



SECURITY CODE

# Secret Net Studio

## Administrator's manual

Setup and operation



© **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 setup and operation</b> .....	<b>7</b>
Organization of the System management .....	7
Central and local management .....	7
Using group policies .....	7
Delegating of administrative privileges .....	8
Management tools overview .....	8
Tools only for local management .....	8
Central and local management tools .....	11
<b>Setting up local authentication</b> .....	<b>16</b>
Setting up secure logon mechanism modes .....	16
One-time login in advanced password-based authentication mode .....	17
User password change by the administrator .....	18
System login in the administrative mode .....	19
<b>Setting up hardware support</b> .....	<b>20</b>
Management of personal identifiers .....	20
Main operations with identifiers .....	21
Presenting an identifier .....	21
Initialization of the identifier .....	21
Verification of ownership .....	21
Working with user identifiers .....	22
Viewing information about user identifiers .....	22
Identifier assignment .....	22
Configure identifier usage modes .....	25
Deleting an identifier .....	26
<b>Setting up Integrity Control</b> .....	<b>28</b>
Setup methods and tools overview .....	28
Data Model .....	28
Default model objects .....	29
IC-AEC Management Program .....	29
Synchronizing central and local databases .....	30
Initial setup of IC mechanisms .....	30
Preparing to build a data model .....	30
General configuration procedure .....	31
Building a new data model .....	31
Adding tasks to a data model .....	32
Adding jobs and including tasks to them .....	34
Calculating reference values .....	37
Activating IC .....	40
Checking jobs .....	40
Saving and loading a data model .....	41
Saving .....	41
Change notifications .....	42
Configuring automatic synchronization start .....	42
Forced start of full synchronization .....	44
Downloading and recovering a data model .....	45
Export .....	45
Import .....	46
Making changes in the data model .....	49
Changing object parameters .....	50
Adding objects .....	53
Deleting objects .....	61
Links between objects .....	62
New calculation and reference values replacement .....	62
Disable local jobs .....	63

Searching for dependent modules .....	64
Replacing environment variables .....	64
<b>Audit parameters .....</b>	<b>66</b>
Configuring event registration on computers .....	66
Setting up log parameters .....	66
Selecting events for registration .....	66
Setting up shadow copying storage parameters .....	67
Application control setup .....	67
Granting log access rights .....	68
Privileges for working with local logs .....	68
Privileges for working with centralized logs .....	69
<b>Local audit .....</b>	<b>70</b>
About event registration .....	70
Local event registration logs .....	70
Shadow copy storage .....	70
Storing and deleting local logs .....	71
Local work with logs .....	71
Exporting local log entries .....	71
Viewing the shadow copy storage .....	73
Clearing the local log .....	74
<b>Additional features of the local administration .....</b>	<b>75</b>
Editing a computer's registration information .....	75
Local alert notifications .....	75
Local registration of licenses .....	76
<b>Appendix .....</b>	<b>77</b>
About the Applications and data control program .....	77
Program interface .....	77
Configuring interface elements .....	78
Program parameters .....	79
Tools for object list management .....	81
Using TCP Ports for network connections .....	84
Recommendations for setting Secret Net Studio on a cluster .....	85
Backing up the IC-AEC database using the command line .....	86
Restoring the System after power failure .....	87
Restoring the IC-AEC database .....	87
Restoring the local database .....	87
<b>Documentation .....</b>	<b>88</b>

## List of abbreviations

<b>AD</b>	Active Directory
<b>CRC</b>	Cyclic Redundancy Check
<b>DNS</b>	Domain Name System
<b>FAT</b>	File Allocation Table
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>LFN</b>	Long File Name
<b>MMC</b>	Microsoft Management Console
<b>NTFS</b>	New Technology File System
<b>PCMCIA</b>	Personal Computer Memory Card International Association
<b>PIN</b>	Personal Identification Number
<b>PKI</b>	Public Key Infrastructure
<b>RPC</b>	Remote Procedure Call
<b>RTF</b>	Rich Text Format
<b>SID</b>	Security Identifier
<b>TCP</b>	Transmission Control Protocol
<b>USB</b>	Universal Serial Bus
<b>DB</b>	Database
<b>AEC</b>	Application Execution Control
<b>IC</b>	Integrity Control
<b>LDB</b>	Local Database
<b>DM</b>	Data Model
<b>OS</b>	Operating System
<b>OM</b>	Operational Management
<b>SW</b>	Software
<b>SS</b>	Security Server
<b>CDB</b>	Central Database
<b>EDS</b>	Electronic digital signature

# Introduction

This manual is designed for Secret Net Studio administrators (hereinafter "Secret Net Studio, the System"). It contains information for administrators about the configuration and management of protection mechanisms included in the product's basic protection package. Before reading this manual, read the general information about Secret Net Studio, which can be found in the document [1].

## Conventions

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

Internal links usually indicate the required page number.

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



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



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



- This icon highlights a warning.

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

## Other information sources

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

# Chapter 1

## About setup and operation

Secret Net Studio mechanisms ensure security of computers. The mechanisms make it possible to restrict access to resources and control user activities. The security mechanisms of Secret Net Studio are described in [1].

### Organization of the System management

#### Central and local management

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

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

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



#### Attention!

We recommend you to centrally manage computers with the Client in the network operation mode. Central management has priority over local management. For example, if certain parameters are set centrally in the group policy, they cannot be changed locally on the computer.

#### Using group policies

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

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

The group policy parameters are applied in the following sequence:

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

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

Group policy parameters are configured using the Control Center. For more details about how to use the Control Center, see [4].

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

## Updating group policies

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

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

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

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

## Delegating of administrative privileges

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

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

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

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

## Management tools overview

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

### Tools only for local management

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

Tools that are only used for local management are as follows:

- Secret Net Studio icon in the Windows Control Panel;
- Secret Net Studio dialog box in the window for resource properties setup;



- program for making additional settings to the mandatory access control subsystem;
- "Secret Net Studio settings" dialog box in the Windows Control Panel.

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

- the Control Center in the local mode (installed as part of the Client);
- user management program (to set parameters for local users);
- Applications and data control program in local operation mode.



#### Note.

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

### Secret Net Studio icon

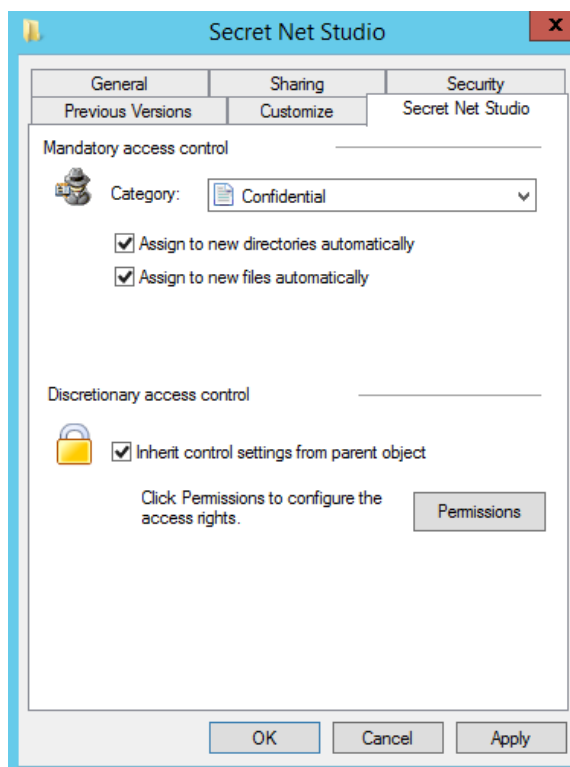


After installing the Client, Secret Net Studio icon appears in the notification area of the taskbar. The icon is designed to notify the user about the availability of active security, to launch main user control commands and to receive data.

### Secret Net Studio dialog box

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

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



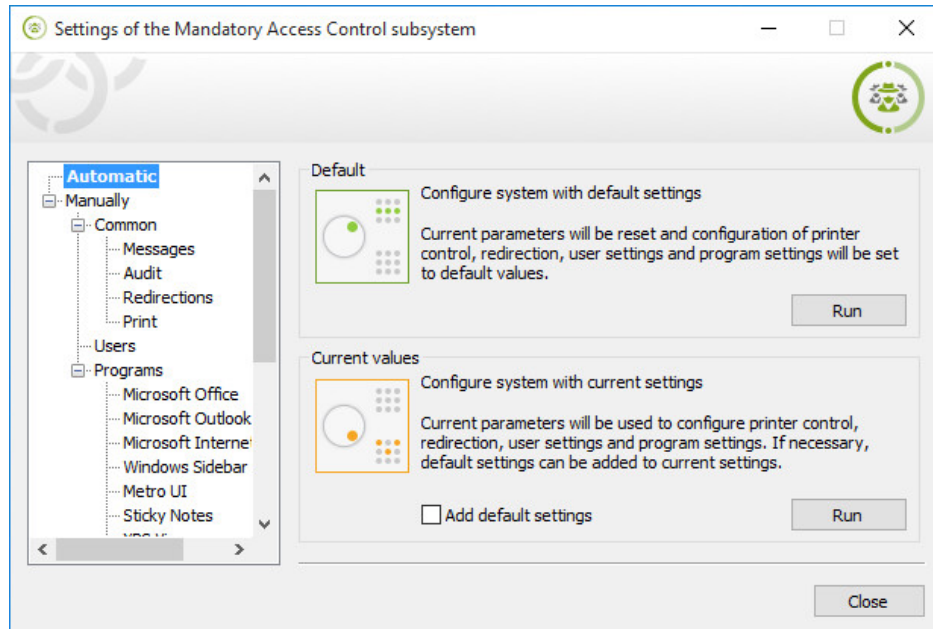
### Setup program for the mandatory access control subsystem

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

To start the program, perform one of the following:

- on a computer running Windows 8 or Windows Server 2012, load the Start screen and click the "Mandatory access control configuration" element;
- on a computer running other OS, click the Start button and click "Mandatory access control configuration" in the Secret Net Studio menu.

The program window is shown in the figure below.

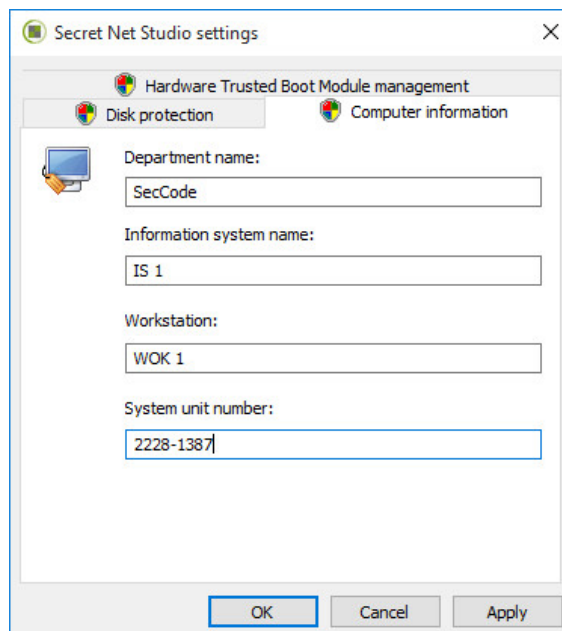


The setup procedure for the mandatory access control subsystem is performed by the administrator.

### **"Secret Net Studio settings" dialog box in the Windows Control Panel**

The "Secret Net Studio settings" dialog box makes it possible to view and edit general system information for local management of the operation of security mechanisms and hardware security tools.

The dialog box can be called up from the Windows OS Control Panel.



## Central and local management tools

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

Central management tools are as follows:

- management software;
- user management software;
- Applications and data control software.



### Note.

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

## Management Program

The Management Program is installed as a separate component of the Control Center for working in the centralized mode or as part of the Client for operating in the local mode.

When working in the centralized mode, the program makes it possible to manage computers from the administrator computer, workstation, to monitor and view logs saved in the Security Server database. To work with the program, you need to establish a connection with the Security Server. There is also an option to start without a connection to the Security Server for working with logs.

When using the management program in the local mode, only local computer control functions are available and only local logs and logs saved in files can be viewed.

To start the program in the centralized mode, perform one of the following:

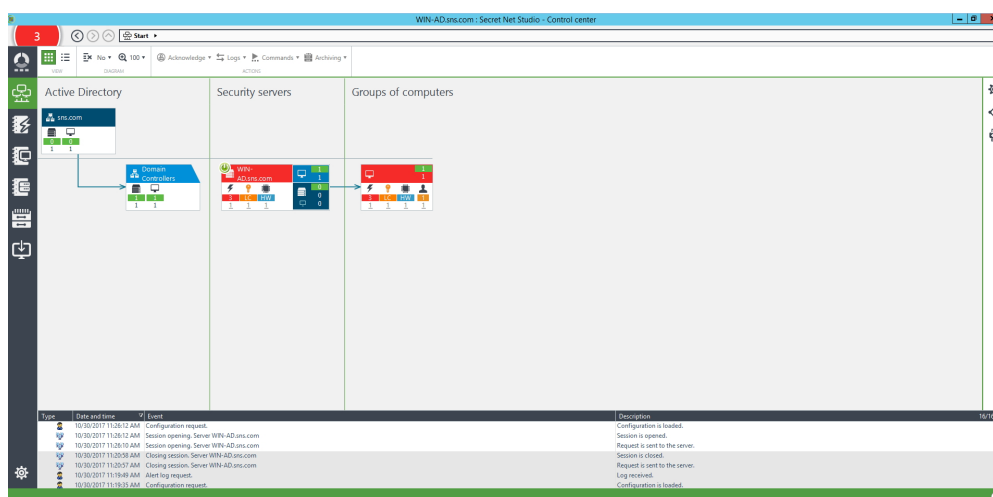
- on a computer running Windows 8 or Windows Server 2012, load the Start screen and click the Control Center element.
- on a computer with other OS, click the Start button and click the Control Center in the program menu.

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

To start the program in the local mode, perform one of the following:

- on a computer running Windows 8 or Windows Server 2012, load the Start screen and click the Local Control Center element;
- on a computer running other OS, click the Start button and click the Local Control Center in the program menu.

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



For more information, see [4].

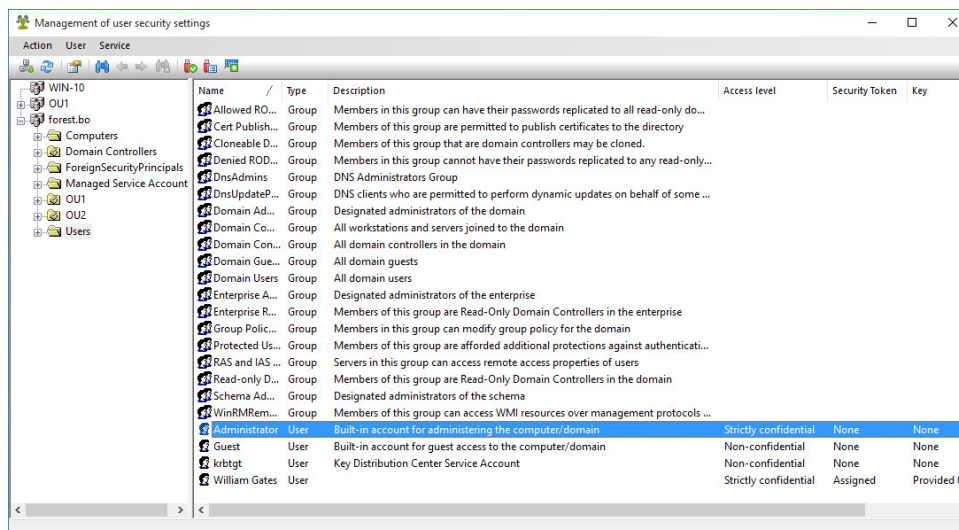
## User Management Program

The User Management Program makes it possible to configure user operation parameters within the System. Actions with both domain and local users can be performed using this program.

To start the program, perform one of the following:

- on a computer running Windows 8 or Windows Server 2012, load the Start screen and click the User Management element;
- on a computer running another OS, click the Start button and click the User Management command in the program menu.

User Management Program window is shown in the figure below.



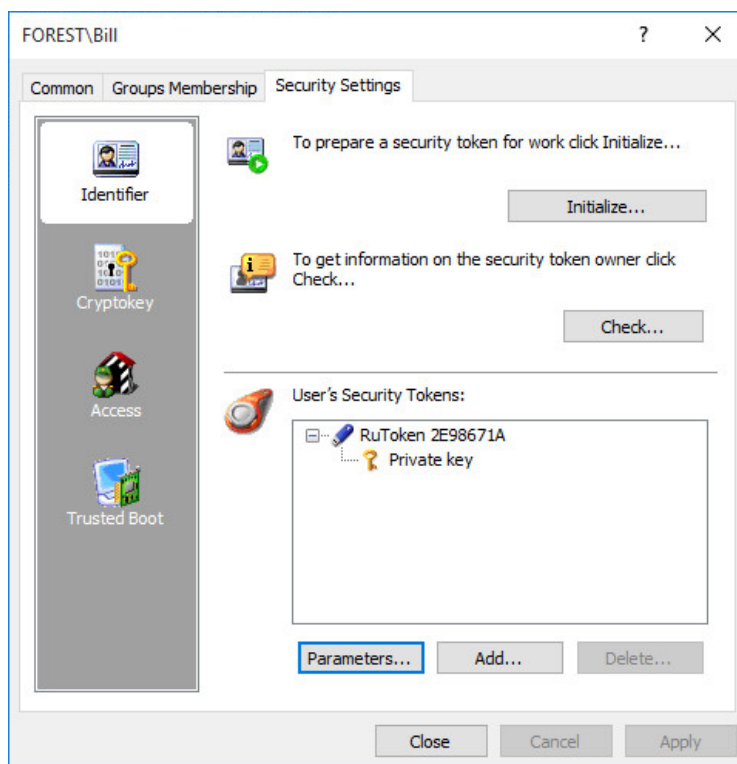
The program interface is similar to the standard interface of Active Directory – Users and Computers. The left-hand part of the window displays a list of containers (the current computer and the structure of sections and organizational subdivisions of the domain), and the right-hand side displays the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

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

### Tip.

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

User parameter management for working in the Secret Net Studio system is performed on the Security Settings tab as shown in the figure below.



### Applications and data control program

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

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

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

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

#### To start the program in the centralized mode:

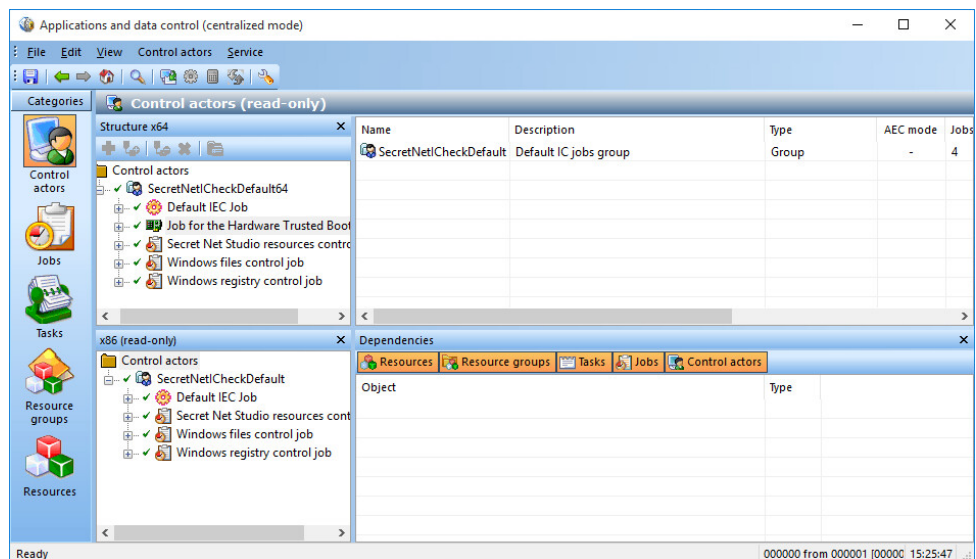
1. Perform one the following:
  - on a computer running Windows 8 or Windows Server 2012, load the Start screen and click the "Applications and data control (centralized mode)" element;
  - on a computer running other OS, click the Start button and click the "Applications and data control (centralized mode)" in the program menu.

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

2. If full access to the CDB is not possible (the management program of the IC-AEC is already working in the centralized mode on another computer with an OS of the same architecture), a message appears with a request to perform further actions. The following options are available:

- cancel the program start (recommended) – to do so, click the Cancel button in the query dialog box;
- start the program with access to the CDB of the IC-AEC in read-only mode – to do so, click the No button in the query dialog box. In this case, the latest data model saved in the CDB will be uploaded to the program. It will not be possible to edit the model;
- start the program and receive full access to the CDB – to do so, click the Yes button in the query dialog box. Any other user currently working with the IC-AEC on another computer will not be to write in the CDB and save changes.

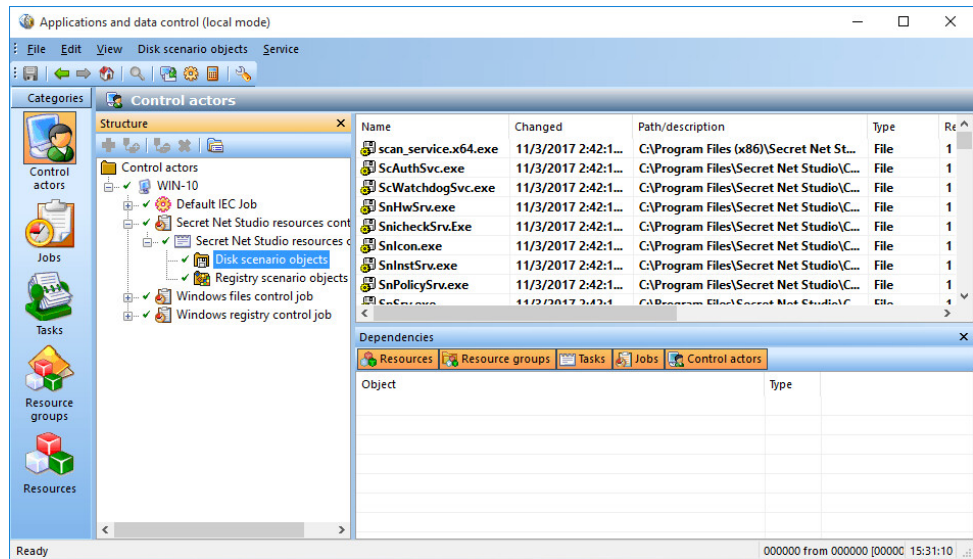
The program window in the centralized mode is shown in the figure below.



#### To start the program in the local mode:

- Perform one of the following:
  - on a computer running Windows 8 or Windows Server 2012, load the Start screen and click the "Applications and data control (local mode)" element;
  - on a computer running another OS, click the Start button and click the "Applications and data control (local mode)" command in the program menu.

