SECURITY code

Secret Net Studio

Operation Principles

User guide

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

Table of contents

Introduction

This manual is designed for the users that have Secret Net Studio software installed on their computers. It contains information on how to work with Secret Net Studio.

This manual is designed for Secret Net Studio administrators. It contains information that administrators need to use additional tools and configuration files (hereinafter additional tools) necessary to work with Secret Net Studio.

Website. Information about SECURITY CODE LLC products can be found on https://www.securitycode.ru.

Technical support. You can contact technical support by phone: +7- 800- 505- 30- 20 or by email support@securitycode.ru.

Training. You can learn more about hardware and software products of SECURITY CODE LLC in authorized education centers. The list of the centers and information about learning environment can be found on https://www.securitycode.ru/company/education/training-courses/. You can contact a company representative for more information about trainings by email education@securitycode.ru.

Chapter 1
General information

What you need to know

Before you start working with a protected computer, we recommend reading 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 placed 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, you need the following:

1. Logon credentials: username and password.
2. If hardware is required for user identification, you need your personal security token assigned using Secret Net Studio tools.
3. If the data encryption mechanism with encrypted containers is enabled, you need a device containing key information to access encrypted containers (a key device). A key device can be a personal security token assigned to you (the same as the one used for identification or another one), a floppy disk, memory stick or USB flash drive.
4. If Trusted Environment is enabled, you need a boot device (a specialized USB flash drive) to start an operating system.
5. 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 security token 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 perform your duties effectively.

Chapter 2
Logging on to the system

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

You can log on to the system in different ways depending on the availability of system support for hardware and personal security tokens.

The table below lists the different available authentication modes.

Mode	Logon method	Application conditions
By name	Standard Windows authentication only (see p. **11**)	For systems with no hardware logon control tools
Only by security token	Only using a personal security token (see p. **11**)	For systems equipped with hardware, when all users have personal security tokens
Mixed	Standard Windows authentication or system entry using a personal security token	For systems equipped with hardware, when some users have no personal security tokens

A single logon mode is set for all users of the computer.

The logon modes **By name** and **Mixed** allow identification by entering the user name manually or by using identification tools activated by Windows features (e.g., Smart Card, eToken, etc.). Information about the use of security tokens in Windows can be found in the operating system documentation. In **Only by security token** mode, you can use only personal security tokens activated via Secret Net Studio tools, but not the ones activated via Windows features.

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

Note. To access USB key or smart card memory, you need to enter a PIN code. By default, the security token is protected by the default PIN set by the device manufacturer. If the default PIN remains unchanged, Secret Net Studio will automatically access the security token 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 security token is connected. The administrator must provide you with the custom PIN when issuing your security token.

Attention! Make sure you do not forget your PIN code, otherwise you will not be able to use the security token.

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

Booting and logging on to the system when using Sobol

If the computer has Sobol installed and it operates in joint mode with the security system, computer booting and user logon to the system can be performed using a single security token.

In this case, your actions depend on whether the user password is written on the security token and whether this password is valid for Windows:

- if the password on the security token is valid for Windows, it is read when logging on to Sobol and remembered for logging on to Windows;
- if the password on the security token is not valid for Windows (for example, the password was changed, but its new value was not written on the security token), then reading this password from the security token allows logging on to Sobol, but not to Windows. In this case, you need to enter the valid password when logging on to Windows;
- if there is no password on the security token, you need to enter the password twice: to log on to Sobol and then to Windows.

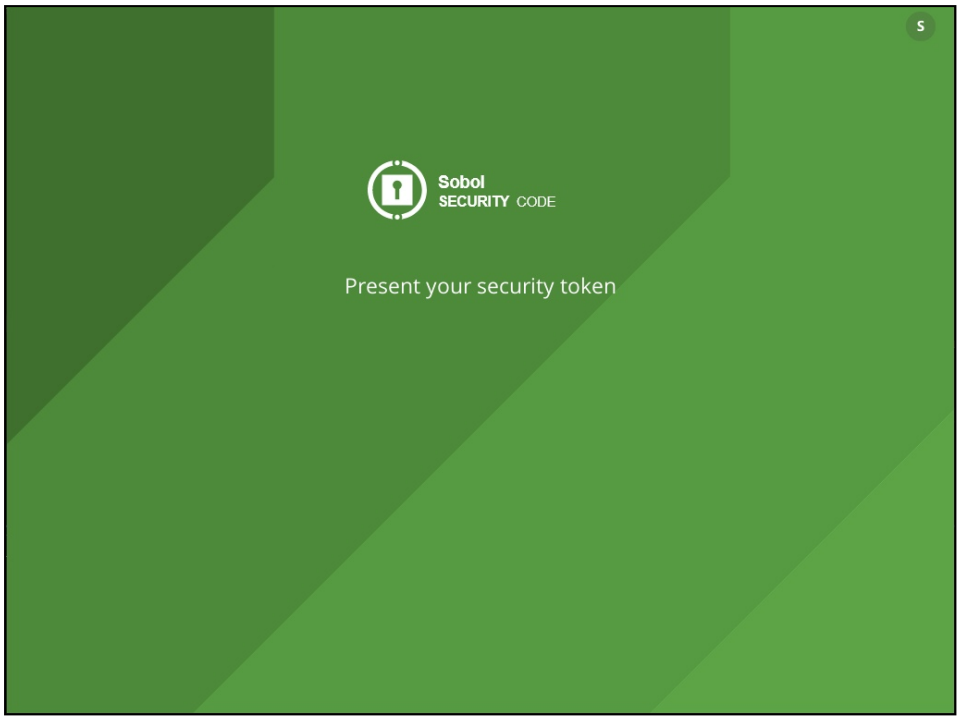
To load the computer and log on to the system using Sobol:

1. Turn on the computer.

   The **Getting ready** window appears.

Note. If an error occurs during this step, contact the administrator.

When Sobol boot is complete, you are prompted to present your security token.



In the center of the window, a timer may appear counting down:

- automatic logon timeout (in seconds) or
- timeout for presenting your security token and entering the password (in minutes and seconds).

Note.

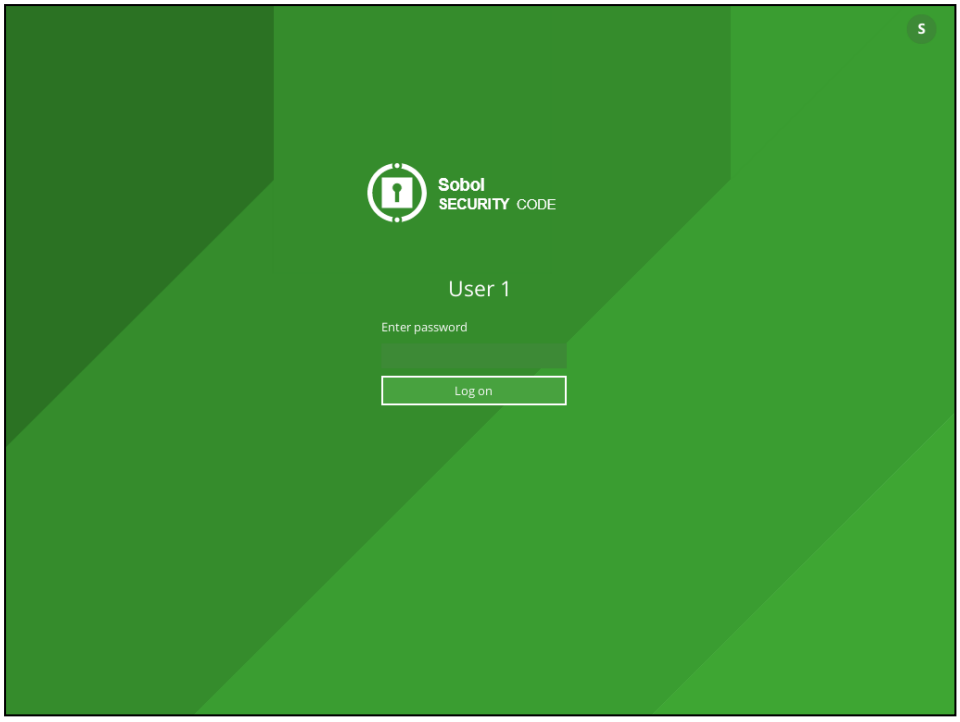
- Automatic logon timeout is displayed if Sobol is configured to boot automatically. In this case, you do not need to enter any credentials. When the specified time is over, the integrity check is performed (if the integrity check mechanism is enabled) and the OS boots.
- The time left to present your security token and enter the password is displayed if the administrator has enabled the logon timeout. If you do not have the time to present your security token and enter the password, the computer will be blocked. Restart your computer and log on again.

2. Present your security token

Note.

- If the security token was already presented, Sobol automatically reads it.
- If several security tokens are presented, Sobol reads the first one detected. To change the security token, press **Esc**.
- If the security token is presented incorrectly, the request remains. Present the security token again.
- When the **Logon is prohibited by administrator** message appears, click **OK** and contact the administrator.

If there is no password saved on the security token, a dialog prompting you to enter it appears.



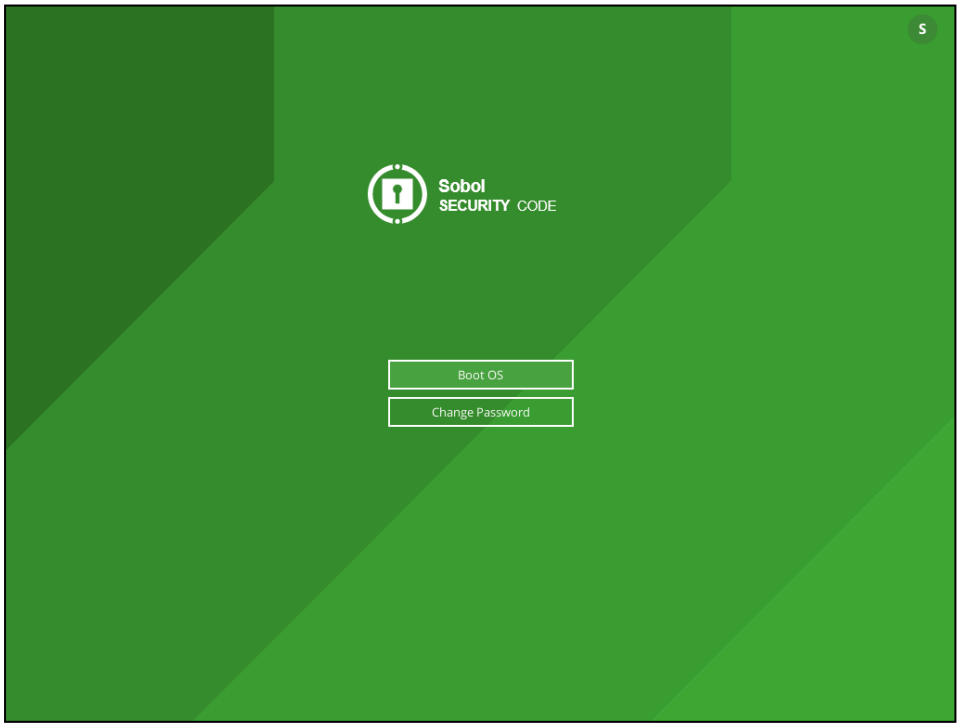
- Enter the password and click **Log on** or press **Enter**.

Note. Each password character is displayed as "*" (asterisk). When entering the password, note that uppercase and lowercase letters are not the same.

Attention!

- If the entered password does not match the presented security token, the **Invalid password or security token** message appears. Click **OK** and present the security token again. Use your security token and do not make mistakes when entering the password.
- The number of failed logon attempts may be limited by the administrator. If you exceed this limit, the message about computer lockout appears on the next logon. In this case. contact the administrator.

