



# Secret Net Studio

## **Administrator's manual**

Centralized management, monitoring and audit



© **SECURITY CODE Ltd., 2017. 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 and conditions of the license agreement. This document or any part of it in printed or electronic form cannot be copied or made available to third parties for commercial purposes without express written consent of the SECURITY CODE Ltd.

The information contained in this document can be changed by its developer without advanced notice. This shall not be a violation of obligations with respect to users on behalf of the SECURITY CODE Ltd.

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

# Table of contents

<b>List of abbreviations</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
<b>About the Control Center</b> .....	<b>7</b>
Starting the Control Center .....	7
The Control Center interface .....	8
Connection to the Security Server .....	9
The Control Center settings .....	10
<b>Control structure</b> .....	<b>13</b>
Diagram and list of control objects .....	13
Structure objects .....	13
Filtering objects .....	14
Controlling the display of objects .....	16
OM structure after installation of Secret Net Studio components .....	17
Editing the OM structure .....	18
Adding objects to the OM structure .....	18
Managing the subordination ratio in the OM structure .....	20
Removing objects from the OM structure .....	21
<b>Configuring security settings</b> .....	<b>22</b>
Lists of security settings .....	22
Saving changes .....	22
Configuring settings in the Policies and Event Registration sections .....	23
Policies section settings .....	23
Event Registration section settings .....	23
Applying settings on computers .....	23
Configuring settings in the Parameters section .....	24
Computer registration information .....	24
Network connection settings .....	25
Settings for transferring local logs .....	25
Settings for archiving centralized logs .....	26
Settings for alert notifications mailing .....	27
The Control Center user privileges .....	29
Alert filtering settings .....	29
Secret Net Studio tracing settings .....	31
<b>Monitoring and operational management</b> .....	<b>32</b>
Viewing details .....	32
General status of the system .....	32
Object labels on the diagram .....	32
Details in the hierarchical list of control objects .....	33
Information about the state of objects .....	36
Details in the system events panel .....	36
Tracking alerts .....	37
Notifications about alerts .....	37
Alert acknowledgment .....	38
Resetting alert counters .....	38
Creating filtration rules based on alert notifications .....	38
Operational Management .....	39
Locking and unlocking computers .....	39
Restarting and shutting down computers .....	40
Updating group policies on computers .....	40
Approving changes to hardware configuration .....	40
Collecting local logs at the administrators command .....	41
Controlling the operation of security mechanisms on computers .....	41
<b>Using centralized logs</b> .....	<b>42</b>
Centralized logs .....	42
Alert log .....	42

Combined computer log .....	42
Security server log .....	42
Storing logs .....	43
Local storage of logs .....	43
Centralized storage .....	43
Log archives created by the Security Server .....	43
Panels to work with log entries .....	44
Loading log entries .....	46
Requests for the alert log .....	46
Requests for the stations log .....	48
Requests for the Security Server log .....	49
Requests for log archives .....	50
Configuring request settings .....	51
Controlling requests .....	52
Entry viewing options .....	53
Display event details modes .....	53
Acknowledgment alerts in the log .....	57
Sorting entries .....	57
Searching entries .....	57
Color coding of entries .....	57
Obtaining information about events from external knowledge bases .....	58
Printing entries .....	58
Exporting entries .....	59
Archiving centralized logs at the administrators command .....	60
<b>Configuring and managing centralized software deployment .....</b>	<b>61</b>
Settings and control features panel .....	61
Managing security mechanism licenses .....	61
Configuring deployment .....	63
Creating a list of centrally installed software .....	63
Creating deployment tasks .....	64
Controlling task execution .....	66
<b>Appendix .....</b>	<b>67</b>
Networking settings .....	67
Color coding settings for log entries .....	68
Recovering logs from archives .....	70
Security Server DBMS maintenance recommendations .....	71
Rebuilding indexes .....	71
Monitoring the database size .....	71
Cleaning up the database if it overflows .....	71
Generating and installing the Security Server certificate .....	73
Configuring a secure connection to directory services .....	75
Secure communication with AD LDS .....	75
<b>Documentation .....</b>	<b>77</b>

## List of abbreviations

<b>AD</b>	Active Directory
<b>DNS</b>	Domain Name System
<b>IP</b>	Internet Protocol
<b>RFC</b>	Request for Comments
<b>DB</b>	Database
<b>OS</b>	Operating System
<b>OM</b>	Operational Management
<b>SS</b>	Security Server

# Introduction

This manual is designed for Secret Net Studio administrators (hereinafter "Secret Net Studio, the System"). It contains information about working with the Secret Net Studio – Control Center component. Before reading this manual, read the following documents: [1], [2].

## Conventions

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

Internal links usually indicate the required page number.

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



- This icon highlights additional information that may contain examples, links to other documents, or other parts of the manual.



- This icon highlights important information that must be taken into account.



- This icon highlights a warning.

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

## Other information sources

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

## Chapter 1

# About the Control Center

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

- the system configuration;
- monitoring of the system state;
- network structure configuration of the system;
- operations with centralized logs.



### Note.

The on-premises(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.

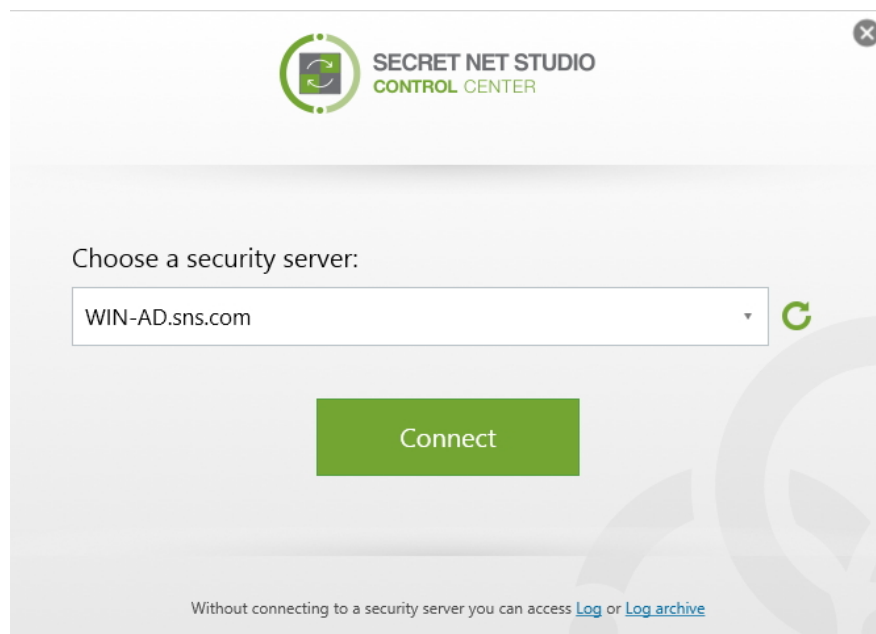
This document describes how to use the Control Center for centralized control. You can perform same functions with the on-premises version similarly.

## Starting the Control Center

### To start the Control Center:

1. Perform one of the following:
  - on a computer running Windows 8 or Windows Server 2012, load the Start screen and click the Control Center element.
  - on a computer with other OS, click the Start button and click the Control Center in 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 to which a connection will be established. 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.

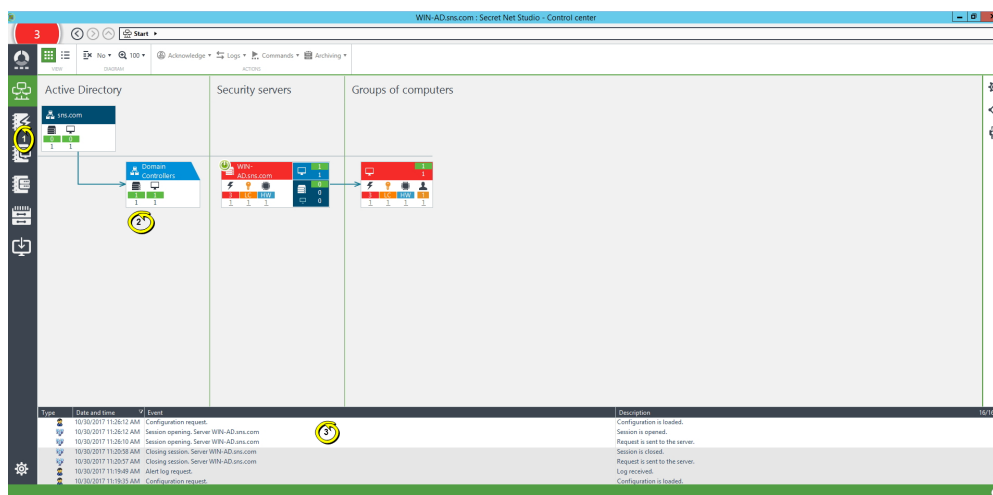
**Note.**

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.

**Comment.**

The figure shows: 1 — the program features navigation panel; 2 — the Computers panel in "Diagram" mode; 3 — the System Events panel.

The Control Center interface has the following parts:

- the program features navigation panel is on the left of the main window and contains shortcuts to control panels and the Control Center configuration tools;
- control panels are designed to display information and perform actions with objects.

The Control Center has the following control panels:

<b>Start</b>
Contains information about the ratio of system alerts and the state of control object groups
<b>Computers</b>
Contains computer administration and management features
<b>Alert Logs</b>
Contains features for loading alert log entries
<b>Station Logs</b>
Contains features for loading stations log entries
<b>Server logs</b>
Contains features for loading Security Server log entries
<b>Archives</b>
Contains features for loading log archives
<b>Deployment</b>
Contains features for configuring automated software installation and updates
<b>System events</b>
Displays details of events involving changes in the state of objects



## 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 re-starting. 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 Settings at the bottom of the navigation panel.

A panel with settings appears as in the figure below.

### Connection to the security server

Manage the program's connection to the security server. View servers available for connection.

WIN-AD.sns.com

Close session




### Configuration


Edit operations management hierarchy. Edit master/subordinate options for security servers and operations management agents.

Edit OM hierarchy...


### Advanced

Refresh operational management configuration.

 Refresh program configuration

 Manage audio alert:

Alert is off

 Stop current alert sound

[Control center settings...](#)

[About](#)

2. In the "Connection to the security 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 "Search for security servers" button on the right.
3. Click "Open Session".

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.

## The Control Center settings

### To configure settings:



1. Click Settings 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 a description of settings, see on p. [67](#)

### The "System events" group

Contains settings for viewing information in the System events panel.