The program window in the local mode is shown in the figure below.



## Chapter 2

# Setting up local authentication

### Setting up secure logon mechanism modes

A secure logon mechanism is defined by several factors which govern the work of the respective modes.

The description of the centralized setup procedure in the Control Center is provided below (see p. 11). Local setup is performed similarly to the use of the Management Program in the local mode.

#### To set up secure login mechanism modes:

1. In the Control Center, in the Computers panel, select the object you want to configure. Right-click the object and click Properties. In the properties panel, click the Settings tab and click "Load Settings".

#### Note.

For details about the Control Center, see document [4].

2. In the Policies section, select the "Logon" group of parameters.
3. Set up the following parameters.

<p><b>Inactivity time limit before the screen is locked</b></p> <p>Determines the maximum inactivity period before the computer is automatically locked by Secret Net Studio.</p> <p>For security reasons, in case of long user inactivity, the computer should be locked. Locking after the expiration of a certain inactivity period is performed by Secret Net Studio. Using standard operating system tools users can specify a different period for locking the computer (screen-saver activation), which should be shorter than that specified by the value of this parameter. Otherwise, the OS parameter will not be valid.</p> <p>If the value is "0", Secret Net Studio tools will not lock the computer</p>
<p><b>Deny secondary logon</b></p> <p>If this mode is enabled, the start of commands and network connections is blocked the user account user who did not perform an interactive logon.</p> <p>After enabling the mode, you should eliminate the possibility of using previously saved logon information. To do this, enable standard Windows OS security parameter Network access: do not allow password and login information storage for network authentication (parameter name may slightly differ depending on the OS version)</p>
<p><b>Security token removal behavior</b></p> <p><b>Do not lock</b> – the computer is not locked if the security token is removed from the reader.</p> <p><b>Lock computer if USB security token is removed</b> – the computer is blocked if the USB key or smart card used to log into Secret Net Studio is removed from the reader (for example, eToken).</p> <p><b>Lock station if any security token is removed</b> – the computer is locked if any of the security tokens supported by Secret Net Studio for user authentication are removed from the reader (eToken, etc.).</p> <p>The locking function is used if the security token was activated by Secret Net Studio and if the user provided this security token to enter the system</p>
<p><b>Number of unsuccessful authentication attempts</b></p> <p>Limits the number of failed login attempts per user in the advanced password-based authentication mode. When the limit is reached, the computer is locked and login is only enabled for the administrator.</p> <p>If the value is zero, this limitation is not applied.</p>
<p><b>Allow interactive logon to domain users only</b></p>



If this mode is enabled, only those users who are registered in the domain can login to the system. Interactive logon of local users (including local administrators) will not be allowed. This parameter is absent if locally configured on the computer with the Client in standalone mode

#### User identification mode

**By name.** To enter the system, the user must provide credentials using only standard Windows OS methods.

**Mixed.** To enter the system, the user may provide a security token activated by Secret Net Studio or use standard Windows OS identification methods.

**Only by identifier.** To enter the system, the user must provide a security token activated by Secret Net Studio. Users without personal security tokens cannot log into the system. The Administrator can only enter the system without presenting a personal security token in administrative mode (see p. 19).

In **By name** and **Mixed** logon modes, the user can process USB keys and smart cards using standard Windows OS methods (see documentation for Windows OS). In the **Only by identifier** mode, personal security tokens activated by Secret Net Studio are used, but not those activated by Windows OS

#### User authentication mode

**Standard authentication** — only standard Windows OS authentication is performed.

**Advanced password-based authentication** — apart from standard Windows OS authentication, password-based authentication will also be performed by Secret Net Studio. If the user's password is saved in the Secret Net Studio database, the user will not be able to log into the system. The administrator may allow a one-time login for the user to save the password by enabling the Trust Windows password authentication parameter of the dialog box for user properties settings.

Login is only allowed if the entered password matches the saved password. If the "Register wrong authentication data" mode is enabled, the incorrectly entered password is saved in Secret Net Studio log as an encrypted character string

#### Password policy

Defines active requirements for user passwords in the advanced password-based authentication mode. The requirements coincide with the parameters of the Windows password policy if the "Use values from the Windows password policy" mode is enabled. If necessary, special requirements may be applied for passwords saved in the Secret Net Studio database (irrespective of Windows password policy parameters). To do this, select the "Set custom values" mode and define requirements similar to standard Windows password policy requirements: Minimum password length, Password expiration and Passwords complexity requirements. Moreover, the computers will eventually use the strictest requirements from those assigned in the Secret Net Studio policies and Windows settings

4. Set up the registration of events related to the operation of the mechanism. To go to the required group of registration settings, click the Audit link in the right part of the group heading.
5. Click Apply at the top of the Settings tab.

## One-time login in advanced password-based authentication mode

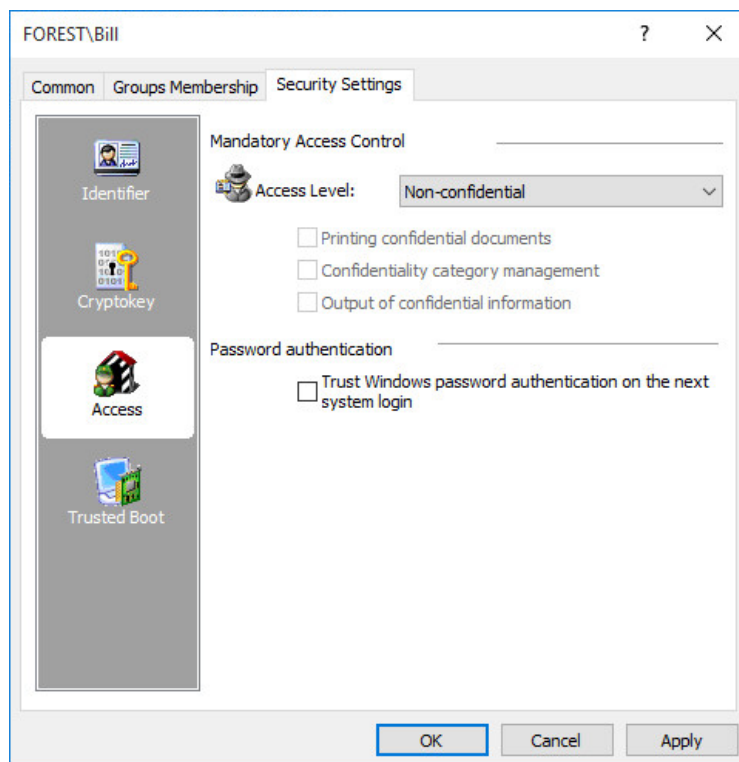
If the advanced password-based authentication mode is enabled Secret Net Studio will additionally perform password-based authentication for the user to login. For this purpose, the user's password must be saved in Secret Net Studio system database. The password is saved when the password is changed by the administrator or by the user if the mode was enabled during the user's working session.

If the current password needs to be saved in the Secret Net Studio database, the administrator can grant the user the permission for one-time login in order to enter and save the password. After the user enters the System, this permission is disabled automatically, and this user can use advanced password-based authentication.

#### To enable a one-time login:

1. Launch the user management program (see p. 12).

2. Call up the setup window for user properties and select the "Security Settings" tab.
3. Select the Access group.



4. Select the "Trust Windows password authentication on the next system login" check box.
5. Click OK.

## User password change by the administrator

User passwords can be changed by the user or by the administrator. Password change by the user is described in the document [8].



### Attention!

For the Client in the network operation mode with the enabled advanced password-based authentication mode (see p. 16), the administrator can only change the user's password in the user management program. In this case, to perform the procedure, the administrator may need additional rights granted during the delegation procedure (see p. 8). If the administrator changes the user's password with other tools, the new password will not be saved in the Secret Net Studio database, which makes it impossible for the user to log into the system with that password.

### To change a user's password:

1. Launch the user management program (see p. 12).
2. Right-click the user in the users' list and click the Password change command.  
A dialog box asking you to change the password appears.
3. Enter a new user password and click OK.  
If the user's password is stored in personal security tokens, a dialog box with a list of personal security tokens belonging to this user appears.
4. Present all listed security tokens (see p. 21).  
The new password is saved in the security tokens, and their status changes to Processed. The Cancel button changes to the Close button.

### Note.

If there are violations when connecting to security tokens, an error message will appear in the table in the Status column.

5. Click Close.

## System login in the administrative mode

In the standard mode of Secret Net Studio operation, all computer users should log in following the same rules defined by the respective security mechanisms. When the computer is booting, before the user's login, the System initializes the security subsystems and performs functional control. After all checks are complete, you can log into the system.

The administrator can activate the administrative login mode if there is a need to access the computer beyond the defined rules or to interrupt the initialization process of the subsystems.

An administrative login mode may be necessary in the following situations:

- when the "Only by identifier" logon mode is enabled if the administrator has no personal security token;
- in the case of repeated functional control errors which lead to delays for initialization of security subsystems.



### Attention!

The administrative login mode should only be used as a last thing for restoring the system's normal operation. Log into the System in the administrative login mode, fix the problem and restart the computer.

### To log into the system in the administrative login mode:

1. Restart the computer.
2. When initialization messages of Secret Net Studio services appear during startup, press <Ctrl> + <Shift> + <Esc> .
3. When you see the Welcome screen (log in prompt), enter the administrator's credentials.

## Chapter 3

# Setting up hardware support

### Management of personal identifiers

A personal identifier (security token) is a storage device for data used for the user identification and authentication. The identifier can store keys for working with encrypted data in encrypted containers.

In Secret Net Studio, the following personal security tokens can be used: eToken, Ru-token, JaCarta and ESMART.

#### Comment.

To store data encryption keys, you can also use removable media, such as memory sticks or USB flash drives. Hereinafter, the term "identifier" will be also applied to removable media used as key media and assigned to users.

A personal identifier is given to the user by the administrator. One personal identifier cannot be assigned to several users simultaneously. However, one user may be assigned several identifiers.

The security administrator may perform the following operations with personal identifiers:

<b>Initialization of the identifier</b>
Formatting, which allows the use of the identifier in the System. Initialization is necessary if a data structure on the identifier was damaged or is absent due to some reason. Removable media for key storage also need to be formatted
<b>Identifier assignment</b>
Adding information about the fact that the user owns the personal identifier of a certain type with unique serial number to the Secret Net Studio database
<b>Cancellation of identifier assignment</b>
Removing information about ownership of the personal identifier by the user from the Secret Net Studio database. Hereinafter, we call this operation "identifier removal" for simplicity
<b>Enabling password storage mode in the identifier</b>
Adding information about enabling password storage mode for the user's identifier to the Secret Net Studio database. A password is saved to the identifier simultaneously with this operation. After the mode is enabled, a user password is obtained from the identifier
<b>Disabling password storage mode in the identifier</b>
This operation is the opposite to the previous one. The password is removed from the personal identifier's memory simultaneously with disabling the storage mode. The identifier remains assigned to the user
<b>Writing and removing keys for working with encrypted data</b>
Used for storing keys in the identifier (or on removable media) for working with encrypted data on encrypted file containers
<b>Verification of ownership</b>
By using this operation, the security administrator can verify which user owns this personal identifier

## Main operations with identifiers

### Presenting an identifier

The identifier must be presented upon the system's request for recording and reading data.

#### To present a USB-key or smart card:

- If you know exactly which identifier to present, put it into the computer's USB slot or apply it to the reading unit.
- If you need to select an identifier from a list of available options, clear the "Use first connected security token" check box and present the identifiers one-by-one. The serial number of each presented identifier appears in the dialog box. When you see the correct identifier, click OK.

#### Note.

If the presented identifier is protected by a **custom** PIN-code (password), the respective dialog box will appear. Enter the PIN-code and click OK.

#### To present other removable media:

1. Insert the removable media into the computer slot and click the Disk button.  
The name of the removable media appears in the dialog box.
2. Select this name from the list and click OK.

### Error message

If there are errors while presenting the identifier, a message explaining the reason for the error appears. Possible error reasons and troubleshooting measures are listed in the table below.

Reason	Action
<b>Identifier contact failure insufficient duration of contact with the reader</b>	Present the identifier again, taking into account general requirements for using the identifiers
<b>Presented token belongs to another user</b>	The procedure will be interrupted. Present the identifier which belongs to this user or an identifier which does not belong to anyone
<b>The presented identifier already contains Secret Net Studio data</b>	If it is acceptable to delete the data from the identifier, you can continue the procedure
<b>The data structure in the identifier was corrupted</b>	Perform the identifier initialization and repeat the action

### Initialization of the identifier

#### To initialize the identifier:

1. Run the user management program (see p. [12](#)).
2. In the Service menu, select the "Initialize security token".  
A dialog box appears asking you to present the identifier.
3. Present the identifier (see above).  
After the identifier's initialization, the respective message appears.

### Verification of ownership

#### To verify the identifier ownership:

1. Run the user management program (see p. [12](#)).
2. In the Service menu, click the "Verify security token" command.

A dialog box appears asking you to Present the identifier.

**3.** Present the identifier (see p. [21](#)).

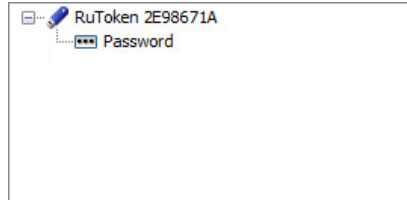
If the Secret Net Studio database contains information about the identifier, it will appear on the screen.

## Working with user identifiers

### Viewing information about user identifiers

Information about personal user identifiers is provided in the user management program (see p. [12](#)). To view the information, open the dialog box of the user settings, select the "Security Settings" tab and click the Identifier parameter group.

The information is shown as a list of assigned identifiers as in the figure below.



The type and serial number are listed for each identifier. Additionally, the following properties of service information storage can be specified:

- markers of storage in the identifier for working with encrypted data in encrypted containers;
- password storage marker.

### Identifier assignment

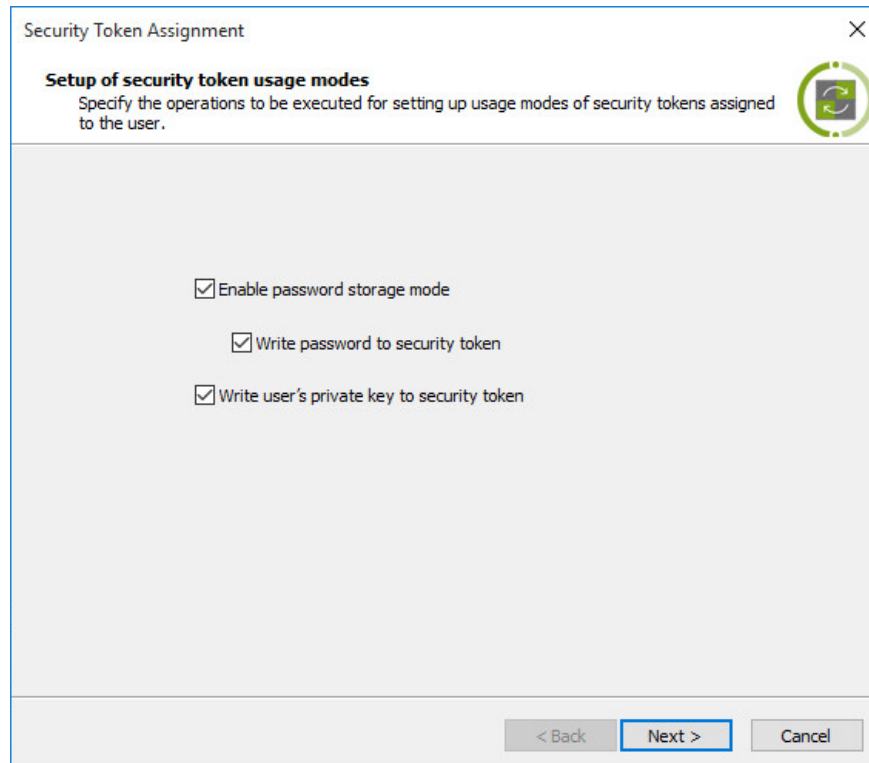
You can assign an identifier to a user using a wizard. When assigning it, you can adjust personal identifier usage modes.

**Notes:**

- To write a key that the user already has for data encryption (private key) to an identifier, the identifier must be presented on which this key is recorded.
- To write a password to an identifier, enter the user's password.

**To assign an identifier to the user:**

- 1.** Run the user management program (see p. [12](#)).
- 2.** Open the user settings window, select the "Security settings" tab and click Add.  
A dialog box appears as in the figure below.



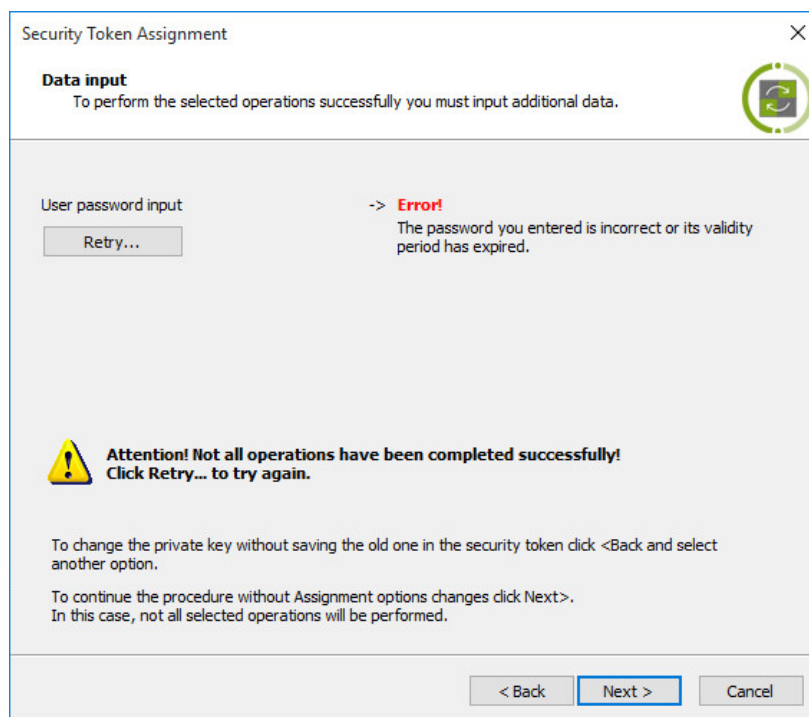
3. Select the check boxes according to the executed operations and click Next> .  
A dialog box with a progress bar appears.
4. If you select "Write password to security token" or "Write user's private key to security token", perform following actions:
  - When the Enter Password dialog box appears, enter the user's password.
  - When the "Present the identifier" dialog box appears, present the user's identifier (see p. 21) containing the user's private key.

Successfully performed operations are assigned the "Completed" status. If an error occurs during the operation, the dialog box will display a respective message.
5. After successfully completing all operations, click the Next > button.  
A dialog box appears asking you to present the identifier.
6. Present the identifier (see p. 21) to be assigned to the user and for data recording. Do not disconnect the identifier from the reader before all operations are complete.

### Data recording errors

Errors may occur when recording data (for example, related to the identifier or DB).

These errors are displayed in the following dialog box with processing results.



#### Attention!

An identifier will not be assigned if an error occurs while performing any operation or if the operation is canceled due to other errors. To fix errors, click "Retry...".

After successful completion of all required operations, each operation should be assigned the Completed status.

7. Click "Repeat" to assign one more identifier with the same settings to the user.
8. To complete the work, click Finish.

#### Assigning an identifier to another user

During the identifier assignment procedure, the following parameters are verified: the identifier's association with another user and presence of saved Secret Net Studio structures in the identifier. If the identifier is assigned to another user registered in the System, the assignment operation is canceled with the respective error message.

If the presented identifier contains Secret Net Studio data but is not assigned to any user of the system (for example, it is used for a local user to login on another computer), a confirmation to continue appears. In this case, the following options are available:

- The identifier contains a private key (or two keys: previous and current), but the user who is assigned with the identifier already has a key. In this case, the System offers to replace the keys in the identifier. Upon continuing the procedure, the private key will be deleted from the identifier. The user's current private key is written to the identifier if the check box "Write user's private key to security token" was selected in the wizard (see above).
- The identifier contains a private key (or two keys: previous and current), and the user who is assigned with the identifier does not have a key. In this case, a request to use the keys from the identifier for the user appears. To leave the key in the identifier and use it for the user that this identifier will be assigned to, click the Yes button in the dialog box. If you click No, the private key will be deleted from the identifier. A user's new private key can be generated and written to an identifier if the check box "Write user's private key to security token" was selected in the wizard (see above). To cancel the identifier assignment procedure, click Cancel.



**Note.**

By using the key from the identifier (clicking Yes in the dialog box), you can, for example, work with one encrypted container for different local users on several computers with the help of that identifier. In the Client's standalone operation mode, the identifier can be used both for local and domain computer users.

- The identifier contains other Secret Net Studio data – a request appears to confirm removal of the detected data. If you are sure that this identifier is no longer used by anyone, click Yes and present this identifier again.

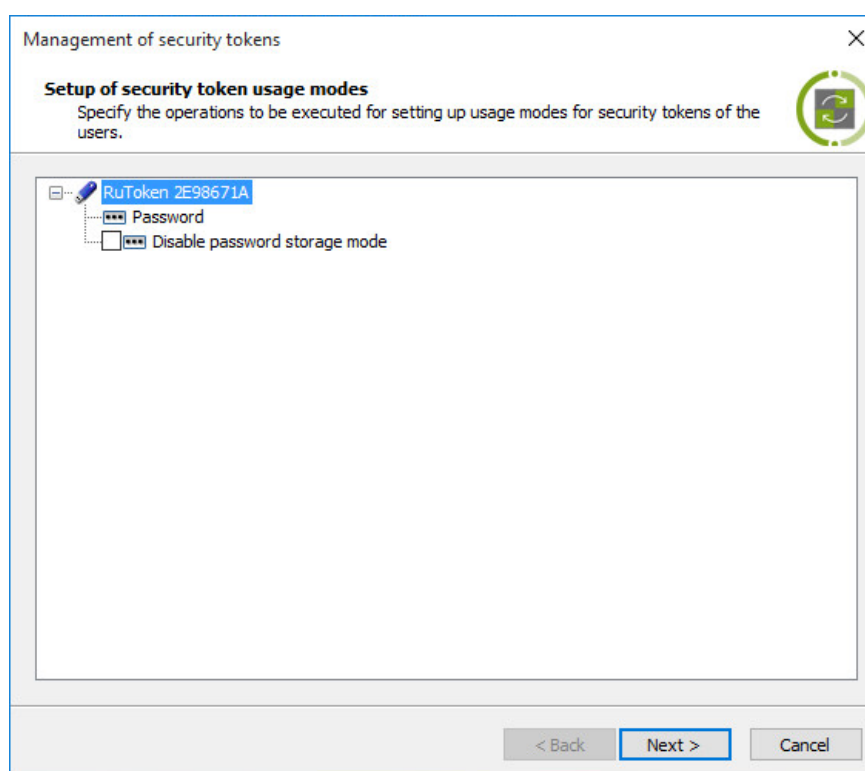
## Configure identifier usage modes

If necessary, you can change usage modes for the identifiers (apart from removable media) assigned to the user. The mode procedure is configured using the wizard.

