SECURITY
code

# Sobol
# Version 4

# Setup and Operation

## Administrator guide

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

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

# Table of contents

# Introduction

This manual is designed for administrators of Hardware Trusted Boot Module Sobol. Version 4 (hereinafter — Sobol, the product). It contains information that administrators need in order to install, configure and use the product.

For information on how to configure Sobol software, see document [**1**].

For information for users on how to work with Sobol, see document [**2**].

**Chapter 1** contains general information about Sobol protection mechanisms.

**Chapter 2** describes how to install the product.

**Chapter 3** describes how to update and remove the product.

**Chapter 4** describes how to configure and work with the product.

**Chapter 5** contains information about built-in IC template management.

**Appendix** contains Sobol messages, events and other information about Sobol operation.

**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.

# Chapter 1
# General information

## Purpose

Sobol is designed to prevent unauthorized access to resources of a protected computer.

Sobol comes in the following modifications described in the table below.

**Tab. 1 Cards used in Sobol**

| Card | Type | Controlled two-channel hardware RNG |
|---|---|---|
| PCIe | 1 | + |
| | 2 | – |
| | 3 | + |
| | 4 | – |
| Mini PCIe Half | 1 | + |
| | 2 | – |
| M.2 | 1 | + |
| | 2 | – |
| | 3 | + |
| | 4 | – |

The core functions of Sobol are:

- user identification and authentication while logging on to the system using security tokens (see Tab. 2 on p. **7**);
- protection from unauthorized boot using removable drives (floppy disks, ZIP, USB drivers, etc.);
- software and hardware integrity check before OS startup for the following objects:
  - files;
  - hard drive sectors;
  - system registry keys;
  - transaction log;
  - PCI devices;
  - SMBIOS data;
- computer lockout in case after it is turned on, control is not transferred to Sobol UEFI Option ROM
- control of the main Sobol components (RNG operation, nonvolatile card memory and personal security tokens);
- registration of events related to information system security;
- interoperation with Continent, Continent RA, Secret Net Studio, Secret Net LSP.

**Note.** Sobol interoperates with other information security products in joint mode. For detailed information about Sobol joint mode, see p. **99**.

Sobol can protect computers and servers of a local network and standalone computers.

## Operation principles

Sobol checks user credentials for logon. A user can log on to the system only if he or she presents the personal security token and types the password; otherwise, logon is denied.

**Note.** To access a computer, a user must be registered in the Sobol user list. Sobol administrator registers a user by assigning a name, a personal security token and a password for him/her. The administrator account is created during Sobol initialization.

The core protection mechanisms of Sobol are:

- user identification and authentication (see p. **7**);
- protection from unauthorized boot from removable drives (see p. **8**);
- software and hardware integrity check before OS startup (see p. **9**);
- watchdog timer (see p. **10**);
- registration of events related to information system security (see p. **11**);
- control of the main Sobol components (see p. **11**).

**Note.** Sobol can operate with IC and watchdog timer mechanisms or without them.

To prepare Sobol for operation, you need to initialize it — to configure system, general, password, log and IC settings, create an administrator account and calculate checksums.

Sobol supports hardware defined and software defined initialization.

Hardware defined initialization is performed before starting using Sobol, including the first installation of a Sobol card. Also, it may be used to reset settings. To perform hardware defined initialization, switch the card to the initialization mode.

Software defined initialization is performed when Sobol is in operation. It may be used to change the parameters that were configured when the card was installed. To perform software defined initialization, select the respective command in the Sobol menu. You do not need to switch the card to the initialization mode.

When Sobol is in operation, the administrator can configure settings, perform card diagnostics and service operations, manage users, work with the Sobol log.

## Identification and authentication

The identification and authentication mechanism of Sobol ensures the verification of user credentials to access a protected computer each time a user attempts to log on.

User identification and user authentication are performed each time a user logs on to the system protected by Sobol.

Sobol identifies a user by a security token unique identifier. To authenticate, Sobol verifies a user's password using a user Secure ID.

**Note.** A Secure ID is a data structure stored in a user's security token.

**Tab. 2 Security tokens used in Sobol**

| iButton security tokens | USB security tokens | |
|---|---|---|
| | **USB keys** | **Smart cards** |
| DS1992 | eToken PRO | eToken PRO |
| DS1993 | eToken PRO (Java) | eToken PRO (Java) |
| DS1994 | vdToken | ESMART Token 64k |
| DS1995 | ESMART Token 64k | JaCarta-2 GOST |
| DS1996 | JaCarta-2 PKI/GOST | JaCarta-2 PKI/GOST |
| SC Button 92 | JaCarta-2 GOST | JaCarta-2 PRO/GOST |
| | JaCarta-2 PRO/GOST | JaCarta PKI |
| | JaCarta PKI | JaCarta PRO |
| | JaCarta PRO | Rutoken Lite SC |
| | JaCarta SF/GOST | Rutoken ECP 2.0 |
| | JaCarta-PRO/GOST | Rutoken ECP SC |
| | Guardant-ID | Rutoken 2151 |
| | Guardant-ID 2.0 | PEK |
| | Foros R301 | FOROS |
| | Rutoken S (RF) | |
| | Rutoken 2151 (RF) | |

| | | |
|---|---|---|
| | Rutoken Lite (RF) | |
| | Rutoken ECP 2.0 (RF, Flash) | |
| | Rutoken ECP 2.0 2100 (RF) | |
| | Rutoken ECP 3.0 | |

USB keys, USB smart card readers Athena ASEDrive IIIe USB V2/V3, USB readers compliant with CCID, as well as USB iButton readers are plugged into computer USB ports. iButton keys are connected to an external, internal or USB iButton reader.

Sobol supports two-factor authentication (for iButton keys) and enhanced two-factor authentication (for USB keys and smart cards).

Two-factor authentication requires a personal security token and a password.

Enhanced two-factor authentication requires a personal security token, a security token PIN and a password.

For security tokens supporting enhanced two- factor authentication, manufacturer sets a default PIN. We recommend changing the default PIN for more effective protection from unauthorized access.

**Attention!**

- You can change a PIN using the tools of a security token manufacturer.
- If an administrator set a PIN for a user security token, he or she should provide the PIN to that user.
- Default PINs for security tokens:
  - for Rutoken S (RF), Rutoken ECP 2.0 (RF, Flash), Rutoken ECP 2.0 2100 (RF), Rutoken 3.0, Rutoken Lite (RF), Rutoken 2151 (RF), Rutoken ECP SC, Rutoken 2151, Rutoken Lite SC, Rutoken ECP 2.0, ESMART Token 64k, vdToken — **12345678**;
  - for eTokenPro, eTokenPro (Java), JaCarta-2 GOST, JaCarta-2 PKI/GOST, JaCarta SF/GOST, JaCarta PKI, JaCarta PRO, JaCarta 2 PRO/GOST, Guardant-ID, Guardant-ID 2.0 — **1234567890;**
  - for Foros R301 — **11111111**.

  If the default PIN is not valid, contact the security token vendor.

If a presented security token is not registered in Sobol:

- user logon to the system is denied;
- unauthorized logon attempt is registered in the Sobol log.

If the entered password does not match the presented security token:

- user logon to the system is denied;
- the number of failed logon attempts increases by one;

  **Note.**
  - If the number of failed logon attempts reaches the maximum permitted value, which is set by the administrator, the user is locked out of the system.
  - If the number of failed logon attempts is less than the maximum permitted value, the counter of failed logon attempts is reset after the first successful logon.
- unauthorized logon attempt is registered in the Sobol log.

Service user data (user name, security token, etc.) is stored in the Sobol nonvolatile memory.

The administrator can set the maximum number of users (see Tab. 5 on p. **27**, **The maximum number of users and log events** parameter).

Administrator can perform the following additional procedures related to identification, authentication, changing user password and Secure ID:

- set a timeout for presenting a security token and typing a password when logging on to the system;
- generate a random password when registering an administrator or a user and changing a password;
- restrict user access to computer according to a user's working time;
- configure password settings (maximum password age, minimum password length, check password complexity, the minimum number of new characters).

**Attention!** Passwords and Secure ID management in joint mode is performed using the tools of a product that operates in tandem with Sobol.

## Protection from unauthorized boot from removable drives

Sobol denies access to removable drives (floppy disks, ZIP, USB drivers, etc.) until an OS is loaded. Access is granted after a successful OS boot.

A boot using removable drives is denied for all users except the administrator.

**Note.**

- The administrator can allow certain users to boot an OS using removable drives (see p. 58).
- The administrator can make a removable drive trusted for an OS boot (see p. 25). Thus, an OS is booted from the removable drive despite such boot type is forbidden for a user.

## Integrity check

The integrity check mechanism ensures the monitoring of changes in the parameters of software and hardware computer resources before booting an OS.

Sobol supports integrity check of objects described in the table below (hereinafter — IC objects).

Furthermore, Sobol supports control of the NTFS, EXT3 and EXT4 transaction log. In this case, Sobol controls integrity of IC objects and templates if partially completed. This procedure is performed before the main integrity check procedure.

**Tab. 3 Sobol IC objects**

| IC objects | Description |
|---|---|
| **Files** | Certain files and groups of files/directories/subdirectories on a computer hard drive |
| **Hard drive sectors** | Master Boot Records, NTFS Boot Sectors, GUID Partition Tables, etc. |
| **System registry items** | Windows registry keys and variables:<br>• registry keys;<br>• parameters (variables) |
| **PCI devices** | PCI and PCIe devices with the respective drivers. Control modes:<br>• Basic (control of presence /absence of a device);<br>• Optimal (control of 256 bytes of a device's configuration space);<br>• Advanced (control of 256 bytes of a device's configuration space and 4 KB of extended configuration space) |
| **SMBIOS data** | SMBIOS data about the motherboard (manufacturer, processor, system slots, memory, UEFI/BIOS, etc.) |

The integrity check mechanism is based on the calculation of the checksums of IC objects and comparing the calculated values with the reference values which were calculated earlier.

The list of IC objects is contained in IC templates. You can manage the IC templates:

- in standalone mode — using the Sobol built-in tool (see p. 79) or the Sobol software (see document [**1**]);
- in joint mode — using the tools of a product that operates in tandem with Sobol p. 100).

**Note.**

- IC template is a service file which contains identification data and the checksums of IC objects. IC templates are stored on a computer hard drive.
- Sobol built-in tool works with a single IC template in the .json format. The administrator creates this template manually and manages it in the Sobol interface.
- Sobol software works with multiple IC templates depending on IC object types:
  - files.nam, files.chk — IC templates for files;
  - sectors.nam, sectors.chk —IC templates for hard drive sectors;
  - registry.nam, registry.chk —IC templates for system registry items;
  - pci.nam, pci.chk —IC templates for PCI devices;
  - smbios.nam, smbios.chk — IC templates for SMBIOS data.

  IC templates are created during the Sobol software installation. The administrator manages them using the Sobol software in an OS.

If Sobol operates in standalone mode, a Sobol administrator calculates reference checksums. In joint mode, reference checksums are calculated by the Sobol administrator or the administrator of a product that operates in tandem with Sobol. Reference checksums are written to IC templates. Then, the IC template checksums are calculated and stored in the protected NVRAM.

Reference checksums are calculated using an IC key according to the algorithms:

- GOST 28147–89 using MAC (Message Authentication Code) Generation Mode;

  **Attention!** Use this algorithm while working in joint mode and ensuring compatibility with older Sobol versions.

- Magma (GOST R 34.12-2015, GOST 34.12-2018) using MAC (Message Authentication Code) Generation Mode (GOST R 34.13-2015, GOST 34.13-2018).

The verification of the checksums is performed when the administrator and users log on to the system. First, the checksums of IC templates are calculated and compared with the reference values. Then, the checksums of IC objects are calculated and compared to the reference values. If an integrity violation is detected, the respective event is registered in the Sobol log.

Sobol supports periodic updating of an IC key. The following actions are performed in this case:

- the checksums of IC templates are verified when the administrator and users log on to the system;
- if the verification is completed with a success, the IC key is updated;
- then, the checksums of IC templates are recalculated.

If the verification is completed with errors, the IC key is not updated, the checksums are not recalculated, and the respective event is registered in the log.

Sobol supports soft and hard IC modes. The Administrator sets the IC mode individually for each user.

If an integrity violation is detected in **hard mode**, the IC key in not updated, user logon to the system is forbidden and a computer is locked.

If an integrity violation is occurred in **soft mode**, the IC key in not updated but user logon to the system is permitted.

**Attention!** When using the IC mechanism, note that:

- do not use OS boot managers that allow installing multiple OSs on a computer;
- do not compress the folder with IC templates;
- NTFS Symbolic Link, NTFS Hardlink and Windows Junction Point are not supported in IC templates;
- integrity check of files converted by other programs such as cryptographic software (BestCrypt, etc.) or disk compression tools (Driverspace, etc.) is not supported;
- integrity check of objects on volume sets and stripe sets (for example, LVM, StripeSet, Volume set, Software RAID) is not supported.

## Watchdog timer

The watchdog mechanism blocks access to the computer if the UEFI/BIOS Option ROM is not provided with control after the computer is turned on and the specified time interval, called a watchdog timer timeout, expires. The watchdog mechanism implemented in Sobol has two stages. The event when the watchdog mechanism triggers is recorded in the Sobol log.

Access to the computer can be blocked by:

- forced automatic restart of the computer with the Reset procedure. To block the computer, the RST watchdog cable is used (see section A, Fig. 1 on p. **11**) which is included in the delivery;
- forced automatic shutdown of the computer. To block the computer, the following components can be used, delivered on request:
  - ATX cable watchdog relay (see section B, Fig. 1 on p. **11**);

    **Note.** ATX cable watchdog relay is designed for use in ATX form factor computers.
  - PWR watchdog cable with two T-Tap connectors (see section C, Fig. 1 on p. **11**), which is used to connect the RST watchdog cable to the Power button cable in parallel;
  - connectors to connect the RST watchdog cable to the Power button cable in parallel (see section D, Fig. 1 on p. **11**).

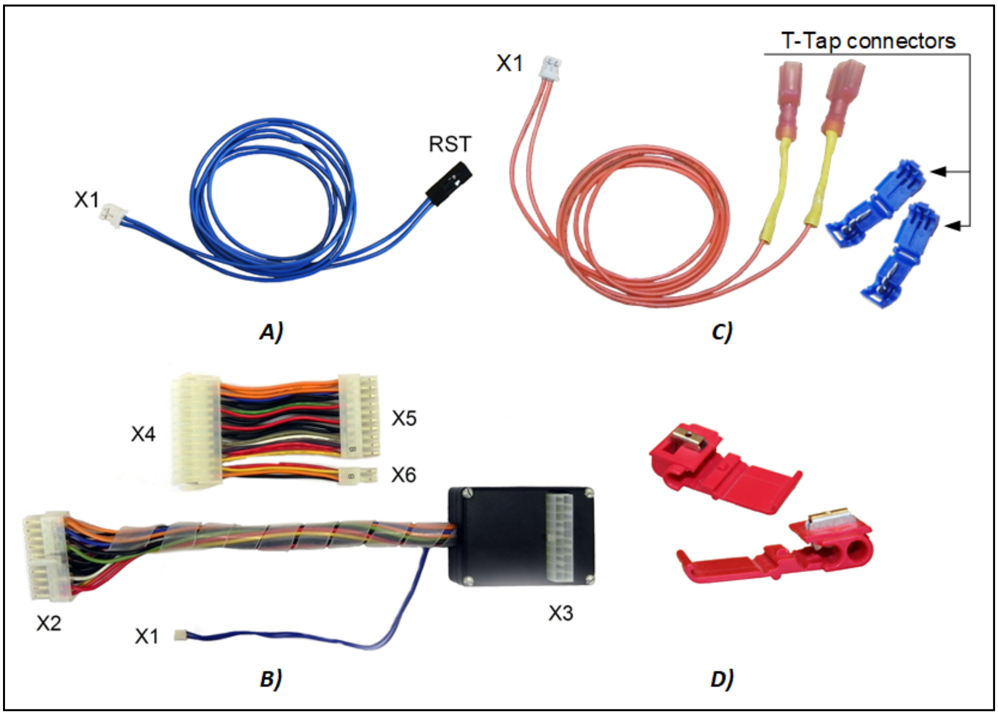


**Fig. 1 Sobol components for watchdog timer**

To use the watchdog timer, you need to connect the RST watchdog cable, PWR watchdog cable or ATX cable watchdog relay to the Sobol card. The watchdog timer does not function without cable or relay connection.

On PCIe cards (type 1,2) of Sobol, a SATA power connector is installed to improve the watchdog timer efficiency. Connecting the SATA power cable to it allows you to maintain the watchdog timer operation if the power at the PCIe slot on the computer motherboard is turned off (e.g. if the PCIe slot is blocked in UEFI/BIOS Setup).

The recommended watchdog timer timeout is determined automatically at the stage of the Sobol initialization. The administrator can modify the timeout value during Sobol initialization or operation. The maximum timeout value is 65534 seconds.

**Attention!** To prevent a loss of applications caused by the watchdog timer when the computer switches from the standby mode, do not use the standby mode in Windows OS if UEFI/BIOS parameters include the ACPI "S3" or "S4" (Suspend To RAM) power saving mode. In these cases, we recommended you to use the sleep mode instead of the standby mode or modify the UEFI/BIOS power saving mode.

## Sobol log

Events logged by Sobol are stored in the log.

The log is stored in a special area of the Sobol nonvolatile memory. Its memory size is limited.

**Note.** The maximum log size can be set to 800, 1600, 2400 or 3200 events depending on the maximum number of Sobol users (see Tab. 5 on p. **27**, **The maximum number of users and log events** parameter).

To work with the log, the following functions are available:

- saving (exporting) to a log file;
- searching for events in the log by their creation time and type;
- automatic events overwriting when the log is 100% full;
- setting the time period for a log audit.

## Monitoring Sobol components performance

The Sobol monitoring mechanism is designed to check the operation of the following Sobol components:

- memory card;
- random number generator (RNG);
- security token.

The check is performed by testing the components. You can launch this procedure before the Sobol initialization or during its operation.

**Note.** We recommend you to test all components before the Sobol initialization. To do this, in the **Diagnostics** section, click **Run all tests**. For detailed information about the **Diagnostics** section, see p. 72.

## Hardware and software requirements

Sobol can be installed on computers with x86-64 processors. To connect the Sobol card to the computer motherboard, there must be a free PCIe slot (version 1.1 and above), or Mini PCIe Express slot (hereinafter - Mini PCIe slot), or M.2 slot (key type A or E).

Sobol operates with NTFS, FAT16, FAT32, EXT2, EXT3, EXT4 file systems.

The layout of the system hard drive must be GPT and there must be at least 50 MB of free space.

The minimum screen resolution supported by Sobol is 1024x768.

Sobol performance does not depend on the type of OS.

**Note.** To manage integrity check templates, you can use Sobol software, which successful operation depends on the computer OS. The requirements for Sobol software installation are specified in document [**1**].

In order for the watchdog timer to operate, the computer motherboard must meet at least one of the following requirements:

- Reset socket is available;
- ATX cable watchdog relay connector is available;
- RST watchdog cable can be connected to the Power button cable in parallel.

When the Reset signal is sent to the computer motherboard slot to which the RST watchdog cable is connected, the computer must be rebooted.

When a signal is sent to the power connector on the computer motherboard to which the ATX cable watchdog relay is connected, or to the Power button cable to which the RST or PWR watchdog cable is connected, the computer must be turned off. Computer software and hardware must be unable to interrupt this mechanism (for example, by disabling it in UEFI/BIOS Setup).

The power connector on the computer motherboard must comply with the ATX specification and have 20 or 24 pins. The power supply unit must meet the requirements of the ATX specification.

# Chapter 2
# Installing Sobol

## Installation procedure

Sobol is installed in the following order:

- install Sobol software (if necessary);

> **Note.**
> - In standalone mode, Sobol can be used both with Sobol software and without it.
> - In joint mode, Sobol Sobol operates correctly when Sobol software is installed.
>
> For detailed information on how to install and work with Sobol software, see document [1].

- install a Sobol card (see p. **13** for a PCIe card (types 1, 2), p. **14** for a PCIe card (types 3, 4),p. **16** for a Mini PCIe Half card (types 1, 2), p. **19** for a M.2 card (types 1, 2, 3, 4);
- initialize Sobol (see p. **24**);
- put Sobol into operation (see p. **43**).

## Install PCIe card

**To install a PCIe card (types 1, 2):**

1. Shut down your computer. Remove the side panel.
2. Switch SW1-1 to the OFF position.

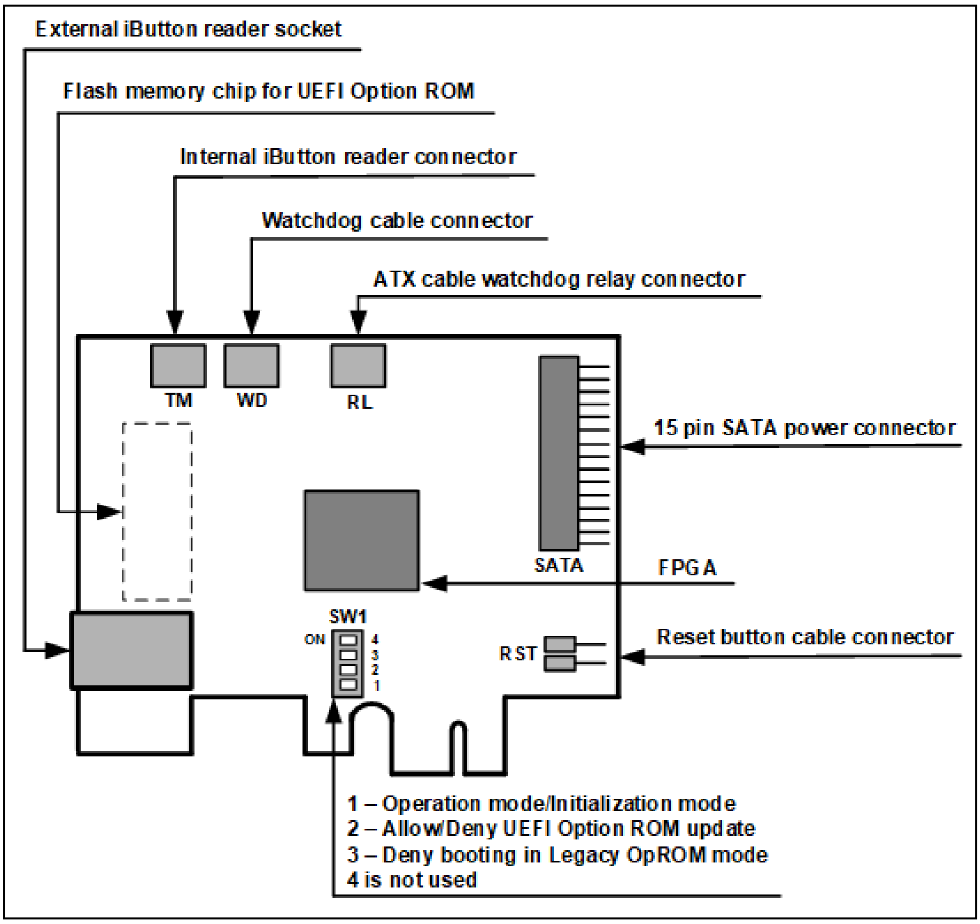

External iButton reader socket
Flash memory chip for UEFI Option ROM
Internal iButton reader connector
Watchdog cable connector
ATX cable watchdog relay connector
TM
WD
RL
15 pin SATA power connector
SATA
FPGA
SW1
ON
4
3
2
1
RST
Reset button cable connector
1 – Operation mode/Initialization mode
2 – Allow/Deny UEFI Option ROM update
3 – Deny booting in Legacy OpROM mode
4 is not used

**Fig. 2 PCIe card connector layout (types 1, 2)**

**Note.**

In Legacy OpROM mode, Sobol blocks blocking the computer in one of the two modes — hard and soft. To select one of the modes, use SW1-3:

- ON — hard mode. This mode blocks UEFI/BIOS Setup booting. To unblock the booting, remove the card (see p. **40**), then, in UEFI/BIOS Setup, select the UEFI boot mode and reconnect the card. The hard mode is available only when Sobol is in operation;
- OFF — soft mode. This mode blocks OS booting. The soft mode may be useful if you are using the UEFI and Legacy OS boot mode. To unblock the booting, in UEFI/BIOS Setup, select the UEFI boot mode. You do not have to remove the card.

**To install a PCIe card (types 3, 4):**

1. Shut down your computer. Remove the side panel.
2. Switch SA1-1 to the OFF position (see Fig. 3 on p. **14**).

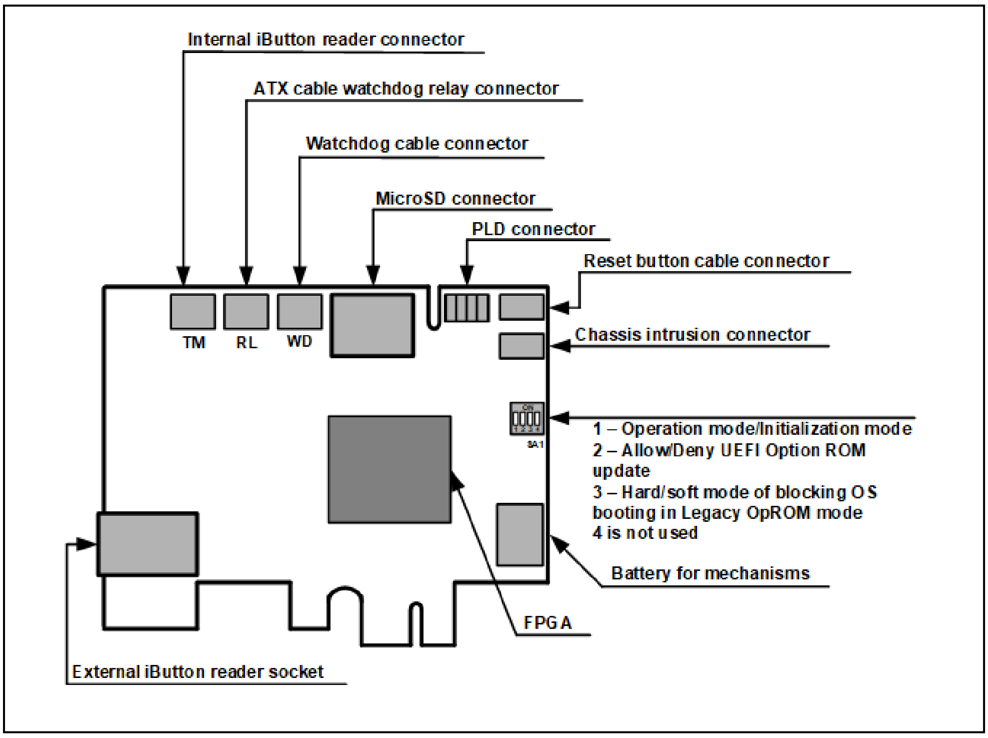

Internal iButton reader connector
ATX cable watchdog relay connector
Watchdog cable connector
MicroSD connector
PLD connector
Reset button cable connector
Chassis intrusion connector
TM
RL
WD
SA1
1 – Operation mode/Initialization mode
2 – Allow/Deny UEFI Option ROM update
3 – Hard/soft mode of blocking OS booting in Legacy OpROM mode
4 is not used
Battery for mechanisms
FPGA
External iButton reader socket

**Fig. 3 PCIe card connector layout (types 3, 4)**

**Note.**

In Legacy OpROM mode, Sobol blocks blocking the computer in one of the two modes — hard and soft. To select one of the modes, use SA1-3:

- ON — hard mode. This mode blocks UEFI/BIOS Setup booting. To unblock the booting, remove the card (see p. **40**), then, in UEFI/BIOS Setup, select the UEFI boot mode and reconnect the card. The hard mode is available only when Sobol is in operation;
- OFF — soft mode. This mode blocks OS booting. The soft mode may be useful if you are using the UEFI and Legacy OS boot mode. To unblock the booting, in UEFI/BIOS Setup, select the UEFI boot mode. You do not have to remove the card.

**To use the Sobol watchdog timer:**

1. To enable forced automatic restart (RST watchdog cable) :
    - disconnect the Reset button cable from the motherboard;
    - connect the Reset button cable to the RST connector on the Sobol card;
    - connect the RST watchdog cable to the WD connector on the Sobol card and to the Reset connector on the motherboard;
    - connect the power cable to the SATA connector on the Sobol card (see Fig. 2 on p. **13**);

- To enable forced automatic shutdown (24-ATX) :
    - disconnect the power cable from the motherboard;
    - connect the power cable to the X4 connector of the ATX cable watchdog relay (see Fig. 1 on p. **11**);
    - connect the X5 connector to the X3 connector;
    - connect the X2 and X6 connectors to the ATX connector on the motherboard;
    - connect the X1 connector to the RL connector on the Sobol card;
    - connect the power cable to the SATA connector on the Sobol card (see Fig. 2 on p. **13**);
- To enable forced automatic shutdown (20-ATX) :

  - disconnect the power cable from the ATX connector on the motherboard;
  - connect the power cable to the X3 connector of the ATX cable watchdog relay (see Fig. 1 on p. **11**);
  - connect the X2 connector to the ATX connector on the motherboard;
  - connect the X1 connector to the RL connector on the Sobol card;
  - connect the power cable to the SATA connector on the Sobol card (see Fig. 2 on p. **13**);
- To enable automatic shutdown (PWR watchdog cable) :
  - fold T-Tap connectors (see C, Fig. 1 on p. **11**) over the wires of the power cable using pliers (see Step 1, Fig. 4 on p. **15**);
  - connect the X1 connector of the PWR watchdog cable (see C, Fig. 1 on p. **11**) to the WD connector on the Sobol card. Then, plug the spades of the PWR watchdog cable into the T-Tap connectors (see Step 2 Fig. 4 on p. **15**);
  - connect the power cable to the SATA connector on the PCIe card (type 1,2) (see Fig. 2 on p. **13**);

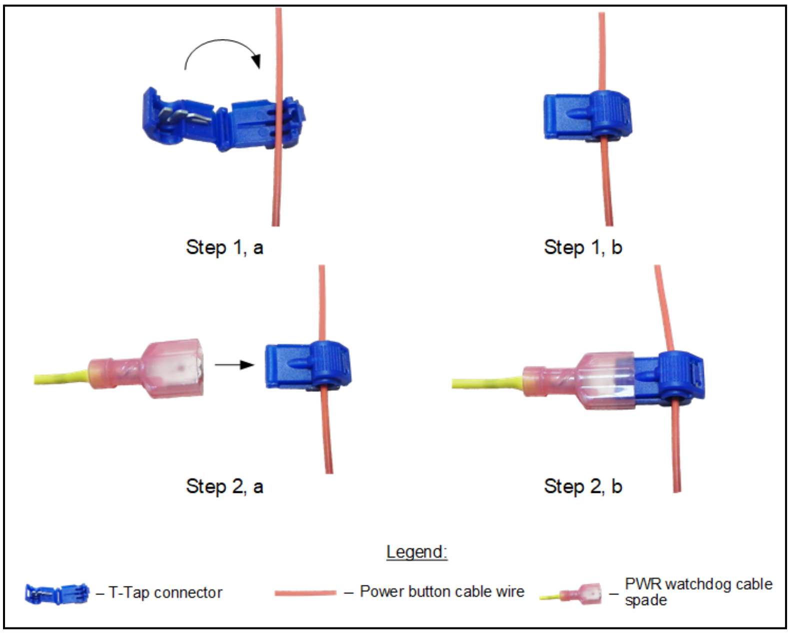


**Fig. 4 Connecting PWR watchdog cable**

- To enable forced automatic shutdown (RST watchdog cable with connectors) :
  - cut off the RST connector from the RST watchdog cable (see Step 1 Fig. 5 on p. **16**);
  - insert one wire of the RST watchdog cable to the connector (see Step 2, Fig. 5 on p. **16**);
  - insert one wire of the Power button cable to the connector (see Step 3, Fig. 5 on p. **16**);
  - press the copper piece using pliers (see Step 4, Fig. 5 on p. **16**);
  - close the cover of the connector (see Step 5, Fig. 5 on p. **16**);
  - repeat Steps 2-5 (see Fig. 5 on p. **16**) with other wires of the cables;
  - connect the X1 connector of the RST watchdog cable to the WD connector on the Sobol card.

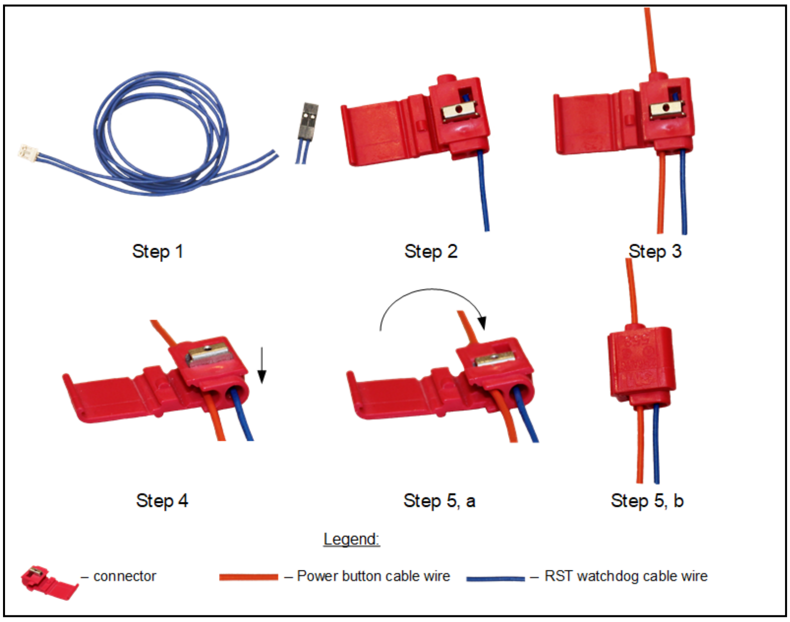


**Fig. 5 Connecting the RST watchdog cable to the Power button cable in parallel**

2. Insert the PCIe card into a free PCIe slot.
3. If necessary, attach an iButton reader to the PCIe card:
   - for the external iButton reader, attach it to the respective socket;
   - for the internal iButton reader, attach it to the TM connector.
4. Put the side panel back.
5. If necessary, connect a USB reader.

## Install Mini PCIe Half card

A Mini PCIe Half card (see Fig. 6 on p. **16**) can be installed autonomously or using an adapter depending on a protected computer form factor. You can use four different adapter kinds which vary in terms of size and ability to attach either the external or the internal iButton reader:

- adapter 1 (see Fig. 7 on p. **17**) ) for the external and the internal iButton readers;
- adapter 2 (see Fig. 8 on p. **17**) and adapter 3 (see Fig. 9 on p. **17**) for the internal iButton reader;
- adapter 4 (see Fig. 10 on p. **18**) for the external iButton reader.

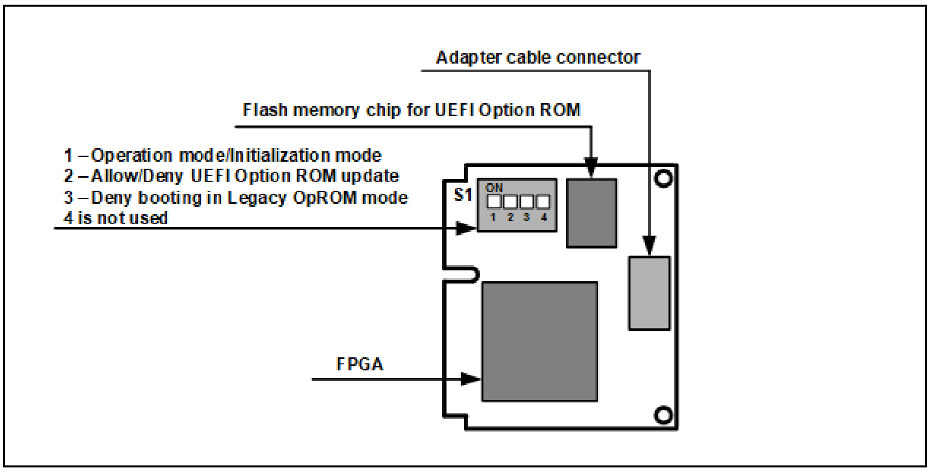

Adapter cable connector
Flash memory chip for UEFI Option ROM
1 – Operation mode/Initialization mode
2 – Allow/Deny UEFI Option ROM update
3 – Deny booting in Legacy OpROM mode
4 is not used
S1
ON
1 2 3 4
FPGA

**Fig. 6 Mini PCIe Half card connector layout (types 1, 2)**

**Note.**

In Legacy OpROM mode, Sobol blocks computer booting in one of the two modes — hard and soft. To select one of the modes, use S1:

- ON — hard mode. This mode blocks UEFI/BIOS Setup booting. To unblock the booting, remove the card (see p. 41), then, in UEFI/BIOS Setup, select the UEFI boot mode and reconnect the card. The hard mode is available only when Sobol is in operation;
- Off — soft mode. This mode blocks OS booting. The soft mode may be useful if you are using the UEFI and Legacy OS boot mode. To unblock the booting, in UEFI/BIOS Setup, select the UEFI boot mode. You do not have to remove the card.

