SECURITY CODE

Secret Net Studio

User manual

© 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

Introduction

This manual is prepared for the users of computers with the Secret Net Studio product software installed (hereinafter "Secret Net Studio, the System"). It contains information on working with Secret Net Studio.

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.

Typical operations

When working on a protected computer, the following operations are frequently performed:

Filling out text fields. If you typed a wrong character when entering your username or password, remove it from the entry line using <Backspace> or <Delete> and enter the correct data.

Password entry. Password characters are not shown directly as they are typed in; instead, either dots or asterisks are displayed. Remember that password entry is both case and language sensitive.

Personal identifier presentation. A personal identifier is a device which is part of what the software and hardware uses for identification and authentication. The personal identifier stores system security data for user. As a rule, the identifier is an electronic key. If a user has been assigned a personal identifier, some operations can be performed only when the identifier is connected or available. Various types of identifiers can be used in the system, and the methods of their presentation may also be different. Instructions on how to use and present the identifier correctly can be obtained from the administrator.

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).

Chapter 1
General information

What you need to know

Before you begin working with a protected computer, we recommend you to read this document to learn basic information about Secret Net Studio and how to use it.

The security administrator plays a key role in managing Secret Net Studio. The security administrator decides which options are available for a user and which security restrictions should be applied in the system.

Users work with resources and perform operations within the scope of their permissions. Unauthorized actions are controlled by Secret Net Studio and depending on a predefined reaction access options may be restricted. Therefore, at the very start, the security administrator should inform you about your privileges when working with a protected computer.

What you need to have

Before working with a protected computer, the IT-administrator must provide you with the following:

1. System login user credentials: username and password.
2. If hardware is required for user identification, you need your personal identifier assigned using Secret Net Studio tools.
3. If the data encryption mechanism with encrypted containers is enabled, you need a device containing key information for access to encrypted containers (a key device). A key device can be a personal identifier assigned to the user (the same as the one used for identification or another one), a floppy disk, memory stick or USB flash drive.
4. In addition, depending on the configuration of Secret Net Studio you may need additional devices or data provided by the administrator in order to work with Secret Net Studio.

Recommendations

Please follow the general recommendations:

1. Remember your username and login password. Make sure your password is not compromised and change it on a regular basis.
2. Do not give your personal identifier or key device to anyone.
3. Please contact the security administrator if you encounter any problems that you cannot fix yourself. For example, if you need additional rights to access resources to efficiently perform your duties.

Chapter 2
Logging in to the System

To begin working with Secret Net Studio, start the computer and log in to the system. Generally, starting the computer protected by Secret Net Studio and logging in to the system do not differ much from the standard procedure. You may need to perform additional steps if the computer is subject to login restrictions.

You can log into the system in different ways depending on the availability of system support for the hardware and personal user identifiers.

The table below lists the different available authentication modes:

Mode	Login method	Application conditions
By name	Standard Windows authentication only (see p. **7**)	For systems with no hardware login control tools
Only by identifier	Only using a personal identifier (see p. **7**)	For systems equipped with the hardware, when all users have personal identifiers
Mixed	Standard Windows authentication or system entry using a personal identifier	For systems equipped with the hardware, when some users have no personal identifiers

A single login mode set for all users of the computer.

The login modes By Name and Mixed allow identification by entering the username manually or by using identification tools activated by Windows features (e.g., Smart Card, eToken, etc.). Information about the use of identifiers in Windows can be found in the operating system documentation. In Only by Identifier mode, you can only use personal identifiers activated by Secret Net Studio tools, but not those activated by Windows features.

If the hardware support feature is used, the administrator issues a personal identifier to each user (depending on the type of tool used, it could be eToken, iKey, Rutoken, ESMART identifiers). If necessary, a computer can be equipped with an additional device for reading data from the personal identifier.

"Presenting" a personal identifier means connecting it to the reading device.

Note.
To access a USB key or smart card memory, you need to enter a special PIN code. By default, the identifier is protected by a default PIN set by the device manufacturer. If the default PIN remains unchanged, the Secret Net Studio system will automatically access the identifier's memory when connected. If the administrator has changed the default PIN to a different one (custom), the system will require the PIN to be entered every time the identifier is connected. The administrator must provide you with the custom PIN when issuing your identifier.

Warning!
Make sure you do not forget your PIN code, otherwise you will not be able to use the identifier.

The personal identifier may also contain user password and key information required for working with encrypted data in encrypted containers.

Login scenarios

To log in, you must enter your usename and password. Once you entered your username and password, the system authenticates you. If the authentication is a success, you will be able to work in the system.

The login procedure begins when the login prompt appears on the screen. Depending on the protection mechanisms and administrator restrictions, the login steps may differ.

Attention!
While the computer is booting up, do not press any keys before the welcome screen (login prompt) appears. Some keys may activate special startup modes requiring administrative permissions. To avoid problems, perform operations in strict compliance with the instructions provided.

Standard login method

To log in using the standard method:

1. Depending on the computer's operating system, prior to login a lock screen appears followed by the welcome screen or login prompt. To begin the login procedure, take one of the following steps:
   - if you are using a Windows 8 or Windows Server 2012 computer, disable the locking screen if it appears (for example, press any key). Check the name of the account that the operating system provides for login. If you need to choose another account, go to the list of users who entered the system (for example, press Esc), and choose the required name or click Another User. A field to enter user credentials appears on the screen;
   - if you are using a Windows 7/Vista or Windows Server 2008 computer, choose the required name or click Another User. A field to enter user credentials appears on the screen.
2. Enter your account data:
   - if necessary, enter the full name of the user or specify the computer or domain name in the User field;
   - Enter your password in the Password field.

   Note.
   For security reasons, password characters are not displayed directly in the entry line. Remember that the password is both case and language sensitive. If you entered incorrect username or password characters, delete them from the entry line using <Backspace> or <Delete> and re-enter the correct data.
3. Click → or OK.

   If the user credentials are entered correctly, the system logs you in.

Login using an identifier

When logging in using a personal identifier activated by Secret Net Studio, the system will automatically detect the name of the user the identifier is assigned to.

To log in using the identifier:

1. Before login, depending on the computer's operating system, a lock screen appears followed by the welcome screen or login prompt. The system is ready to read data from the identifier. Present your own personal identifier.

   Note.
   If the identifier is protected by a custom PIN, a prompt appears. Enter the PIN and click OK.
2. The response of the System depends on the user password information contained in the personal identifier. The following scenarios are possible:
   - the identifier contains the user's current password;
   - the identifier does not contain a password or contains a password different from the user's password (for example, the password has expired or was changed but not saved to the personal identifier).

Situation 1	**If the identifier contains the current password,** the user will log in to the system without being asked to enter the password after a successful check of the user's rights
Situation 2	**If the identifier does not contain a password or contains another password,** a dialog for entering user account details will appear displaying the name of the user who owns the presented identifier

Enter the current password in the Password field and click → or OK.

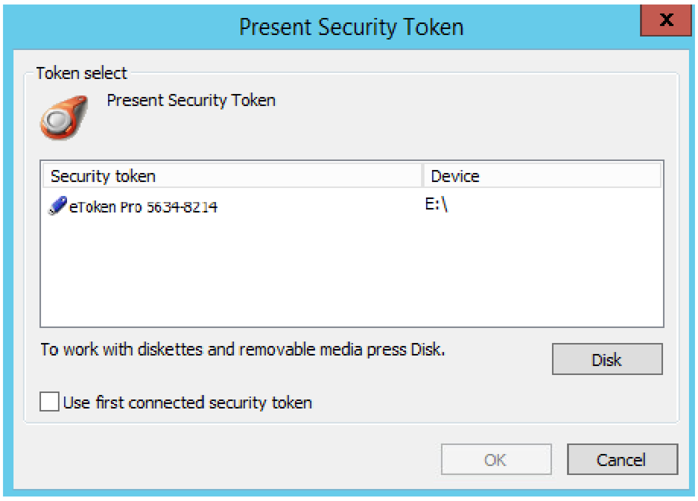
Note.
For security reasons, password characters are not displayed directly in the entry line. Remember that the password is both case and language sensitive.

If the password you entered is correct and **no** password is saved in the identifier, the system logs you in.

If the password you entered is correct and it should be saved to the identifier instead of an old password, a prompt appears. In this case, perform the following steps:

- Click Yes in the prompt box.

  A dialog box appears on the screen listing the identifiers where you can save the new password.



Present Security Token

Token select

Present Security Token

Security token	Device
eToken Pro 5634-8214	E:\

To work with diskettes and removable media press Disk.

□ Use first connected security token

- To save the password, present the identifiers one by one.

  Note.
  If the identifier is protected by a custom PIN, a prompt appears. Enter the PIN and click OK.

  Once your new password is successfully saved to the identifier, its status in the list changes to Processed. After this, you can remove the identifier from the reader.

- Once all identifiers are processed, click Cancel.