### To configure the user's identifier modes:

1. Run the user management program (see p. 12).
2. Open the user settings dialog box, select the "Security settings" tab and click the "Parameters..." button.

A dialog box appears as in the figure below.



The dialog box contains a list of identifiers assigned to the user.

**Note.**

Removable disks assigned to the user are not displayed in the list.

Enabled modes and executable operations are indicated for each identifier in the list. For example, if password storage mode is enabled for the identifier, then the "Disable password storage mode" operation will be available.

3. Select the boxes according to the executed operations and click the Next > button.
4. If the "Write password to security token" check box was selected, the "Enter the password" dialog box appears. Enter a new user password and click OK.  
After successful password entry, the notation "Completed" appears in the dialog box to the right of the name of the operation.
5. Click Next>.

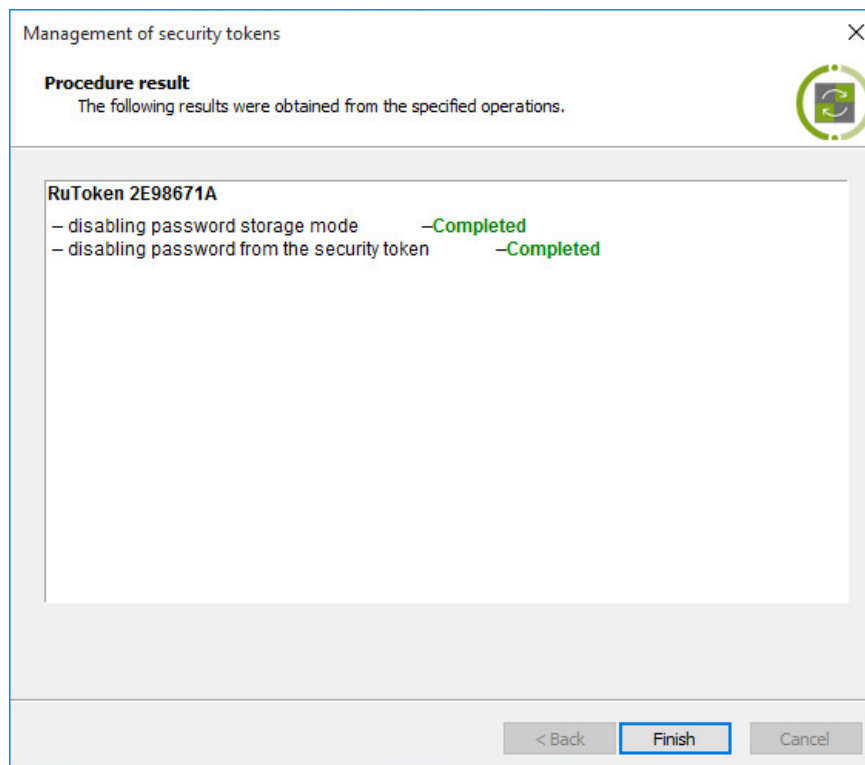
If any operation, apart from "Enable password storage mode" operation, was selected, the "Present the identifier" dialog box appears. The names of identifiers for which operations were selected and their processing status are displayed in the dialog box: Not processed.

6. Present all listed identifiers (see p. 21).

After the identifier is presented successfully, its status will change to Processed. If the identifier was presented with an error, an error message will appear in the processing status column. After presenting all identifiers, the Cancel button will be replaced with Close.

7. Click Close.

A dialog box with operation execution results appears. If the operations were executed with errors, the error description appears in the dialog box.



After successful completion of all required operations, each operation should be assigned the Completed status.

8. Click Finish.

## Deleting an identifier

After the identifier deletion procedure, the user loses the ability to use the identifier for login and password and keys storage.

### To delete an identifier:

1. Run the user management program (see p. 12).
2. Open the user settings dialog box and select the "Security Settings" tab.
3. Select the identifier from the list and click "Delete..."

If the selected identifier is the only one which holds keys for working with encrypted data in encrypted containers, a dialog box appears to confirm the operation.

4. Click Yes.

A dialog box appears asking you to confirm the deletion of the identifier from memory.

5. Click Yes.

A dialog box appears asking you to present the identifier.

6. Present the identifier (see p. [21](#)).

The status of the presented identifier changes to "Processed".

**Note.**

If there are violations during identifier presentation, an error message will appear in the dialog box table in the "Status" column.

7. Click Close.

The record of the deleted identifier disappears from the list of identifiers.

## Chapter 4

# Setting up Integrity Control

The Integrity Control (IC) mechanism monitors the integrity of computer resources. This mechanism compares the current values of controlled parameters with their reference values. Their reference values are defined or calculated when setting up the mechanism. If a mismatch between current and reference values is detected during the control, the System alerts the administrator about the resource integrity violation and performs the predefined action, such as locking the computer.

You can set up the IC mechanism along with the Application Execution Control mechanism (AEC). Applications and data control is used for these mechanisms. In this chapter you can find information about how to set up the Integrity Control either separately or together with the AEC mechanism. For information about the AEC, see document [5].

## Setup methods and tools overview

### Data Model

**Composition** Integrity Control and Application Execution Control parameters are contained within the unified data model. **A data model (DM)** contains a hierarchy of objects and a description of connections between them. The model uses five categories of objects:

Object	Description
<b>Resource</b>	Describes the file or directory, register variable or Windows registry key. Determines the location of the controlled resource and its type
<b>Resource group</b>	Combines several descriptions of resources of the same type (files and directories or objects of the system register). For example, executable files or register keys related to a specific application. Determined by the type of resources in the group
<b>Job</b>	A job is a collection of resource groups of the same or different types. For example, a job may simultaneously include a group of system files and a group of objects of the Windows system register
<b>Task</b>	Determines the parameters for performing integrity control. For example, control methods, algorithms for calculating control values, control schedule, system response to unauthorized actions. It contains a set of jobs and groups of resources to be controlled. For example, when the AEC is used, it can combine descriptions of executable files that are permitted to be run by a specific group of users
<b>Control actor</b>	A control actor can be a computer or a group of users and computers (also for individual users in local control). Determines the computers for which integrity control is performed in accordance with assigned tasks and users who are permitted to run programs preset by tasks of the AEC

**Structure** Objects of one category are subordinate or superior in relation to objects of another category. For example, resources are subordinate in relation to groups of resources, and groups are subordinate to jobs. The inclusion of resources in groups, groups in jobs and jobs in tasks is known as establishing connections between objects. Ultimately, tasks are assigned to the actors. A model including all objects of all categories between which all required connections are established is a detailed instruction defining what and how things should be controlled.

#### Comment.

The model may also contain objects that are not related to others or incomplete chains of objects, but only those fragments will work that connect all levels of the model.

## Storage

The data model consists of two parts. One part is related to the AEC, the other to the IC. Each of these model parts has its own set of tasks. Jobs, resource groups and resources may be included in either part of the model.

The IC-AEC local database (LDB) is arranged as a combination of files stored in a sub-directory of Secret Net Studio setup directory. The IC-AEC LDB stores a data model in each computer.

For the Clients in the network operation mode, an IC-AEC central database (CDB) is generated in a special-purpose centralized storage. Two data models are created to arrange centralized management: one for computers with 32-bit Windows operating systems and one for computers with 64-bit operating systems. Each of the centralized data models is common for all protected computers managed by the Windows operating systems with the respective bit depths.

In the centralized mode of the IC-AEC control program, data models for the IC mechanism can be created using replicated and non-replicated tasks. These two types of tasks differ in their method of generation of jobs and the place of calculating and storing the reference values.

Tasks	Characteristics
<b>Replicated</b>	Reference values for such tasks are calculated centrally and stored in the IC-AEC CDB. When synchronized together with the tasks, the reference values are replicated to the preset workstations and stored in the IC-AEC LDB. Therefore, reference values of replicated task resources are the same on all computers to which such task is related
<b>Non-replicated</b>	For non-replicated tasks, reference values are not replicated but calculated on workstations and only stored in the IC-AEC LDB

## Default model objects

During installation of the Client, the presence of a data model in the IC-AEC database is checked. If a model is absent, it is created automatically and filled with default objects.

During initial configuration, the following jobs are added into the model:

- Secret Net Studio resource control job;
- Windows registry control job;
- Windows files control job.

The jobs include ready jobs with resources configured according to the pre-programmed list. For these objects, links are established with the following actor:

- in the local model with the Computer actor;
- in the centralized model with IC SecretNetIcheckDefault (for 32-bit OS) or SecretNetIcheckDefault64 (for 64-bit OS). The actor has a list of security domain computers with the respective bit depth of the operating system and the Client.

The model is also complemented with additional tasks not linked to the jobs.

## IC-AEC Management Program

The Applications and data control program (hereinafter the IC-AEC Management Program), which is included in the Client, is used for setting up IC and AEC mechanisms.

The IC-AEC Management Program makes it possible to generate data model elements using automated and manual tools. Manual tools can be used at all levels of the model for generating and modifying objects and links. Automated tools are preferable when working with many objects. However, this requires deeper control of the results. Manual tools can be used for generating small fragments of the model. In this case, the process is under control and devoid of random errors. We recommend you to combine these two methods.

The IC-AEC Management Program can work in the centralized and local modes. The centralized mode is used for setting up working parameters of mechanisms on computers with the Client in the network operation mode.

To operate the IC-AEC Management Program, you should be included in the local group of the computer's administrators. To use centralized mode, the user should also be included in the group of security domain administrators.

The program's launch procedures are described on p. 13.

## Synchronizing central and local databases

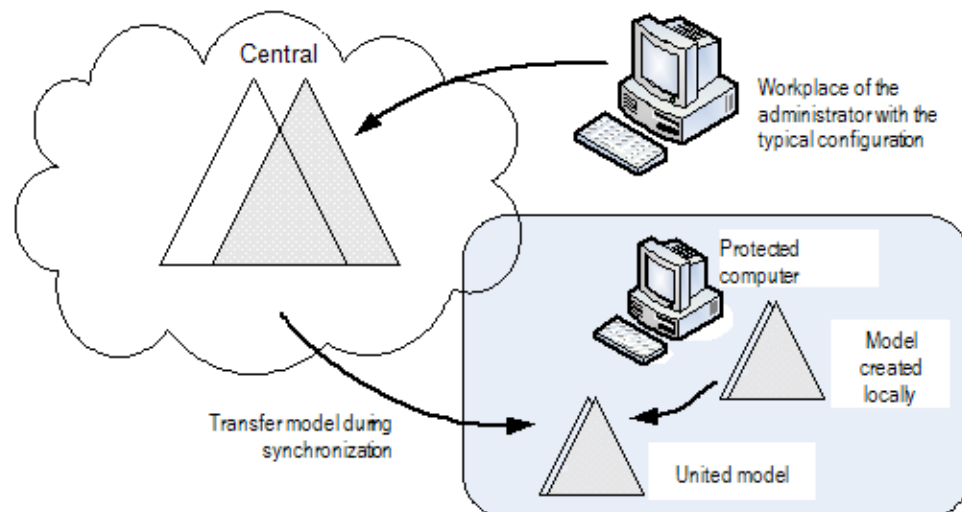
During synchronization, changes from the IC-AEC central database are transferred to all affected computers. The changes are saved in the IC-AEC local database. Synchronization may be performed:

- during computer booting;
- during user login;
- after login (in the background mode while the user is working);
- periodically at predetermined time intervals;
- forcibly on the administrator's command;
- immediately after adding changes to the IC-AEC central database.

### Note.

To synchronize immediately after saving the data model in the central database, change notifications should be distributed to the computers. Distribution of notifications can be started manually or automatically (see p. 42). For prompt synchronization, certain Windows OS parameters should be defined on the computers (see p. 84).

As a result of synchronization, a united actual data model is created in the IC-AEC local database. This contains locally and centrally created jobs as well as related tasks, resource groups and resources.



### Protection against resource duplication during synchronization

If the local database receives a description of a resource that is already stored in the local database from the central database, it only saves one description of the resource, but all resource links remain. If this resource's monitoring in the central database was discontinued, the resource links earlier stored in the local database are restored.

## Initial setup of IC mechanisms

This section describes the procedure for the initial setup of the IC mechanisms. An approach based on the maximum usage of automated tools (data model wizard and task generation utility) is offered as the main setup method.

### Preparing to build a data model

When preparing to build a data model, the software and data on protected computers are analyzed. IC and AEC prerequisites are worked out, including the following:

- information about protected computers (e.g., installed software, users and their duties);
- list of resources actor to integrity control procedure;
- list of software products available to various user groups.

From the computers with the Client in the network operation mode, identify the groups with full match, partial match, and unique configuration of software and data. Prepare the administrator workstation to perform the configuration. On the workstation, install all software whose resource description is to be automatically executed by the tools designed for adding the tasks to the data model.

**Note.**

Centralized models are edited in accordance with the following characteristics: only a data model with the same bit depth as that of the installed Windows OS can be edited. A data model with a different bit depth is available as read-only (it is also possible to export data from that model to another one). Therefore, if the System includes computers with Windows versions that have different bit depth, we recommend you arrange two workstations for the administrator one with an installed 32-bit OS and the other with a 64-bit OS.

## General configuration procedure

To use the IC mechanism on the computer, perform the configuration in the following order:

1. Configure the new data model with control settings by default (see p. 31).
2. Include additional objects to the data model:
  - tasks for integrity control (see p. 32);
  - IC jobs (see p. 34).
3. Create controlled resource reference values (see p. 37).
4. Enable IC mechanism (see p. 40). Before starting the mechanism, we recommend you to check that control job parameters are correct (see p. 40).

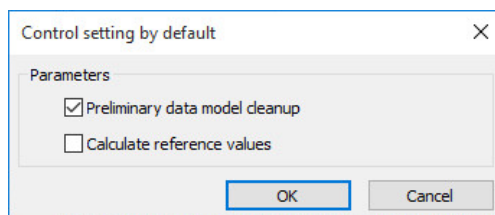
Also, it may be necessary to adjust and review the data model adjustment. If you want to remake the model, it is better to do it from scratch. If only a small part of the model requires remaking, you can use individual model modification procedures (see p. 49).

## Building a new data model

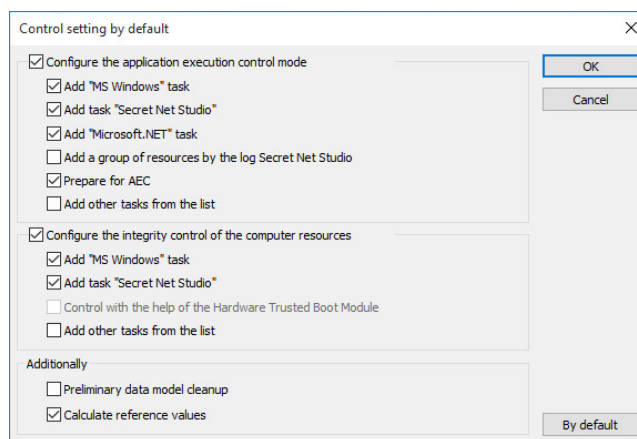
A data model is automatically provided with Windows OS essential resource descriptions along with those related to some applied software products. A newly created model has a default control setup.

**To build a new data model:**

1. In the Control Center, click the File | New data model command.
  - In the centralized mode, a dialog box appears as in the figure below:



- In the local mode, a dialog box appears as in the figure below:



2. Based on the selected work mode, set up the respective parameters and click OK.
  - When working in the centralized mode, we recommend that no changes are made to the default parameter values.
 

The previous data model will be deleted. Then, the automatic data model build procedure will start. Upon successful completion, the main IC-AEC Management Program window will offer new data model features to work with.
  - The local mode enables a detailed set up of parameters prior to building a new data model. In addition to standard tasks, a model can be enhanced with application resource-based ones. Such tasks can be added by selecting the "Add other tasks from the list" check box.

**Note.**

For the AEC mechanism, we recommend that the Perform AEC preparation parameter is set as active in order to enable the resource preparation procedure. Such resources will be marked as In progress, and the System will search for modules associated with executable files. This is the operation's primary purpose; without it the AEC will not be fully configured.

Once a model is successfully built, the main IC-AEC Management Program will be updated with a new structure.

## Adding tasks to a data model

The current configuration stage is aimed to enhancing the data model with a fragment that includes a list of miscellaneous essential tasks (except Windows resources and Secret Net Studio). This can be achieved using manual or special tools – a task generation mechanism. Tasks are created based on information about software products installed on the computer. Such information can be found in the MS Installer details and the Windows OS Start menu shortcuts. We recommend you to use a generating mechanism when supplying a data model with complex tasks that contain a great amount of resources.

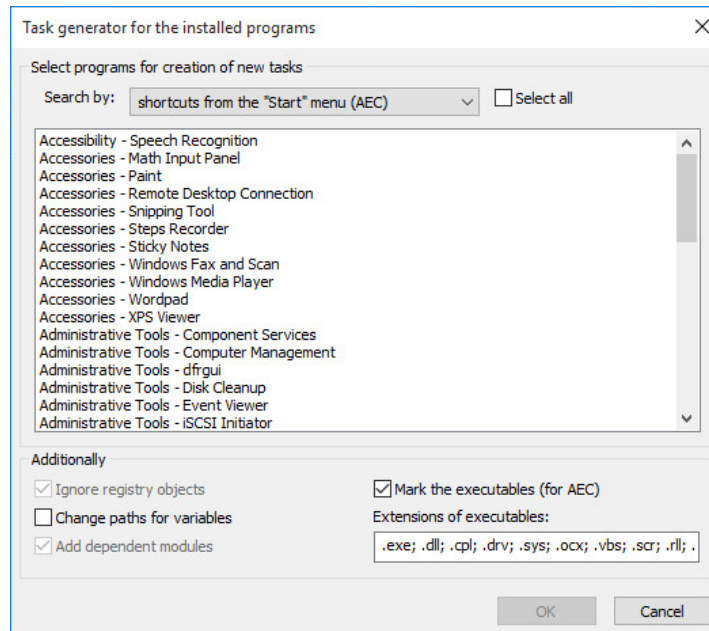
Prior to starting the generation procedure, you can view the list of software currently installed and note the particular components (of a program) that can serve as a basis for task generation. In this case, the tasks shall automatically include the resources referring to executable modules of a selected software product. There is also an option to set supplementary filtering parameters for resources.

**To add tasks to a model:**

1. In the Service menu, click the "Task Generator..." command.

A dialog box appears as in the figure below:





The dialog box provides a selection of programs as well as the ability to set up additional parameters for resource selection.

2. In the "Search by" drop-down list, select the software product list.
3. Select the software from the list, then set up additional parameters for resource selection.

**Tip.**

To select several items in the list, use the <Ctrl> key on the keyboard. To select all items, select the "Select all" check box.

Parameter	Description
<b>Ignore registry objects</b>	Registry objects should not be considered as tasks
<b>Change paths for variables</b>	When recording a data model, the file location paths are replaced with environment variables
<b>Add dependent modules</b>	Dependent modules are the files, which the execution of source files depends on. These are, for example, drivers and libraries that are not directly integrated into the applications; however, if these files are missing, applications will not be able to work as intended. Dependent modules are added to the same resource group where the source file is found. Dependent modules are recursively integrated into the list: the files which are dependencies for the actual dependent modules are also integrated into the list
<b>Mark the executables (for AEC)</b>	Executables are designated with a special symbol when displayed on the main window of the IC-AEC Management Program. Executables are files with extensions listed in the "Extensions for executables" line as well as files that have received non-typical extensions; such a file list is created through the parameters of a software program — seep. 79). If necessary, edit the list of extensions to be used in this selection of resources


**Note.**

When selecting from the MS Installer list, each of the additional conditions listed above can be specified. When selecting via Start menu shortcuts, only two of the conditions are available: "Change paths for variables" and "Mark executables".

4. Click OK.

The generation procedure starts. A message box about successful completion appears.

**5. Click OK.**

As a result, the model contains new tasks including resource groups but not linked with superior objects (i.e., jobs), which is indicated by .

## Adding jobs and including tasks to them

Jobs are created based on previously generated tasks. Integrity control-related jobs must be configured as follows:

- methods and algorithms for secure resource control;
- system reaction in case of resource integrity failure;
- list of events which are entered into the log;
- schedule, according to which the verification should be performed.

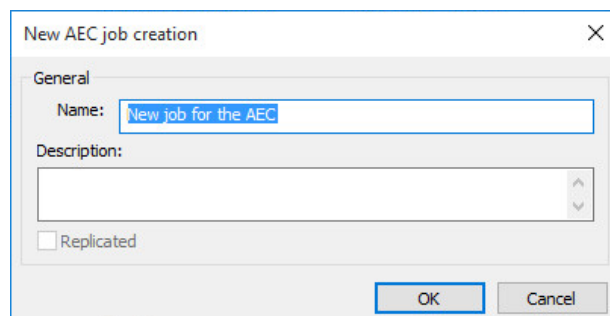
### To create a job:

1. Go to the "Jobs" category and in the "Jobs" menu, select the "Create job" command.

A dialog box asking you to select a job type appears.

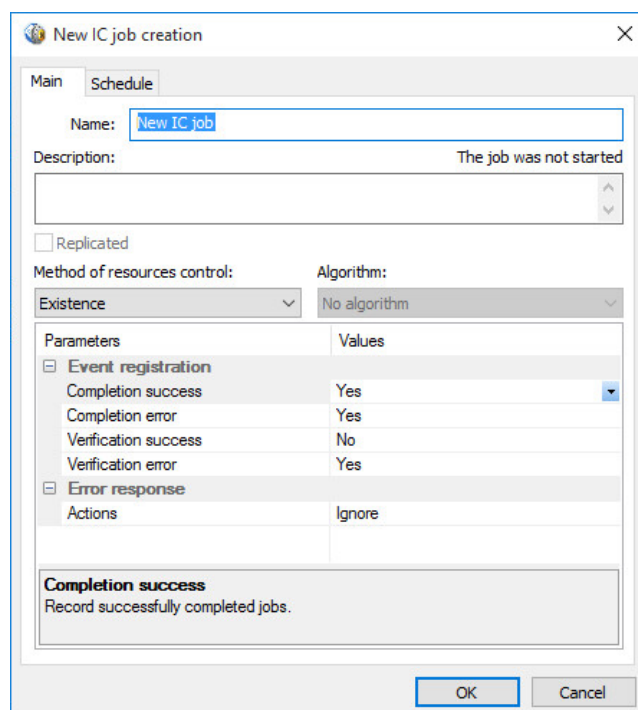
2. Choose the job type and click OK.

If an AEC job is selected, a dialog box appears as in the figure below:



Type a job name, a brief description and click OK.