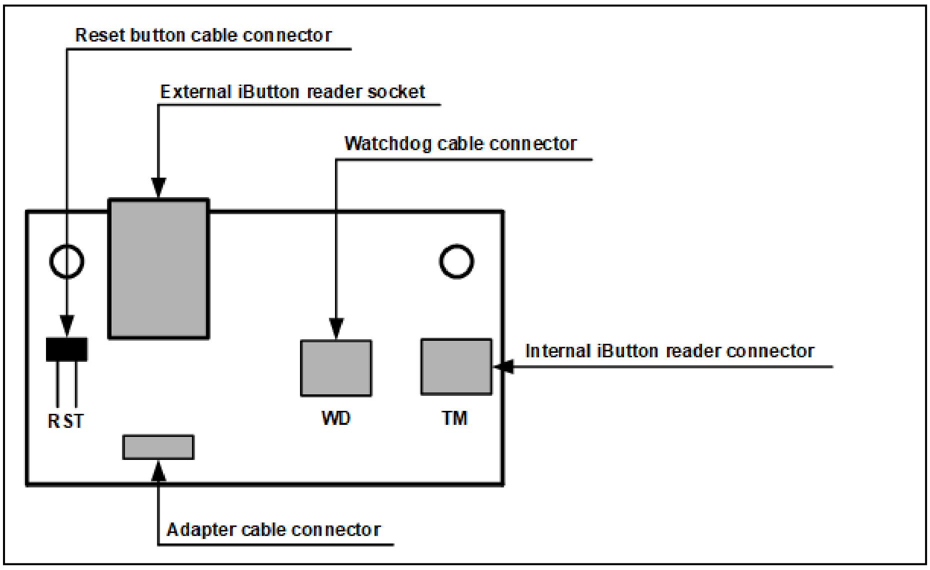

Reset button cable connector
External iButton reader socket
Watchdog cable connector
Internal iButton reader connector
RST
WD
TM
Adapter cable connector

**Fig. 7 Adapter 1 connector layout for Mini PCIe Half and M.2 cards (types 1, 2)**

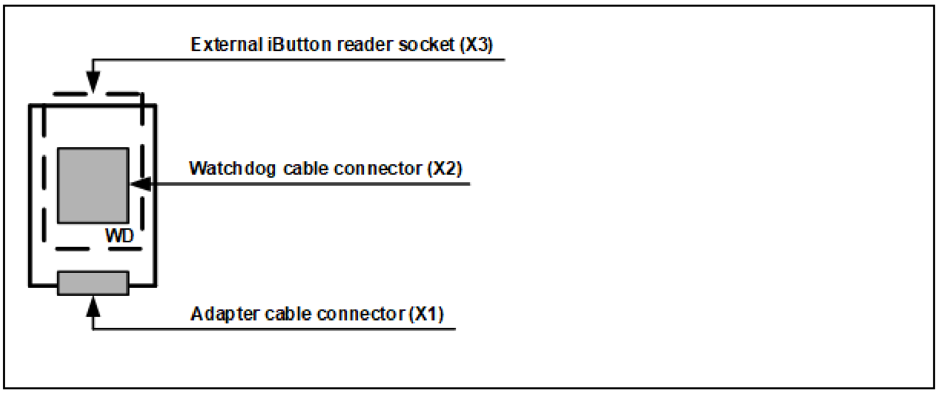

External iButton reader socket (X3)
Watchdog cable connector (X2)
WD
Adapter cable connector (X1)

**Fig. 8 Adapter 2 connector layout for Mini PCIe Half and M.2 cards (types 1, 2)**

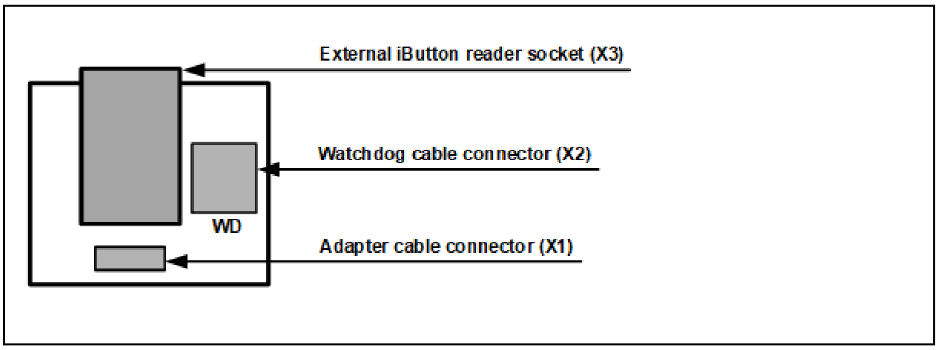

External iButton reader socket (X3)
Watchdog cable connector (X2)
WD
Adapter cable connector (X1)

**Fig. 9 Adapter 3 connector layout for Mini PCIe Half and M.2 cards (types 1, 2)**

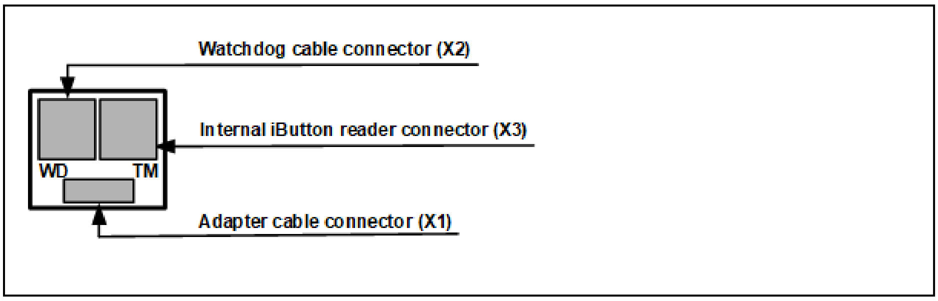

Watchdog cable connector (X2)
Internal iButton reader connector (X3)
WD
TM
Adapter cable connector (X1)

**Fig. 10 Adapter 4 connector layout for Mini PCIe Half and M.2 cards (types 1, 2)**

**To install a Mini PCIe Half card using an adapter:**

1. Shut down your computer. Remove the side panel.
2. Switch S1-1 to the OFF position (see Fig. 6 on p. **16**).
3. Connect the adapter cable to the respective card (see Fig. 6 on p. **16**) and adapter connectors (Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**).
4. **To use the Sobol watchdog timer:**
   - To enable forced automatic restart (RST watchdog cable) :
     - disconnect the Reset button cable from the motherboard;
     - for a type 1 adapter, connect the Reset button cable to the RST connector on the adapter (Fig. 7 on p. **17**);
     - for an adapter type 2, 3 or 4, do not connect the Reset button cable anywhere;
     - connect one X1 connector of the RST watchdog cable (see A, Fig. 1 on p. **11**) to the WD connector on the adapter (see Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**) and the other one to the Reset connector on the motherboard.
   - To enable automatic shutdown (PWR watchdog cable) :
     - fold T-Tap connectors over the wires of the power cable using pliers (see Step 1, Fig. 4 on p. **15**);
     - connect the X1 connector of the PWR watchdog cable to the WD connector on the adapter. Then, plug the spades of the PWR watchdog cable into the T-Tap connectors (see Step 2, Fig. 4 on p. **15**);
   - To enable forced automatic shutdown (RST watchdog cable with connectors) :
     - cut off the RST connector from the RST watchdog cable (see Step 1 Fig. 5 on p. **16**);
     - insert one wire of the RST watchdog cable to the connector (see Step 2, Fig. 5 on p. **16**);
     - insert one wire of the Power button cable to the connector (see Step 3, Fig. 5 on p. **16**);
     - press the copper piece using pliers (see Step 4, Fig. 5 on p. **16**);
     - close the cover of the connector (see Step 5, Fig. 5 on p. **16**);
     - repeat Steps 2-5 (see Fig. 5 on p. **16**) with other wires of the cables;
     - connect the X1 connector of the RST watchdog cable to the WD connector on the adapter.
5. Insert the Mini PCIe Half card into a free Mini PCIe slot.
6. Insert the adapter into a free slot.

   **Note.** You can also attach the adapter to a Standard/Low Profile bracket, insert it in a free slot or insert it in any other way.

7. If necessary, attach the iButton reader to the adapter:
   - for the external iButton reader, attach it to the respective socket on the adapter of types 1, 2 or 3 (see Fig. 7 on p. **17**, Fig. 8 on p. **17** or Fig. 9 on p. **17**);
   - for the internal iButton reader, attach it to the TM connector on the adapter of types 1 or 4(see Fig. 7 on p. **17** or Fig. 10 on p. **18**).
8. Put the side panel back.
9. If necessary, connect a USB reader.

**To install a Mini PCIe Half card autonomously:**

1. Shut down your computer. Remove the side panel.
2. Switch S1-1 to the OFF position (see Fig. 6 on p. **16**).

3. Insert the Mini PCIe Half card into a free Mini PCIe slot. Put the side panel back.
4. If necessary, connect a USB reader.

## Install an M.2 card

An M.2 card can be installed autonomously or using an adapter or a WD module depending on the protected computer form factor. For M.2 cards (types 1, 2), you can use four adapter types (see the description on p. **16**). For M.2 cards (types 3, 4), you can use six WD module types which differ in terms of size and the ability to attach either the external or the internal iButton reader (see Fig. 13 on p. **20**, Fig. 14 on p. **20**, Fig. 15 on p. **20**, Fig. 16 on p. **21**, Fig. 17 on p. **21**, Fig. 18 on p. **22**).

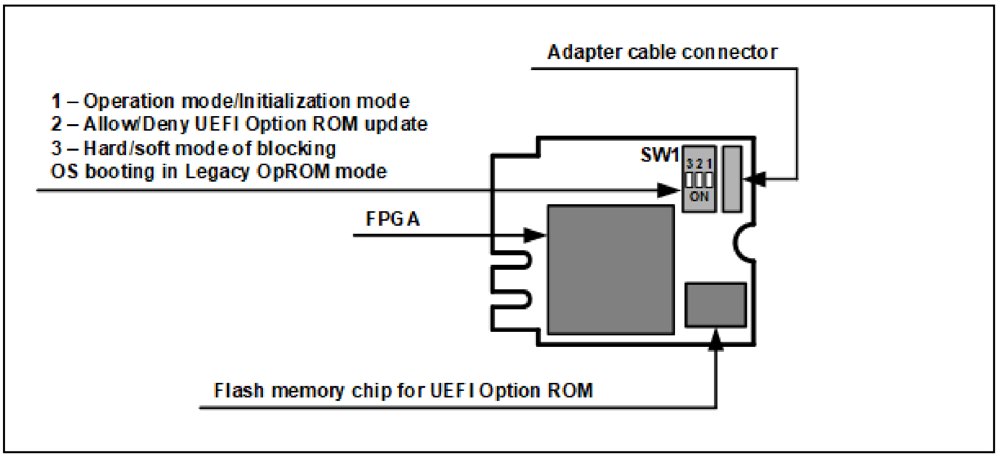

Adapter cable connector
1 – Operation mode/Initialization mode
2 – Allow/Deny UEFI Option ROM update
3 – Hard/soft mode of blocking
OS booting in Legacy OpROM mode
SW1
3 2 1
ON
FPGA
Flash memory chip for UEFI Option ROM

**Fig. 11 M.2 card (types 1, 2) connector layout**

**Note.**

In Legacy OpROM mode, Sobol blocks computer booting in one of the two modes — hard and soft. To select one of the modes, use SW1-3:

- ON — hard mode. This mode blocks UEFI/BIOS Setup booting. To unblock the booting, remove the card (see p. 41), then, in UEFI/BIOS Setup, select the UEFI boot mode and reconnect the card. Hard mode is available only when Sobol is in operation.
- OFF — soft mode. This mode blocks OS booting. The soft mode may be useful if you are using the UEFI and Legacy OS boot mode. To unblock the booting, in UEFI/BIOS Setup, select the UEFI boot mode. You do not need to remove the card.

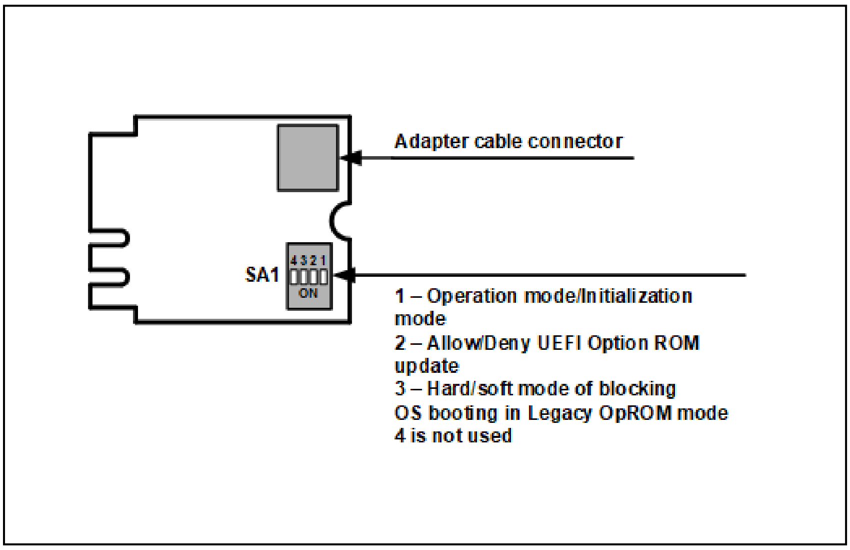

Adapter cable connector
SA1
4 3 2 1
ON
1 – Operation mode/Initialization mode
2 – Allow/Deny UEFI Option ROM update
3 – Hard/soft mode of blocking
OS booting in Legacy OpROM mode
4 is not used

**Fig. 12 M.2 card (types 3, 4) connector layout**

**Note.**

In Legacy OpROM mode, Sobol blocks computer booting in one of the two modes — hard and soft. To select one of the modes, use SA1-3:

- ON — hard mode. This mode blocks UEFI/BIOS Setup booting. To unblock the booting, remove the card (see p. 41), then, in UEFI/BIOS Setup, select the UEFI boot mode and reconnect the card. Hard mode is available only when Sobol is in operation.
- OFF — soft mode. This mode blocks OS booting. The soft mode may be useful if you are using the UEFI and Legacy OS boot mode. To unblock the booting, in UEFI/BIOS Setup, select the UEFI boot mode. You do not need to remove the card.

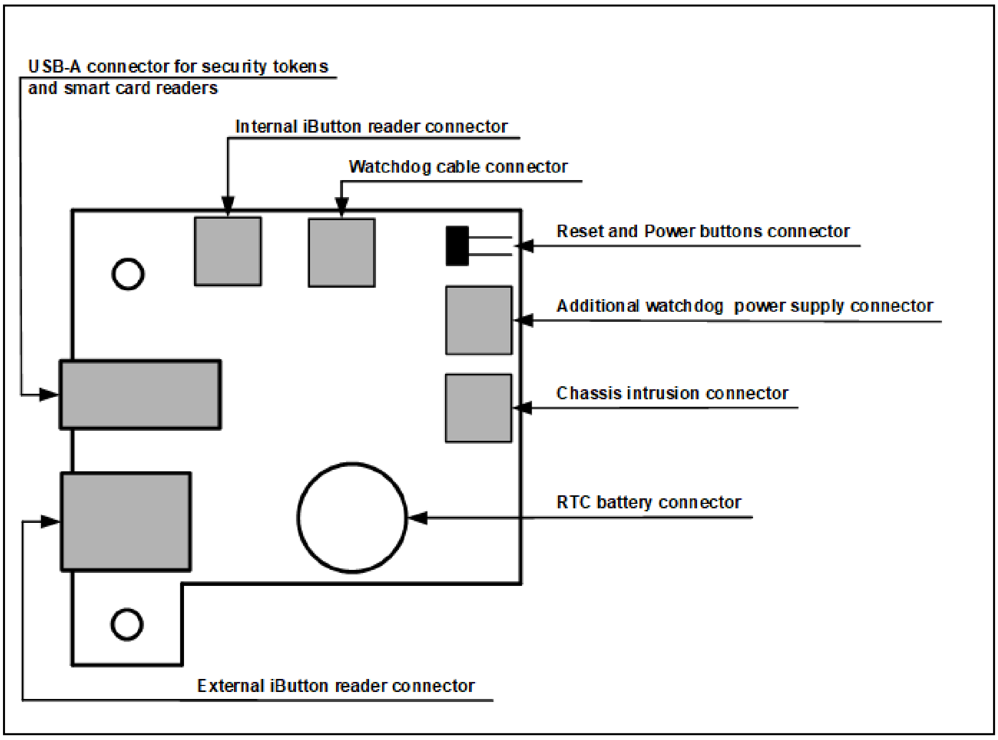

USB-A connector for security tokens and smart card readers
Internal iButton reader connector
Watchdog cable connector
Reset and Power buttons connector
Additional watchdog power supply connector
Chassis intrusion connector
RTC battery connector
External iButton reader connector

**Fig. 13 WD module – 1 for M.2 cards (types 3, 4) connector layout**

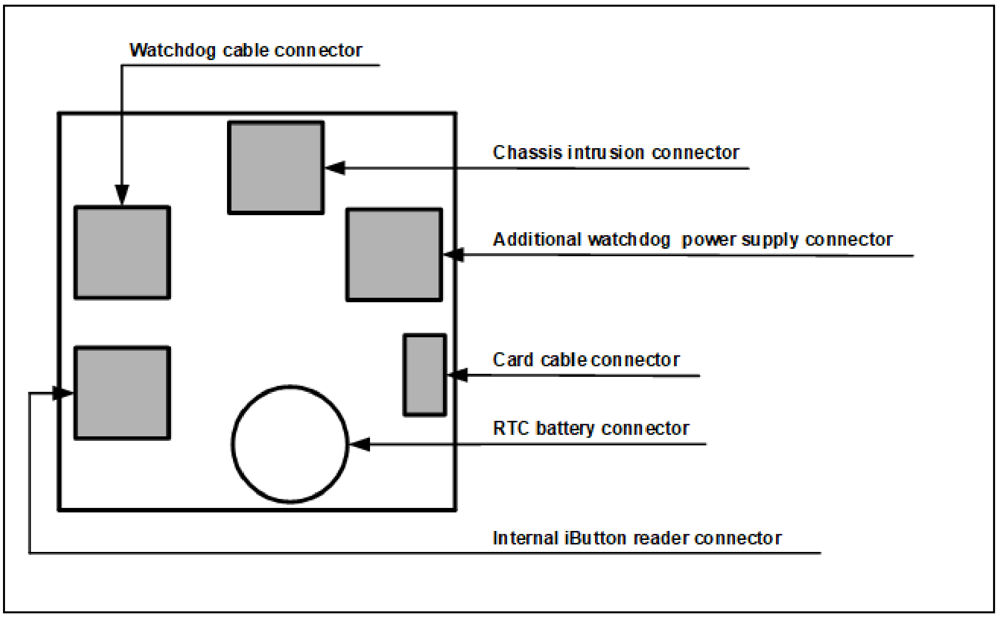

Watchdog cable connector
Chassis intrusion connector
Additional watchdog power supply connector
Card cable connector
RTC battery connector
Internal iButton reader connector

**Fig. 14 WD module – 2 for M.2 cards (types 3, 4) connector layout**

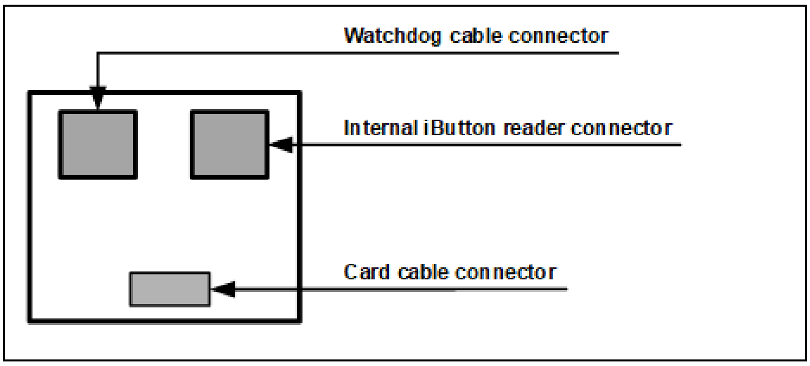


**Fig. 15 WD module – 3 for M.2 cards (types 3, 4) connector layout**

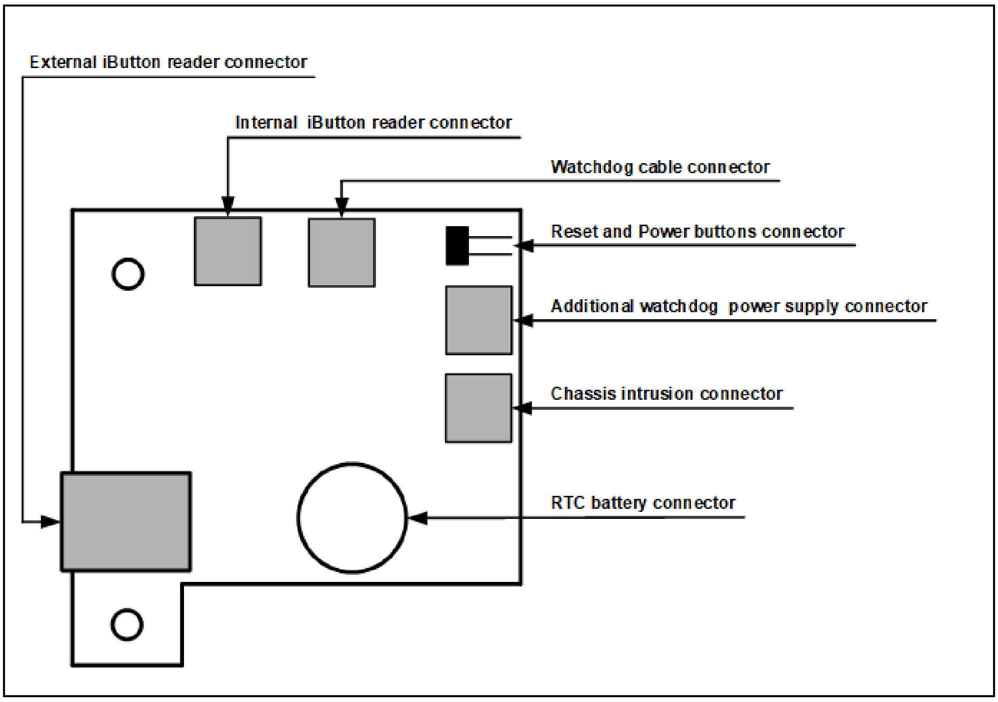

External iButton reader connector
Internal iButton reader connector
Watchdog cable connector
Reset and Power buttons connector
Additional watchdog power supply connector
Chassis intrusion connector
RTC battery connector

Fig. 16 WD module – 4 for M.2 cards (types 3, 4) connector layout

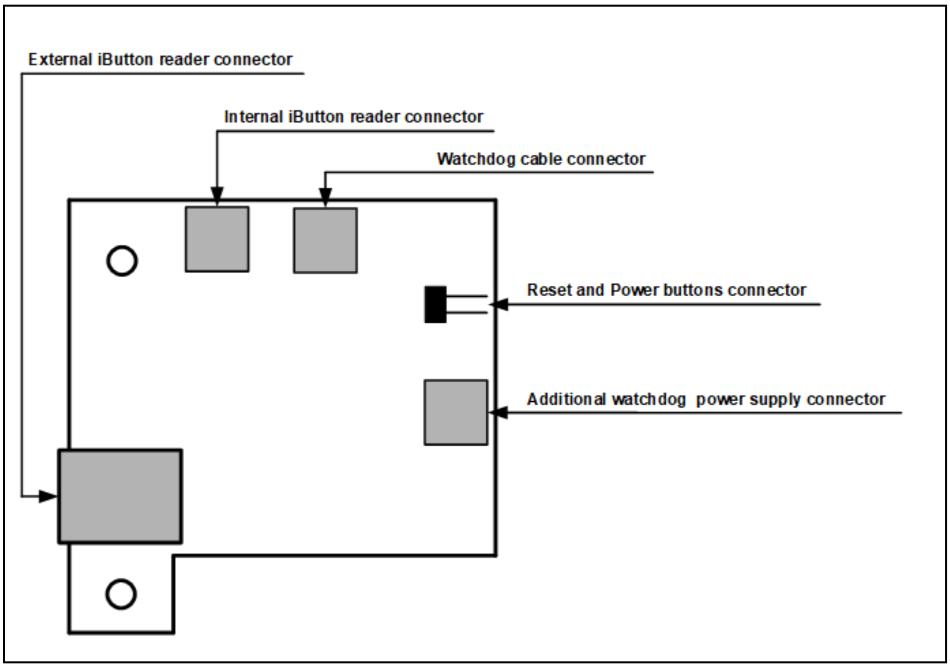

External iButton reader connector
Internal iButton reader connector
Watchdog cable connector
Reset and Power buttons connector
Additional watchdog power supply connector

Fig. 17 WD module – 5 for M.2 cards (types 3, 4) connector layout

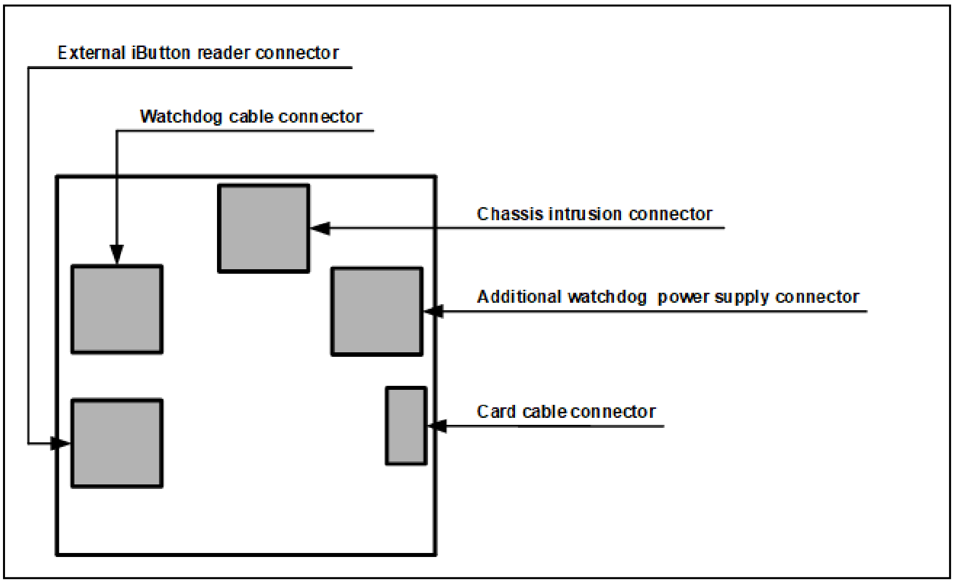

External iButton reader connector
Watchdog cable connector
Chassis intrusion connector
Additional watchdog power supply connector
Card cable connector

**Fig. 18 WD module – 6 for M.2 cards (types 3, 4) connector layout**

**To install an M.2 card (types 1, 2) using an adapter:**

1. Shut down your computer. Remove the side panel.
2. Switch SW1-1 of the M.2 card (types 1, 2) (see Fig. 11 on p. **19**) to the OFF position.
3. Connect the adapter cable to the respective card (see Fig. 11 on p. **19**) and adapter connectors (see Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**).
4. To use the Sobol watchdog timer:
   - (RST watchdog cable):
     - disconnect the Reset button cable from the motherboard;
     - for a type 1 adapter, connect the Reset button cable to the RST connector on the adapter (see Fig. 7 on p. **17**);
     - for an adapter type 2, 3 or 4, do not connect the Reset button cable;
     - connect the X1 connector of the RST watchdog cable (see A, Fig. 1 on p. **11**) to the WD connector on the adapter (see Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**). Then, connect another connector of this cable to the Reset slot of the motherboard;
   - (PWR watchdog cable):
     - fold T-Tap connectors over the wires of the power cable using pliers (see Step 1, Fig. 4 on p. **15**);
     - connect the X1 connector of the PWR watchdog cable to the WD connector on the adapter. Then, plug the spades of the PWR watchdog cable into the T-Tap connectors (see Step 2, Fig. 4 on p. **15**);
   - (RST watchdog cable with connectors):
     - cut off the RST connector from the RST watchdog cable (see Step 1, Fig. 5 on p. **16**);
     - insert one wire of the RST watchdog cable to the connector (see Step 2, Fig. 5 on p. **16**);
     - insert one wire of the Power button cable to the connector (see Step 3, Fig. 5 on p. **16**);
     - press the copper piece using pliers (see Step 4, Fig. 5 on p. **16**);
     - close the cover of the connector (see Step 5, Fig. 5 on p. **16**);
     - repeat Steps 2-5 (see Fig. 5 on p. **16**) with other wires of the cables;
     - connect the X1 connector of the RST watchdog cable to the WD connector on the adapter.
5. Find a free M.2 connector and insert the Sobol card in it.
6. Insert the adapter into a free slot.

   **Note.** You can also attach the adapter to a Standard/Low Profile bracket or in any other way.

7. If necessary, attach the iButton reader to the adapter:
   - for the external iButton reader, attach it to the respective connector on the adapter of types 1, 2 or 3 (see Fig. 7 on p. **17**, Fig. 8 on p. **17** or Fig. 9 on p. **17**);

- for the internal iButton reader, attach it to the TM connector on the adapter of types 1 or 4 (see Fig. 7 on p. **17** or Fig. 10 on p. **18**).

**8.** Put the side panel back.

**9.** If necessary, connect a USB reader.

**To install an M.2 card (types 1, 2) autonomously:**

**1.** Shut down your computer. Remove the side panel.

**2.** Switch SW1-1 to the OFF position.

**3.** Find a free M.2 connector and insert the Sobol card in it. Put the side panel back.

**4.** If necessary, connect a USB reader.

**To install an M.2 card (types 3, 4) using a WD module:**

**1.** Shut down your computer. Remove the side panel.

**2.** Switch SA1-1 of the M.2 card (types 3, 4) (see Fig. 12 on p. **19**) to the OFF position.

**3.** Connect the WD module cable to the respective connectors of the M.2 card (see Fig. 12 on p. **19**) and WD module (see Fig. 13 on p. **20**, Fig. 14 on p. **20**, Fig. 15 on p. **20**, Fig. 16 on p. **21**, Fig. 17 on p. **21**, Fig. 18 on p. **22**).

**4.** To use the Sobol watchdog timer:

- (RST watchdog cable):
  - disconnect the Reset button cable from the motherboard;
  - for the WD 1,4 or 5 module, connect the Reset button cable to the RST connector on the WD module (see Fig. 7 on p. **17**);
  - for the WD 2, 3 or 6 module, do not connect the Reset button cable anywhere;
  - connect the X1 connector of the RST watchdog cable (see A), Fig. 1 on p. **11**) to the WD connector on the WD module. Then, connect another connector of this cable to the Reset slot of the motherboard;
- (PWR watchdog cable):
  - fold T-Tap connectors over the wires of the power cable using pliers (see Step 1, Fig. 4 on p. **15**);
  - connect the X1 connector of the PWR watchdog cable to the WD connector on the WD module. Then, plug the spades of the PWR watchdog cable into the T-Tap connectors (see Step 2, Fig. 4 on p. **15**);
- (RST watchdog cable with connectors):
  - cut off the RST connector from the RST watchdog cable (see Step 1, Fig. 5 on p. **16**);
  - insert one wire of the RST watchdog cable to the connector (see Step 2, Fig. 5 on p. **16**);
  - insert one wire of the Power button cable to the connector (see Step 3, Fig. 5 on p. **16**);
  - press the copper piece using pliers (see Step 4, Fig. 5 on p. **16**);
  - close the cover of the connector (see Step 5, Fig. 5 on p. **16**);
  - repeat Steps 2-5 (see Fig. 5 on p. **16**) with other wires of the cables;
  - connect the X1 connector of the RST watchdog cable to the WD connector on the WD module.

**5.** Find a free M.2 connector and insert the Sobol card in it.

**6.** Insert the WD module into a free slot.

**Note.** You can also attach the WD module to a Standard/Low Profile bracket or in any other way.

**7.** If necessary, attach the iButton reader to the WD module:

- for the external iButton reader, attach it to the respective TM connector on the WD module 1, 4 or 5;
- for the internal iButton reader, attach it to the TM connector on the WD module 2, 3 or 6.

**8.** Put the side panel back.

**9.** If necessary, connect a USB reader.

**To install an M.2 card (types 3, 4) autonomously:**

**1.** Shut down your computer. Remove the side panel.

**2.** Switch SA1-1 to the OFF position.

**3.** Find a free M.2 connector and insert the Sobol card in it. Put the side panel back.

**4.** If necessary, connect a USB reader.

# Initialize Sobol

To initialize Sobol, take the following steps:

1. Configure system settings (see p. **25**).
2. Configure general settings (see p. **27**).
3. Configure log settings (see p. **30**).
4. Configure password settings (see p. **30**).
5. Create and configure an administrator account (see p. **32**).
6. Configure integrity check settings and calculate checksums (see p. **37**).

**Attention!** Before starting the initialization, disconnect all USB Mass Storage devices from your computer (USB, CD and DVD drives, etc).

## Start initialization

### To start the initialization:

1. Power on your computer.

   The computer is controlled by Sobol. The card memory and RNG tests begin.

   **Attention!**

   - If a computer is not controlled by Sobol after power-on, take the following actions:
     - in UEFI/BIOS Setup, allow booting from a network adapter option ROM;
     - use the watchdog timer (see p. **14** for a PCIe card, p. **18** for a Mini PCIe card p. **22** and for a M.2 card);
     - disable CSM;
     - errors while forming IC templates and checksum calculation may occur if Fast boot mode is used on Windows 10. For Sobol correct operation, disable Fast boot mode using Windows standard tools.

     In this case, OS boot is performed only from a hard drive (if the hard drive exists in the UEFI/BIOS Setup boot menu).
   - If Legacy OpROM is enabled in UEFI/BIOS Setup, a message appears showing that such boot is not supported. In order for Sobol to operate, enable UEFI boot.

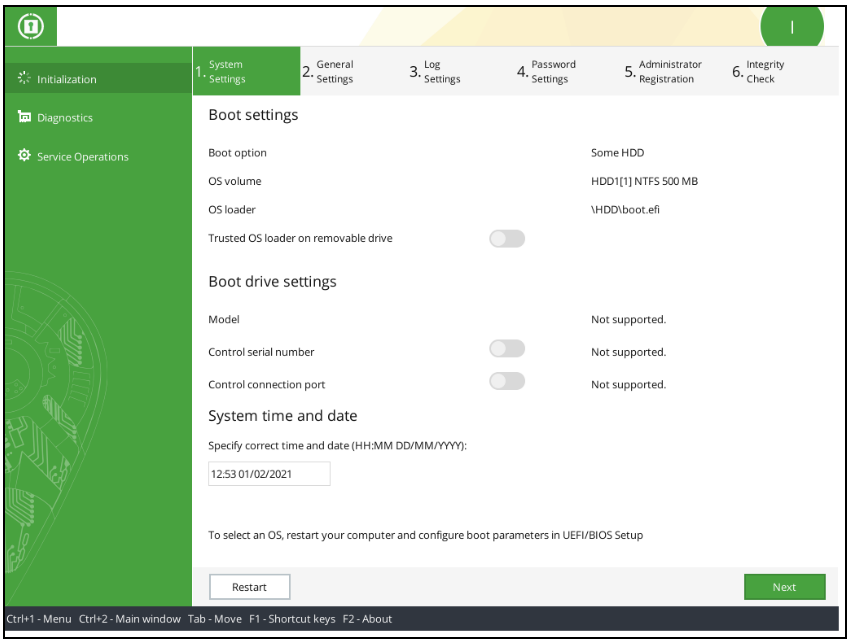
   **Note.** If the test ended with an error, the computer will be blocked for all users including the administrator. For detailed information about the error, see p. **92**.

   After the test is successfully complete, a dialog box appears prompting you to select the interface language.

2. Select the interface language.

   **Note.** You can change the interface language while Sobol is in operation. For more detail, see p. **52**.

   The initialization dialog box appears.



Boot settings

Boot option: Some HDD

OS volume: HDD1[1] NTFS 500 MB

OS loader: \HDD\boot.efi

Trusted OS loader on removable drive

Boot drive settings

Model: Not supported.

Control serial number: Not supported.

Control connection port: Not supported.

System time and date

Specify correct time and date (HH:MM DD/MM/YYYY): 12:53 01/02/2021

To select an OS, restart your computer and configure boot parameters in UEFI/BIOS Setup

**Fig. 19 Sobol initialization section**

The **I** indicator in the top right corner displays that Sobol is being initialized.

The navigation panel contains procedures available during the initialization:

- **Initialization** - start the initialization;
- **Diagnostics** - check if Sobol components work correctly;

  **Note.** Before Sobol initialization, we recommend checking all Sobol components. To do this, in the **Diagnostics** section, click **Run all tests**. For detailed information about the **Diagnostics** section, see p. 72.

- **Service operations** — set the system time and date, perform operations with security tokens and UEFI Option ROM. For detailed information, see p. **73**.

**Note.** The menu items **Diagnostics** and **Service operations** will become available after system settings have been configured during the initialization (see p. 24).

The display area of the main window contains information about the procedure (its progress, parameters, messages, etc.) and the respective buttons.

The ribbon at the bottom contains a description for shortcut key actions.

To work in the interface, use the mouse or the following keys on the keyboard:

- <Ctrl>+<1>/<Ctrl>+<2> — to move a pointer to the navigation panel/display area;
- <Tab> — move the cursor from one menu item or a parameter to another;
- <Enter> — select a menu item or a parameter;
- <Space> — to change a parameter value (if necessary, enter a new value using the keyboard);
- <F1> — shortcut key list;
- <F2> — view information about Sobol (see p. **101**).

**Note.** You can use additional control keys when configuring Sobol settings.

3. Select **Initialization**.

   The initialization starts. The initialization steps are displayed at the top of the main window.

   **Note.** During Sobol initialization, you can go back to the previous steps and reconfigure the settings as long as the administrator is not registered (see p. 32).

## Configure system settings

**Attention!** After the system settings are configured, the menu items **Diagnostics** and **Service operations** will not be available on the next step.

The **System Settings** window contains parameters described in the table below.

**Note.** When an OS boots from the network card, system settings are different from the ones described in this section. For the description of network OS boot settings, see p. 100.

