



SECURITY CODE

Secret Net Studio

Administrator's manual

Setup and operation. Local protection



© **SECURITY CODE Ltd., 2017. All rights reserved.**

All rights to the operating instructions are reserved.

This document is part of the product package, and it is covered by all terms and conditions of the license agreement. This document or any part of it in printed or electronic form cannot be copied or made available to third parties for commercial purposes without express written consent of the SECURITY CODE Ltd.

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

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

Table of contents

List of abbreviations	6
Introduction	7
Local protection	7
Device control settings	8
About device control	8
Device list	8
Inheritance rules for parameters in the device list	9
Management options	9
Specific features of group policy application with device lists	10
Default device parameters	10
General configuration procedure for using only permitted devices	11
Device list management	11
Loading a device list	11
Creating a device list in a group policy	12
Adding and removing device list elements	13
Control of device connections and changes	14
Configuring a device control policy	14
Confirming hardware configuration	15
Selective discretionary access control	15
Configuring access rights for devices	15
Configuring event logging and audit of device operations	16
Shadow copying setup for output data	17
Managing shadow copying for devices	17
Selecting devices for shadow copying	17
Printer control settings	18
About restricting access to printers	18
Printer list	18
Management options	18
Initial printer use parameters	19
General configuration procedure for printing only on permitted printers	19
Printer list management	19
Loading a printer list	19
Creating a printer list in a group policy	20
Adding and removing elements	20
Selective printer access control	21
Configuring user print permissions	21
Configuring event registration	21
Configuring shadow copying for output data	22
Managing the shadow copying function for printers	22
Selecting printers for shadow copying	22
Configuring printed document marking	22
Marking mode management	23
Marker editing program	26
Application execution control settings	30
Setup methods and tools overview	30
Data Model	30
Default model objects	31
IC-AEC Management Program	31
Synchronizing central and local databases	32
Initial setup of IC mechanisms	33
Preparing to build a data model	33
General configuration procedure	34
Building a new data model	34
Adding tasks to a data model	35
Adding jobs and including tasks to them	36
Enabling AEC soft mode operation and task creation by log	38

Configuring links between actors and AEC jobs	40
Preparing resources for application execution control	40
Enabling and configuring process isolation	41
Calculating reference values	43
Granting privileges when working with AEC	46
Enabling AEC hard mode	46
Saving and loading a data model	47
Saving	47
Change notifications	48
Configuring automatic synchronization start	48
Forced start of full synchronization	50
Downloading and recovering a data model	51
Export	51
Import	52
Making changes in the data model	55
Changing object parameters	55
Adding objects	57
Deleting objects	66
Links between objects	67
Disable local jobs	67
Searching for dependent modules	68
Replacing environment variables	68
Mandatory access control settings	70
About mandatory access control	70
Confidentiality categories of resources	70
Access levels and user privileges	71
Flow control mode	71
Configuring mandatory access control	72
General configuration procedure	72
Configuring confidentiality categories	73
Assigning access levels and privileges to users	74
Assigning confidentiality categories to resources	74
Event registration setup	75
Configuring the use of printers	75
Additional configuration of the flow control mode	76
Recommended configuration procedure	76
Setup program for the flow control mode	76
Selecting confidentiality levels for network interfaces	77
Enabling and disabling the flow control mode	78
Configuring joint operation with applications	78
Confidential resource handling rules	81
Stored data security settings	84
Discretionary access control for folders and files	84
Granting privileges to modify rights to access resources	84
Assigning the resource administrator	84
Configuring event logging and audit of resource operations	84
Overwriting deleted information	85
Protecting local disks	85
Enabling disk protection	85
Enabling and disabling logical partition protection	88
Disabling disk protection	88
Data encryption in encrypted containers	89
Granting privileges to create encrypted file containers	89
Event registration setup	89
Managing encryption user keys	89
Terminal session security settings	92
Using identifiers in terminal sessions	92
Disabling pre-authentication	92
Software methods for identifier processing	93
Restricting the use of local devices and resources	93

Clipboard redirection control	94
Redirection control for local devices of the terminal client	94
Printer redirection control	95
Protection of confidential information during terminal sessions	95
Appendix	97
List of groups and classes for device control	97
Examples of configuring removable disk use	98
Local assignment of removable disks to users	98
Centralized creation of a list of removable drives	99
Backing up the IC-AEC database using the command line	100
The flow control mode configuration program	101
Automatic setup	101
Manual setup	102
Emergency disabling of local disk protection	111
Using the emergency recovery wizard	111
Using a boot disk for emergency recovery	111
Documentation	113

List of abbreviations

AD	Active Directory
BIOS	Basic Input/Output System
FAT	File Allocation Table
GPT	GUID Partition Table
IEEE	Institute of Electrical and Electronics Engineers
LFN	Long File Name
MBR	Master Boot Record
MMC	Microsoft Management Console
NTFS	New Technology File System
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
PKI	Public Key Infrastructure
ReFS	Resilient File System
RPC	Remote Procedure Call
RTF	Rich Text Format
TCP	Transmission Control Protocol
USB	Universal Serial Bus
DB	Database
AEC	Application Execution Control
IC	Integrity Control
LDB	Local Database
DM	Data Model
OS	Operating System
CDB	Central Database

Introduction

This manual is designed for Secret Net Studio administrators (hereinafter "Secret Net Studio, the System"). It contains information for administrators about the configuration and management of the following protection mechanisms:

- discretionary access control;
- control over device connections and changes;
- application execution control;
- mandatory access control;
- printer control;
- protection of information on local disks;
- data encryption in encrypted containers;
- overwriting deleted information.

Before reading this manual, read the following documents: [1], [3].

Conventions

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

Internal links usually indicate the required page number.

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



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



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



- This icon highlights a warning.

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

Other information sources

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

Local protection

The local protection group includes subsystems that use the following security mechanisms:

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

Chapter 1

Device control settings

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 devices — 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 connect the device 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. 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.

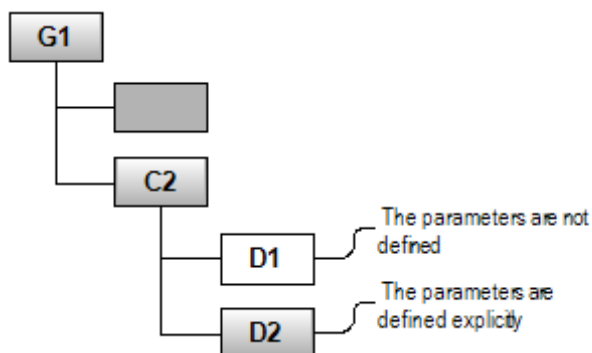
For a full list of groups and classes, see Appendix on p. [97](#).

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 documents [3], [4].

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

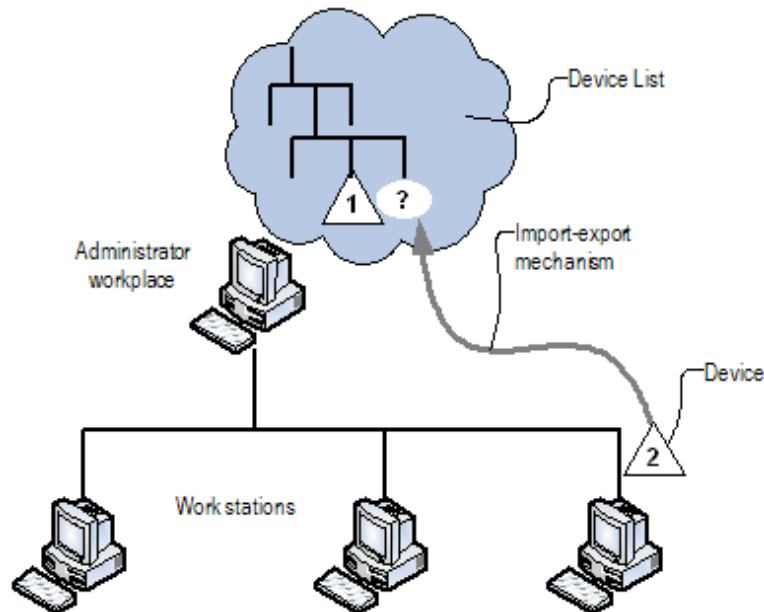
This option is preferable when you need to ensure general device control principles on protected computers and there is no need to configure individual devices in the centralized mode. The security administrator just has to configure usage parameters for device groups, classes and models in the required 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.

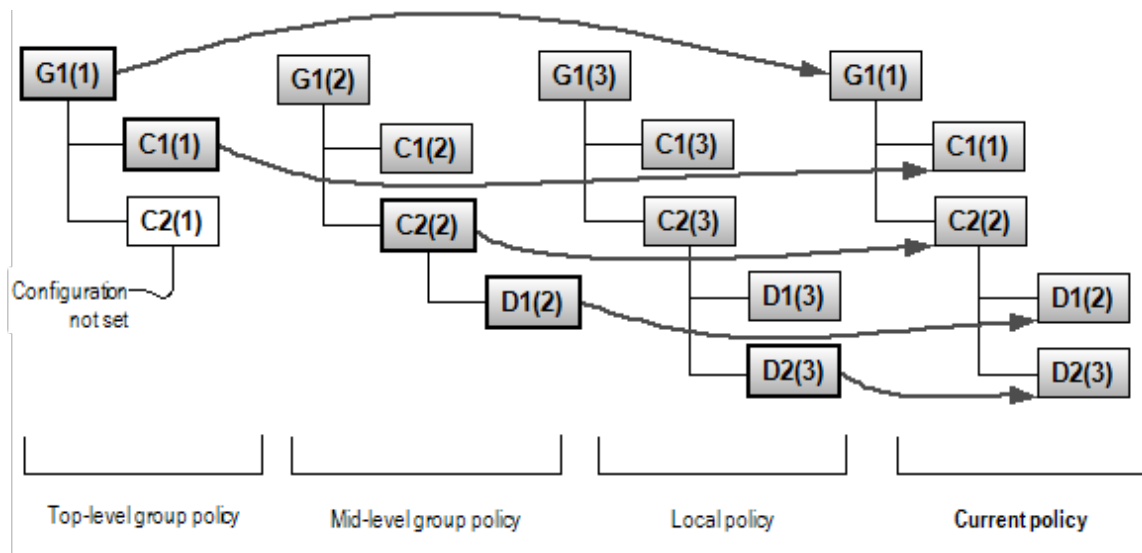
The devices that require configuring should be added to the group policy list. You can add information to the devices list policy about devices that are connected to a computer with the Client.

For the description of available options for adding devices, see p. 13



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 if only parameters are 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 applied to all users of the computer:

- The "Device is always connected to the computer" control mode is enabled for Local devices and Network groups. For other groups, the "Device connection is allowed" mode is enabled.
- For all detected hard drives as well as for removable and optical disks, the "Device is always connected to computer" control mode is enabled, with the additional "Lock computer if device is changed" parameter. 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.
- For devices supporting confidentiality category assignment, the "Device is available without regard to confidentiality categories" access mode is enabled.
- For network interfaces operation regardless of session confidentiality in the flow control mode (Mandatory Access Control) is enabled.
- 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 permitted devices

To ensure that only permitted devices can be connected to and used on a computer, perform the configuration in the following order:

1. After installing Secret Net Studio, connect all devices that will be used with the computer. These devices will be registered in the System with access permissions and control parameters inherited from higher elements of the list (models, classes, and groups).
2. Configure the device usage parameters for the current hardware configuration:
 - control policy (see p. 14);
 - user access control (see p. 15);
 - shadow copying (see p. 17);
 - mandatory restriction of user access (see p. 74 and p. 77).
3. To restrict the use of devices in terminal connections, disable redirection (see p. 94).
4. Disable parameter inheritance for certain devices from higher elements of the list and disable permissions for the respective models, classes, and groups (see p. 14). For example, you can disable permissions for the Secure Digital Devices group.

As a result, the user will only be able to connect and use permitted devices, while other devices will not be available for use. Later, you will have the option to remotely allow using new devices using the Control Center. For this purpose, when requested by a user, the security administrator suggests connecting the required device (for example, a USB flash drive) to the user's computer. Once the device is connected, even if it is not permitted to be used, information about it will appear in the list of local policy devices. To allow the usage of the device, you must open local policy settings and perform the required steps to allow its usage.



Note.

Specific instructions for configuring the use of removable drives can be found in the Appendix on p. 98.

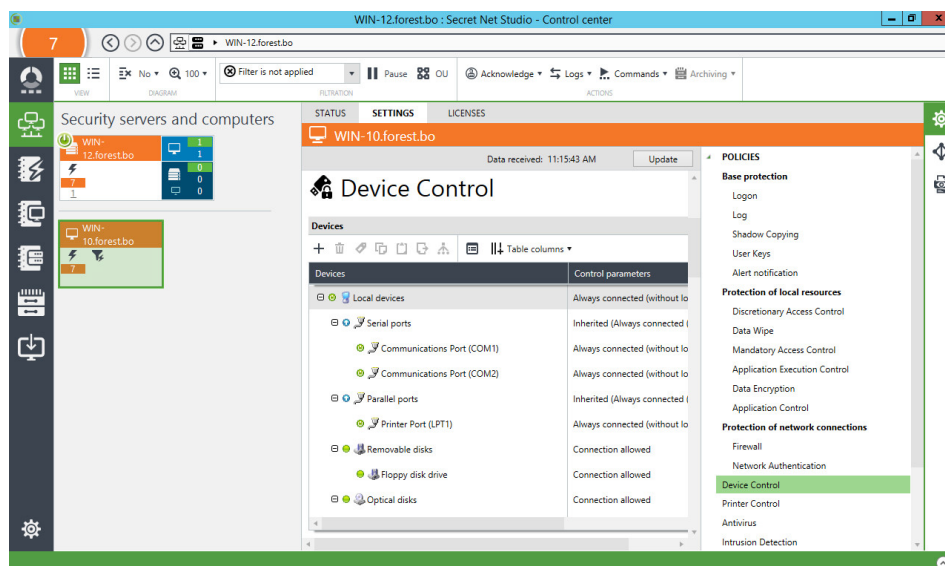
Device list management

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".
- In the Policies section, select the Device Control parameters 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, p. 94). 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.
	Control mode is disabled for the device
	Control mode is enabled for the device and the device should always remain connected to the computer
	Control mode is enabled for the device and the device can be connected to or disconnected from the computer
	Control mode is enabled for the device, and the device cannot be connected to the computer

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 [4]).

Adding and removing device list elements

Group policy device list makes it possible to add information about specific devices. In this way, you can configure device parameters in the centralized or local mode if the device is not connected to your computer earlier or, for some reason, is not listed.

You can add devices by:

- using the device import wizard;
- copying from the clipboard.



Attention!

When adding a device, its preset control and access parameters are copied. However, in some cases, the parameters may be assigned default values if previous values cannot be retrieved for technical reasons. Once you added a device, make sure to check its parameters and, if necessary, edit them.

Using the device import wizard

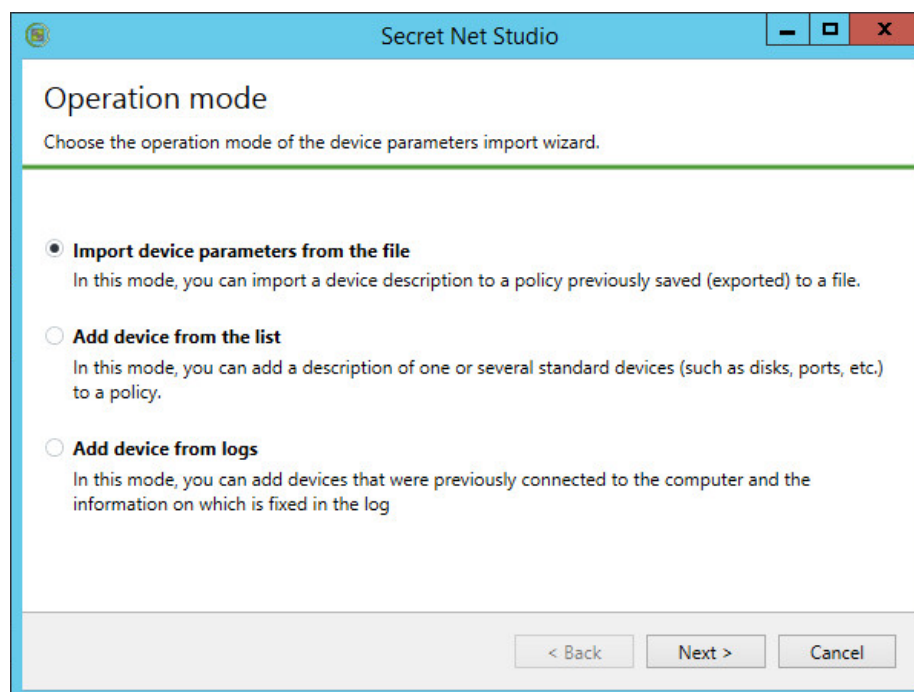
The import wizard provides the following options:

- importing a device from a file where information about the device is saved (exported);
- adding a standard device from a predefined list (for example, input/output port).