The dialog box closes and the system logs you in.

Specific login features when advanced authentication mode is enabled

Secret Net Studio system provides the following user authentication modes:

Mode	Description
Standard authentication	During user login, the standard Windows authentication procedure is performed
Advanced password-based authentication	Apart from the standard Windows authentication, additional system authentication using the user's password is performed Secret Net Studio

For advanced password-based authentication, the password must be saved in the Secret Net Studio system database in order to perform the check. The password is automatically saved when changed by the administrator or the user. However, password mismatch situations may occur when the current and saved password are different. In this case, the system asks for password synchronization.

Login when mandatory access control is enabled

If the Mandatory Access Control mechanism is enabled (see p. **17**), user permissions are also checked during login. Login restrictions are set in the following cases:

- a confidentiality category is assigned to devices connected to the computer;
- confidential information flow control mode is enabled.

Login when devices with a confidentiality category are used

The administrator can assign confidentiality categories to certain devices. If a user logs in when devices with assigned confidentiality categories are connected to the computer, the user access level and device categories are checked. If a device with a confidentiality category higher than your access level is detected, the device will not be available.

Login when flow control mode is enabled

If the confidential data flow control mode is enabled in the Mandatory Access Control subsystem, a dialog box asking you to select the session's confidentiality level appears after a successful check of the user's login rights.

When selecting the confidentiality level, you inform the system of the confidentiality category of the documents you are going to work with during the current session.

If the flow control mode is enabled, a stricter scan for devices with assigned confidentiality categories is conducted. System login is prohibited in the following cases:

- devices with a confidentiality category higher than the session confidentiality level are found;
- devices with different confidentiality categories are found;
- when logging in to the system for configuration purposes, devices with a confidentiality category higher than non-confidential are found .

> **Note.**
> System login for configuration purposes is required only once, after you create or rename a user account. Such a login must be performed during a non-confidential session.

For details about working with the System when mandatory access control is enabled, see p. **18**.

What to do if you encounter a problem

If login rules are violated, the System interrupts the login procedure. The System and Windows OS messages that are displayed in the case of incorrect user behavior or system failures during login are shown below.

```
Incorrect user behavior.
Incorrect username or password.
```

Reason. The username is not found in the system database or an incorrect password is entered.

User actions. Check if the Caps Lock key is not activated and switch the keyboard layout (Esp/Eng).

If an error occurs, re-enter your username and password. The administrator can limit the number of password entry attempts. If the attempt limit is exceeded, the System will display a respective message and lock the computer. In this case, contact your administrator.

If you forget your password, contact your administrator.

```
Access to the system is not allowed. Secret Net Studio
authentication error. Incorrect password or username.
```

Reason. Advanced password-based authentication mode is enabled. The entered password must be the same as the password stored in the Secret Net Studio database. The entered account details differ from the saved values.

User actions. Make sure the entered account data is correct (see above) and, if necessary, re-enter the correct data.

If the username and password were entered correctly, the situation may be caused by a password mismatch. This means that an old password is stored in the Secret Net Studio database that was not updated when the password was changed. In this case, enter your old password. The Password Entry dialog box appears asking you to enter a new password. To log in and synchronize the passwords, enter your new password and make sure the Synchronize Passwords check box is selected.

```
The identifier's password differs from the current password.
Do you want to save your current password to the identifier?
```

Reason. The personal identifier's password is different from the system password.

User actions. You can update the password in the identifiers (see p. **13**) or do it later. We recommend you to update the password immediately.

```
The personal identifier of this user is not registered on
this computer.
Incorrect data format in the personal identifier.
Incorrect password stored in your identifier.
Incorrect personal identifier PIN entered.
```

Reason. During login, an identifier was connected that does not belong to the entering user, or it does not contain the required information.

The identifier may be broken or there was a data reading error involving the identifier.

User actions. Repeat the login procedure by connecting the correct identifier. Make sure your personal identifier is correctly connected to the reading device.

If the error persists, contact the administrator.

```
Password has expired.
```

Reason. An expired password has been entered during login. This is a warning.

User actions. Close the message box and change the password (see p. **13**).

```
Domain controller not found.
Failure establishing trust relationship between domains.
System error during user authentication.
Local authentication error.
```

Reason. The information required for login is entered correctly, but login is impossible because of missing network components, network interaction problems or other system errors.

User actions. Contact your system administrator to find out why the required network components are missing and try to log in again when the problem is fixed.

Sometimes, a computer can only be used in stand-alone mode, without any access to network resources. Click OK to continue working in the stand-alone mode.

```
Access to the system is not allowed. You have no access to
the devices connected to the system: <list of devices with
descriptions>. To log in, disconnect devices that are
unavailable for you.
```

Reason. The confidentiality category of some devices connected to the computer is higher than your access level.

User actions. Disconnect the devices. If you need to remove a device restriction, contact the administrator.

```
Access to the system is not allowed. Conflict of device
confidentiality categories: <list of devices with
descriptions>. To log in, disconnect the conflicting devices.
```

Reason. Devices with different confidentiality categories are connected to the computer. This is not allowed when working in the flow control mode.

User actions. Disconnect devices with an assigned confidentiality category different from the session's confidentiality category.

```
The following devices are connected to the system:
<description of devices>. Login is only possible using a
<device confidentiality category> level. Continue?
```

Reason. A confidentiality category is assigned to devices connected to the computer. When working in the control flow, the privacy mode session level should match this category.

User actions. Continue the operation to open a session with the same confidentiality level as the devices' category. If you need to open a session with a different confidentiality level, disconnect the devices.

```
Access to the system is not allowed. You are logging in to
the computer for configuration purposes. A session with the
lowest confidentiality level should be used. Connected
devices: <list of devices with descriptions>. To log in,
disconnect devices that are assigned an elevated
confidentiality category.
```

Reason. You are using a new account to log in. When working in the flow control mode, use a non-confidential session to log in with this account. It is impossible to log in because devices are connected to the computer that are assigned a confidentiality category other than non-confidential.

User actions. Disconnect the devices and log into a non-confidential session. Once you have logged in, close the current user session, log out and re-connect the devices. Next time you log in, you will be able to open a session with the same confidentiality level as the devices.

```
The computer is locked by the security system. Locking
reasons: <information on reasons>.
Contact the administrator to unlock the computer.
```

Reason. Computers may be locked by the Secret Net Studio system for the following reasons: violations related to the integrity control of protected objects, hardware configuration changes, functional control errors, etc.

User actions. The computer can be unlocked only by the administrator. Contact the administrator.

Chapter 3
Using basic protection tools

Temporary computer locking

If you need to stop working on your computer for a while, you do not have to power off your computer to protect yourself against unauthorized use. You can temporarily lock your computer's keyboard and screen.

You can temporarily lock your computer using one of the following methods:

- using the keyboard;
- using the identifier connected during login.

Before you enable the lock mode, we recommend you to save any changes made to open documents.

Note.
The computer may enter the temporary lock mode automatically if the mouse or keyboard are not used for a certain time. This period is called the inactivity interval. Automatic locking is activated in the standard Windows way.

To enable locking using the standard method:

1. Press <Ctrl>+<Alt>+<Del>.
2. In the standard dialog box that appears, click Lock (Lock Computer).

To lock the computer using an identifier:

1. Switch the computer to the general operating mode with the desktop and task bar displayed on the screen.
2. Eject the identifier that was connected for login from the reader.

   Note.
   The computer will be locked when ejecting the identifier if the security administrator has enabled the appropriate response for the computer. The locking function applies during a local user session if the identifier was enabled by Secret Net Studio and the user connected this identifier for login.

Unlocking the computer

A user working with a computer or the security administrator can unlock a computer that is temporarily locked.

Unlocking the computer using the standard procedure:

1. Depending on the operating system running on your computer, do the following:
   - if you are using a Windows 8 or Windows Server 2012 computer, disable the locking screen (for example, press any key). The locked session username and password entry field appears;
   - if you are using a Windows 7/Vista or Windows Server 2008 computer, choose the locked session user account. The password entry field appears.
2. Enter the password and click → or OK.

Unlocking the computer using an identifier:

1. Connect the identifier. If the identifier remained connected to the reader after the lock mode was enabled, remove the identifier and re-connect it to the reader.

   If the identifier contains your password, the computer will be unlocked. If the password is missing, the user credentials entry dialog box with the current username will appear.
2. Enter the current password in the Password field and click → or OK.

Password change

To change the password:

1. Press <Ctrl>+<Alt>+<Del>.

A screen with the commands appears.

2. Click Change a Password.

If the current password policy does not permit you to change the password, en error message will appear and the procedure will be interrupted. In this case, contact your administrator to change the password.

If you are allowed to change the password, the respective dialog box appears.

3. If necessary, change the input language (the current language is displayed on the Windows taskbar, in the notification area) and complete the dialog box fields:

- in the Old Password field, enter your current password;
- in the New Password field, enter your new password;
- in the Confirm Password field, re-enter the new password.