1. Configure the system settings using Tab. 4 on p. **25**.

   **Note.** If you want the OS to boot from the network card, use  on p. 100.

2. To save parameters, select **Next**, or **Restart** to restart the computer.

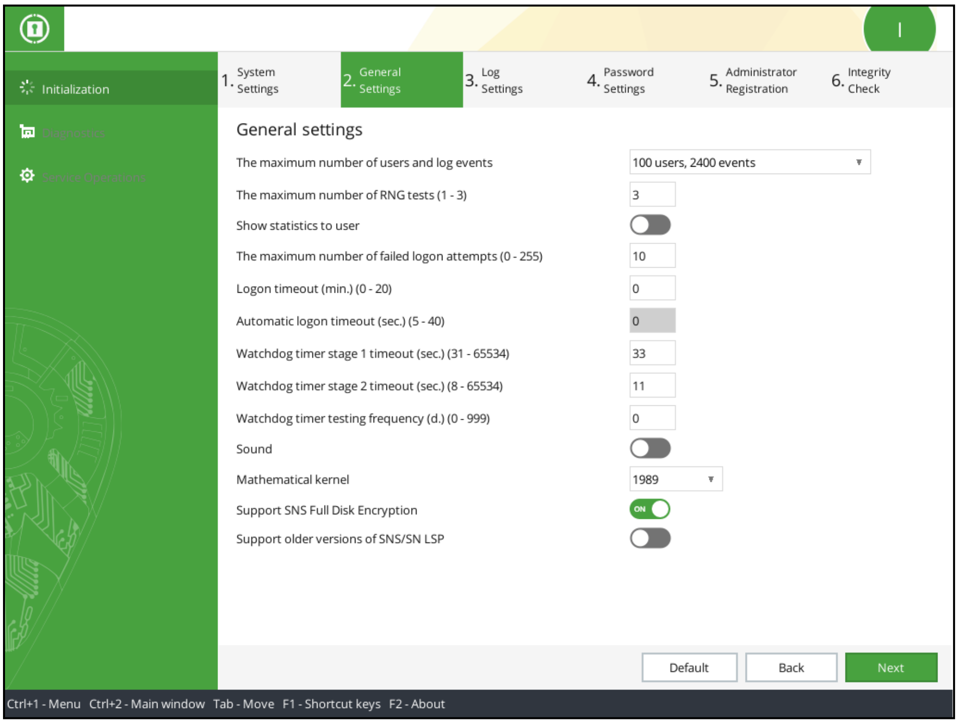
**Tab. 4 The Sobol system settings**

| **Boot option** |
|---|
| Displays the selected boot option.<br>To configure the parameter, restart your computer and configure the boot parameters in UEFI/BIOS Setup |
| **OS volume** |
| Displays the drive and the disk partition where the OS is installed.<br>To configure the parameter, restart your computer and configure the boot parameters in UEFI/BIOS Setup |
| **OS loader** |
| Displays the full name of the selected OS loader (the file name and the path).<br>To configure the parameter, restart your computer and configure the boot parameters in UEFI/BIOS Setup |
| **Trusted OS loader on removable drive** |

| |
|---|
| Allows you to use a removable drive as a trusted OS loader. Takes the following values:<br>• ON — trust an OS loader specified in the OS loader parameter;<br>• OFF — do not use a removable drive as a trusted OS loader.<br>The default values is OFF.<br>Note that:<br>• this parameter is available only for a removable boot drive;<br>• if you enable this parameter, an OS is loaded from the trusted boot drive despite booting from removable drives being forbidden for a user;<br>• this parameter will be automatically set to OFF if you modify the OS boot parameters |
| **Model** |
| Displays the model of the drive where the OS is installed.<br>To configure the parameter, restart your computer and configure the boot parameters in UEFI/BIOS Setup |
| **Control serial number** |
| Displays the serial number of the drive where the OS is installed and also allows you to control it. Takes the following values:<br>• ON — control the serial number of the system drive;<br>• OFF — do not control the serial number of the system drive.<br>The default value is OFF |
| **Control connection port** |
| Displays the port of the motherboard to which the hard drive with the installed OS is connected. Also allows you to control it. Takes the following values:<br>• ON — control the connection port;<br>• OFF — do not control the connection port.<br>The default value is OFF |
| **System time and date** |
| Displays the system time and date. Set the required time and date if necessary |

## General settings

The General Settings window is shown in the figure below.



General settings

| | |
|---|---|
| The maximum number of users and log events | 100 users, 2400 events |
| The maximum number of RNG tests (1 - 3) | 3 |
| Show statistics to user | ○ |
| The maximum number of failed logon attempts (0 - 255) | 10 |
| Logon timeout (min.) (0 - 20) | 0 |
| Automatic logon timeout (sec.) (5 - 40) | 0 |
| Watchdog timer stage 1 timeout (sec.) (31 - 65534) | 33 |
| Watchdog timer stage 2 timeout (sec.) (8 - 65534) | 11 |
| Watchdog timer testing frequency (d.) (0 - 999) | 0 |
| Sound | ○ |
| Mathematical kernel | 1989 |
| Support SNS Full Disk Encryption | ON |
| Support older versions of SNS/SN LSP | ○ |

1. Set the general settings values using Tab. 5 (except for Language).

   **Note.** You can change the language while Sobol is in operation (see p. 52).

   **Attention!** The settings **The maximum number of users and log events**, **Mathematical kernel** and **Support SNS Full Disk Encryption** are configured only when Sobol is being initialized. You cannot modify these settings after you put Sobol into operation.

   To set the default values, click **Default**.

2. To save parameters and go to the next step, click **Next**.

   To save parameters and return to the previous step, click **Back**. In this case, the changes will be saved as well.

### Tab. 5 The general settings

| **The maximum number of users and log events** |
|---|
| Defines the maximum number of user accounts that can be created during operation and the maximum number of log entries considering the selected number of users. The parameter takes the following values:<br>• 50 users, 3200 events;<br>• 100 users, 2400 events;<br>• 150 users, 1700 events;<br>• 200 users, 1000 events;<br>• 260 users, 150 events.<br>The default value is 100 users, 2400 events.<br>**Attention!** This parameter can be configured only during Sobol initialization. You cannot edit this parameter during Sobol operation. |
| **The maximum number of RNG tests** |
| Defines the number of attempts to test RNG operation performed while a user logs on to the system. Takes a value from 1 to 3. The default value is 3.<br>If the first attempt is successful, the test is completed and continues its operation. If the number of attempts reaches the selected value, you receive a message of RNG testing error |

**Show statistics to user**

Allows you to configure the display of an information window after a user logs on to the system. Takes the following values:

- ON — show statistics to a user;
- OFF — show statistics to a user.

The default value is OFF

**The maximum number of failed logon attempts**

Defines the allowed number of failed logon attempts. Takes a value from 0 to 255. The default value is 10.
Note that:

- If the parameter value is 0, the number of failed logon attempts is not limited.
- If the number of failed logon attempts of a user reaches the selected value, the user logon is blocked.
- If a user logs on to the system successfully before the number of failed logon attempts reaches the selected value, the counter of failed logon attempts resets

**Logon timeout**

Defines the period of time (in minutes) for users to log on to the system. Takes a value from 0 to 20. The default value is 0.
Note that:

- If the parameter value is 0, there is no timeout.
- When a user logs on, the period of time to present a security token and type a password is shown on the screen. When the time expires, a user receives a message that current session is ended.
- If the **Automatic logon timeout** value is not 0 (see the parameter below), **Logon timeout** is disabled

**Automatic logon timeout**

Defines the time period (in seconds) upon expiration of which automatic logon is performed. Takes a value 0 or from 5 to 40. The default value is 0.
Note that:

- If the parameter value is 0, a user/administrator cannot log on to the system without using personal security tokens.
- To use automatic logon, the AUTOLOAD user must be on the user list. If the AUTOLOAD user does not exist, Automatic logon timeout is disabled.
- If the AUTOLOAD user is on the user list and the **Logon timeout** value is 0 (see the parameter above), **Automatic logon timeout** is disabled

**Watchdog timer stage 1 timeout**

Defines the period of time (in seconds) upon expiration of which a computer will be automatically blocked if UEFI/BIOS Option ROM has not taken control. If UEFI/BIOS Option ROM boots successfully, the watchdog timer stage 2 triggers.
Recommended timeout is determined during initialization and set as the default value. An administrator can edit **Watchdog timer timeout** from the determined value to 65534

**Watchdog timer stage 2 timeout**

Defines the period of time (in seconds) upon expiration of which a computer will be automatically blocked if an OS controlled by Sobol has not started.
Recommended timeout is determined during initialization and set as the default value. An administrator can edit **Watchdog timer timeout** from the determined value to 65534

**Note.** If Sobol runs on a computer without a monitor, we recommend setting the watchdog timer timeout 7-10 seconds greater than the automatically defined value. This is due to the fact that it takes longer to start a computer without a monitor. As a result, the watchdog timer may trigger before UEFI/BIOS Option ROM takes control.

**Watchdog timer testing frequency**

Defines the period of time (in days) during which the watchdog timer is tested. Takes a value from 0 to 999. The default value is 0.
Note that:

- Testing is performed with the specified frequency when a user logs on to the system.
- If the parameter value is 0, the testing is not performed

**Sound**

Allows you to configure sound for the following events:

- logon countdown (see Logon timeout above);
- automatic logon without entering credentials;

Takes the following values:

- ON — play sound;
- OFF — do not play sound.

The default value is OFF

**Mathematical kernel**

Defines the algorithm for checksum calculation. Takes the following values:

- 1989 — GOST 28147-89 in MAC Generation Mode;
- 2015/2018 — the Magma algorithm (GOST R 34.12-2015, GOST 34.12-2018) in MAC Generation Mode (GOST R 34.13-2015, GOST 34.13-2018)

The default value is 1989.

**Attention!**

- To use in joint mode and to ensure compatibility with the older versions, select 1989.
- The administrator who operates with multiple s must set the same value for this parameter.
- This parameter can be configured only during initialization. You cannot edit this parameter during operation.

**Language**

Defines the interface language.
Takes the following values:

- Russian;
- English;

The parameter can be changed while Sobol is in operation and comes into effect after computer restart.

**Support SNS Full Disk Encryption**

Allows you to access disk volumes encrypted by SNS.
Takes the following values:

- ON — SNS Full Disk Encryption is enabled;
- ON — SNS Full Disk Encryption is disabled.

The default value is OFF.

**Support older versions of SNS/SN LSP**

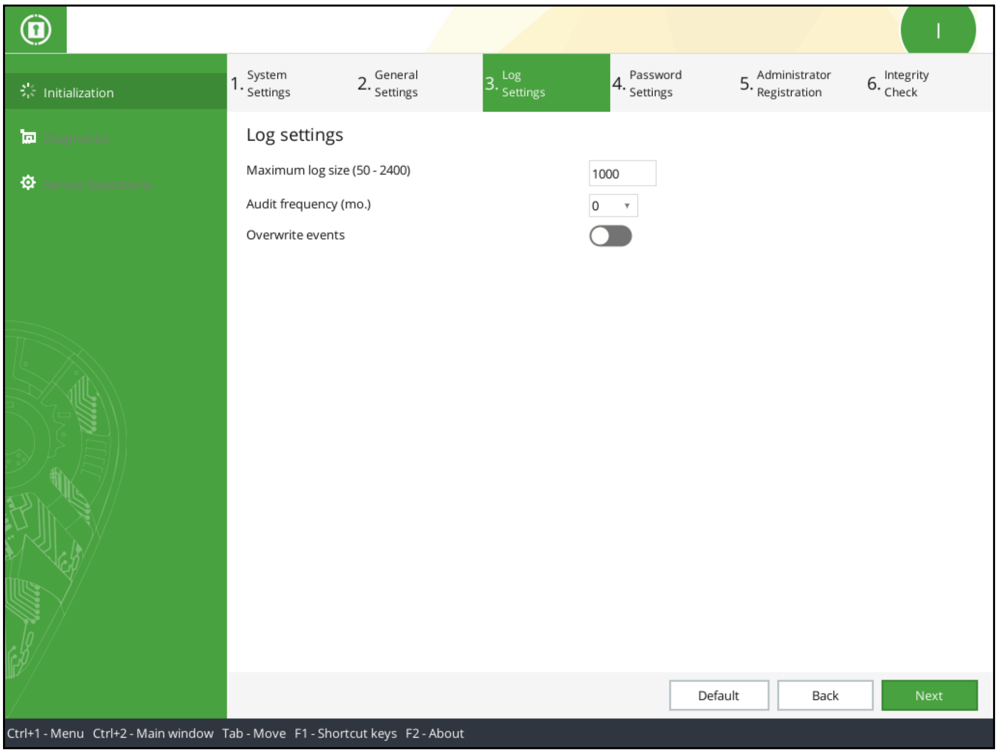
Ensures compatibility with earlier versions of SNS/SN LSP.
Takes the following values:

- ON — SNS Full Disk Encryption is enabled;
- ON — SNS Full Disk Encryption is disabled.

The default value is OFF

## Configure log settings

The figure below illustrates the Log Settings window.



Log settings

Maximum log size (50 - 2400) 1000

Audit frequency (mo.) 0

Overwrite events

1. Configure the log settings using the table below.

   **Note.** You can configure the log settings during Sobol initialization or operation (see p. 68).

   To reset the settings, click **Default**.

2. To save parameters and go to the next step, click **Next**.

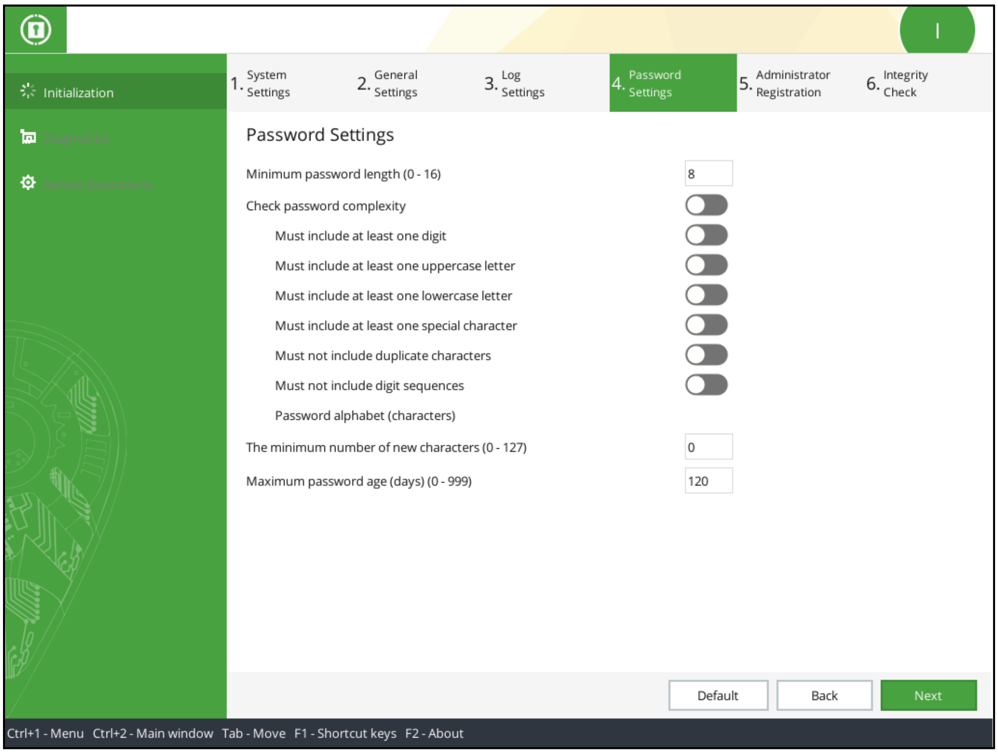
   To save parameters and return to the previous step, click **Back**. In this case, the changes will be saved as well.

**Tab. 6 Sobol log settings**

| **Maximum log size** |
|---|
| Defines the number of events to be saved to the log. Its range depends on **The maximum number of users and log events** general parameter (see Tab. 5 on p. **27**). Takes the following values:<br>• for users — from 50 to 200;<br>• for events — from 800 to 3200 (the default value is 1000) |
| **Audit frequency** |
| Defines the frequency (in months) of performing an audit of the Sobol log. Takes a value from 0 to 12. The default value is 0. Note that:<br>• if the parameter value is 0, the audit is never performed;<br>• if the value is from 1 to 12, sends a warning prompting the administrator to perform an audit according to the selected value |
| **Overwrite events** |
| Enables overwriting events when log is 100% full. Takes the following values:<br>• ON — event overwriting is performed;<br>• OFF — event overwriting is not performed.<br>The default value is OFF |

## Password settings

The Password Settings window is shown in the figure below.



Password Settings

| | |
|---|---|
| Minimum password length (0 - 16) | 8 |
| Check password complexity | ○ |
| Must include at least one digit | ○ |
| Must include at least one uppercase letter | ○ |
| Must include at least one lowercase letter | ○ |
| Must include at least one special character | ○ |
| Must not include duplicate characters | ○ |
| Must not include digit sequences | ○ |
| Password alphabet (characters) | |
| The minimum number of new characters (0 - 127) | 0 |
| Maximum password age (days) (0 - 999) | 120 |

**Fig. 20 The Password settings window**

1. Configure the password settings using the table below.

   To set the default values, click **Default**.
2. To save parameters and go to the next step, click **Next**.

   To save parameters and return to the previous step, click **Back**. In this case, the changes will be saved as well.

**Tab. 7 The Sobol password settings**

| |
|---|
| **Minimum password length** |
| Defines the minimum length of the password (in characters). Takes a value from 0 to 16. The default value is 8.<br>Note that:<br>• If the parameter value is 0, a user can have a blank password (a password will not be requested);<br>• If the parameter value is from 0 to 5 and **Check password complexity** is ON, **Minimum password length** is set to 6;<br>• If a user password length less than Minimum password length, the user must change the password when logging on to the system |
| **Check password complexity** |
| Allows you to configure password complexity check according to configured requirements (see the parameters below). Takes the following values:<br>• ON — check password complexity;<br>• OFF — do not check password complexity.<br>The default values is OFF.<br>When the value is ON, all password complexity parameters (see below) are set to ON |
| **Must include at least one digit** |
| **Must include at least one uppercase letter** |
| **Must include at least one lowercase letter** |
| **Must include at least one special character** |
| **Must not include the same adjacent characters** |
| **Must not include digit sequences** |

| |
|---|
| Allow you to establish complexity requirements for Sobol password. Takes the following values:<br>• ON — establish the requirement;<br>• OFF — do not establish the requirement.<br>The default values is OFF.<br>Note that:<br>• If Check password complexity is OFF, these parameters are unavailable for editing.<br>• If it is ON, the parameters become available and take the OFF value by default. |
| **Password alphabet** |
| Displays the number of characters that can be used in a password. The parameter value is counted automatically when requirements for password complexity are established (see the parameters above) |
| **The minimum number of new characters** |
| Defines the number of characters which must be changed in a new password compared to the old one. Takes a value from 0 to 127. The default value is 0.<br>Note that:<br>• if the parameter value is 0, the same password can be set again;<br>• if the parameter value is bigger than **Minimum password length**, a valid new password must meet the following requirements:<br>  • length of the new password must not be less than **The minimum number of new characters**;<br>  • all characters of the new password must be different from the respective characters of the old password |

## Administrator registration

**Attention!** After the administrator registration you cannot return to the previous steps.

While registering, the administrator receives the following credentials:

- a Secure ID and a password;
- a security token.

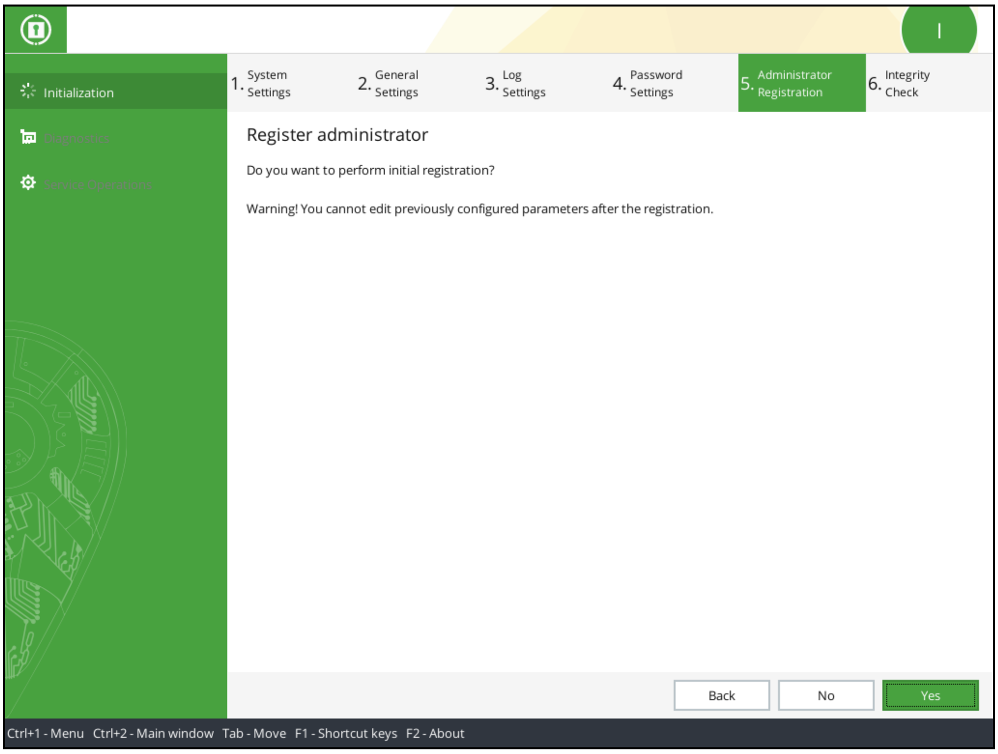
For detailed information about the initial registration, see p. **33**. For detailed information about the registration, see p. **35**.

During the **initial registration**, new registration data is recorded on the security token. If the security token already contains data (e.g. data recorded during the initialization of another), it is deleted and the administrator cannot control another Sobol.

At the **registration**, service information recorded during the initial registration is read without being changed. It allows the administrator to use the same security token to log on to the system on different computers with Sobol.

**Attention!** To register the administrator, select the same mathematical kernel as the one that was selected during the initial registration (see p. 27).

When you go to this step, the window appears as in the figure below.



Register administrator

Do you want to perform initial registration?

Warning! You cannot edit previously configured parameters after the registration.

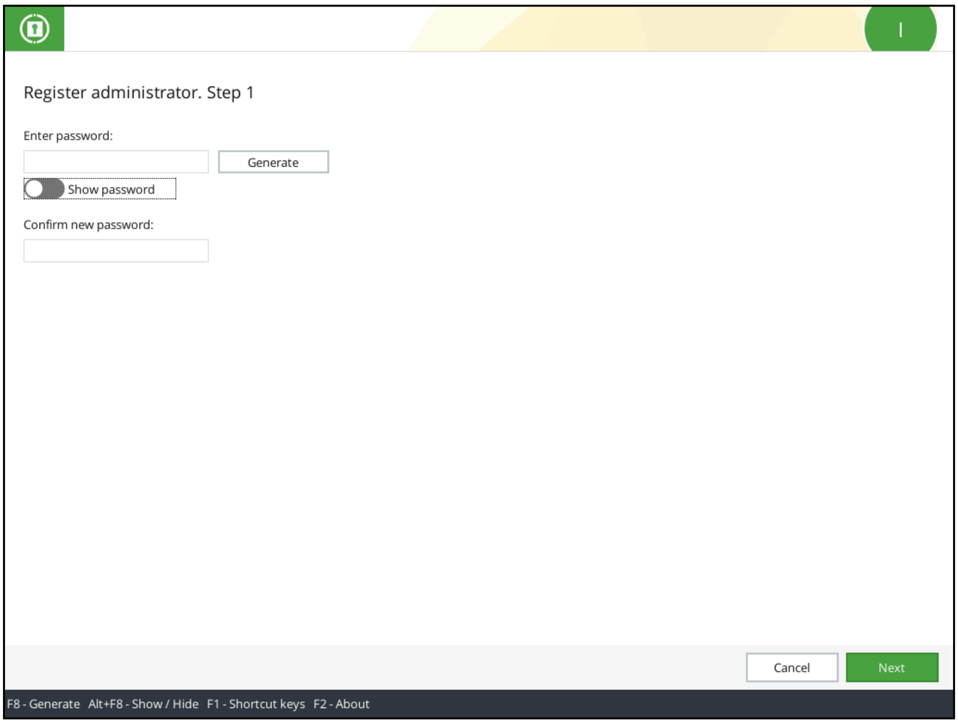
Back
No
Yes
Ctrl+1 - Menu  Ctrl+2 - Main window  Tab - Move  F1 - Shortcut keys  F2 - About

**Note.** Before starting the initial registration, prepare the required number of security tokens including tokens for creating backups of the administrator security token. We recommend creating at least one backup.

**To start the initial administrator registration:**

1. In the **Register administrator** window, select **Yes**.

   The window appears as in the figure below.



Register administrator. Step 1

Enter password:

Confirm new password:

Cancel
Next
F8 - Generate  Alt+F8 - Show / Hide  F1 - Shortcut keys  F2 - About

2. In the **Enter password** text box, type a new password that meets the requirements (see below) or generate a random password automatically clicking **Generate**.

**Attention!**

A password must contain only the following characters:

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

If the password complexity check is enabled, a password must meet the complexity requirements set at the Password Settings step of the initialization (see p. 30).

To generate a new random password, press <F8> or select **Generate**;

**Note.**

While generating a random password, note that:

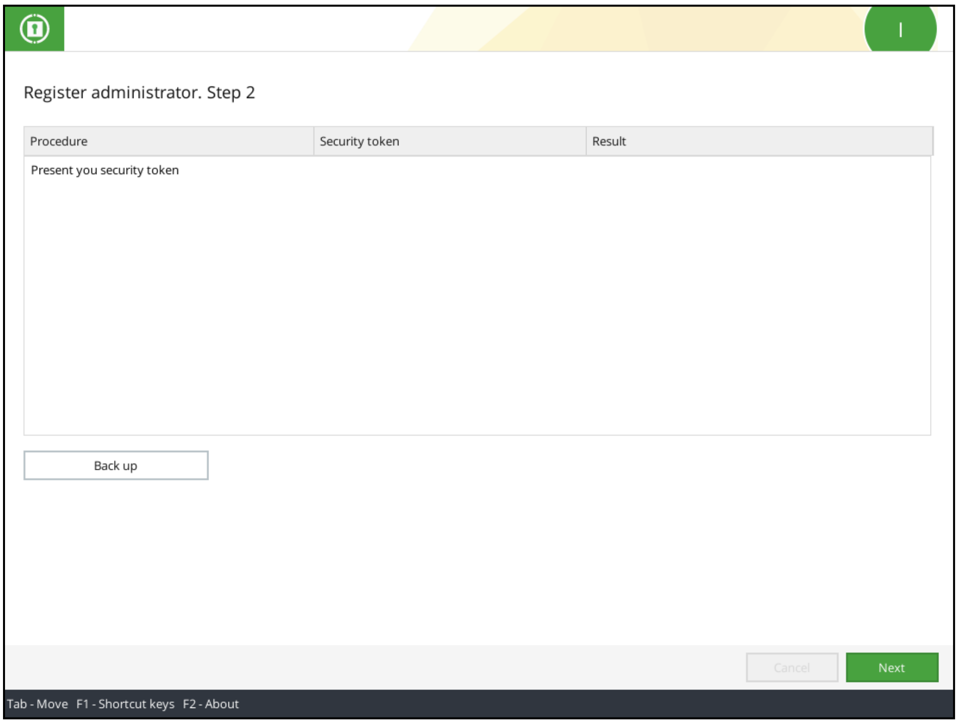
- if password complexity check is enabled, a password meets the complexity requirements set at the Password Settings step of the initialization (see p. 30);
- if password complexity check is disabled, a generated password consists of digits and lowercase Latin letters;
- the Sobol-generated password be edited.

To view the password, press <Alt>+<F8> or turn on the **Show password** toggle.

3. In the **Confirm new password** text box, type the password again.
4. Click **Next**.

**Note.** If a password entry error is detected, the respective message with the error description appears (see p. 93). Click **OK** and enter the correct password.

After you type the password correctly, a window prompting you to present the security token appears.



Register administrator. Step 2

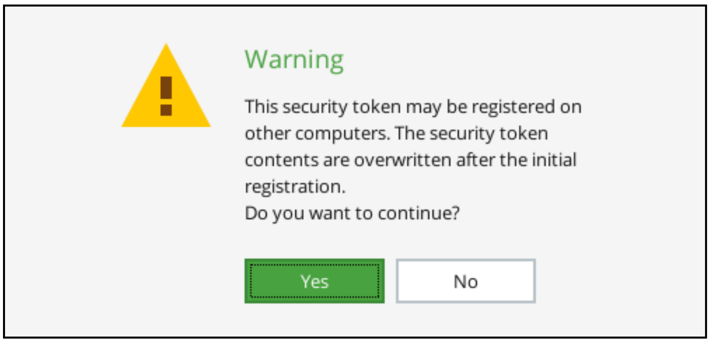
| Procedure | Security token | Result |
|---|---|---|
| Present you security token | | |

5. Present a security token to be assigned to the administrator.

**Note.**

- If the security key is already presented (the iButton key already touches the reader / the USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
- If several security tokens are presented simultaneously, the one that Sobol finds first is read.
- If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and click **OK**. Default PIN is provided on p. 8.

- If the security token is presented incorrectly, the security token prompt dialog box stays on the screen. Present the security token again.
- If the security token was registered previously on other computer and already contains service information, the following warning appears.



Warning

This security token may be registered on other computers. The security token contents are overwritten after the initial registration.
Do you want to continue?

If you are sure that nobody uses this security token, select **Yes** and present it again.

**Attention!** When writing information to a security token, service information on it will be deleted permanently. In this case, the user to whom this security token belongs will not be able to use it to log on to the system.

If you want to use another security token, select **No** and repeat step **5**.

- If the security token data structure is corrupted, the respective message appears. Sobol then suggests you to format the security token.

**Attention!** To fix the data structure corruption of the security token, format it.
After you format the iButton key, all the data stored on it will be deleted permanently.
After you format USB keys /smart cards, only information related to Sobol is lost.

To format a security token, select **Yes** in the respective dialog box. The security token is being formatted and prepared for the further work.

To continue without formatting, select **No** and present another security token.

**Note.** You can format the security token later by using **Format security token** command (see p. 74).

After the administrator is assigned with a personal security token, you receive the respective message. To create a security token backup, select **Back up**.

**Note.** Security token backups can be used by the administrator for emergency logon to the system in case the original security token is damaged or lost. We recommend creating at least one backup.

**6.** Select the way to continue the procedure:

- if you are sure that the backups are not necessary, go to step **9**;
- to create a security token backup, select **Back up**.

  A window requesting your security token appears.

**7.** Present the security token for backup.

**Note.** If you receive any messages, take step **5**.

When the backup is created, you receive the respective message.

**8.** Repeat step **6**.

**9.** Select **Next**.

**To start the registration:**

**1.** In the **Register Administrator** window, select **No**.

A dialog box prompting you to enter an administrator password appears.

**2.** Enter the password assigned to the administrator during the initial registration for another and select **Next**.

A dialog box prompting you to present a security token appears.

**3.** Present the security token assigned to the administrator during the initial registration for another Sobol.

**Note.**
- If the security token is already presented (the iButton key touches the reader / the USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
- If several security tokens are presented simultaneously, the one that Sobol finds first is read.
- If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and click **OK**. Default PIN is provided on p. 8.

If the security token is valid, checks if the entered password matches the information stored on the security token:

- If the entered password is incorrect or the presented security token is not assigned to the administrator, you receive the respective message.

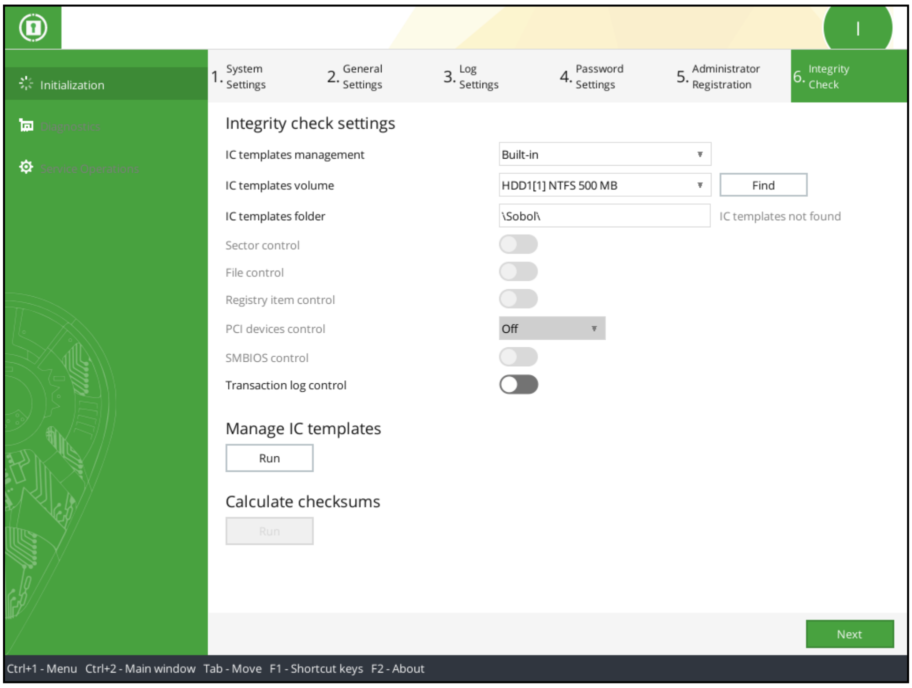
  Click **OK**. In the **Register Administrator. Step 2** window, select **Cancel**. The message prompting you to select the type of administrator registration appears.
- If the entered password matches a presented security token, service information is read and then saved to the Sobol nonvolatile memory. To save the changes and to go to the next step, select **Next**. To return to the previous step, select **Back**.

## Configure IC settings and calculate checksums

**Attention!** In case there are encrypted volumes on your computer that were created using SNS and **Support SNS Full Disk Encryption** is enabled (see on p. 27), a dialog box prompting you to enter the password for the encrypted volumes appears. For more detail, see Secret Net Studio documentation.

If access to encrypted volumes is not granted, configuring IC of resources on encrypted volumes is not available. To get access to the encrypted volumes, restart the computer and perform initialization again.

The figure below illustrates the **Integrity Check Settings** window.



Integrity check settings

IC templates management: Built-in

IC templates volume: HDD1[1] NTFS 500 MB [Find]

IC templates folder: \Sobol\ — IC templates not found

Sector control

File control

Registry item control

PCI devices control: Off

SMBIOS control

Transaction log control

Manage IC templates [Run]

Calculate checksums [Run]

**Attention!** We recommend installing Sobol software before a Sobol card is installed. If Sobol software is not installed beforehand, you can skip the configuration of IC settings and calculation of checksums for now and return to them later when Sobol is in operation ( p. 63).

1. In the **IC template management** drop-down list, select one of the following options:
   - **Sobol software** — using Sobol software;

     **Note.** Sobol software is installed on and used in an OS. For more detail, see document [**1**].
   - **Built-in** — using built-in IC template management.

     **Note.** IC templates can be configured now or when Sobol is in operation (see p. 63). If you want to manage IC templates now, click **Start** and follow the instructions from p. 79.
2. In the **IC templates volume** drop-down list and the **IC templates folder** text box, specify the required options in one of the following ways:
   - click **Find**. Sobol searches for IC templates in standard folders

     **Note.**
     - IC templates will be found in standard folders if Sobol software have been installed beforehand or the administrator have created them earlier.
     - The standard folder for Windows is **\Sobol**.
     - The standard folder for Linux are **/sobol** and **/boot/sobol**.
     - If the standard folders are not found or do not contain IC templates, you receive a message about an error. Follow the recommendations from p. 95.
   - if IC templates were created on other volumes, in the drop-down list, select the volume with the IC templates and enter the path to the folder with them in the respective field.

     **Note.** For folders on FAT16, FAT32 disks, long names (more than 8 characters) should be shortened, i.e. progra~1. You can find out the short form of the name using the DIR command or Total Commander.

If the folder with IC templates is found and these templates are valid , the IC parameters are available for editing.

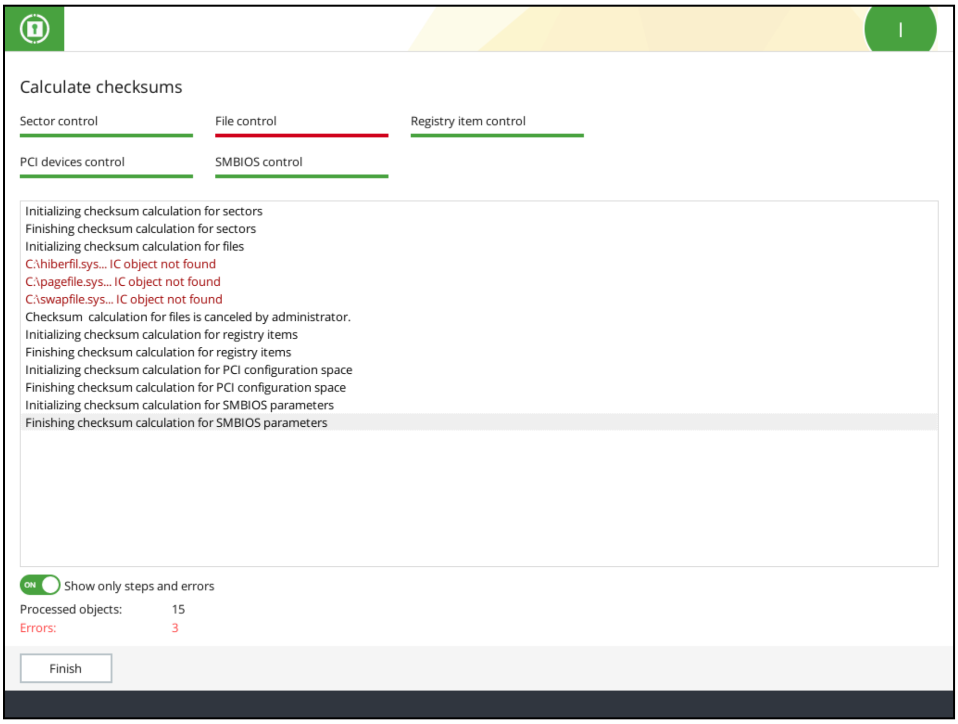
**Note.**
- The **Sector control**, **File control**, **Registry item control**, **SMBIOS control** parameters are enabled.
- The **PCI device control** parameter is set to Basic.

3. Enable IC for the required objects:
   - to enable IC for disk sectors / files / registry items / SMBIOS structures, turn on the **Sector control**, **File control**, **Registry item control**, **SMBIOS control** toggles;
   - to enable IC PCI devices, select the required option in the drop-down list **PCI device control** (see Tab. 3 on p. **9**).
   - to enable IC for a transaction log, turn on the **Transaction log control** toggle.
4. Configure the **IC key update frequency** parameter:
   - to update the IC key automatically, specify the number of days until the next update (from 1 to 999);
   - to disable IC key update, set 0.

**Note.**
- The parameter is available only if you select mathematic kernel version 2015/2018 when configuring general settings during Sobol initialization (see p. **29**).
- The default value of the parameter is 0.

5. Calculate the reference checksums for IC objects. To do so, select **Start** in the **Calculate checksums** section.

   The calculation process is displayed on the screen.



```
Initializing checksum calculation for sectors
Finishing checksum calculation for sectors
Initializing checksum calculation for files
C:\hiberfil.sys... IC object not found
C:\pagefile.sys... IC object not found
C:\swapfile.sys... IC object not found
Checksum  calculation for files is canceled by administrator.
Initializing checksum calculation for registry items
Finishing checksum calculation for registry items
Initializing checksum calculation for PCI configuration space
Finishing checksum calculation for PCI configuration space
Initializing checksum calculation for SMBIOS parameters
Finishing checksum calculation for SMBIOS parameters
```

ON Show only steps and errors

Processed objects: 15

Errors: 3

**Note.**
- The process color indicators:
  - green – successful checksum calculation;
  - red – errors during checksum calculation;
  - black – messages.
- By default, Sobol shows only errors and calculation process steps. To view all the calculation results, turn off the **Show only steps and errors** toggle.