If an integrity control job is selected, the following dialog box appears as in the figure below:



Parameters	Values
<b>Event registration</b>	
Completion success	Yes
Completion error	Yes
Verification success	No
Verification error	Yes
<b>Error response</b>	
Actions	Ignore

3. Type an integrity control job name and a brief description.
4. Specify a resource control method by selecting it from the list.

The methods are listed in the table below.

Control method	What is to be controlled
<b>Existence</b>	Existence of resources under a selected path
<b>Content</b>	Resource content integrity
<b>Attributes</b>	Standard attributes defined for resources
<b>Access rights</b>	Confidentiality categories and Windows access attributes (i.e., a security descriptor) defined for resources



When selecting a type of data to be controlled, it is essential to consider that only a selected part of resources will undergo the control procedure. Information about whether control methods apply to each resource type, regarding the type of data controlled, is provided below. When selecting a control method, it may turn out that a job has resources associated with it that are incompatible with the algorithm implemented in the job. Such a situation, when a task to undergo the control procedure contains a great number of heterogeneous resources, is a typical one. However, such a situation should not be feared, because the control subsystem ignores incompatible resources. When calculating reference values, it is vital to define either an ignore or a request parameter for incompatible resources. Therefore, a task can be associated with multiple jobs to control, thereby excluding any potential chance of failure due to the presence of resources incompatible with jobs.

Details on correspondence of resource types and control methods are presented in the following table.

	Object content	Object attributes	Access rights	Object existence
<b>File</b>	Yes	Yes	Yes	Yes
<b>Directory</b>	Yes	Yes	Yes	Yes
<b>Registry key</b>	Yes	No	Yes	Yes
<b>Registry value</b>	Yes	No	No	Yes

5. If the Content control method is selected, specify an algorithm by selecting it from the drop-down list.

The following algorithms are available: CRC32, EDS, hash, cryptographic checksum, full match, integrated EDS.

#### Algorithm special features

The full match algorithm, unlike the others, allows the controlled object to be recovered in case of integrity violation. However, implementation of this algorithm significantly increases the database size, because the object copy is the control reference value.

The integrated EDS algorithm enables integrity control of files that are updated through software and operating system updates. The distinguishing feature of this algorithm is that during the integrity control procedure, the files are checked for their integrated digital signature (the Microsoft Authenticode format). An intact file certificate is a key condition to successful completion. If file signature was not detected during the reference values calculation procedure, this file will be ignored when controlling through this algorithm.

6. Configure event registration. To do this, in the Parameters column, select the event you need. Then, in the respective row of the Values column, a drop-down list appears. Select Yes to register an event, or No to cancel event registration.

Available events are listed in the following table.

Event	Description
<b>Completion success</b>	Integrity control has been finished successfully
<b>Completion error</b>	Integrity violation detected during job processing
<b>Verification success</b>	Resource integrity control success
<b>Verification error</b>	Violation of resource integrity

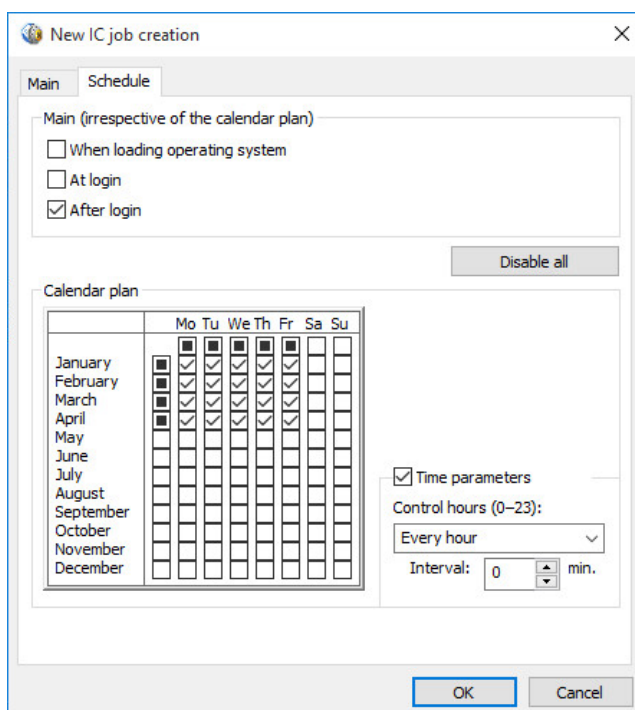
7. Configure system reaction. To do this, in the Parameters column, select the Action row, then in the Values, select the option you need. The following options are available:

Reaction	Description
<b>Ignore</b>	No system reaction
<b>Lock computer</b>	Computer will be locked. The unlocking can be done only by a security administrator
<b>Restore from reference value</b>	The current value of a controlled resource parameter is being restored from a reference value. Not all methods trigger the reaction
<b>Restore with lock</b>	The current value of a controlled resource parameter is being restored from a reference value. Computer will be locked. The unlocking can be done only by a security administrator. Not all methods trigger the reaction
<b>Accept as reference value</b>	The current value of a controlled resource parameter is being accepted as a reference value. This reaction is not available for replicating jobs

The recovery option for files and registry values has the following special features:

- Recovery is not available, if "Existence" is set as the control method;
- Recovery is available, if "Content" is set as the control method along with the "Full match" algorithm;
- File and folder attributes can be recovered, if "Attributes" is set as the control method (except for Secret Net Studio confidentiality marks).



8. Select the Schedule tab and schedule control procedures based on the job-related requirements.



The dialog box has two sections. Configure the control time in the upper section regardless of the calendar (during operating system start, during user login and upon system login). The lower section displays the calendar together with schedule settings.

Field	Description
<b>Main (irrespective of the calendar plan)</b>	Use this field group to define the stage at which the System shall perform resource integrity control. This procedure can be performed during operating system load, during user login and upon system login. The "At login" method indicates that the control procedure is initiated once the user enters her/his identification credentials and, until the procedure is completed, the system login is suspended. If the method is set as "After login", the procedure is initiated once the user has logged in and is performed in the background
<b>Calendar plan</b>	Field group to schedule control procedure by month, weekday, hour and minute
<b>Calendar</b>	Is used to schedule control procedure by month and weekday
<b>Time parameters</b>	This field group enables control periods to be defined for 24 hours
<b>Control hours</b>	Select from the drop-down list or enter the period value for control for 24 hours. Please note that the zero hour is the count-down starting point. Therefore, if 4 is set as a value meaning perform control procedure every fourth hour, the procedure will be performed at 0, 3, 7, 11 o'clock, etc. Control hours can be set not only by specifying periods but also by directly entering exact time values. For example, if the following is entered: 2, 7-9, 16-18, 21, the control procedure will be performed at 2, 7, 8, 9, 16, 17, 18 and 21 o'clock
<b>Interval</b>	Specify control periods during the control hour. If no value is entered, the procedure will be performed once at the beginning of the hour. Therefore, if control is to be performed at 7 o'clock, for example, and the Interval value is set for 10, the process will primarily initiate at 7:00, then repeat every 10 minutes over the specified hour

#### 9. Click OK.

The additional structure window displays a new job for integrity control , not related to any actor. A replicated job is marked by .



#### Attention!

Jobs created through the means of centralized override are displayed in bold in a program running locally. These jobs cannot be removed from a data model. No task inclusion allowed for such jobs.

### Including tasks into a job

#### To include a task:

1. Select the "Jobs" category on the category panel.
2. In the structure window, right-click the job and click the Add tasks/groups | Existing command.

A dialog box appears showing the list of all tasks and resource groups not included in the job.

3. Select tasks to be included into the job and click OK.

#### Tip.

To select multiple tasks, use the <Ctrl> key on the keyboard or select the "Select all" check box.

### Calculating reference values

Calculation of reference values is required for controlled resources that are a part of integrity control jobs as well as AEC jobs, provided that the integrity control option is available for allowed software products. If a data model is created using a creation wiz-

ard (see p. 31). If a data model is built using a task generation tool or manually, the reference values are to be calculated separately.

At the configuring stage, we recommend you to implement the following calculation methods:

- calculating reference values for all controlled resources within a local data model (when the Applications and data control tool is in its centralized mode, reference values are only calculated for resources related to replicated jobs);
- calculating controlled resource reference values related to a particular job.

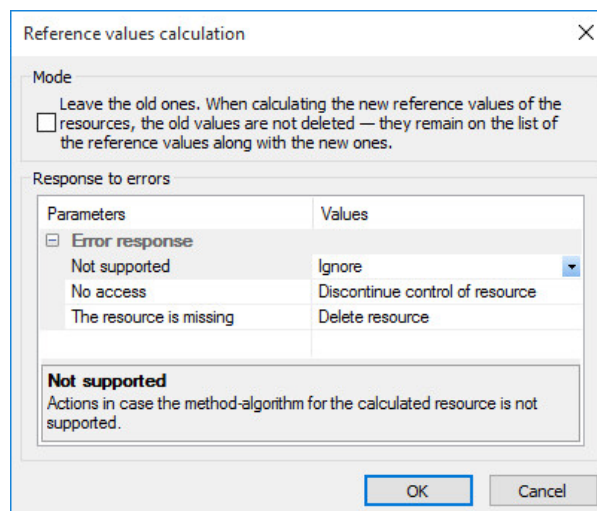
In the local mode, reference values can be calculated for all resources contained within a local data model. Exceptions are resources whose reference values were calculated in the centralized mode (i.e. resources are included in replicated jobs).

Centralized mode offers various reference value calculation methods for both replicated and non-replicated jobs. The replicated job reference value is calculated in the same way as in the local mode (these reference values will then be transmitted to computers). Resource reference values for newer non-replicated jobs are automatically calculated on computers after being transmitted to the local database during synchronization. If any changes are made to a non-replicated job, you can initiate a reference value calculation procedure.

### To perform a reference value calculation in the local mode:

1. Based on the resources for which reference value calculation is needed do the following:
  - in the "Service" menu, click the Reference values | Calculation command to calculate reference values for all controlled resources in a data model;
  - open the context menu of that job and click the "Reference values calculation" command to calculate reference values for the resources of a particular job.

The "Reference values calculation" dialog box appears as in the figure below.



2. If you want to retain the previous reference values, select the "Leave the old ones" check box.

#### Note.

You may need to retain previous ("older") values, for example when controlling content of files that are updated together with related software. For more details, see onp. 62.

3. Configure the System to react to potential errors during reference values calculation. To do this, in the left part of the table, select the error type and the System reaction to it in the right part.

The following types of errors are possible:

- calculation method/algorithm is not supported for this resource;
- the resource cannot be read or has been blocked;

- no requested resource found at the specified location.

For each type of error, you can specify one of the reactions listed in the table below.

Reaction	Description
<b>Ignore</b>	No system reaction for specified error
<b>Display request</b>	When an error occurs, a respective error message is displayed, prompting a choice of actions to rectify the problem
<b>Delete resource</b>	When an error occurs, the resource is deleted from the data model
<b>Discontinue control of resource</b>	The resource will no longer be controlled but will remain in the model. Please note that in such a case, resource control will be discontinued for a job where an error occurred and for other jobs that this resource is associated with

#### 4. Click OK.

Reference values calculation starts. The calculation progress can be tracked through a progress bar.

If an error occurs during calculation and the system reaction is "Display request", the procedure will be paused, and a dialog box appears, prompting to select whether to continue the calculation or not.

Available options to continue the procedure are listed in the following table.

Option	Description
<b>Ignore</b>	The calculation procedure will continue. No system reaction for this error. The resource which caused an error will remain as part of the task (or tasks). During integrity control of a resource, an alert event will be registered with a respective system reaction (except for the integrated EDS algorithm-based control; if a file lacks such a signature during reference values calculation, this resource will be ignored for control procedures)
<b>Discontinue control</b>	The calculation procedure will continue. The resource that caused the error will remain as part of the task (or tasks) and will be removed from control procedures for all jobs that this resource is associated with
<b>Delete</b>	The calculation procedure will continue. The resource that caused the error will automatically be deleted from the data model
<b>Interrupt</b>	The calculation procedure will be interrupted. To calculate reference values, please resolve the problem that caused an error, then restart the calculation procedure

#### 5. Click the respective button in the dialog box.

Based on the selected option, the procedure will either be continued or interrupted; either of the options will trigger a corresponding message box to appear on the screen.

#### 6. Before clicking OK, read carefully the message displayed in the message box.

#### To calculate reference values for replicated jobs (in the centralized mode):

1. Based on the resources for which reference values calculation is needed, do the following:
  - in the "Service" menu, click the Reference values | Calculation command to calculate reference values for all replicated jobs;
  - right-click the job and click the "Local reference values calculation" command to perform the reference values calculation for resources of a separate replicated job.

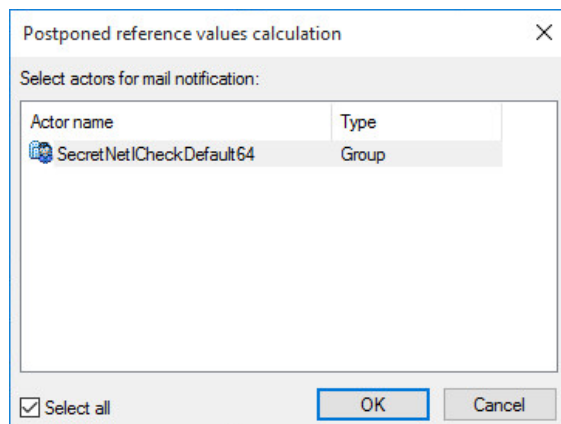
The "Reference values calculation" dialog box appears.

2. Perform the actions, as instructed for the reference values calculation procedure in the local mode, starting from step 2 (see above).

### To calculate reference values for a non-replicated job (in the centralized mode):

1. Right-click the non-replicated job and click the required option:
  - click the "Postponed reference values calculation" command to postpone reference values calculation for a non-replicated job until next CDB and LDB synchronization on computers;
  - click the "Remote reference values calculation" command to initiate an immediate reference values calculation.

A dialog box appears asking you to select an actor. The dialog box contains the list of actors that the selected job is associated with.



2. Select actors for whose computers it is required to calculate the resource reference values for a specified job. Click OK.

#### Note.

An immediate reference values calculation (upon clicking of "Remote reference values calculation" command) is only performed for computers currently turned on. If computer is currently turned off, the reference values calculation procedure for non-replicated jobs can either be performed by clicking the "Postponed reference values calculation" command or locally on this computer.

## Activating IC

The IC mechanism is activated when integrity control jobs are connected with the actors "Computer" and "Group (of computers)". In the centralized mode, the mechanism will be activated on a computer once this computer's local database is synchronized with the centralized database.

### To activate the IC mechanism:

1. On the category panel, select the "Control Actors" category.
2. Through the additional structure window or the object list, select a computer or a group of computers, right-click them and click the Add jobs | Existing... command.

A dialog box showing the integrity control job list appears. For each job on the list, there is a number of control actors associated with it.

3. Select the jobs to be assigned to an actor and click OK.

The IC mechanism will be activated for the specified computer (or group of computers).

## Checking jobs

Prior to starting the use of the IC mechanism, you can check whether the job parameters are correct. During the check jobs are executed immediately, regardless of the schedule. It ensures the timely resolution of errors related to job configuration.



The check is performed for each job separately. Reference values must be calculated for a job and be associated with an actor.

The check has two modes: light mode and full imitation. In light mode, events are not recorded in the log and the reaction to errors is not processed. Once the check procedure is completed, a list of detected errors is displayed. In the full imitation mode, events are recorded in the log and the System processes the reaction to errors.

In the local mode, the check can be performed for any integrity control jobs associated with a computer (including jobs created in centralized mode). Centralized mode enables a local check of replicated jobs, as well as remote check of any centralized jobs on turned on computers of selected actors.

**To start checking jobs (in the local mode):**

1. In the Service menu, click the "Job start" command.  
A dialog box showing the list of all integrity control jobs appears.
2. Select the required job from the list. If the full imitation mode is required, select the "Full imitation" check box.
3. Click OK.

The job starts; upon completion, a message box about successful completion or with a list of detected errors appears.

**To perform the replicated job check (in the centralized mode):**

1. In the Service menu, click the "Job start" command.  
A dialog box showing the list of integrity control replicated jobs appears.
2. Follow the steps, as instructed to start checking in the local mode, starting from step 2 (see above).

**To perform the remote job check (in the centralized mode):**

1. Right-click and click the "Remote job start" command.  
A dialog box appears asking you to select a actor. The dialog box contains the list of actors the selected job is associated with.
2. Select actors on the computers where the check must be performed. Click OK.

The job starts; upon completion, a message box about successful completion or with a list of detected errors appears.

**Note.**

The remote job check can only be performed for computers currently turned on.

## Saving and loading a data model

### Saving

After any changes are made to the data model, its current state can be saved in the database. To save the model, click the Save command in the File menu.

In the program's centralized operation mode, the data model can be saved in the central database on condition of full access to the database. If full access is blocked (for example, because the IC-AEC management program was launched in centralized mode on another computer), when you try to save the model, you will be notified that it is impossible to add changes to the database. In this case, the program will go into read-only mode for central database access. As a result, it will be impossible to save changes within the current session. You will be able to write data in the central database only during the next program operation session.

To load the current version of the data model during the next session, you can export the model to a file, restart the program and import the model from the file (see p. 45, p. 46).

## Change notifications

Notifications about changes in the data model, performed in the centralized mode, are distributed among working computers in the domain according to the Notifications group parameter settings (for a description of the program's parameter settings, see on p. 79). The function is available for the Clients in the network operation mode.

If the parameter value is Yes, notifications are sent when the model is saved.

If the parameter value is No, a notification is not sent. However, you can force notifications to be sent. To force sending notifications, click the "Notify about changes" command in the "Service" menu.

## Configuring automatic synchronization start

After adding changes to the IC-AEC central database, these changes must be synchronized on the computers with the subsequent recalculation of the resource reference values (if necessary). Synchronization is started locally on the computers at predetermined time intervals.

Synchronization start parameters are configured in the program's centralized operation mode. The parameters may be defined for separate computers and for groups. In this case, the parameters have application priorities: computer parameters have the highest priority, followed by group parameters, apart from the default group "SecretNetICheckDefault", and, finally, the default parameters of the group. For example, if synchronization parameters for the computer and for the group to which it belongs are different, only computer parameters will be effective on that computer.

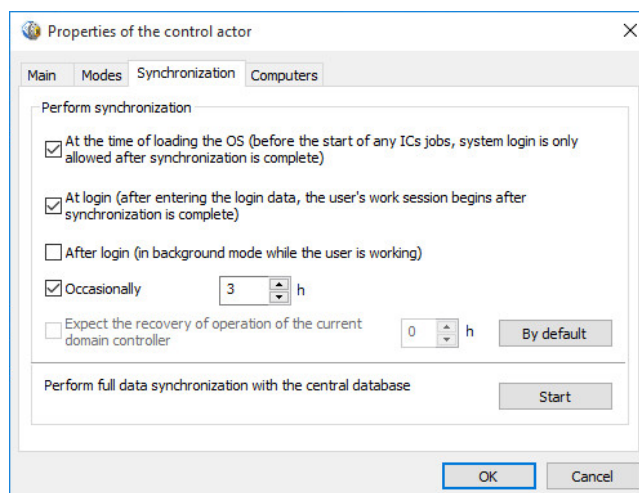
### Comment.

Parameters for the groups that include the computer are effective if the model has no actor for this computer with its own synchronization parameters. In this case, the following algorithm of parameter application between the groups is defined: if the computer is included in another group apart from the default group "SecretNetICheckDefault", the parameters from the first group (not the "SecretNetICheckDefault") are effective on that computer. If there are several groups with different parameters, the default group's parameters are applied.

For early recognition of conflicting group synchronization parameters, there is a procedure for verifying these parameters. Verification should be performed if the model has several groups which may include the same computers.

### To configure synchronization start parameters:

1. In the centralized mode of the IC-AEC management program, select the "Control actors" category on the categories panel.
2. In the additional window, select the structures or, in the list of objects, a computer or group (of computers), right-click them and click the "Properties" command. In the "Properties of the control actor" window, select the "Synchronization" tab, as in the figure below.



3. Configure synchronization start parameters. See the description of the parameters in the table below.

Parameter	Description
<b>At the time of loading...</b>	If selected, synchronization starts when an operating system loads before IC job execution starts. Therefore, any IC jobs are synchronized with the central database before their execution on the computer. In this case, the user can only enter the System after synchronization is complete. This parameter may cause entry delays in the event of changes to large jobs in the central database and low capacity of communications channels
<b>At login...</b>	If selected, synchronization starts after the user enters his/her account data for login but before IC job execution starts. Start of the user working session is delayed until the synchronization ends. This parameter may cause entry delays in case of changes to huge jobs in the central database and low capacity of communications channels
<b>After login...</b>	If selected, synchronization is performed in background mode after start of the user working session
<b>Occasionally</b>	If selected, synchronization is started when the computer is on, at predefined intervals (in hours)
<b>Expect the recovery of operation of the current domain controller</b>	<i>Not available in the current version</i>

**Note.**

If automated synchronization start is disabled (the check boxes "At the time of loading...", "At login...", "After login..." and "Occasionally" are selected), synchronization on the computer may be performed only after receiving notifications about changes or at the administrator's command. For this purpose, the computer must be on.

4. Click OK.

**To check and adjust the synchronization start parameters in groups:**

1. In centralized mode of the IC-AEC management program, click the "Check group synchronization" command from the "Service" menu.

**Note.**

The command is not available if the list of actors in the data model contains only one group by default "SecretNet\CheckDefault".

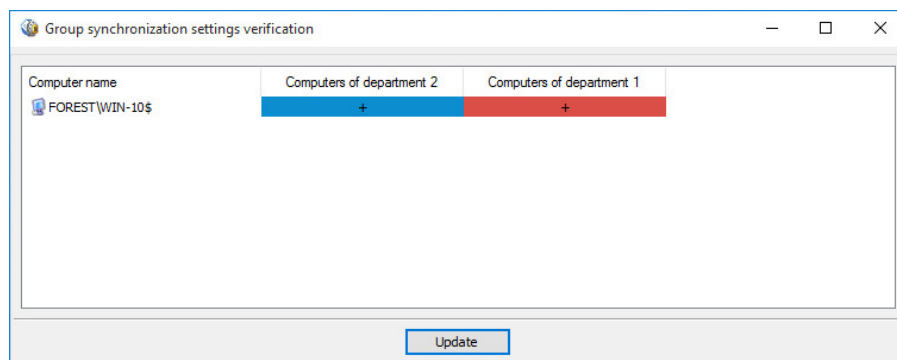
The program checks the computers' inclusion in groups with different synchronization parameters. The results will be displayed after the check.

- Message that there are detected conflicts — if there are no mismatched synchronization start parameters for all computers in the group.