After successfully entering the credentials, the window with the **Boot OS** button appears.



3. Click **Boot OS** or press **Enter**.
Integrity of the objects is checked (if planned).

Note.
- If an error occurs, a respective messages appear. Click **OK**.
- If you do not need complex notifications during the integrity check, select **Do not ask again**.
- Click **Finish** when the check is completed.
- If the **Computer is locked** message appears, turn off the computer and contact the administrator for help.

The operating system starts booting.

4. Next, when the the operating system is booting, your actions depend on what information about the password is contained in the security token. The following options are possible:
   - The password read from the security token during Sobol logon is valid for Windows.

     In this case, you will be logged on to the system without password request after successful verification of user rights.
   - There is no password on the security token or the security token contains another password which is not valid for Windows.

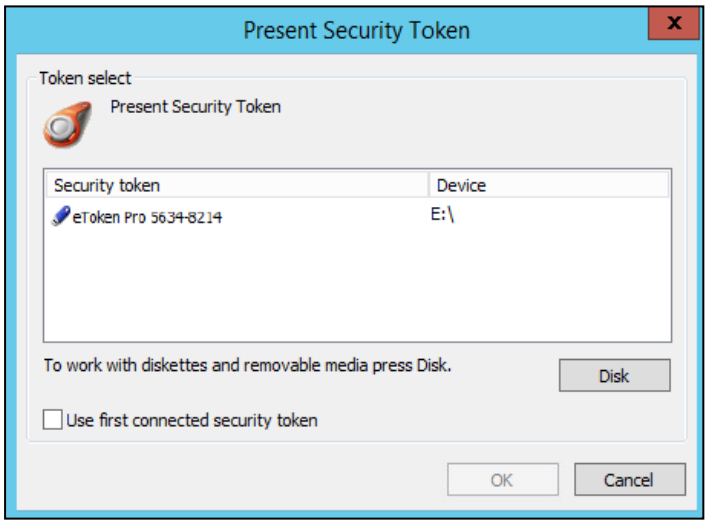
     In this case, a dialog box prompting you to enter user credentials appears, which displays the user name of the owner of the presented security token.

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

   If the entered password is valid and the security token cannot store passwords, you will be logged on to the system.

   If the entered password is valid and needs to be written on the security token — the corresponding request appears. In this case, do the following:
   - Click **Yes**.

     A dialog box containing the name of your security token appears.



   - To write the password, present the security token.

     After the new password is successful written on the security token, its status on the list changes to **Processed**. After that the security token can be disconnected.
   - Click **Close**.

   After the dialog box closes, you are logged on.

Logon scenarios

To log on, please enter your user name and password. Once you entered your user name and password, the system authenticates you. If authentication is a success, you will be able to log on to the system.

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

The logon procedure starts when the logon prompt appears. If the administrator enabled notifications, a message containing information about implemented security measures appears on the welcome screen.

Attention! If the message containing information about implemented security measures appears, by logging on to the system, you accept the rules and restrictions on working with information.

Depending on the security mechanisms and administrator restrictions, logon steps may differ (see the respective instructions in the subsections below).

If the administrator enabled notifications, after logon, a message containing information about your last successful logon and the number of failed logon attempts since the last successful logon appears in the taskbar system notification area.

Note.
- If notifications are enabled, at the first logon, the following message appears: **Previous user logon data is missing**.
- The message containing information about your last successful logon may not appear if two and more messages are displayed.

Standard logon method

To log on using the standard logon method:

1. Depending on the computer's operating system prior to logon, a lock screen appears followed by the welcome screen or logon prompt. To start the logon procedure, take one of the following steps:
   - if you are using Windows 11/10 or Windows Server 2022/2019/2016, disable the lock screen if it appears (for example, press any key). Check the name of the account that the operating system provides for logon. If you need to choose another account, in the bottom-left corner, choose the required name or click **Other User**. A field to enter user credentials appears on the screen;
   - if you are using a Windows 8.1 or Windows Server 2012 R2 computer, disable the lock screen if it appears (for example, press any key). Check the name of the account that the operating system provides for logon. 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 **Other User**. A field to enter user credentials appears on the screen;
   - if you are using Windows 7 or Windows Server 2008 R2, choose the required name or click **Other 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, the real password is not displayed in the entry line. The password is both case and language sensitive. If invalid user name or password characters are entered, delete them from the entry line using **Backspace** or **Delete** and re-enter the data.
3. Click →.

   If the user credentials are correct, you enter the system.

Logging on via a security token

When logging on by a security token activated by Secret Net Studio, the system will automatically detect the name of the user the security token is assigned to.

To log on using the security token:

1. Before you log on, depending on the computer operating system, a lock screen appears followed by the welcome screen or logon prompt. The system is ready to read data from the security token. Present your own security token.

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

2. The response of the security system depends on the user password information contained in the security token. The following scenarios are possible:
   - the security token contains the current user password;
   - the security token does not contain a password or contains a password different from a user password (for example, a password has expired or was changed but not saved to the security token).

Situation 1	**If the security token contains the current password,** the user will log on to the system without request to enter the password after a successful check of user rights
Situation 2	**If the security token does not contain a password or contains another password,** a dialog box for entering user account details will appear displaying the name of the user who owns the presented security token

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

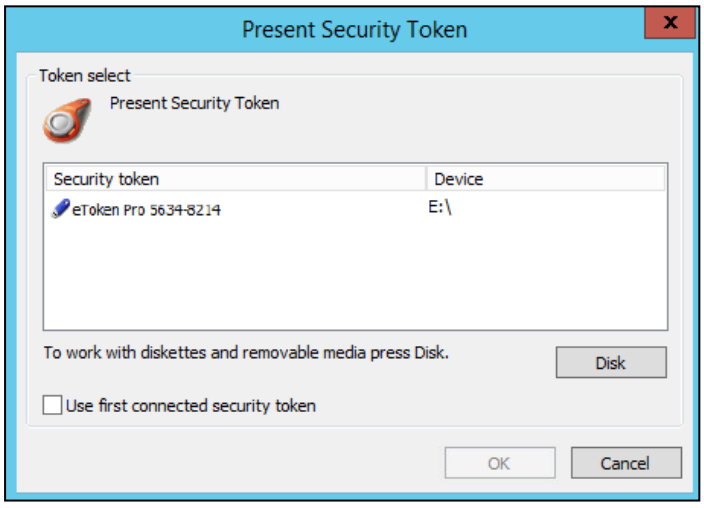
Note. For security reasons, the real password is not displayed in the entry line. The password is both case and language sensitive.

If the password you entered is correct and **no** password is saved in the security token, you enter the system.

If the password you entered is correct and it should be saved to the security token 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 security tokens where you can save the new password.



- To save the password, present the security tokens one by one.

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

  Once your new password is successfully saved to the security token, its status in the list changes to **Processed**. After this, you can remove the security token from the reader.
- Once all security tokens are processed, click **Cancel**.

The dialog box closes and you enter the system.

Logon features when advanced authentication mode is enabled

Secret Net Studio provides the following user authentication modes:

Mode	Description
Standard authentication	During user logon, 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

For advanced password-based authentication, the password must be saved in the Secret Net Studio 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.

Logon when mandatory access control is enabled

If the Mandatory Access Control mechanism is enabled (see p. 21), user permissions are also checked during logon. Logon restrictions are set in the following cases:

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

Logon when devices with a confidentiality category are used

The administrator can assign confidentiality categories to certain devices. If a user logs on 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, Secret Net Studio prompts you to disable this device. Otherwise, logon cannot be performed.

Logging on with enabled flow control

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 logon rights.

When selecting the confidentiality level, you inform the system about 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 performed. System logon is prohibited in the following cases:

- devices with a confidentiality category that is different from the session confidentiality level are found;
- devices with different confidentiality categories are found;
- when logging on to the system for configuration purposes, devices with a confidentiality category higher than **Non-confidential** are found.

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

For details about working with the security system when mandatory access control is enabled, see p. 22.

What to do if you encounter a problem

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

Incorrect user behavior.
Incorrect user name or password.

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

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

If an error occurs, re-enter your user name and password. The administrator can limit the number of password entry attempts. If you exceed the attempt limit, the security system will display a respective message and lock out 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 user name.

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 user name 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 asking you to

enter a new password appears. To log on and synchronize the passwords, enter your new password and make sure the **Synchronize Passwords** check box is selected.

The security token password differs from the current password. Do you want to save your current password to the security token?

Reason. The password on the security token is different from the system password.

User actions. You can update the password in the security tokens (see p. **16**) or do it later. We recommend updating the password immediately.

The security token of this user is not registered on this computer.
Incorrect data format on the security token.
Incorrect password stored on your security token.

Reason. During logon, a security token was connected that does not belong to the entering user, or it does not contain the required information.

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

User actions. Repeat the logon procedure by connecting the correct security token. Make sure your security token is correctly connected to the reading device.

If the error persists, contact the administrator.

Incorrect security token PIN entered.

Reason. During logon, a security token PIN was entered incorrectly.

User actions. Enter your PIN again.

If you forget a security token PIN, contact your administrator.

Password has expired.

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

User actions. Close the message box and change the password (see p. **16**).

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

Reason. The information required for logon is entered correctly, but logon 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 on again when the problem is fixed.

Sometimes, a computer can only be used in standalone mode, without any access to network resources. Click **OK** to continue working in standalone 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 on, 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 on, 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>. Logon 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 device 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 on 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 on, disconnect devices that are assigned an elevated confidentiality category.

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

User actions. Disconnect the devices and log onto 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 on, 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 out by Secret Net Studio 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
Base protection tools

Temporary computer lock

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 security token connected during logon.

Before you lock the computer, we recommend saving any changes in 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 an 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, click **Lock** (**Lock Computer**).

To lock the computer using a security token:

1. Switch the computer to the general operating mode with the desktop and task bar displayed on the screen.
2. Remove the security token that was connected for logon from the reader.

Note. The computer will be locked when removing the security token if the security administrator has enabled the appropriate response for the computer. The locking function is put into action during a local user session if the security token was enabled by Secret Net Studio and the user connected this security token for logon.

Unlocking a computer

A user working with a computer can unlock the 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:
   - for computers with Windows 10/8.1 or Windows Server 2019/2016/2012 R2, disable the lock screen (for example, press any key). The locked session credentials input box appear;
   - for computers with Windows 7 or Windows Server 2008 R2, choose the locked session user account. The password input box appears.
2. Enter the password and click → or **OK**.

Unlocking the computer using a security token:

1. Connect the security token. If the security token remained connected to the reader after the computer was locked, disconnect the security token and -connect it again.

   If the security token contains your password, the computer will be unlocked. If the password is missing, the user credentials input box with the current user name will appear.
2. Enter the current password in the **Password** field and click → or **OK**.

Changing password

To change the password:

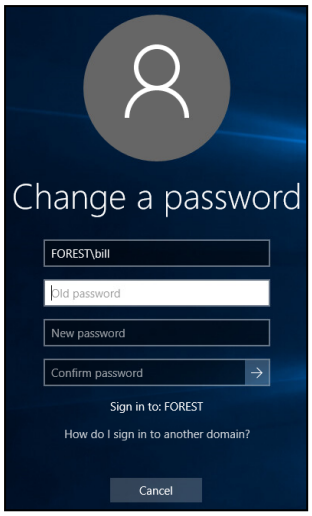
1. Press **Ctrl+Alt+Del**.

   A screen with the commands appears.
2. Click **Change a Password**.