#### The "Number of events field in the "System events" window"

Determines the maximum number of notifications displayed in the System events panel. 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 in the System events window. 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 folder where the Control Center temporary files are located. To specify another folder, type the full path to it or click the button on the right and select the required folder 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 the user's session of working with the Control Center. When work with the program is complete, temporary files from the most recent session are deleted, regardless of the configured storage period

### The "Event colors" group

Contains the settings for log entry color coding by sources of registration, categories or event codes. Formatting is based on preset rules that determine the conditions for the contents of fields in log entries. For a description of how settings are configured, see on p. [68](#).

### 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 "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 (see Step **1** of the procedure described above).

#### The "Sound signal" field

Determines the type of alert sound. A sound adapter should be installed on the computer to play the signal.

This setting can have the following values:

- "Alarm," "Horn" — the selected standard sound signal of the program;
- `<wav - file_name>` — a sound stream from the specified file. To select a file to play, use the standard Open File dialog box. To call the dialog box, specify the value "Choose..."

#### The "Number of signal retries" field

Determines the number of times the signal is repeated. To limit the number of repetitions, select the required numeric value. If "indefinite" is set, the signal will repeat until forced off

#### The "Retry interval" field

Determines the pause between repetitions of the sound signal

**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 "Additional Protection Mechanisms" group**

Contains switches to enable/disable additional protection mechanism not included in the basic distribution kit.

## Chapter 2

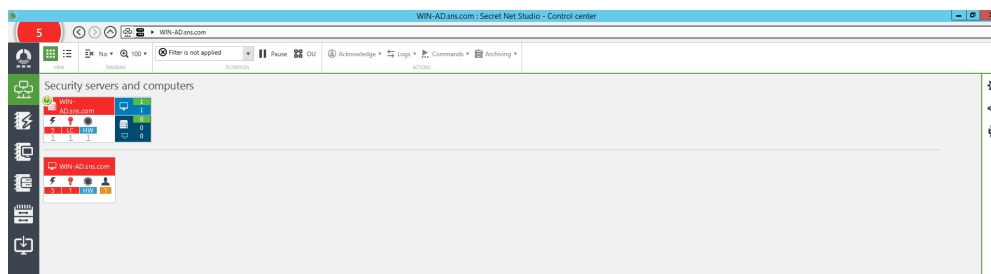
# Control structure

### Diagram and list of control objects

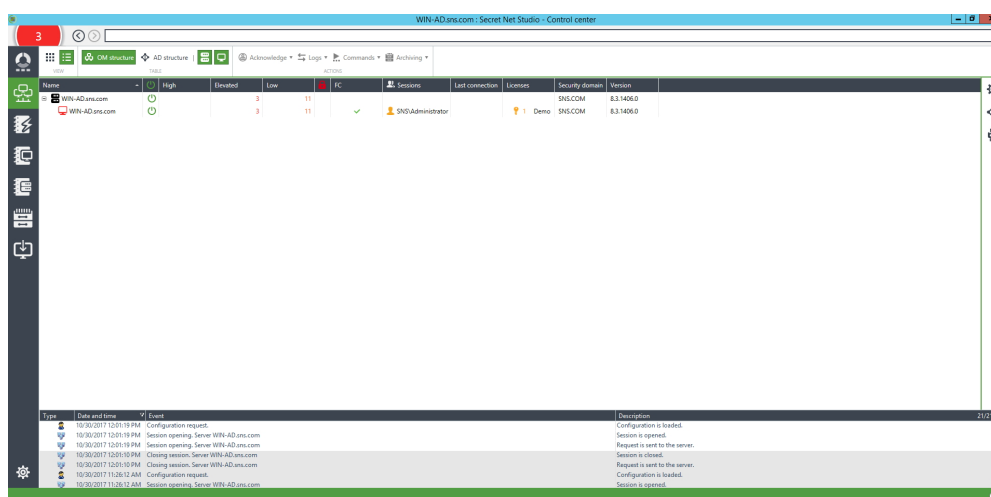
The Computers panel has the following modes for displaying control objects:

- "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, in 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 domains, 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 AD domains and business units appears 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. 8.

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. 13. 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
	Domain or business unit
	Security Server
	Computer or computer group

## Filtering objects

You can limit the number of displayed objects by:

- filtering objects by association with domains and business units;
- filtering computers by their state;
- filtering by object types.

### Filtering objects by association with domains and business units

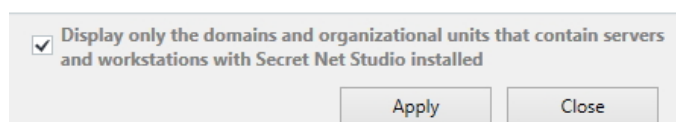
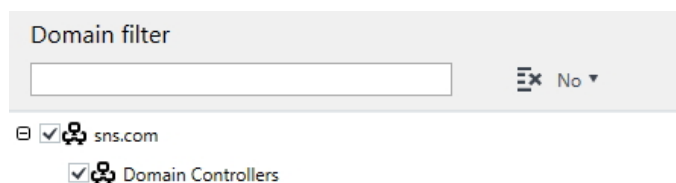
Business units or domains whose objects do not need to be displayed in the Computers panel can be present in AD structure. For example, business units that have no protected computers. If necessary, you can use domain and business unit filtering to disable the display of unnecessary objects. Filtering applies both to the diagram and the table list of objects.

#### To enable the display of objects of specific domains and business units:



1. In the Computers panel, click "AD filter".

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 then Close.

The diagram displays objects related to selected domains and business units.

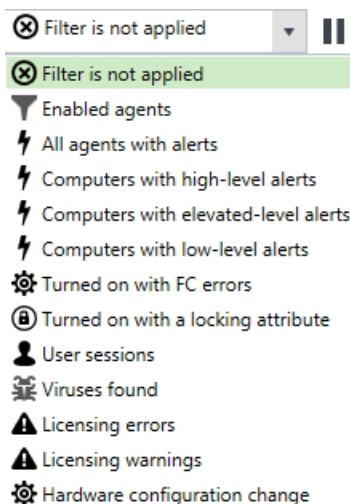
### Filtering protected computers by their state

In the computer list mode (see p. 13), 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. Filtering applies to the diagram.

#### 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 dropdown 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.

#### 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. 13).

#### Using navigation features to move about the OM structure

Navigation features at the top of the program's main window 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.



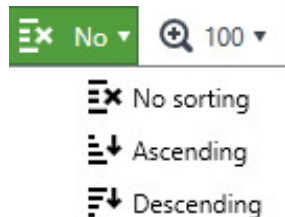
## Sorting objects

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 the 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 the "Grouping by organizational units" button.

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 document [2]. 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.

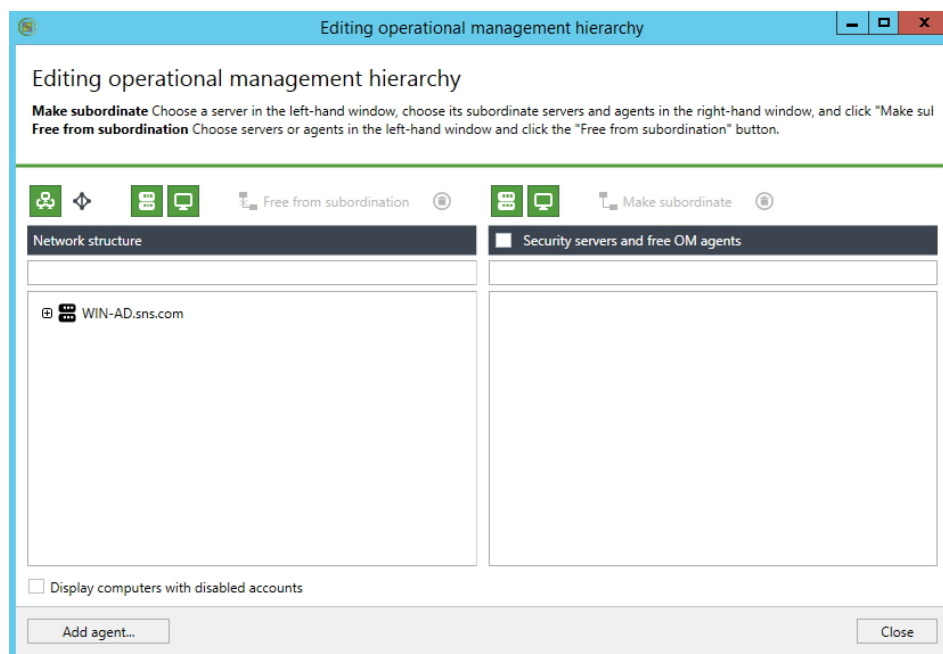
## Editing the OM structure

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 call up the OM structure editing dialog box:



1. Click Settings at the bottom of the navigation panel.  
A panel with settings and configuration features appears.
2. Click "Edit OM Hierarchy".  
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.

#### Note.

If necessary, object lists can be filtered by hiding objects of certain types, accounts that are disabled or whose name do not contain the given string of characters. To filter, use respective elements above object lists (buttons and the field for typing a string of characters for searching) and select or unselect "Display computers with disabled accounts."

3. Generate a structure of objects (see the description of procedures below) 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.

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.