If an error occurs, the message with its description appears. Read the message and click **OK**.

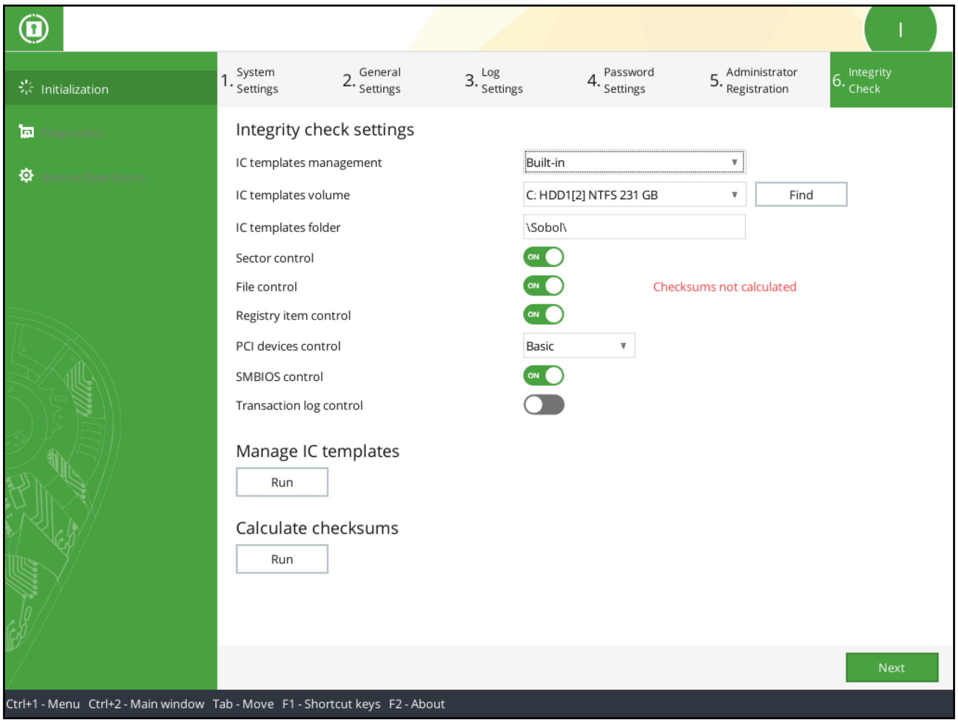
**Note.** If you do not need any notifications about checksum calculation, select the **Don't ask again** check box.

To interrupt the checksum calculation, press <Esc> or select **Cancel**.

6. Once the procedure is complete, read the results and click **Finish**.

> **Note.** If you have enabled IC for PCI devices, when disconnecting a controlled device from a PCI bus, a group of error messages may occur during the checksum recalculation. In this case, pay attention only to the Not found error messages. Other error messages from the group occur due to peculiarities of assigning addresses to PCI devices in UEFI: when you delete a device and restart the computer, configuration data and device addresses may change.

The **Integrity Check** window appears. If the checksum calculation for an IC object is completed with an error, a message appears next to the respective parameter of the object.



Integrity check settings

IC templates management: Built-in

IC templates volume: C: HDD1[2] NTFS 231 GB   Find

IC templates folder: \Sobol\

Sector control: ON

File control: ON   Checksums not calculated

Registry item control: ON

PCI devices control: Basic

SMBIOS control: ON

Transaction log control

Manage IC templates

Run

Calculate checksums

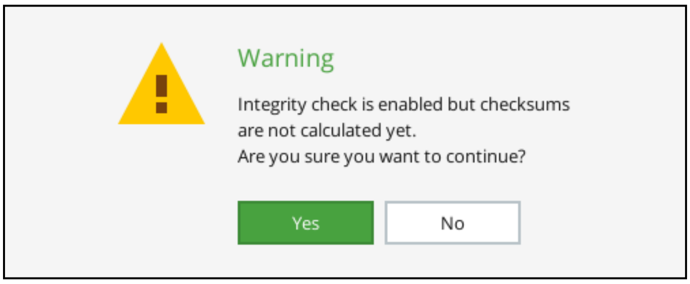
Run

Next

Ctrl+1 - Menu  Ctrl+2 - Main window  Tab - Move  F1 - Shortcut keys  F2 - About

**7.** In the **Integrity Check** window, select **Next**.

If an error occurred during the checksum calculation, the respective message appears.



Warning

Integrity check is enabled but checksums are not calculated yet.
Are you sure you want to continue?

To complete the initialization, select **Yes**. Checksum calculation may be performed when Sobol is in operation.

> **Note.** To return to IC settings configuration and checksum calculation, select **No**.

## Complete initialization

When the initialization is completed, the respective message appears.

**To complete the initialization:**

1. Select **OK**. The computer shuts down automatically.
2. Put Sobol into operation (see below).

# Chapter 3
# Updating and uninstalling Sobol

## Updating Sobol

You can update the following Sobol components:

- Sobol software;

  **Note.** For the instruction on how to update Sobol software, see [**1**].

- UEFI/BIOS Option ROM (see p. **77**);
- FPGA.

  **Note.** For details on how to update FPGA, contact the Security Code support.

## Uninstall Sobol

To uninstall Sobol, take the following steps:

- uninstall the Sobol software if it was installed;

  **Note.** For more details about Sobol software removal, see document [**1**].

- remove the Sobol card from the computer (see p. **40** for PCIe, p. **41** for Mini PCIe Half, p. **41** for M.2).

**Attention!**

- After uninstalling Sobol, all the service information about its configuration is stored in the nonvolatile memory of the Sobol card. Thus, you can install and use Sobol without initialization if the administrator and user security tokens contain registration information. After uninstalling Sobol, the administrator must store the Sobol card the way that prevents it from unauthorized physical access.
- To delete service information from the Sobol memory, perform the initial registration during the initialization (see p. **24**).

## Remove a PCIe card

**To remove a PCIe card:**

1. Shut down your computer.
2. Remove the side panel.
3. If the iButton reader is attached to the Sobol card, remove it:
   - if you use the external reader, remove it from the Sobol card socket on the back of the system unit;
   - if you use the internal reader, remove it from the TM connector (see Fig. 2 on p. **13**).
4. Remove the Sobol card from the PCIe slot.
5. If the watchdog timer enables forced automatic restart of the computer, take the following steps:
   - disconnect RST watchdog cable from the WD connector of Sobol card (see Fig. 2 on p. **13**) and from the Reset connector on the motherboard;
   - disconnect the Reset button cable from the Reset connector on the Sobol card (see Fig. 2 on p. **13**) and connect it to the Reset connector on the motherboard;
   - disconnect the power cable from the SATA connector (see Fig. 2 on p. **13**).
6. If the watchdog timer enables forced automatic shutdown of the computer, take the following steps:
   - for the 24-ATX connector:
     - disconnect the X1 connector (see B), Fig. 1 on p. **11**) from the RL connector on the PCIe card (see Fig. 2 on p. **13**);
     - disconnect the X2 and X6 connectors from the ATX connector on the motherboard;
     - disconnect the X5 connector from the X3 connector;
     - disconnect the power cable from the X4 connector of the ATX cable watchdog relay;
     - connect the power cable to the ATX connector on the motherboard;
     - disconnect the power cable from the SATA connector on the PCIe card (type 1,2) (see Fig. 2 on p. **13**);
   - for the 20-ATX connector:

  - disconnect the X1 connector (see B), Fig. 1 on p. **11**) from the RL connector on the PCIe card (see Fig. 2 on p. **13**);
  - disconnect the X2 connector from the ATX connector on the motherboard;
  - disconnect the power cable from the X3 connector of the ATX cable watchdog relay;
  - connect the power cable to the ATX connector on the motherboard;
  - disconnect the power cable from the SATA connector on the PCIe card (type 1,2) (see Fig. 2 on p. **13**);
- for the PWR watchdog cable:
  - disconnect the PWR watchdog cable from the WD connector on the Sobol card (see Fig. 2 on p. **13**) and from the T-Tap connectors (see C), Fig. 1 on p. **11**). Keep the connectors folded over the wires of the Power button cable to provide isolation;
  - disconnect the power cable from the SATA connector on the PCIe card (type 1,2) (см. Fig. 2 on p. **13**);
- for connecting the RST watchdog cable to the Power button cable in parallel:
  - disconnect the RST watchdog cable from the WD connector on the PCIe card (see Fig. 2 on p. **13**). Keep the connectors folded over the wires of the Power button cable to provide isolation;
  - disconnect the power cable from the SATA connector on the PCIe card (type 1,2) (see Fig. 2 on p. **13**).

**7.** Put the side panel back.

## Remove a Mini PCIe Half card

**To remove an adapter and a Mini PCIe Half card:**

1. Shut down your computer.
2. Remove the side panel.
3. If an iButton reader is attached to the adapter, remove it:
   - if you use the external reader, remove it from the required connector of the adapter (see Fig. 7 on p. **17**, Fig. 8 on p. **17** or Fig. 9 on p. **17**);
   - if you use the internal reader, remove it from the TM connector of the adapter(see Fig. 7 on p. **17** or Fig. 10 on p. **18**).
4. Remove the card from the Mini PCIe slot.
5. Remove the adapter from the slot of the system unit.
6. If the watchdog timer enables forced automatic restart of the computer, take the following steps:
   - disconnect the RST watchdog cable from the WD connector (see Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**) and the Reset connector on the motherboard;
   - if you use the type 1 adapter, disconnect the Reset button cable from the RST connector (see Fig. 7 on p. **17**) and connect the Reset cable to the Reset connector on the motherboard.
7. If the watchdog timer enables forced automatic shutdown of the computer, take the following steps:
   - for the PWR watchdog cable — disconnect the PWR watchdog cable from the WD connector (see Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**) and from the T-Tap connectors (see C, Fig. 1 on p. **11**). Keep the connectors folded over the wires of the Power button cable to provide isolation;
   - for connecting the RST watchdog cable to the Power button cable in parallel — disconnect the RST watchdog cable from the WD connector (see Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**). Keep the connectors folded over the wires of the Power button cable to provide isolation;
8. Put the side panel back.

**To remove a Mini PCIe Half card:**

1. Shut down your computer.
2. Remove the side panel.
3. Remove the card from the Mini PCIe slot.
4. Put the side panel back.

## Remove an M.2 card

**To remove an adapter and an M.2 card (types 1, 2):**

1. Shut down your computer. Remove the side panel.

2. If the iButton reader is connected to the adapter, remove it:
   - for the external iButton reader, remove it from the respective connector on the adapter (see Fig. 7 on p. **17**, Fig. 8 on p. **17** or Fig. 9 on p. **17**);
   - for the internal iButton reader, remove it from the TM connector on the adapter (see Fig. 7 on p. **17** or Fig. 10 on p. **18**).
3. Remove the card from the M.2 slot.
4. Remove the adapter from the slot of the system unit.
5. If the watchdog timer enables forced automatic restart of the computer, take the following steps:
   - disconnect the RST watchdog cable from the WD connector on the adapter (see Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**) and the Reset connector on the motherboard;
   - for the type 1 adapter, disconnect the Reset button cable from the RST connector on the adapter (see Fig. 7 on p. **17**) and connect the Reset cable to the Reset connector on the motherboard.
6. If the watchdog timer enables forced automatic shutdown of the computer, take the following steps:
   - for the PWR watchdog cable:
     - disconnect the PWR watchdog cable from the WD connector on the adapter (see Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**) and from the T-Tap connectors (see B, Fig. 1 on p. **11**). Keep the connectors folded over the wires of the Power button cable to provide isolation;
   - for connecting the RST watchdog cable to the Power button cable in parallel:
     - disconnect the RST watchdog cable from the WD connector on the adapter (see Fig. 7 on p. **17**, Fig. 8 on p. **17**, Fig. 9 on p. **17** or Fig. 10 on p. **18**). Keep the connectors folded over the wires of the Power button cable to provide isolation.
7. Put the side panel back.

**To remove a WD module and an M.2 card (types 3, 4):**

1. Shut down your computer. Remove the side panel.
2. If the iButton reader is connected to the WD module, remove it:
   - for the external iButton reader, remove it from the respective connector on the WD 1, 4 or 5 module;
   - for the internal iButton reader, remove it from the TM connector on the WD 2, 3 or 6 module.
3. Remove the card from the M.2 slot.
4. Remove the WD module from the slot of the computer system unit.
5. If the watchdog timer enables forced automatic restart of the computer, take the following steps:
   - disconnect the RST watchdog cable from the WD connector on the WD module and the Reset connector on the motherboard;
   - for WD 1, 4 or 5 module, disconnect the Reset button cable from the RST connector on the WD module and connect it to the Reset connector on the motherboard.
6. If the watchdog timer enables forced automatic shutdown of the computer, take the following steps:
   - for the PWR watchdog cable:
     - disconnect the PWR watchdog cable from the WD connector on the WD module and from the T-Tap connectors (see B, Fig. 1 on p. **11**). Keep the connectors folded over the wires of the Power button cable to provide isolation;
   - for connecting the RST watchdog cable to the Power button cable in parallel:
     - disconnect the RST watchdog cable from the WD connector on the WD module. Keep the connectors folded over the wires of the Power button cable to provide isolation.
7. Put the side panel back.

**To remove an M.2 card:**

1. Shut down your computer. Remove the side panel.
2. Remove the card from the M.2 slot.
3. Put the side panel back.

## Putting Sobol into operation

**To put Sobol into operation using a PCIe card:**

1. Shut down your computer. Remove the side panel.
2. If the iButton reader is attached to the card, remove it:
   - if you use the external reader, remove it from the card socket on the back of the system unit;
   - if you use the internal reader, remove it from the TM connector.
3. Remove the Sobol card from the PCIe slot.
4. Switch SW1-1 for a PCIe card (type 1,2) (see Fig. 2 on p. **13**), SA1-1 for a PCIe card (type 3,4) (see Fig. 3 on p. **14**) to the ON position .
5. Insert the Sobol card into a free PCIe slot.
6. If necessary, attach an iButton reader to the PCIe card:
   - for the external iButton reader, attach it to the respective socket;
   - for the internal iButton reader, attach it to the TM connector.
7. Put the side panel back.

When all the steps above are taken, shut down the computer and start configuring Sobol (see p. **44**).

**To put Sobol into operation using a Mini PCIe Half card:**

1. Shut down your computer. Remove the side panel.
2. Put the Sobol card into operation. To do so, switch S1-1 to the ON position (see Fig. 6 on p. **16**).
3. Put the side panel back.

When all the steps above are taken, shut down the computer and start configuring Sobol (see p. **44**).

**To put Sobol into operation using an M.2 card:**

1. Shut down your computer. Remove the side panel.
2. Put the Sobol card into operation. To do so, switch SW1-1 on an M.2 card (types 1, 2 ), switch SA1 on an M.2 card (types 3, 4) to the ON position .
3. Put the side panel back.

Once all the steps above are taken, shut down the computer and start configuring Sobol (see p. **44**).

# Chapter 4
# Sobol setup and use

Before using Sobol, you must log on to the system (for more information, see below), register Sobol users (see p. **54**) and set up their accounts (see p. **58**).

Sobol makes it possible:

- manage OS boot options (see p. **50**);
- configure general Sobol settings (see p. **52**);
- configure password settings (see p. **52**);
- configure a user list and account settings (see p. **54**);
- change your password (see p. **66**) and your Secure ID (see p. **1**);
- change users' passwords and Secure IDs (see p. **61**);
- work with the log (see p. **68**);
- manage integrity check (see p. **63**);
- control the operation of Sobol (see p. **72**);
- perform a number of service operations.

For instructions on how to complete Sobol configuration, see p. **78**

## Log on as an administrator

**Attention!** Before you log on to the system, disconnect all USB Mass Storage devices (flash drives, CD and DVD drives, etc) from computer USB ports.

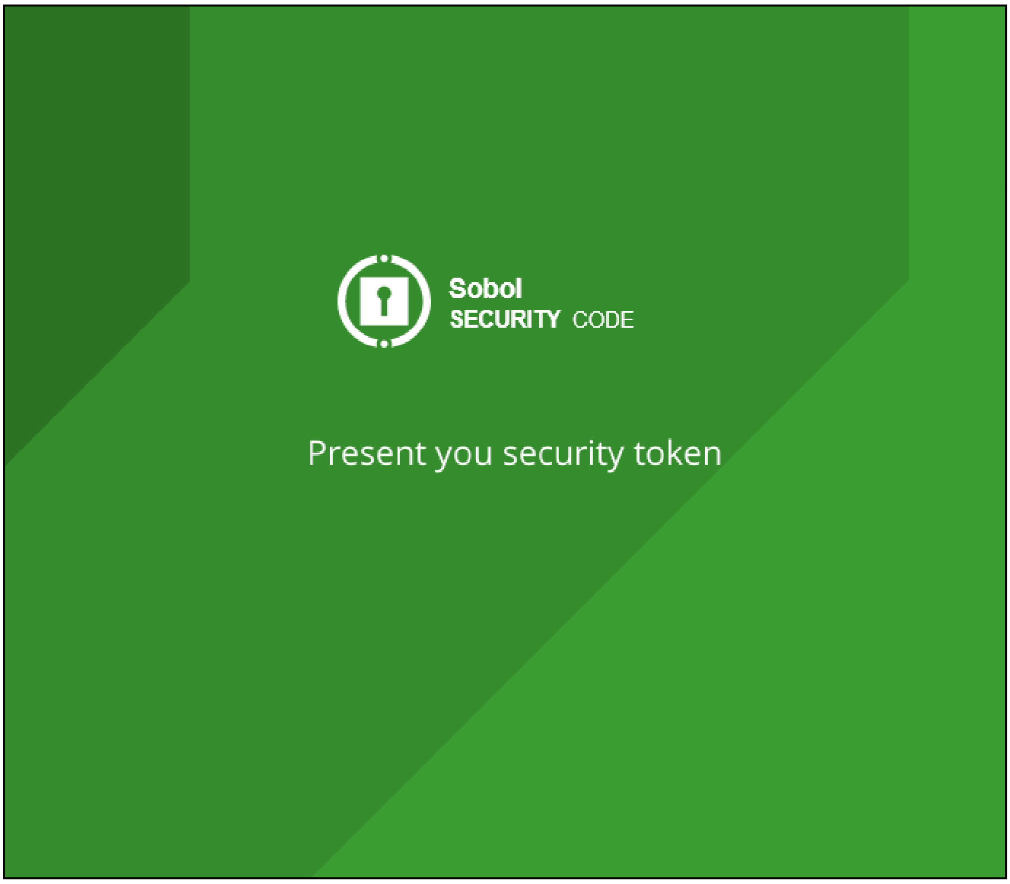
**To log on to the system as administrator:**

**1.** Turn on or reboot the computer.

takes control over the process. The card memory and RNG tests begin.

**Note.** When starting Sobol, errors leading to computer lockout may occur. The error message appears respectively. You can find the list of possible errors and the steps to fix them on p. 92.

After the tests are completed, the window requesting the security token appears.



Sobol
SECURITY CODE

Present you security token

In the top right corner of the window, the Sobol mode is indicated: S — the standalone mode, J — the joint mode.

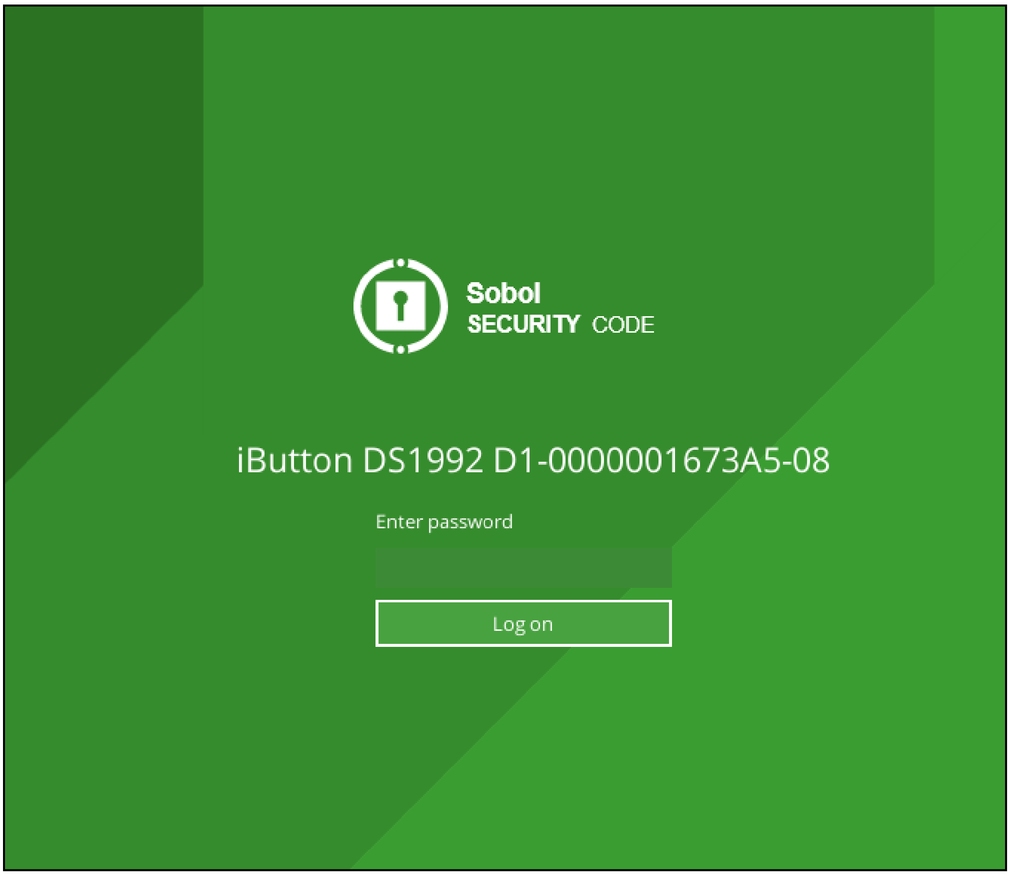
**Note.** If logon timeout is enabled (see Tab. 5 on p. 27), you will see the time left to present the security token and enter the password. The computer is to be locked unless you perform these actions in time. If so, reboot the computer and repeat the logon.

**2.** Present your administrator security token.

**Note.**

- If you already presented the security token (the IButton key touches the reader / the USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
- If several security tokens are presented at once, the serial number of the first one is displayed. To change the security token, press <Esc>.

After the security token information is read, the dialog box prompting you to enter the password appears.



iButton DS1992 D1-0000001673A5-08

Enter password

3. Enter the administrator password.

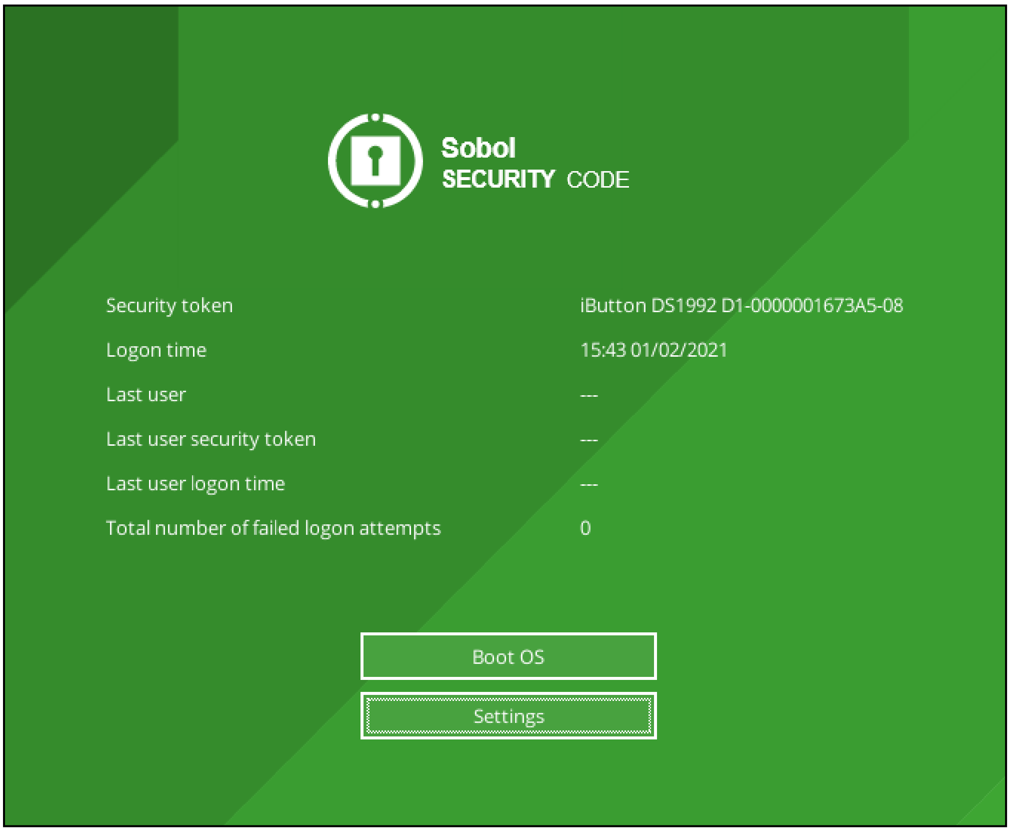
**Note.** To opt out of entering the password, press <Esc>. The request to present a security token appears again.

4. Click **Log on**.

**Note.**

- If you present an unregistered security token or enter a wrong password, displays the Wrong security token or password warning. Press any button and repeat steps 2–4 of this procedure.
- If the message This password does not meet complexity and/or minimum length requirements appears, click **OK** and change the password. p. 66).

After you enter the correct password, the following window appears.



Security token iButton DS1992 D1-0000001673A5-08

Logon time 15:43 01/02/2021

Last user ---

Last user security token ---

Last user logon time ---

Total number of failed logon attempts 0

The information window contains the following:

| Field | Description |
|---|---|
| **Security token** | The number and type of the security token presented during the logon |
| **Logon time** | The time (HH:MM) and the date (DD/MM/YYYY) when the administrator entered the password during the current logon |
| **Last user** | The name of the last user who logged on before the current administrator logon.<br>No information if a registered user did not log on to the system or if his or her account was deleted from the user list after the logon. |
| **Last user security token** | The number and type of the security token of a user logged on to the system last before the current administrator logon.<br>No information if the name of the previous user was not specified |
| **Last user logon time** | The time (HH:MM) and the date (DD/MM/YYYY) of the last user logon before the current administrator logon.<br>No information if the name of the previous user was not specified |
| **Total number of failed logon attempts** | The number is counted after the last Sobol initialization. The mistakes are incorrect security token presentation and a wrong password.<br>No information if no mistakes were made |

**5.** Select the way you want to continue the procedure:

- Click **Boot OS** to boot the operating system.

**Note.**
- If log audit is enabled (see Tab. 6 on p. 30) and the warning about the need for audit appears, the **Boot OS** button is unavailable. Click **Settings**. The event logging window appears on the screen ( on p. 68).
- In case there are encrypted volumes on your computer that were created using SNS, you will be prompted to enter the password for the encrypted volumes. For more detail, see Secret Net Studio documentation.

If integrity check is enabled, the integrity of specified objects is checked before the operating system boots.

**Note.**

- To pause the check, press <Esc> or select **Stop**.
- If an error occurs, the respective message appears. Read the message (you can find the list of error messages on p. 95). To continue the check, select **OK**.
- If you do not need notifications, in the error message window, select **Don't ask again**.
- After the check is complete and the operating system boots, fix the errors. Then, recalculate the checksums of the objects (see p. 63);
- If IC templates have been modified or checksums have been calculated, a message prompting you to restart the computer will appear. Click **OK**. The computer will be restarted.

After the integrity check is complete, click **Finish**. The operating system boots.

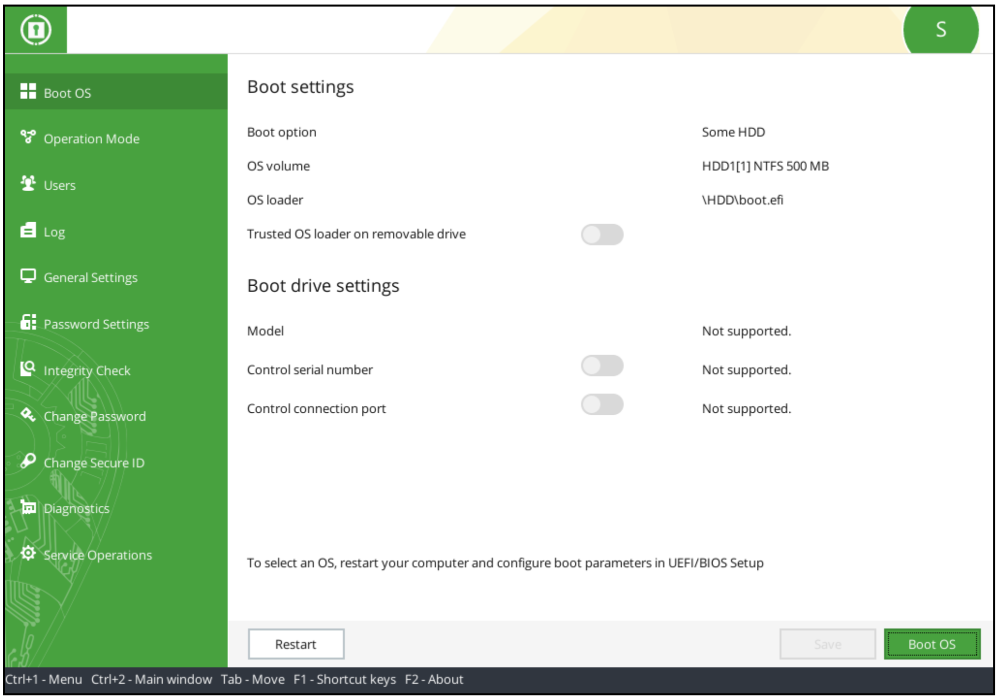
- To configure Sobol, click **Settings**.

  The administrator menu appears as in the figure below.

# Administrator menu

**Attention!** In case there are encrypted volumes on your computer that were created using SNS and **Support SNS Full Disk Encryption** is enabled (see  on p. 27), a dialog box prompting you to enter the password for the encrypted volumes appears. For more detail, see Secret Net Studio documentation.

The Sobol administrator menu appears as follows.



Boot settings

Boot option — Some HDD

OS volume — HDD1[1] NTFS 500 MB

OS loader — \HDD\boot.efi

Trusted OS loader on removable drive — ○

Boot drive settings

Model — Not supported.

Control serial number — ○ — Not supported.

Control connection port — ○ — Not supported.

To select an OS, restart your computer and configure boot parameters in UEFI/BIOS Setup

The letter in the top right corner of the menu indicates the operation mode: S — the standalone mode, J — the joint mode.

The menu on the left contains commands available to the administrator when operates.

**Note.** Some commands are unavailable if is in joint mode. For more information about configuring Sobol in this mode, see p. 99.

The main area of the window on the right of the operation menu displays information about a performed command (the implementation status, parameters, messages, etc) and control keys.

The information bar in the bottom of the window displays keyboard shortcuts.

Use the left mouse button or the following keys:

- <Ctrl>+<1>/<Ctrl>+<2> — set the cursor in the menu / in the main area of the window;
- <Tab> — move the cursor from one menu item or a parameter to another;
- <Enter> — select a menu item or a parameter;
- <Space> — to change a parameter value (if necessary, enter a new value using the keyboard);
- <F2> — view information about Sobol (see p. **101**).

**Note.** You can use additional control keys when configuring Sobol settings. To view the list of control keys, press <F1>.

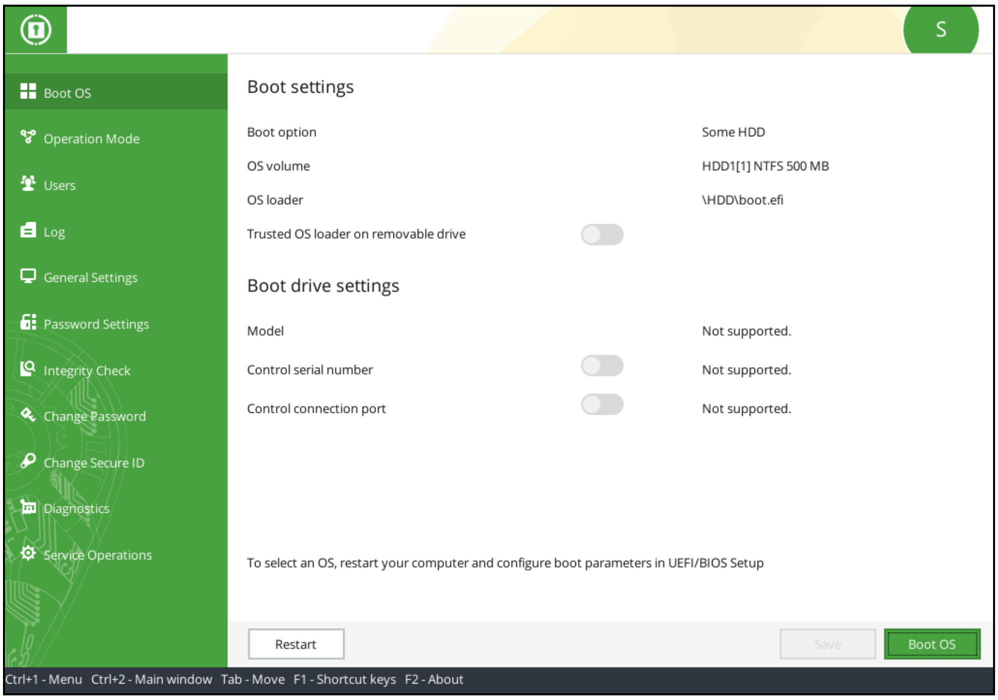
Select the administrator menu and configure the following settings:

- **Boot OS** — view and configure OS boot settings, OS boot after Sobol configuration (see p. **50**);
- **Operation Mode** — change the operation mode (see p. **50**);
- **Users** — manage users (see p. **54**);
- **Log** — manage the Sobol log (see p. **68**);
- **General Settings** — configure Sobol general settings (see p. **52**);
- **Password Settings** — configure passwords (see p. **52**);
- **Integrity Check** — configure IC, calculate checksums (see p. **63**), start the IC templates managements program (see p. **79**);
- **Change Password** — change the administrator password (see p. **64**);
- **Change Secure ID** — change the administrator secure ID (see p. **64**);
- **Diagnostics** — check Sobol operation (see p. **72**);
- **Service Operations** — format a security token, create its backup copy, software initialization, save and modify UEFI/BIOS Option ROM (see p. **73**).

## Boot OS

The **Boot OS** menu item (see the figure below) contains OS and disk boot options as well as the button for an OS boot.

**Attention!** If you change boot option in UEFI/BIOS setup, you receive the respective message and the **Save** button appears in the **Boot option** window. To save new parameters, select **Save**.



Boot settings

| | | |
|---|---|---|
| Boot option | | Some HDD |
| OS volume | | HDD1[1] NTFS 500 MB |
| OS loader | | \HDD\boot.efi |
| Trusted OS loader on removable drive | ○ | |

Boot drive settings

| | | |
|---|---|---|
| Model | | Not supported. |
| Control serial number | ○ | Not supported. |
| Control connection port | ○ | Not supported. |

To select an OS, restart your computer and configure boot parameters in UEFI/BIOS Setup

**Note.** If an OS is to boot from the network card, see the respective system settings on p. **100**.

**To configure the options:**

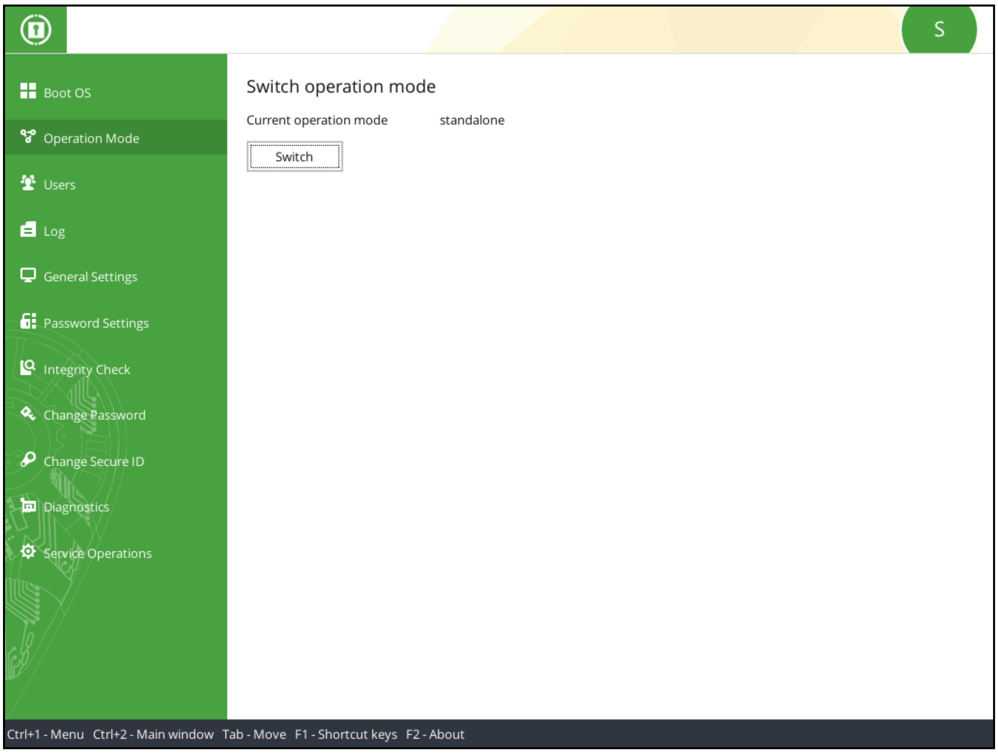
1. Set their values using Tab. 4 on p. **25** (except for System time and date).

   **Note.**
   - If an OS is to boot from the network card, use  on p. **100**.
   - You can change the system time in **Service Operations** (see p. **75**).

2. To save the changes, select **Save**.

## Operation mode

In the administrator menu, after you select **Operation mode**, the window appears as in the figure below.



Switch operation mode

Current operation mode standalone

Switch

The **Current operation mode** parameter displays the operation mode which can be:

- standalone — is in standalone mode;
- joint — operates with other information security tools.

