SECURITY code

Secret Net Studio

Setup and Operation

Administrator guide

© Security Code LLC, 2021. All rights reserved.

All rights to the operating instructions are reserved.

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

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

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

Table of contents

List of abbreviations ... **9**

Introduction ... **10**

Local authentication ... **11**
- Setting up secure logon mechanism modes ... 11
- One-time logon in advanced password-based authentication mode ... 13
- Functional control ... 15
- Lock out a workstation ... 15
- Logon in regular logon mode ... 16
- System logon in administrative logon mode ... 16
- User password change by the administrator ... 16
- Using Sobol in tandem with Secret Net Studio ... 17
  - Enable joint mode between Sobol and Secret Net Studio ... 18
  - Manage Sobol CM keys ... 20
  - Copy the Sobol administrator security token ... 21
  - Grant access to computers with Sobol ... 21
- Authentication with Microsoft account ... 22

Security Tokens ... **23**
- Management of security tokens ... 23
- Main operations with security tokens ... 24
  - Presenting a security token ... 24
  - Initializing security tokens ... 24
  - Verifying token ownership ... 25
- Working with security tokens ... 25
  - Viewing information about user security tokens ... 25
  - Assigning security tokens ... 25
  - Configure security token usage modes ... 28
  - Deleting a security token ... 29

Setting up terminal session security settings ... **31**
- Using security tokens in terminal sessions ... 31
  - Disabling pre-authentication ... 31
  - Software methods for processing security tokens ... 32
- Restricting the use of local devices and resources ... 32
  - Redirection control for local devices of the terminal client ... 33
  - Clipboard redirection control ... 33
  - Printer redirection control ... 34
- Protection of confidential information during terminal sessions ... 34

Self-protection ... **35**
- Setting up administrative privileges control ... 36
- Enabling and disabling self-protection ... 37
- Switching self-protection to emergency mode ... 37

Shadow Copy ... **39**
- General information ... 39
  - Shadow copy repository ... 39
  - Search in the shadow copy repository ... 39
- General configuration procedure ... 40
- Configuring shadow copy repository ... 40
- Configuring the shadow copying mechanism for devices ... 40
- Searching and viewing data in the shadow copy repository ... 41
  - Opening the main repository folder ... 41
  - Searching and viewing files ... 42

Local audit ... **45**
  - Local event registration logs ... 45
  - Privileges for working with local logs ... 45

Storing and deleting local logs 46
Exporting local log entries 46
Clearing the local log 48
Configuring event registration on computers 48
Setting up log parameters 48
Selecting events for registration 49
Application control setup 49

Software Passport 51
General information 51
Enabling the mechanism 51
Registering licenses for the mechanism 51
Enabling the mechanism on the protected computers 53
The mechanism configuration 55
Generating key information to approve Software passports 55
Granting privileges to the users 55
Editing the OM structure 56
Configuring the mechanism settings centrally 57
Configuring Software Passport settings locally 59
Operations with passports 61
Collecting the Software passport data on the protected computer 62
Building the passport project 63
Comparing passports 64
Verification of the approved passport signature 65
Approving the passport project 66
Backing up the passports 66
Deleting the outdated passports 66
Recovering the passports from backup copies 66
Events registered in the Security Server log 67

Device Control 68
About device control 68
Device list 68
Inheritance rules for parameters in the device list 69
Management options 69
Specific features of group policy application with device lists 70
Default device parameters 70
General configuration procedure for using only allowed devices 71
Features of composite devices 72
Device list management 72
Loading a device list 72
Management commands 73
Creating a device list in a group policy 74
Adding and removing device list elements 74
Control of device connections and changes 80
Configuring a device control policy 80
Confirming hardware configuration 81
Selective discretionary access control 81
Configuring access rights for devices 81
Configuring event logging and audit of device operations 82

Print Control 83
About restricting access to printers 83
Printer list 83
Management options 83
Initial printer use parameters 84
General configuration procedure for printing only on allowed printers 84
Printer list management 84
Loading a printer list 84
Creating a printer list in a group policy 85
Adding and removing elements 85
Selective printer access control 86
Configuring user print permissions 86

Configuring event registration ... 86
Configuring printed document marking ... 87
Marking mode management ... 88
Marker editing program ... 90

Integrity Check ... 95
Setup methods and tools overview ... 95
Data Model ... 95
Default model objects ... 96
IC-AEC Management Program ... 96
Synchronizing central and local databases ... 97
Initial setup of IC mechanisms ... 98
Preparing to build a data model ... 98
General configuration procedure ... 98
Building a new data model ... 98
Adding tasks to a data model ... 99
Creating jobs and adding tasks to them ... 101
Enabling AEC soft mode operation and task creation by log ... 103
Configuring links between actors and AEC jobs ... 104
Preparing resources for application execution control ... 105
Enabling and configuring process isolation ... 106
Calculating reference values ... 108
Activating IC ... 111
Granting privileges when working with AEC ... 111
Enabling AEC hard mode ... 112
Checking jobs ... 112
Saving and loading data model ... 113
Saving ... 113
Change notifications ... 114
Configuring automatic synchronization start ... 114
Forcing full synchronization ... 116
Downloading and restoring data model ... 116
Export ... 117
Import ... 118
Editing the data model ... 121
Changing object parameters ... 122
Adding objects ... 125
Deleting objects ... 133
Links between objects ... 134
New calculation and reference values replacement ... 134
Disable local jobs ... 135
Searching for dependent modules ... 135
Replacing environment variables ... 136

Mandatory Access Control ... 137
About Mandatory Access Control ... 137
Resource confidentiality categories ... 137
Access levels and user privileges ... 138
Flow control mode ... 139
Configuring mandatory access control ... 140
General configuration procedure ... 140
Configuring confidentiality categories ... 140
Assigning access levels and privileges to users ... 141
Assigning confidentiality categories to resources ... 142
Configuring event registration ... 143
Configuring the use of printers ... 143
Additional configuration of the flow control mode ... 143
Recommended configuration procedure ... 143
Flow control mode configuration program ... 144
Selecting confidentiality levels for network interfaces ... 145
Enabling and disabling the flow control mode ... 145
Configuring joint operation with applications ... 146
Confidential resource handling rules ... 148

Discretionary Access Control **151**
Granting privileges to modify rights to access resources 151
Assigning the resource administrator 151
Configuring event logging and audit of resource operations 151
Disk Protection **152**
Enable Disk Protection 152
Enable and disable logical partition protection 153
Disable the disk protection mechanism 154
Full Disk Encryption **155**
Configure encryption settings 155
Enable Full Disk Encryption subsystem 156
Data encryption and decryption 157
Local encryption in case of local storage of recovery data 157
Local encryption in case of centralized storage of recovery data 159
Local decryption 160
Encryption and decryption in the Control Center 161
Change the security domain key 162
Change encryption keys 164
Restore access to encrypted disks 167
Save recovery data locally 167
Export recovery data on the Security Server 169
Restore access using a recovery code 171
Data Encryption **173**
Granting privileges to create encrypted file containers 173
Event registration setup 173
Managing encryption user keys 173
Key issue and change 173
Key copying 175
Configuring key change parameters 175
Data Wipe **176**
Data wipe configuration 176
Exclusion list 177
Residual data lazy processing 177
Wiping data from drives 178
Firewall **180**
Network packet processing procedure 181
Change rule priority 182
Configuring access rules 182
Creating an access rule 183
Change access rules 190
Deleting an access rule 191
Managing system rules 191
Create a system rule 192
Managing system rules 193
Managing application rules 195
Creating an application rule 195
Managing application rules 199
Managing network traffic filtering rules 200
Connection to the management server 201
Creating and editing network traffic filtering rules 201
Viewing network traffic filtering rules 204
Deleting network traffic filtering rules 204
Managing network protocols 204
Configuring ICMP protocol protection mode 205
Managing network services 207
Stateful Packet Inspection 209

Configuring learning mode 209
Managing the firewall on protected computers 210

Network Authentication 212
Configuring connection protection for the <everyone> group 213
Configuring packet processing parameters 214
Configuring an SMB connection 215
Configuring the computer's IP address acquisition parameters 216
Managing the network authentication mechanism on protected computers 217

Antivirus 218
Configuring group policies 218
Scan profiles 219
Configuring scan profiles 220
Schedule-based scanning 225
List of exclusions 226
Event registration 227
Managing antivirus on protected computers 227
License overview 229
Managing quarantine 229
Antivirus management utility 230
Troubleshooting 230

Intrusion detection and prevention 231
Configuring group policies 231
Network attack detectors 232
Signature analyzers 237
Windows telemetry blocking 239
Network adapter control 239
Managing the intrusion detection tool 239
License overview 240

Updating antivirus and intrusion detection tool databases 241
Configuring update parameters 241
Downloading updates from a network share 243
Update utility 243

Trusted Environment 245
System requirements 245
Enabling Trusted Environment 246
Registering TE license 246
Creating TE boot drive 246
Enabling the TE mechanism 248
Configuring Trusted Environment 249
TE OS interface 250
Entering TE administrator mode 250
Changing TE administrator password 251
Selecting TE operation mode 252
Configuring integrity control in TE 254
Configuring computer attack detection 256
Unlocking computer 257
Working with event log 258
Disabling Trusted Environment 259

Sandbox 261
Enable Sandbox 261
Analyze programs and create lists 261
Configure rules 262
Configure logs 262
Update Sandbox rule database 262

Appendix 263
User management program 263

Using TCP Ports for network connections ... 265
List of groups, classes and models for device control ... 265
Examples of configuring external drives use ... 267
Local assignment of external drives to users ... 267
Centralized creation of a list of external drives ... 268
About the Applications and data control program ... 268
Program start ... 268
Program interface ... 269
Configuring interface elements ... 271
Program parameters ... 272
Tools for object list management ... 275
Backing up the IC-AEC database using the command line ... 277
The flow control mode configuration program ... 278
Automatic setup ... 278
Manual setup ... 279
Disabling local disk protection in an emergency ... 288
Emergency recovery disk for the Disk Protection and Full Disk Encryption mechanisms ... 288
Create an emergency recovery disk ... 289
Change the password for disks ... 290
Reset the password for disks ... 291
Disk protection removal and data decryption ... 291
Restore Secret Net Studio bootloader ... 292
Restore configuration of security subsystems ... 293
Delete configuration of security subsystems ... 293
Remove an encrypted disk form configuration ... 294
Recommendations for setting up Secret Net Studio in a cluster ... 295
Restoring the security system after power failure ... 295
Restoring the IC-AEC database ... 295
Restoring the local database ... 296
TE operation errors ... 296
Local Control Center errors ... 296
Errors on computer startup ... 297
Default TE IC objects ... 298
Restrictions and recommendations when working with TE ... 298
Incompatible hardware and configuration ... 298
Recommended computer configuration ... 299
Formatting the TE boot drive ... 300
Documentation ... 301

List of abbreviations

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

Introduction

This document is designed for administrators of Secret Net Studio. It contains information on how to configure and manage the security mechanisms of Secret Net Studio:

- basic protection:
  - logon protection (local authentication, security tokens);
  - terminal session protection;
  - self-protection;
  - shadow copying;
  - local audit (logs, alert notifications);
  - software passport;
- local protection:
  - device control;
  - print control;
  - integrity control;
  - application execution control;
  - mandatory access control;
  - discretionary access control ;
  - information protection on local drives;
  - full disk encryption;
  - data encryption in cryptocontainers;
  - deleted information wiping;
- network protection:
  - firewall;
  - network authentication;
- antivirus;
- intrusion detection and prevention;
- trusted environment;
- sandbox.

Conventions

We use conventions to highlight certain text elements.

Internal links refer to the page with the required information.

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

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

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

Information sources

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

Chapter 1
Local authentication

Setting up secure logon mechanism modes

The way in which the secure logon mechanism operates is defined by several settings, which you configure locally or centrally.

In centralized mode, you can configure secure logon mechanisms both for Secret Net Studio users and for computers with Secret Net LSP. You can do so only on the level of Security Server group policies, security domains and organizational units.

Not all mechanism parameters can be applied to computers with Secret Net LSP. You can find out about the limitations by looking at the icons next to each setting:

- Windows icon — a setting can be applied to a Client with Secret Net Studio;
- Linux penguin— a setting can be applied to a Client with Secret Net LSP.

Note. Depending on a Linux distribution, some settings can also be applied in a different way. For more detail, see Secret Net LSP documentation.

Tip. You can configure icon display in the Control Center. To do so, at the bottom of the navigation panel, click **Settings**, and, on the appeared menu, click **Control Center settings**. In the appeared dialog box, on the menu on the right, click **Policies** and select/clear the **Show supported platforms for policies** check box.

The description of the centralized configuration procedure via the Control Center is provided below. Local configuration is performed similarly via the Local Control Center.

To configure secure logon mechanism modes:

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

   Note. For details about the Control Center, see document [**1**].

2. In the **Policies** section, click **Logon**.
3. Configure the following settings:

Inactivity time limit before the screen is locked
Determines the maximum inactivity period before the computer is automatically locked by Secret Net Studio. 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 the one specified by the value of this parameter. Otherwise, the OS parameter will not be valid. If the value is **0**, Secret Net Studio tools will not lock the computer
Deny secondary logon
If this mode is enabled, the start of commands and network connections is blocked when entering credentials of a user that did not perform an interactive logon. After enabling the mode, you should eliminate the possibility of using previously saved logon information. To do so, enable standard Windows OS security parameter **Network access: do not allow password and logon information storage for network authentication** (parameter name may slightly differ depending on the OS version)

Security token removal behavior
Do not lock – the computer is not locked if the security token is removed from the reader. **Lock computer if USB security token is removed** – the computer is blocked if the USB key or smart card used to log on to Secret Net Studio is removed from the reader (for example, iButton, eToken). **Lock station if any security token is removed** – 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.). 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
Number of unsuccessful authentication attempts
Determines the maximum number of failed logon attempts per user in the advanced password-based authentication mode. When the number is reached: • computers with Secret Net Studio are locked according to the **Computer lock duration after the threshold is reached** policy. After that, only an administrator is allowed to log on; • computers with Secret Net LSP are locked according to the **Computer lock duration after the threshold is reached** policy. After that, a user can log on using another account. If the value is **0**, this limitation is not applied. This parameter can be applied to computers with Secret Net Studio and Secret Net LSP
Computer lock duration after the threshold is reached
Determines the period after which a computer is unlocked if it was locked when a user reached the maximum number of failed logon attempts: • computers with Secret Net Studio are locked for a set period of time. After lock time is up, a user can log on to the system. Before lock time is up, only an administrator is allowed to log on. If the value is **0**, a computer will remain locked until an administrator unlocks it manually; • on computers with Secret Net LSP, user accounts are locked for a set period of time. After lock time is up, a user can log on to the system. Before lock time is up, only an administrator can unlock a user account. If the value is **0**, a computer will remain locked until an administrator unlocks it manually. This parameter can be applied to computers with Secret Net Studio and with Secret Net LSP
Allow interactive logon to domain users only
If this mode is enabled, only the users registered in the domain can log on to the system. Interactive logon of local users (including local administrators) will not be allowed. This parameter is absent from the Local Control Center of 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 security token.** To enter the system, the user must provide a security token activated by Secret Net Studio. Users without security tokens cannot log on to the system. An administrator can enter the system without presenting a security token only in administrative mode (see p. **16**). 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). The **Only by security token** mode uses security tokens activated by Secret Net Studio, but not the ones by Windows OS. When using a Microsoft account in Windows OS 8 and 10, logon by security token is available only on computers included in the security domain. If you choose two different identification modes for two protected computers, firewall rules for authenticated users do not trigger between them (see p. **180**)

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 password is saved in the Secret Net Studio database, the user will not be able to log on to the system. The administrator may allow a one-time logon for the user to save the password by enabling the **Trust Windows password authentication on the next login** setting. To perform the operations with users in the **User Management** program, select the **Synchronize user data on the authentication server** check box when performing each operation or in the Control Center, select **Trust Windows authentication**. Logon is allowed only 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
Contains settings for user passwords in the **Advanced password-based authentication** mode. The settings match the settings of the Windows password policy if the **Use values from the Windows password policy** mode is enabled. If necessary, special settings may be configured for passwords saved in the Secret Net Studio database (regardless of Windows password policy settings). To do so, select the **Set custom values** mode and configure the settings similar to standard Windows password policy settings: **Minimum password length**, **Maximum password age** and **Password complexity requirements**. Moreover, the computers will eventually use the strictest requirements from those assigned in the Secret Net Studio policies and Windows settings
User notification
Notify user about last successful logon — after a user logs on to the system, he or she receives the following message: • date and time of the last logon; • a number of failed logon attempts since the last successful logon. If there is no data about the last successful logon, the user receives the following message: **Last logon info is missing**. The notification may not appear if there are other messages. **Notify user about security measures before logon** — before a user logs on to a system, a notification appears containing information about data protection measures implemented in the system. By logging on to the system, a user accepts the rules and restrictions on working with the information

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 bottom of the **Settings** tab.

One-time logon 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 log on. For this purpose, information about the user password must be saved in the Secret Net Studio database. This information can be saved at the first successful user logon or when the password is changed by an administrator or by a user.

For the Client in standalone mode, users can enable the setting **Trust Windows password authentication at the next system logon**, which allows them to perform a one-time logon after the **Advanced password-based authentication** mode is enabled. In this case, information about passwords is saved to the Secret Net Studio database. After that, this setting is disabled automatically, and the advanced password-based authentication will be applied to the user. When creating users in the user management program, this setting is enabled by default. Before enabling the **Advanced password-based authentication** mode, we recommend you to enable this setting for user accounts (see below).

For the Client in network mode, advanced authentication is performed for domain users using Secret Net Studio Authentication Server. The trust in Windows password-based authentication at the first user logon is defined by the settings of a

security domain (the Control Center, the parameters group **Windows authentication**, the parameter **Trust Windows password authentication at the next system logon**). If this setting is enabled and the first logon is performed on the Client after the advanced password-based authentication policy is enabled, information about the user will be saved in the Authentication Server database. Then, if **Trust Windows password authentication at the next system logon** is disabled, the **Advanced password-based authentication** mode will be applied to the user.

Note. In network mode, in the user management program, the setting **Trust Windows password authentication at the next system logon** is disabled and unavailable for editing.

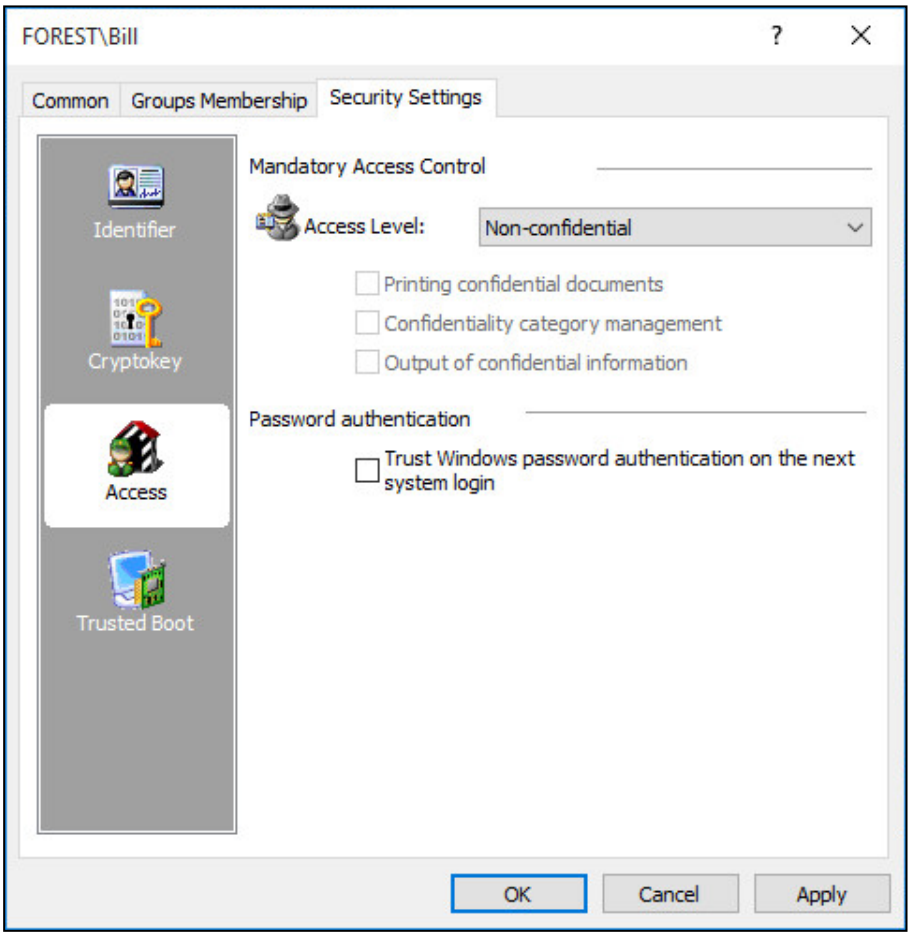
Information about a domain user can be added to the Authentication Server database in the user management program when creating a user, changing the password of an existing user (**Synchronize user data on the Authentication server**) and when running the command **Synchronize with the security system** in the context menu of the user.

Note. To delete a user from the Authentication Server database, select **Synchronize user data on the Authentication server** when deleting this user in the user management program.

The same rules apply to both local users and users in standalone mode.

To enable a one-time logon in standalone mode:

1. Start the user management program (see p. 263).
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 at the next system logon** check box.
5. Click **OK**.

Functional control

Functional control is a self-control mechanism of the security system designed to ensure that all core Secret Net Studio security subsystems operate correctly. If functional control shows that at least one of the security subsystems does not operate correctly:

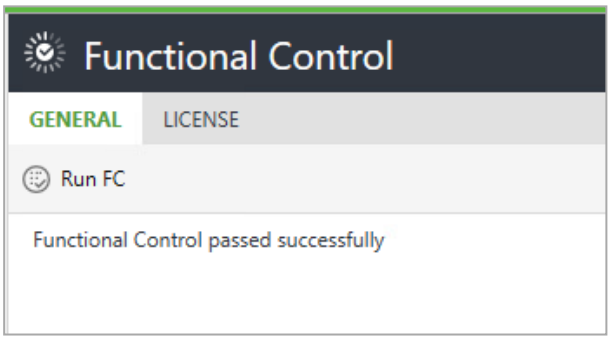
- a user without privileges is denied access to the System, only the administrator can log on;
- the administrator receives a notification saying functional control has been violated;
- an unauthorized access attempt is registered in the Secret Net Studio log.

The initialization and functional control of the security subsystems are performed during the computer boot and before the user's logon. The user is allowed to log on if all the checks are successful.

Functional control can be run while working on the computer in centralized or local management mode.

To run functional control:

1. In the Control Center or Local Control Center, open the **Computers** panel and select the **Status** tab for the required computer.
2. Select **Functional Control**. Details about the mechanism appear on the right.



3. Click **Run FC**.

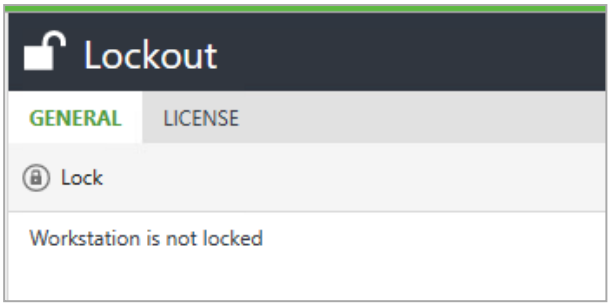
   If the procedure finishes successfully, the **Functional Control passed successfully** message appears.

Lock out a workstation

Some security system events can cause workstation lockout. Also, the administrator can lock out or unlock the computer by means of Secret Net Studio in centralized or local mode. If the workstation is locked out, a user without privileges is not allowed to log on. When the workstation is unlocked, access restrictions are removed.

To lock out/unlock a workstation:

1. In the Control Center or Local Control Center, open the **Computers** panel and select the **Status** tab for the required computer.
2. Select **Lockout**. Details about the status of the computer appear on the right.



3. Click **Lock/Unlock**.

   A dialog box prompting you to confirm the action appears.

4. Click **Yes**.

Logon in regular logon mode

In regular logon mode, any user, including the administrator, must log on according to the same rules set by the respective security mechanism.

Note. Steps of logon when Secret Net Studio is running are given in document [1].

If notifications are enabled before logon (on the lock screen) or after logon (in the task bar), notifications can appear (see p. 13).

Attention! If the message about security measures taken in the System appears on the lock screen, logging on will mean that you accept the rules and restrictions.

System logon in administrative logon mode

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

The administrative logon mode may be useful in the following situations:

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

Attention! The administrative logon mode must only be used as a last thing for restoring the system normal operation. Log on to the system in the administrative logon mode, fix the problem and restart the computer.

To log on to the system in administrative logon 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 (logon prompt), enter the administrator credentials.

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 document [**3**].

Attention! For the Client in the network operation mode with the enabled advanced password-based authentication mode (see p. 11)), the administrator can change the user password only via the user management program. In this case, to perform the procedure, the administrator may need additional rights granted during the delegation procedure. If the administrator changes the user 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 user password:

1. Run the user management program (see p. 263).
2. Right-click the user in the user 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 password is stored in personal security tokens, a dialog box with a list of personal security tokens belonging to the user appears.
4. Present all listed security tokens (see p. 24).

   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 appears in the table in the **Status** column.
5. Click **Close**.

Using Sobol in tandem with Secret Net Studio

Secret Net Studio can be used in tandem with Sobol (also known as Hardware Trusted Boot Module), which allows the following:

- domain and local users can log on to computers with Sobol using security tokens initialized and assigned to users via Secret Net Studio;
- create integrity check tasks for Sobol with Secret Net Studio tools (see p. 95);
- automatically transfer events from Sobol log to Secret Net Studio log (see table below).

Sobol events	Secret Net Studio events
User logon	Hardware Trusted Boot: user logon
Administrator logon	
Checksums are not calculated	Hardware Trusted Boot: missing checksum
Sobol was switched to standalone mode	Hardware Trusted Boot: electronic lock disabled or Hardware Trusted Boot: electronic lock enabled
Sobol was switched to joint mode	
Log was deleted	Hardware Trusted Boot: log has been cleared
External request error	Hardware Trusted Boot: parameter synchronization error
Checksums were recalculated	Hardware Trusted Boot: checksum recalculation
Checksums were automatically recalculate	
Administrator Secure ID was changed	Hardware Trusted Boot: authenticator has been changed
User Secure ID was changed	
Security token was not registered	Hardware Trusted Boot: user logon prohibited
Invalid password	
Logon attempt limit was exceeded	
User was blocked	
Integrity check error	Hardware Trusted Boot: resource integrity violation

Sobol events	Secret Net Studio events
External requests were processed	Hardware Trusted Boot: synchronization of parameters
New user was added	
User was deleted	
All users were deleted	
New user was added	
Administrator password was changed	Hardware Trusted Boot: password changed
Administrator changed password of user	
User password was changed	
Checksum error in security token memory	Hardware Trusted Boot: CRC error in identifier memory
Main boot drive parameters were changed	Hardware Trusted Boot: Boot disk settings have been changed
Password configuration time/date was forward system time	Hardware Trusted Boot: System date and time changed
System time and date were changed	
System date was set back	
Last logon time was adjusted	
Error while exporting log	Hardware Trusted Boot: Log export error
Log was exported	Hardware Trusted Boot: Log export completed

To enable joint mode for computers with the Client in centralized mode consider the following:

1. A single Sobol administrator token or its copies must be used to initialize all Sobol instances.

   Attention! To initialize Sobol version 4.3, you must set the cryptographic kernel to **1989** (see Sobol documentaion).

2. After installing Sobol on the computer of the security administrator and switching it to joint mode, the security administrator must generate centralized management keys and write them to the security token.
3. After connecting Sobol to Secret Net Studio the security administrator must enable the Sobol logon mode for their security token. This mode can be enabled when configuring security token use modes (see p. **28**).

Enable joint mode between Sobol and Secret Net Studio

To enable and configure Sobol to operate in tandem with Secret Net Studio, perform procedures in the following order:

1. For clients in network operation mode do the following on the security administrator computer:
   - install Sobol. During the installation perform the initial administrator registration and create a required number of administrator security token backups. After the installation switch Sobol from standalone mode to joint mode. For information on installing and configuring Sobol see its documentation;
   - install the Client in network operation mode (see document []);
   - generate Sobol CM keys (see below);
   - connect Sobol to Secret Net Studio (see below);
   - present the security token of the Sobol administrator;
   - configure user settings to organize their access to domain computers (assign security tokens, passwords, create the list of computers).

2. On each protected computer do the following:
   - install Sobol. If you are going to use it in tandem with the Client in network mode, perform administrator registration, using the security token prepared during step **1**;

     Note. For information on installing and configuring Sobol see its documentation.
   - install the Client in network mode (see document []);
   - connect Sobol to Secret Net Studio (see below);
   - present the Sobol administrator security token.
3. Do the following on computers with the Client in standalone mode:
   - install Sobol in the following order:
     - during the installation perform the administrator registration or the initial administrator registration and create the required number of the administrator security token backups;
     - after the installation switch Sobol from standalone mode to joint mode.

     Note. For information on installing and configuring Sobol see its documentation.
   - install the Client in standalone mode (see document []);
   - connect Sobol to Secret Net Studio (see below);
   - present the Sobol administrator security token;
   - configure setting for users and security tokens.

Generate CM keys

Sobol CM keys are generated via the "User management" program.

To generate keys:

1. Run **User management** (see p. 263).
2. On the menu bar, select **Service > Generate keys for the Control Center of Hardware Trusted Boot Module**.

   The **Present Security Token** dialog box appears.
3. Present the security token for storing Sobol CM keys (see p. 24). After the keys are generated and written to the token click **OK**.

Warning. Do NOT lose the CM keys. If you lose them, you will have to create the Sobol CM structure again.

Connect Sobol to Secret Net Studio

To connect Sobol:

1. On the Windows Control Panel, select **Secret Net Studio management**.

   The **Secret Net Studio settings** dialog box appears.
2. Select **Hardware Trusted Boot Module management**.
3. Do the following:
   - if necessary, enter the factory number of the product kit in the respective field and click **Apply**. The factory number can be found in the product kit passport and on the card itself;
   - to connect Sobol, click **Connect**.

     Note. After connecting Sobol the **Allow automatic OS loading** field appears. Select it if you need to organize automatic Sobol logon without presenting the security token. Automatic Sobol logon will be enabled after computer restart.
4. On the computer with the Client in network mode, a dialog box requiring to present a security token with Sobol CM keys appears. Present the required security token.

   Secret Net Studio switches to joint operation mode with Sobol and the respective message appears.
5. Click **OK** in the **Secret Net Studio management** dialog box.

Disable joint mode between Secret Net Studio and Sobol

To disable joint mode:

1. On the Windows Control Panel, select **Secret Net Studio management**.

   The **Secret Net Studio settings** dialog box appears.
2. Select **Hardware Trusted Boot Module management**.
3. Click **Disable**.

   Joint mode with Sobol is disabled and the respective message appears.

   Attention! To enable joint mode again you must restart the computer.
4. If you do not plan to further use the joint mode, on the computer start, log on to Sobol as administrator and switch it to standalone mode (see Sobol documentation).

Manage Sobol CM keys

Sobol CM keys are managed via the **User management** program.

Load keys

To perform any operations with Sobol CM keys (grant users access to computers, work with Sobol keys) they must first be loaded. Keys stay loaded to the security system until **User management** is closed.

To load keys:

1. Run **User management** (see p. 263).
2. On the menu bar, select **Service > Load keys for the Control Center of Hardware Trusted Boot Module**.

   The **Present Security Token** dialog box appears.
3. Present the security token (see p. 24) with Sobol CM keys.

   After the keys are successfully loaded the respective message appears.

Copy keys

To improve key storing security we recommend saving the key copies to multiple security tokens.

To copy keys:

1. Run **User management** (see p. 263).
2. On the menu bar, select **Service > Copy keys for the Control Center of Hardware Trusted Boot Module**.

   The **Present Security Token** dialog box appears.
3. Present the security token (see. p. 24), with Sobol CM keys.

   A dialog box requiring to present a security token to save key copies appears.
4. Present the security token where you want to save keys.

   If the saving is successful, the security token status changes to **Processed**.
5. Click **Close**.

Delete keys

Warning. After deleting Sobol CM keys they cannot be restored. The deletion procedure causes irreversible clearing of all settings in the current Sobol CM schema in the domain. Returning to such schema will require complete Sobol CM reinitialization in the entire domain. The reinitialization is performed in the following order:

- generate new Sobol CM keys;
- enable Sobol joint mode for all security tokens;
- configure user access to computers;
- disable joint mode on all computers with Sobol and connect Sobol to Secret Net Studio.

To delete keys:

1. Run **User management** (see p. 263).
2. On the menu bar, select **Service > Delete keys for the Control Center of Hardware Trusted Boot Module**.

   The message about the consequences appears.
3. Click **Yes**.

   A dialog box requiring to confirm the operation appears.
4. Click **Yes**.

   Keys are deleted from the security system and the dialog box requiring to delete keys from security tokens appears.
5. Present the security token with Sobol CM keys.

   Keys are deleted from the security token.

Copy the Sobol administrator security token

Secret Net Studio allows assigning Sobol administrator security token to a security system user. After the assigning such security token has a special icon when it is viewed on the security token list.

If an insufficient number of security token backups were created during the Sobol initialization, you may copy the security token contents to another drive. The new security token can also be used for Sobol administration.

To copy a Sobol administrator security token for a domain user (for the Clients in centralized mode), load Sobol CM keys (see p. 20).

To copy a Sobol administrator security token:

1. Run **User management** (see p. 263).
2. On the menu bar, select **Service > Copy the security token of the Hardware Trusted Boot Module administrator**.

   The **Present Security Token** dialog box appears.
3. Present the security token (see. p. 24) of the Sobol administrator.

   A dialog box requiring the password appears.
4. Enter the Sobol administrator password and click **OK**.

   A dialog box requiring to present a security token to copy the administrator token data appears.
5. Present the security token to copy the Sobol administrator token data .

   After successfully writing data to the new token its status changes to **Processed**.
6. Click **OK**.

Grant access to computers with Sobol

On some computers with the Client in network mode and Sobol in joint mode the users may be granted access to log on to Sobol and then to the OS using security tokens initialized and assigned via the security system tools. That way a user will be able to use a single security token to log on the Sobol and to the OS.

To grant such a permission to a domain user, do the following:

- assign a security token allowed to log on to Sobol (see p. 25) to the user. For security tokens already assigned to the user this can be done by configuring security token use modes (see p. 28);
- create a list of computers where the user is allowed to log on to Sobol (see below).

Before creating the list of computers, load Sobol CM keys (see p. 20).

To create the list of computers:

1. In the **User management** program, open the **Properties** of the domain user and select the **Security Settings** tab (see p. 263).
2. Click **Trusted Boot**.
3. Click **Add**.

   A standard Windows dialog box for selecting objects appears.
4. Select computers the user is to access and add them to the list.
5. To delete a computer from the list, select the computer and click **Delete**.
6. After creating the list of computers, click **OK** or **Apply**.

Authentication with Microsoft account

The logon protection mechanism interacts differently with Microsoft accounts depending on the version of the OS.

Windows 8 – Windows 10

Microsoft users of these OSs can use security tokens to log on only to domain computers.

In Windows 10, version 2004, you cannot select a session privacy level if flow control is enabled. To lift the restriction, disable the **Require Windows Hello sign-in for Microsoft accounts** setting in Windows account settings.

Note. For more details about the mandatory access control mechanism on p. 137.

Chapter 2
Security Tokens

Management of security tokens

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

In Secret Net Studio, the following security tokens can be used: eToken, Rutoken, JaCarta, ESMART, Guardant ID, vdToken, and iButton.

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

A security token is granted to the user by the administrator. One security token cannot be assigned to several users simultaneously. However, several security tokens may be assigned to one user.

The security administrator may perform the following operations with security tokens:

Initialization of the security token
Formatting which allows using the security token in the security system. Initialization is necessary if a data structure on the security token was damaged or is missing due to some reason. External drives to store keys must also be formatted
Security token assignment
Adding information about the fact that the user owns the security token of a certain type with a unique serial number to the Secret Net Studio database
Cancellation of security token assignment
Removing information about the ownership of the security token by the user from the Secret Net Studio database. Hereinafter, we call this operation **identifier removal** for simplicity
Enabling password storage mode in the security token
Adding information about enabling the password storage mode for the user's security token to the Secret Net Studio database. The password is saved to the security token simultaneously with this operation. After the mode is enabled, the user password is obtained from the security token
Disabling password storage mode in the security token
This operation is the opposite to the previous one. The password is removed from the security token memory simultaneously with disabling the storage mode. The identifier remains assigned to the user
Writing and removing keys for working with encrypted data
Used for storing keys in the security token (or on external drives) for working with encrypted data on encrypted file containers
Verification of ownership
By using this operation, the security administrator can verify which user owns a given security token

Main operations with security tokens

Presenting a security token

A security token must be presented upon the system request for recording and reading data.

To present a USB token or a smart card:

- If you know exactly which security token to present, connect it to the computer via a USB port or tap it against the reading device.
- If you need to select a security token from a list of available options, clear the **Use first connected security token** check box and present the security tokens one by one. The serial number of each presented security token appears in the dialog box. When you see the correct security token, click **OK**.

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

To present iButton:

1. If you know which security token should be presented, put it to the reading device and keep holding until the dialog box closes.
2. If you need to choose one from the available security tokens, clear the **Use the first presented identifier** check box and present security tokens one by one. Herewith, the serial number of the security token will be displayed in the dialog box. If the required security token is found, keep holding it and click **OK**.

To present other external drive:

1. Connect the external drive to the computer and click **Disk**.

   The name of the external drive appears in the dialog box.
2. Select this name from the list and click **OK**.

Error message

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

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

Initializing security tokens

To initialize a security token:

1. Run the user management program (see p. 263).
2. In the **Service** menu, select **Initialize security token**.

   A dialog box appears asking you to present the security token.
3. Present the security token (see above).

After the token is initialized, the respective message appears.

Verifying token ownership

To verify security token ownership:

1. Run the user management program (see p. **263**).
2. In the **Service** menu, click **Verify security token**.

   A dialog box appears asking you to present the token.
3. Present the security token (see p. **24**).

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

Working with security tokens

Viewing information about user security tokens

Information about user security tokens is provided in the user management program (see p. **263**). 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.

Assigning security tokens

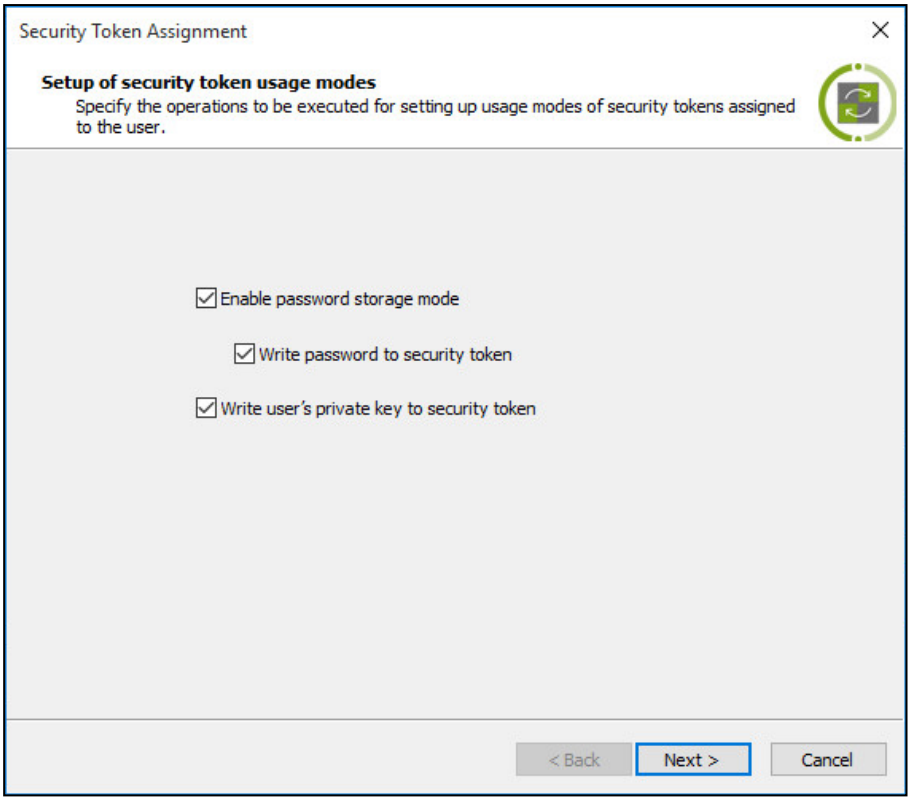
You can assign a security token to a user by means of a wizard. When assigning it, you can adjust security tokens usage modes.

Notes:.
- To write a key that the user already has for data encryption (private key) to a security token, present the token with this key.
- To write a password to a security token, enter the user password.

To assign a security token to the user:

1. Run the user management program (see p. **263**).
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 private user key to security token**, perform following actions:
   - When the **Enter Password** dialog box appears, enter the user password.
   - When the **Present Security Token** dialog box appears, present the user token (see p. **24**) containing the private user 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.

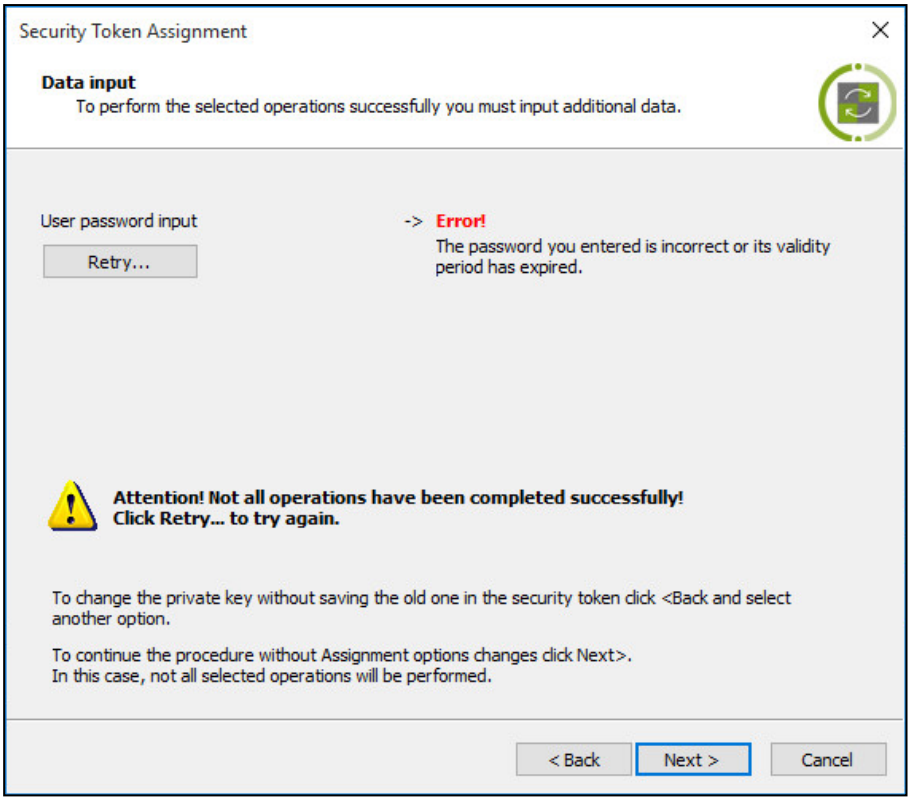
   A dialog box asking you to present the token appears.

6. Present the token (see p. **24**) to be assigned to the user and for data recording. Do not disconnect the token from the reader before all operations are complete.

Data recording errors

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

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



Attention! A security token 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 security token with the same settings to the user.
8. To complete the work, click **Finish**.

Assigning a security token to another user

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

If the presented security token 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 log on to another computer), a confirmation to continue appears. In this case, the following options are available:

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

private user key to security token was selected in the wizard (see above). To cancel the security token assignment procedure, click **Cancel**.

Note. By using the key from the security token (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 security token. In the Client standalone operation mode, the security token can be used both for local and domain computer users.

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

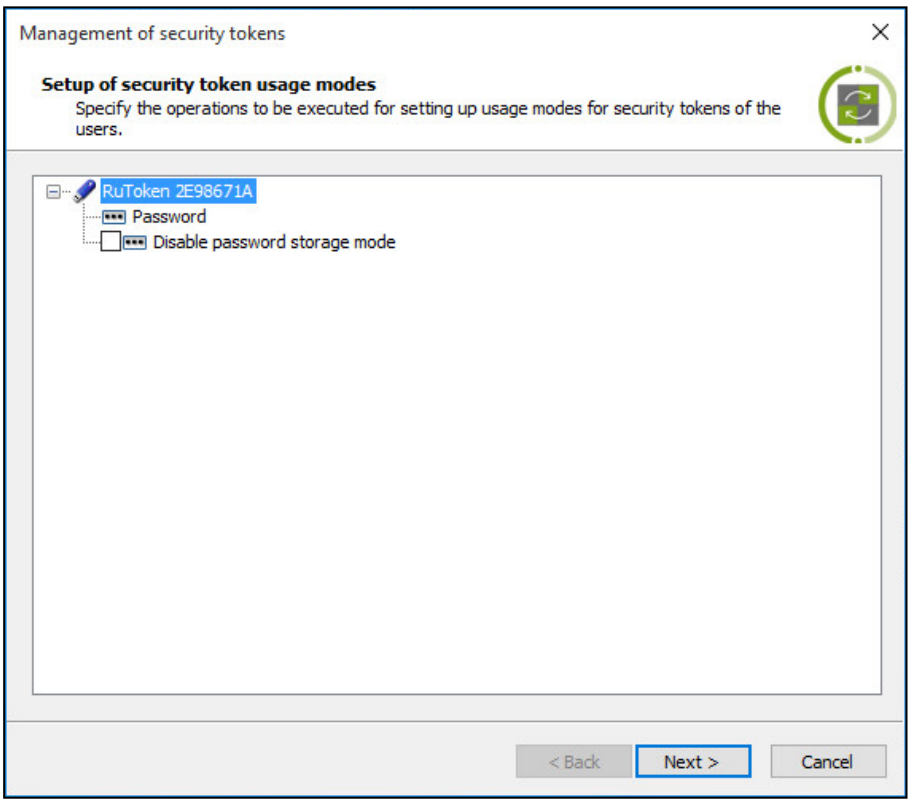
Configure security token usage modes

If necessary, you can change usage modes for the security tokens (apart from external drives) assigned to the user. The mode procedure is configured using the wizard.

To configure the user security token modes:

1. Run the user management program (see p. **263**).
2. Open the user settings dialog box, select the **Security settings** tab and click **Parameters**.

   A dialog box appears as in the figure below.



   The dialog box contains a list of security tokens 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 security token in the list. For example, if password storage mode is enabled for the security token, then the **Disable password storage mode** operation will be available.

3. Select the boxes according to the executed operations and click **Next**.
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**.

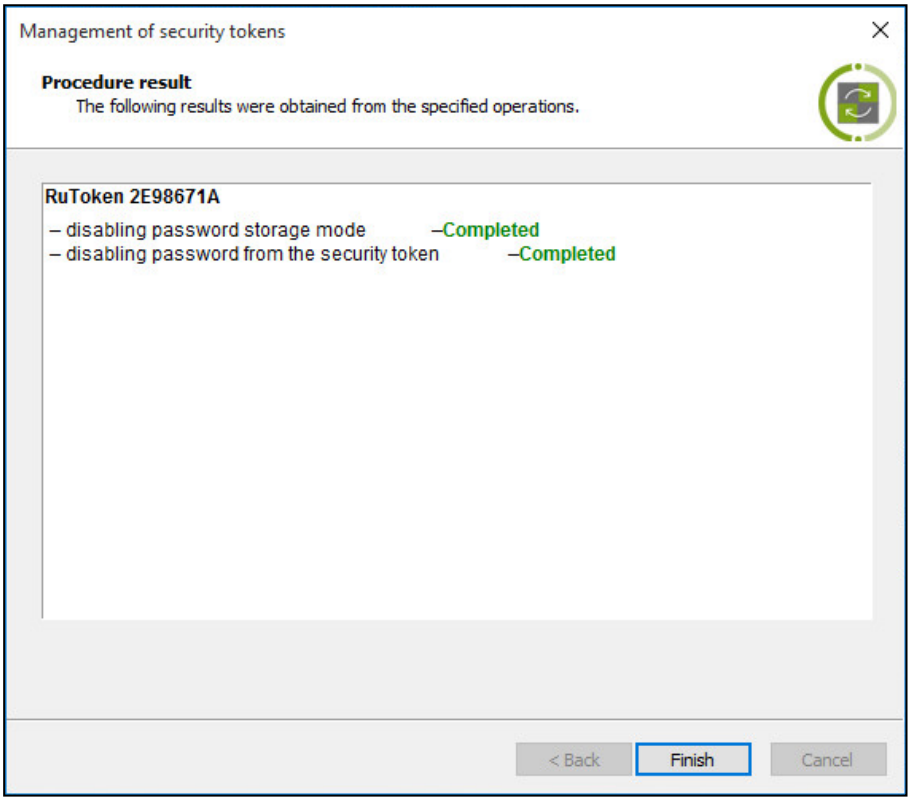
   If any operation, apart from **Enable password storage mode**, was selected, the **Present Security Token** dialog box appears. The names of security tokens for which operations were selected and their processing status is **Not processed**.

6. Present all listed security tokens (see p. **24**).

   After the security token is presented successfully, its status will change to **Processed** . If the security token was presented with an error, an error message will appear in the processing status column. After presenting all security tokens, 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 a security token

After the security token deletion procedure, the user loses the option to use the security token for logon and password and keys storage.

To delete a security token:

1. Run the user management program (see p. **263**).
2. Open the user settings dialog box and select the **Security Settings** tab.
3. Select a security token from the list and click **Delete**.

   If the selected security token 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 asking you to confirm the deletion of the security token appears.

5. Click **Yes**.

A dialog box asking you to present the security token appears.

6. Present the security token (see p. 24).

   The status of the presented security token changes to **Processed**.

   Note. If there are violations during security token presentation, an error message will appear in the dialog box table in the **Status** column.

7. Click **Close**.

   The record of the deleted security token disappears from the security token list.

Chapter 3
Setting up terminal session security settings

Using security tokens in terminal sessions

Security tokens assigned to users can be used for terminal logon during a remote connection. For this purpose, any of the following logon protection identification modes should be enabled on the terminal server (see p. 11):

- **Mixed** (selected by default);
- **Only by security token**.

Note that user pre-authentication is required by default in the Remote Desktop Connection tools version 6.0 and higher (as part of Windows Vista OS and higher). Pre-authentication is performed by entering user account data (name and password) prior to connecting to the terminal server. Therefore, the following specific features arise when establishing the connection:

- If **Mixed** identification mode is selected on the terminal server, terminal logon with the user account data takes place immediately after pre-authentication on the terminal client machine. Presenting an security token to the terminal server is not expected.
- If the **Only by security token** identification mode is selected on the terminal server, during a remote connection, pre-authentication is completed first (the user enters name and password for initiating the connection); then, when connecting to the terminal server, the user must present his/her security token.

If pre-authentication is disabled, the user signs in to the terminal session by security token without prior name and password prompt.

Disabling pre-authentication

The pre-authentication requirement for tools ensuring connection to the remote desktop can be applied both on the terminal client side and on the terminal server side. If the user account data request is disabled on the client side, terminal login from that computer will be possible only if pre-authentication is disabled on the respective server. If the requirement is disabled on the terminal server, remote connections will be allowed for any clients, irrespective of whether the pre-authentication is enabled or disabled.

Disabling on the terminal client

Disabling pre-authentication on the terminal client is supported by Remote Desktop Connection tools version 6.0 and higher. The above-mentioned versions of tools are installed by default starting from Windows Vista OS and higher. To view information about currently used versions, right-click the **Remote Desktop Connection** window header and click **About**.

To disable pre-authentication on the terminal client:

1. Log on using the account data of the user who will be opening terminal sessions on that computer.
2. In a text editor (for example, Notepad), open the **Default.rdp** file from the user documents folder.

> **Note.** The **Default.rdp** file is a hidden system file. It is created automatically in the system folder of the user documents folder (**%USERPROFILE%\Documents** or **%USERPROFILE%\My Documents**) after the first terminal logon from that computer. The file is updated when the connection parameters are modified.
>
> To open the file, select the system folder of the documents folder (the folder icon can be found in the left-hand section of the dialog box) and enter **Default.rdp** in the file name input field.

3. Make sure the text contains the line with the **enablecredsspsupport** parameter. If this parameter is missing, add the following line:

   enablecredsspsupport:i:0

   Note. If this parameter is present, check its value and, if necessary, edit it.

4. Save the changes.

Disabling on the terminal server

To disable pre-authentication on the terminal server:

1. In the Windows Control Panel, go to **System** section in the left-hand area of the window and click the **Remote Settings** link.

   A setup dialog box for system properties appears with a tab for remote access parameters selected.

2. Clear the check box allowing connections with network-level authentication only (with **Network Level Authentication**). To do so, select the **Allow remote connections to this computer** (**Allow connections from computers running any version of Remote Desktop**).

   Note. Changing the field allowing connections with network-level authentication may only be blocked by an active group policy. In this case, open the respective snap-in for group policy management and change the status of the following parameter: Require user authentication for remote connections by using **Network Level Authentication**. This setting can be found in the computer group of configuration policies, section **Administrative Templates** / **Windows Components** / **Remote Desktop Services** / **Remote Desktop Session Host** / **Security**.

3. Save the changes.

Software methods for processing security tokens

In terminal sessions, various methods may be used for processing security tokens connected on terminal clients. The following methods are supported (listed in order of usage priority):

1. Virtual channels method. It is applied if the Client or the Secret Net Studio data protection tool (version 7.0 or later) is installed on the terminal client. This method does not require additional settings and is available all the time (cannot be disabled).
2. Method based on the RPC (Remote Procedure Call) protocol. It is applied if the Client or the Secret Net Studio data protection tool (version 5.0 or later) is installed on the terminal client. To use this method, additional configuration of TCP ports for network connections is required. This method is disabled by default. To use this method, set a zero value for the **NoRemoteConnect** parameter in the following system registry key: **HKLM\Software\Infosec\Secret Net 5\HwSystem**.
3. Method using the **Smart Card** mode. It is applied when the Client is not installed on the terminal client. To use this method, the **Smart Card** mode should be enabled in the remote connection parameters. To block this method, create the **NoSCRedirection** parameter of the **REG_DWORD** type with value **1** in the following system registry key: **HKLM\Software\Infosec\Secret Net 5\HwSystem**.

Restricting the use of local devices and resources

Secret Net Studio supports blocking the use (redirection) of local devices and computer resources in terminal connections through the Remote Desktop Protocol (RDP). Blocking is carried out by disabling the redirection of certain types of local devices and resources. If the redirection is prohibited in Secret Net Studio, users will not be able to use the respective local devices and resources of their computers in terminal sessions (irrespective of the current remote connection settings).

Prohibition to redirect may be applied depending on the computer's role in the remote connection. The use of devices and resources may be blocked on the terminal server side (to ensure the prohibition is applied to all incoming terminal sessions), on the terminal client side (for all outgoing sessions) or regardless of the computer's role in the remote connection.

Redirection control for local devices of the terminal client

Redirection control is available for local devices with the following connection types:

- devices connected to serial (COM) ports;
- devices connected to parallel (LPT) ports;
- connected drives;
- Plug and Play devices.

By default, redirection of local devices connected to the terminal client computer is enabled. During remote sessions, parameters defined in accordance with standard Windows redirection policies for ports, disks and other Plug and Play devices are applied.

The centralized configuration procedure via the Control Center is described below. Local configuration is performed in the same way via the Local Control Center.

To allow or deny local device redirection:

1. In the Control Center, open the **Computers** panel and select the object you want to configure. Right-click the object and click **Properties**. On the **Settings** tab, click **Load settings**.
2. In the **Policies** section, select **RDP connections control**.
3. Select the required value for the **Redirection of devices in RDP connections** parameter in the drop-down list of each device connection type:
   - **Allowed** — users can configure the use of devices by setting the remote connection parameters; Configuring will still be available regardless of the parameters defined in standard Windows policies;
   - **Connection of remote devices to the computer is not allowed** — blocks device use on the terminal server side (blocking is applied to all incoming terminal sessions);
   - **The computer devices cannot be used remotely** — blocks device use on the terminal server side (blocking is applied to all outgoing terminal sessions);
   - **Prohibited** — blocks device redirection regardless of the computer role in the remote connection (terminal client or server);
   - **Use Windows policy** — users can configure the device usage by remote connection parameters if allowed by standard Windows redirection policies.

   Note. Denial of Plug and Play device redirection is only supported on the terminal server side (**Connection of remote devices to the computer is not allowed**).
4. Click **Apply**.

Clipboard redirection control

By default, clipboard redirection in terminal connections is enabled. During remote sessions, parameters defined in accordance with standard Windows redirection policies are applied.

The centralized configuration procedure via the Control Center in the centralized mode is described below. Local configuration is performed in the same way via the Local Control Center. For information about the Control Center, see document [**1**].

To allow or deny clipboard redirection:

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

2. In the **Policies** section, select **Application Control**.
3. Select the required value for the **Redirection of clipboard in RDP connections** parameter in the drop-down list:
   - **Allowed** — users can configure the use of the clipboard by setting the remote connection parameters; Configuring will still be available regardless of the parameters defined in standard Windows policies;
   - **Connection of remote clipboards to the computer is not allowed** — blocks clipboard use on the terminal server side for remote connections of any terminal clients (blocking is applied to all incoming terminal sessions);
   - **The computer clipboard cannot be used remotely** — blocks clipboard use on the terminal server side for remote connections of any terminal clients (the blocking is applied to all outgoing terminal sessions);
   - **Prohibited** — blocks clipboard redirection regardless of the computer's role in the remote connection (terminal client or server);
   - **Use Windows policy** — users can configure the clipboard use by remote connection parameters if allowed by standard Windows redirection policies.
4. Click **Apply**.

Printer redirection control

By default, the redirection of printers installed on the terminal client computer is enabled. During remote sessions, printer use parameters defined in accordance with standard Windows redirection policies are applied.

The centralized configuration procedure via the Control Center in the centralized mode is described below. Local configuration is performed in the same way via the Local Control Center. For information about the Control Center, see document [**1**].

To deny or allow printer redirection:

1. In the Control Center, open the **Computers** panel and select the object you want to configure. Right-click the object and click **Properties**. On the **Settings** tab, click **Load settings**.
2. In the **Policies** section, select **RDP redirections control**.
3. Select the required value for the **Redirection of printers in RDP connections** parameter in the drop-down list:
   - **Allowed** — users can configure the use of printers by setting the remote connection parameters; Configuring will still be available regardless of the parameters defined in standard Windows policies;
   - **Connection of remote printers to the computer is not allowed** — blocks printer use on the terminal server side (blocking is applied to all incoming terminal sessions);
   - **The computer devices cannot be used remotely** — blocks printer use on the terminal server side (blocking is applied to all outgoing terminal sessions);
   - **Prohibited** — blocks printer redirection regardless of the computer's role in the remote connection (terminal client or server);
   - **Use Windows policy** — users can configure the printer use by remote connection parameters if allowed by standard Windows redirection policies.
4. Click **Apply**.

Protection of confidential information during terminal sessions

If the MAC flow control is enabled, you can enable the automatic assignment of a confidentiality level to terminal sessions. This will ensure that equal levels are used for confidentiality sessions on the terminal client and on the terminal server.

Parameters for automatic assignment of confidentiality levels for user sessions are configured when the flow control mode is enabled (see p. **145**).

Chapter 4
Self-protection

The Self-protection mechanism prevents unauthorized modification of Secret Net Studio configuration.

The Self-protection mechanism controls the following operations with the Client components:

- critical services and processes stopping;
- driver uploading;
- system registry keys modification and deletion;
- file editing and deletion (even as System);
- modification of privileges for access to files, folders and system registry keys.

Neither OS administration tools nor other special tools (such as Process Explorer and Kill Process) can be used to perform these operations.

You can perform operations listed above using Secret Net Studio managing tool if you have respective privileges.

Additionally, the mechanism includes the **Administration privilege control** feature that provides separation between the roles of the security administrator and the local administrator.

Administration privilege control enables the control of local administrator access to the following Secret Net Studio components:

- Local Control Center;
- Application and data control (centralized mode);
- Application and data control;
- Mandatory access control configuration;
- User management;
- Client setup wizard in uninstallation mode;
- Secret Net Studio management in the Windows Control Panel.

To access these tools in administrator mode, as well as to switch the self-protection mechanism to the emergency mode using **snsshell.exe** (see p. **37**), specify the security administrator PIN.

Events related to the Self-protection mechanism are registered in the Secret Net Studio log.

You can manage the Self-protection mechanism either centrally using the Control Center or locally using the Local Control Center. Only the following users are allowed to manage Self-protection:

- to manage self-protection locally, a user must be added to the local **Administrators** group and have the privilege to manage Self-protection mechanism. By default, the local **Administrators** group has this privilege;
- to manage self-protection centrally, a user must be added to the **Security Domain Administrators** group and have privileges to edit policies and administer the security system. By default, **Security Domain Administrators** group has these privileges.

After the Client installation is finished, self-protection is enabled. To complete self-protection setup:

1. Add users that will manage the Self-protection mechanism to the **Security Domain Administrators** group and grant them the respective privileges (see **The Control Center user privileges** section in document [**1**]).
2. Configure the Self-protection mechanism (see below).

3. Configure event registration parameters for the Self-protection mechanism (see p. 49).

Setting up administrative privileges control

This section describes the centralized setup of the setting via the Control Center. Local setup is performed similarly but via the Local Control Center.

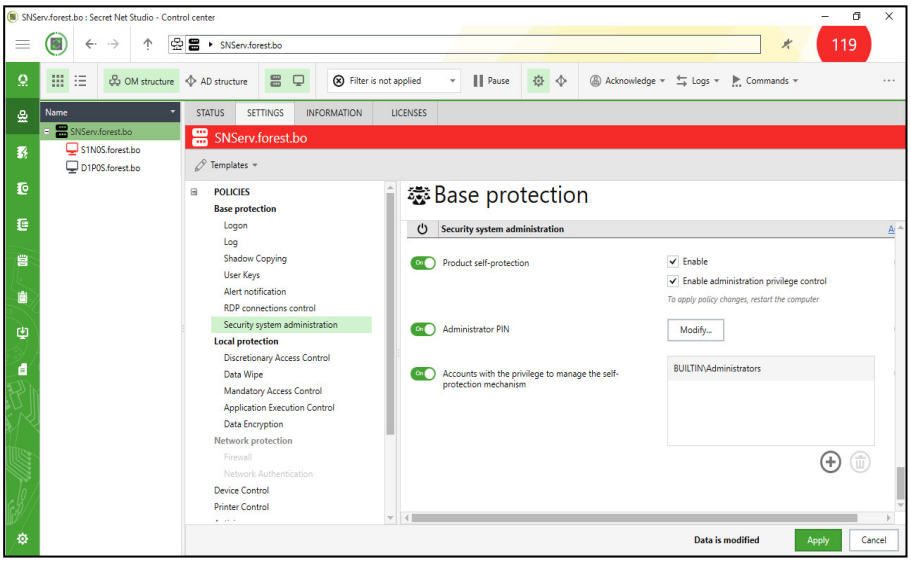
To configure administrative privileges control:

1. In the Control Center, open the **Computers** panel and select the object that you want to configure. Right-click that object, click **Properties**, then click **Settings** and click **Load settings**.

   Tip. To configure the Self-protection mechanism directly on the protected computer, run Local Control Center, then, on the **Computer** panel, click **SETTINGS**, and on the **Policies**>**Base protection** section, click **Security system administration**.

2. In the **Policies > Base protection** section, click **Security system administration**.

   An example of the **Self-protection** subsection view is shown in the figure below.



   Tip. Before configuring group policies, enable the toggle switch near the required parameter.

3. Configure the **Enable administrative privilege control** feature that prompts users to enter administrator PIN when they attempt to start the Local Control Center in administrator mode:
   - select the check box to enable the feature. A dialog box asking you to enter the administrator PIN appears. Enter the administrator PIN and click **Yes**;
   - clear the check box to disable the feature.

   Note. This feature is disabled by default. It can only be used if self-protection is enabled.

4. In the **Administrator PIN** field, click **Modify**. In the **Change password** window, enter the new password, confirm it and click **Apply**.

   This password is necessary to disable the Self-protection mechanism in case of emergency using the **snsshell.exe** tool (see p. 37) and to access the following programs in administrator mode:

- Local Control Center;
- Application and data control (centralized mode);
- Application and data control;
- Mandatory access control configuration;
- User management;

- Client setup wizard in uninstallation mode;
- Secret Net Studio management in the Windows Control Panel.

Attention! When entering the password, consider the following requirements:
- Minimum password length is 8 characters and maximum password length is 32 characters. The password may contain the following characters:
  - 1234567890 — digits;
  - abcdefghijklmnopqrstuvwxyz — English lowercase letters;
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ — English uppercase letters;
  - _$!@#;%^:&?*)(-+=/|.,<>`~ \ — special characters.
- Consider the following recommendations:
  - change your password with the frequency specified in the password policy;
  - use a combination of letters, digits and special characters for a robust password.

5. In the **Accounts with the privilege to manage the self-protection mechanism** field, add the users and user groups to have privileges to locally manage the Self-protection mechanism. To add or remove users and groups, click the respective buttons under the list.

Note. The list cannot be empty.

6. Click **Apply**.

Enabling and disabling self-protection

You can enable and disable self-protection via the Control Center or the Local Control Center. To enable and disable self-protection, the user must have the required rights and privileges (see p. 35). To complete the operation, restart the computer.

To enable or disable self-protection:

1. In the Control Center, open the **Computers** panel and select the object that you want to configure. Right-click that object, click **Properties**, then click **SETTINGS** and click **Load settings**.

Tip. To configure the Self-protection mechanism directly on the protected computer, run Local Control Center, then, on the **Computer** panel, click **SETTINGS**, and on the **Policies**>**Base protection** section, click **Security system administration**.

2. On the **Policies** > **Base protection** section, click **Security system administration**.
3. For **Product self-protection** in the **Enable** field:
   - clear the check box to disable the mechanism;
   - select the check box to enable the mechanism.
4. Click **Apply** at the bottom of the window.
5. Restart the computers, where you enabled or disabled the mechanism.

Switching self-protection to emergency mode

In case of emergency, when security components cannot be managed, but you need to change their configuration, the self-protection mechanism can be temporarily switched to the emergency mode.

Note. We recommend you to use this mode only in case of emergency. Otherwise, use normal Secret Net Studio tools.

In emergency mode, self-protection does not work fully. You can modify and delete system registry keys and executable files related to the Client components. However, you cannot perform unauthorized changes to the Client via local management tools. For example, you cannot uninstall the Client, or its components as well as switch the Client from network operation mode to standalone operation mode if you do not have the privilege to locally manage the self-protection mechanism.

The mechanism can be switched to the emergency mode using the **snsshell.exe** tool from the Secret Net Studio setup folder. This tool allows you to switch self-protection to the emergency mode for Windows in normal mode or protected mode for the duration of the current session. After you restart the computer, self-protection works in normal mode again, but any configuration changes made in emergency mode are saved.

To switch self-protection to emergency mode:

1. Start the computer in protected mode (or normal mode) and log on to Windows as a local administrator.
2. In the command prompt, open the Client installation directory and run the command:

   ```
   snsshell.exe selfprot deactivatesd
   ```

   An administrator PIN request appears in the command prompt window.
3. Enter the administrator PIN and press **Enter**.

   Note. By default, after the Client installation, Secret Net Studio administrator PIN is set to **12345678**.

   If you enter the correct PIN, a message appears, saying that self-protection is disabled. The message also suggests changing the administrator PIN.
4. Change the required security settings.

   Note. For example, modify a required system registry key, replace or rename the program module file that caused the error.
5. Restart the computer.

Chapter 5
Shadow Copy

General information

The shadow copying mechanism creates backups of data that can be moved to removable drives. The backups are saved in a special repository that can be accessed only by users with the respective privileges. The mechanism affects devices for which the shadow copy is enabled.

Shadow copy repository

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

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

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

Search in the shadow copy repository

You can perform a search in the shadow copy repository using the Local Control Center. This function is based on the Windows Search component, in which in order to accelerate the search, an index-database with detailed information about files is used. An actual index is created when indexing files periodically. The indexing of the shadow copy repository is started automatically at given times.

New files added to the shadow copy repository may be missing in the index when searching. Therefore, if the search produces no results, it may be due to the missing of the new files in the index.

Search by names

When saving a duplicate to the shadow copy repository, a new inner name is created for the file based on its checksum and timestamp. The file extension is not changed, but it may be deleted if its length exceeds the maximum length of the file name.

The duplicate name and the initial file name are compared in the record containing information about the shadow copy event. Thus, using the log record, the file can be restored as it was sent to a removable drive.

When searching by names in the shadow copy repository, no initial but inner names are used. If you want to search by initial file names, you should use the tools for searching by the Secret Net Studio log records — initial file names are given in the **Shadow copying** category event descriptions.

Search by file content

Windows Search supports a wide range of file types to search by file content. For example, a word or a phrase can be found in files with the following extensions: txt, htm, html, xml, as well as in documents saved in Microsoft Office.

Note. The list of file formats and types supported by Windows Search is available on the Microsoft website.

The list of file formats and types supported by Windows Search is expanded when installing the Client.

General configuration procedure

Configuration of the shadow copying mechanism is performed as follows:

1. Grant privileges for viewing and managing logs to users who will perform audit and manage the shadow copy repository (see p. 45).
2. Configure the shadow copy repository parameters for computers on which the mechanism will be enabled (see p. 40).
3. Specify devices on which the shadow copy will be enabled (see p. 40).
4. We recommend performing regular audit of the repository contents (see p. 41).

Configuring shadow copy repository

When setting up the parameters, the maximum volume of the repository can be changed and rewriting can be enabled or disabled.

The centralized configuration procedure via the Control Center is described below. Local setup is performed in the same way via the Local Control Center.

To configure the repository 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 [1].

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 way Secret Net Studio reacts if the repository 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 deny data output, clear the check box. When the maximum size of the storage is reached, the security 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**.

Configuring the shadow copying mechanism for devices

You can disable the shadow copying mechanism for all devices and printers. If the shadow copying mechanism is enabled, parameters specified for devices will come into force. Shadow copying is available for the following types of devices:

- removable drives;
- floppy disk drives;
- optical disk drives that can write data;
- printers.

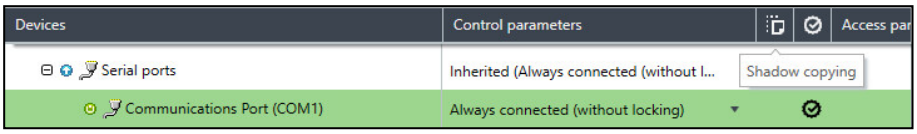
The centralized configuration procedure is described below. Local configuration is performed the same way via the Local Control Center. For detailed information about using the Control Center, see document [**1**].

To manage the shadow copying mechanism:

1. In the Control Center, open the **Computers** panel and select the object you want to configure. Double-click the selected object to open its **Properties** menu. In the **Properties** menu select the **Settings** tab and click **Load Settings**.
2. In the **Policies** section, select the **Device Control** group. Select the required value for the **Shadow Copying** function:

- **Disabled for all devices** — no shadow copying when writing data to devices.
- **Defined by device settings** — shadow copying is performed for devices with shadow copying mode enabled.

3. Select the required element in the list. Set the check box of the **Shadow Copying** column the way you need:
   - select it to enable the copy saving mode;
   - clear it to disable the mode.



4. In the **Policies** section, select the **Print Control** | **Settings parameters** group. Select the required value for **Shadow Copying**:
   - **Disabled for all printers** — no shadow copying when printing.
   - **Defined by printer settings** — shadow copying is performed for printers with shadow copying mode enabled.
5. Select the required element in the list. Set the check box of the **Shadow Copying** column the way you need:
   - select it to enable copy save mode;
   - clear it to disable copy save mode.

Note. If no devices or printers are connected to a computer, you cannot select the check box in the **Shadow Copying** column.

6. Click **Apply**.

Searching and viewing data in the shadow copy repository

The local Control Center enables you to configure the request parameters for the local log. You can use requests to search by data files while loading records with special selection criteria. Such requests enable searching files in the shadow copy repository and loading the log records related to these files.

To view the shadow copy repository and perform standard operations with files (copy, run, 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 files from the repository are blocked.

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

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

Opening the main repository folder

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

To open the window with the main folder of the repository:

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

   The panel for calling up the configuration tools appears.

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

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

Searching and viewing files

When registering a shadow copy event, duplicate copies of files to be placed on removable drives are placed in service folders of the repository. The duplicate files are assigned internal names, which are 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 repository.

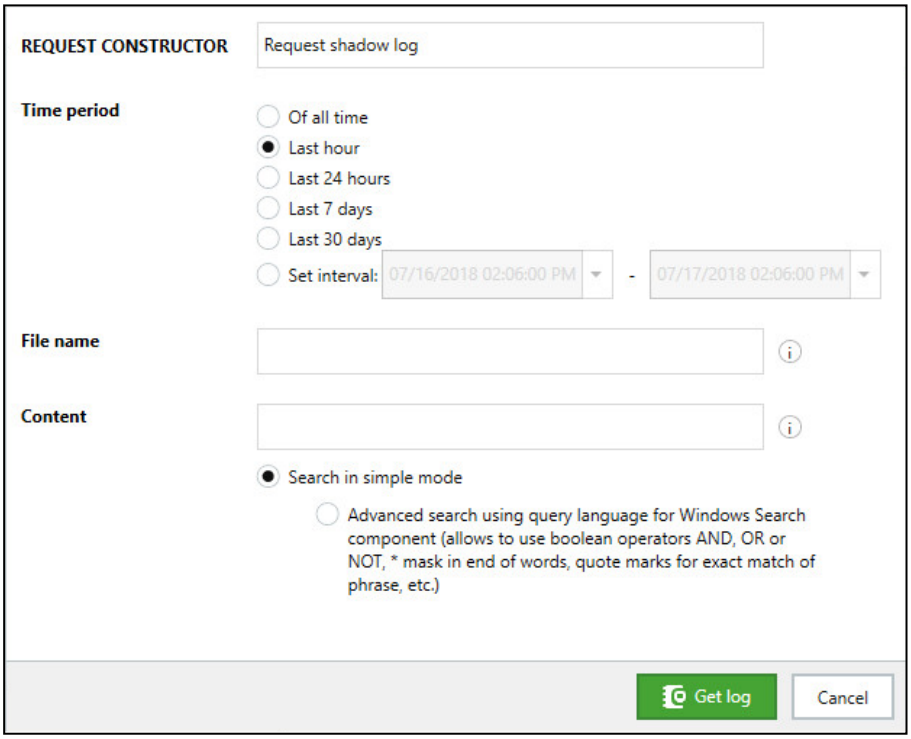
The Local Control Center makes it possible to generate the required file with an original name and quickly go to that file. This file is created in a temporary repository folder based on the duplicate file. The file is generated using the Secret Net Studio log record that contains information on a shadow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

Attention! The folder with temporary repository files is automatically cleared every time you start the Control Center.

To configure parameters for requesting records and viewing temporary copies in the repository:

1. In the Local Control Center, go to the **Logs** panel.
2. In the request management panel, click **New > Request shadow log**.

   The request constructor panel appears.



3. In the **REQUEST CONSTRUCTOR** field, type the request name.
4. Configure the following settings:

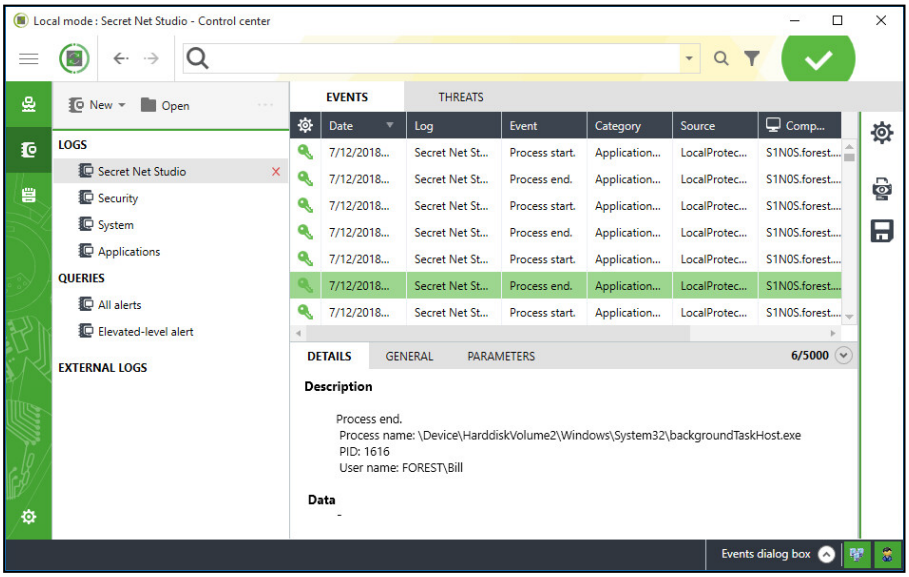
Time period
Specify the time period to search for log records. The time period can be one of the following: • **Of all time**; • **Last hour**; • **Last 24 hours**; • **Last 7 days**; • **Last 30 days**; • **Set interval** — set the time period manually
File name
The search string in file names. Initial file names being contained in the Secret Net Studio log records (see p. **39**). To search for two and more files, you can specify several string values delimited by ";". For example, type **OB***; ***OB**; ***OB*** to search for combination of strings containing the **OB** letters
Content
The search string in file contents. Search by content is available in files which types and formats are supported by Windows Search (see p. **39**)
Search in simple mode or advanced search
If you select **Search in simple mode**, strings in the **File name** and **Content** fields are considered as they are specified. In other words, files containing these strings will be found. This mode is case insensitive. In one field, you can specify several string values delimited by a comma or semicolon. If you select **Advanced search...**, the strings are analyzed, and if they contain logical operators or special characters, the search is performed according to the rules of the query language for Windows Search. In this case, logical operators **AND**, **OR**, **NOT**, wild cards and other symbols can be used. The search strings must be quoted. The comprehensive list of the query language features with examples of use is available on the following website: **http://msdn.microsoft.com/enus/ library/bb231270 (v=VS.85).aspx**

5. Click **Get log**.

   The search will be performed, and in the display area, a list of found records about shadow copy events will appear.

6. Select the record of the shadow copy event that contains information about the file location on the removable drive.

   The additional information dialog box displays detailed event information.



7. In the additional information dialog box, click the command link, which is presented as the original name of the file in the **Description** section.

The program creates a copy of the file with the original name in the temporary repository folder and then the Explorer window appears. The window displays a list of files in the temporary folder with the required file highlighted.

Chapter 6
Local audit

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 (logon 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 with log entries locally, use the Local Control Center.

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.

Privileges for working with local logs

The following privileges are granted for working with local logs:

- **View the security system log**. The user can download local Secret Net Studio log entries for viewing;
- **Manage the security system log**. The user can download local Secret Net Studio log entries 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 the privilege for log management, we recommend you to grant both privileges. So, to view shadow copies, you need to explicitly grant the privilege to view the log.

The description of the centralized setup procedure at the administrator workplace in the Control Center is provided below. 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 [**1**].

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**.

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 in 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.