To add a device to the group policy list:

1. Right-click in any area of the list of group policy devices and click the "Add device" command.

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



2. Select an option, click the Next> button and follow the wizard's instructions.

Exporting information 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 only supported for devices and models.

To export information:

1. Right-click the required device or model and click the Export command.

A dialog box appears.

- Specify the name of the file for saving the information.

Using the clipboard for adding devices

Device information can be copied to the clipboard from the device list from another policy.

The methods for using the clipboard for device copying and adding to the group policy list are standard Windows methods.

Removing devices

If you need to remove a device from the group policy list, right-click the device and click the Remove command.

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 those computers where the Client is installed in the network operation mode, you can configure a device control policy in the group policies (see p. 12).

To configure a device control policy:

- Load the device list (see p. 11).
- Select the list line with the required element (group, class, model or device).
- If necessary, enter additional information about the element in the cell of the Commentary column. To do this, click the button in the right part of the cell.

Note.

By default, the Commentary column is not displayed. Click the Table columns button 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.

- Specify the required parameters in the cell of the Control parameters column. To do this, 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.

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 [4].

Selective discretionary access control

The following operations are performed when configuring control of user access to devices:

1. Configuring user access rights for devices.
2. Configuring event logging and audit of device operations.

Configuring access rights for devices

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

To configure access rights for devices:

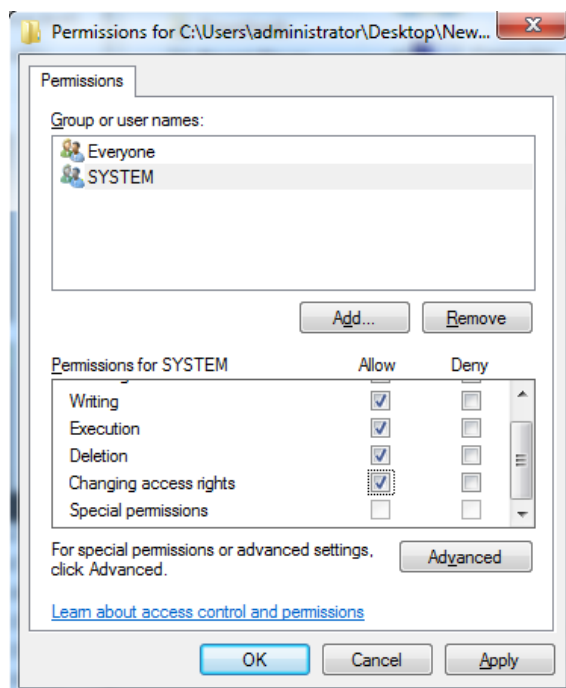
1. Load the device list (see p. 11).
2. Select the line with the required list element (class or device).
3. Click the button in the cell of the Permissions column.



Devices	Control parameters	Access pa
Secure Digital	Connection allowed	Permissions but c
Memory cards	Inherited (Connection allowed)	<input type="checkbox"/> Inherited

The "Permissions..." dialog box appears.

Note that the "Permissions..." dialog box can only be opened for those 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 the Advanced button and configure parameters in the dialog box.

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. 11), 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. 11).
2. Select the line with the required list element (class or device).
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.

Shadow copying setup for output data

Managing shadow copying for devices

You can disable the shadow copying function for all devices connected to your system as disks. If the shadow copying function is enabled, parameters defined for devices will apply.

For general management of the shadow copying function:

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.
3. Select the required value for the Shadow Copying function:
 - Disabled for all devices — no shadow copying when writing data to the devices;
 - Defined by device settings — shadow copying is performed for devices with shadow copying mode enabled.
4. Click Apply.

Selecting devices for shadow copying

Shadow copying is available for the following types of devices:

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

Copy saving mode can be enabled for the devices listed above and classes these devices belong to.

To manage the copy save mode in the device list:

1. Load the device list (see p. 11).
2. Select the required list line (class or device).
3. Select or clear the check box in the "Shadow Copying" column:
 - select it to enable the copy saving mode;
 - clear it to disable the mode.

Devices	Control parameters	Shadow copying	Access p
Secure Digital	Connection allowed	<input type="checkbox"/>	
Memory cards	Inherited (Connection allowed)	<input checked="" type="checkbox"/> Inherited	

4. Click Apply.

Chapter 2

Printer control settings

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 installation of 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 where the Client is 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 documents [3], [4].

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 stand-alone 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 a printer's parameters, 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. 20 for a description of available options for adding printers.

Initial printer use parameters

A freshly installed 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 permitted printers

To ensure that documents are printed on the printers permitted 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 System.

2. Add these printers to the group policy list.
3. Configure the parameters for using printers:
 - user access control (see p. 21);
 - shadow copying (see p. 22);
 - mandatory access control (see p. 75).
4. To restrict the use of printers in terminal connections, disable redirection (see p. 95).
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 permitted 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 himself/herself, add it to the required policy list and configure its usage parameters.

Printer list management

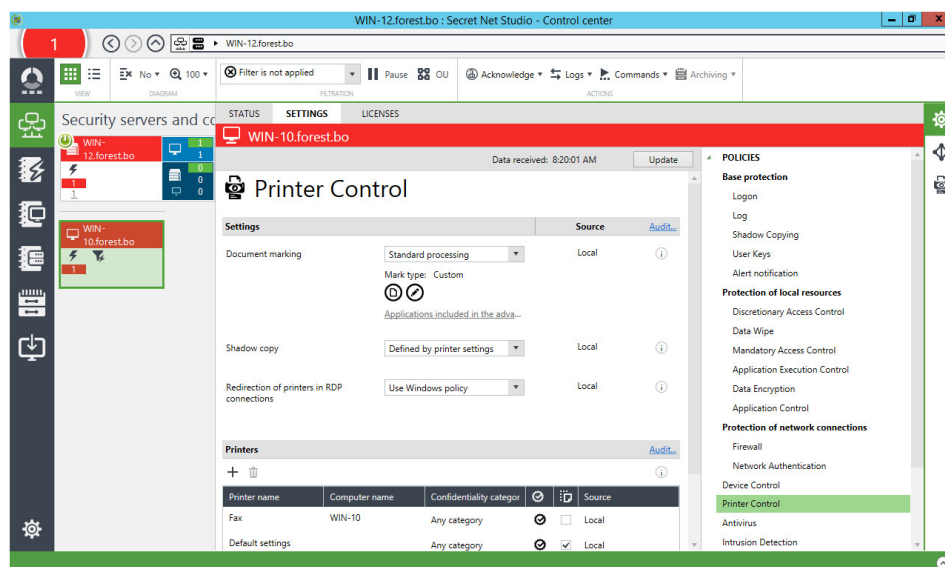
Loading a printer list

The procedure for loading a printer list when working with the Control Center in the centralized mode is described below. Printers are loaded locally in the same way as when using the Control Center in the local mode. See information about how to use the Control Center in the document [4].

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 Printer 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 [4]).

Adding and removing elements

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

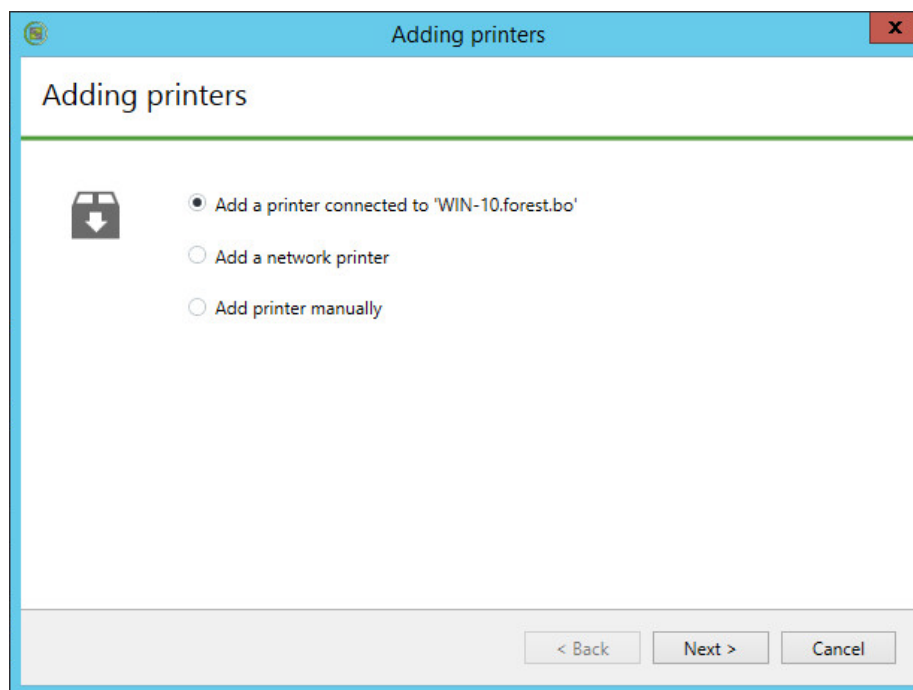
Using the adding wizard

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



2. Select a desired option, then click the Next> button and follow the wizard's instructions.

Removing printers

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

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. 18).
2. Select the required element in the list.
3. Click the cell of the Permissions column.



Printer name	Computer name	Confidentiality categories	Permissions	Source
Fax	WIN-10	Any category		Local
Default settings		Any category		Local

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 printer 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, Printer control group. To go to the required group of registration settings from the respective group of parameters in the Policies section (see p. 19), click the Audit link in the right part of the Settings or Printers group heading.

Configuring shadow copying for output data

Managing the shadow copying function for printers

The shadow copying function can be disabled for all printers. If the shadow copying function is enabled, parameters set for printers will be applied when printing documents.

The centralized configuration procedure when using is described below. Local configuration is performed the same way as in the local Control Center. See information about on how to use the Control Center in the document [4].

To manage the shadow copying function:

1. In the Control Center, open the Computers panel and select the object you want to configure. Right-click the object and click the Properties command. In the properties menu, select the Settings tab and download the settings from the Security Server.
2. In the Policies section, select the Printer Control / Settings parameters group.
3. Select the required value for the Shadow Copying function:
 - Disabled for all printers — no shadow copying when printing;
 - Defined by printer settings — shadow copying is performed for printers with shadow copying mode enabled.
4. Click Apply.

Selecting printers for shadow copying

You can control shadow copying for specific printers or for the Default Settings element in the printer list.

To manage shadow copying in the printer list:

1. Load the printer list (see p. 18).
2. Select the required element in the list.
3. Set the checkbox of the Shadow Copying column the way you need:
 - select it to enable copy save mode;
 - clear it to disable copy save mode.

Printer name	Computer name	Confidentiality categories	<input checked="" type="checkbox"/>	Source
Fax	WIN-10	Any category	<input checked="" type="checkbox"/>	Shadow copying
Default settings		Any category	<input checked="" type="checkbox"/>	Local

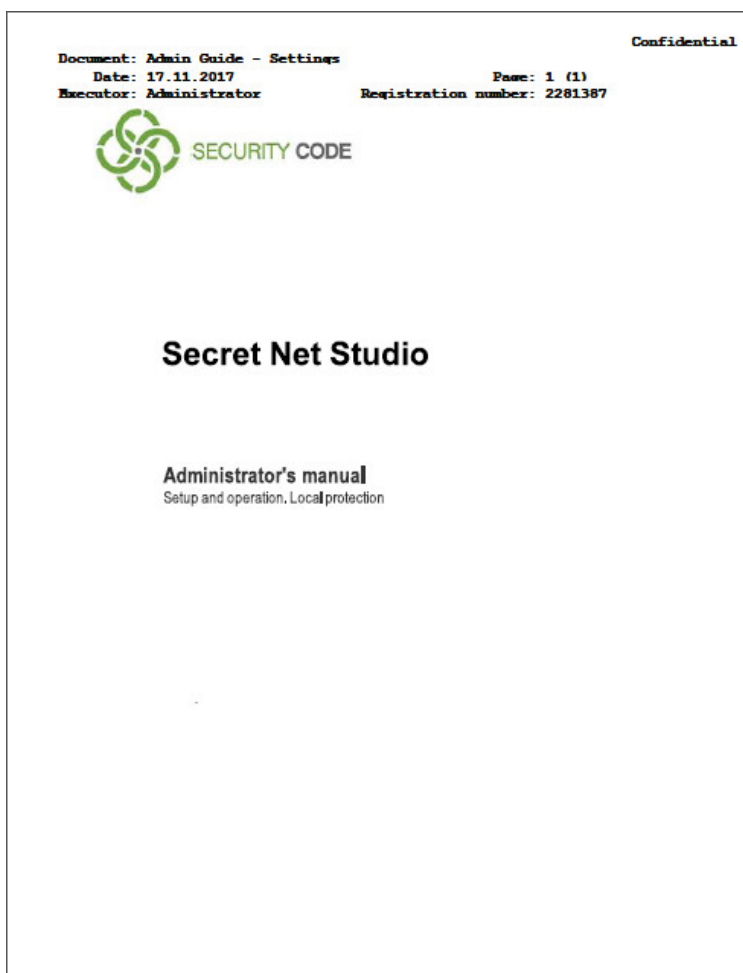
4. Click Apply.

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 System is configured to use 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 as in the local Control Center. See information about how to use the Control Center in the document [4].

To enable and configure 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 the Properties command. In the properties menu, select the Settings tab and click "Load Settings".
2. In the Policies section, select the Printer Control / Settings parameters group.

3. Select the required value for the Document marking function:

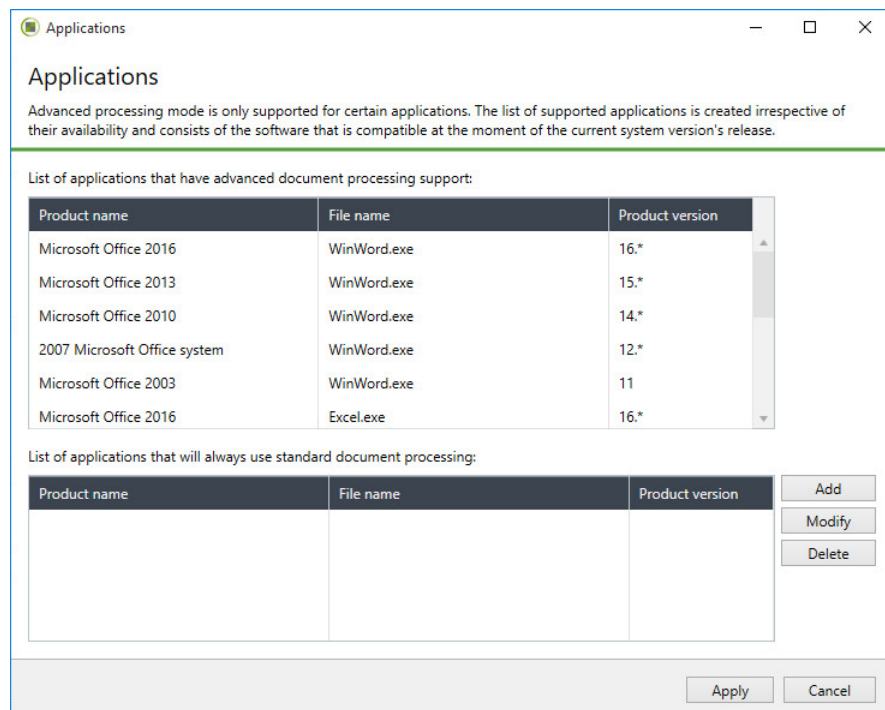
- Standard processing — this mode can be used in all supported applications. This mode is more suitable for printing whole documents. When printing a document fragment, the marker will only contain information about printed pages, without taking into account the total number of document pages (since 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 (see p. 22). 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. When the current value is Disabled for all printers, only Print document events are logged.

4. Configure the parameters for using markers: To do this, click Edit button and configure the parameters in the marker edit program window (for the description of the interface and the general procedures for using the program can be found here: p. 26). 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 this, use the Applications included in advanced processing link.

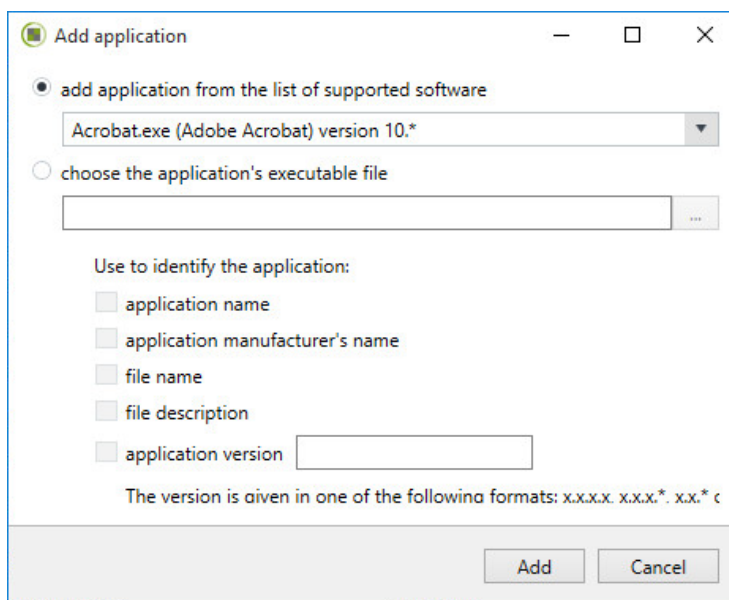
A dialog box with the list of applications appears.