> **Note.**
> For security reasons, password characters are not displayed directly in the entry field. Remember that the password is both case and language sensitive.

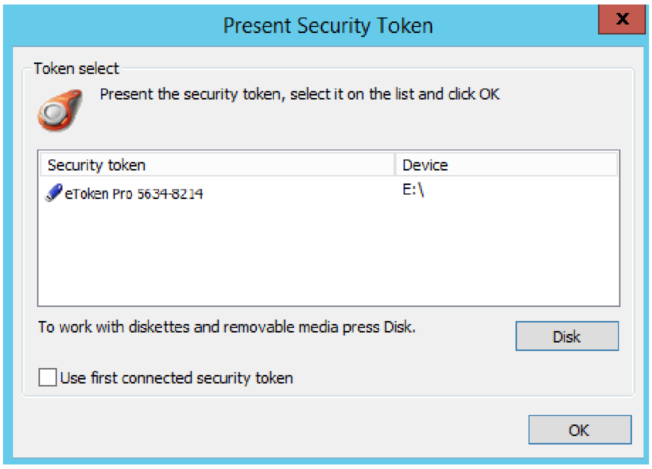
4. Click → or OK.

> **Note.**
> If the password does not comply with system requirements or you have entered the old password incorrectly, an error message appears. Click OK in the message box and re-enter the passwords correctly.

If the "Change a password dialog box" fields are completed correctly, a message notifying that the password is changed appears.

5. Click OK.

If your old password is stored in a personal identifier, a dialog box with a list of your personal identifiers appears, as in the figure below.



Present Security Token

Token select

Present the security token, select it on the list and click OK

Security token	Device
eToken Pro 5634-8214	E:\

To work with diskettes and removable media press Disk.

□ Use first connected security token

6. To change your password, connect each identifier one by one.

> **Note.**
> If the identifier is protected by a custom PIN, a dialog box appears. Enter the PIN and click OK.

Once your new password is successfully saved to the identifier, its status in the list changes to Processed. After this, you can remove the identifier.

7. Once you finished, click OK.

Local alert notifications

Secret Net Studio can notify a computer user about events that may be attributed to unauthorized access (to a computer, resources, etc.). These events are classified as alerts with the appropriate severity level. A sound signal and a warning message appear for a short time to indicate a local alert.

The administrator can decide whether to enable or disable local alerts or pass control over to users.

To enable or disable local notifications:

- On the Windows taskbar, right-click the Secret Net Studio icon in the Notification area and click Alert Notifications. If there is a checkmark to the left of the command, then alert notifications are enabled.

Note.
If the administrator has enabled or disabled local alerts for all computer users, the user cannot change the status.

Chapter 4
Using local protection tools

Discretionary access control over file resources

Discretionary access is based on granting access rights and privileges to users.

To isolate access to folders and files on local drives, a mechanism for discretionary access control over file system resources is used.

The administrator can permit or restrict operations with certain file system resources. Access isolation options depend on the resource type. No full or partial user access isolation is applied to specific-use resources or those required for the computer's operation. For example, it is impossible to modify access permissions for a root folder of a system drive or the entire system folder.

Changing access rights for folder and files

If the Discretionary Access Control mechanism is enabled for file system resources, the access rights controlled by Secret Net Studio are applied to folders and files on the computer's local disks. Access rights permit or prohibit certain operations with resources: reading, recording, execution, deletion and modifying access rights.

Rights can be assigned expressly or inherited from a higher file system hierarchy element. Expressly assigned rights have a higher priority compared to inherited rights.

Note.
Access right inheritance mode is strictly enforced for a resource when moving it to another logical partition. In this case, even if access rights were expressly assigned to the resource in its initial location, access rights from a higher hierarchy element will be applied because inheritance mode is enabled. When copying a resource (in the same or another logical partition), the rights inheritance mode is enabled for the created copy of the resource.

By default, all users have permission to access any resources for reading, writing, execution and deletion. The following user categories are allowed to change access rights for resources:

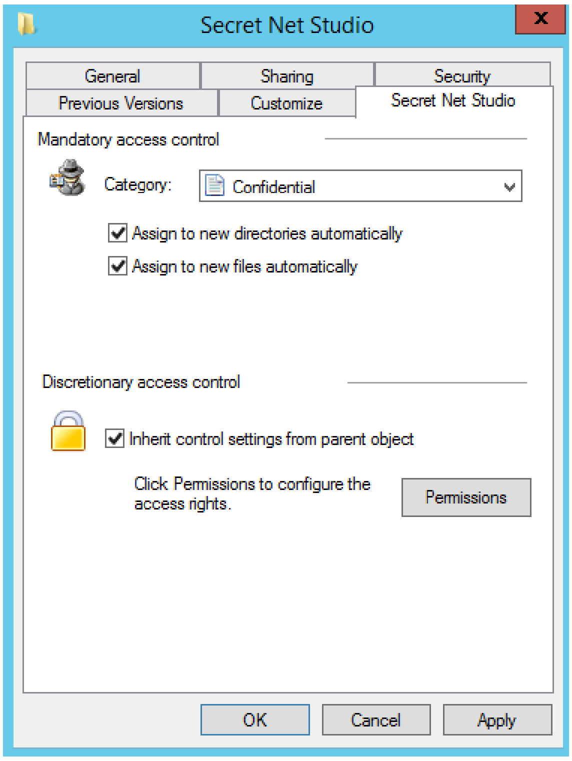
- security administrators or authorized employees granted the Access Rights Management privilege; this privilege makes it possible to change access rights for all resources (irrespective of the access rights assigned to the resources);
- resourse administrators or users with permission to change access rights for this resource.

The user with the Access Rights Management privilege performs the initial assignment of resource administrators. Then the resource administrators manage access rights for all respective resources by permitting or prohibiting the execution of operations by other users.

This procedure uses Windows OS Explorer.

To change access rights to a resource:

1. Right-click a folder or a file and click Properties. In the Properties window select the Secret Net Studio tab.



Mandatory access control

Category: Confidential

☑ Assign to new directories automatically

☑ Assign to new files automatically

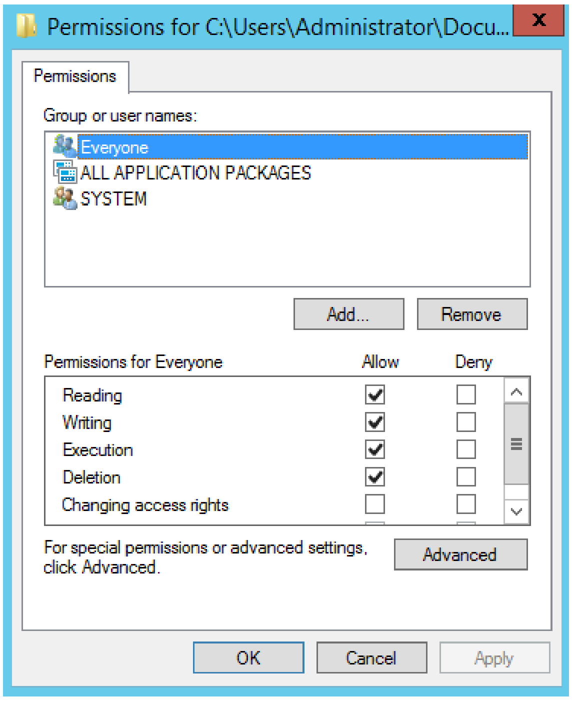
Discretionary access control

☑ Inherit control settings from parent object

Click Permissions to configure the access rights.

2. If the "Inherit control settings from parent object" check box is selected (i.e. right inheritance mode is enabled for the resource), clear this check box to expressly assign access rights. Click Permissions if the check box is not selected or if you need to view the inherited access rights.

   The "Permissions..." Windows OS dialog box appears. This dialog box operates in the same way as other standard Windows tools.



Group or user names:

Everyone
ALL APPLICATION PACKAGES
SYSTEM

Permissions for Everyone	Allow	Deny
Reading	☑	□
Writing	☑	□
Execution	☑	□
Deletion	☑	□
Changing access rights	□	□

For special permissions or advanced settings, click Advanced.

3. If necessary, edit the list of accounts in the upper part of the dialog box using Add and Remove.

4. To modify access parameters, select the required account in the list and assign permissions and prohibitions for the execution of operations. If you need more information (for example, about the source of the inherited parameters) or if you want to set up special parameters (including audit parameters for the resource's

operations), click Advanced and perform the required steps in the Windows security parameters window.

5. Once the setup is complete, click OK.

Data wiping

When you delete files, some data may be left on storage devices in the memory areas that are occupied by these files. Secret Net Studio implements the mechanism for wiping the deleted information. This mechanism makes it impossible to recover and reuse data after it is deleted.