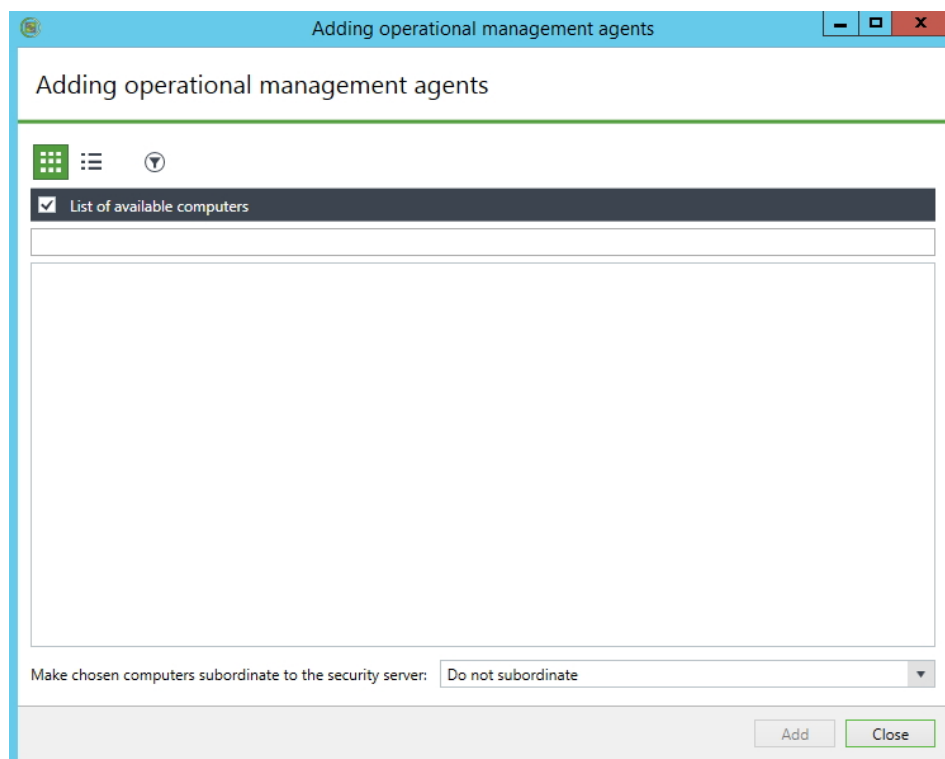
### To add computers:

1. Call up the OM structure editing dialog box (see p. 18).

2. If objects are added and at the same time subordinated to the Security Server, select the server that these will be subordinated to in the Network Structure list (on the left). Select the server from the security domain that the AD container with computers corresponds to.

3. 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 outside the OM structure (the security domain of the selected server is based on the displayed container).

**Note.**

Computers can be listed in a simple or table form. If necessary, the list can be filtered by hiding accounts that are disabled and/or whose names do not contain the given string of characters. List controls are located at the top of the dialog box.

4. In the list, select the computers that are to be added to the structure.
5. To subordinate it to the Security Server, select the computer of the required server in the field "Make chosen computers subordinate to the security server"

**Note.**

Computers can be subordinated later (see p. 20).

6. Click Add.

A dialog box appears as in the figure below where licenses to use the System's components (subsystems) on protected computers can be selected.

## Adding agents

Choose licenses for protection components from the list of available components.  
License set defines which security modules will be enabled on agents.

List of agents	Licenses for protection components
SL-t2-0.testsn7.ru	<ul style="list-style-type: none"> <li><input type="checkbox"/> Base protection 1000 .inst. (left 999), to 01.11.2020, for service ▼</li> <li><input type="checkbox"/> Discretionary Access Control 1000 .inst. (left 999), to 01.11.2020, for service ▼</li> <li><input type="checkbox"/> Data Wipe 1000 .inst. (left 999), to 01.11.2020, for service ▼</li> <li><input type="checkbox"/> Device Control 1000 .inst. (left 999), to 01.11.2020, for service ▼</li> <li><input type="checkbox"/> Application Execution Control 1000 .inst. (left 999), to 01.11.2020, for service ▼</li> <li><input type="checkbox"/> Mandatory Access Control 1000 .inst. (left 999), to 01.11.2020, for service ▼</li> <li><input type="checkbox"/> Printer Control 1000 .inst. (left 999), to 01.11.2020, for service ▼</li> <li><input type="checkbox"/> Firewall 1000 .inst. (left 999), to 01.11.2020, for service ▼</li> <li><input type="checkbox"/> Intrusion Detection 1000 .inst. (left 999), to 01.11.2020, for service ▼</li> <li><input type="checkbox"/> Antivirus Antivirus 1000 .inst. (left 999), to 01.11.2020, fo... ▼</li> </ul>

7. 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.
8. Click Add.

## 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. Re-subordination 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. 18).
2. In the Network Structure list (on the left), select the objects to be withdrawn from subordination.
3. Click "Free from Subordination" Confirm your operation in the dialog box that appears.

The selected objects are no longer displayed in the Network Structure list and 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. 18) or withdrawn from subordination to another Security Server (see above).

#### To subordinate objects:

1. Call up the OM structure editing dialog box (see p. 18).
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 "Security servers and free OM agents" located above the list.
4. Click "Make subordinate".

## Removing objects from the OM structure

Protected computers and the Security Server should only be removed from the OM structure in the Control Center if some components do not work on these computers. For example, due to the System that was an incorrectly removed or when a computer needs to be moved 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. 20) and then reestablish the subordination ratio.

### To remove objects:

1. Call up the OM structure editing dialog box (see p. 18).
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.

## Chapter 3

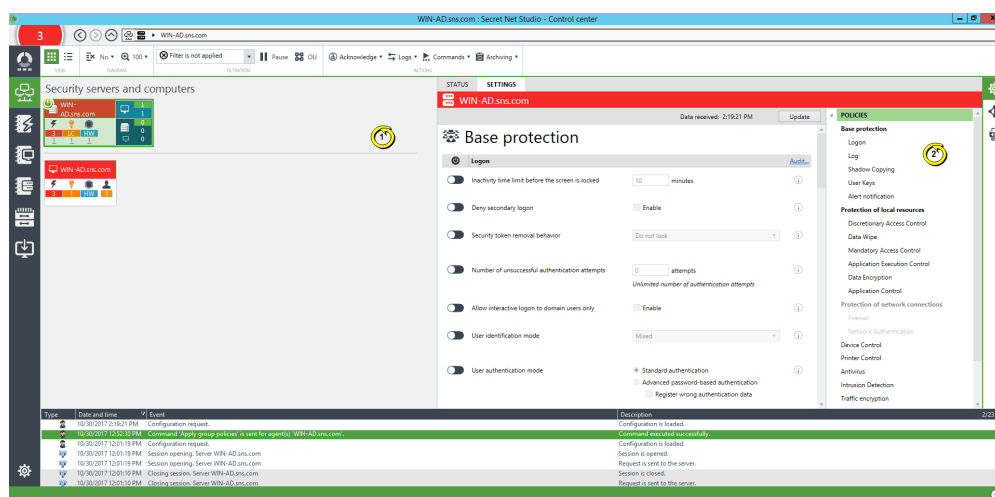
# Configuring security settings

### Lists of security settings

Security settings are managed in the Computers panel on the Settings tab. This tab appears as a panel of object properties. To show or hide the properties panel, right-click the object (for example, the Security Server) and click the Properties command.

To manage security settings of the selected object, first load settings from the Security Server by going to the Settings tab and clicking "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.



#### Comment.

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 delimited with 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 top 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 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

The Policies section includes the following groups of settings:

- Basic security groups ("Logon," "Log," "Shadow Copying," "User Keys," "Alert notification") bring together settings of mechanisms for the Client's basic security;
- Local resources security groups ("Discretionary Access Control," "Data Wipe," "Mandatory Access Control," "Application Execution Control," "Disk Protection and Data Encryption," "Application Control") bring together settings of mechanisms for the Client's local security;
- Network connection security groups ("Network Authentication," "Firewall") bring together settings of mechanisms for the Client's network security;
- The Device Control group contains settings of mechanisms for device connection and modification control and device control;
- The Printer Control group contains settings of the printer control mechanism;
- The Antivirus group contains the antivirus settings;
- The Intrusion Detection group contains settings of the intrusion detection and prevention mechanism;
- The Update group contains settings to automatically check for antivirus database updates.

Details of mechanism configuration are provided in related documents.

If the control of event registration 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 options" 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;
- "Log archival" 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;
- "Tracing management" contains settings for tracing how the Secret Net Studio operates (service function).

## Computer registration information

Computer registration information can be viewed and edited in the "Registration Information" group. This group is available when selecting a protected computer.

When editing registration information, you can specify the importance of the object and enter information about the computer data.

The degree of importance of the object determines the significance assigned to alerts registered on the computer in question. If an object is assigned high importance, incoming notifications of alerts affecting this object will be kept in a higher system. Events with "elevated" and "low" alerts will be interpreted by a "higher" and "elevated" system, respectively.



The information on the computer within the registration information can be edited in the Control Center and locally on the protected computer. For a description of local editing, see document [3].

After changes are made to registration information, click Apply at the top of the Settings tab.

## 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 [3]).

### 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 onp. 67).
2. Click Apply at the top of the Settings tab.

## Settings for transferring local logs

Settings for transferring local logs are managed 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 event, settings can be customized on individual computers and will have a higher priority compared with settings made 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 breaks 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 log collection settings. 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) and prevents logs from overflowing on protected computers (because user access to the computer can be limited if the local log overflows).

### To configure log transfer settings:

1. Configure basic settings in the "Collect logs" tab:
  - If log collection should run every time computers are connected to the Security Server, select "When an agent connects to the security server."

- If logs that are about to overflow should be transferred to the Security Server, select "When filling the log 80% or more."

**Comment.**

Secret Net Studio monitors how full the local log on the computer is once the preset maximum size of the log exceeds 256 KB. It is transferred after confirmation of the Security Servers readiness is received. During the server's peak times, receipt of an overflowing 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."

**Comment.**

Copies of the contents of local logs are kept on the computer as evt-files in \OmsAgentEvtCopy, a sub-folder located in the Client setup folder. These files are managed and deleted by the administrator. Log copying is used for troubleshooting. This feature should be disabled in the normal mode of operation.

4. If the transfer of local logs of connected computers should start at specific times, configure a log collection schedule by selecting the required mode in the drop-down list.

**Periodically**

Log transfer starts at equal 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 the link "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.

## 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:

<b>Periodically</b>
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.
<b>Weekly</b>
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.

**Settings for alert notifications mailing**

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 by e-mail.

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 In/Out category alert occur, notifications are delivered to the system administrator.
- When any alert 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
<b>Edit</b>	Opens a dialog box where you can configure the settings of the selected rule (see below)
<b>Add</b>	Adds a new rule to the list. Settings of the new rule are configured in the dialog box (see below)
<b>Remove</b>	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.

**Note.**

The string of characters you enter should meet RFC 821 requirements.

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.

## 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 "Rule title" field, edit the name for the element in the list of rules.
2. Configure event analysis settings in the Alerts group of fields:

<b>Source</b>
Contains the component or subsystem name specified at event registration as a source. Select the required source
<b>Category</b>
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
<b>Events</b>
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. 44). 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:

<b>Subject</b>
Contains a string that will appear in notifications as the e-mail subject
<b>List of emails</b>
Contains the list of e-mail addresses of notification recipients. Addresses are delimited by ";"
<b>Additional information</b>

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 performing operational management commands
- "Edit policies" — the privilege for managing settings in the Policies and Event Registration sections
- "Acknowledge alert notifications" — the privilege for executing 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

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 privilege for "Edit object hierarchy and parameters," 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 "Edit policies" 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.