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.



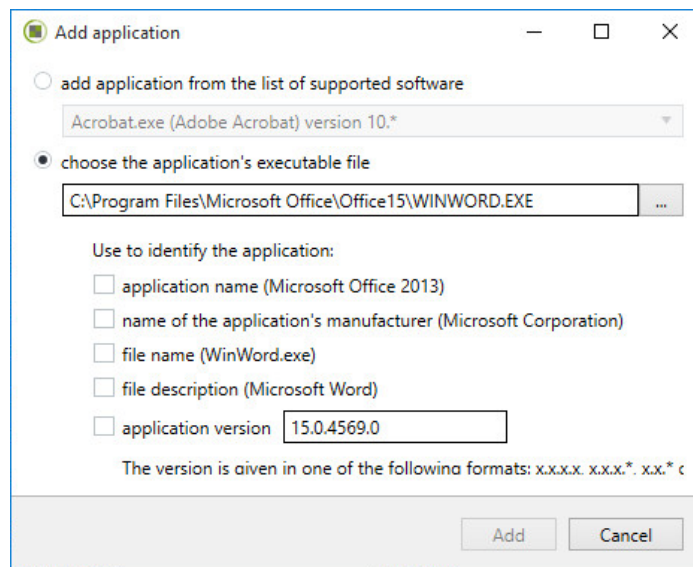
Select the required option in the dialog box and click Add. You can select one of the following options to add an application:

- 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:

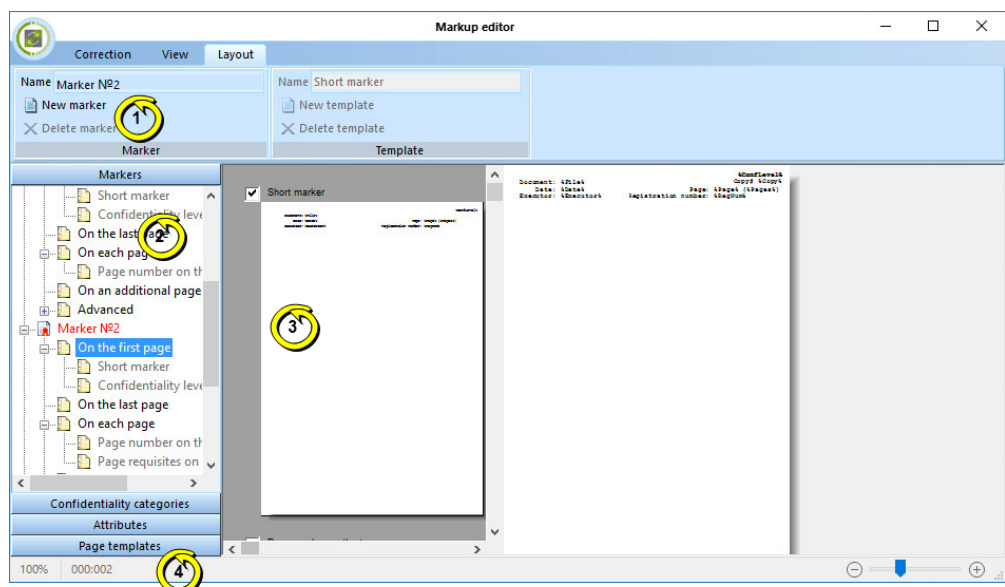
1. Complete steps 1–2 of the procedure described above.
2. Set the Document marking parameter to Disabled.
3. Click Apply.

Marker editing program

The marker editing program is designed for configuring the marking of printed documents. The program can be launched from in the dialog box for configuring the parameters of the Document marking group policy (see p. 23).

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, hover your cursor over any tab header and double-click it.

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 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.

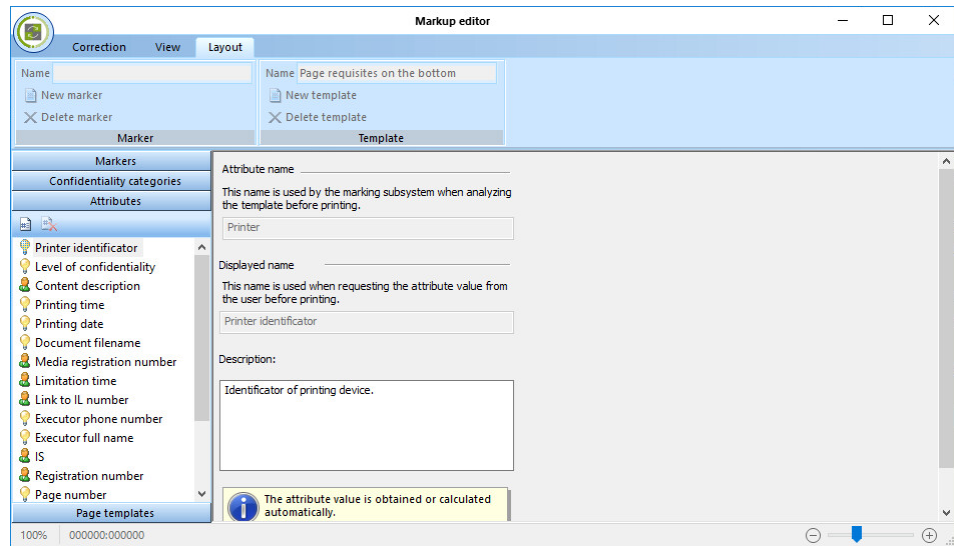
4 – Status bar

Contains scale and cursor position indicators that are used for working with page templates

Procedure for marker editing

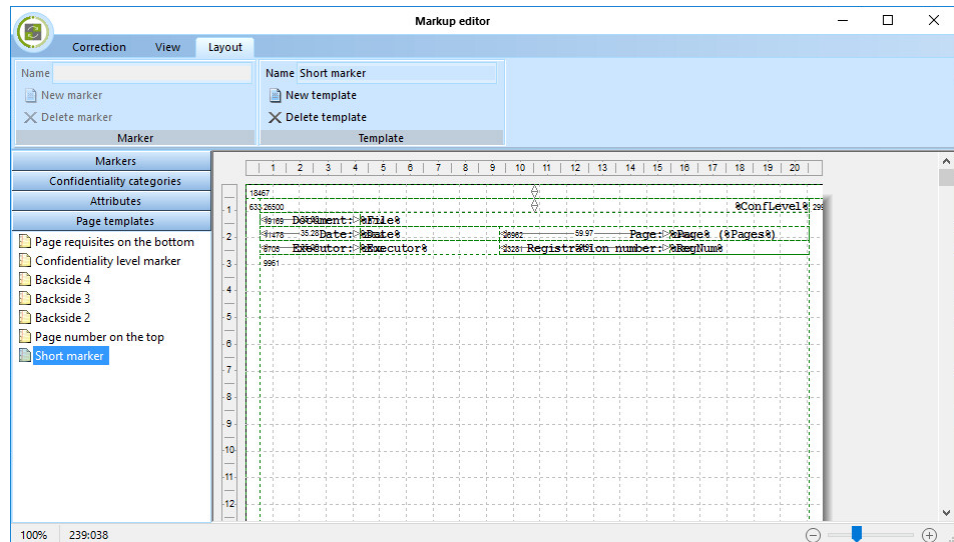
The following procedure is recommended for marker editing in the program:

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



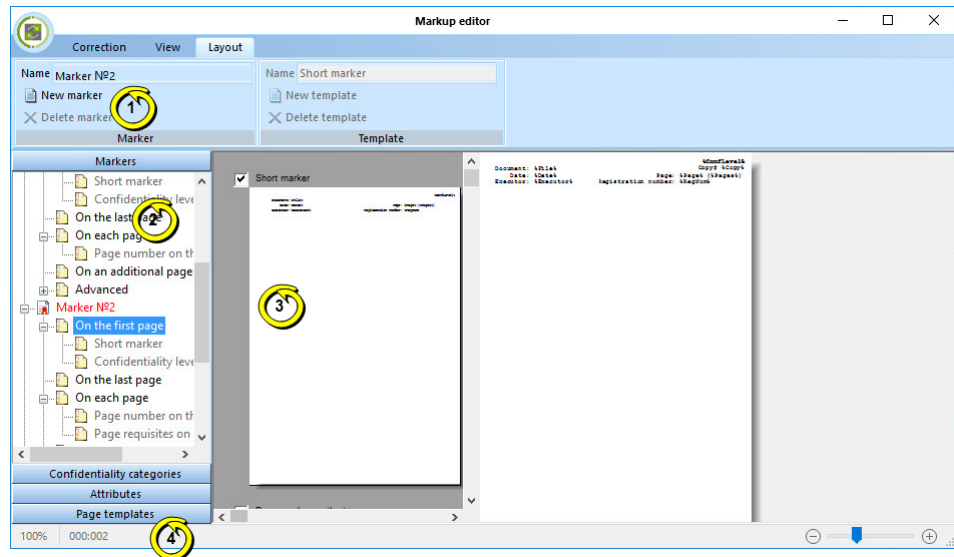
If the required attributes are not on the list, modify existing attributes or add new ones.

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



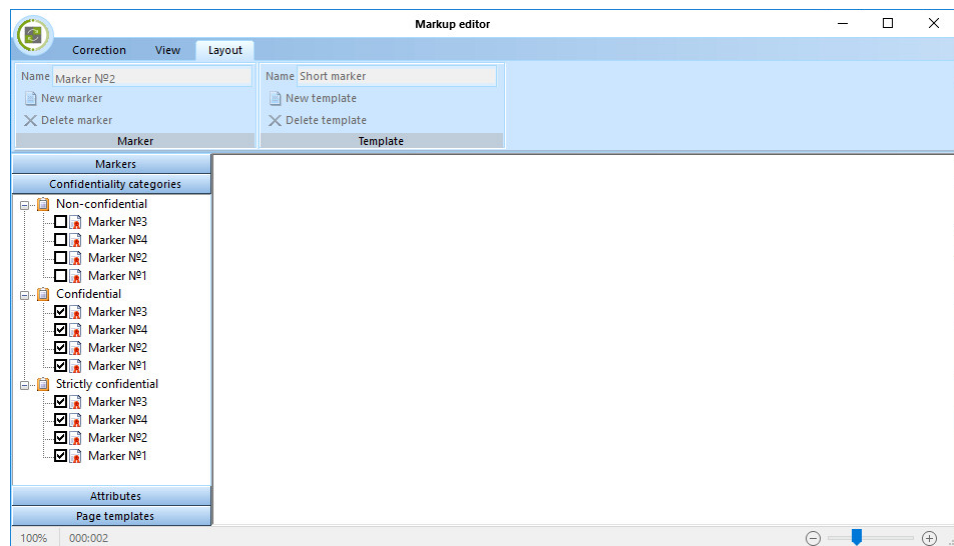
If the required templates (with the required layout and attribute set) are not on the list, modify existing templates or add new ones. Layout editing is performed using standard methods.

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 this, click the button that can be found in the upper-left corner of the window and click the Save marking description command.
6. Close the program.

Chapter 3

Application execution control settings

The Application Execution Control (AEC) mechanism is designed to restrict the use of software on a computer. Access is permitted only to those programs that are needed by the users for their work. A list of resources is defined for each user including programs, libraries and scenarios. Attempts at running other resources are blocked and logged as alerts.

AEC can be set up along with the configuration of the integrity control mechanism (IC). Applications and data control, a common configuration tool, is used for these mechanisms. This chapter covers the procedure for working with the program for implementing AEC, either separately or along with the IC. For the description of the IC mechanism, see document [3].

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 register). 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 register
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 permitted 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 who are permitted to run programs preset by tasks of the AEC

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

Comment.

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

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, using IC-AEC management, is imported to the IC-AEC database. 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 pre-programmed list. For these objects, links are established with the following actor:

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

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

IC-AEC Management Program

The Applications and data control program (hereinafter the IC-AEC Management Program), which is included in the Client, is used for setting up IC and AEC mechanisms. This chapter covers methods for working with the program to set up the AEC mechanism. A description of the interface can be found in the document [3].

The IC-AEC Management Program makes it possible to generate data model elements using automated and manual tools. Manual tools can be used at all levels of the model for generating and modifying objects and links. Automated tools are

preferable when working with many objects. However, this requires deeper control of the results. Manual tools can be used for generating small fragments of the model. In this case, the process is under control and devoid of random errors. We recommend you to combine these two methods.

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

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

To start the program in the local mode:

- Perform the actions corresponding to the version of the installed operating system:
 - on a computer running Windows 8 or Windows Server 2012 operating system, load the Start screen and click the "Applications and data control" element;
 - on a computer running other OS, click the Start button and click the "Applications and data control" command in the program menu.

To start the program in the centralized mode:

1. Perform the actions corresponding to the version of the installed operating system:
 - on a computer running Windows 8 or Windows Server 2012 operating system, load the Start screen and click the "Applications and data control (Centralized mode)" element;
 - on a computer running other OS, click the Start button and click the "Applications and data control (Centralized mode)" command in the program menu.

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

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

Synchronizing central and local databases

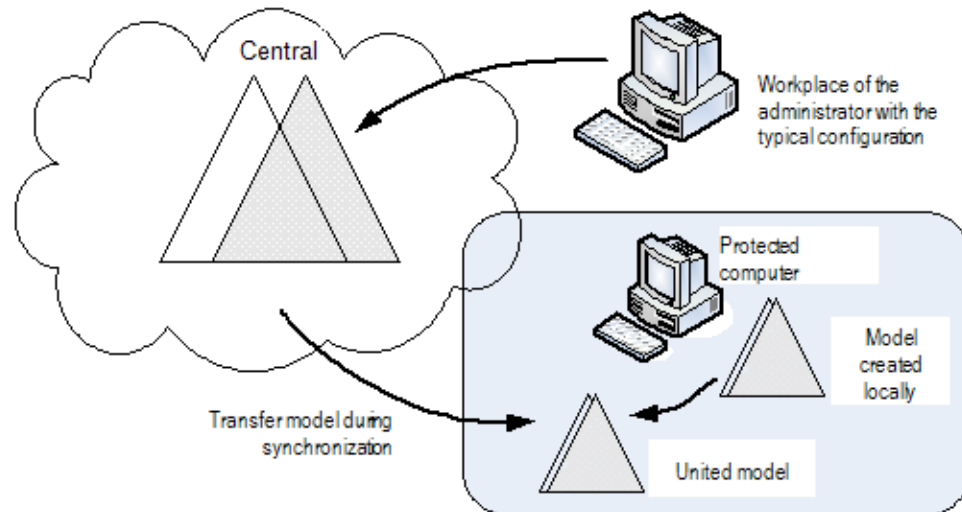
During synchronization, changes from the IC-AEC central database are transferred to all affected computers. The changes are saved in the IC-AEC local database. Synchronization may be performed:

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

Note.

To synchronize immediately after saving the data model in the central database, change notifications should be distributed to the computers. Distribution of notifications can be started manually or automatically (see p. 48). For prompt synchronization, certain Windows OS parameters should be defined on the computers.

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

**Protection against resource duplication during synchronization**

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

Initial setup of IC mechanisms

This section describes the procedure for the initial setup of the 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 actor to integrity control procedure;
- list of software products available to various user groups.

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

Note.

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

General configuration procedure

To use the 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. 34).
2. Include additional objects to the data model:
 - tasks for use in AEC (see p. 35);
 - AEC jobs (see p. 36).

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 log Secret Net Studio (see p. 38).

3. Establish links between AEC jobs and actors (see p. 40).
4. Specify resources to control (see p. 40).
5. Enable the process isolation mode (see p. 41).
6. Create controlled resource reference values (see p. 43).
7. Grant privileges to users that should not be subject to AEC restrictions (see p. 46).
8. Enable AEC hard operation mode (see p. 46).

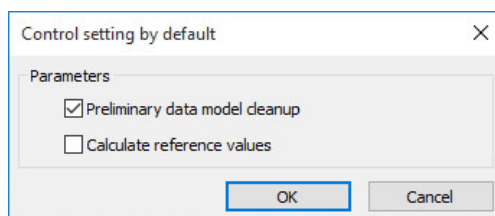
Also, it may be necessary to adjust and review the data model adjustment. If you want to remake the model, it is better to do it from scratch. If only a small part of the model requires remaking, you can use individual model modification procedures (see p. 55).