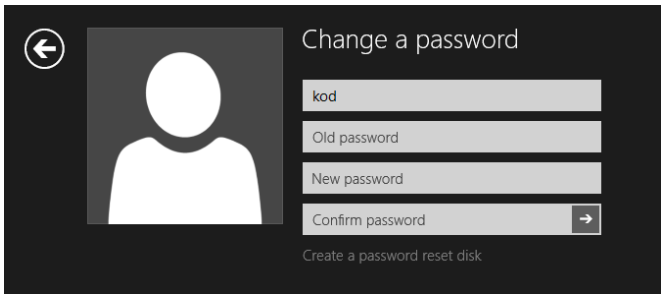
   If the current password policy does not allow you to change the password, an error message will appear and the procedure will be interrupted. In this case, contact your administrator to change the password.

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

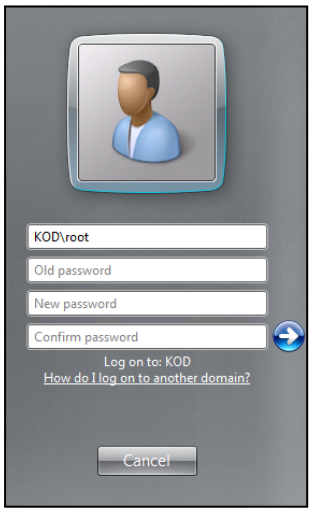
- on a computer running Windows 11/10 or Windows Server 2022/2019/2016:



- on a computer running Windows 8.1 or Windows Server 2012 R2:



- on a computer running Windows 7 or Windows Server 2008 R2:



3. If necessary, change the input language (the current language is displayed on the Windows taskbar, in the notification area) and fill in 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, the real password is not displayed in the entry field. The password is both case and language sensitive.

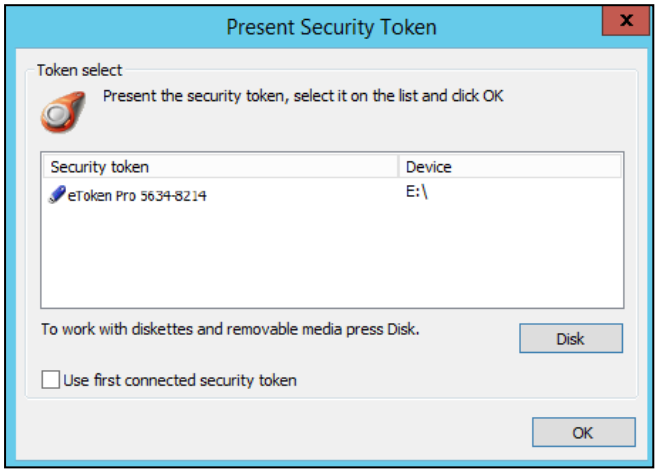
4. Click → or **OK**.

Note.
If the password does not meet system requirements or you have entered the incorrect old password, an error message appears. Click **OK** in the message box and re-enter the correct password.

If the **Change a password** dialog box fields are filled in correctly, a message notifying that the password is changed appears.

5. Click **OK**.

   If your old password is stored on the security token, a dialog box with a list of your security tokens appears, as in the figure below.



6. To change your password, connect each security token one by one.

Note.
If the security token 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 security token, its status on the list changes to **Processed**. After this, you can disconnect the security token.

7. Once you have 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. The color of the Secret Net Studio icon in Windows taskbar changes, and a warning message appears for a short time to indicate a local alert.

The administrator can decide whether to enable/disable local alerts and reset the alert state or pass control over to users.

To manage local notifications:

1. On the Windows taskbar, right-click the Secret Net Studio icon in the notification area. The **Alert notifications** and **Reset alert state** commands allow you to manage local notifications.

   If there is a check mark to the left of the **Alert notifications** command, alert notifications are enabled.

Note.
- If the **Alert notifications** and **Reset alert state** commands are unavailable, user privileges to manage local notifications are restricted by the administrator.
- If the administrator has enabled or disabled local alerts for all computer users, the user cannot change the status.

2. To disable notifications, click **Alert notifications** if the command is available.
3. To reset the alert state, click **Reset alert state** if the command is available.

Chapter 4
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 is used. With the mechanism the administrator can allow or deny operations with certain file system resources.

Access isolation options depend on the resource type. Thus, permissions for managing access to resources required for the computer's operation are limited. For example, it is impossible to modify access permissions for a root folder of a system drive and the entire system folder.

Changing access permissions for folders and files

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

Permissions can be assigned explicitly or inherited from a higher file system hierarchy element. Explicitly assigned permissions have a higher priority compared to inherited permissions.

Note. Access permission inheritance mode is strictly enforced for a resource when moving it to another logical partition. In this case, even if access permissions were expressly assigned to the resource in its initial location, access permissions 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 permissions 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 permissions for resources:

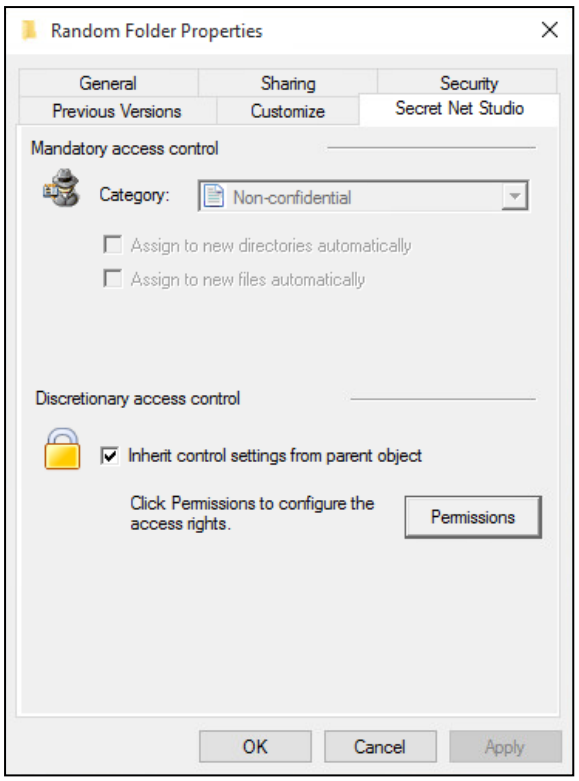
- security administrators or authorized employees with the privilege to manage access permissions; this privilege makes it possible to change access permissions for all resources (irrespective of the access permissions assigned to the resources);
- resource administrators or users with permission to change access permissions for this resource.

The user with the privilege to manage access permissions performs the initial assignment of resource administrators. Then, the resource administrators manage access permissions for all respective resources by allowing or deny the execution of operations by other users.

This procedure uses Windows File Explorer.

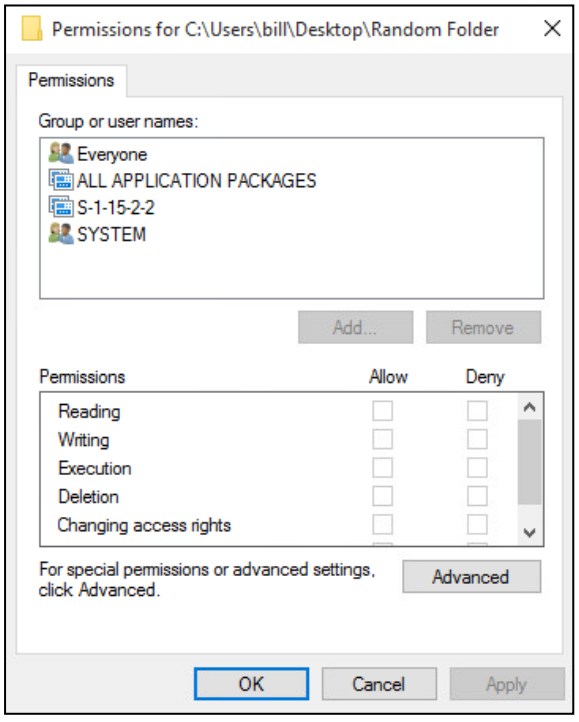
To change access permissions to a resource:

1. Right-click a folder or a file and click **Properties**. In the properties dialog box, select the **Secret Net Studio** tab.



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

   The **Permissions** dialog box appears. The dialog box operates identically to standard Windows tools.



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 the permissions. If you need more information (for example, about the source of the inherited permissions) or if you want to set up special settings (including audit settings for operations with resources), click **Advanced** and perform the required steps in the Windows security settings window.
5. Once the setup is complete, click **OK**.

Data Wipe

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 deleted information. This mechanism makes it impossible to recover and reuse deleted data.

The security administrator can enable automatic data wiping for files that are deleted on local and/or external drives. 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** (files in the **Recycle Bin** are not considered deleted) or if you delete selected objects by pressing **Shift+Delete**.

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

To selectively delete the files by wiping data:

1. In Explorer, select the required objects (files and/or folders), right-click one of the selected objects and click **Remove 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 allowed programs for each user. When starting a program that is not on the list, alerts are logged as unauthorized access attempts (UA). Application Execution Control can be used in hard or soft operation modes.

In hard mode the user can only work with programs that exist in the list of allowed programs. The system will block other programs starting and warn the user that access to a device or file is denied.

If you need to add programs to the list of allowed programs, contact the security administrator with the privilege to grant users access to information system resources.

In soft mode, the security system does not block the start programs that are not included in the list of allowed programs. The soft mode is used at the implementation stage of the security system 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 assigned confidentiality categories (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 access level is compared to the resource confidentiality category. Access to the resource is granted if its confidentiality category is not higher than the user 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 confidentiality level set during user logon (see p. **13**).

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 set: **Non-confidential**, **Confidential** and **Strictly confidential**);
- each user is assigned one of the available levels of access to confidential information. The set of user access levels in Secret Net Studio is the same as the set of confidentiality categories for resources;
- a user is allowed to access a resource if the user access level is not lower than the resource confidentiality category. For example, a user 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 access level; • devices with different confidentiality categories; • devices with a confidentiality category higher than **Non-confidential** during initial user entry on the computer (configuration entry)
A device cannot be connected if its confidentiality category is higher than the current user's access level	A device cannot be connected if its confidentiality category differs from the current user's session level
All network interfaces can be used	Network interfaces cannot be used if their current session confidentiality level is not specified in the list of allowed levels
There are no access restrictions to devices if the **device is available regardless of confidentiality categories** mode is enabled for them	
Access to files	
If a confidentiality category is assigned to a file-containing device, the system considers the file's category the same as the device's category when accessing the file (irrespective of the file system type). It is prohibited to change a file's confidentiality category	
Access to a file is prohibited if its confidentiality category is higher than the category assigned to the file-containing device	
Users can access the file if their access level is not lower than the file's confidentiality category	Users can access the file if the user session confidentiality level is not lower than the file's confidentiality category
It is not allowed to delete a confidential file to the Recycle Bin	It is not allowed to delete any file to the Recycle Bin
Access to folders	
If a confidentiality category is assigned to a folder-containing device, the system considers the folder's category the same as the device's category when accessing this folder (irrespective of the file system type). It is prohibited to change a confidentiality category of the folder	
Access to a folder is prohibited if its confidentiality category is higher than the category assigned to the folder-containing device	
Confidential files are placed in folders with a confidentiality category not lower than the file's confidentiality category. For example, a folder with the confidential category can contain both non-confidential files and files with the confidential category	
A user without access to a file can view the contents of the confidential folder that contains the file, but cannot open the file. Therefore, no confidential information should be contained in confidential file names	
It is not allowed to delete a confidential folder to the Recycle Bin	It is not allowed to delete any folder to the Recycle Bin
Inherit the folder confidentiality category	

