SECURITY code

Sobol
Version 4

Basic Operations

User Guide

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

Table of contents

Introduction

This guide is designed for the product users Hardware Trusted Boot Module Sobol. Version 4" (hereinafter — Sobol). It contains the information which users need to work with Sobol.

The guide is organized in the following way:

- the **Power on computer** section describes how to log on to the information system from a computer with Sobol;
- the **Change password** section describes how to change an individual password and Sobol Secure ID;
- the **Shut down and restart computer** section describes how to shut down a computer with Sobol.

Web-site. 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. Technical support web-page:https://www.securitycode.ru/.

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

Power on computer

In order for you to work on a computer with Sobol, the administrator must register you as a Sobol user and give you the credentials listed in the section below.

After the user provides the credentials and the controlled objects integrity is checked (if the integrity check mechanism is enabled by the administrator), the operating system (hereinafter — OS) boots.

In case of Sobol errors and failures, contact your administrator.

User credentials

To power on a computer with Sobol, you need the following credentials:

- your Secure ID contained in a security token;

  Note. Security ID is a data structure which is involved in the user authentication procedure. Each user has a unique Secure ID.

- a password which corresponds to the security token;
- a security token PIN (can be enabled if using USB keys).

Remember your password and PIN. Do not share them with anyone.

Keep your security token with you as you will need it every time you power on your computer.

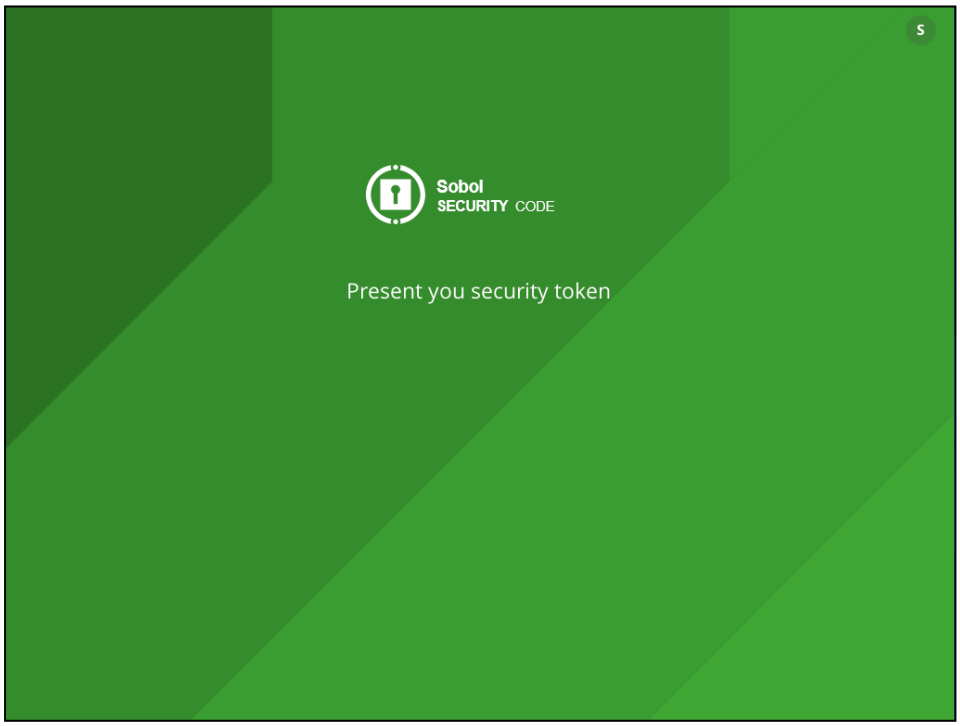
OS booting

Attention! Before powering on a computer with Sobol, disconnect from USB ports all USB Mass Storage devices (flash drives, CD and DVD drives, etc.).

To boot an OS:

1. Power on your computer. The **Getting ready...** window appears.

   When Sobol is successfully loaded, you are prompted to present your security token.



   Sobol operation mode is indicated in the top right corner: **S** is for the standalone mode, **J** is for the joint mode:

   - the standalone mode means that Sobol operates autonomously;
   - the joint mode means that Sobol operates in tandem with other products (for example, Secret Net Studio).

   A timer may appear in the center of the window:

   - for an automatic logon timeout (in seconds);

- for a timeout to present your security token and enter the password (in minutes and seconds).