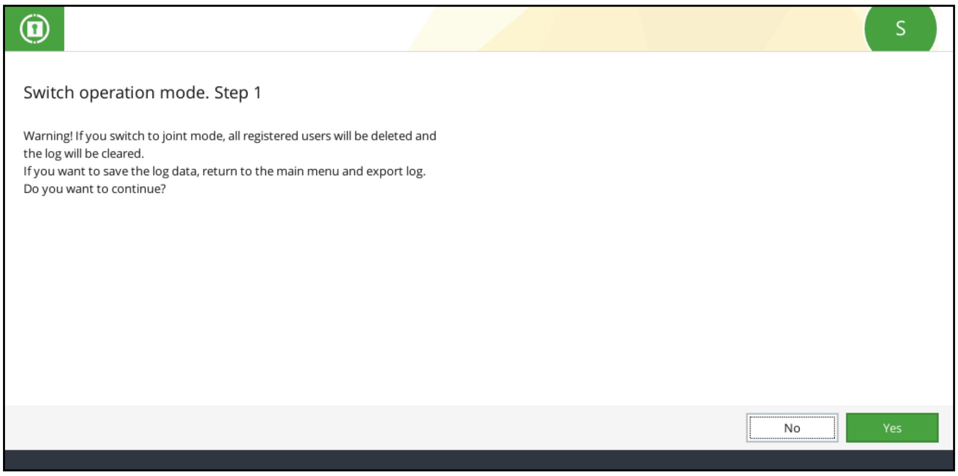
### To switch Sobol operation mode to joint:

**Attention!** When you switch Sobol operation mode to joint:

- the user list and the log are cleared;
- the privileges of the administrator are restricted (see p. 99).

1. In the **Change operation mode** dialog box, click **Change**.

   The confirmation request appears as in the figure below.



Switch operation mode. Step 1

Warning! If you switch to joint mode, all registered users will be deleted and the log will be cleared.
If you want to save the log data, return to the main menu and export log.
Do you want to continue?

2. Choose your further action:
   - select **No** to go back to the administrator menu and to export the log;
   - select **Yes** to continue.

   The window requesting your security token appears.
3. Present your security token.

**Note.** Select **Cancel** to cancel mode switching.

Service information stored in the card nonvolatile memory will be saved on the security token. After that, the success message appears.

4. Select **Next**.

   The message about the successful switching to the joint mode appears.

5. Select **OK**.

**To switch Sobol operation mode to standalone:**

**Attention!** When you switch Sobol operation mode to standalone:

- the user list and the log are cleared;
- the administrator is granted all privileges for configuration;

1. In the **Change operation mode** window, select **Change**.

   The following dialog box appears.

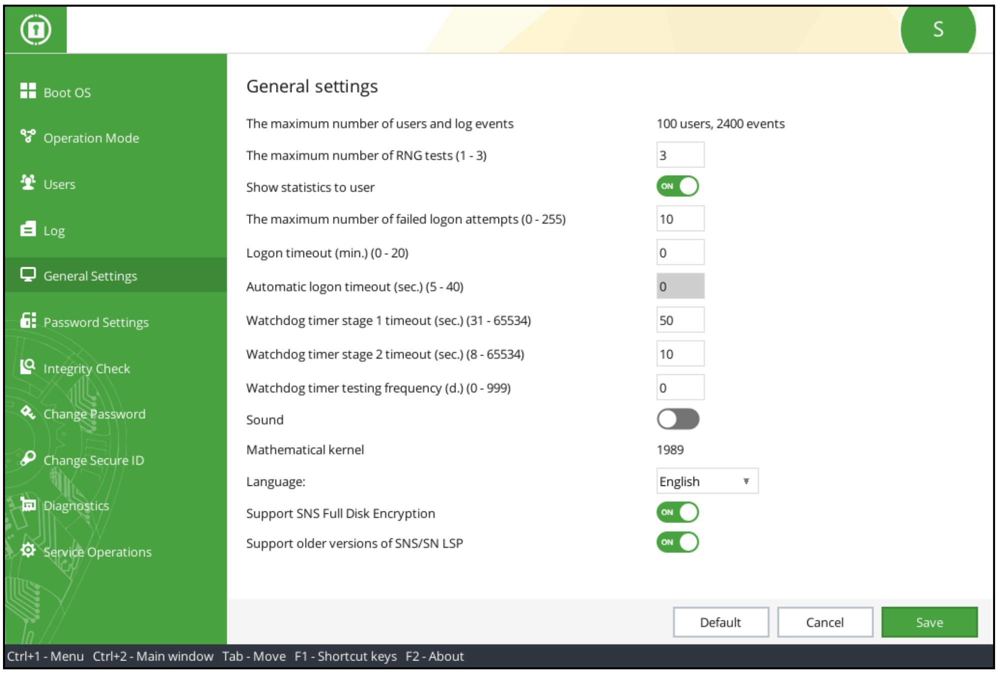
2. Select **Yes**.

   **Note.** To cancel changing the operation mode, select **No**.

## General settings

**Attention!** Some general settings are unavailable when Sobol is in joint mode (see p. 99).

In the administrator menu, select **General settings**. The window appears as follows.



General settings

The maximum number of users and log events 100 users, 2400 events

The maximum number of RNG tests (1 - 3) 3

Show statistics to user ON

The maximum number of failed logon attempts (0 - 255) 10

Logon timeout (min.) (0 - 20) 0

Automatic logon timeout (sec.) (5 - 40) 0

Watchdog timer stage 1 timeout (sec.) (31 - 65534) 50

Watchdog timer stage 2 timeout (sec.) (8 - 65534) 10

Watchdog timer testing frequency (d.) (0 - 999) 0

Sound

Mathematical kernel 1989

Language: English

Support SNS Full Disk Encryption ON

Support older versions of SNS/SN LSP ON

**To configure settings:**

1. Set the values of general settings according to Tab. 5 on p. **27**.
2. Select **Save** to save the changes.

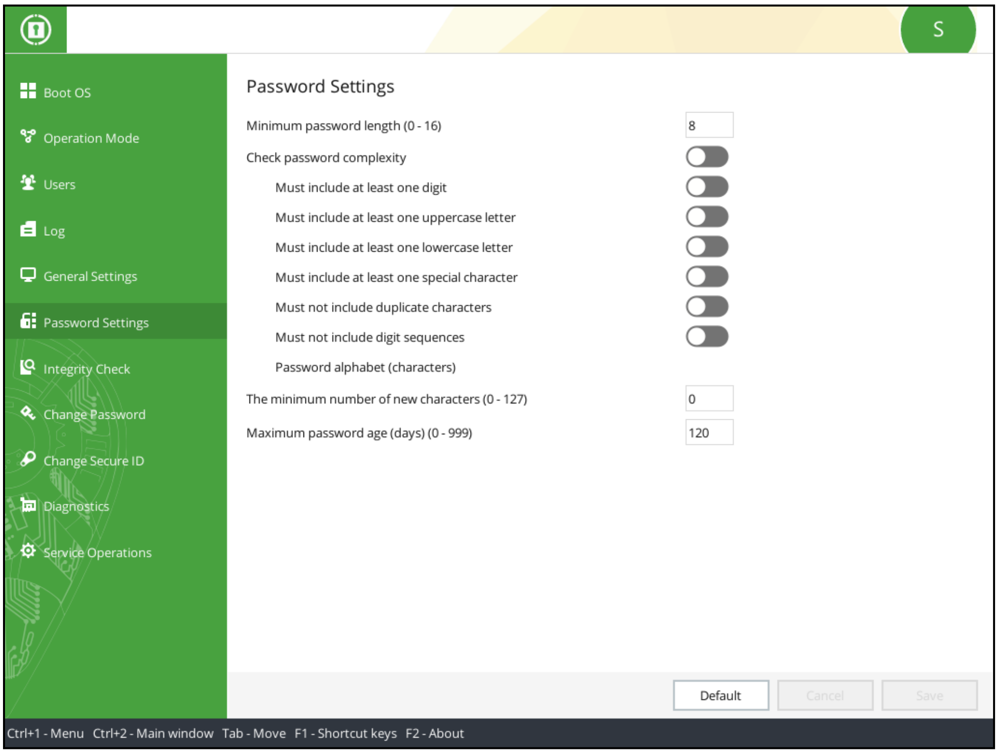
   To leave the previously set values, select **Cancel**.

   To reset the settings to the default values, select **Default**.

## Password settings

**Attention!** Password settings are unavailable when Sobol is in joint mode (see p. 99).

In the administrator menu, select **Password settings**. The window appears as follows.



Password Settings

Minimum password length (0 - 16) 8

Check password complexity ○

Must include at least one digit ○

Must include at least one uppercase letter ○

Must include at least one lowercase letter ○

Must include at least one special character ○

Must not include duplicate characters ○

Must not include digit sequences ○

Password alphabet (characters)

The minimum number of new characters (0 - 127) 0

Maximum password age (days) (0 - 999) 120

**To configure settings:**

1. Configure password settings according to Tab. 7 on p. **31**.
2. Select **Save** to save the changes.

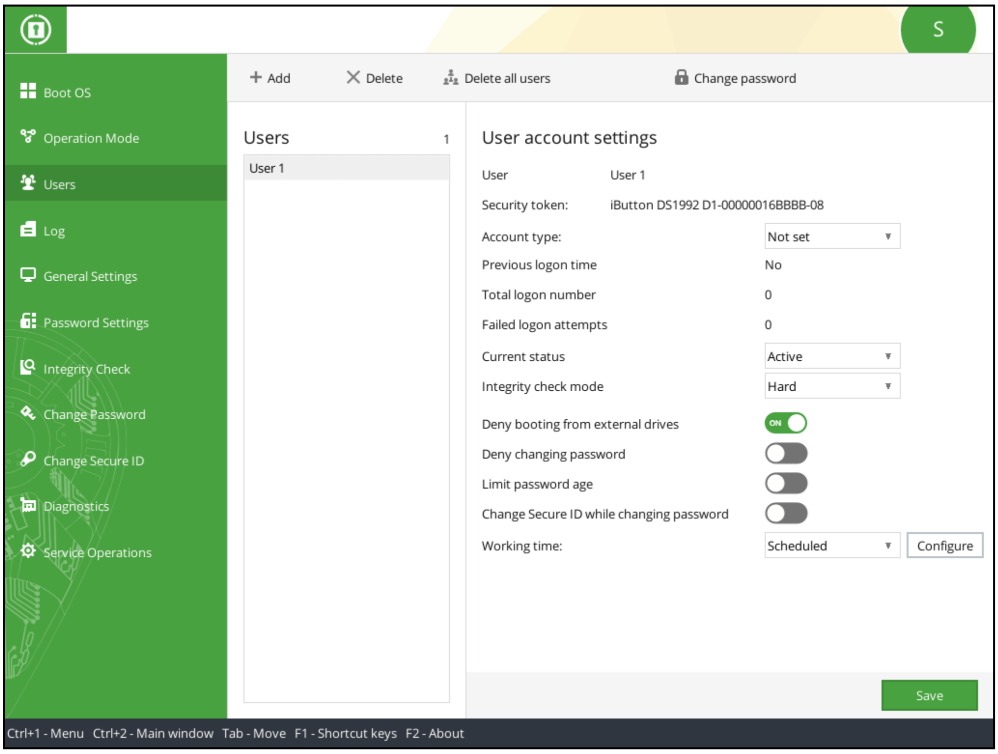
   To leave the previously set values, select **Cancel**.

   To reset the settings to the default values, select **Default**.

# Users

**Attention!** User management is unavailable when Sobol is in joint mode. In this mode, you can only view the user lists and account parameters (see p. 100).

In the administrator menu, select **Users**. The window appears as follows.



Users 1

User 1

User account settings

User User 1

Security token: iButton DS1992 D1-00000016BBBB-08

Account type: Not set

Previous logon time No

Total logon number 0

Failed logon attempts 0

Current status Active

Integrity check mode Hard

Deny booting from external drives ON

Deny changing password

Limit password age

Change Secure ID while changing password

Working time: Scheduled Configure

On the left of the display area, you can see the number and the list of users. The maximum account number is defined by the **The maximum number of users and log events** parameter (see Tab. 5 on p. **27**). You can set it during Sobol initialization. If no users are registered (after Sobol initialization, for example) the user list is empty.

On the right of the display area, you can see the parameters of a user account selected in the list. For more information about user account settings, see p. **58**.

On the top, you can see the user management panel with the following commands:

- **Add** (**<Ins>**) — register a new user (see below);
- **Delete** (**<Del>**) — delete a user account selected in the list (see p. **61**);
- **Delete all users** (**<Ctrl>**+**<Del>**) — delete all user accounts (see p. **61**);
- **Change password**(**<Ctrl>**+**<P>**) — change the password and the security token of a user selected in the list (see p. **61**).

**Note.** To see the full list of control keys, press <F1>.

## User registration

When registering a new user, he or she is assigned the following attributes:

- a name;
- a secure ID and a password;
- security token.

Registered user accounts are saved in the Sobol nonvolatile memory.

The initial user registration procedure is described on p. **55**. The user registration procedure is described on p. **54**.

During the **initial user registration**, service information is saved to the user's security token.

During the **user registration**, the service information stored on the security token after the initial registration is read without being modified. In this case, a user can log on to the system on different computers with Sobol using the same security token.

**Attention!** To repeat the user registration, select the mathematical kernel similar to the one that was selected during the initial registration (see p. 27).

**Note.** When you register a user on a number of computers with Sobol, do the following: on the first computer: perform the initial registration of a user, then register the user on the rest of them. If you do so, the user can log on to the system on all the computers using a single security token.

**Attention!** If the security token already contains service information about the user registration on other computer with Sobol, it will be deleted so that the user cannot use it to work on that computer.

## Initial user registration

### To perform initial user registration:

1. On the user management panel, (see  on p. **54**) select **Add** or press <Insert>.

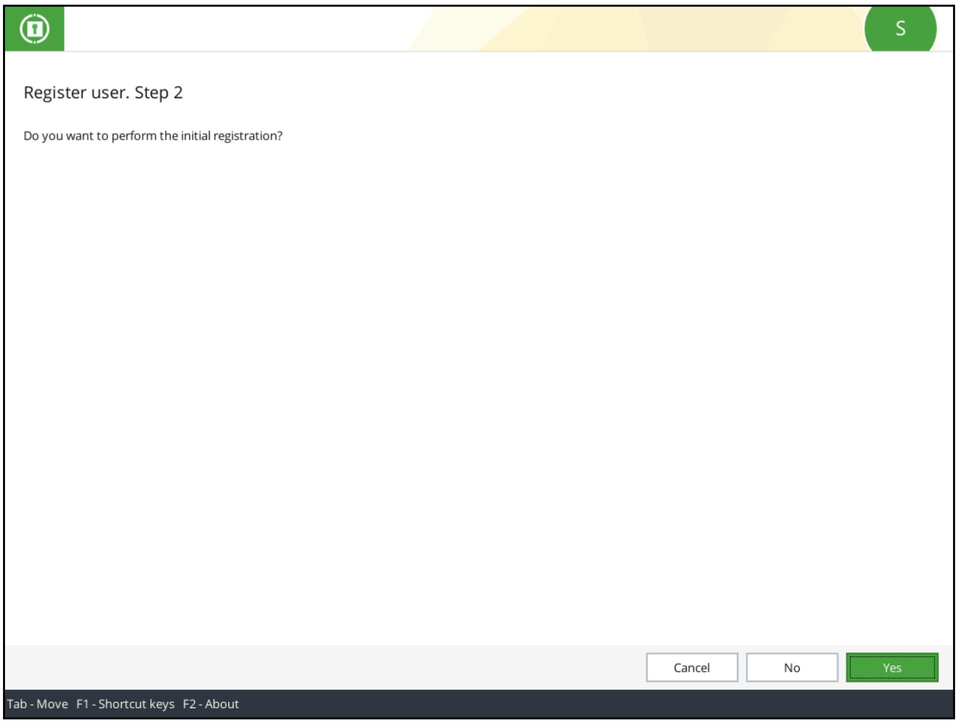
   **Note.**. If you receive a warning message about the exhaustion of the user list, delete one or more user accounts (seep. **61** ) and repeat the registration.

   The window prompting you to enter a new user name appears.

2. Type the name of the new user and click **Next**.

   **Note.**
   - The maximum user name length is 40 Latin, Cyrillic and special characters including the space.
   - To change the keyboard layout, press <F12>.
   - If an entered user name already exists in the system, A user with this name already exists warning appears. Press any key and type another name.

   The dialog box appears as follows.



Register user. Step 2

Do you want to perform the initial registration?

3. Click **Yes**.

   The dialog box prompting you to enter a user password appears.

4. Type a password or generate a random one by selecting **Generate** or pressing <F8>.

   To view the password, press <Alt>+<F8> or set **ON** for **Show password**.

> **Note.**
> When you type a password, take the following into account:
> - if the password you entered is shorter than required, after you click **Next**, the **Minimum password length is ... characters** warning appears. Click **OK** and type a password once again considering the restriction;
> - a password can contain only the following:
>   - 1234567890 — digits;
>   - abcdefghijklmnopqrstuvwxyz — lowercase Latin characters;
>   - ABCDEFGHIJKLMNOPQRSTUVWXYZ — uppercase Latin characters;
>   - _$!@#;%^:&?*)(-+=/|.,<>`~"\ — special characters;
> - if the password complexity check is enabled, a password must correspond to the complexity rules defined by the password settings (see p. 52).
>
> When you generate a random password, take the following into account:
> - if the password complexity check is enabled, a generated password corresponds to the complexity rules defined by the password settings (see p. 52);
> - if the complexity check is disabled, the generated password contains digits, lowercase or uppercase Latin characters;
> - the generated password can be edited.

5. Type the entered password again in the **Confirm new password** text box.

> **Attention!** After the registration procedure is complete, provide a user with the password.

6. Click **Next**.

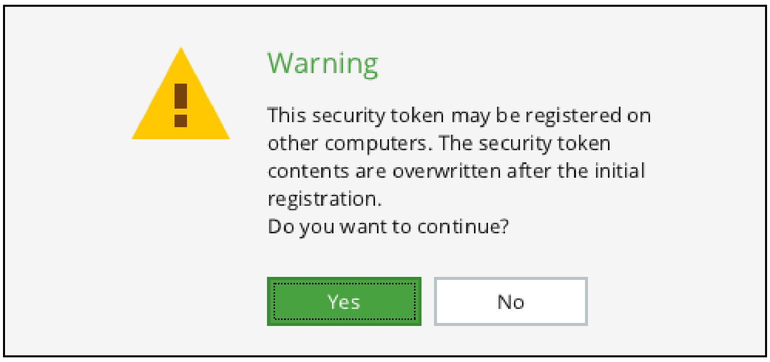
> **Note.** If a password entry error is detected, the respective message with the error description appears (see p. 93). Click **OK** and type the correct password.

After you type the password correctly, the window prompting you to present the security token appears.

7. Present the security token assigned to the user.

> **Note.**
> - If the security token is already presented (the iButton key touches the reader / the USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
> - If several security tokens are presented simultaneously, the one that Sobol finds first is read.
> - If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and click **OK**. Default PIN is provided on p. 8.

- If the security token is presented incorrectly, the security token prompt dialog box stays on the screen. Present the security token again.
- If the security token was registered previously on other computer and already contains service information, the following warning appears.



Warning

This security token may be registered on other computers. The security token contents are overwritten after the initial registration.
Do you want to continue?

If you are sure that nobody uses this security token, select **Yes** and present it again.

> **Attention!** When writing information to a security token, service information on it will be deleted permanently. In this case, the user to whom this security token belongs will not be able to use it to log on to the system.

If you want to use a different security token, click **No** and repeat step **7**.

- If the security token data structure is corrupted, the respective message appears. Sobol then suggests you format the security token.

> **Attention!** To fix the data structure corruption of the security token, format it.
> After you format the iButton key, all the data stored on it will be deleted permanently. After you format USB keys /smart cards, only information related to Sobol is lost.

To format the security token, select **Yes**. The security token is to be formatted and prepared for the further work.

To continue without formatting, select **No** and present another security token.

**Note.** You can format the security token later by using **Format security token** command (see p. 74).

After you assigned a security token to a user and saved the user account to the Sobol nonvolatile memory, you receive the **User has been successfully registered** message.

**8.** Click **Finish**.

The new user name appears in the users list. Configure the account parameters of this user (see p. 58).

**Attention!** To register a user, his or her presence is required, because his or her private password is prompted.

### User registration

**To register a user:**

**1.** Repeat steps **1–2** of the initial registration procedure.

**Note.** The name assigned to a user during the registration can differ from the one assigned during the initial registration on other computer.

**2.** In the appeared dialog, (see  on p. 54) click **No**.

The password is requested.

**3.** Ask the user to type his or her current password and then click **Next**.

The security token is requested.

**4.** Present the security token assigned to the user during the initial registration.

**Note.**

- If the security token is already presented (the iButton key touches the reader / the USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
- If several security tokens are presented simultaneously, the one that Sobol finds first is read.
- If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and click **OK**. Default PIN is provided on p. 8.

- If the security token is presented incorrectly, the security token prompt dialog box stays on the screen. Present the security token again.
- If the entered password does not match the presented security token (the password is wrong or the security token does not belong to the user), you receive the **Invalid password or security token** message.

  Click **OK** and repeat steps **2**–**4**.
- If an entered password matches a presented security token, service information is read and then saved to the Sobol nonvolatile memory.

After the information is saved, a success message appears. The new user name appears in the users list.

**5.** Configure the registered user account settings (see below).

## Configure user accounts

User account settings define the status of the account as well as allow you to choose the operation modes of the security mechanisms for each user.

**To configure settings:**

1. In the user list, select the user account you are to configure (see  on p. **54**).
2. In **User account settings**, configure the required parameters using the table below.
3. Select **Save** to save the changes.

User account settings are provided in the following folder:

| |
|---|
| **User name** |
| Displays the name assigned to the user during registration. |
| **Account type** |
| Displays the account type of a user. Takes the following values:<br>• Not set;<br>• Internal;<br>• External;<br>• System;<br>• Guest;<br>• Temporary;<br>The default value — not set. |
| **Security token** |
| Displays the type and number of a user's security token. |
| **Last logon time** |
| Displays the time (HH:MM) and the date (DD/MM/YYYY)of the last user logon to the system. |
| **Total logon number** |
| Displays the total number of user logons to the system since registration. |
| **Failed logon attempts** |
| Displays the number of failed logon attempts.<br>• 0 if the number of failed logon attempts is less than the Failed logon attempts limit general parameter value (see Tab. 5 on p. **27**) and if a user ended a session by successfully logging on to the system;<br>• greater than 0, if the number of failed logon attempts reached the Failed logon attempts limit general parameter value (see Tab. 5 on p. **27**). In this case, a user account is locked automatically. To unlock a user account, set **Failed logon attempts** to 0 and **Current status** to Active |
| **Current status** |
| Displays the account status which defines the user logon. Takes the following values:<br>• Blocked — user logon is prohibited;<br>• Active — user logon is allowed;<br>If despite the user logon prohibition a logon was attempted, the Logon is prohibited by administrator warning appears and then the computer is locked |
| **Integrity check mode** |
| Defines an integrity check mode for a particular user. The parameter takes the following values:<br>• Hard — if the integrity of monitored objects is violated, a user logon is prohibited, the computer is locked and the respective error is saved to the log;<br>• Soft — if the integrity of monitored objects is violated, a user logon is allowed, the computer is not locked, but the respective error is saved to the log |

**Deny booting from external drives**

Use this parameter to deny booting from external drives (floppy disk, DVD/CD-ROM, ZIP devices, USB devices, etc) for users. The parameter takes the following values:

- ON — booting from external devices is prohibited;
- OFF — booting from external devices is allowed

**Deny changing password**

Use this parameter to deny password changes for users. The parameter takes the following values:

- ON — password change is prohibited;
- OFF — password change is allowed.

After you enable this parameter, Change Secure ID while changing password is unavailable.

**Note.** If password change is prohibited for a user with an expired password, do the following to change his or her password:

- log on to the system as an administrator, set **Deny changing password** for the user to **OFF** and then reboot the computer;
- let the user log on to the system and change the password;
- reboot the computer;
- log on to the system as an administrator, set **Deny changing password** for the user to **ON** and then reboot the computer.

**Limit password age**

Use this parameter to limit the password age for users. The parameter takes the following values:

- ON — the password age is limited;
- OFF — the password age is unlimited.

If the password age is limited, the current password becomes invalid once the maximum password age is reached. When logging on to the system, the user will be asked to change his/her password.

If the **Change Secure ID** while changing password is enabled for the user, the **Secure ID age** is limited as well.

To enable the parameter, the respective user must be present. Ask him or her to enter the password and present the security token. If the password is correct, the parameter is set to ON

**Change Secure ID while changing password**

Use this parameter to enable changing a Secure ID along with changing a password. The parameter takes the following values:

- ON — a Secure ID must be changed when changing a password;
- OFF — it is not necessary to change a Secure ID when changing a password

**Working time**

Use this parameter to set time intervals during which a user can access the computer.

Takes the following values:

- Unrestricted — a user is allowed to work anytime;
- Scheduled — a user is allowed to work according to the given schedule.

The default value is Unrestricted.

The instruction on how to configure the working time is shown below.

**Note.** If the parameter is set to Unrestricted after the schedule is created, the schedule will not be reset. To return to the created schedule, set the **Working time** value to Scheduled.

## Configure user schedule

Sobol makes it possible to configure the user work schedule according to their working hours. If need be, you can set the time and date when a user is allowed to log on to the system or limit access temporarily.

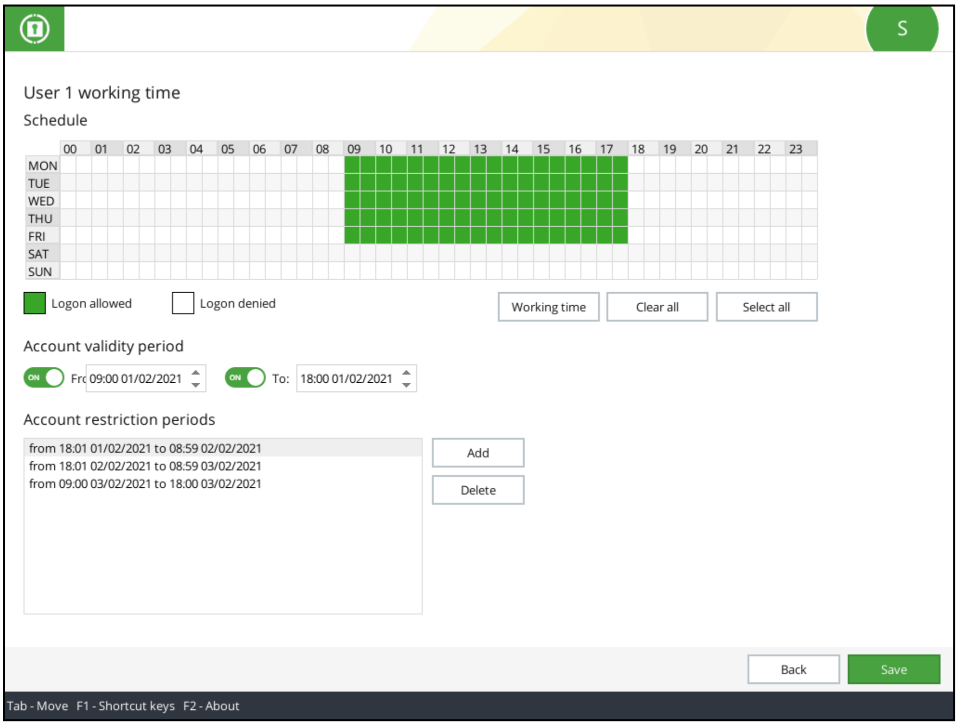
**To configure the user schedule:**

1. In **Users** (see  on p. **54**), select the user for whom you want to configure the schedule.
2. In **User account settings**, select the parameter **Working time** and assign Scheduled to it.

   **Note.** If the value Scheduled is selected, but the schedule is not configured, a user can log on to the system anytime.

3. Click **Configure**.

   A dialog box with user schedule parameters appears.



User 1 working time

Schedule

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| MON | | | | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | |
| TUE | | | | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | |
| WED | | | | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | |
| THU | | | | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | |
| FRI | | | | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | |
| SAT | | | | | | | | | | | | | | | | | | | | | | | | |
| SUN | | | | | | | | | | | | | | | | | | | | | | | | |

🟩 Logon allowed □ Logon denied

Account validity period

ON Frc 09:00 01/02/2021 ON To: 18:00 01/02/2021

Account restriction periods

from 18:01 01/02/2021 to 08:59 02/02/2021
from 18:01 02/02/2021 to 08:59 03/02/2021
from 09:00 03/02/2021 to 18:00 03/02/2021

**4.** Configure the **Schedule** parameter using the following:

- **Working time** — configure the standard work schedule (from 9 a.m. to 5 p.m., Monday through Friday);
- **Clear All** — delete the whole schedule;
- **Select All** — select the whole schedule.

**Note.** The cell color indicators:

- green — a user is allowed to log on at the given time.
- white — a user is not allowed to log on at the given time.

If need be, you can configure the schedule manually by selecting the respective time and weekday in the schedule configuration table.

To configure the schedule, use the left mouse button click or the following keys:

- <UP/DOWN> and <LEFT/RIGHT> arrows — navigate the schedule;
- <SPACE> — change the color of a cell;
- <SHIFT>+<UP/DOWN> and <LEFT/RIGHT> arrows — select a row and/or a column.

**5.** In the field **Account validity period**, switch the toggle to ON in the area:

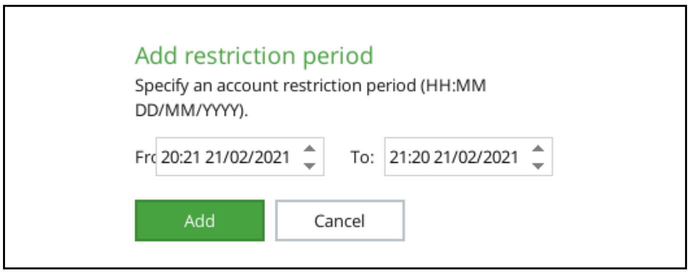
- from: HH:MM DD/MM/YYYY — a user is allowed to log on to the system from this time;
- to: HH:MM DD/MM/YYYY — a user is allowed to log on to the system until this time;

**Note.** If need be, configure only the start time or the finish time using the <UP/DOWN> arrows.

**6.** To configure the parameter **Account restriction periods**:

- Click **Add**.

  A dialog box appears.



Add restriction period

Specify an account restriction period (HH:MM DD/MM/YYYY).

Frc 20:21 21/02/2021 To: 21:20 21/02/2021

- Specify the account restriction period.
- Click **Add**.

The value is displayed in the parameter dialog box.

**Note.** To delete the account restriction period, click **Delete.**

7. Select **Save** to save the changes.

   To return to the user account settings dialog box, click **Back**.

## Delete a user account

**To delete a user account:**

1. In the users list (see  on p. **54**), select the required user;
2. On the users management panel, select **Delete** or press <**Delete**>.

   The respective dialog box appears.
3. Select **Yes**.

The selected user account is deleted from the Sobol nonvolatile memory. The user name will be deleted from the list.

## Delete all user accounts

**To delete all user accounts:**

1. On the users management panel (see  on p. **54**), select **Delete all users** or press the key combination <**Ctrl**>+<**Delete**>.

   The respective dialog box appears.
2. Select **Yes**.

All user accounts are deleted from the Sobol nonvolatile memory. The users list will be empty.

## Change user Secure ID and password

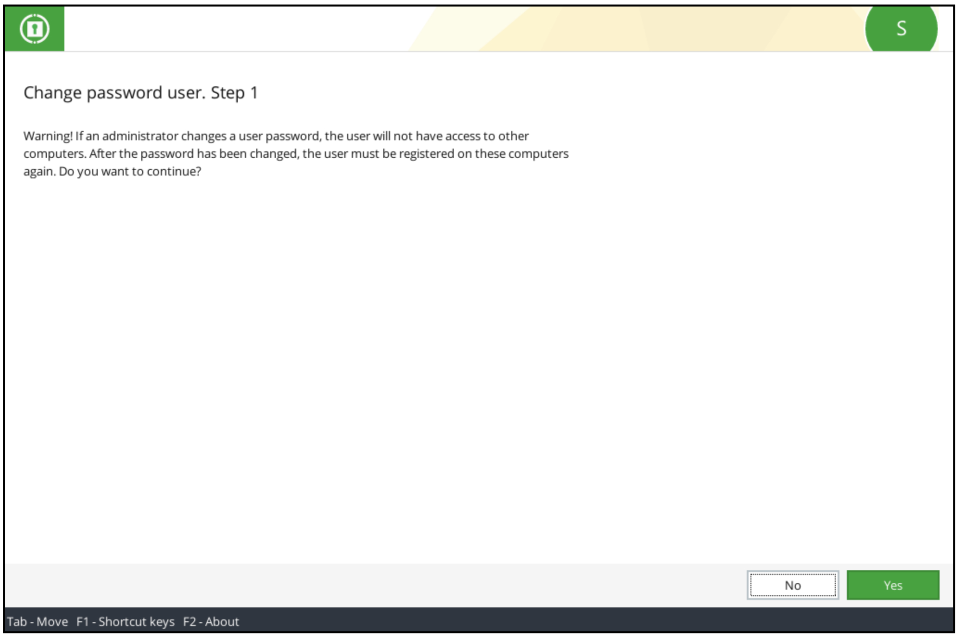
Before changing the Secure ID and the password of a user, take the following into account:

1. You can do this only if a password was compromised, that is for the **emergency** password change. Otherwise, a user changes his or her password. (see document  [**2**]).
2. The Secure ID and the password of a user are changed correctly only if the user is registered with the security token on a single computer with Sobol.
3. If the user is registered on more than one computer using this security token, he or she will lose access to all computers except the one used to change the Secure ID and the password. In this case, register the user on other computers.

**To change the Secure ID and the password of a user:**

1. In the user list, (see  on p. **54**) select the required user.
2. At the top of the window, select **Change password** or press <**Ctrl**>+<**P**>.

The window appears as follows.



Change password user. Step 1

Warning! If an administrator changes a user password, the user will not have access to other computers. After the password has been changed, the user must be registered on these computers again. Do you want to continue?

3. If you are sure that you need to change the Secure ID and the password, select **Yes**.

   The dialog prompting you to enter a new password appears.

   **Note.** The current user's password is not requested in this case.

4. In the respective text box, type the new user password or generate a random one by selecting **Generate** or pressing **<F8>**.

   To view the entered password, press <**Alt**>+<**F8**> or set **Show password** to **ON**.

   **Note.**

   When you type a password, take the following into account:

   - if the password you entered is shorter than required, after you select **Next**, the **Minimum password length is ... characters** warning appears. Select **OK** and type a password once again considering the restriction;
   - a password can contain only the following:
     - 1234567890 — digits;
     - abcdefghijklmnopqrstuvwxyz — lowercase Latin characters;
     - ABCDEFGHIJKLMNOPQRSTUVWXYZ — uppercase Latin characters;
     - _$!@#;%^:&?*)(-+=/|.,<>`~"\ — special characters;
   - if the password complexity check is enabled, a password must correspond to the complexity rules defined by the Sobol password settings (see p. 52).

   When you generate a random password, take the following into account:

   - if the password complexity check is enabled, a generated password corresponds to the complexity rules defined by the Sobol password settings (see p. 52);
   - if the complexity check is disabled, the generated password contains digits, lowercase or uppercase Latin characters;
   - a generated password can be edited.

5. Type the entered password again in the **Confirm new password** text box.

6. Select **Next**.

   **Note.** If a password entry error is detected, you receive the respective message with the error description (see p. 93). Select **OK** and type the correct password.

   After you type the password correctly, the window prompting you to present the security token appears.

7. Present the administrator security token.

   **Note.**

   - If the securyty token is already presented (the iButton key touches the reader/USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
   - If several security tokens are presented simultaneously, the one that Sobol finds first is read.
   - If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and select **OK**. Default PIN is provided on p. 7.

   - If the security token is presented incorrectly, the security token prompt dialog box appears.

- If the presented security token does not belong to the user, you receive the **Invalid password or security token** message.

When the security token is successfully read, you receive the **Password has been successfully changed** message.

8. Select **Finish**.

## Configure automatic OS booting

Sobol provides automatic OS booting upon the security token presentation. It can be useful on platforms without data input devices (a keyboard, a mouse).

**Note.** An input device (a keyboard or a mouse) are required if integrity is violated.

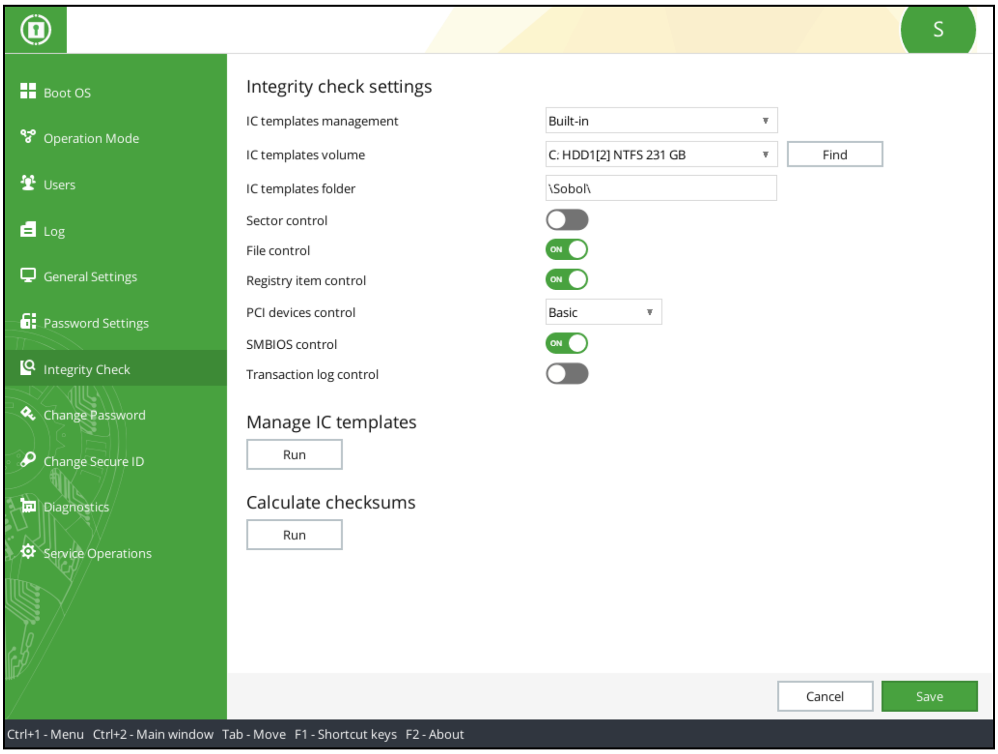
**To configure the automatic OS booting:**

1. Set the general parameter value (see p. **52**):
   - **Show statistics to a user — OFF**.
2. Set password parameters values (see p. **52**):
   - **Minimum password length— 0**;
   - **Check password complexity — OFF**.
3. Configure the account parameters of a user who needs the automatic OS booting (see p. **58**):
   - set an empty password for this user;
   - **Deny changing password — ON**;
   - **Limit password age — OFF**.
4. Set the log parameter values (see p. **71**):
   - **Overwrite events — ON**;
   - **Time period for audit — 0**.