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 directory confidentiality category. Restriction: The assigned confidentiality category must be equal to the current session's confidentiality level
If automatic confidentiality category assignment mode is disabled: • when creating, saving, or copying a subfolder/file, it is assigned non-confidential category; • when moving a subfolder/file within a logical partition, it retains its confidentiality category (the file can be moved if its confidentiality category is not higher than the confidentiality category of the upper-level folder). The appropriate user privilege is required to move subfolders	If automatic confidentiality category assignment mode is disabled: • when creating, saving, or copying a subfolder/file, it is assigned the same category as the session's confidentiality level, but not higher than the folder's confidentiality category; • when moving a subfolder/file within a logical partition, it retains its confidentiality category (the subfolder/file can be moved if its confidentiality category is not higher than the folder's confidentiality category or the session's confidentiality category)
Folders where automatic confidentiality category assignment is disabled should be used when storing files with different confidentiality categories (lower than or equal to the folder's confidentiality category). To avoid accidentally changing file confidentiality categories when performing operations with them, we recommend using folders with the same mode of automatic category assignment	
Working with applications	
An application is assigned the highest confidentiality category assigned to the files opened in it. The application's confidentiality level does not become lower after the confidential file is closed; it is retained until the application is closed	The application is assigned the confidentiality level of the current user session. Only files with the same or lower confidentiality category can be opened. The category of files with a lower confidentiality level is elevated to the session's confidentiality level (the higher category is assigned when saving the file)
When some applications start, they automatically access certain files. For example, files that were previously opened in the application. However, the file (document) is not actually opened. A specific feature of the Mandatory Access Control mechanism is that when interacting with confidential files in this manner, the user is prompted to elevate the application's confidentiality level to the file confidentiality level. If you do not intend to use the suggested confidentiality level, you can simply decide not to elevate the application's confidentiality level	
Changing the confidentiality category of a resource	
A user who is **not** granted the **Confidentiality category management** privilege cannot elevate a file's confidentiality category higher than its own access level (however, a file's confidentiality category can only be elevated if its category is lower than the directory's confidentiality category)	A user who is **not** granted the **Confidentiality category management** privilege cannot elevate a file's confidentiality category higher than the session's confidentiality category (however, a file's confidentiality category can only be elevated if its category is lower than the directory's confidentiality category)
A user granted the **Confidentiality category management** privilege can: • elevate the confidentiality category of directories and files within the user's access level; • assign a lower confidentiality category to directories and files with a current confidentiality category, but not higher than the user's access level; • change the automatic confidentiality category assignment mode for a directory if the directory current confidentiality category is not higher than the user's access level	A user granted the **Confidentiality category management** privilege can: • elevate the confidentiality category for directories and files, but not higher than the current session's level; • assign a lower confidentiality category to directories and files with a current confidentiality category not higher than the current session's level; • change the automatic confidentiality category assignment mode for a directory if the directory current confidentiality category is not higher than the current session's level
Printing confidential documents	

Disabled flow control	Enabled flow control
If the Print Control mechanism is enabled: • a user **not** granted the **Printing confidential documents** privilege can only print non-confidential documents; • a user granted the **Printing confidential documents** privilege can print confidential documents with a confidentiality category not higher than the user's access level	If the Print Control mechanism is enabled: • a user **not** granted the **Printing confidential documents** privilege can only print non-confidential documents (as long as the document has not been edited); • a user granted the **Printing confidential documents** privilege can print confidential documents with a confidentiality category not higher than the current session's level
If the Print Control mechanism is disabled, any user with access to confidential documents can print the documents, irrespective of whether the user has the **Printing confidential documents** privilege or not. Moreover, the documents will be printed without the confidentiality mark	
Output to external media	
A user who has access to confidential documents can copy files or save their contents to any media, irrespective of the **Output of confidential information** privilege	A user **not** granted the **Output of confidential information** privilege cannot copy confidential files or save their contents to external media

Confidential resource management

Access to confidential file contents is granted to a user if the file confidentiality category is not higher than the user access level. At the same time, the confidentiality category of the device where the file is located is also taken into account.

The confidentiality category of the local drive has higher priority than the categories of files and folders. If the confidentiality category of a file (folder) is lower than the drive confidentiality category, Secret Net Studio treats the category of that file equal to the category of the local drive. Conversely, when the confidentiality category of a file is higher than the confidentiality category of the drive, Secret Net Studio denies access to the file.

Files and folders on the USB, PCMCIA, IEEE 1394 and Secure Digital devices connected to a computer are not assigned any confidentiality category. These files and folders has the same confidentiality category as the device where they are located.

Access levels for users and confidentiality categories for devices are assigned by the administrator. The user can change the 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).

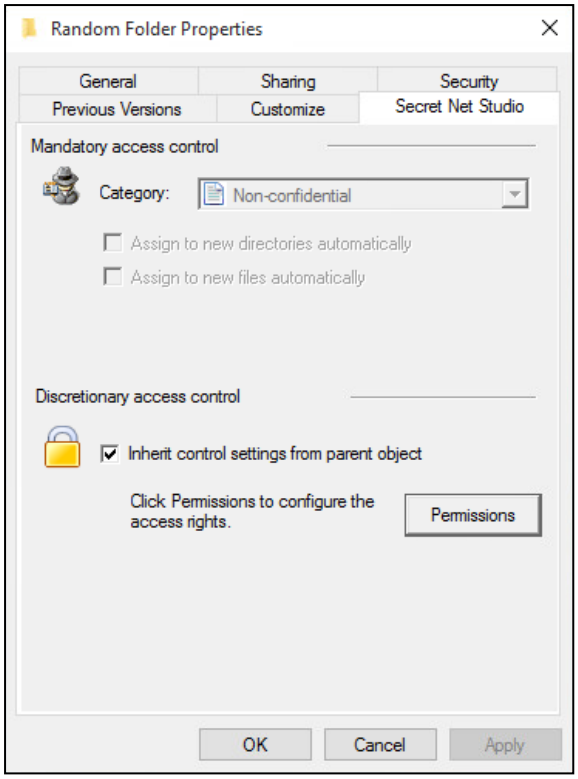
Attention! Note the following general recommendations:

- 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 folders;
- 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 local drive where the objects are located, because a device's category has a higher priority;
- files and folder on the USB, PCMCIA, IEEE1394 and Secure Digital devices cannot be assigned the confidentiality category. They have the same category as the device.

This procedure uses Windows File Explorer.

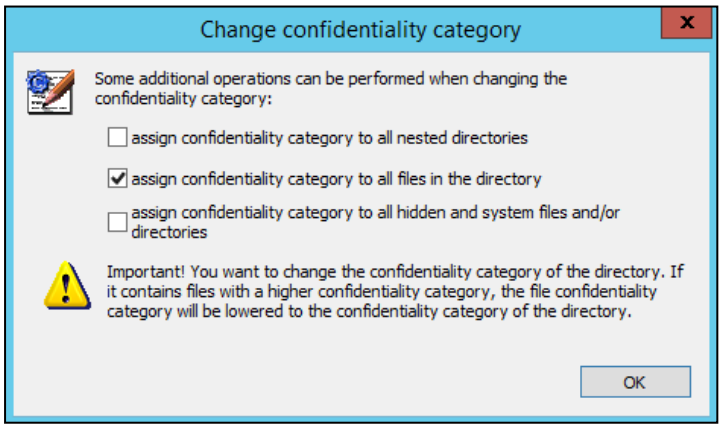
To change the confidentiality category of a folder:

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



2. Configure the required settings:
   - Select the required confidentiality category in the **Category** drop-down list.
   - 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 a folder contains files or subfolders, a dialog box asking you to change the confidentiality category of files and subfolders appears:

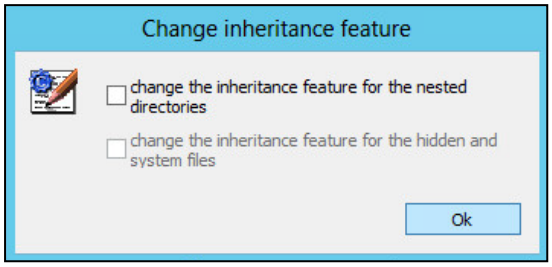


   - If you need to assign a selected confidentiality category to subfolders and also change the status of **assign to new directories automatically** and **assign to new files automatically** settings, select the **assign confidentiality category to all nested directories** check box.
   - If you need 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 and folders, select the **assign confidentiality category to all hidden and system files and/or directories** check box.

     Attention! To avoid system failures, we recommend that you do not assign a confidentiality category to hidden and system files and folders that is not the lowest one (**Non-confidential** by default), unless it is absolutely necessary.
   - Click **OK**.

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

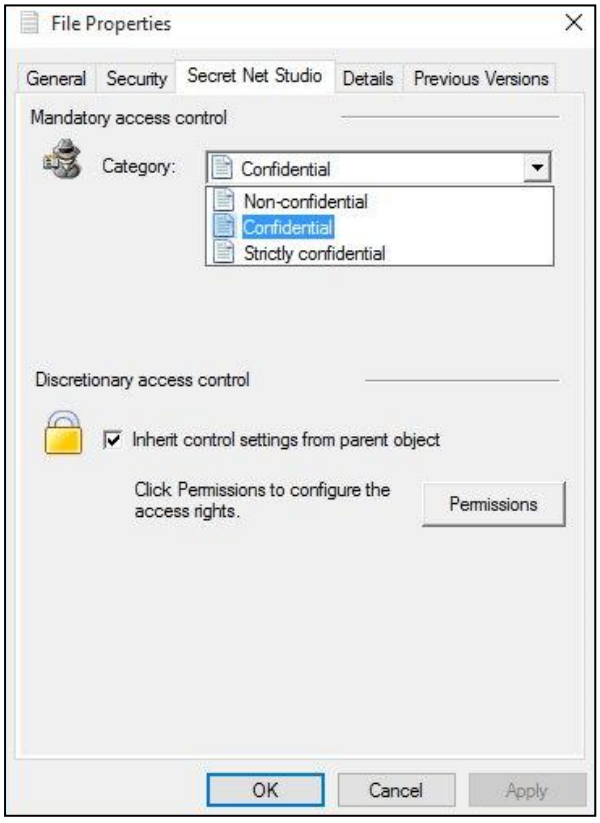
If the value of the **Assign to new directories automatically** or **Assign to new files automatically** settings is changed for a folder containing subfolders, the directory's confidentiality category remains the same and the following dialog box appears:



- If you need to change the status of subfolder settings **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 settings **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 files** 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 the **Secret Net Studio** tab.



2. Choose the required confidentiality category of the files in the **Category** drop-down list.
3. Click **OK**.

Working with confidential documents

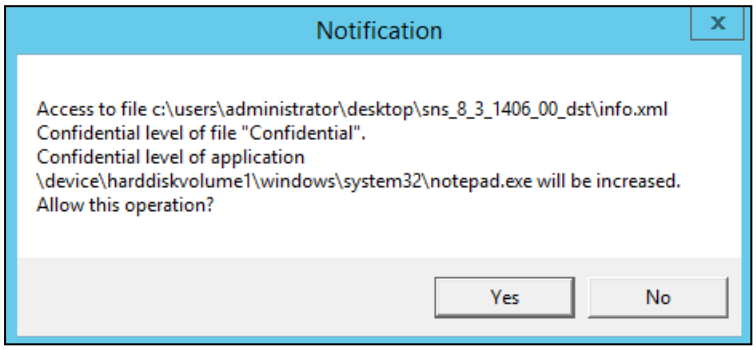
Before you begin working with confidential documents in an editor (for example, MS Word), we recommend saving and closing all previously opened non-confidential documents.

Opening a document

To open a confidential document:

1. Run a 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:



   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 saving 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.