Exporting local log entries

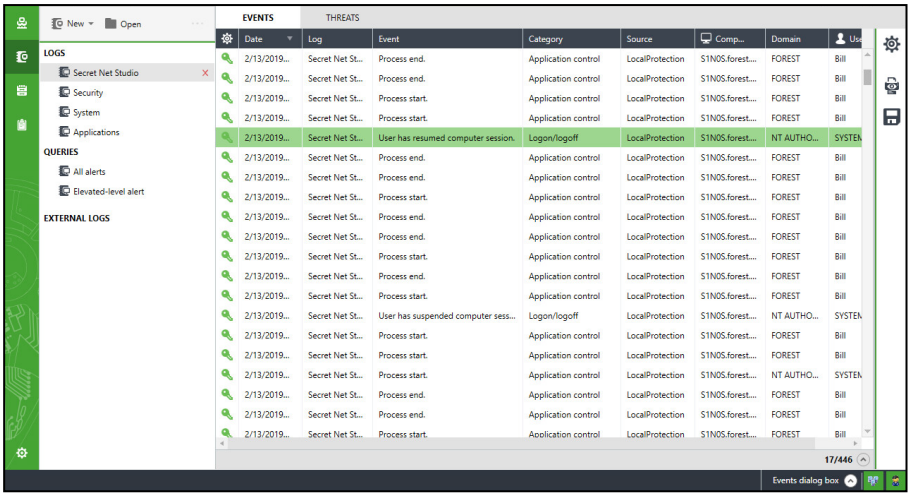
The Control Center allows to export (save) local log entries to files. When exporting, you can clear the log after saving the entries. The following table lists the supported formats for saving.

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:

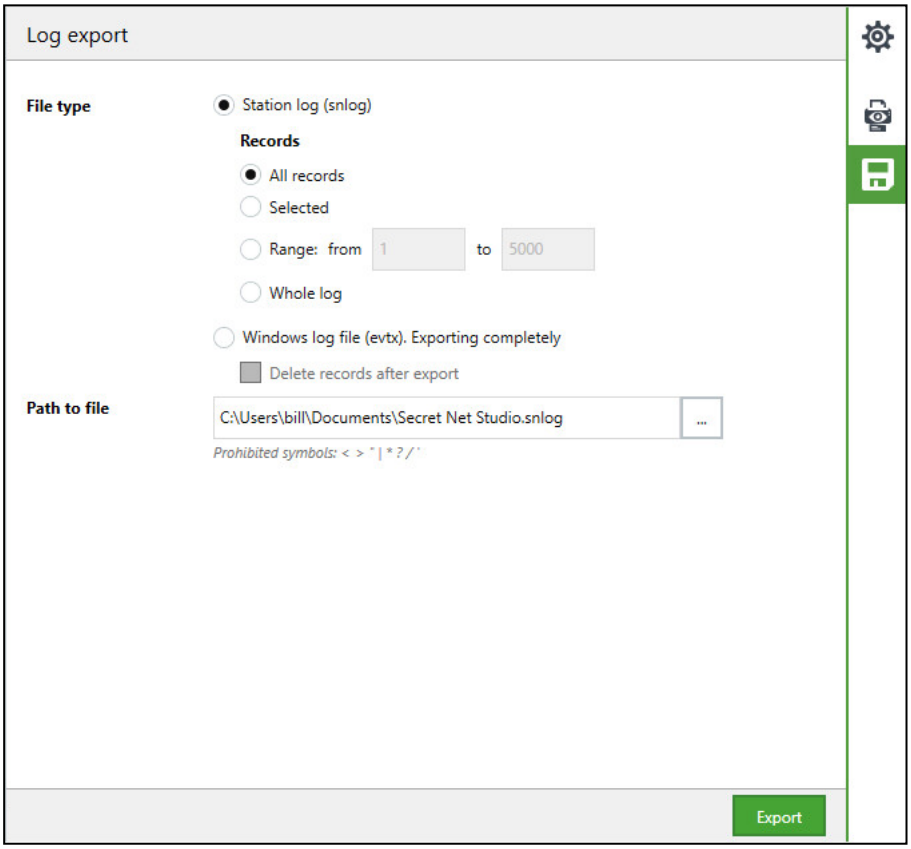
1. Load the entries of the required log to the program.

   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, Secret Net Studio will automatically clear the log after exporting the records to **evtx** file. To clear the Secret Net Studio log, you must be granted the privilege to of manage the security system log (see p**p. 45**)

7. Click **Export**.

Clearing the local log

You can clear the local log (delete entries) when exporting to **evtx** file (see p. **46**) or by running the **Clear log** command in the context menu of the log (this command can only be used for standard Windows OS logs).

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 centralized configuration procedure via the Control Center is described below. Local setup is performed in the same way via the Local Control Center.

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 [**1**].

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.

Erase events if necessary
When the log is full, Secret Net Studio will automatically delete the required number of the oldest records from the log
Erase events older than <...> days
When the log is full, Secret Net Studio will automatically remove the records with storage time exceeding 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
Do not erase events (clear log manually)

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 to avoid log flooding, because this might lead to system failures and computer lockout

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 centralized configuration procedure is described below. Local configuration is performed the same way via the Local 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 [1].

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**.

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 started by users;
- event registration for all security system processes – 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 to quickly flood with records of these events. For most mechanisms this registration mode is not required. Therefore, the registration of events related only 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 information on enabling and configuring process isolation, see p. **106**.

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 centralized configuration procedure via the Control Center is described below. Local setup is performed the same way via the Local 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 [**1**].

2. In the **Event Registration** section, select the **Application Control** group of settings.
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 registering applications started only by the user is enough, clear the check box.
4. For the remaining settings in the **Application Control** group, select the events to be registered in the log.
5. Click **Apply**.

Chapter 7
Software Passport

General information

Software Passport is a security mechanism designed to control software configuration and integrity on the protected computers. The control is performed by scanning executable files and calculating their checksums. A set of controlled files is a software environment for collecting data and analyzing its alterations.

Executable files recognition is performed using their extension. A set of file extensions and search directories can be configured. Scanning starts on a schedule or on a command of the Control Center user.

After the scanning, the software environment data of a protected computer is uploaded to the Security Server and receives the Workstation passport project status. The data is compared to the results of the previous scanning stored as approved passport. The alterations are analyzed and the passport project can be approved as the current passport of the protected computer, if necessary.

Enabling the mechanism

By default, the **Software Passport** mechanism is not enabled after you install Secret Net Studio. To enable it, do the following:

1. Register the licenses for the mechanism.
2. Turn on the mechanism on the protected computers.

Registering licenses for the mechanism

The Software passport mechanism requires a separate license that must be registered on the protected computers. The license can be added using the Control Center.

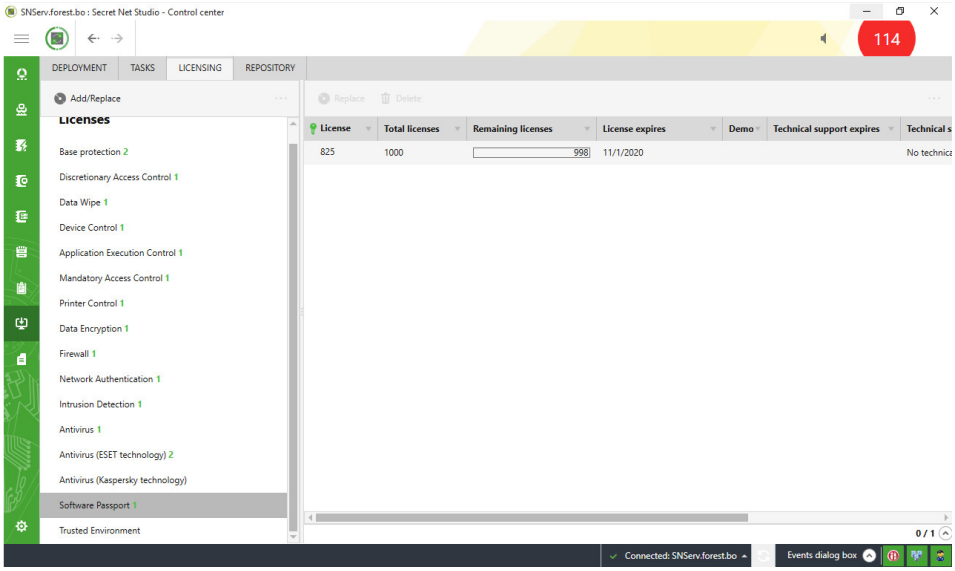
You can register the license centrally using the Control Center on the administrator's workstation or directly on the protected computer in local mode. We recommend registering the license in the centralized repository. Thus, the Clients receive the licenses from the Security Server. License registration in local mode may be required for computers without permanent connection to the Security Server (for example, the Clients in the offline mode).

Registering the licenses in the centralized repository

You can register the license in the centralized repository using the Control Center in the centralized mode. A security administrator (a user included in the group of security domain administrators) has the privileges for the operation.

To register the license in the centralized repository:

1. On the **Deployment** panel, click the **Licensing** tab, and click **Add/Replace**.



2. In the dialog box, select the needed license file.
3. If the added licenses need to be activated, choose the activation method and click **Apply**.

Note. The license registration and activation procedure are the preparatory steps of the centralized installation of Secret Net Studio Client. We recommend using this installation method. For detailed information about centralized deployment, see document[**1**], chapter 5.

Registering the license for a computer centrally

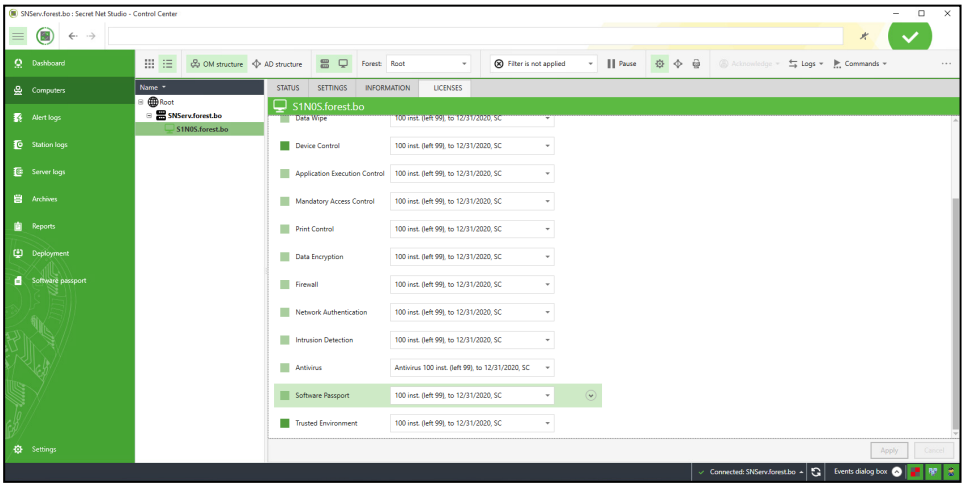
If the Client has no license for the Software Passport mechanism, you can register one from the set of available licenses in the repository. This operation is required in case, for example, the Client had been installed before the license was registered in the repository.

Note. The license is registered automatically if the Client was installed centrally after the license registration in the repository.

The centralized license registration procedure is performed using the Control Center in the centralized mode. A security administrator (a user included to the group of security domain administrators) has the privileges for the operation.

To register the license on a computer centrally:

1. Go to the **Computers** panel, right-click the required computer and click **Properties**. In the appeared dialog box, go to the **Licenses** tab.



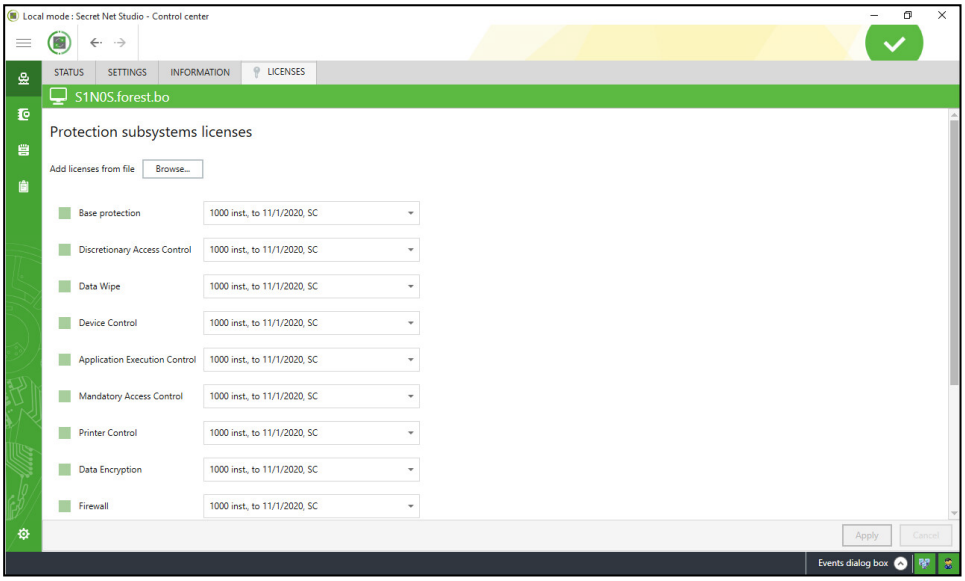
2. In the list of protection subsystems, select the **Software Passport** element. After the data is loaded, select the license from the drop-down list. To view the information about the selected license, click the button on the right.
3. Click **Apply** at the bottom of the dialog box.

Registering the license on a computer locally

If a protected computer has no connection to the Security Server, you can register the license for the Software Passport mechanism locally on this computer. This procedure can be performed in the Local Control Center. A local administrator (a user included to a local Administrators group) has the privileges for the operation.

To register the license locally on a computer:

1. On the **Computer** panel, click **Licenses**, then click **Browse**.



2. In the appeared dialog box, select the required license file.
3. After the licenses are loaded, go to the **Software Passport** protection subsystem. You can see if the license is added by the indicator on the left. Plus, the drop-down list must contain information about the license. To view the information, click the button on the right.
4. Click **Apply** at the bottom of the dialog box.

Enabling the mechanism on the protected computers

The Software Passport mechanism can be enabled either automatically or manually. Automatic enabling can be performed during the centralized installation after the license is registered in the repository (by default, the deployment task includes the installation procedure of the mechanism).

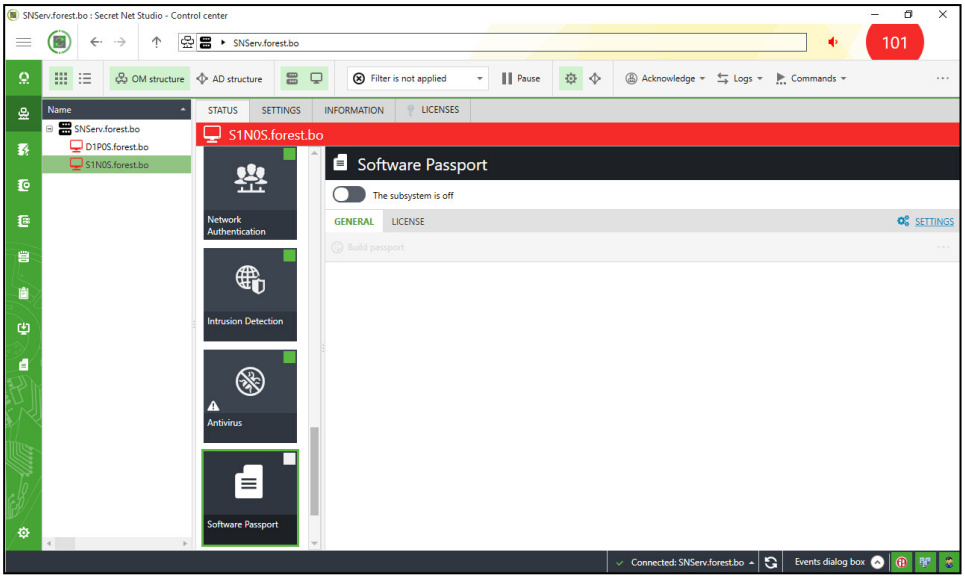
If the Software Passport mechanism license was registered on a computer after the Client had been installed, you should enable the mechanism manually, either centrally or locally.

Enabling the mechanism for the computer centrally

The centralized enabling of the mechanism is performed in the Control Center. A security administrator (a user included to a group of security domain administrators) has the privileges for the operation.

To enable the mechanism on a computer centrally:

1. Go to the **Computers** panel, right-click the required computer and click **Properties**. On the **Status** tab, click **Software Passport**. A panel containing information about the mechanism appears on the right.



2. Click the toggle switch to the left of the panel's title to put it on the **On** mode.

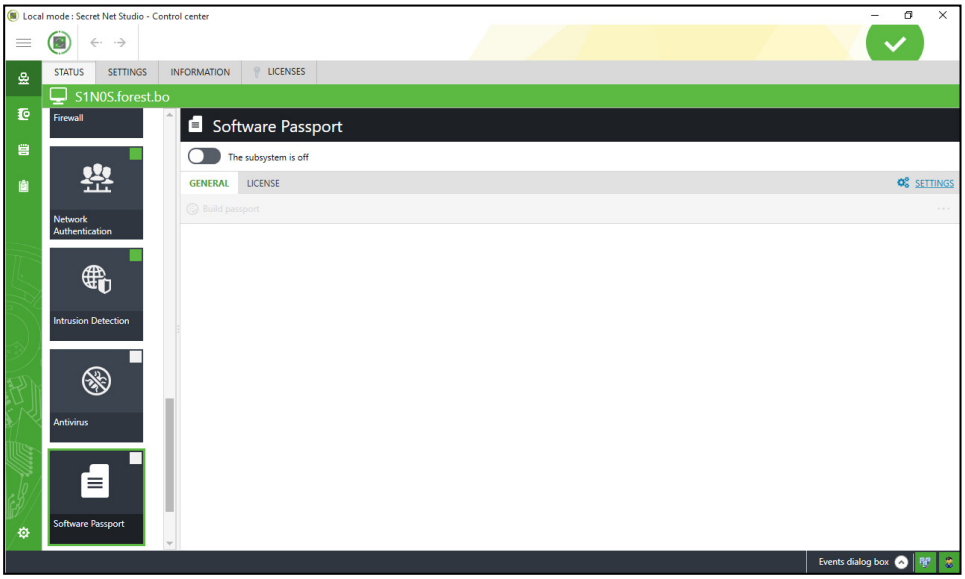
Note. During the first time you enable the mechanism (when the code modules are not installed on a computer), you should restart your computer to complete the procedure. To restart the computer remotely, use the respective command in the computer's shortcut menu; or on the program's toolbar, go to the **Commands** menu.

Enabling the mechanism locally on a computer

If the protected computer has no connection to the Security Server, you can enable the **Software Passport** mechanism locally on the computer. This procedure is performed in the Local Control Center. A local administrator (a user included to a local group of administrators) has the privileges for the operation.

To enable the mechanism locally on a computer:

1. On the **Computer** panel, go to the **Status** tab, click the **Software Passport** tile. A panel containing information about the mechanism appears on the right.



2. Click the toggle switch to the left of the panel's title to put it on the **On** mode.

Note. During the first time you enable the mechanism (when the code modules are not installed on a computer), you should restart your computer to complete the procedure.

The mechanism configuration

The Software Passport mechanism configuration is performed in the following order:

1. Generating key information for software passports confirmation.
2. Granting privileges to users.
3. Editing the OM structure.
4. Configuring the functional parameters of the mechanism.

Generating key information to approve Software passports

To approve the **Software Passport** project, you should use the key information generated in Secret Net Studio. The key information includes cryptographic keys (public and private) that can also be used for encrypting mechanisms in encrypting containers. The public key is stored in the Secret Net Studio database while the private key is stored on a user key carrier drive.

The key information is generating in the User management program. Cryptographic keys can be created while assigning an identifier to a user or later. For the description of the procedure, see p. 25. To create the cryptographic keys, in the Security Token Assignment wizard, select the **Write user's private key to security token** check box. If you need to generate key information after the identifier was assigned, an administrator can perform the **Issue** / **Replace** procedure while managing the cryptographic keys (see p. 173).

Granting privileges to the users

Privileges for managing the Software Passport mechanism can be divided between the employees according to their functions. The functions are shown in the following table:

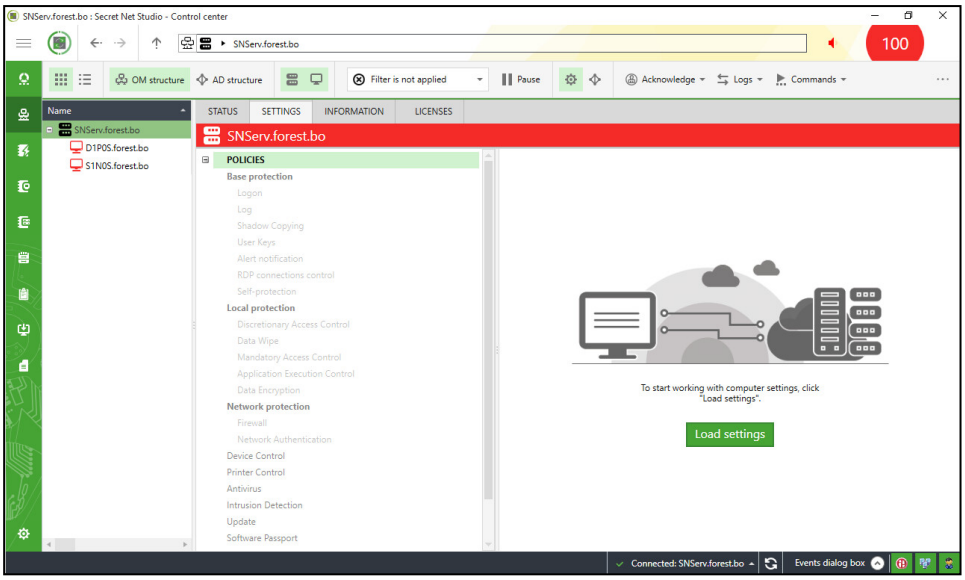
Role	Functions
Administrator (a user included in a group of security domain administrators)	• Appoints necessary privileges for other roles. • Enables the **Software Passport** mechanism on the protected computers. • Configures the mechanism's parameters (scanning schedule, a list of file extensions and folders to be controlled, event registration). • Loads logs for viewing information about events concerning operation of the mechanism. • Launches a synchronization of the passports' database on the Security Server
Controller	• Imports the software passports of the protected computers to the **Security Server** database. • Approves passport projects (verifies with electronic signature). • Launches scanning and collecting Software Passports from the Control Center
Operator	• Launches scanning and collecting of software passports in the Local Control Center. • Saves collected software passports as files (in local mode). • Loads for display and compares passports' contents in the Control Center

Privileges can be granted using the Control Center. A security administrator (a user included in a group of security domain administrators) has the privileges for the operation.

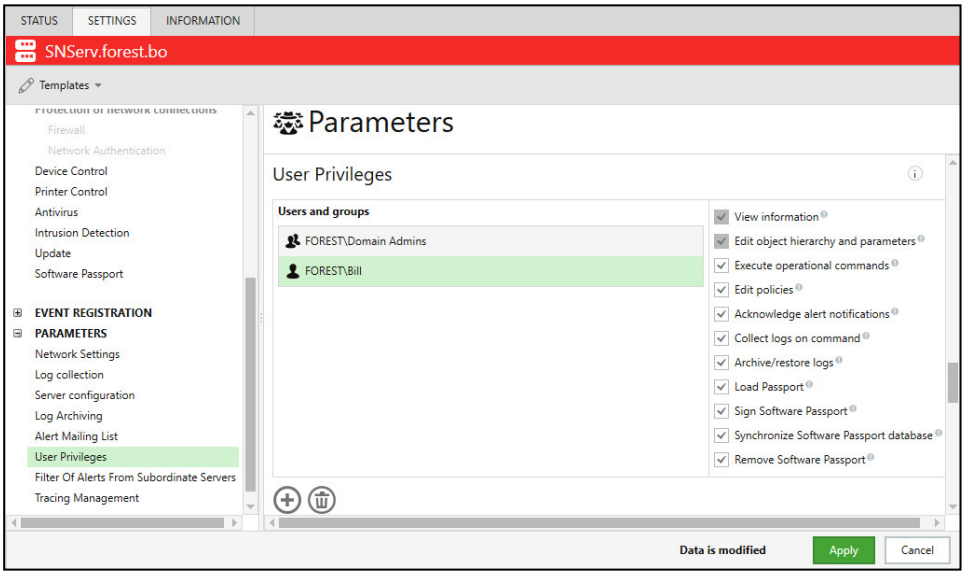
To grant privileges:

1. Go to the **Computers** panel, right- click the Security Server and click **Properties**. In the appeared dialog box, go to the **Settings** tab and click **Load**

Settings.



2. After the settings are loaded, go to the **Parameters** section and click **User Privileges**.



3. In the **Users and Groups** list, add accounts to be used as a controller and an operator. Click **Add user** and select the required accounts in the dialog box.

> **Note.** You can remove an account from the list. Select the account you want to remove from the list, click **Remove user**.

4. For users with the controller function, select the **Execute operational commands**, **Load passport** and **Sign software passport** privileges.

> **Note.** An operator function requires only the **View information** privilege that is granted by default. For operations in local mode, a user should be included in a local group of administrators.

5. Click **Apply**.

Editing the OM structure

To process and analyze software environment status data of the protected computers, these computers should be presented in the OM structure. Installing the Client subordinate to the Security Server automatically adds this computer to the OM structure. If the Client was installed without being subordinate to the Security Server, you should perform the respective operations to add the computer to the

structure and make it subordinate to the respective Security Server. The operations are performed in the Control Center. For detailed information about editing the OM structure, see document [**1**].

Note. The OM structure should contain all computers on which data is collected for the Software Passport mechanism, even computers with no permanent connection to the Security Server (for example, computers with the Client in the local mode). The object's presence in Active Directory structure is enough to add the computer to the OM structure. If the object is not presented (a computer is not connected to AD domain), create it manually with the same name using standard AD tools for managing computers and users.

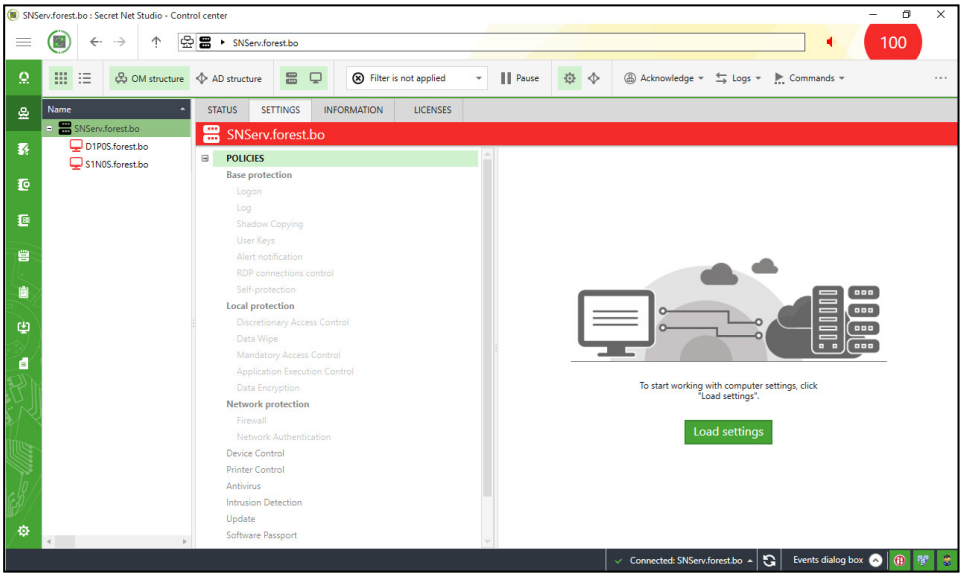
Configuring the mechanism settings centrally

Centralized configuration of Software Passport settings is performed in the Control Center. The parameters can be specified directly for the protected computers (local policy parameters), for domains, organization units and the Security Servers. The parameters are applied similarly to the other mechanisms. Local policy parameters have the lowest priority, the Security Server parameters have the highest priority.

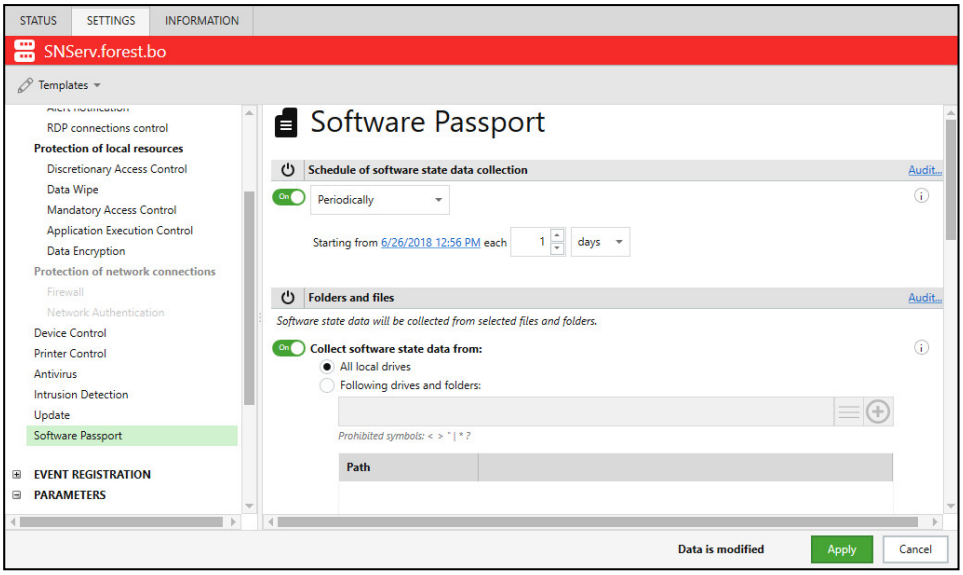
A security administrator (a user included to a group of security domain administrators) has the privileges for the operation.

To configure mechanism's parameters:

1. On the **Computers** panel, right-click the required object, click **Properties**. In the dialog box, go to the **Settings** tab and click **Load Settings**.



2. After the parameters are loaded, go to the **Policies** section and click **Software Passport**.



Note. Only the parameters you specified explicitly are applied in the policies of a domain, an organization unit or the Security Server. To specify parameters, use toggle switches to the left of each parameter. You should put it to the **On** position.

3. To start software passport building at specific time periods, configure the schedule. Select the required mode in the **Schedule of software state data collection** group of fields:

Periodically
The process starts at regular intervals. The interval's duration is specified in minutes, hours or days. The mode starts the operation at certain date and time. To specify the time, click a link with the current date and time values and, in the appeared dialog box, specify the new values
Weekly
The process starts at scheduled moments of time. The schedule is presented as a table. The columns of the table contain the days of the week and the rows contain the hours. To select the time for the operation, click the respective cell in the table. The scheduled operation repeats weekly

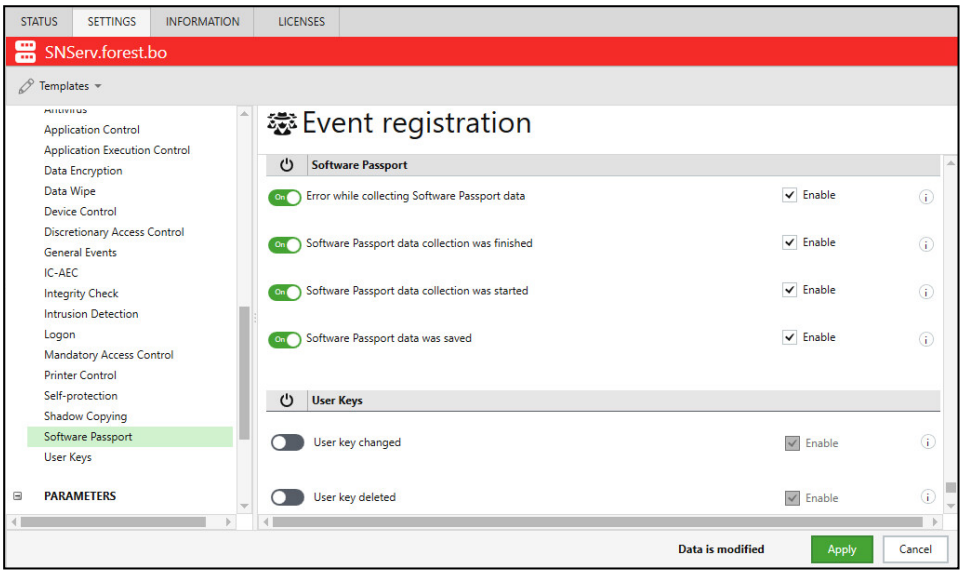
4. In the **Folders and files** group of fields, specify a scanning area while collecting data. You can select the respective check boxes:

All local drives
While collecting data, the scanning is performed in all folders on all local drives of the computer except those on the list of exclusions
Following drives and folders
While collecting data, the scanning is performed only in folders from the list. To add a folder in the list, specify the full path (with the drive) in the respective text box and click the **Add** button on the right. You can also add a path using system-wide environment variables (**%ProgramFiles%**, for example). To select the variable, click the **Add from default list** button that is next to the **Add** button. To delete and edit elements in the list, use the respective buttons under the list
Exclude drives and folders
While collecting data, the folders and files specified in the list are skipped. The list of exclusions can be configured similarly to the list of the **Following drives and folders**

5. In the **File extensions** group of fields, specify the extensions of files to be scanned. You can select the respective check boxes:

All file extensions
While collecting data, the scanning is performed for all detected files
Selected
While collecting data, the scanning is performed only for files with the extensions specified in the list. To add an extension to the list, type it in the respective text box and click the **Add** button. You can also add an extension from the list of default file extensions: click the **Add from default list** button that is next to the **Add** button. To delete or edit elements in the list, use the respective buttons under the list

6. On the **Settings** tab, go to the **Event Registration** section and click **Software passport**.



Note. Only the parameters you specified explicitly are applied in the policies of a domain, an organization unit or the Security Server. To specify parameters, use toggle switches to the left of each parameter. You should put it to the **On** position.

7. Enable registration of the required events in the local logs of the protected computers. You can select the respective check boxes:

Software Passport data collection was started
The event is registered at the start of the data collection process
Error while collecting Software Passport data
The event is registered in case of an error during the data collection process (for example, in case of failed access attempts to the file during the scan)
Software Passport data collection was finished
The event is registered after the data collection process is finished
Software Passport data was saved
The event is registered when the Software passport is saved as a file (on the protected computer locally) or when the Software passport is transferred to the Security Server

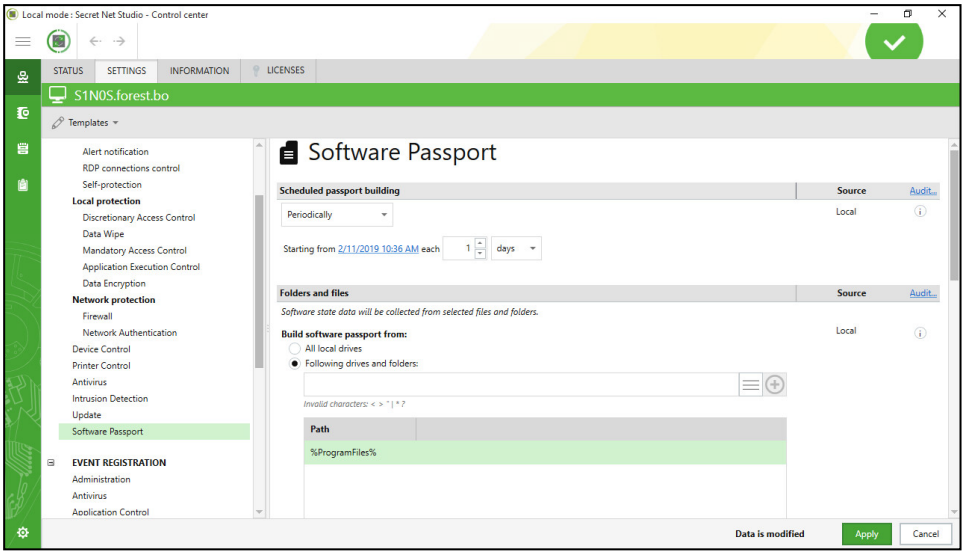
8. Click **Apply**.

Configuring Software Passport settings locally

If the protected computer has no connection to the Security Server, you can configure the **Software passport** mechanism locally on this computer. The operation is performed in the Local Control Center. A local administrator (a user included to a local group of administrators) has the privileges for the operation.

To configure the mechanism settings locally:

1. On the **Computer** panel, go to the **Settings** tab and in the **Policies** section, click **Software Passport**.



> **Note.** Parameters of the local policy cannot be edited if you specified them explicitly in the policies of a domain, an organizational unit or the Security Server. You can edit only the parameters that have the **Local** status in the **Source** column.

2. If you need to build software passports periodically, specify the schedule. Select the required mode in the **Scheduled passport building** group of fields:

Periodically
The process starts at regular intervals. The interval's duration is specified in minutes, hours or days. The mode starts the operation at certain date and time. To specify the time, click a link with the current date and time values and, in the appeared dialog box, specify the new values
Weekly
The process starts at scheduled moments of time. The schedule is presented as a table. The columns of the table contain the days of the week and the rows contain the hours. To select the time for the operation, click the respective cell in the table. The scheduled operation repeats weekly

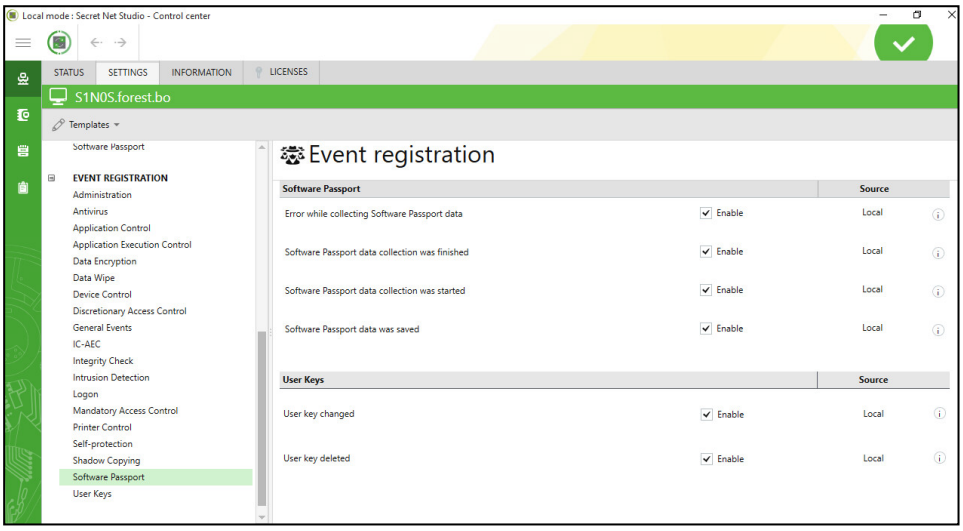
3. In the **Folders and files** group of fields, specify a scanning area while collecting data. You can select the respective check boxes:

All local drives
While collecting data, the scanning is performed in all folders on all local drives of the computer except those in the list of exclusions
Following drives and folders
While collecting data, the scanning is performed only in specified folders. To add a folder in the list, specify the full path (with the drive) in the respective text box and click the **Add** button on the right. You can also add a path using system-wide environment variables (**%ProgramFiles%**, for example) To select the variable, click the **Add from default list** button that is next to the **Add** button. To delete and edit elements in the list, use the respective buttons under the list
Exclude drives and folders
While collecting data, the folders and files specified in the list are skipped. The list of exclusions can be configured similarly to the list of the **Following drives and folders**

4. In the **File extensions** group of fields, specify the extensions of files to be scanned. You can select the respective check boxes:

All file extensions
While collecting data, the scanning is performed for all detected files
Selected
While collecting data, the scanning is performed only for files with the extensions specified in the list. To add an extension to the list, type it in the respective text box and click the **Add** button. You can also add an extension from the list of default file extensions: click the **Add from default list** button that is next to the **Add** button. To delete or edit elements in the list, use the respective buttons under the list

5. On the **Settings** tab, go to the **Event registration** section and click **Software passport**.



Note. Parameters of the local policy cannot be edited if you specified them explicitly in the policies of a domain, an organization unit or the Security Server. You can edit only the parameters that have the **Local** status in the **Source** column.

6. Enable registration of the required events in the local logs of the protected computers. You can select the respective check boxes:

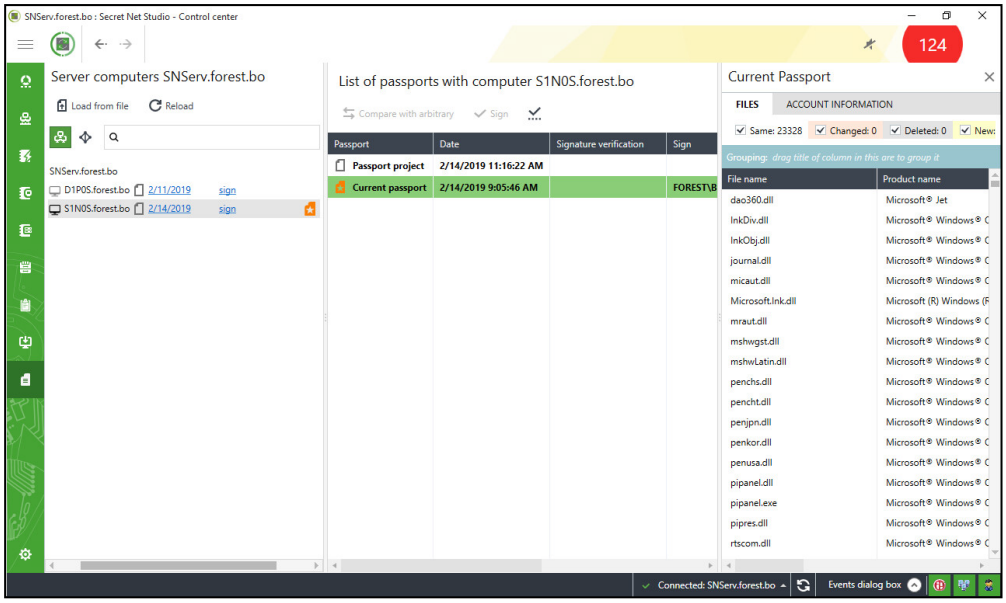
Software Passport data collection was started
The event is registered at the start of the data collection process
Software Passport data collection error
The event is registered in case of an error during the data collection process (for example, in case of failed access attempts to the file during the scan)
Software Passport data collection was finished
The event is registered after the data collection process is finished
Software Passport data was saved
The event is registered when the Software passport is saved as a file (on the protected computer locally) or when the Software passport is transferred to the Security Server

7. Click **Apply**.

Operations with passports

Processing of the Software passports is performed using the Control Center. To operate the mechanism, on the navigation panel, click **Software Passport**.

The panel appears as in the figure below.



An overall sequence of the scanning and collecting procedures on the protected computer is as follows:

1. Collecting the Software passport data on the protected computer.
2. Creating the Software passport project (loading collected data to the Security Server database).
3. Comparing the Software passport project to the existing passports of the computer.
4. Checking the validity of the signature for approved passports.
5. Approving the Software passport project as a current passport.

To operate with passports' database you can perform the following actions:

- create a backup copy;
- delete the outdated passports;
- recover the passports from the backups.

Collecting the Software passport data on the protected computer

Collecting software environment status data on the protected computers can be performed either according to the specified schedule (see above) or on command via the Control Center. You can also start the data collection process either locally or centrally.

Starting the data collection centrally

The centralized start of the Software passport data collection of the protected computer is performed in the Control Center. A user with the **Execute operational commands** and **Load software passports from a file** privileges can start the process centrally.

To start the data collection centrally:

1. On the left of the **Software Passport** panel, select the required computer. If necessary, use the search and filtration tools to find the computer faster.
2. Right-click the computer and click **Build new Passport**. The data collection process starts and its current status is displayed next to the name of the computer in the list. After the process is finished, the **Load to server** button appears.

Starting the data collection locally on a computer

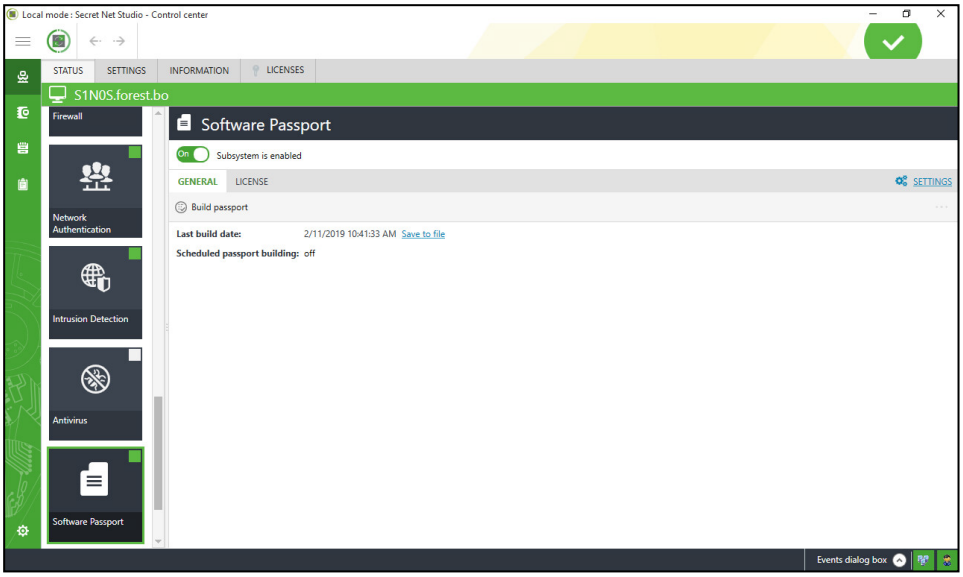
If the protected computer has no connection to the Security Server, you can start the Software passport data collection locally on this computer. If the computer has

no network connection at the time of the passport project building, you should create a file that must be uploaded to the Security Server database.

The local data collection is performed in the Local Control Center. A local administrator (a user included in a local group of administrators) has the privileges for the operation.

To start the data collection locally on a computer:

1. On the **Computer** panel, go to the **Status** tab and click the **Software Passport** button. A dialog box appears as in the figure below.



> **Note.** Check the data about time of the previous data collection. It is specified in the **Last build date** line. If the previously collected data is up-to-date (for example, the recent data collection by schedule), you can skip the new data collection process and proceed to step 3.

2. To start the data collection, click **Build passport**. You can see the respective status of the process in the **Software passport** dialog box. When the process is finished, the last build date is changed and the **Save as file** link appears.
3. If necessary, save the collected data as a file to load it to the **Security Server** database. Click the **Save as file** link and, in the dialog box, specify a destination folder.

Building the passport project

While loading the Software passport data to the Security Server database, a new passport project is created in the list of passports of the protected computer. If there is already a project in the list, it will be replaced with the new one.

The software passport data loading procedure is performed in the Control Center. You can upload it directly from the protected computer or using the file created during the local data collection. A user with the **Execute operational commands** and **Load software passports from a file** privileges can start the process centrally.

To upload data and build the passport project:

1. On the left of the **Software Passport** panel, select the required computer. If necessary, use the search and filtration tools to find the computer faster.
2. Right-click the computer and select one of the following commands:
   - **Load last** — to download data directly from the protected computer (the computer must be started and have network connection);
   - **Load from file** — to load data from file created during the local data collection.

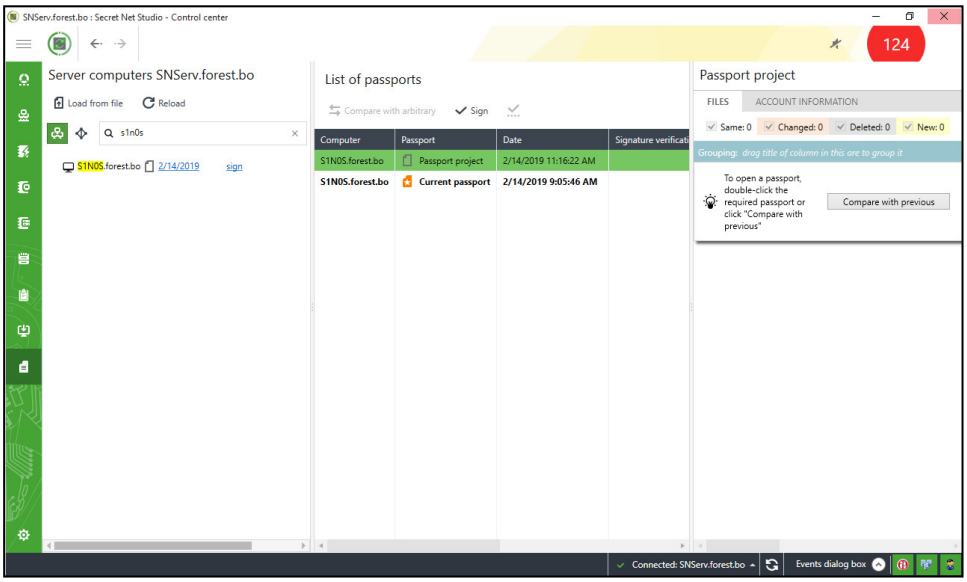
3. If you load data from a file, a dialog box where you can edit the computer accounting information appears. If necessary, specify the up- to- date accounting information.

Comparing passports

If the passports list of the protected computer contains several passports (for example, the current approved passport and a previously approved passport), you can compare these passports concerning their software environment data. You can compare the passports using the Control Center. A user with the **View information** privilege has the right to compare passports.

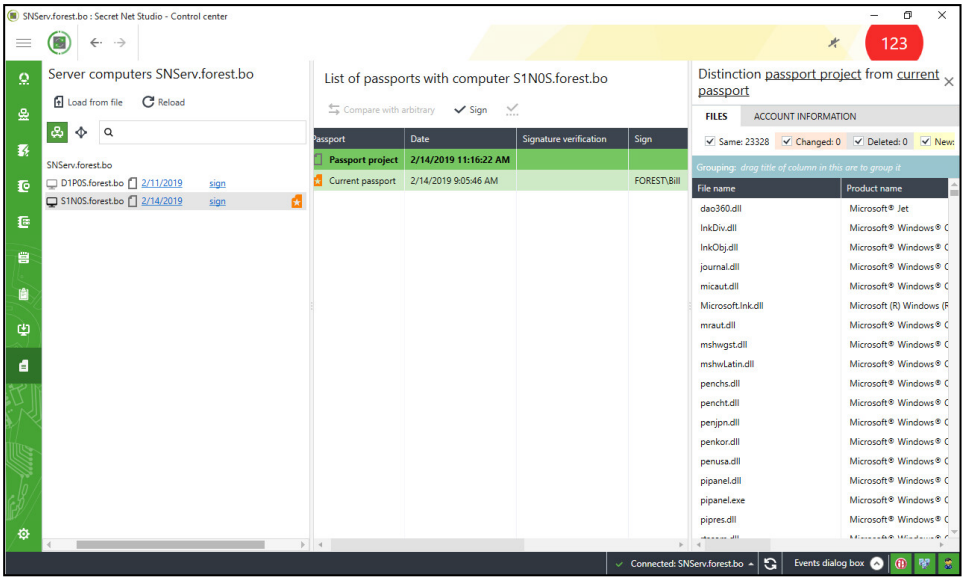
To compare the passports data:

1. In the list of passports, select the passports you need to compare. If you need to compare the nearest passports (for example, the passport project and the current approved passport), you can just select one that was created later (it is the **Passport** project in the figure below). To compare any two passports, select them in the list by pressing **Ctrl**.



2. Right-click the passport and select one of the following commands:
   - **Compare with previous** — to compare with the previous passport in the list;
   - **Compare with arbitrary** — to compare with another passport you selected.

   After the data is loaded, the results of comparison appear on the screen.



3. The **Files** tab contains information about files. A general summary of the comparison is displayed above the list. The summary contains information about a number of detected files: same ones, changed ones, deleted and new files. You can enable list filtration for each set of files. It makes the viewing more convenient by disabling a display of unnecessary elements (for example, the same files). To enable the filtration, clear the check boxes near the names of the respective buttons.

> **Note.** The list of files uses a coloring scheme that depends on the results of the comparison. Each element is highlighted by the color that is respective to the button in the **Summary** panel. For example, the **Same** files in the compared passports are displayed on a white background.

4. To manage the list of files, you can use grouping and sorting tools:
   - the grouping mode applies combined type of displaying a table and a list. It allows collapsing groups of elements. The configuration is performed in the **Grouping** field. To perform grouping of elements with same values of columns (for example, products' names or versions), consistently drag the titles of the columns and drop them in the grouping area. You can also move the titles within the area and change the sorting mode;
   - the sorting is performed as usual. To sort a table by the column's values, click the column's heading. For reverse sorting, click the heading once again.
5. If necessary, you can configure the contents of each column and their order in the table. Right-click the heading row, click **Column settings** and, in the appeared dialog box, configure the display settings.
6. Go to the **Account Information** tab. This tab contains a set of parameters of computers accounting information. The values saved in the compared passports are specified in separate columns.
7. After finishing the data analysis, you can clear the table using the **Close** button in the upper right corner.

Verification of the approved passport signature

To protect the approved passport from a forgery, there is a signature verification procedure. The procedure is performed using the Control Center. A user with the **View information** privilege has the right for the verification.

To verify the passport signature:

1. Load the cryptographic keys from your key container. The keys can be loaded either automatically during the logon using the security token or on the special

command **User Keys > Load keys** in the Secret Net Studio icon shortcut menu.

Note. For detailed information about loading and uploading cryptographic keys, see document [3]].

2. Launch the Control Center. On the left of the **Software Passport** panel, select the required computer. If necessary, use the search and filtration tools to find the computer faster.
3. Right-click the approved passport and click **Verify signature**. The program performs the signature verification and, when the process is finished, will display a result in the **Signature Verification** column.

Approving the passport project

The Software passport approval is performed using the Control Center. A user with the **The Software passport approval** privilege has the right for the operation.

To approve the passport project:

1. Load the cryptographic keys from your key container. The keys can be loaded either automatically during the logon using security token or on the special command **User Keys > Load keys** in the Secret Net Studio icon shortcut menu.

   Note. For detailed information about loading and uploading cryptographic keys, see document [3]

2. Run the Control Center. On the left of the **Software Passport** panel, select the required computer. If necessary, you can use the search and filtration tools to find the computer faster.
3. Right-click the passport project and click **Sign**. A dialog box asking you to confirm the operation appears.
4. In the dialog box, click **Sign**. After the operation is finished, the passport project becomes the current passport of the computer. The previous passport stays in the list as one of the earlier approved passports.

Backing up the passports

To upload and store the passports on the Security Server, there is a special file structure called the Software passports repository. The repository is located in the Security Server installation folder, the **\Passport** subfolder. If you need to create a backup copy of the passports, copy the contents of the **\Passports** subfolder to the required object.

Deleting the outdated passports

You can delete the outdated passports from the list except the approved one. In case if there are no backup copies of the passports repository, you cannot recover deleted passports.

The passports deleting procedure is performed in the Control Center. A user with the **Delete the Software passport** privilege has the right for the operation.

To remove one or several passports from the computer:

1. On the list of the passports, select those that you want to delete.
2. Right-click one of the selected passports, click **Remove** and, in the appeared dialog box, confirm the procedure.

Recovering the passports from backup copies

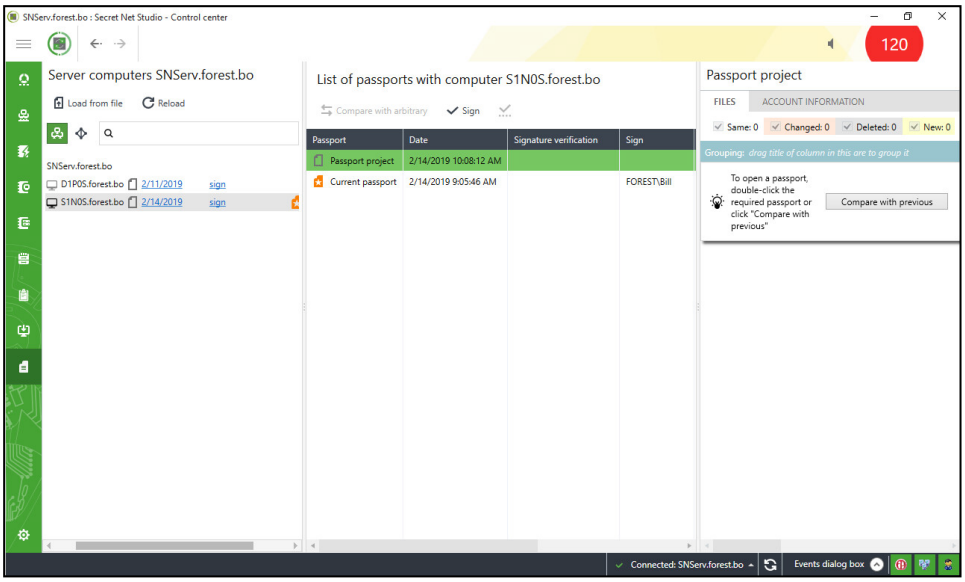
The Software passport repository on the Security Server can be complemented using backup copies. After doing so, you can download passports that were deleted as outdated to the Control Center.

The recovering procedure is performed on the Security Server and in the Control Center. A user with the **Synchronize the Software passports database** privilege has the right for the operation.

To recover the software passport from a backup copy:

1. On a workstation with the Security Server, copy backup files to the **\Passport** subfolder that is in the installation folder of the Security Server.

2. In the Control Center, go to the **Software Passport** panel, select the Security Server. To view security servers, click the **OM structure** button in the search and filtration area above the list of objects.



3. Right-click the selected Security Server and click **Synchronize database**.

Events registered in the Security Server log

The operations with the passports performed in the Control Center are registered in the **Security Server** log. The types of the registered events are as follows:

- signing a software passport;
- failed to sign a software passport;
- removing a software passport;
- failed to remove a software passport;
- uploading a software passport;
- failed to upload a software passport;
- synchronizing a software passport;
- failed to synchronize a software passport;
- Software Passport data collection was started;
- Software Passport data collection was finished;
- Software Passport data collection error;
- Software Passport data saved.

Chapter 8
Device Control

About device control

Secure device access is provided by device connection control mechanism and by device access control mechanism. The device connection control mechanism is designed for detecting and responding to computer hardware configuration changes, as well as for maintaining an up-to-date list of computer devices. The other mechanism is used to restrict user access to devices based on the device list. Some of the device access restrictions functions are implemented using the mandatory access control mechanism.

Device list

A hierarchical device list structure represents devices installed or connected to protected computers. The devices are combined in classes, while the classes are combined in groups. Groups represent the highest combination level. The number of groups is fixed. The following groups are available:

- **Local devices** — includes devices within a computer without any connection restrictions (for example, serial and parallel ports, processors, random access memory);
- **USB devices** — includes devices connected to a USB bus;
- **PCMCIA devices** — includes devices connected to a PCMCIA bus;
- **IEEE1394 devices** — includes devices connected to a IEEE1394 bus;
- **Secure Digital** — includes devices connected to a Secure Digital bus;
- **Network** — includes network interface devices. If a removable device is used as the network interface, this device can also be included in a different group. In this case, you can configure the system reaction to device connection before it is registered as the network interface.

Some classes can be additionally divided into models. Models represent devices with the same identification codes assigned by manufacturers (VID and PID). The device list includes predefined models, for example, models of electronic identifiers. You can also add models to the list based on available devices if the manufacturer specified identification codes in these devices. Later, when detecting a new device with the same identification codes, this device will be automatically added as an instance to the same model. This helps to manage devices with the same identification code without having to configure the parameters of each device individually.

Each object level (group, class, model, device) has its own set of parameters that are used to configure the following mechanisms: device connection and change, device control, shadow copying and mandatory access control. The device list hierarchy usually makes it possible to configure parameters on the level of each individual device as well as on the level of classes and groups.

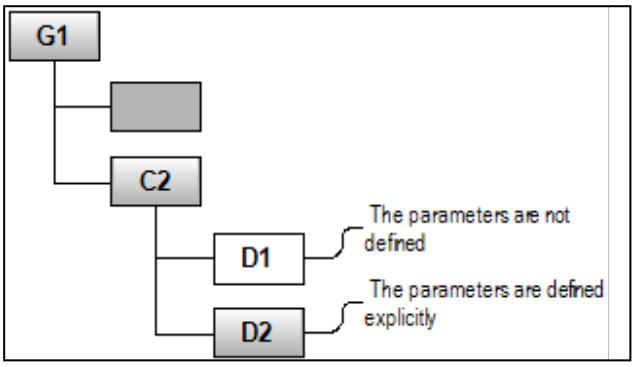
For a full list of groups and classes, capabilities of creating device models, see **Appendix** on p. **265**.

The device list is created on the computer immediately after the installation of the Client, when the operating system is run for the first time. This list of devices is considered the computer's reference hardware configuration. It is stored in the Secret Net Studio local database and is loaded in the local policy.

You can create a device list in the group policy to manage devices on computers where the Client is installed in the network operation mode. Once created, the device list includes groups, classes and predefined device models. If necessary, you can add specific devices to the list.

Inheritance rules for parameters in the device list

Access rights for each object and device control settings are defined in accordance with inheritance rules or explicit parameter settings as a part of group or local policy. Parameters can be configured for groups, classes, models or specific devices. When configuring the parameters, you can follow the principle of inheriting the parameters from higher- level elements of the list hierarchy. Explicitly configured parameters have higher priority over inherited parameters. For example, if specific access parameters are explicitly configured for a device, they will be applied regardless of which parameters are configured for a class and group.



In the figure above, the **D1** device inherits the parameters configured for the **C2** class. Explicitly configured parameters are applied to the **D2** device, which may differ from the parameters configured for the **C2** class.

Management options

Devices are managed using the Control Center, which can be installed as a separate Secret Net Studio component for operating in the centralized mode or as a part of the Client for operating in the local mode. For more details on how to use the Control Center, see document [**1**].

The following device management options are available:

- management using only the local policy of each computer;
- management using group policies for upper- level elements (device groups, classes and models) and the local policy of each computer for specific devices;
- management using group policies for all elements of the devices list.

Management options using group policies are not available if the Client is installed in the standalone mode.

Group policy parameters are edited on the security administrator's workstation using the Control Center in the centralized mode. Local policy parameters can be configured both in the centralized and local modes.

Group policy management options for the higher level elements

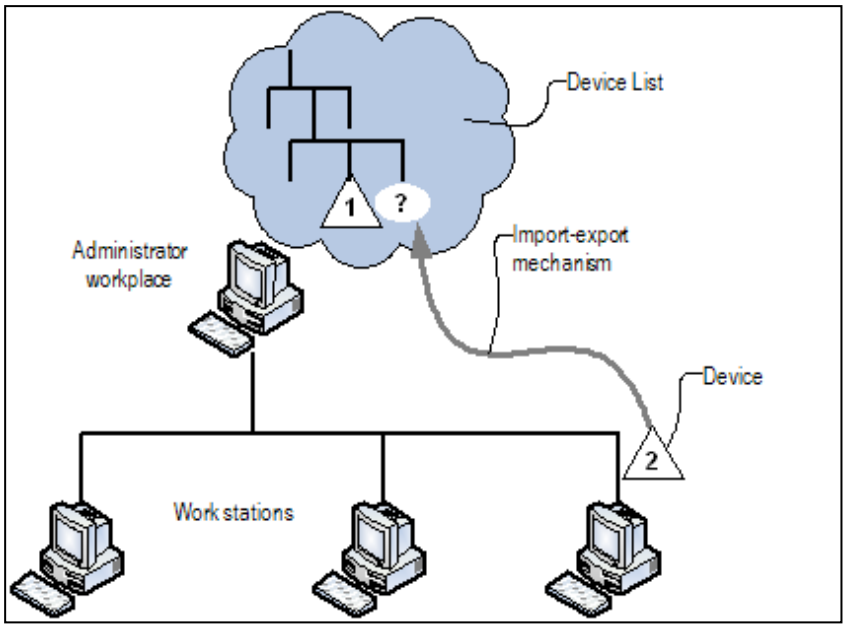
This option is preferable when you need to ensure general device control principles on protected computers and there is no need to configure individual devices in the centralized mode. The security administrator just has to configure usage parameters for device groups, classes and models in the required group policies, for example, in the organizational unit policy. Group policy takes priority over local policies set on each computer. Parameters for the use of specific devices are configured in the local policy of each computer.

Group policy management options for all elements of the devices list

If you need to apply the same parameters for using specific devices on several computers, you can configure them in the domain, organizational unit or the Security Server policies.

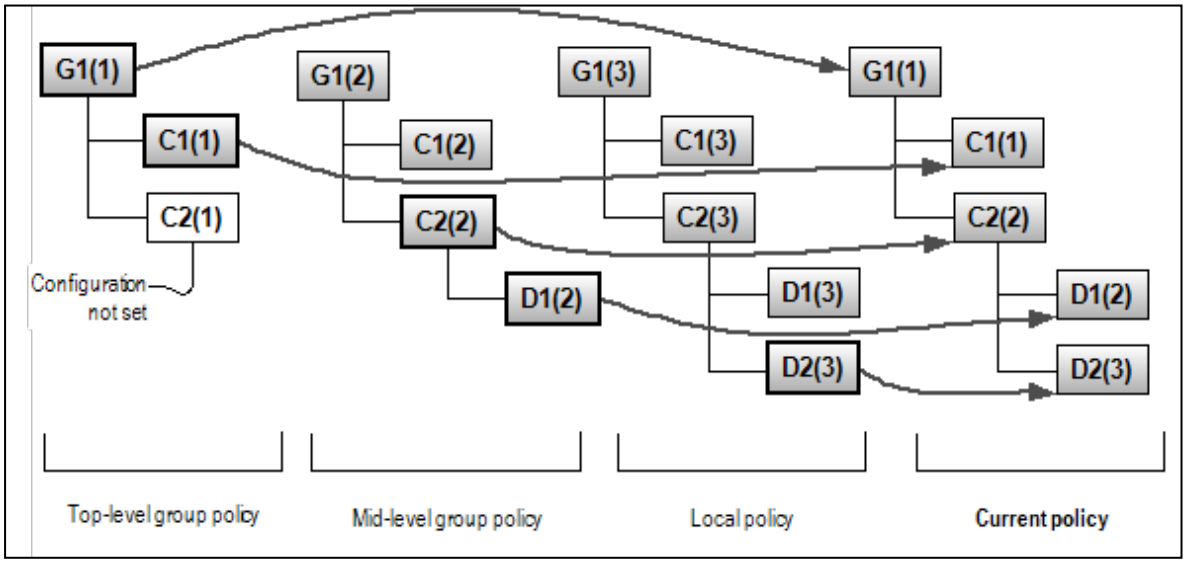
The devices that require configuring should be added to the group policy list. You can add information about devices that are connected to a computer with the Client to the device policy list.

For the description of available options for adding devices, see p. **74**.



Specific features of group policy application with device lists

When a user logs in, device control and access values are set in accordance with the current policy. The current policy is defined when the set group policy parameters are applied according to their priority. Local policy parameters have the lowest priority. They take effect only if parameters are not defined in the group policies of other levels (in the policies of domains, organizational units and the Security Servers). The group policy of the root Security Server has the highest priority. The figure below shows an example of group policy parameter application for groups (**G**), classes (**C**) and devices (**D**):



Default device parameters

Once Secret Net Studio is installed, the following device usage rules are configured in the local policy and applied to all users of the computer:

- The **Device is always connected to the computer** control mode is enabled for the **Local devices** and **Network** groups. **Device connection is allowed** is set for other groups.
- The **Device is always connected to computer** control mode with the additional **Lock computer if device is changed** parameter is set for all detected hard drives as well as for removable and optical disks. At the same time, the **Device connection is allowed** mode is enabled for the classes to which such devices belong to.
- Devices that support access isolation are granted full access to three standard groups of users: **System**, **Administrators** and **All**.
- **Shadow Copying** is disabled for all devices.
- **Device is available without regard to confidentiality categories** access mode is set for devices supporting confidentiality category assignment.
- For network interfaces operation is allowed regardless of session confidentiality in the flow control mode (**Mandatory Access Control**).
- All **Hardware control** and **Device control** category events are logged.
- Local devices and resources can be used in terminal sessions.

General configuration procedure for using only allowed devices

Devices connected to a computer are configured directly on the protected computer via the local management tools.

Attention! Before starting the configuration, you must enable the **Device connection** and **Deny device connection** event registration from the **Device control** category. Analyzing these events allows you to detect composite devices (see p. 72). After you install the security system, the registration of these events is enabled by default.

To establish a connection and operation only for allowed devices on a computer, take the following steps for each device:

1. Connect a device.

   The device is registered in the security system and is assigned access permissions and control parameters from the parent objects (models, classes, groups) that the device is related to.

2. Analyze the log's entries to determine if the device is a composite one.

   To do so, in the Control Center, go to the **Logs** panel and open Secret Net Studio log with the **Device control** filtering parameters and the respective time.

   If the device is composite, the entries have several records of the **Device connection** and **Deny device connection** event registration. Save information about the registration methods for this device. The name, class and group of the device can be found in the log records.

3. Configure the device profile for the current hardware configuration:
   - control policy (see p. 80);
   - user access control (see p. 81);
   - shadow copying (see p. 39);
   - mandatory access control (see p. 142 and p. 145).

   Attention! A composite device requires a configuration of all methods of its display in the list of devices according to the recommendations provided in the **Operational features of the composite devices** paragraph.

4. To limit the use of devices in the terminal connections, enable redirection control (see p. 31).
5. Disable parameters' inheritance for the specific devices from the parent objects in the list and disable the permissions for the respective models, classes and groups (see p. 80). For example, you can disable the permissions for the **Secure Digital** device groups.

6. Repeat steps **1**–**5** for all the required devices.

As a result, the user will only be able to connect and use allowed devices, whereas other devices will not be available. Later, you will be able to remotely allow using new devices via the Control Center. For this purpose, upon user request, the security administrator offers to connect the required device (for example, a USB flash drive) to the user's computer. Once the device is connected, even if it is not allowed to be used, information about it will appear in the list of local policy devices. To allow using the device, you must open local policy settings and perform the required steps.

Note. Specific instructions for removable drives' profile configuration can be found in the **Appendix** on p. 267.

Features of composite devices

Some devices can be identified as composite when connected. To configure a composite device, perform the configuration of the same type for each representation of the device in the list.

Note. Such devices are detected by analyzing Secret Net Studio log entries for the **Device connection** and **Deny device connection** events from the **Device control** category registered at the moment of their connection to a computer.

For example, let us take a look at an operation with MMC/SD cards. Most of the cards are identified as devices of the **Secure Digital** group. To control access to SD cards, the parameters of the device control, privileges and shadow copying must be configured for the **Secure Digital** group, the **Memory card** class or a specific device that requires access configuration.

Some computers also identify the MMC/SD cards as removable drives. Thus, they appear in the list as devices of the **Removable storage** class, the **Local devices** group and the **Secure Digital** group. In this case, you must assign the same parameters of the device control, privileges and shadow copying parameters to both devices added to the list.

When you connect the SD card using the USB Card Reader, MMC/SD cards may not appear as devices of the **Secure Digital devices** group, but only as the connected USB Card Reader device of the **Storage devices** class, the **USB devices** group. In this case, to control access to SD card, the parameters of the device control, privileges and shadow copying must be configured via the USB Card Reader device of the **Storage devices** class, the **USB devices** group.

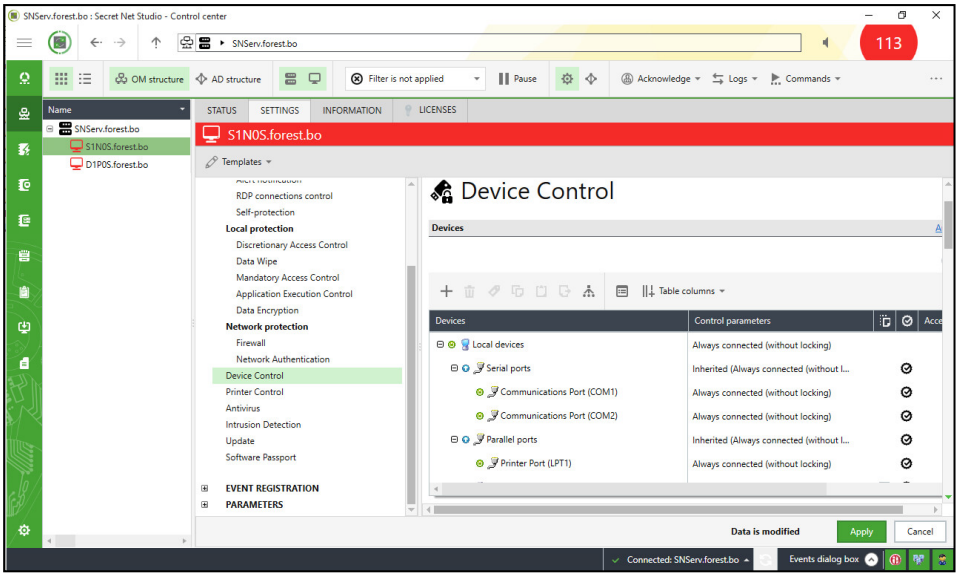
Device list management

Loading a device list

To load a device list:

1. In the Control Center, click the **Computers** panel and select the object you want to configure. Double-click the selected object to open its **Properties** menu. In the **Properties** menu, select the **Settings** tab and click **Load Settings**.
2. In the **Policies** section, select the **Device Control** settings group.

   An example of a list is shown in the figure below.



All detected devices are automatically added to the device list in the local policy. In addition, this list also includes information about devices connected to the computer's terminal clients during terminal sessions (as long as these devices are allowed for usage). Currently connected devices are displayed as normal, while the names of disconnected devices are crossed out.

The device element list has a certain parameter configuration that ensures the correct operation of all the required devices in terms of the management logic in Secret Net Studio. Parameter configuration varies for different list elements and depends on whether the devices belong to certain groups, classes as well as on specific features of the device use. Special status icons are provided to conveniently view the device list and quickly obtain basic information about the current parameter configuration. These icons are listed in the following table:

Icon	Description
	Control parameters for devices are inherited from a higher-level element of the device list
(gray)	Control mode is disabled for the device
	Control mode is enabled for the device and the device should always remain connected to the computer
(green)	Control mode is enabled for the device and the device can be connected to or disconnected from the computer
(red)	Control mode is enabled for the device, and the device cannot be connected to the computer

Management commands

The main commands to work with the list of devices and ways to run the commands are provided in the table below. Other commands are described in the instructions.

Command	Button	Keys	Can be run from the shortcut menu
Add a device		**Ctrl+N**	Yes
Delete the device		**Del**	Yes
Add a model for a device		**Ctrl+M**	Yes

Command	Button	Keys	Can be run from the shortcut menu
Save (export)		**Ctrl+S**	Yes
Show device information		—	No
Open up the list		**Right arrow**	No
Collapse the list		**Left arrow**	No
Open up everything		—	No
Collapse everything		—	No

Creating a device list in a group policy

During Secret Net Studio installation, the list of devices is created individually for each computer within the local policy. You can use group policies of domains, organizational units and the Security Servers for centralized management of device lists.

By default, group policies do not contain any device lists. Therefore, to implement centralized management, you need to create a device list in the respective group policy. Group policy is configured using the Control Center (see document [**1**]).

Adding and removing device list elements

You can add information about specific devices in the group policy list. It allows you to configure device parameters centrally or locally if the device has not been connected to your computer earlier or is not on the list.

This chapter contains the following instructions:

- adding device model (see below);
- adding devices using the import wizard (see p. **75**), including:
  - adding devices using their identifiers (see p. **76**);
  - adding devices from a **.csv** file and creating it manually (see p. **78**);
  - exporting information about devices from the device list (see p. **79**);
- adding devices using the clipboard (see p. **80**);
- removing devices (p. **80**);
- removing devices from the list (see p. **80**).

Attention! When adding a device, its preset control and access parameters are copied. However, if the previous values cannot be assigned for technical reasons, the parameters can be set by default. Once you added the device, make sure to check its parameters and edit them if necessary.

Adding device model

Adding the device model allows you to control devices of the same model without having to configure parameters separately for each of them.

You can add model of the added devices if their identification codes (VID and PID) have been included by the manufacturer.

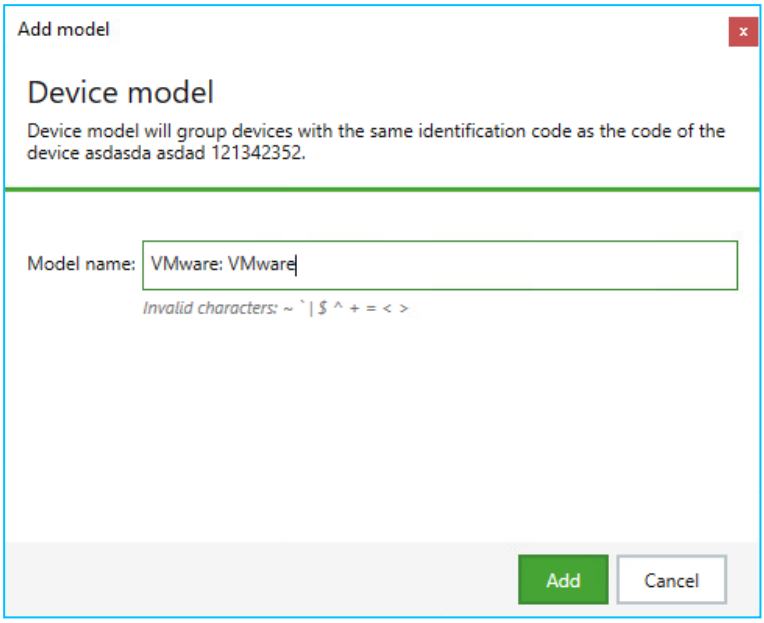
When a model is added, it inherits all the settings of the superior object: the device class. You can edit these settings later.

Note. Models are preset for some device classes (see p. **265**).

To add a model:

1. Select a device with identification codes (VID and PID) and run the **Add model for the device** command.

   The opening dialog box of the wizard for adding models appears.



2. Specify the name of the model and click **Add**.

   A new model is added to the group policy list.

3. Click **Apply**.

Using the device import wizard

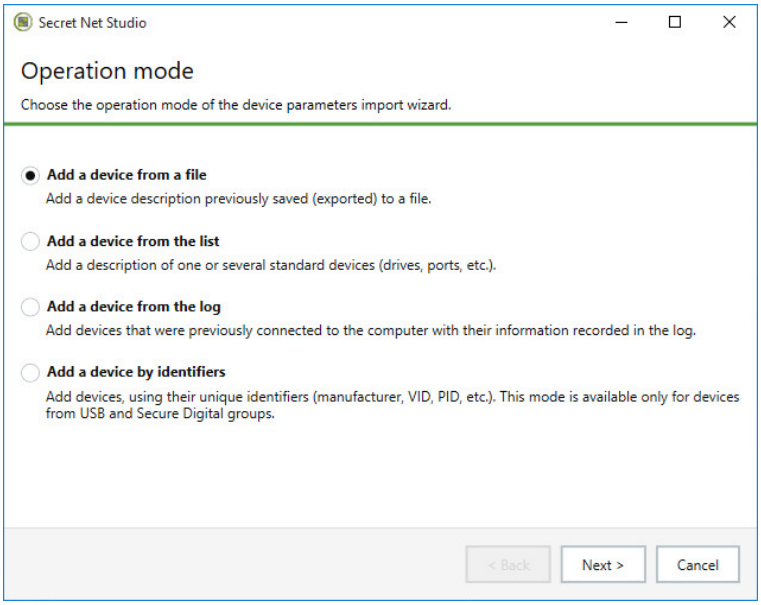
The device import wizard provides the following:

- importing a device from the file where information about the device is saved (exported);
- adding a standard device from a predefined list (for example, input/output port);
- adding a device previously registered in the Secret Net Studio log;
- adding a device by parameters.

To import a device to the group policy list:

1. Click **Add device**.

   The opening dialog box of the device import wizard appears as in the figure below.



2. Select an option, click **Next** and follow the wizard instructions.

The procedure of adding devices using their identifiers is described below.