## Integrity check

**Attention!** In joint mode, the Sobol administrator can only select a volume or a folder with integrity check templates and calculate checksums. Other integrity check parameters are unavailable (see p. **100**).

After you select **Integrity check**, the window looks as follows.



Integrity check settings

IC templates management: Built-in

IC templates volume: C: HDD1[2] NTFS 231 GB

IC templates folder: \Sobol\

Sector control: off

File control: ON

Registry item control: ON

PCI devices control: Basic

SMBIOS control: ON

Transaction log control: off

Manage IC templates

Calculate checksums

Run
Cancel
Save
Ctrl+1 - Menu Ctrl+2 - Main window Tab - Move F1 - Shortcut keys F2 - About

**To set the up the integrity check mechanism and calculate checksums:**

Set integrity check parameter values using the instruction on integrity check setup during Sobol initialization (see p. **37**, steps **1-6**).

If integrity check templates are managed with the Sobol software, you can configure integrity check templates. To do so, in **IC template management**, select **Run**.

For instructions on how to work with Sobol IC template management software, see Chapter 5 (see p. **79**).

## Change administrator Secure ID

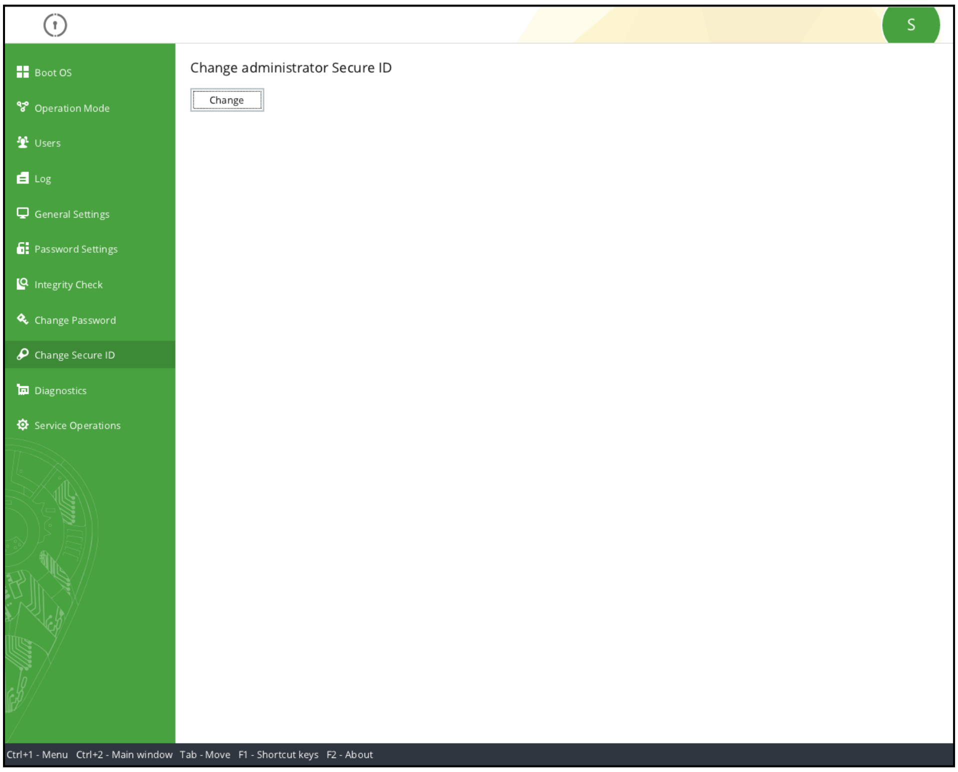
**Attention!** You cannot change the Secure ID of the administrator while Sobol is in joint mode. For more information about Sobol configuration, see p. 99.

When changing the Secure ID of the administrator, the data on his or her security token is modified.

**Attention!** The maximum password age parameter is not set for an administrator. He or she must change the password and the Secure ID according to the organization security policy.

**To change an administrator security token:**

1. In the administrator menu, select **Change Secure ID**.



Change administrator Secure ID

2. Select **Change**.

   The window prompting you to enter the administrator password appears.

3. Type the current administrator password and select **Next**.

   The windows prompting the security token appears.

   **Note.** You can refuse to change the Secure ID before presenting the security token. To do so, select **Cancel**.

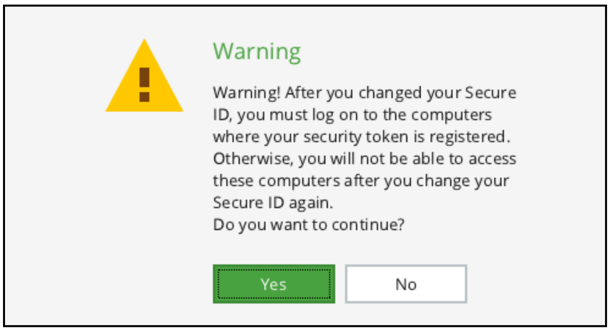
4. Present the administrator security token.

   **Note.**
   - If the securyty token is already presented (the iButton key touches the reader/USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
   - If several security tokens are presented simultaneously, the one that Sobol finds first is read.
   - If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and select **OK**. Default PIN is provided on p. 7.

   If you presented your security token correctly, the old password you entered is compared to the data stored on the security token:

- If your old password does not match the presented security token, you receive the **Invalid password or security token** message.

  Select **OK** and then present the administrator security token or Select **Cancel** and try to change your Secure ID again.
- If the entered password matches the security token:
  - when you change your Secure ID for the first time, the new Secure ID is saved to your security token. The old Secure ID is saved there as well. After changing the Secure ID, an administrator still has access to other computers with Sobol, on which he or she is registered as an administrator;
  - when you change your Secure ID next time, the following warning appears.



Warning

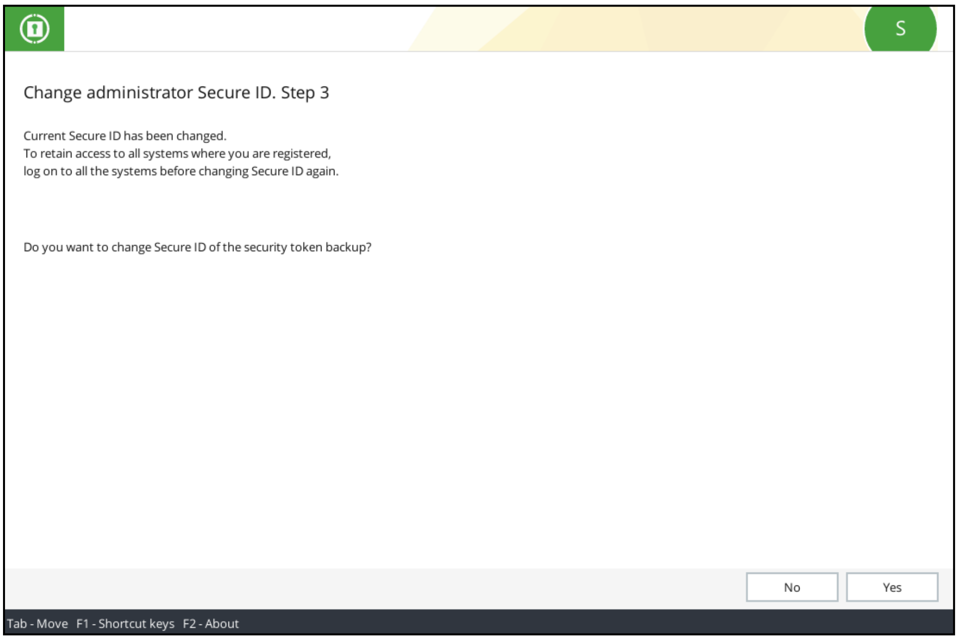
Warning! After you changed your Secure ID, you must log on to the computers where your security token is registered. Otherwise, you will not be able to access these computers after you change your Secure ID again.
Do you want to continue?

**Note.** An administrator security token stores a current Secure ID and a previous one. When you change your Secure ID, a new one is saved to the security token and a previous one is deleted from it. This way, you have access to other computers with Sobol, on which you are registered as an administrator. If you did not log on to any of these computers after having changed your Secure ID for the last time, you lose access to them, because the previous Secure ID used to access those computers is deleted from your security token. In this case, we recommend that you cancel the procedure of changing the Secure ID, log on to the required computers and then change your Secure ID.

To cancel the procedure of changing your Secure ID, select **No**.

To save the new Secure ID to your security token, select **Yes** and present the security token.

After the data saved to the security token, the window appears as in the figure below.



Change administrator Secure ID. Step 3

Current Secure ID has been changed.
To retain access to all systems where you are registered,
log on to all the systems before changing Secure ID again.

Do you want to change Secure ID of the security token backup?

**Attention!** After you change your Secure ID, be sure to log on to all the computers with Sobol on which you are registered as an administrator. Unless you do so, you will lose access to those computers.

**5.** If no backups were created, select **No**. The procedure of changing the Secure ID is completed.

If there are backups, select **Yes**. The window prompting your security token appears.

**Note.** We recommend changing your Secure ID on all your security token backups created during Sobol initialization. This allows you to use them.

6. Present an administrator security token backup.

**Note.**
- If the security token is already presented (the iButton key touches the reader / the USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
- If several security tokens are presented simultaneously, the one that Sobol finds first is read.
- If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and select **OK**. Default PIN is provided on p. 7.

- If you presented the security token incorrectly, the window prompting a security token remains. Present the security token again.
- If the presented security token is not a backup one, you receive the **Invalid password or security token** message.

  Select **OK** and present an administrator security token backup again.

If you presented the security token correctly, a new administrator Secure ID is saved to it. After, the window prompting you to save a new Secure ID to another security token backup.

7. Go to step **5**.

## Change administrator password

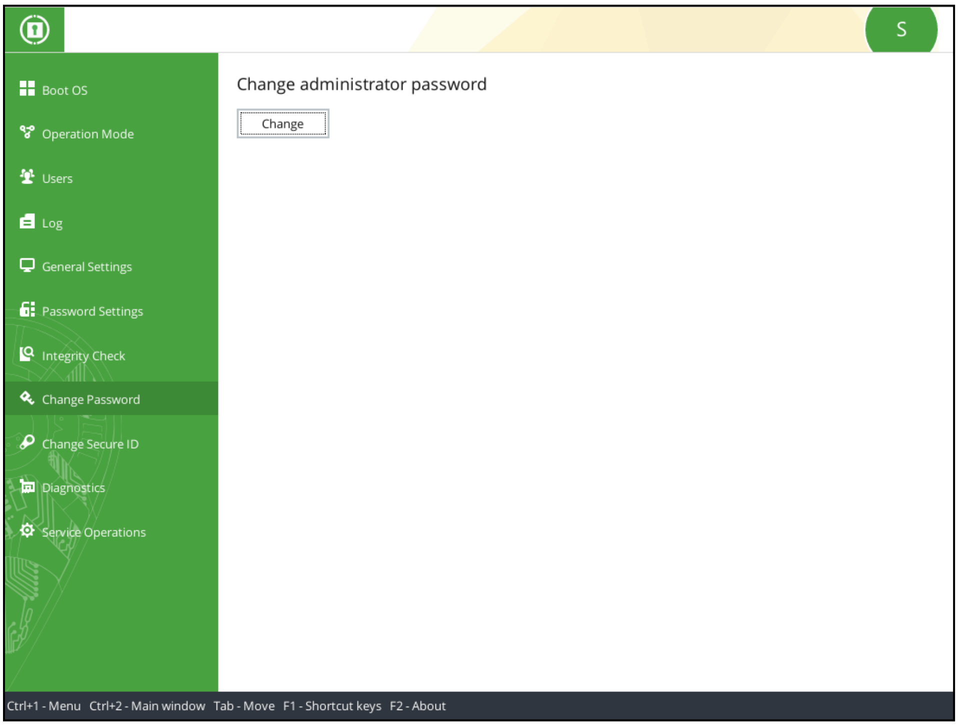
**Attention!** You cannot change the password of the administrator while Sobol is in joint mode. For more information about Sobol configuration, see p. 99.

When changing the password of the administrator, the data on his or her security token is modified.

**Attention!** The maximum password age parameter is not set for an administrator. He or she must change the password and the Secure ID according to the organization security policy.

**To change an administrator password:**

1. In the administrator menu, select **Change Password**.



2. Select **Change**.

   The window prompting the current administrator password appears.

**Note.** To cancel the operation, select **Cancel** before presenting the security token.

3. Enter the current administrator password and select **Next**.

   The window prompting a new password appears.

4. In the respective text box, type the new administrator password or generate a random one by selecting **Generate** or pressing **<F8>**.

   To view the entered password, press <**Alt**>+<**F8**> or set **Show password** to **ON**.

   **Note.**
   When you type a password, take the following into account:
   - if the password you entered is shorter than required, after you select **Next**, the **Minimum password length is ... characters** warning appears. Select **OK** and type a password once again considering the restriction;
   - a password can contain only the following:
     - 1234567890 — digits;
     - abcdefghijklmnopqrstuvwxyz — lowercase Latin characters;
     - ABCDEFGHIJKLMNOPQRSTUVWXYZ — uppercase Latin characters;
     - _$!@#;%^:&?*)(-+=/|.,<>`~"\ — special characters;
   - if the password complexity check is enabled, a password must correspond to the complexity rules defined by the Sobol password settings (see p. 52).

   When you generate a random password, take the following into account:
   - if the password complexity check is enabled, a generated password corresponds to the complexity rules defined by the Sobol password settings (see p. 52);
   - if the complexity check is disabled, the generated password contains digits, lowercase or uppercase Latin characters;
   - a generated password can be edited.

5. Type the entered password again in the **Confirm new password** text box.

6. Select **Next**.

   **Note.** If a password entry error is detected, you receive the respective message with the error description (see p. 93). Select **OK** and type the correct password.

   After you type the password correctly, the window prompting you to present the security token appears.

   **Note.**You can refuse to change the password before presenting the security token. To do so, select **Cancel**.

7. Present the administrator security token.

   **Note.**
   - If the securyty token is already presented (the iButton key touches the reader/USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
   - If several security tokens are presented simultaneously, the one that Sobol finds first is read.
   - If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and select **OK**. Default PIN is provided on p. 7.

   If you presented your security token correctly, the old password you entered is compared to the data stored on the security token:

   - If your old password does not match the presented security token, you receive the **Invalid password or security token** message.

     Select **OK** and then present the administrator security token or select **Cancel** and try to change your password again.
   - If your old password matches the presented security token, the respective service information is saved to the security token.

   After the service information is saved, the **Do you want to set the new password for the administrator security token backup?** dialog box appears.

8. If no backups were created, select **No**. The procedure of changing the password is completed.

   If there are backups, select **Yes**. The window prompting your security token appears.

   **Note.** We recommend setting a new password for all administrator security token backups created during the Sobol initialization. By doing so, you can use the backups.

9. Present the backup administrator security token.

   **Note.**
   - If the securyty token is already presented (the iButton key touches the reader/USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
   - If several security tokens are presented simultaneously, the one that Sobol finds first is read.
   - If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and select **OK**. Default PIN is provided on p. 7.

   - If you presented the security token incorrectly, the window prompting a security token remains. Present the security token again.

- If the presented security token is not a backup one, you receive the **Invalid password or security token** message.

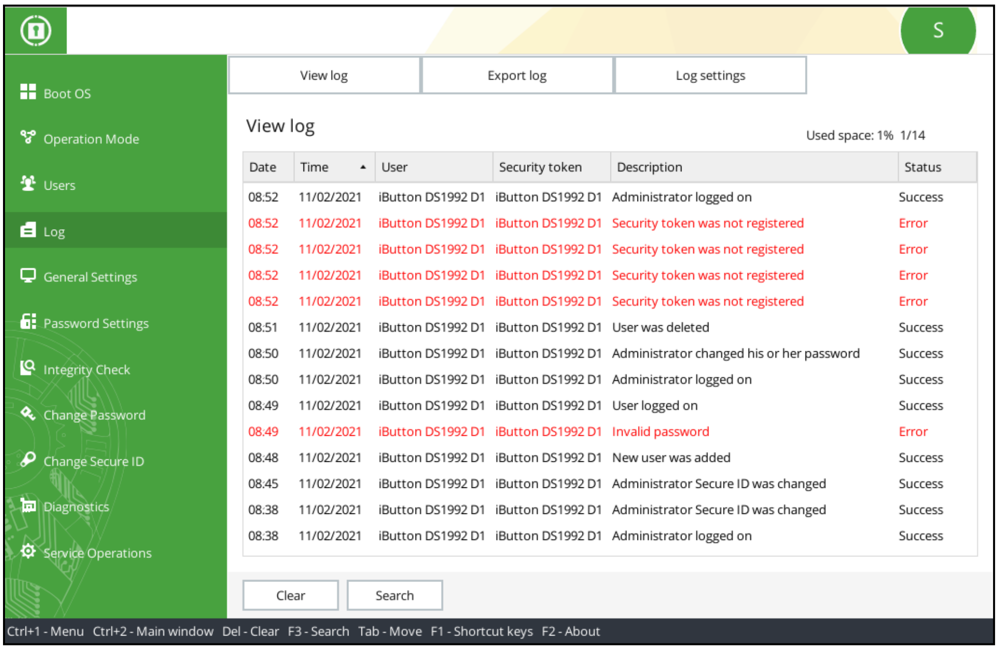
  Select **OK** and present an administrator security token backup.

If you presented your security token correctly, the respective service information is saved to the security token. After, the dialog box for setting a new password for another administrator security token backup appears.

**10.** Go to step **8**.

# Log

In the administrator menu, select **Log settings**. The window appears as follows.



View log

Used space: 1%  1/14

| Date | Time | User | Security token | Description | Status |
|---|---|---|---|---|---|
| 08:52 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Administrator logged on | Success |
| 08:52 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Security token was not registered | Error |
| 08:52 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Security token was not registered | Error |
| 08:52 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Security token was not registered | Error |
| 08:52 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Security token was not registered | Error |
| 08:51 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | User was deleted | Success |
| 08:50 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Administrator changed his or her password | Success |
| 08:50 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Administrator logged on | Success |
| 08:49 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | User logged on | Success |
| 08:49 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Invalid password | Error |
| 08:48 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | New user was added | Success |
| 08:45 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Administrator Secure ID was changed | Success |
| 08:38 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Administrator Secure ID was changed | Success |
| 08:38 | 11/02/2021 | iButton DS1992 D1 | iButton DS1992 D1 | Administrator logged on | Success |

At the top of the **Log** window, there are the following tabs:

- **View log** — view the log (see below), search for records according to set parameters (see p. **69**), clear the log (see p. **70**);
- **Export log** — export the log into a file (see p. **70**);
- **Log settings** — configure the log (see p. **71**).

## View the log

**To view the log:**

**1.** In the **Log** window, select the **View log** tab (see  on p. **68**).

In the main window area, the log is displayed.

Sobol event records are provided in a table and are highlighted in the following colors:

- red — critical events;
- black — information messages and events related to the actions of Sobol users and the administrator, implemented successfully.

Every row of the events table contains data about a single event. Events are sorted in the order from the last registered event (at the top of the table ) to the first one (at the bottom of the table ).

The events table elements and their descriptions are provided in the table below.

| Column name | Description |
|---|---|
| **Time** | The time of the event registration (HH:MM) |
| **Date** | The date of the event registration (DD/MM/YY) |
| **Description** | The description (type) of an event |

| Column name | Description |
|---|---|
| **User** | The name of a user whose actions resulted in the event registration The type of the presented security token of an administrator and users not registered in the system (including those deleted from the Sobol user list) is recorded |
| **Security token** | The security token ID of a user whose actions resulted in the event registration |
| **Status** | A result of the event. If the event was a success, it is assigned the **Success** status, otherwise - **Error** |

2. Read the log content.

   To move lines up and down, press <↑> and <↓>, to page, press <**PgUp**> and <**PgDn**>, to scroll records, use the scroll bar.

   For the list of Sobol logged events, see p. **97**.

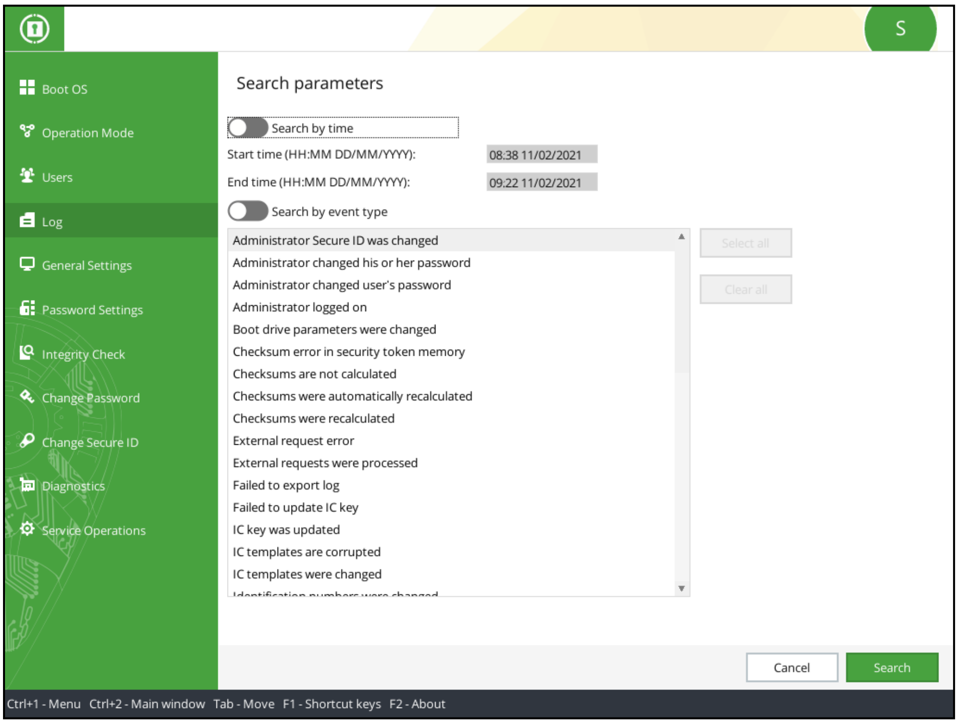
## Search records

In the Sobol log, you can search for event records by their creation time and type. You can use both these parameters simultaneously.

**To search for records by time:**

1. In the **Log** window, select the **View log** tab (see  on p. **68**). Select **Search** or press <**F3**>.

   The following window appears.



Search parameters

Search by time

Start time (HH:MM DD/MM/YYYY): 08:38 11/02/2021

End time (HH:MM DD/MM/YYYY): 09:22 11/02/2021

Search by event type

Administrator Secure ID was changed
Administrator changed his or her password
Administrator changed user's password
Administrator logged on
Boot drive parameters were changed
Checksum error in security token memory
Checksums are not calculated
Checksums were automatically recalculated
Checksums were recalculated
External request error
External requests were processed
Failed to export log
Failed to update IC key
IC key was updated
IC templates are corrupted
IC templates were changed
Identification numbers were changed

2. Turn on the **Search by time** toggle.

   The **Event start** and **Event end** parameters become available.

3. In the **Event start**, specify the lower limit of the event time interval in the following format: hours:minutes day/month/year.

4. In the **Event start**, specify the upper limit of the event time interval in the following format: hours:minutes day/month/year.

5. Select **Select events**.

   Records matching the search appear.

**To search for records by type:**

1. In the **Log** window, select the **View log** tab (see  on p. **68**). Select **Search** or press <**F3**>.

   The **Search settings** window appears (see  on p. **69**).

2. Turn on the **Search by type** toggle.

3. Select all required types and then select **Select events**.

   **Note.** To select all types, select **Select all**. To cancel the selection, select **Clear all**.

   Records matching the search appear.

## Clear the log

**Attention!**

- Before you clear the log, read the content.
- You cannot clear the log when Sobol is in joint mode (see p. 100).

**To clear the log:**

1. In the **Log** window, select the **View log** tab (see  on p. **68**). Select **Clear** or press <**Delete**>.

   The respective window appears.
2. Select **Yes**.

   All log records are deleted from the log. The following new record appears in the log — **Delete log**.

## Export the log

You can export the Sobol log into a file created in advance. You can create a file to export the log in two ways:

- using the command line (see below);
- using Sobol software (see document [**1**]).

**To create a file using the command line:**

1. Run the command line in Windows OS or the terminal in Linux OS.
2. Go to the folder where you want to create the file.

   **Note.** The file is created in the Sobol default folder:
   - in Windows OS— in **\Sobol**;
   - in Linux OS — in **/sobol** or **/boot/sobol.**

   If the standard folder is not found, create it in the system drive.
3. Run the following command:
   - for Windows OS:

     ```
     fsutil file createNew log.csv 360000
     ```
   - for Linux OS:

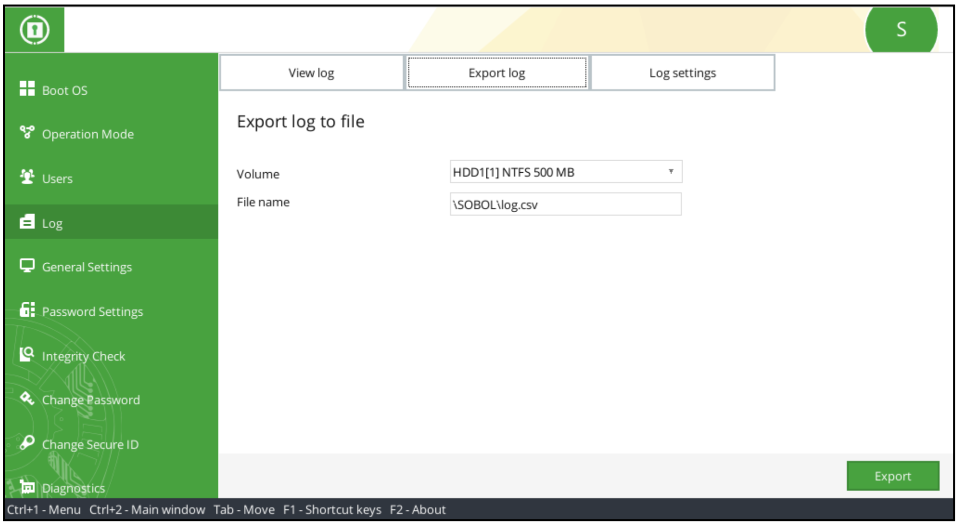
     ```
     dd if=/dev/zero of=log.csv count=1 bs=360000
     ```

   **Note.**
   - Export the log into a file with the csv. extension. For example, **log.csv**.
   - The file size is 360 times the number of records. The maximum number of records is defined by the **The maximum number of users and log events** parameter (see p. 27). You can set the following values, when typing the command:
     - 800 events — 288000;
     - 1600 events — 576000;
     - 2400 events — 864000;
     - 3200 events — 1152000.
   - In Linux OS, you can set file size differently:
     - 1000 events— 288K;
     - 1600 events — 576K;
     - 2400 events— 864K;
     - 3200 events— 1152K.

**To export the log into a file:**

1. In the **Log** window, select the **Export log** tab (see  on p. **68**).

   The following window appears.



Export log to file

Volume: HDD1[1] NTFS 500 MB

File name: \SOBOL\log.csv

2. Specify the volume (disk, partition), the name of the file to export the log.
3. Select **Export**.

   After the log is exported, the respective success message appears.

**Note.** You can view the exported log via a text editor or a spreadsheet. Data columns are separated by tabs, data is enclosed in double quotes. The contents of the log can be analyzed using standard text editor or spreadsheet tools, for example, to identify possible unauthorized access attempts.

If any errors occur, the respective window appears (see p. **94**).

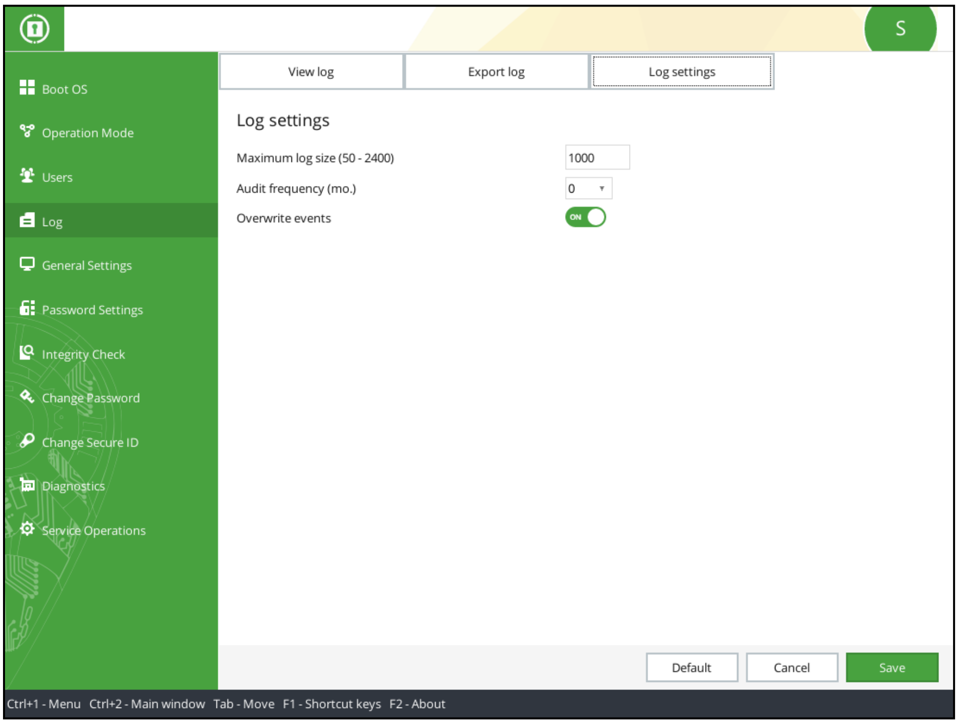
## Configure log settings

**Attention!** Some log settings are unavailable when Sobol is in joint mode (see p. 100).

**To configure log settings during Sobol operation:**

1. In the **Log** window, go to the **Log settings** tab (see  on p. **68**).

   The following window appears.



Log settings

Maximum log size (50 - 2400): 1000

Audit frequency (mo.): 0

Overwrite events: ON

2. Configure the log settings using Tab. 6 on p. **30**.
3. Select **Save** to save the changes.

To cancel, select **Cancel**.

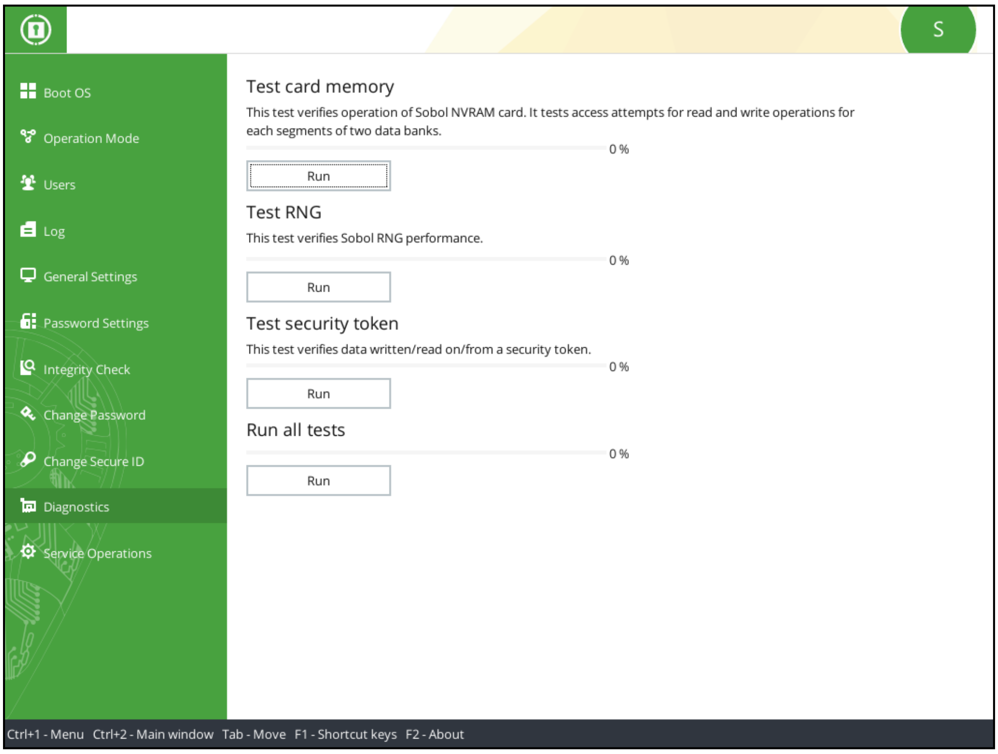
To set default values, select **Default**.

## Diagnostics

To test Sobol, select **Diagnostics**:

- in the Sobol initialization menu (see Fig. 19 on p. **25**);
- in the administrator menu when Sobol operates (see below).

The window appears as follows.



Test card memory

This test verifies operation of Sobol NVRAM card. It tests access attempts for read and write operations for each segments of two data banks.

0 %

Test RNG

This test verifies Sobol RNG performance.

0 %

Test security token

This test verifies data written/read on/from a security token.

0 %

Run all tests

0 %

Sobol provides the following operability tests:

- **Test card memory** — tests Sobol memory banks. During the test, read and write access to every segment of two memory banks is attempted.

  **Attention!** During the Sobol card memory test, do not reboot or shut down the computer. It can result in data loss from NVRAM.

- **Test RNG**— test the RNG processor operability.
- **Test security token** — checks for security token read/write faults.

  **Attention!** Present a security token for the test: the IButton key touches the reader / the USB key is in the USB port / the smart card is in the USB smart card reader.

- **Run all tests**— run all tests simultaneously.

  **Note.** After you run all tests, the window prompting a security token does not appear. Present a security token in advance.

**To run Sobol tests:**

1. Select a test and select **Run**.

   A test begins. The progress is indicated.

   To cancel the procedure, select **Cancel**.

   After a test is finished, the message with results appears.

2. Read the message referring to the error list if necessary (see p. **96**).

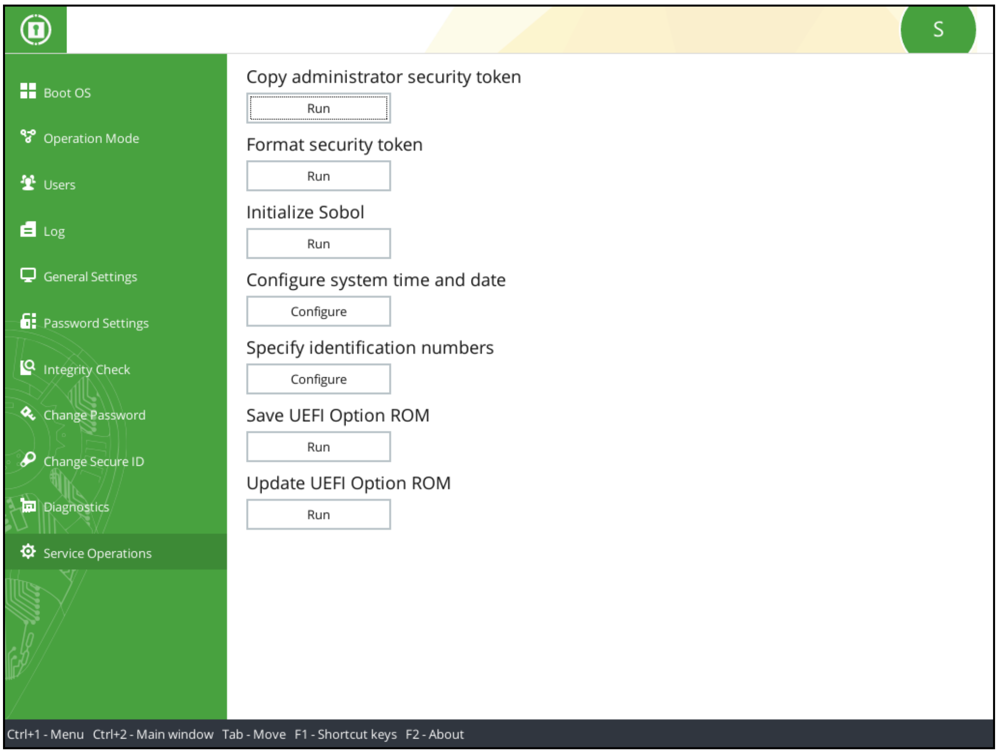
   **Attention!** If a card memory read errors occurs, the computer is locked for all users including the administrator. For more information about this error, see p. 92.

## Service operations

For **Service operations**, see:

- the Sobol initialization menu (see Fig. 19 on p. **25**);
- the administrator menu (see below).

After you select this menu item, the window appears as follows.



Sobol provides the following service operations:

- **Copy administrator security token** (see below);
- **Format security token** (see p. **74**);
- **Initialize Sobol** (see p. **75**);
- **Configure system time and date** (see p. **75**);
- **Save UEFI Option ROM** (see p. **76**);
- **Update UEFI Option ROM** (see p. **77**).