The security administrator can enable automatic data wiping for files that are deleted on local and/or removable disks. Automatic data wiping occurs when you run the standard commands to delete the files in the operating system. In particular, this happens when you empty the Recycle Bin (the files in the Recycle Bin folder are not considered deleted) or if you delete the selected objects by using <Shift> + <Delete>.

In addition, you may be permitted to selectively delete files by wiping data.

To selectively delete the files by wiping data:

1. In Explorer, select the file objects to delete (files and/or folders), right-click menu for one of the selected objects and select Delete Permanently.

   Note.
   This command is only available if the security administrator has set a non-zero number of data overwriting cycles for deleting file objects as selected by the user.

   A dialog box appears asking you to confirm the operation.

2. Click Yes.

Application Execution Control

When the application execution control module is enabled, the administrator can define a list of permitted programs for each user. When starting a program not included in the list, alerts are logged as unauthorized access attempts (UA). Application execution control can be used in hard-mode and soft-mode operation modes.

The hard mode of application execution control means that the user can only work with programs included in the list of permitted programs. The system will block other programs starting warning the user that access to a device or file is denied.

If you need to expand the list of permitted programs, contact the security administrator entitled to grant users access to information system resources.

In the soft mode of application execution control, the System does not block the start programs that are not included in the list of permitted software. The soft mode of application execution control is used at the Secret Net Studio system implementation stage in order to collect information about the programs users work with.

Mandatory access control

The mandatory access control mechanism:

- restricts user access to information with an assigned confidentiality category (confidential information);
- controls the connection and use of devices with assigned confidentiality categories;
- controls confidential data flows in the system;
- controls the use of network interfaces where acceptable user session confidentiality levels are assigned;
- controls confidential document printing.

By default, the system provides the following confidentiality categories: non-confidential (for public information), confidential and strictly confidential. If necessary, more categories can be added with different names in accordance with your company standards.

If a user (or a program started by a user) attempts to access a resource, the user's access level is compared to the resource's confidentiality category. Access to the resource is granted if its confidentiality category is not higher than the user's access level.

Flow control mode

The Mandatory Access Control subsystem may operate in flow control mode, which ensures strict compliance with mandatory access isolation principles and prevents the unauthorized copying or moving of confidential data.

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 (see p. **9**).

Confidential resource policy rules

The mandatory restriction of user access to resources with assigned confidentiality categories is based on the following approach:

- folders, files and devices are assigned confidentiality categories (by default, the following categories are used in the System: non-confidential, confidential, and strictly confidential);
- each user is assigned one of the available levels of access to confidential information. The set of access levels used in the System is the same as the set of confidentiality categories for resources;
- 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 granted the "confidential" access level can only work with confidential and non-confidential files.

The table below lists the Mandatory Access Control mechanism operation rules applied when the confidential data flow control mode is enabled or disabled.

Disabled flow control	**Enabled flow control**
Access to devices	
User access to the system is not allowed if connected devices have a confidentiality category higher than the user's access level	User access to the system is not allowed if the following devices are connected: • devices with a confidentiality category higher than the user'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	

<table>
<tr><th>Disabled flow control</th><th>Enabled flow control</th></tr>
<tr><td>Users can access the file if their access level is not lower than the file's confidentiality category</td><td>Users can access the file if the user session confidentiality level is not lower than the file's confidentiality category</td></tr>
<tr><td>It is not permitted to delete a confidential file to the Recycle Bin</td><td>It is not permitted to delete any file to the Recycle Bin</td></tr>
<tr><td colspan="2"><b>Access to folders</b></td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td colspan="2">Access to a folder is prohibited if its confidentiality category is higher than the category assigned to the folder-containing device</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td>It is not permitted to delete a confidential folder to the Recycle Bin</td><td>It is not permitted to delete any folder to the Recycle Bin</td></tr>
<tr><td colspan="2"><b>Inheriting the folder's confidentiality category</b></td></tr>
<tr><td>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</td><td>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</td></tr>
<tr><td>If automatic confidentiality category assignment mode is disabled:
• when creating, saving, or copying a subfolder/file, it is assigned non-confidential category;
• when moving a subfolder/file within a logical partition, it retains its confidentiality category (the file can be moved if its confidentiality category is not higher than the confidentiality category of the upper-level folder). The appropriate user privilege is required to move subfolders.</td><td>If automatic confidentiality category assignment mode is disabled:
• when creating, saving, or copying a subfolder/file, it is assigned the same category as the session's confidentiality level, but not higher than the folder's confidentiality category;
• when moving a subfolder/file within a logical partition, it retains its confidentiality category (the subfolder/file can be moved if its confidentiality category is not higher than the folder's confidentiality category or the session's confidentiality category)</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2"><b>Working with applications</b></td></tr>
<tr><td>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</td><td>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)</td></tr>
</table>

<table>
<tr><th>Disabled flow control</th><th>Enabled flow control</th></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2"><b>Changing the confidentiality category of a resource</b></td></tr>
<tr><td>A user who is <b>not</b> 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)</td><td>A user who is <b>not</b> 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)</td></tr>
<tr><td>A user granted the Confidential Category Management privilege can:
• 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</td><td>A user granted the Confidential Category Management privilege can:
• 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</td></tr>
<tr><td colspan="2"><b>Printing confidential documents</b></td></tr>
<tr><td>If the Printer Control mechanism is enabled:
• a user <b>not</b> 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</td><td>If the Printer Control mechanism is enabled:
• a user <b>not</b> 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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2"><b>Output to external media</b></td></tr>
<tr><td>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</td><td>A user <b>not</b> 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.</td></tr>
</table>

Confidential resource management

Access to confidential file content is granted to a user if the file's confidentiality category is not higher than the user's access level. At the same time, the confidentiality category of the device where the file is located is also analyzed and has a higher priority compared to the file confidentiality category. If the file's category is lower than the confidentiality level of the device, the System considers the file's category the same as the device's category. When the file's category is higher than the device's confidentiality category, the situation is considered invalid, and access to the file is not granted.

Access levels for users and confidentiality categories for devices are assigned by the administrator. The user can change folder and file categories within the scope of granted permissions.

Changing confidentiality categories of folders and files

To change the confidentiality category of a folder or file, you need the Confidentiality Category Management privilege. If you are not granted the privilege, you can only elevate categories for files within your own access level or the session's confidentiality level (however, you can still elevate the confidentiality category of a file if its confidentiality category is lower than the folder's category).

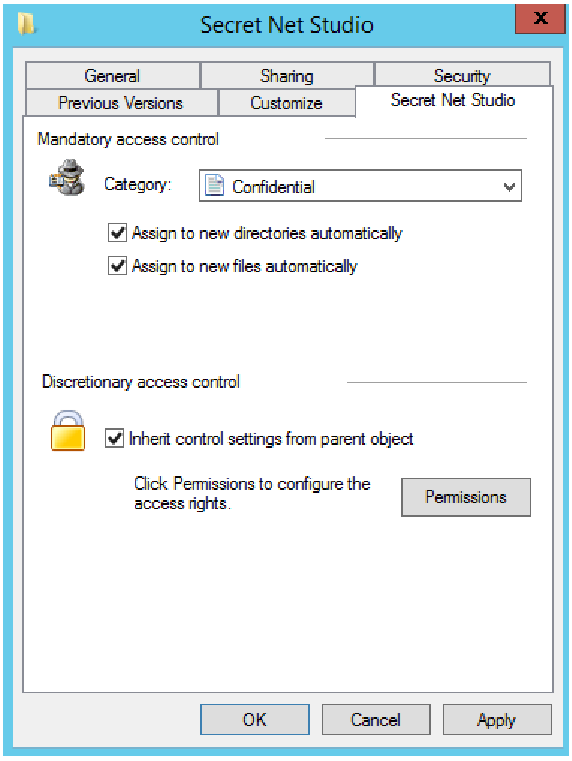
Attention! Note the following general recommendations:

- confidentiality categories other than the lowest category (by default "non-confidential") should not be assigned to system folders, folders containing application software, or to My Documents folders or other similar catalogs;
- to avoid the accidental elevation of file confidentiality categories, store them in files 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.

This procedure uses Windows OS Explorer.

To change the confidentiality category of a folder:

1. Right-click the folder (group of selected folders) and click Properties. In the Properties window select Secret Net Studio tab.



Category: Confidential

☑ Assign to new directories automatically

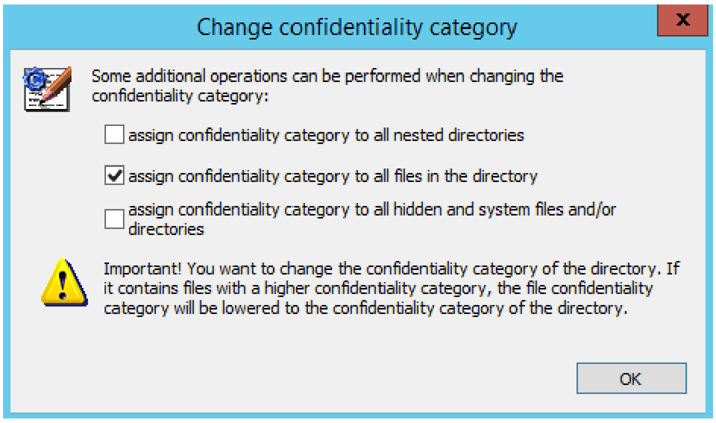
☑ Assign to new files automatically

☑ Inherit control settings from parent object

Click Permissions to configure the access rights.