Adding devices using their identifiers

Adding devices using their identifiers allows you to register devices in the DC policy and facilitates the following:

- creating a list of devices without connecting them to the computer;
- registering a lot of single model devices simultaneously.

The mode is supported only for the **USB** and the **Secure Digital** device groups.

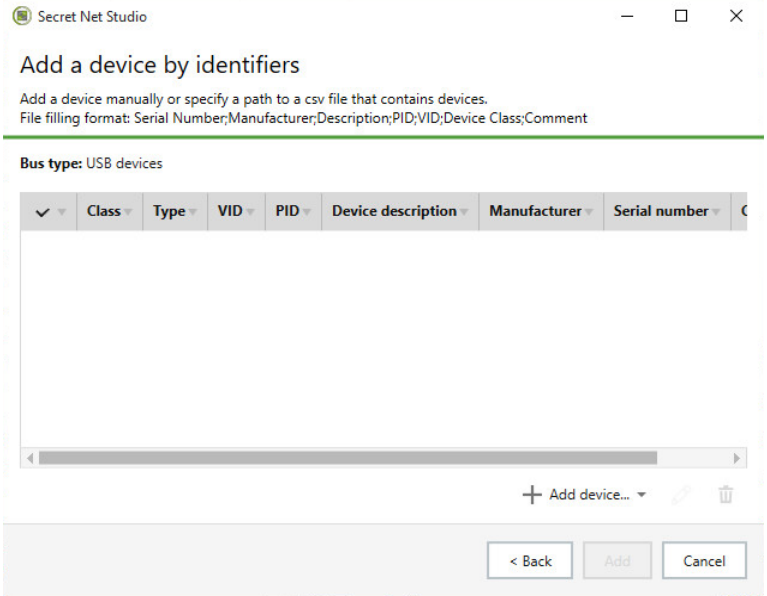
To add a device to the group policy list:

1. Select the **USB devices** group, the **Secure Digital** group or an object from one of the groups, then click **Add device**.

   The opening dialog box of the device import wizard appears.

2. Select **Add devices using their identifiers** and click **Next**.

   The dialog box for adding devices using their identifiers appears.



Note. The **Status** parameter can have one of the following values:

- **Device is ready to be added** – all device parameters matching the predefined values have been entered;
- **Device is ready to be added but its parameters do not match the predefined values** – all device parameters have been entered, but some of them do not match the predefined values;
- **Device is not ready to be added** – some of the device parameters have been entered.

The **Status** column is sorted in a standard way. To sort a table, click on its heading. To sort backwards, click on the heading again.

3. Create a device import list by adding devices manually or from a .csv file (the procedure of adding devices is described below).

   All added devices are on the list where you can edit or remove a selected device by clicking **Edit** or **Remove** respectively.

4. Click **Add**.

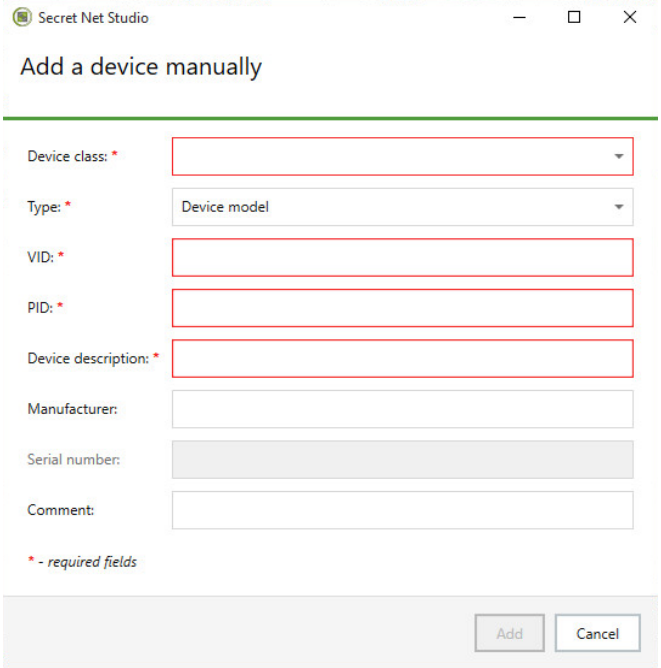
   New objects are added to the device group policy list.

5. Click **Apply**.

To add devices manually:

1. Click **Add device manually** (new devices are added manually by entering their parameters).

   The dialog box for adding device manually appears as in the figure below.



Note. Fields in red must be filled out.

2. Enter device parameters:

Parameter	Description
Device class	Contains the name of the device class. Select the device class from the drop-down list. **Secure Digital** device group includes the **Memory cards** device class. **USB** device group includes several device classes, each with its own identifier (see the table below)
Type	Contains the device type name. Select the device type from the drop-down list
VID	Contains the device manufacturer ID
PID	Contains the device model ID
Device description	Contains information about the device

Parameter	Description
Manufacturer	Contains the name of the manufacturing company
Serial number	Contains the unique identification number of the device
Comment	Contains additional information about the device

List of device class identifiers for the USB group.

ID	Device class
1002	Network adapters and modems
1003	HID devices (mouse, keyboard, UPS, etc.)
1006	Scanners and digital cameras
1007	Printers
1008	Storage devices
1256	Bluetooth adapters
1257	Mobile phones (smartphones, PDAs)
1258	Security tokens and smartcard readers
1299	Others

Note. The number of available parameters depends on the device class.

3. Click **Add**.

   The dialog box for adding devices by identifiers appears.

Adding devices from file

Devices are added by means of the .csv file which has been created earlier and contains device parameters. The procedure of the file creation is described below.

To add a device from a file:

1. Click **Add devices from file**.

   The dialog box for selecting a **.csv** file appears.

2. Specify the file name in the **File name** field and click **Open**.

   New list items containing information about the parameters of added devices appear in the dialog box for adding devices. The **Status** parameter is defined for each added device. The **Device is ready to be added** status means that all the device parameters are correct and the device is ready to be added to the group policy list. If the **Status** parameter has any other value, it means that the device parameters are not correct and the device is not ready to be added to the group policy list. To change the device status, select the required list item and configure its settings by clicking **Edit**.

   Note. If the class of the device does not match the class of the device group object, the respective warning appears. The new list item does not appear in the dialog box of the device import wizard.

3. Click **Add**.

   The dialog box for adding devices using their identifiers appears.

Creating a file containing device parameters

The file containing device parameters allows to make information adding fully automatic. Created in .csv format, it is a representation file containing parameters of the device being connected. The file is created manually.

Tip. You can use the file **\Tools\SecurityCode\SnDeviceAd\SnDeviceAd.csx** from the installation disk as a template or use the sample file below.

To create a file manually:

- Create the file **SnDeviceAD.csv** in a text editor, form its contents and save it.

File structure

The file has the following structure:

Serial Number;Manufacturer;Description;PID;VID;Device Class;Comment parameter_ value_ 1;parameter_ value_ 2;parameter_ value_ 3;parameter_ value_ 4;parameter_value_5;parameter_value_6;parameter_value_7
...
parameter_ value_ A;parameter_ value_ B;parameter_ value_ C;parameter_ value_ D;parameter_value_E;parameter_value_F;parameter_value_G

The example of the contents is given below.

Serial Number;Manufacturer;Description;PID;VID;Device Class;Comment

;HP;HP LaserJet A4;0517;03f0;1007;Printer for print A4

1704HS03V1E8;Microsoft;Mouse;C077;046D;1003;Wired mouse

ZKY4VDHF;Transcend;USB;1000;8564;1008;USB for users

The example contains the following information:

For the first device — the printer.

1. Serial number is not specified for the printer.
2. Manufacturer: HP.
3. Device description: HP LaserJet A4.
4. ID of the device model: 0517.
5. ID of the device manufacturer: 03f0.
6. Device class: Printers.
7. Comment: Printer for print A4.

For the second device — the mouse.

1. Serial number: 1704HS03V1E8.
2. Manufacturer: Microsoft.
3. Device description: Mouse.
4. ID of the device model: C077.
5. ID of the device manufacturer: 046D.
6. Device class: HID devices (mouse, keyboard, etc.).
7. Comment: Wired mouse.

For the third device — USB drive.

1. Serial number: ZKY4VDHF.
2. Manufacturer: Transcend.
3. Device description: USB.
4. ID of the device model: 1000.
5. ID of the device manufacturer: 8564.
6. Device class: Storage devices.
7. Comment: USB for users.

Exporting about devices from the device list

You can export information about devices in the group policy list to files. The information is exported to device description files for Secret Net Studio(***.sndev**). Later you can import the file contents using the import wizard (see above).

Note. Exporting to the **.sndev** file format is supported only for devices and models.

To export information:

1. Click **Save**.

   The standard dialog box for saving Windows files appears.
2. Specify the name of the file to save the information.

Adding devices using the clipboard

Device information can be copied to the clipboard from the device list of another policy. The methods of using the clipboard for device copying and adding are standard.

Removing models

Contrary to the class, the model can be removed from the list. When removing a model, the device samples it contains become subordinate to the device class.

Note. Removing all the device samples do not imply removing the device model.

To remove a model:

1. Select a model from the list and click **Remove**.
2. Click **Apply**.

Removing devices

To remove a device from the group policy list, click **Remove**.

Note. To select several devices of the same type (at the third nested level) press and hold the <Ctrl> key.

Control of device connections and changes

Configuring a device control policy

A device control policy can be configured:

- individually for each device;
- for a model, class or group of devices using parameter inheritance.

Control parameters set by the local policy are applied by default on computers. For the computers with the Client installed in the network operation mode, you can configure a device control policy in the group policies (see p. **74**).

To configure a device control policy:

1. Load the device list (see p. **72**).
2. Select the line with the required element (group, class, model, device).

   Note. To select several devices of the same type (at the third nested level) press and hold the **<Ctrl>** key.

3. If necessary, enter additional information about the element in the cell of the **Commentary** column. To do so, click the button in the right part of the cell.

   Note. By default, the **Commentary** column is not displayed. Click **Table columns** above the device list to enable its display. Additional information about devices is saved in the log when registering events related to a certain device.

4. Specify the required parameters in the cell of the **Control parameters** column. To do so, click the button in the right part of the cell. If you need to disable parameter inheritance from a higher-level object and explicitly assign a control policy, clear the **Inherit control settings from parent object** check box and configure the control parameters.

Device is not controlled
Click this option button to disable control mode for the selected object
Device is always connected to the computer

Click this option button to enable the control mode that demands the device to always be connected to the computer. If the device state changes, a corresponding alert will be logged as an unauthorized access attempt and the system will be expecting the security administrator to approve hardware changes. To increase protection you can select **Lock computer if device is changed**. That way the computer will be locked every time the device's state changes. Only a security administrator will be able to unlock the computer
Device connection is allowed
Click this option button to enable the control mode that allows to connect and disconnect the device. If the device state changes, the corresponding events are logged. Hardware change approval is not required in this case. This parameter is only available for devices where the connection process is monitored and which can be locked
Device connection is not allowed
Click this option button to enable the control mode that prohibits to connect the device to the computer. Device connection attempts are registered in the log as alerts. This parameter is only available for devices where the connection process is monitored and which can be locked

5. Click **Apply** at the bottom of the **Settings** tab.

Confirming hardware configuration

Hardware configuration changes are monitored by Secret Net Studio for devices with the **Device is always connected to the computer** control mode enabled. When changes are detected, event alerts are logged. When the **Lock computer if device is changed** mode is also enabled, the computer is locked. Only the administrator can unlock the computer and confirm hardware changes.

Hardware changes are confirmed in the Control Center. Description of the procedure can be found in document [**1**].

Selective discretionary access control

The following operations are performed to configure user access to devices:

1. Configuring user access rights for devices.
2. Configuring event logging and audit of device operations (see p. **82**).

Configuring access rights for devices

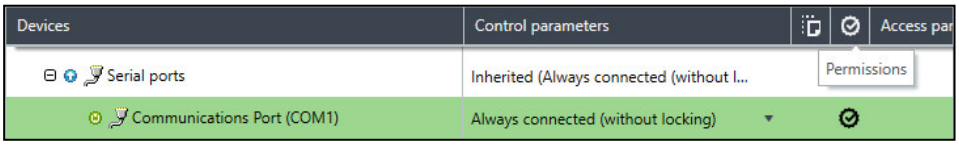
User access rights can be assigned for individual devices or classes.

To configure access rights for devices:

1. Load the device list (see p. **72**).
2. Select the line with the required list element (class or device).

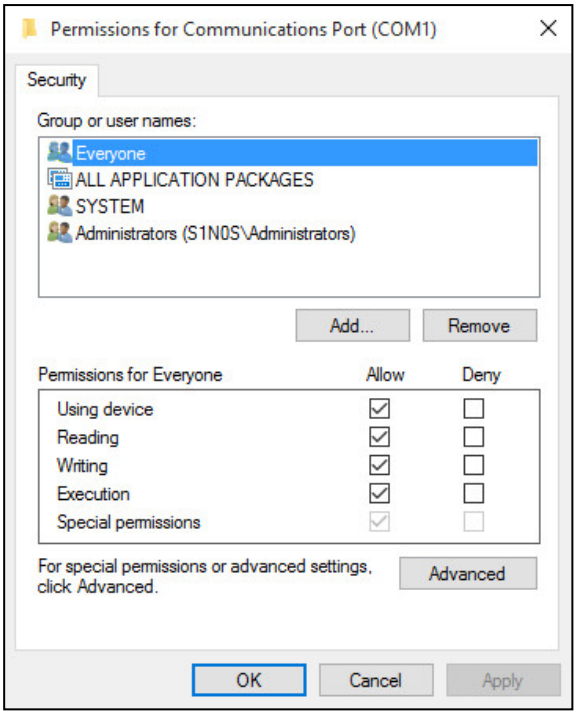
Note. To select several devices of the same type (at the third nested level) press and hold the **Ctrl** key.

3. Click the button in the cell of the **Permissions** column.



The **Permissions** dialog box appears.

Note that the **Permissions** dialog box can only be opened for devices available for permission configuration: ports, disks, removable media (you cannot change permissions for the system disk).



4. If necessary, edit the list of accounts in the upper section of the dialog box.
5. To modify access parameters, select the required account in the list and assign permissions and prohibitions for performing operations. Take into account the parameter inheritance principle: explicitly defined parameters take priority over those inherited from parent objects.

   To configure additional permissions, click **Advanced** and configure settings.
6. After closing the **Permissions** dialog box, click **Apply**.

Configuring event logging and audit of device operations

Changing the list of logged events

The event registration log must be configured in order to keep track of events related to the device access mechanism. The configuration is performed using the Control Center. You can enable and disable event logging on the **Settings** tab of the object properties panel, in the **Event Registration** section, **Device Control** group. To go to the required group of registration settings from the respective group of parameters in the **Policies** section (see p. 72), click the **Audit** link in the right part of the **Settings** group or **Devices** group heading.

Configuring success and failure audit

You can configure the audit of device operations for classes and for certain devices.

To configure the audit:

1. Load the device list (see p. 72).
2. Select the line with the required list element (class or device).

   Note. To select several devices of the same type (at the third nested level) press and hold the **Ctrl** key.
3. Click the button in the cell of the **Permissions** column.

   The **Permissions** dialog box appears.
4. Click **Advanced**.

   A dialog box for configuring additional parameters appears.
5. Go to the **Audit** dialog box and configure Windows audit parameters.
6. After closing the **Permissions** dialog box, click **Apply**.

Chapter 9
Print Control

About restricting access to printers

Printer list

Printer use parameters are configured in a separate **Printers** list. Parameters can be applied by default when printing using any printer or can be configured for specific printers.

Printing devices included in the printer list can also be included in the device list as devices. In this case, you can configure system reaction to connecting the device before it is registered as a printer.

The printer list is created on the computer immediately after installing the Client. This list is in the local policy and stored in the Secret Net Studio local database.

You can create a printer list in the group policy to manage printers on computers with the Client installed in the network operation mode.

Management options

Printers are managed using the Control Center, which can be installed as a separate component of Secret Net Studio for operating in the centralized mode, or as a part of the Client for operating in the local mode. For details on how to use the Control Center, see document [**1**].

There are three primary options that you can use to configure printer parameters:

- local policy management of each computer;
- group policy management of most parameters and local policy management for specific computers;
- group policy management of most parameters and local policy management for specific printers.

Group policy options are not available for computers with the Client installed in standalone mode.

Group policy parameters are configured on the security administrator's computer using the Control Center in the centralized mode. Local policy parameters can be configured both centrally and locally.

Group policy management of common default parameters

This option is preferable when you need to set the same printer management parameters on protected computers and there is no need to configure individual devices centrally. The security administrator just has to configure usage parameters for the **Default settings** element in the required group policies, for example, in the organizational branch policy. Group policy parameters will be applied on computers regardless of which parameters are configured for this element in the local policy of each computer. Parameters for the use of specific printers are configured in the local policy of each computer.

Group policy management of common default parameters and for specific printers

If you need to apply the same parameters for using specific printers on several computers, you can configure them in the domain, organizational unit or Security Server policies.

To configure printer settings, you should first include it in the printer list of a group policy. You can add any available printer to the printer list.

See p. **85** for a description of available options for adding printers.

Initial printer use parameters

A freshly installed security system contains the following default printer use rules are set in the local policy:

- Standard user groups have access to printers: **System** , **All** and **All Application Packages**.
- **Shadow Copying** is disabled.
- Printers can be used to print documents of any confidentiality category.
- Local printers can be used in terminal sessions.

General configuration procedure for printing only on allowed printers

To ensure that documents are printed on the printers allowed on a certain computer, perform the configuration in the following order:

1. Once Secret Net Studio is installed, open the list of the operating system printers and make sure all printers intended to be used are in the list. If some printers are not in the list, install these printers (add them to the OS printer list) as recommended by their manufacturers.

   Note. You can connect to the same printer differently. For example, if a printer (physical device) is installed locally or as a network printer with an IP address. To control access to printers that will be connected using different methods, install each printer (add them to the operating system list) for each connection method. This will ensure that these printers will be correctly identified by the security system.

2. Add these printers to the group policy list.
3. Configure the parameters for using printers:
   - user access control (see p. **86**);
   - shadow copying (see p. **39**);
   - mandatory access control (see p. **143**).
4. To restrict the use of printers in terminal connections, disable redirection (see p. **31**).
5. In the printer list, prohibit printing for all users for the **Default settings** element and enable printing restrictions for all document confidentiality categories.

As a result, the user will be able to print documents only on allowed devices, while other printers will not be available for use. When you need to allow a new printer to be used for printing (or the same printer connected in a different manner), the administrator can install it themselves, add it to the required policy list and configure its usage parameters.

Printer list management

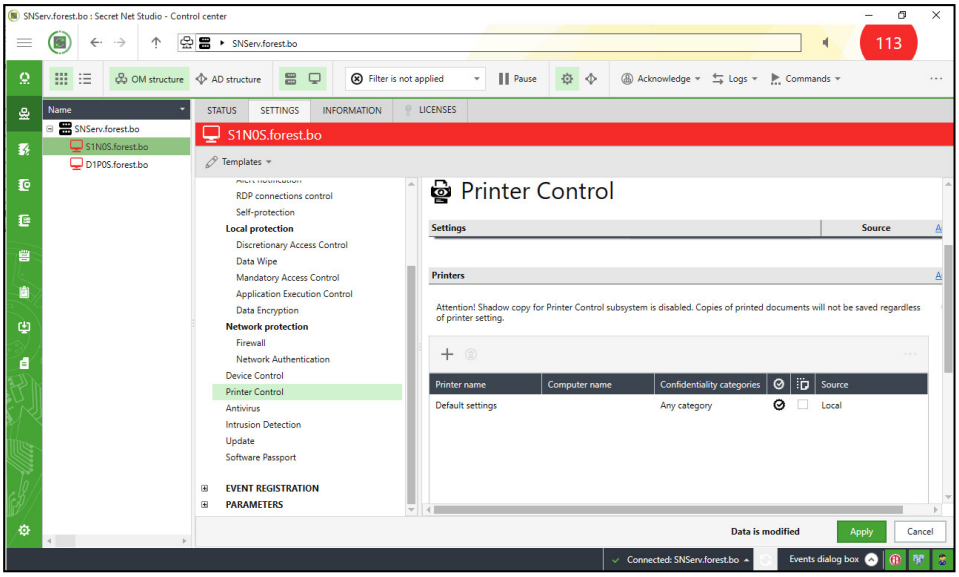
Loading a printer list

This section describes the centralized procedure for loading a printer list via the Control Center. Printers are loaded locally in the same way via the Local Control Center. See information about how to use the Control Center in document [**1**].

To load a printer list:

1. In the Control Center, open the **Computers** panel and select the object you want to configure. Right-click the object and click **Properties**. In the properties panel, select the **Settings** tab and click **Load Settings**.
2. In the **Policies** section, select the **Print Control** / **Printers group**.

   An example of a list is shown in the figure below.



The initial printer list contains one **Default settings** element. Printer parameters defined for this element are applied to all printers, except those that are explicitly present in the printer list. You can add printers to the policy list using a special wizard. Explicitly defined parameters for specific printers have higher priority over the parameters of the **Default settings** element.

Creating a printer list in a group policy

You can use group policies of domains, organizational units and Security Servers for centralized management of printer parameters.

By default, group policies do not contain any printer lists. To implement centralized management, you need to create a printer list in the respective group policy. Group policy is configured using the Control Center (see document [**1**]).

Adding and removing elements

You can add elements to the printer list corresponding to specific printers. A special wizard is used for adding elements.

Using the adding wizard

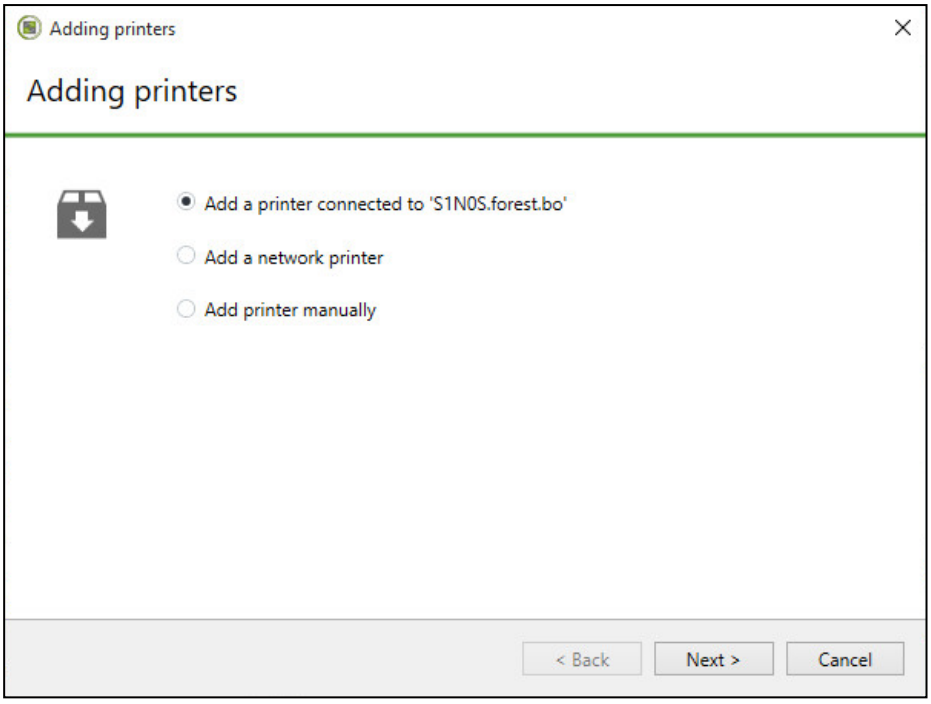
The adding wizard provides the following options:

- adding a printer connected to a selected computer;
- adding a network printer;
- adding a printer manually.

To add a printer to the group policy list:

1. Right-click any element in the printer list and click **Add printer**.

The add printer wizard's dialog box appears as in the figure below.



2. Select a desired option, then click **Next** and follow the wizard instructions.

Removing printers

If you need to remove a printer from the group policy list, right-click the printer and click **Delete**.

Selective printer access control

When configuring printer access control, the following operations are performed:

1. Configuring user print permissions.
2. Configuring event registration.

Configuring user print permissions

User print permissions may be configured for certain printers or for the **Default settings** element.

To configure user print permissions:

1. Load the printer list (see p. **83**).
2. Select the required element in the list.
3. Click the cell of the **Permissions** column.

The **Permissions** dialog box appears.

4. If necessary, edit the list of accounts in the upper section of the dialog box.
5. To modify access parameters, select the required account in the list and assign permissions or prohibitions for printing.

Configuring event registration

The event registration must be configured in order to keep track of events occurring in relation to the Print Control mechanism. The configuration is performed using the Control Center. You can find the events on the **Settings** tab of the object properties

panel, in the **Event Registration** section, **Print Control** group. To go to the required group of registration settings from the respective group of parameters in the **Policies** section (see p. **84**), click the **Audit** link in the right part of the **Settings** or **Printers** group heading.

Configuring printed document marking

When the marking mode is enabled, special markers (labels) containing user account data for printing are automatically added to documents during the printing process. A marker is a specific form containing some information and is usually located in the headers/footers or margins of the page. This is usually information about the printed document (for example, when it was printed, by whom, page count). The marker is a set of templates representing layouts for certain pages of the document: the first page, the last page, intermediary pages, etc. The templates define the areas for placing the information attributes.

When printing a document, page layouts from respective templates overlap document pages and, as a result, the marker-related information is printed with the document contents on the printed sheets. This information is printed out, regardless of the position of the document text on the sheet. An example of a printed page with a marker in the header is shown in the figure below.

Markers can be used when printing documents with any confidentiality category, including non-confidential documents. You can also use several markers for each category, enabling the user to select the required marker from the available options.

By default, the security system uses a set of markers with predefined templates and attributes. If necessary, you can configure marking in accordance with the document layout requirements used in your organization. To configure marking,

you can modify the parameters of existing objects (markers, templates, attributes, confidentiality category) and add new objects.

Marking mode management

Parameters determining the operation of the document marking mode are presented in the lists of group policy objects.

Attention! The same marker use parameters must be applied on computers included in the same security domain. We recommend configuring these parameters in a single common group policy.

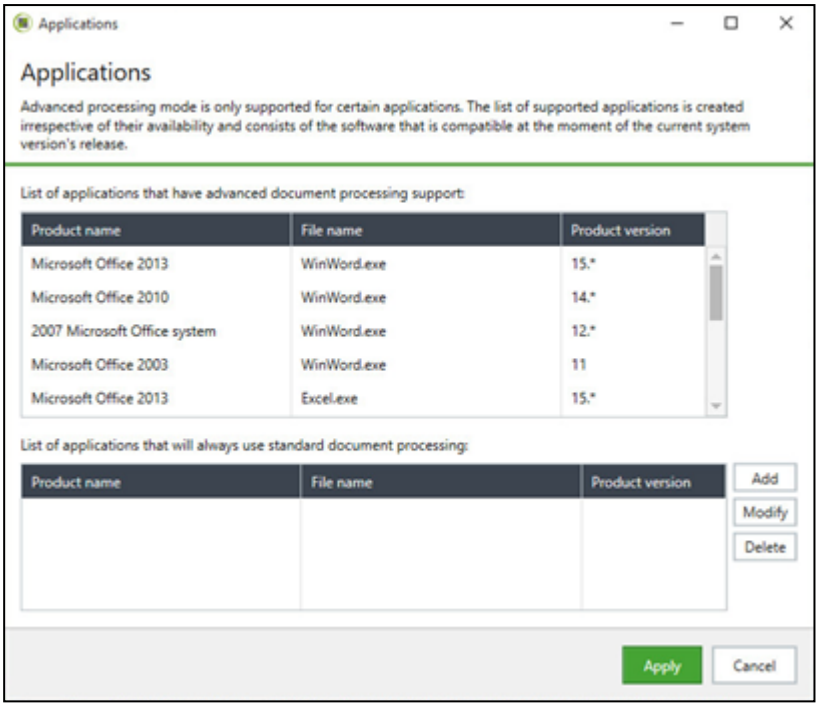
The centralized configuration procedure is described below. Local configuration is performed in the same way via the Local Control Center. See information about how to use the Control Center in document [**1**].

To enable and configure the marking mode:

1. In the Control Center, open the **Computers** panel and select the object you want to configure. Right-click the object and click **Properties**. In the properties menu, select the **Settings** tab and click **Load Settings**.
2. In the **Policies** section, go to **Print Control** > **Settings**.
3. Select the required value for the **Document marking** function:
   - **Standard processing** — this mode can be used in all supported applications. This mode is more suitable for printing whole documents. When printing a document fragment, the marker will only contain information about printed pages, without taking into account the total number of document pages (since the printed fragment is considered an individual document). The Secret Net Studio log records the document print start events and the document print finish events. When shadow copying is enabled, a copy of the printed fragment (not the whole document) is saved in the storage.
   - **Advanced processing** — in this mode printing is only available for compatible applications (see below). When sending to print, the entire document is processed regardless of the printed fragment size. Therefore, when part of a document is printed, pages are counted and numbered taking into account the total number of pages in the document. Print start and print finish events are registered in the Secret Net Studio log, start print and finish print events are also logged for each copy of the document.

   Note. If the marking mode is disabled, print events are registered in the Secret Net Studio log regardless of the state of the group policy parameter that defines the behavior of the shadow copying function for all printers. If the **Shadow copying** parameter is set to **Defined by printer settings**, start print and finish print events are logged. When the current value is **Disabled for all printers**, only **Print document** events are logged.
4. Configure the parameters for using markers. To do so, click **Edit** and configure the parameters in the marker edit program window (for the description of the interface and the general procedures for using the program, see p. **90**). If you need to restore default marking parameters, click the **Default** button.
5. If the **Standard processing** mode is selected, complete the procedure by clicking **Apply**.
6. If the **Advanced processing** mode is selected, check the list of compatible applications and, if necessary, specify the programs where the standard processing mode should be applied. To do so, use the **Applications included in advanced processing** link.

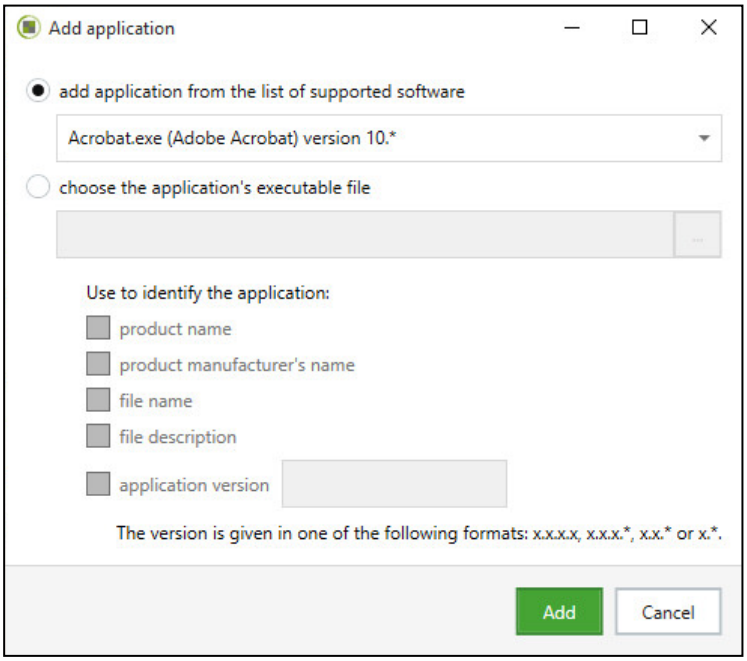
   A dialog box with the list of applications appears.



7. View the list of compatible applications. This list is created automatically, regardless of whether the applications are installed and includes programs compatible with the current version of Secret Net Studio.
8. If necessary, edit the list of programs that use standard processing and click **Apply**. To edit the list, use the corresponding buttons on the right.

Button	Description
Add	Brings up the add application dialog box (see below)
Modify	Brings up the dialog box for configuring the selected application recognition parameters (see below)
Delete	Removes the selected application from the list

When you click **Add**, a dialog box for selecting and configuring the application recognition parameters appears as in the figure below.

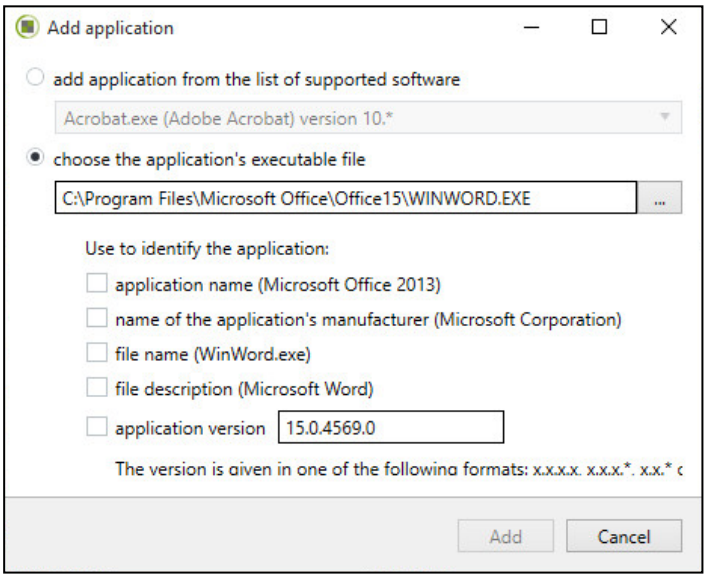


Select the required option in the dialog box and click **Add**. You can select one of the following options to add an application:

- adding from a list of compatible applications — to do this, click the **add application from list of supported software** option box and select the application from the drop-down list (the system will automatically configure the application recognition parameters);
- adding an application using its executable file — to do this, select the **choose the application's executable file** option box, click the button located on the right and select the file in the standard open file dialog box. Make sure that the application is already installed on the computer. Select the correct file and configure system recognition parameters. For this purpose, select the methods the system will use to identify the application (for example, by application manufacturer, file name or application version).

Note. An application will be identified using the values retrieved from the selected file. In particular, the application manufacturer's name must match the name in the file. Therefore, for example, a localized name of the same manufacturer will be considered different.

When changing the selected application, a dialog box for configuring the recognition parameters appears.



In the dialog box, select the methods the system will use to identify the application and click **Change**.

9. After you finish working with the applications list, click **Apply**.

To disable marking mode:

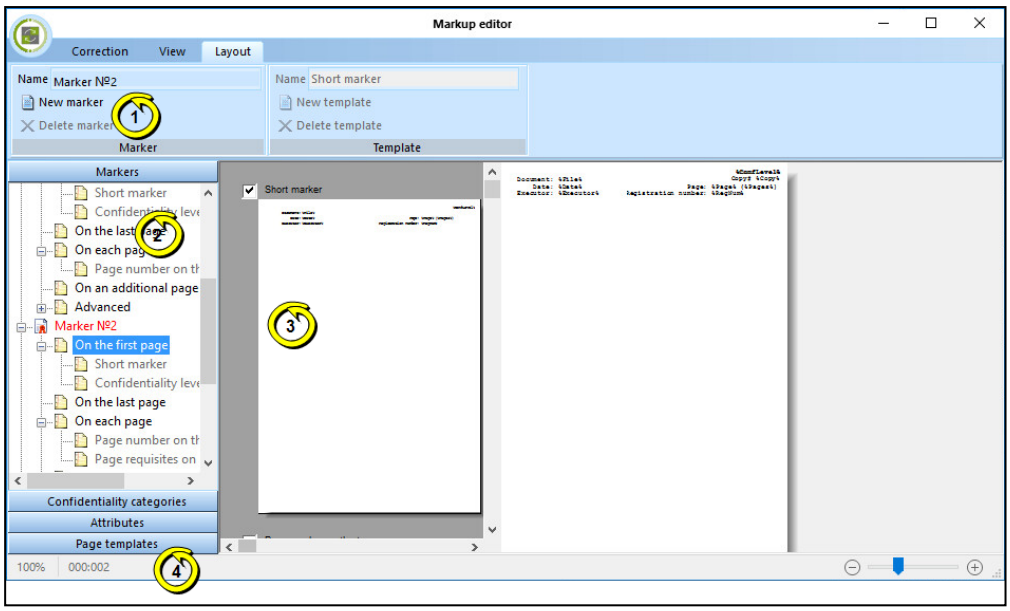
1. Complete steps **1**, **2** of the procedure described above.
2. Set the **Document marking** parameter to **Disabled**.
3. Click **Apply**.

Marker editing program

The marker editing program is designed for configuring the marking of printed documents. The program can be launched from the dialog box for configuring the parameters of the **Document marking** group policy (see p. **88**).

Program interface

The marker editing program window is shown in the figure below.



The program window may include the following interface elements:

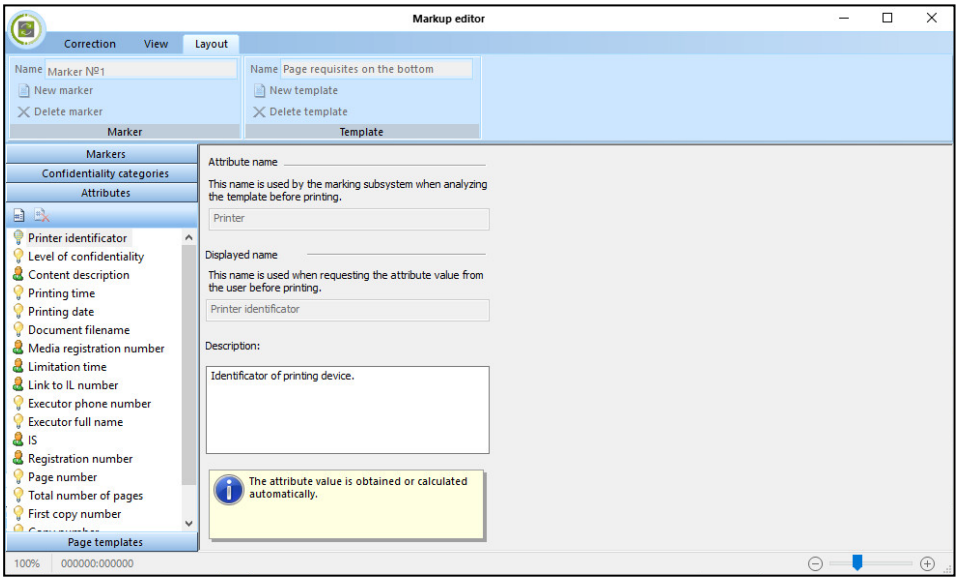
1 — Ribbon
Contains control commands (tools) for performing program actions. The ribbon contains separate tabs where commands are grouped depending on their purpose. Click the tab header to open the tab. The program window workspace can be expanded by enabling ribbon auto-minimize. In this mode, only tab headers are displayed. To maximize it again click the tab header. To switch between the ribbon display modes, double-click any tab header
2 — Object selection bar
Contains object lists and object use parameters. Objects and parameters are grouped into the following sections: • **Markers** — this section is designed for marker (label) list creation. Each marker has its own page layout templates that are displayed during document printing: first page, last page, specific pages, additional page or on the reverse side of the sheet. The marker can contain several templates. Data positions are specified in the templates, not in the marker. The list of markers is created using the **Marker** group commands in the **Layout** tab. • **Confidentiality categories** — this section is designed for selecting the markers that will be used for printing documents with certain confidentiality categories. • **Attributes** — this section is designed for creating the list of attributes that will be used in the page template layouts. Attributes are variables whose values are defined before printing a document. The attribute information can be requested from the user, or automatically provided by the security system (for example, the current date). Attributes that support automatic information retrieval are indicated with a special icon. In the list, you can add and remove attributes that support data request from users. The attribute list is edited using add and remove element buttons in the toolbar at the top of the **Attributes** section. • **Page templates** — this section is designed for creating the list of layout templates that are displayed in the markers for specific pages. A template is a page layout that overlaps the document contents during printing. The list of templates is created using the **Template** group commands in the **Layout** tab. To go to the required section, use the corresponding buttons on the object selection panel

3 — Editing area
Designed for displaying and configuring selected object parameters. Depending on the type of the object selected, the editing area contains: • when selecting a marker — the area displays the general marking view for all pages when printing documents with a marker; • when selecting a marker element related to specific pages — the area is divided in two parts: the left part contains the list of templates available for selection; the right side contains the general page marking view when the selected templates are used; • when selecting an attribute — the editing area contains the fields with attribute parameters: internal and displayed attribute name, description and information about the attribute usage; • when selecting a template — the editing area contains the page template for layout configuration. The configuration process includes placing layout elements (text, borders, attribute values) inside rectangular areas, which are similar to labels in text editors. The scale and general display parameters for the editing area are controlled using commands from the **View** tab. Layout elements and texts are controlled by commands in the **Edit** tab. To edit text in a label, double-click it. A dialog box for entering text and inserting attributes appears
4 — Status bar
Contains scale and cursor position indicators that are used for working with page templates

Procedure for marker editing

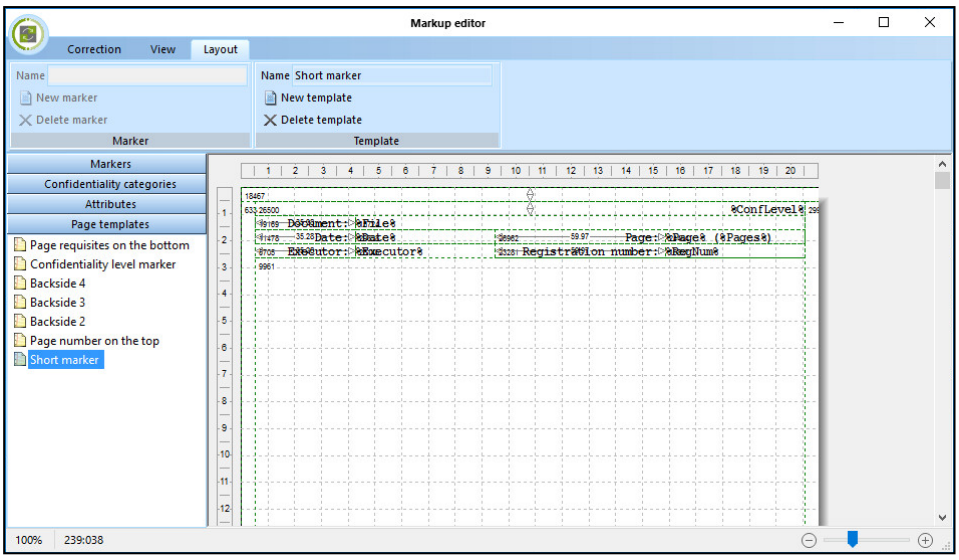
The following procedure is recommended for marker editing in the program:

1. In the object selection panel, go to the **Attributes** section.



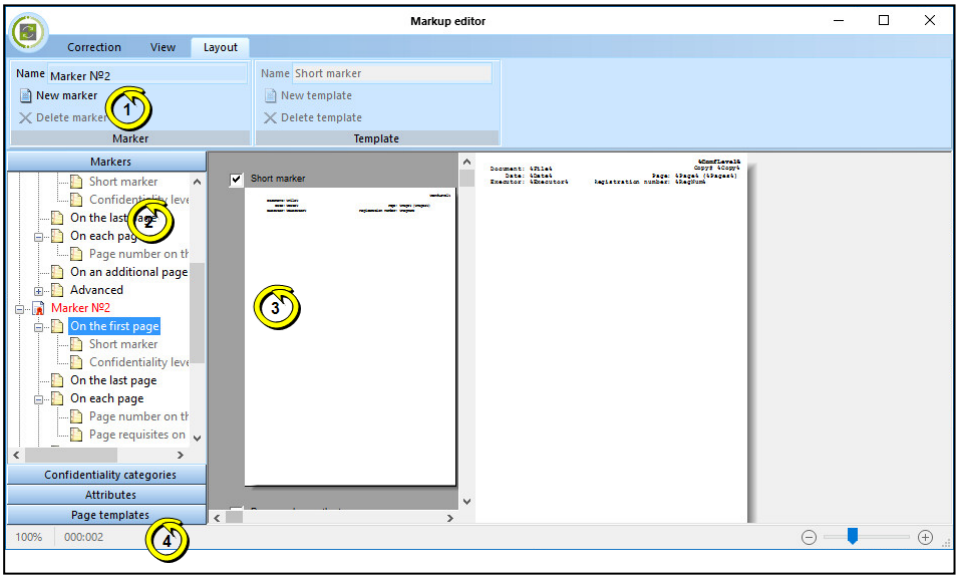
   If the required attributes are not on the list, modify existing attributes or add new ones.

2. In the object selection panel, go to the **Page templates** section.



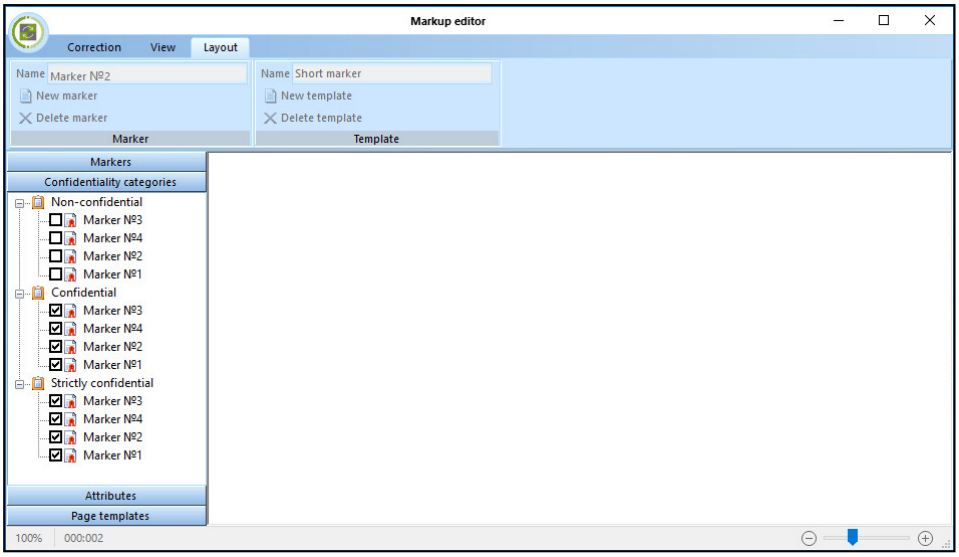
If the required templates (with the required layout and attribute set) are not on the list, modify existing templates or add new ones. Layout editing is performed using standard methods.

3. In the object selection panel, go to the **Markers** section.



If the required markers (with the required template name and layout) are not on the list, modify existing markers or add new ones. To modify a marker's template layouts, select the required page (page range) and select the required templates in the left-hand editing area.

4. In the object selection panel, go to the **Confidentiality categories** section.



Select the markers for each confidentiality category that will be used when printing documents.

5. Save the changes. To do so, click the button that can be found in the upper-left corner of the window and click **Save marking description**.
6. Close the program.

Chapter 10
Integrity Check

The Integrity Check (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 values and reference values is detected during the check, Secret Net Studio 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.

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
Resource	Describes the file or directory, register variable or Windows registry key. Determines the location of the controlled resource and its type
Resource group	Combines several descriptions of resources of the same type (files and directories or objects of the system registry). For example, executable files or register keys related to a specific application. Determined by the type of resources in the group
Job	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 registry
Task	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 allowed to be run by a specific group of users
Control actor	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 allowed 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 should be controlled.

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

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.

Storage

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
Replicated	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
Non-replicated	For non-replicated tasks, reference values are not replicated but calculated on workstations and only stored in the IC-AEC LDB

Generation of an AEC data model

A data model for a AEC mechanism can be generated based on data of the programs that have been run from Secret Net Studio log. For centralized management, it is necessary to create a log file in **.dvt** or **.snlog** format containing a selection of records for the required period. Then the file is imported to the IC-AEC database using IC-AEC management. When the IC-AEC control program is used in local mode, data on the running programs can be uploaded directly from the local log. Then, based on this data, the AEC tasks are generated for the actors.

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 preprogrammed 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, the user must be included in the local Administrators group To use centralized mode, the user should also be included in the group of security domain administrators.

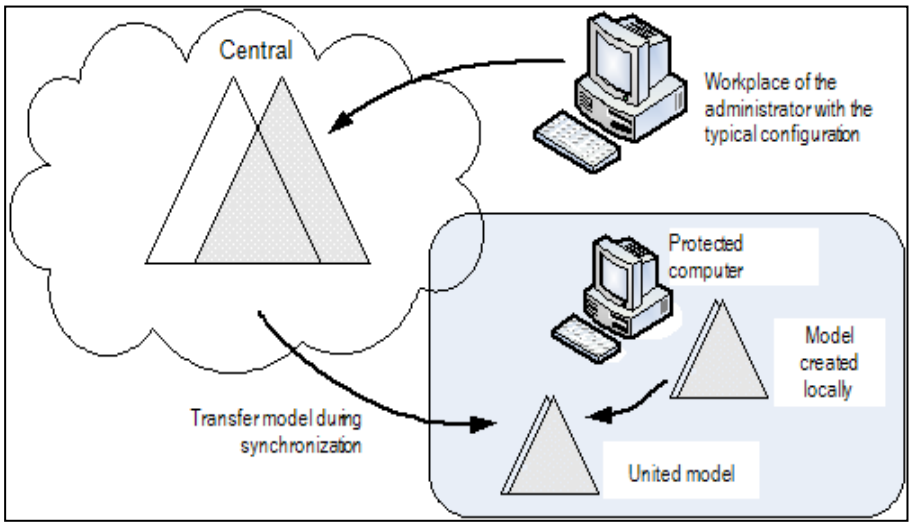
Synchronizing central and local databases

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 logon;
- after logon (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. 114). For prompt synchronization, certain Windows OS parameters should be defined on the computers (see p. 265).

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 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 AEC 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 to pass integrity check;
- 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 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 your system includes computers with Windows versions that have different bitness, we recommend arranging 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 AEC mechanism on the computer, perform the configuration in the following order:

1. Configure the new data model with control settings by default (see p. **98**).
2. Include additional objects to the data model:
   - tasks for integrity control for use in AEC (see p. **99**);
   - IC AEC jobs (see p. **101**).

   Note. To generate AEC tasks and jobs, you can collect information on user activity during work. This method involves using the mechanism in the soft operation mode and getting information on started programs from the Secret Net Studio log (see p. 103).
3. Establish links between AEC jobs and actors (see p. **104**).
4. Specify resources to control (see p. **105**).
5. Enable the process isolation mode (see p. **106**).
6. Create controlled resource reference values (see p. **108**).
7. Grant privileges to users that should not be subject to AEC restrictions (see p. **111**).
8. Enable AEC hard operation mode (see p. **112**).
9. Enable IC mechanism (see p. **111**). Before starting the mechanism, we recommend you to check that control job parameters are correct (see p. **112**).

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. **121**).

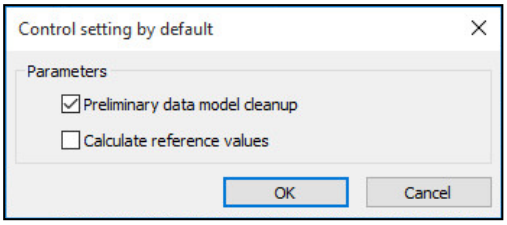
Building a new data model

A data model is automatically provided with Windows OS essential resource descriptions along with those related to some applied software products. A newly

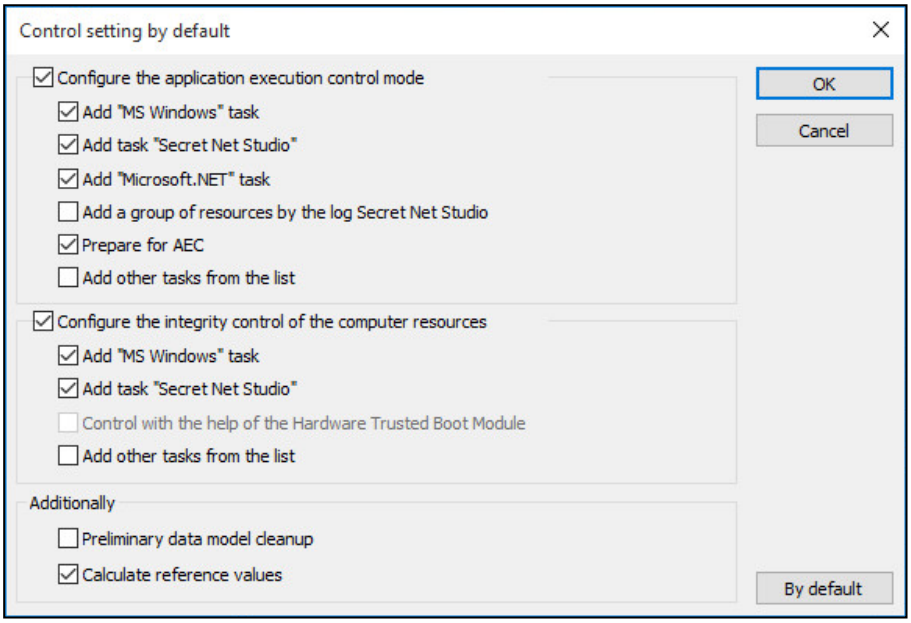
created model has a default control setup.

To build a new data model:

1. In **Applications and data control**, click **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. Depending on the selected work mode, set up the respective parameters and click **OK**.
   - When working in the centralized mode, we recommend keeping 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 Secret Net Studio 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 enhance 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.

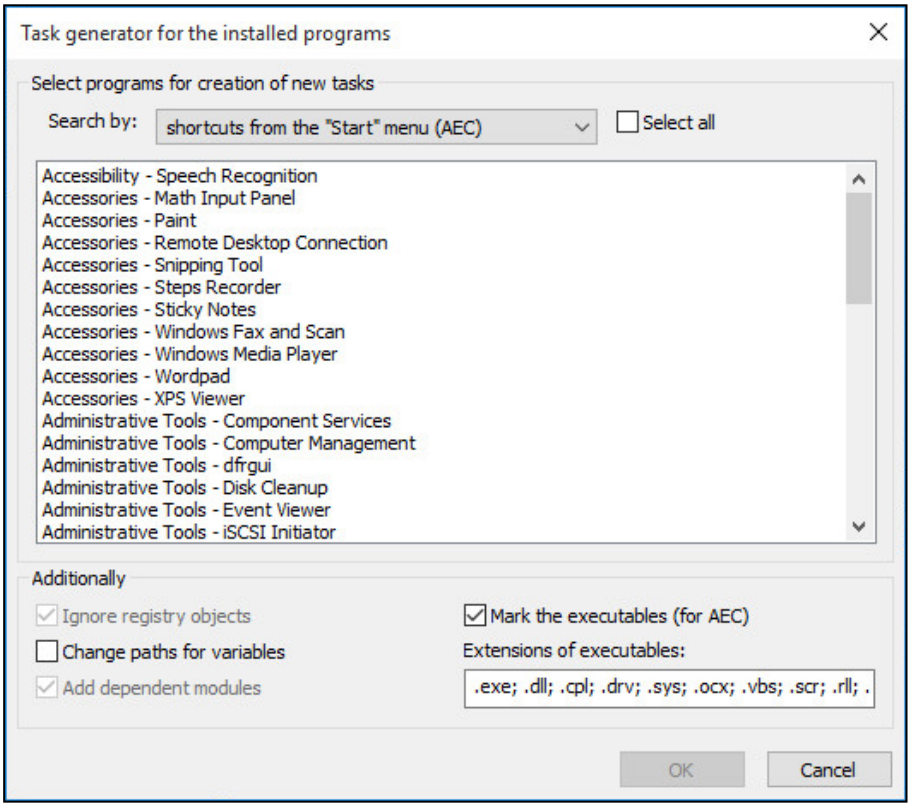
Prior to starting the generation procedure, you can view the list of software currently installed and note the particular components (of a program) that can serve as a basis for task generation. In this case, the tasks shall automatically include the resources referring to executable modules of a selected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

Furthermore, the AEC-tasks can be supplemented by using Secret Net Studio log-based AEC task generation method (see p. **103**).

To add tasks to a model:

1. In the **Service** menu, click **Task Generator**.

   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
Ignore registry objects	Registry objects should not be considered tasks

Parameter	Description
Change paths for variables	When recording a data model, the file location paths are replaced with environment variables
Add dependent modules	Dependent modules are the files that 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 added into the list: the files that the dependent modules depend on are also added to the list
Mark the executables (for AEC)	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 — see p. 272). 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 ⛔.

Creating jobs and adding 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.

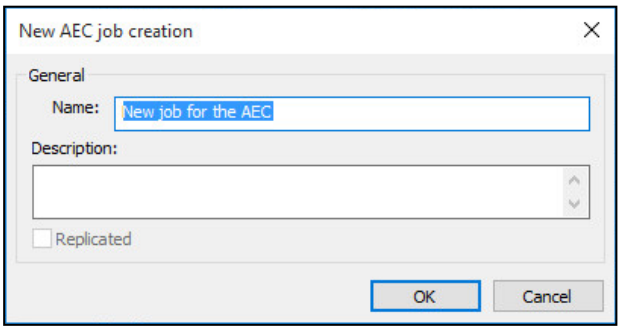
To create an AEC job:

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

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

2. Select **Application Execution Control** and click **OK**.

   A dialog box appears as in the figure below.



3. Enter a job name, a brief description and click **OK**.

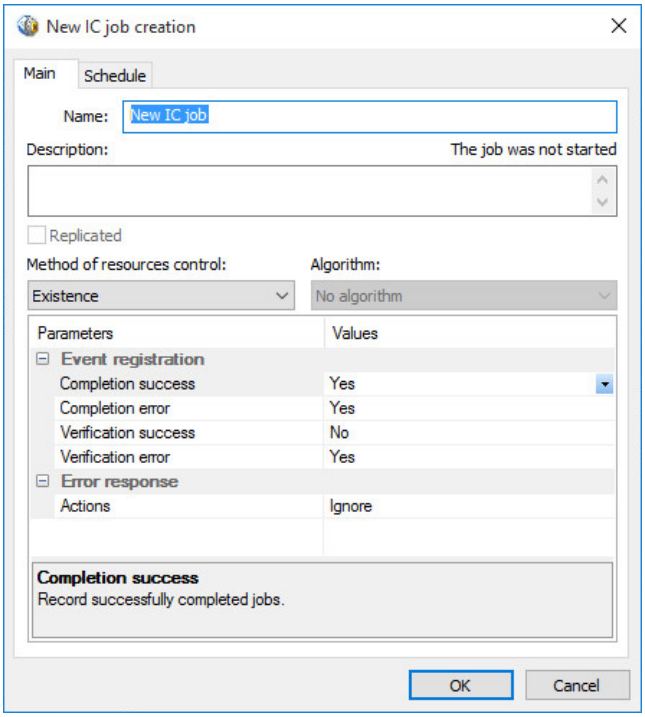
To create an IC job:

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

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

2. Select **Integrity Control** and click **OK**.

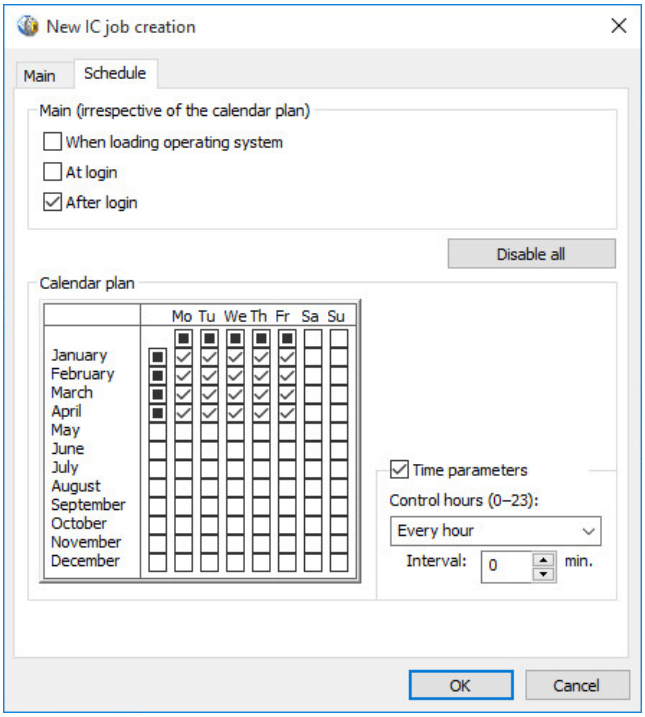
   A dialog box appears as in the figure below.



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

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.

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



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 **Add tasks/groups > Existing**.

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

Enabling AEC soft mode operation and task creation by log

For AEC task creation using Secret Net Studio log records, these tasks are performed in the following order:

1.	Enabling AEC soft mode
2.	Logging information
3.	Adding AEC tasks created by log

Enabling AEC soft mode

There are two operating modes for AEC: soft and hard. Soft mode is used to set up the mechanism; hard mode is the main operation mode. In soft mode, the user can run any program. If the user runs programs not marked as allowed, an alert is recorded in the Secret Net Studio log. In hard mode, the user can only run programs marked as allowed. Other programs cannot be run, and the alerts are recorded in the Secret Net Studio log.

Soft mode is used to collect information about possible errors during the AEC mechanism setup.

To enable AEC soft mode:

1. In the **Categories** panel, select the **Control actors** category.
2. Select the structures or, in the list of objects, a computer or group (of computers), open the context menu and click **Properties**. In the **Control actor properties** dialog box, select the **Modes** tab.
3. Select the following check boxes:
   - **The modes are set in a centralized way** (for centralized control);
   - **AEC mode enabled**;
   - **Soft mode**.
4. Click **OK**.

AEC mechanism starts in soft mode for the selected computer (or group).

Logging information about programs and scripts in use

The AEC model can be created on the basis of Secret Net Studio log records. To collect the required data, users can run any applications and scripts. A certain period of time is allocated for this. Information about running applications and scripts is recorded in the log. During data collection, enable registration of all events from the AEC category for those computers which will use AEC.

When data collection is finished, AEC tasks are created in the data model on the basis of information about running applications from the Secret Net Studio log. Information can be exported to the data model directly from the local Secret Net Studio log or from the file with log records saved in advance.

Note. The description of the log entry saving procedure is given on p. 46.

Adding AEC tasks created by log

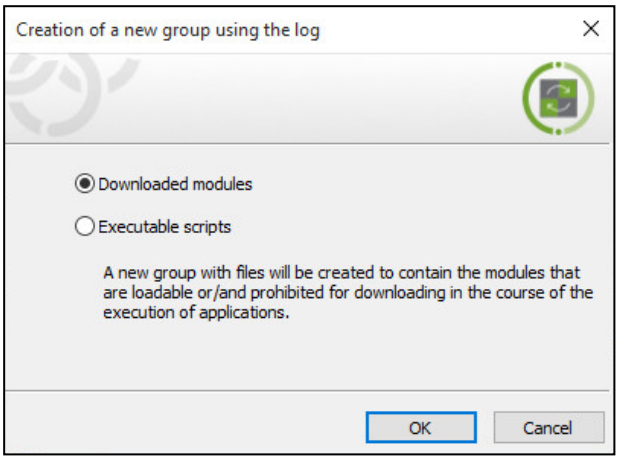
At this stage, tasks that are added to AEC jobs are created on the basis of Secret Net Studio log records.

Note. A **.dvt** file or **snlog** file with previously exported log data are used as a source for adding AEC tasks in the centralized mode. In local mode, the security log or the Secret Net Studio log can be used as a source.

To add AEC tasks created by log:

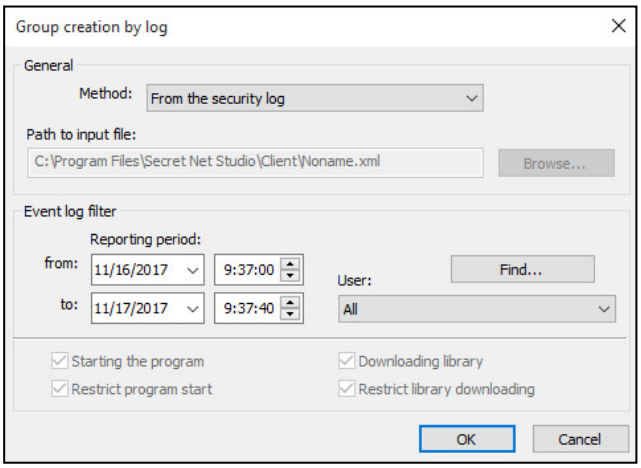
1. Select an actor in the main **IC-AEC Management Program** window.
2. Select a previously created AEC task linked to the selected actor or create a new AEC task.
3. Right-click the task and select **Add tasks/groups > New group by log**.

   A dialog box asking you to select a resource type appears as in the figure below.



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

   A dialog box appears as in the figure below.



6. Specify the required parameters (path to **.dvt** file or **.snlog** file if in the centralized mode, or log type in the local mode as well as additional selection criteria if necessary) and click **OK**.

A resource group generated on the basis of log records will be added to the task.

Repeat this procedure for other actors.

Configuring links between actors and AEC jobs

At this stage, it is necessary to assign created AEC jobs to actors. Jobs are assigned to the following actors: **Computer** and **Group** (**Computer**, **User** and **User group** in local mode). For the jobs to be assigned to the required actors, the jobs must be

added to the data model. The data model must contain actors that correspond to computers with unique installed software configuration as well as groups including computers with the same installed software configuration.

To add an actor to a model:

1. In the **Categories** panel, select the **Control actors** category.
2. In the **Control actors** menu, click **Add to list**.

   A dialog for selecting an actor type (in the centralized mode) or the standard Windows dialog box appears in order to select users and user groups (in the local mode).
3. Specify the type of objects being added. Then, select the required objects from existing ones or, if you are adding a group of computers, specify the group name, its description, and create the list of computers that are included in it.
4. Click **OK**.

   The **Applications and data control** program window displays new actors marked with a symbol ! (i.e. not linked with other objects).

To associate an actor with a job:

1. In the **Category** panel, select the **Control Actors** category.
2. Use an additional structure window or search option to find an actor to be associated with a job, right-click the actor and click **Add jobs > Available**.

   A dialog box showing the list of available jobs appears. Each job has a number of actors it is associated with.
3. Select an AEC job that you wish to assign to an actor.

   Tip. To select multiple jobs, use the **Ctrl** key or click **Select all**.
4. Click **OK**.

The selected jobs will be assigned to an actor.

Preparing resources for application execution control

The resources can be controlled by the application execution control mechanism if they have an executable attribute and are included in the AEC job. Assigning the executable attribute to the resources is called preparing resources for AEC. This attribute is assigned to all files with defined extensions.

In addition, a search for dependent modules may be performed for each resource with the executable attribute (see p. **135**). Discovered dependent modules are added to the data model to the same resource group as the initial modules. They are also assigned the executable attribute.

Files with the executable attribute included in the AEC job form a list of programs that are allowed to be started. After establishing a link between job and user and enabling soft or hard mode, Secret Net Studio starts to control the programs launched by the user and register the respective events in the log.

During automated data model configuration (see p. **99**), resource preparation for AEC is included in the corresponding procedures and is performed by default. During manual model configuration and its modification, resource for AEC are prepared as a separate procedure.

In some cases (for example, during manual configuration of tasks for application execution control or after adding new resources to the model), it may be necessary to create a new list of resources with the executable attribute. For this purpose, two additional options are available within the resource preparation procedure:

- Before starting procedure execution, you can reset the executable attribute for all resources that have the attribute in the data model. In this case, all resources in the model will be analyzed.
- It is necessary to perform a search of dependent modules. In this case, a search of dependent modules for each resource with the executable attribute will be

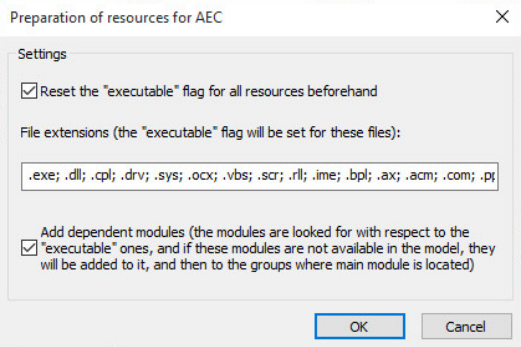
performed in the computer's resources. Discovered dependent modules will be added to the data model to the same resource groups as the initial modules.

Note. In the program's centralized operating mode, the procedure for preparing resources requires that the data model has at least one AEC job with resources to control.

To prepare resources:

1. In the **Service** menu select **AEC resources**.

   A dialog box for configuring procedure settings appears.



2. If you want to analyze all the model's resources (including those with previously assigned executable attributes), select the **Reset the "executable" flag for all resources beforehand** check box. In this case, the list of resources with executable attributes will be created again. In addition, the procedure execution time will be related to the overall number of resources in the data model.

   If you only want to analyze resources without the **executable** attribute, clear the check box.
3. Delete from the list or add to the list file extensions to which you want to assign the executable attribute.
4. To add dependent modules to the data model, select the **Add dependent modules** check box.

   If it is not necessary to add dependent modules, clear the check box.
5. Click **OK**.

Preparing resources to be used in the application execution control mechanism starts. A window with information on the progress of the process appears. After completion, a message about successful completion will appear.

Enabling and configuring process isolation

If it becomes necessary to ensure an isolated environment for certain processes (prohibit data exchange with other processes), the actions can be performed as follows:

1. Enable the process isolation mode.
2. Add files of isolated processes to the resource list.
3. Enable isolation for resources.

Enable the process isolation mode

By default, the process isolation mode disabled. The mode is enabled for the control actor.

To enable the isolation mode:

1. In the **Categories** 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 the object and click **Properties**. In the **Properties of the control actor** dialog box, select the **Modes** tab.
3. Select the **Process isolation enabled** check box.
4. Click **OK**.

The process isolation mode starts working for the selected computer (or group of computers).

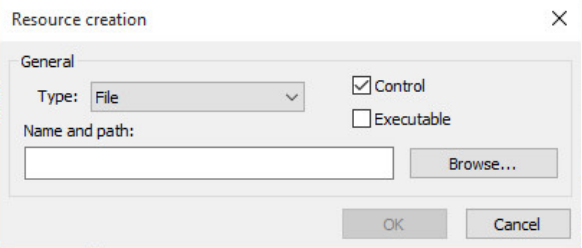
Add files of isolated processes to the resource list

Executable files of processes that are to be isolated should be added to the lists of task resources for the AEC. Isolation can be enabled for files with **.exe** extension (for example, the Notepad editor startup file, **notepad.exe**) as well as for files listed in the **Names of executable modules of processes** in the parameters of the program – see p. 272.

To add a file to the list of resources:

1. Right-click the resource group for files and folders in the AEC task and click **Add Resources > New single**.

   The dialog box for setting the resource parameters appears as in the figure below.



2. Set the parameters of the added resource (see the table below) and click **OK**.

Parameter	Explanation
Type	Specify the type of added resource: File
Name and path	Type the name and full path to the resource being added or click **Browse** and use the standard OS procedure
Control	The selected check box means that this resource will be controlled after enabling the integrity control mechanism. If the control of this resource is not required, 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
Executable	The parameter is used to denote executable files, which comprise lists of programs allowed to start when the application execution control is turned on

   The resource appears in the list of the main program window.

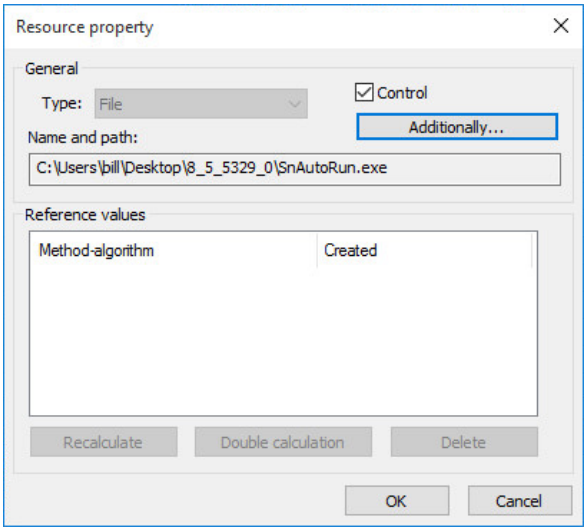
Enable isolation for resources

After process files are added to the list of resources, the procedure for enabling isolation for each resource is performed.

To enable isolation for a resource:

1. Select a resource from the objects list, right-click it and select **Properties**.

   The dialog box for setting the resource parameters appears as in the figure below.



2. Click **Additionally**. In the resulting dialog box, select the **Isolate the process** check box and click **OK**.
3. Click **OK**.

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 wizard (see p. 98). 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.

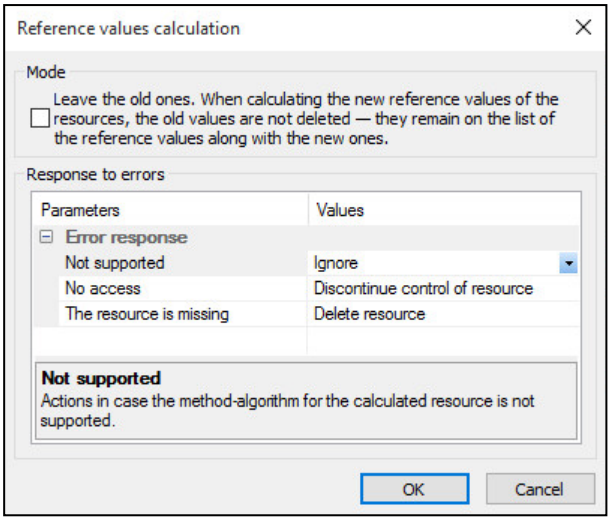
In the local mode, reference values can be calculated for all resources contained within a local data model. Exceptions are resources whose reference values were calculated in the centralized mode (i.e. resources are included in replicated jobs).

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. Depending on the resources for which reference value calculation is needed do the following:
   - in the **Service** menu, click the **Reference values** > **Calculate** 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** 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 p. 134.

3. Configure the security system to react to potential errors during reference values calculation. To do so, in the left part of the table, select the error type and the security 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
Ignore	No system reaction for specified error
Display request	When an error occurs, a respective error message is displayed, prompting a choice of actions to rectify the problem
Delete resource	When an error occurs, the resource is deleted from the data model
Discontinue control of resource	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
Ignore	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)
Discontinue control	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
Delete	The calculation procedure will continue. The resource that caused the error will automatically be deleted from the data model
Interrupt	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 **Reference values > Calculation** to calculate reference values for all replicated jobs;
   - right-click the job and click **Local reference values calculation** to perform the reference values calculation for resources of a separate replicated job.

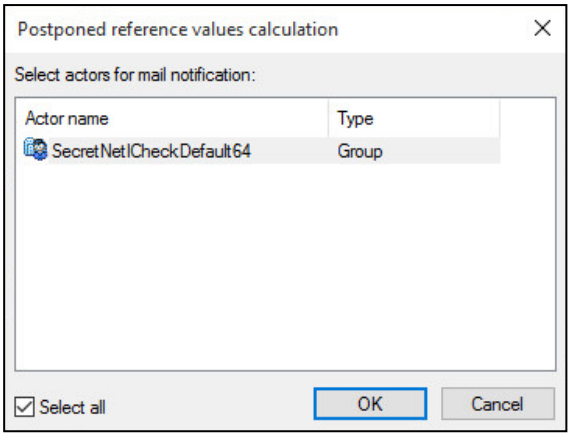
   The **Reference values calculation** dialog box appears.

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 asking you to select an actor appears. 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 **Remote reference values calculation**) 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 **Postponed reference values calculation** 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. In 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 **Add jobs > Existing**...

   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).

Granting privileges when working with AEC

Secret Net Studio provides a privilege for removing AEC restrictions for a user. AEC is not applied to users who are granted this privilege.

By default, the privilege is granted to users included in the local group of administrators.

The centralized configuration procedure is described below. Local configuration is performed in the same way via the Local Control Center. For information about the Control Center, see document [**1**].

To grant the privilege:

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 menu, select the **Settings** tab and download the settings from the Security Server.
2. In the **Policies** section, select the **AEC** group of parameters.
3. Edit the list of users and user groups who are granted the privilege for the **Application execution control: Accounts to which Application execution control rules do not apply** parameter.
4. Click **Apply**.

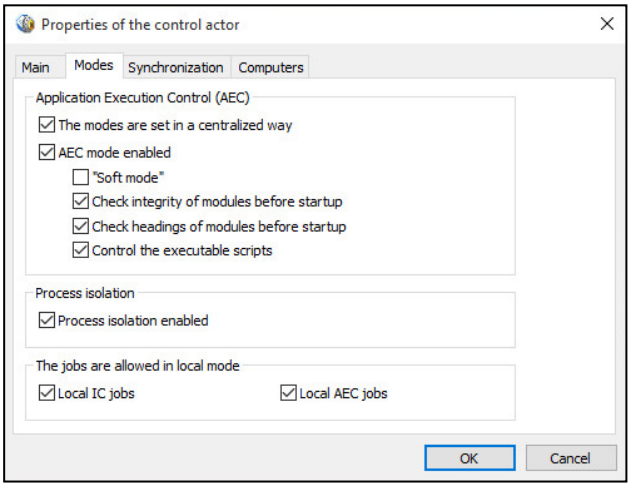
Enabling AEC hard mode

When AEC is launched and operates in hard mode, it only allows certified software products, libraries and scenarios to be run. Other resources are blocked and cannot be run, while the unauthorized access attempts are registered in the Secret Net Studio log as alerts.

AEC parameters can be set in the centralized or local mode. In the centralized mode, parameters can be configured for separate computers and computers in groups. If AEC configuration parameters for a computer and the group that this computer belongs to are different, this computer will still be an actor to all active parameters (i.e. parameters are "summed"). For example, if soft mode is enabled for a group, this mode will be active even for a computer with this parameter disabled.

To activate AEC in hard mode:

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 click **Properties**. In the **Control Actor Properties** dialog box, select the **Modes** tab.



3. In the centralized mode, select the **The modes are set in a centralized way (for centralized control)** check box.
4. Select the **AEC mode enabled** check box and clear the **Soft mode** check box (if available).
5. If necessary, configure any additional control parameters.

Parameter	Description
Perform module integrity control before startup	Certified software undergoes an integrity control procedure
Verify headings of modules before startup	While the procedure is in progress, an additional mechanism is enabled, which ensures the efficient division of resources into executable and non-executable files (i.e. files to be checked and files to be ignored)
Control executable scripts	Scenarios (scripts) that are non-certified and unregistered in the database are blocked

6. Click **OK**.

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 associated with an actor.

The check has two modes: light mode and full imitation. In the 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 security 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 **Job start**.

   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 **Full imitation**.
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 **Job start**.

   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 **Remote job start**.

   A dialog box asking you to select a actor appears. 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 that are currently turned on.

Saving and loading 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 **Save** 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. **117**, p. **118**).

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. 272). 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 **Notify about changes** 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.

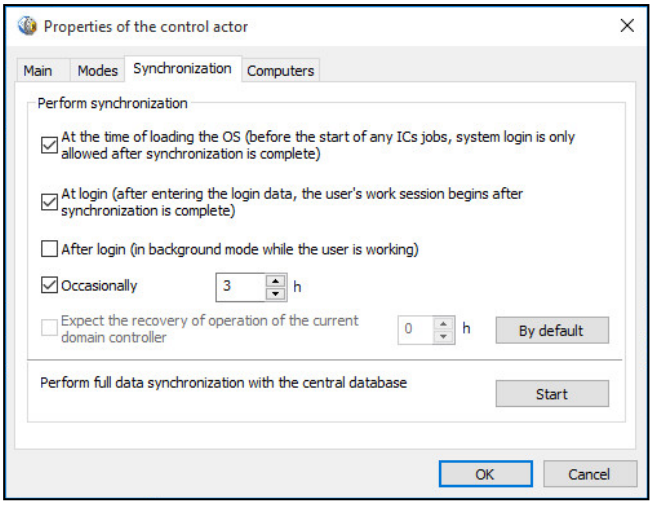
Synchronization start parameters are configured in the program's centralized operation mode. The parameters may be defined for separate computers and for groups. In this case, the parameters have application priorities: computer parameters have the highest priority, followed by group parameters, apart 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 **Properties**. 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
At the time of loading...	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 log on 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
At login...	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
After login...	If selected, synchronization is performed in background mode after start of the user working session
Occasionally	If selected, synchronization is started when the computer is on, at predefined intervals (in hours)
Expect the recovery of operation of the current domain controller	*Not available in the current version*

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 turned 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 **Check group synchronization** in the **Service** menu.