## 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. 23), 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 generated as you work in the "Filter of Alerts from Subordinate Servers" group or by using controls in the system events panel (see p. 38).

**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
<b>Edit</b>	Opens a dialog box where you can configure settings of the selected rule (see below)
<b>Add</b>	Adds a new rule to the list. Settings of the new rule are configured in the dialog box (see below)
<b>Remove</b>	Removes the selected element from the list

3. After configuring the rules, enable the filter by clearing the check box next to "Disable filter."
4. Click Apply.

**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:

<b>Source</b>
Contains the component or subsystem name specified at event registration as a source. Select the required source
<b>Category</b>
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
<b>Events</b>
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. 44). Sources, category codes and identifiers of events appear, respectively, in the following fields of the tab: "Source," "Category" and "Events".

3. Click Apply.

## Secret Net Studio 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.

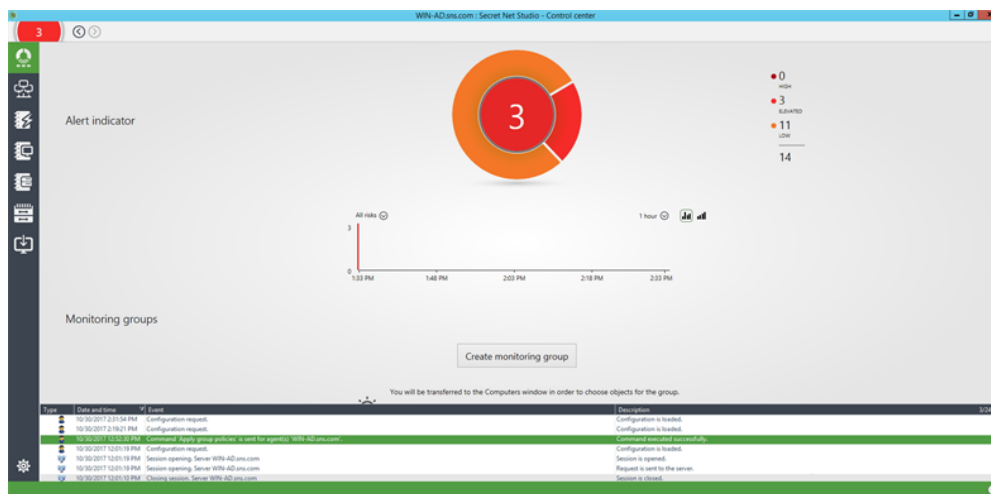
## Chapter 4

# Monitoring and operational management

### Viewing details

#### General status of the system

The Start panel, which is shown in the figure below, contains details of the general status of system security. To view these details, click Start at the top of the navigation panel (on the left in the main window).



There is a round alert indicator showing the overall state of the system in the center of the panel. The inside of the circle shows the number of unresolved alerts with the highest level in the System and is colored accordingly. The outside part shows the ratio of existing alerts of different levels.

All unresolved alerts in the system are listed on the right of the indicator.

#### Comment.

- Numbers in the indicator and the list on the right are hyperlinks. You can click them to view information about these events in the alert log.
- Once acknowledged, these alerts will no longer show up in this panel.
- To find out more about alert levels, seep. [37](#).

Below the alert indicator is a chart of the distribution of registered alerts over a time interval. To select the required interval, use the field with a drop-down list in the top right corner of the chart; to configure the display of alerts by their level, use the field with a drop-down list in the top left corner of the chart.

At the bottom of the panel, there are monitoring groups, which are rectangular indicators with information about the state of computers within such groups. Information shown on indicators is further detailed on p. [32](#).

Initially, the list of monitoring groups is empty. To add items to it, go to the Computers panel and select the required Security Server or computer group. To create new groups and manage their composition, use commands from the Monitoring sub-menu of the context menu in the list of computers (commands are available in "Chart" mode).

#### 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 p. [13](#).





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:

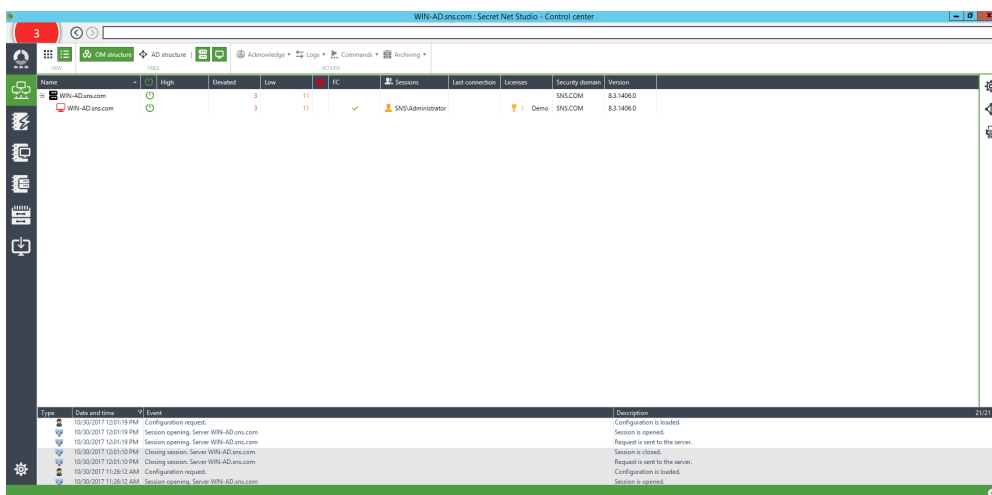
Icon	Description
	The computer/s is/are locked. The number corresponds to the number of reasons for locking. In this example, there is one reason
	A virus was detected on the computer(s). The number represents a counter of registered virus detections
	Alerts were registered on the computer(s). The number 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 a counter of events of the relevant type
	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
	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
	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, on the View tab double-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:

<b>"Power on" icon</b>
Shows the icon if the computer or server is on
<b>High, Elevated, Low</b>
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)
<b>"Lock" icon</b>
Shows the enabled lock icon if the computer is locked. To get more information about the reason for locking, hover the cursor over the cell and information will be displayed in a message box next to the cursor
<b>Functional control (FC)</b>
Shows an icon that corresponds to the result of functional control when the computer starts up. To get more information, hover the cursor over the cell, and information will be displayed in a message box next to the cursor
<b>Sessions</b>
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
<b>Last connection</b>
Shows the time of the last connection to the Security Server for a computer that is off
<b>Licenses</b>
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.
<b>Security domain</b>
Shows the name of the security domain that the object belongs to
<b>Version</b>
Shows the version number of the installed Secret Net Studio software (the Security Server or the Client)

### 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. Click Print.



The settings panel appears as in the figure below.

Print computer list

**Records**  All records  
 Selected

**Detailed information**  add detailed information for computer

4. Configure the information output settings.

<b>"Records" group of fields</b>
<p>This specifies which records will be printed or saved:</p> <ul style="list-style-type: none"> <li>"All records" — the operation is performed for all computers in the list;</li> <li>"Selected" — the operation is only performed for those computers that are selected in the table</li> </ul>
<b>"Detailed information" field</b>
<p>If the check box is selected, the System will additionally provide for computers the information that is not explicitly indicated in the table (for example, the reason for locking)</p>

5. To open the preview page, click "Preview..." at the bottom of the "Print computer list" panel.

#### Note.

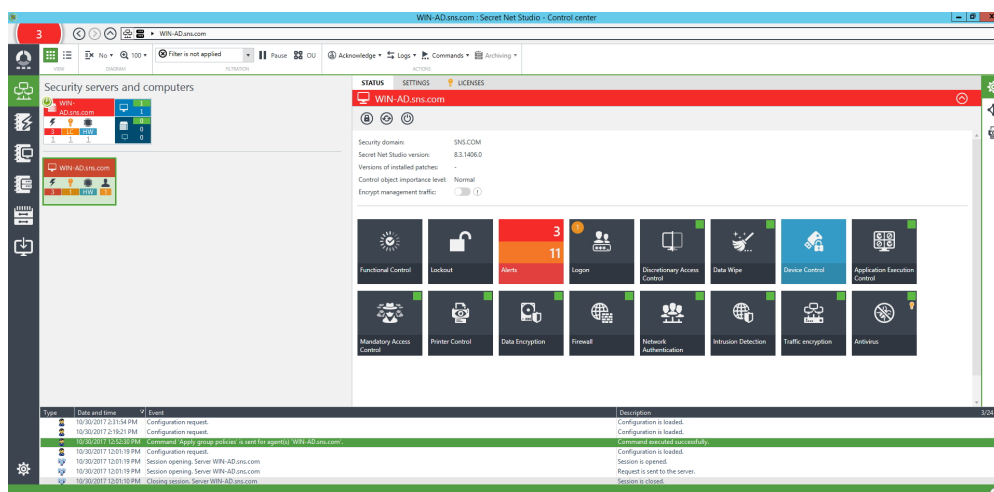
The preview window makes it possible to send a document for printing by using the standard button on the toolbar.

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 Status tab. When information display is enabled, the Computers panel looks like in the figure below.



Key information about the object and security domain that it belongs to and controls available for the object appear 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.

Type	Date and time	Event	Description
	10/30/2017 2:14:44 PM	Configuration request	Configuration is loaded.
	10/30/2017 2:16:21 PM	Configuration request	Configuration is loaded.
	10/30/2017 12:20:19 PM	Configuration request	Configuration is loaded.
	10/30/2017 12:21:19 PM	Session opening, Server WIN-AD.sns.com	Session is opened.
	10/30/2017 12:21:19 PM	Session opening, Server WIN-AD.sns.com	Request is sent to the server.
	10/30/2017 12:21:19 PM	Closing session, Server WIN-AD.sns.com	Session is closed.
	10/30/2017 12:21:19 PM	Closing session, Server WIN-AD.sns.com	Request is sent to the server.
	10/30/2017 4:42:45 PM	Configuration request	Configuration is loaded.

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.);
- "Alert events" are notifications of alert registration on protected computers (for example, "Station alerts").

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 parameters for displaying the data in the system event panel (see p. 10).

## 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 indicators and event distribution charts on the Start 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 the System together 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 on ). 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 using the alert log in the "Alert Logs" panel (see p. 57).

## 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, the system 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. The system 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. 36.

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.

## 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 "Computer locked by the 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. 32). 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.