2. Configure the required parameter values:
   - Select the required confidentiality category in "Category" drop-down list box.
   - If you want the selected category to be assigned automatically to any created subfolders and/or files in the future, select the "Assign to new directories automatically" and/or "Assign to new files automatically" check boxes respectively.
3. Click OK.

   If there a folder contains files or subfolders, a dialog box appears asking you to change the confidentiality category of the files and subfolders:



Change confidentiality category

Some additional operations can be performed when changing the confidentiality category:

□ assign confidentiality category to all nested directories

☑ assign confidentiality category to all files in the directory

□ assign confidentiality category to all hidden and system files and/or directories

Important! You want to change the confidentiality category of the directory. If it contains files with a higher confidentiality category, the file confidentiality category will be lowered to the confidentiality category of the directory.

- If you need to assign a selected confidentiality category to subfolders and also change the status of "Assign to new directories automatically" and "Assign to new files automatically" parameters, select the "assign confidentiality category to all nested directories" check box.
- If you need to assign the confidentiality category assigned to a folder to all files in the folder (except for hidden and system files), select the "assign confidentiality category to all files in the directory" check box. If the first field is checked, this category will also be assigned to the files in subfolders.
- If you also need the confidentiality category to be assigned to hidden and system files, select the "assign confidentiality category to hidden and system files" check box.

Attention!

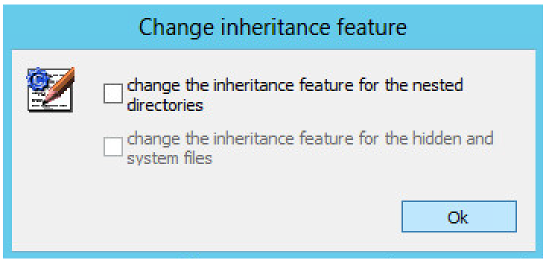
To avoid system failures, we recommend you not to assign a confidentiality category to hidden or system files that is not the lowest one (by default "non-confidential"), unless it is absolutely necessary.

- Click OK.

Comment.

If a catalog or subfolder contains files with a higher confidentiality category than the one assigned to the catalog, such files will be automatically assigned the same lower confidentiality category that is assigned to the catalog.

If the value of the "Assign to new directories automatically" or "Assign to new files automatically" parameter is changed for a catalog containing subfolders, the catalog's confidentiality category remains the same and the following dialog box appears:



Change inheritance feature

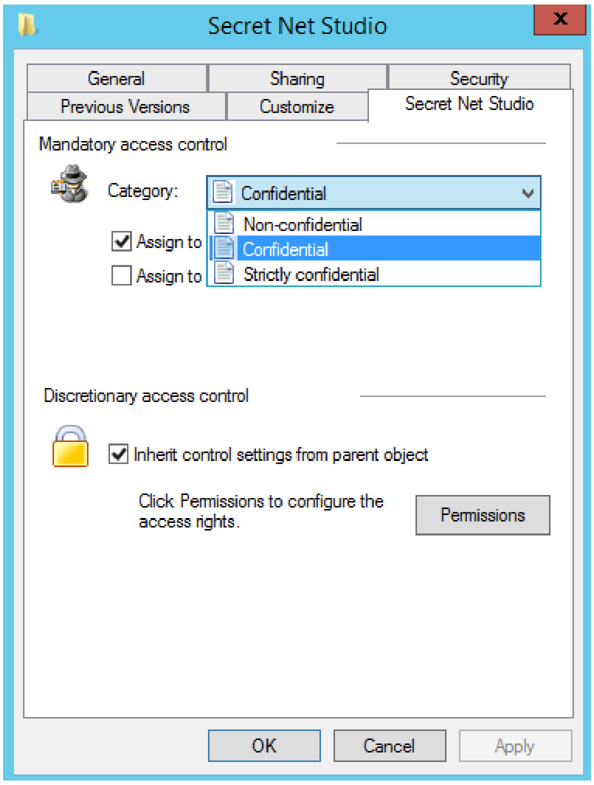
□ change the inheritance feature for the nested directories

□ change the inheritance feature for the hidden and system files

- If you need to change the status of subfolder parameters "Assign to new directories automatically"and "Assign to new files automatically", select the "change the inheritance feature for the nested directories" check box.
- If you also need to change the status of subfolder parameters for "Assign to new directories automatically" and "Assign to new files automatically" for hidden and system files, select the "change the inheritance feature for the hidden and system filed" check box.
- Click OK.

To change the confidentiality category of files:

1. Right-click the file (group of selected files) and click Properties. In the Properties window select Secret Net Studio tab.



Mandatory access control

Category: Confidential

☑ Assign to

☐ Assign to

Discretionary access control

☑ Inherit control settings from parent object

Click Permissions to configure the access rights.

2. Choose the required confidentiality category of the file(s) in the "Category" drop-down list box.
3. Click OK.

Working with a confidential document

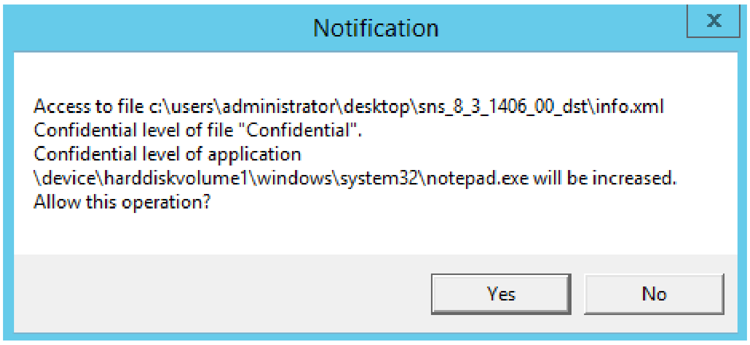
Before you begin working with confidential documents in an editor (for example, MS Word), we recommend you to save and close all previously opened non-confidential documents.

Opening a document

To open a confidential document:

1. Start the document editor program.
2. Select Open File in the program and select the confidential document in the standard Open Document dialog box.

   If the confidential information flow control is off, the following message appears:



Access to file c:\users\administrator\desktop\sns_8_3_1406_00_dst\info.xml
Confidential level of file "Confidential".
Confidential level of application
\device\harddiskvolume1\windows\system32\notepad.exe will be increased.
Allow this operation?

This notification is displayed every time a document is opened with a confidentiality category higher than the application's category.

3. Click Yes to open the document.

Saving a document

When saving a confidential document with the same or different name, keep in mind that the document file's confidentiality category will always remain the same if the document is saved to a folder where the confidentiality category is the same as the category of the document, and the "Assign to new files automatically" mode is enabled for the folder.

Attention!

In order to retain the document's confidentiality category, we recommend you to save it to a folder with a confidentiality category not lower than the document's category. Otherwise, the following situations may occur:

- if the document is saved to a folder with a lower confidentiality category and the "Assign to new files automatically" mode is enabled for the folder, the document's confidentiality category will be lowered to the folder's confidentiality category;
- if the document is saved to a non-confidential folder or to a confidential folder where the "Assign to new files automatically" mode is disabled, the document file will be assigned the non-confidential category.

Printer control

Printing a document with a Secret Net Studio marker

If the Document Marking mode is enabled, special markers with specified information about the document will be automatically added while printing.

The marker is a set of data fields that can be added to each page of the document (above or below the text), as well as at the end of a printed document. Default system markers can be configured in accordance with your company's requirements.