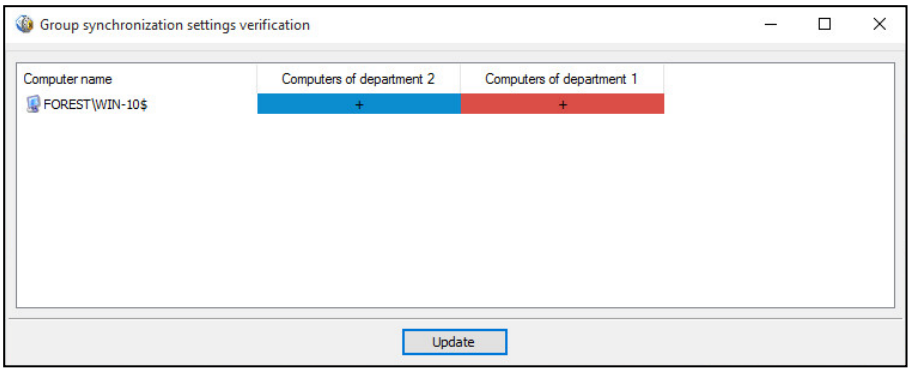
Note. The command is not available if the list of actors in the data model contains only one group by default **SecretNetICheckDefault**.

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 an 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**.

Forcing 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. **114**). 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 **Properties**. In the **Properties of the control actor** window, go to the **Synchronization** tab.
3. Click **Start**.

   The synchronization process starts.

Downloading and restoring 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 not sure 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 restoring procedure is used for such purposes.

To restore a model from a DB:

1. In the **File** menu, click **Restore from database**.

   A warning about the possibility of losing 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:

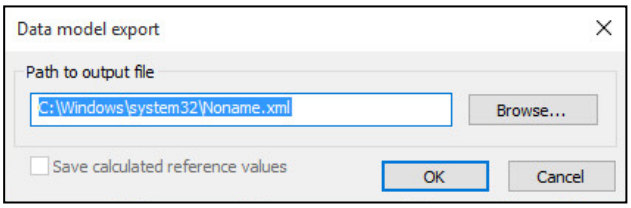
- exporting the entire data model;
- selective exporting of objects from specific categories (does not apply to **Control Actors** category objects).

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. 277.

To export the current data model:

1. In the **File** menu, click **Export model to XML**.

   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:

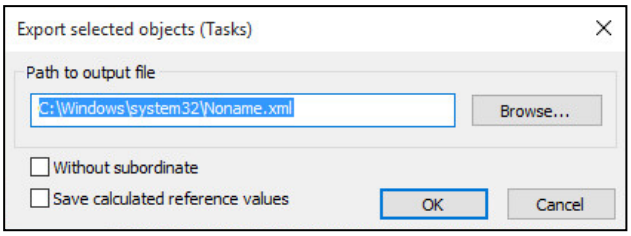
1. In the category panel, select the category that contains objects to be exported (except the **Control actors** category).
2. In the structure window or in the object list area, find the objects to be exported.

   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 **Export selected**. 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 toutput 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.

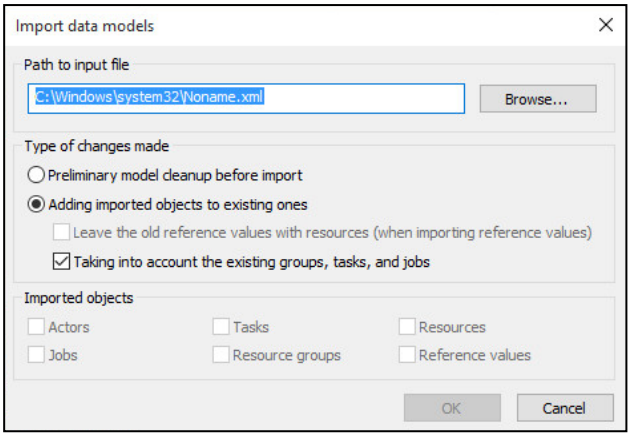
Resource lists exported from another data model are added by importing from a file with a saved data model. This method is used when transferring security mechanism settings from one computer to another. Computers must have the same configurations and use the same software.

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 **Import model from XML**.
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 so, select one of the check boxes listed below.

Check box	Description
Preliminary model cleanup before import	The current data model's objects are deleted before importing. After importing, the model will only consist of objects contained in the file
Adding imported objects to existing ones	After importing, the model will contain both imported objects and objects of the current data model. 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. 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<N>**, where **N** is an enumerator of the duplicated object. Objects from the **Resources** category are not duplicated. 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

5. In the **Imported objects** field group, select the object categories for importing. To do so, 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 so, 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.

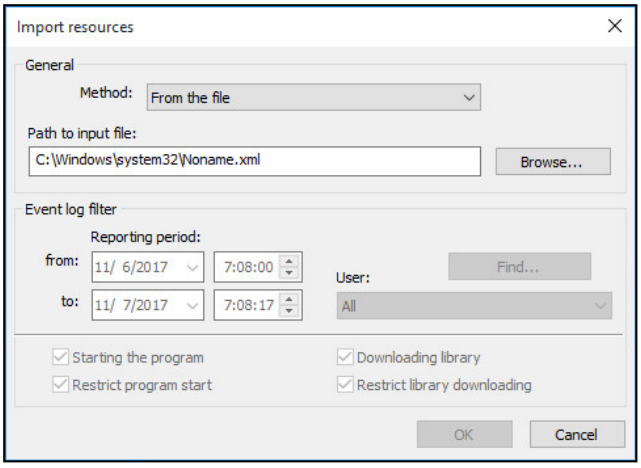
7. Click **OK**.

To import objects from the current category:

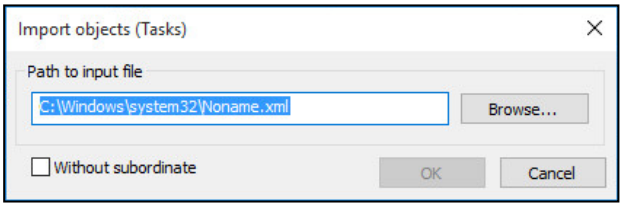
1. On the category panel, select the category from where you want to import objects (except **Control actors** category).
2. Select the root element in the structure window. Open the menu with the name of the selected element (e.g., **Job**) and click **Import and adding**.

   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).

Editing the data model

When creating the data model, as well as when 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
Changing object parameters	p. **122**
Changing resource parameters	p. **122**
Changing resource group parameters	p. **123**
Changing job parameters	p. **123**
Changing job parameters	p. **124**
Viewing control actor parameters	p. **124**
Adding objects	p. **125**
Adding an individual resource manually	p. **125**
Adding several resources manually	p. **129**
Importing a resource list from Windows OS security log	p. **128**
Importing a resource list from the Secret Net Studio log	p. **128**
Adding a resource to a group	p. **129**
Adding a resource group manually	p. **129**
Adding a resource group based on a directory	p. **129**
Adding a resource group based on a registry key	p. **130**
Adding a resource group using import tools	p. **130**
Adding a job manually	p. **130**
Adding a job using a job generator	p. **99**
Adding a job using import tools	p. **120**
Adding tasks	p. **101**
Adding actors	p. **111**
Deleting objects	p. **133**
Deleting an object	p. **133**
Deleting all objects of a specific category	p. **134**
Linking objects	p. **134**
Linking objects	p. **134**
Deleting the link between objects	p. **134**
Generating AEC job for the Secret Net Studio log	p. **103**
Preparation of resources for AEC	p. **105**
New calculation and reference values replacement	p. **134**
Dependent modules search	p. **136**
Replacing environment variables	p. **136**

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. 136).

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. 272 — see document [**1**]) 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 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 **Properties**.

   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 **Double Recalculation**.

   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 so, click **Additionally** and perform the following actions in a dialog box:
   - to permit the process to perform any script, select the **Allow the execution of any scripts** check box;
   - to allow the process to run files from specific folders, select the **Allow the execution of any modules from the specified 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 (**+**). To delete a folder from the list, select it and click (**-**);
   - 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 **Properties**.

   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**.

Task parameters

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

To change task parameters:

1. Select a task , right-click it and click **Properties**.

   The dialog box for setting the task parameters appears.
2. If a script requires changes, click **Script** (generation of a script is described onp. **131**).
3. Make changes in the **Name and Description** fields and click **OK**.

Job parameters

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

- job name and description;
- job 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 job. When changing control methods and algorithms, take into account the types of resources related to the job, 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.

Properties of an application execution control job determine the following parameters: job name, brief description and type (replicated/non-replicated).

To change job parameters:

1. Select a job , right-click it and click **Properties**.

   The dialog box for setting the job parameters appears.

2. Change the modifiable parameters and click **OK**. Actions are performed in the same way as in the job creation procedure (see p. **101**).

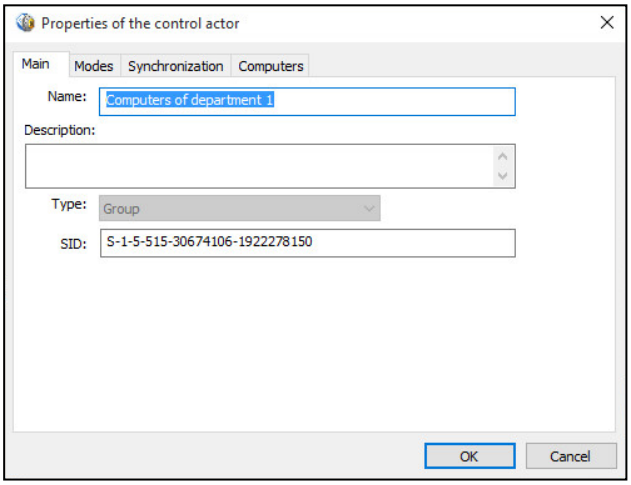
Actor parameters

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 **Properties**.

   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
Automatically, during job generation	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
Manually	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
Using import tools	The list of resources can be imported from the following sources: • a file with a saved data model (see p. **118**); • the Windows security log or the Secret Net Studio log on a specific computer, or a saved log file (see below)
By adding the resource to a group	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 asking you to select the resource type appears.
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 the table below) and click **OK**.

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

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

Parameter	Description
Control	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
Executable	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):

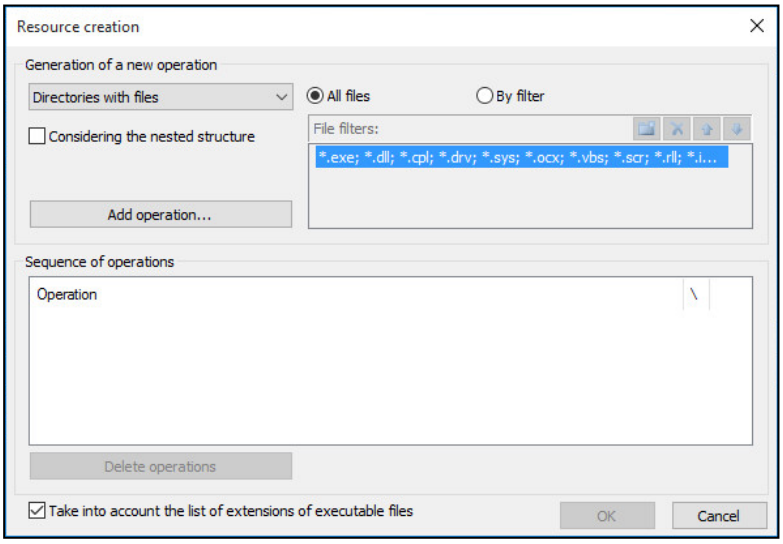
Parameter	Description
Name	Enter the name of the resource, unique for the list of resources. For example, the name of the file from which the scenario (script) can be indicated as the resource name
Description	Enter additional information about the resource
Contents	**Enter the scenario (script) text** – 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 **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 **Add operation**.

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
Resource selection version	The following options are available: • **Selected files** (standard file selection procedure, additional conditions are not available). • **Files by directory** (files included in the folders are added, nesting is taken into account, a filter can be used). • **Directories with files** (nesting is taken into account, a filter can be used). • **Directories by directory** (nesting is taken into account). • **Variables by key** (variables are selected by the register key, nesting is taken into account). • **Key with variables** (keys with variables are selected, nesting is taken into account)
Considering the nested structure	The nesting of resources is taken into account for all selection versions, with the exception of the **Selected Files** version
All files	All resources for the **Files by directory** and **Directories with files** versions are selected
By filter	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
Taking into account the list of extensions of executable files	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. **272**). 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 following extensions ***.exe**; ***.dll**; ***.cpl**; ***.drv**; ***.sys**; ***.ocx**; ***.vbs**; ***.scr**; ***.rll**; ***.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, press **F2**, and edit the list of file extensions.
- To add a new filter, click **New**, and enter the list of file extensions in the line that appears.
- To remove a filter from the list, select it and click **Delete**.
- To move a line within the list, select it and click the arrow button.

2. Setting the resource selection parameters. To do so, 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 **Delete Operations**.

   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 **Delete Operations**.

   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.

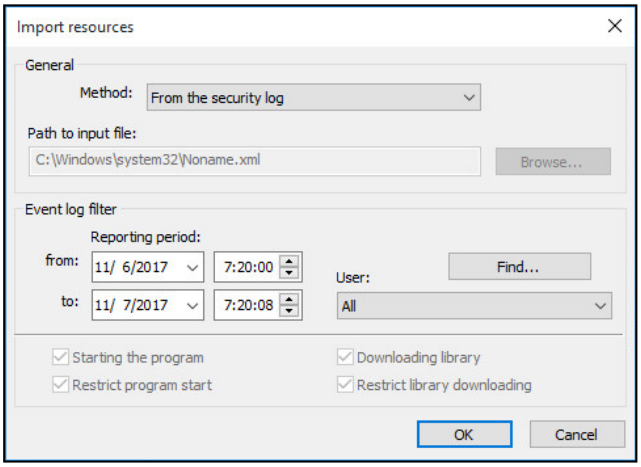
9. Check the list of completed operations, and if it contains all resources you had planned to include in the data model, click **OK**.

   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 **Resources > Create resources > Import and adding from the menu**.

   A dialog box appears as in the figure below.



2. Select **From the security log** 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 **Find.**

     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 **Resources > Create resources > Import and adding from the menu**.

   A dialog box appears (see the previous procedure).

2. Select **From the security log** 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 **Add Resources** 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 p. 120), 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 **Resource Groups > Create group > Manually 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 **Resource Groups > Create group > By directory 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 **Resource Groups > Create group > By registry key 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 **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 resource group using import methods:

1. Select the **Resource Group** category.
2. Click **Import and adding** 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. **120**).

Adding tasks

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

- manually;
- manually with a script;
- using a task generator;
- using import tools (see p. **120**).

To add a task manually:

1. Select the **Tasks** category and click the **Tasks > Create task > Manually** command from the menu.

   The dialog box for setting the task parameters appears.
2. Enter a job name, a brief description and click **OK**.

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

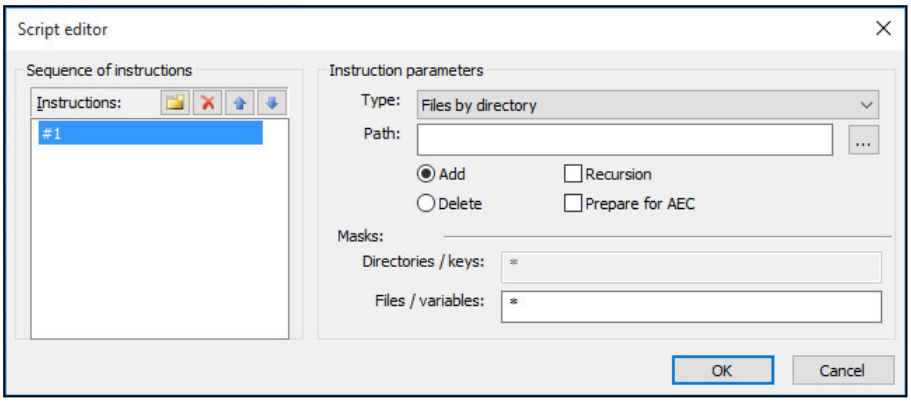
To add a task with a script manually:

1. Select the Tasks category and select **Tasks > Create task > Manually** command from the menu.

   The dialog box for setting the task parameters appears.

2. Enter the task name and its brief description.
3. Click **Script**.

   A dialog box appears as in the figure below.



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

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
Files by directory	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
Directories with files	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
Variables by key	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
Keys with variables	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
Installed programs (MSI)	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
Secret Net Studio components	Select the Client resources
Files from variables in the specified registry key	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
Downloaded Windows drivers and services	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. **135**). 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 the 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 jobs

Job adding procedures are described in detail on p. **101**.

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 **Add to list**.

   A dialog box prompting you to select the type of added actors appears.
3. Select **Computer** and click **OK**.

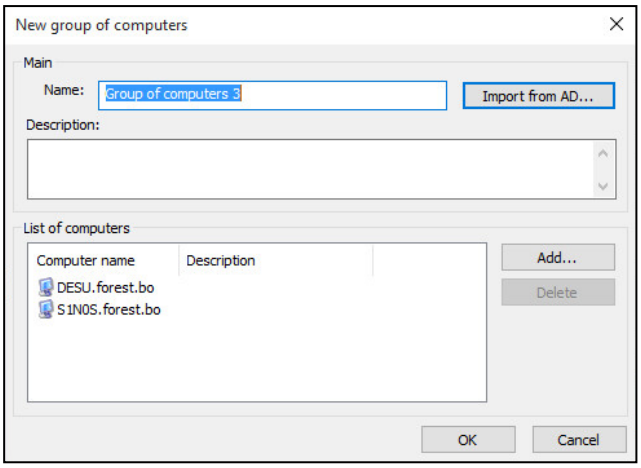
   A dialog box with the list of security domain computers with the Client appears.
4. Select the required computer in the list and click **OK**.

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 **Add to List**.

   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 so, 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 **Add to List**.

   A Windows dialog box prompting you 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 **Delete**.

   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 showing the object to be deleted with superior or subordinate objects appears. If you also want to delete subordinate objects from the data model, select **Delete subordinate**. 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 **Delete All**.

   A dialog box with links to the objects appears.

2. If you want to delete all subordinate objects, select **Delete subordinate**. 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 **Add *object name* > Existing**.

   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 **Exclude from > *objectname***.

   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 are 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. **108**). 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 **Properties**.

   The **Resource properties** dialog box appears (see p. 122).
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. 108).

To delete old reference values:

- From the menu, click **Service > Reference values > Delete old**.

  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 **Properties**. 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

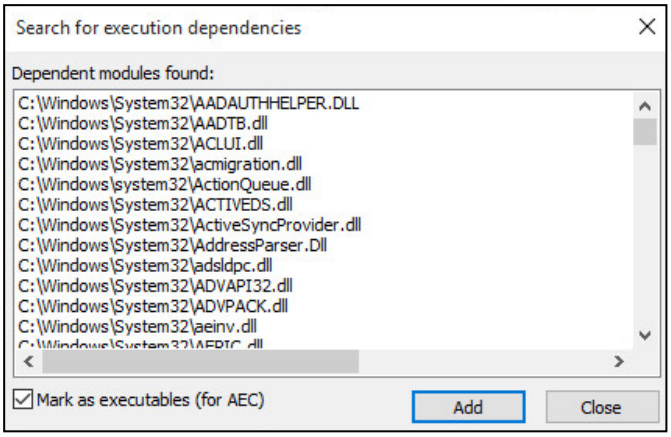
When the user works with applications, executable files may be run together with modules (drivers and libraries) which are not directly integrated into the applications. Such modules are called dependent.

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 **Dependencies**.

   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. Right-click a resource in the data model and click **Environment Variables**.

   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 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 11
Mandatory Access Control

About Mandatory Access Control

The Mandatory Access Control mechanism ensures isolation of user access to confidential resources. A resource is considered confidential if its confidentiality category differs from the public information category (by default, **Non-confidential**). A category can be assigned to the following resources: You can assign a confidentiality category to the following resources:

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

Note. Files and folder located on devices from groups USB, PCMCIA, IEEE1394, Secure Digital (external drives) are not assigned a confidentiality category individually. Those files and folders inherit the confidentiality category from the device where they are located.

For network interfaces, you can assign confidentiality levels of sessions where these interfaces can operate (in the flow control mode).

For printers, you can assign confidentiality categories for the documents that are allowed to be printed out.

The user is granted access to confidential information based on his/her access level.

Resource confidentiality categories

A confidentiality category is a resource attribute. By default, the following confidentiality categories are used in MAC:

- **Non-confidential**;
- **Confidential**;
- **Strictly confidential**.

You can add other categories and set their names in accordance with the standards of your company. Maximum number of categories is 16.

Once the Client is installed, all folders and files on the computer local drives are assigned the **Non- confidential** category (if they were not assigned a confidentiality category before). Confidentiality categories for the required files can be elevated by the users within their access levels. Only users with the **Manage confidentiality categories** privilege can lower resource categories or elevate folder categories.

For the devices that can be assigned a confidentiality category or for which acceptable session confidentiality levels can be selected, the **Device is available regardless of confidentiality categories** or **Adapter is always available** access mode is enabled by default. For printers, the mode allowing to print documents of any confidentiality category is enabled by default. These modes allow devices and printers to be used regardless of the user access level. The administrator assigns the confidentiality categories or levels to devices and printers.

Inheriting a confidentiality category

Devices inherit their confidentiality category from classes which they belong to. At the same time, for a class, you can assign a public information category only (**Non-confidential** by default) or enable the **Device is available regardless of confidentiality categories** mode. This prevents the copying of confidential data to an unauthorized device (when the mechanism operates in the flow control mode and the user does not have the privilege to output confidential information).

In accordance with inheritance rules, explicitly configured parameters have a higher priority over inherited parameters of senior hierarchy elements (see p. 69). Therefore, the explicitly assigned confidentiality category for device is applied regardless of the category is assigned for the respective class.

Confidentiality categories for devices and classes are assigned by the administrator via the device list of the group policy.

The confidentiality category of a local drive has a higher priority than the categories of files and folders stored on that drive. If the confidentiality category of a file/folder is lower than the drive confidentiality category, Secret Net Studio treats the category of that file/folder equal to the category of the local drive. Conversely, when the confidentiality category of a file/folder is higher than the confidentiality category of the drive, Secret Net Studio considers it incorrect and denies access to the file/folder.

On local drives, file system objects within folders with a category different from the category for public information (**Non-confidential** by default) are subject to inheritance. The confidentiality category of objects within a folder, is inherited in accordance with the inheritance features defined in the folder attributes.

New subfolders and files on local drives may be assigned a confidentiality level of the parent folder automatically by inheriting the level from that folder. A category is assigned automatically if the following features are enabled for a folder: **Automatically assign to new directories** and/or **Automatically assign to new files**. The user with the **Confidentiality category management** privilege can modify the features.

Files and folders located on connected devices from groups USB, PCMCIA, IEEE1394 and Secure Digital (external drives) are not assigned confidentiality categories individually. Such files and folders always inherit confidentiality categories from the devices where they are located.

Access levels and user privileges

Access levels

A user can access confidential information if the respective access level is assigned to this user. The set of user access levels in Secret Net Studio is the same as the set of confidentiality categories for resources (see above).

A user is allowed to access a resource if the user access level is not lower than the resource confidentiality category. For example, a user with the **Confidential** access level can read **Confidential** or **Non-confidential** category files, but the user cannot open **Strictly confidential** category files. The highest access level makes it possible to open files of any confidentiality category.

By default, all users are assigned the **Non-confidential** access level. For the description of the access level assignment procedure, see p. 141.

User privileges

MAC include user privileges listed in the following table:

Privilege	Description
Confidentiality category management	Allows the user: • to change confidentiality categories of folders and files within the user's access level; • to manage the confidentiality category inheritance mode for folders (see p. 142)
Printing confidential documents	Allows the user to print confidential documents. The privilege is applied when the **Print Control** function is enabled
Output of confidential information	Allows the user to output confidential information to external media when the flow control mode is enabled. External media in Secret Net Studio are removable disks that have the **Regardless of Confidentiality Category** access mode enabled

Privileges are granted by the security administrator to the users who are authorized to manage resource confidentiality settings, print and copy confidential information (see p. 141). By default, users are not granted these privileges.

Flow control mode

The flow control mode for confidential information ensures strict compliance with the principles of mandatory access control and prevents the unauthorized copying or moving of confidential data. This mode is disabled by default. For correct Secret Net Studio operation, additional configuring is required before enabling this mode. Basic setup is performed locally using a special program that is part of the Client.

Session confidentiality level

If the flow control mode is enabled, the option to use devices and access confidential files depends on the session's confidentiality level set during user login. A session level cannot be higher than the user access level. A session is finished when the user finishes the computer session. The session level cannot be changed before the session is closed.

When performing operations with resources, their confidentiality categories are compared to the session level. Access is granted if the resource confidentiality category is lower than or the same as the session level. Access to resources of a higher category is prohibited. All created, copied or modified documents are assigned the same confidentiality category as the session level.

For example, during logon, the user can select the **Confidential** session level which will deny access to strictly confidential resources, even if the required access level is granted. However, non-confidential documents that are copied or saved during a confidential session will become confidential after the operations are completed.

Due to the specific features of work during confidential sessions, all operations related to system configuration changes must be performed during non-confidential sessions with the flow control mode disabled. In particular, confidential sessions cannot be used for configuring software, changing mode or for initial user logon on a computer (when creating a user account). A session level other than **Non-confidential** should be selected only for working with confidential data.

Note. When using a Microsoft account in Windows 10 version of the year 2004 and with the flow control mode enabled, choosing a confidentiality level is only available on computers included in a domain.

Assigning a confidentiality level to a session

Depending on the configured parameters, a confidentiality level can be assigned to sessions manually by the user or automatically by the security system. A level is assigned automatically in the following cases:

- when the **strict control of terminal connections** parameter is enabled. This parameter defines the condition for the terminal session confidentiality level during terminal login. This level should be the same as the local session confidentiality level on the terminal client (the flow control mode should also be enabled on the client);
- when the **automatic selection of the session's maximum level** parameter is enabled. If the parameter is enabled, the same confidentiality level of the session as the user access level is forced.

Using devices and network interfaces

In the flow control mode, the use of devices with a confidentiality category that differs from the session level is prohibited. If at the moment of user login devices with different confidentiality categories are connected to the computer, access will be denied due to conflicts with the connected devices. In addition, login is prohibited if the confidentiality category of connected devices is higher than the user access level.

The flow control mode makes it possible to restrict the use of network interfaces. For each network interface, you can specify the confidentiality levels of sessions where the interface will be available for the user. If a session is opened with a confidentiality level that is not included in the list of allowed levels for a network interface, Secret Net Studio will block it.

Configuring mandatory access control

General configuration procedure

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

1. Set the number and names of confidentiality categories (see below).
2. Assign access levels and privileges to users (see p. **141**).
3. Assign confidentiality categories to resources (see p. **142**).
4. Configure the list of events to be registered (see p. **143**).
5. To add markers to documents during printing, enable the marking mode (see p. **88**).
6. To restrict the printing of confidential documents, configure the use of printers (see p. **143**).
7. To use the flow control mode, configure and enable the mode (see p. **143**).

You can find the latest recommendations given by developers for configuring the mechanism for working with applications in the Release Notes.

Before using this mechanism, explain the rules for working with confidential resources to users.

Configuring confidentiality categories

Attention! To avoid conflicts with confidentiality category names on computers with the Client in the network operation mode, the number and names of categories must be defined in a single general group policy applied to the computers. In the Control Center, we recommend you to configure one of the following group policies (listed in ascending order of parameter use priority):

- domain policy for all computers included in the domain;
- company unit policy for all computers associated with that unit;
- the Security Server policy for all computers connected to this Security Server.

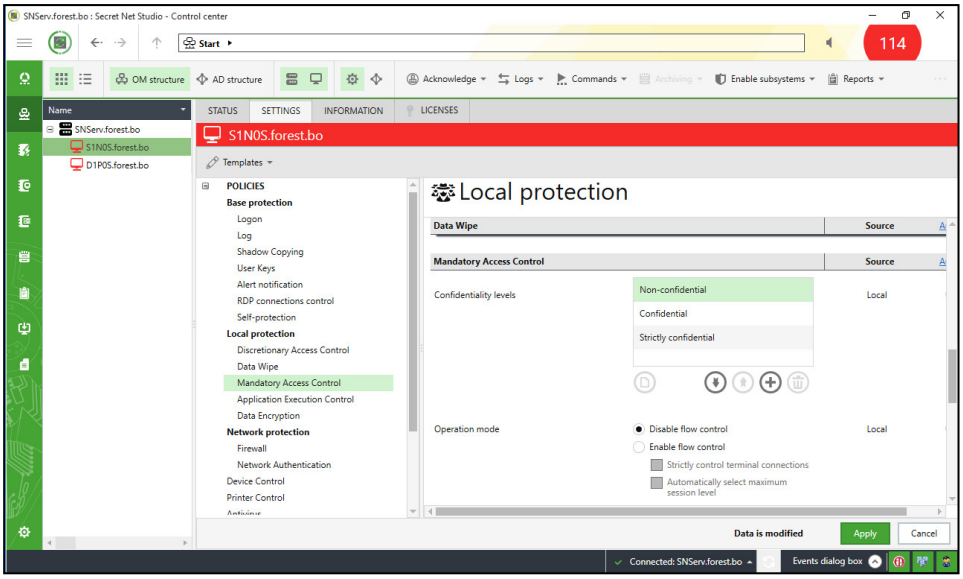
For example, all computers that are supposed to process confidential information can be included in a separate organizational unit and categories in that unit's policy can be configured.

The centralized configuration procedure when using the Control Center in the centralized mode is described below. Local configuration is performed the same way via the Control Center.

To configure the number and names of confidentiality categories:

1. In the Control Center, click the **Computers** panel and select the object you want to configure. Right- click the object and click **Properties** . In the **Properties** panel, select the **Settings** tab and click **Load Settings**.
2. In the **Policies** section, select **Mandatory Access Control**.

   A window with **Mandatory Access Control** group of parameters appears as in the figure below.



3. Create a list of confidentiality categories for the **Confidentiality level names** parameter. To add, delete or move elements, use the respective buttons under the list. To rename a category, double-click it. To restore categories, click **Default**.

   Note. The list is sorted based on the importance of categories in terms of data confidentiality. The lowest level (priority) is assigned to the first element of the list, while the highest level is assigned to the last element. New categories are placed at the end of the list. You can move them to the required position later. All categories can be removed, except for the first three elements of the list.

4. Click **Apply**.

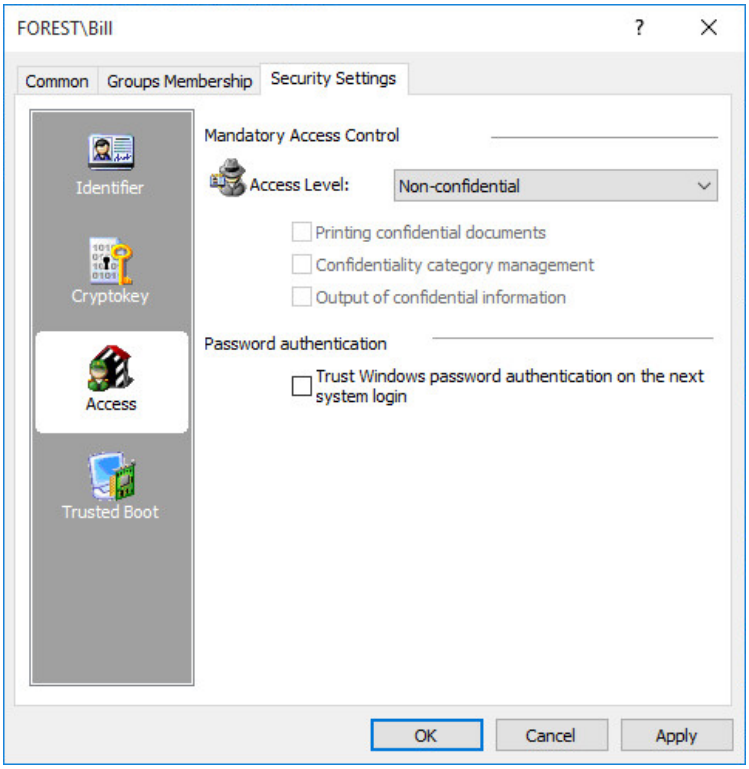
Assigning access levels and privileges to users

The security administrator assigns access levels and privileges to users.

A privilege can only be granted to those users who were assigned an access level.

To assign an access level and privileges:

1. Run the user management program (see p. 263).
2. Open the setup window for user properties and select the **Security Settings** tab.
3. Select the **Access** group.



4. From the drop-down list, select the user access level.

   For an access level that differs from the public information category (by default, **Non-confidential**), privilege assignment is unavailable.
5. To grant or cancel user privileges, select or clear the respective check boxes.
6. Click **OK**.

Note. Changes will take effect when the user logs on next time.

Assigning confidentiality categories to resources

A confidentiality category can be assigned to the following resources:

- devices for which access isolation is supported using MAC;
- folders and files.

Assigning confidentiality categories to devices

A confidentiality category can be assigned to local physical drives (except drives with a system logical partition) and any devices included in the USB, PCMCIA, IEEE1394 or Secure Digital device groups.

Confidentiality categories can be assigned:

- to each device individually;
- to a group, class or model in the device list for the categories to be inherited by new devices (only the public information category — **Non-confidential**).

To assign confidentiality categories to objects in the device list:

1. Load the device list (see p. 72).
2. Select the required list line (group, class, model or device).
3. Specify the required parameters in the cell of the **Access parameters** column. To do so, click the button in the right part of the cell. If you need to explicitly configure the parameters for that class or model, clear the **Use the category settings from a parent object for new devices** check box. To assign a confidentiality category, select the required category (a full list of categories is only provided for a specific device). If the device should operate regardless of the user access level, select **Without category**. Click **Apply**.

4. Click **Apply**.

Assigning confidentiality categories to folders and files

Confidentiality categories are assigned to resources by authorized users who are granted the Confidential category management privilege.

For information on changing confidentiality categories of folders and files, see document [**3**].

Attention! Follow the recommendations below when assigning confidentiality categories to resources :

- Do not assign a category other than the public information category (by default, **Non-confidential**) to system folders, application setup folders, the **My documents** folder and all similar folders.
- To avoid elevating file confidentiality categories by accident , store them in folders with the same confidentiality category assigned to the files. Take into account the confidentiality category of the device where the objects are located, because a device's category has a higher priority.

Configuring event registration

The event registration log must be configured in order to keep track of events occurring related to MAC. The configuration is performed using the Control Center. You can find the events, for which logging can be enabled or disabled, on the **Settings** tab of the object properties panel, in the **Event Registration** section, **Mandatory Access Control** group. To go to the required group of registration settings from the respective group of parameters in the **Policies** section (see p. **140**), click the **Audit** link.

Configuring the use of printers

If necessary, you can restrict the use of printers for printing documents that are assigned certain confidentiality categories. By default, a document with any confidentiality category can be printed on all printers.

You can assign confidentiality categories for specific printers or for the **Default Settings** element in the printer list.

Also, you can configure user rights for printing documents (see p. **86**).

To configure the use of printers:

1. Load the printer list (see p. **83**).
2. Select the required element in the list.
3. Specify the required parameters in the cell of the **Control parameters** column. To do so, click the button in the right part of the cell. Select the required confidentiality levels.
4. Click **Apply**.

Additional configuration of the flow control mode

Recommended configuration procedure

We recommend the following configuration procedure when using MAC the in the flow control mode:

1. Grant the security administrator permission to control MAC. To do this:
   - assign the account the highest level of access to confidential information and grant the **Confidentiality category management** privilege (see p. **141**);
   - add the security administrator in local groups of computer administrators.
2. Take the following steps on each computer:
   - create accounts for all users who will use the computer. The operating system automatically creates a user account during the first login (if the user has not logged into that computer before);

- start the applications that will be used and configure the application parameters;
- start the configuration program for the flow control mode (see p. **144**), enable the automatic setup mode for the required applications and perform the automatic setup procedure.

3. Set confidentiality levels for network interfaces (see p. **145**).
4. Enable the flow control mode (see p. **145**).
5. Make sure the applications operate correctly on computers in confidential sessions. In case of errors, configure joint operation with application software (see p. **146**).

Flow control mode configuration program

To ensure the operation of the Mandatory Access Control mechanism while the flow control mode is enabled, additional local settings are required on the computer. For this purpose, the flow control mode configuration program is used (hereinafter – the configuration program). The configuration is performed before enabling the flow control mode as well as during system operation when adding new users, programs, printers.

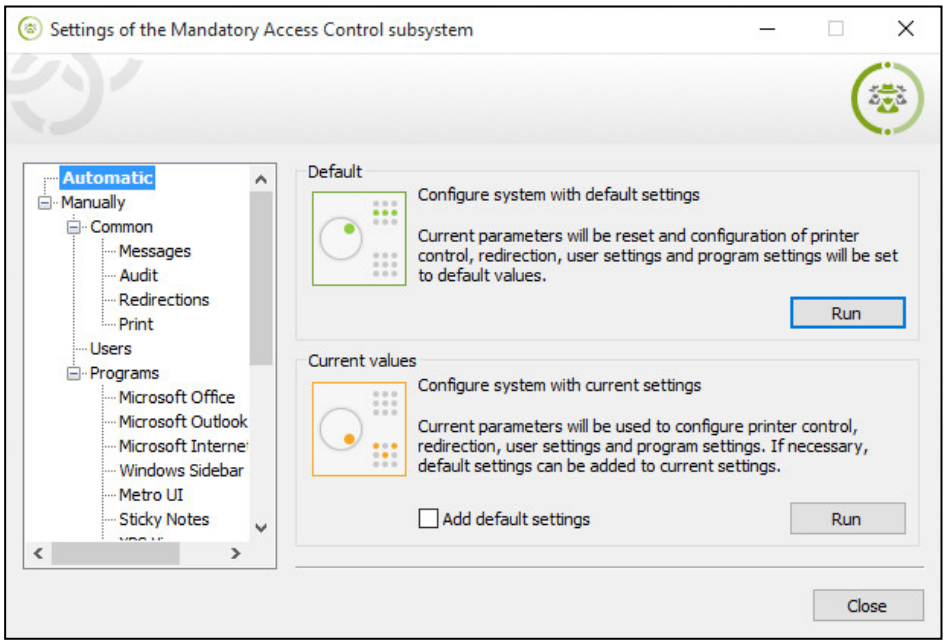
To start the configuration program, perform the actions corresponding to the version of the installed operating system:

1. Click **Start** and select **Settings of the Mandatory Access Control subsystem** in the program menu.

   If the **Administrator privileges control** function is enabled, a dialog box asking for an administrator PIN appears.
2. In the **Administrator PIN** field, enter PIN and click **OK**.

Note. The configuration program cannot be started in the following cases:
- if the current user is not included in the local group of administrators;
- if MAC is disabled.

The configuration program window appears as in the figure below.



The configuration program may operate in the normal mode, which provides all edition and configuration options or in the mode for viewing the current state of parameters (read-only mode). In the normal mode, the configuration program is started under the following conditions:

- the user is granted the highest level of access to confidential information;
- the user is granted the **Confidential Category Management** privilege;

- the flow control mode is disabled.

If one of the above conditions is not met, the configuration program can only be started in the read-only mode.

The configuration program provides the tools for both automatic and manual configuration. During automatic configuration, the basic procedure is performed, after which the mechanism operation and compatibility with standard and most commonly used software are ensured. Tools for starting the automatic configuration process are available in the configuration program window by default. Manual configuration is available to perform specific operations. For example, to use the configuration program with software that is not included in the list for automatic configuration.

For program operating instructions, see **Appendix** on p. **278**.

Selecting confidentiality levels for network interfaces

When configuring network interface parameters, you can select session confidentiality levels in which the interface will be available to users in the flow control mode.

To configure the use of interfaces in the flow control mode:

1. Load the device list (see p. **72**).
2. In the **Network** group, select the required list element (group, class or network interface).
3. Specify the required parameters in the cell of the **Access parameters** column. To do so, click the button in the right part of the cell. If you need to explicitly configure the parameters for that class or model, clear the **Use the category settings from a parent object for new devices** check box. Select the required confidentiality levels. If the device should operate irrespective of the session confidentiality level, clear check boxes for all levels. Click **Apply**.
4. Click **Apply**.

Enabling and disabling the flow control mode

To enable the flow control mode:

1. In the Control Center, open the **Computers** panel and select the object you want to configure. Right-click the object and click **Properties**. In the properties panel, select the **Settings** tab and click **Load settings**.
2. In the **Policies** section, select **Mandatory Access Control**.
3. In the **Operation mode**, select the **Flow control enabled** check box and, if necessary, configure the parameters of automatic assignment of confidentiality levels for user sessions:
   - to restrict the confidentiality level options for terminal connections — select the **Strict control of terminal connections** check box. In this case, the confidentiality level of the terminal session will equal the confidentiality level of the local session on the terminal client (respectively, the flow control mode should be enabled on the Client);
   - to enabled forced assignment of the highest possible confidentiality levels to user sessions — select the **Automatic selection of the session's maximum level** check box. In this case, the session will be assigned the same confidentiality level as the access level of the user who logs in.
4. Click **Apply**.

To disable the flow control mode:

1. Log in using a non-confidential session.
2. Complete steps **1**, **2** of the procedure described above.
3. Select the **Flow control enabled** check box for the **Operation mode** parameter.

4. Click **Apply**.

Configuring joint operation with applications

When MAC operates in the flow control mode, some applications may fail to start or operate. If such failures only occur when working with the application during confidential sessions, they may be caused by the prohibition to run the application files.

To ensure correct operation of applications in the flow control mode, a redirection function for service file output is available. To use this function, copies of certain service directories of applications with various confidentiality levels are created. Depending on the session confidentiality level, file operations of the application software are automatically redirected to a copy of a directory with the respective confidentiality category. Therefore, it becomes possible for the application to work with service directories, while data is saved with the required confidentiality category.

If an application stops working correctly after enabling the flow control mode, take the following steps to troubleshoot and configure the joint operation:

1. Check the availability of a prepared template for configuring the application. To do this, run the configuration program (see p. 144) and go to the **Manually > Programs** section. If the application is on the list, enable the automatic configuration mode and apply the automatic configuration using the current parameter values. If the application is not on the list, go to other troubleshooting and configuration procedures.

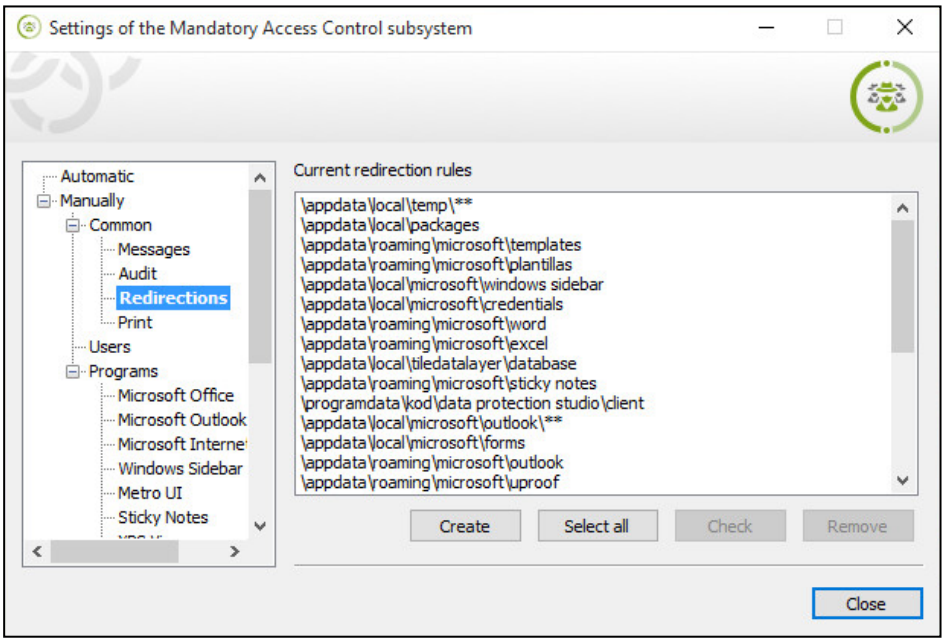
   Note. The list of applications in the configuration program is designed for applying templates for configuring joint operation. By default, the automatic configuration mode is disabled for most elements of the list (for example, for AutoCAD, Photoshop and other software products). Therefore, enable this mode to apply a template. For the configuration program operating instructions, see **Appendix** on p. 278.

2. Log in with the flow control mode disabled or using a non-confidential session. Run the Control Center locally and clear the Secret Net Studio local log.
3. Close the session, enable the flow control mode and log in using a confidential session.
4. Run the application. If the application starts successfully, reproduce the operations that resulted in the software errors.
5. Close the session, log in using a non-confidential session and disable the flow control mode.
6. Run the Control Center locally and load the log records. Find records related to prohibited access for the **Mandatory Access Control** category. By viewing the additional event descriptions, define the processes related to the application and paths that are used for calls.
7. Analyze the paths and, if possible, classify them based on the designation of directories. Directories where failures may occur when calling files:

Directories containing user documents
Contain user document files. For example, the **\Documents** directory in the user account. Probable causes of access denial: general recommendations on the assignment of categories to directories and files are not followed (see p. 143) or rules for confidential resource handling are applied (see p. 148). Redirection is not recommended for such directories. To ensure access, correct resource confidentiality categories should be assigned (directory categories should match the categories of files stored in them)

Temporary application data directories
The directories are used by applications to write and read temporary data during a working session The created files are usually deleted once the session is closed. Probable causes of access denial: there is an attempt to create a file in the directory with a confidentiality category lower than the session's level. In most cases, no redirection is required for such directories. It is enough to assign the maximum confidentiality category without automatic assignment of a category for created objects. Due to this, the application will be allowed to create files during sessions with any confidentiality level
Directories containing application configuration parameters
The directories contain configuration files that are created when the application is started for the first time; these files are not modified later if the application operates in the normal mode. Read-only access to such files during all other sessions is allowed for loading application parameters. Probable causes of access denial: there is an attempt to create or modify configuration files in a directory that was created when configuring the application parameters. In most cases, no redirection is required for such directories. If you need to modify configuration files, configure the application using a non-confidential session.
Directories containing application's operational data
The directories are used by application to read and write service data during each session. Files are not removed after the session is closed and can be rewritten during later sessions. Correct file handling in such directories is ensured by the redirection function (see below)

8. To create redirection rules, start the configuration program and go **Manually > Common > Redirections**.



Click **Create** to add rules. Each redirection rule should contain a part of the path that identifies the redirection directories. For example, **\AppData\Local\Temp** is the temporary directory in the user account. All directories whose path partially matches the specified value will be redirected during confidential sessions. In the above example, the rule ensures redirection of temporary directories (with all their contents) of all computer users.

Recommendations on creating the redirection rule list

- If possible, do not select the directories containing a lot of data for redirection. When configuring redirection from source directories, you can copy only subfolders without files or nested files without directories instead of duplicating the whole data. This type of copying will be performed if the redirection rule contains the ** template substring (two asterisks) or the * substring (one asterisk), respectively.
- The path section in the redirection rule should be set with optimal accuracy to identify the directories. Usually, it is enough to specify two-three nested levels. If the specified path part is too short, this may result in redirecting directories that are not related to the required application. If the specified path part is too detailed, more rules may need to be created (for example, for each user). This will make configuring more difficult and affect the subsystem's data processing speed.

9. Enable the flow control mode, log in using a confidential session and make sure the application is operating correctly. If the application will be used on computers with the flow control mode enabled, configure the use of these directories locally (see steps **7**, **8**).

Confidential resource handling rules

This section covers rules for confidential resource handling when the **Mandatory Access Control** mode is enabled. The table below lists the rules that apply when the flow control mode is enabled and disabled.

Disabled flow control	Enabled flow control
Access to devices	
User access to the system is not allowed if connected devices have a confidentiality category higher than the user's access level	User access to the system is not allowed if the following devices are connected: • devices with a confidentiality category higher than the user access level; • devices with different confidentiality categories; • devices with a confidentiality category higher than **Non-confidential** during initial user entry on the computer (configuration entry)
A device cannot be connected if its confidentiality category is higher than the current user's access level	A device cannot be connected if its confidentiality category differs from the current user's session level
All network interfaces can be used	Network interfaces cannot be used if their current session confidentiality level is not specified in the list of allowed levels
There are no access restrictions to devices if the **device is available regardless of confidentiality categories** mode is enabled for them	
Access to files	
If a confidentiality category is assigned to a file-containing device, the system considers the file's category the same as the device's category when accessing the file (irrespective of the file system type). It is prohibited to change a file's confidentiality category	
Access to a file is prohibited if its confidentiality category is higher than the category assigned to the file-containing device	
Users can access the file if their access level is not lower than the file's confidentiality category	Users can access the file if the user session confidentiality level is not lower than the file's confidentiality category
It is not allowed to delete a confidential file to the Recycle Bin	It is not allowed to delete any file to the Recycle Bin
Access to folders	
If a confidentiality category is assigned to a folder-containing device, the system considers the folder's category the same as the device's category when accessing this folder (irrespective of the file system type). It is prohibited to change a confidentiality category of the folder	

Disabled flow control	Enabled flow control
Access to a folder is prohibited if its confidentiality category is higher than the category assigned to the folder-containing device	
Confidential files are placed in folders with a confidentiality category not lower than the file's confidentiality category. For example, a folder with the confidential category can contain both non-confidential files and files with the confidential category	
A user without access to a file can view the contents of the confidential folder that contains the file, but cannot open the file. Therefore, no confidential information should be contained in confidential file names	
It is not allowed to delete a confidential folder to the Recycle Bin	It is not allowed to delete any folder to the Recycle Bin
Inherit the folder confidentiality category	
If automatic confidentiality category assignment mode is enabled when creating, saving (re-writing), copying, or moving a subfolder/file to a folder, it is assigned a folder confidentiality category	If automatic confidentiality category assignment mode is enabled when creating, saving, copying, or moving a subfolder/file to a folder, it is assigned a directory confidentiality category. Restriction: The assigned confidentiality category must be equal to the current session's confidentiality level
If automatic confidentiality category assignment mode is disabled: • when creating, saving, or copying a subfolder/file, it is assigned non-confidential category; • when moving a subfolder/file within a logical partition, it retains its confidentiality category (the file can be moved if its confidentiality category is not higher than the confidentiality category of the upper-level folder). The appropriate user privilege is required to move subfolders	If automatic confidentiality category assignment mode is disabled: • when creating, saving, or copying a subfolder/file, it is assigned the same category as the session's confidentiality level, but not higher than the folder's confidentiality category; • when moving a subfolder/file within a logical partition, it retains its confidentiality category (the subfolder/file can be moved if its confidentiality category is not higher than the folder's confidentiality category or the session's confidentiality category)
Folders where automatic confidentiality category assignment is disabled should be used when storing files with different confidentiality categories (lower than or equal to the folder's confidentiality category). To avoid accidentally changing file confidentiality categories when performing operations with them, we recommend using folders with the same mode of automatic category assignment	
Working with applications	
An application is assigned the highest confidentiality category assigned to the files opened in it. The application's confidentiality level does not become lower after the confidential file is closed; it is retained until the application is closed	The application is assigned the confidentiality level of the current user session. Only files with the same or lower confidentiality category can be opened. The category of files with a lower confidentiality level is elevated to the session's confidentiality level (the higher category is assigned when saving the file)
When some applications start, they automatically access certain files. For example, files that were previously opened in the application. However, the file (document) is not actually opened. A specific feature of the Mandatory Access Control mechanism is that when interacting with confidential files in this manner, the user is prompted to elevate the application's confidentiality level to the file confidentiality level. If you do not intend to use the suggested confidentiality level, you can simply decide not to elevate the application's confidentiality level	
Changing the confidentiality category of a resource	

Disabled flow control	Enabled flow control
A user who is **not** granted the **Confidentiality category management** privilege cannot elevate a file's confidentiality category higher than its own access level (however, a file's confidentiality category can only be elevated if its category is lower than the directory's confidentiality category)	A user who is **not** granted the **Confidentiality category management** privilege cannot elevate a file's confidentiality category higher than the session's confidentiality category (however, a file's confidentiality category can only be elevated if its category is lower than the directory's confidentiality category)
A user granted the **Confidentiality category management** privilege can: • elevate the confidentiality category of directories and files within the user's access level; • assign a lower confidentiality category to directories and files with a current confidentiality category, but not higher than the user's access level; • change the automatic confidentiality category assignment mode for a directory if the directory current confidentiality category is not higher than the user's access level	A user granted the **Confidentiality category management** privilege can: • elevate the confidentiality category for directories and files, but not higher than the current session's level; • assign a lower confidentiality category to directories and files with a current confidentiality category not higher than the current session's level; • change the automatic confidentiality category assignment mode for a directory if the directory current confidentiality category is not higher than the current session's level
Printing confidential documents	
If the Print Control mechanism is enabled: • a user **not** granted the **Printing confidential documents** privilege can only print non-confidential documents; • a user granted the **Printing confidential documents** privilege can print confidential documents with a confidentiality category not higher than the user's access level	If the Print Control mechanism is enabled: • a user **not** granted the **Printing confidential documents** privilege can only print non-confidential documents (as long as the document has not been edited); • a user granted the **Printing confidential documents** privilege can print confidential documents with a confidentiality category not higher than the current session's level
If the Print Control mechanism is disabled, any user with access to confidential documents can print the documents, irrespective of whether the user has the **Printing confidential documents** privilege or not. Moreover, the documents will be printed without the confidentiality mark	
Output to external media	
A user who has access to confidential documents can copy files or save their contents to any media, irrespective of the **Output of confidential information** privilege	A user **not** granted the **Output of confidential information** privilege cannot copy confidential files or save their contents to external media

Chapter 12
Discretionary Access Control

You can perform the following operations when configuring the discretionary access control for:

1. Granting permission to modify rights to access any resources.
2. Assigning the resource administrator.
3. Configuring event logging and audit of resource operations.

Granting privileges to modify rights to access resources

The discretionary access control mechanism supports changing access rights for any folders and files on local disks, regardless of the rights to access the resources for privileged users. To do this, a user should be granted the Access rights management privilege. This privilege makes it possible to assign resource administrators, who will be able to configure access rights to resources for other users.

By default, the privilege to control access rights is granted to users included in the local group of administrators.

The centralized configuration procedure when using the Control Center in the centralized mode is described below. Local configuration is performed in the same way via the Local Control Center.

To grant the privilege:

1. In the Control Center, open the **Computers** panel and select the object you want to configure. Right-click it and click **Properties**. In the properties panel, select the **Settings** tab and click **Load Settings**.
2. In the **Policies** section, select **Discretionary Access Control**.
3. In the **Discretionary Access Control** section, click **Add**, edit the list of users and user groups who are granted the privilege.
4. Click **Apply** at the bottom of the **Settings** tab.

Assigning the resource administrator

Within the **Discretionary Access Control** mechanism, resource administrators can modify access rights of other users regarding certain folders and files on local disks. A resource administrator is a user who is granted the **Access rights change** permission in the resource access parameters. The procedure for changing access rights is described in document [**3**].

Configuring event logging and audit of resource operations

Changing the list of logged events

The event registration must be configured in order to track events related to the **Discretionary Access Control**. The configuration is performed in the Control Center. You can find the events, for which logging can be enabled or disabled, on the **Settings** tab of the object properties panel, in the **Event logging** section, **Discretionary Access Control** group. To go to the required group of registration settings from the respective group of parameters in the **Policies** section (see p. **151**), click the **Audit** link in the right part of the group heading.

Configuring success and failure audit

Audit parameters for resource operations are configured when access rights to that resources are modified.

Chapter 13
Disk Protection

Access to computer local disks (logical partitions) is protected by the disk protection mechanism. The mechanism blocks access to disks in case of an unauthorized OS boot. An OS boot is considered authorized if it is performed by the OS with the Client installed. All other ways to boot an OS are considered unauthorized in terms of the mechanism's operation (for example, booting from an external drive or booting another OS installed on the computer).

The setup procedure for the disk protection mechanism includes the following steps:

1. Enabling the mechanism (see below).
2. Enabling/disabling logical partition protection (see p. **153**).

Instructions on how to disable the disk protection mechanism are given on p. **154**.

You can recover data on the disks protected by the disk protection mechanism using an emergency recovery disk (see p. **288**).

Enable Disk Protection

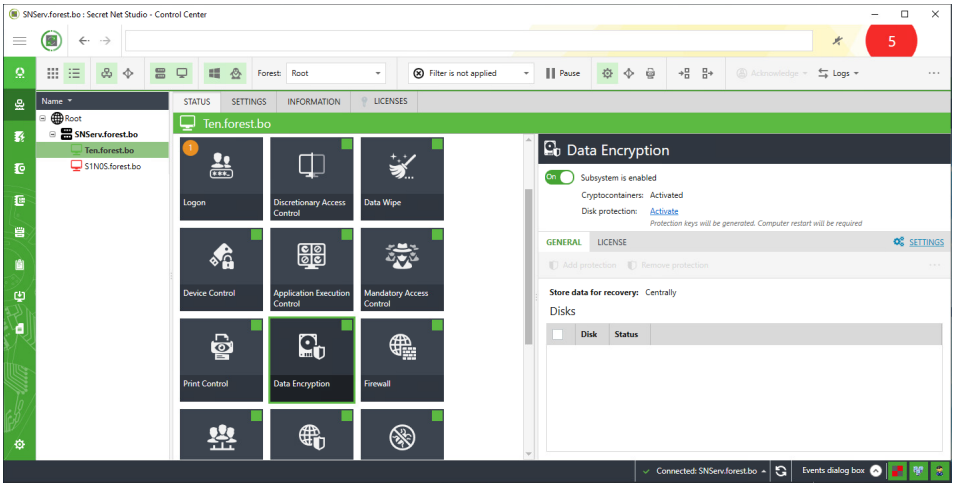
By default, once the Client is installed and the license is registered, the Disk Protection mechanism is disabled. The mechanism is enabled by the administrator.

When enabling the mechanism, a recovery file is generated. It contains a special key which is the basis for future modification of boot sectors of logical partitions on the computer's hard disks. It is mandatory to generate a new recovery file when the mechanism is enabled for the first time. If the centralized mode of recovery data storage is enabled, the file is stored on the Security Server. If the centralized mode is disabled, the recovery file can only be created on the local computer, an external drive or a network resource — then it can be easily copied. If the centralized mode is disabled, the recovery file is created on the local computer.

Attention! If the system drive (the physical disk from which the operating system is started) uses the Master Boot Record (MBR), the boot virus check function must be disabled in the computer's BIOS settings. To disable the function, set the **Disabled** value for the **Boot Virus Detection** parameter (availability of this function and the parameter name depend on the BIOS version).

To enable the disk protection mechanism centrally:

1. In the Control Center, open the **Computers** tab and select an object the parameters of which you need to modify. Right-click the object and click **Properties**. In the properties panel, open the **Settings** tab and load settings from the Security Server.
2. In the **Policies** section, select the group of parameters **Recovery data storage/ Recovery data storage for system and non-system partitions**. Select the **Centralized storage** check box.
3. Open the **Status** tab and click the **Data Encryption** tile. On the right, the information about the mechanism appears.

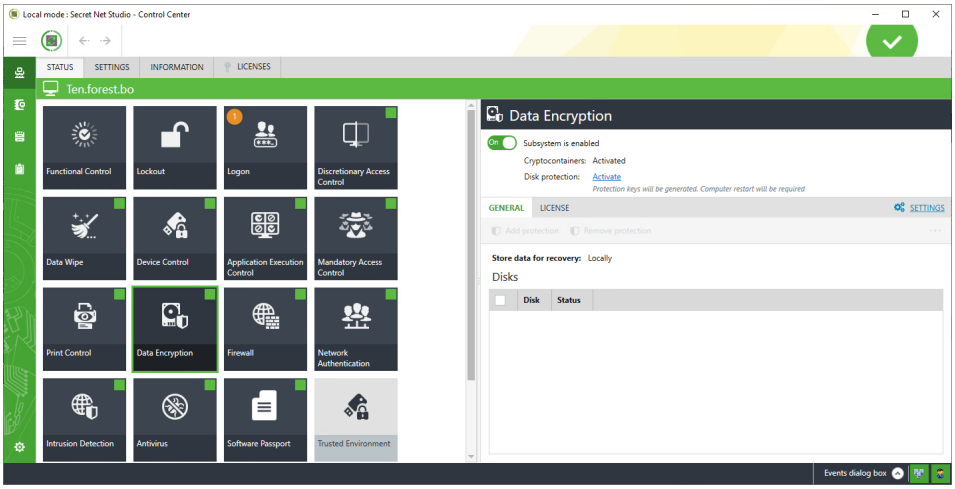


In the **Disk protection** field, click **Activate**.

4. Once the mechanism is enabled, reboot the computer and wait until the OS is loaded.

To enable the disk protection mechanism locally:

1. Open the **Status** tab and click the **Data Encryption** tile. On the right, the information about the mechanism appears.



In the **Disk protection** field, click **Activate**.

2. Once the mechanism is enabled, reboot the computer and wait until the OS is loaded.

   When the mechanism is run for the first time, after the OS boot-up, a dialog box prompting you to specify the path to the recovery file appears.

3. Specify the path to the required file and click **Finish**.

Enable and disable logical partition protection

By default, once the Disk Protection mechanism is enabled, protection is disabled for all logical partitions. You can selectively enable protection for required partitions.

This mechanism can protect up to 128 logical partitions with up to 32 physical disks. Logical partitions to be protected must use the FAT, NTFS or ReFS file system. The mechanism supports MBR and GPT partition styles. Disks with other partition styles are not supported (for example, dynamic disks).

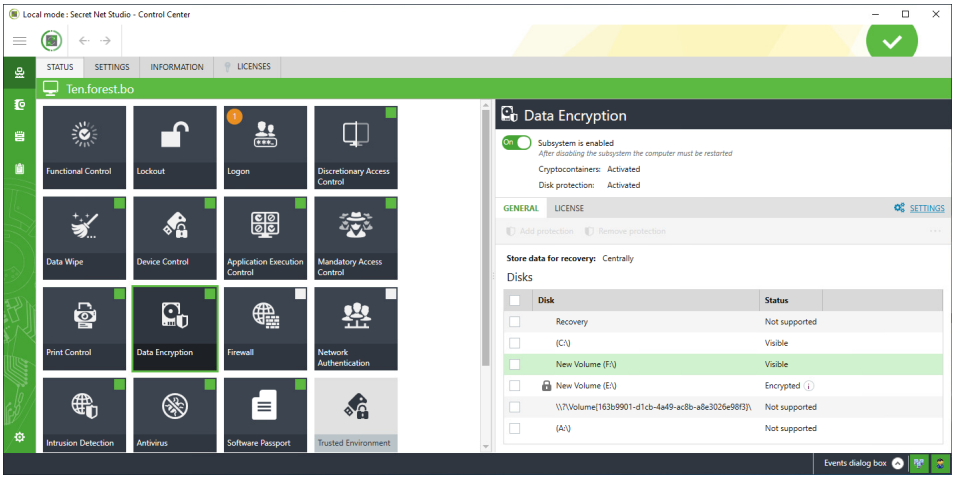
The procedures for enabling/disabling the logical partition protection via the Control Center are described below. To enable/disable partition protection locally, use the Local Control Center.

Note. To enable/disable disk protection centrally, you must disable the centralized mode of recovery data storage (see p. 152).

To enable/disable protection:

1. In the Control Center, open the **Computers** tab and select a computer where you need to configure settings. Right-click the object and click **Properties**. On the properties panel, open the **Status** tab and select the **Data Encryption** tile.

   On the right, you can see a list of disks available to be protected.



2. Select the required logical partitions and click **Add protection**. If you need to disable protection for a logical partition, clear the check box from the left of its name and click **Remove protection**.

Disable the disk protection mechanism

Before disabling the disk protection mechanism, you must disable protection for all logical partitions. In this case, the key is not removed from the system and can be used on this computer again. The procedure of disabling the disk protection mechanism using the Control Center is described below. To disable the disk protection mechanism locally, use the Local Control Center.

To disable the disk protection mechanism:

1. In the Control Center, open the **Computers** tab and select an object the parameters of which you need to modify. Right-click the object and open the **Properties** panel. On the properties panel, open the **Status** tab and select the **Data Encryption** tile. On the right, the information about the mechanism appears.
2. Turn off the toggle. The mechanism will be disabled and **The computer must be restarted** message appears.
3. After the mechanism is disabled, restart the computer.

Chapter 14
Full Disk Encryption

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

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

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

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

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

- encryption key — a key for encrypting data on disks;
- security domain key — a key for encrypting data to recover access to encrypted disks (hereafter – recovery data);

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

You can start Full Disk Encryption operations:

- locally on your computer using Secret Net Studio Encryption and disk protection program (hereafter – encryption wizard);
- locally on your computer using the Local Control Center;
- centrally for one or several computers using the Control Center.

Data encryption is available for users and user groups, for whom the privilege to encrypt is granted.

When you turn on the Full Disk Encryption subsystem, Secret Net Studio bootloader is installed on the computer. If there are encrypted disks on your computer, Secret Net Studio bootloader starts and you are prompted to enter the password for the disks. Disk access recovery operations become available as well.

Note.
- For more details about the features and limitations of Full Disk Encryption subsystem, see document [**1**] (**Full Disk Encryption** section).
- For instructions on how to work with encrypted disks, see document [**3**] **Full Disk Encryption** section).

Configure encryption settings

Data encryption is available for users and user groups for whom the privilege to encrypt disks is granted.

The privilege of local encryption is granted in the Control Center (centralized configuration) or in the Local Control Center (local configuration) by the administrator who has the privilege to edit policies.

The Full Disk Encryption settings are configured in the Control Center (centralized configuration) or in the Local Control Center (local configuration). The administrator configuring these settings must be granted the privilege to edit policies.

Below you can see the description of procedures on how to grant the privilege of local encryption and configure the settings centrally. The local procedures are similar to them.

To grant the privilege of local encryption:

1. In the Control Center, select the **Computers** panel and select the object for which you want to configure the settings. Right-click the object and select **Properties**. Select the **Settings** tab and load the settings from the Security Server.
2. In the **Policies** section, go to the **Full Disk Encryption** group of settings.
3. Edit the list of users and user groups for whom the privilege of encryption is granted, using the parameter **Accounts with the privilege to encrypt local partitions of hard drives**.

   The users who are in the local **Administrators** group have this privilege by default.

To configure encryption settings:

1. In the Control Center, select the **Computers** panel and select the object for which you want to configure the settings. Right-click the object and select **Properties**. Select the **Settings** tab and load the settings from the Security Server.
2. In the **Policies** section, go to the **Full Disk Encryption** group of settings.
3. Configure the mode of system and non-system disk encryption by setting one of the following values to the parameters **System partition encryption** and **Non-system partition encryption**:
   - **Defined by the user** (default value) — a user can encrypt and decrypt partitions themselves using the encryption wizard.
   - **Encrypt** — partitions will be encrypted forcibly with the respective notification on the computer. Local decryption is forbidden.
   - **Do not encrypt** — earlier encrypted partitions will be decrypted forcibly with the respective notification on the computer. Local encryption if forbidden.
4. If necessary, configure the storage mode for recovery data on the Security Server. To do so, in the **Policies** section, go to the **Store recovery data** group and select the **Store centrally** check box for the parameter **Store recovery data for system and non-system partitions**.

   Note.
   - The policy is available for Clients in network mode.
   - If you switch the computer to the standalone mode, recovery data will be stored locally. The policy must be disabled.
   - The policy applies to the Disk protection mechanism as well.
5. Click **Apply**.

Enable Full Disk Encryption subsystem

After Secret Net Studio Client is installed, and the license is registered, the Full Disk Encryption subsystem is disabled by default. The administrator, whom is granted the privilege to enable/disable Secret Net Studio subsystems, can enable the subsystem.

Note. You can disable the subsystem unless there are no encrypted disks.

The instruction on how to enable the subsystem centrally via the Control Center is given below. You can enable the subsystem locally in the same fashion via the Local Control Center.

To enable the subsystem:

1. In the Control Center, select the **Computers** panel and select the object for which you want to enable the subsystem. On the **Status** tab, select **Full Disk Encryption**.
2. Set the toggle **Subsystem is enabled** to **ON**.

A warning about the computer restart appears.

3. Restart the computer.

   While restarting, Secret Net Studio bootloader is being installed. If Secret Net Studio bootloader has been successfully installed, the subsystem will be enabled.

   When enabling the subsystem, error may occur if the computer does not meet the requirements. The requirements for the Full Disk Encryption subsystem are given on p. **155**.

Note. You can enable the subsystem centrally in the table view of the CO structure. Right-click the required computer and select **Enable subsystems > Full Disk Encryption > Enable**.

Data encryption and decryption

This section contains information on the following procedures:

- local decryption in case of local storage of recovery data (see p. **157**);
- local decryption in case of centralized storage of recovery data (see pp. **159**);
- local decryption via the encryption wizard (see p. **160**);
- encryption and decryption in the Control Center (see p. **161**).

Local encryption in case of local storage of recovery data

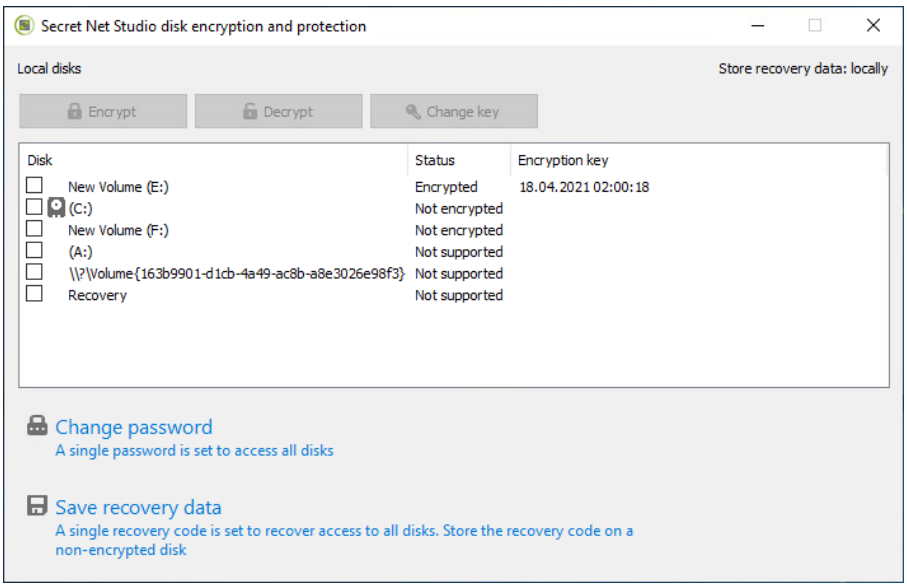
Local encryption is performed using the Secret Net Studio disk encryption and protection wizard on a computer with disks you want to encrypt. The user, encrypting disks, must be granted the privilege to encrypt disks (see p. **155**).

If necessary, you can save the recovery file required for creating an emergency recovery disk. The emergency recovery disk makes it possible to restore access to encrypted partitions. The file contains all the information required for the full restoration of access in case the password was lost or the drive was corrupted.

To encrypt disks:

1. Right- click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

   The Secret Net Studio disk encryption and protection wizard appears as in the figure below.



Note. You can launch the encryption wizard from the context menu of a disk. In **Encryption**, select **Encrypt** and go to step **4** of this instruction.

2. Select the disk you want to encrypt.

Note.
- You can encrypt several disks simultaneously. All computer disks are encrypted with the same password.
- The system disk is shown as .
- A disk with the status **Not supported** cannot be encrypted. For the requirements for disks supported by the Full Disk Encryption subsystem, see p. 155.

3. Click **Encrypt**.

   A dialog box prompting you to enter the password appears.

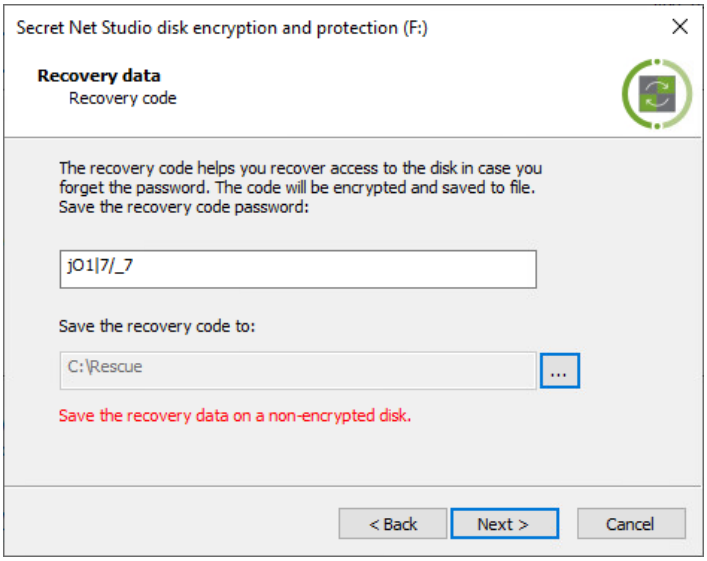
4. Set a password to access the disk or enter a password for earlier encrypted disks.

   Note. The password must meet the requirements shown in the password request dialog box.

   If necessary, select the **change password at the first access to encrypted disks** check box. In this case, the user must change the password at the first boot of the system with encrypted disks.

5. Click **Next**.

   The dialog box to save the recovery code appears as in the figure below.



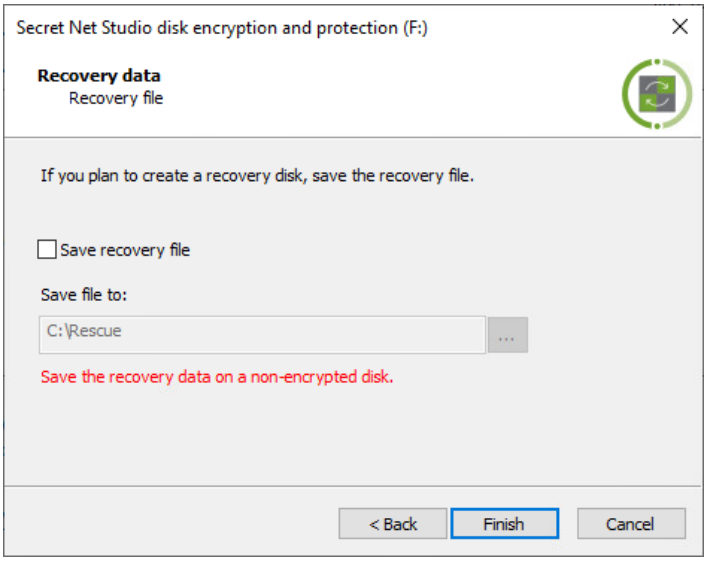
6. Save the system-generated password for the recovery code. Specify the path to save the recovery code.

   Attention! Save the recovery data onto a disk different from the encrypted one.

   Note. You can save the recovery code for a second time later on (see p. 167).

7. Click **Next**.

   The dialog box to save the recovery file appears as in the figure below.



8. If necessary, select the check box **Save recovery file** and specify the path to save the recovery file.

Attention!
- The recovery file which you are asked to save at this stage becomes obsolete once the encryption has started. We recommend you to create a recovery file manually after the encryption process has finished (see p. 167, p. 169).
- Save the recovery data onto a disk different from the encrypted one.

9. Click **Finish**.

   The encryption process begins. You can follow the process in the appeared window.

Attention! During the encryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note.
- To pause the process, click **Pause**. The encryption process will be paused until you click **Resume**.
- To cancel the process, click **Cancel**. The disk will not be encrypted.
- During the encryption, you can restart the computer from the Windows Start menu. After the restart, the Secret Net Studio bootloader window appears. You need to enter the password to access encrypted disks. After logging on to an OS, the encryption process resumes.

The respective message will appear once the process has finished. The disk will be assigned the status **Encrypted** in the encryption wizard. In the Control Center, on the **General** tab of the **Full Disk Encryption** element, you can now see information about the encrypted partition.

Local encryption in case of centralized storage of recovery data

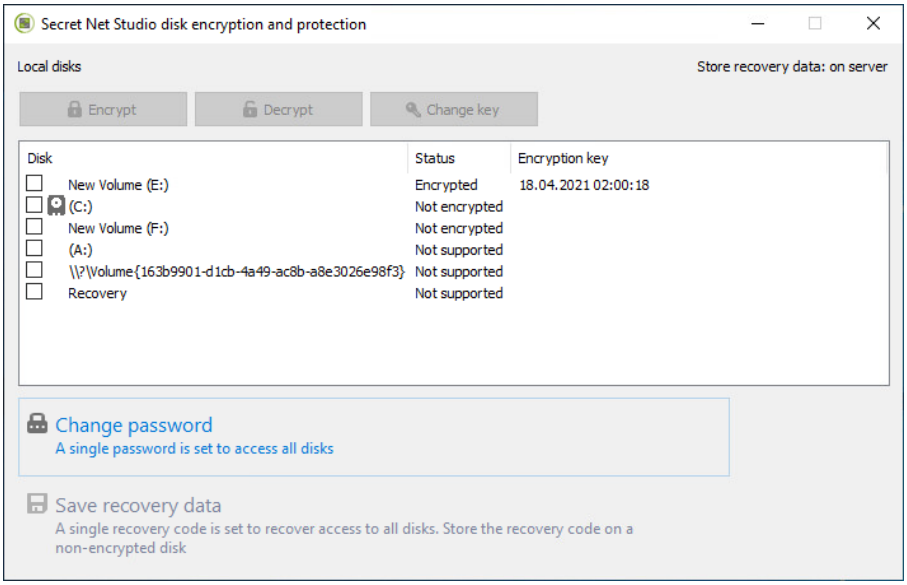
For centralized storage of recovery data, enable the respective setting in the Control Center or in the Local Control Center (see p. 155).

Local encryption is performed using Secret Net Studio encryption wizard on a computer with disks you want to encrypt. The user, encrypting disks, must be granted the privilege to encrypt disks (see p. 155).

To encrypt disks:

1. Right- click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

   The Secret Net Studio disk encryption and protection wizard appears as in the figure below.



Note. You can launch the wizard from the context menu of a disk. In **Encryption**, select **Encrypt** and go to step **4** of this instruction.

2. Select the disk you want to encrypt.

Note.
- You can encrypt several disks simultaneously. All computer disks are encrypted with the same password.
- The system disk is shown as .
- A disk with the status **Not supported** cannot be encrypted. For the requirements for disks supported by the Full Disk Encryption subsystem, see p. 155.

3. Click **Encrypt**.

A dialog box prompting you to enter the password appears.

4. Set a password to access the disk or enter a password for earlier encrypted disks.

Note. The password must meet the requirements shown in the password request dialog box.

If necessary, select the check box **change password at the first access to encrypted disks**. In this case, the user must change the password at the first boot of the system with encrypted disks.

5. Click **Finish**.

The encryption process begins. You can follow the process in the appeared window.

Attention! During the encryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note.
- To pause the process, click **Pause**. The encryption process will be paused until you click **Resume**.
- To cancel the process, click **Cancel**. The disk will not be encrypted.
- During the encryption, you can restart the computer from the Windows Start menu. After the restart, the Secret Net Studio bootloader window appears. You need to enter the password to access encrypted disks. After logging on to an OS, the encryption process resumes.

The respective message will appear once the process has finished. The disk will be assigned the status **Encrypted** in the encryption wizard.