Building a new data model

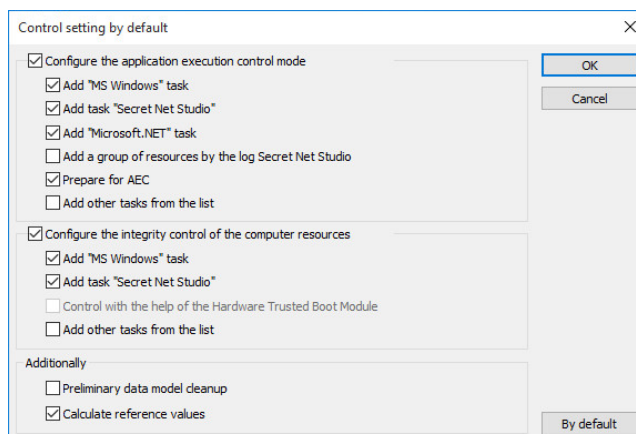
A data model is automatically provided with Windows OS essential resource descriptions along with those related to some applied software products. A newly created model has a default control setup.

To build a new data model:

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



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



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

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

Note.

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

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

Adding tasks to a data model

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

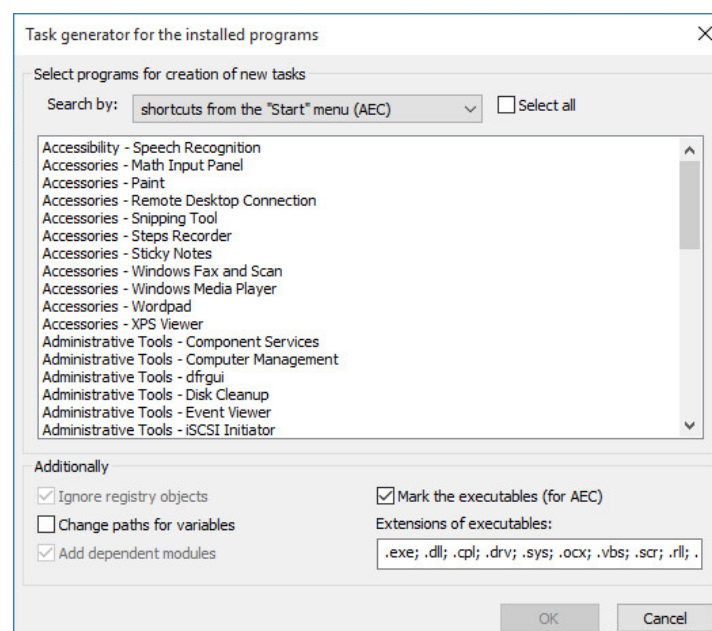
Prior to starting the generation procedure, you can view the list of software currently installed and note the particular components (of a program) that can serve as a basis for task generation. In this case, the tasks shall automatically include the resources referring to executable modules of a selected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

Furthermore, the AEC-tasks can be supplemented by using Secret Net Studio log-based AEC task generation method (see p. 38).

To add tasks to a model:

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

A dialog box appears as in the figure below:



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

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

Tip.

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

Parameter	Description
Ignore registry objects	Registry objects should not be considered as tasks
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, which the execution of source files depends on. These are, for example, drivers and libraries that are not directly integrated into the applications; however, if these files are missing, applications will not be able to work as intended. Dependent modules are added to the same resource group where the source file is found. Dependent modules are recursively integrated into the list: the files which are dependencies for the actual dependent modules are also integrated into the list
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). If necessary, edit the list of extensions to be used in this selection of resources

Note.

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

4. Click OK.
The generation procedure starts. A message box about successful completion appears.
5. Click OK.
As a result, the model contains new tasks including resource groups but not linked with superior objects (i.e., jobs), which is indicated by .

Adding jobs and including tasks to them

Jobs are created based on previously generated tasks.

To create a job:

1. Go to the "Jobs" category and in the "Jobs" menu, select the "Create job" command.
A dialog box asking you to select a job type appears.
2. Choose the job type and click OK.
The following dialog will appear:

New AEC job creation

General

Name:

Description:

Replicated

OK Cancel

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

New IC job creation

Main Schedule

Name:

Description:

Replicated

Method of resources control: Algorithm:

Parameters	Values
<input checked="" type="checkbox"/> Event registration	
Completion success	Yes
Completion error	Yes
Verification success	No
Verification error	Yes
<input checked="" type="checkbox"/> Error response	
Actions	Ignore

Completion success
Record successfully completed jobs.

OK Cancel

New IC job creation

Main Schedule

Main (irrespective of the calendar plan)

When loading operating system

At login

After login

Disable all

Calendar plan

	Mo	Tu	We	Th	Fr	Sa	Su
January	■	■	■	■	■		
February	■	■	■	■	■		
March	■	■	■	■	■		
April	■	■	■	■	■		
May							
June							
July							
August							
September							
October							
November							
December							

Time parameters

Control hours (0-23):

Interval: min.

OK Cancel



Attention!

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

Including tasks into a job

To include a task:

1. Select the "Jobs" category on the category panel.
2. In the structure window, right-click the job and click the Add tasks/groups | Existing command.
A dialog box appears showing the list of all tasks and resource groups not included in the job.
3. Select tasks to be included into the job and click OK.

Tip.

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

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.	Information logging
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 Category 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 the Properties command. 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 and 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. The procedure for saving log records to the file is described in document [4].

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.

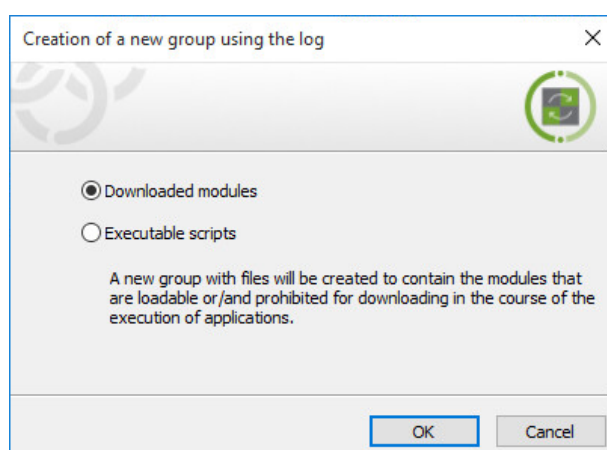
Note.

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:

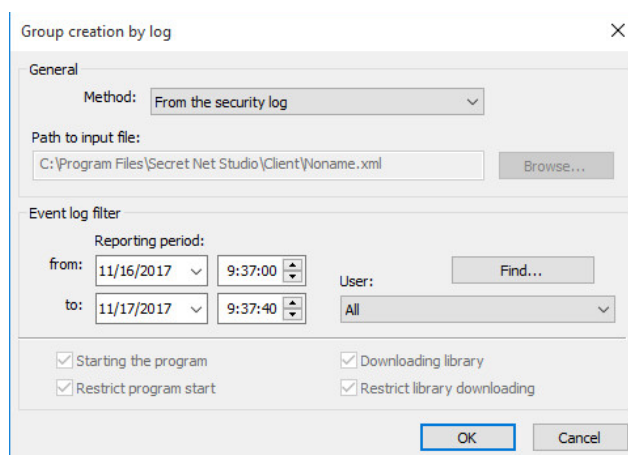
1. Select an actor in the main IC-AEC Management Program window.
2. Select a previously created AEC task linked to the selected actor or create a new AEC task.
3. Right-click the task and select Add tasks/groups | New group by log.

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:
 - Loadable modules – if the group should contain files downloaded during the work of the application;
 - Executed 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). For the jobs to be assigned to the required actors, the jobs should be added to the data model. A 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 Category panel, select the "Control actors" category.
2. In the "Control actors" menu, click the "Add to list" command.
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 IC-AEC Management 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, open the context menu and click the Add jobs | Available command.
A dialog box showing the list of available jobs appears. Each job has a number of actors it is associated with.
3. Select a AEC job that you wish to assign to an actor.

Tip.

To select multiple jobs, use the <Ctrl> key on the keyboard or click the "Select all" field.

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. 68). 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. 35), 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.

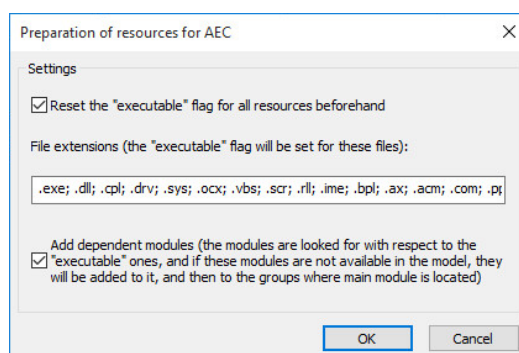
Note.

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 the AEC resources command.

A dialog box appears where procedure settings can be configured.



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 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), open the context menu and select the "Properties" command. In the Control Actor Properties 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).

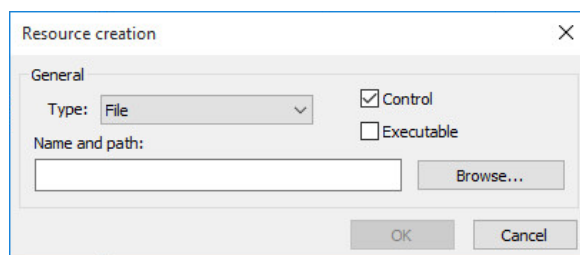
Add files of isolated processes to the resource list

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 Process Modules List in the parameters of the program .

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 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 the Browse button 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.

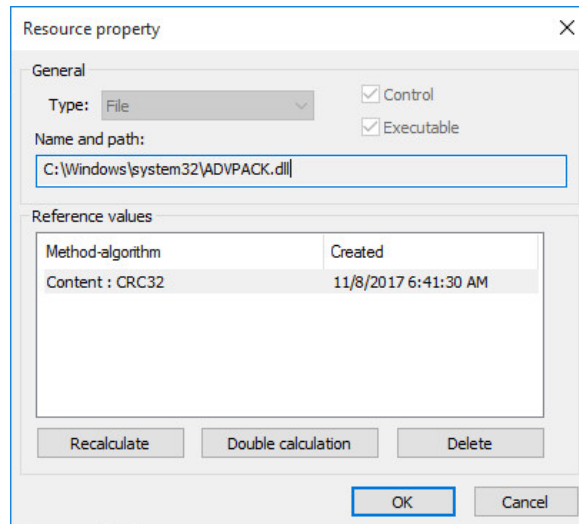
Enable isolation for resources

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 the "Properties" command.

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



2. Click the More button. 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. 34). If a data model is built using a task generation tool or manually, the reference values are to be calculated separately.

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

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

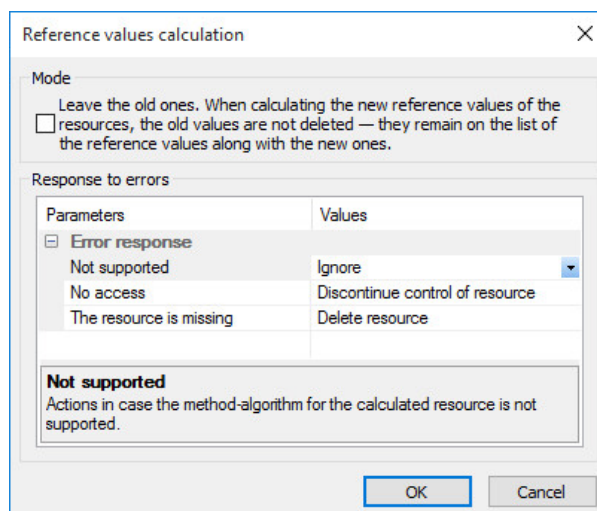
In the local mode, reference values can be calculated for all resources contained within a local data model. Exceptions are resources whose reference values were calculated in the centralized mode (i.e. resources are included in replicated jobs).

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

To perform a reference value calculation in the local mode:

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

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



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

Note.

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

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

The following types of errors are possible:

- calculation method/algorithm is not supported for this resource;
- the resource cannot be read or has been blocked;
- no requested resource found at the specified location.

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

Reaction	Description
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 the Reference values | Calculation command to calculate reference values for all replicated jobs;
 - right-click the job and click the "Local reference values calculation" command to perform the reference values calculation for resources of a separate replicated job.

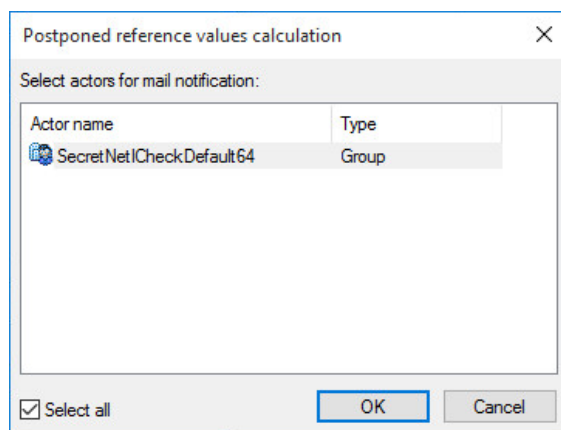
The "Reference values calculation" dialog box appears.

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

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

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

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



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

Note.

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

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

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

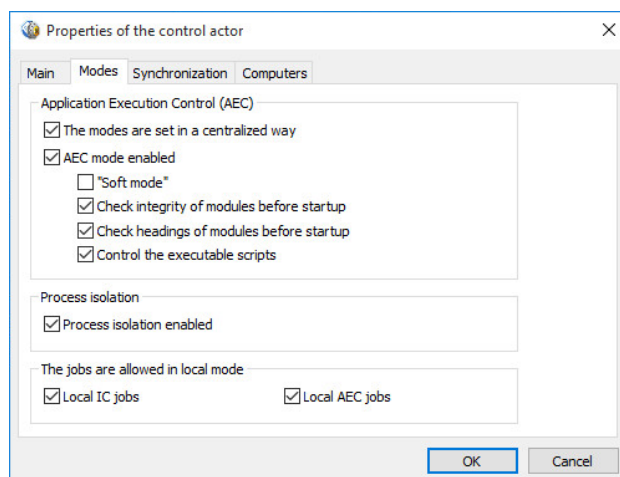
When AEC is launched and operates in hard mode, it only allows certified software products, libraries and scenarios to be run. Other resources are blocked and cannot be run, while the unauthorized access attempts are registered in the Secret Net Studio log as alerts.

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.

- In the additional window, select the structures or, in the list of objects, a computer or group (of computers), right-click them and click the Properties command. In the "Control Actor Properties" dialog box, select the Modes tab.



- In the centralized mode, select the "The modes are set in a centralized way (for centralized control)" check box.
- Select the "AEC mode enabled" check box and clear the "Soft mode" check box (if available).
- 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.

- Click OK.

Saving and loading a data model

Saving

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

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

To load the current version of the data model during the next session, you can export the model to a file, restart the program and import the model from the file (see p. 51, p. 52).

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 in the document [3]). The function is available for the Clients in the network operation mode.

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

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

Configuring automatic synchronization start

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

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

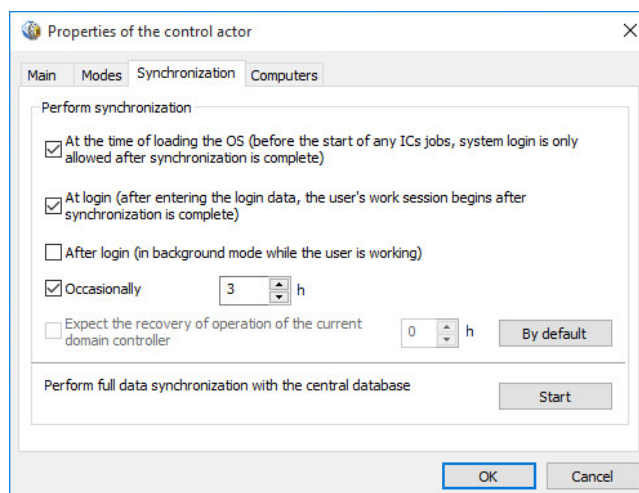
Comment.

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

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

To configure synchronization start parameters:

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



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

Parameter	Description
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 enter the System after synchronization is complete. This parameter may cause entry delays in the event of changes to large jobs in the central database and low capacity of communications channels
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	<i>Not available in the current version</i>

Note.

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

4. Click OK.

To check and adjust the synchronization start parameters in groups:

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

Note.

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

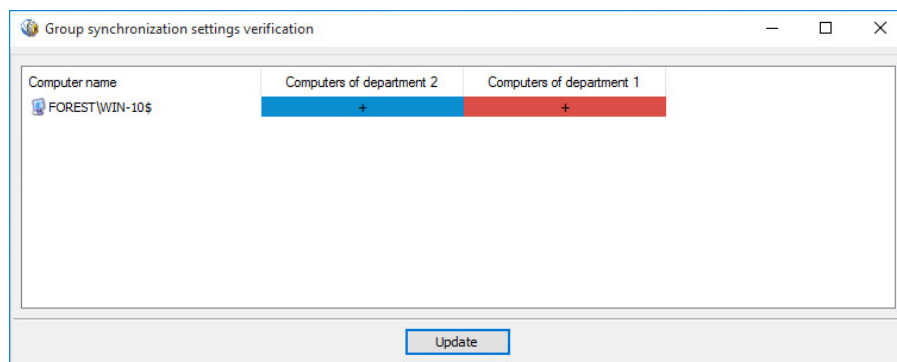
The program checks the computers' inclusion in groups with different synchronization parameters. The results will be displayed after the check.