Note.
- Automatic logon timeout is displayed if Sobol is configured to boot automatically. In this case, your credentials are not required. When the specified time is over, the integrity check is performed (if the integrity check mechanism is enabled) and the OS boots (see p. 7).
- The time left to present your security token and enter the password is displayed if the logon timeout mode is enabled by the administrator. If you cannot present the security token and enter the password in the allowed time, the computer is blocked. Restart your computer and log on again.

2. Present your security token:

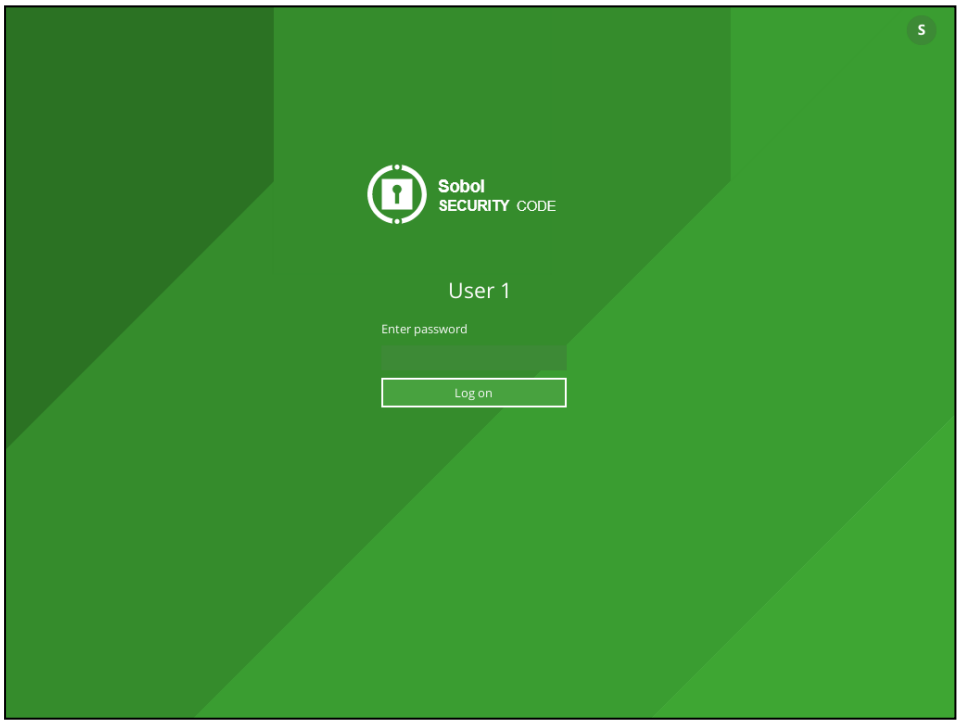
- for iButton — place the security token to the reader;
- for USB key — connect the security token to a USB port;
- for smart card — insert the security token to a USB smart card reader.

Note.
- If the security token is already presented (iButton is in contact with the reader / USB key is connected to a USB port / smart card is inserted into the reader), Sobol automatically reads it.
- If several security tokens are presented, Sobol reads the first one being detected. Press <Esc> to change the security token.
- If the security token is presented incorrectly, the request remains on the screen. Present the security token again.
- If the message **Logon is prohibited by administrator** appears, click **OK** and contact the administrator to find out the cause of the blocking.

After the security token is presented successfully, you can be prompted to enter the PIN.

Note. The PIN is required if the administrator has set a PIN for your security token. If the PIN is required, enter it and click **OK** or press <Enter>.

After the security token information is successfully read, you are prompted to enter the password.



Note. You are not prompted to enter the password if it has zero length (blank password).

3. Enter your password and click **Log on** or press <Enter>.

Note. All entered characters are displayed as "*".

Attention!