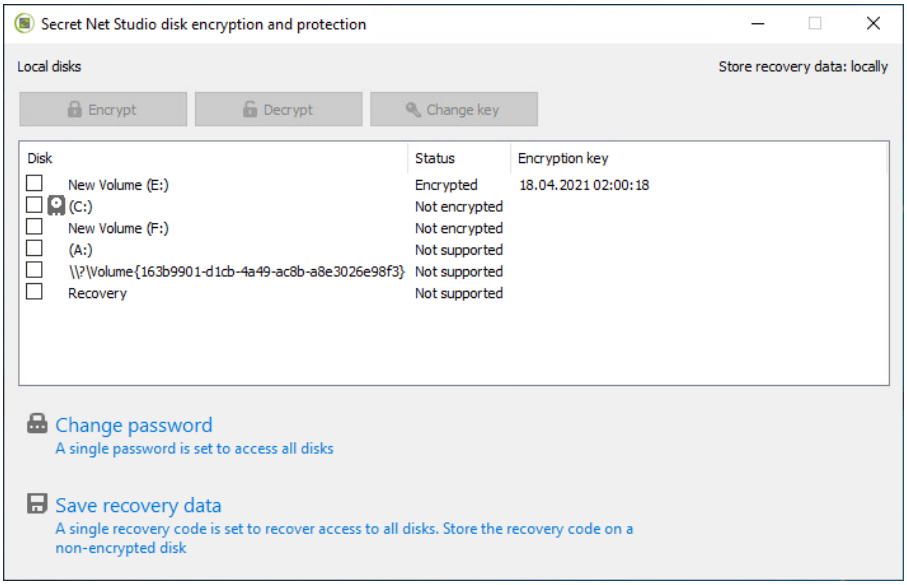
Local decryption

You can decrypt disks locally using Secret Net Studio encryption wizard on a computer with disks you want to decrypt. The user, decrypting disks, must be granted the privilege to encrypt disks (see p. 155).

To decrypt disks:

1. Right- click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

   The Secret Net Studio disk encryption and protection wizard appears as in the figure below.



   Note. You can launch the wizard from the context menu of a disk. In **Encryption**, select **Decrypt** and go to step **4** of this instruction.

2. Select the disk you want to decrypt.

   Note.
   - You can decrypt several disks simultaneously.
   - The system disk is shown as .

3. Click **Decrypt**.

   A dialog box prompting you to enter the password appears.

4. Enter the password for the disk.

5. Click **Finish**.

   The decryption process begins. You can follow the process in the appeared window.

   Attention! During the decryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

   Note.
   - To pause the process, click **Pause**. The decryption process will be paused until you click **Resume**.
   - To cancel the process, click **Cancel**. The disk will not be decrypted.
   - During the decryption, you can restart the computer from the Windows Start menu. After logging on to an OS, the decryption process resumes.

   The respective message will appear once the process has finished. The disk will be assigned the status **Not encrypted** in the encryption wizard.

Encryption and decryption in the Control Center

Centralized encryption is available for computers with Secret Net Studio in standalone and network modes. When starting on a standalone computer, its disks will be encrypted. In network mode, you can start the procedure for one or several computers.

The procedure can be performed when storing recovery data locally or centrally.

You can start centralized encryption in the Control Center or in the Local Control Center. If you start the encryption procedure, you must have the privilege to encrypt disks (see p. 155) and edit policies.

A respective notification appears on computers for which encryption is started. Depending on recovery data storage mode, do the following:

- if the centralized storage mode is in use, specify the password to access the disks;
- if the local storage mode is in use, specify the password to access the disks, as well as data recovery storing settings.

Note. For more details about computer events and user actions, see document [3].

For centralized storage of recovery data, enable the respective setting in the Control Center or in the Local Control Center (see p. 155).

For the instruction on how to start centralized encryption in the Control Center, see below. The instruction on how to start local encryption in the Local Control Center is similar to the described one.

To encrypt/decrypt an object:

1. In the Control Center, select the **Computers** panel and select the object which you want to encrypt. Right-click the object and click **Properties**. Select the **Settings** tab. In network mode, load the settings from the Security Server.

   Note. If the Security Server is selected, a group policy will be applied and encryption will start on all the computers with the Full Disk Encryption subsystem enabled and subordinate to this Security Server.

2. In the **Policies** section, go to the **Full Disk Encryption** group of settings.
3. Specify the action for system and non-system disk partitions by setting one of the following values for **Encrypt system partitions** and/or **Encrypt non-system partitions**:
   - to encrypt — **Encrypt**;
   - to decrypt — **Do not encrypt**.

   Note. When selecting the value **Do not encrypt**, the decrypting process will start after restarting the computer and mounting the encrypted partitions. Further disk encryption of this computer will be forbidden.

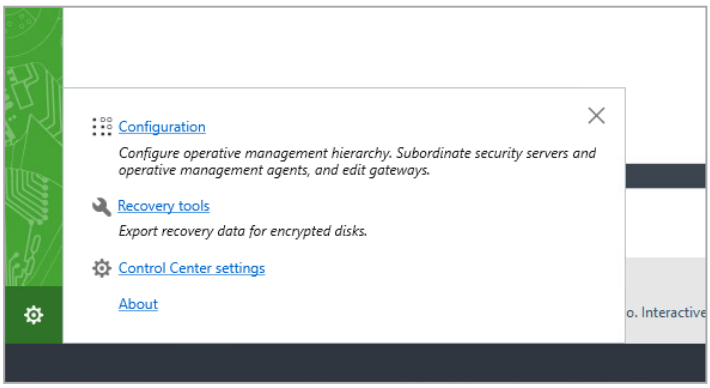
4. Click **Apply**.

Change the security domain key

The security administrator changes the security domain key on the Security Server in the Control Center.

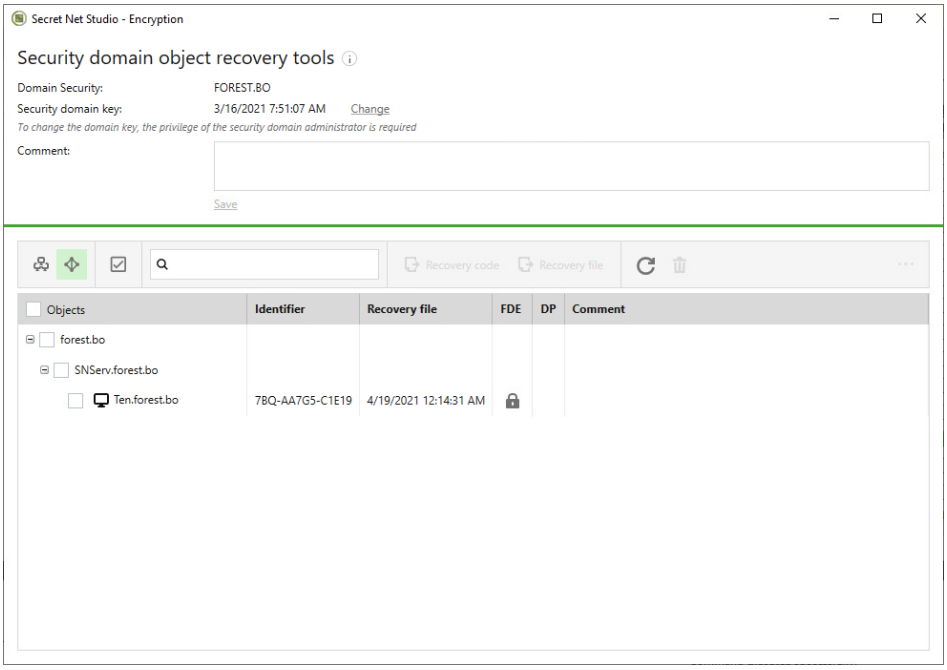
To change the security domain key:

1. In the Control Center, at the bottom of the navigation panel, click **Settings**. The settings launch panel appears.



2. Select **Recovery tools**.

   The recovery tools dialog box appears as in the figure below.



3. Click **Change**.

   You are prompted to enter the password for the security domain key.

4. Enter the password and click **Next**.

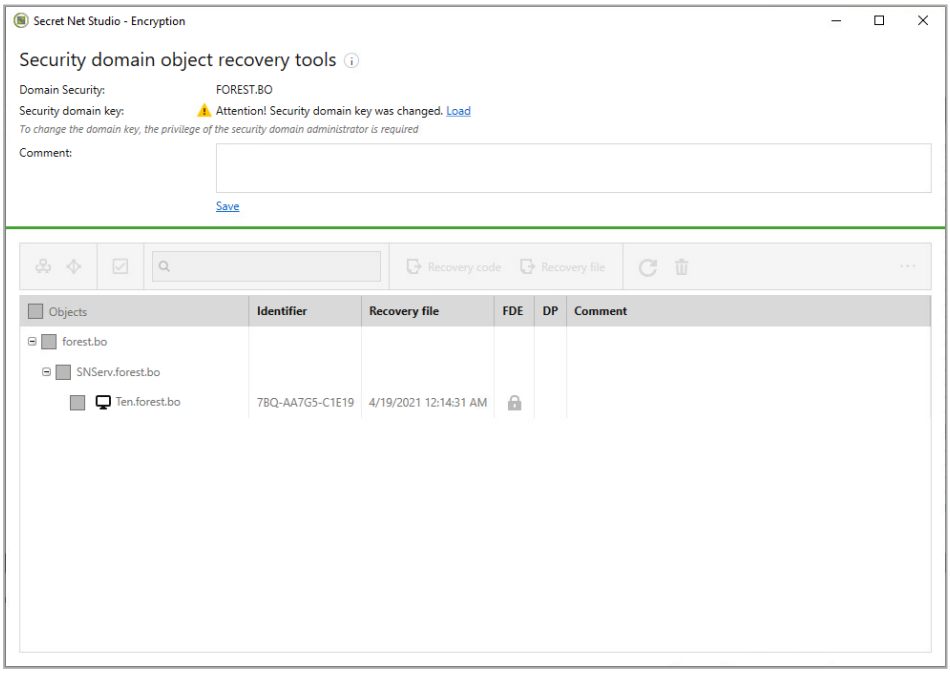
   A request to set a new password appears.

5. Set a new password for the security domain key and confirm it.

   Note. The password must meet the requirements shown in the password request dialog box.

6. Click **Finish**.

   A notification about the key change appears in the recovery tools dialog box. Operations with encrypted disks will become unavailable.



7. Click **Load**.

   A notification about the security system configuration change and the need to restart the computer appears on the computers which are subordinate to the given Security Server and have encrypted disks.

Operations with encrypted disks in the recovery tools dialog box will become available.

Change encryption keys

You can change encryption keys:

- in the Control Center or in the Local Control Center;
- in the disk encryption and protection wizard.

In the Control Center, you can change encryption keys centrally on the computers subordinate to the Security Server and with either the local or centralized mode of storing recovery data:

- when storing recovery data in centralized mode, as a result of the procedure, the recovery code will be changed on the Security Server;
- when storing recovery data in local mode, as a result of the procedure, the user will receive a notification about a recovery code change and a need to save the new recovery data.

The disk encryption and protection wizard allows you to change encryption keys locally for computer disks. Such a change is available only for computers with local storage of recovery data. As a result of the change, the recovery code is changed. You need to save the new recovery data.

To change encryption keys, you must have the privilege to encrypt disks (see p. **155**).

For the instructions on how to change encryption keys in the Control Center and the encryption wizard, see below. The procedure for changing encryption keys in the Local Control Center is similar to the one for the Control Center.

To change encryption keys in the Control Center:

1. In the Control Center, select the **Computers** panel and select the object for which you want to change encryption keys. Right-click the object and click **Properties**. Select the **Settings** tab. In network mode, load the settings from the Security Server.

   Note. If the Security Server is selected, a group policy will be applied and the operation will start on all the computers with the Full Disk Encryption subsystem enabled and subordinate to this Security Server.

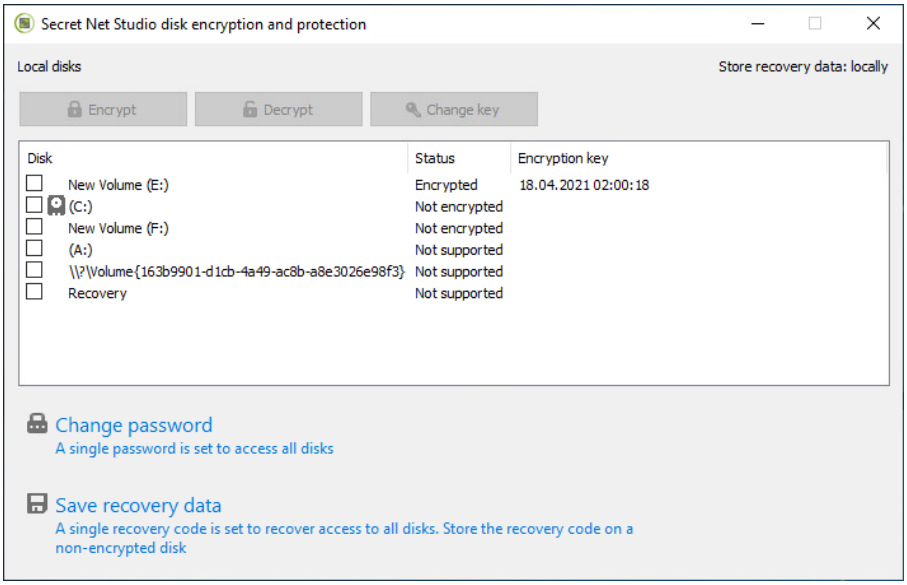
2. In the **Policies** section, go to the **Full Disk Encryption** group of settings.
3. Select the encrypted disks for which you want to change encryption keys.
4. Click **Change the encryption key**.
5. Click **Apply**.

   A notification to restart the computer appears. After the restart, the process of changing the encryption keys begins.

To change encryption keys in the disk encryption and protection wizard:

1. Right-click the Secret Net Studio icon in the Windows taskbar. Select **Encrypt**.

   The Secret Net Studio encryption wizard appears as in the figure below.



Note. You can launch the encryption wizard from the context menu of a disk. In **Encryption**, select **Change the encryption key** and go to step **4** of this instruction.

2. Select the encrypted disk for which you want to change encryption keys.

Note.

- You can change encryption keys for several encrypted disks simultaneously. All computer disks are encrypted with the single key.
- The system disk is shown as .

3. Click **Change key**.

A dialog box prompting you to enter the password appears.

4. Type the password to access encrypted disks and click **Finish**.

The process of decrypting data for changing the key begins.

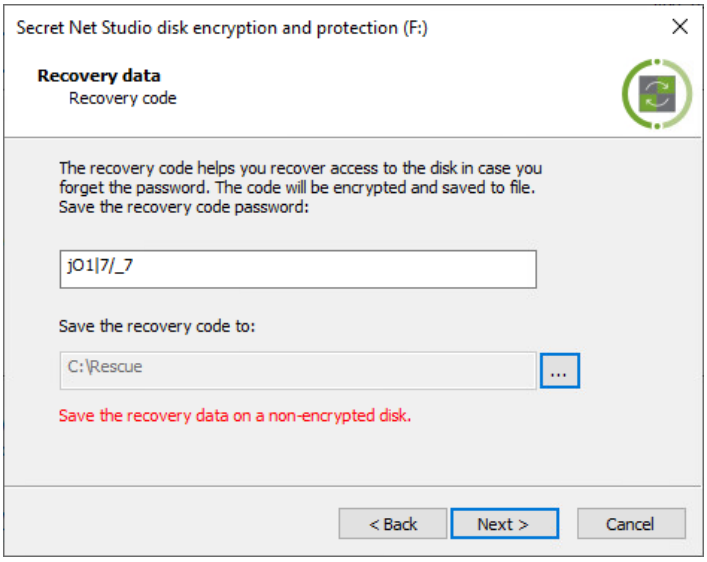
Attention! During the decryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note. During the decryption, you can restart the computer from the Windows Start menu. After logging on to an OS, the process resumes.

After the process is complete, you are prompted to enter the password for encrypted disks in order to save the new recovery data.

5. Type the password and click **Next**.

The dialog box to save the recovery code appears as in the figure below.



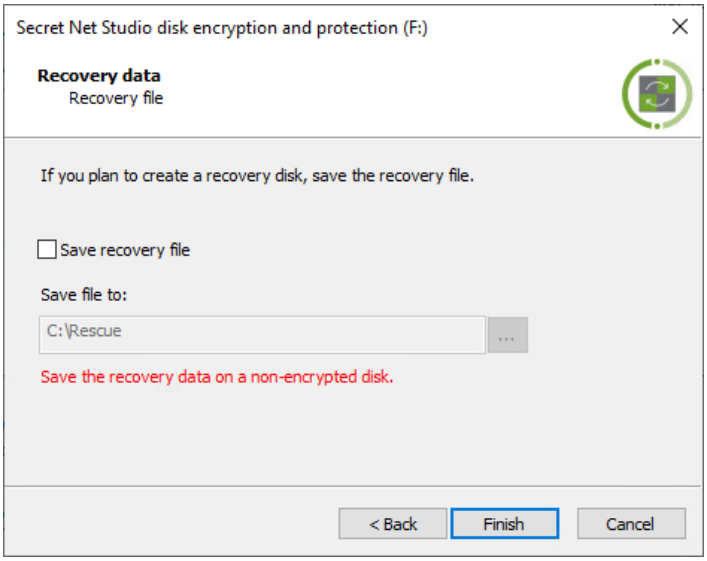
6. Save the system-generated password for the recovery code. Specify the path to save the recovery code.

Attention! Save the recovery data onto a disk different from the encrypted one.

Note. You can save the recovery code for a second time later on (see p. 167).

7. Click **Next**.

   The dialog box to save the recovery file appears as in the figure below.



8. If you need to create an emergency recovery disk, select the check box **Save recovery file** and specify the path to save the recovery file.

Attention! Save the recovery data on a disk different from the encrypted one.

9. Click **Finish**.

   The process of encrypting data with the new key begins.

Attention! During the encryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note. During the encryption, you can restart the computer from the Windows Start menu. After logging on to an OS, the process resumes.

Restore access to encrypted disks

Secret Net Studio Full Disk Encryption subsystem provides the following capabilities to restore data on encrypted disks:

- **In case of losing the password for disks**, you can restore access to them using the recovery code, the password for the recovery code and the ID of an encrypted disk (see p. **171**).

  The ID of an encrypted disk and recovery code are saved in a file. If recovery data are stored locally, the file is created and kept locally on the computer with disks being encrypted (see p. **167**). If recovery data are stored centrally, the file must be exported to the Security Server (see p. **169**).

  The password for the recovery code is generated automatically every time the recovery code is saved or exported. The recovery code is encrypted with this password. The password for the recovery code must be kept in a reliable place and sent only over a secure communication channel.

  Access restoration is performed by the administrator in Secret Net Studio bootloader.

- **If an encrypted disk is corrupted or service information is overwritten**, you can decrypt a disk, restore Secret Net Studio loader or restore the configuration of the Full Disk Encryption subsystem using the emergency recovery disk (see p. **288**). When creating a disk which is going to be used to decrypt and restore the configuration, you need the recovery file.

  If recovery data are stored locally, the recovery file is created and kept locally on the computer with disks being encrypted (see p. **167**). If recovery data are stored centrally, the recovery file must be exported to the Security Server (see p. **169**).

Attention! When using the Full Disk Encryption subsystem, we strongly recommend you to create an emergency recovery disk with a valid recovery file. So, if the system disk is encrypted and Secret Net Studio bootloader is not working correctly, an OS will not be booted. You can fix the issue using only the emergency recovery disk.
The recovery file which you are asked to save in the encryption wizard at the encryption stage becomes obsolete once the encryption has started. We recommend you to create a recovery file manually after the encryption process has finished (see p. **167**, p. **169**).

Note. For more detail about the capabilities of the emergency recovery disk, see p. **288**.

Save recovery data locally

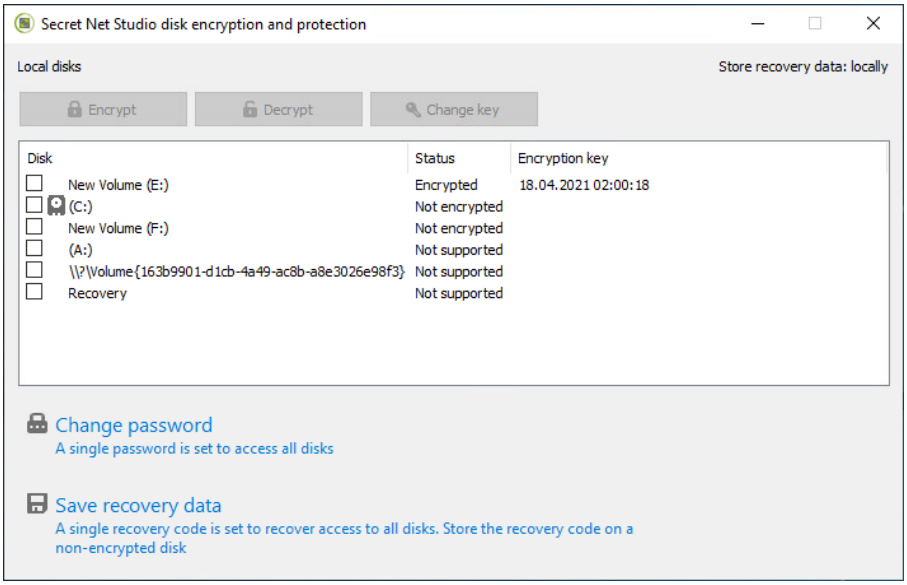
If recovery data was not saved when encrypting data on disks, it can be saved later in Secret Net Studio encryption wizard. This operation is available only for computers with local storage of recovery data.

The administrator, saving recovery data, must be granted the privilege of encryption (see p. **155**).

To save recovery data:

1. Right- click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

   The Secret Net Studio encryption wizard appears as in the figure below.



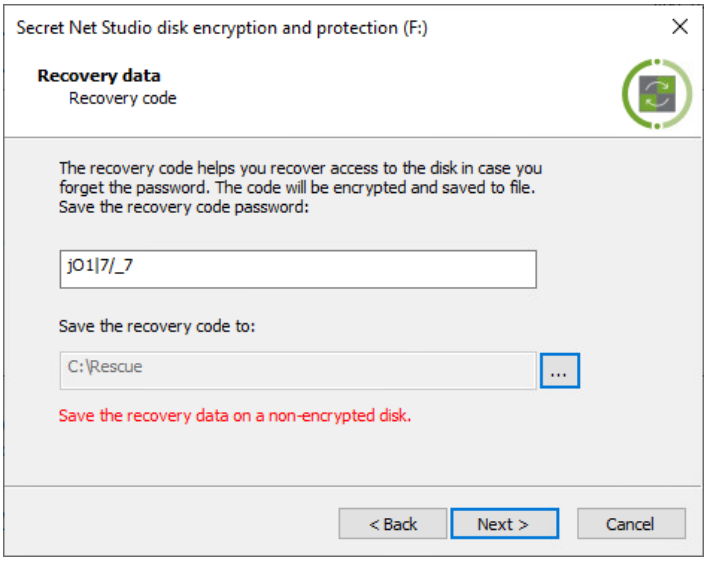
Note. You can launch the encryption wizard from the context menu of a disk. In **Encryption**, select **Encrypt** and go to step **4** of this instruction.

2. Click **Save recovery data**.

   A dialog box prompting you to enter the password appears.

3. Enter the password and click **Next**.

   The dialog box to save the recovery code appears as in the figure below.

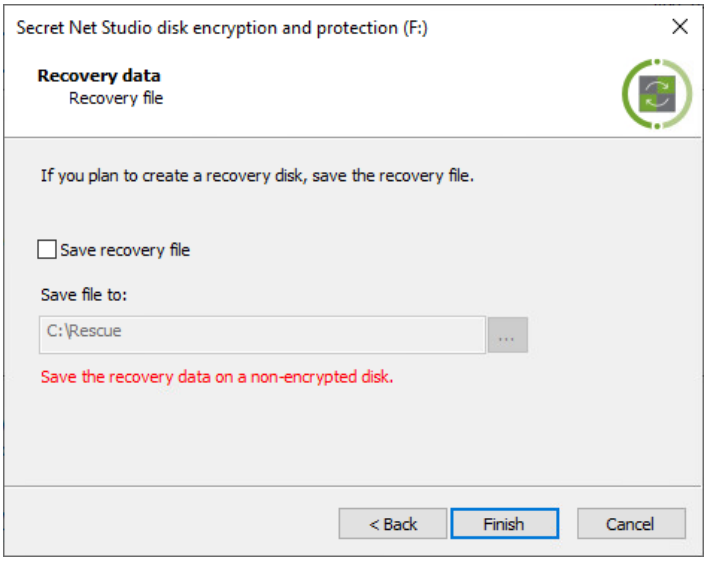


4. Save the system-generated password for the recovery code. Specify the path to save the recovery code.

Attention! Save the recovery data onto a disk different from the encrypted one.

5. Click **Next**.

   The dialog box to save the recovery file appears as in the figure below.



6. If necessary, select the check box **Save recovery file** and specify the path to save the recovery file.

Attention! Save the recovery data on a disk different from the encrypted one.

7. Click **Finish**.

   A notification that the recovery data was saved successfully appears.

Export recovery data on the Security Server

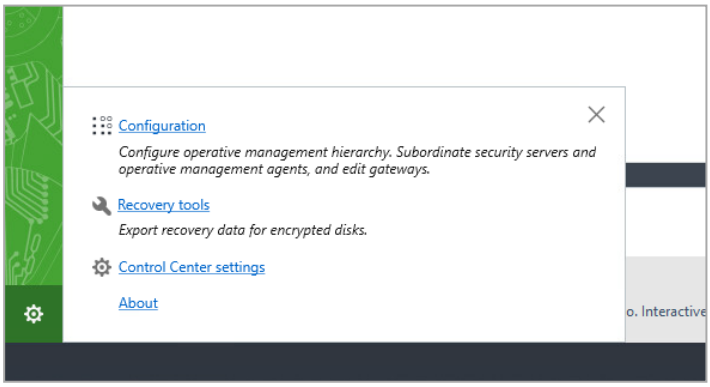
If you want to save recovery data centrally, you need to export the data on the Security Server and send it to the user. A recovery code and file can be sent over an open communication channel. The password for the recovery code must be sent only over a secure communication channel.

The administrator exports the recovery file and code in the Control Center.

To export recovery data, you must have the privilege to encrypt disks (see p. **155**).

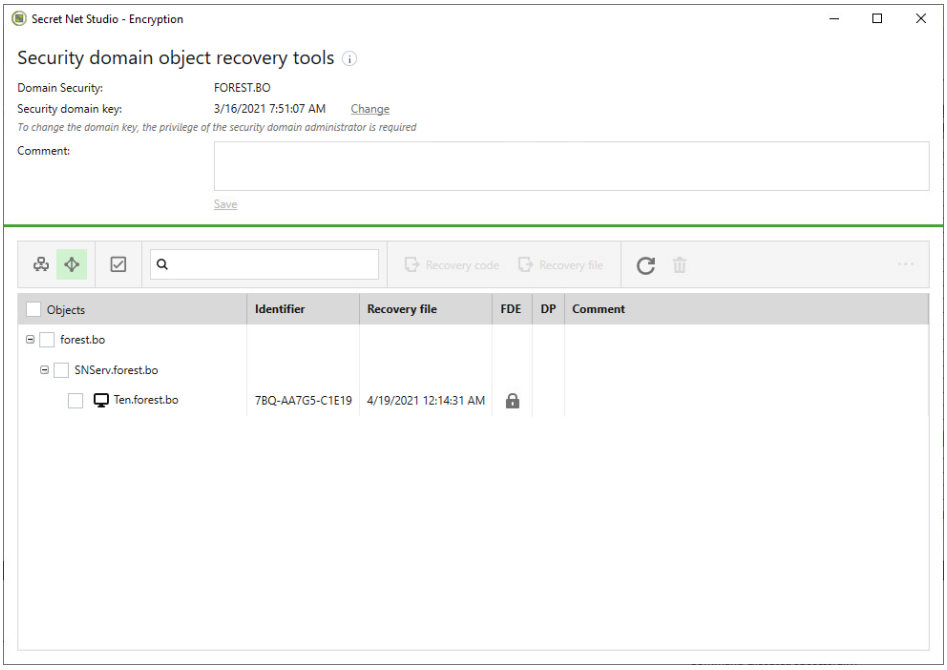
To export the recovery code:

1. In the Control Center, at the bottom of the navigation panel, click **Settings**. The settings launch panel appears.



2. Select **Recovery tools**.

   The recovery tools dialog box appears as in the figure below.



3. Select the object for which you want to export the recovery code.

Note.
- Objects can be presented as a control object structure and an AD structure. To select the display mode, click and respectively.
- You can select several objects.
- When selecting a computer, the recovery code for all the disks of this computer is exported to a single file.
- When selecting a Security Server or several computers, recovery codes for each computer are exported to separate files.

4. Click **Recovery code**.

   You are prompted to enter the password for the security domain key.
5. Enter the security domain key and select **Next**.

   A dialog box to specify a path appears.
6. Specify the path to save the recovery code and click **Finish**.

   A dialog box showing a generated password for the recovery code appears.
7. Save the password for the recovery code to send it to the user over a secure channel later. Click **Finish**.

To export the recovery file:

1. In the Control Center, at the bottom of the navigation panel, click **Settings**. The settings launch panel appears.
2. Select **Recovery tools**.

   The recovery tools dialog box appears.
3. Select the object for which you want to export the recovery file.

Note.
- Objects can be presented as a control object structure and an AD structure. To select the display mode, click and respectively.
- You can select several objects.
- When selecting a computer, the recovery file for all the disks of this computer is exported.
- When selecting a Security Server or several computers, recovery files for each object are exported separately.

4. Click **Recovery file**.

   You are prompted to enter the password for the security domain key.

5. Enter the security domain key and select **Next**.

   A dialog box to specify a path appears.

6. Specify the path to save the recovery file and click **Finish**.

Restore access using a recovery code

Encrypted disks access restoration is performed by the administrator in Secret Net Studio bootloader. The administrator must have a file with a recovery code and the ID of an encrypted disk, as well as know the password for the recovery code.

If the restoration is successful, the password for the disks, the IDs of the encrypted disks, the recovery code and its password should be changed. In this case:

- in case of centralized storage of recovery data, these data are updated on the Security Server while mounting encrypted disks;
- in case of local storage of recovery data, the user will be prompted to save the new data.

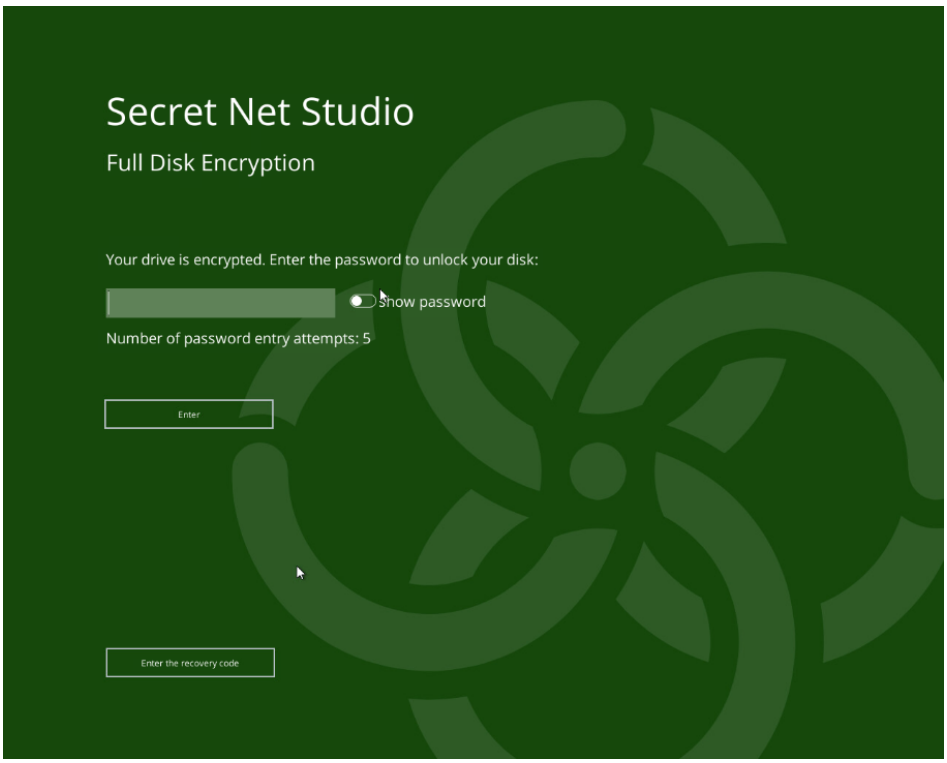
To restore access:

1. Turn on the computer.

   Secret Net Studio bootloader window appears.

2. Select **Restore access**.

   A dialog box to save the recovery data appears as in the figure below.



3. Compare the ID of the encrypted disk with the ID from the file with the recovery code. They must match.

   Note. If the IDs do not match, the data from the file are not suitable to restore access to disks on this computer.

4. Enter the recovery code and the password for it.
5. Click **Next**.

   If the entered data are correct, access to the disks will be restored. A dialog box prompting you to set a new password appears.

6. Set a new password to access the disk. Confirm the password.
7. Click **Next**.

An OS boots. If recovery data are stored centrally, the recovery data will be updated on the Security Server. If recovery data are stored locally, when the user logs on to the OS, they will be prompted to enter the password for the disks to save the new recovery data.

Note. For more detail about computer events and user actions in case of local storage of recovery data, see document [**3**].

Chapter 15
Data Encryption

Granting privileges to create encrypted file containers

The data encryption mechanism in encrypted file containers supports creating encrypted file containers by users who have the privilege to create encrypted containers.

By default, the permission to create encrypted file containers is granted to users included in the local **Administrators** group or the **Users** group.

The centralized configuration procedure when using the Control Center in the centralized mode is described below. Local configuration is performed in the same way in the Local Control Center.

To grant the privilege:

1. In the Control Center, open the **Computers** panel and select the object you want to configure. Right-click the object and click **Properties**. In the properties panel, select the **Settings** tab and click **Load Settings**.
2. In the **Policies** section, go to the **Data Encryption**.
3. For the **Accounts with the privilege** to create encrypted file containers parameter, edit the list of users and user groups who are granted the privilege.
4. Click **Apply**.

Event registration setup

Event registration setup is required to keep track of events related to the data encryption function in the encrypted file containers. Configuration is performed in the Control Center. You can find the events for which logging can be enabled or disabled on the **Settings** tab, in the **Event Registration > Data Encryption** group. To go to the registration settings from the respective group of parameters in the **Policies** section, click the **Audit** link in the right part of the group heading.

Managing encryption user keys

To work with encrypted data in encrypted file containers, users need to load encrypted keys (key information) from their key drivers. The key information can be stored in a personal identifier assigned to a user or on a external drive.

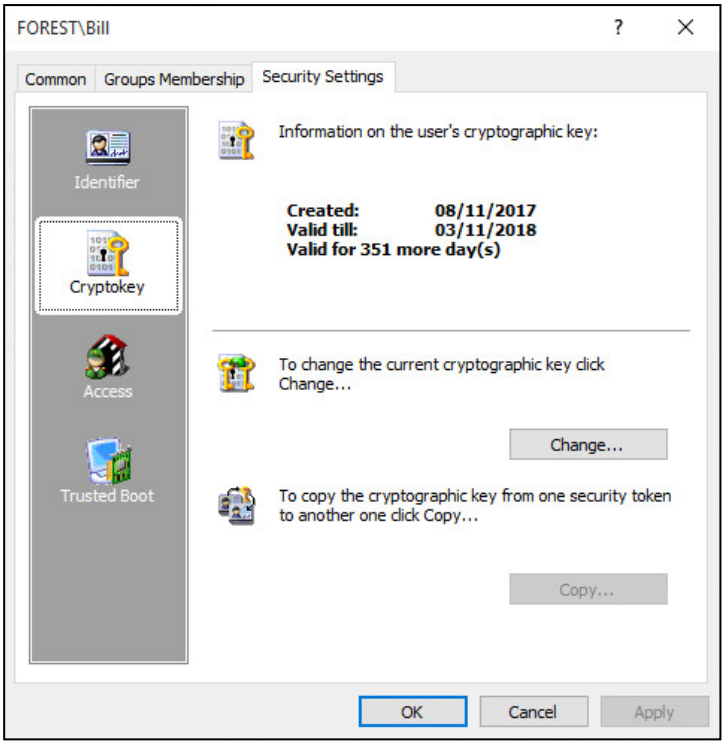
Key issue and change

Key information can be generated and a private key can be saved to a key device when assigning a personal security token to a user. For the description of the assignment procedure, see p. 25. If a user is assigned an security token, but no key information was generated, or existing keys need to be changed, the administrator can perform the procedure to issue/change the keys.

To issue/change keys:

1. Launch the user management program.
2. Open the setup window for user properties and select the **Security Settings** tab.
3. Select the **Cryptokey** group.

   Information about the user's key will be displayed in the dialog box as in the figure below.



4. Click **Issue** (if the user has keys already, this button will be displayed as **Change**). The button is available if at least one security token is assigned to the user.

   If the user already has keys, a dialog box will appear asking you to select one of the following two key change options: save the user's old key or don't save it.

5. Select the required option in the dialog box and click **Next**.

   Attention! The **don't save the key** option is only recommended when it is impossible to read the current key from the user security tokens. To confirm your selection, type **Continue** in the text box and click **Next**. In this case, the program will go to the **Save keys** step.

   If the **save old key** option is selected, a dialog box will appear displaying the progress of the key reading procedure, together with a prompt to present the security token.

6. Provide the security token containing the old user key.

   After successful completion of the operation, the word **Completed** appears in the dialog box to the right of the name of the operation. If an error occurs during the operation, the dialog box will display a corresponding message.

   Note. It is impossible to continue the procedure without fixing the error.

7. If an error occurs, click the **Repeat** button to perform the operation again. Once the key is loaded, click **Next**.

   A dialog box will appear on the screen displaying the progress of the operation together with a prompt to present security tokens.

8. Present all listed security tokens.

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

9. Click **Close**.

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

10. Fix errors. To do this, click **Back** and perform the operation again. Once errors are fixed, click **Finish**.

Attention! We strongly recommend fixing errors that occurred when writing keys to the security tokens. After successful completion of all required operations, each operation should be assigned the **Completed** status.

Key copying

User keys generated by Secret Net Studio can be copied from one user security token to another. Copying is performed by the security administrator.

To copy keys:

1. Launch the user management program.
2. Open the setup window for user properties and select the **Security Settings** tab.
3. Select the **Cryptokey** group.
4. Click **Copy**. The button is available if at least two security tokens are assigned to the user.

   A dialog box asking you to present the security token appears.
5. Present the security token containing the user keys.

   Key reading is initiated, and the dialog box displaying the list of the user's security tokens appears.
6. Present the security token to which the keys should be saved.

   Once the keys are successfully saved to the security token, its status changes to Processed.
7. Click **Close**.

Configuring key change parameters

The administrator can configure the following parameters for changing the keys generated by Secret Net Studio tools:

- Maximum key validity period
- Minimum key validity period
- Key expiration warning

These parameters are applied to all users. After expiry of the maximum key validity period, the user's key information becomes invalid. In this case, the user should change the keys (see document [**3**]). The user can only change keys after the minimum validity period expired.

These parameters are interdependent. The minimum validity period and key expiration warning period cannot be the same or exceed the maximum key validity period.

The centralized configuration procedure when using the Control Center in the centralized mode is described below. Local configuration is performed in the same way in the local Control Center.

To configure these settings:

1. In the Control Center, open the **Computers** panel and select the object you want to configure. Right-click the object and click **Properties**. In the properties panel, select the **Settings** tab and click **Load settings**.
2. In the **Policies** section, click **User keys**.
3. Set the required values for the following parameters: **Maximum key validity period**, **Minimum key validity period** and **Key expiration warning**.

   Note. If zero value is set, the parameter is not applied.
4. Click **Apply** at the bottom of the **Settings** tab.

Chapter 16
Data Wipe

The Data Wipe subsystem is designed to wipe memory areas with data remained from deleted objects. It prevents restoration of data after it was deleted and ensures security when reusing data drives. Wiping can be performed:

- automatically on certain types of devices (local and removable drives, RAM) or for user-selected file objects when deletion mode is enabled in the Control Center;

  Note. You can exclude selected objects (files and folders) from processing while wiping data automatically (see p. 177).

- on command from the shortcut menu for user-selected file objects;
- on command from the shortcut menu of the Secret Net Studio icon on local drives (except for the system drive) and external drives that are connected to a protected computer.

Attention! The virtual memory pagefile is wiped by using standard Windows tools when the computer is turned off. If RAM deletion mode is enabled in Secret Net Studio, we recommend you to enable the following standard Windows security option: **Shutdown: Clear virtual memory pagefile**.
Files are not erased when moved to the Recycle Bin, because the files are not deleted from the disk in this case. These files are erased when the Recycle Bin is cleared.

This chapter contains descriptions of the following procedures:

- configuration of the mechanism (p. **176**);
- configuration of the exclusion list for automatic data wipe (p. **177**);
- monitoring of the residual data lazy processing (p. **177**);
- data wipe on the drives (p. **178**).

Data wipe configuration

The centralized configuration procedure when using the Control Center in centralized mode is described below. Local configuration is performed similarly in the local Control Center.

To configure the mechanism:

1. In the Control Center, open the **Computers** panel and select the object you need to configure. Right-click the object and click **Properties**. In the properties menu, select the **Settings** tab and click **Load settings**.
2. In the **Policies** section, click **Data Wipe**.
3. Specify the required values for the following parameters:
   - Number of wipe cycles for local drives;
   - Number of wipe cycles for external drives;
   - Number of wipe cycles for RAM;
   - Number of wipe cycles for the **Remove permanently** command;
   - Number of wipe cycles during erasing data from the drive.

   Note. If the parameter value is **0**, wiping is not performed. To ensure that data is erased, **2** wiping cycles are usually enough.

   Tip. To view help information, click .

4. Click **Apply**.

Exclusion list

This function allows you to exclude objects (files and folders) from processing while wiping data automatically on local and removable drives.

Note.
- If you add a folder to the exclusion list, all the objects of this folder are not processed by the data wipe mechanism.
- You can create the exclusion list for both local and group policy.

The centralized configuration procedure when using the Control Center in centralized mode is described below. Local configuration is performed similarly in the local Control Center.

To configure the exclusion list:

1. In the **Data Wipe** section, go to the **Exclusions** setting:

2. Perform the required action:
   - to add an object to the list, enter its full path and click . You can use the variables from the drop-down list. To open the list, click ;
   - to change the path to an object, select the object and click ;
   - to delete an object from the exclusion list, click .
3. To save changes, click **Apply**.

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

Residual data lazy processing

The residual data lazy processing mechanism reduces the load on the computer while deleting large amounts of data. Residual data to be wiped is added to a processing queue. Data is wiped in an orderly fashion and ends before computer shutdown.

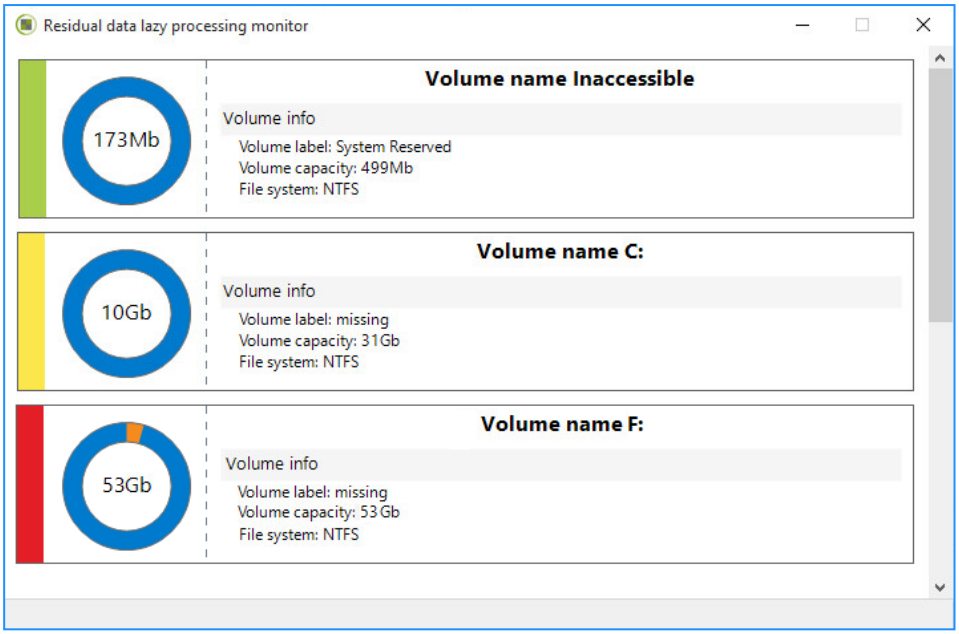
You can monitor this process using the **Residual data lazy processing monitor** dialog box.

Attention! The monitor is available only when the data wipe mechanism is enabled and a number of wipe cycles is more than **0** (see p. 176).

To open the Residual data lazy processing monitor:

- Right-click the Secret Net Studio icon in the system control area of Windows OS taskbar and select **Deleting data** | **Residual data lazy processing monitor**.

  A dialog box appears as in the figure below.



The monitor displays information for each volume on which the lazy processing is performed.

The information contains the following:

- the volume name and mount point;
- information about a volume (volume label, volume capacity and file system);
- the vertical indicator that displays the delay before processing residual data based on a number of wipe cycles:
  - green — processing time less than 10 seconds;
  - yellow — processing time from 10 to 60 seconds;
  - red — processing time more than 60 seconds;
  - gray — processing time estimation is in progress;
- the pie chart that indicates the ratio of the free space to the amount of disk space occupied by residual data to be wiped setting aside a number of wipe cycles:
  - blue — free space;
  - orange — amount of disk space occupied by residual data to be wiped.

Wiping data from drives

The function is designed for permanent deleting of all information (including a partition table, logical volumes, file objects and residual data) from the following drives:

- local drives of a protected computer (except for the system drive);
- external drives that are connected to a protected computer.

Attention! Only users included in the group of local computer administrators can use this function.

To wipe data from drive:

1. Right-click the Secret Net Studio icon in the system control area of Windows OS taskbar and click **Deleting data** > **Deleting data from the local drive**.

   A dialog box asking you to select a drive appears.

2. In the drop-down list, select the drive that data should be wiped from.

   Note. If an external drive is not connected or there is only the system local drive, the drive list will be empty.

   The **Description** field displays the information about the drive.

3. Click **Next**.

   The consent prompt for data wipe appears.

4. If you are sure you want to permanently erase all data from the drive, click **Next**.

   Data wipe process begins.

   Note. Data wipe process may take some time. It depends on the number of wipe cycles in the Control Center. (the **Number of data wipe cycles during erasing data from the drive** parameter).

   When process finishes, a message box about successful completion appears.

5. Click **Finish**.

Chapter 17
Firewall

The firewall protects servers and workstations in the local area network against unauthorized access and controls network access.

The protection mechanism filters traffic at network, transport and application layers according to specified traffic filtration rules.

The firewall performs the following functions:

Function	Description
Network traffic filtering	Network traffic filtering is based on special rules with extensive settings. Network connections can be restricted at the following levels: • users; • computers; • user groups; • connection settings: service and application protocols, ports, network interfaces, applications, weekdays, time of day
Learning mode	With learning mode enabled, all network traffic is allowed. For each packet the system checks for a filtering rule that is configured in the firewall; default rules are excluded from the procedure. Several rules of the same type are grouped and replaced with a single rule

You can configure the firewall centrally via the Control Center. Configuration is performed at the Computer object level, separately for each protected computer.

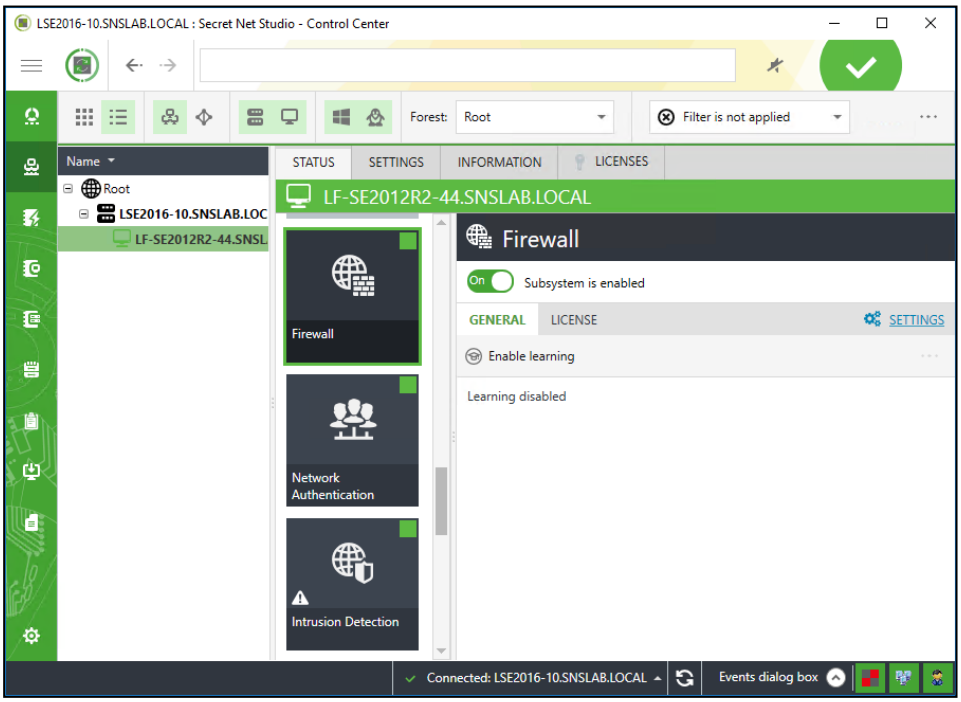
Note. Secret Net Studio also contains the **Local Control Center** component. This component only allows you to view firewall settings on a protected computer.

The initial firewall configuration allows all network traffic to pass through.

To configure the firewall:

1. Open the Control Center.

   The main program window appears.



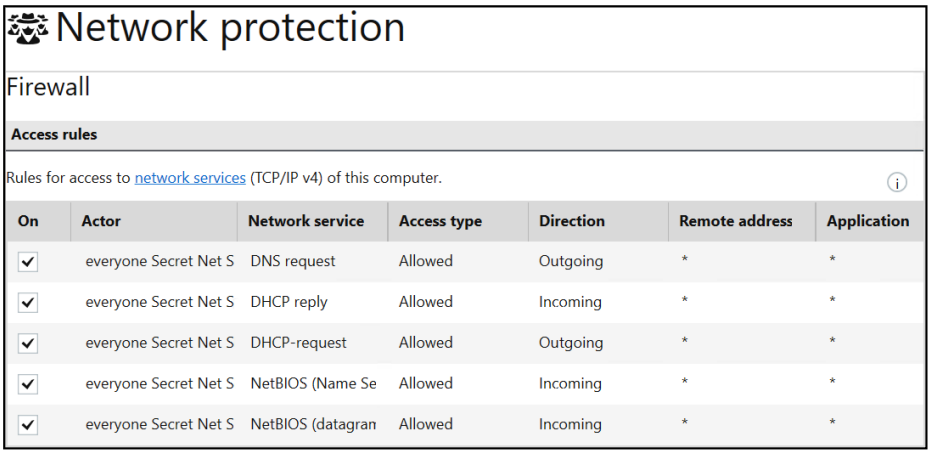
Tip. To view firewall settings directly on a protected computer, open the Local Control Center, select the **Settings** tab, and select the **Firewall** element in the **Policies** section. Parameters cannot be configured in the local mode.

2. Open the **Computers** view on the left side of an open window and; select the computer you need, right-click the selected item, and then click **Properties** on the shortcut menu.

   An information about the computer status appears on the right side of the window.

3. Select the **Settings** tab. If necessary, click the **Load settings** button. In the **Policies** section, click **Firewall**.

   Interface of firewall configuration appears on the right side of the window as in the figure below.



On	Actor	Network service	Access type	Direction	Remote address	Application
✓	everyone Secret Net S	DNS request	Allowed	Outgoing	*	*
✓	everyone Secret Net S	DHCP reply	Allowed	Incoming	*	*
✓	everyone Secret Net S	DHCP-request	Allowed	Outgoing	*	*
✓	everyone Secret Net S	NetBIOS (Name Se	Allowed	Incoming	*	*
✓	everyone Secret Net S	NetBIOS (datagran	Allowed	Incoming	*	*

4. Configure the parameters required and click the **Apply** button to save changes.

Attention! If protected computers have different user authentication modes selected (see p. 11), the firewall rules for authenticated users between them will not work.

Network packet processing procedure

The Secret Net Studio network packet processing procedure depends on traffic direction.

- Incoming packets are first checked for compliance with network protocol settings; then, for compliance with system rules and then, if a packet passes the previous stages, it is checked for compliance with access rules.
- Outgoing packets are first checked for compliance with access rules; then, for compliance with system rules and then, if a packet passes the previous stages, it is checked for compliance with network protocol settings.

By default, object access rules are processed based on the order of their creation and position in the table of rules. The rules at the top of the table have the highest priority (see p. **182**).

If network packet properties match its description in a rule, a predefined action is performed. If access is denied, the packet is not checked for compliance with the rest of the rules. If access is granted, the packet compliance check is continued. Network packets that are not subjects to any of the rules pass through the firewall.

Note. Service rules enabling network traffic required for the Secret Net Studio to functioning are applied even when a packet was blocked at the previous stages.

Packet processing procedure for application rules:

- first, packets are processed according to the incoming traffic processing procedure;
- once the data is converted via operation with folders and named pipes, compliance with application rules is checked;

- once operations with folders and named pipes, as well as further conversion of a response into outgoing packages is complete, the corresponding processing procedure (outgoing packet processing) is performed.

If these operations are performed by a protected computer, it is not required to check for compliance with application rules.

Change rule priority

By default, object access rules are processed based on the order of their creation and position in the rules table. The rules at the top of the table have the highest priority.

With the Secret Net Studio you can change rule processing priority.

To change rule priority:

1. From the list, select the rule.
2. To change the rule priority, click the **Up** or **Down** button.

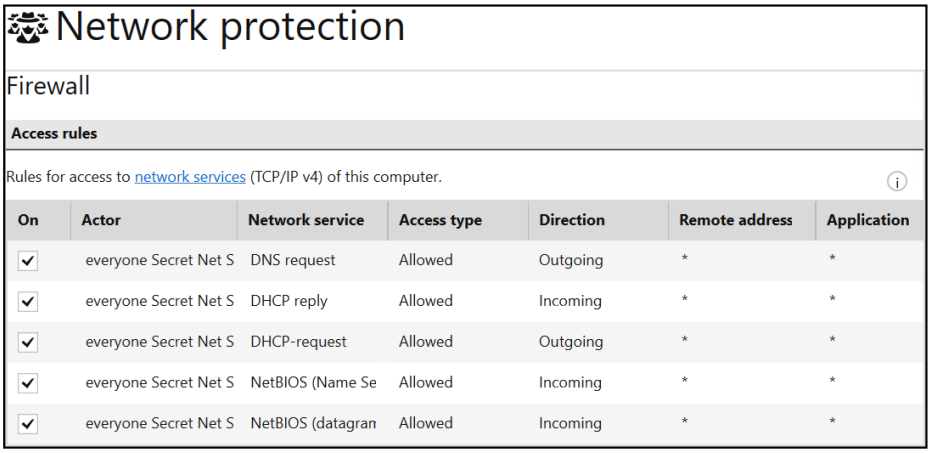
Configuring access rules

Access rules govern access for authenticated and anonymous users to the network services of a protected computer. These rules have higher priority than the application rules (see p. **195**).

Attention!
- By default, the access rules govern all computer network interfaces.
- Changes to the rule settings take effect within 4-6 minutes.

To manage the rules:

1. Go to the **Access rules** section in the interface of the firewall configuration.



For each rule, the following information is displayed in the table:

Column	Value
On	Rule operation management: • unselected — the rule function is temporarily suspended; • selected — the rule is enabled
Actor	Name of the account or account group the rule applies to
Network service	Name of the network service the rule applies to
Access type	Type of access to a protected computer: • **allowed**; • **denied**
Direction	Network traffic direction the rule applies to

Remote address	Name or IP address of the computer the rule applies to. An asterisk (*) symbol indicates that the rule applies to all remote computers
Application	Path to the application that the rule applies to. An asterisk (*) symbol indicates that the rule applies to all applications

Note. If there are rules, which have been added to the learning mode, the table will contain **Auto-learning** column. To remove auto-learning mark, press the **Remove auto-learning sign** button.

2. Perform the required operations:
   - create rules (see p. **183**);
   - edit rule parameters (see p. **190**);
   - delete rules (see p. **191**);
   - assign rule priority (see p. **182**).
3. Click **Apply**.

Creating an access rule

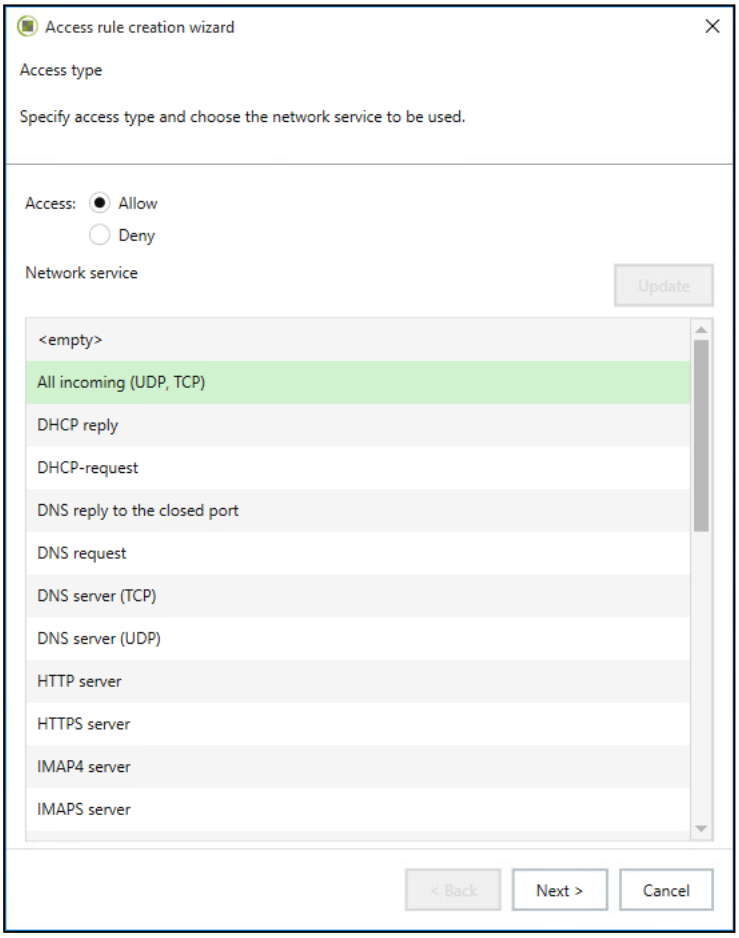
There is a special wizard for creating rules.

Tip. Use the buttons below to manage the rule creation procedure:
- **< Back** — to return to a previous dialog box;
- **Next >** — to proceed to the next dialog box;
- **Cancel** — to stop creating a rule.

To create an access rule:

1. Click the **Add** button.

   Access rule creation wizard appears.

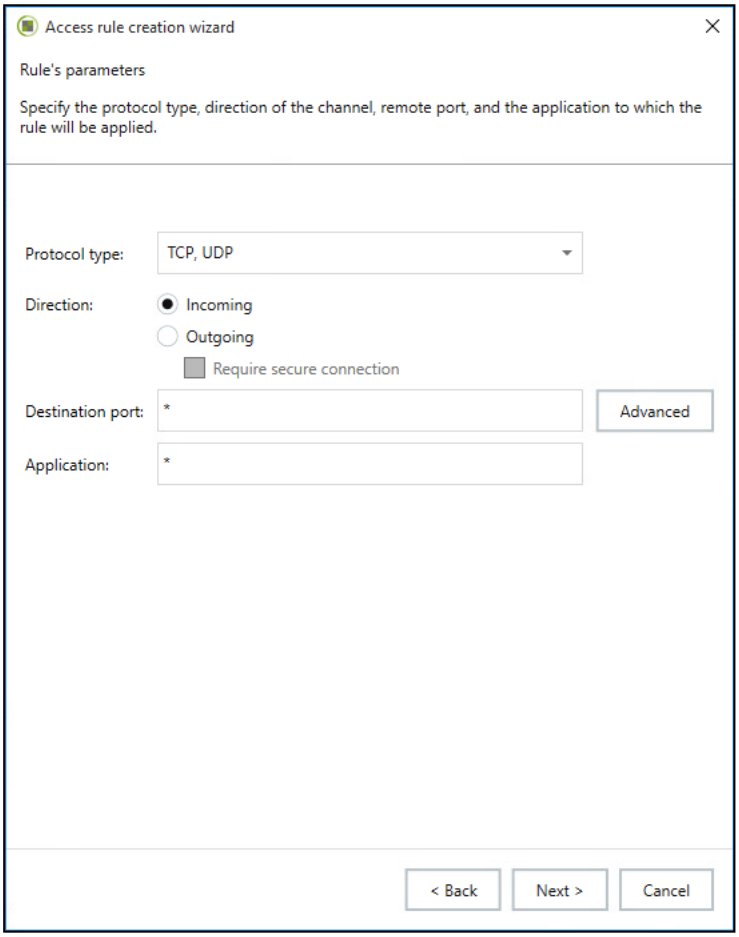


2. Configure the parameters and click **Next**.

Section	Value
Access	Click the button: • **Allow** — if it is necessary to grant access to a protected object when a rule is triggered; • **Deny** — if it is necessary to deny access to a protected object when a rule is triggered
Network service	Select the name of a network service to configure the network protocol parameters in the created rule. Select the **<empty>** value to define network service parameters manually

Note. The network services list shows the services that are set by default. To display manually created services (see p. 207), click the **Update** button.

A dialog box appears as in the figure below.



Note. If you select a network service in the previous step of the wizard, the dialog box will be configured according to the service parameters. In this case, when you change these parameters, the name of the selected network service will be replaced in the rule with a brief description of the specified parameters. The list of network services will not be changed.

3. Specify the required parameters and click **Next**.

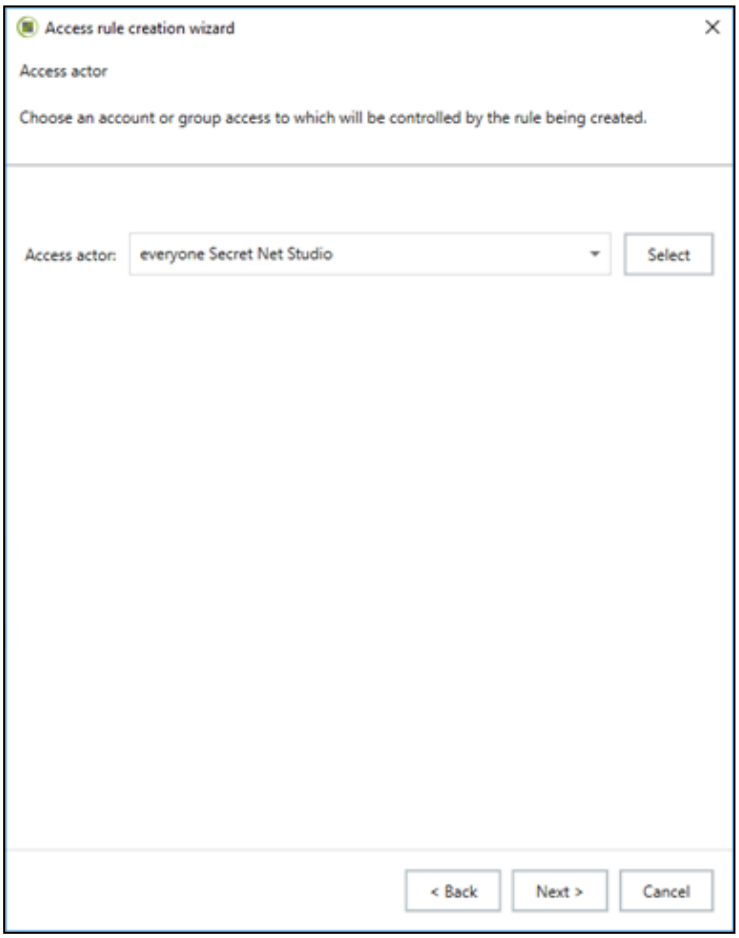
Section	Value
Protocol type	Select a protocol type the rule applies to
Direction	Select traffic direction that is subject to the rule (regarding a protected object)
Require secure connection	Select the check box if an outgoing network connection requires a secure data transfer channel

Section	Value
Destination port	Type the numbers of the ports that are a subject to the rule: • for incoming traffic, specify the ports numbers which receive the IP packets; • for outgoing traffic, specify the ports numbers to which the IP packets are sent; • leave an asterisk (*) symbol if the rule must govern all computer ports. Use "," as a separator. Use "-" (hyphen) to specify a range of ports. Click **Advanced** to configure a list of ports in the pop-up dialog box
Application	Type the path to the executable file of an application subject to the rule: • specify the path to an application. You can also use Windows system variables to specify the path to an application; • leave an asterisk (*) symbol if the rule must govern all applications. A created rule will filter network traffic for an application that operates directly on a protected computer

Attention! To ensure the access rule works properly, you must to specify the full path to the application's executable file.

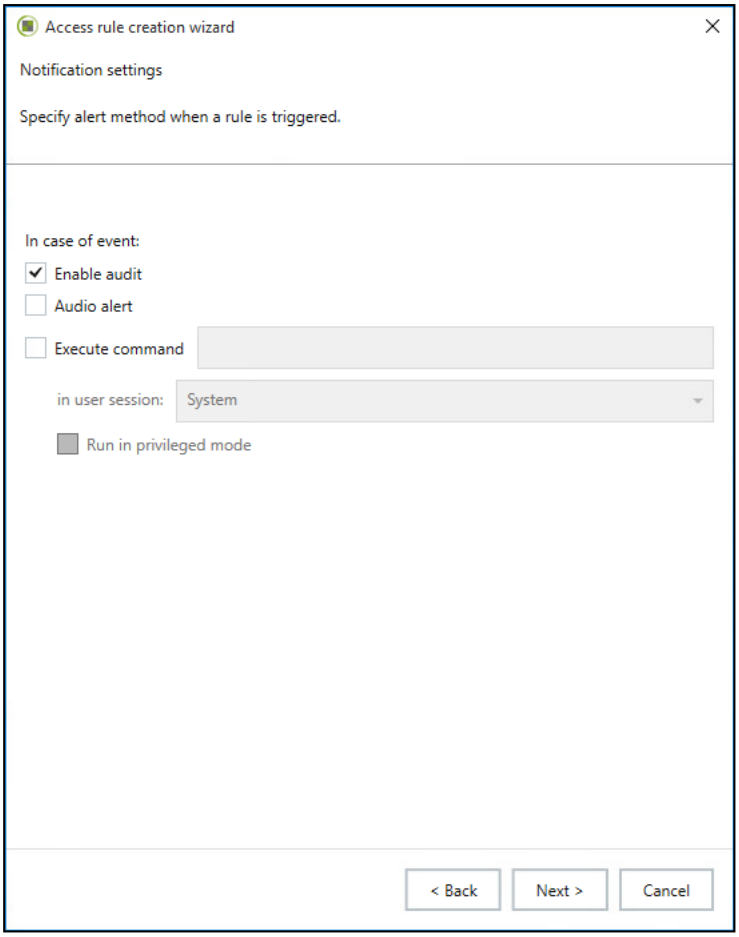
Attention! While using the **Require secure connection** parameter, network connections are not be established through a not secure channel (if a license to use the network authentication mechanism is available).

The **Access actor** dialog box appears.



4. Specify the name of the account or account group to be governed by the rule and click **Next**.

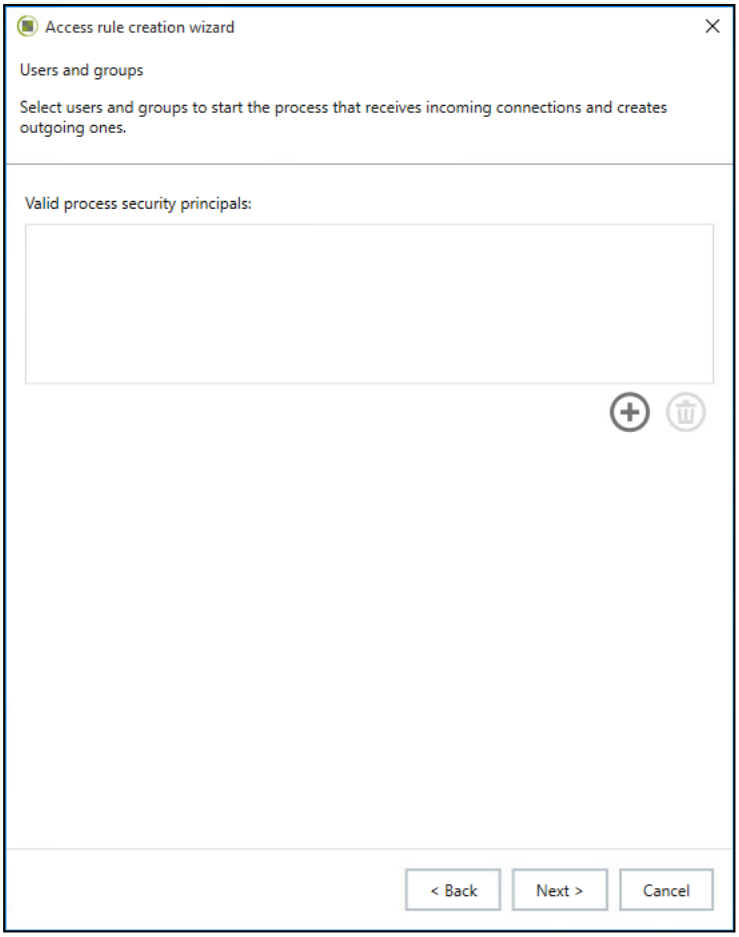
   The **Notification settings** dialog box appears.



5. Define the rule triggering alert methods and click **Next** (If necessary).

Section	Value
Enable audit	Select this check box to log the event when a rule is triggered. If event logging is not required, clear this check box
Audio alert	Select this check box if an audio alert is required to notify that a rule has been triggered on a protected computer. If audio alerts are not required, clear this check box
Execute command	Select this check box to run an executable file automatically when a rule is triggered. In the text box, which becomes available when the check box is selected, type the full path and the executable file name (with a parameter). For example, **C:\windows\notepad.exe 1.txt**
in user session	The field becomes available once the **Execute command** check box is selected. Select the user session where the specified command should be executed. • **System** — execute the command with system permissions; • **Console** — execute the command on behalf of a user during the user's session; • **All user sessions** — execute the command during all user sessions
Run in privileged mode	Select to execute the command with full user permissions, even if User Account Control (UAC) is enabled for the user

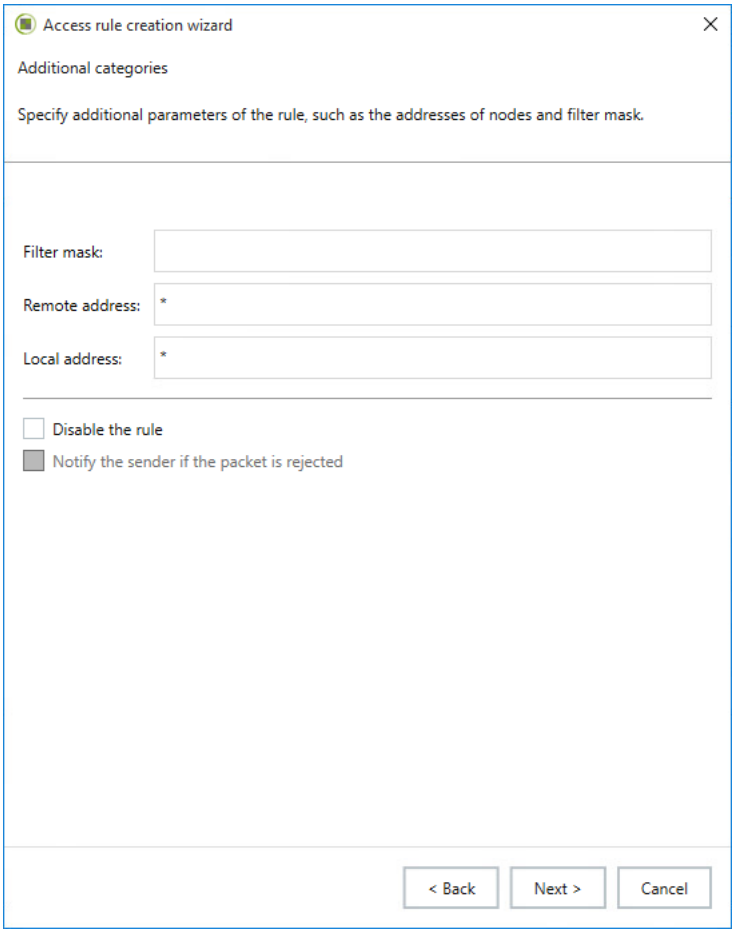
The **Users and groups** dialog box appears.



Tip. Click the **Add** button to select accounts via the standard Windows dialog box. To delete an account, select it from the list and click the **Delete** button.

6. Specify the name of the account or account group that will run the processes for which the rule will be applied to and click **Next**.

   The **Additional categories** dialog box appears.



7. Specify the additional parameters for the rule and click **Next**.

Section	Value
Filter mask	Type a value to define the need for processing an IP packet. If the box is filled in, the rule only concerns those IP packets with contents matching the filter mask. This box supports the following special characters: • ***** — for any number of characters; • **?** — for a single character. For example, the value ***abcd*** will match any packet whose body contains the sequence abcd
Remote address	To define a suitable set of remote addresses, type a computer name, IP address, IP address range (e.g., **192.168.0.3–192.168.0.9**) or a subnet (e.g., **192.168.1.0/24** or **10.10.0.0/255.255.0.0**)
Local address	Type a computer name, IP address, IP address range or a subnet to define a suitable set of local addresses
Disable the rule	Rule operation management: • **unselected** — the rule is enabled; • **selected** — the rule function is temporarily suspended
Notify the sender if the packet is rejected	Managing notifications about packet blocking caused by the functioning of a blocking rule: • **unselected** — the sender does not receive notifications about blocked packets; • **selected** — the sender receives notifications about blocked packets. If a rule is triggered, RST packets will be generated for a TCP protocol, while ICMP packets (type: Destination Unreachable) will be generated for the other protocols (excluding ICMP, AH, ESP)

Tip. Leave an asterisk (*) symbol in the **Remote address** or **Local address** fields for the rule to govern any addresses.
Use a semicolon (;) to separate multiple IP addresses, address ranges or subnets.

Note. The **Notify the sender if the packet is rejected** check box can be modified for rules with **Prohibit access** type access and **Incoming** traffic direction.

The **Rule application schedule** dialog box appears.

8. If necessary, configure the rule application schedule and click **Finish**:

- select the **Schedule** check box. A table enabling schedule configuration becomes available;
- click to choose weekdays and times for the rule application to be allowed (active rule) or blocked (inactive rule).

Note. The time when the rule is applied is defined by the time zone set on the protected computer.

The rule will be created and displayed in the list of rules.

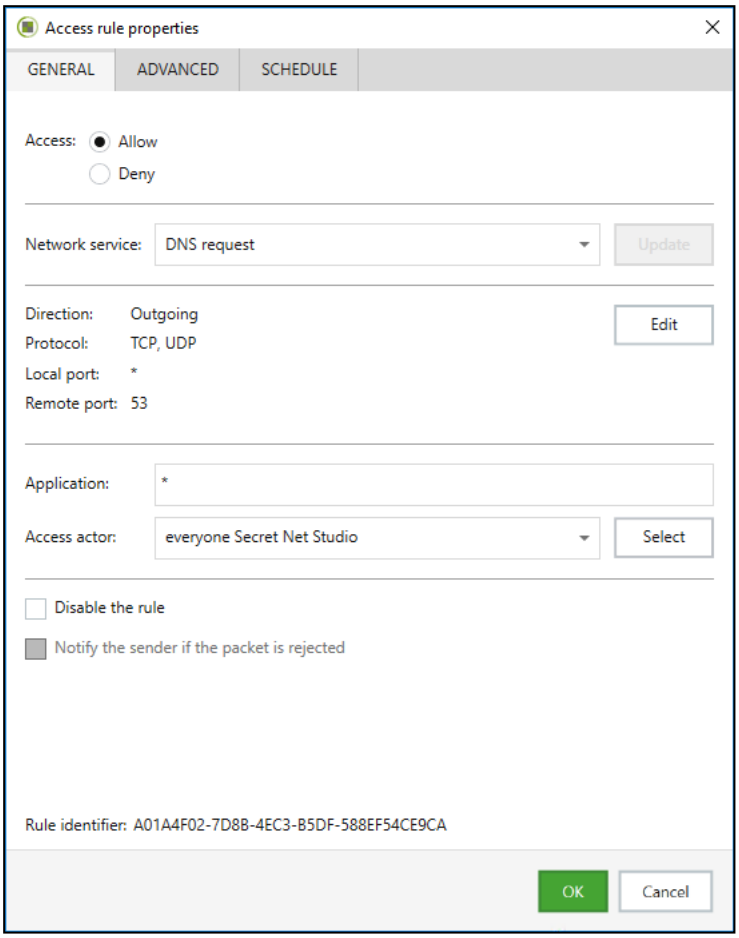
Change access rules

Access rule parameters defined during its creation can be changed.

To change rule parameters:

1. In the table, select an access rule.
2. Click **Edit**.

   The **Access rule properties** dialog box appears.



   Rule parameters in this box are the same as those described in the rule creation procedure.

3. To manage a rule:
   - select the **Disable the rule** check box to suspend the rule. The rule will be disabled;
   - clear the **Disable the rule** check box to restore the rule. The rule will be enabled.
4. Specify the required parameter values and click **OK**.

Attention! If a rule that blocks service protocols (DNS, DHCP, etc.) was created by mistake, connection with the remote computer agent may be lost. In this case, the rules must be deleted using the Control Center (see below); then, run the following command on the protected computer as the local administrator:
C:\Program Files\Secret Net Studio\Client\Components\Network Protection\ScAuthModCfg.exe /r

Deleting an access rule

To delete an access rule:

1. Select the rule.

   Tip. Use the **Ctrl** and **Shift** keys to select multiple rules.

2. Click **Delete**.

   The selected rules will be deleted.

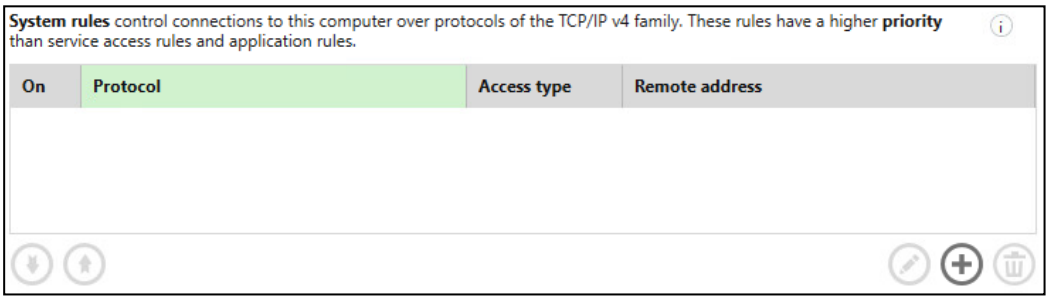
Managing system rules

System rules control connections with a computer via TCP/IP protocols. These rules have a higher priority than network service access rules and application rules.