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

Note.

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

- List of computers with conflicting parameters:



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

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

Forced start of full synchronization

The start of the IC-AEC central database changes synchronization on the computers may be performed automatically according to the predefined parameters (see p. 48). In the centralized operating mode, the administrator can launch an unscheduled full synchronization of IC-AEC central database changes on certain computers.

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

To start full synchronization:

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

The synchronization process starts.

Downloading and recovering a data model

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

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

To recover/retrieve a model from a DB:

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

Export

The export procedure can be performed using the following methods:

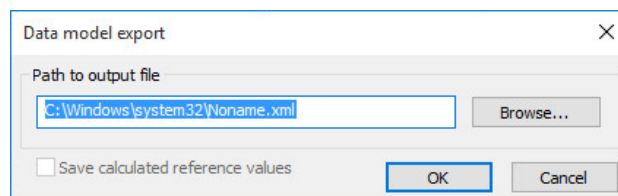
- exporting the entire data model;
- selective exporting of objects from specific categories (does not apply to "Control Actors" category objects).

Note.

To automate backing up of the IC-AEC DB, the option for exporting and importing the data model by launching the program from the command line is provided. A description of startup parameters is provided in the Appendix on p. 100.

To export the current data model:

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



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

Note.

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

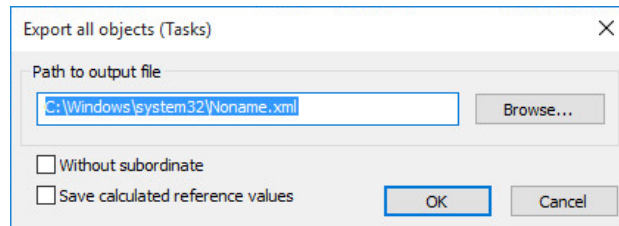
4. Click OK.

For the selective export of objects:

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

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

A dialog box appears as in the figure below.



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

Note.

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

7. Click OK.

Import

A file can be imported in the following ways:

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

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

Note.

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

For general import to the data model:

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

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

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

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

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



Attention!

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

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

Note.

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

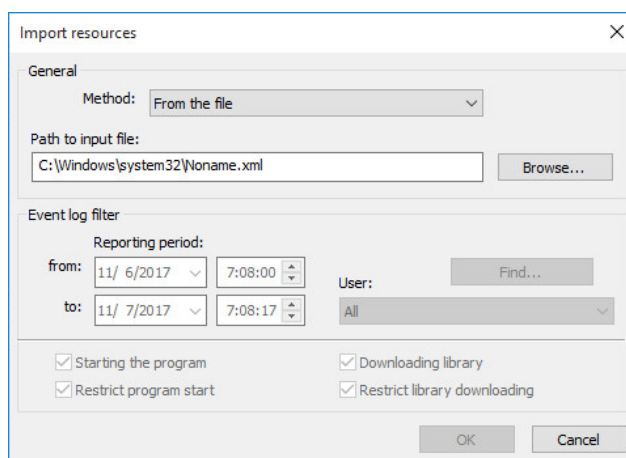
7. Click OK.

To import objects from the current category:

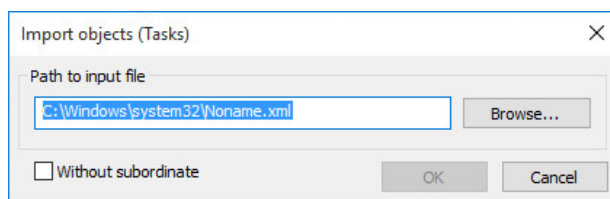
1. On the category panel, select the category from where you want to import objects (except "Control actors" category).
2. Select the root element in the structure window. Open the menu with the name of the selected element (e.g., "Job") and click "Import and adding" command.

A dialog box asking you to configure import settings appears.

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



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



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

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

Note.

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

Making changes in the data model

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

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

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. 68).

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 document [3]) the following additional parameters can be customized:

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

To change resource parameters:

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

The dialog box for setting the resource parameters appears.

2. If necessary, change the status of the Control attribute.
3. To recalculate a reference value, select it in the list and click Recalculate.
The reference value will be recalculated, and in the Created column, in the line corresponding to it, a new entry consisting of the date and time of recalculation appears.
4. To calculate a new reference value and save its previous value, click the "Double Recalculation" button.
The new reference value will be recalculated and saved along with the previous value.
5. To delete the reference value, select it in the list and click Delete.
6. If the resource is an executable file, set up additional parameters of exceptions for the AEC mechanism and process isolation. To do this, click Additionally and perform the following actions in a dialog box:
 - to permit the process to perform any script, select the "Permit Performance of Any Scripts" check box;
 - to allow the process to run files from specific folders, select the "Permit Performance of Any Modules from Indicated Directories" check box and generate a list of directories. To add a folder to the list, enter the path to it (the path can be entered manually or selected in the standard dialog box called up by clicking the button on the right of the entry line) and click the addition "+" button. To delete a folder from the list, select it and click the delete "-" button;
 - to enable process isolation, select the "Isolate the process" check box;
 - click OK.
7. Click OK.

Resource group parameters

Parameters determining properties of a resource group are:


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

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

To change group parameters:

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

Job parameters

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

To change job parameters:

1. Select the job, right-click it and click the Properties command.
The dialog box for setting the job parameters appears.
2. If a script requires changes, click Script (generation of a script is described onp. [64](#)).
3. Make changes in the Name and Description fields and click OK.

Task parameters

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

To change task parameters:

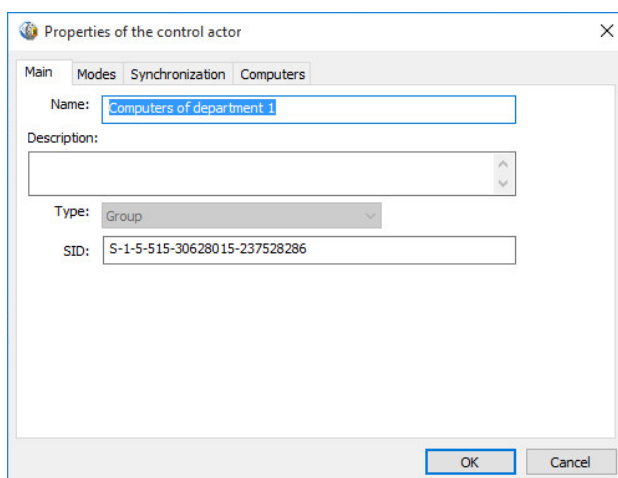
1. Select the task, right-click it and click the Properties command.
The dialog box for setting the task parameters appears.
2. Change the modifiable parameters and click OK.

Actor parameters

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

To change actor parameters:

1. Select the actor, right-click it and click the Properties command.
A dialog box appears as shown in the figure below:



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

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

Adding objects

Adding objects does not cause any changes in how security mechanisms operate. To apply changes, the added objects must be linked to already existing objects. For example, a new resource added to a model must be included in a resource group. A

resource group must be included in a job, and the job, in turn, must be included in a task (a resource group can also be included directly in the task). And, finally, the task must be linked to an actor– a computer, user or group of users/computers.

Adding a resource

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

Method	Description
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: <ul style="list-style-type: none"> • a file with a saved data model (see. p. 52); • 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 appears asking you to select the resource type.

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

3. Click OK.

A dialog box for setting the resource parameters appears.

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

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

Parameter	Description
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
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):

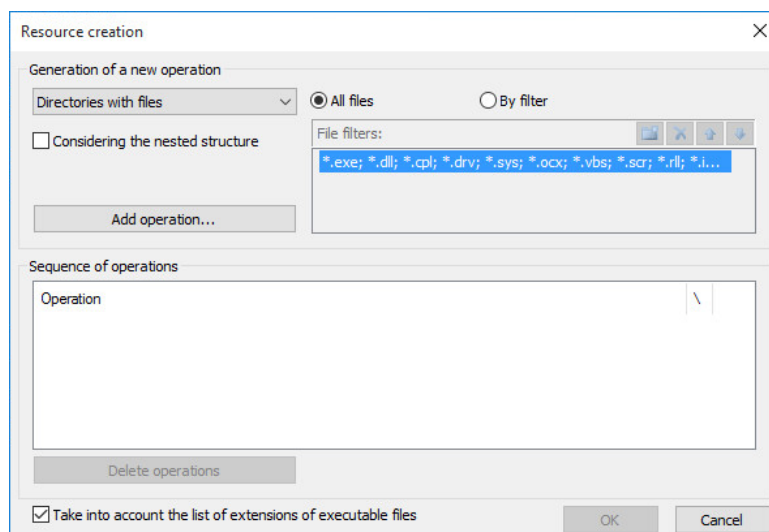
Parameter	Description
Name	Enter the name of the resource, unique for the list of resources. For example, the name of the file from which the scenario (script) can be indicated as the resource name
Description	Enter additional information about the resource
Contents	Enter the scenario (script) text – 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 the Resources | Create resource(s) | Multiple command from the menu.

A dialog box appears as in the figure below:



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

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

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

Parameter	Explanation
Resource selection version	The following options are available: <ul style="list-style-type: none"> 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 (in the document [3]). Files with this attribute, when displayed on the main window of the IC-AEC management program, are marked with a special symbol

Setting filters.

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

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

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

- 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.

- Select the required files.

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

Note.

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

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

- 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.

- Select the directory and click OK.

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

Note.

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

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

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

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

8. Select a register key and click OK.

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

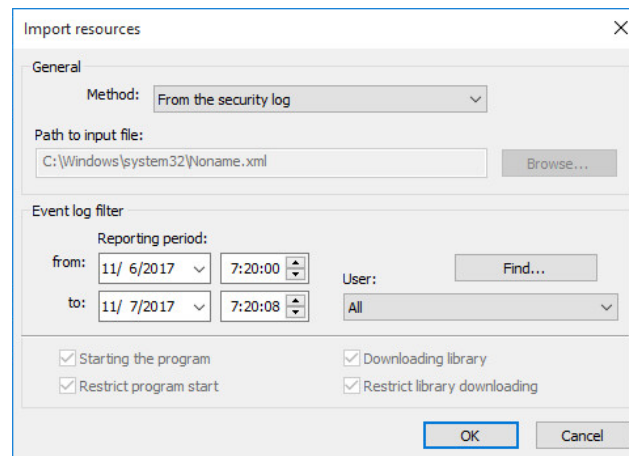
9. Check the list of completed operations, and if it contains all resources you had planned to include in the data model, click OK.

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

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

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

A dialog box appears as in the figure below:



2. Select the "From the security log" value in the Method drop-down list.

Filter settings will become available, based on which resources will be selected from the Windows OS security log. Settings include the reporting period (date and time) and user name.

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

To select the user:

- Click the "Find..." button.

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

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

4. Click OK.

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

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

A dialog box appears (see the previous procedure).

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

Note.

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

3. Set the filter parameters and click OK.

Note.

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

To add a resource to a group:

1. Select the Resource Group category.
2. In the additional structure window, select the group to which you want to add new resources, call up the context menu and click the "Add Resources" command and then:
 - Existing — to select resources from those available in the data model, but not included in this group.
 - New single — to add an individual resource (see above for the description of the procedure for manually adding an individual resource).
 - Multiple new — to add several resources (see above for the description of the procedure for manually adding several resources).
 - Import — to import a list of resources from another source: from a file (for a description of the object import procedure, see onp. 54), from security log or Secret Net Studio log (for a description of the resource import procedure, see above).

The selected resources will be added to the group.

Adding a resource group

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

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

Note.

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

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

To add a resource group manually:

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

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

To add a resource group by directory:

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

A standard Windows OS dialog box for directory selection appears.

3. Select the directory and click OK.

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

To add a resource group by registry key:

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

A standard Windows OS dialog box for registry viewing appears.

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

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

To add a resource group by log:

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

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

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

4. Click OK.

A setting dialog box appears.

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

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

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

6. Set the filter settings and click OK.

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

To add a group of resources using import methods:

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

The dialog box for setting the import parameters appears.

3. Perform actions to import category objects (see a description of the import procedure on p. 52).

Adding jobs

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

- manually;
- manually with a script;
- using a job generator (see p. 35);
- using import tools (see p. 52).

To add a job manually:

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

The dialog box for setting the job parameters appears.

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

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

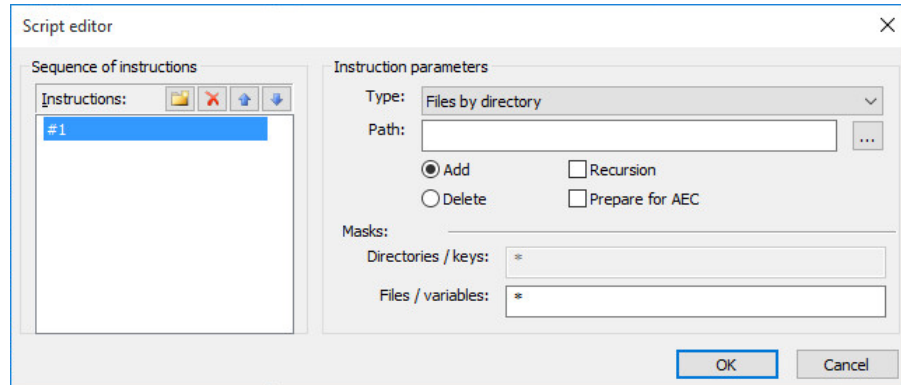
To add a job with a script manually:

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

The dialog box for setting the job parameters appears.

2. Enter the job's name and its brief description.
3. Click the Script button.

A dialog box appears as in the figure below.



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

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

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

5. Select the resource type and specify the path.

Available types are listed in the following table.

Resource type	Description
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	Resources from the software of the Client are selected Secret Net Studio
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

Resource type	Description
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. 68). To add dependent modules, select the "Prepare for AEC" check box. This will also automatically select all dependent modules for files specified with the mask. They are added to the model and are marked as executable. In other words, the result is the same as when performing the procedure for searching and adding dependent modules, but not on this computer or on all computers where the generated script will be run.

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

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


Note.

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

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

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

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

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

Adding tasks

Task adding procedures are described in detail on p. 36.

Adding actors

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

To add computers (the centralized mode):

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

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

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

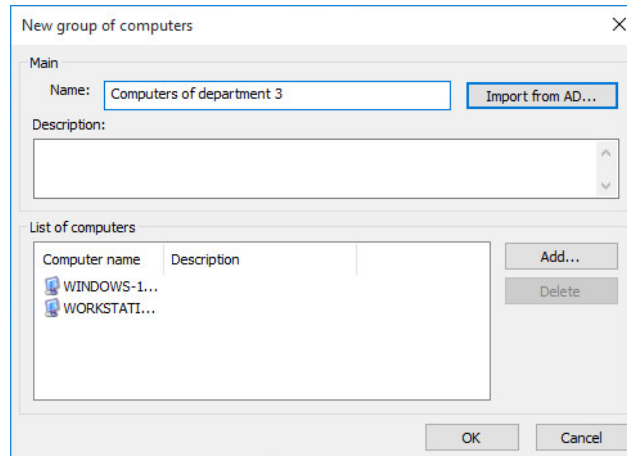
3. Select the Computer field and click OK.

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

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

To add a computer group (the centralized mode):

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



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

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

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

Deleting objects

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

**Attention!**

After deleting resources from a task, recalculate reference values.

**Warning.**

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

To delete an object:

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

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

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

3. Click Yes.

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

To delete all objects of a certain category:

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

A dialog box with links to the objects appears.

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

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

Links between objects

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

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



Attention!

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

To establish links between objects:

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

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

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

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

To delete links between objects:

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

Note.

The object may be simultaneously deleted from all superior objects.

A warning message on deleting links with superior objects appears.

2. Click Yes.

Disable local jobs

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

You can disable the local jobs in the properties of the required actor in the centralized operating mode. The parameters can be defined for separate computers and for

groups of computers. In this case, the disabled parameters have priority. For example, if the "Local AEC jobs" check box is disabled for the group, such jobs will be prohibited on the computer, even if this parameter is enabled for this computer.