**Note.**

A situation will not be considered as a conflict if a computer included in the groups with different parameters is also available in the model as a separate actor. In this case, according to the priority for the application of parameters, the parameters applied for this computer will be those that are specified for it as a actor (regardless of parameters set for groups where this computer is included).

- List of computers with conflicting parameters:



The list shows the computers and groups that have mismatched parameters for starting synchronization of these computers.

2. If there are computers that have conflicting parameters, move or minimize the window from the list. In the main program window, follow the steps to resolve the conflicts (for example, edit the lists of computers in groups or add these computers as separate actors with their own parameters). To repeat the verification, go to the window with the list again and click Update.

## Forced start of full synchronization

The start of the IC-AEC central database changes synchronization on the computers may be performed automatically according to the predefined parameters (see p. 42). In the centralized operating mode, the administrator can launch an unscheduled full synchronization of IC-AEC central database changes on certain computers.

Synchronization can be launched for selected computers and for groups. However, the current load of the data transfer channels for local and network resources should be taken into account. Do not start synchronization for computer groups unless it is necessary. If the central database stores a significant data volume, full synchronization will take a long time to complete. During synchronization, the work of users on the selected computers will be limited.

### To start full synchronization:

1. In the centralized mode of the IC-AEC management program, select the "Control actors" category on the categories panel.
2. In the additional window, select the structures or, in the list of objects, a computer or group (of computers), right-click them and click the Properties command. In the "Properties of the control actor" window, go to the "Synchronization" tab.
3. Click Start.

The synchronization process starts.

## Downloading and recovering a data model

The data model is downloaded from a DB each time the program starts, or the download can be executed by running a corresponding command.

If you are unsure whether the changes being made to a model are correct, please make sure you do not save them directly to the DB. In this case, you are able to access the original model available within the DB. A recovery procedure is used for such purposes.

### To recover/retrieve a model from a DB:

1. In the File menu, click the "Restore from database" command.  
A warning about the loss of the made changes appears.
2. Click Yes.  
The program downloads a previously saved model from the DB.

## Export

The export procedure can be performed using the following methods:

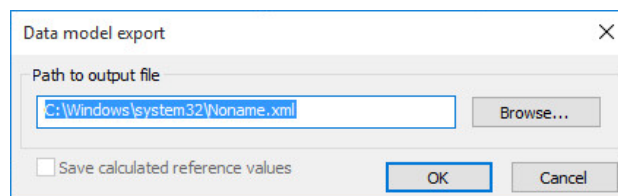
- exporting the entire data model;
- selective exporting of objects from specific categories (does not apply to "Control Actors" category objects).

### Note.

To automate backing up of the IC-AEC DB, the option for exporting and importing the data model by launching the program from the command line is provided. A description of startup parameters is provided in the Appendix on p. 86.

### To export the current data model:

1. In the File menu, click the "Export model to XML" command.  
A dialog box asking for export parameter configuration appears as in the figure below.



2. Specify the full name of the file in the "Path to output file" field. To specify it, use the keyboard or click Browse to select the file that appears in the standard file save dialog box of Windows.
3. If the model contains resources with calculated reference values and these values need to be saved in the file, select in the "Save calculated reference values" check box.

### Note.

When the resource export mode is enabled, along with the reference values, the program need to save the current model in the database. A respective message appears after the "Save calculated reference values" check box is selected.

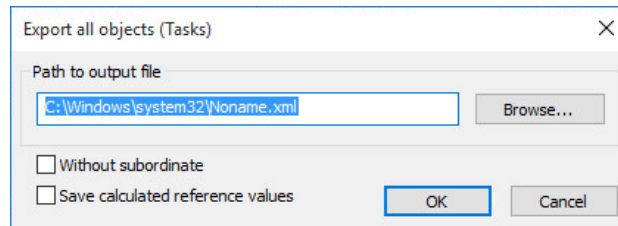
4. Click OK.

### For the selective export of objects:

1. On the category panel, select the category that contains objects to be exported (except the "Control actors" category).
2. In the structure window or in the object list area, find the objects to be exported.  
The following object selection options are provided:

- all objects attributed to the current category: for this purpose, select the root element with the category name in the structure window;
  - a group of randomly selected objects: for this purpose, select the required objects in the object list area by pressing the <Ctrl> and <Shift> keys;
  - an individual object in the structure window or in the object list area.
3. Right-click the object (objects) and click the "Export selected..." command. Depending on what objects were selected, this command will be named: "Export all objects", "Export incoming to folder" or "Export selected objects".

A dialog box appears as in the figure below.



4. Specify the full name of the file in the "Path to output file" field. To specify it, use the keyboard or click Browse to select the file that appears in the standard file save dialog box of Windows.
5. By default, along with the selected objects, the objects included in the chains of their related objects at the lower hierarchy levels will also be exported (for example job – task – resource group – resources). If only the selected objects need to be exported, select the "Without subordinate" check box. This check box is not included in the dialog box if the export procedure is performed for resources.
6. If the exported objects contain resources with calculated reference values and these values need to be saved in the file, select the "Save calculated reference values" check box.

**Note.**

When the resource export mode is enabled, along with the reference values, the program needs to save the current model in the database. A respective message appears after the "Save calculated reference values" check box is selected.

7. Click OK.

## Import

A file can be imported in the following ways:

- the general import of objects to the data model allows all data contained in the file to be imported;
- import of objects to the current category (not applicable to the "Control actors" category) allows objects belonging to the same category to be imported from the file.

Resource lists exported from another data model are added by importing from a file with a saved data model. This method is used when transferring security mechanism settings from one computer to another. Computers must have the same configurations and use the same software.

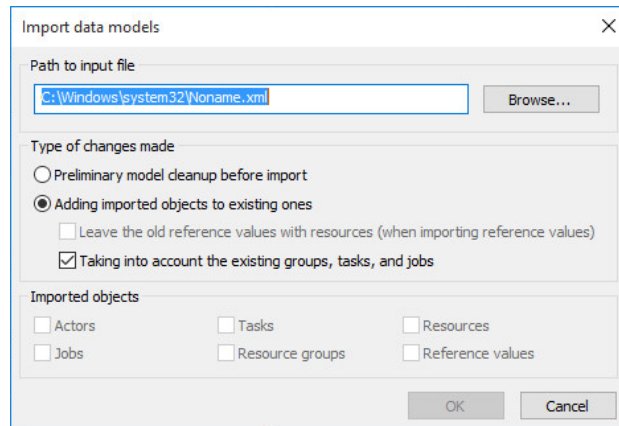
**Note.**

If the file with tasks and scripts was created by centralized tools, script execution will start in the local mode when imported to the program.

**For general import to the data model:**

1. In the File menu tab, click the "Import model from XML" command.
2. If the object lists were changed after the last time the model was saved in the database, a message warning about the loss of changes after the model download appears. Click Yes.

A dialog box asking you to configure import settings appears as in the figure below.



3. Specify the full name of the file, containing the data on the objects in the "Path to input file" field. To specify it, use the keyboard or click Browse to select the file that appears in the standard file open dialog box of Windows.
4. Select an import mode in the field group "Type of changes made". To do this, select one of the check boxes listed below:

Check box	Description
<b>Preliminary model cleanup before import</b>	The current data model's objects are deleted before importing. After importing, the model will only consist of objects contained in the file
<b>Adding imported objects to existing ones</b>	<p>After importing, the model will contain both imported objects and objects of the current data model.</p> <p>When importing, objects may be duplicated. This happens if the "Taking into account the existing groups, jobs and tasks" parameter is disabled or if the model already has objects from these categories with the same names.</p> <p>If the objects belong to Tasks, Jobs or Resource groups categories, the data model will hold pairs of duplicates after importing. The added object of each pair will have a name: object_name&lt;N&gt;, where N is an enumerator of the duplicated object. Objects from the Resources category are not duplicated.</p> <p>When importing resources with reference values, you can select a mode for saving reference values of duplicated resources. To save all reference values, select the "Leave the old reference values with resources (when importing reference values)" check box. Otherwise, after importing, only reference values contained in the file will remain</p>

5. In the "Imported objects" field group, select the object categories for importing. To do this, select the respective categories (if the selected file doesn't have any information on objects from a certain category, the respective field will be blocked).



#### Attention!

While selecting, take into account possible links of objects between different categories. Only objects from the selected categories are imported, and their links to other objects from the categories, which were not selected, are dismissed. For example, imported tasks will not include jobs and resource groups if the categories "Jobs" and "Resource groups" are not selected.

6. If the "Resources" category is selected and the file contains information about resource reference values, you can enable resource import mode together with reference values. To do this, select the "Reference values" check box.

**Note.**

When the resource import mode is enabled along with the reference values, the program will need to save the imported model in the database. A respective message appears after the "Reference values" check box is selected.

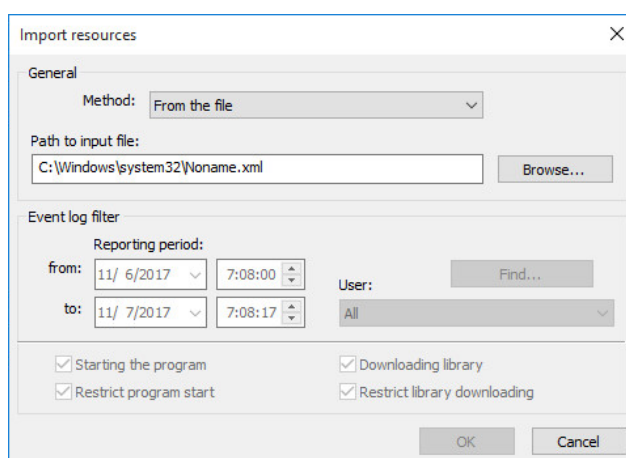
7. Click OK.

**To import objects from the current category:**

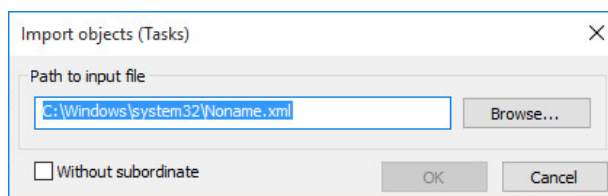
1. On the category panel, select the category from where you want to import objects (except "Control actors" category).
2. Select the root element in the structure window. Open the menu with the name of the selected element (e.g., "Job") and click "Import and adding" command.

A dialog box asking you to configure import settings appears.

- If the "Resources" category is selected, a dialog box appears as in the figure below:



- If the "Tasks", "Jobs" or "Resource" groups categories are selected, a dialog box appears as in the figure below:



3. Specify the full name of the file that contains information about the objects in the "Path to input file" field. To specify it, use the keyboard or click Browse to select the file that appears in the standard file open dialog box of Windows.
4. By default, along with the objects from the selected category, the objects included in the chains of their related objects at the lower hierarchy levels will also be imported (for example, resource group – resources). If you only want to import objects from the selected category without objects included in it, select the "Without subordinate" check box. This check box is not available in the import setup dialog box for the "Resources" category.
5. Click OK.

The objects contained in the file will be added to the object list for the current category. When importing, the objects may be duplicated, i.e., in the current data model there are objects identical to the imported ones. If the objects belong to "Tasks", "Jobs" or "Resource" groups categories, the data model will hold pairs of duplicates after importing. In this case, one object from each pair will be renamed as follows: object\_name<N>, where N is an enumerator of the duplicated object (for example, Resource group and Resource group1). Objects from the "Resources" category are not duplicated.



**Note.**

The targeted import of resource reference values is not performed. If you want to import reference values, follow the instructions for general import of the data model (see above).

## Making changes in the data model

When creating the data model, as well as during using Secret Net Studio, changes can be made in the model. The need for changes is, as a rule, determined by the following factors:

- occurrence of new resource protection tasks;
- updating the computer's software;
- changes in tasks (schedule, control method);
- complete or temporary removal of control over tasks.

All operations associated with changes in the data model can be nominally combined in the following groups:

Operation group	Link
<b>Changing object parameters</b>	p. <a href="#">50</a>
Changing resource parameters	p. <a href="#">50</a>
Changing resource group parameters	p. <a href="#">50</a>
Changing job parameters	p. <a href="#">50</a>
Changing job parameters	p. <a href="#">50</a>
Viewing control actor parameters	p. <a href="#">50</a>
<b>Adding objects</b>	p. <a href="#">53</a>
Adding an individual resource manually	p. <a href="#">53</a>
Adding several resources manually	p. <a href="#">53</a>
Importing a resource list from Windows OS security log	p. <a href="#">53</a>
Importing a resource list from the Secret Net Studio log	p. <a href="#">53</a>
Adding a resource to a group	p. <a href="#">53</a>
Adding a resource group manually	p. <a href="#">53</a>
Adding a resource group based on a directory	p. <a href="#">53</a>
Adding a resource group based on a registry key	p. <a href="#">53</a>
Adding a resource group using import tools	p. <a href="#">53</a>
Adding a job manually	p. <a href="#">53</a>
Adding a job using a job generator	p. <a href="#">32</a>
Adding a job using import tools	p. <a href="#">46</a>
Adding tasks	p. <a href="#">34</a>
Adding actors	p. <a href="#">40</a>
<b>Deleting objects</b>	p. <a href="#">61</a>
Deleting an object	p. <a href="#">61</a>
Deleting all objects of a specific category	p. <a href="#">61</a>
<b>Linking objects</b>	p. <a href="#">62</a>
Linking objects	p. <a href="#">62</a>
Deleting the link between objects	p. <a href="#">62</a>
<b>New calculation and reference values replacement</b>	p. <a href="#">62</a>
<b>Dependent modules search</b>	p. <a href="#">64</a>
<b>Replacing environment variables</b>	p. <a href="#">64</a>

This section covers questions related to the features of the above operations and describes the procedures for their performance.

## Changing object parameters

Each object has a set of parameters. The option of changing the values of certain parameters might be unavailable.

The parameters of objects from each category are given below along with explanations of their application.

### Resource parameters

Parameters determining the properties of a resource are:

- resource type;
- name and full path (with the exception of scripts);
- control feature;
- reference values;
- additional parameters.

"Type" and "Name and Type" parameter values are set when creating the resource description and cannot be changed.

#### Note.

The path can be set explicitly (absolute path) or by using environment variables (see p. 64).

A reference value is a calculated control value for a resource. A resource may consist of several tasks, and each of them may use its own control method. Moreover, depending on the resource type and control method, different algorithms may be used. Therefore, a resource may have several reference values.

The Control attribute means that after enabling the integrity control mechanism (i.e. after linking the task with the computer), this resource will be an actor to control. The absence of the attribute means that the resource, even if it is included in the integrity control task, will not be controlled. Therefore, by setting or removing an attribute, the control of a specific resource can be enabled or disabled.

For executable process files (files with .exe extension as well as files in the "Names of Executable Process Modules" list in the parameters of the program — see p. 79) the following additional parameters can be customized:

- exception parameters that will be applied during operation of the AEC mechanism allow the process to perform any scripts (for example, those run in Internet Explorer) or files from certain folders, including subfolders. Using this function, the option of starting in the hard AEC mode for programs like Photoshop CS2 and SolidWorks is realized;
- process isolation parameters make it possible to provide an isolated environment for the process (prohibit data exchange with other processes).

### To change resource parameters:

1. Select a resource from the objects list, right-click it and click the Properties command.  
The dialog box for setting the resource parameters appears.
2. If necessary, change the status of the Control attribute.
3. To recalculate a reference value, select it in the list and click Recalculate.  
The reference value will be recalculated, and in the Created column, in the line corresponding to it, a new entry consisting of the date and time of recalculation appears.
4. To calculate a new reference value and save its previous value, click the "Double Recalculation" button.  
The new reference value will be recalculated and saved along with the previous value.
5. To delete the reference value, select it in the list and click Delete.

6. If the resource is an executable file, set up additional parameters of exceptions for the AEC mechanism and process isolation. To do this, click **Additionally** and perform the following actions in a dialog box:
  - to permit the process to perform any script, select the "Permit Performance of Any Scripts" check box;
  - to allow the process to run files from specific folders, select the "Permit Performance of Any Modules from Indicated Directories" check box and generate a list of directories. To add a folder to the list, enter the path to it (the path can be entered manually or selected in the standard dialog box called up by clicking the button on the right of the entry line) and click the addition "+" button. To delete a folder from the list, select it and click the delete "-" button;
  - to enable process isolation, select the "Isolate the process" check box;
  - click OK.
7. Click OK.

### Resource group parameters

Parameters determining properties of a resource group are:


- group name;
- description;
- type of resources in the group.

The group's name and brief description can be changed at any time. The type of resources can only be changed if the group does not contain any resource.

#### To change group parameters:

1. Select the group, right-click it and click the **Properties** command.  
A dialog box with group parameters appears. In the **Name** and **Description** fields changes are made manually, and in the **Type** field, the value is selected from a list.
2. Make the changes and click OK.

### Job parameters

In job properties specify the name, description of the job and script (for centralized control). Jobs with a script are denoted by  icon.

#### To change job parameters:

1. Select the job, right-click it and click the **Properties** command.  
The dialog box for setting the job parameters appears.
2. If a script requires changes, click **Script** (generation of a script is described onp. [59](#)).
3. Make changes in the **Name** and **Description** fields and click OK.

### Task parameters

Properties of an integrity control task are determined by the group of common parameters and schedule. The common group of parameters consists of:

- task name and description;
- task type — replicated/non-replicated (only for centralized control);
- control methods and algorithms;
- system reaction to control results.

Control methods and algorithms, system reaction and schedule are parameters that determine the procedure of resource integrity control within the framework of the given task. When changing control methods and algorithms, take into account the types of resources related to the task, since only a certain integrity control method (or selection of methods) can be applied to each type of resource. It should also be mentioned that after changing the control method, it might be necessary to adjust

the system reaction to the verification result. For example, the content recovery method can only be used with the full match algorithm.

### To change task parameters:

1. Select the task, right-click it and click the Properties command.  
The dialog box for setting the task parameters appears.
2. Change the modifiable parameters and click OK. Actions are performed in the same way as in the task generation procedure (see p. 34).

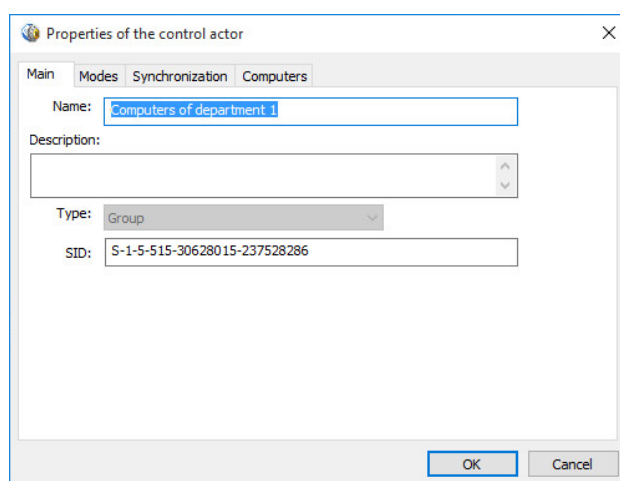
### Actor parameters

Properties of the control actor define the basic parameters (name, type, etc.) and, depending on the actor type, you can configure additional parameters to apply the modes, synchronize data and computer lists for the groups.

### To change actor parameters:

1. Select the actor, right-click it and click the Properties command.

A dialog box appears as shown in the figure below:



The following dialog boxes can be provided depending on actor type and the program's operation mode:

- Main — contains the actor's main parameters (name, description, type, and ID of the actor).
  - Modes — a dialog box is provided for computers and computer groups, and contains the following parameters:
    - method of setting AEC mode (centralized or local);
    - AEC mode status (enabled or disabled);
    - AEC operation mode;
    - modes for additional verification of module integrity and their headers before startup, and scenario (script) performance control;
    - status of the process isolation mode;
    - permission or prohibition of the performance of IC and AEC tasks created in local data models.
  - Synchronization — the dialog box is provided for computers and computer groups in the program's centralized mode and contains CDB and LDB synchronization parameters.
  - Computers — the dialog box is provided for computer groups and designed for viewing and editing the group contents (editing not enabled for "SecretNetICheckDefault" default groups).
2. Change the parameters and click OK.

## Adding objects

Adding objects does not cause any changes in how security mechanisms operate. To apply changes, the added objects must be linked to already existing objects. For example, a new resource added to a model must be included in a resource group. A resource group must be included in a job, and the job, in turn, must be included in a task (a resource group can also be included directly in the task). And, finally, the task must be linked to an actor – a computer, user or group of users/computers.

### Adding a resource

New resources can be added to a data model using one of the following methods:

Method	Description
<b>Automatically, during job generation</b>	Job generation is accompanied by the automatic inclusion of all resources related to it. Before generation begins, an additional condition can be set: whether to include or not include the register objects and whether to add the dependent modules or not. The added resources are connected to the Job object
<b>Manually</b>	Resources are selected from the general list of the computer's resources. Either an individual resource (for example, a file or register key), after being explicitly indicated, or several resources satisfying the set condition can be added manually. The added resources are not connected to other objects
<b>Using import tools</b>	The list of resources can be imported from the following sources: <ul style="list-style-type: none"> <li>• a file with a saved data model (see. p. 46);</li> <li>• the Windows security log or the Secret Net Studio log on a specific computer, or a saved log file (see below)</li> </ul>
<b>By adding the resource to a group</b>	The resource is included in one of the existing groups. The resource may be selected from a list of those already included in the model, as well as from the general list of all computer resources. The added resource is connected to the Resource Group object.

#### For manual addition of an individual resource:

1. Select the Resources category and click the Resources | Create resource(s) | Single command from the menu.

A dialog box appears asking you to select the resource type.

2. Select the required resource type:
  - Windows Resource – if a file, directory, register variable or register key is added;
  - Executable Resource – to add an executable scenario (script).

3. Click OK.

A dialog box for setting the resource parameters appears.