Print 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:

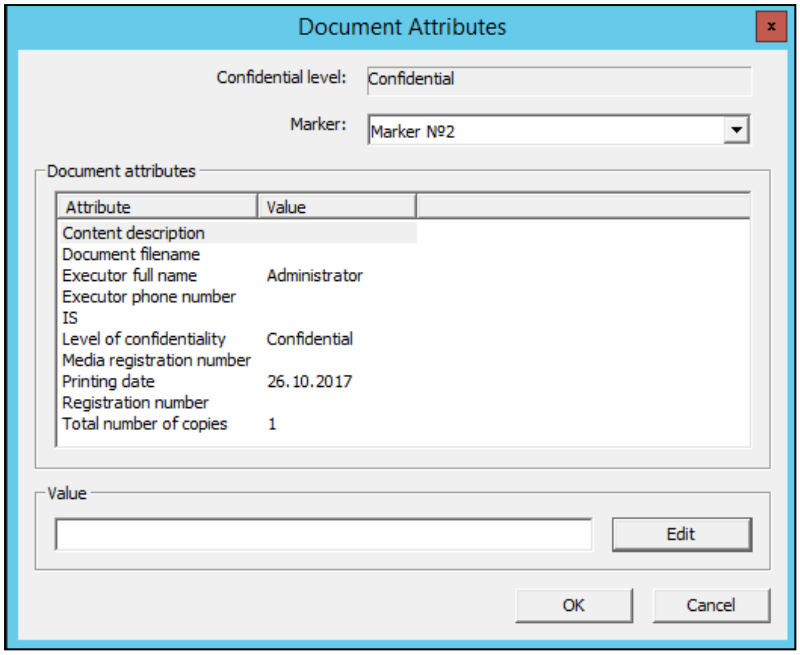
- mandatory fields that are automatically filled out by the security system (for example, **Data, File**);
- custom fields to be filled out by the user prior to printing the document (for example, **Record Number**).

To print a document with a marker:

1. Open a 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 in the figure below.



4. If necessary, change the current marker by selecting the required one in the **Marker** drop-down list. 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 click **Edit**.
5. Click **OK**.

   The document will now be printed with the marker.

Full Disk Encryption

Secret Net Studio allows you to encrypt data on system and non-system disks using the Full Disk Encryption mechanism. Encryption prevents unauthorized access to confidential information on disks.

You can do the following using the Full Disk Encryption mechanism:

- work with information on encrypted disks;
- change the password for encrypted disks;
- restore access to encrypted disks;
- create an emergency recovery disk.

> **Note.** To view the recovery data storage mode, in the Windows taskbar, right-click Secret Net Studio icon and select **Encryption**. The encryption wizard starts. In the top-right corner of the window, you can see the storage mode:
> - locally — recovery data are stored on your computer;
> - on server — recover data are stored centrally.

If the administrator granted you the encryption privilege, the following operations are also available:

- data encryption and decryption on disks;
- changing encryption keys;
- saving recovery data.

> **Attention!** If you save recovery data yourself, remember the passwords and locations where you saved files, as only these data can help you to restore access to encrypted disks.

To access an encrypted disk, you must enter the password before logon. Once you have gained access to an encrypted disk, you can work in an OS as usual.

If errors occur during the operation of the Full Disk Encryption mechanism or you need to restore access to encrypted disks in case of password loss, contact the administrator.

Local encryption in case of local storage of recovery data

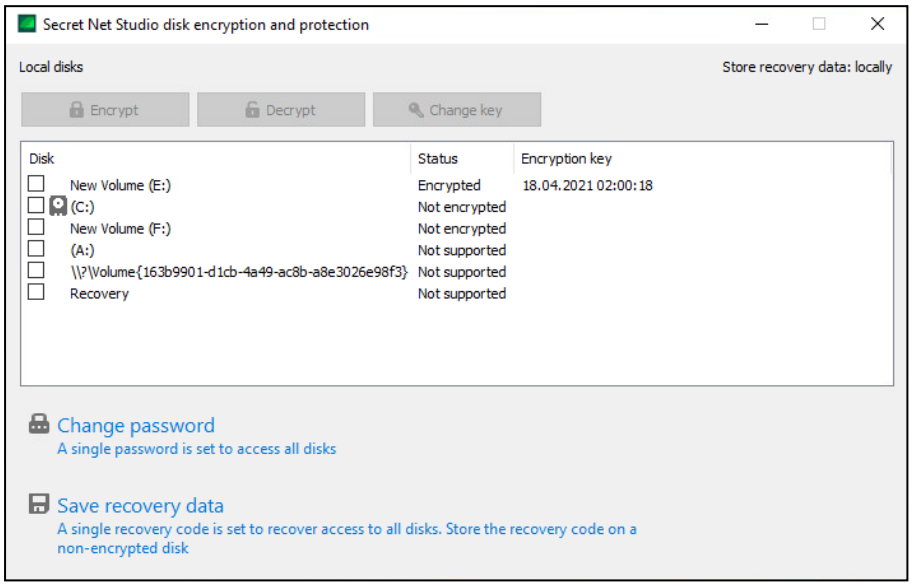
Local encryption is performed using the Secret Net Studio encryption wizard on a computer with disks you want to encrypt. This operation is only available if the administrator gave this privilege to you.

If necessary, you can save the recovery file required for creating an emergency recovery disk. The emergency recovery disk makes it possible to restore access to encrypted partitions. The file contains all the information required for the full restoration of access in case of password loss or drive corruption.

To encrypt disks:

1. Right-click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

   The Secret Net Studio disk encryption protection wizard appears as in the figure below.



   Note. The encryption operation can be run from the shortcut menu of a disk. In **Encryption**, select **Encrypt** and go to step **4** of this instruction.

2. Select the disk you want to encrypt.

   Note.
   - You can encrypt several disks simultaneously. All computer disks are encrypted with the same password.
   - The system disk is shown as  .
   - A disk with the **Not supported** status cannot be encrypted.

3. Click **Encrypt**.

   A dialog box prompting you to enter the password appears.

4. Set a password to access the disk or enter a password for earlier encrypted disks.

   Note. The password must meet the requirements shown in the password request dialog box.

   If necessary, select the check box **change password at the first access to encrypted disks**. In this case, you must change the password at the first boot of the system with encrypted disks.

5. Click **Next**.

   The dialog box for saving the recovery code appears as in the figure below.

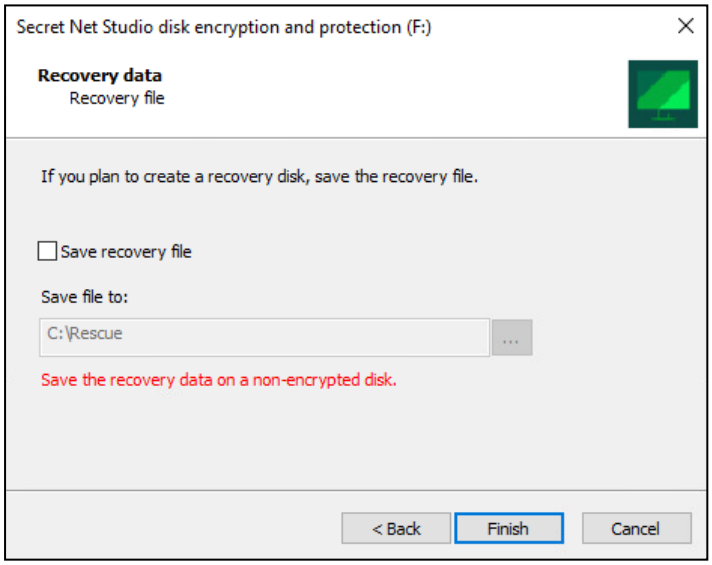
6. Save the system-generated password for the recovery code. Specify the path to save the recovery code.

Attention! Save the recovery data onto a disk different from the encrypted one.

Note. You can save the recovery code for a second time later on (see p. 37).

7. Click **Next**.

The dialog box for saving the recovery file appears as in the figure below.



8. If necessary, select the **Save recovery file** check box and specify the path to save the recovery file.

Attention!

- The recovery file which you are asked to save at this stage becomes obsolete once the encryption has started. We recommend creating a recovery file manually after the encryption process has finished (see p. 37).
- Save the recovery data onto a disk different from the encrypted one.

9. Click **Finish**.

The encryption process begins. You can follow the process in the appeared window.

Attention! During the encryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note.
- To pause the process, click **Pause**. The encryption process will be paused until you click **Resume**.
- To cancel the process, click **Cancel**. The encrypted part will be decrypted. The disk will not be encrypted.
- During the encryption, you can restart the computer from the Windows Start menu. After the restart, the Secret Net Studio bootloader window appears. You need to enter the password to access encrypted disks. After logging on to an OS, the encryption process resumes.

The respective message will appear once the process has finished. The disk status will change to **Encrypted** in the encryption wizard. In the Control Center, on the **General** tab of the Full Disk Encryption element, you can now see information about the encrypted partition.

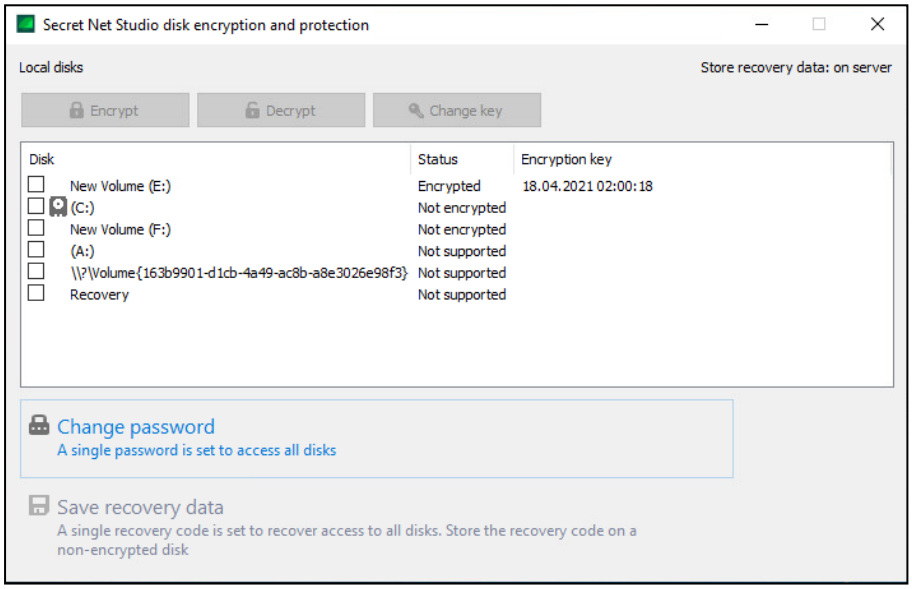
Local encryption in case of centralized storage of recovery data

Local encryption is performed using Secret Net Studio encryption wizard on a computer with disks you want to encrypt. This operation is only available if the administrator gave this privilege to you.

To encrypt disks:

1. Right-click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

   The **Secret Net Studio disk encryption and protection** wizard appears as in the figure below.



Note. The encryption operation can be run from the shortcut menu of a disk. In **Encryption**, select **Encrypt** and go to step **4** of this instruction.

2. Select the disk you want to encrypt.

Note.
- You can encrypt several disks simultaneously. All computer disks are encrypted with the same password.
- The system disk is shown as  .
- A disk with the **Not supported** status cannot be encrypted.

3. Click **Encrypt**.

   A dialog box prompting you to enter the password appears.

4. Set a password to access the disk or enter a password for earlier encrypted disks.

Note. The password must meet the requirements shown in the password request dialog box.

If necessary, select the **change password at the first access to encrypted disks** check box. In this case, you must change the password at the first boot of the system with encrypted disks.

5. Click **Finish**.

   The encryption process begins. You can follow the process in the appeared window.

Attention! During the encryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note.
- To pause the process, click **Pause**. The encryption process will be paused until you click **Resume**.
- To cancel the process, click **Cancel**. The disk will not be encrypted.
- During the encryption, you can restart the computer from the Windows Start menu. After the restart, the Secret Net Studio bootloader window appears. You need to enter the password to access encrypted disks. After logging on to an OS, the encryption process resumes.

The respective message will appear once the process has finished. The disk status will change to **Encrypted** in the encryption wizard.