To disable local jobs:

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

Searching for dependent modules

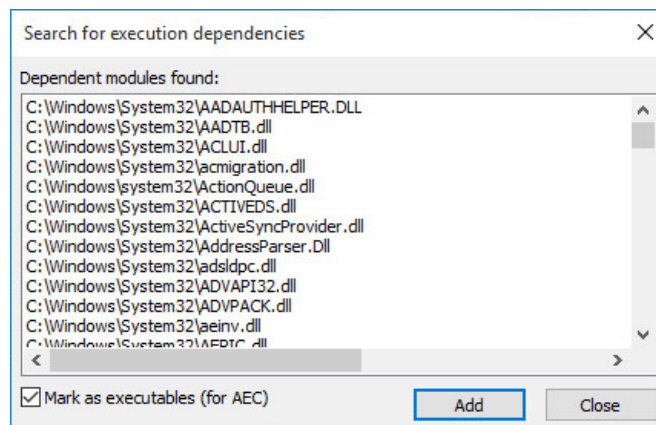
When the user works with applications, executable files may be run together with modules (drivers and libraries) which are not directly integrated into the applications. Such modules are called dependent.

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

To find and include dependent modules:

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

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



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

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

Replacing environment variables

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

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

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

To replace environment variables:

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

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

2. Specify the change direction:

- To replace absolute paths with environment variables, leave the default check box.
- To replace environment variables with absolute paths, select in the "Names of environment variables to value of paths in files and folders" check box.

3. Select the variables from the list for which the action is to be performed.

4. Click OK.

Chapter 4

Mandatory access control settings

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.

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.

Confidentiality categories of resources

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

- non-confidential;
- confidential;
- strictly confidential.

If necessary, you can add other categories with different names in accordance with the standards of your company. Maximum number of categories — 16.

Once the Client is installed, all folders and files on the computer's local disks are assigned the non-confidential category (if the resources 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 who are granted the privilege to manage confidentiality categories can assign lower categories for resources or higher categories for folders.

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 required categories or confidentiality 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. 9). 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 when working with the device list of group policy.

A device's confidentiality category has a higher priority over the categories of files and folders stored on that device. If the file's (folder's) category is lower than the device's confidentiality level, the System considers the file's (folder's) category the same as the device's category. Conversely, when the file's (folder's) category is higher than the device's confidentiality category, the System considers it incorrect and prohibits access to the file (folder).

Between the file system objects, inheritance is applied within folders with a category other than the public information category (non-confidential by default). The confidentiality category of objects, within a folder, is inherited in accordance with the inheritance features defined in the folder's attributes.

New subfolders and files can be assigned the folder's confidentiality category automatically by inheriting the parent folder's category. 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 who is granted the confidentiality category management privilege can modify the features.

Access levels and user privileges

Access levels

A user can access to confidential information if the respective access level is assigned to this user. The set of access levels used in the System is the same as the set of confidentiality categories for resources (see above).

A user is allowed to access a resource if the user's access level is not lower than the resource confidentiality category. For example, a user with the confidential access level can to 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. 74.

User privileges

MAC include user privileges listed in the following table:

Privilege	Description
Confidentiality category management	Allows the user: <ul style="list-style-type: none"> 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. 74)
Printing confidential documents	Allows the user to print confidential documents. The privilege is applied when the Printer 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. 74). 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 the correct operation of

the System, 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 login, the user can select the confidentiality level of the session as confidential, which will prohibit 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 login on a computer (when creating a user account). A session level other than non-confidential should be selected only for confidential data processing.

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 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. 74).

3. Assign confidentiality categories to resources (see p. 74).
4. Configure the list of events to be registered (see p. 75).
5. To add markers to documents during printing, enable the marking mode (see p. 23).
6. To restrict the printing of confidential documents, configure the use of printers (see p. 75).
7. To use the flow control mode, configure and enable the mode (see p. 76).

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.

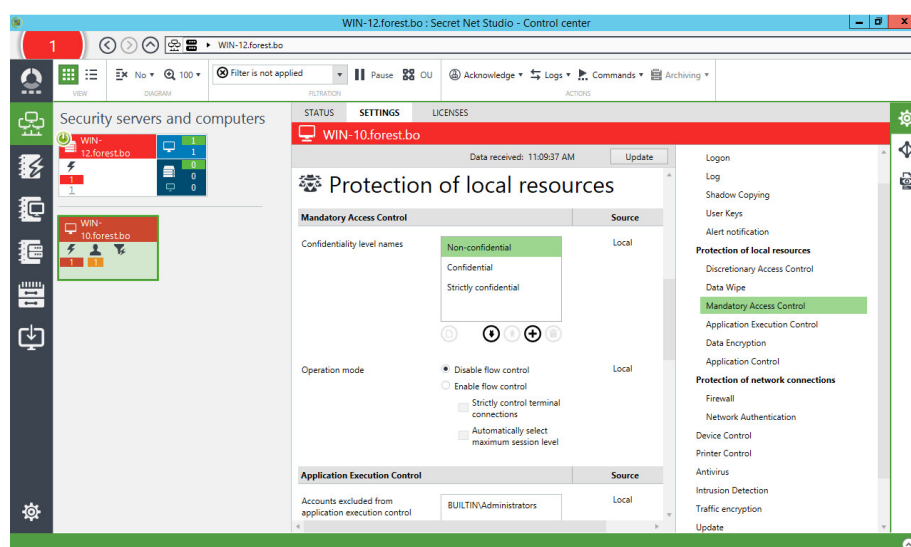
For example, all computers that are supposed to process confidential information can be included in a separate organizational unit and categories in that unit's policy can be configured.

The centralized configuration procedure when using the Control Center in the centralized mode is described below. Local configuration is performed in the same way as in the Control Center. See information about the Control Center in the document [4].

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 the "Mandatory Access Control" group.

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.

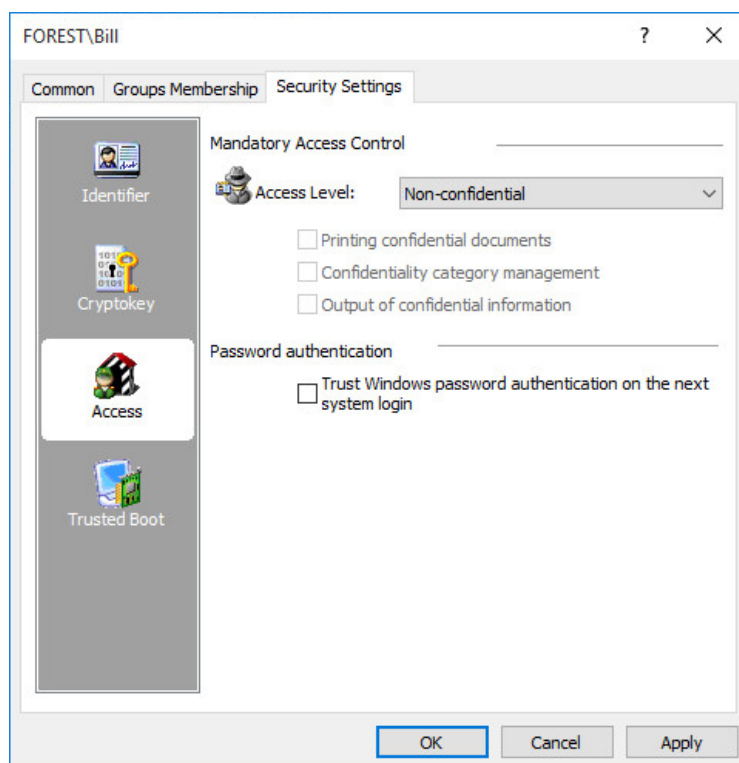
Assigning access levels and privileges to users

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 document [3]).
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 into the System 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 disks (except disks with

the 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. 11).
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 this, click the button in the right part of the cell. If you need to explicitly configure the MAC parameters for that object, clear the "Use the category settings from a parent object for new devices" check box. To assign categories, when configuring parameters of a class or model, select the "Non-confidential" check box. To assign a confidentiality category to a certain device, select the "Confidentiality category is assigned to the device" check box and select the required category in the drop-down list (a full list of categories is only provided for a specific device). If the device should operate regardless of the user access level, select the "Without considering the category" check box.
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.

See document [8].



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.

Event registration setup

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. 73), 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. 21).

To configure the use of printers:

1. Load the printer list (see p. 18).
2. Select the required element in the list.

3. Specify the required parameters in the cell of the "Control parameters" column. To do this, 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's account 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. 74);
 - include 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 setup program for the flow control mode (see p. 76), enable the automatic setup mode for the required applications and perform the automatic setup procedure.
3. Set confidentiality levels for network interfaces (see p. 77).
4. Enable the flow control mode (see p. 78).
5. Make sure the applications operate correctly on computers in confidential sessions. In case of errors, configure joint operation with application software (see p. 78).

Setup program for the flow control mode

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 setup program is used (hereinafter – the setup program). The setup is performed before enabling the flow control mode as well as during system operation when adding new users, programs, printers.

To start the setup program, perform the actions corresponding to the version of the installed operating system:

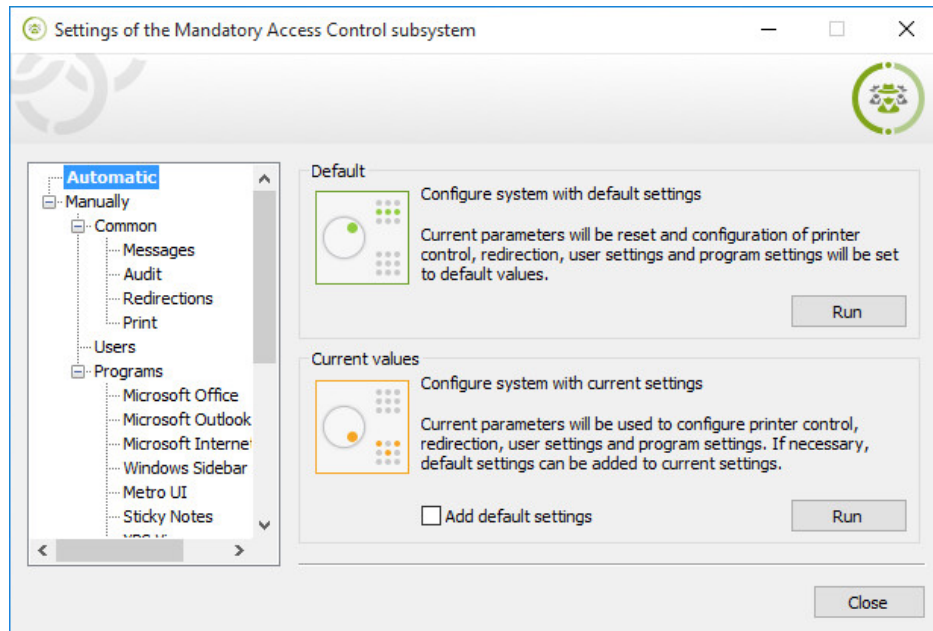
- on a computer running Windows 8 or Windows Server 2012 operating system, load the Start screen and select the "Settings of the Mandatory Access Control subsystem" element;
- on a computer running other OS, click the Start button and select "Settings of the Mandatory Access Control subsystem" in the program menu.

Note.

The setup 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 setup program window is shown in the figure below.



The setup 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 setup 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 setup program can only be started in the read-only mode.

The setup 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 setup program window by default. Manual configuration is available to perform specific operations. For example, to use the setup program with software that is not included in the list for automatic configuration.

For program operating instructions, see appendix on p. **101**.

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. **11**).
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 this, click the button in the right part of the cell. If you need to explicitly configure the Mandatory Access Control parameters for that object, 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's confidentiality level, clear check boxes for all levels.
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 setup program (see p. **76**) and go to the Manually | Programs section. If the application is on the list, enable the automatic setup mode and apply the automatic setup using the current parameter values. If the application is not on the list, go to other troubleshooting and setup procedures.

Note.

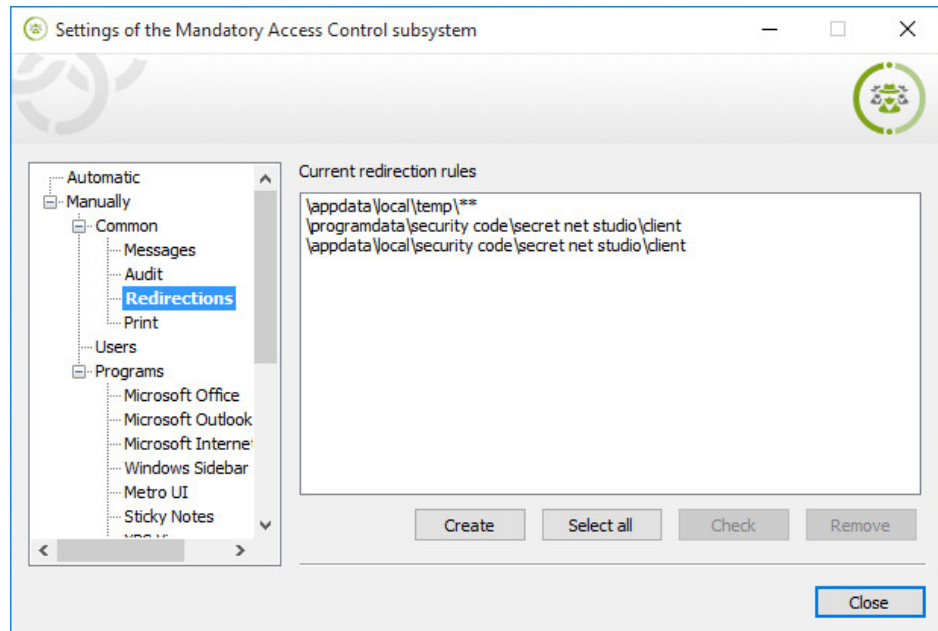
The list of applications in the setup program is designed for applying templates for configuring joint operation. By default, the automatic setup mode is disabled for most elements of the list (for example, for AutoCAD, Photoshop and other software products). Therefore, enable this mode to apply a template. For the setup program operating instructions, see appendix on p. **101**.

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
<p>Contain user document files. For example, the \Documents directory in the user account.</p> <p>Probable causes of access denial: general recommendations on the assignment of categories to directories and files are not followed (see p. 75) or rules for confidential resource handling are applied (see p. 81).</p> <p>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)</p>
Temporary application data directories
<p>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.</p> <p>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.</p> <p>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</p>
Directories containing application configuration parameters
<p>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.</p> <p>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.</p> <p>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.</p>
Directories containing application's operational data
<p>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.</p> <p>Correct file handling in such directories is ensured by the redirection function (see below)</p>

8. To create redirection rules, start the setup program and go the Manually | Common | Redirections section.



Use the Create button 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 for redirection the directories containing a great deal of data. 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: <ul style="list-style-type: none"> • devices with a confidentiality category higher than the user's 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 permitted 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 permitted to delete a confidential file to the Recycle Bin	It is not permitted 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.	
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 permitted to delete a confidential folder to the Recycle Bin	It is not permitted to delete any folder to the Recycle Bin
Inheriting the folder's confidentiality category	

Disabled flow control	Enabled flow control
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 catalog confidentiality category. Restriction: The assigned confidentiality category must be equal to the current session's confidentiality level
<p>If automatic confidentiality category assignment mode is disabled:</p> <ul style="list-style-type: none"> 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. 	<p>If automatic confidentiality category assignment mode is disabled:</p> <ul style="list-style-type: none"> 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	
A user who is not granted the Confidential 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 catalog's confidentiality category)	A user who is not granted the Confidential 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 catalog's confidentiality category)

Disabled flow control	Enabled flow control
<p>A user granted the Confidential Category Management privilege can:</p> <ul style="list-style-type: none"> • elevate the confidentiality category of catalogs and files within the user's access level; • assign a lower confidentiality category to catalogs 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 catalog if the catalog's current confidentiality category is not higher than the user's access level 	<p>A user granted the Confidential Category Management privilege can:</p> <ul style="list-style-type: none"> • elevate the confidentiality category for catalogs and files, but not higher than the current session's level; • assign a lower confidentiality category to catalogs and files with a current confidentiality category not higher than the current session's level; • change the automatic confidentiality category assignment mode for a catalog if the catalog's current confidentiality category is not higher than the current session's level
Printing confidential documents	
<p>If the Printer Control mechanism is enabled:</p> <ul style="list-style-type: none"> • a user not granted the Confidential Document Printing privilege can only print non-confidential documents; • a user granted the Confidential Document Printing privilege can print confidential documents with a confidentiality category not higher than the user's access level 	<p>If the Printer Control mechanism is enabled:</p> <ul style="list-style-type: none"> • a user not granted the Confidential Document Printing privilege can only print non-confidential documents (as long as the document has not been edited); • a user granted the Confidential Document Printing privilege can print confidential documents with a confidentiality category not higher than the current session's level
<p>If the Printer Control mechanism is disabled, any user with access to confidential documents can print the documents, irrespective of whether the user has the Confidential Document Printing privilege or not. Moreover, the documents will be printed without the confidentiality mark</p>	
Output to external media	
<p>A user who has access to confidential documents can copy files or save their contents to any media, irrespective of the Confidential Information Output privilege</p>	<p>A user not granted the Confidential Information Output privilege cannot copy confidential files or save their contents to external media. External media in the Secret Net Studio system are removable disks that have the Irrespective of Confidentiality Category access mode enabled.</p>

Chapter 5

Stored data security settings

Discretionary access control for folders and files

You can perform the following operations when configuring the discretionary access control :

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 in the local Control Center. For information about the Control Center in the document [4].