To manage system rules:

1. Go to the **Access rules** section in the interface of the firewall configuration and click the **Show specialized access rules** link.

   A table containing the list of system rules appears.



   The following information is displayed for each rule:

Column	Value
On	Rule operation management: • **unselected** — the rule function is temporarily suspended; • **selected** — the rule is enabled
Protocol	Name of protocol subject to the rule
Access type	Type of access to a protected computer: • **allowed**; • **denied**
Remote address	Name or IP address of the computer the rule applies to, or asterisk (*) if the rule governs all remote computers

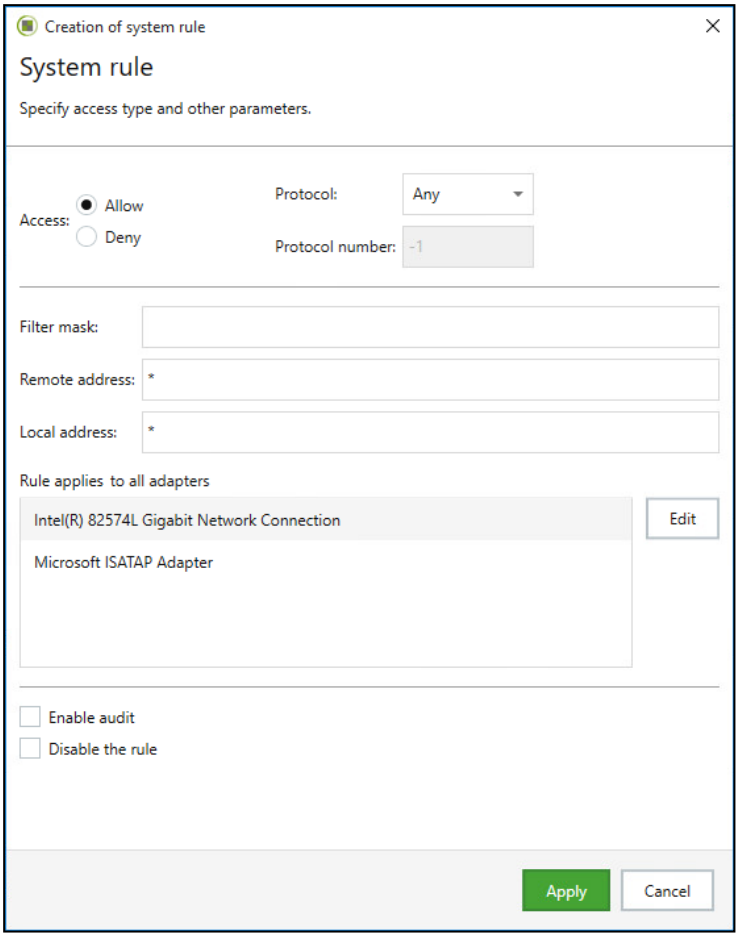
2. Perform the required actions:
   - create rules (see p. **192**);
   - edit rule parameters (see p. **193**);
   - delete rules (see p. **191**);
   - assign rule priority (see p. **182**);
   - configure ICMP protocol protection mode (see p. **205**).
3. Click **Apply**.

Create a system rule

To create a system rule:

1. Click the **Add** button.

   The **System rule** dialog box appears.



2. Specify the rule parameters and click **Apply**.

Section	Value
Access	Click the button: • **Allow** — if it is necessary to grant access to a protected object when a rule is triggered; • **Prohibit** — if it is necessary to deny access to a protected object when a rule is triggered
Protocol	Select a protocol type subject to a rule or select: • **Any** — if a rule is needed to govern all protocol types from the list; • **Other** — if the required protocol type is not in the list. In this case, the **Protocol number** box becomes available
Protocol number	If a protocol type is selected, this text box value is defined automatically and cannot be modified. If the **Protocol** box is set to **Other**, type the number of the protocol subject to the rule
Filter mask	Type a value to define the need for processing an IP packet. If the box is filled in, the rule only concerns those IP packets with contents matching the filter mask. This box supports the following special characters: • ***** — for any number of characters; • **?** — for a single character. For example, the value ***abcd*** will match any packet whose body contains the sequence abcd

Section	Value
Remote address	Type a computer name, IP address, IP address range (for example, **192.168.0.3-192.168.0.9**) or a subnet (for example, **192.168.1.0/24** or **10.10.0.0/255.255.0.0**) to define an allowable set of remote addresses. Leave an asterisk (*) character if the rule must be applied to all remote computers
Local address	Type a computer name, IP address, IP address range or a subnet to define a suitable set of local addresses. Leave an asterisk (*) character if the rule must be applied to all local computers
Rule applied to all adapters	For the rule to govern only specific adapters, click **Edit** and select the adapters
Enable audit	Manage logging of events when the rule is triggered: • **unselected** — event logging is disabled; • **selected** — event logging is enabled
Disable the rule	Rule operation management: • **unselected** — the rule is enabled; • **selected** — the rule function is temporarily suspended
Notify the sender if the packet is rejected	Managing notifications about packet blocking caused by the functioning of a blocking rule

The newly created rule will be displayed in the rules list.

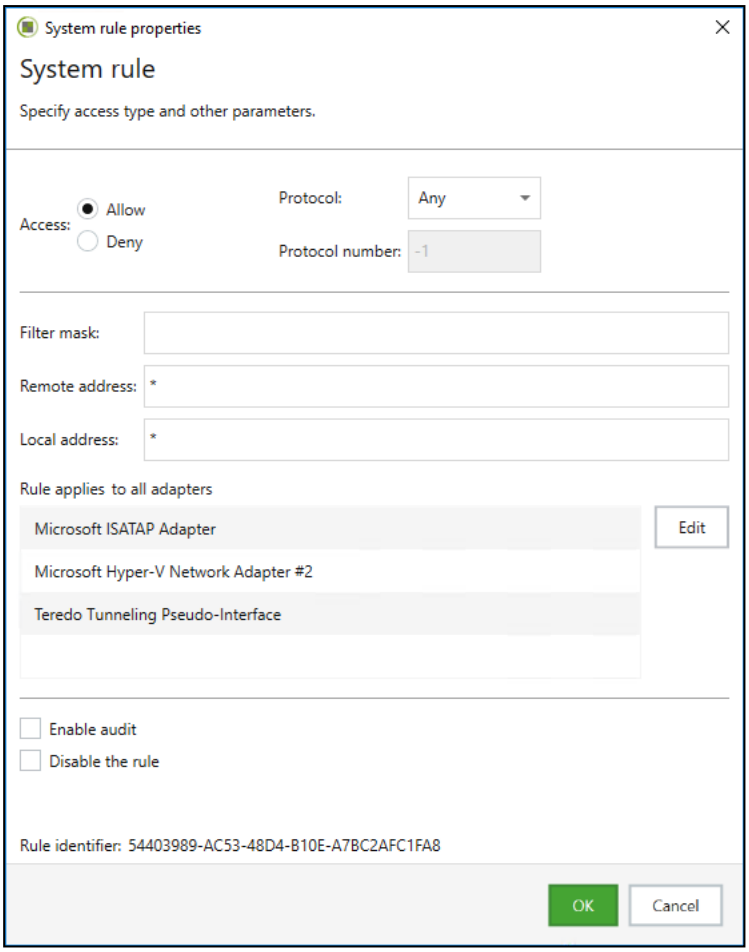
Managing system rules

The system rule parameters defined during its creation can be changed.

To change rule parameters:

1. In the table, select a system rule that you want to change.
2. Click **Edit**.

The **System rule** dialog box appears.



Rule parameters in the configuration dialog box are the same as those described in the rule creation procedure.

3. To manage a rule:
   - select the **Disable the rule** check box to suspend the rule. The rule will be disabled;
   - clear the **Disable the rule** check box to restore the rule. The rule will be enabled.
4. Change the required parameter values and click **OK**.

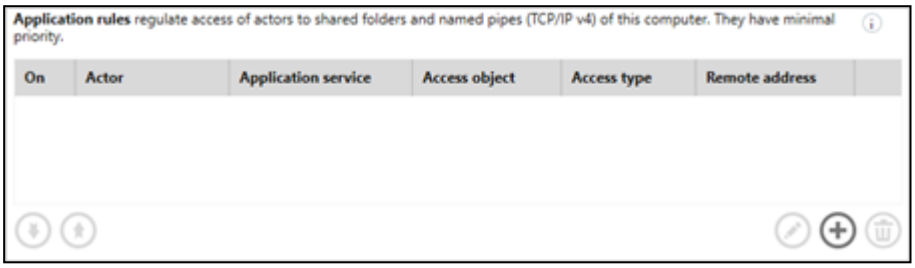
Managing application rules

Application rules govern access for authenticated and anonymous users to shared folders and named pipes on a specific computer. These rules have the least priority.

To manage the rules:

1. Go to the **Access rules** section in the interface of the firewall configuration and click the **Show specialized access rules** link.

   A table containing the list of application rules appears.



   The following information is displayed for each rule:

Column	Value
On	Rule operation management: • **unselected** — the rule function is temporarily suspended • **selected** — the rule is enabled;
Actor	Name of the account or account group the rule applies to
Application service	Name of application service: • **Shared folders**; • **Named pipes**
Access object	Name of shared folder or channel subject the rule applies to. An * (asterisk) character indicates that the rule applies to all objects of this type
Access type	Type of access to a protected computer: • **allowed**; • **denied**
Remote address	Name or IP address of the computer the rule applies to. An asterisk (*) character indicates that the rule applies to all remote computers

2. Perform the required actions:
   - create rules (see p. **195**);
   - edit rule parameters (see p. **199**);
   - delete rules (see p. **191**);
   - assign rule priority (see p. **182**).
3. Click **Apply**.

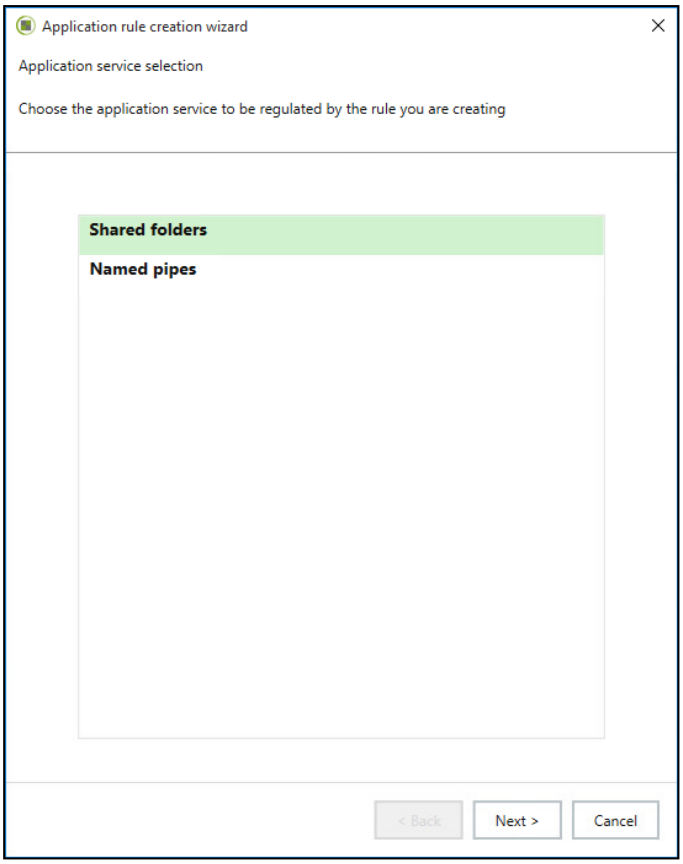
Creating an application rule

There is a special wizard for creating application rules.

To create a rule:

1. Click **Add**.

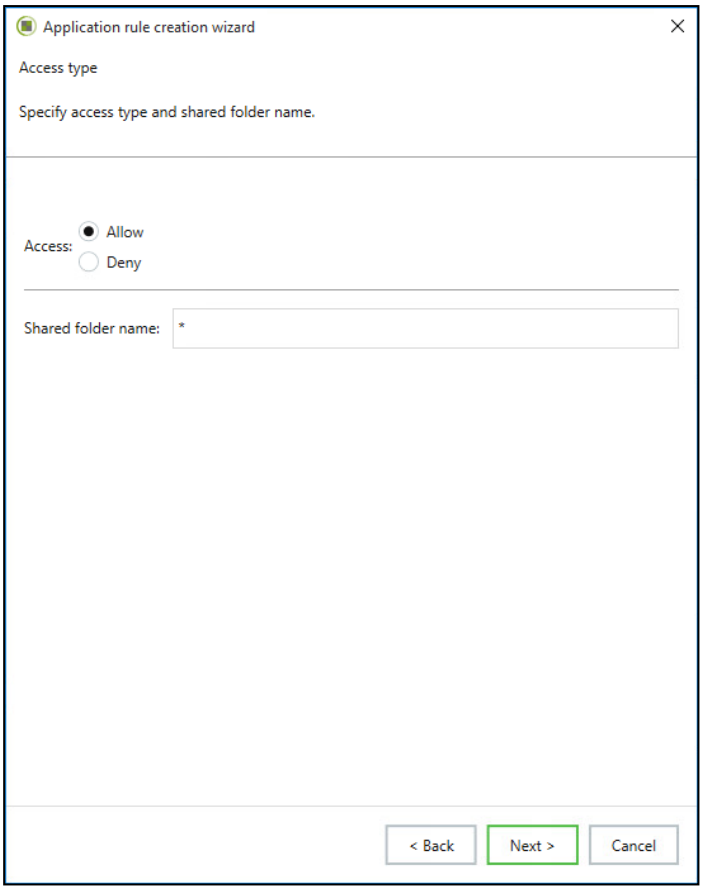
The first dialog box of the rule creation wizard appears.



2. Select an application service for which you wish to create a rule and click **Next**:
   - **Shared folders** — the new rule will govern user access to a specified shared folder via the SMB protocol;
   - **Named pipes** — the new rule will govern user access to a specified channel via **Named Pipes** protocol.

Note. Application rules enable restricting user access to shared folders and their contents (for example, **\\server\share**). Granular access control to the subfolders of shared folders (for example, **\\server\share\folder**) is not provided.

A dialog box asking you to configure the rule parameters appears.



3. Define the parameters and click **Next**.

Field	Value
Access	Select a value: • **Allow** — if it is necessary to grant access to a protected object when a rule is triggered; • **Prohibit** — if it is necessary to deny access to a protected object when a rule is triggered
Shared folder name/Named pipe	Specify the name for a folder or a pipe that is to be subject to the rule. Put an * (asterisk) character if the rule is to govern all folders or named pipes on this computer

- A shared folder name is specified without the name of the computer where it is located. For instance, if the path to the folder on the server is **\\server\share**, you only need to specify its name: **share**.
- The folder or pipe name may contain special characters: **?** (question mark) to replace a single character, and an ***** (asterisk) to replace several characters, including an empty space.
- Should access to shared folders of a protected object be restricted for all users (i.e. a blocking rule governs the **<everyone>** account where the shared folder name is specified as an ***** (asterisk)), then, users who want to browse the list of shared folders on this computer have to create an allow rule for the IPC$ shared folder.

A dialog box asking you to select accounts governed by the rule appears.

4. Specify the name of the account or account group to be governed by the rule and click **Next**.

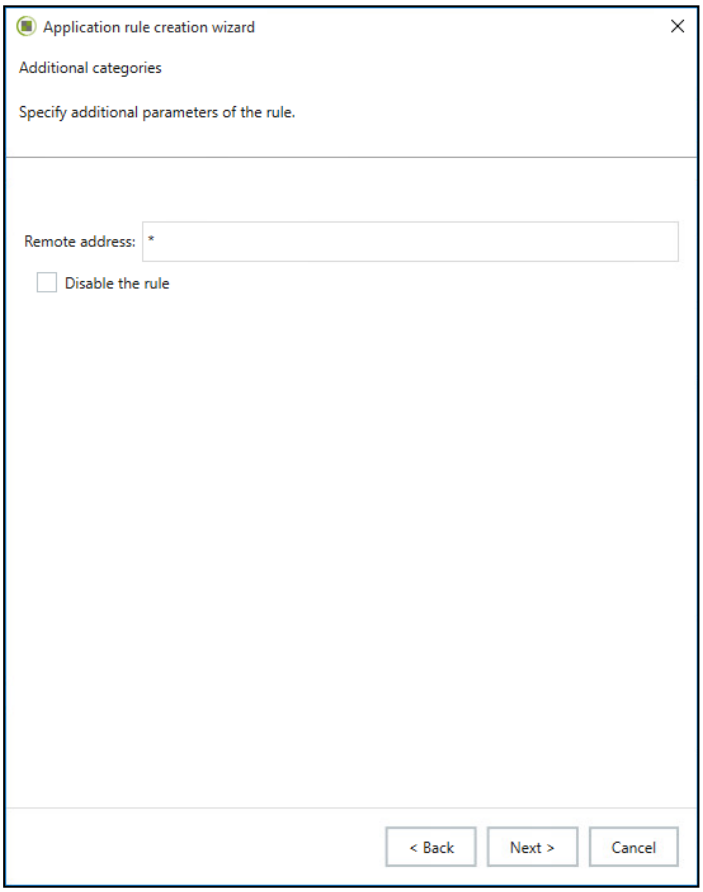
Tip. Use the **Select** button to select accounts via the standard Windows dialog box.

A dialog box prompting you to configure rule triggering notifications appears.

5. If necessary, define the rule triggering alert methods and click **Next**.

Field	Value
Enable audit	Select this check box to log the event when the rule is triggered. If event logging is not required, clear this check box
Audio alert	Select this check box if an audio alert is required to notify that a rule is triggered on a protected computer. If audio alerts are not required, clear this check box
Execute command	Select this check box to run an executable file automatically when a rule is triggered. In the text field, which becomes available when the option is selected, enter the exact path and the executable file name (with a parameter). For example, **C:\windows\notepad.exe 1.txt**
in a user session	The field becomes available once the **Execute command** option is selected. Select the user session where the specified command should be executed. • **System** — execute the command with system permissions; • **Console** — execute the command on behalf of a user during the user's session; • **All user sessions** — execute the command during all user sessions

The **Additional categories** dialog box appears.



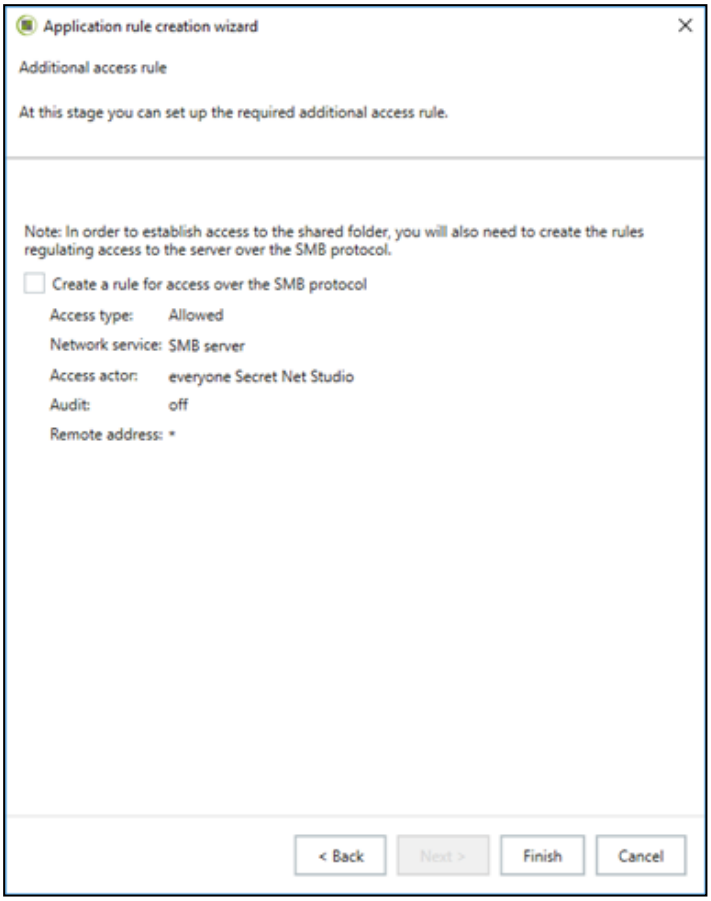
6. Specify the additional parameters for the rule and click **Next >**.

Field	Value
Remote address	Type a name or an IP address (subnet mask) for the computer that is to be governed by the rule when there is an attempt to gain access to a shared folder or a named pipe on the protected computer. Put an asterisk (*) character if a rule must govern all computers that attempt access
Disable the rule	Select this checkbox to enable the rule later

The **Rule application schedule** dialog box appears.

7. Configure the rule application schedule, if necessary, and click **Next**:
   - select the **Schedule** check box. A table enabling schedule configuration becomes available;
   - click table cells to highlight weekdays and periods of time for the rule to apply (active rule) or not (inactive rule).

   The **Additional access rule** dialog box appears.



For application rules to function properly, it is also necessary to configure the IP package pass-through rules at the transport level via SMB protocol. This also requires creating an access rule that allows packets to pass through via TCP protocol on port 445 (and/or 139) for an account (group) listed in the application rule.

Attention! If package pass-through via SMB protocol is blocked, application rules are disabled, because IP packets are blocked on the transport level.

8. If it is necessary to create an allow rule for the SMB protocol, select the **Create a rule for access over the SMB protocol** check box.
9. Click **Finish**.

   The new rule will be added to the list of application rules.

   When creating an additional SMB rule, the access rules list will also show the rule allowing an account (group) specified in an application rule to use SMB protocol.

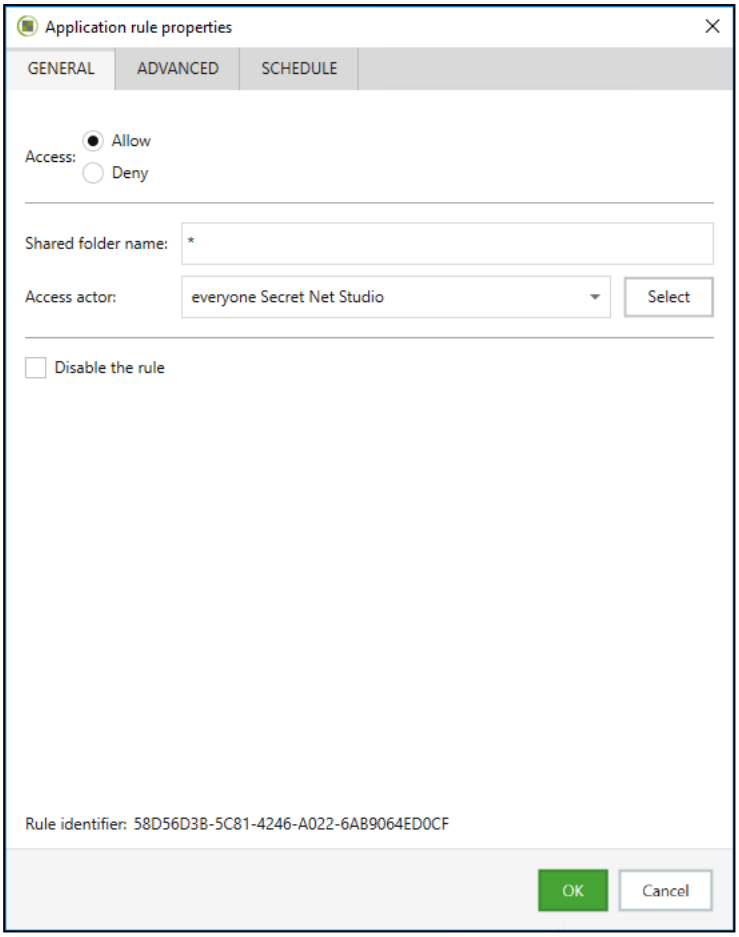
Managing application rules

The application rule parameters defined during its creation can be changed.

To change rule parameters:

1. In the table, select an application rule.
2. Click **Edit**.

   The **Application rule properties** dialog box appears.



Rule parameters in the configuration dialog box are the same as those described in the rule creation procedure.

3. To manage a rule:
   - select the **Disable the rule** check box to suspend the rule. The rule will be disabled;
   - clear the **Disable the rule** check box to restore the rule. The rule will be enabled.
4. Specify the required parameter values and click **OK**.

Managing network traffic filtering rules

Network traffic filtering rules are designed to filter network protocol commands, command parameters and to control access to resources that contain certain mobile code types.

Network traffic filtration rules are managed by the command line utility **ScAuthSrvConfig.exe** (when Secret Net Studio in the network mode) or **ScLocalSrvConfig.exe** (in the local mode).

The **ScAuthSrvConfig.exe** utility can be found on the Security Server, in the default setup folder **Secret Net Studio\Server\Authentication Server**.

Note. To enter configuration management mode, **ScAuthSrvConfig.exe** must be sent the parameters for connecting to the management server (see below).

The **ScAuthSrvConfig.exe** utility can be found on the protected computer in the default setup folder **Secret Net Studio \Client\Components\Network Protection**.

Attention! You must have local administrator rights to change local configuration via **ScLocalSrvConfig.exe**.

Connection to the management server

To enter configuration management mode, the **ScAuthSrvConfig.exe** must be sent the parameters for connecting to the management server. Open the command prompt and run the following command:

```
ScAuthSrvConfig [@argfile] [/?|h|help] [/v|version] <domain>
[/local] [kdc] [/p|password <value>] [/a|admin <value>] [/q
<value>] [/s <value>]
```

where:

- **@argfile** — read arguments from file;
- **/?** — display detailed information about the utility;
- **/v** — display the utility version number;
- **domain** — Kerberos domain;
- **/local** — local mode (configuration recovery);
- **kdc** — the Key Distribution Center location;
- **/p <value>** — domain administrator password;
- **/a <value>** — domain administrator name;
- **/q <value>** — query execution command;
- **/s <value>** — path to the script file to be executed.

Example.

Connecting to the management server running on a used computer:

```
ScAuthSrvConfig.exe DOMAINNAME 127.0.0.1 /admin Administrator
```

where:

- **DOMAINNAME** — security domain;
- **127.0.0.1** — network address of the configuration server;
- **Administrator** — Secret Net Studio administrator name.

Creating and editing network traffic filtering rules

To add a new network traffic filtering rule, open the command prompt and run the following command:

```
add network_stream_filtration_rule <protected_computer>
/filter <value> [/flt-case-insensetive | /flt-case-sensitive]
[/at allow|deny] [/order <value>] [/local_addrs <value>]
[/local_ports <value>] [/remote_addrs <value>] [/remote_ports
<value>] [/direction <value>] [/audit 1|0] [/enable 1|0]
```

The following rule parameters are available:

Parameter	Description	Available values
add network_ stream_filtration_ rule or add nsfr	Command to create a filtering rule	
modify network_ stream_filtration_ rule or modify nsfr	Command to edit a filtering rule	
protected_computer	Full domain name of a protected computer the rule will be applied to	
filter	Filter mask	• ***** — for any number of characters; • **?** — for a single character
flt-case-insensitive	Case insensitive search	

Parameter	Description	Available values
flt-case-sensitive	Case sensitive search. Default value	
at (access type)	Access rule type	• **deny** — the connection will be terminated if a sequence that fits the filter mask is found. Default value; • **allow** — only audit (if allowed) will be performed if a sequence that fits the filter mask is found
direction	The list of connection (network traffic) directions to which the rule will apply. ";" is used as a separator	• **in** — the rule will be applied to incoming connections, incoming traffic. Default value; • **in_reply** — the rule will be applied to incoming connections, response traffic. • **out** — the rule will be applied to outgoing connections, outgoing traffic. • **out_reply** — the rule will be applied to outgoing connections, response traffic
local_addrs	The list of local addresses/networks/ranges for which the rule applies. ";" is used as a separator	
local_ports	The list of local ports/ranges for which the rule applies. ";" is used as a separator	
remote_addrs	The list of remote addresses/networks/ranges for which the rule applies. ";" is used as a separator	
remote_ports	The list of remote ports/ranges for which the rule applies. ";" is used as a separator	
audit	Enable/disable audit when the rule is triggered	• **1** — audit is enabled; • **0** — audit is disabled
order	Rule application procedure. The parameter only affects rule triggering	
enable	Current rule status	• **1** — the rule is enabled; • **0** — the rule is disabled

The following command is used to edit a filtering rule:

```
modify network_stream_filtration_rule(nsfr) <protected_
computer> <rule_id> [/filter <value>] [/at allow|deny]
[/order <value>] [/local_addrs <value>] [/local_ports
<value>] [/remote_addrs <value>] [/remote_ports <value>]
[/direction <value>] [/audit 1|0] [/enable 1|0]
```

where **<rule_id>** is the identifier of the rule to be modified.

Examples

Example 1. Single command filtering

Creating a rule to be applied to outgoing network connections through port 23. The rule is triggered when identified in the outgoing **cmd** command:

```
add nsfr SP-VM01 /filter "cmd1" /direction out /remote_ports
23
```

Example 2. Filtering a sequence of commands.

Creating a rule to be applied to outgoing network connections through port 23. The rule is triggered when a sequence of **cmd1**, **cmd2** and **cmd3** commands is identified in outgoing data. Any number of characters can be between these commands.

```
add nsfr SP-VM01 /filter "cmd1*cmd2*cmd3" /direction out
/remote_ports 23
```

Example 3. Filtering a command parameter

Creating a rule to be applied to outgoing network connections through port 23. The rule is triggered when the **cmd** command with the **param** parameter is identified in outgoing data.

```
add nsfr SP-VM01 /filter "cmd*param" /direction out /remote_
ports 23
```

Example 4. Filtering access to resources that contain certain mobile code types

To filter access to resources that contain certain mobile code types, network traffic filtering rules are used. As a filter, these rules contain text sequences that are typical for a certain type of mobile code. For example, to prohibit a mobile code in the HTTP protocol, you will need to create rules for outgoing connections, for response traffic with filtering by **Content-Type** header. Extra filtering can be applied by checking the **Content-Disposition** heading and its **filename** parameter.

List of **Content-Type** headers for various mobile code types:

Mobile code type	Filtered string
JavaScript	Content-Type: text/javascript Content-Type: text/jscript Content-Type: text/x-javascript Content-Type: text/ecmascript Content-Type: text/x-ecmascript Content-Type: application/javascript Content-Type: application/x-javascript Content-Type: application/ecmascript Content-Type: application/x-ecmascript
Adobe Flash	Content-Type: application/x-shockwave-flash
VBScript	Content-Type: text/vbscript
Java	Content-Type: application/java-archive Content-Type: application/jar
ActiveX	Content-Type: application/ocx Content-Type: application/x-ms

An example of creating a set of mobile code filtering rules:

```
add nsfr SP-VM01 /filter "Content-Type: application/ocx"
/flt-case-insensitive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter "Content-Type: application/x-ms"
/flt-case-insensitive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter " Content-Disposition*filename*ocx"
/flt-case-insensitive /direction out_reply /remote_ports 80
```

The rules block loading Active-X components via HTTP protocol, port 80.

Viewing network traffic filtering rules

To view the list of network traffic filtering rules, run the following command:

```
show network_stream_filtration_rules(nsfrs) <protected_
computer>
```

where **<protected_computer>** is the protected computer name.

Example.

```
show nsfrs SP-VM01
id {ca541ade-b955-4cf2-8894-d020aac9d9ac}
order 124000
access deny
content-filter cmd1*cmd2*cmd3
direction out
proto 6
local-addr *(*)
remote-addr *(23)
```

Use the following command to view detailed information about an individual rule for filtering network traffic:

```
show network_stream_filtration_rule(nsfr) <protected_
computer> <id>
```

where:

- **<protected_computer>** is the protected computer name.
- **<id>** — rule identifier.

Example.

```
show nsfr SP-VM01 {ca541ade-b955-4cf2-8894-d020aac9d9ac}
server: sp-vm01
id {ca541ade-b955-4cf2-8894-d020aac9d9ac}
order 124000
access deny
content-filter cmd1*cmd2*cmd3
enabled 1
direction out
proto 6
local-addr *(*)
remote-addr *(23)
audit 1
```

Deleting network traffic filtering rules

To delete a network traffic filtering rule, run the following command:

```
delete network_stream_filtration_rule(nsfr) <protected_
computer> <id>
```

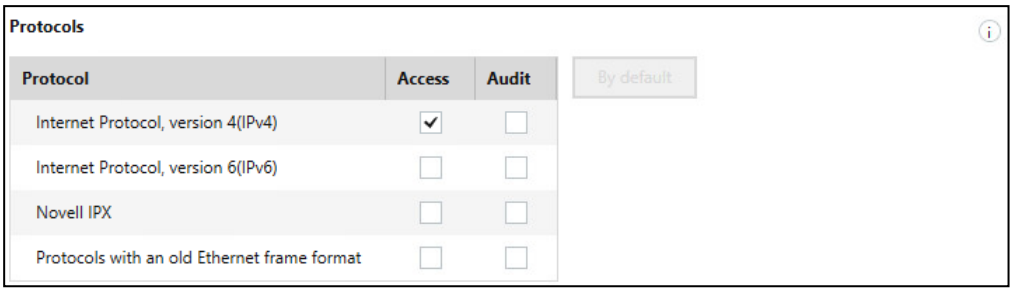
Managing network protocols

The Secret Net Studio configures access to protected computers via IPv4, IPv6, Novell IPX network protocols, as well as other protocols with older Ethernet frame format (LLC, IPX). These protocols, apart from IPv4, are blocked by default. These

settings have a higher priority than network service access rules, application rules and system rules.

To manage network protocols:

1. Open the **Protocols** section on the interface of the firewall configuration.



2. In the **Access** column, clear the check boxes to disable protocols. Select the check boxes to enable these protocols.

   Attention! By default, access to protected computers is only granted via the IPv4 protocol. It is not recommended to enable other protocols, as the traffic will not be monitored by the Secret Net Studio firewall.

3. In the **Audit** column, select the protocols for which events must be logged for every packet that passes through. If event logging is not required, clear this check box.

   The audit (event logging) mode for all protocols is disabled by default.

   Attention! When audit mode is enabled, the number of events logged by Secret Net Studio will be very big. This may cause the system to slow down.

   Comment. The **Audit** check box value in the protocol settings is not associated with the **Enable audit** value specified in the access rule properties.

4. To save the new parameter values, click **Apply** at the bottom of the **Settings** tab.

   Tip. Use the **By default** button to restore the table's original version.

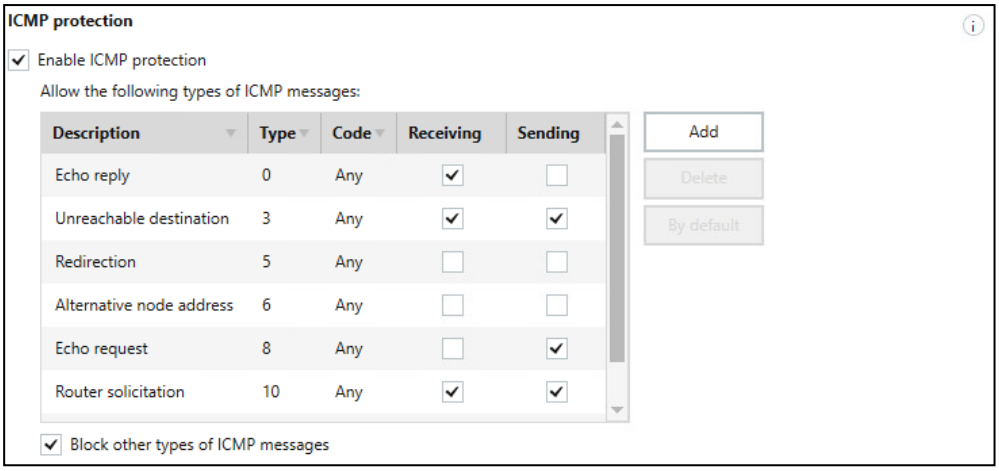
Note. The **Protocols with old Ethernet frame format** option makes it possible to block Ethernet frames which contain a frame value in the heading instead of its type. Through such frames, IPX, SMB over NetBEUI and event IP traffic can reach the protected server.

Configuring ICMP protocol protection mode

The ICMP protocol protection mode is used to exchange messages via this protocol. The ICMP protocol packet management mode is disabled by default.

To configure mode parameters:

1. Go to **ICMP protection** section in the interface of the firewall configuration.


ICMP protection
Enable ICMP protection
Allow the following types of ICMP messages:
Description
Type
Code
Receiving
Sending
Echo reply 0 Any
Unreachable destination 3 Any
Redirection 5 Any
Alternative node address 6 Any
Echo request 8 Any
Router solicitation 10 Any
Add
Delete
By default
Block other types of ICMP messages

ICMP protocol packet types are shown as a table. The following information is displayed for each type:

- packet type description;
- packet type;
- packet code;
- means to manage packet pass-through.

2. Configure the necessary parameters.

Parameter	Value
Enable ICMP protection	Select this check box if it is necessary to enable ICMP protection
Receiving and Sending columns	Allow or prevent incoming and outgoing packets to pass through. To allow, select the corresponding check box; clear to prevent it
Block other types of ICMP messages	Select this check box to prevent all ICMP packet types passing through, except for the types specified in the table. If you need to allow packets to pass through, clear the check box

Tip. Use the buttons on the right to add ICMP message types (**Add**), delete selected rows (**Delete** — you cannot delete default rows) or restore the table to its default settings (**By default**).

3. To save the new parameter values, click **Apply** at the bottom of the **Settings** tab.

   ICMP protocol packet processing mode will be configured according to the specified parameter values.

Managing network services

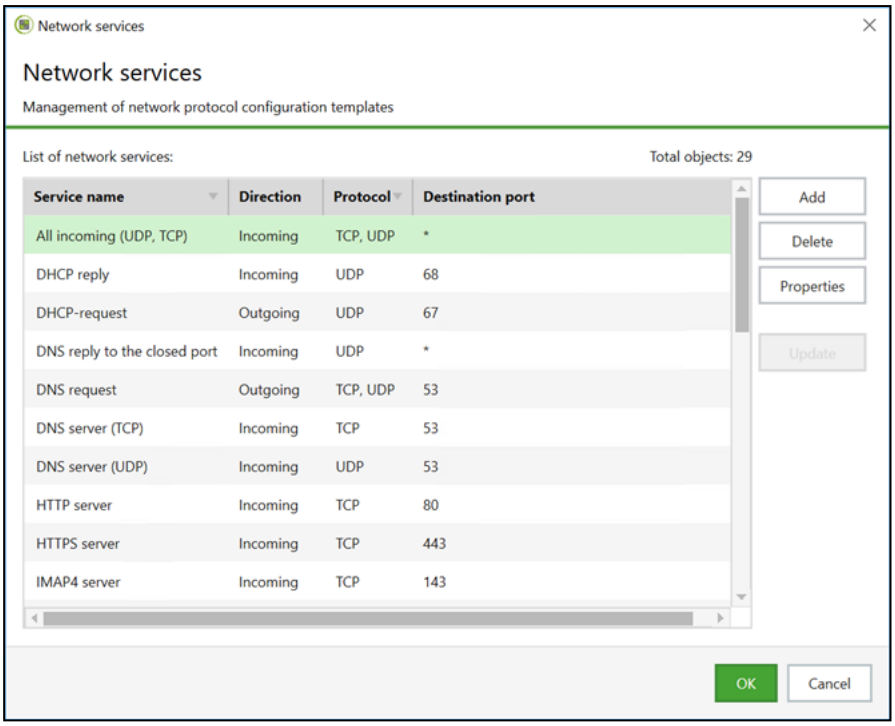
Network services are a list of the most common network protocol templates. The following information is displayed for each service:

- network service name;
- traffic direction governed by the network service;
- network service protocol type;
- computer port governed by the network service.

To manage network services:

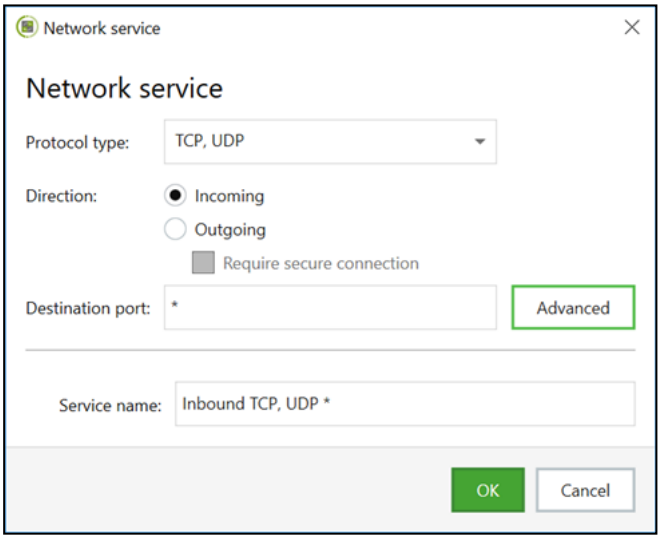
1. Click the **network services** link in the **Access rules** section of the firewall configuration interface.

The **Network services** dialog box appears.



2. To create a network service, click **Add**.

   The **Network service** dialog box appears.



3. Specify the required parameters and click **OK**.

Field	Value
Protocol type	Select the type of protocol for the network service
Direction	Click one of the buttons to specify a traffic direction for the network service: • **Incoming**; • **Outgoing**
Require secure connection	If a secure connection is required for the network service, select this check box (see p. **214**)

Field	Value
Destination port	Type the numbers of the ports for the network service: • for incoming traffic, specify the ports numbers which receive the IP packets; • for outgoing traffic, specify the ports numbers to which the IP packets are sent; • leave an asterisk (*) symbol if the service must govern all computer ports. Use "," as a separator. Use "-" (hyphen) to specify a range of ports. Click **Advanced**to configure a list of ports in the pop-up dialog box
Service name	Enter a name for the network service template to be saved

A network service will be created and displayed in the network service list.

4. To delete a network service, select it from the list and click **Delete**. The selected network services will be deleted.
5. To modify the parameters of a network service, select the required one from the list and click the **Properties** button. In the pop-up window, change the required service parameters based on the description in step **3** of this procedure, and click **OK**.
6. Click **OK** in the pop-up window to save changes.
7. Click **Apply** at the bottom of the **Settings** tab.

Stateful Packet Inspection

Stateful Packet Inspection protects computers from network attacks by filtering the passing traffic. Parameters allow to maintain a state table of the active sessions, examines the contents of IP packets for compliance with the table and drops packets that do not correspond to the current state of the connection.

By default, stateful packet inspection is disabled.

To enable stateful packet inspection:

1. Go to the **Stateful Packet Inspection** section of the firewall configuration.

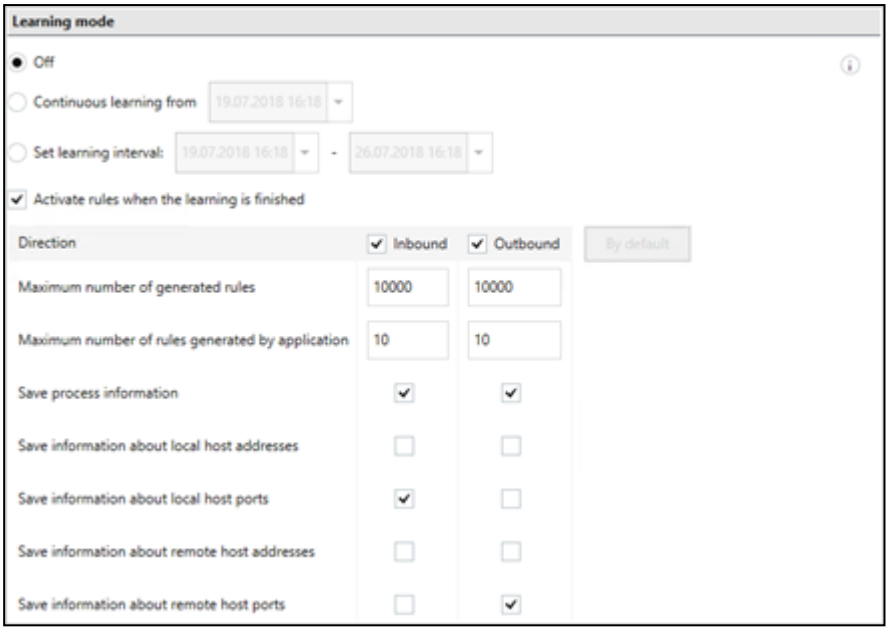
2. If it is necessary to enable stateful packet inspection, select the **Enable Stateful Packet Inspection** check box.
3. If necessary, select the **Block packets that do not match the state table** check box.

Configuring learning mode

The learning mode is used when launching the protection system stage. This mode allows a base set of access rules to be composed that are required for the protected computer to function. Access rules are composed based on the network activity information of applications installed on this computer.

To configure mode parameters:

1. Go to the **Learning mode** section of the firewall configuration.



2. If it is necessary to enable learning mode, click **Continuous learning from** or **Set learning interval** and specify the start date or an interval for this mode to be active.
3. Configure the learning mode parameters.

Field	Value
Activate rules after the end of learning	Select this checkbox if you want all rules composed during the active period of the learning mode to apply upon the its completion
Direction	Specify the traffic direction to apply learning mode to
Maximum number of rules to be generated	Type the maximum number of rules to be generated while the learning mode is active
Maximum number of rules that can be generated for the application	Type the maximum number of rules to be generated while the learning mode is active for each application
Save information about the process	Select this checkbox for the generated rules to be active for particular applications whose processes caused network activity. If the checkbox is left clear, rules will be generated for all applications
Save information about remote/local host ports/addresses	Select the corresponding check boxes to save the necessary information in the rules

Tip. Use the **By default** button to restore the table's original version.

4. To save the new parameter values, click **Apply** at the bottom of the **Settings** tab.

   Learning mode will be configured based on the defined parameter values.

Managing the firewall on protected computers

The Secret Net Studio Control Center makes it possible manage learning mode on a single computer.

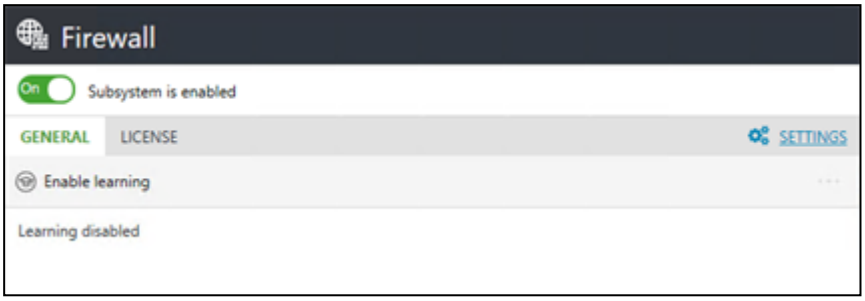
To manage the firewall:

1. In the object list right-click the computer you need to configure and click **Properties**.

   An information window with computer status appears.

2. Open the **Status** tab and select the **Firewall** element.

   The firewall control panel appears.



3. To enable/disable firewall, move the switch to the **On/Off** position.
4. To manage the learning mode, click the button:

- **Enable learning** — to enable the learning mode. After that, the following two buttons appear in the panel;
- **To interrupt learning and save rules** — to disable the learning mode and save rules formed during the learning;
- **To interrupt learning without saving rules** — to disable the learning mode and delete rules formed during the learning.

Learning mode allows you to create a basic set of access rules (see p. **209**).

Note. Click the **Settings** link to configure local firewall policies.
To see current license information, select the **License** tab and click **Go to the license information** link.

Chapter 18
Network Authentication

Secret Net Studio has a network protection mechanism implemented for authorized subscribers. This mechanism operates based on the IPsec framework of open standards and ensures data exchange security.

Subscriber authorization is based on the Kerberos protocol. This protocol is highly resistant to Man-in-the-middle attacks and password interception attempts. This mechanism provides authorization of access subjects as well as secure objects. This prevents unauthorized imitation of a secure information system, used in certain attacks.

The network authentication mechanism performs the following functions:

Function	Description
Network connection authorization	Adds service data to network packets that meet rules acquired from the control and authorization server. Analyzes incoming packet service data along with the transfer of information to the firewall module to ensure rule-based filtering
Inalterability control for transferred network packets	Ensures authenticity, integrity and confidentiality of transferred data
Traffic encryption	Ensures cryptographic protection of network traffic

The network authentication mechanism is configured centrally via the Control Center. Configuration is performed at the Computer object level, separately for each protected computer.

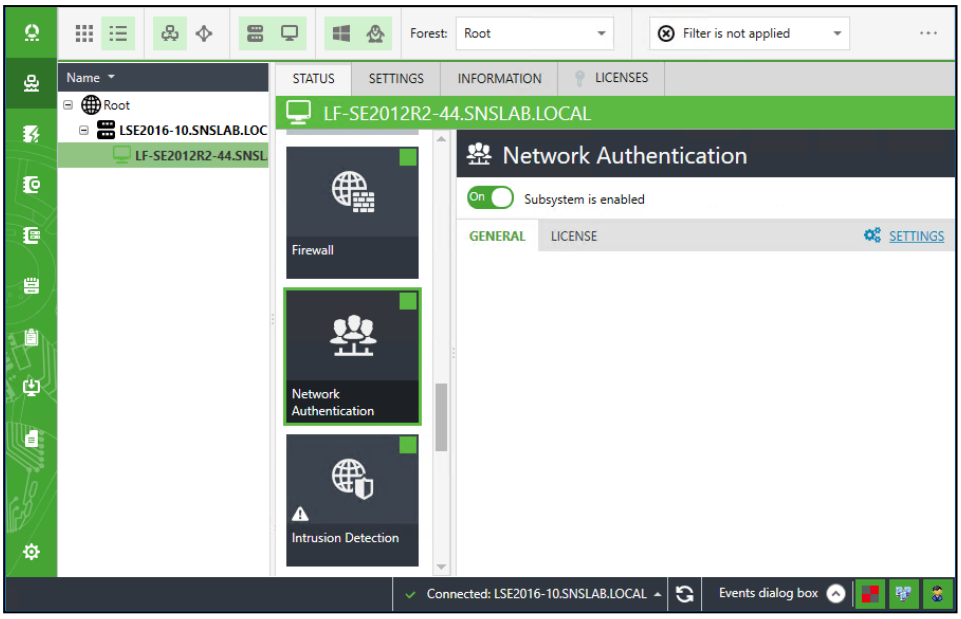
Note. Secret Net Studio also includes the Local Control Center component. This component allows you only to view network authentication mechanism settings on a protected computer.

Attention! The configuration of the network authentication mechanism from a Windows local user account is not supported.

To configure these parameters:

1. Open the Control Center.

The main program window appears.



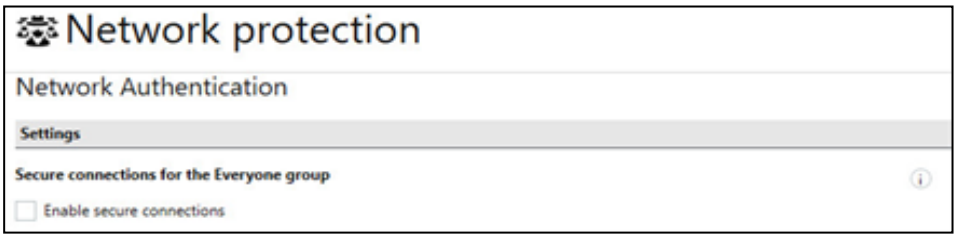
Tip. To view network authentication mechanism settings directly on a protected computer, open the Local Control Center, click the **Settings** tab and select the **Network authentication** element in the **Policies** section. Parameters cannot be configured in the local mode.

2. Open the **Computers** view and select the computer you need on the left side of the window. Right-click the selected computer and click **Properties**.

   Computer status appears on the right side of the window.

3. Select the **Settings** tab. If necessary, click **Load settings**. In the **Policies** section, click **Network authentication**.

   Interface for authentication mechanism configuration appears on the right side of the window.



4. Configure the required parameters and click **Apply** to save changes.

Configuring connection protection for the <everyone> group

To allow network connection protection in access rules configured for the **<everyone>** group, select the **Enable connection protection** check box, and click **Apply** at the bottom of the **Settings** tab.

Configuring packet processing parameters

Secret Net Studio has a networking protection mechanism for authorized subscribers. This mechanism based on the IPsec framework open standards and ensures data exchange security.

The current version uses the following protocols:

Name	Description
AH (Authentication Header) protocol	Guarantees transferred data authenticity and integrity for each IP packet. Ensures protection against the Man-in-the-middle attacks
ESP (Encapsulating Security Payload) protocol	Encodes and controls transferred data integrity
ISAKMP (Internet Security Association and Key Management Protocol)	Ensures key exchange and connection parameter regulation

There are several configuration modes. The Administrator can set an individual protection mode for each protected computer.

The network authentication default parameters are configured as follows:

- the packet signature mode with **Whole packet** signature level is enabled;
- anti-replay-attack protection mode is enabled;
- the SMB connection user defining scenario is run as a user account.

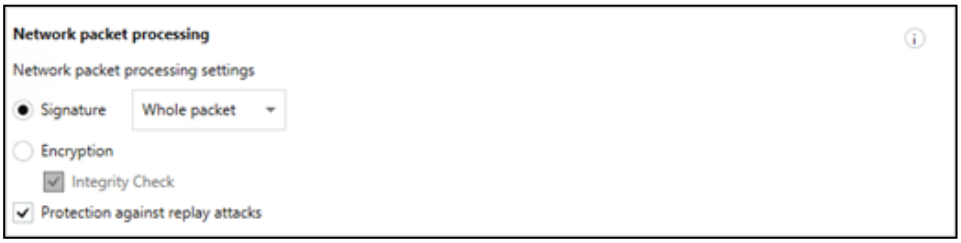
Transferred data protection and integrity is ensured through:

- packet signature mode — AH protocol in transfer mode, hashing algorithm: HMAC-MD5;
- encryption and integrity control mode — ESP protocol in transfer mode, encoding algorithm — AES CBC 128, hashing algorithm: HMAC-SHA;
- anti-replay-attack protection mode: ISAKMP.

Note. The current version of the Secret Net Studio does not allow simultaneous use of AH and ESP protocols.

To configure these parameters:

1. In the **Network authentication** menu, select the **Settings > Network packet processing** section:



2. Configure the network packet protection parameters.

Attention! To establish a secure connection:
- configure access rules for a remote receiving computer required exchanging data with a sending computer (see p. 182);
- enable IP packet signature mode on the sending computer.

If any of these conditions are skipped, a secure connection cannot be established.

Parameter	Description
Signature	Select this option button to enable packet signature mode, then select a signature level: • **Only marking** — only the first packet in the series is signed, the rest are marked to be identified as part of an authenticated series; • **Packet headers** — headers of each packet are signed; • **Whole packet** — each packet is signed as a whole. Whether an outgoing packet is signed or not is defined by the security parameters of the remote computer (IP packet receiver). If the receiving computer allows data exchange with the sending computer and the corresponding rules are configured, all packets sent to the receiving computer will be signed once the packet signature mode is enabled
Encryption	Select this option button to enable data encryption
Integrity Check	Select this check box to enable integrity check for encoded packets. If integrity check is not required for packets, clear the **Integrity Check** check box
Protection against replay attacks	Select this check box to activate the protection mode that will prevent passive data capture and transmission

3. Click **Apply** at the bottom of the **Settings** tab.

Configuring an SMB connection

There are the several scenarios in Secret Net Studio for determination the user of an SMB connection:

- the computer account is always considered as an SMB connection user;
- a connection user is the account of a user who initiates it. Note that other users are either authorized or unauthorized to use an established SMB connection.

All activity of users authorized to use this connection type occurs through the account of the initiating user. If a connection-initiating user is inactive for more than 30 seconds, the next user or service in line requiring an SMB connection is considered as the actual connection user.

Priority to be provided with an SMB connection (bottom to top): anonymous users, services, authorized Secret Net Studio users.

When implementing a scenario where a connection user is a connection-initiating user, other users are:

- authorized to use the SMB connection — all low priority subscriber activity occurs through the higher priority subscriber;
- unauthorized to use an SMB connection — upon request of a higher priority subscriber to use a connection, it becomes unavailable to lower priority subscribers.

To select a scenario:

1. Go to the **Settings > Scenario for SMB connection user definition** section.

Note. If an SMB connection is created before the mechanism component is launched (e.g., a mapped drive with the selected **reconnect at login** check box), the priority of service equals that of the users, and all further connections will occur through the computer account.

2. Specify a scenario to define an SMB connection user.

Parameter	Description
As computer account	Select this option button for SMB connections to be established under the computer account
As user account	Select this option button for SMB connections to be established under the user account
Block SMB traffic of other users	Select this check box for SMB connections to be restricted for all, except the connection initiating user

Comment. All users will be granted access to an object through a single account (the first that accesses to the terminal server) under the following condition:

- access to a protected object is granted through a terminal server;
- the SMB connection is established under a user account;
- the **Block SMB traffic of other users** check box is unselected.

If the **Block SMB traffic of other users** check box is selected, a connection will only be accessible to the user who initiated the connection to the terminal server.

If computer accounts are used, all users of the terminal server will be granted access to a protected object through the same single account.

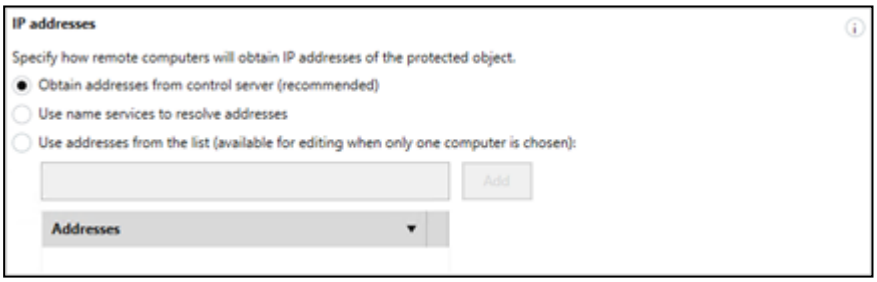
3. To save the new parameter values, click **Apply** at the bottom of the **Settings** tab.

Configuring the computer's IP address acquisition parameters

Secret Net Studio network protection tools allow a computer to be identified by both its name and its IP address. It can be used when a computer name is not automatically converted to an IP address.

To configure these parameters:

1. In the **Network authentication** menu, go to the **Settings > IP addresses** section.



2. Configure the parameters.

Parameter	Description
Obtain addresses from control server	By default, the Clients will automatically acquire IP addresses for a protected computer from the Security Server governing this computer
Use name services to resolve addresses	Select this option button for the Clients to refer to the DNS, WINS and NetBIOS services to acquire addresses
Use addresses from the list	Select this option button if you want to explicitly specify the addresses. Type the IP address of a protected computer in the text box and click **Add**. To remove the entered IP address, select it from the list and click **Delete**

3. To save the new parameter values, click **Apply** at the bottom of the **Settings** tab.

Managing the network authentication mechanism on protected computers

The Control Center makes it possible to manage the work of the network authentication mechanism on a single selected computer.

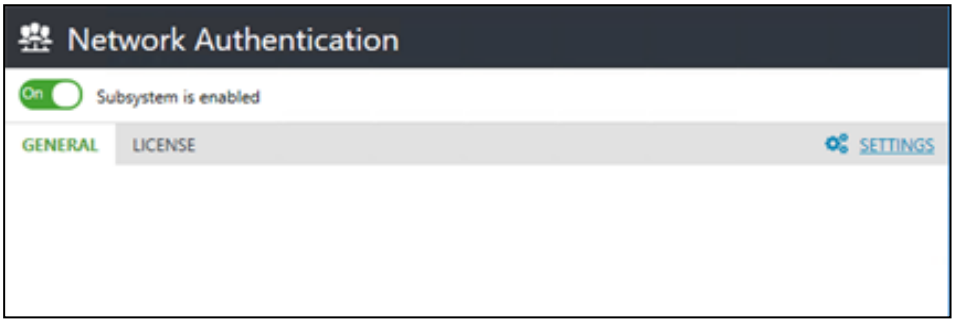
To manage the network authentication mechanism

1. Select the computer from the object list, right-click the selected computer and click **Properties**.

   An information about the computer status appears.

2. In the **Status** tab, select the **Network authentication** element.

   A control panel to manage the network authentication mechanism appears.



3. To enable/disable network authentication, move the switch to the **On/Off** position.

Note. Click the **Settings** link to configure local firewall policies.
To see current license information, select the **License** tab and click **Go to the license information** link.

Chapter 19
Antivirus

Secret Net Studio antivirus enables you to check file objects for malware registered in the signature database and via heuristic data analysis. When scanning the PC, hard drives, network folders, external drives and other objects are scanned. Antivirus detects and blocks the external and internal attacks targeted at protected computers.
To ensure the antivirus protection, you can use one of the following antivirus options:

- Antivirus;
- Antivirus (Kaspersky technology).

Antivirus is specified by the Secret Net Studio license.

You can configure the antivirus in the centralized mode using the Control Center, which can be performed at different levels of the control object structure:

- at the Domain, Security Server and Organizational unit object levels you can configure the antivirus parameters based on group policies. The parameter values set for the Security Server level have a higher priority over those set for the Computer object level;
- at the Computer object level you can configure the antivirus parameters for a single computer and to perform certain antivirus operations (e.g. scan, manage quarantined objects, etc.) on this computer.

Note. Secret Net Studio also includes the Local Control Center. This component allows managing the Antivirus on a protected computer.

All subsystem activity data is registered in the Secret Net Studio log.

Configuring group policies

Antivirus functional parameters are presented in the following groups:

- scan profiles. A scan profile is a set of predefined scanning parameters to be applied for a system check in the respective mode;
- the scan schedule determines time and period of the check respectively with a selected scanning profile;
- exceptions determine the list of files and folders to ignore during the check.

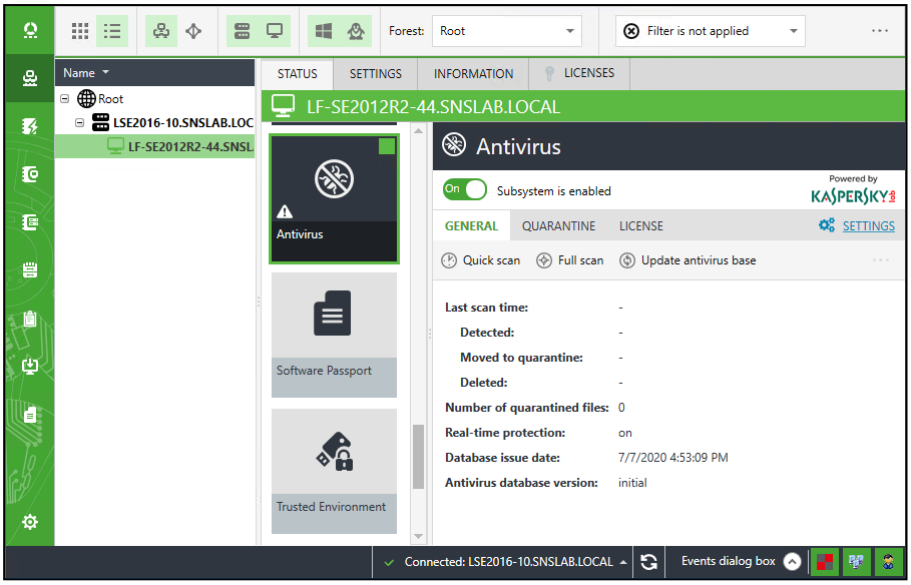
To configure these parameters:

1. Open the Control Center.

   Tip. To configure antivirus settings directly on a protected computer, open the Local Control Center, on the **Computers** panel click the **Settings** tab. In the **Policies** section, click **Antivirus**. Further configuration is similar in centralized mode.

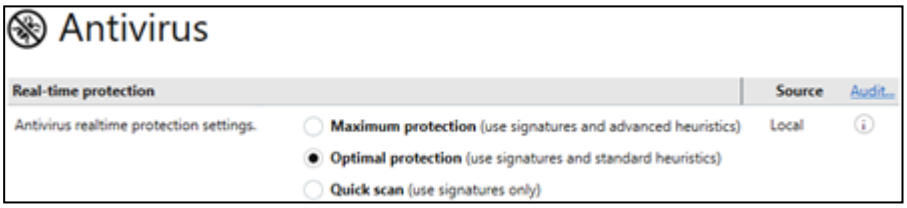
   The main program window appears.
2. Click **Computers** on the **Computers** panel, right-click the needed object and click **Properties**.

   An information message showing the object status appears as in the figure below.



3. Select the **Settings** tab. If necessary, click **Load settings** . In the **Policies** section, click **Antivirus**.

   A dialog box appears as in the figure below.



Tip. If you are configuring group policy, turn on the switch in the upper left corner of the needed settings section.

4. Configure the required parameters and click **Apply**.

Scan profiles

Secret Net Studio contains the following scan mode profiles:

Name	Purpose
Real-time protection	This profile defines the scanning parameters for system objects in real time. Computer viruses are detected using signature and heuristic methods when attempting to access executable files, documents, images, archives, scripts, and other types of potentially dangerous files
External drive scanning	Defines automatic scanning parameters for all external drives. Works only with **Real-time protection**
Context scanning	This profile defines the parameters for scanning initiated by the user via the Windows Explorer context menu
Full scan	This profile defines the parameters for scanning initiated by the administrator through the Control Center or schedule. In this mode, all active processes, automatic startup parameters and boot sectors are checked
Quick scanning	This profile defines the parameters for quick scanning initiated by the administrator through the Control Center, by a user on a protected computer or schedule. In this mode, the system is quickly scanned to detect any vulnerabilities. System vulnerabilities include active memory processes, vulnerable files and folders, as well as removable media
Mail antivirus	This profile defines the parameters for scanning message attachments in Microsoft Outlook for malware. Mail antivirus supports Microsoft Outlook versions 2013-2019 and 365

Note. For the correct operation of Secret Net Studio mail antivirus, Internet Explorer version 11 is required.

Configuring scan profiles

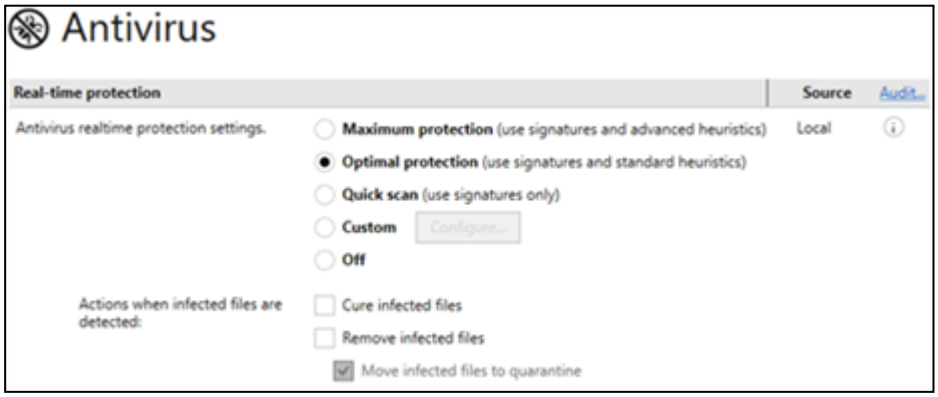
Select a category to configure in the parameter settings menu.

Profiles have the following common settings:

Parameter	Description
Heuristics	Choose an heuristic level: • **Advanced** — a high probability of detecting unknown viruses, high false-detection rate. The scan in this mode is slower than in normal mode; • **Standard mode** — limited heuristics: lower probability of detecting unknown viruses, lower false-detection rate; • **Off** — heuristic scan is disabled
Actions when infected files are detected	Actions to be performed upon detection of infected files. • **Cure infected files** — choosing this option will initiate an attempt to cure infected files; • **Remove infected files** — infected files will be deleted; • **Move infected files to quarantine** — deleted files will be moved to quarantine. Files remain in their original location, but their attribute is changed to **Hidden** and **.quarantine** will be added to the file name. Quarantined files can be restored in the future, if necessary (see p. **227**)
Files	Configure the parameters of files to be ignored during scanning: • **Skip files larger than** — if selected, specify the size of files to be ignored during scanning; • **Maximum file scan time** — if selected, a file scan time will not be longer than the specified value. Select the check box **Scan archives** and configure additional parameters: • **Skip files larger than** — if selected, specify the size of archives to be ignored during scanning; • **Maximum archive scan time** — if selected, an archive scan time will not be longer than the specified value; • **Maximum archive nesting**— if selected, objects deeper than the specified nesting level will be ignored. By default, archives scanning is enabled. You can also configure the scan parameters for files with different extensions: • **Scan all files** — if selected, all files scan will be scanned; • Scan only files with the following extensions — only files with specified extensions will be scanned. Specify file extensions, use characters "?" and "*", if necessary. Use a comma to separate; • **Skip files with the following extensions** — files with specified extensions will be ignored; Specify file extensions (use a comma to separate)

Below you will find information on how to configure individual settings of the scan profiles.

Real-time protection



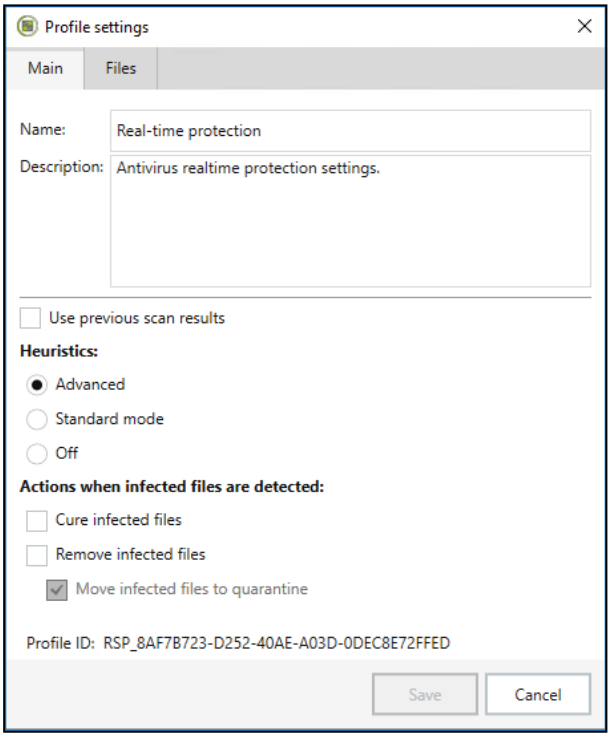
To configure real-time protection parameters:

1. Define the antivirus protection level during a real-time scan.

- **Maximum protection** — Secret Net Studio scans all files on any access attempt, and scans all local and external drives. The scanning involves advanced heuristic analysis of new threats (see p. 220).
- **Optimal protection** — Secret Net Studio scans files with the following extensions: zip, xl*, ws*, vxe, vxd, vb*, tsp, tmp, th*, ta*, sys, swf, sl*, sh*, scr, sc*, rtf, reg, ra*, prg, prf, pp*, png, pif, ph*, pdf, otm, osx, om, ms*, md*, lnk, js*, jp*, isp, ins, inf, ico, ht*, hlp, gif, exe, drv, do*, dll, crt, cpl, com, cmd, cla, chm, cab, bin, bdx, bat, asx, asp*, ar*, ad* during any access attempt, and scans all local and external drives. The scanning involves heuristic analysis in normal mode (see p. 220). Files and archives larger than 100 MB are skipped.
- **Quick scan** — Secret Net Studio scans files with the following extensions: zip, xl*, ws*, vxe, vxd, vb*, tsp, tmp, th*, ta*, sys, swf, sl*, sh*, scr, sc*, rtf, reg, ra*, prg, prf, pp*, png, pif, ph*, pdf, otm, osx, om, ms*, md*, lnk, js*, jp*, isp, ins, inf, ico, ht*, hlp, gif, exe, drv, do*, dll, crt, cpl, com, cmd, cla, chm, cab, bin, bdx, bat, asx, asp*, ar*, ad* during any access attempt, and scans all local and external drives. Heuristic analysis is not used, only signatures are checked. Files and archives larger than 50 MB are skipped.
- **Custom** — user-defined real-time protection parameter-based scan.
- **Off** — real-time object scanning is not performed.

2. For a user-defined scan profile, click **Configure**.

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



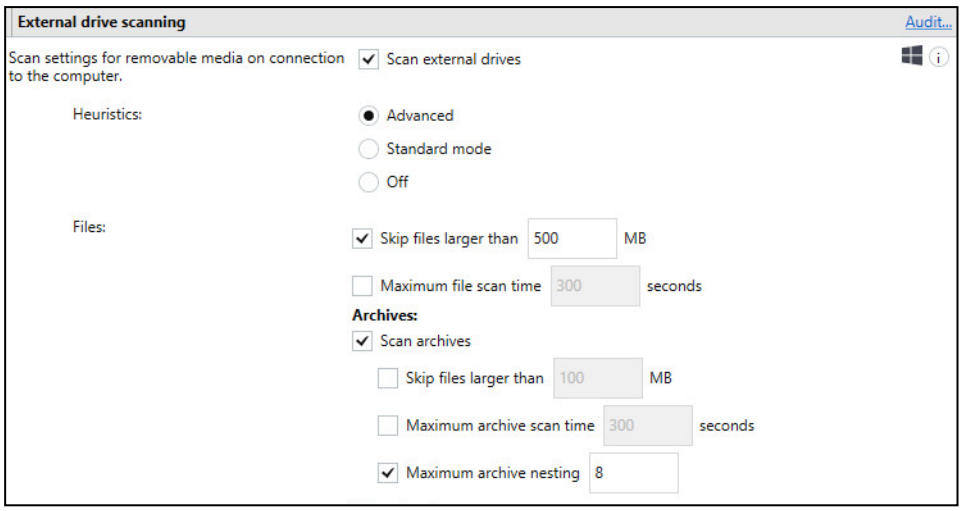
3. On the tabs **Main** and **Files**, configure the required settings (see p. 220) and click **Save**.

   Note. The way the parameter **Cure infected files** is configured does not affect the antivirus.

   Note. The option **Use previous scan results** is not available in Secret Net Studio version 8.7.

4. Click the **Audit** link to configure antivirus event logging parameters (see p. 227).
5. At the bottom of the **Settings** tab, click **Apply**.

External drive scanning



To configure scanning parameters:

1. Select the **Scan external drives** option to enable scanning.

   Note. The **Scan external drives** works only with **Real-time protection**.

2. Configure the heuristics parameters and choose actions, which should be taken in case of infected files are detected (see p. **219**).Specify the scan parameters for files and archives (see p. **220**).
3. Click the **Audit** link to configure antivirus event logging parameters (see p. **227**).
4. At the bottom of the **Settings** tab, click **Apply**.

Context scanning

To configure scanning parameters:

1. Configure the heuristics parameters and choose actions, which should be taken in case of infected files are detected (see p. **220**).
2. Click **Additional settings** and select the **Files** tab. Configure scan settings for files and archives (see p. **219**), and click **Save**.

   Note. The option **Use the results of previous scans** is not available in Secret Net Studio version 8.7.

3. At the bottom of the **Settings** tab, click **Apply**.

Full/quick scanning

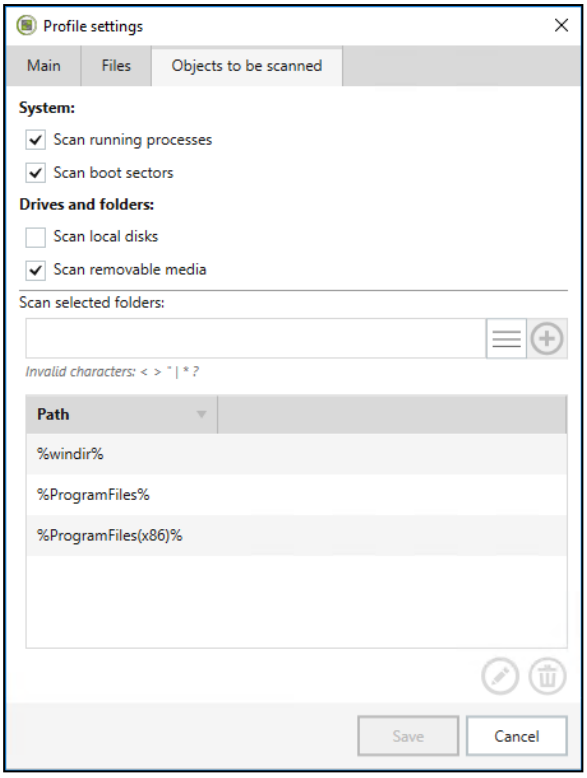
To configure scanning parameters:

1. Configure the heuristics parameters and choose actions, which should be taken in case of infected files are detected (see p. **220**).
2. Click **Additional settings** and select the **Files** tab. Configure scan parameters for files and archives (see p. **220**), and click **Save**.

   Note. The option **Use the results of previous scans** is not available in Secret Net Studio version 8.7.

3. Select the **Objects to be scanned** tab.

   A dialog box appears as in the figure below.

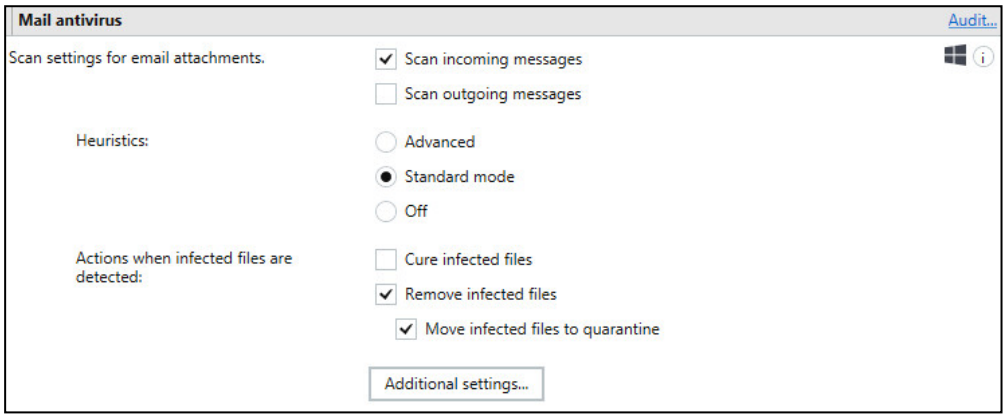

Profile settings
Main
Files
Objects to be scanned
System:
Scan running processes
Scan boot sectors
Drives and folders:
Scan local disks
Scan removable media
Scan selected folders:
Invalid characters: < > " | * ?
Path
%windir%
%ProgramFiles%
%ProgramFiles(x86)%
Save
Cancel

4. Configure the needed parameters, and click **Save**.

Parameter	Description
System	Select objects to be scanned
Drives and folders	• Select drives and folders to be scanned when using this profile. • Specify the path to the folder to be checked and click Add. If necessary, use environment variables from the drop-down list. Click **Edit** to edit the path. Click Delete to remove the folder from the list

5. At the bottom of the **Settings** tab, click **Apply**.

Mail antivirus



To configure mail antivirus settings:

1. Select the check boxes **Scan incoming messages** and **Scan outgoing messages** to enable scanning. Scanning only incoming massages is enabled by default.

> **Attention!** The user can stop the mail antivirus by disabling the **SNS.AVMailAddin** add-in in Microsoft Outlook. In this case, the respective message box appears in the antivirus control panel (see p. 227). When the application is restarted, the mail antivirus operation will be resumed.

2. Configure the heuristics parameters and choose actions, which should be taken in case of infected files are detected.

> **Note.** Outgoing messages will not be sent if a threat is detected.

3. To configure scan parameters, click **Additional settings**. On the **Files** tab configure scan parameters for files and archives (see p. **220**).
4. Select the **Automatically move files with following extensions to quarantine** check box to move to the quarantine files with specified extensions. Specify file extensions (use a comma to separate) and click **Save**. The mail antivirus quarantine is an individual folder **\Documents\Secret Net Studio\Mail** on a user's computer.