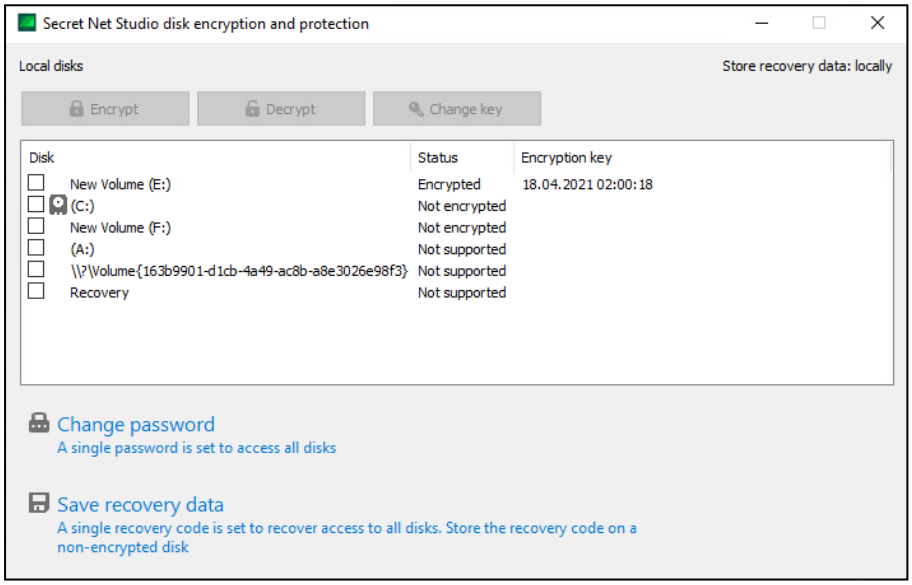
Local decryption

You can decrypt disks locally using Secret Net Studio encryption wizard on a computer with disks you want to decrypt. This operation is only available if the administrator gave this privilege to you.

To decrypt disks:

1. Right-click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

   The Secret Net Studio disk encryption and protection wizard appears as in the figure below.



Note. The decryption operation can be run form the shortcut menu of a disk. In **Encryption**, select **Decrypt** and go to step **4** of this instruction.

2. Select the disk you want to decrypt.

Note.
- You can decrypt several disks simultaneously.
- The system disk is shown as  .

3. Click **Decrypt**.

   A dialog box prompting you to enter the password appears.
4. Enter the password for the disk.
5. Click **Finish**.

   The decryption process begins. You can follow the process in the appeared window.

Attention! During the decryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note.
- To pause the process, click **Pause**. The decryption process will be paused until you click **Resume**.
- To cancel the process, click **Cancel**. The decrypted part will be encrypted. The disk will not be decrypted.
- During the decryption, you can restart the computer from the Windows Start menu. After logging on to an OS, the decryption process resumes.

The respective message will appear once the process has finished. The disk status will change to **Not encrypted** in the encryption wizard.

Actions taken in case of centralized encryption and decryption

The centralized encryption and decryption processes are started by the administrator.

When starting encryption by the administrator:

1. In a dialog box for requesting data for encryption, set a password to access disks and confirm it.

   Note. The password must meet the requirements shown in the password request dialog box.

   If necessary, select the **Change password** check box at the first access to encrypted disks. In this case, you must change the password at the first boot of the system with encrypted disks.

   Then, your actions depend on the recovery data storage mode:

   - in case of local storage, go to step **2** of this instruction;
   - in case of centralized storage, go to step **6** of this instruction.

2. Click **Next**.

   The dialog box for saving the recovery code appears.

3. Save the system-generated password for the recovery code. Specify the path to save the recovery code.

   Attention! Save the recovery data onto a disk different from the encrypted one.

4. Click **Next**.

   The dialog box for saving the recovery file appears.

5. If necessary, select the **Save recovery file** check box and specify the path to save the recovery file.

   Attention!
   - The recovery file which you are asked to save at this stage becomes obsolete once the encryption has started. We recommend creating a recovery file manually after the encryption process has finished (see p. 37).
   - Save the recovery data onto a disk different from the encrypted one.

6. Click **Finish**.

   The encryption process begins. You can follow the process in the appeared window.

   Attention! During the encryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

   Note. To pause the process, click **Pause**. The encryption process will be paused until you click **Resume**.

   The respective message will appear once the process has finished. The disk status will change to **Encrypted** in the encryption wizard.

When starting decryption by the administrator:

If the administrator started the decryption process centrally, a dialog box with information about the process appears.

Attention! During the decryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note.
- To pause the process, click **Pause**. The decryption process will be paused until you click **Resume**.
- During the decryption, you can restart the computer from the Windows Start menu. After logging on to an OS, the decryption process resumes.

The respective message will appear once the process has finished. The disk status will change to **Not encrypted** in the encryption wizard.

Turn on a computer with encrypted disks

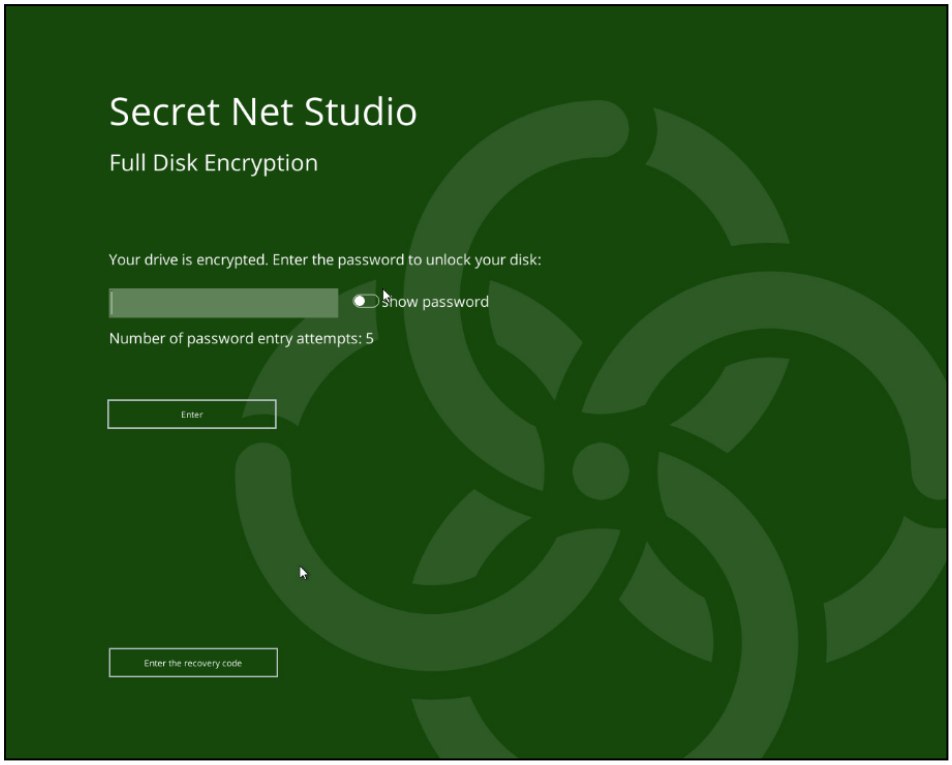
If there are encrypted disks on your computer, Secret Net Studio bootloader window prompting you to enter the password for the disks.

You can work in Secret Net Studio bootloader windows using the mouse and the keyboard. If the computer does not have the mouse, you can use only the keyboard:

- Use **Tab** to switch between active areas (fields, buttons, toggles);
- Use **Enter** to press buttons.

To work on a computer with encrypted disks:

1. Enter the password for the encrypted disks.



2. Click **Next**.

Attention! In case of an invalid password entry the respective message appears. After 5 consecutive unsuccessful attempts, the access will be blocked and a message appears. The access will be available after computer restart.

An OS boots.

If the option of changing the password when accessing encrypted disks for the first time is enabled during the encryption setup, a request to set a new password appears.

In this case, enter a new password, confirm it and click **Next**. The OS boots.

Note. The password must meet the requirements shown in the password request dialog box.

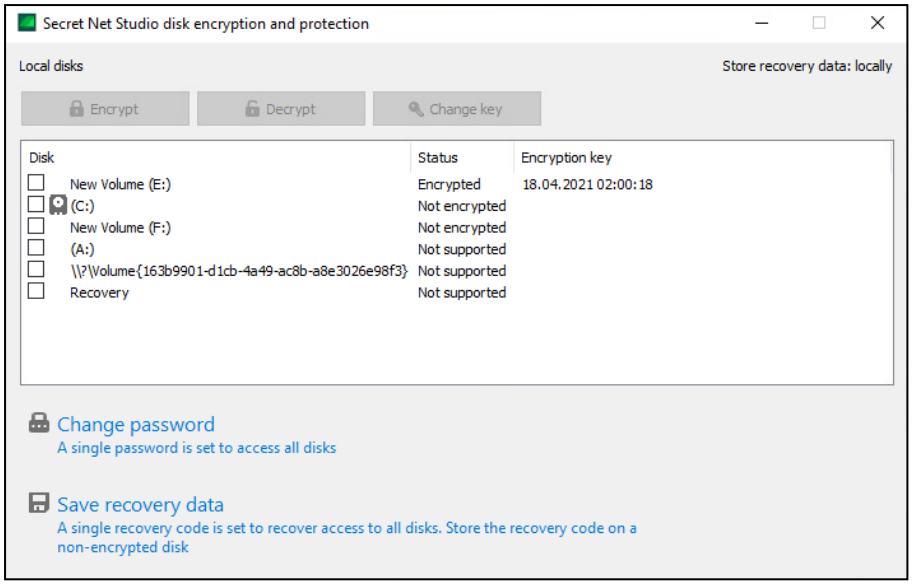
Change the password for disks

You can change the password for encrypted disks using Secret Net Studio encryption wizard.

To change the password for disks:

1. Right-click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

   The Secret Net Studio disk encryption and protection wizard appears as in the figure below.



Note. You can run the password change operation from the shortcut menu of a disk. In **Encryption**, select **Change password** and go to step **3** of this instruction.

2. Select **Change password**.

   A dialog box prompting you to change the password appears.

3. Enter the current password.

Attention! In case of an invalid password entry the respective message appears. After 5 consecutive unsuccessful attempts, the access will be blocked and a message appears. The access will be available after computer restart.

4. Enter a new password and confirm it.

Note. The password must meet the requirements shown in the password request dialog box.

5. Click **Finish**.

Change encryption keys

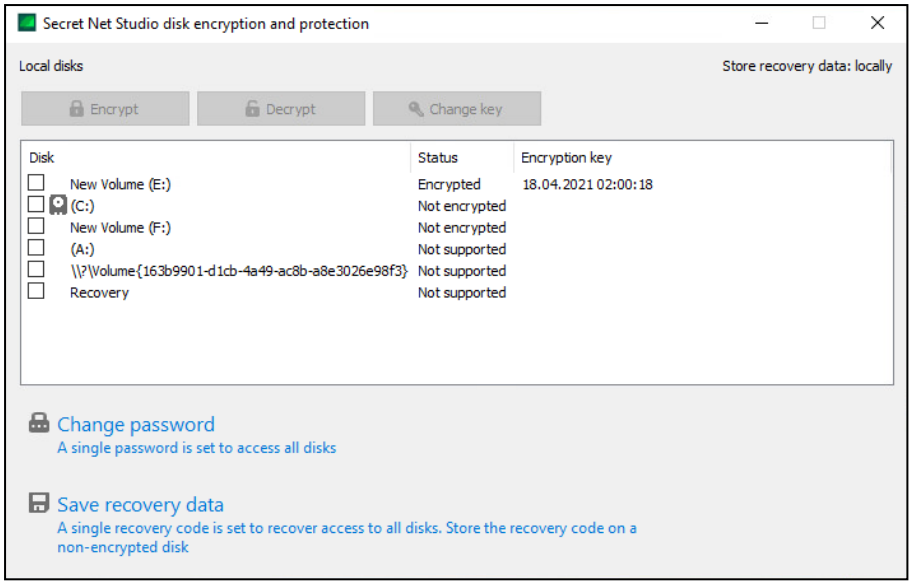
If the administrator granted the encryption privilege to you, you can change encryption keys for disks on your computer. Local encryption keys change is available only for computers with local storage of recovery data and is performed in the Secret Net Studio encryption wizard. As a result of the change, the recovery code is changed. You need to save the new recovery data.