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.

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 the document [8].

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. 84), 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. The procedure for changing access rights is described in the document [8].

Overwriting deleted information

Secret Net Studio can automatically overwrite memory areas with remaining data from deleted objects. This makes it impossible to recover the data after deletion and ensures secure reuse of the data storage media. Overwriting can be performed automatically on certain types of devices (local and removable disks, RAM) or for user-selected file objects.



Attention!

The virtual memory pagefile is overwritten 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 instance. Such files are erased when the Recycle Bin is cleared.

The centralized configuration procedure when using the Control Center in the centralized mode is described below. Local configuration is performed in the same in the local Control Center. For information about the Control Center, see document [4].

To configure this function:

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, click Data Wipe.
3. Specify the required values for overwriting parameters:
 - Number of wipe cycles for local disks;
 - Number of wipe cycles for removable media;
 - Number of wipe cycles for RAM;
 - Number of wipe cycles for "Delete permanently" command.

Note.

If the parameter value is "0", wiping is not performed. To ensure that data is erased, two wiping cycles are usually enough.

4. Click Apply.

Protecting local disks

Access to a computer's local disks is protected by the disk protection mechanism. The mechanism blocks access to disks in the case of an unauthorized access to a computer. A OS loading is considered authorized if performed by the OS with the Client installed. All other methods for loading the OS are considered unauthorized in terms of the mechanism's operation (for example, loading from an external medium or loading another OS installed on the computer).

The setup procedure for the disk protection mechanism contains the following stages:

1. Enabling the mechanism.
2. Enabling and disabling logical partition protection.

Enabling disk protection

By default, once the Client is installed and the license is registered, the disk protection function is disabled. The function is enabled by the administrator.

When enabling the mechanism, a special key is generated or loaded, which is the basis for future modification of boot sectors of logical partitions on the computer's hard disks. The new key generation is mandatory when the function is enabled for the first time. After this, you can use the same key to re-enable the mechanism.

To be able to remove disk protection, in case of an emergency, the key copy should be saved. You can save the key in the following ways:

- create a system drive for emergency recovery where the key will also be saved;
- save the key to a user-defined folder.



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).

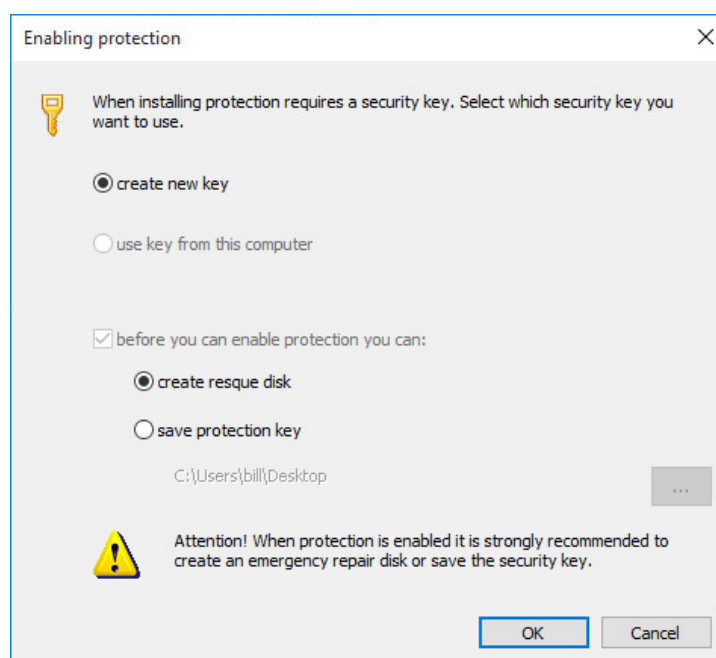
To enable disk protection:

1. In the Windows Control Panel, select "Manage Secret Net Studio".

A dialog box appears.

2. On the "Disk protection" tab, click "Enable protection".

A dialog box appears as in the figure below..



3. If the disk protection function was used on that computer and was disabled later, select which key should be used.

- create new key (recommended) — when enabling the function, a new key will be generated and the previous key will become invalid. To generate a new key, select this check box;
- use key from this computer— the previously used key will be loaded (use this option only if you are absolutely confident that the key is not compromised, or if you need to remove the protection of logical partitions after incorrectly disabling the function). To load a previously used key, select this check box.

4. Select an option to save a copy of the key. To do this, leave selected "before you can enable protection you can:" check box(the field is unavailable, if a new key is generated) and click the required saving option:

- create resque disk (recommended) — boot disk with a copy of the key will be created. To create the disk, click this option button;

- save protection key— the key file will be saved to the selected folder. To save the key, click this option button. The current selected path to the folder is displayed below. To select another folder, click the button on the right and select the required folder in the standard dialog box.

Note.

If you select a previously used key when a copy of the key is available, you can cancel saving the new copy. For this purpose, clear "the before you can enable protection you can:" field.

5. Click OK.

The disk protection mechanism is enabled.

If you selected one of the key saving options, the mechanism will be enabled after the key is successfully saved. A special wizard is automatically started (see below for details on how to use the wizard) for creating the boot disk for emergency recovery. Once the key is saved, a corresponding message is displayed.

6. Once the function is enabled, restart the computer.**Wizard for emergency recovery disk creation**

Software tools ensuring disk protection include a special wizard for creating a boot disk for emergency recovery. You can use compact discs or USB flash drives as media for boot disk creation. In addition, you can create a disk image file and use it for creating the disk using other software tools.

The wizard starts when an option for creating the rescue disk is selected, when enabling the disk protection function (see above) or when using the emergency recovery wizard (see p. 111).

To create the boot disk for emergency recovery:

1. In the wizard's start dialog box, click Next.
A dialog box appears.
2. Depending on which key should be loaded, take the corresponding step:
 - to load the key from a special storage on your computer (the last generated key) — select the "use key from this computer" check box;
 - to load the key from file — clear the "use key from this computer" check box (if selected) and click the Show button. In the standard dialog box that appears, select the key file. The file must have the .RK extension. This key loading method is used, for example, when you cannot load the key from the computer's storage or when the emergency recovery disk was created on another computer.
3. Once the key is loaded, click Next.
A dialog box appears where record settings can be configured.
4. In the "Medium type" field, select the required medium for boot disk creation: compact disc or USB flash drive.
5. If a compact disc is selected for boot disk creation, the option of saving the disk image file in a specified folder is available. To save the file, select the save disk image in the "folder" field. The current selected path to the folder is displayed below. To select another folder, click the button on the right and select the required folder in the standard dialog box.
6. To write the boot disk, select the "write the image on the medium in the device" check box, and select the device. The drop-down list contains the names of devices that are compatible with the selected type of medium.
7. Click Next.
Disk formatting begins. The progress of the process will be displayed in the information window as a progress bar.
8. Once the disk is created, click Finish.

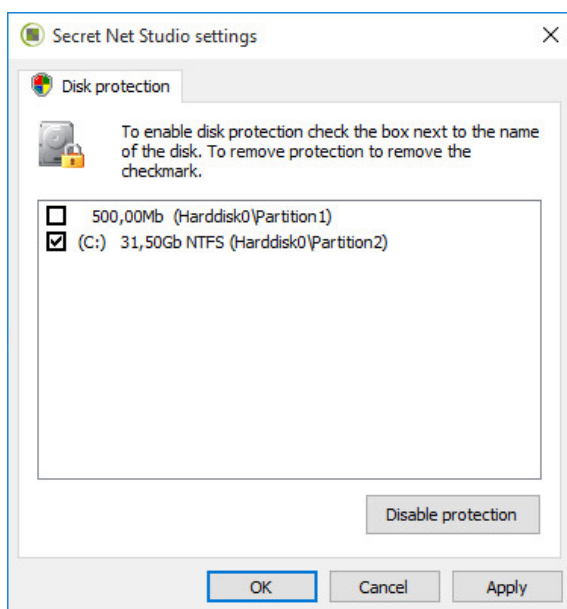
Enabling and disabling logical partition protection

By default, once the disk protection mechanism is enabled, the protection mode is disabled for all logical partitions. You can selectively enable the protection mode for the required partitions.

This mechanism ensures the protection of up to 128 logical partitions with up to 32 physical disks. Logical partitions with the protection mode enabled must use the FAT, NTFS or ReFS file system. Supported disks have a master boot record (MBR) or a partitions table on GUID identifiers (GUID Partition Table — GPT). Disks with other types of logical partitions are not supported (for example, dynamic disks).

To enable/disable the protection mode:

1. In the Windows Control Panel, select "Manage Secret Net Studio".
A dialog window appears.
2. Select the "Disk protection" tab.
The dialog box lists the disks for which you can enable the protection mode.



3. Select the logical partitions for which protection mode should be enabled. If you need to disable the protection of a logical partition, clear the check box.
4. Click OK and restart the computer.

Disabling disk protection

When disk protection is disabled, protection is disabled for all logical partitions, and the system restores the initial state of the boot area on the physical disk used to launch the operating system. The key, however, is not removed from the system and can be reused on that computer.

To disable disk protection:

1. In the Windows Control Panel, select "Manage Secret Net Studio".
A dialog box appears.
2. Select the "Disk protection" tab and click the "Disable protection" button.
The function will be disabled, and the button will change to "Enable protection".
3. Restart the computer.

Data encryption in encrypted containers

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 "Encrypted Container Creation" privilege.

By default, the permission to create encrypted file containers is granted to users included in the local group of administrators 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. For information about the Control Center, see the document [4].

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" section, "Data encryption" group. To go to the registration settings from the respective group of parameters in the Policies section (see above), 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 media. The key information can be stored in a personal identifier assigned to a user or on a removable medium.

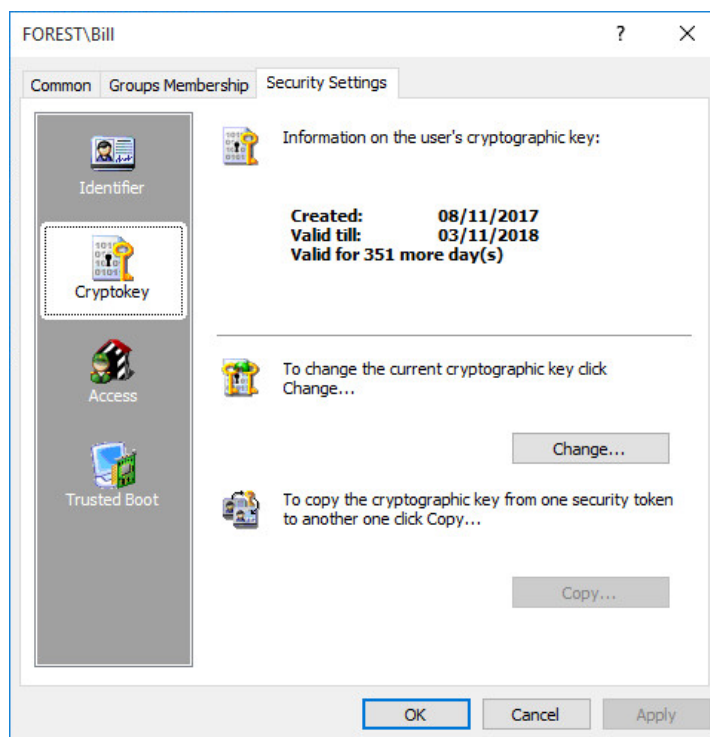
Key issue and change

Key information can be generated and a private key can be saved to a key device when assigning a personal identifier to a user. For the description of the assignment procedure, see document [3]. If a user is assigned an identifier, 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 (see document [3]).
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 identifier 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> button.



Attention!

The don't save the key option is only recommended when it is impossible to read the current key from the user identifiers. To confirm your selection, enter the word "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 identifier.

6. Provide the identifier containing this user's old 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 identifiers.

8. Present all listed identifiers.

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

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 identifiers. 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 identifier to another. Copying is performed by the security administrator.

To copy keys:

1. Launch the user management program (see document [3]).
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 identifiers are assigned to the user.

A dialog box appears asking you to present the identifier.

5. Present the identifier containing the user keys.

Key reading is initiated, and the dialog box displaying the list of the user's identifiers appears.

6. Present the identifier to which the keys should be saved.

Once the keys are successfully saved to the identifier, its status changes to Processed.

7. Click Close.

Configuring key changes 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 [8]). 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. For information about the Control Center, see document [4].

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.

Chapter 6

Terminal session security settings

Using identifiers in terminal sessions

Personal identifiers assigned to users can be used for terminal login during remote access connections. For this purpose, any of the following login protection identification modes should be enabled on the terminal server (see document [3]):

- Mixed (enabled by default);
- Only by identifier.

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 enabled on the terminal server, terminal login with the user account data takes place immediately after pre-authentication on the terminal client machine. Presenting an identifier to the terminal server is not expected.
- If the Only by identifier identification mode is enabled 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 own personal identifier.

If pre-authentication is disabled, the user signs in to the terminal session by identifier 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, open the context menu of the Remote Desktop Connection window header and click the About command.

To disable pre-authentication on the terminal client:

1. Sign in 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's documents folder.

Comment.