The following types of fields are used in markers:

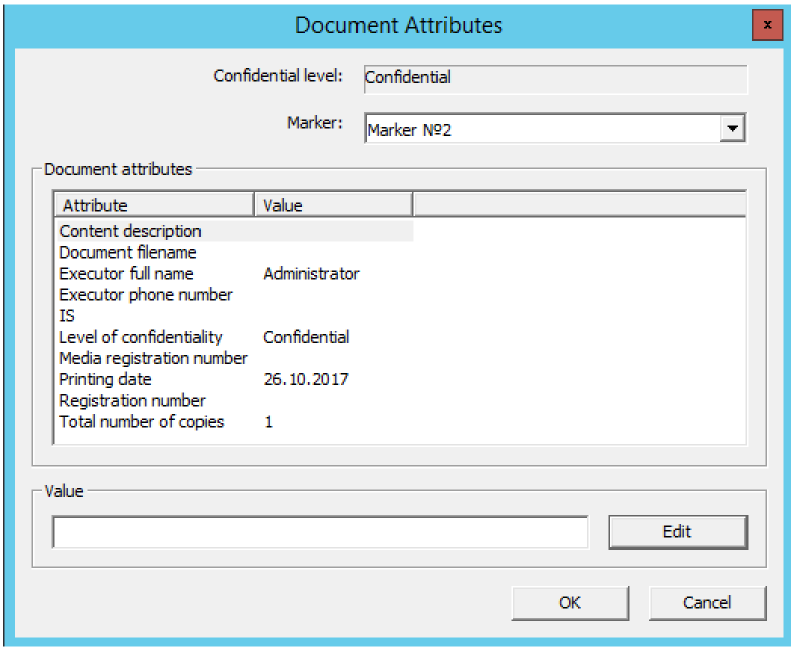
- mandatory fields that are automatically filled out by the System (for example, Data, File);
- custom fields to be filled out by the user prior to printing the document (for example, Record Number).

To print a document with a marker:

1. Open the document in an editor.
2. Click the print document command in the program.

   The standard print setup dialog box appears.
3. Configure the parameters and click Print.

   The Document Attributes dialog box appears, as shown in the figure below.



Confidential level: Confidential

Marker: Marker №2

Document attributes

Attribute	Value
Content description	
Document filename	
Executor full name	Administrator
Executor phone number	
IS	
Level of confidentiality	Confidential
Media registration number	
Printing date	26.10.2017
Registration number	
Total number of copies	1

Value

4. If necessary, change the current marker by selecting the required one in the Marker drop-down list box. Then, set the values for the editable marker fields. To change the values, select the required attribute in the list, enter the required value in the field below and Edit.
5. Click OK.

   The document will now be printed with the marker.

Working with cryptographic keys

A user's key information is located on a key device: a personal identifier, key floppy disk or other removable device (for example, a USB flash drive). It is required to work with encrypted data in encrypted containers.

The period of key information validity is set by the administrator. At some point before its expiration, the user will be prompted to change the key information. When the period expires, the key becomes invalid and you will **not** be able to use it. If you need to resume work with key information, it must be changed. This operation is performed by each user individually.

Loading and unloading an encrypted key

Encrypted user keys are loaded automatically or forced by a user command. They are automatically loaded during user login if an identifier is used where encrypted keys are also stored. Loading is forced by using the command in the context menu of the Secret Net Studio icon in the system area of the Windows task bar.

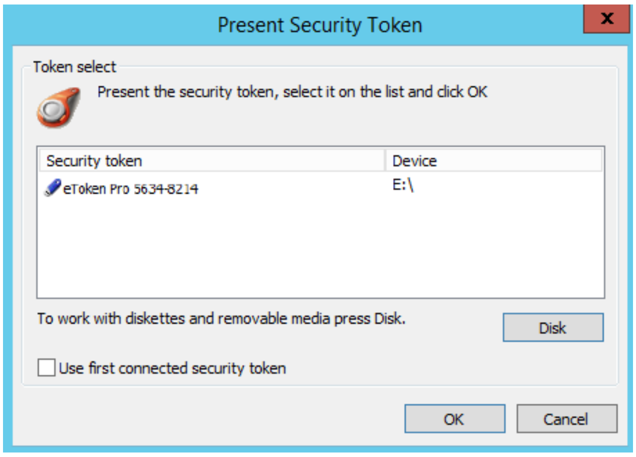
To unload keys, you can also use a special command or let the system do it automatically after you finish your session.

To force encrypted key loading:

1. Right-click the Secret Net Studio icon in the system area of the Windows task bar and select Load Keys.

   > **Note.**
   > This command is available if there are currently no loaded keys.

   The following dialog box appears:



Present the security token, select it on the list and click OK

Security token	Device
eToken Pro 5634-8214	E:\

To work with diskettes and removable media press Disk.

☐ Use first connected security token

2. Present the key device. Depending on the key device type (a personal identifier or a removable device), perform the appropriate step:
   - if you are using a personal identifier, present it;
   - if you are using a removable disk as the key device, present it and click Disk.

     Tip.
     If several disks are connected, choose the required device's line in the list and click OK.

   Do not disconnect the key device from the reader until the key information is read.

To force encrypted key unloading:

- Right-click the Secret Net Studio icon in the system area of the Windows task bar and click Unload Keys.

  Note.
  This command is available if there are loaded keys.

Updating key information

Key information stored on a key device can only be updated after expiration of the minimum validity period of personal key information.

Key information is updated in two steps:

1. Updating key information on a key device.

   Key information is saved on a key device in two places: the user's valid private key and the old key (appears after the private key is updated). When loading key information, the System reads both the valid private key and the old one.

   The first step is to generate a new private key which is later saved to a key device as a replacement for the valid key. The previously valid key is saved as the old one on the identifier. The previous old key is deleted.

2. The update (re-encryption) of control information in encrypted containers means the decryption of information on the old key and its encryption on the new one.

   To retain access to the encrypted information, you need to re-encrypt the control information on all available encrypted containers. Re-encryption of control information starts automatically after the key update.

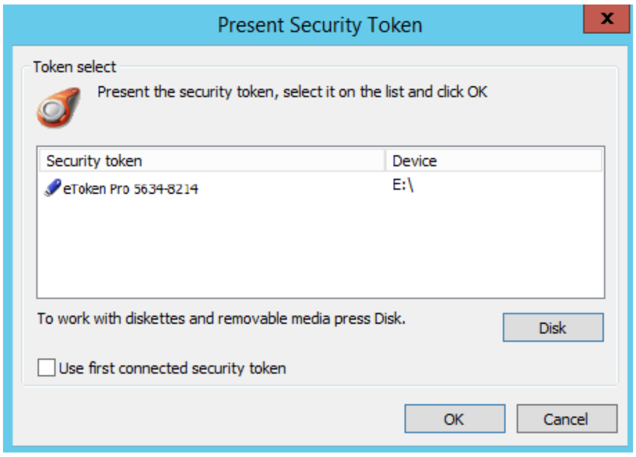
   Attention!
   The encrypted container must be available for automatic re-encryption of control information. For example, if an encrypted container is not available in the network or is located on a currently disconnected removable device, re-encryption is not possible. In this case, once the keys are changed for re-encryption of control information, you have to perform an operation involving the encrypted container (for example, connect the encrypted container) prior to the next key change. Otherwise, the previous key pair will be replaced during the next key change, and you will not be able to gain access to the encrypted container due to a key mismatch. To restore access, you need to add the user again to the list of persons who have access to the encrypted container.

To update the key information:

1. Right-click the Secret Net Studio icon in the system area of the Windows task bar and click Change Keys.

   Note.
   This command is available if there are no currently loaded keys.

   The following dialog box appears:



Present the security token, select it on the list and click OK

Security token	Device
eToken Pro 5634-8214	E:\

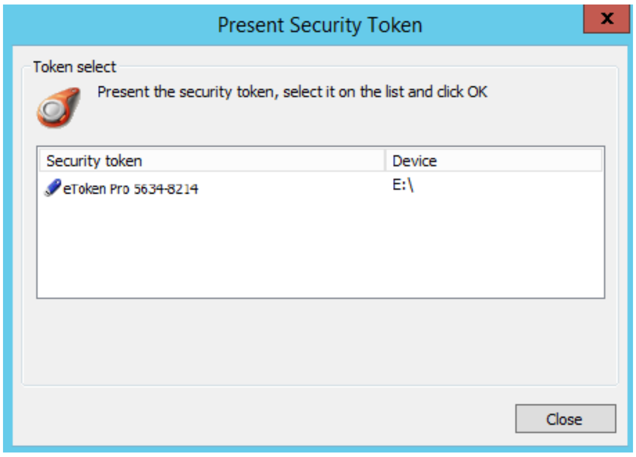
To work with diskettes and removable media press Disk.

□ Use first connected security token

2. Present one of the key devices containing the current key information. Depending on the key device type (a personal identifier or a removable device), perform the appropriate step:
   - if you are using a personal identifier, present it;
   - if you are using a removable disk as the key device, present it and click Disk.

   Tip.
   If several disks are connected, choose the required device's line in the list and click OK.

   Do not disconnect the key device from the reader until the key information is read. Another dialog box appears on the screen listing all your key devices where you can save the new key information.



Present the security token, select it on the list and click OK

Security token	Device
eToken Pro 5634-8214	E:\

3. Present all key devices one by one. If you are using a removable disk as the key device, present it and click Disk.

   Note.
   If the identifier is protected by a custom PIN, a prompt will be displayed. Enter the PIN and click OK.

   If the key information is successfully saved to the device, its status in the list will change to Processed. After this, you can remove the key device from the reader.

4. Once all the media are processed, click Close.

If only some of the key devices were processed successfully, a the respective dialog box appears after clicking Close (or Cancel).