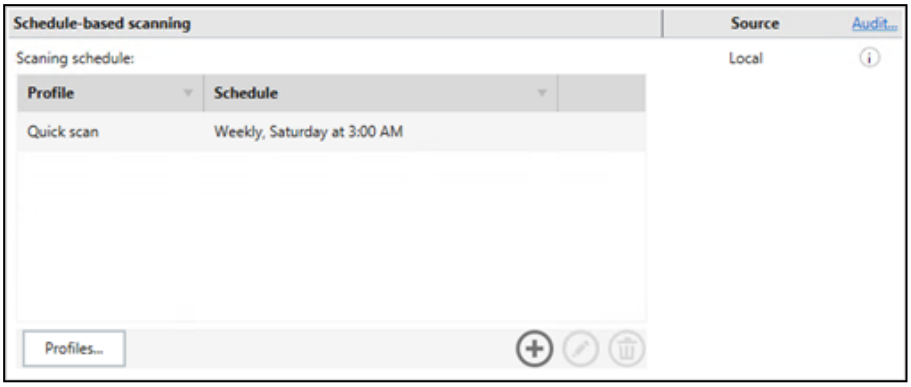
> **Note.** On the tabs **Main** and **Objects to be scanned**, you can change the parameters mentioned in steps **1** and **2** of this procedure.

5. At the bottom of the **Settings** tab, click **Apply**.

Schedule-based scanning

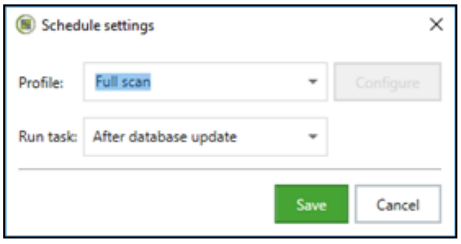
To configure schedule-based scanning:

1. In the antivirus settings area, go to the **Schedule-based scanning** section.



Tip. Use the buttons at the bottom of the list to change the schedule.

2. To add a new scanning routine to the schedule, click the **Add** button. A dialog box appears as in the figure below.



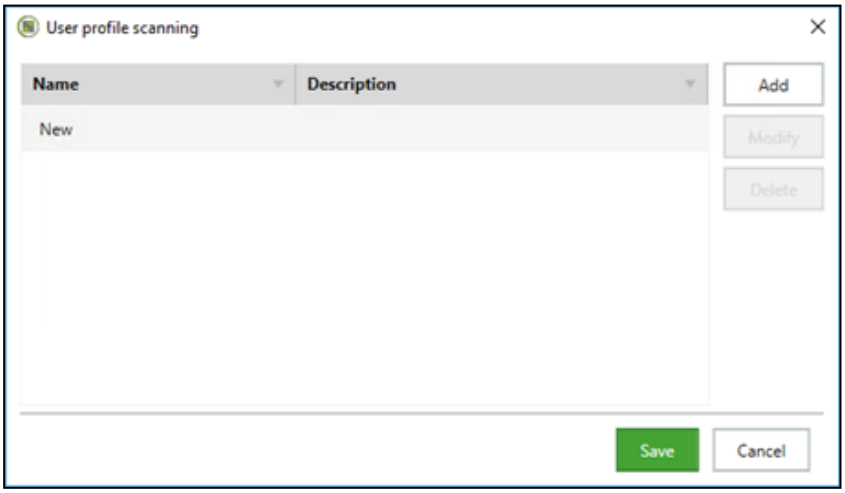
3. Select the scan profile and scanning frequency from the drop-down list, and click **Save**.

Tip. To change settings of the selected user profile, click the **Edit** button.

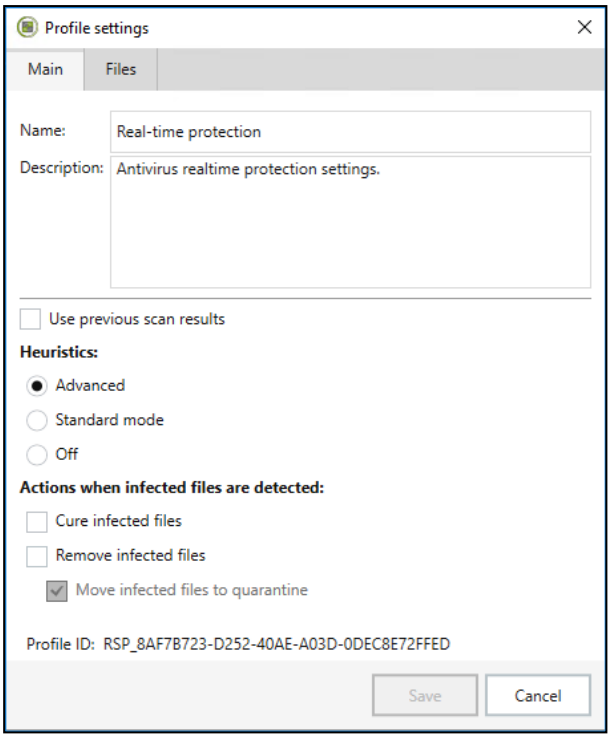
4. At the bottom of the **Settings** tab, click **Apply**.

To create and configure scan profile:

1. Click **Profiles**. A dialog box appears as in the figure below.



2. Click **Add**. The **Profile settings** dialog box appears as in the figure below.



3. On the **Main** and **Files** tabs, specify the scanning profile name and description and configure settings (see p. 219).

Note. The option **Use the results of previous scans** is not available in Secret Net Studio version 8.7.

4. Select the **Objects to be scanned** tab. Configure the needed parameters (see p. 219), and click **Save**.

Note. When configuring real-time scan parameters (**Real-time protection** profile), the **Objects to be scanned** tab is not available.

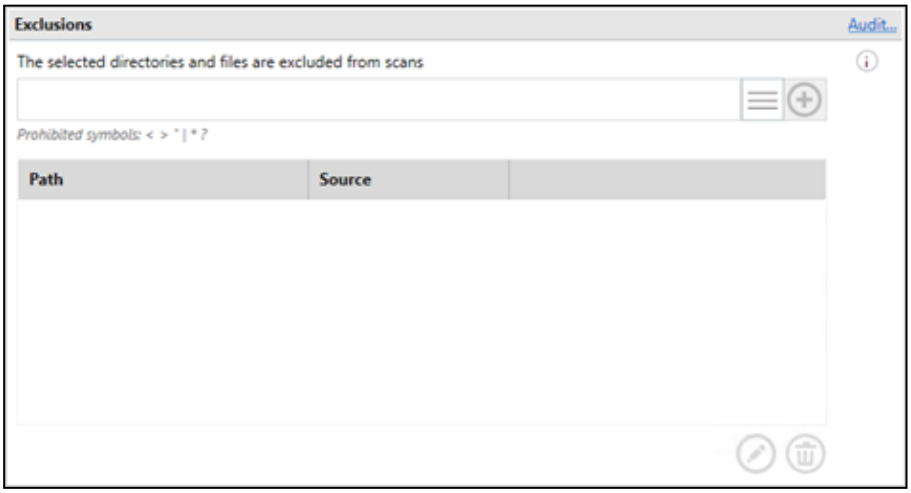
5. At the bottom of the **Settings** tab, click **Apply**.

List of exclusions

Objects from the list of exclusions are always ignored during scanning irrespective of a scanning profile being used.

To configure the list of exclusions:

1. Go to the **Exclusions** section in the antivirus parameters.



2. To add a folder or a file, specify its path to it and click the **Add** button. If necessary, use environment variables from the drop-down list.

Attention! You must specify the full path to the file or directory. For example, **D:\Work**.

When you add a directory to the list of exclusions, all objects in that directory will be ignored during scanning.

Tip. To change the path to an object, select it from the list and click the **Edit** button. To remove an object from the list of exclusions during the checks, select it and click the **Delete** button.

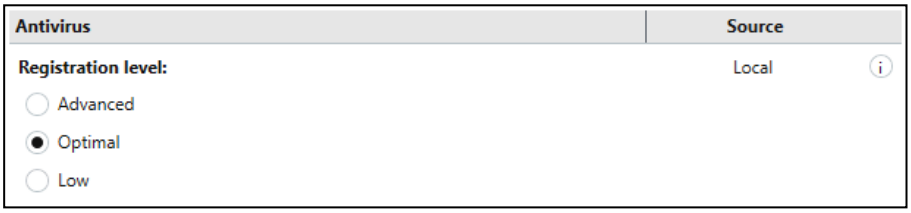
3. At the bottom of the **Settings** tab, click **Apply**.

Event registration

To configure event registration parameters:

1. In the list of parameters and policies, go to the **Event Registration** section and select **Antivirus**.

   A dialog box appears as in the figure below.



2. Select the event registration level.
   - **Advanced**.

     Register all events.

     Attention! The number of registered events can be very large.
   - **Optimal**.

     Register all important and some informational events.
   - **Low**.

     Register only important events.
3. At the bottom of the **Settings** tab, click **Apply**.

Managing antivirus on protected computers

Using the Control Center you can perform the following actions on an individual computer:

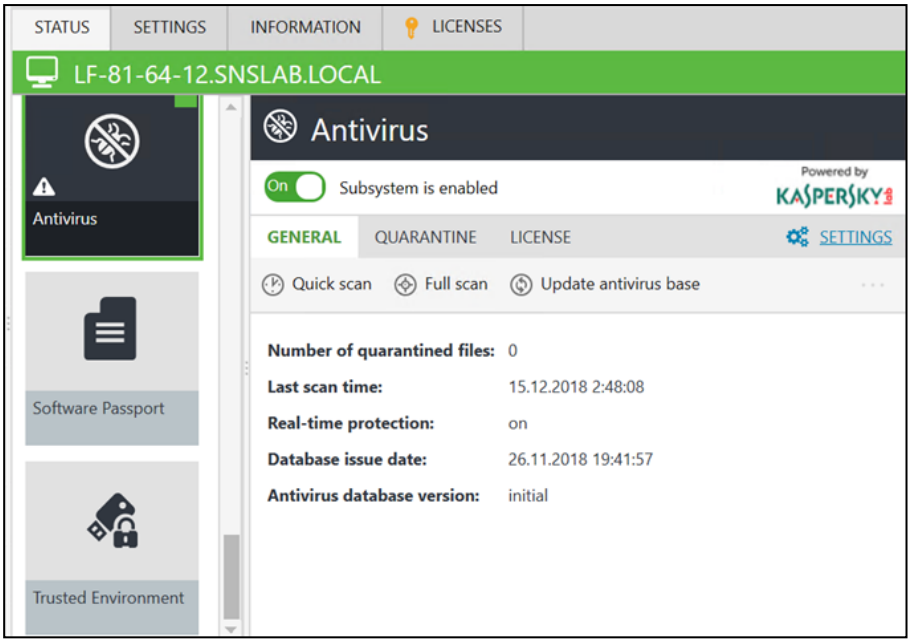
- run the scanning procedure;
- run the antivirus database updates procedure;
- browse and manage quarantined objects;
- browse license information.

To manage antivirus:

1. Right-click the needed object and click **Properties**.

   An information window appears, showing the status for this computer.
2. Select the **Antivirus** object on the **Status** tab.

   A dialog box appears as in the figure below.



Note. Messages, warnings and errors can be displayed at the top of the dialog box. For example, expired license warning.

3. To enable/disable antivirus, turn on/off the switch in the upper left corner.
4. Perform the required actions using the **Quick scan**, **Full scan** and **Update antivirus base** option buttons (see p. 241).

Note. Scanning parameters are configured by using the policies (see p. 218). Click the **Settings** link to configure antivirus policies.

License overview

You can browse information about license and technical support term on the **License** tab.

Note. To see current license information, select the **License** tab and click **Go to the license information** link.

The Secret Net Studio license determines the type of the antivirus currently in use: Antivirus or Antivirus (Kaspersky technology).

Note. Only one type of the antivirus can be licensed at a time.

When you change the license of the used type of the antivirus to a license of another version, the new antivirus and its databases will be installed automatically. The previous antivirus will be removed. Scanning tasks in process will be executed and completed correctly by the previous antivirus before it is deleted.

Note. If the antivirus profile **Real-time protection** is enabled in the Control Center, you will be prompted to restart your computer after changing the Kaspersky license to another version of the antivirus.

30 days prior to the expiration of the license term daily warnings about expiry date will appear in the Control Center. After the registered license expires, Antivirus and Antivirus (Kaspersky technology) will no longer receive updates.

Managing quarantine

On the **Quarantine** tab you can browse list of the files and folders moved to the quarantine on a particular computer. There are also buttons to control the elements of the list.

To manage quarantine:

1. Select the **Quarantine** tab.
2. Perform the required actions.

Button	Description
Request	The list of quarantined objects on a given computer will be loaded
Restore	The selected file will be restored from the quarantine. To restore several files at once, select them in the list of objects and click the **Restore** button. To restore from the quarantine a file located in a shared folder, use the **sns.av_cli.exe** tool (see p. **230**)
Delete	The selected file will be deleted from the quarantine
Delete all	All files in the quarantine will be deleted

Attention! Objects restored from the quarantine are added to the exceptions list for all scanning profiles. This is done to prevent an object from being moved to quarantine again during subsequent scanning.
Files stored in quarantine for over 30 days will be deleted automatically. Use the antivirus management utility (**sns.av_cli.exe**) included in the product to configure this parameter.

Antivirus management utility

Attention! The antivirus management utility is designed for technical support specialists. WE DO NOT RECOMMEND using this utility for standard antivirus program configuration.

Secret Net Studio includes **sns.av_cli.exe**, an antivirus program management utility (for more information, see document **Additional tools**). With this utility, you can restore a file from the quarantine, even if the computer is not connected to the network and there is no way to restore the file in the Control Center Secret Net Studio. The function is available for administrator only.

To restore files from the quarantine, open the command prompt and type the following command:

```
sns.av_cli.exe -c:restore_file -p:"<path to file>"
```

Examples:

```
sns.av_cli.exe -c:restore_file -p:"c:\checkAV\test
heuristic\heur\!ITW#460.vxe.quarantine"
```

```
sns.av_cli.exe -c:restore_file -p:"\\computer\open_
share\!test for localize\!ITW#460.vxe.quarantine"
```

You can restore a quarantined file from the removable media on any computer. To do this, you need to install Secret Net Studio antivirus and using the utility **sns.av_cli.exe** run the command for restoring the file from the quarantine, specifying the path to the file with the **.quarantine** extension.

Troubleshooting

If you encounter problems while running the Secret Net Studio software (for example, slow system operation), you should review the information about the processes executed by the Secret Net Studio antivirus.

To view information about processes:

1. Launch Windows Task Manager and go to the **Processes** tab.
2. Each antivirus scan causes an independent process of the kind of **SNS.scan_worker**.exe. Find the processes in the table and browse detailed information about them in the **Command line** column. The row can contain the following values:
   - **on_access** — real-time protection process;
   - **on_demand** — schedule-based scanning process or scanning on demand process;
   - **on_mount** — external drive scanning process;
   - **on_mail** — email attachment scanning process.

Chapter 20
Intrusion detection and prevention

Secret Net Studio detects and blocks the external and internal intrusion attempts directed at a protected computer.
The following functions are available:

Function	Description
Network attack detectors	Filtration of incoming traffic used to block external attacks. Attack detectors operate on OSI link, network, transport layers. Incoming data is analyzed by examining behavior
Signature analyzers	Monitoring of incoming and outgoing network traffic for elements registered in the decision rule base and malicious web resource database. Attacking computers can be blocked for a predefined time period
Windows telemetry blocking	Blocking of collection of system data by Windows
Network adapter control	Control of promiscuous mode enabling

The intrusion detection tool is managed in the centralized mode using the Control Center and can be managed at different levels of the control object structure:

- at the Domain, Security server and Organizational unit object levels it is possible to configure the parameters of this mechanism based on group policies. The parameter values set for the Security Server level have a higher priority over those set for the Computer object level;
- the Computer object level enables you to configure the parameters of this tool for a single computer and to manage the tool on this computer.

Note. Secret Net Studio also contains the Local Control Center. This component allows you to directly the manage intrusion detection tool on a protected computer.

All information about the operation of the mechanism for detecting and preventing intrusions is registered in the Secret Net Studio log.

Configuring group policies

The intrusion detection tool enables the following features:

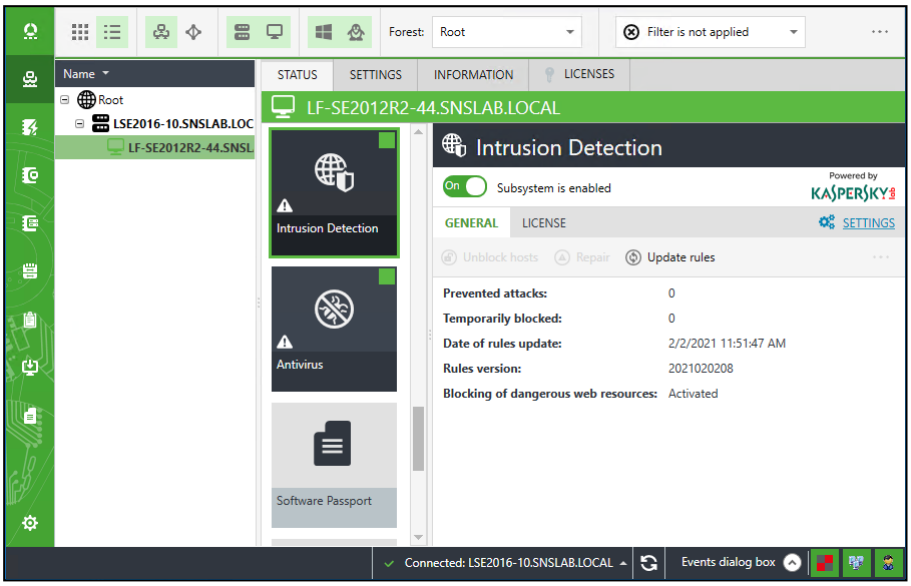
- use of an attack detector to block attacks and detect port scanning attempts;
- use of a signature analyzer to scan incoming and outgoing traffic for registered signatures;
- block access to the malicious web resources (phishing URLs, botnet URLs, ransomware URLs, malicious IP addresses). Malicious web resources databases are provided by Kaspersky Lab with the appropriate license for Secret Net Studio (see p. **240**);
- blocking of collection of system data by Windows;
- network adapter control.

To configure and manage the tool:

1. Open the **Control Center**.

   Tip. To configure the intrusion detection and prevention parameters directly on a protected computer, open the **Local Control Center**, on the **Computers** panel click the **Settings** tab. In the **Policies** section, click **Intrusion detection**. Further configuration is similar in the centralized mode.

   A dialog box appears as in the figure below.

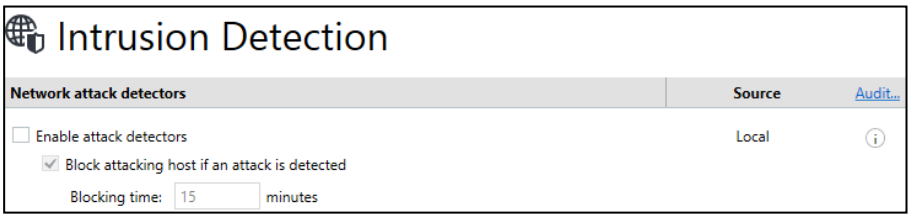


2. Click **Computers** on the **Computers** panel, right-click the needed object and click **Properties**.

   A message box showing the object status appears.

3. On the **Settings** tab, in the **Policies** section, click **Intrusion detection**.

   A dialog box asking you to configure the selected parameters appears as in the figure below.



4. Configure the required parameters and click **Apply**.

Network attack detectors

To use the network attack detectors, specify their parameters. Then enable detectors.

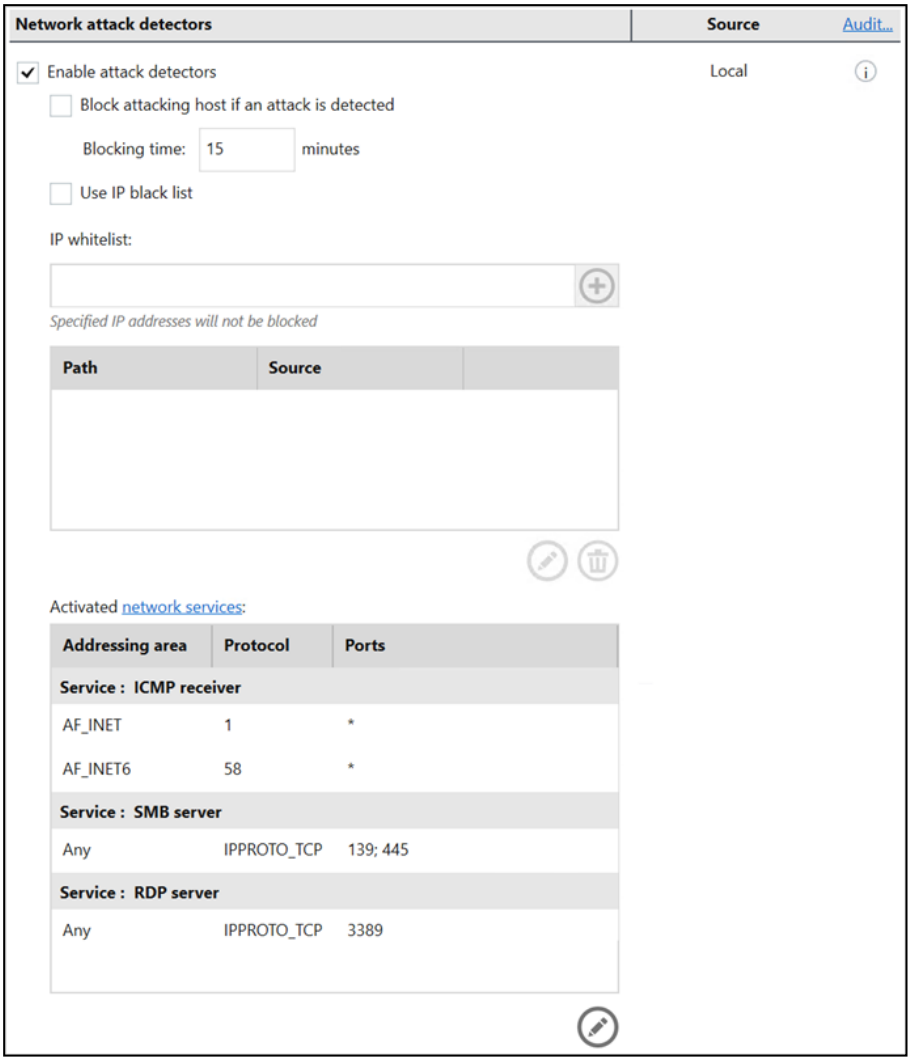
To configure and enable detectors:

1. Specify the common parameters for the network attack detectors (see below).
2. Specify the parameters for each detector (see p. **234**).
3. If you are going to use DoS detector, specify a list of the network services (see p. **235**).

Detector common parameters configuring

To configure the network attack detectors:

1. In the **Intrusion detection** settings menu, select the group of parameters **Network attack detectors**.



2. Select the **Enable attack detectors** option to activate the network attack detectors. Configure parameters that are common to all detectors.

Parameter	Description
Block attacking host if an attack is detected	When attack detectors are enabled, this function is activated by default for all detectors. In this case, the IP address of the attacking host will be blocked
Blocking time (minutes)	Host block duration. The default time is 15 minutes
Use IP black list	When attack detectors are enabled, this feature is enabled by default for all detectors. In this case, malicious IP addresses from the Kaspersky database will be blocked

Parameter	Description
IP whitelist	Enter the IP address (for example, **192.168.100.25**) or subnet mask in the CIDR notation (for example, **192.168.100.0/24**) and click the **Add** button. The IP address will be added to the whitelist. Addresses from the whitelist are not blocked by the network attack detectors. To change or delete an IP address, select it in the table and click the **Edit** or the **Delete** button. If the whitelist is generated by group policy tools, you cannot edit it at the individual computer level. In this case, the completion of the whitelist will be available (only for this computer)

Once the detectors are activated, only the detectors that are also enabled and configured will work (see below).

Enabling and configuring network attack detectors

To enable detectors:

1. Enable the required detectors and configure their parameters.

Parameter	Description
Port scanning	Select this option to enable port scanning detection
Detection period	The period during which Secret Net Studio calculates how many times the ports of protected computers have been addressed
Maximum number of calls to ports within the specified period	Once this number is reached, the server is considered as an attacking server
ARP-spoofing	Select this option to enable detection of Man in the middle type attacks used in ARP protocol-based networks
Period after ARP request during which ARP response is expected	Specify the time for the detector to wait for an ARP response. The attack detector will be triggered if more than one response is received
Action with ARP responses, without ARP requests	Specify the action for the detector to take regarding ARP responses without ARP requests: • **Ignore**; • **Log** — record an audit event; • **Log and send ARP responses**; • **Active ARP-spoofing detector** — an ARP request will be issued for each ARP response received without an ARP request; • **Active countermeasures to ARP-spoofing** — an ARP request will be issued for each ARP response received without an ARP request. Initial response will be blocked. Suspicious ARP packets can also be rejected in this mode
SYN-FLOOD	Detection of Denial-of-service type attacks that send a large number of SYN requests in a short period of time
Period during which half-open connections will be taken into consideration	Define the time to consider new connections over TCP
Number of half-open connections required to consider host in attacker	Define the number of half-open connections to exceed in order to trigger the attack detector

Parameter	Description
Block packets if the detector is triggered	When attack detectors are enabled, the **Block attacking host if an attack is detected** function is activated by default for all detectors (see p. 233). To disable the lock for the **SYN-FLOOD** detector, clear the **Block packets if the detector is triggered** option. If this option is selected and the number of half-open connections created within a specified period of time exceeds the specified value, no more connections will be created
Abnormal traffic	Select this option to detect abnormal traffic
Block packets if the detector is triggered	When attack detectors are enabled, the **Block attacking host if an attack is detected** function is activated by default for all detectors (see p. 233). To disable the lock for the **Abnormal traffic** detector, clear the **Block packets if the detector is triggered** option. If this option is selected, abnormal traffic packets will be blocked when the detector is triggered
DDoS	Detection of attacks from multiple computers
Number of active remote hosts required to trigger the detector	The attack detector will be triggered once the specified number of remote addresses sending traffic to a protected computer has been reached
DoS	Detection of denial-of-service attacks
Time interval during which port calling is taken into account	Specify a time interval during which port calling will be taken into account
Number of packets required to detect an attack	The number of packets sent from a server, within the specified time interval, for a server to be considered an attacker if reached. This value will not be applied to configured network services
Amount of data required to detect an attack	The data size sent from a server within a specified time interval for a server to be considered an attacker if reached. This value will not be applied to configured network services
Slow down traffic from the attacking host	Select this option to automatically reduce the transmission speed of data from the attacking server, losing a portion of packets. It only works if the **Block attacking host if an attack is detected** function is active. After the traffic is slowed down by 2 times, the attacking host will be blocked
Service	The table displays the network services configured before (see p. 235). For each service, specify the maximum number of packets and their maximum size in kilobytes. These values will only be applied to services

Configuring network services

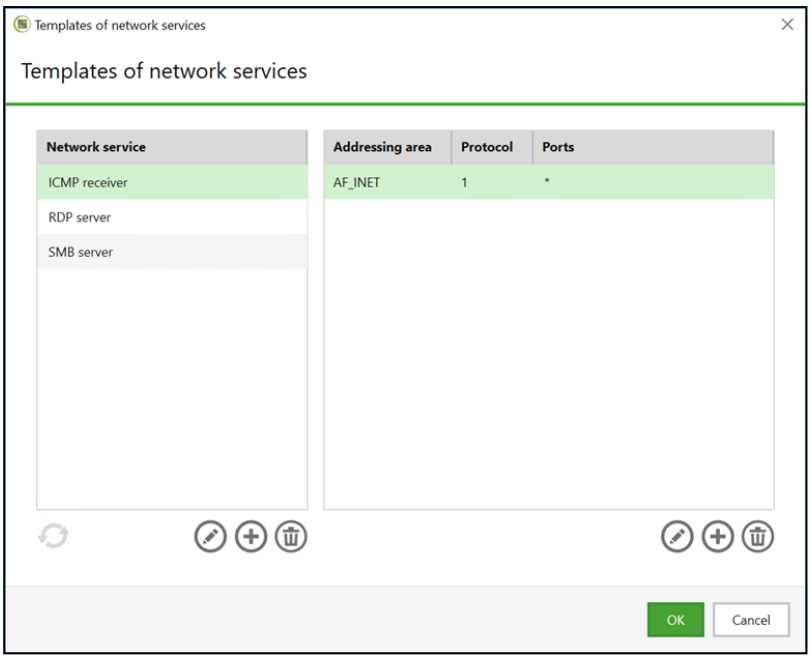
To define individual DoS detector triggering parameters for different ports and protocols, configure the list of network services. Network services can be created using templates.

Note. The list of network service templates is common to all computers in a security domain.

To manage templates:

1. In the **Intrusion detection** settings menu, click the **network services** link.

   A dialog box appears as in the figure below.



Tip. To edit the list of network services templates, use the following buttons on the left side of the dialog box:

- To rename a network service template, click the **Edit** button;
- To delete a template, click the **Delete** button;
- To refresh the list of network services templates, click the **Refresh** button.

Tip. To configure a network service template, use the buttons on the right of the dialog box:

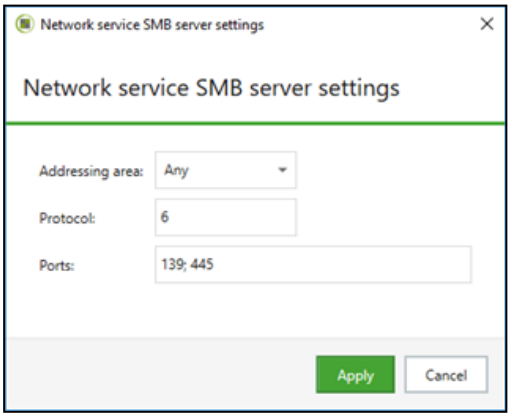
- To add a new network service setting, click the **Add** button;
- To change network service setting, click the **Edit** button;
- To delete a network service setting, click the **Delete** button.

2. To create a new network service template, click the **Add** button on the left side of the dialog box. Specify a new service name and click the **Add** button.

   The template appears in the list.

3. To configure the created template, select it on the left side of the dialog box, and use buttons on the right side of the dialog box. For example, to add a new network service setting, click the **Add** button.

   A dialog box appears as in the figure below.



4. Configure the network service parameters and click **Apply**.

Parameter	Description
Addressing area	Select an addressing area for the network service: • **AF_INET** — IPv4 address family; • **AF_INET6** — IPv6 address family; • **Any** — IPv4 and IPv6 address families

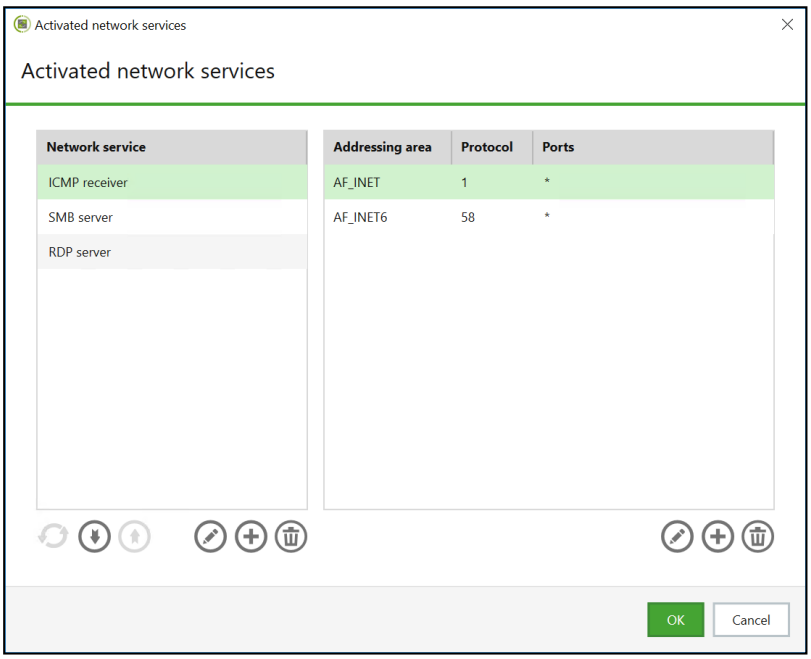
Parameter	Description
Protocol	Specify the protocol number governed by the network service
Ports	Specify the number of the ports governed by the network service. Use a ";" (semicolon) character to separate values. Specify the "*" (asterisk) character if all ports must be governed by the network service

5. To save changes, click **OK** in the **Templates of network services** dialog box. Then click **Apply** at the bottom of the **Settings** tab.

To manage network services:

1. In the **Intrusion detection** settings menu, click the **Edit** button, which is located under the **Activated network services** table.

   A dialog box appears as in the figure below.



Tip. To edit the list of network services, use the following buttons on the left side of the dialog box:
- Use the **Up** and **Down** buttons to manage the priority of used network services;
- To rename a network service, click **Edit**. This action does not affect network service templates;
- To delete a network service, click **Delete**;
- To refresh the list of network services settings, click **Refresh**.

Tip. To edit the network service settings, use the buttons on the right of the dialog box:
- To add a new network service setting, click **Add**;
- To change settings of a network service, click **Edit**;
- To delete a setting of a network service, click **Delete**.

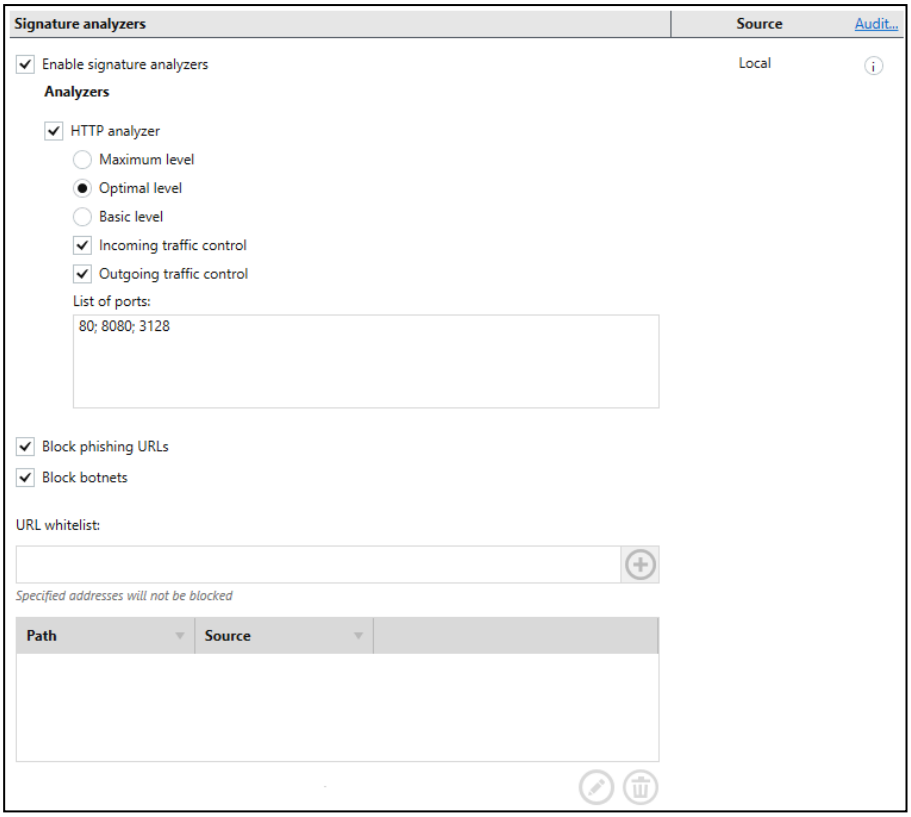
2. To add a new network service, click the **Add** button on the left side of the dialog box, then choose service from the list of templates and click the **Add** button. To configure the network service, select the name on the left side of the window and use buttons on the right side of the window. Configuration is similar to configuring network service templates (see p. **236**).
3. To save changes, click **OK**in the **Activated network services** dialog box. Then click **Apply** at the bottom of the **Settings** tab.

   New services appear in the table.

Signature analyzers

To configure the analyzers:

1. In the **Intrusion Detection** settings menu, click **Signature analyzers**.



2. Configure the parameters.

Parameter	Description
Enable signature analyzers	Select this option to activate the signature analyzers
HTTP analyzer	Select this option to enable HTTP traffic analyzer. Select the protection level: • **Maximum** — all signature types are checked; • **Optimal** — main signatures are checked; • **Basic** — only critically important signatures are checked
Incoming traffic control	Incoming traffic will be monitored for the presence of signatures registered in the decision rule base
Outgoing traffic control	Outgoing traffic will be monitored for the presence of signatures registered in the decision rule base
List of ports	Type the ports to be checked by the HTTP analyzer. Use a ";" (semicolon) character to separate values. By default, the list contains ports **80**, **8080** and **3128**. This list cannot be empty. If your organization uses a proxy server, add the port of the proxy server to the list for correct analyzer operation
Block phishing URLs	Select this option to block phishing URLs from the Kaspersky database
Block botnets	Select this option to block botnets from the Kaspersky database
URL whitelist	Type a URL without a protocol prefix and parameters (for example, test.ru) or a URL mask (for example,***.test.ru**, where * is any sequence of characters), and click the **Add** button. The URL will be added to the whitelist. URLs from the whitelist are not blocked by the signature analyzers. To change or delete a URL address, select it in the table and click the **Edit** or **Delete** button. If the whitelist is generated by group policy tools, you cannot edit it at the individual computer level. In this case, the completion of the whitelist will be available (only for this computer)

3. Click **Apply** at the bottom of the **Settings** tab.

Windows telemetry blocking

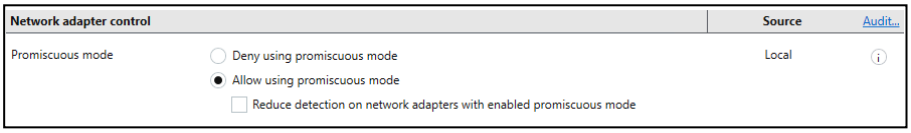
In order to block collecting system data by Windows and sending the data to Microsoft, in the Intrusion detection settings menu, select the group of parameters **Windows telemetry blocking** and select the check box **Block Windows telemetry**.

Network adapter control

When the promiscuous mode is on, a network adapter receives all packets irrespective of their destination. Secret Net Studio allows you to control a network adapter mode on protected computers.

To configure promiscuous mode control:

1. In the **Intrusion Detection** settings menu, select the group of parameters **Network adapter control**.



2. Configure the parameters:
   - **Deny using promiscuous mode** — enabling the promiscuous mode for network adapters will not be available;
   - **Allow using promiscuous mode** — enabling the promiscuous mode for network adapters will be available;
   - **Reduce detection on network adapters with enabled promiscuous mode** — an attack detection algorithm will be changed on network adapters with the enabled promiscuous mode in order to exclude false positives of network attack detectors.

Managing the intrusion detection tool

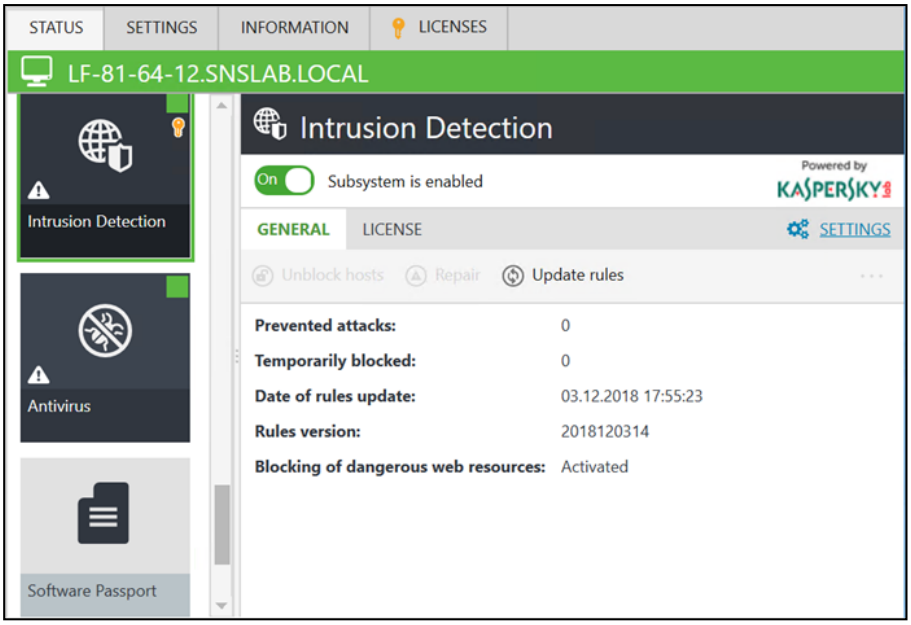
Using the Control Center you can unblock hosts on an individual computer.

To manage this mechanism:

1. Click **Computers** on the **Computers** panel, right-click the needed object and click **Properties**.

   A dialog box showing the computer status appears.
2. Select the **Intrusion Detection** object on the **Status** tab.

   A dialog box appears as in the figure below.



Note. Messages, warnings and errors can be displayed at the top of the dialog box. For example, expired license warning.

3. To enable/disable intrusion detection, turn on/off the switch in the upper left corner.
4. Perform the required action using the following buttons:

Button	Description
Unblock hosts	Click to remove block from all hosts blocked by the intrusion detection tool on the computer
Repair	If the Secret Net Studio server data and network protection components are not synchronized (for example, when the computer name changed), emergency mode is activated. If the **Resolve** button is enabled, data synchronization is possible
Update rules	The decision rule base and malicious web resources database will be updated (see p. **241**)

Note. To go to the intrusion detection mechanism group policy configuration, click the **Settings** link (see p. **231**).

License overview

You can browse information about license and technical support term on the **License** tab.

Note. To see current license information, select the **License** tab and click **Go to the license information** link.

The Secret Net Studio license determines availability of the feature of blocking access to malicious web resources using Kaspersky databases for the **Intrusion Detection** component.

30 days prior to the expiration of the license term daily warnings about expiry date will appear in the Control Center. After the registered license expires, **Intrusion Detection** component will continue working, but the decision rule base and malicious web resources database will no longer receive updates.

Chapter 21
Updating antivirus and intrusion detection tool databases

To ensure full protection against malware, Secret Net Studio makes it possible to automatically update the antivirus database on the protected computers, decision rule base and malicious web resources database. Also you can update bases using a standalone antivirus database update utility (see p. 243).

Note. Database updates are not supported, if the Secret Net Studio license is not activated (see p. 229).

Automatic update function is managed in the centralized mode using the Control Center and can be managed at different levels of the control object structure:

- at the Domain, Security Server and Organizational unit object levels you can configure the parameters based on group policies. The parameter values set for the Security Server level have a higher priority over those set for the Computer object level;
- at the Computer object level you can configure the parameters for a single computer.

Note. Secret Net Studio also includes the Local Control Center. This component allows managing the automatic update function on a protected computer.

Configuring update parameters

To configure the update parameters:

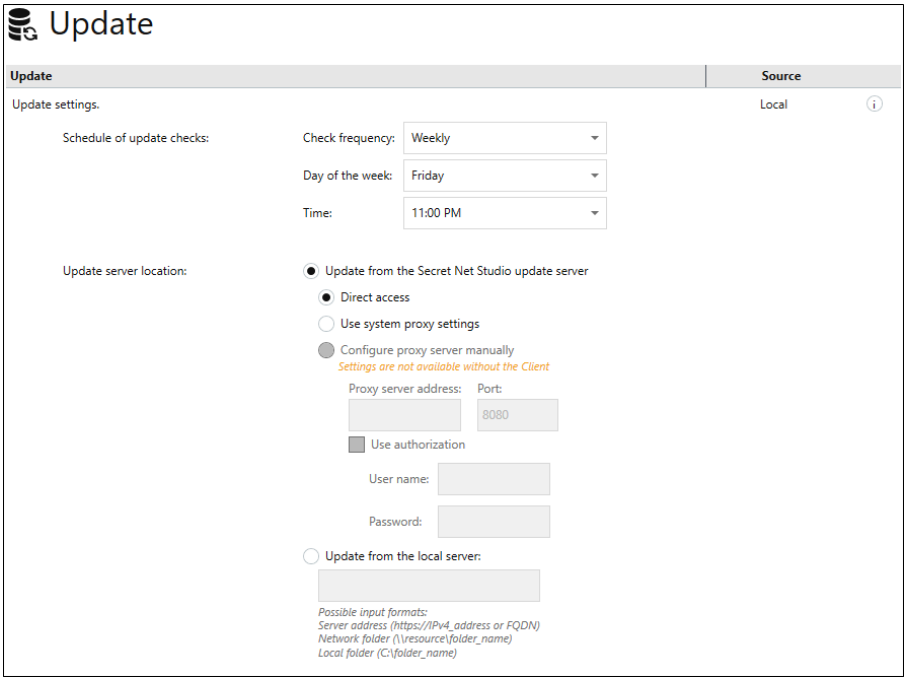
1. Open the Control Center.

   Tip. To configure update settings directly on a protected computer, open the **Local Control Center**, on the **Computers** panel click the **Settings** tab. In the **Policies** section, click **Update**. Further configuration is similar in centralized mode.

   The main program window appears.
2. Click **Computers** on the **Computers** panel, right-click the needed object and click **Properties**.

   An information message showing the object status appears as in the figure below.
3. Select the **Settings** tab. If necessary, click **Load settings**. In the **Policies** section, click **Update**.

   A dialog box appears as in the figure below.



4. In the **Schedule of update checks** group, define how often the software will check for updates. In weekly mode, you can set the day and time of day for the software to update. For daily mode, you can set the exact time. If the **Scheduler is disabled** option is selected, Secret Net Studio will not check for updates automatically.

Note. We recommend you to update databases daily. If you have a large number of workstations in your network, it is recommended that you divide them into groups and configure them to update at different times.

5. To update from the Secret Net Studio server, click **Update from the Secret Net Studio update server** and, if necessary, type the path to the proxy server.

Parameter	Description
Direct access	Select this option if there is a direct connection with the update server (direct access)
Use system proxy settings	Automatic proxy-server detection is used (not recommended)
Configure proxy server manually	Select this option to configure the proxy server manually. Specify the proxy server address and port. If a proxy server requires authorization, type the username and password

6. If the local network has a server containing updates for Secret Net Studio antivirus database, or if the updates are located in the network folder, click **Update from the local server** and specify:
   - the IP address or fully qualified domain name (FQDN) of the local update server. For example, **https://192.168.10.1** or **us.domain.loc**;
   - path to a network or local directory with updates (see p. 243). For example, **\\server\sns-updates\packages**.

   Note. If updates are installed on a computer from the network folder, the computer account must be able to access the resource.
   If the protected computer is not connected to the Internet, the antivirus databases can be updated by using the update utility (see p. 243).

7. At the bottom of the **Settings** tab, click **Apply**.

Downloading updates from a network share

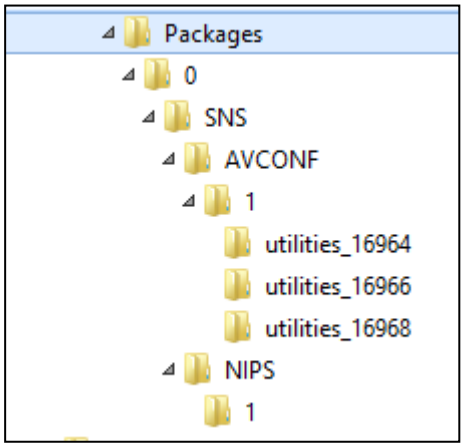
To download updates from a network share:

1. Install the Secret Net Studio update server software on a computer with Internet access and configure the update from the Secret Net Studio server (see document [**1**]).
2. Create a network share and grant authorized users access to it.
3. Configure Secret Net Studio clients or cascade update servers to update from the created network resource.
4. Configure the syncing of the folder **C:\ProgramData\SECURITY CODE LLC\Secret Net Studio\server\Update server\Packages**, which is located on the installed update server with the created network resource.

   Note. You can configure the syncing by means of any directory replication tool, such as Robocopy (included in Windows Vista and later).

Manually migrating updates

If you need to migrate updates manually, copy the contents of the directory **C:\ProgramData\SECURITY CODE LLC\Secret Net Studio\server\Update server\Packages** or the directory which synchronized with it (see above) to removable media and transfer it to a server on a private network to a similar folder.



Attention! When you manually migrate updates, you must not change the file structure of the **Packages** folder.

Update utility

Secret Net Studio includes a standalone antivirus database update utility. When you run the utility, it checks the current version of the antivirus databases in the installed antivirus program. If necessary, it installs current updates contained in the utility.

When you install the update, Secret Net Studio checks the compatibility of the downloaded archive contents with the version of the product installed on the protected computer. It also verifies and checks the integrity of the archive.

You can download the utility from the SECURITY CODE LLC website.

To download and run the utility:

1. Follow the link https://updates.securitycode.ru:43444.
2. To download the utility, click one of the links:
   - Current package for update Antivirus.
   - Current package for update Antivirus (Kaspersky technology).

   Note. The file name indicates the antivirus database version included in the utility.
3. On the protected computer, run to execute the downloaded utility file. A message appears describing the antivirus database update results.

   Note. If there is not enough free space on the drive, the updates will not be installed.

If there is an error when applying the update, the database will automatically roll back to the previous version. In all other cases, you only can roll back to previous versions of the antivirus databases by using the **sns.av_cli.exe** utility (see p. **230**) or the update server management program (see document [**1**]).

Chapter 22
Trusted Environment

Trusted Environment is the Secret Net Studio protection mechanism that controls computer's OS and security system outside the OS. TE performs the following security functions:

- IC of Secret Net Studio modules (drivers, services, applications) before the computer's OS boots up;
- Secret Net Studio modules startup and operation control while the user is wo rking on the computer;
- system disk authenticity control before the computer's OS boots up;
- write-blocking of memory pages with Secret Net Studio modules while the user is working on the computer;
- attack detection and prevention, or OS stop when attack prevention is impossible. These actions are performed while the user is working on the computer;
- security events registration in the TE log.

Tip. TE is available in Secret Net Studio 8.5 and later.

When TE operates, you can boot the OS only with the special boot USB flash drive (hereinafter TE boot drive), which is created using Secret Net Studio in advance. TE boot drive contains:

- TE OS — the special OS based on Linux, which interacts with computer's memory, file system and OS in order to implement TE security functions;
- TE hypervisor, which ensures TE OS boot and TE security functions implementation;
- TE loader (MBR or UEFI), which reads TE OS and hypervisor and places them on the RAM;
- TE settings.

Attention! TE boot drive should be used only on trusted AWP.

TE requires a separate license.

Tip. TE is a new Secret Net Studio mechanism, which is actively being developed. Setting features and screenshots may differ from figured in this document. If you have a question about TE work, you can refer to the SECURITY CODE Ltd. Service Department.

System requirements

The following table lists the hardware and software requirements for TE:

Requirement	Value
Processor	Dual core or more (supporting Hyper-Threading technology). Virtual technology. SLAT for AMD Family 10h, Intel Core i3, i5, i7 and later processors
OS	Windows 7 SP1 (x64) and later
System disk space	2 MB or more
Motherboard	Free USB port
UEFI/BIOS	The first boot device is USB flash drive
USB flash drive volume	32 MB or more
License	The Secret Net Studio TE license

Note. Check the restrictions and recommendations for the current TE version (see p. 257).

Enabling Trusted Environment

For the operation of TE mechanism, perform the following actions:

- register a TE license;
- create a TE boot drive;
- enable TE.

Registering TE license

TE license registration procedure is similar to that of other Secret Net Studio licenses.

License may be registered centrally and locally:

- when installing Secret Net Studio;
- when using Secret Net Studio.

Tip. By default, TE is disabled after license registration.

Registering when installing Secret Net Studio

A TE license can be registered with other licenses when installing Secret Net Studio. Installation instructions are contained in document [**1**]:

- for local installation, see chapter Installing Secret Net Studio locally, section Installing the Client;
- for centralized installation, see chapter Installing the Client centrally.

Registering when using Secret Net Studio

A TE license can be registered individually when using Secret Net Studio is used. The installation instructions are given in document [**1**]:

- for local registration, see chapter Additional features of the local administration, section Local registration of licenses;
- for central registration, see chapter Configuring and managing centralized software deployment, section Managing security mechanism licenses.

Creating TE boot drive

A TE boot drive can be created on any computer with TE (centrally and locally).

Tip.

- We recommend creating a TE boot drive on the computer with the Secret Net Studio typical configuration on which TE will be used. When creating TE boot drive, the list of controlled Secret Net Studio modules is being generated.
- We recommend creating a TE boot drive on TE administrator's trusted AWP.

A TE boot drive can be created when TE is either enabled or disabled.

To create a TE boot drive, you need a separate USB flash drive.

Before starting the creation procedure, connect the USB flash drive to the computer.

Attention! Creating a TE boot drive will wipe all data from the USB flash drive. The TE service information requires only a part of the USB flash drive memory. If you want to use USB flash drive as normal, you need to wipe all information from the device.

The procedure of TE boot drive creation via the Local Control Center is described below. The procedure of creating a TE boot drive via the Control Center in centralized mode is the same.

To create a TE boot drive:

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

   The Local Control Center starts.

2. On the **Computer** panel, go to the **Status** tab, and click **Trusted Environment**.

   A panel containing information about the mechanism appears on the right.

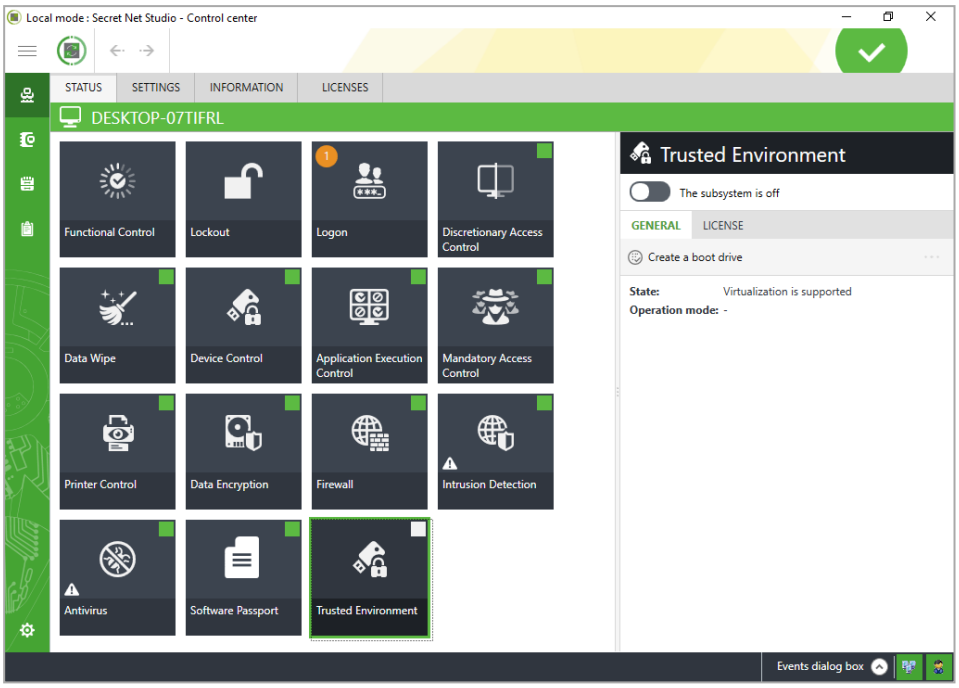
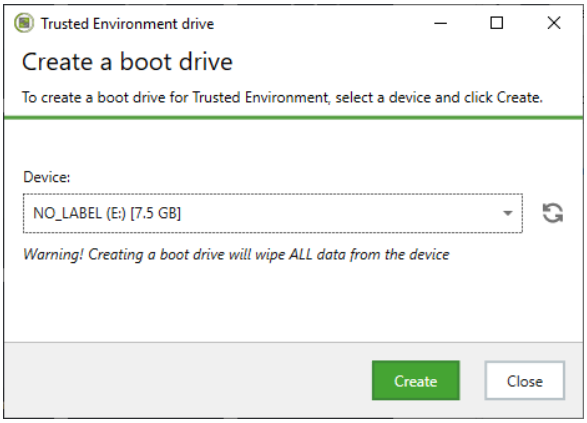


Fig.1 Information about the Trusted Environment mechanism

3. Click **Create a boot drive**.

   A TE boot drive creation dialog box appears.



4. In the dropdown list, select the required USB flash drive.
5. Click **Create**.

   Writing data to the USB flash drive starts. A message about successful completion appears on the dialog box.
6. Click **Close**.

   The TE boot drive is ready for use.

Enabling the TE mechanism

TE is enabled locally on the computer on which TE will be used.

Attention! Before enabling TE, make sure:

- The computer meets the system requirements on p. 245. This information is displayed in the Local Control Center (see the **General** tab on the panel with information about TE (Fig.1 on p. 247)). The list of possible values when the computer does not meet the system requirements is on p. 296.
- A TE boot drive is ready for use (see p. 246). You cannot load the OS without this drive.

Note. Secret Net Studio 8.7 does not support simultaneous operation of Trusted Environment and Disk Protection with Full Disk Encryption. Before enabling Trusted Environment, disable Disk Protection and Full Disk Encryption.

To enable TE:

1. In the Windows **Start** menu, click **Security Code**, then click **Local Control Center**.

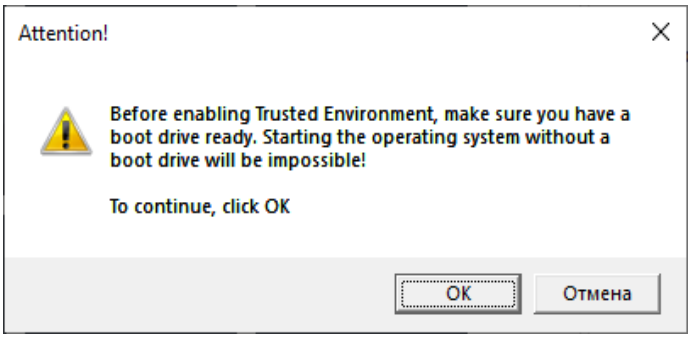
   The Local Control Center starts.

2. On the **Computer** panel, go to the **Status** tab and click **Trusted Environment**.

   A panel containing information about the mechanism appears on the right.

3. Click the toggle switch on the right side of the panel to set it to **On**.

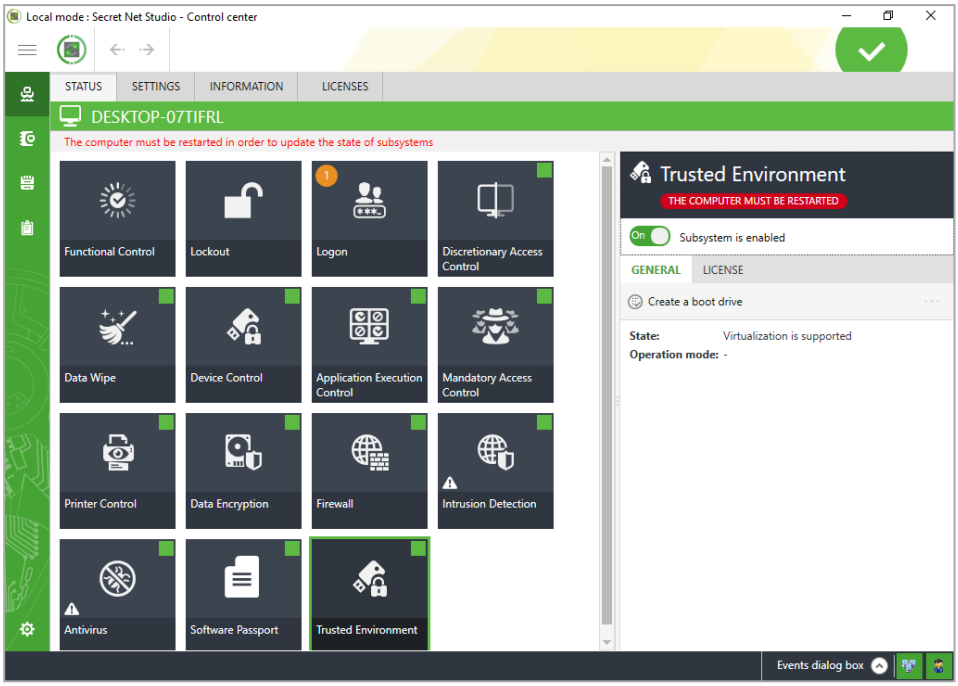
   The **Attention** dialog box appears as in the figure below.



4. If the TE boot drive has already been created, click **OK**.

   Tip. If the TE boot drive has not been created, click **Cancel** and create the drive using the instruction on p. 246.

   The warning to restart the computer appears in the Control Center as in the figure below.



5. Connect the TE boot drive to the computer.

Attention!
- Make sure that the USB flash drive is selected as the first boot drive in the UEFI/BIOS settings.
- In some UEFI/BIOS settings, the boot order is reset to the default value every time after the computer is turned on. In this case, set the required boot order in the UEFI/BIOS setting when turning on the computer.

Attention! If you turn on the computer without the TE boot drive, the following message appears on the lock screen: **Trusted Environment does not function. The computer will be turned off. Before turning on the computer, connect the bootable media**. Logging in to the OS is impossible.

6. Restart the computer.

TE OS loading starts. After successful loading, the TE OS menu appears on the screen (see Fig.2 on p. **251**).

TE operates in soft mode (see p. **252**).

Tip. If the system requirements are not met, errors may occur after restarting the computer. In this case, follow the instructions from error messages.
If a BSOD error occurs, find out the reason using the error code. Codes and description of errors related to TE are listed on p. **297**.

Configuring Trusted Environment

The TE administrator configures TE in TE administrator mode locally.

For the instruction on logging in to TE administrator mode, see p. **250**.

The TE administrator may perform the following actions:

- select TE operation mode (see p. **252**);
- configure IC settings (see p. **254**);
- work with the event log (see p. **258**);
- change a TE administrator password (see p. **251**);
- unlock the computer (see p. **257**).

Before configuring TE, read the description of TE OS interface and instructions on performing typical actions (see below).

TE OS interface

TE OS interface is text based (see Fig.2 on p. **251**). The interface language is English.

Management is performed using the keyboard. The typical commands listed below simplify the use of this manual.

- To navigate the menu, press ↑ and ↓ .
- To navigate interface buttons, press → and ← .
- To select a menu item or an interface button, or select a log entry etc., press **Enter**.
- To check * in the option list (for example, when selecting TE operation mode), press **Space**.
- To exit or cancel, press **Esc** or select **Exit** or **Cancel** .

Entering TE administrator mode

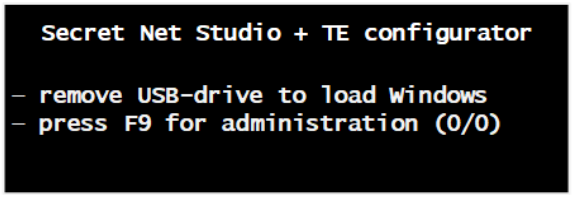
Attention! Before turning on the computer, make sure:
- the TE boot drive is connected to the computer;
- the USB flash drive is selected as the first boot drive in the UEFI/BIOS Setup.

Attention! If you turn on the computer without the TE boot drive, the following message appears on the lock screen: **Trusted Environment does not function. The computer will be turned off. Before turning on the computer, connect the bootable media**. Logging on to the OS is impossible.

To enter TE administrator mode:

1. Turn on the computer.

TE OS loading starts. After successful loading, the TE OS menu appears on the screen.



Tip.
- If the system requirements are not met, errors may occur after restarting the computer. In this case, follow the instructions from error messages.
- If a BSOD error occurs, find out the reason using the error code. Codes and description of errors related to TE are listed on p. **297**.
- If TE functions in hard mode and events which shut down the OS occur (see Tab.1 on p. **252**), the message about new events appears on the screen. In this case, follow the instruction on unlocking the computer on p. **257**.

2. Press **F9**.

Tip. To boot the OS without logging on to the TE administrator mode, disconnect the TE boot drive.

3. Enter the TE administrator password.

Attention!
- When a TE OS first boots, the TE administrator password is set to **12345678**.
- For security purposes, we recommend you to change the TE administrator password after a TE OS first boot-up time (see p. **251**).

The TE administrator menu appears on the screen.

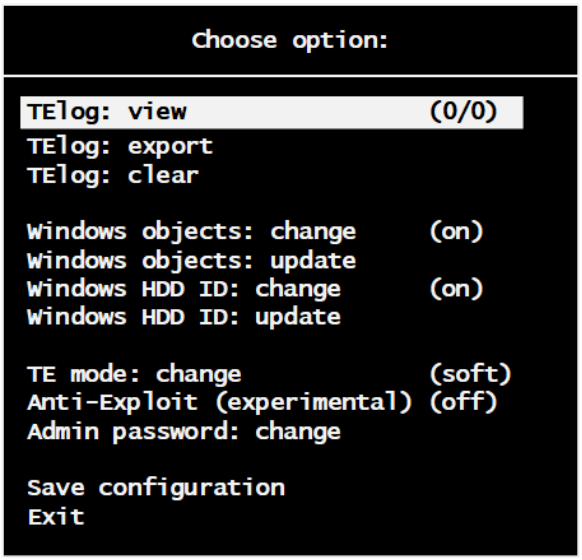


Fig.2 TE administrator menu

Attention! When you first log on to TE OS, the TE log location is defined. To save this location, select the item **Save configuration** in the TE administrator menu.

4. Select the required setting to configure:

- **TElog: view** — view TE event log;
- **TElog: export** — export TE event log;
- **TElog: clear** — clear TE event log;
- **Windows objects: change** — change the IC object list;
- **Windows objects: update** — update the reference checksums of IC objects;
- **Windows HDD ID: change** — set the system disk identifier control;
- **Windows HDD ID: update** — update the system disk identifier;
- **TE mode: change** — change TE operation mode;
- **Admin password: change** — change the TE administrator password.

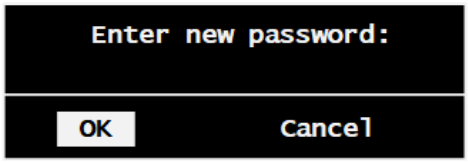
Changing TE administrator password

Attention! For security purposes, we recommend changing the TE administrator password after a TE OS first boot-up time. Then, change the password in compliance with the organization security policy.

To change the TE administrator password:

1. In the TE administrator menu (see Fig.2 on p. **251**), select the item **Admin password: change**.

The dialog box to enter a new password appears.



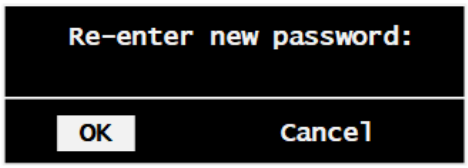
2. Enter a new password.

Tip.

- Password can consist of only following symbols:
  - 1234567890 — numbers;
  - abcdefghijklmnopqrstuvwxyz — English characters of lower case;
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ — English characters of upper case;
  - _$!@#;%^:&?*)(-+=/|.,<>`~"\ — special symbols.
- To set a strong password, we recommend you to observe the following requirements:
  - minimum length is 6 symbols;
  - contains at least one numeral;
  - contains at least one character of upper case;
  - contains at least one character of lower case;
  - contains at least one special symbol;
  - avoids two and more same neighboring symbols;
  - avoids two and more neighboring numerals in ascending (123...) or descending (987...) order;
  - avoids the match of a new and the previous passwords.

3. Select **OK**.

   The dialog box to confirm the password appears.



4. Enter the new password again.
5. Select **OK**.

   After successful confirmation, the message about the password change appears.

Tip. If an error occurs, the message **Passwords not matched** appears. In this case, select **OK** and repeat the password change procedure.

6. Select **OK**.
7. In the TE administrator menu, select the item **Save configuration**.

   The message about successful saving appears.
8. Select **OK**.

Selecting TE operation mode

Secret Net Studio TE may operate in soft and hard modes.

In soft mode, TE detects and prevents computer attacks and registers security events in the TE log.

In hard mode, TE also stops computer operation if an attack cannot be prevented.

Specific TE reactions in soft and hard modes to various computer attacks are listed in the table below.

Tab.1 TE operation mode features

Attack type	TE reaction	
	Soft mode	Hard mode
Client driver modified [1] (patch installation)	Detect Prevent	Detect Prevent

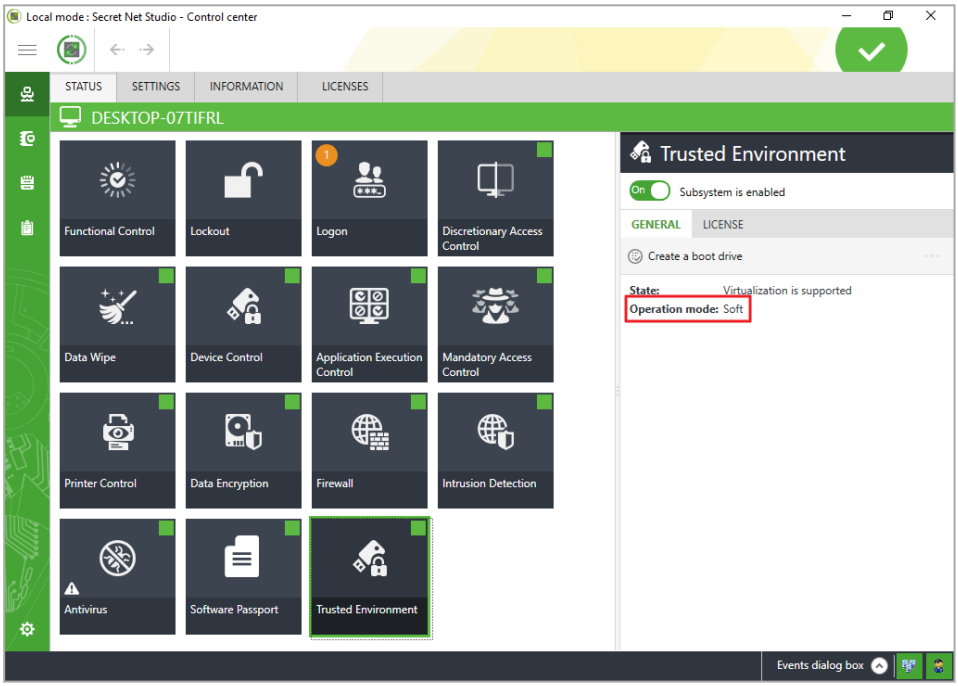
Client driver stop	Detect	Detect Stop OS
Client process stop [2]	Detect Prevent	Detect Prevent
Malware detected[3]	Detect Prevent	Detect Prevent
IC object integrity violation	Detect	Detect Stop OS

[1] Client driver– Secret Net Studio driver, controlled by TE.
[2] Client process– Secret Net Studio process, used by TE API for protection.
[3] Malware, detected during computer attacks (see p. **256**).

By default, TE operates in soft mode.

You can see the current TE operation mode:

- in the **Local Control Center — Computer panel >Trusted Environment > Operation mode**:

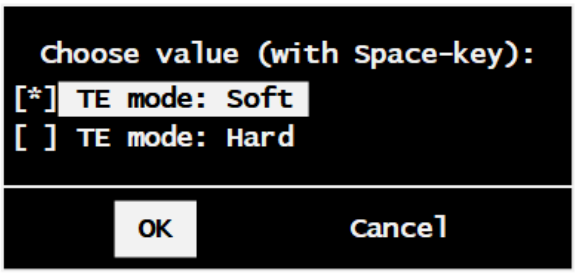


- in the TE administrator menu (see Fig.2 on p. **251**) — **TE mode: change**.

Attention! Updating, repairing and uninstalling components of the Client (including patches) are allowed only in TE soft mode and when TE is disabled. If you try to perform these operations in TE hard mode, a message appears: **To modify or uninstall the program, its components or patches, you must switch Trusted Environment to "soft" operation mode**.

To switch the TE operation mode:

1. In the TE administrator menu (see Fig.2 on p. **251**), select **TE mode: change**.
   TE operation mode selection window appears as in the figure below.



2. Select the required operation mode and press **Space**:
   - **TE mode: Soft** — to set TE to soft mode;
   - **TE mode: Hard** — to set TE to hard mode.
3. Select **OK**.

   Note. To cancel changes, select **Cancel**.
4. In the TE administrator menu, select **Save configuration**.

   The changes are saved. Success message appears.
5. Select **OK**.

Configuring integrity control in TE

Integrity Control function in TE allows to:

- block Secret Net Studio driver code modification in the memory;
- periodically check Secret Net Studio process operation;
- protect IC objects from unauthorized deletion.

When TE starts, critical Secret Net Studio services and drivers are placed under control. You can find the list of critical drives and services on p. **296**.

If integrity of an IC object is violated, when TE is in hard operation mode, OS operation will be stopped. BSOD with error code **0x5ECCODE0** appears (see p. **297**). Information about violations is registered in the TE event log.

You can edit the automatically created list of IC objects in the following ways:

- change IC object path (see below);
- place a selected IC object under control/remove a selected IC object from control (see p. **255**);
- add objects to the list (see p. **256**);
- remove objects from the list (see p. **256**).

Attention! After making changes in the kits you need to recalculate checksums of the IC objects .

To change IC object path:

1. In the TE administrator menu (see Fig.2 on p. **251**), select **Windows objects: change**.

   A window with a table of IC objects appears as in the figure below.

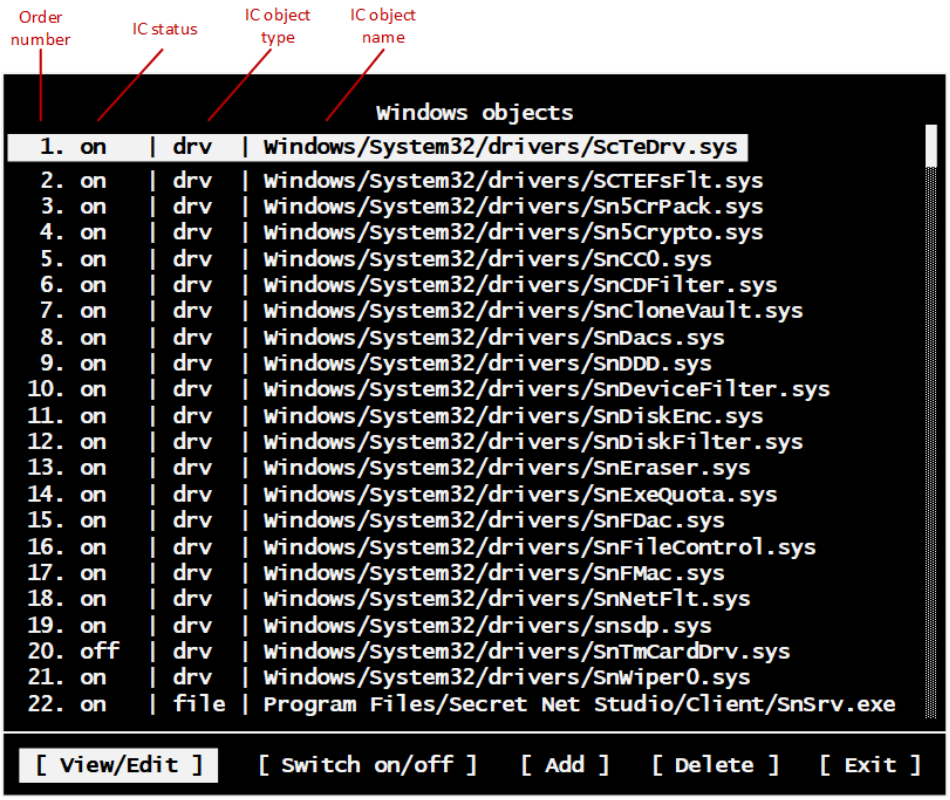


Fig.3 Window with IC object table

2. Select the required object in the table and select **[View/Edit]**.

   A window for changing paths to the file or to the driver appears as in the figure below.

Fig.4 Window for changing paths to the file or to the driver

3. Select the next action:
   - to change the path to the file, select **[Set file path]** and enter the path to the file;
   - to change the path to the driver, select **[Set driver path]** and enter the path to the driver;
   - to return to the IC object table, select **[OK]**.
4. Select **[Exit]** or press **Esc**.
5. In the TE administrator menu, select **Save configuration**.

   Wait for the changes to be saved. A message appears saying that changes are successfully saved.
6. Select **OK**.

To place an IC object under control/remove an IC object from control:

1. In the TE administrator menu, (see Fig.2 on p. **251**) select **Windows objects: change**.

   A window with a table of IC objects appears (see Fig.3 on p. **255**).
2. Select the required object in the table and select **[Switch on/off]**.

   Selected IC object is placed under control/removed from control (the status switches to **on/off** in the second column of the IC object table).

3. Select **[Exit]** or press **Esc**.
4. In the TE administrator menu, select **Save configuration**.

   Wait for the changes to be saved. A message appears saying that changes are successfully saved.
5. Select **OK**.

To add an object to the IC object list:

1. In the TE administrator menu (see Fig.2 on p. **251**), select **Windows objects: change**.

   A window with a table of IC objects appears (see Fig.3 on p. **255**).
2. Select **[Add]**.

   A window for selecting object appears.
3. Select the object you want to add to the list of controlled objects.
4. Press **Enter**.

   A window for changing paths to the file or to the driver appears (see Fig.4 on p. **255**).
5. If necessary, change path to the file/driver and select **[OK]**.

   The object is added to the IC object list.
6. Select **[Exit]** or press **Esc**.
7. In the TE administrator menu, select **Save configuration**.

   Wait for the changes to be saved. A message appears saying that changes are successfully saved.
8. Select **OK**.

To remove an object from the IC object list:

1. In the TE administrator menu, (see Fig.2 on p. **251**) select **Windows objects: change**.

   A window with a table of IC objects appears (see Fig.3 on p. **255**).
2. Select **[Delete]**.

   The object is removed from the list.
3. Select **[Exit]** or press **Esc**.
4. In the TE administrator menu, select **Save configuration**.

   Wait for the changes to be saved. A message appears saying that changes are successfully saved.
5. Select **OK**.

To recalculate checksums of IC objects:

1. In the TE administrator menu, (see Fig.2 on p. **251**) select **Windows objects: update**.

   A message appears saying that the operation is successfully finished.
2. Select **OK**.
3. In the TE administrator menu, select **Save configuration**.

   A message appears saying that changes are successfully saved.
4. Select **OK**.

Configuring computer attack detection

Note. Computer attack detection function in TE (Anti-Exploit) is currently experimental. By default, this function is disabled.

TE allows you to detect the following computer attack types:

- SMEP reset;
- executing commands in a stack;
- External Blue vulnerability exploit;

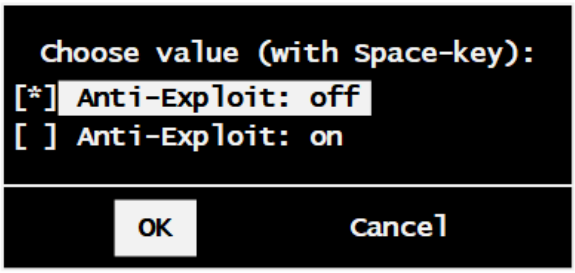
- writing data to a protected extent.

If an attack is detected, TE prevents it or stops OS operation depending on the attack type (see Tab.1 on p. **252**). Information about the attack is registered in the TE event log.

To enable/disable attack detection function:

1. In the TE administrator menu (see Fig.2 on p. **251**), select **Anti-Exploit (experimental)**.

   A window for configuring attack detection function appears:



2. Select the required option and press **Space**:
   - **Anti-Exploit: off** — to disable attack detection;
   - **Anti-Exploit: on** — to enable attack detection.
3. Select **OK**.

   Note. To cancel changes, select **Cancel**.

4. In the TE administrator menu, select **Save configuration**.

   Wait for the changes to be saved. A message appears saying that changes are successfully saved.
5. Select **OK**.

Unlocking computer

In TE hard operation mode, if a certain event happens (see Tab.1 on p. **252**), OS operation is stopped and the computer is locked out. Then a message with information about new events in TE log appears as in the figure below.