**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. 32).

**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 when previewing details in the system event panel. To approve the configuration, call up the context menu of the notification "Hardware configuration has been modified on the <computer\_name> agent" and click the "Approve Hardware Configuration" command.



## 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. 25).

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. 36).
3. Click the button of the required mechanism (for example, "Data Wipe").  
A dialog box appears under the button with information about the mechanism.
4. To enable or disable the security mechanism, move the switch on the right 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.

## Chapter 5

# 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 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 [3].

Local logs are delivered for centralized storage to the Security Server database in accordance with the preconfigured settings (see p. 25).

Details received from local logs are saved in full in the combined log. Together with these details, the 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. 25);
- On the command of the Control Center user (see p. 41).



#### 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. 26);
- On the command of the Control Center user (see p. 60).

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.

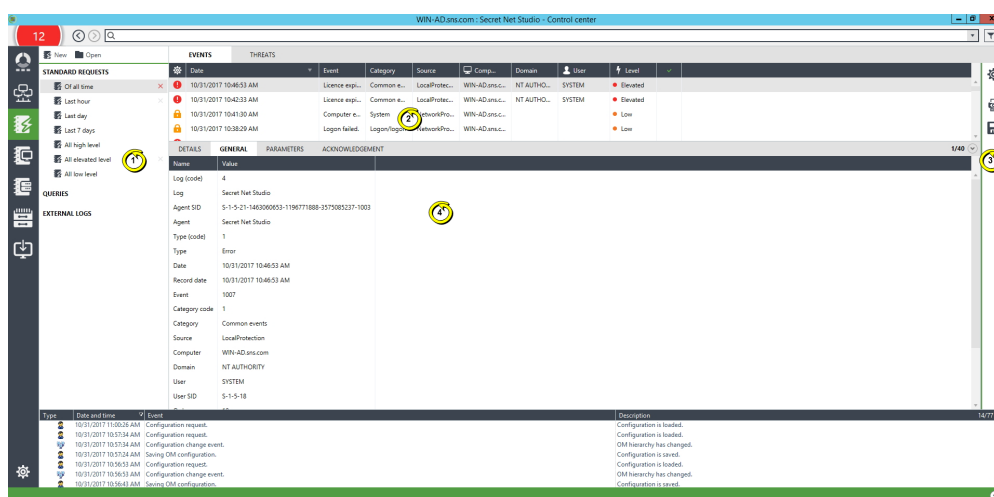
## Panels to work with log entries

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 Log" 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 shortcut 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.

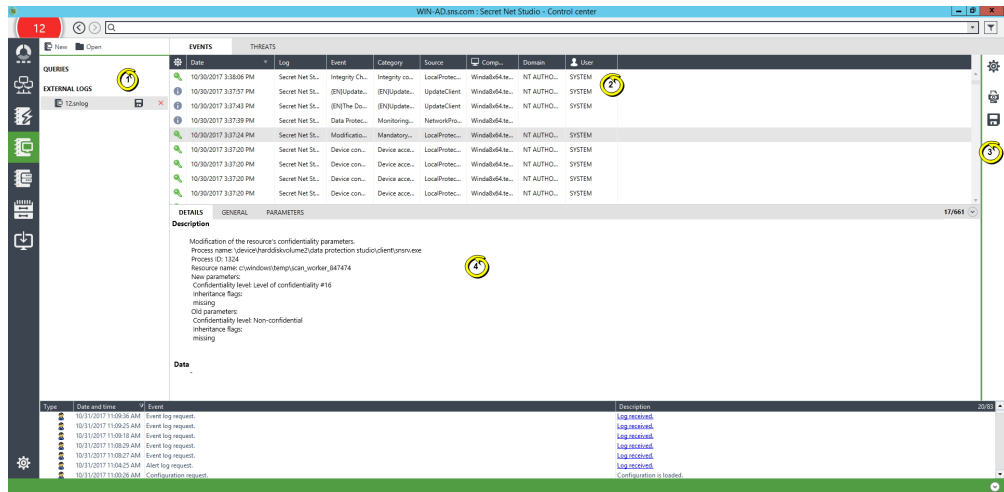
The "Alert logs" panel is shown in the figure below.



### 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.

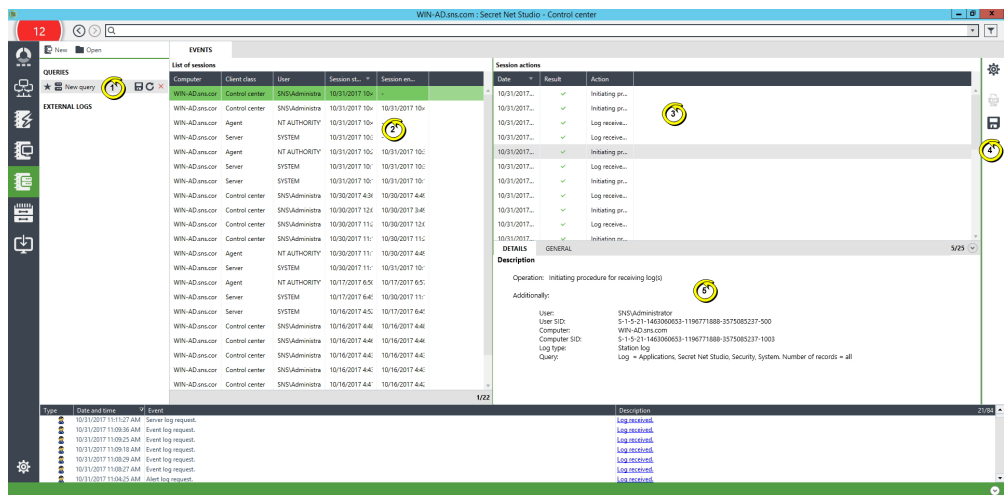
The "Station log" panel is shown in the figure below.



**Comment.**

The figure shows: 1 — the request control panel; 2 — the information pane; 3 — the entry management panel; 4 — the event description pane.

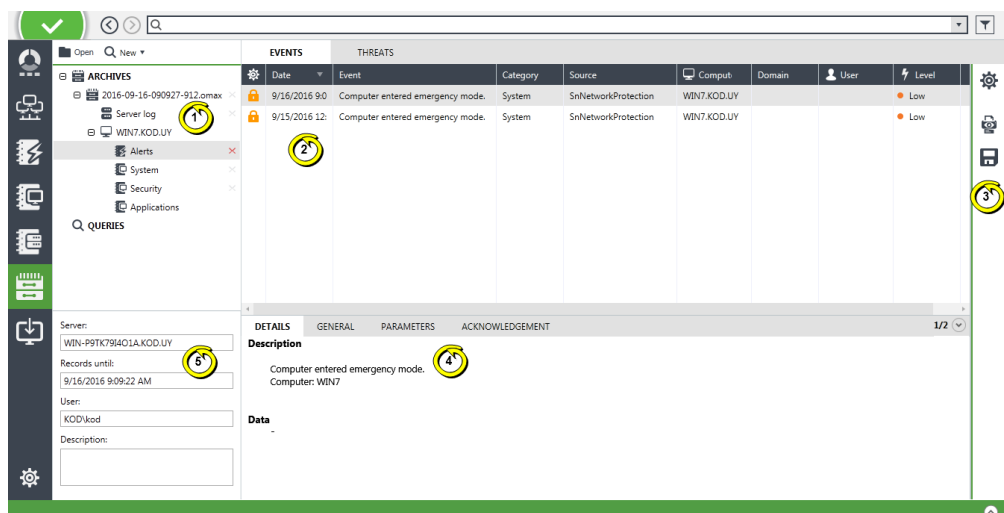
The "Server log" panel is shown in the figure below.



**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:

<b>Request control panel</b>
Contains lists of requests for loading entries. Requests are grouped in the following sections: <ul style="list-style-type: none"> <li>• "Standard requests" are requests with predefined criteria for picking entries loaded from the log (only for an alert log)</li> <li>• "Requests" are requests created by the user to load entries from a log</li> <li>• "External logs" are requests created as entries when loading from files</li> <li>• "Archives" are requests generated as a result of analysis of the contents of loaded archives</li> </ul>
<b>Information pane</b>
Contains information about events in the log in the form of a table with a list of entries.
<b>Panel for information display configuration</b>
Contains buttons for calling configuration controls for requests, printing, and entry export
<b>Event description pane</b>
Contains detailed information about the selected event. Information about events is grouped in the following tabs: <ul style="list-style-type: none"> <li>• "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;</li> <li>• "General" — contains the full list of fields and their values in the entry about a registered event. The list is provided as a table;</li> <li>• "Parameters" — contains the list of Secret Net Studio settings received from a detailed description of the event. The list is provided as a table;</li> <li>• "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.</li> </ul> <p>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.</p>

## 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 Start panel. The system condition indicator, with the total number of alerts (if there are any unacknowledged events), appears in the top left corner of the main Control Center window.

Alert counters on the Start 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. 32 and p. 33).

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. 51) 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. 7), 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. 51).

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. 51) 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. 7) 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 Log panel to configure request settings (see p. 51).

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 Log panel.

#### To create a general request:

1. Click New in the request control panel.  
A new request is created in the Server Log panel and a panel appears on the right to configure its settings.
2. Configure the settings of the new request (see p. 51) 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. 7), or when the program is used in the Server Log panel.

#### To create a request to import entries from the file in the "Server 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 Server Log 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, (un-archiving is performed in the 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. 7), 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:**

- 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.
- Configure settings of the new request (see p. 51) and click Find in Archives. This initiates importing entries from the selected archives.

**Configuring request settings**

To get required information in a log entry request, you can modify entry loading and filtration settings. Settings can be configured in a special settings panel.

**To configure entry request settings:**

- 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.

**REQUEST CONSTRUCTOR**

**Time period**

Of all time  
 Last hour  
 Last 24 hours  
 Last 7 days  
 Last 30 days  
 Set interval:  -

**Alerts**

Level	Acknowledgement	Event type
<input checked="" type="checkbox"/> High	<input checked="" type="checkbox"/> Not acknowledged	<input checked="" type="checkbox"/> Failure audit
<input checked="" type="checkbox"/> Elevated	<input type="checkbox"/> Acknowledged	<input checked="" type="checkbox"/> Errors
<input checked="" type="checkbox"/> Low		

**Last events count**

All events  
 Specify how many:

**Security server data base**

[Switch to advanced mode](#)

- 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.