To save the current key information to unprocessed key devices, click Yes and repeat step **3**.

What to do if you encounter a problem

If key information management rules are violated, the System interrupts the operation being executed. Below are the System messages displayed in such cases.

```
Error reading the personal identifier. Repeat the operation?
Private key is not loaded.
```

Reason. Loss of contact between the reading device and the personal identifier, or a removable drive was disconnected while reading.

User actions. Restore contact between the reading device and the personal identifier or reconnect the removable drive. Click OK.

```
The connected personal identifier does not belong to the
current user.
The connected user key failed the authenticity test.
No electronic identifier has been connected.
Unknown electronic identifier type.
```

Reason. You presented a personal identifier that belongs to another user.

User actions. Present your own personal identifier.

```
The key has expired.
```

Reason. Key information required to work with encrypted data in encrypted containers has expired.

User actions. Update key information upon system request.

```
The user does not have a key.
The user does not have a private key.
The user does not have electronic identifiers.
```

Reason. The administrator has not issued a key information device to you.

User actions. Contact the administrator for assistance.

Handling encrypted resources

Secret Net Studio can encrypt the contents of file system objects (files and folders). Special repositories are used for encryption and decryption operations: encrypted containers or crypto containers. Encrypted containers can be connected to a system of local disks, removable storage devices or network resources.

A physical encrypted container is a file that can be connected to the System as an additional disk. An encrypted container is a disk image, but all operations related to it are performed by the encryption mechanism driver. The driver processes user data in containers in the transparent data encryption mode. This means that once the encrypted container is connected as a disk, the user performs file operations on the disk as on any other storage device. No additional operations are required to encrypt or decrypt files; all cryptographic file operations are performed automatically.

Once Secret Net Studio is installed, a special Secret Net Studio Encrypted Containers folder is added to the list of system resources for data storage. The folder is configured for operations with the list of encrypted containers. To open the Encrypted Containers folder, click its shortcut in the list of the Computer object's control elements in Explorer.

Encrypted container creation

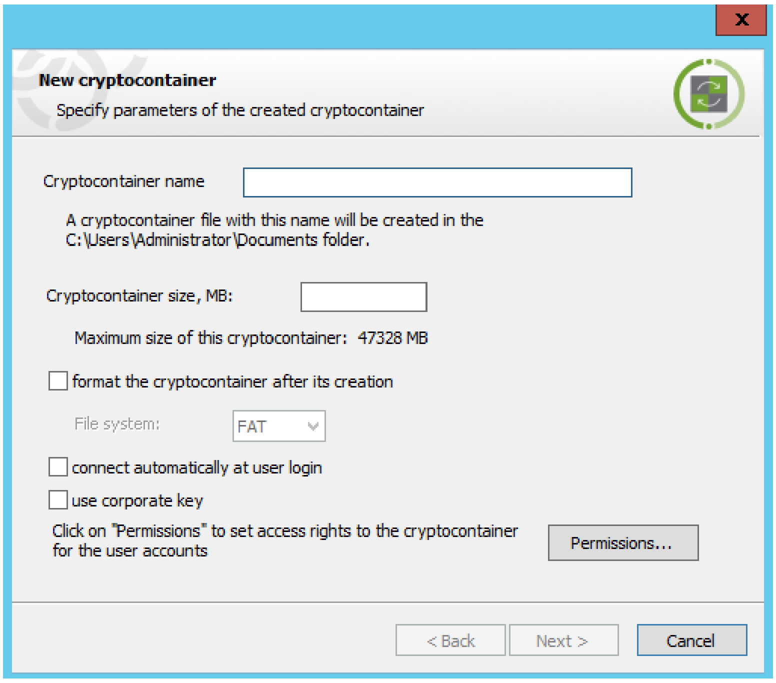
The right to create encrypted containers is available to users with the appropriate privileges. This privilege is granted by default to all accounts included in the local group of administrators. A user who creates an encrypted container is granted the right to manage it and can delegate (grant) the access rights to other users.

The creation procedure can occur in the folder where the encrypted container file will be located or in the list of encrypted containers in the Secret Net Studio Encrypted Containers folder.

To create an encrypted container in the selected folder:

1. Select the folder where the encrypted container file will be located.
2. Right-click the folder, point to Create and click Secret Net Studio Encrypted Container.

   A "New cryptocontainer" dialog box appears, as in the figure below.



New cryptocontainer

Specify parameters of the created cryptocontainer

Cryptocontainer name

A cryptocontainer file with this name will be created in the C:\Users\Administrator\Documents folder.

Cryptocontainer size, MB:

Maximum size of this cryptocontainer: 47328 MB

□ format the cryptocontainer after its creation

File system: FAT

□ connect automatically at user login

□ use corporate key

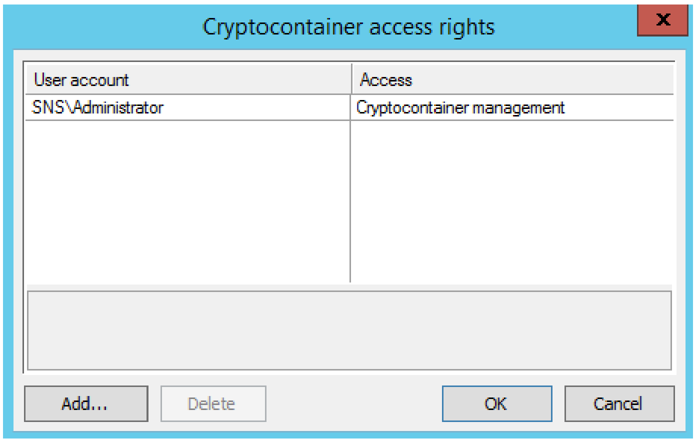
Click on "Permissions" to set access rights to the cryptocontainer for the user accounts

3. Enter the name and size of the encrypted container to be created in the respective fields.
4. To prepare the encrypted container's file system immediately after its creation, select the "format the cryptocontainer after its creation" and select the file system type in the respective drop-down list.
5. If necessary, enable the automatic connection of the encrypted container each time the user logs. For this purpose, select "connect automatically at user login" check box.
6. To improve encrypted container protection, select "use corporate key" check box. In this case, a special key will be created to ensure access to the encrypted container only on that computer (you need to copy the key to other computers in order to work with the encrypted container on them). If this check box is not selected, no corporate key for the encrypted container is created.

   Note.
   The corporate key is saved in the computer's system registry. Therefore, you will need write access to the registry in order to create the key. By default, such rights are granted to the local group of administrators.

7. To set up access rights to the encrypted container for the user accounts, click Permissions.

   A dialog box asking you to set up access rights appears, as in the figure below.



User account	Access
SNS\Administrator	Cryptocontainer management

8. Edit the list of accounts by clicking the Add and Delete buttons. You can only add users to the who have encrypted keys. To change access rights to an account, select it in the Access list and specify the value for it (to open the list of available values, click the button in the right-hand part of the cell).
9. Click OK.
10. Click Ready in the dialog of the encrypted container creation wizard.

    The encrypted container file with the .SnDisk extension will be added to the selected folder.

To create an encrypted container while working with the list of encrypted containers:

1. In the Secret Net Studio Encrypted Containers folder, right-click anywhere within the list area and click Create.

   A dialog box asking you to create encrypted container appears. The dialog box differs from the dialog box described above in one aspect: there is a field for specifying the encrypted container location.
2. In the Encrypted Container field, select a catalog for the file and complete the said of this procedure starting from step **3**.

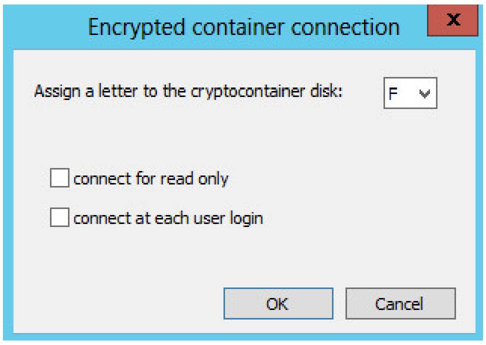
Encrypted container connection

When connecting an encrypted, an additional disk appears in the system that is the image of the encrypted container. Once the connection is established, you can handle files on this disk in the same way as on any other device (after the disk is formated, if it was not done when the encrypted container was being created).

To connect an encrypted container:

1. Load encrypted keys (see p. **25**).
2. Right-click the encrypted container and click Connect.

   A dialog box asking you to set up connection parameters appears.



Assign a letter to the cryptocontainer disk: F

□ connect for read only

□ connect at each user login

3. Select the drive letter in the "Assign a letter to the cryptocontainer disk" dropdown list box.
4. If necessary, set up additional connection parameters:

- to enable write protection for the encrypted container, select "connect for read only" check box;
- to enable automatic connection of the encrypted container during login, select "connect at each user login" check box.