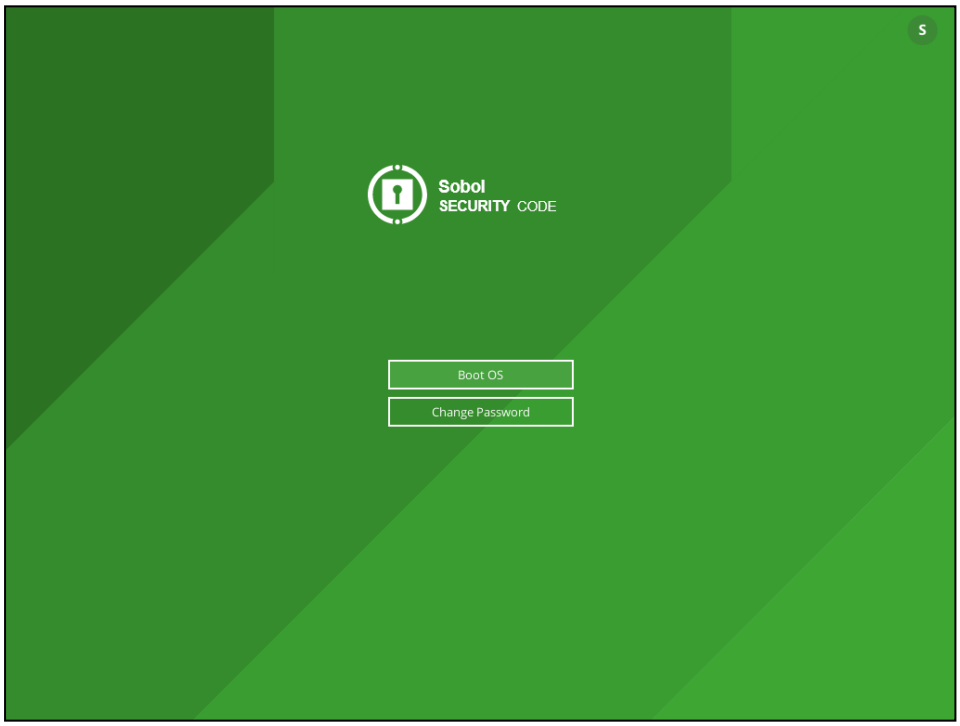
- If the presented security token is not registered or the password is incorrect, the following message appears: **Invalid password or security token**. Click **OK** and repeat steps **2**, **3**. Use your security token and enter the valid password.
- The number of failed logon attempts per session is 5. If you exceed the limit, your computer is blocked. In this case, contact the administrator.
- The total number of failed logon attempts can be limited by the administrator. If you have exceeded this limit, when trying to log on next time, you will see a message saying that the computer has been blocked. In this case, contact the administrator.
- When the **Password does not meet complexity and/or minimum length requirements** or **Password expired** messages appear:
  - if you are allowed to change the password, click **OK** and change it following the instructions on p. 9 (starting from step **2**);
  - if you are not allowed to change the password, the computer is blocked. Contact the administrator.

If the password is entered successfully, the expiration date of your account is checked.

Note. The administrator can configure your work schedule or set a logon restriction. If there are restrictions set for you, it is checked how long your account has been used and how much time left you have:

- if your account has expired, the **Your account has expired** message appears. Contact the administrator;
- if a logon is performed at a time that has not been specified, the **Logon cannot be performed because of the account restrictions. Please try again later** message appears. Please try again later;
- if the validity period has not started, the **Logon cannot be performed because of the account restrictions** message appears. Please try again later.

If the checks of your account validity period are completed successfully, the window appears as in the figure below.



Note. The window can contain help information (see p. 8).

4. Click **Boot OS**.

Attention! If there are any encrypted disks on your computer that were created using Secret Net Studio, and IC is enabled, you will be prompted to enter the password for the encrypted disks at this stage. Enter it to decrypt the volumes.

After you have successfully presented your credentials, one of the following scripts will be performed:

- The OS will boot.
- The integrity check will start if the integrity check mechanism is enabled by the administrator.

Note. Before the integrity check, the IC key may be updated with further recalculation of the controlled object checksums.