Note. Encryption keys change can be started centrally by the administrator. After the operation, computer restart is required. At system logon, you will see a message that the recovery code has been changed. You need to save the new recovery data. Go to step **4** of the next instruction.

To change encryption keys in the encryption wizard:

1. Right-click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

   The Secret Net Studio encryption wizard appears as in the figure below.



Note. You can run the keys change operation from the shortcut menu of a disk. In **Encryption**, select **Change encryption key** and go to step **4** of this instruction.

2. Select the encrypted disk for which you want to change encryption keys.

Note.

- You can change encryption keys for several encrypted disks simultaneously.
- The system disk is shown as .

3. Click **Change key**.

   A dialog box prompting you to enter the password appears.

4. Type the password to access encrypted disks and click **Finish**.

   The process of decrypting data for changing the key begins.

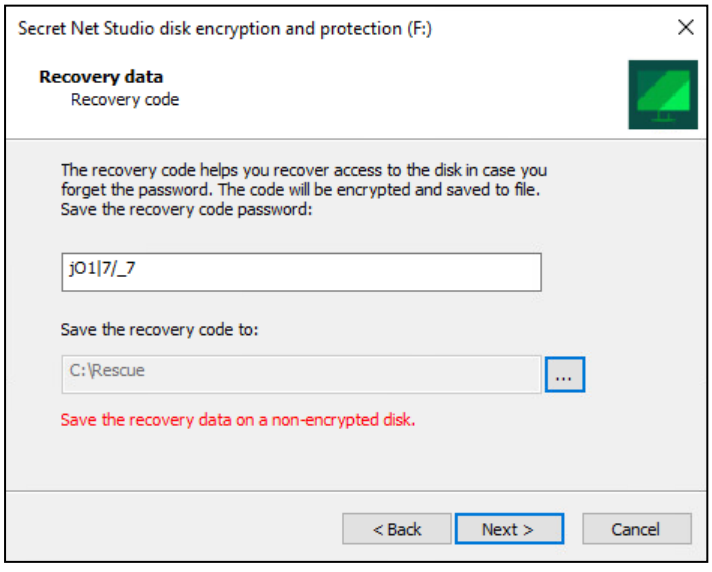
Attention! During the decryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note. During the decryption, you can restart the computer from the Windows Start menu. After logging on to the OS, the process resumes.

   After the process is complete, you are prompted to enter the password for encrypted disks in order to save the new recovery data.

5. Type the password and click **Next**.

   The dialog box for saving the recovery code appears as in the figure below.



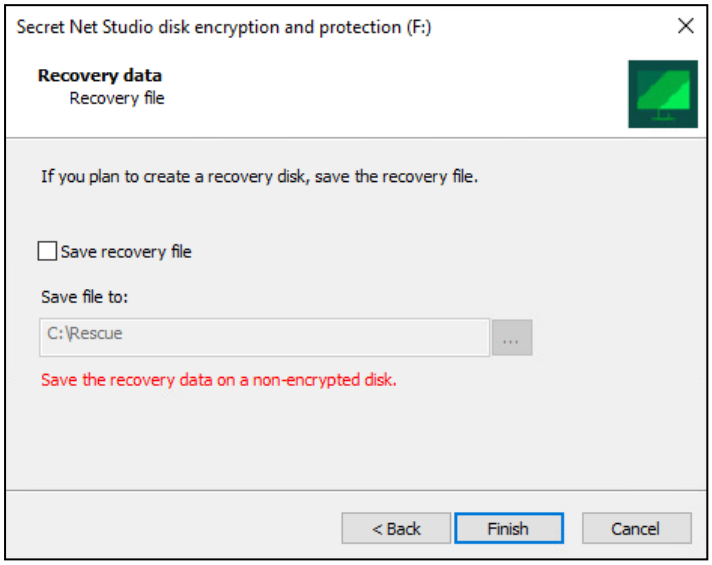
6. Save the system-generated password for the recovery code. Specify the path to save the recovery code.

Attention! Save the recovery data onto a disk different from the encrypted one.

Note. You can save the recovery code for a second time later on (see p. 37).

7. Click **Next**.

The dialog box for saving the recovery file appears as in the figure below.



8. If necessary, select the **Save recovery file** check box and specify the path to save the recovery file.

Attention! Save the recovery data on a disk different from the encrypted one.

9. Click **Finish**.

The process of encrypting data with the new key begins.

Attention! During the encryption, in order to avoid data corruption or loss, you must not restart the computer using the Reset button or turn off the drive.

Note. During the encryption, you can restart the computer from the Windows Start menu. After logging on to an OS, the process resumes.

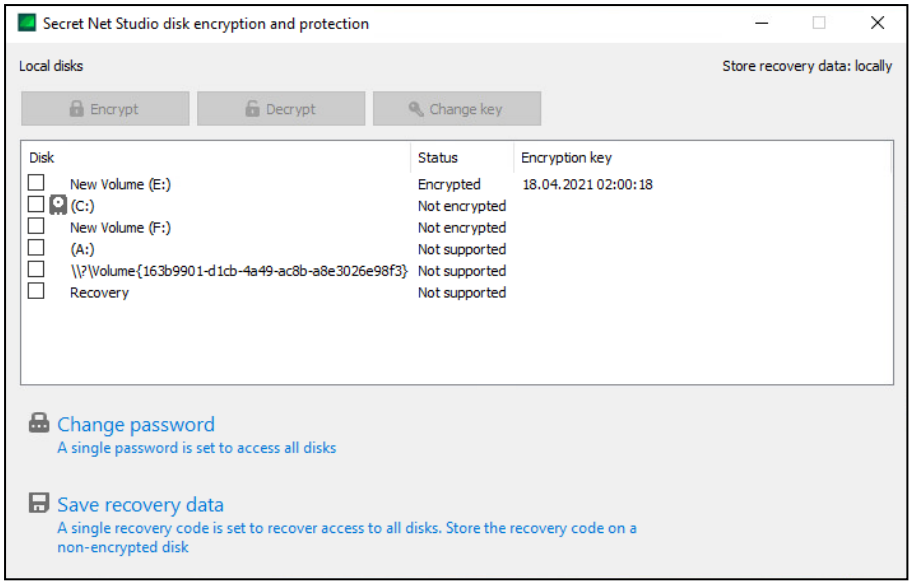
Save recovery data

If the administrator granted you the encryption privilege, you can save recovery data for the second time for encrypted disks on your computer. The operation is available only for computers with local storage of recovery data and is performed in the Secret Net Studio encryption wizard.

To save recovery data:

1. Right-click the Secret Net Studio icon in the Windows taskbar. Select **Encryption**.

The Secret Net Studio encryption wizard appears as in the figure below.



Note. The operation can be run from the context menu of a disk. In **Encryption**, select **Save recovery data** and go to step **3** of this instruction.

2. Select **Save recovery data**.

   A dialog box prompting you to enter the password for disks appears.
3. Type the password and click **Next**.

   The dialog box for saving the recovery code appears.
4. Save the system-generated password for the recovery code. Specify the path to save the recovery code.

Attention! Save the recovery data onto a disk different from the encrypted one.

5. Click **Next**.

   The dialog box for saving the recovery file appears.
6. If necessary, select the **Save recovery file** check box and specify the path to save the recovery file.

Attention!
- The recovery file which you are asked to save at the encryption stage will become obsolete once the encryption has started. We recommend creating a recovery file manually after the encryption process has finished.
- Save the recovery data onto a disk different from the encrypted one.

7. Click **Finish**.

Working with encryption keys

A user's key information is located on a key device: a personal security token, 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. The key information can be changed by the user individually or by the administrator.

Loading and unloading an encryption key

Encryption user keys are loaded automatically or forced by a user command. They are automatically loaded during user logon if a security token 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.

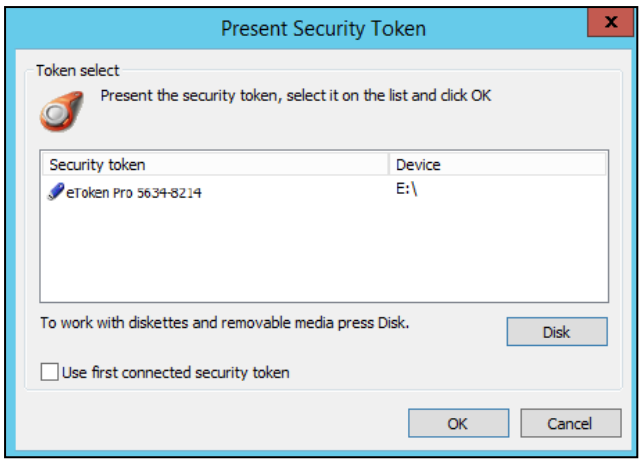
To unload keys, you can also use a special command or let the system do it automatically after you finish your session.

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:



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

   Tip. If multiple disks are connected, select the required device on 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 current private key and the old key (appears after the private key is updated). When loading key information, the security system checks both the current 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 security token. 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.

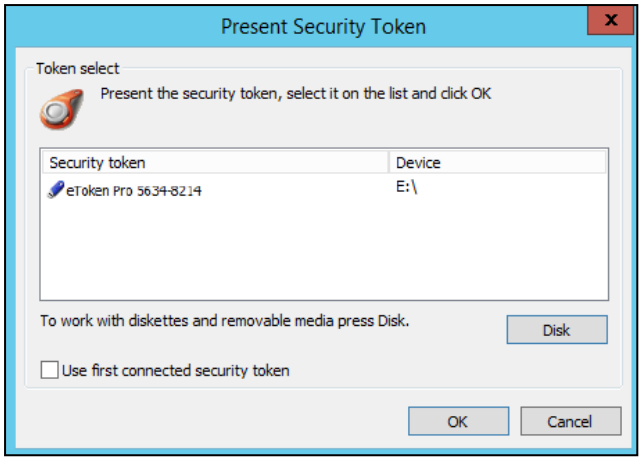
Attention! The encrypted container must be available for automatic re-encryption of control information. For example, if an encrypted container is not available in the network or is located on a currently disconnected removable device, re-encryption is not possible. In this case, once the keys are changed 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 to the list of users with access to the encrypted container again.

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.

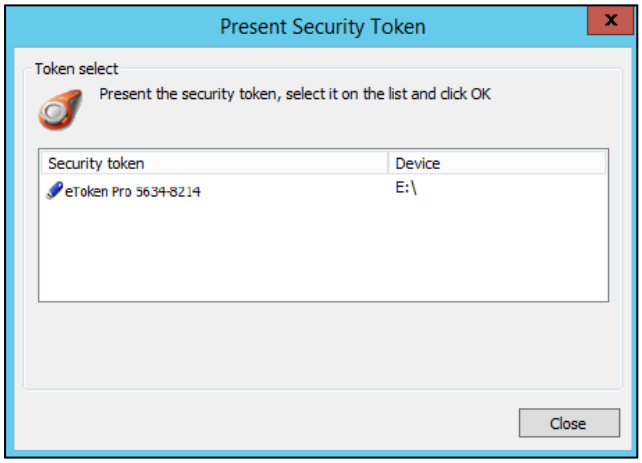
The following dialog box appears:



2. Present one of the key devices containing the current key information. Depending on the key device type (a personal security token or a removable device), perform the appropriate step:
   - if you are using a personal security token, 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 listing all your key devices where you can save the new key information appears.