**REQUEST CONSTRUCTOR**

**Request rules**

Rule	Operator	Condition	
<input type="checkbox"/> Type	Equal	Failure audit; Error	AND OR ⊕ ▾ ✕
<input type="checkbox"/> Threat level	Equal	High; Elevated; Low	⊕ ▾ ✕

**Acknowledgement**  Not acknowledged  
 Acknowledged

**Last events count**  All events  
 Specify how many:

**Security server data base**


- 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 make a sampling of entries from those already loaded, click "Search in results".



## 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.

Button	Description
	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.
<b>Open</b>	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.

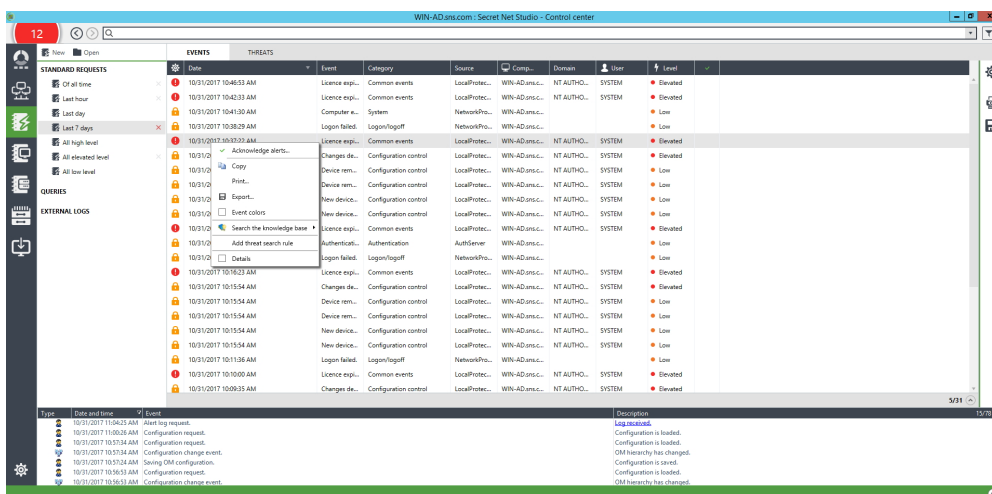
## Entry viewing options

### Display event details modes

Loaded information about events is displayed in the information pane of the respective panel (see p. 44). 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.

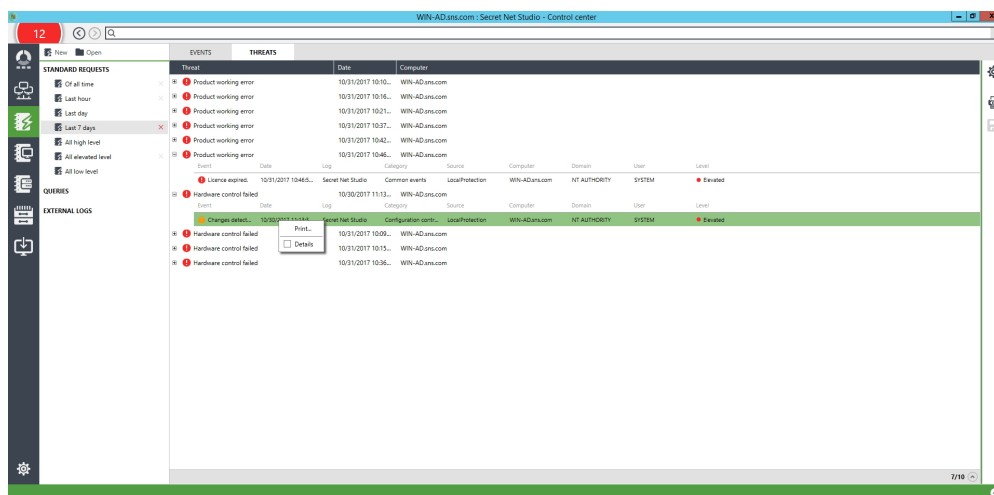


You can use the context menu of entries to perform necessary actions such as copying, printing, saving, etc.

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.

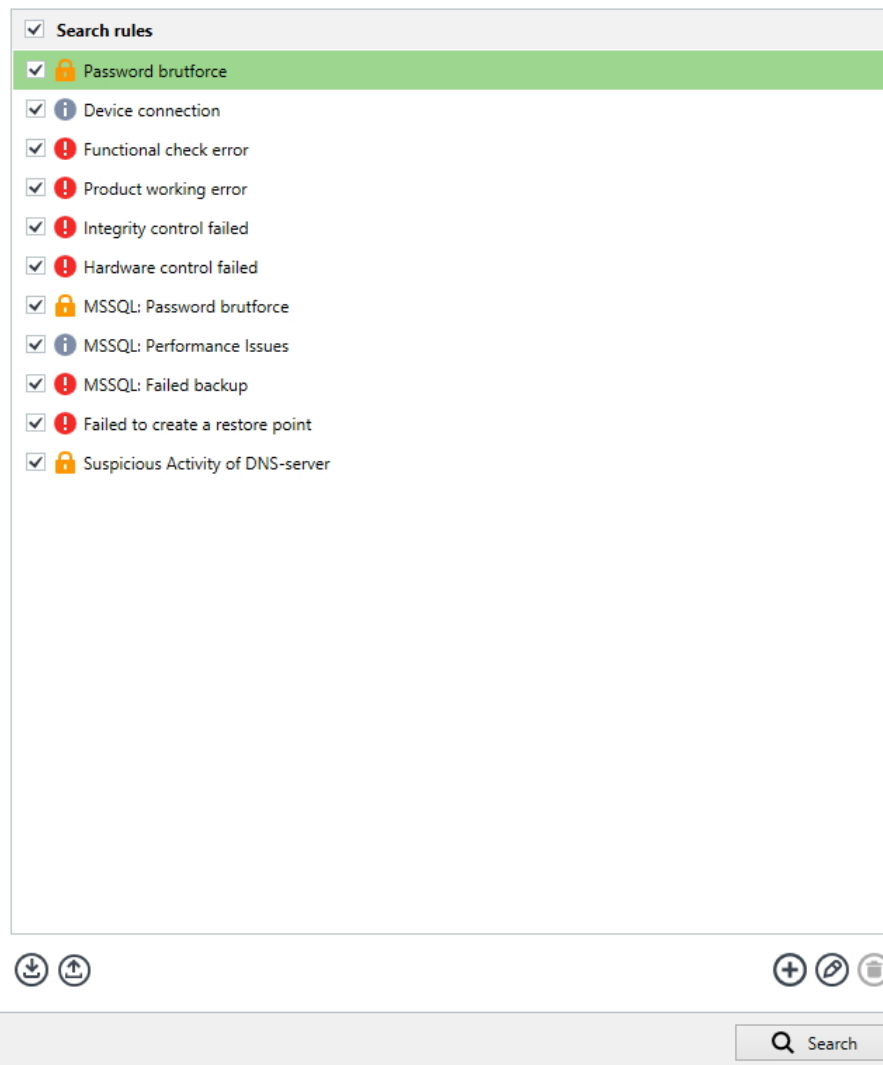
There is a threat counter on the right of the line under the table: <number of the selected event>/<total number of events>.

#### 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.

## THREAT SEARCH

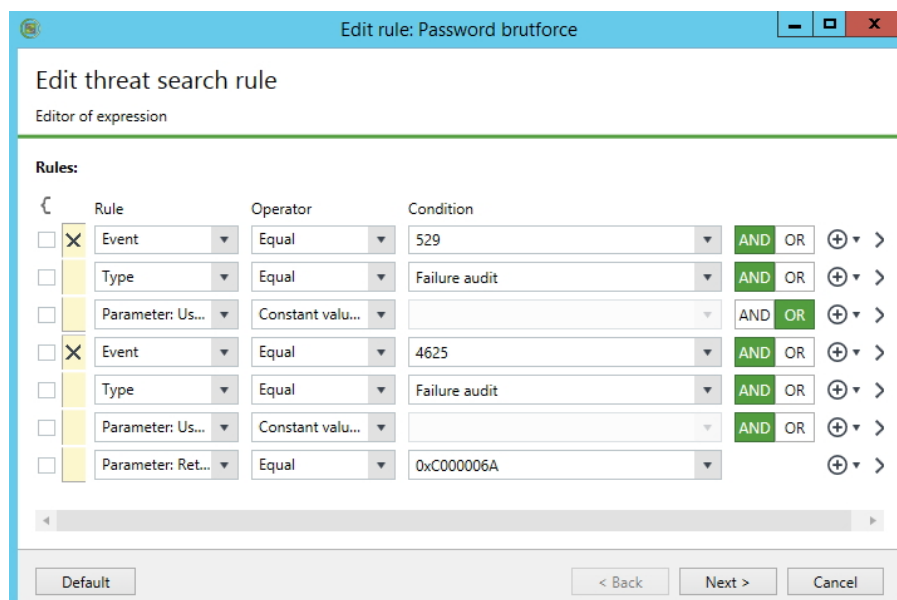


Rules for searching threat events in loaded log entries appear in the list. By default, the list contains preset search rules of a general nature. These search rules cannot be removed from the list.

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)
  - 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, select it from the list and click "Edit Threat Rule" under the list of rules on the right.

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.

**Note.**

If the search rule you are editing is on the list of standard rules, you can return to the configuration of default settings supported for this rule. To do this, click By Default at the bottom of the dialog box and confirm your operation when prompted.

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. 46).
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. 46).
2. Click "Search in Results".

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 on p. 68.

**To enable the color coding mode:**

1. Load log entries (see p. 46).
2. Right-click any entry and click the "Event Color" command.  
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. 46).
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. 46).
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 pane).

The print settings panel appears as in the figure below.

Print log

Records

All records

Selected

Range: from 0 to 0 lines

Detailed information  Add detailed information about events to print

Preview... Print

#### 4. Configure print settings.

"Records" group of fields
Determines entries to be printed: <ul style="list-style-type: none"> <li>"All records" will export the entries displayed in accordance with the current filtering settings;</li> <li>"Selected" will only print the entries selected in the table;</li> <li>"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.</li> </ul>
"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 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 OK.

## 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. 46).
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.

Log export

Path to file  ...

Records

All records

Selected

Range: from  to

Whole log

Export

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.

"Records" 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. 26).

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.