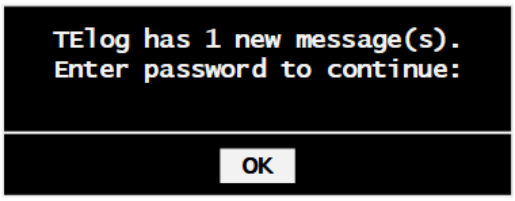


Fig.5 Message with information about new events (TE hard operation mode)

The OS can only be started after a TE administrator views the TE event log.

To unlock the computer:

1. In the message window, enter TE administrator password and select **OK**.

   The TE event log window appears (see Fig.6 on p. **258**).
2. View detailed information about the event that caused computer lockout. That event has the **New** status.

   Note. There may be several events that cause computer lockout. To unlock the computer, view the information about every new event.

   Attention! Perform administrative actions according to the current security policy of your organization.
3. Select **Exit** or press **Esc**.

TE administrator menu appears (see Fig.2 on p. **251**).

4. Select **Exit**.

The computer is unlocked and ready to boot the OS.

Working with event log

TE registers the following event types:

- an unauthorized attempt to stop a Secret Net Studio service;
- a Secret Net Studio driver unload attempt;
- IC object integrity violation;
- a Secret Net Studio driver code modification attempt;
- an error while entering TE administrative mode.

The TE event log is stored on the system drive.

The TE event log overwrites old events with new events.

The TE administrator can do the following while working with the log:

- view the log, including detailed information about every event in the log;
- clear the log;
- export the log to a file on the TE boot drive.

Viewing events

To view the TE event log:

1. In the TE administrator menu, (see Fig.2 on p. **251**) select **TElog: view**.

Event log window appears as in the figure below.

Fig.6 TE event log

Note. If the event log is empty, the **TElog is empty** message appears.

2. Select the next action:

- To navigate in the log, use ↑ and ↓.
- To view detailed information about an event, select **Select**. The event information window appears as in the figure below.

To return to the event log window, select **OK**.

Note. The event loses the **New** status after you view its detailed information. Viewing is necessary to unlock the computer, operating in TE hard mode (see p. 257).

- To delete a selected event, in the event log window or in the detailed event information window, select **Delete**.
- To return to the TE administrator menu, select **Exit**.

Clearing TE event log

Attention! Before clearing the log, look through it carefully.
You can save it to a file (see p. 259).

To clear the event log:

1. In the TE administrator menu (see Fig.2 on p. **251**), select **TElog: clear** or in the event log window, (see Fig.6 on p. **258**) select **Clear TElog**.

   The log is cleared. A success message appears.
2. Select **OK**.

Exporting event log

To export the event log:

1. In the TE administrator menu (see Fig.2 on p. **251**), select **TElog: export**.

   The log is saved to **te.snlog** on the TE boot drive.

   A success message appears.
2. Select **OK**.

Disabling Trusted Environment

You can disable TE locally on the computer, where it operates.

Attention! TE can be disabled only in soft operation mode (see p. 252).

To disable TE:

1. In the Windows **Start** menu, click **Security Code**, then click **Local Control Center**.

   The Local Control Center starts.
2. In the **Local Control Center**, on the **Computer** panel, click **Trusted Environment**.

On the right side of the window, you can see the information about the **Trusted Environment** subsystem.

3. Set **Subsystem is enabled** to **off**.

   A message appears, saying that the computer must be restarted.

4. Restart the computer.

   Trusted Environment is disabled. The OS will boot in standard mode.

Chapter 23
Sandbox

Sandbox is a mechanism which protects the computer resources from damage by running unknown software in an isolated environment. The mechanism analyzes the program operation and assigns it a trust level according to which the program is added to the lists of trusted or prohibited programs. Unknown software can be run either by users or administrators.

Note. Sandbox is available only in Secret Net Studio version 8.7 and later.

Enable Sandbox

The Sandbox mechanism can be enabled automatically or manually. The mechanism is enabled automatically during the centralized installation of the Client after the license is registered in the centralized storage (by default, the mechanism check box is selected in the deployment task).

If the license for Sandbox is registered after the installation of the Client, the mechanism must be enabled manually: centrally or locally.

Below you can find the description of the enabling process for Sandbox by means of the Control Center. To enable the mechanism locally, the same procedure is performed in the Local Control Center.

To enable the mechanism using the Control Center:

1. Open the **Computers** panel, select the required computer, right-click it and select **Properties**. In the **Status** tab, click the **Sandbox** tile. Information about the mechanism appears to the right of the tile.
2. Set the toggle to **ON**.

Analyze programs and create lists

You can perform an analysis of programs in Sandbox to determine their trust levels or add them manually to the black and/or white lists. The user can perform an additional program analysis.

To execute a program in Sandbox:

1. Open **Start** menu and select **Sandbox** in the **Security Code** group.
2. Open the **Sessions** panel and click **Run**.

   The dialog for adding programs appears.
3. Specify the path to the program to be analyzed and click **Run**. Select a set of rules if necessary.

   The program is executed in Sandbox in a new container for analysis or in one of the existing containers.
4. Perform all the necessary operations in the program being analyzed and then quit it. Once you quit the program, a dialog containing the analysis results appears:
   - if the program is assigned the required trust level, Sandbox adds it to the white list;
   - if the program is not assigned the required trust level, Sandbox force-quits the program, adds it to the black list and notifies the user about it.
   - If the user quits the program before the check is completed, Sandbox saves the context of the program analysis and then uses it next time when the program is run via Sandbox.

To add a program to the black/white list:

1. Open **Start** menu and select **Sandbox** in the **Security Code** group.

2. Open the **Lists** panel, select the tab containing the required list and click **Add**.

   The dialog for adding programs appears.
3. Specify the path to the program to be added to the list and click **Add**.

   The program is added to the list.

Configure rules

You can create new rules and sets of rules, edit the existing ones and delete those which are not necessary. All the operations are performed in Sandbox.

To create a set of rules for Sandbox:

1. In **Sandbox**, open the **Rules** tab and click **Create new rule**.

   The dialog for creating sets of rules appears.
2. Specify the name for the new set of rules, select a template if necessary and click **Create**.

   The specified set of rules is added to the list of rule sets.
3. Click **Save**.

To add Sandbox rules to a set:

1. In **Sandbox**, open the **Rules** panel, select a set of rules to be added and click **Create** in the drop-down list.

   The dialog for creating rules appears.
2. Select a category and a type for the rule, specify the name of the object, configure the settings and click **Add**.

   The rule is added to the specified set. To copy a rule contained in the set, select the rule to copy and click **Duplicate**.

To edit a Sandbox rule in the set:

1. In **Sandbox**, open the **Rules** panel, select the set of rules in the drop-down list containing the rule to be edited and double-click it.

   The dialog for editing rules appears.
2. Configure the rule settings and click **Apply**.

To delete a set of Sandbox rules:

- In **Sandbox**, open the **Rules** panel, select the set of rules to be deleted in the drop-down list and click **Delete**to the right of the list of rule sets.

To delete a single rule:

- In **Sandbox**, open the **Rules** panel, select the set of rules containing the rule to be deleted, select the rule in the list and click **Delete** below the list of rules.

Configure logs

Sandbox contains its own event logs. A standalone log with events registered according to audit configuration in the rule set is created for each session Logs are managed by the administrator. Logs can be cleared and exported.

Update Sandbox rule database

The Sandbox rule database, Antivirus database and IPS database are updated in the same manner. See the update details on p. **241**.

Appendix

User management program

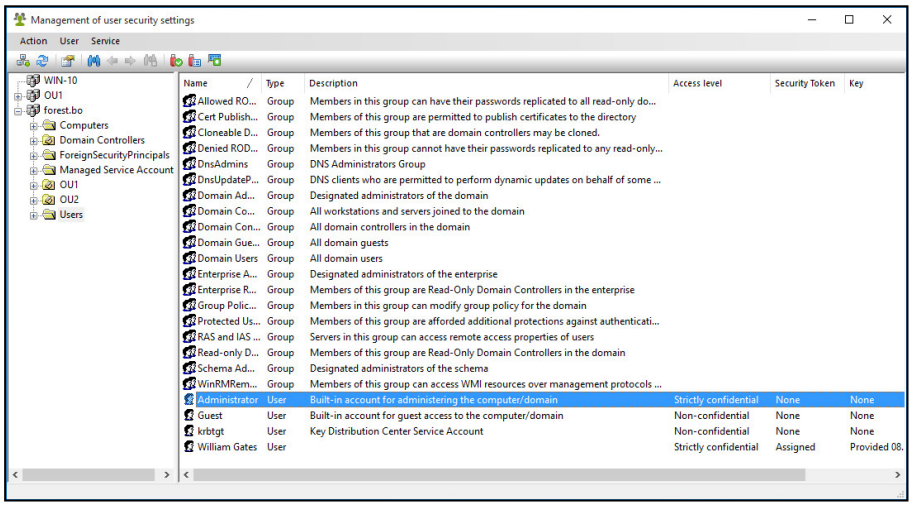
The user management program makes it possible to configure user operation parameters within the security system. Actions with both domain and local users can be performed using this program.

To run the program:

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

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

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



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

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

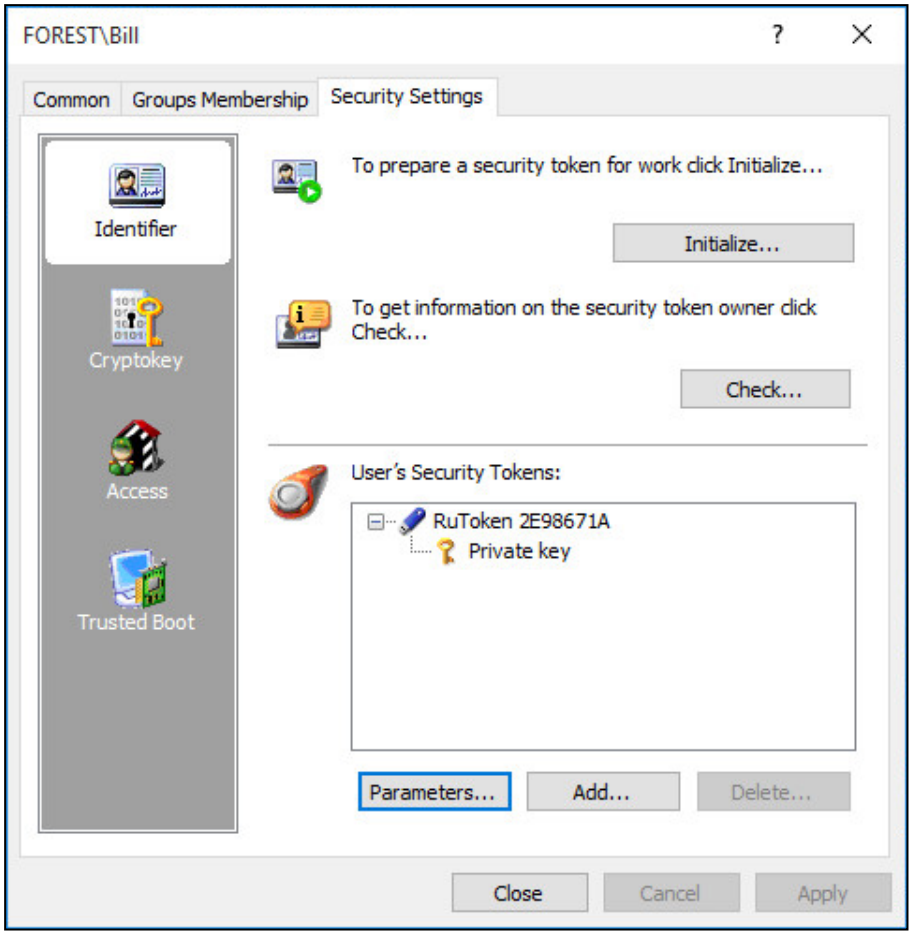
For the centralized management, the structure of the current domain is downloaded to the program by default. If necessary, the structures of other Active Directory domains can also be downloaded if it is possible to connect to these domains. To do so, in the **Action** menu, click **Connect to Active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

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

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

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

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



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.

List of groups, classes and models for device control

Tab.2 Device groups, classes and models

Group	Class	Model
Local devices	Serial ports. Parallel ports. Removable disks. Optical disks. Physical drives. Processors. Random access memory. Motherboard. Hardware support. Virtual disks	___
USB devices	Network cards and modems. Interface devices (mouse, keyboard, UPS, etc.) Scanners and digital cameras. Printers. Storage devices. Bluetooth adapters. Cell phones (smart phones, tablets) Digital identifiers and readers. Other	Model creation is provided. There are predefined models of security tokens

Group	Class	Model
PCMCIA devices	Serial ports and modems. Parallel ports. Storage devices. Network adapters. Other	Model creation is provided
IEEE1394 devices	Storage devices. Printers. Scanners and digital cameras. Network devices. Digital video cameras. Other	Model creation is provided
Secure Digital devices	Memory cards	Model creation is provided
Network	Ethernet connection. Wireless connection (WiFi). Bluetooth connection. 1394 connection (FireWire). IR connection (IrDA)	Model creation is provided for FireWire connections

Examples of configuring external drives use

Local assignment of external drives to users

This section covers an example of a local setup for control of user access to external drives. As a result of this setup, users will be granted permissions to connect and use specific devices (for each user — a separate removable disk or several disks) to which other users will not have access.

1. Connect the device.

   Note. The device must be connected for it to appear in the device list of the local policy. If the device was connected before and information about it is available in the device list, there is no need to connect the device.

2. Run the local Control Center. For this purpose, click the **Start** button and select **Local Control Center** in the program menu.
3. In the Control Center, open the **Computer** panel and select the **Settings** tab.
4. In the **Policies** section, select **Device Control**.
5. Select the connected device line.
6. In the cell of the **Control parameters** column, clear **Inherit control settings from parent object** (if selected) and select the **Device connection is allowed** control mode.
7. Click the cell of the **Permissions** column.

   The **Permissions...** dialog box appears.
8. Edit the list of accounts in the upper section of the dialog box. Add the account of the user who will be permitted to use the device and then remove the elements you do not need.
9. Specify access parameters for the elements of the list: enable permissions for performing operations for the account of the user who will be allowed to use the devices and disable for all other elements (if they are on the list).
10. Close the dialog boxes saving the changes and, if necessary, repeat the procedure for all other devices.
11. Click **Apply**.

Centralized creation of a list of external drives

Secret Net Studio makes it possible to restrict the connection of devices and allow only devices authorized by the security administrator to be used. To do this, the following methods can be used:

- creating a device list on an individual computer (see p. 71);
- centralized creation of a list of devices that are used in group policies (domains, business units or the Security Server).

If a device is connected to the same computers, use the first method for creating the device lists. If you need to create a uniform list of connected devices for computers in a domain, business unit or those subordinate to the Security Server, you can use the respective group policy tools in the Control Center. However, do not add too many devices to the list (hundreds or more), because this can take a long time when updating group policies on the computers.

The list of connected devices in a group policy is created as follows:

1. Define the device control policy in the respective group policy (see p. 74).
2. Add the required devices to the group policy list (see p. 74).
3. Enable the **Device connection is allowed** control mode for the added devices. In the parameters of the models and/or classes to which the added devices belong, enable the **Device connection is not allowed** control mode. For the description of the device control policy setup, see p. 80.

About the Applications and data control program

Program start

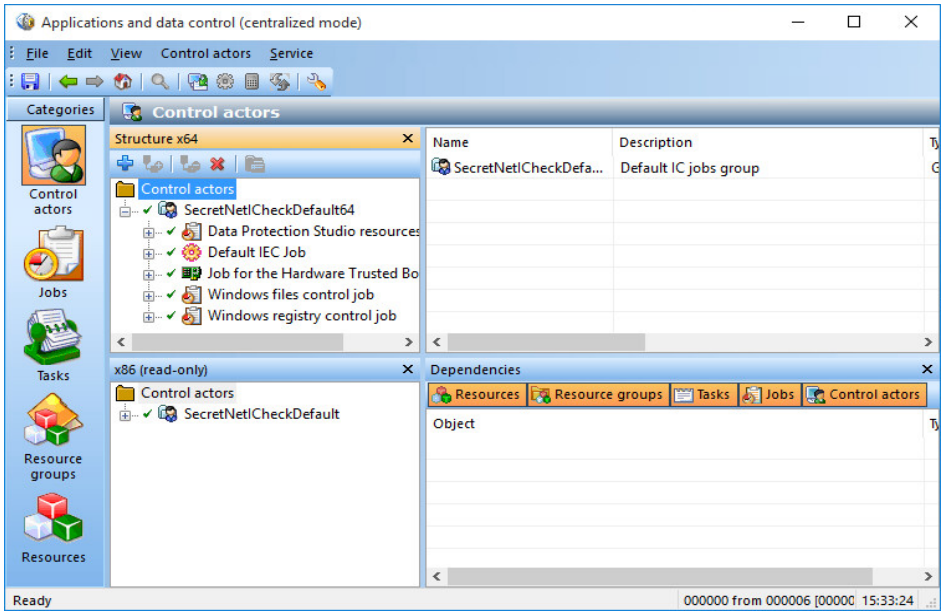
To start a program in centralized mode:

1. In the Security Code group of the Start menu, select **Applications and data control (centralized mode)**

   When started, the program checks if it is possible to get full access to the data model of the respective bitness in the centralized database of the Integrity Check and Application Execution Control. Only one computer of the system has full access.
2. If it is not possible to get full access to the centralized database (e.g. the IC Control Center already operates centrally on another computer of the same OS bitness), the respective message appears prompting you to select one of the following options:
   - cancel the start of the program (recommended) - to do so, click **Cancel**;
   - start the program with access to the centralized database in read-only mode - to do so, click **No**. In this case, the data model last saved in the centralized database is loaded to the program. The data model cannot be edited;
   - start the program and get full access to the centralized database - to do so, click **Yes**. As a result, the user of the another computer operating the IC program will not be able to write in the centralized database and save the changes.

   Attention! If the control of administrator privileges is enabled, you are prompted to introduce the administrator PIN.
   - To start the program as administrator, introduce the respective PIN and click **OK**.
   - To start the program in limited functionality mode, click **Cancel** or close the PIN prompt dialog box.

Below you can see sample window of the program in centralized mode.

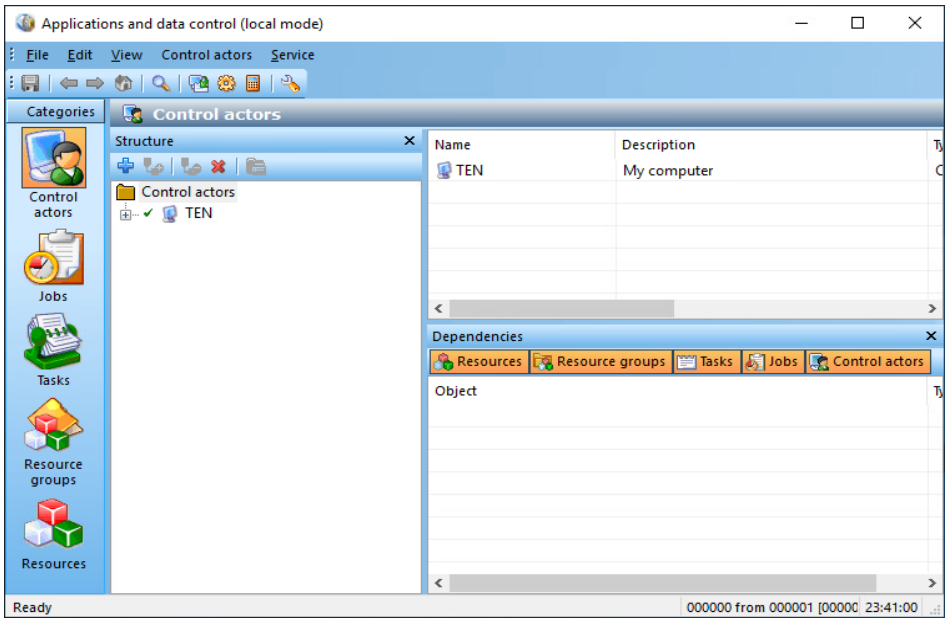


To run the program in local mode:

- In **Start** menu, the **Security Code** group, select **Applications and data control**.

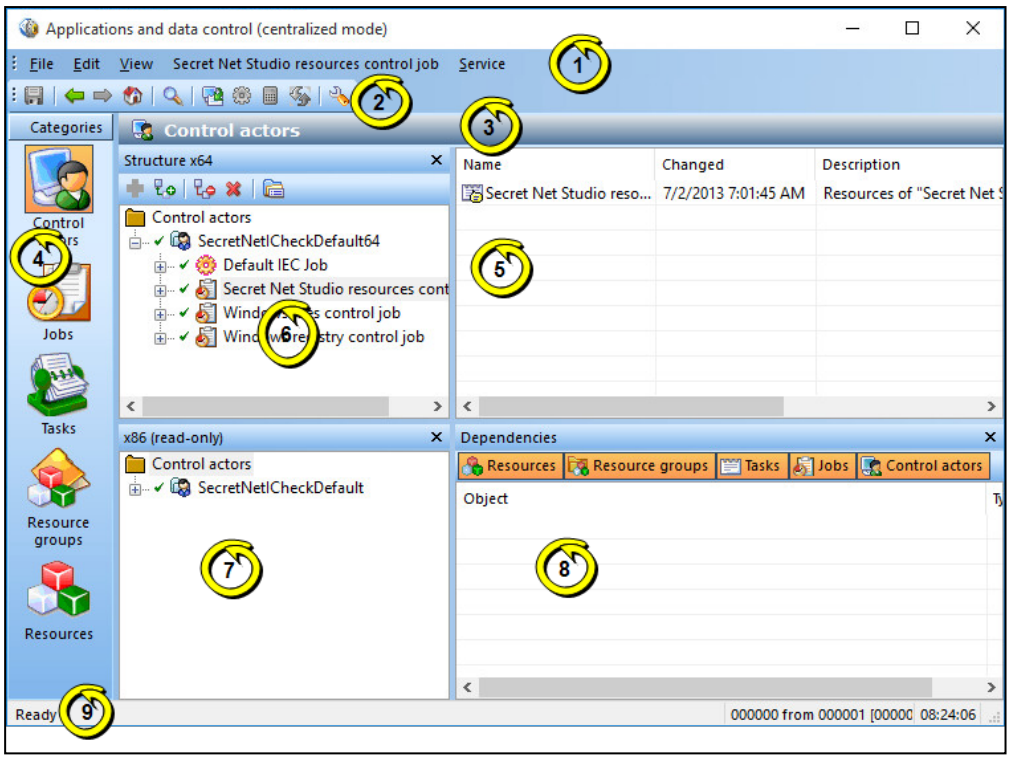
> **Attention!** If the control of administrator privileges is enabled (see p. 36), you are prompted to introduce the respective PIN.
> - To start the program as administrator, introduce the PIN and click **OK**.
> - To start the program in limited functionality mode, click **Cancel** or close the PIN prompt dialog box.

Below you can see the window of the program in local mode.



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:

1 — Menu
Contains program commands
2 — Main window toolbar
Contains hot keys for commands and software tools
3 — Informative title
Contains the name of the category of objects selected for display
4 — Category panel
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
5 — Object list area
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: • white background – the object is linked to superior or subordinate objects; • pink background – the object is not linked to superior or subordinate objects; • gray background – the resource is not under control. In local mode, centrally installed object names are highlighted. You can change the color scheme (see p. **272**)

6 — Structure window
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 **Add to working model**
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 main window of the program. 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 main window of the program. 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
View | Status bar	Enables or disables status bar display **(9)**
View | Panels | Buttons	Enables or disables toolbar display **(2)**
View | Panels | Heading	Enables or disables information title display **(3)**
View | Panels | Categories	Enables or disables categories panel display **(4)**
View | Panels | Structure	Enables or disables structure window display **(6)**
View | Panels | Structure for reading	Enables or disables display of the structure window for data models of different bit depth **(7)**

Command	Description
View | Panels | Dependencies	Enables or disables display of the dependencies window **(8)**

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.

Text, Background color
These define, respectively, the colors of symbols and the background for displaying information on objects linked to both superior and subordinate objects
Error text, Background color of the error
These define, respectively, the colors of symbols and the background for displaying information on objects not linked to superior or subordinate objects
Text (not controlled), Background (not controlled)
These define, respectively, the colors of symbols and the backgrounds for displaying: • information on resources with disabled integrity control attribute; • integrity control jobs without a schedule
Text (not local), Background color (not local)
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.

Dialog when preparing for AEC
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)

Reference value calculation dialog
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.

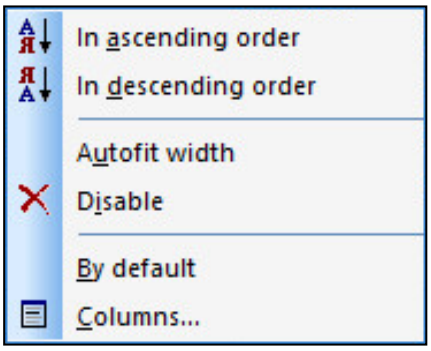
Command	Button	Description
View mode | Back		Go to the previously selected structure element
View mode | Next		Go to the next selected structure element
View mode | Home		Go to the root structure element

Configure table column view

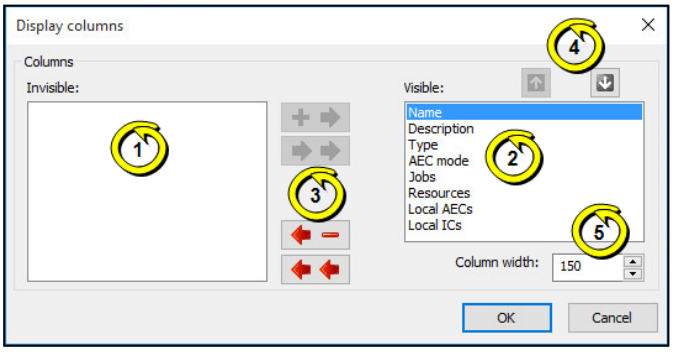
The object list and dependency window share the same table form used to display the list of objects. Table column configuration is based on the object category being displayed. To display the information as well as possible, you can change column width, add or delete columns, or move them relative to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

Consider the register
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
Entire value
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
Search in field
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. 271).

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.

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.

The flow control mode configuration program

The program for configuring the flow control mode is designed to configure the parameters of MAC in the flow control mode. For information on running the program and its operating conditions, see p. 144.

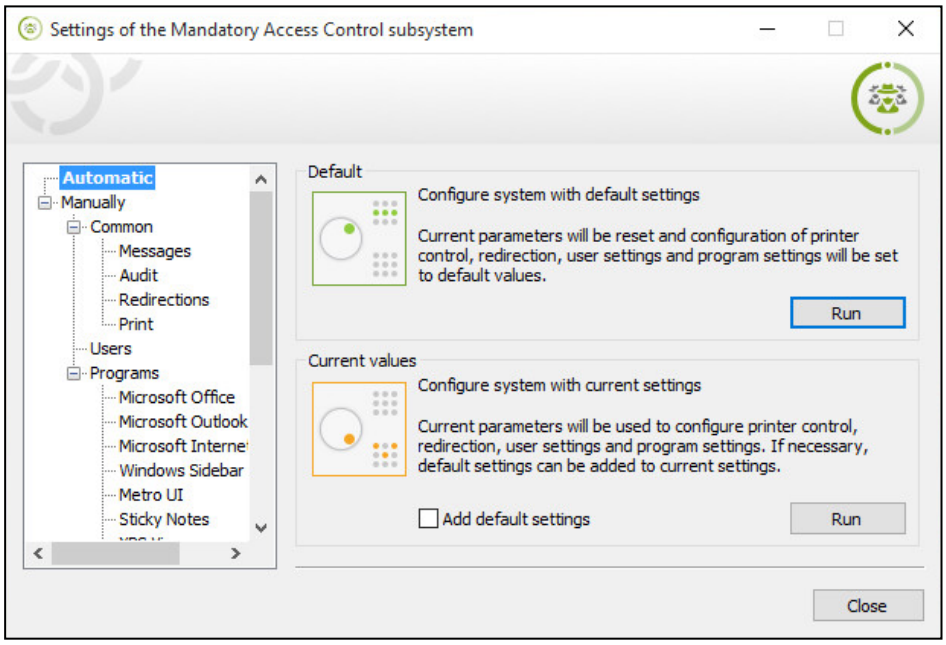
Automatic setup

The system governing **Mandatory Access Control** and **Print Control** settings can be configured automatically. During automatic setup, you can use parameter values that are set by default or the current values configured during the manual setup.

Automatic setup with default values is applied when it is necessary to remove the current configuration and restore initial parameter values. This may be required if the parameter values are set incorrectly or deleted or during the initial system setup with minimum configuration for operating in the flow control mode.

Use current values to repeat the use of the parameter values that are set for the system. In this way, you can restore the system configuration after the mechanism's failure or when adding new users, programs, printer or other objects to the system that are used in MAC and Print Control. In addition to the current parameter values, you can add initial values (default values) during setup. This does not remove the current values.

To perform automatic setup, select the **Automatic** mode as in the figure below.



To delete the current configuration and set up your system using default values:

- In the **Default** section, click **Run**.

  The automatic system setup process begins. Once the process is complete, a message appears.

To set up your system using the current parameter values:

1. If you need to add initial values to the current values, select the **Add default settings** check box.
2. In the **Current values** section, click **Run**.

   The automatic system setup process begins. Once the process is complete, a message appears.

Manual setup

The setup program can be used to manually modify the parameters related to the operation of the **Mandatory Access Control** and **Print Control** mechanism. This ensures the operation of the mechanism taking into account the specific features of a computer's software environment and user preferences.

Tools for manual parameter setup are available in the following main sections:

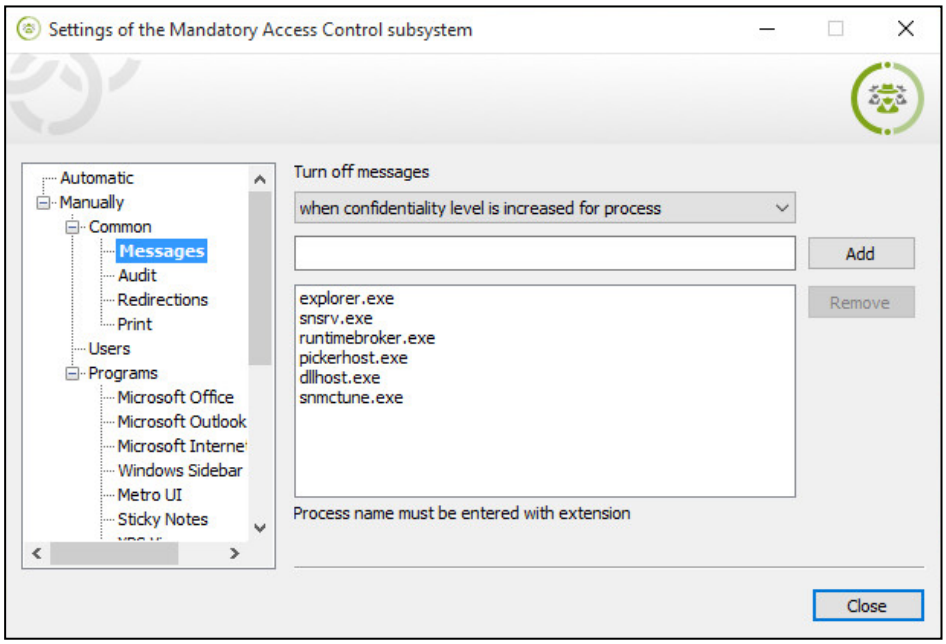
- **Common** — setup of common operation parameters for users and applications;
- **Users** — setup of parameters related to user accounts;
- **Programs** — setup of parameters related to applications.

Disabling system alerts

It is possible to disable alerts in the following cases:

- when elevating the confidentiality level of a process (for example, **explorer.exe**) due to accessing a file with a higher confidentiality category (applicable when the flow control mode is disabled);
- when elevating the confidentiality level of a file with a selected extension or a file from a selected folder. This option is designed to ensure automatic creation and editing of service files that are used by some applications (for example, by MS Word), in the flow control mode when working in confidential sessions;
- when moving a confidential file with a selected extension to external media which results in resetting the confidentiality category of the file (applicable when the flow control mode is enabled during confidential sessions).

To configure the parameters for disabling alerts, select **Manually**. Then, go to the **Common** | **Messages** subsection.



To disable alerts when elevating the confidentiality level for processes:

1. In the **Turn off messages** drop-down list, select **when confidentiality level is increased for process**.

   The list of processes (executable files) for which alerts are disabled will be displayed below.

2. Edit the list of file names:
   - to add an element to the list, type the name of the executable file in the list (with its extension), and click **Add**;
   - to remove elements from the list, select them and click **Remove**.

To disable alerts when elevating confidentiality categories of files with specific extensions:

1. In the **Turn off messages** drop-down list, select **when confidentiality level is increased for file "(by extension)"**.

   The list of file extensions for which alerts are disabled will be displayed below.
2. Edit the list of extensions:
   - to add an element to the list, enter the file name extension in the line in the following format: **.<extension>** (for example, **.Ink**). Then, click **Add**;
   - to remove elements from the list, select them and click **Remove**;
   - to disable alerts for all file extensions, add ".*" to the list or select the **Turn off messages for all file types** check box. The list editing tools will become inactive. To reactivate the list of extensions, clear the check box.

To disable alerts when elevating confidentiality categories of files from specific directories:

1. In the **Turn off messages** drop-down list, select **when confidentiality level is increased for file (by directory)**.

   Below, you will see the list of directories; alerts will be disabled for files from these directories (regardless of file extensions).
2. Edit the list of paths to directories:
   - to add an element to the list, enter the directory path and click **Add**;

     Note. The directory path is entered taking into account the following specific features:
     - a string can contain both full path (indicating a specific directory) and partial path (making it possible to define a subset of paths to directories). If a subset of paths is specified, the string should start with "\";
     - the path to a directory is specified WITHOUT "\" at the end;
     - directory names should be in the **LFN (Long File Name)** format.
   - to remove elements from the list, select them and click the Remove button.

To disable alerts when confidential information is output to external media:

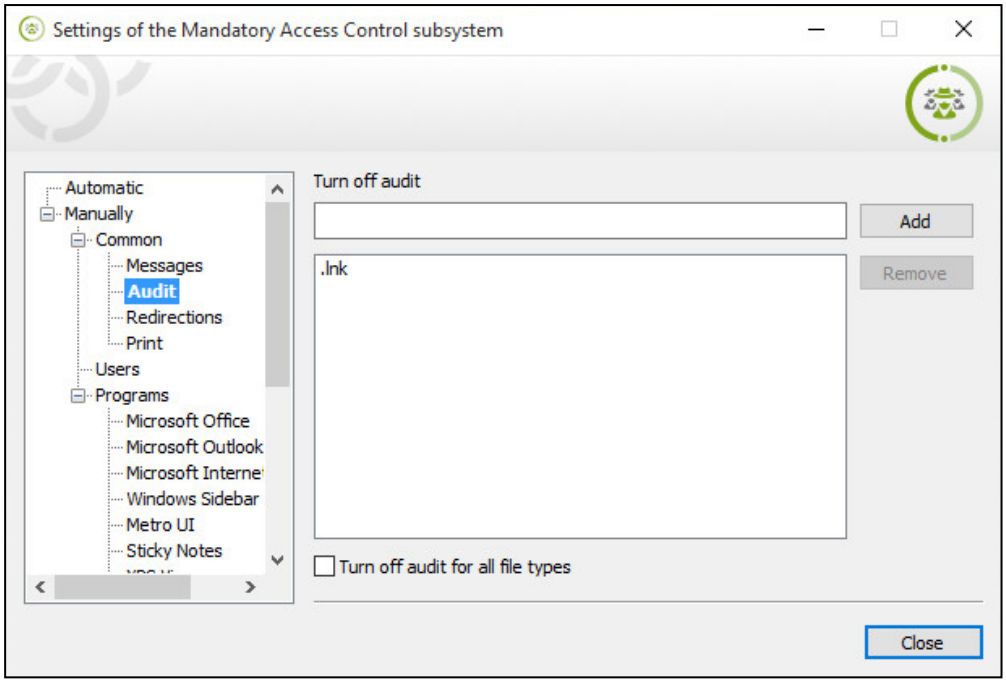
1. In the **Turn off messages** drop- down list, select **when outputting confidential information**.

   The list of file extensions for which alerts are disabled will be displayed below.
2. Edit the list of extensions:
   - to add an element to the list, enter the file name extension in the line in the following format: **.<extension>** (for example, **.Ink**). Then, click **Add**;
   - to remove elements from the list, select them, and click **Remove**;
   - to disable alerts for all file extensions, add ".*" to the list or select the **Turn off messages for all file types** check box. The list editing tools will become inactive. To reactivate the list of extensions, clear the check box.

Disabling file event logging

The Secret Net Studio log records the internal system calls to files during the operation of the **Mandatory Access Control** and **Print Control** mechanism. If necessary, logging these events can be disabled with respect to certain file extensions. This allows you to reduce the amount of information that is stored in the log.

To configure the parameters for disabling event logging, select **Manually** and go to the **Common** | **Audit** subsection.



To disable logging of file events for files with certain extensions:

- Create a list of file extensions:
  - to add an element to the list, enter the file name extension in the line in the following format: **.<extension>** (for example, **.Ink**). Then, click the **Add** button;
  - to remove elements from the list, select them and click **Remove**;
  - to disable event registration for all file extensions, add ".*" to the list or select the **Turn off audit for all file types** check box. The list editing tools will become inactive. To reactivate the list of extensions, clear the check box.

Redirection of common service files output

The **Mandatory Access Control** and **Print Control** mechanism checks that the user access level and the access object confidentiality category (folder, file) match. However, some applications (for example, MS Word) call service files which are stored in special folders. It is not possible to change the confidentiality categories of these files depending on the user access level. When using MAC in the flow control mode, such features result in conflicts and the incorrect operation of applications.

To fix this problem, Secret Net Studio contains the function for redirecting the output of common service files. This function can be used during confidential sessions. To ensure that the application operates during sessions with different confidentiality levels, separate folders (depending on the number of categories) are created where common service files are saved. These copies are assigned the corresponding confidentiality categories. If an application attempts to call a common file during a confidential session, the security system redirects this call to a copy of a shared file which is located in a separate folder that was created for the session with this confidentiality level.

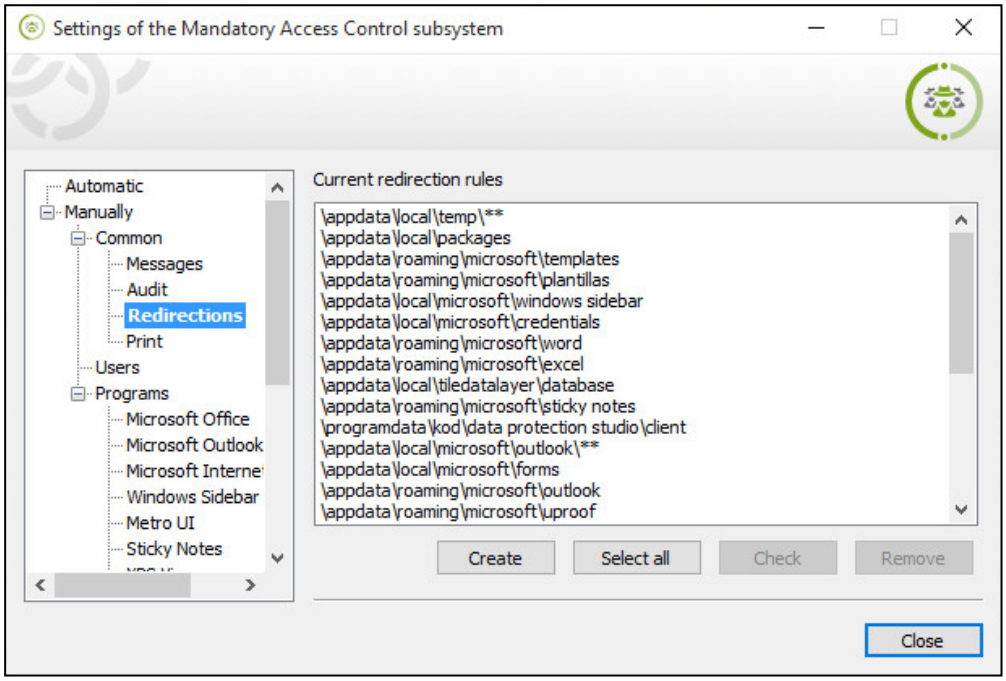
When configuring the file output redirection, a list of paths to folders containing common files is created. For these files, additional folders with various confidentiality categories should be created. These folders will store the files that are used in the sessions with corresponding confidentiality levels. For example, to process calls from the English MS Word version, the list must contain the following record: **\AppData\Roaming\Microsoft\Templates**. Depending on the user's session confidentiality level, when the application calls the folders, the information for common files will be read/written in one of the additionally created subfolders

\Templates (1) , **\Templates (2)** etc, in the directory **\AppData\Roaming\Microsoft**.

Note. As a result of the output redirection function, changes made in common service files are independent from when working with an application during sessions with various confidentiality levels. For example, if a common file was changed during a strictly confidential session, these changes will not be taken into account during sessions with other confidentiality levels, because other copies of the common file are called during these sessions.

During the automatic configuration (see p. 278), redirection folders are only created for the system disk. It is possible to choose disks if the list of paths is created manually.

To create the list of paths for file output redirection, select **Manually** and go to the **Common** | **Redirection** subsection.



To add paths to the list:

1. Click **Create**.

   A dialog box for adding paths to folders appears.

2. Create the list of paths in the dialog box:
   - to add an element to the list, enter the path and click **Add**;

     Note. The path is entered in **LFN (Long File Name)** format taking into account the following features:
     - a string can contain both full path (indicating a specific folder) and partial path (making it possible to define a subset of paths to folders). If a subset of paths is specified, the string should start with "\";
     - the path to a folder is specified WITHOUT "\" at the end;
     - if it is not necessary to copy files from a source folder to redirection folders, add the "**" (two asterisks) template substring at the end of the path. In this case, the structure of subfolders of the source folder without files will be created in the redirection folders. For example, this option is applied by default to the folders for user temporary files.
     - if it is not necessary to copy subfolders from the source folder to redirection folders, add the "*" (one asterisk) template substring at the end of the path. In this case, only copies of source folder files will be created in the redirection folders.

   - to remove elements from the list, select them and click **Remove**.

3. Click **Create**.

4. If there are several local disks on the computer, a dialog box for disk selection will appear. Folder search will be performed on these disks. Select the required disks in the dialog box and click **OK**.

   The search for folders matching the entered path criteria begins. The following folders will be created for found folders: <*directory_name*>(1), <*directory_name*>(2), etc with the respective confidentiality categories (for example, **Confidential** for the first folder and **Strictly confidential** for the second). The contents of the respective source folders will be created in the new folders (depending on specified template substrings). Once the search is finished, paths to folders will be added to the paths for file output redirection.

   Note. The select disk option makes it possible to speed up the folder search process by skipping the contents of those folders that were not selected. However, situations may occur when defined paths will match the folders on the disks that were not processed. In such cases, the security system will attempt to redirect output for these folders. Due to the corresponding structures are not available on the disk, the application may not work correctly. Therefore, if not all disks are covered by the folder search, we recommend specifying such paths that do not match the respective folders on the disks that were not been selected.

To check if redirection is possible:

1. Select paths in the list for which the redirection function should be selected (to select all elements of the list, click **Select All**).
2. Click **Check**.
3. If there are several local disks on the computer, a dialog box for disk selection will appear. Folder search will be performed on these disks. Select the required disks in the dialog box and click **OK**.

   The search for folders matching the selected path criteria begins. The availability and correctness of folder configuration will be checked for found folders (<*directory_name*>(1), <*directory_name*>(2), etc.) with the respective confidentiality categories. If necessary, folders will be created and refilled with data. Once the search and check process is complete, a message appears.

To remove paths from the list:

1. Select paths in the list to be deleted (to select all elements of the list, click **Select All**).
2. Click **Remove**.

   Selected paths will be immediately removed from the list. However, the redirection folders and files contained in them will not be removed.

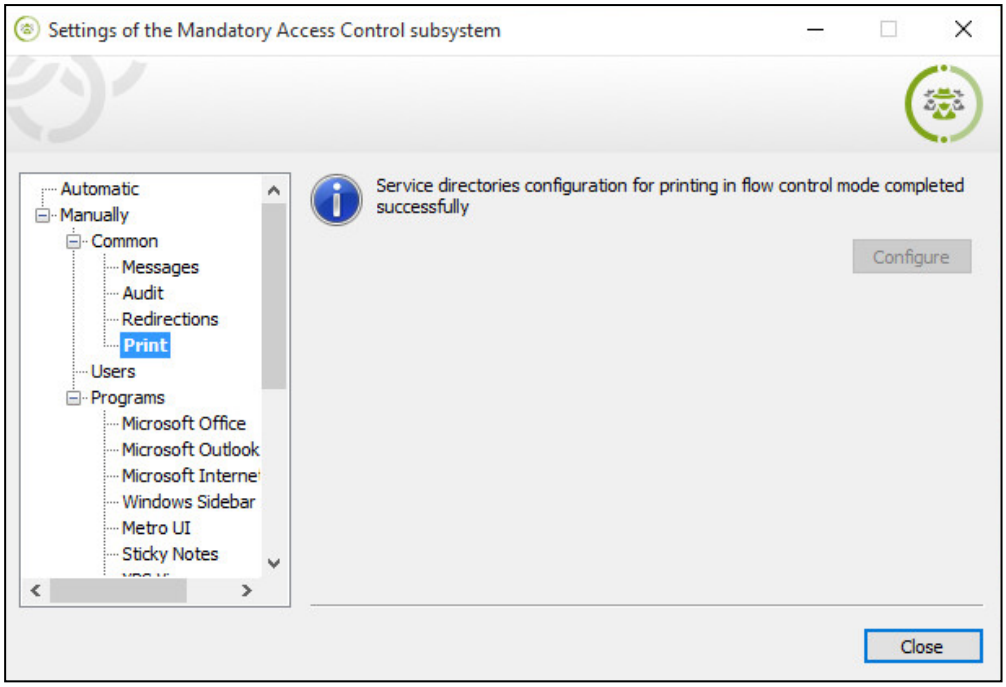
System configuration for printing

To print in the flow control mode (during confidential sessions), some service folders of the Windows OS should be configured.

Folder parameters are sufficiently configured during the general automatic configuration process (see p. **278**).

The setup program verifies the current system parameters. If you are configuring the printing in the flow control mode, print setup tools are inactive. When configuration is required, the program makes it possible to start the process manually.

To configure the parameters for printing, select **Manually** and go to the **Common** | **Print** subsection.



To start the print configuration process:

- Click **Configure** (the button is only active if configuration is not completed).

  The system setup process begins. Once the process is complete, a message appears.

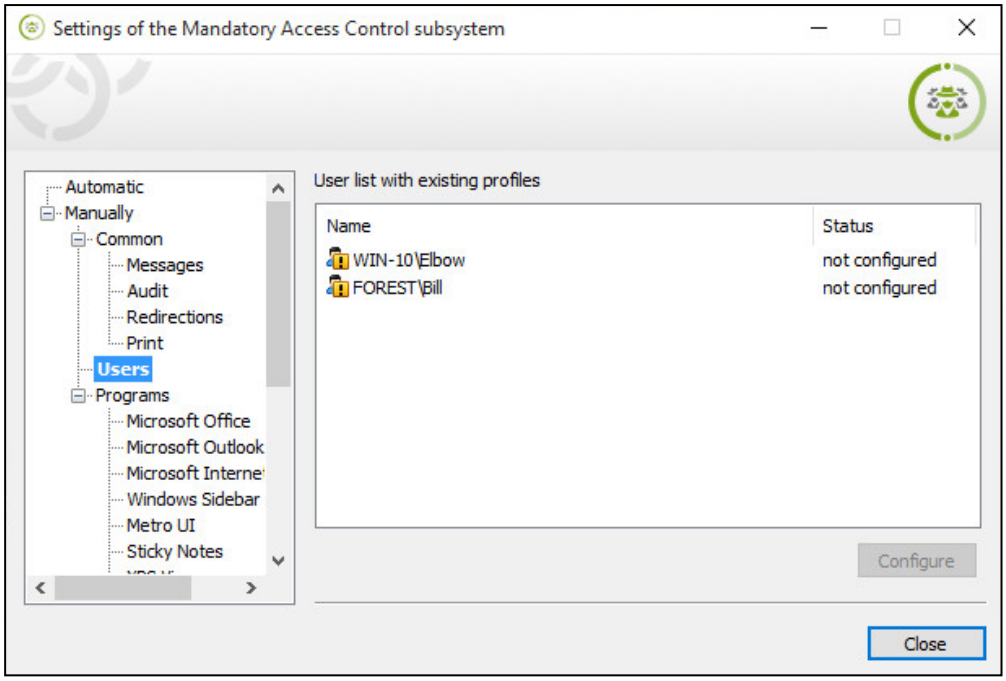
Configuring user account parameters

In the flow control mode (during confidential sessions), it is necessary to configure user account parameters. The configuration process involves creating a directory structure for file output redirection with respect to the user's temporary folders and assigning the respective confidentiality categories with a certain configuration of inheritance attributes for these directories. The configuration process is performed for those users in whose name system logon was performed on that computer at least once.

All user profiles are sufficiently configured during the general automatic configuration process p. **278**). When adding a new user or when renaming an existing user, it is necessary to configure the user account for the flow control mode. The account setup process can be started manually.

The setup program checks the current user account parameters. If the security system confirms the user's ability to work in the flow control mode, that user is shown with **configured** status. If it is necessary to configure the user, that user is shown with **not configured** status.

To configure user accounts, select **Manually** and select the **Users** subsection.



To start the user account configuration process:

1. Select the users in the list whose accounts should be configured (if a user's account is already configured, it will have the **configured** status).
2. Click **Configure**.

   The configuration process begins. Once the process is complete, a message appears.

Creating a list of applications for configuration

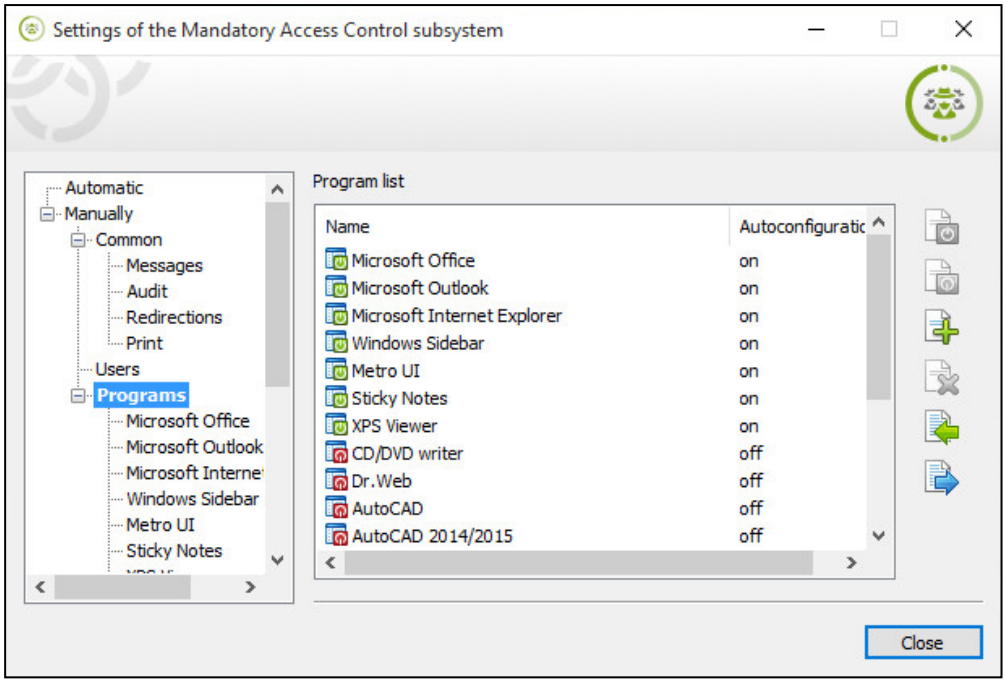
Some applications are not fully compatible with MAC when the flow control mode is enabled. To ensure that these applications work correctly, additional configuration of application-related parameters is required.

Using the program, you can configure parameters for the applications included in the list. The list is created regardless of the availability of installed applications on the computer. By default, once the Client is installed, the list contains the names of applications with detected incompatibilities and the required configuration procedure is determined.

Parameters related to applications can be configured during the general automatic setup (see p. **278**). Automatic configuration with default values is always applied to those applications that have autoconfiguration status **on** in the default list of applications (for example, for Microsoft Office). However, the application's presence in the list and its autoconfiguration status are not taken into account. If autoconfiguration with current values is performed, it is only applied to those applications that have the **on** status in the current list of applications.

The application parameters configuration process can also be started manually.

To create the list of applications, select the **Manually** and select the **Programs** subsection.



The following operations are available when creating the list of applications:

- list import from an **.xml** file (with prior removal of all elements of the current list);
- export of an existing list to **.xml** file;
- control of the application's autoconfiguration mode;
- adding a list from **.xml** file (without deleting the elements of the current list);
- removing selected list elements.

To import the list from an xml file:

1. Click the **Import** button.

   A standard file selection dialog box appears.
2. Select the required file.

   The program will load the list of applications stored in the selected file. The current list will be deleted.

To export an existing list to xml file:

1. Click the **Export** button.

   A standard file saving dialog box appears.
2. Specify the name and location of the file to be saved.

To change the application autoconfiguration mode:

1. Select the application from the list that requires autoconfiguration to be enabled or disabled.
2. Select the option:
   - To enable the mode, click **Enable autoconfiguration**.
   - To disable the mode, click **Disable autoconfiguration**.

To add lists from an xml-file:

1. Click the **Add** button.

   A standard file selection dialog box appears.
2. Select the required file.

   The list will be loaded in addition to the current list of applications in the program, stored in the specified file.

To remove an application from the list:

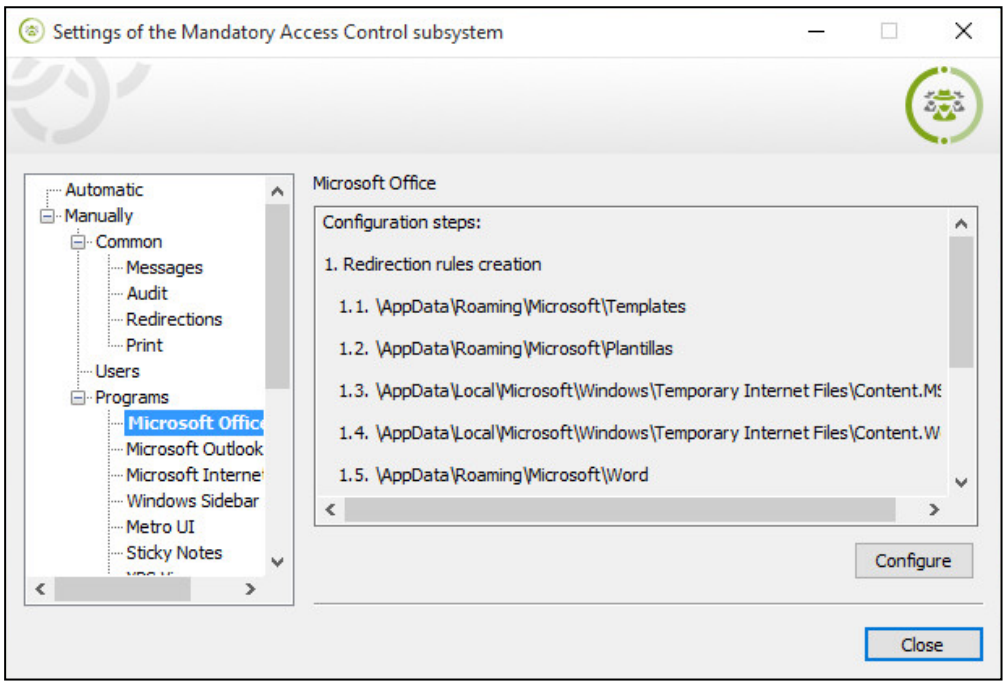
1. Select the application to be removed from the list.
2. Click the **Remove** button and confirm the action in the dialog box that appears.

Application parameters configuration

For the application to operate correctly in the flow control mode (during confidential sessions), application parameters must be configured.

Application parameters can be configured during the automatic configuration if the list of applications is assigned the enabled autoconfiguration status. You can also start the configuration procedure for an application manually.

To configure the application parameters, select the **Manually** and select **Programs** | **<application_name>**.



To start the application parameters configuration process:

1. Click the **Configure** button.
2. If there are several local disks on the computer, a dialog box for disk selection will appear. Folder search will be performed on these disks to create redirection rules. Select the required disks in the dialog box and click **OK**.

   The parameter configuration process begins. Once the process is complete, a message appears.

Disabling local disk protection in an emergency

Standard procedures are provided for disabling the protection of logical partitions (see p. **153**). When such procedures cannot be performed, you can use an emergency recovery boot disk for disabling disk protection .

Using a boot disk for emergency recovery

A boot disk is used for emergency recovery when it is impossible to start the operating system in the normal way from the system disk. For example, when a failure occurs when decoding modified data on the system disk, the start is blocked.

Using the boot disk, you can restore the initial state of the boot section on the physical disk, from where the operating system is started and/or the state of boot sections of logical partitions. For the description of the procedure for creating an emergency recovery disk, see p. **152**.

Attention! To boot from the emergency recovery disk, loading from external media must be enabled on the computer. For example, starting from an USB flash drive may require enabling the Floppy or Forced FDD emulation mode in the computer's BIOS.

When loading from the emergency recovery disk, the program starts automatically that checks if it is possible to recover the disks. If modified disks are found, and they can be recovered using a key on the boot disk, prompts appear on to remove protection from logical partitions and recover the respective sections of the system disk. To restore the initial state of an object, click **Yes**.

Emergency recovery disk for the Disk Protection and Full Disk Encryption mechanisms

With the emergency recovery disk you can:

- change the password to access encrypted disks (see p. **290**);
- reset the password for encrypted disks using the recovery code (see p. **291**);
- decrypt data on encrypted disks and remove disk protection (see p. **291**);
- restore or delete Secret Net Studio bootloader (see p. **292**);
- restore the configuration file for the Disk Protection and Full Disk Encryption subsystems (see p. **293**);

  Note. The configuration file for the Disk Protection and Full Disk Encryption subsystems contains all data about encrypted /protected disks of a computer.

- delete the configuration file for the Disk Protection and Full Disk Encryption subsystems (see p. **293**);
- delete an encrypted disk from the Full Disk Encryption configuration (see p. **294**).

To work with the emergency recovery disk, you need to boot from this disk. The operations are performed in console mode using the keyboard.

```
                    Secret Net Studio Full Disk Encryption

---------------------------- Main menu -----------------------------
[1] Password change
[2] Password reset with recovery-code
[3] Volume decryption
[4] Bootloader recovery
[5] Bootloader remove
[6] Advanced settings
[7] Reboot
--------------------------------------------------------------------
Type 1..7 to select option: _
```

Fig.7 The main menu of Secret Net Studio emergency recovery disk

```
-------------------- Advanced settings menu ----------------------
[1] Remove encrypted volume from configuration
[2] Configuration recovery
[3] Configuration remove
[4] Bootloader recovery with windows-loader overwrite
[5] System information
------------------------------------------------------------------
Type 1..5 to select option (or press ESC to return): _
```

Fig.8 The advanced settings menu of Secret Net Studio emergency recovery disk

Create an emergency recovery disk

You can create an emergency recovery disk using SnRescue from Secret Net Studio setup disk.

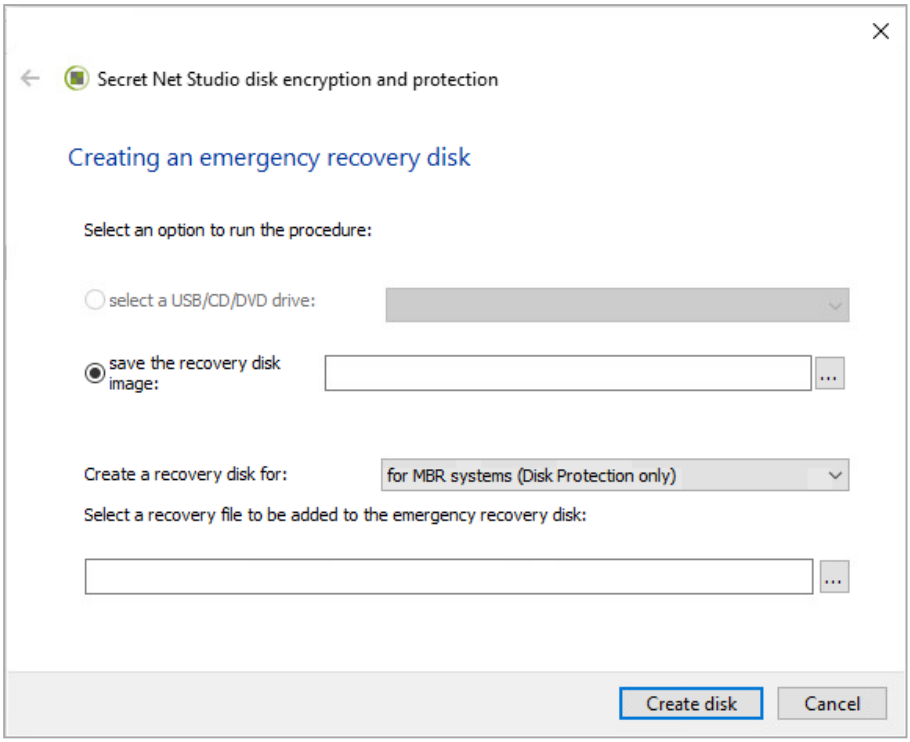
Attention! To create a disk that is going to be used for configuration recovery and data decryption, you need a recovery file. We recommend you to use a recovery file saved after encryption of all required disks. The recovery file is saved:

- in case of local storage of recovery data, in Secret Net Studio encryption wizard on a computer with encrypted disks (see p. 167);
- in case of centralized storage of recovery data, in the Control Center on a Security Server for a computer with encrypted disks (see p. 169).

To create an emergency recovery disk:

1. Run as administrator one of the following:
   - for 32 bit OS — **\Tools\SecurityCode\SnRescue\SnRescue32.exe**;
   - for 64 bit OS — **\Tools\SecurityCode\SnRescue\SnRescue.exe**.

   The Secret Net Studio emergency disk creation wizard dialog box appears as follows.



2. Choose one of the following options:
   - **select a USB/CD/DVD drive:** — select a drive which will be an emergency recovery disk;
   - **save the recovery disk image:** — specify the path to save the emergency recovery disk image.
3. Specify the target and subsystem for which you want to create an emergency recovery disk. To do so, select one of the following values in the drop-down list Create a recovery disk for:
   - **for MBR systems (Disk Protection only)** — the disk will be created to restore access to a disk protected by the Secret Net Studio disk protection mechanism;
   - **for UEFI systems (without the recovery file)** — the disk will be created to restore Secret Net Studio bootloader;
   - **for UEFI systems** — the disk will be created to restore the configuration of a disk encrypted with Secret Net Studio Full Disk Encryption mechanism.
4. If necessary, specify the path to a recovery file which must be added to the emergency recovery disk.
5. Click **Create disk**.

   A dialog box showing the disk creation process appears. After the process has finished, a message showing the path to the disk image will appear.
6. Click **Finish**.

Change the password for disks

You can use this command to change the password for disks, encrypted using Secret Net Studio Full Disk Encryption mechanism.

To change the password:

1. Start the computer with an encrypted disk using the emergency recovery disk.

   The main menu of Secret Net Studio emergency recovery disk appears (see Fig.7 on p. 289).
2. Enter the number of the command **Password change** and press **Enter**.

   You are prompted to enter the password to access disks.

3. Enter the password and press **Enter**.

   Note. To show the password characters, press **F5**.

   A request to set a new password appears.
4. Enter the new password and press **Enter**.

   Note. To show the password characters, press **F5**.

   A message about the successful password change appears.
5. Press any key to return to the main menu of the emergency recovery disk.

Reset the password for disks

You can use this command to reset the password for disks, encrypted using Secret Net Studio Full Disk Encryption mechanism. To reset the password, you need an emergency recovery disk.

Note. You can save the recovery code:
- in case of local storage of recovery data, in the Secret Net Studio encryption wizard on a computer with encrypted disks (see p. 167);
- in case of centralized storage of recovery data, in the Control Center on a Security Server for a computer with encrypted disks (see p. 169).

To reset the password:

1. Start the computer with an encrypted disk using the emergency recovery disk.

   The main menu of Secret Net Studio emergency recovery disk appears (see Fig.7 on p. 289).
2. Enter the number of the command **Password reset with recovery-code** and press **Enter**.

   The identifier of an encrypted disk and the request for the recovery code appear.
3. Enter the recovery code corresponding to the identifier and press **Enter**.

   You are prompted to enter the recovery code.
4. Enter the password for the recovery code and press **Enter**.

   Note. To hide the password characters, press **F5**.

   If you entered the valid password, you are prompted to set a new password for the encrypted disks.
5. Enter the new password and press **Enter**.

   Note. To show the password characters, press **F5**.

   The password to access encrypted disks will be changed.
6. Press any key to return to the main menu of the emergency recovery disk.

Disk protection removal and data decryption

The purpose of the command is to remove protection of a disk protected by Secret Net Studio disk protection mechanism, as well as to decrypt data on disks encrypted with Secret Net Studio Full Disk Encryption mechanism.

To remove disk protection and decrypt data:

1. Using an emergency recovery disk, boot the computer with the disk you want to decrypt or remove protection from.

   The main menu of Secret Net Studio emergency recovery disk appears (see Fig.7 on p. 289).
2. Enter the number of the command **Volume decryption** and press **Enter**.

   A list of protected/ encrypted disks appears.
3. Enter the number of the required disk.

   You are prompted to enter the password for the disk.

4. Enter the password and press **Enter**.

Note. To show the password characters, press **F5**.

If you entered the valid password, the process of removing disk protection or decrypting data begins.

Note. To abort the process, press **ESC**. A list of protected/ encrypted disks appears. If you select the disk for which the operation was started, the process resumes.
If the disk is left partially protected/ encrypted, it will be entirely protected/ encrypted after the logon.

The respective message will appear once the process has finished.

Note. If there are several protected/ encrypted disks and protection was removed not from all the disks (or not all the disks were decrypted) using the emergency recovery disks, a request to save a new recovery file appears after the logon.

Restore Secret Net Studio bootloader

If you have issues with the computer boot, you can delete and restore Secret Net Studio bootloader using the emergency recovery disk. The following two ways to do so are available:

- restore only Secret Net Studio bootloader;
- restore Secret Net Studio bootloader and overwrite Windows OS bootloader.

Attention! After deleting Secret Net Studio bootloader, restore it. If, after the restoration, OS boot errors occur, restore Secret Net Studio bootloader and overwrite Windows OS bootloader.

To delete Secret Net Studio bootloader:

1. Using an emergency recovery disk, boot the computer on which you want to restore Secret Net Studio bootloader.

   The main menu of Secret Net Studio emergency recovery disk appears (see Fig.7 on p. **289**).
2. Enter the number of the command **Bootloader remove** and press **Enter**.

   A request to confirm the operation appears.
3. Enter y and press **Enter**.

   Information about Secret Net Studio bootloader removal and the files to be deleted is displayed. Next, a message about the successful bootloader deletion appears.
4. Press any key to return to the main menu of the emergency recovery disk.

To restore Secret Net Studio bootloader:

1. Using an emergency recovery disk, boot the computer on which you want to restore Secret Net Studio bootloader.

   The main menu of Secret Net Studio emergency recovery disk appears (see Fig.7 on p. **289**).
2. Enter the number of the command **Bootloader recovery** and press **Enter**.

   A request to confirm the operation appears.
3. Enter **y** and press **Enter**.

   A message about the successful Secret Net Studio bootloader restoration appears.
4. Press any key to return to the main menu of the emergency recovery disk.

To restore Secret Net Studio and overwrite Windows OS bootloader:

1. Using an emergency recovery disk, boot the computer on which you want to restore Secret Net Studio bootloader.

   The main menu of Secret Net Studio emergency recovery disk appears (see Fig.7 on p. **289**).
2. Enter the number of the command **Advanced settings** and press **Enter**.

The advanced setting menu appears. Fig.8 on p. **289**).

3. Enter the number of the command **Bootloader recovery with windows-loader overwrite** and press **Enter**.

   A request to confirm the operation appears.

4. Enter y and press **Enter**.

   A message about the successful bootloader restoration appears.

5. Press any key to return to the advanced settings menu of the emergency recovery disk.

Restore configuration of security subsystems

You can use this command to restore the configuration file of Secret Net Studio Full Disk Encryption and Disk Protection subsystems. The configuration file on the computer is substituted with the one on an emergency recovery disk. A backup copy of the configuration file on the computer is saved.

Attention! Using an emergency recovery file with an invalid recovery file may lead to a loss of data kept on encrypted/ protected disks.
To avoid this, we recommend you to use a recovery file saved after encryption of all required disks.

To restore the configuration of security subsystems:

1. Using an emergency recovery disk, boot the computer on which you want to restore the configuration of security subsystems.

   The main menu of Secret Net Studio emergency recovery disk appears (see Fig.7 on p. **289**).

2. Enter the number of the command **Advanced settings** and press **Enter**.

   The advanced settings menu appears (see Fig.8 on p. **289**).

3. Enter the number of the command **Configuration recovery** and press **Enter**.

   A recovery file will be searched for on the emergency recovery disk.

   Note. If a recovery file was not found, repeat the procedure of emergency recovery disk creation with the option to write a recovery file onto it(see p. **289**).

   If the file was found, you are asked to overwrite the configuration file.

4. Enter **y** and press **Enter**.

   The configuration file will be overwritten. A message showing the path to save a backup copy of the previous configuration file appears.

5. Press any key to return to the advanced settings menu of the emergency recovery disk.

Delete configuration of security subsystems

You can use this command to delete the configuration file of Secret Net Studio Full Disk Encryption and Disk Protection subsystems. As a result of this operation and after computer restart, an empty configuration file is created unless Secret Net Studio bootloader is deleted. A backup copy of the configuration file on the computer is saved.

Attention! This command may lead to loosing access to data on encrypted/ protected disks. In this case, to restore access, you need a valid recovery file and use the respective command (see p. **293**). We strongly recommend you to apply this command only if the configuration file is corrupted.

To delete the configuration of security subsystems:

1. Using an emergency recovery disk, boot the computer on which you want to restore the configuration of security subsystems.

   The main menu of Secret Net Studio emergency recovery disk appears (see Fig.7 on p. **289**).

2. Enter the number of the command **Advanced settings** and press **Enter**.

   The advanced settings menu appears (see Fig.8 on p. **289**).

3. Enter the number of the command **Configuration remove** and press **Enter**.

   A request to confirm the operation appears.

4. Enter **y** and press **Enter**.

   The configuration file will be deleted. A message showing the path to save a backup copy of the configuration file appears.

5. Press any key to return to the advanced settings menu of the emergency recovery disk.

Remove an encrypted disk form configuration

If one of encrypted non-system partitions on a hard drive with several encrypted partitions is damaged, information about the damaged partition can be removed from the configuration. In this case, only encrypted data on the damaged partition will be lost. Data on other partitions will be available.

Note. You can use this command in the following cases:

- A hard drive with encrypted partitions was installed in another computer; the encrypted partition was formatted and new data were written on it. To save the new data and the data on other encrypted partitions, you can use this command on the computer where the partitions were encrypted. A formatted partition will no longer be considered encrypted.
- The configuration of the Full Disk Encryption subsystem is damaged. If you know for which encrypted partition the configuration file is damaged, you can use this command to save data on other encrypted partitions.
- The configuration of an encrypted partition was changed (the size was changed, a partition was deleted and so on). To save data on other encrypted partitions, you can use this command.

To remove an encrypted disk from the configuration:

1. Using an emergency recovery disk, boot the computer on which you want to restore the configuration of security subsystems.

   The main menu of Secret Net Studio emergency recovery disk appears (see Fig.7 on p. **289**).

2. Enter the number of the command **Advanced settings** and press **Enter**.

   The advanced settings menu appears (see Fig.8 on p. **289**).

3. Enter the number of the command **Remove encrypted volume** from configuration and press **Enter**.

   A list of encrypted disks appears.

4. Enter the number of the required disk.

   A request to confirm the operation appears.

5. Enter **y** and press **Enter**.

   Information about the selected encrypted partition will be removed from the configuration of the Full Disk Encryption subsystem.

6. Press any key to return to the advanced settings menu of the emergency recovery disk.

Recommendations for setting up Secret Net Studio in 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 security 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.

Restoring the security 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 [**1**]). 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, it takes 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.

TE operation errors

Local Control Center errors

The **State** parameter on the **Trusted Environment** subsystem information window (see Fig.1 on p. **247**), shows whether the computer meets the system requirements to install TE or not.

If the computer does not meet any requirement, the **State** parameter is set to one of the values in the table below.

Error message
The operating system version is lower than required
Number of processors is lower than required
Virtualization support is disabled
Second Level Address Translation is not supported by the hardware
The type of disk used (NVMe, VHD, etc.) is not supported
Working in the virtual environment is not supported
Incompatible hardware detected

Errors on computer startup

If you start the computer, while TE is operating in hard mode, a BSOD system error may occur. Such error may be caused by a computer attack or other information security breach. If you cannot deal with the problem by yourself, contact the Security Code technical support.

You can find the codes of BSOD system errors related to TE and their brief descriptions in the table below.

Error code	Description
0x5ECC0DE0	Client process integrity violated
0x5ECC0DE1	Error while initializing TE driver
0x5ECC0DE2	SMEP register reset
0x5ECC0DE3	Driver checksum error
0x5ECC0DE4	Driver modification attempt
0x5ECC0DE5	Driver unloaded
0x5ECC0DE6	Unauthorized process termination
0x5ECC0DE7	Watchdog is triggered for process
0x5ECC0DE8	Process checksum error
0x5ECC0DE9	Ring-0 attack
0x5ECC0DEA	TE driver internal error

Default TE IC objects

When TE starts, Secret Net Studio drivers, services and applications are placed under control. You can find the list of those files in the table below.

Full file name	File type
SystemRoot\System32\Drivers\Sn5CrPack.sys	Driver
SystemRoot\System32\Drivers\Sn5Crypto.sys	Driver
SystemRoot\System32\Drivers\SnCC0.sys	Driver
SystemRoot\System32\Drivers\SnCDFilter.sys	Driver
System-Root\System32\Drivers\SnCloneVault.sys	Driver
SystemRoot\System32\Drivers\SnDacs.sys	Driver
SystemRoot\System32\Drivers\SnDDD.sys	Driver
System-Root\System32\Drivers\SnDeviceFilter.sys	Driver
SystemRoot\System32\Drivers\SnDiskEnc.sys	Driver
SystemRoot\System32\Drivers\SnDiskFilter.sys	Driver
SystemRoot\System32\Drivers\SnEraser.sys	Driver
SystemRoot\System32\Drivers\SnExeQuota.sys	Driver
SystemRoot\System32\Drivers\SnFDac.sys	Driver
System-Root\System32\Drivers\SnFileControl.sys	Driver
SystemRoot\System32\Drivers\SnFMac.sys	Driver
SystemRoot\System32\Drivers\SnNetFlt.sys	Driver
SystemRoot\System32\Drivers\snsdp.sys	Driver
System-Root\System32\Drivers\SnTmCardDrv.sys	Driver
SystemRoot\System32\Drivers\SnWiper0.sys	Driver
SystemRoot\System32\Drivers\ScTeDrv.sys	Driver
SystemRoot\System32\Drivers\SCTEFsFlt.sys	Driver
%ClientInstallDir%\SnSrv.exe	Service
%ClientInstallDir%\SnicheckSrv.exe	Service
%ClientInstallDir%\SnIcon.exe	Application

Restrictions and recommendations when working with TE

TE is a new Secret Net Studio security mechanism that is currently in active development. Current section contains restrictions and recommendations for using the current TE version (Secret Net Studio version 8.7).

Incompatible hardware and configuration

Below you can see TE operation peculiarities that occur when you use TE with specific hardware. The peculiarities are relevant even if the computer corresponds to the minimal system requirements specified on p. **245**.

1. Virtual environment.

TE functions only if a single hypervisor is active. The virtual environment is not supported. To use TE, you need a physical computer.

Note. The current restriction is checked by the Client. If the configuration does not correspond to the requirements, TE is impossible to enable.

2. Hard drives.

- Current TE version operates only with SATA/AHCI hard drives.

Working with SCSI, NVMe hard drives and with VHD1 (and other types) drive images is not supported.

Note. The current restriction is checked by the Client. If the configuration does not correspond to the requirements, TE is impossible to enable.

- We recommend you to use the hard drive in AHCI mode. Operation in IDE mode is unstable.
- The current version does not support RAID configuration and full-disk encryption.
- We do not recommend you to use TE on a configuration with several OS's, because the current TE version does not support loading the specific OS where TE is installed.

3. System boards.

Gigabyte H67A-UD3H-B3 with UEFI/BIOS version F81 is not supported due to its incorrect interaction with the drive controller.

Note. The current restriction is checked by the Client. If the configuration does not correspond to the requirements, TE is impossible to enable.

4. USB controllers.

- Unstable operation is observed with USB 3.1. Use USB 3.0/2.0 to connect TE boot drives.
- Connection of several USB drives is not supported. Before switching on the computer, connect only the boot drive.

5. CPUs.

TE is partially tested on AMD platform. Full mechanism functionality is not guaranteed.

Recommended computer configuration

For correct TE operation, we recommend you to configure the computer in the following ways.

1. UEFI/BIOS.

- We recommend you to update UEFI/BIOS to the latest version.
- In UEFI/BIOS Setup, you must enable all virtualization functions. Virtualization options are usually located in the **CPU configuration** section.
- In UEFI/BIOS Setup you must allow CSM (Compatibility Support Module) use. In CSM settings, we recommend to select the **UEFI and Legacy** mode.

Note. If the CSM settings do not contain the **UEFI and Legacy** mode, select the **Legacy** mode.

- In UEFI/BIOS Setup, in USB settings we recommend you to activate **Full Initialization** and **USB boot first** (if these options exist).

2. Hard drive.

- We do not recommend you to use a hard drive with S.M.A.R.T. errors, because operation with such drives is unstable.
- TE does not support the use of drives with enabled hardware encryption.

Note. If the hard drive supports hardware encryption, disable the function first. After that, TE works with that drive as if it does not support hardware encryption.

3. Windows OS.

Windows sleep mode causes unstable operation. We recommend you to set the following configuration via **powercfg.cpl**:

- disable sleep mode;
- set all CPU modes to 100%;
- deny the system hard drive disconnection.

Formatting the TE boot drive

To use the full capacity of a USB flash drive, that was previously used as a TE boot drive, you need to format the USB flash drive using the standard Windows Disk Management *diskpart.exe* tool.

Attention! All data on the USB flash drive will be wiped. To use the USB flash drive as a TE boot drive, perform the procedure of creating a TE boot drive (see p. 246).

To format the TE boot drive:

1. Connect the TE boot drive to the computer.
2. Run the tool via the Windows OS command line as an administrator.
3. Run the following command:

   ```
   diskpart
   ```

   The tool *diskpart.exe* launches.
4. Run the following command:

   ```
   list disk
   ```

   The list of drives connected to the computer appears.
5. In the list, find the necessary USB flash drive and remember its number.
6. Run the following commands:

   ```
   select disk <drive number>
   clean
   create partition primary
   ```

   The USB flash drive will be formatted. A primary partition will be created on the drive.
7. Format the USB flash drive into the required file system in any convenient way.

Documentation

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