4. Specify the parameters of the added resource (see table below) and click OK.

The following parameters are specified for a file, folder, register variable or register key:

Parameter	Description
<b>Type</b>	Specify the type of added resource: file, folder, register variable or register key
<b>Name and path</b>	Manually enter the name and full path to the resource being added or click Browse and use the standard OS procedure

Parameter	Description
<b>Control</b>	The selected check box means that this resource will be controlled after enabling the IC mechanism. If for any reason the control of this resource needs to be postponed indefinitely, clear the check box. In this case, the description of the resource will be saved in the data model, and it can later be placed under control
<b>Executable</b>	This parameter is available if the type of added resource is a file. It is used to denote executable files, which contain lists of programs allowed to start when the application execution control is enabled

The following parameters are set for an executable scenario (script):

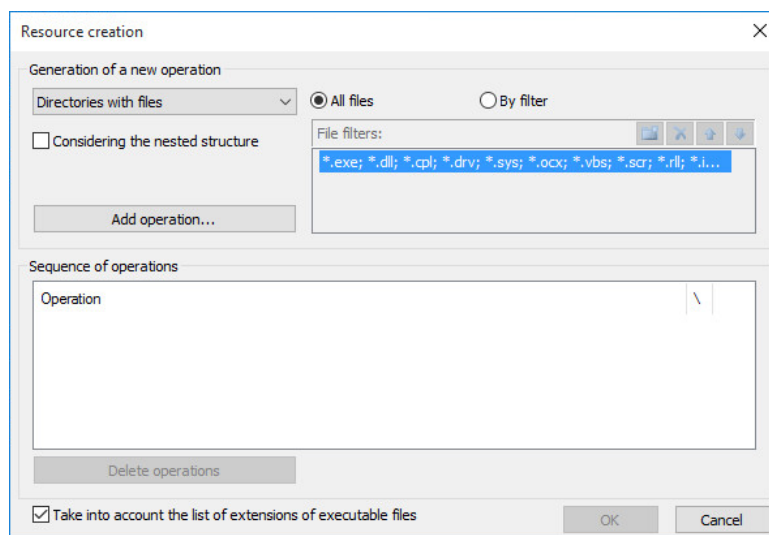
Parameter	Description
<b>Name</b>	Enter the name of the resource, unique for the list of resources. For example, the name of the file from which the scenario (script) can be indicated as the resource name
<b>Description</b>	Enter additional information about the resource
<b>Contents</b>	Enter the scenario (script) text – the sequence of executable commands and/or actions processed using the Active Scripts technology. The script text can be entered manually or loaded from a file using the "Load..." button. To load the text, files containing scripts using the Active Scripts technology (e.g., vbs files) can be used

The resource appears in the list of the main program window. Later, all necessary operations can be performed with the resource (adding it to a group, including in a job, etc.).

#### To add several resources manually:

1. Select the Resources category and click the Resources | Create resource(s) | Multiple command from the menu.

A dialog box appears as in the figure below:



The dialog box contains two parts. The upper part of the dialog box ("Generation of a new operation" group) is for naming the resource selection version and setting additional conditions. Additional conditions are set depending on the selected version. Several conditions can be set for the same version for adding the resources using the filters. To perform an operation, select a version, set additional conditions and then click the "Add operation..." button.

The lower part of the dialog box ("Sequence of operations" group) is for displaying the sequence of performed operations.

Parameters used during operation performance are described in the table below.

Parameter	Explanation
<b>Resource selection version</b>	The following options are available: <ul style="list-style-type: none"> <li>Selected files (standard file selection procedure, additional conditions are not available).</li> <li>Files by directory (files included in the folders are added, nesting is taken into account, a filter can be used).</li> <li>Directories with files (nesting is taken into account, a filter can be used).</li> <li>Directories by directory (nesting is taken into account).</li> <li>Variables by key (variables are selected by the register key, nesting is taken into account).</li> <li>Key with variables (keys with variables are selected, nesting is taken into account)</li> </ul>
<b>Considering the nested structure</b>	The nesting of resources is taken into account for all selection versions, with the exception of the Selected Files version
<b>All files</b>	All resources for the "Files by directory" and "Directories with files" versions are selected
<b>By filter</b>	Enabling the filter for "Files by directory" and "Directories with files" versions. If the list has several filters, then the one selected in the list will be used to select the files
<b>Taking into account the list of extensions of executable files</b>	Set the "executable" attribute for files that have certain extensions or names set by Extensions of Executable and Names of Executable Process Modules parameters (see p. 79). Files with this attribute, when displayed on the main window of the IC-AEC management program, are marked with a special symbol

#### Setting filters.

When the "By Filter" parameter is enabled, the list of filters becomes accessible. Each filter corresponds to one line where extensions of files added to the data model are listed. By default, the list contains one filter that ensures the selection of files with the extensions \*.exe; \*.dll; \*.cpl; \*.drv; \*.sys; \*.ocx; \*.vbs; \*.scr; \*.rl; \*.ime; \*.bpl; \*.ax; \*.acm; \*.com; \*.ppl; \*.cmd; \*.bat. If necessary, the list can be modified or new filters can be added. In the line, file extensions are separated by a semicolon, comma or space.

- To change a filter, select a line, click <F2>, and edit the list of file extensions.
- To add a new filter, click the New button, and enter the list of file extensions in the line that appears.
- To remove a filter from the list, select it and click the Delete button.
- To move a line within the list, select it and click the arrow button.

2. Setting the resource selection parameters. To do this, select the desired option in the drop-down list: Selected files, Files by directory, Directories with files, Directories by directory, Variables by key, or Keys with variables.

3. If you selected "Selected files", click "Add Operation". For other options, go to step 5.

A standard Windows OS dialog box for file selection appears.

4. Select the required files.

A list of operations appears in the lower part of the dialog box. An operation corresponds to each selected file.

#### Note.

If it is necessary to delete an operation, select it in the list and click the "Delete Operations" button.

If it is not necessary to add other resources, go to step 9.

5. If you selected "Files by directory", "Directories with files" or "Directories by directory", configure additional settings (when using a filter, select it in the list) and click "Add Operation". For other options, go to step 7.

A standard Windows OS dialog box for directory selection appears.

6. Select the directory and click OK.

The directory selection dialog box closes, and a description of the performed operation is added in the lower part of the Resource Creation dialog box.

**Note.**

If it is necessary to delete an operation, select it in the list and click the "Delete Operations" button.

If it is not necessary to add other resources, go to step 9.

7. If you selected "Variables by key" or "Keys with variables", select "Considering the nested structure", if necessary, and click "Add Operation".

A standard Windows OS dialog box for viewing the registry appears.

8. Select a register key and click OK.

The register viewing dialog box closes, and a description of the performed operation is added in the lower part of the Resource Creation dialog box.

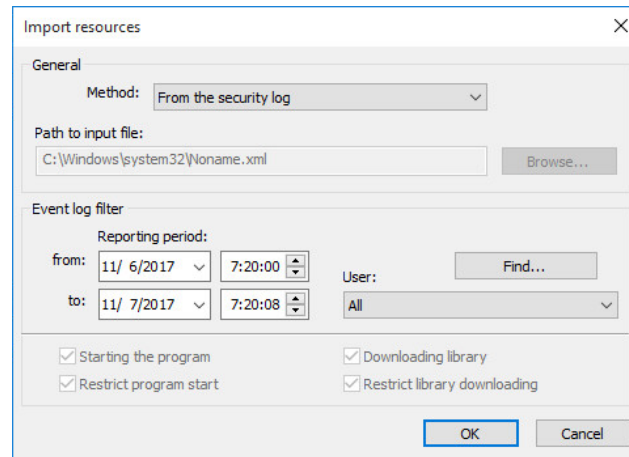
9. Check the list of completed operations, and if it contains all resources you had planned to include in the data model, click OK.

The Resource Creation dialog box closes, and the selected resources will be added to the data model.

**To import the resource list from the Windows OS security log:**

1. Select the Resources category and select the Resources | Create resources | Import and adding command from the menu.

A dialog box appears as in the figure below:



2. Select the "From the security log" value in the Method drop-down list. Filter settings will become available, based on which resources will be selected from the Windows OS security log. Settings include the reporting period (date and time) and user name.

3. Set the reporting period and indicate the user, based on the results of whose work the resources will be selected. You can also select "All" (in this case resources to which all users referred to, will be selected) or select an individual user.

To select the user:

- Click the "Find..." button.

The "Find..." button disappears, and security log analysis starts; if users' access attempts to resources were recorded in the log, the users are included in the drop-down list.

- Select the required user in the drop-down list.

4. Click OK.

**To import the list of resources from the Secret Net Studio log:**

1. Select the Resources category and click the Resources | Create resources | Import and adding command from the menu.

A dialog box appears (see the previous procedure).



2. Select the "From the security log" value in the Method drop-down list. Filter settings become available based on which resources will be selected from the log. Settings include the reporting period (date and time), user name and type of registered event.

**Note.**

Information on resources related to the following events is imported from the Secret Net Studio log: program startup, prevent program startup, loading the library and prevent loading the library.

3. Set the filter parameters and click OK.

**Note.**

Information about resources connected with all foreseen events is imported by default. To cancel the importing of resources related to a certain event, remove the appropriate mark. For the procedure to be performed, at least one mark needs to be placed.

**To add a resource to a group:**

1. Select the Resource Group category.
2. In the additional structure window, select the group to which you want to add new resources, call up the context menu and click the "Add Resources" command and then:
  - Existing — to select resources from those available in the data model, but not included in this group.
  - New single — to add an individual resource (see above for the description of the procedure for manually adding an individual resource).
  - Multiple new — to add several resources (see above for the description of the procedure for manually adding several resources).
  - Import — to import a list of resources from another source: from a file (for a description of the object import procedure, see onp. 48), from security log or Secret Net Studio log (for a description of the resource import procedure, see above).

The selected resources will be added to the group.

**Adding a resource group**

A new resource group can be added to the data model:

- manually;
- by directory;
- by registry key;
- by log;
- using import tools.

**Note.**

A group of resources can be added directly to the job either manually, by folder, or by registry key. The group of resources added in this manner will be linked to the superior object.

The file with previously exported log data is used as a source for adding a resource group in the centralized control mode. In local mode, the security log or Secret Net Studio log may be used as a source.

**To add a resource group manually:**

1. Select the "Resource Group" category.
2. Click the Resource Groups | Create group | Manually command in the menu. The dialog box for configuring resource group settings appears.
3. Fill out the dialog box fields and click OK. Specify the type of resource group (in the Type field).

The new group will be added to the list of resource groups.

**To add a resource group by directory:**

1. Select the "Resource Group" category.
2. Click the Resource Groups | Create group | By directory command in the menu.

A standard Windows OS dialog box for directory selection appears.

3. Select the directory and click OK.

The new group will be added to the list of resource groups, and directory files will be added to the list of this group's resources.

**To add a resource group by registry key:**

1. Select the "Resource Group" category.
2. Click the Resource Groups | Create group | By registry key command in the menu.

A standard Windows OS dialog box for registry viewing appears.

3. Select the required registry key in the respective section and click OK.

Resources corresponding to the selected registry key will be added to the data model as a part of the new group.

**To add a resource group by log:**

1. Select the "Resource Group" category.
2. Click the Resource Groups | Create group | By log command in the menu.

A dialog box to select a resource type appears. The resource types are defined on the basis of log records: loadable application modules or executable scripts.

3. Select a resource type to obtain from the log:
  - Downloaded modules – if the group should contain files that were downloaded during the work of the application;
  - Executable scripts – if the group should contain scripts with download records registered in the log.

4. Click OK.

A setting dialog box appears.

5. In the centralized mode, click Select and select the file to which data from the log was previously exported (in 'dvt' or 'snlog' format).

In the local mode, select the method (the security log or the Secret Net Studio log).

Depending on the mode and the selected method, event log settings will become available.

6. Set the filter settings and click OK.

A message appears for adding a new object to the model.

**To add a group of resources using import methods:**

1. Select the "Resource Group" category.
2. Click the "Import and adding" command in the "Resource Groups" menu or in the context menu called for the "Resource Groups" folder.

The dialog box for setting the import parameters appears.

3. Perform actions to import category objects (see a description of the import procedure on p. 46).

**Adding jobs**

A new job can be added to a data model using one of the following methods:

- manually;
- manually with a script;
- using a job generator (see p. 32);
- using import tools (see p. 46).

**To add a job manually:**

1. Select the Jobs category and click the Jobs | Create job(s) | Manually command from the menu.

The dialog box for setting the job parameters appears.

2. Enter a job name, a brief description and click OK.

In the data model, a new job appears not connected to other objects.

### To add a job with a script manually:

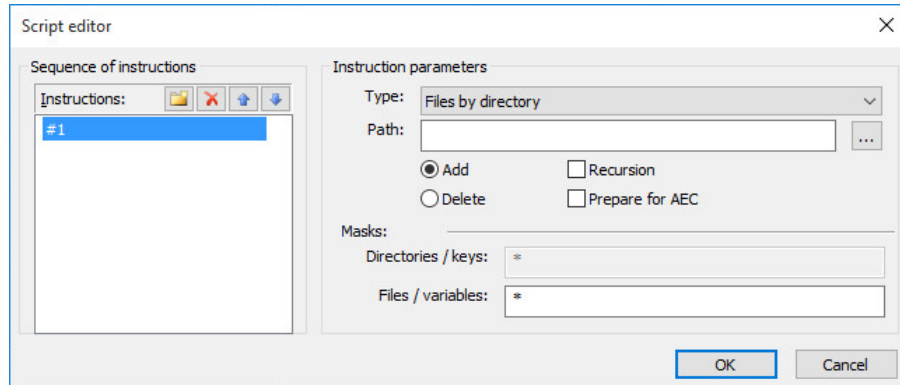
1. Select the Jobs category and select the Jobs | Create job(s) | Manually command from the menu.

The dialog box for setting the job parameters appears.

2. Enter the job's name and its brief description.

3. Click the Script button.

A dialog box appears as in the figure below.



A job script is a sequence of commands determining the resource selection rules for a job.

4. To add a command, click the button in the left part of the dialog box and enter the command name describing its meaning content.

In the right part, fields for configuring command parameters become available.

5. Select the resource type and specify the path.

Available types are listed in the following table.

Resource type	Description
<b>Files by directory</b>	Files are selected from the directory indicated in the "Path" field. To select files, the mask indicated in the "Files/Variables" field can be used
<b>Directories with files</b>	Directories and files are selected based on the indicated path. When selecting, masks for directories and files indicated in the "Masks group" fields can be used
<b>Variables by key</b>	Only registry variables are selected by the pre-set registry key. A path is indicated to set the basic registry key. During selection, the mask indicated in the "Files/Variables" field can be used
<b>Keys with variables</b>	Registry variables are selected by the pre-set registry key as well as keys. A path is indicated to set the basic registry key. When selecting, masks indicated in the "Masks group" field can be used
<b>Installed programs (MSI)</b>	Resources of the program selected in the list of installed programs (Microsoft Installer) are chosen. To select directories and files, masks indicated in the "Masks" group field can be used
<b>Secret Net Studio components</b>	Resources from the software of the Client are selected Secret Net Studio
<b>Files from variables in the specified registry key</b>	Files received from registry variables by the pre-set registry key are selected. A path is indicated to set the basic registry key (for example, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run). During selection, the mask indicated in the "Files/Variables" field can be used

Resource type	Description
<b>Downloaded Windows drivers and services</b>	Files of the operating system's drivers and services are selected

Depending on the selected type, certain parameter entry fields may be unavailable.

**6.** Specify actions for the command.

The Add check box is used to add the selected resources to the general list of job resources. The Delete check box is used to delete resources from the general list generated by previous commands.

**7.** To apply the command to all embedded resources, select the Recursion check box.

**8.** When "Files by directory" or "Directories with files" type is selected, if necessary, use the option for adding to the list of dependent modules (see p. 64). To add dependent modules, select the "Prepare for AEC" check box. This will also automatically select all dependent modules for files specified with the mask. They are added to the model and are marked as executable. In other words, the result is the same as when performing the procedure for searching and adding dependent modules, but not on this computer or on all computers where the generated script will be run.

**9.** Depending on the selected resource type, enter a resource selection mask in the Directories/Keys or Files/Variables fields.

Several masks can be entered in the field by dividing them with the following symbols: "," (comma), ";" (semicolon) or space. By default, a "\*" mask is set. It means that all resources satisfying command parameters are selected. If the "\*" mask is deleted and the field is left empty, the command is not run.


**Note.**

For the resource type "Installed MSI Programs", the mask can be specified in the Name field. In this case, one of the following methods for setting the mask can be used: <text fragment>\*, \*<text fragment> or \*<text fragment>\*.

**10.** To add and configure the next command, repeat actions 4–9.

To change the command execution sequence, use the respective buttons on the left of the dialog box.

**11.** Click OK. Then, click OK in the job properties dialog box.

In the main program window, the job with  icon appears.

### Adding tasks

Task adding procedures are described in detail on p. 34.

### Adding actors

In the centralized mode, computers and groups containing computers can be added to the data model. In the local mode, you can add users and user groups. After you add the actors, they are identified in the list by ! sign (as not related to other objects).

#### To add computers (the centralized mode):

**1.** In the category panel, select the "Control Actors" category.

**2.** From the "Control Actors" menu, click the "Add to list" command.

A dialog box to select the type of added actors appears.

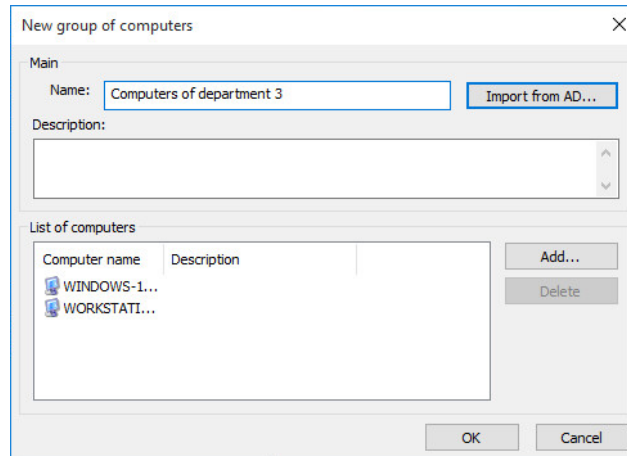
**3.** Select the Computer field and click OK.

A dialog box with the list of security domain computers with the Client appears.

**4.** Select the required computer in the list and click OK.

**To add a computer group (the centralized mode):**

1. In the category panel, select the "Control Actors" category.
2. From the "Control Actors" menu, click the "Add to List" command.  
A dialog box to select the type of added actors appears.
3. Select the "Computer group" check box and click OK.  
A dialog box to configure the created group appears.



4. If there is a group in Active Directory with computers required for creating a group in the data model, you can import information on this object from AD. To do this, click "Import from AD" and, in the Windows dialog box, select the required computer group.
5. Enter the name and additional information about the created group in the respective fields.
6. Generate the list of computers in the group. To add and remove items in the list, use the buttons on the right.
7. Click OK.

**To add users and user groups (the local mode):**

1. In the category panel, select the "Control Actors" category.
2. From the "Control Actors" menu, click the "Add to List" command.  
A Windows dialog box to select the users and groups appears.
3. Select the required objects and click OK.

**Deleting objects**

When deleting an object from a data model, consider its links to other superior or subordinate objects. So, before deleting a resource, check which tasks it is controlled by and analyze the probable consequences of its removal.

**Attention!**

After deleting resources from a task, recalculate reference values.

**Warning.**

In the local mode, you cannot delete the "Computer" actor, tasks, jobs, resource groups or resources added into the model through centralized control. Nor can you delete links between such objects. In the centralized mode, you cannot delete a default group "SecretNetICheckDefault" or "SecretNetICheckDefault64" (depending on the OS bit depth).

**To delete an object:**

1. Select the object, right-click it and click the Delete command.

If the confirmation is disabled in the program settings, the object is deleted from the data model. All subordinate objects without any links to any other superior objects will be deleted.

2. If the confirmation is enabled in the program settings, a dialog box appears showing the object to be deleted with superior or subordinate objects. If you also want to delete subordinate objects from the data model, select the "Delete subordinate" check box. In this case, all subordinate objects without any links to any other superior objects will be deleted.

3. Click Yes.

The object (objects) will be deleted from the data model.

#### To delete all objects of a certain category:

1. Select the category (Control actors, Jobs, Tasks, or Resource groups) in the structure window right-click the root folder and click the "Delete All" command.

A dialog box with links to the objects appears.

2. If you want to delete all subordinate objects, select the "Delete subordinate" check box. Click Yes.

All objects from the selected category will be deleted from the data model.

## Links between objects

Depending on the method used for adding new objects into the model, the links may be established automatically. For example, when adding a new resource of the model into the group, the link resource-group is established. A link may also be established when the object is imported.

In other cases, the model receives objects without links to other objects, for example if a new job or task is created manually. That is why, after adding, absent links between superior and subordinate objects should be established manually.



#### Attention!

In the local mode, centrally created objects cannot be added: to job – task, to task – resource group, to group – resource.

#### To establish links between objects:

1. Select the object's category, right-click the required object and click the Add <name of the object> | Existing command.

A dialog box with a list of objects not linked to this object appears.

2. Select the required objects from the list and click OK.

As a result, a link between the selected objects and a superior object will be established.

#### To delete links between objects:

1. Select the category of the object whose link to the superior object should be deleted, select the object, right-click it and click the Delete from | <name of the object> command.

#### Note.

The object may be simultaneously deleted from all superior objects.

A warning message on deleting links with superior objects appears.

2. Click Yes.

## New calculation and reference values replacement

If you making changes to a data model, you can perform a new reference values calculation for the resources under control in the same way as when configuring the data model (see p. 37). The following methods are also available:

- reference values calculation for a specific resource;
- reference values calculation for several randomly selected resources.

The reference values calculation for a resource is performed across all tasks which include this resource. As one resource can be included in different tasks and each task has its own control method for the resource, the reference values calculation is performed for each method.

During the reference values recalculation, it may be necessary to save previous (old) values. For example, when controlling the content of files changed during automated software update.

**Note.**

If the integrated EDS algorithm is used for content control, in most cases, it is not necessary to save previous reference values for this algorithm. As a general rule, signed file certificates remain unchanged after a software update. That is why reference values for these files remain valid before and after a software update.

Previous (old) reference values are automatically deleted from the local database after each successful completion of integrity control task. If necessary, you can run a command for the immediate deletion of old reference values.

**To recalculate a reference value for a certain resource:**

1. Select a resource from the objects list, right-click it and click the Properties command.  
A Resource properties dialog box appears (see p. 50).
2. Select a reference value from the list and click Recalculate.  
The reference value will be recalculated and the calculation date in its line will change.
3. Perform recalculations for the remaining reference values and click OK.

**To calculate reference values for the selected resources:**

1. Select the Resources category or expand the model structure so that you can see resources in the object list window.
2. Select a resource or several resources from the list, right-click them and click "Reference values calculation".  
A "Reference values calculation" dialog box appears.
3. Perform actions as instructed for the reference values calculation procedure in the local mode, starting from step 2 (see p. 37).

**To delete old reference values:**

- From the menu, click the Service | Reference values | Delete old command.  
Old reference values will be deleted from the data model.

## Disable local jobs

By default, local and centralized jobs can be performed on computers. If necessary, you can disable the local jobs (created in the local database in the program's local operating mode) so that only centralized jobs are performed on the computers.

You can disable the local jobs in the properties of the required actor in the centralized operating mode. The parameters can be defined for separate computers and for groups of computers. In this case, the disabled parameters have priority. For example, if the "Local AEC jobs" check box is disabled for the group, such jobs will be prohibited on the computer, even if this parameter is enabled for this computer.

**To disable local jobs:**

1. In the category panel, select the "Control Actors" category.
2. In the additional window, select the structures or, in the list of objects, a computer or group (of computers), right-click them and select the "Properties" command. In the "Properties of the control actor" window, select the "Modes" tab.
3. Clear the the respective check boxes:
  - to disable integrity control jobs – clear the "Local IC jobs" check box;

- to disable application execution control jobs – clear the "Local AEC jobs" check box.