<b>"Events until" field</b>
These fields determine the time interval. Entries registered until this time will be placed in the archive
<b>"Logs" field</b>
This field determines the types of logs whose entries should be archived
<b>"Comment" field</b>
Enter a brief description of the newly created archive in this field

## Chapter 6

# Configuring and managing centralized software deployment

The Control Center supports centralized deployment of the Client on computers. During deployment, the System automatically performs actions specified for installing or removing the Client, its components or updates on computers. The start of software installation or removal on computers is controlled by the Security Server on behalf of a special service.

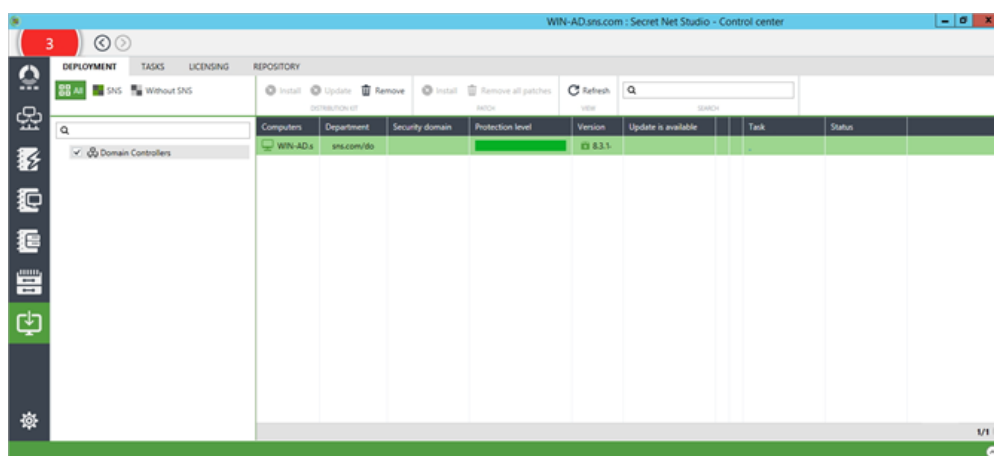


### Attention!

For centralized software deployment, computers should meet hardware and software requirements for the Client installation (see document [2]). Among other things, you should allow the following ports to be used for access to shared resources: 137, 138, 139, 445. By default, these ports are closed by the firewall if there are no shared folders 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 security mechanism licenses

Secret Net Studio system uses license limitations for subsystems that apply security mechanisms. Licenses are delivered as files with data for registration in Secret Net Studio system.

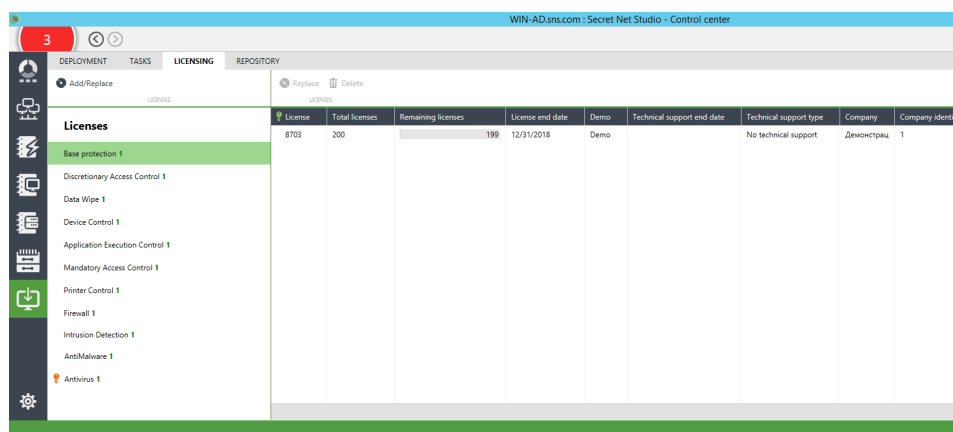
When creating software deployment tasks (see p. 64), specify the relevant licenses. Licenses can be selected from the list of those registered in the System or added separately for the deployment task.

To manage registered licenses, use the Licensing tab in the Deployment panel. The tab contains details of licenses registered in the security domain of the connection server (the Security Server that the program is connected to):

- Purpose of licenses (subsystems these apply to)
- Total number and current number of inactive (remaining) licenses
- Expiration of license features
- License types
- Details of the licensee

### To register licenses:

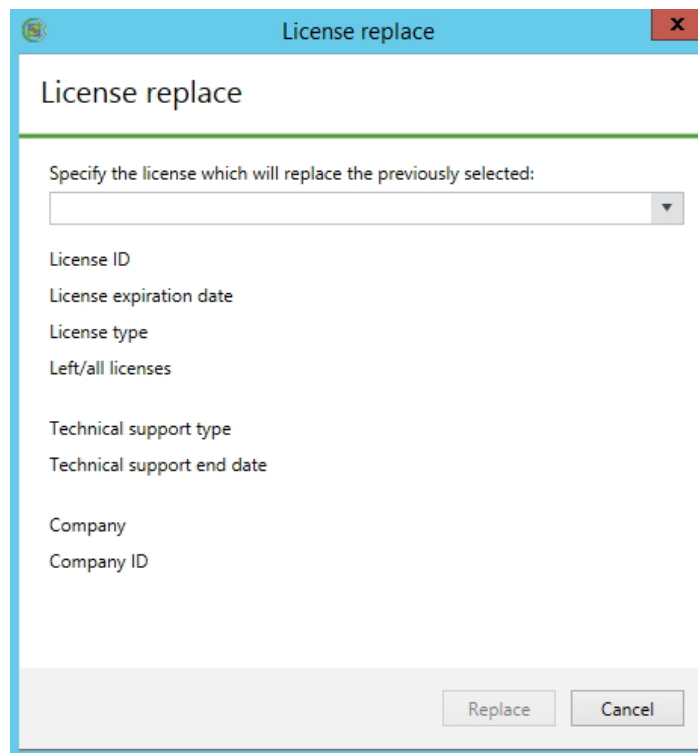
1. Go to the Licensing tab in the Deployment panel.



2. Click Add/Replace above the list of licensable subsystems in the Licenses section. A dialog box appears.
3. Select the required file with licenses.

### To replace registered licenses:

1. Go to the Licensing tab in the Deployment panel.
2. In the Licenses list (on the left), select the subsystem for which licenses should be replaced.
3. In the list of available licenses for the subsystem (on the right), select the license to be replaced.
4. Click Replace above the list of licenses. A dialog box appears as shown in the figure below.



5. Select the license in the drop-down list and click Replace.

**To delete registered licenses:**

1. Go to the Licensing tab in the Deployment panel.
2. In the Licenses list (on the left), select the subsystem for which licenses should be deleted.
3. In the list of available licenses for the subsystem (on the right), select the license to be deleted.

**Note.**

A license that is used on at least one protected computer cannot be deleted.

4. Click Delete above the list of licenses.  
A dialog box appears.
5. Click Yes.

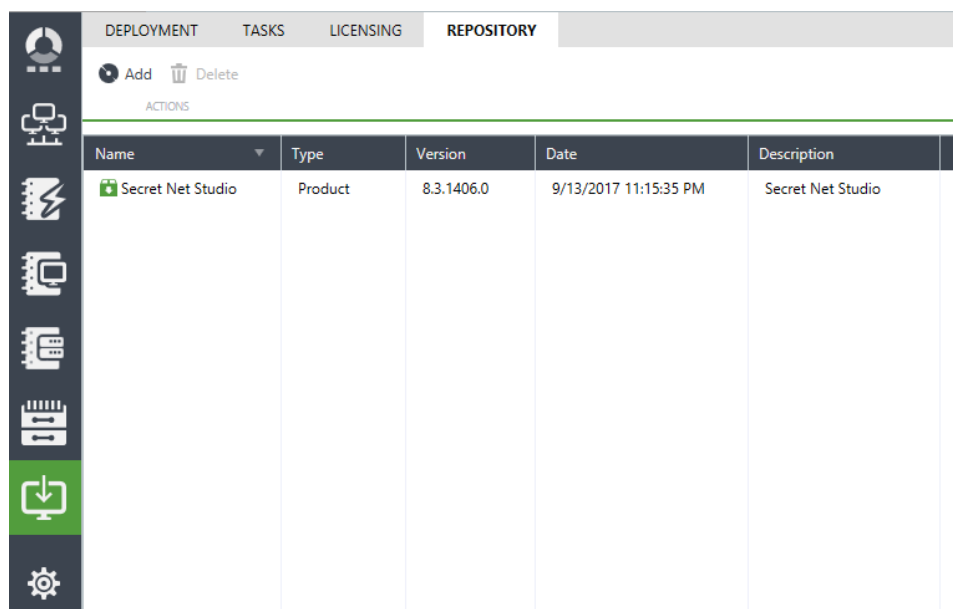
## Configuring deployment

### Creating a list of centrally installed software

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

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

1. On the Deployment tab, click Repository.



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

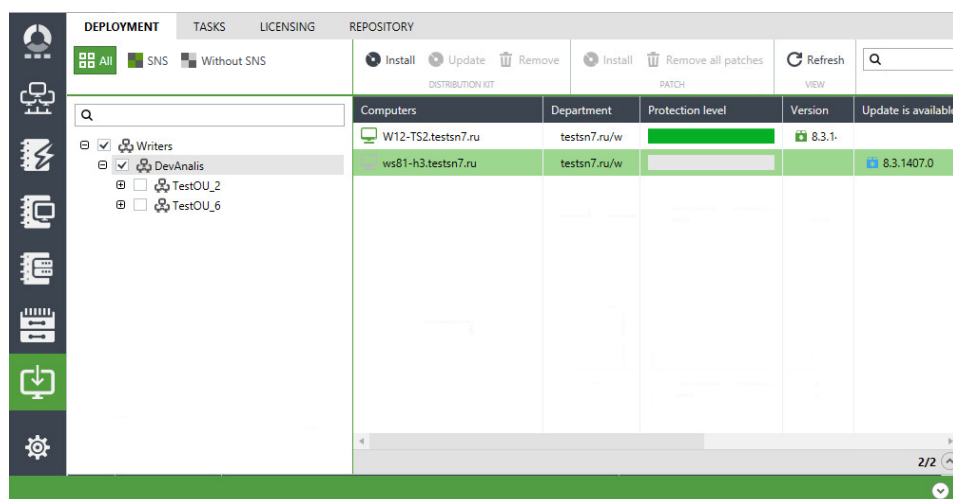
- Right-click anywhere in the list and select Add.  
The Add dialog box appears.
- In the Source Path field, enter or select the path to the folder containing the distribution kit to create the installation package. For example, if you want to use the Secret Net Studio system setup disk to create the installation package, select the installation disk's root folder.  
After analyzing the contents of the specified folder, the remaining fields in the Add dialog box will be automatically filled.
- Click Add and wait until the installation package is created (it may take a while for the files to be sent to the Security Server).  
When the process is complete, a new item appears in the list with information about the installation package.