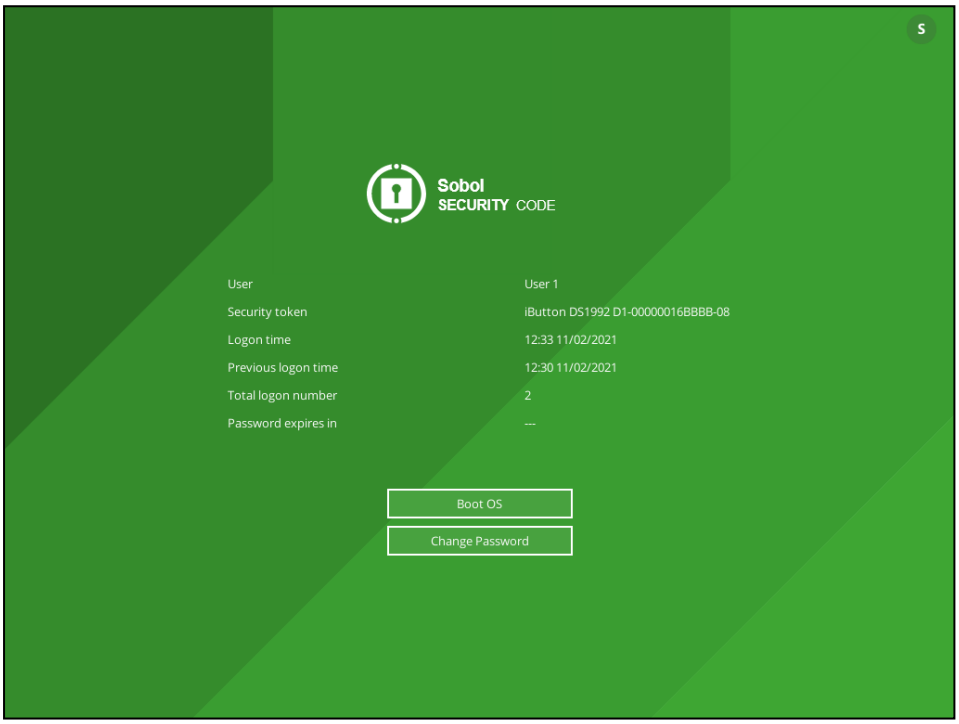
If the integrity check is completed successfully, the OS starts to boot.

Note.

- In case of an error, the check stops and an error message appears. Click **OK**.
- If you do not want to receive notifications during the integrity check, select **Don't ask again** in the error message window.
- When the integrity check is finished, click **Finish**. The **Controlled object integrity violated** message appears.
- If hard mode is enabled, the computer is blocked if the controlled objects integrity is violated. Shut down the computer and contact the administrator.
- If soft mode is enabled, you will be able to continue working on the computer if the controlled objects integrity is violated. Click **OK**. The OS starts to boot.

Help information

If the help information display is enabled by the administrator, a window as in the figure below appears after you enter the credentials.



Note. Help information is not displayed in joint mode.

The window displays the following information about the user account:

Field	Description
User	A name that is registered in the list of Sobol users
Security token	Type and number of the presented security token
Logon time **Previous logon time**	The time (hours:minutes) and the date (day/month/year) of your successful logon in the current or previous session. The time and date are set when you click **Log on** while entering the password in Sobol
Total logon number	Number of your successful logon attempts since your registration in the list of Sobol users
Password expires in	Number of days until your password is expired. Displayed only if password expiration mode is enabled by the administrator

Change password

You can change the password if it is allowed by the administrator.

Note. When changing the password, the Secure ID can also be changed if this mode is enabled by the administrator.

To change the password:

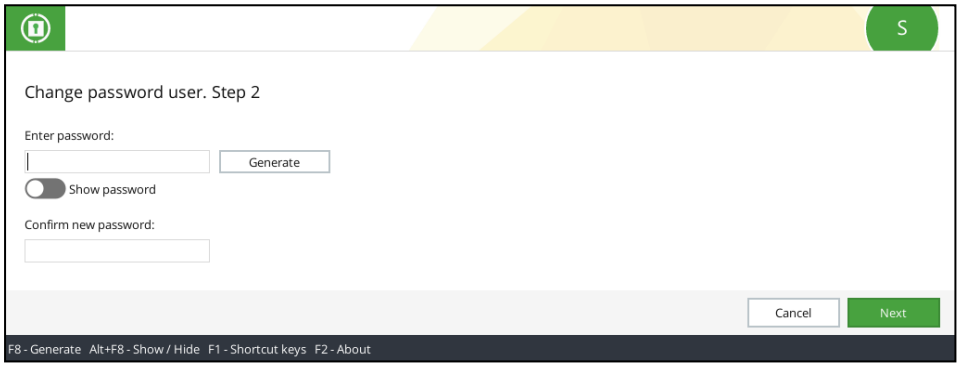
1. After you successfully logged on, in the Sobol window, click **Change Password** (see p. 8).