4. Click OK.

## Searching for dependent modules

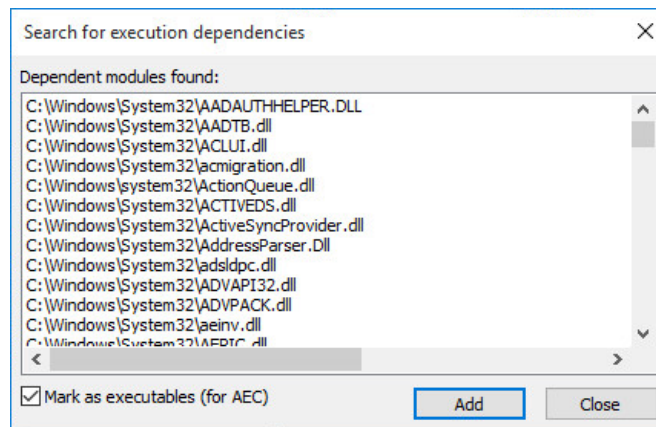
When the user works with applications, executable files may be run together with modules (drivers and libraries) which are not directly integrated into the applications. Such modules are called dependent.

When building a data model with automated tools (wizard and task generation utility), dependent modules and their inclusion in the data model are searched for by default. When manually building a data model and including new resources in the data model, the search for dependent modules is performed separately (see below).

### To find and include dependent modules:

1. Select a resource or several resources from the object list, right-click them and click the "Dependencies" command.

A dialog box with a list of found dependent modules appears as in the figure below.



2. Clear the "Mark as executables (for AEC)" check box if you do not need the dependent modules to be marked as executable in the data model.
3. Click Add.

The modules will be added to the data model. Then a message box informing about successful completion appears.

## Replacing environment variables

For a data model transferred from one computer to another to work properly, as well as when exporting individual resources, tasks and jobs, it might be necessary to replace absolute paths to resources with environment variables.

This procedure is performed on the computer from where the model will be transferred or its individual elements will be exported.

Replacing environment variables with absolute paths is a reverse operation performed when, for some reason, it is necessary to restore the absolute paths.

### To replace environment variables:

1. Select a resource in the data model and click the "Environment Variables" command in the context menu.

A dialog box containing a list of environment variables available on the computer appears.

2. Specify the change direction:

- To replace absolute paths with environment variables, leave the default check box.



- To replace environment variables with absolute paths, select in the "Names of environment variables to value of paths in files and folders" check box.
3. Select the variables from the list for which the action is to be performed.
  4. Click OK.

## Chapter 5

# Audit parameters

### Configuring event registration on computers

#### Setting up log parameters

When setting up parameters, the restriction on the maximum volume of the Secret Net Studio log and the policy of rewriting stored information can be changed.

The description of the centralized setup procedure at the administrator's workplace in the Control Center is provided below (seep. 11). Local setup is performed in the same way as using the Control Center in the local mode.

#### To set up log parameters:

1. In the Control Center, click the Computers panel and select the object you want to configure. Right-click the object and click Properties. In the properties panel, select the Settings tab and click "Load Settings".

#### Note.

For information about the Control Center, see document [4].

2. In the Policies section, select Log.
3. For the "Maximum size of the security system log" parameter, set the value of the maximum size of the log in kilobytes. The range is from 64 to 4,194,240 KB (in increments of 64).
4. For the "Event overwrite policy" parameter, select the method for clearing the log when it is full. For this purpose, select one of the check boxes below.

<b>Erase events if necessary</b>
When the log is full, the System will automatically remove from the log the required number of the oldest records
<b>Erase events older than &lt;...&gt; days</b>
When the log is full, the System will automatically remove the records whose storage time exceeds the preset period. New records will not be added if the log reaches its maximum size and does not contain records older than the preset period. Entry range – from 1 to 365 days.
<b>Do not erase events (clear log manually)</b>
After the maximum size is reached, records are kept in the log. New events are not registered in the log. The log can only be cleared using the Control Center. Clearing should be performed regularly in order not to allow the log to be full, because this might lead to system failures and lock the computer

5. Click Apply.

#### Selecting events for registration

By default, all possible events are registered in the Secret Net Studio log except for Application Control, Integrity Control and Discretionary Access Control categories.

#### Attention!

Some events must be registered. Such events may include Registration category events. Registration of such events cannot be disabled.

The description of the centralized setup procedure at the administrator's workplace in the Control Center is provided below (seep. 11). Local setup is performed in the same way as in the Control Center.

**To set up the list of events to be registered:**

1. In the Control Center, click the Computers panel and select the object you want to configure. Right-click the object and click Properties. In the properties panel, select the Settings tab and click "Load Settings".

**Note.**

For information about the Control Center, see document [4].

2. Select the "Event Registration" section.
3. Select the Enable check box for the events that need to be registered in the log.
4. Click Apply.

## Setting up shadow copying storage parameters

When setting up the parameters, the limit of the maximum storage volume can be changed and the re-recording can be enabled or disabled.

The description of the centralized setup procedure at the administrator's workplace in the Control Center is provided below (see [1.1](#)). Local setup is performed in the same way as in the Control Center.

**To set up the storage settings:**

1. In the Control Center, click the Computers panel and select the object you want to configure. Right-click the object and click Properties. In the properties panel, open the Settings tab and click "Load Settings".

**Note.**

For information about the Control Center, see document [4].

2. In the Policies section, select the "Shadow Copying" group of parameters.
3. For the "Storage size" parameter, set the required storage size as a percentage of disk space.
4. Select the version of system reaction if the storage is full:
  - to allow data output, select the "Automatically rewrite old data in case of storage overflow" check box. In this case, copies of the output data will replace the oldest copies placed in storage;
  - to prohibit data output, clear the check box. When the maximum size of the storage is reached, the system will block new data output attempts.
5. Configure the registration of events related to the mechanism. To go to the required group of registration settings, click the "Audit" link.
6. Click Apply.

## Application control setup

Secret Net Studio can register the events of startup and ending processes of executable files as well as access operations to these processes.

The following options are available for audit monitoring of the startup and ending processes:

- event registration for applications which are launched by users;
- event registration for all processes in the System – not only user applications, but also system ones.

**Note.**

Registration of all system process events may significantly increase the load on the core of Secret Net Studio and cause the log be quickly full with records of these events. In most cases, this registration mode is not required. Therefore, the registration of events only related to user applications is enabled by default.

Attempts to access such processes are controlled if the process isolation mode is enabled. For proper use of isolation mode, we recommend configuring it along with the

AEC mechanism. For procedures to enable and configure the isolation, see in the document [5].

Registration of allow or prohibit events may be enabled for the following operations with isolated and not isolated processes:

- access to the clipboard;
- access to the contents of the process window;
- transfer of data between processes using the drag-and-drop method.

Application control of event registration setup is performed in the Control Center.

The description of the centralized setup procedure at the administrator's workplace in the Control Center is provided below (seep. 11). Local setup is performed in the same way as in the Control Center.

#### To set up Application Control:

1. In the Control Center, click the Computers panel and select the object you want to configure. Right-click the object and click Properties. In the properties panel, select the Settings tab and click "Load Settings".

#### Note.

For information about the Control Center, see document [4].

2. In the "Event registration" section, select the "Application control" group of parameters.
3. To enable audit of starting and ending monitoring for all system processes, select the "Audit of system processes (in addition to custom processes)" check box. If the registration of Applications launched only by the user is enough, clear the check box.
4. For the remaining parameters in the "Application control" group of parameters, select the events to be registered in the log.
5. Click Apply.

## Granting log access rights

Access to log entries is granted to employees responsible for managing the Secret Net Studio. The rights for loading entries and managing log contents are determined by user privileges:

- privileges for working with local logs;
- privileges for working with centralized logs.

### Privileges for working with local logs

The following privileges are granted for working with local logs:

- View the Secret Net Studio log. The user can download the Secret Net Studio local log entries for viewing;
- Security system log management. The user can download Secret Net Studio local log records for viewing and log cleaning.

#### Note.

Secret Net Studio log management privilege includes permission to view Secret Net Studio log. However, in all cases, when users need a privilege for log management, we recommend you to grant both privileges.

The description of the centralized setup procedure at the administrator's workplace in the Control Center is provided below (seep. 11). Local setup is performed in the same way in the local Control Center.

#### To grant privileges:

1. In the Control Center, click the Computers panel and select the object you want to configure. Right-click the object and click Properties. In the properties panel, select the Settings tab and click "Load Settings"

**Note.**

For information about the Control Center, see document [4].

2. In the Policies section, select Log.
3. Edit lists of privileged users and user groups for the parameters "Accounts with the privilege to view the security system log" and "Accounts with the privilege to manage the security system log".
4. Click Apply.

## Privileges for working with centralized logs

Using the Control Center you can download entries from centralized logs. The privileges provided for working with the program are described in the document [4].

## Chapter 6

# Local audit

### About event registration

#### Local event registration logs

The information about registered events is stored as entries containing detailed information for event analysis.

#### Secret Net Studio log

The event log of Secret Net Studio (hereinafter, the Secret Net Studio log ) accumulates information about events registered in the computer by the Secret Net Studio tools.

Data contained in the Secret Net Studio log allows the operation of security mechanisms to be controlled (log-in security, hardware configuration control, integrity control, etc).

The composition of registered events is defined by specified parameters of a security policy.

The Secret Net Studio log uses the same data format and entry field composition as the standard Windows OS logs. To work locally with log entries, the Control Center is used in on-premises mode.

#### Standard Windows OS logs

Standard Windows OS logs only register events related to the operating system. Standard logs contain:

- the application log that contains data on errors, warnings and other events occurring when working with the application;
- the system log that contains data on errors, warnings and other events occurring in the operating system;
- the security log that stores information about user access to the computer, the application of group policies and changes in access rights, as well as on events caused by the use of system resources.



#### Note.

Descriptions of the contents of Windows OS standard logs and event registration setup procedures are available in the operating system documentation.

The subsystems of Secret Net Studio do not register events in standard logs (except for the application log, where certain specific errors related to the OS operation can be registered).

When working in the local mode, you can use the Control Center to load and view entries of standard logs, locally stored on the computer. In this case, it is still possible to upload the entries to other tools for working with Windows OS logs.

#### Shadow copy storage

In a shadow copy storage, duplicates (copies) of data are stored on removable media. The duplicate storage is a specially arranged location in the system folder on the computer's local disk.

Access to the shadow copy storage is provided on the basis of log management privileges. If a user is granted log viewing privilege, the user will be given read-only access to the storage. If a user has log management privileges, they can perform administrative operations with the storage.

The storage size and methods for filling it are determined by the parameters of the security policy.

## Storing and deleting local logs

When events are registered, related entries are placed into respective local logs (standard Windows OS logs and Secret Net Studio log) and stored on the computer locally. While the entries are kept in the local storage, they can be loaded to the Control Center in local mode or to other programs that allow loading of logs (except for Secret Net Studio log).

On the Clients in the network operation mode, local logs are kept in the local storage until they are transferred to the centralized storage on the Security Server. After entries are transferred, local logs are deleted.

In the standalone mode, the logs can only be stored in the local storage.

While events are registered, log entries in the local storage can be replaced by new entries. Information in logs is overwritten in accordance with preset parameters of event registration.

In the Control Center, the user can export log records to files. If the user is granted the respective privilege, he or she can also delete the logs.

## Local work with logs

The Control Center in the on-premises(local) mode can be used for working locally with logs (seep. 11). The procedures for downloading and managing entries in the local logs and logs stored in files are the same as in the centralized operation mode. Information about how to work with the Control Center in the centralized mode is provided in the document [4]. Below you can find the description of the features only available when you work with the program in the local mode.

## Exporting local log entries

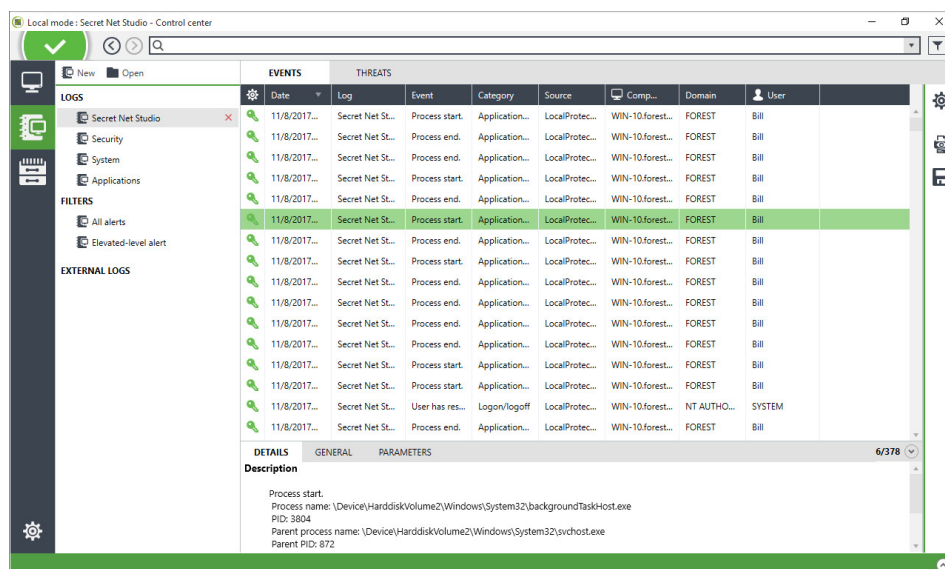
The Control Center makes it possible to export (save) local log entries to files. When exporting, you can clear the log after saving the entries. The following table lists the supported formats for saving.

Name	Format	Description
*.snlog	Secret Net Studio log entries	You can save the entries loaded into the program in full or selectively. The log is not cleared
*.evtx	Standard format for Windows event logs	The file stores all contents of the selected log (including entries that are not loaded into the program). When a log is exported in this format, it can be cleared after the entries are saved

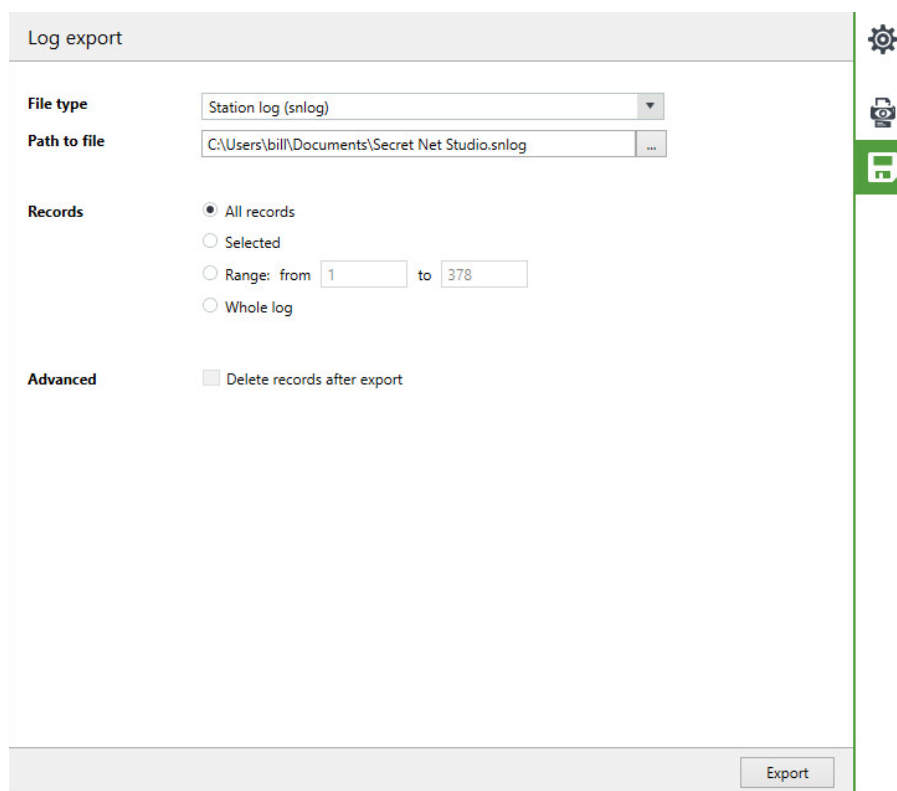
### To export entries:

1. Load the entries of the required log to the program.

The Control Center window in the local mode with loaded Secret Net Studio log entries is shown in the figure below.



2. If you want to export some of the loaded entries (when exporting to "snlog" file), 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.



4. In the "File type" drop-down list, select the required export format.
5. In the "Path to file" field, enter the full name of the file to save or click the button in the right part of the field to select the file in the Windows file saving dialog box.
6. Configure export settings.

**"Records" group of fields**



Defines what entries will be exported to "snlog" file:

- "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 filtration settings)

#### Delete records after export

If selected, the System will automatically clean the log after exporting the records to .evtx file.

To clear the Secret Net Studio log, you must be granted the privilege of "Security system log management" (see p. 68)

7. Click Export.

## Viewing the shadow copy storage

To view the shadow copy storage and perform standard operations with files (copy, start, open, etc.), use the Windows OS Explorer program. The Explorer program can be called up from the Control Center in local mode.



#### Attention!

When using the Explorer program, all operations related to deleting the files from the storage are blocked.

The following features are provided to view the files in the shadow copy storage:

- opening the main storage folder;
- opening the temporary files folder, where a copy of the selected file with its original name was previously created.

#### Opening the main storage folder

The main folder of the shadow copy storage is the root folder in the storage file structure.

#### To open the window with the main folder of the storage:

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

The panel for calling up the configuration tools appears.

2. Click "Open the folder of the shadow repository..." link.

The Explorer program window with the contents of the main folder of the storage appears.

#### Creating a temporary copy of a file

When registering a shadow copy event, duplicate copies of files to be placed on removable media are placed in special service folders in the storage. The duplicate files are assigned internal names generated on the basis of file checksums and timestamps. Therefore, it may be difficult to go to the required file when viewing the contents of the storage.

The Control Center makes it possible to generate the required file with an original name and quickly go to that file. This file is created in a temporary storage folder based on the duplicate file. The file is generated by using a Secret Net Studio log entry that contains information on the shadow copy event with the original file name.



#### Attention!

The folder with temporary storage files is automatically cleaned each time you start the Control Center.

#### To open a window with a temporary copy of the file in the storage:

1. Load the entries of the Secret Net Studio local log into the program.



## Chapter 7

# Additional features of the local administration

## Editing a computer's registration information

The computer registration information may indicate the following details:

- name of the department where the computer is used;
- name of the company's information system;
- the computer's location;
- system unit number.

You can enter the registration information when installing the Client software or later. The options for editing the accounting information are provided in the Control Center (see the document [4]), as well as in the Secret Net Studio settings dialog box

### To edit the registration information in the Secret Net Studio settings dialog box:

1. In the Windows Control Panel, select Secret Net Studio management icon.  
This Secret Net Studio settings dialog box appears.
2. Select the "Computer information" tab.
3. Enter computer information in the respective fields.
4. Click Apply or OK.

## Local alert notifications

An alert is an event registered in the Secret Net Studio log or a standard OS security log, and its type is Audit Failure or Errors. When such events occur, the Secret Net Studio may locally notify the current computer user of this fact.

The mode for local alert notification can be enabled and disabled for all users of the computer (computers), or users can be provided the option to manage the mode independently.

The description of the centralized setup procedure at the administrator's workplace in the Control Center is provided below (see. 11). Local setup is performed in the same way in the local Control Center.

### To manage the local alert notification mode:

1. In the Control Center, click the Computers panel and select the object you want to configure. Right-click the object and click Properties. In the properties panel, select the Settings tab and click "Load Settings"

#### Note.

For information about the Control Center, see document [4].

2. In the Policies section, select the "Alert Notification" group of parameters.
3. For the "Local alert notification" parameter, specify the mode of operation or select "User-defined".

#### Note.

The user switches the local notification mode using the "Alert Notification" command in the context menu of Secret Net Studio icon located in the Windows task bar.



4. Click Apply.

## Local registration of licenses

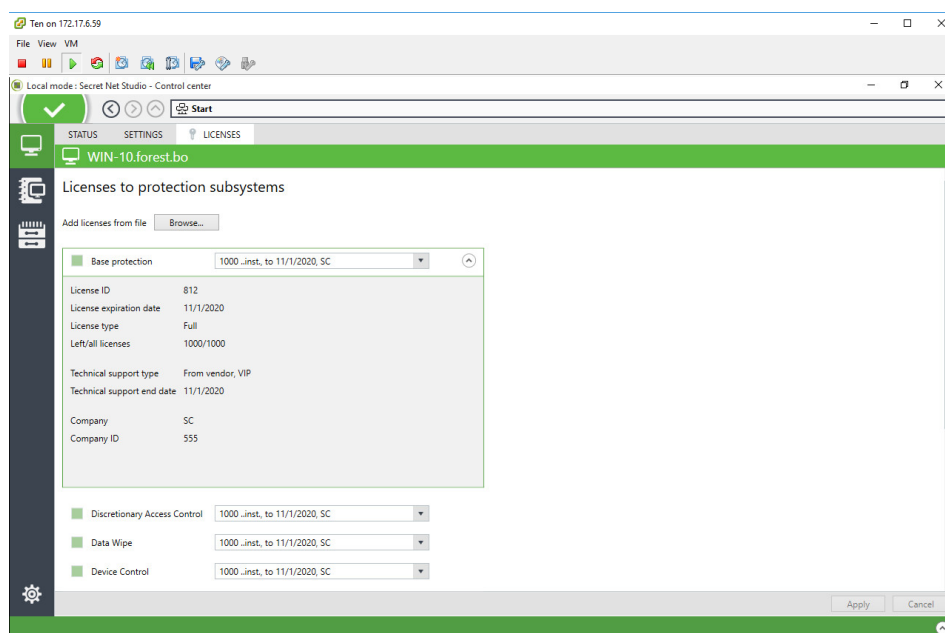
The Secret Net Studio uses license limitations for the use of several subsystems that apply security mechanisms. Licenses are registered by using special files.

For the Clients in network operation mode, licenses are registered on the Security Server. When the Client connects to the Security Server, the system checks the license terms, and the Client license is downloaded from the Security Server to the local Client storage. Licenses are registered on the Security Server in the centralized mode in the Control Center (see the document [4]).

The System also provides for local registration of licenses on protected computers. The Client may require local registration in the standalone mode, as well as in the network mode, if you cannot connect to the Security Server for a long time.

### For local registration of licenses:

1. Run the Control Center in the local mode (see p. 11).
2. In the Computers panel, select the Licenses tab.



The tab displays a list of licensed subsystems and information about the status of the current license. Activated subsystems (with valid licenses) have marks to the left of their names. To display detailed information on the subsystem's license, hover your mouse over the line with the subsystem name and click the button which appears in the highlighted line to the right.