## Creating deployment tasks

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

### To add a deployment task:

- On the Deployment tab, click Deployment.



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

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



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

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

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

#### Note.

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

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

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

The screenshot shows the 'Distribution kit installation' task settings panel. It includes the following sections and options:

- Task name:** 1 Software installation
- Distribution kit:** 8.3.1406.0 (dropdown menu)
- Subordination to server:** WIN-AD.sns.com
- Installation folder:**
  - Install to default folder
  - Install to chosen folder: C:\Program Files\Secret Net Studio\Client
- Restart timeout after installation:**
  - Not enforced
  - Set time (min.): 15
- Parameters:** (empty text box)
- Security subsystems:**
  - Add licenses from file: Browse...
  - Base protection: 200 ..inst. (left 200), to 12/31/2018 (demo), Дем... +1
  - Discretionary Access Control: 200 ..inst. (left 200), to 12/31/2018 (demo), Дем... +1
  - Data Wipe: 200 ..inst. (left 200), to 12/31/2018 (demo), Дем... +1
  - Device Control: 200 ..inst. (left 200), to 12/31/2018 (demo), Дем... +1
  - Application Execution Control: 200 ..inst. (left 200), to 12/31/2018 (demo), Дем... +1
  - Mandatory Access Control: 200 ..inst. (left 200), to 12/31/2018 (demo), Дем... +1
  - Printer Control: 200 ..inst. (left 200), to 12/31/2018 (demo), Дем... +1

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

Click Install at the bottom of the panel.

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

## 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 document [2]). 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. When a task needs to be delayed:
  - To interrupt execution on all computers, to which the task relates, select it and click Cancel above the tasks list in the Task section;
  - To interrupt execution on individual computers, select them in the list and click Cancel above the list of computers in the Computer section.
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.

# Appendix

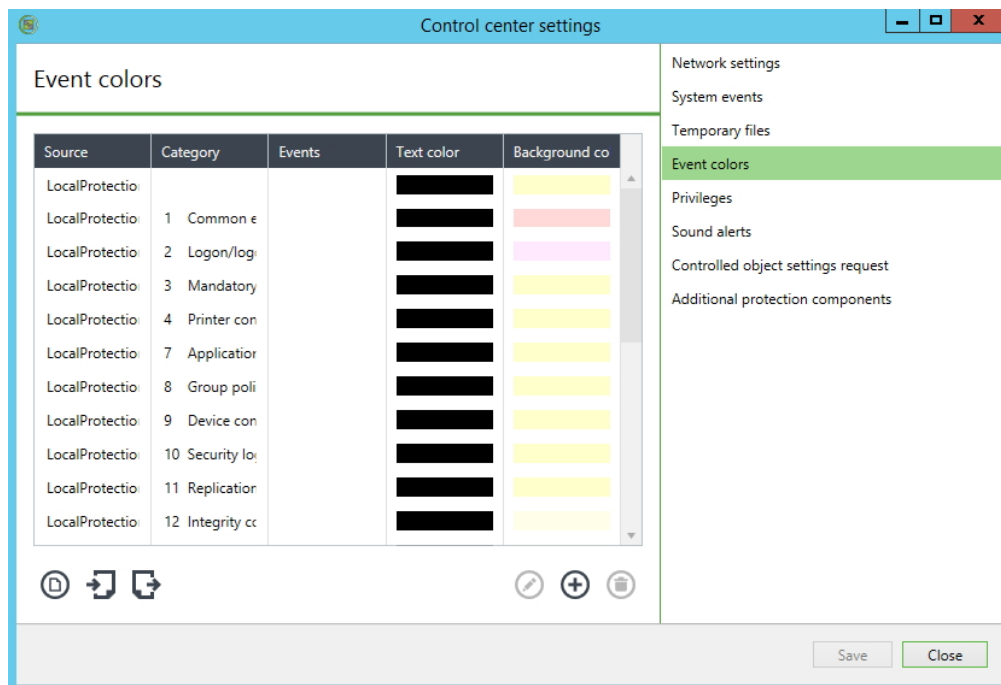
## Networking settings

Description	Range
<b>Timeout settings group</b>	
<b>DNS resolutions</b>	30–1000 sec
<b>Server connections</b>	30–1000 sec
<b>Sending a request to server</b>	30–1000 sec
<b>Completion of transfer of the next block</b> 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
<b>Workstation events</b> 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
<b>For the server getting a response to the watchdog request</b> 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
<b>Block size settings group</b>	
<b>For receiving data from the server</b> 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
<b>For transferring data to the server</b> 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

## Color coding settings for log entries

When configuring program settings (see p. 10), 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
<b>Take default values</b>	Returns the original list of rules used by default
<b>Import</b>	Loads a list of rules saved to a file
<b>Export</b>	Saves the current list of rules to a file
<b>Edit</b>	Opens a dialog box where you can configure settings of the selected rule (see below)
<b>Add</b>	Adds a new rule to the list. New rule settings are configured in the dialog box (see below)
<b>Remove</b>	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:

<b>Source</b>
Contains the component or subsystem name specified at event registration as a source. Select the required source
<b>Category</b>
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
<b>Events</b>
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. 44). 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.

## Recovering logs from archives

Centralized log entries, placed into an archive from the Security Server DB, can be recovered in the server database with the help of the Control Center. Recovered entries can be loaded for view in the same way as for other entries stored in the DB.



### Attention!

Archives may only be recovered by a user with the privilege for "Archiving/recovering 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 "Recover the log archive" command.  
A dialog box appears with a list of recoverable archives.
2. Select the required archive, logs (for an archive that contains several logs) and click Recover.

## Security Server DBMS maintenance recommendations

### Rebuilding indexes

To speed up the processing of requests to the Security Server database, the system automatically creates indexes, special objects, in the DBMS. 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, in turn, will affect server performance.

To maintain a normal database operation, we recommend regularly running the procedure for rebuilding indexes in the DBMS server (on average, once a week). The procedure for rebuilding indexes does not require stopping the server; however, for optimal performance, we recommend running the command at times of minimum load.

To rebuild the index, 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 DBMS server, create a folder on the local disk and copy the contents of `\Tools\SecurityCode\ClearMSSQL\` to it from the setup disk.
2. Open for editing the copied \*.cmd files and specify the database administrator password provided during the setup of the DBMS server. The password must be specified instead of 'manager' substring.

Next, run the 'rebuild.cmd' file at a time of minimum load for the DBMS server. You can use the Windows Task Scheduler to run the file at a specific time.



#### Note.

You can configure the periodical rebuilding of indexes by using standard DBMS server control tools. To do this, create a task for the server to perform the procedure at specific times. An example of a command sequence for this task is provided in `\Tools\SecurityCode\ClearMSSQL\runjob.sql`. You can build a task based on a commands sequence in 'runjob.sql' file by using 'runjob.cmd' file.

### Monitoring the database size

If the Security Server database is hosted in a freeware version DBMS (for example, MS SQL Server 2012 Express), the database size cannot exceed the internal DBMS limit. Depending on the version, the limit may be set to 4 or 10GB.

The Security Server monitors the size of the database. When the database reaches a specific size (by default, 80% of the limit), the server object in the operating control program will be displayed with a special icon signaling that the database is full (see p. 32). In addition, a respective warning will be displayed in the general server settings.

When there is a risk of database overflow, you need to urgently reduce its size. To do this, you can perform emergency archiving of centralized logs by running an administrator command (see p. 60).

### Cleaning up the database if it overflows

If the Security Server database overflows, the database will be locked and the server becomes inoperable. To avoid this, monitor the size of the database (see above) and regularly perform actions to maintain an acceptable database size. In particular, you need to properly configure the automatic archiving of centralized logs (see p. 26).

If the database has overflowed, clean up the database to restore the server.



#### Attention!

Cleaning the database will result in the loss of all information stored in it, including the contents of logs received for centralized storage.

**To clean up the database:**

- 1.** On the Security Server, stop IIS services (WWW Publishing Service) and Secret Net Studio Security Server (server service).
- 2.** If the DBMS server doesn't have a folder with batch files to rebuild the indexes, create such a folder on the local disk and prepare files (see actions **1** – **2** in the section on configuring the rebuilding of indexes).
- 3.** Run 'clear.cmd' file. Once this file is successfully processed, run the procedure for rebuilding the indexes by using the 'rebuild.cmd' file.
- 4.** Restart the Security Server.



## 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. Perform the action in accordance with the version of the installed operating system:
  - On a Windows Server 2012 computer, load the Start screen and select the Certificates element.
  - on a computer with other OS, click the Start button and select the Certificates command in the program menu.

A configuration dialog box appears as in the figure below.

2. In the "Certificate Properties" group of fields, specify the required values.

#### Note.

"Organization" and "Organization Unit" are optional fields.

3. In the "Installation" group of fields, specify the locations of the certificate 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 Yes.

The following dialog box appears as in the figure below.

5. Specify the account data of the user with the right to write to 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 "Default Web Site" 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 Default Web Site 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 SS is installed on a Windows Server 2012 domain controller, the account name includes SecretNetLDS.
  - If SS is installed on a domain controller in another OS, the account name includes SecretNetLDS\$.
  - If SS 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 snap-ins 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).

**Note.**

On a Windows Server 2008 OS computer, instead of exporting and importing, you can copy the certificate along with the private key in the Certificates snap-in. The certificate is copied from the Personal section of the snap-in with computer certificates to sections ADAM\_SecretNet\Personal and ADAM\_SecretNet-GC\Personal of snap-ins with service certificates. After this, you will not have to grant access permissions to certificate key files.

5. Put the CA certificate on computers subordinated to the Security Server in the Trusted Root Certification Authorities section of the storage in the computer context. The certificate can be distributed, for example, with the help of group policies. To do this, use the file with this certificate (if the file is missing, you can create it by exporting the certificate from storage). The certificate file is imported in the group policy snapin to the section Security Settings | Open Key Policies | Trusted Root Certification Authorities.
6. If there is another Security Server, apply the above steps to that server as well.
7. On every Security Server:
  - 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.
  - 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. 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.

# Documentation

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