   Note. If the **Change Password** button is inactive you are not allowed to change your password.

   You are prompted to enter your current (old) password.
2. Enter your current (old) password and click **Next**.

   Note. When changing the password, you can use the shortcut keys. To view the shortcut keys, press <F1>.

   The **Enter password** window appears:



3. In the **Enter password** text box, type a new password or use random password generator.

   Note.
   The password can contain only the following characters:
   - 1234567890 — digits;
   - abcdefghijklmnopqrstuvwxyz - lowercase Latin letters;
   - ABCDEFGHIJKLMNOPQRSTUVWXYZ - uppercase Latin letters;
   - _$!@#;%^:&?*)(-+=/|.,<>`~"\ - special characters.

   To generate a random password, click **Generate** or press <F8>.

   Note. When generating a random password, take into account the following:
   - if the complexity check is enabled, the password generated must meet the complexity requirements set by the administrator;
   - if the complexity check is disabled, the password generated must consist of digits and lowercase Latin letters;
   - a password generated by Sobol can be edited.

   To view the password, press the <Alt>+<F8> or turn on the **Show Password** toggle.
4. In the **Confirm new password** text box, enter the new password again.
5. Click **Next**.

   Note. If the entered password is incorrect, a message describing the error appears. Click **OK** and enter the correct password.

   If the password is entered successfully, you are prompted to present your security token.

   Note. Before presenting the security token, you can cancel the password change. To do so, click **Cancel**.
6. Present your security token.

   Note.
   - If the security token has already been presented (iButton is in contact with the reader / USB key is inserted / smart card is in contact with the reader), Sobol automatically reads it.
   - If several security tokens are presented, Sobol reads the first one being detected.

   If the administrator has set a PIN for your security token, you are prompted to enter it after presenting the security token.

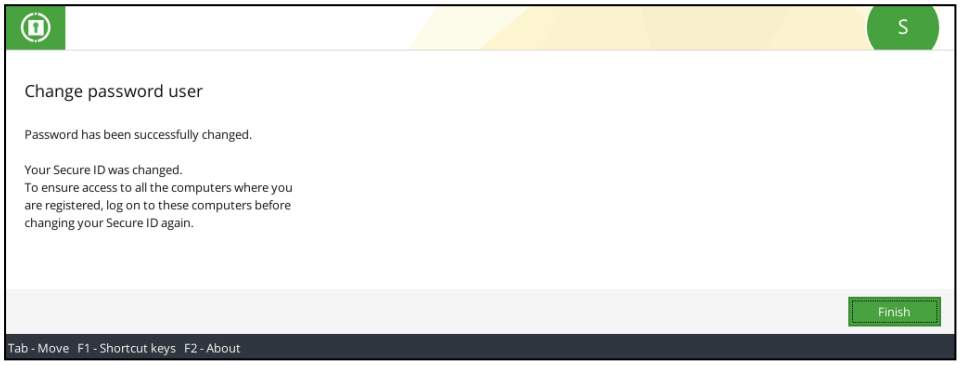
   Note. When you are prompted to enter the PIN, enter it and click **OK**.

If the security token is presented correctly, the old password is compared to the information stored in the security token memory:

- if the old password does not match the presented security token, the **Invalid password or security token** warning appears. Click **OK**. Present your security token or click **Cancel** and try to change the password again.
- If the old password matches the presented security token, the security token saves the service information related to the new password.

After the service information has successfully been saved, the **Password has been successfully changed** message appears.

If your Secure ID is also changed, you receive the respective message.



Having changed the Secure ID, you must log on to each computer on which you are registered as a Sobol user at least once before the Secure ID is changed again.

Note. Your security token stores two Secure IDs (the current one and the previous one). When a new Security ID is written, the old one is deleted and the current one is saved, allowing you to access other computers on which you are registered as a Sobol user. If you have not logged on to any of these computers since the last time the Secure ID was changed, you will lose access to it, because the old Secure ID, which is required for your authentication on this computer, has already been deleted from the security token memory.

7. Click **Finish**.

Shut down and restart computer

To shut down and restart a computer with Sobol, follow the respective instructions for the OS running on your computer.