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 security token is protected by a custom PIN, a prompt appears. 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, 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 security system interrupts the operation being executed. Below are the security 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 security token, or a removable drive was disconnected while reading.

User actions. Restore contact between the reading device and the personal security token 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 security token that belongs to another user.

User actions. Present your own personal security token.

```
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.

Working with encrypted containers

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.

Create encrypted containers

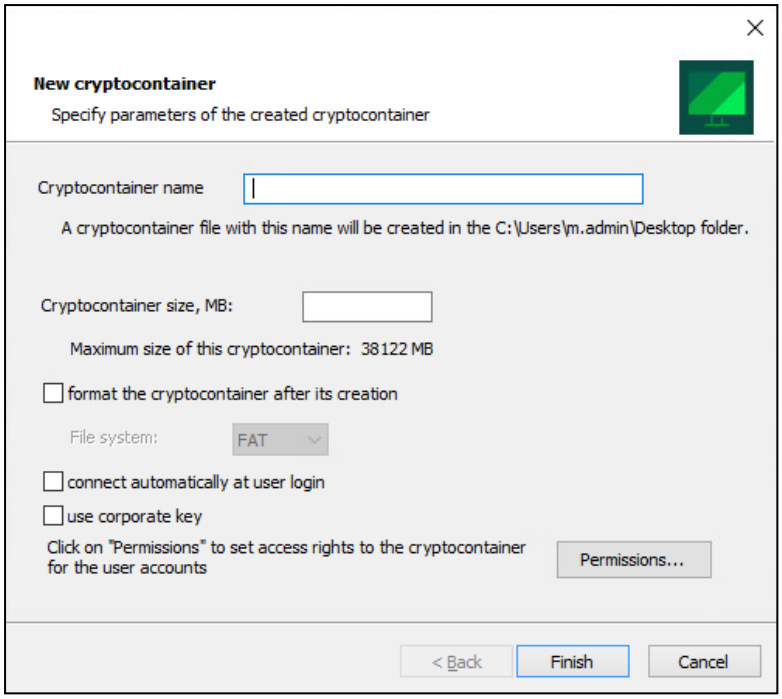
The right to create encrypted containers is available to users with the appropriate privileges. This privilege is granted by default to all accounts included in the local group of administrators. A user who creates an encrypted container is granted the right to manage it and can delegate (grant) the 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 display area of the folder, point to **New** and click **Secret Net Studio encrypted containers**.

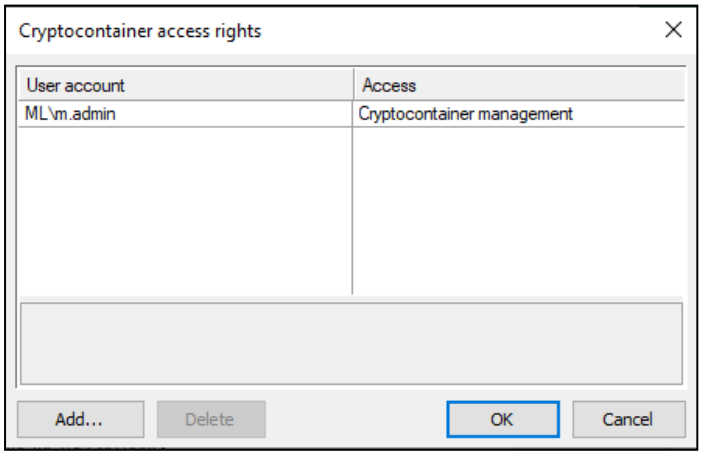
   A **New cryptocontainer** dialog box appears, as in the figure below.



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** check box 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 the **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 the 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 grant access permissions to the encrypted container for the user accounts, click **Permissions**.

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



8. Edit the list of accounts by clicking **Add** and **Delete**. You can only add users who have encryption keys. To change access rights for an account, select it in the **Access** list and specify the value for it (to open the list of available values, click the button on the right of the cell).

   Attention!
   The maximum number of users with access rights to a single encrypted container is 200.

9. Click **OK**.
10. Click **Ready** in the dialog box 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 prompting you to create an 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 folder for the file and complete this procedure starting from step **3**.

Connect encrypted containers

When connecting an encrypted container, 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 formatted, if it was not done when the encrypted container was created).

To connect an encrypted container:

1. Load encrypted keys (see p. **38**).
2. Right-click the encrypted container and click **Connect**.

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

3. Select the drive letter in the **Assign a letter to the cryptocontainer disk** drop-down list.
4. If necessary, set up additional connection parameters:
   - to enable write protection for the encrypted container, select the **connect for read only** check box;
   - to enable automatic connection of the encrypted container during logon, select the **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.

Disconnect encrypted containers

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 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 logical drive 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.

View and configure encrypted container settings

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

To open the dialog box, 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. **41**).

Re-encrypt 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 changing user keys, where only part of the control information is re-encrypted). When using the security 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**.

Delete encrypted containers

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

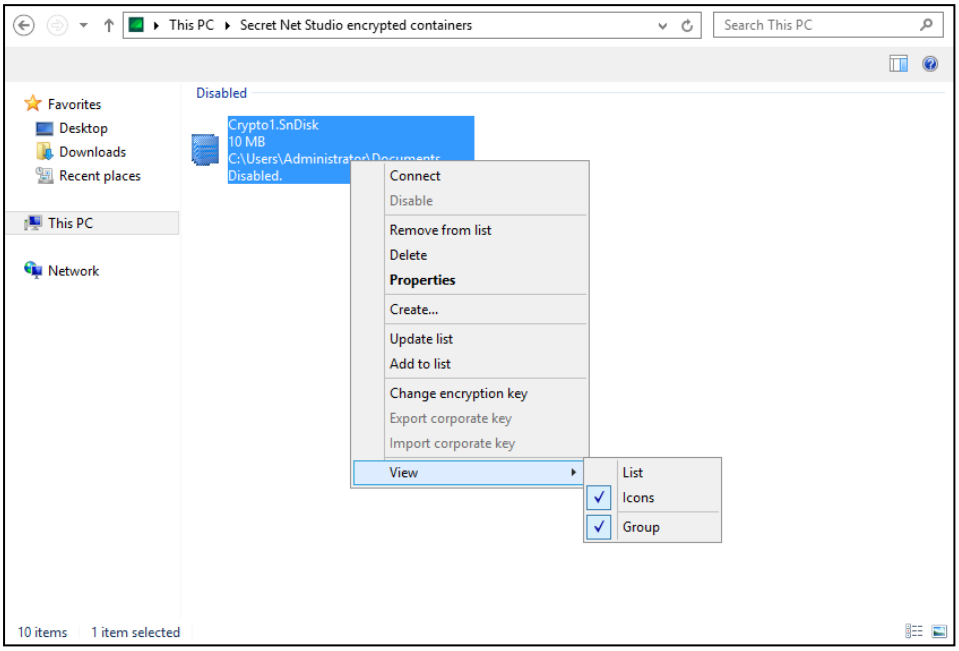
You can remove encrypted containers in one of the following ways when working with the list of encrypted containers in the **Secret Net Studio Encrypted Containers** folder:

- remove it 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**;
- delete 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**.

Manage encrypted container list

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



Shortcut 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
Working with Trusted Environment

If Trusted Environment is enabled, you need a boot device (a specialized USB flash drive containing service information) to start the computer.

Logging on to the system, working on a computer and shutting it down is performed in normal mode.

Starting the computer

To start the computer with enabled Trusted Environment:

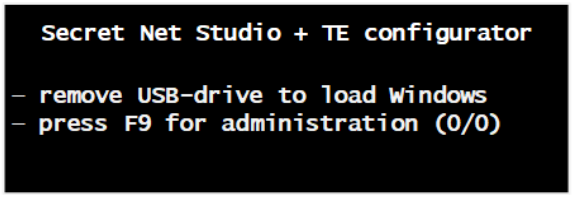
1. Connect a boot drive to the computer.

   Attention! When you start the computer without a boot device, the operating system will boot. The following message appears on the lock screen: **Functional check error. Reasons: Trusted Environment does not function**. You will be unable to log on to the system.

2. Start the computer.

   Loading data from the boot drive begins.

   If data is successfully loaded, the Trusted Environment menu appears.

   Note. In case of errors, turn off the computer by holding the Power button on the system unit. Start the computer again. If errors still occur, contact the administrator.

3. Disconnect the boot drive.

   The operating system will boot.

4. Log on to the system (see p. **10**).

Chapter 6
Using network protection tools

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 7
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 targeted at hard drives, network folders, external data storage media, email messages and other objects.

Note. File scan is available only with access to read files and folders. Otherwise, you will receive an error message and a scan will not performed.

You can also scan selected files from the Windows shortcut menu (see p. **48**).

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

Attention! We do not recommend scanning network folders. Infected network files are moved to a local quarantine, so they are harder to restore.

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

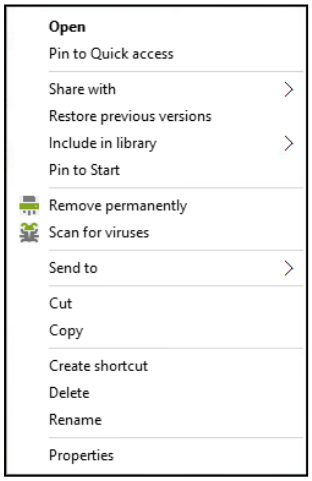
The behavior of Antivirus and its response to detected malware are configured centrally by the administrator using the Control Center.

Context scanning

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

To do a scan:

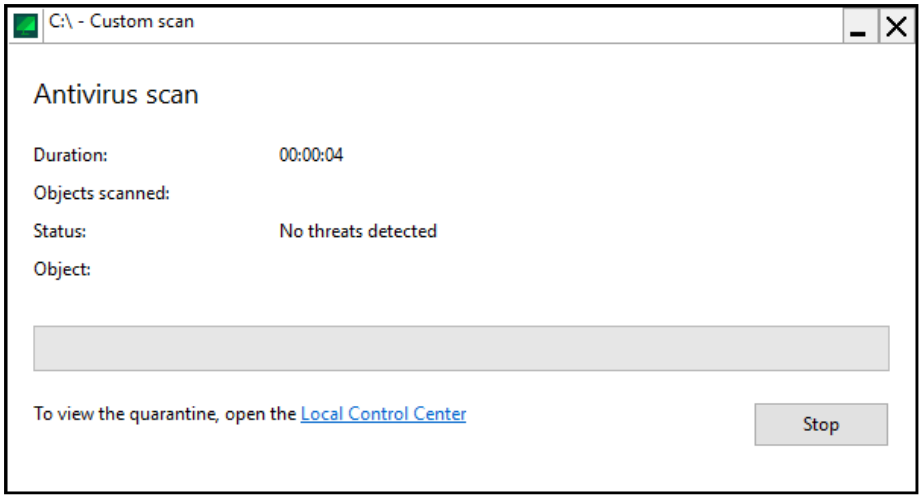
1. Right-click the file(s), folder(s) or drive(s).



2. Click **Scan for viruses**.

Tip.
- You can run multiple scans simultaneously.
- If you need to scan object(s) from the exclusion list, right-click the object(s) while holding **Shift** and click **Scan for viruses (ignore white list)**.

Secret Net Studio Antivirus scans the object(s) and the following window appears.



Tip. To stop the scan, click **Stop** or close the dialog box.

3. When the scan is completed, check the results and click **Close**.

   To view detailed results of the scan and the list of quarantined files, click the **Local Control Center** link or, in the Local Control Center, on the **Computer** panel, on the **Status** tab, click **Antivirus** and, on the **Antivirus** panel, go to the **Quarantine** tab.

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 respective message appears.

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

This mechanism settings are configured by the security administrator using the Control Center.