**Note.**

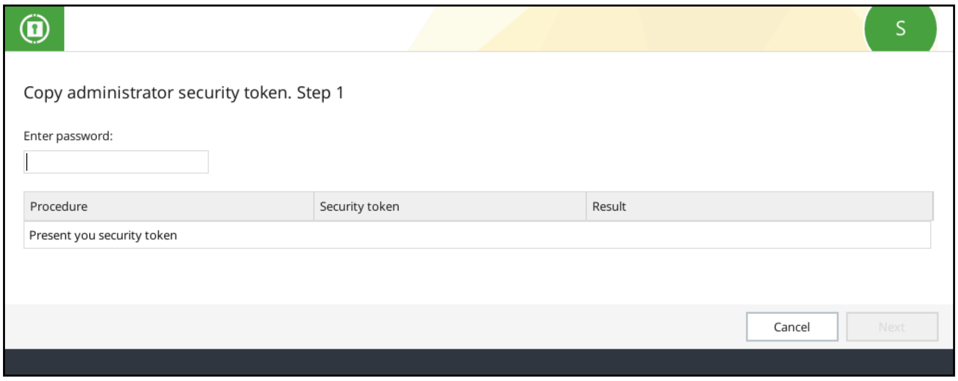
- The **Copy administrator security token** and the **Initialize Sobol** operations are available only when Sobol is in operation.
- The **Update UEFI Option ROM** operation is available after you set the switch SW1-2 of the PCIe (types 1, 2) / M.2 (types 1, 2) cards, the switch SA1-2 of the PCIe (types 3, 4) / M.2 (types 3, 4) cards and the switch S1-2 of the Mini PCIe Half card to ON.  (see Fig. 2 on p. **13**, see Fig. 3 on p. **14**Fig. 6 on p. **16**, Fig. 11 on p. **19**).

## Copy an administrator security token

**To copy an administrator security token:**

1. In the **Service operations** window (see the fig. above), in the **Copy administrator security token** area, select **Run**.

   The window appears as in the figure below.



Copy administrator security token. Step 1

Enter password:

| Procedure | Security token | Result |
|---|---|---|
| Present you security token | | |

2. In the **Enter password** text box, type the current administrator password.
3. Present the administrator security token.

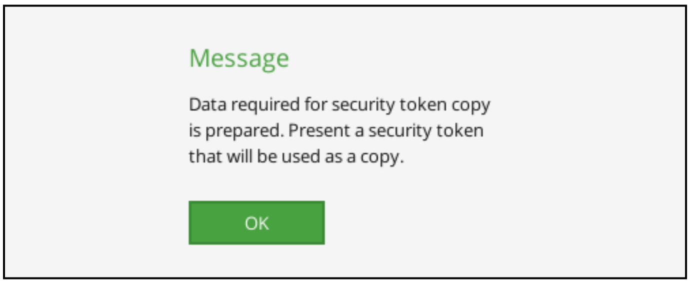
**Note.**
- If the security token is already presented (the iButton key touches the reader / the USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
- If several security tokens are presented simultaneously, the one that Sobol finds first is read.
- If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and select **OK**. Default PIN is provided on p. 7.

4. Select **Next**.

   If a presented security token does not belong to the administrator or the password is incorrect, you receive the **Invalid password or security token** message.

   Present an administrator security token and type a correct password.

   If the user credentials are correct, you receive a message as in the figure below.



Message

Data required for security token copy is prepared. Present a security token that will be used as a copy.

5. Select **OK**.

   The window prompting a security token appears.

6. Present the security token for a backup.

**Note.**
- If the securyty token is already presented (the iButton key touches the reader/USB key is in the USB port / the smart card is in the USB smart card reader), Sobol reads it automatically.
- If several security tokens are presented simultaneously, the one that Sobol finds first is read.
- If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and select **OK**. Default PIN is provided on p. 7.

   The message indicating that the security token is ready for creating a backup appears.

7. Select **Copy**.

   When the security token is successfully copied, you receive the respective message.

8. Select **Finish**

## Format a security token

**Attention!**
- Only security tokens that are **not registered** on a computer used for formatting can be formatted.
- After you format an IButton key, all data stored on it is lost beyond recovery. After you format a USB key, only data related to Sobol is lost.

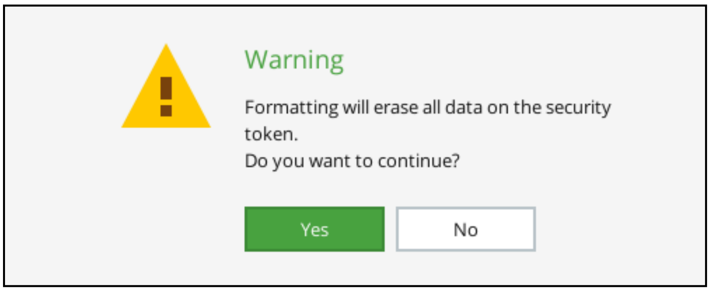
**To format a security token:**

1. Present a security token you need to format.

**Note.** If several security tokens are presented simultaneously, the one that Sobol finds first is read.

2. In the **Service operations** window (see  on p. **73**), in the **Format security token** area, select **Run**.

   You receive a message as in the figure below.



Warning

Formatting will erase all data on the security token.
Do you want to continue?

3. If you are sure you want to format a security token, select **Yes**.

   **Note.** If you present a security token protected by PIN, the respective dialog box appears. Enter PIN and click **OK**. Default PIN is provided on p. 7.

   After the security token is formatted, you receive the respective message.

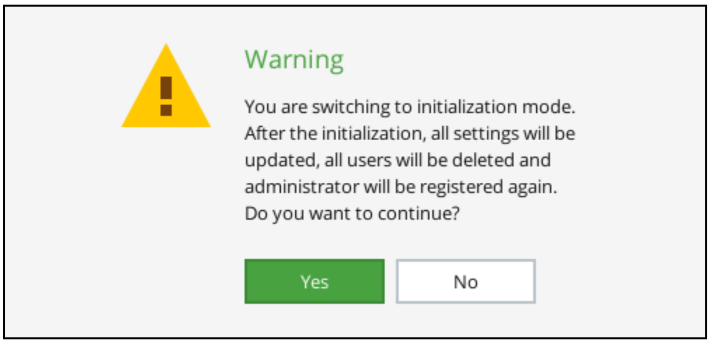
## Initialize Sobol

**Note.** You can initialize during Sobol operation without switching the card for initialization.

**To initialize Sobol:**

1. In the **Service operations** window, (see  on p. **73**) select **Run.**

   The following warning appears.



Warning

You are switching to initialization mode. After the initialization, all settings will be updated, all users will be deleted and administrator will be registered again.
Do you want to continue?

2. To continue initialization, select **Yes**.
3. Perform the Sobol initialization procedure referring to p. **25**.

   After the initialization is finished, the respective message appears. The computer is to be rebooted.
4. Select **OK**.

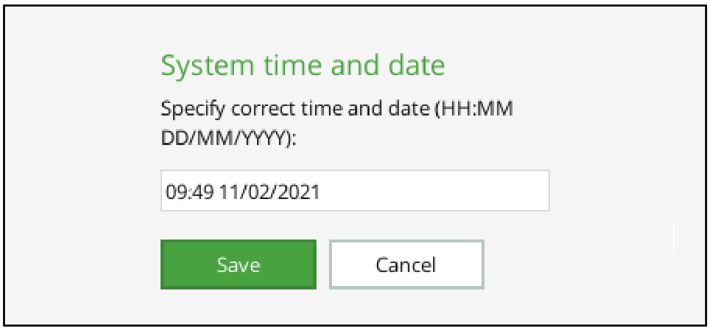
   The computer reboots.

## Configure the system time and date

**To configure the system time and date:**

1. In the **Service operations** window (see  on p. **73**), in the **Configure system time and date** area, select **Set**.

   A dialog box appears as in the figure below.



System time and date

Specify correct time and date (HH:MM DD/MM/YYYY):

09:49 11/02/2021

2. Specify the correct values and select **Save**.

> **Attention!** Make sure the time/date you set do not fall behind the time/date when a user password was set. Otherwise, a user cannot log on to the system.

After you change the system time and date, you receive the respective message.

## Save UEFI Option ROM

You can save the Sobol UEFI option ROM to a file created beforehand. You can create file in two ways:

- using the command line (see below);
- using Sobol software (see document [**1**]).

**To create a file using the command line:**

1. Run the command line in Windows OS or in Linux OS.
2. Go to the folder where you want to create the file.

> **Note.** The file is created in the Sobol default folder:
> - in Windows OS— in **\Sobol**;
> - in Linux OS — in **/sobol** or **/boot/sobol**.
>
> If the standard folder is not found, create it in the system drive.

3. Run the following command:
   - for Windows OS:

```
fsutil file createNew bios.bin 1062400
```

   - for Linux OS:

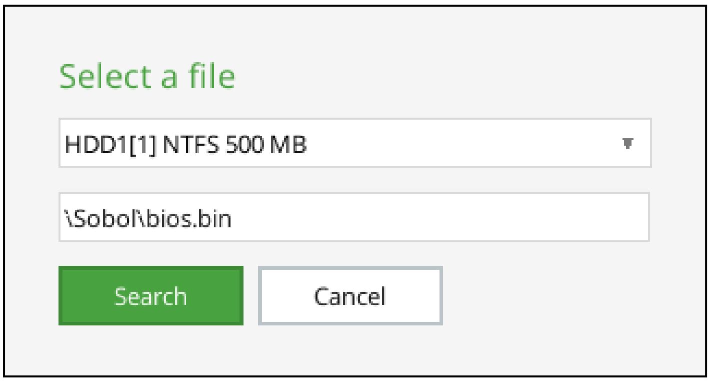
```
dd if=/dev/zero of=bios.bin count=1 bs=1062400
```

> **Note.** You can enter any name for the file.

**To save the UEFI option ROM to a file:**

1. In the **Service operations** window (see  on p. **73**), in the **Save UEFI Option ROM** area, select **Run**.

   A dialog box appears as in the figure below.



Select a file

HDD1[1] NTFS 500 MB

\Sobol\bios.bin

2. Change the volume and/or a file name if necessary.
3. Select **OK**.

> **Note.** If the path to a file is incorrect, the error message appears. Select **OK** and try again.
> Make sure you use short forms for long names (more than 8 characters) of files stored on disks with FAT16 and FAT32. For example, pcim~1.bin. For a file name short form, use the DIR command or a file manager such as Total Commander.

After you save the UEFI Option ROM, you receive the respective message.

## Update UEFI Option ROM

> **Attention!**
> - All Sobol settings are reset after you update the UEFI option ROM.
> - Before updating, set the switch SW1-2 of the PCIe (types 1, 2) / M.2 (types 1, 2)cards, the switch SA1-2 of the PCIe (type 3,4) / M.2 (types 3, 4) and the switch S1-2 of the Mini PCIe Half card to ON (see Fig. 2 on p. **13**, Fig. 6 on p. **16**, Fig. 11 on p. **19**).
> - After updating UEFI Option ROM, perform Sobol initialization.

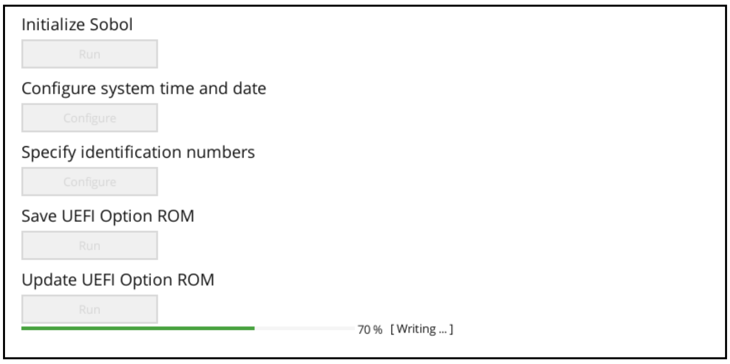
**To update the UEFI option ROM:**

1. In the **Service operations** window (see  on p. **73**), in the **Update UEFI Option ROM** area, select **Run**.

   The window for selecting an UEFI Option ROM file appears (see  on p. **76**).
2. Change the volume (disk, partition) and/or a file name if necessary.
3. Select **OK**.

   > **Note.** If the path to a file is incorrect, the error message appears. Select **OK** and try again.
   > Make sure you use short forms for long names (more than 8 characters) of files stored on disks with FAT16 and FAT32. For example, pcim~1.bin. For a file name short form, use the DIR command or a file manager such as Total Commander.

   The UEFI option ROM updating begins.



70 % [Writing ... ]

   After the procedure is finished, you receive the respective message.
4. Select **OK**.

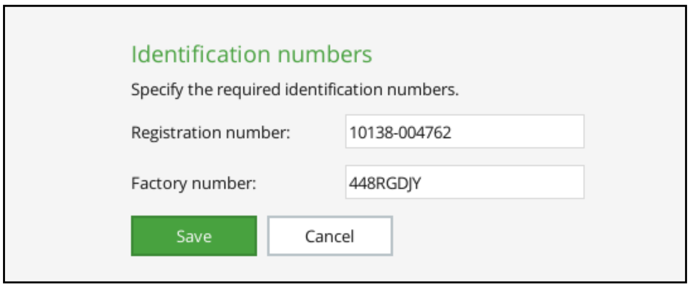
   The computer will be shut down. When you start it next time, the new UEFI option ROM will be used.
5. Perform Sobol initialization.

## Specify identification numbers

**To specify identification numbers:**

1. In the **Service Operations** dialog box, go to **Specify identification numbers** and click **Specify**.  on p. **73**).

   A dialog box appears.



Identification numbers

Specify the required identification numbers.

Registration number: 10138-004762

Factory number: 448RGDJY

2. In the fields **Registration number** and/or **Factory number**, enter the identification number of your Sobol copy.

**Note.**

- A registration number is a serial number assigned to each Sobol copy.
- A factory number is a unique number which is randomly generated when manufacturing Sobol.
- The numbers can contain only the following:
  - digits (0-9);
  - Latin letters (A-Z, a-z);
  - special characters (N-).
- The length of both the registration and the factory number must not be greater 12 characters.
- The registration and factory numbers are kept in a hidden Sobol memory area.

To view information on identification numbers, press <F2>.

3. Select **Save** to save the changes.

## Complete Sobol configuration

To complete Sobol configuration, do one of the following:

- shut down the computer if you do not need to continue working;
- in the administrator menu, select **Boot OS** if you need to continue working on the computer (see Fig. 19 on p. **25**).

  If the integrity check is on, before the OS boots, the set objects are checked. Select **Finish** after the check is completed.

  **Note.**

  - To abort the check, press <**Esc**> or select **Stop**.
  - If an error occurred, the integrity check is stopped. Read an error message (for a list of errors, see p. **95**). To resume the check, select **OK**.
  - If you do not need Sobol notifications during checksums calculation, select **Don't ask again** in the error message window.
  - After the check is finished and the OS boots, address error causes. Calculate integrity check objects checksums (see p. **63**).

  The OS booting begins.

# Chapter 5
# IC template management

Sobol allows you to add/remove objects to/from IC templates to enable/disable integrity check for these objects.

IC template is a service file that contains information about objects being checked for integrity when the IC mechanism is enabled.

IC template contains the following:

- resources — the object identification data;
- checksums.

To manage IC templates:

- in standalone mode — use either built-in IC template management or Sobol software;

  **Note.** You can select the way to manage IC templates in the Sobol administrator menu, the **Integrity Check** section (see p. 63).

- in joint mode — use the tools of a product that operates in tandem with Sobol.

This chapter provides guidelines on using built-in IC template management.

**Note.** For detailed information about the purpose, setup and operation of the Sobol software, see document [**1**].

## Purpose of built-in IC template management

Built-in template management allows you to configure IC templates using the administrator menu. You can perform the following procedures:

- create resource groups (see p. **80**);
- add resources to a group (see p. **82**);
- rename groups, move resources between groups (see p. **88**);
- sort resources (see p. **88**);
- export and import resources (see p. **89**);
- delete groups and resources (see p. **90**).

Built-in IC template management operates with a template created by the administrator (see p. **79**).

On computers running Windows, built-in IC template management allows you to check integrity of the following objects:

- files;
- hard drive sectors;
- registry items;
- PCI devices;
- SMBIOS tables.

On computers running Linux, built-in IC template management allows you to check file and hard drive sector integrity. On computers running CentOS 7.3, you can also check PCI device and SMBIOS tables integrity.

## Create an IC template

You can create an IC template manually using the command line.

**To create an IC template:**

1. In Windows, run the command prompt; in Linux, run the command line terminal.

2. Go to the Sobol folder:
   - in Windows — the **\Sobol** folder;
   - in Linux — the **/sobol** or **/boot/sobol** directories.

**Note.** If standard folders are not found, create them in a system volume.

3. To create an IC template and its backup, run the following command:
   - in Windows:

```
fsutil file createNew icheck.json 34000000
fsutil file createNew icheck_backup.json 34000000
```

   - in Linux:

```
dd if=/dev/zero of=icheck.json count=1 bs=32M
dd if=/dev/zero of=icheck_backup.json count=1 bs=32M
```

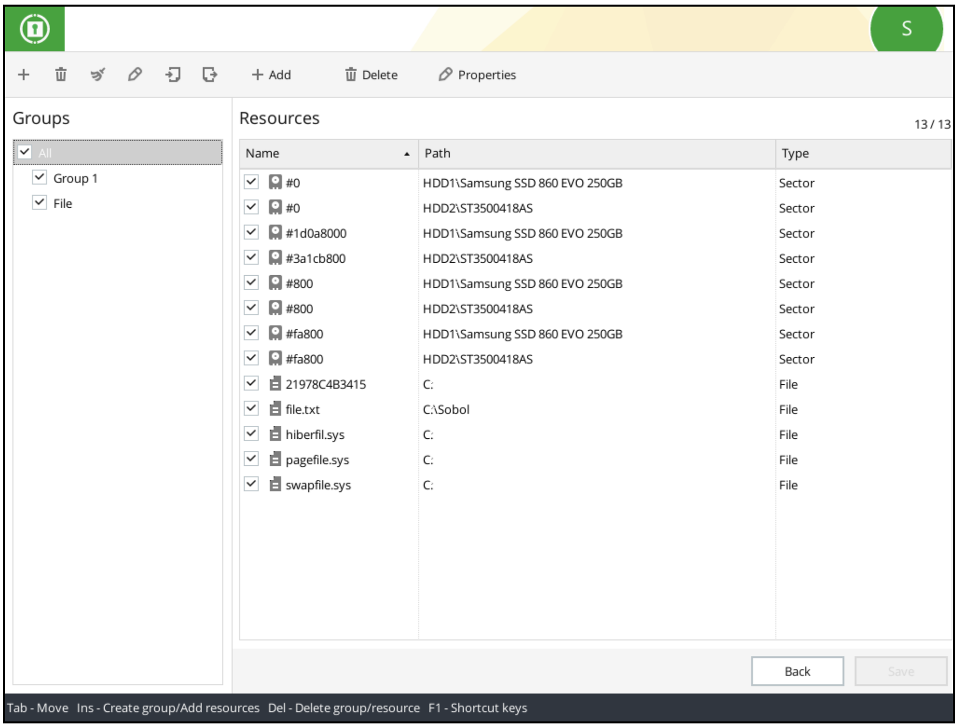
An IC template file (**icheck.json**) and its backup files (**icheck_backup.json**) are created in the standard Sobol folder. When you edit an IC template using built-in IC template management, all changes are saved in the template and backup files.

## Start built-in IC template management

**To start built-in IC template management:**

1. In the administrator menu (see  on p. **49**), select **Integrity Check**.
2. In the appeared window (see  on p. **63**), in the **IC template management** section, select **Start**.

   A window appears as in the figure below.


S
+ Add
Delete
Properties
Groups
☑ All
☑ Group 1
☑ File
Resources
13 / 13
Back
Save
Tab - Move  Ins - Create group/Add resources  Del - Delete group/resource  F1 - Shortcut keys

| Name | Path | Type |
|---|---|---|
| ☑ #0 | HDD1\Samsung SSD 860 EVO 250GB | Sector |
| ☑ #0 | HDD2\ST3500418AS | Sector |
| ☑ #1d0a8000 | HDD1\Samsung SSD 860 EVO 250GB | Sector |
| ☑ #3a1cb800 | HDD2\ST3500418AS | Sector |
| ☑ #800 | HDD1\Samsung SSD 860 EVO 250GB | Sector |
| ☑ #800 | HDD2\ST3500418AS | Sector |
| ☑ #fa800 | HDD1\Samsung SSD 860 EVO 250GB | Sector |
| ☑ #fa800 | HDD2\ST3500418AS | Sector |
| ☑ 21978C4B3415 | C: | File |
| ☑ file.txt | C:\Sobol | File |
| ☑ hiberfil.sys | C: | File |
| ☑ pagefile.sys | C: | File |
| ☑ swapfile.sys | C: | File |

The **Groups** section contains a list of resource groups and buttons to manage them.

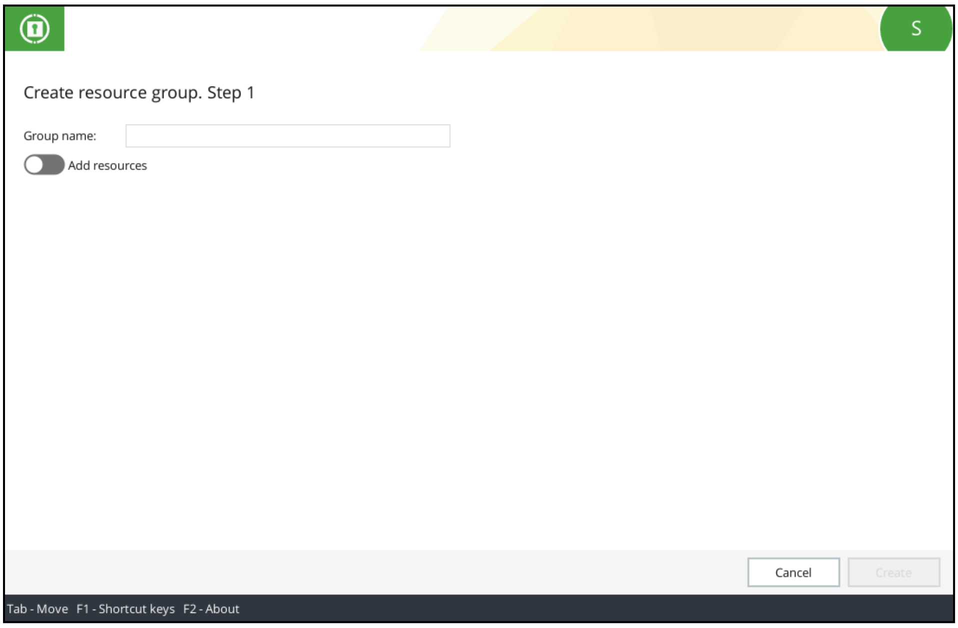
The **Resources** section contains a list of resources included in a selected group and buttons to manage them.

## Creating a resource group

**To create a resource group:**

1. In the **Groups** section (see  on p. **80**), select +.

   A window appears as in the figure below.



Create resource group. Step 1

Group name:

Add resources

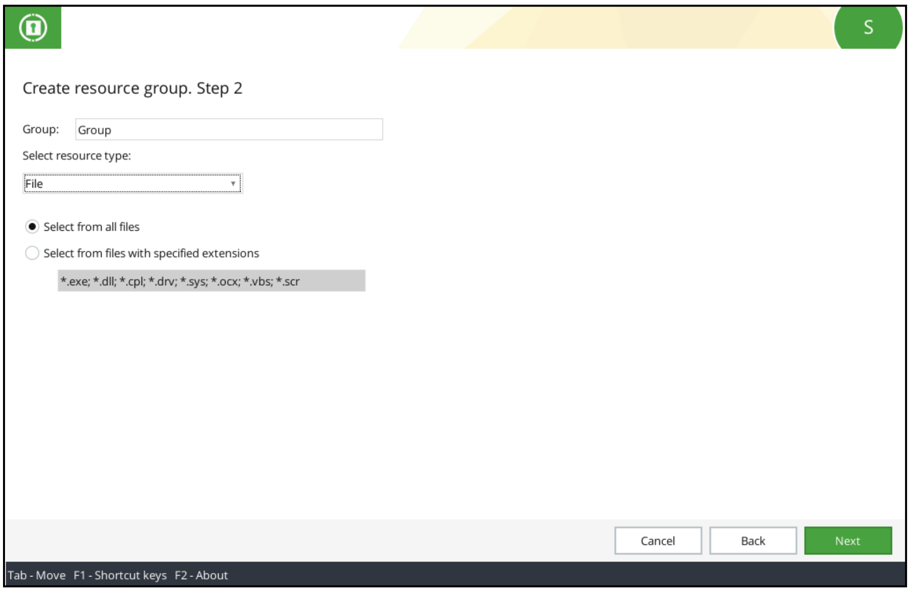
2. Enter a name for a resource group.

> **Note.** To switch keyboard layout, press **<F12>**.

3. Then:
   - To create an empty group, select **Create**.

     A new group appears in the **Groups** section.
   - To create a group and to add resources to this group, turn on the **Add resources** toggle and select **Create**.

     A window appears as in the figure below.



Create resource group. Step 2

Group: Group

Select resource type: File

● Select from all files

○ Select from files with specified extensions

*.exe; *.dll; *.cpl; *.drv; *.sys; *.ocx; *.vbs; *.scr

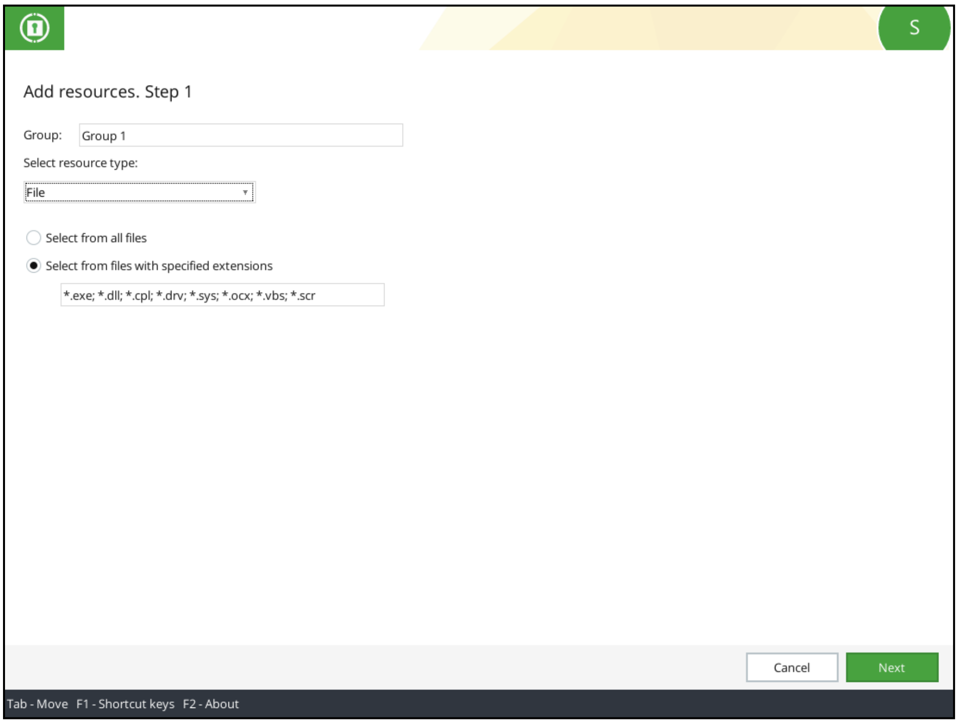
4. For detailed information about adding resources to a group, see:
   - p. 82 for files;
   - p. 83 for registry items;
   - p. 84 for registry keys;
   - p. 85 for hard drive sectors;
   - p. 86 for device configuration.

# Add resources to a group

**To add resources to a group:**

1. In the **Groups** section (see  on p. **80**), select the required group.
2. In the **Resources** section, select **Add**.

   A window appears as in the figure below.



Add resources. Step 1

Group: Group 1

Select resource type:

File

○ Select from all files

● Select from files with specified extensions

*.exe; *.dll; *.cpl; *.drv; *.sys; *.ocx; *.vbs; *.scr

**Note.** When you add resources while creating a group (see p. **81**), the window heading differs from one in the figure above.

3. Proceed to procedures for adding the required type of resources:
   - see below for files;
   - p. **83** for registry items;
   - p. **84** for registry keys;
   - p. **85** for hard drive sectors;
   - p. **86** for device configuration.

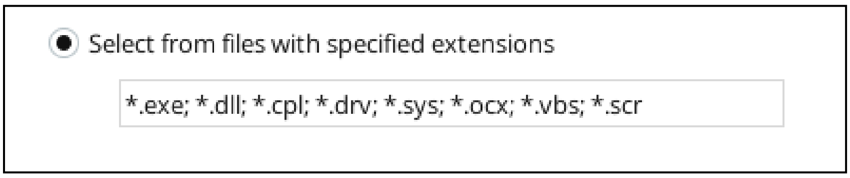
## Add files to a group

**To add files to a group:**

1. In the **Add resources. Step 1** window (see the figure above), in the drop-down list, select the required file type.

   Now you can select the required way to add files.
2. Select the way to add files:
   - **Select from all files** — to select files manually;
   - **Select from files with specified extensions** — to add files filtered by extensions specified in the text box below.

     If you selected this option, specify the required file extensions.

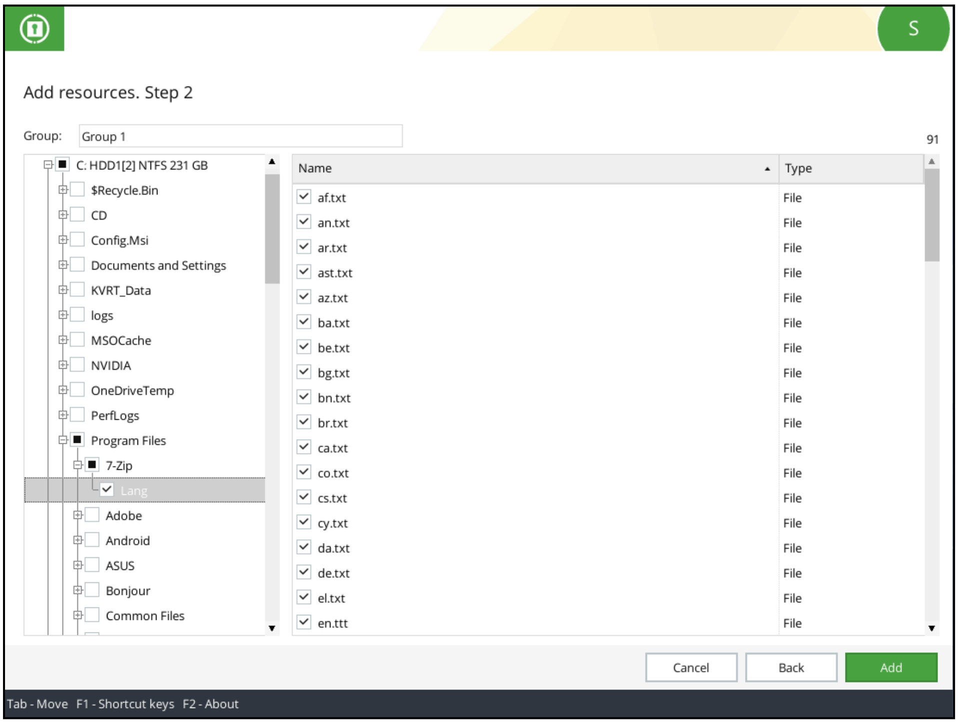


● Select from files with specified extensions

*.exe; *.dll; *.cpl; *.drv; *.sys; *.ocx; *.vbs; *.scr

3. Select **Next**.

   A window where you can select the required resources appears. The folder structure is shown on the left; files included in the selected folder are shown on the right.



Add resources. Step 2

Group: Group 1

91

- ■ C: HDD1[2] NTFS 231 GB
  - □ $Recycle.Bin
  - □ CD
  - □ Config.Msi
  - □ Documents and Settings
  - □ KVRT_Data
  - □ logs
  - □ MSOCache
  - □ NVIDIA
  - □ OneDriveTemp
  - □ PerfLogs
  - ■ Program Files
    - ■ 7-Zip
      - ☑ Lang
    - □ Adobe
    - □ Android
    - □ ASUS
    - □ Bonjour
    - □ Common Files

| Name | Type |
|---|---|
| ☑ af.txt | File |
| ☑ an.txt | File |
| ☑ ar.txt | File |
| ☑ ast.txt | File |
| ☑ az.txt | File |
| ☑ ba.txt | File |
| ☑ be.txt | File |
| ☑ bg.txt | File |
| ☑ bn.txt | File |
| ☑ br.txt | File |
| ☑ ca.txt | File |
| ☑ co.txt | File |
| ☑ cs.txt | File |
| ☑ cy.txt | File |
| ☑ da.txt | File |
| ☑ de.txt | File |
| ☑ el.txt | File |
| ☑ en.ttt | File |

4. Select the required files and folders.

   **Note.** Selecting files and folders note that:

   - To select a file, select ☑.
   - The selected folder may be indicated as follows:
     - ■ — the folder contents are selected partly/subfolders are not opened and the files are not selected;
     - ☑ — all the files and subfolders are selected.
   - To select a folder that contains subfolders, open all the subfolders.
   - If you previously selected **Select from files with specified extensions**, you can only view the folder structure, files of the selected folder are not shown. When you add the folder to the IC template, all files with the specified extensions are selected.

5. Select **Add**.

   **Note.**

   - If you add resources while creating a group, select **Create**.
   - To return to the previous step, select **Back**.
   - To cancel adding resources, select **Cancel**.

   The selected resources are added to the group. The main window of Built-in IC template management appears.

6. To save changes, select **Save**.

   **Note.** To return to the administrator menu, select **Back**.

## Add registry variables to a group

**Note.** This feature is available only in Windows.

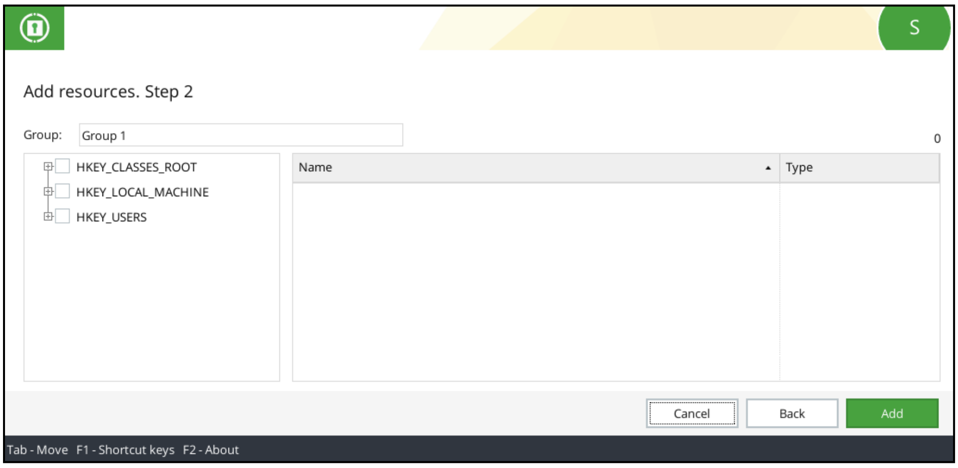
**To add registry variables to a group:**

1. In the **Add resources. Step 1** window (see the figure above), in the drop-down list, select **Registry variable**.

   The **OS volume** drop-down list appears.

2. In the **OS volume** drop-down list, select the required volume.
3. Select **Next**.

A window where you can select the required resources appears. The registry structure is shown on the left; the variables of the selected section/subsection are shown on the right.



Add resources. Step 2

Group: Group 1

0

- □ HKEY_CLASSES_ROOT
- □ HKEY_LOCAL_MACHINE
- □ HKEY_USERS

| Name | Type |
|---|---|

4. Select the required resources.

**Note.** Selecting registry variables note that:

- To select a variable, select ☑.
- The selected section may be indicated as follows:
  - ▣ — the section contents are selected partly/subsections are not opened and the variables are not selected;
  - ☑ — all the variables and subsections are selected.
- To select a section that contains subsections, open all the subsections.

5. Select **Add**.

**Note.**
- If you add resources while creating a group, select **Create**.
- To return to the previous step, select **Back**.
- To cancel adding resources, select **Cancel**.

The selected resources are added to the group. The main window of Built-in IC template management appears.

6. To save changes, select **Save**.

**Note.** To return to the administrator menu, select **Back**.

## Add registry keys to a group

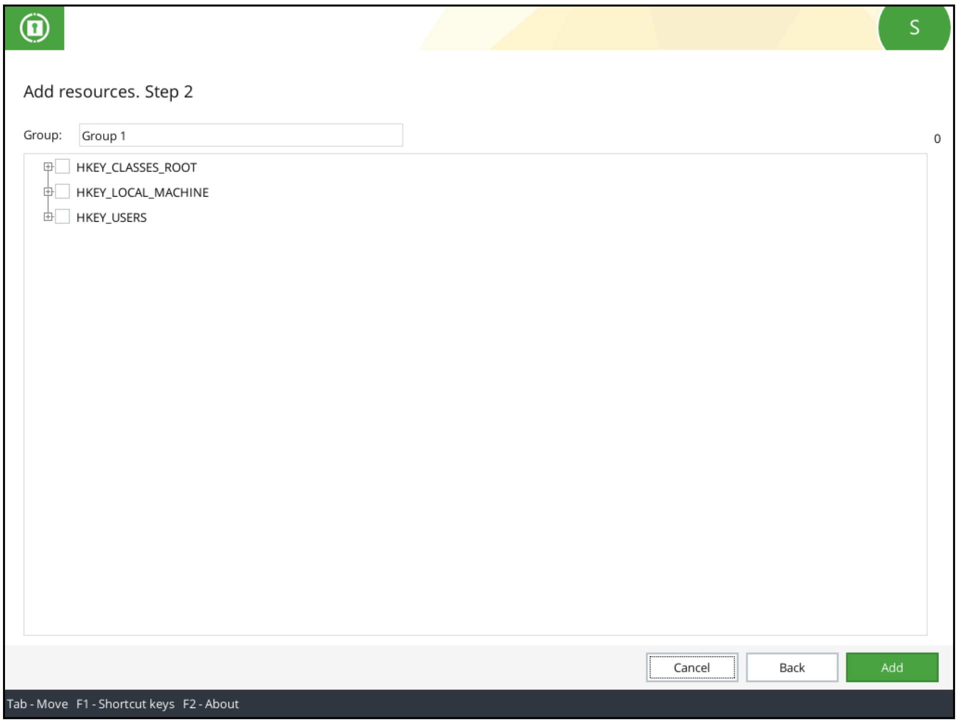
**Note.** This feature is available only in Windows.

**To add registry keys to a group:**

1. In the **Add resources. Step 1** window (see  on p. 82), in the drop-down list, select **Registry key**.

   The **OS volume** drop-down list appears.
2. In the **OS volume** drop-down list, select the required OS volume.
3. Select **Next**.

   A window where you can select the required resources appears.



Add resources. Step 2

Group: Group 1

4. Select the required resources.

> **Note.** Selecting registry keys note that:
> - The selected section may be indicated as follows:
>   - ▣ — the section contents are selected partly/subsections are not opened and the keys are not selected;
>   - ☑ — all the keys and subsections are selected.
> - To select a section that contains subsections, open all the subsections.