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 login 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 `enablecredsspssupport` parameter. If this parameter is missing, add the following line:

```
enablecredsspssupport: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 this, 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 parameter can be found in the computer's group of configuration policies, section Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Session Host / Security.

3. Save the changes.

Software methods for identifier processing

In terminal sessions, various methods may be used for processing personal identifiers 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 (not 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 (see document [3]). 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 `NoSCR redirection` 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.

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

To prohibit or allow 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.

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

To prohibit or allow 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 "Device 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's 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.

Prohibition 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.

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

To prohibit 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 "Printer 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 flow control mode of MAC 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. [78](#)).

Appendix

List of groups and classes for device control

Tab.1 Device groups and classes

Group	Class
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
PCMCIA devices	Serial ports and modems. Parallel ports. Storage devices. Network adapters. Other
IEEE1394 devices	Storage devices. Printers. Scanners and digital cameras. Network devices. Digital video cameras. Other
Secure Digital devices	Memory cards
Network	Ethernet connection. Wireless connection (WiFi). Bluetooth connection. 1394 connection (FireWire). IR connection (IrDA)

Examples of configuring removable disk use

Local assignment of removable disks to users

This section covers an example of a local setup for control of user access to removable disks. 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:
 - on a computer running Windows 8 or Windows Server 2012 OS, load the Start screen and select Local Control Center;
 - on a computer running other OS, 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 removable drives

Secret Net Studio makes it possible to restrict the connection of devices (as well as removable drives) and allow only equipment authorized by the security administrator to be used. To do this, the following methods can be used:

- creating a device list on an individual machine (see p. [11](#));
- 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. [12](#)).
2. Add the required devices to the group policy list (see p. [13](#)).
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. [14](#).

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. 76.

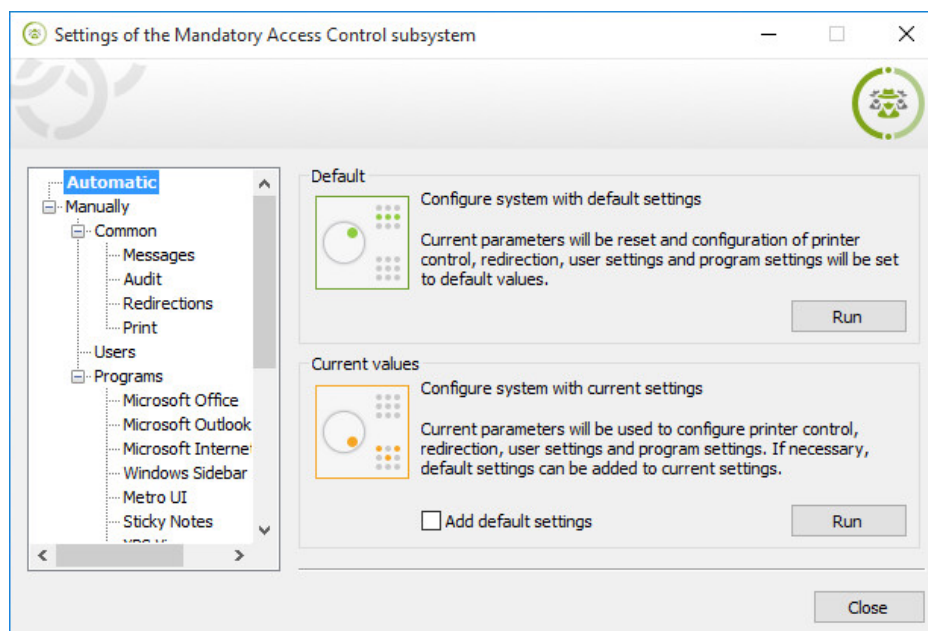
Automatic setup

The System for operating the Mandatory Access Control and Printer Control function 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 printer 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 values 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 Printer 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:

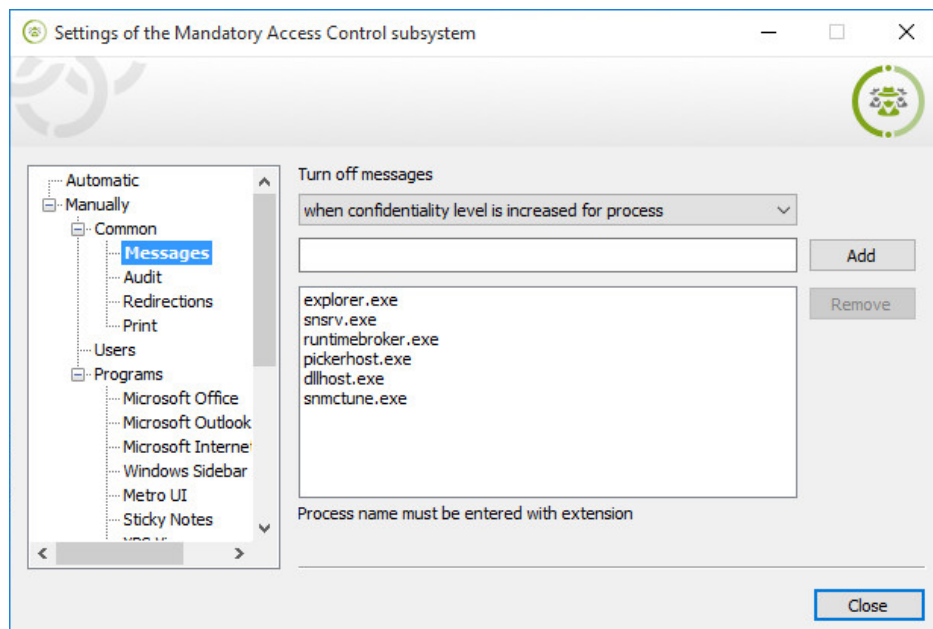
- Common — setup of common operation parameters for users and applications;
- Users — setup of parameters related to user accounts;
- Programs — setup of parameters related to applications.

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 the Add button;
 - to remove elements from the list, select them+ and click the Remove button.

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 the Add button;
 - to remove elements from the list, select them and click the Remove button;
 - 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 the Add button;

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".

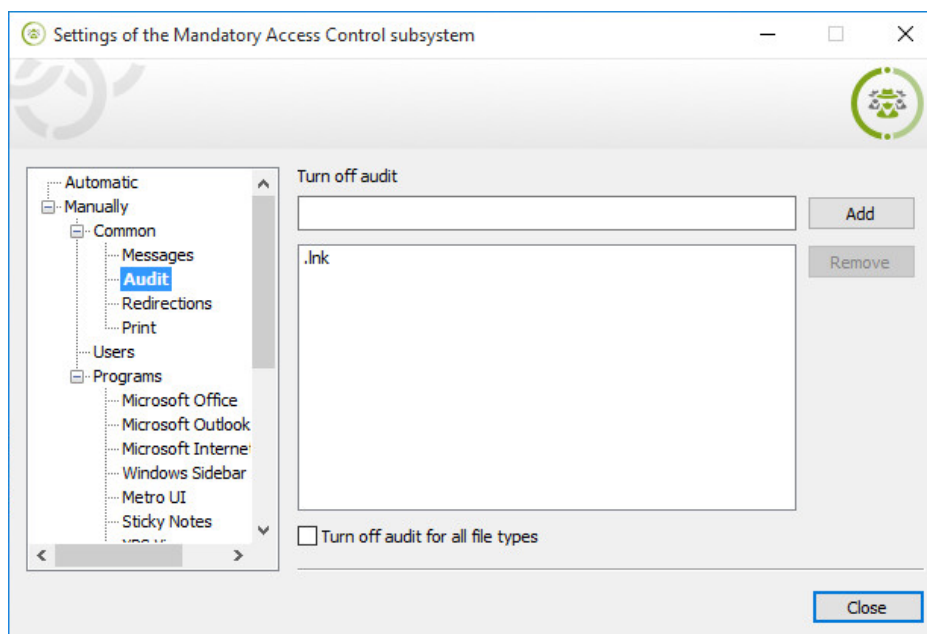
The list of file extensions for which alerts are disabled will be displayed below.

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 the Add button;
 - to remove elements from the list, select them, and click the Remove button;
 - 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 Printer 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, .lnk). Then, click the Add button;
 - to remove elements from the list, select them and click the Remove button;
 - 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 Printer 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, the System 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 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.

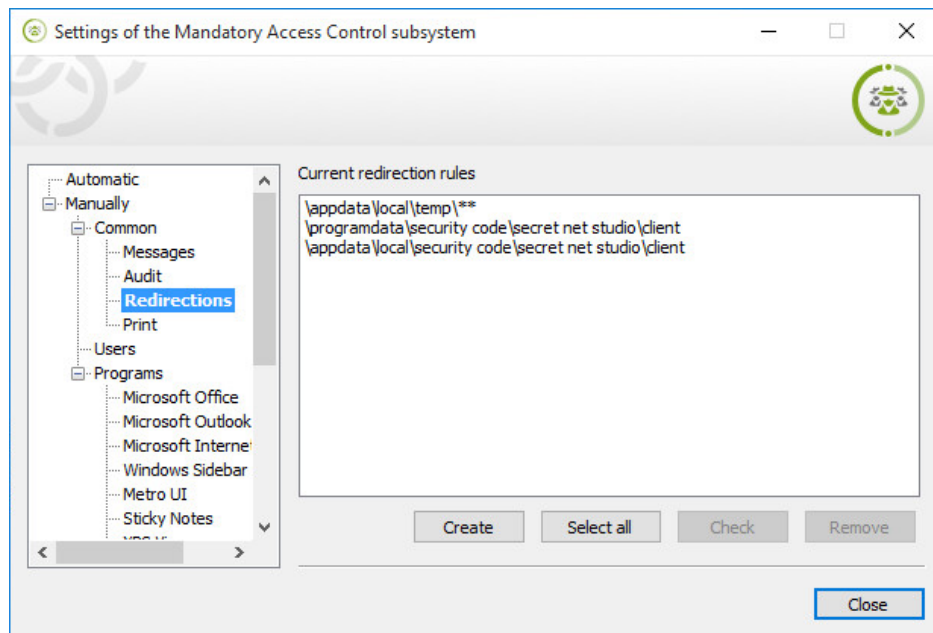
When configuring the file output redirection, a list of paths to folders containing common files is created. For these files, additional folders with various confidentiality categories should be created. These folders will store the files that are used in the sessions with corresponding confidentiality 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 automatic setup of the System (see p. 101), 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 the Create button.

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 the Add button;

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 the Remove button.

3. Click the Create button.

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 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 the "Select All" button).
2. Click the Check button.
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 the "Select All" button).
2. Click the Remove button.

Selected paths will be immediately removed from the list. However, the redirection folders and files contained in them will not be removed.

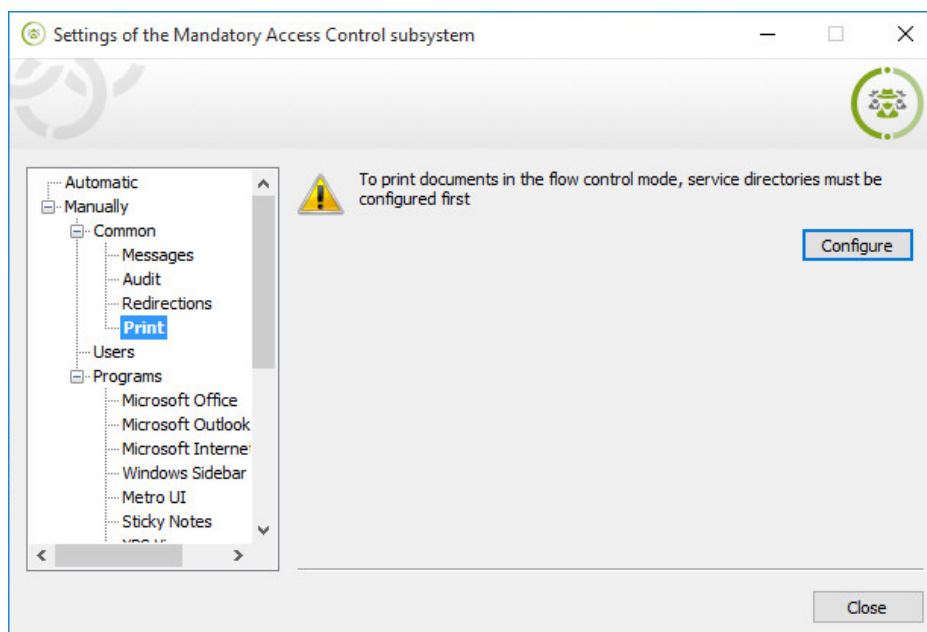
System configuration for printing

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. 101).

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 the Configure button (the button is only active if configuration is not completed).

The system setup process begins. Once the process is complete, a message appears.

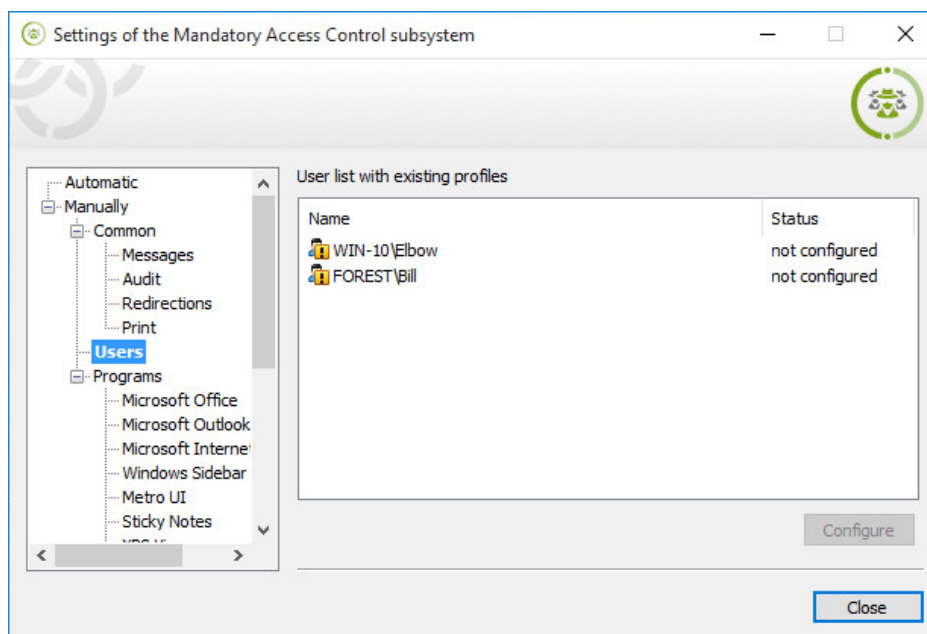
Configuring user account parameters

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 login was performed on that computer at least once.

All user profiles are sufficiently configured during the general automatic configuration process (p. 101). When adding a new user to the System 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 System ensures 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 the Configure button.

The configuration process begins. Once the process is complete, a message appears.

Creating a list of applications for configuration

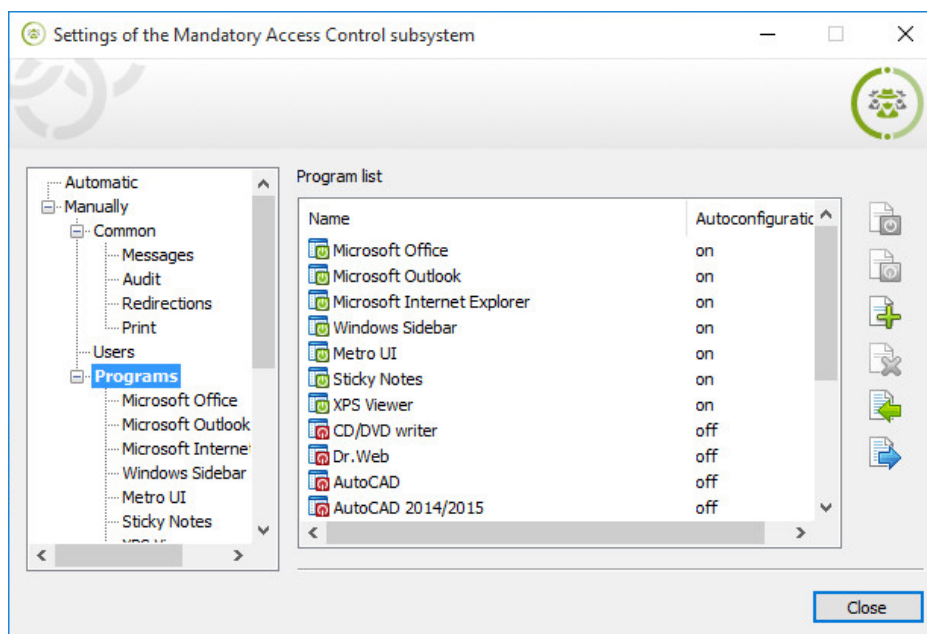
Some applications are not fully compatible with MAC when the flow control mode is enabled. To ensure that these applications work correctly, additional configuration of application-related parameters is required.

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. 101). 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:

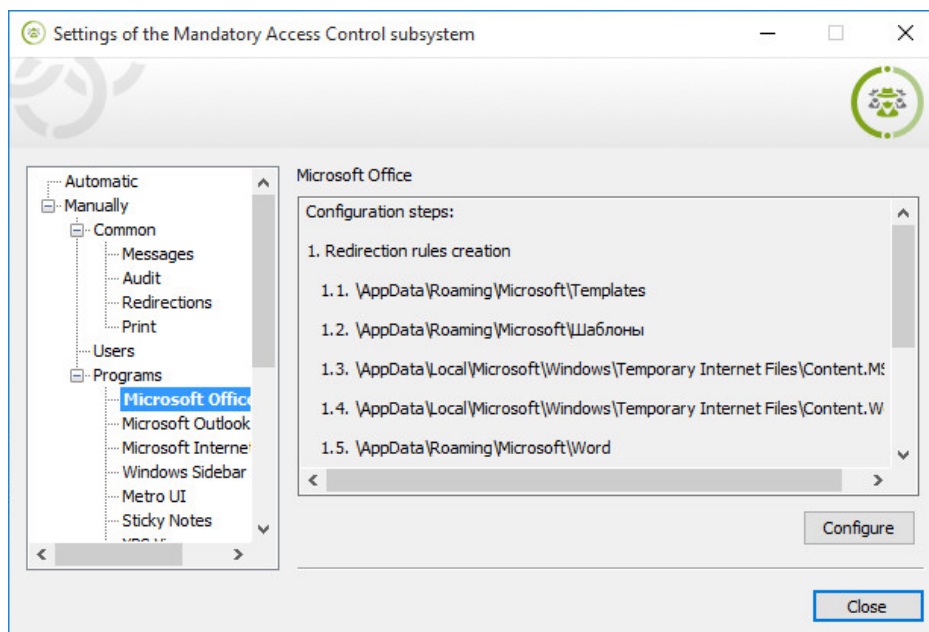
1. Select the application to be removed from the list.
2. Click the Remove button and confirm the action in the dialog box that appears.

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.

Emergency disabling of local disk protection

Standard procedures are provided for disabling the protection of logical partitions (see p. 88). When such procedures cannot be performed, you can use emergency tools for disabling disk protection:

- emergency recovery wizard;
- boot disk for emergency recovery.

Using the emergency recovery wizard

The emergency recovery wizard provides the following options:

- restoring the initial state of the boot section on the physical disk from where the OS is started;
- restoring the initial state of boot sections of protected logical partitions;
- calling a wizard to create the boot disk for emergency recovery.

The emergency recovery wizard can operate regardless of the current status of the Secret Net Studio local disk protection function. To perform procedures, load the key that was used to enable the computer disk protection.



Warning.

We recommend using the emergency recovery wizard only when it is impossible to remove disk protection using standard procedures (see p. 88).

To disable disk protection:

1. Run TblRescue.exe in the setup folder of the Client.
The emergency recovery wizard's dialog box appears.
2. Click Next.
A dialog box for selecting operation mode appears.
3. Leave the "disabling protection for this computer's disks" check box selected and click the Next button.
A dialog box for loading and validating the key appears.
4. To load the key, click the Display button and select the required file in the standard open file dialog box. The file must have the .RK extension.
Once the key is loaded, the wizard dialog box displays the available operations that can be performed using the key.
5. Click Next>.
The program will complete the listed operations. After this, the wizard's closing dialog box appears.
6. Click Done.

To call the wizard for creating the emergency recovery disk:

1. Run TblRescue.exe in the setup folder of the Client.
The emergency recovery wizard's opening dialog box appears.
2. Click Next.
A dialog box for selecting operating mode appears.
3. Select the "create a boot disk for disabling protection in an emergency" check box, and click the Next button.
A dialog box for selecting the key loading option appears.
4. Take the steps described in the procedure for creating the emergency recovery boot disk (see p. 87).

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. [87](#).

**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.

Documentation

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