5. Click OK.

   A new element appears in the list of computer drives in Explorer. In the Secret Net Studio Encrypted Containers folder, the encrypted container will be moved to the Connected section.

Encrypted container disconnection

When an encrypted container is disconnected, the respective additional disk is removed from the system. After disconnection any operations involving the container's contents will be impossible.

Connected encrypted containers are disconnected automatically when the user logs off. You can also force disconnection using a special command.

To force an encrypted container disconnection:

1. Close all open files in the encrypted container.
2. In the list of the computer's drives in Explorer or in the Secret Net Studio Encrypted Containers folder, right-click the connected encrypted container and click Disconnect.
3. Confirm your decision in the request dialog box that appears in order to continue.

   The encrypted container will be removed from the list of the computer's drives in Explorer. The encrypted container in the Secret Net Studio Encrypted Containers folder will be moved to the Disconnected section.

Viewing and configuring encrypted container parameters

When working in the Secret Net Studio Encrypted Containers folder, you can open a dialog box to view and set up encrypted container parameters. The parameters can be modified by users granted the encrypted container configuration rights.

To open the dialog, select an encrypted container in the list of the Secret Net Studio Encrypted Containers folder, right-click it and select Properties.

The dialog box contains general information about the encrypted container (its state, size and so on), as well as tools for enabling the automatic connection mode and editing the list of accounts with access rights. The configuration procedure is the same as when creating an encryption container (see p. **28**).

Re-encryption of encrypted containers

When an encrypted container is created, a generic encryption key is created. All other containers are encrypted on the basis of this generic key. The entire contents of an encrypted container are re-encrypted when the generic key is changed (unlike to changing of user keys, where only part of the control information is re-encrypted). When using the System, you need to regularly update both user keys and generic container keys.

To re-encrypt containers:

1. In the Secret Net Studio Encrypted Containers folder, right-click anywhere within the list area and click Change Encryption Key.

   A dialog box with the list of encrypted containers appears.
2. Select the required encrypted containers and click Change Keys.

Encrypted container removal

Connected encrypted containers are exclusively managed by the encryption mechanism driver. While an encrypted container is connected, it cannot be removed.

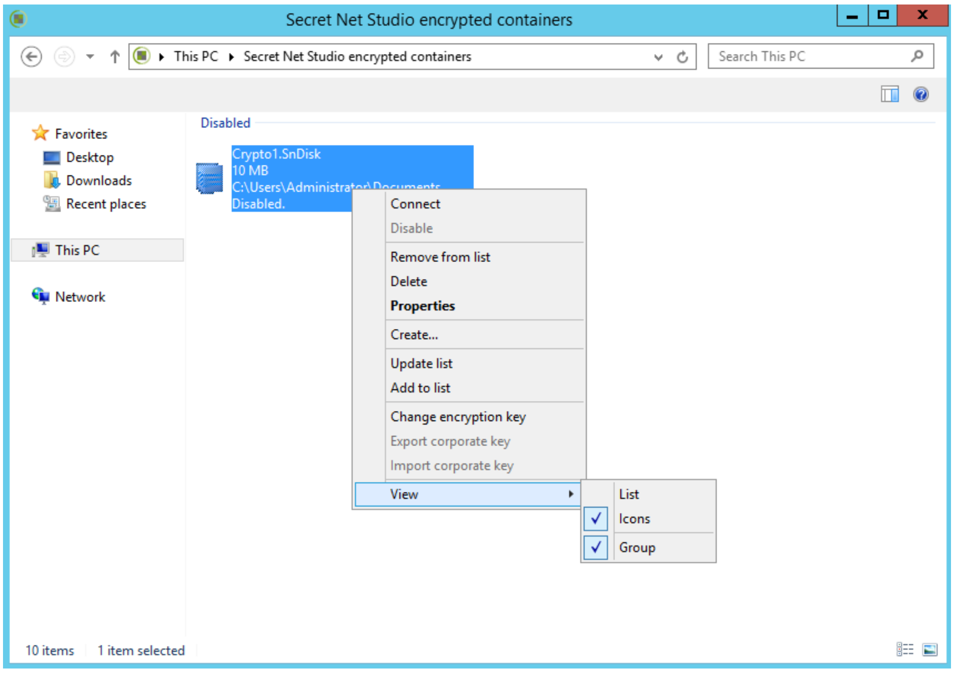
You can remove encrypted containers in one of the following ways when working with the list of encrypted containers in the Secret Net Studio Encrypted Containers folder:

- remove from the list of encrypted containers while the encrypted container file remains in its current location: right-click the encrypted container and click "Remove from list";
- remove the encrypted container file and its respective record from the list of encrypted containers: right-click the encrypted container and click Delete.

Note.
If the encrypted container file was moved or deleted from the folder using another method (for example, when working with the folder in Explorer), the container's record remains in the list of Secret Net Studio Encrypted Containers folder in the Unavailable section. To remove such elements, right-click them and click Delete.

Encrypted container list management

An example of encrypted containers in the Secret Net Studio Encrypted Containers list is shown in the figure below:



Context menu commands can be used to manage the list.

Command	Description
Add to list	Starts adding an encrypted container from a file. You can select the encrypted container in the standard open file dialog box
Update list	Re-reads data on the availability of encrypted containers in the System
View	Contains commands for switching display and element grouping modes

Chapter 5
Using network protection tools

Personal firewall

Secret Net Studio firewall is used to protect a computer against unauthorized access and to restrict network access.

Network traffic is filtered based on the rules created for applications with a wide range of settings. Network connections can be restricted at the level of users, computers, user groups (computers), and connection parameters, service and application protocols, ports, network interfaces, applications, days of week, time of day.

The firewall is set up by the administrator in the Control Center.

Chapter 6
Using antivirus and intrusion detection tools

Antivirus protection

Secret Net Studio automatically scans a computer for malware. It detects and blocks external and internal network attacks directed to a computer scanning hard drives, network folders, external data storage media, email messages and other objects.

You can also scan selected files from the Windows context menu (see p. **34**).

If infected objects are detected, the respective alert will appear on the screen. One of the following actions will also be performed: remove infected files, isolate infected files (move to quarantine), block access to infected files and repair.

Note. To reset the alert after malware is detected, on the Windows taskbar right-click the Secret Net Studio icon in the Notification area and click Reset Alert.

The behavior of Antivirus and its response to detected malware are centrally configured by the administrator using the Control Center.

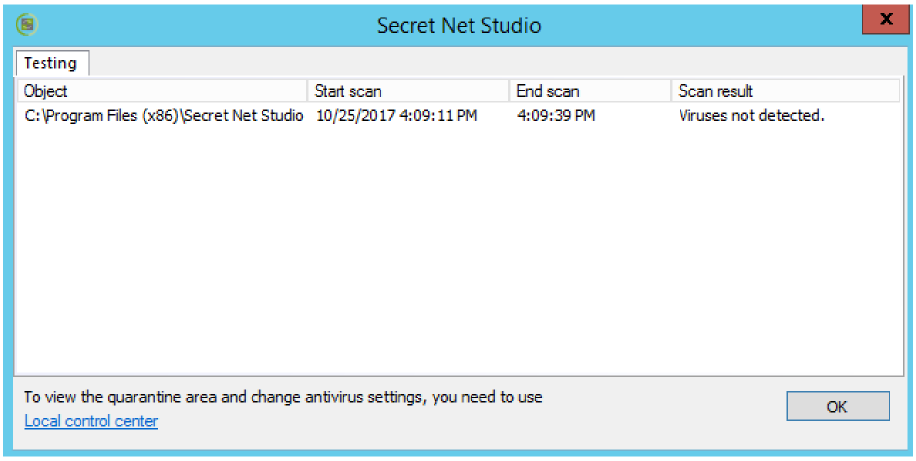
Context scanning

Using Secret Net Studio, you can scan selected files for viruses.

To check the files:

1. Right-click the file or folder.
2. Click Scan for Viruses.

   Secret Net Studio antivirus scans the files and the following window appears.



Object	Start scan	End scan	Scan result
C:\Program Files (x86)\Secret Net Studio	10/25/2017 4:09:11 PM	4:09:39 PM	Viruses not detected.

To view the quarantine area and change antivirus settings, you need to use Local control center

You can view detailed results of the scan and the list of quarantined files in the Control Center.

To view the scan results:

- On the Windows taskbar right-click the Secret Net Studio icon in the Notification area, point to Antivirus and click Check Results.

Intrusion detection

Secret Net Studio ensures detection and blocking of external and internal threats to a computer. The network traffic is scanned for network attacks, and the attacking computers are blocked for time specified by the administrator.

When an attack is detected or access to an application is blocked, a message appears on the screen.

Note. To reset the alert after an external or internal intrusion is detected,on the Windows taskbar right-click the Secret Net Studio icon in the Notification area and click Reset Alert.

This mechanism's parameters are configured by the security administrator in the Control Center.