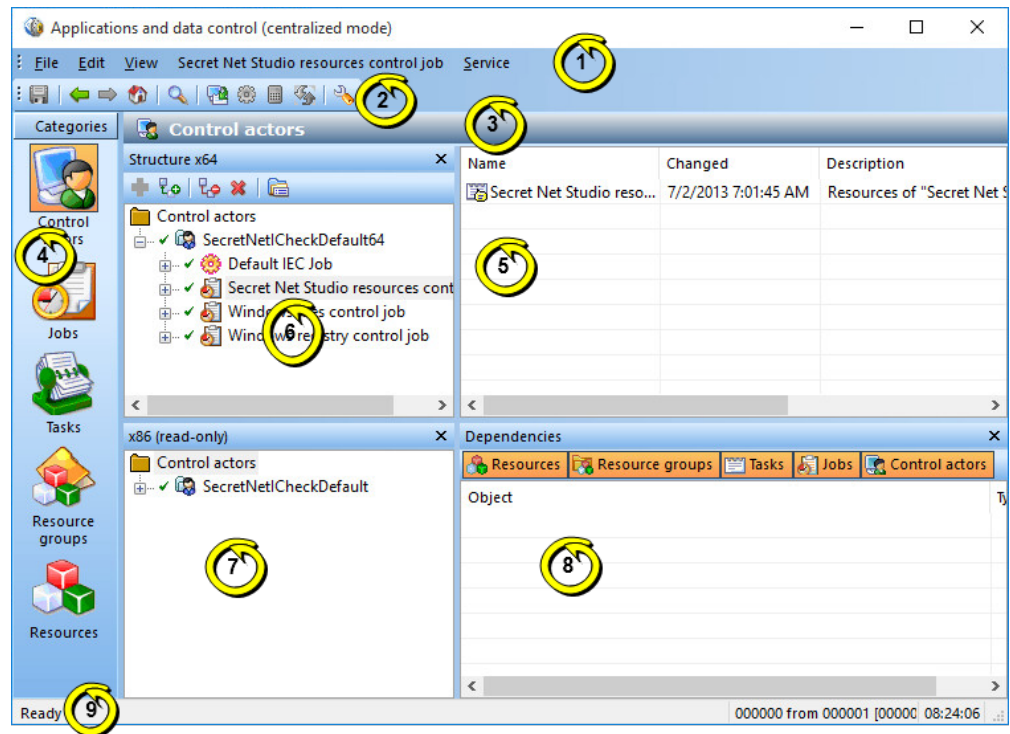
3. If there is a file with licenses to be registered, click the Select button located above the licensed subsystems list. In the selection dialog box, select the file with licenses.  
After data processing, the license list will be amended.
4. To manage subsystem activation (by enabling or disabling licenses), use the controls located to the left of the subsystem names. When the license is disabled, you will see a blank field with information on the subsystem's license and a message about license removal will appear.
5. To save the current configuration of the licenses, click Apply.

# Appendix

## About the Applications and data control program

### Program interface











The main window of the program in the centralized mode is shown in the figure below:







The main program window may include the following interface elements:

<b>1 – Menu</b>
Contains program commands
<b>2 – Main window toolbar</b>
Contains hot keys for commands and software tools
<b>3 – Informative title</b>
Contains the name of the category of objects selected for display
<b>4 – Category panel</b>
Contains shortcuts for performing commands identical to the View menu. Click the shortcut on the panel to display objects which belong to the required category
<b>5 – Object list area</b>
Contains a list of objects linked to the selected element in the structure window. By default, the following color scheme is used for the line background: <ul style="list-style-type: none"> <li>• white background – the object is linked to superior or subordinate objects;</li> <li>• pink background – the object is not linked to superior or subordinate objects;</li> <li>• gray background – the resource is not under control.</li> </ul> In local mode, centrally installed object names are highlighted. You can change the color scheme (see p. 79)
<b>6 – Structure window</b>

Contains a hierarchical list of objects. The selected object category is the root element of the hierarchy. The following icons are used for the objects:

 — actor;  — AEC job;  — replicated AEC job;  — IC job;  — replicated IC job;  — task;  — task with script;  — group of files and catalogs;  — group of scripts;  — group of registry objects.

The following icons are used for links between objects:

-  (lower part of the circle is red) — the object does not include other objects;
-  (upper part of the circle is red) — the object is not included into any other object;
-  — the object has no links;
-  — the object has all possible links with other objects.

Toolbar buttons in this window are designed for object list management.

The structure window contains the object list for the data model which corresponds to the bit depth of the Windows OS. The object list is editable

### 7 — Structure window for the data model with different bit depth

Appears only in the program's centralized operating mode. This window's purpose is similar to the structure window's purpose (6), but it contains the data model object list with different bit depths (for example, models for 64-bit Windows OS versions if a 32-bit OS is installed on the computer).

The object list is available in read-only mode. You can copy objects to the structure window (6). To do this, right-click the required object and click the "Add to working model..." command

### 8 — Dependency window

Contains a list of objects linked to the selected element in the object list area. Buttons which manage the object list filtering are located in the upper part of the window

### 9 — Status bar

Contains the program's service messages. On the right-hand side, there are highlighted zones with the following information (in order from left to right):

- enumerator of the selected object, total number and number of the selected objects in the object list or in the additional dependency window;
- current time

## Configuring interface elements

The user can change the content of displayed interface elements and manage their location in the program's main window. The main window view is saved in the system register and is used in subsequent sessions of the user's work with the program.

The menu and toolbar may be placed anywhere on the screen using standard tools available to Windows OS applications.

The category panel is always located along the left side of the program's main window. The location of additional windows is fixed and cannot be changed. To change the size of the panel and additional windows, use their internal boundaries.

Interface element management is performed through the commands in the View menu.

Command	Description
<b>View   Status bar</b>	Enables or disables status bar display (9)
<b>View   Panels   Buttons</b>	Enables or disables toolbar display (2)
<b>View   Panels   Heading</b>	Enables or disables information title display (3)
<b>View   Panels   Categories</b>	Enables or disables categories panel display (4)
<b>View   Panels   Structure</b>	Enables or disables structure window display (6)
<b>View   Panels   Structure for reading</b>	Enables or disables display of the structure window for data models of different bit depth (7)

Command	Description
<b>View   Panels   Dependencies</b>	Enables or disables display of the dependencies window <b>(8)</b>

## Program parameters

Program parameters are configured in the "Application settings" dialog box. The parameters are described below.

### To configure these parameters:

1. Click the Service | Settings... command.  
The "Application Settings" dialog box appears.
2. Select names of groups from the list on the left of the dialog box one by one, specify the required setting values (parameters are displayed on the right). In most cases, to change the parameter value, select the required value from the drop-down list.

### General | Confirmations group of parameters

It contains parameters for confirming performed operations. If the value is Yes, a request to confirm the operation is displayed when this operation is executed.

### General | Colors of the list elements group of parameters

It contains color formatting parameters for the table lines located in the object list area. The cell with each parameter's value contains a rectangle painted in the current selected color. The parameter value can be changed by standard color selection tools, which you can open by clicking the button in the right of the cell.

<b>Text, Background color</b>
These define, respectively, the colors of symbols and the background for displaying information on objects linked to both superior and subordinate objects
<b>Error text, Background color of the error</b>
These define, respectively, the colors of symbols and the background for displaying information on objects not linked to superior or subordinate objects
<b>Text (not controlled), Background (not controlled)</b>
These define, respectively, the colors of symbols and the backgrounds for displaying: <ul style="list-style-type: none"> <li>• information on resources with disabled integrity control attribute;</li> <li>• integrity control jobs without a schedule</li> </ul>
<b>Text (not local), Background color (not local)</b>
These define, respectively, the colors of symbols and the background for displaying information on the resources located on other computers and regarded as network resources for this computer. This is only used in the program's local operation mode

### General | Interface group of parameters

It contains separate interface parameters that are not related to the above-mentioned groups.

<b>Dialog when preparing for AEC</b>
If the value is Yes: a dialog box for configuring resource search parameters appears when the resource preparation procedure for including it into the AEC mechanism is launched (for example, on the Service   AEC resources command). If the value is No: the parameters defined in the Suite of tools   Preparation for AEC group of parameters will be used for resource preparation (see below)
<b>Reference value calculation dialog</b>

If the value is Yes: a dialog box for configuring calculation parameters appears when the integrity control procedure for the reference value calculation is launched (for example, via the Service | Reference values | Calculation command). If the value is No: the parameters defined in the Suite of tools | Reference values calculation group of parameters will be used for reference value calculation (see below)

#### **Grid in the list**

If the value is Yes, lines separating table cells are displayed in the object list area and in the additional dependency window

### **Suite of tools | Preparation for AEC group of parameters**

It contains parameters defined by default when creating a list of resources to be included in the AEC mechanism.

#### **Reselection of executables**

If the value is Yes, the program automatically resets the executable attribute from all resources in the data model before searching for executable resources (files). This makes it possible to set the executable attribute for those resources that meet the defined search requirements. If the value is No, the attribute is not reset

#### **Extensions of executables**

It contains a list of file extensions. The list is applied when searching for executable resources or adding new resources (apart from separate files). The executable attribute will be applied to those files whose extensions are included in this list. The parameter value is changed by editing the text content of the field. The list of extensions is formed in the following way: .<extension1>; <...>; .<extensionN>

For centralized control, the list is applied to computers with the corresponding OS bit depths (32-bit or 64-bit) and related to subjects with the enabled Modes are set centrally parameter in the AEC mechanism parameters

#### **Names of executable modules of processes**

It contains a list of file names which are executable modules of the processes, but the extensions in the names differ from the standard .exe (for example, soffice.bin, someimage.imgext). Similar setting and control functions are available for the selected files and for the files with an .exe extension

#### **Add modules**

If the value is Yes, when searching for executable resources, the program includes dependent modules (files that govern the execution of initial files, for example all libraries required to launch winword.exe) in the resource list. If the dependent module's description is missing in the data model, it will be automatically created and added to the resource group where the initial file description is stored. Dependent modules are recursively integrated – the files which govern execution of these dependent modules are also included in the list.

If the value is No, the search for dependent modules is not performed

### **Suite of tools | Reference values calculation group of parameters**

It contains default values for parameters of the reference values calculation procedure.

#### **Leave old**

If the value is Yes, previously calculated reference values will be saved in the list of the resource reference values after the regular calculation procedure. If the value is No, all previously calculated reference values are deleted

#### **Not supported**



It defines the program's reaction if the integrity control method or algorithm set in the job is not applicable for the resource:

- Ignore – no actions performed;
- Display request – a dialog box for selecting a procedure continue option appears;
- Delete resource – the resource is removed from the overall list of resources (from the data model);
- Discontinue control of resource – the control attribute is reset for the resource

#### **No access**

It defines the program's reaction if the program did not receive access to the resource when attempting to calculate a reference value (for example, no access to read the file or the file is blocked by another process). The reaction type selection is performed in the same way as for the "Not supported" parameter

#### **The resource is missing**

This defines the program's reaction if the program did not find the resource when attempting to calculate a reference value (for example, the file was moved). The reaction type selection is performed in the same way as for the "Not supported" parameter

### **Suite of tools | Import and adding group of parameters**

It contains default values for parameters of the procedure for importing objects and adding resources to the data model.

#### **With allowance for existing**

If the value is Yes, the imported objects replace the model's objects if their names match. If the value is No, the model's objects remain unchanged and the imported objects are renamed as follows: *object\_name*<*N*>, where *N* is an enumerator of the duplicated object (for example, Resource group and Resource group1).

#### **Mark the executables**

If the value is Yes, when adding new files to the data model (apart from separate files), the executable attribute is automatically assigned to those files whose extensions are included in the Extensions of executables list or specified in the Names of executable process modules list. If the value is No, this verification is not performed

### **Notifications | General group of parameters**

It contains the only parameter for sending notifications about changes in the data model. It is only used in centralized control mode.

#### **Mailout when saving**

If the value is Yes, a notification about changes will be sent to all security domain computers effected by these changes in the data model when saving the data model

### **Object Repository | Removed Objects group of parameters**

It contains the only setting parameter for removing an object from the centralized data model. It is only used in centralized control mode.




#### **Lifetime**

It defines the time that the centralized data model object marked for removal remains in the centralized control mode storage and is accounted for in synchronization. The parameter value is set in hours

## **Tools for object list management**

### **Navigation during object structure management**

In certain cases, it is convenient to switch between structure elements using standard commands and/or toolbar keys.

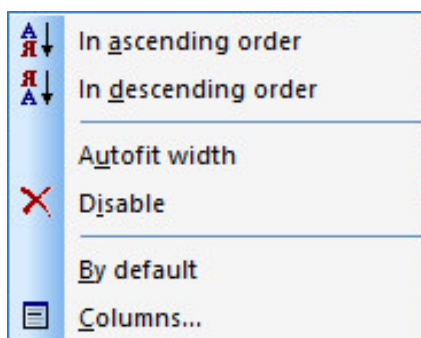
Command	Button	Description
<b>View mode   Back</b>		Go to the previously selected structure element
<b>View mode   Next</b>		Go to the next selected structure element
<b>View mode   Home</b>		Go to the root structure element

### Configure table column view

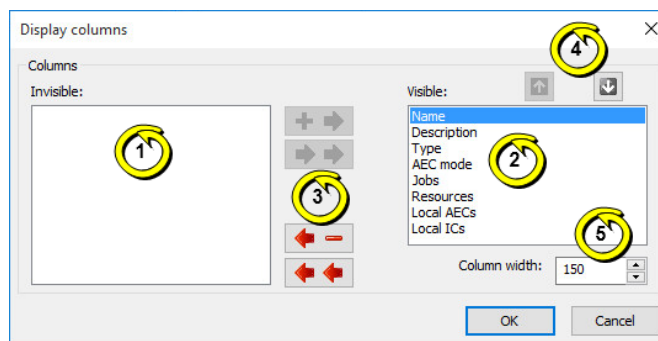
The object list and dependency window share the same table form used to display the list of objects. Table column configuration is based on the object category being displayed. To display the information as well as possible, you can change column width, add or delete columns, or move them relative to each other. The actions described resemble standard Windows operations.

#### To manage columns using the setup dialog box:

1. Right-click in the column header section and click the "Columns..." command.



A dialog box prompting column view configuration appears as in the figure below:



#### Comment.

The figure shows: 1 — list of columns not shown in the table; 2 — list of columns shown in the table; 3 — buttons to switch between lists; 4 — buttons to manage column order; 5 — column width value configuration field (in pixels).

2. Configure column display mode.

#### To restore the table to its default view:

- Right-click the column header and select the "Restore default" command.
- Table view (column width and configuration) is restored to its default settings.

### Object list sorting parameters

The tables in the object list or additional dependency window are sorted by values in the specific columns. The sorting methods are similar to standard table management methods used in most Windows applications. The column header used for sorting the

table indicates the corresponding direction of sorting.

### Object search in lists

The search is performed based on the values given in the displayed table columns from the object list or the supplementary dependency window.

#### To find an object:

1. Select an object in the table to start the search from.
2. Click the Edit | Find... command.  
A dialog box prompting search parameter configuration appears.
3. In the "Find..." field, specify the object to find and, if necessary, configure the search parameters. Click OK.

<b>Consider the register</b>
If the check box is selected, only objects whose details contain a specified line of characters entered in the same case (upper-case/lower-case) will be found. If there is no selection, the case (upper-case/lower-case) will not be considered
<b>Entire value</b>
If the check box is selected, only objects whose details contain a specified line of characters entered as a single word (or words) will be found. If there is no selection, the line of characters can appear as a part of other lines
<b>Search in field</b>
If the check box is selected, the parameter defines the name of the column (from the drop-down list) to be considered when searching the table. If there is no selection, all displayed columns in table are searched

Once the search is complete, the table object that was found is highlighted. If the specified line is not found, a respective message box appears.

To find other objects that could meet the configured search parameters, the search can be resumed from the currently selected object.

### Switching by object links

When a data model has a proper layout, each object must be a part of one or more interlinked (dependent) object chains. A dependency window is used when it is necessary to establish what objects the particular object is linked with (see p. 78).

#### To switch to a linked object:

1. In the object list section, select an object or a group of objects.  
The list of objects appears in the dependency window.
2. If necessary, you can configure the filter by object category in the dependency window. Shortcuts in the upper part of dependency window can be used to switch between filtering options.
3. In the dependency window object list, find the object to switch to in the objects structure, right-click it and click the "In-tree switch" command.

In the structure window, the respective tree branch expands and the desired object is highlighted.

## Using TCP Ports for network connections

Some modules of Secret Net Studio use TCP-ports for networking. When the Client is installed on a computer, this results in automatic changes being made to the following Windows OS parameters:

1. RPC-calls from non-authenticated Clients are permitted. This is achieved by creating RestrictRemoteClients parameter with zero value in the HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC registry key.
2. Anonymous connections with named channel are permitted. This is achieved by creating NullSessionPipes with SnIcheckSrv and SnHwSrv values in the HKLM\System\CurrentControlSet\Services\LanManServer\Parameters registry key.

Additionally, you must enable the following TCP ports in Windows firewall:

- 21326 — to work with electronic identifiers via terminal access;
- 21327 — for online synchronization of specified IC-AEC jobs.

Changes listed are sufficient to interact via the network using TCP. There is an alternative way to establish connection via named channels: go to Windows firewall and manually activate standard rules for "Shared files and printers" that grant permissions to use ports 139 and 445.

Permission to use ports 137 and 138 on protected computers is the key condition for establishing a connection. These ports are open by default in the operating system. For blocked connections, consider checking the standard Windows firewall rules which allow the use of these ports; and enable them, if necessary.

Devices that monitor network traffic between computers must not prevent the use of these ports.

## Recommendations for setting Secret Net Studio on a cluster

Using cluster technologies, a group of computers (nodes), working separately under their OS, may be united into one server. When configuring the Clients installed in a cluster, follow the recommendations:

1. All services of the Client should constantly work on all cluster nodes, including inactive ones. Do not cluster these services, i.e. do not include them in the resource which is managed by the cluster service. Otherwise, switching will cause the System performance drop on inactive nodes. The functional control mechanism will block the cluster work after detecting the absence of basic security subsystems.
2. The shared resource (physical disk or network adapter) in the list of Secret Net Studio devices should be switched to "Device connection is allowed" or "Device is not controlled" mode. If "Device is always connected to the computer" mode is enabled for such a resource (enabled by default for physical disks and network adapters), you may notice a hardware configuration error when you switch the resource when using the control mechanism.

**Note.**

The same may occur on a standalone computer with several SCSI disks.

3. Do not enable integrity control for files located on a shared resource. The reason for this is that the cluster node loses access to the shared resource when switched to inactive mode. If a control procedure was defined for this node, an integrity check error for the monitored objects will be registered during its execution.
4. When configuring the AEC for the user, do not indicate a local path for executable files located in the cluster's shared resource. In this case, you should use network paths for authorized executable modules.
5. For the Client in the standalone mode, you should select similar domain user settings on all cluster nodes. Otherwise, Secret Net Studio work will differ depending on which node is active. In particular, this recommendation is valid for the mandatory access control mechanism, as far as it processes network calls to files and defines access possibility according to user settings from the local database on the cluster.

## Backing up the IC-AEC database using the command line

IC-AEC data models can be exported and imported by running the Applications and data control program from the command line. To start it, go to the Client setup folder and run SnICheckAdm.exe with the required parameters.

The parameters are listed in the table.

Parameter	Value	Description
HIDE	Absent	Blocks the opening of the program window
MODE	LOCAL CENTRAL	Local operation mode (by default) Centralized operation mode
LOAD	Absent	Loading a data model from the DB (LDB or CDB, depending on the operation mode) is in progress
IMPORT	File name in quotes, for example: "C:\Catalog 1\model.xml"	Data model import from the file
EXPORT	File name in quotes, for example: "C:\Catalog 1\model.xml"	Data model export to the file
SAVE	Absent	Saving a data model to the DB (LDB or CDB, depending on the operation mode) is in progress
CALC	Absent	Reference values calculation is being performed. The data model must be saved in advance. Reaction to errors during calculation - according to the parameters established in the program
EXIT	FORCE (optional)	Completing the program operation. If the FORCE value is present, the check of whether to save of DB changes is not performed (and the respective query about the presence of unsaved changes is not displayed)

The set parameters are applied according to their sequence in the command line (from left to right). It is not case sensitive.

Add the "/" or "-" symbols in front of each parameter. All elements of the line (parameters, values) are separated by spaces.

Example:

```
SnICheckAdm.exe /hide /mode central /load /export "D:\Dir1\Data.xml" /exit force
```

In the above example, the program runs in centralized mode without opening a window. A data model is loaded to the program from the CDB and then exported to the specified XML file. After the export, the program operation is completed without checking for unsaved changes.

## Restoring the System after power failure

In most cases, a sudden computer power failure results in Secret Net Studio performance drop during subsequent startups. There are, however, situations when power failures cause the computer to be locked or other kinds of uncommon system behavior.

In such cases, problems might be caused by the following components being corrupted:

- IC-AEC database;
- local database of Secret Net Studio;
- software modules of Secret Net Studio.

Below is a series of recommended measures for the administrator to take in order to restore proper functioning of the IC-AEC DB and local database protection system. For further problem resolution, we recommend you to add the \Icheck and \GroupPolicy subfolders located in the Secret Net Studio setup folder to the antivirus software exception list. If the measures described work, please try reinstalling Secret Net Studio on the computer (see document [2]). If the problems listed above persist further, please contact the technical support.

### Restoring the IC-AEC database

If the IC-AEC database is corrupted during computer booting processes, the System waits for a long time for the integrity control subsystem to start. The waiting time may last up to one hour. Functional control errors notifying about the absence of IC-AEC subsystem are also common for these cases.

#### To restore the IC-AEC database:

- Delete the \Icheck folder from the Secret Net Studio component setup folder and restart the computer.

After restoring the IC-AEC database, the local parameters of the IC and AEC mechanisms will return to their default values. During computer booting, synchronization is performed automatically. As a result, centrally defined parameters are uploaded to the computer. Previously defined local parameters should be restored manually.

### Restoring the local database

If the Secret Net Studio local database is corrupted, functional control errors appear during computer booting. These error messages notify that Secret Net Studio core is absent or nonfunctional.

#### To restore the local database:

1. Start the command prompt (cmd.exe).
2. Go to the \GroupPolicy folder located in Secret Net Studio setup folder.
3. Enter commands one-by-one:
  - del \*.chk
  - del \*.log
  - del \*.edb
4. Enter esentutl /p snet.sdb command (answer OK to the request).
5. Enter the following commands again: del \*.chk, del \*.log and del \*.edb.
6. Restart the computer.

After restoring the local database, Secret Net Studio parameters in the local security policy will return to their default values. During computer booting, centrally defined parameters are applied automatically according to the action of group policies. Previously defined security policy parameters should be restored manually.

## 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