error description
Error of reading data from DB	616	An error while reading data from the Security Server database. The error description is specified in Details
Error in reading configuration from storage	617	An error while reading the configuration from the storage
Signed container was created for inbound gateway	618	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID; • Gateway name
Error while creating signed container for inbound gateway	619	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID; • Gateway name
Inbound gateway was added to configuration	620	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID; • Gateway name; • Server name; • Full synchronization; • Partial synchronization

Name	ID	Description
Error while adding inbound gateway to configuration	621	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID; • Gateway name; • Server name; • Full synchronization; • Partial synchronization; • Error description
Gateway properties were updated	622	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID; • Gateway name; • Full synchronization; • Partial synchronization
Error while updating gateway properties	623	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID; • Gateway name; • Full synchronization; • Partial synchronization; • Error description
Gateway was deleted from configuration	624	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID
Error while deleting gateway from configuration	625	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID; • Error description
Forced gateway synchronization was performed	626	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID; • Full synchronization; • Partial synchronization
Error while forcing gateway synchronization	627	The following information is specified in the "Details" tab: • User; • User SID; • Gateway ID; • Full synchronization; • Partial synchronization; • Error description

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