5. Select **Add**.

> **Note.**
> - If you add resources while creating a group, select **Create**.
> - To return to the previous step, select **Back**.
> - To cancel adding resources, select **Cancel**.

The selected resources are added to the group. The main window of Built-in IC template management appears.

6. To save changes, select **Save**.

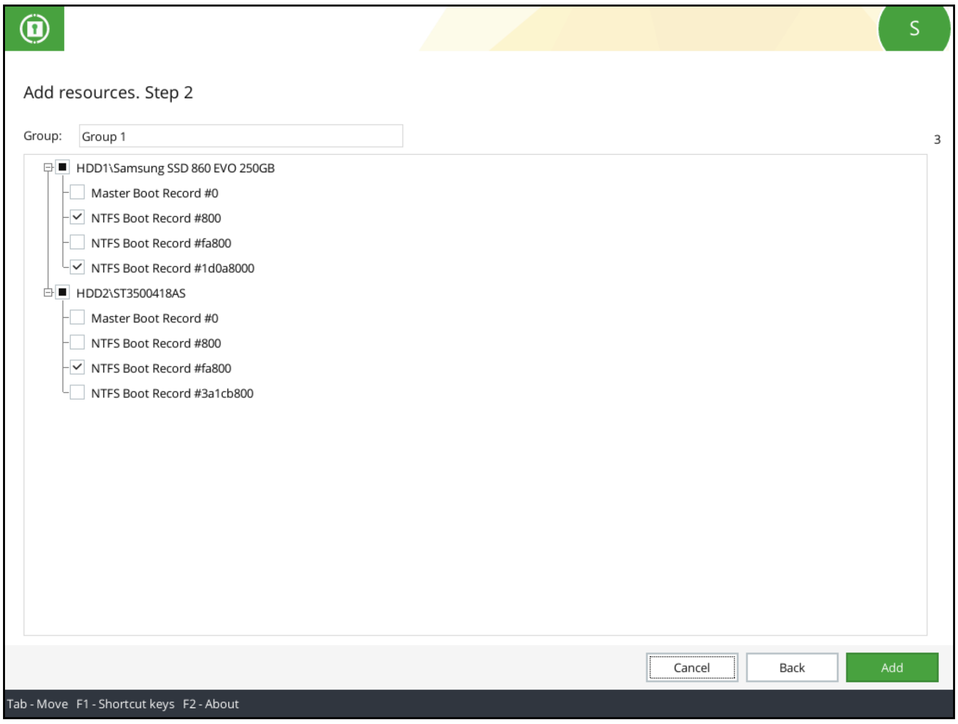
> **Note.** To return to the administrator menu, select **Back**.

## Add drive sectors to a group

**To add hard drive sectors to a group:**

1. In the **Add resources. Step 1** window (see  on p. 82), in the drop-down list, select **Drive sector**.
2. Select **Next**.

   A window where you can select the required resources appears.



Add resources. Step 2

Group: Group 1

3

- ▣ HDD1\Samsung SSD 860 EVO 250GB
  - □ Master Boot Record #0
  - ☑ NTFS Boot Record #800
  - □ NTFS Boot Record #fa800
  - ☑ NTFS Boot Record #1d0a8000
- ▣ HDD2\ST3500418AS
  - □ Master Boot Record #0
  - □ NTFS Boot Record #800
  - ☑ NTFS Boot Record #fa800
  - □ NTFS Boot Record #3a1cb800

3. Select the required resources.

**Note.** Selecting drive sectors note that:

- To select a drive sector, select ☑.
- To select all sectors in a drive, select ☑ next to the required disk.
- If you select drive sectors partly, the drive has the following indicator: ▣.

4. Select **Add**.

**Note.**

- If you add resources while creating a group, select **Create**.
- To return to the previous step, select **Back**.
- To cancel adding resources, select **Cancel**.

The selected resources are added to the group. The main window of Built-in IC template management appears.

5. To save changes, select **Save**.

**Note.** To return to the administrator menu, select **Back**.

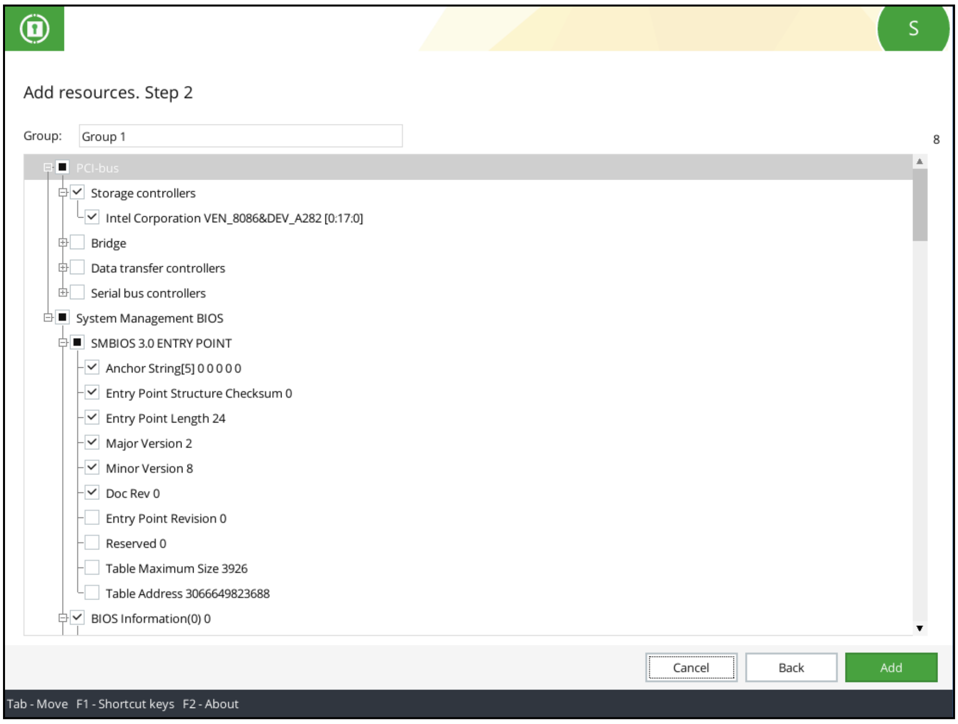
## Add device configuration to a group

**Note.** This feature is available only in Windows.

**To add device configurations to a group:**

1. In the **Add resources. Step 1** window (see  on p. 82), in the drop-down list, select **Device configuration**.
2. Select **Next**.

A window appears as in the figure below.



Add resources. Step 2

Group: Group 1

8

- ▣ PCI-bus
  - ☑ Storage controllers
    - ☑ Intel Corporation VEN_8086&DEV_A282 [0:17.0]
  - □ Bridge
  - □ Data transfer controllers
  - □ Serial bus controllers
- ▣ System Management BIOS
  - ▣ SMBIOS 3.0 ENTRY POINT
    - ☑ Anchor String[5] 0 0 0 0 0
    - ☑ Entry Point Structure Checksum 0
    - ☑ Entry Point Length 24
    - ☑ Major Version 2
    - ☑ Minor Version 8
    - ☑ Doc Rev 0
    - □ Entry Point Revision 0
    - □ Reserved 0
    - □ Table Maximum Size 3926
    - □ Table Address 3066649823688
  - ☑ BIOS Information(0) 0

3. Select the required resources.

> **Note.** Selecting devices note that:
>
> - To select a device, select ☑.
> - The selected device groups may be indicated as follows:
>   - ▣ — the group contents are selected partly/subgroups are not opened and the devices are not selected;
>   - ☑ — all the devices and subgroups are selected.
> - To select a folder that contains subfolders, open all the subfolders.

4. Select **Add**.

> **Note.**
>
> - If you add resources while creating a group, select **Create**.
> - To return to the previous step, select **Back**.
> - To cancel adding resources, select **Cancel**.

The selected resources are added to the group. The main window of Built-in IC template management appears.

5. To save changes, select **Save**.

> **Note.** To return to the administrator menu, select **Back**.

## To enable IC for groups and resources

### To enable/disable IC for a group:

1. In the **Groups** section (see  on p. **80**), select the required group.
2. Select:
   - ☑ — to enable IC for a group;
   - □ — to disable IC for a group;

IC is enabled/disabled for the group and all its resources.

### To enable/disable IC for a resource:

1. In the **Groups** section (see  on p. **80**), select the required group.
2. In the **Resources** section, select:
   - ☑ — to enable IC for a resource;

- □ — to disable IC for a resource;

IC is enabled/disabled for the resource.

> **Note.** If you manually configured different IC parameters (enable/disable) for resources within a single group, this group has the following icon: ▣.

# Managing resources

## Group and resource properties

The group and resource properties allow you to rename groups, view the resource data and move resources between groups.

**To rename a group:**

1. In the **Groups** section (see  on p. **80**), select the required group.
2. Select ✎.

   A dialog box appears prompting you to enter the group name.
3. Enter the group name.

   > **Note.** To switch a keyboard layout, press **<F12>**.
4. Select **Save**.

**To view the resource data:**

1. In the **Resources** section (see  on p. **80**), select the required resource.
2. Select **Properties**.

   A dialog box appears. It contains the following resource data:
   - name;
   - path;
   - type;
   - the list of groups where the resource is located.

**To move a resource between groups:**

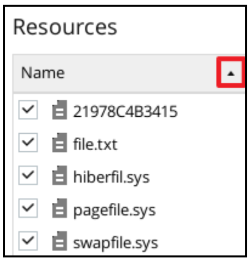
1. In the **Resources** section (see  on p. **80**), select the required resource.
2. Select **Properties**.
3. In the list of groups:
   - select ☑ to add resource to a group;
   - select □ to remove resource from a group.

## Sort resources

Resources can be sorted alphabetically (and reversed) by name, path and type.

**To sort resources:**

- In the **Resources** section (see  on p. **80**), select the sorting command in the required column.



Resources

Name ▲

☑ 21978C4B3415

☑ file.txt

☑ hiberfil.sys

☑ pagefile.sys

☑ swapfile.sys

The resources are sorted by the selected column.

## Exporting and importing resources

Labels allow matching drives and volumes while importing/exporting resources.

During the export, administrator labels drives and volumes of a computer where the export is performed.

During the import, administrator matches labels from the file being imported with volumes and drives of a computer where the import is performed.

**Note.** We recommend that you import/export resources between computers with the same configuration and installed software.

You must create the export file before performing the export.

**To create an export file:**

1. In Windows, run the command prompt; in Linux, run the command line terminal.
2. Go to a folder where you need to create the export file.
3. To create the file, run the following command:
   - in Windows:

     ```
     fsutil file createNew export.json 34000000
     ```

   - in Linux:

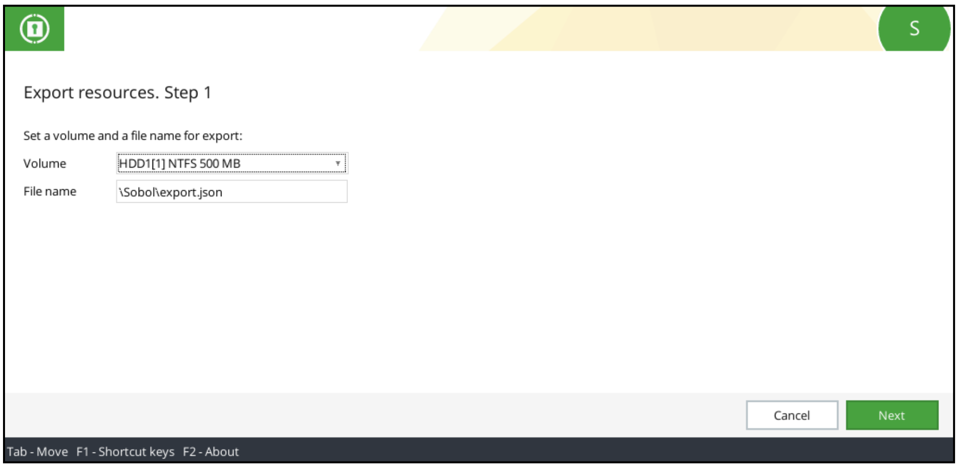
     ```
     dd if=/dev/zero of=export.json count=1 bs=32M
     ```

   **Note.**
   - You can specify any name for the export file.
   - You can create the export file of a larger size.

**To export resources:**

1. In the **Groups** section (see  on p. **80**), select ⇥.

   A window appears as in the figure below.



Export resources. Step 1

Set a volume and a file name for export:

Volume: HDD1[1] NTFS 500 MB

File name: \Sobol\export.json

2. Specify the export parameters:
   - in the **Volume** drop-down list, select a volume where the export file is located;
   - in the **File name** text box, enter the export file name.
3. Select **Next**.

   A windows appears where you must select the resource groups to be exported.
4. Select the required groups.
5. Select **Next**.

   A window appears where you must set the required labels.
6. Set labels for drives and/or volumes that contains IC objects.
7. Select **Export**.

   The export progress is shown on the screen. .

   **Note.** To stop the export, select **Cancel**.

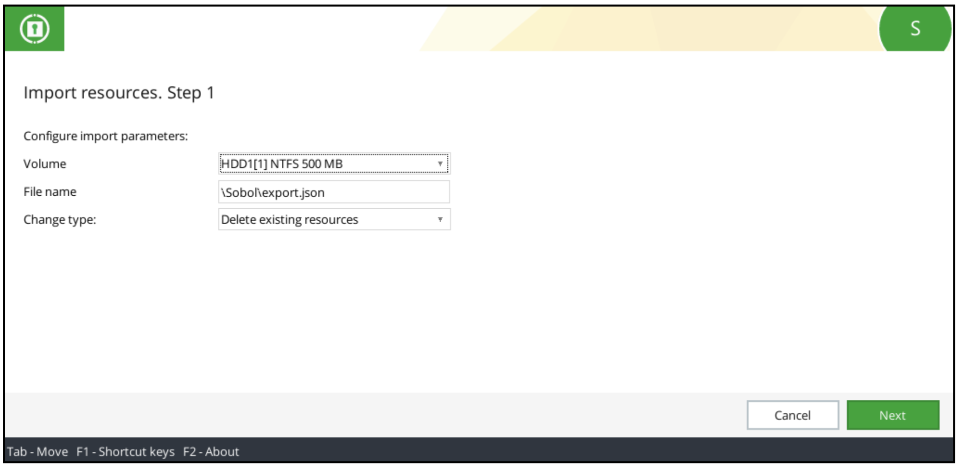
When the export is completed, you can see the time spent for the procedure.

8. Select **Finish**.

**To import resources:**

1. In the **Groups** section (see  on p. **80**), select .

   A window appears as in the figure below.



Import resources. Step 1

Configure import parameters:

Volume: HDD1[1] NTFS 500 MB

File name: \Sobol\export.json

Change type: Delete existing resources

2. In the **Volume** drop-down list, select a volume where a file to be imported is located.
3. In the **File name** text box, specify a full name of the file to be imported.
4. In the **Change type** drop-down list, select the required option:

**Delete existing resources**

All groups and resources of the current IC template are deleted before the import. After the import, the IC template will only contain the groups and resources from the imported file.

**Add to existing resources**

The groups and resources from the imported file are added to the IC template without deleting already existing resources. Groups can be duplicated during the import. To configure the duplicating, set the Keep existing groups toggle to the respective position:

- **ON** — the groups are not duplicated;
- **OFF** — the groups that have the same names are duplicated and the imported objects has the following name: **object_nameN** where **N** is the sequence number of the duplicated object.

**Note.** Resources are not duplicated.

5. Select **Next**.

   A window appears where you must match the labels from the imported file with the drives and/or volumes.
6. Match the labels with the drives and/or volumes.
7. Select **Import**.

   The import progress is shown on the screen.

   **Note.** To stop the import, select **Cancel**.

   When the import is completed, you can see the time spent for the procedure.
8. Select **Finish**.

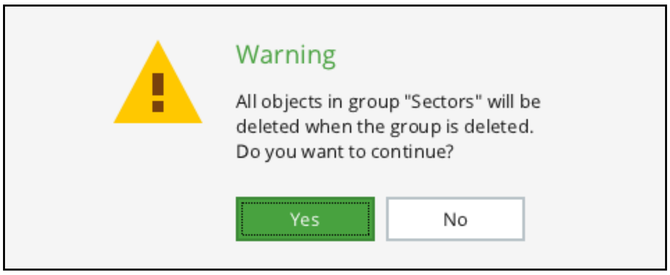
## Deleting groups and resources

**Attention!** When you delete a group, all the resources included in this group are deleted as well.

**To delete a group\resource:**

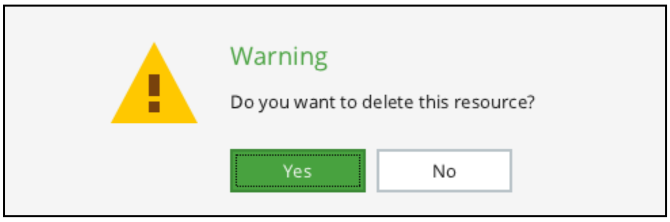
1. In the **Groups** or **Resources** section (see  on p. **80**), select the required group or resource.
2. Select .

   - When you delete a group, a dialog box appears as in the figure below.


Warning

All objects in group "Sectors" will be deleted when the group is deleted. Do you want to continue?

- When you delete a resource, a dialog box appears as in the figure below.


Warning

Do you want to delete this resource?

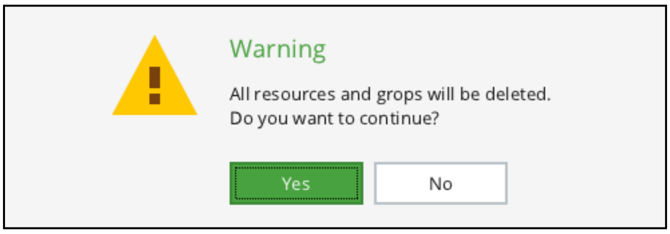
**3.** Select **Yes**.

**Note.** To cancel the procedure, select **No**.

**To delete all groups and resources:**

**1.** In the **Groups** section (see  on p. **80**), select ✓.

**2.** A dialog box appears as in the figure below.


Warning

All resources and grops will be deleted. Do you want to continue?

**3.** Select **Yes**.

**Note.** To cancel the procedure, select **No**.

# Appendix

## Sobol messages

### Boot error messages

When boots, errors can occur leading to computer lockout. In this case, the following error messages may appear:

| **Card: Watchdog timer triggered. System halted** | |
|---|---|
| **Cause** | Watchdog timer timeout expired |
| **Solution** | Unplug all removable devices from your computer and restart it. If the error occurs again, perform the initialization (see Sobol Card: Please enable HPET (High Precision Event Timer) in BIOS Setup ) p. 24) |

| **Sobol Card: Please enable HPET (High Precision Event Timer) in BIOS Setup. System halted** | |
|---|---|
| **Cause** | HPET (High Precision Event Timer) is disabled |
| **Solution** | Restart your computer. In UEFI/BIOS Setup, enable the HPET function |

| **Sobol Card: Internal error [error code]. System halted** | |
|---|---|
| **Cause** | An error occurred when accessing the card |
| **Solution** | Restart your computer. If the error remains, contact your vendor with the error code |

| **Sobol Card: Firmware error [error code]. System halted** | |
|---|---|
| **Cause** | Sobol nonvolatile memory, which stores UEFI Option ROM, is damaged |
| **Solution** | Contact your vendor with the error code |

| **Sobol Card: Memory integrity error. Reinitialization required. System halted** | |
|---|---|
| **Cause** | Sobol nonvolatile memory containing Sobol settings information is damaged. The damage can be a result of restarting the computer while using Sobol nonvolatile memory |
| **Solution** | Perform the initialization (see Sobol Card: OS boot forbidden) p. 24) |

| **Sobol Card: OS boot forbidden. System halted** | |
|---|---|
| **Cause** | UEFI/BIOS of the computer motherboard is configured incorrectly |
| **Solution** | In UEFI/BIOS Setup, disable Fast Boot |

| **Sobol Card: Random numbers generators error. System halted** | |
|---|---|
| **Cause** | When Sobol starts, the RNG test is performed. If the test result does not comply with GOST requirements, the computer is blocked for all users including the administrator |
| **Solution** | Restart your computer. If the test error repeats, check that the Sobol card is connected correctly and that the M.2/Mini PCIe/PCIe connector in which the card is plugged works properly. If the error occurs again, contact the vendor technical support |

| **Sobol: Legacy OpROM mode not supported. Please enable UEFI OpROM** | |
|---|---|
| **Sobol: Legacy OpROM mode is not supported. System halted** | |
| **Cause** | The computer started in Legacy OpROM mode. Sobol blocked the start of the computer |
| **Solution** | If SW1-3 is set to ON on PCIe or M2 cards (types 1, 2), SA1-3 is set to ON on PCIe or M.2 cards (types 3, 4) or SA1-3 is set to ON on Mini PCIe Half, remove the card, select UEFI in UEFI/BIOS Setup and insert the card again. If SW1-3, SA1-3 or S1-3 is set to OFF, select UEFI in UEFI/BIOS Setup |

### Messages about events that cause computer lockout

When working with Sobol, a number of events may lead to computer lockout. In this case, the following messages may appear:

| **Password expired. Contact your administrator** | |
|---|---|
| **Cause** | The user password expired and password change is prohibited by the administrator |

| | |
|---|---|
| **Solution** | Enable password change for the user (see p. **58**) |
| **Logon is prohibited by administrator** | |
| **Cause 1** | An administrator has blocked access for this user: the **Current user status** parameter is set to **Blocked** (see p. **58**). The computer is blocked when this user tries to log on |
| **Cause 2** | The number of failed logon attempts has exceeded **The maximum number of failed logon attempts** parameter (see p. **27**). Logon for this user is blocked |
| **Solution** | To allow this user to log on, set **Current user status** to **Active** (see p. **58**) |
| **Log is more than 90% full. Clear the log or enable event overwriting** | |
| **Cause** | The Sobol log is 90% full |
| **Solution** | The message appears when Sobol successfully booted, logon to the computer is blocked for all users except the administrator. Clear the log (see p. **70**) or enable events overwriting (see **Overwrite events** in Tab. 6 on p. **30**) |
| **User list integrity is violated. Only administrator is allowed to log on** | |
| **Cause** | While writing information to a user list, an error occurred due to technical reasons (for example, the computer was suddenly switched off), which led to Sobol nonvolatile memory change. As a result, current checksum of the user list calculated at Sobol start do not match the reference checksum. Logon is blocked for all users except the administrator |
| **Solution** | Restart the computer. If the error repeats, clear the user list (see p. **61**) and register users again (p. **54**). If the error remains, contact your Sobol vendor |
| **Log integrity is violated. Only administrator is allowed to log on** | |
| **Cause** | While writing events to the log, an error occurred due to technical reasons (for example, the computer was suddenly switched off), which led to Sobol nonvolatile memory change. As a result, the current checksum of the log calculated at the start of Sobol do not match the reference checksum. Logon is blocked for all users except the administrator |
| **Solution** | Clear the log (see p. **70**) |
| **Boot parameters are changed. Boot is denied** | |
| **Cause 1** | Boot parameters are changed in UEFI/BIOS Setup(e.g. boot order) |
| **Solution 1** | Perform one of the following actions:<br>• save a new boot configuration in Sobol (see p. **50**);<br>• return to the previous boot parameters in UEFI/BIOS Setup |
| **External drive is selected for boot. Boot is denied** | |
| **Cause** | A user tries to boot an OS from a removable device when it is prohibited |
| **Solution** | Perform one of the following actions:<br>• disconnect the removable device;<br>• allow the user to boot OS from the removable device by changing settings in the user's account. Turn off the **Deny booting from external drives** toggle (see p. **58**) |

## Warnings and information messages

The following Sobol messages notify about incorrect actions or inform about the current Sobol state.

**Note.** This section does not contain information about messages that describe further actions. Such messages and recommendations can be found in the respective procedures.

### Messages when entering password

| | |
|---|---|
| **Entered passwords do not match** | |
| **Cause** | When registering an administrator/a user or changing the administrator/user password, the confirmed password does not match the entered password |
| **Solution** | Enter the password again |
| **Minimum password length is ... characters** | |

| | |
|---|---|
| **Cause** | When registering an administrator/a user or changing the administrator/user password, the number of characters in the entered password is less than set in Minimum password length (see p. **31**) |
| **Solution** | Enter a password of an allowed length |
| **New password matches the old one** | |
| **Cause** | When changing an administrator/a user password, a new password matches the current one. The message appears if The minimum number of new characters is set to a value other than 0 (see p. **32**) |
| **Solution** | Enter the password different from the current one |
| **Not enough new characters compared to the old password** | |
| **Cause** | When changing an administrator/a user password, the number of new characters in a new password is less than the Minimum number of new characters (see p. **32**) |
| **Solution** | Enter the password that differs from the current one by the number of characters greater than or equal to the Minimum number of new characters (see p. **32**) |
| **Password must be at least N characters** | |
| **Cause** | When changing a user password, the number of characters in a new password is greater than the Minimum password length value, but differs from the current password by less number of characters than The minimum number of new characters (N in message).<br>The message does not appear if the user's password changed by an administrator |
| **Solution 1** | Suggest that the user set a password with at least N characters |
| **Solution 2** | Set The minimum number of new characters equal to or less than the Minimum password length value |

### Messages when registering user

| **A user with this name already exists** | |
|---|---|
| **Cause** | A new user name already exists in the Sobol user list |
| **Solution** | Change the user name and reenter it |
| **Security token is already registered on this computer** | |
| **Cause** | When registering a new user, a security token assigned to another user registered on this computer is presented |
| **Solution** | Assign a security token to the user again, presenting a security token that is not assigned to the other users of this computer |

### Messages when configuring the user schedule

| **The start date and/or time is greater than the finish one** | |
|---|---|
| **Cause** | During the configuration of the user schedule, the start date and/or time was specified greater than the finish one |
| **Solution** | Change the start date/time or the finish date/time |

### Log messages

| **Log is 70% full** | |
|---|---|
| **Cause** | The Sobol log is 70% full |
| **Solution** | The message appears to inform a user and an administrator. Continue your work |
| **Failed to export the log to file** | |
| **Cause** | The error occurred while exporting the log |
| **Solution** | Create a new file to export the log and try to export the log again (see p. **70**). If the error remains, contact the vendor technical support |
| **File not found** | |

| | |
|---|---|
| **Cause** | The file to export the log is not found |
| **Solution** | Create a new file to export the log and try to export the log again (see p. **70**) |

### Messages when using security tokens

| **This security token does not belong to current user** | |
|---|---|
| **Cause** | The presented security token does not belong to the current user |
| **Solution** | Present the current user's security token |
| **Invalid security token PIN ...** | |
| **Cause** | The entered PIN is incorrect |
| **Solution** | Enter the correct PIN |
| **Invalid password or security token** | |
| **Cause** | The presented security token is not registered in Sobol, or the entered password does not correspond to the presented security token |
| **Solution** | Present your security token, enter the correct password |

## Integrity check messages

When integrity check errors are detected, the following messages displayed in the tables below appear.

**Note.**

- If an integrity check error occurs when a user logs on to Sobol in hard integrity check mode, the computer is blocked.
- Messages may differ while working with the Sobol software and Built-in IC template management.

### Calculate checksums

| **Checksum calculation finished with error** | |
|---|---|
| **Cause** | An error occurred during calculation of IC object checksums |
| **Solution** | Find out and fix the cause of the error. Calculate checksums |

### Integrity check objects control

| **IC object contents are changed** | |
|---|---|
| **Cause** | The reference checksum of IC object does not match the current checksum calculated for this object |
| **Solution** | Find out and fix the cause of the IC contents change. Calculate checksums |
| **IC template contents are changed** | |
| **Cause** | The contents of IC templates are modified |
| **Solution** | If IC templates' modification is caused by adjusting a list of controlled objects via the IC template management software (built-in or auxiliary), calculate checksums.<br>In other cases, find out the cause of IC templates' modification, fix it, then calculate checksums |
| **IC templates or checksums are changed. The computer will be restarted** | |
| **Cause** | IC templates are changed or the reference checksums do not match the current ones |
| **Solution** | Restart your computers. The checksums will be recalculated |
| **Failed to save IC template settings** | |
| **Cause** | An error occurred while writing data to IC templates |
| **Solution** | If the templates were changed after the list of controlled objects was edited using either the Sobol software or Built-in template management, calculate checksums.<br>In other cases, determine the cause of the problem and calculate checksums |
| **Failed to read IC template settings** | |

| | |
|---|---|
| **Cause** | An error occurred while reading IC templates |
| **Solution** | Create new IC templates and calculate checksums |
| **Failed to read IC object** | |
| **Cause** | Calculation of checksums for this IC object failed. Getting access to read IC object failed |
| **Solution** | Find out and fix the cause of denied access to read IC object. Calculate checksums |
| **IC object not found** | |
| **Cause** | Specified IC object is not found |
| **Solution** | Find out and fix a cause of IC object not being found. If necessary, exclude this object from IC templates and calculate checksums |
| **IC templates are not found in standard Sobol folder** | |
| **Cause** | IC templates or the standard folders for the IC templates are not found.<br>The standard IC template folders:<br>• in Windows OS: in folder **\Sobol**;<br>• in Linux OS: in folders **/sobol** and **/boot/sobol** |
| **Solution** | Using the Sobol software:<br>• to create the IC templates, install/reinstall the Sobol software;<br>• to use the existing templates, specify the volume and the folder that contain the required IC template.<br>Using Built-in IC template management:<br>• to create the IC template, follow the procedure on p. 79;<br>• to use the existing templates, specify the volume and the folder that contain the required IC template |
| **IC templates are corrupted** | |
| **Cause** | The IC templates' structure is violated |
| **Solution** | Create new IC templates and calculate checksums |
| **Transaction log error on volume containing file with templates** | |
| **Transaction log error on volume containing checksum file** | |
| **Transaction log error on volume containing IC object** | |
| **Cause** | Transaction log may contain data about incomplete modifications |
| **Solution** | Boot the OS. When exiting the OS, close all file operations |
| **Unsupported IC template format** | |
| **Cause** | The IC template file format is not supported by Sobol |
| **Solution** | Contact your Sobol vendor |
| **Failed to save IC template backup** | |
| **Cause** | Sobol standard folder does not contain IC templates backup. But modifications saved in main IC templates |
| **Solution** | Enter the OS and create a file named **icheck_backup.json** in the Sobol standard folder (see p. 79) |

## Sobol test errors messages

If errors detected while testing Sobol performance (see p. 72), the following messages appear.

### RNG test errors

| | |
|---|---|
| **RNG channel 0 test finished with error ... times from ... attempts** | |
| **RNG channel 1 test finished with error ... times from ... attempts** | |
| **Cause** | The specified number of Sobol RNG tests failed. The test checks whether the generated number distribution is uniform |
| **Solution** | Repeat the RNG test. If the error remains, contact Security Code service department |

### Security token test error

| | |
|---|---|
| **Failed to read data from this security token** | |
| **Error while writing data: security token failure** | |
| **Cause** | An error occurred when writing/reading data to/from a security token. The security token or the reader may be damaged |
| **Solution** | Present another security token and repeat the test. If the test finished successfully, the security token/reader works properly. Format the previously presented security token and repeat the test. If the error remains, the security token may be damaged, contact Security Code technical support |
| **Error while reading security token: no device found** | |
| **Cause** | While performing all tests consecutively a security token was not presented during a security token test |
| **Solution** | Present the security token and repeat the test or check the security token separately |

## Events logged by Sobol

| Event | Event description |
|---|---|
| **Administrator changed password of user** | An administrator has changed the password of a user, which name is specified in the second column in a table of records |
| **Administrator logon** | An administrator has successfully logged on to the computer |
| **Administrator password was changed** | An administrator has changed their password to log on to the computer |
| **Administrator Secure ID was changed** | An administrator has successfully changed his or her security ID |
| **Checksum error in security token memory** | An error when testing security token IC is detected |
| **Checksums are not calculated** | An administrator have not set integrity check after Sobol initialization, checksums have not been calculated. If a user tries to log on in hard IC mode, his or her access is blocked |
| **Checksums were automatically recalculated** | Reference checksums are calculated on an external program request |
| **Checksums were recalculated** | Reference checksums are recalculated |
| **Error while exporting log** | The size of exported events is larger than the size of file for the log export |
| **External request error** | A request from Sobol nonvolatile memory, received from external programs, cannot be processed |
| **External requests were processed** | Requests from Sobol nonvolatile memory, received from external programs, are processed with no errors |
| **Failed to update IC key** | An IC key for calculating checksums of IC objects is not updated on specified time due to errors detected when checking objects' IC before an OS boots |
| **IC key was updated** | An IC key used to calculate checksums of IC objects is successfully updated |
| **IC were changed** | IC templates are modified |
| **Integrity check error** | Current checksums do not correspond to the reference checksums while checking objects' integrity before the OS boots |
| **Invalid password** | When logging on, you have presented a security token that assigned to a registered user, but have entered an incorrect password.<br>Security ID has been previously changed twice using another Sobol, and a user has never logged on this computer |

| Event | Event description |
|---|---|
| **Last logon time was adjusted** | The last time of a user's logon is modified according to the computer's time changed by an administrator |
| **Log was deleted** | An administrator cleared the Sobol log |
| **Log was exported** | Export of the Sobol log is completed |
| **Logon attempt limit was exceeded** | The number of failed logon attempts of this user has exceeded the maximum number |
| **Main boot drive parameters were changed** | The main boot disk of the computer is changed |
| **New user was added** | An administrator has added a new user to the user list |
| **Password configuration time/date was forward system time** | User password setting time or date outpaces the time or date set on the protected computer |
| **Request: Add user** | Inquiry to add a new user to the Sobol users' list is received from an external program and successfully processed |
| **Request: Delete user** | Inquiry to delete a user from the Sobol users' list received from an external program and successfully processed |
| **Resources were exported** | Resources are exported from an IC template |
| **Resources were imported** | Resources are imported into a IC template |
| **Security token was not registered** | When logging on, you have presented the security token that does not belong to any of users registered on this computer.<br>The password entered by an administrator is incorrect |
| **Sobol was switched to joint mode** | The Sobol joint mode is enabled by an administrator |
| **Sobol was switched to standalone mode** | The Sobol standalone mode is enabled by an administrator |
| **System date was set back** | When Sobol boots, forced system time setting back is detected |
| **System time and date were changed** | Time and date are changed by an administrator during Sobol operation |
| **User logon** | A user has successfully logged on to the computer |
| **User logon attempt at forbidden time** | A user has logged on to the computer at forbidden time |
| **User password was changed** | The user, which name is specified in the third column in a table of records, has successfully changed his or her password |
| **User Secure ID was changed** | The specified user has successfully changed his or her security ID |
| **User was blocked** | The user, whose logon is blocked, tries to log on |
| **User was deleted** | An administrator has deleted a user from the user list |
| **Watchdog timer test** | The watchdog timer test is successful |
| **Watchdog timer triggered** | Computer logon when the watchdog timer is not connected |

# Operation in joint mode

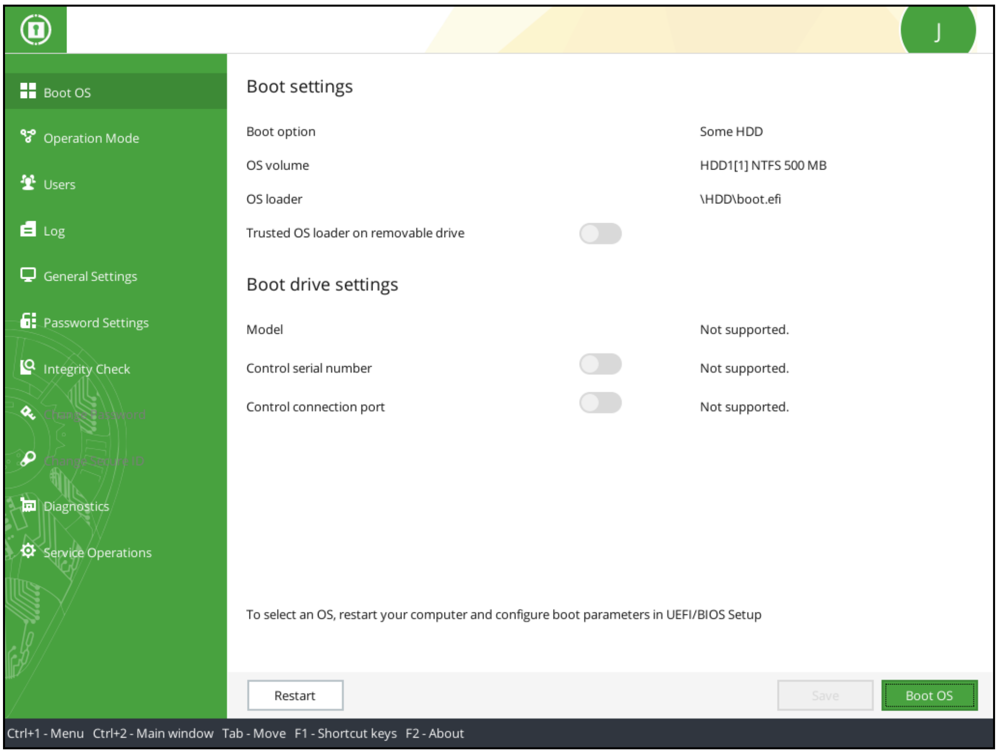
The joint mode allows you to use Sobol in tandem with other information security products (for example, Secret Net Studio). In this case, the product that operates in tandem with Sobol gets a part of control functions.

Note that when switching Sobol to joint mode:

- some general parameter management is limited;
- password parameters cannot be configured;
- user management is limited;
- password and Secure ID cannot be changed;
- IC mechanism management is limited;
- log management is limited.

## Administrator menu

In joint mode, the Sobol administrator menu is changed.



Boot settings

| | |
|---|---|
| Boot option | Some HDD |
| OS volume | HDD1[1] NTFS 500 MB |
| OS loader | \HDD\boot.efi |
| Trusted OS loader on removable drive ○ | |

Boot drive settings

| | |
|---|---|
| Model | Not supported. |
| Control serial number ○ | Not supported. |
| Control connection port ○ | Not supported. |

To select an OS, restart your computer and configure boot parameters in UEFI/BIOS Setup

## General settings

During the initialization, in the **Mathematical kernel** drop-down list, select **1989**.

In joint mode, you can not manage the following parameters:

- **Show statistics to user**. The parameter is **Off** by default, the information window does not appear when a user logs on;
- **The maximum number of failed logon attempts**;
- **Automatic logon timeout**;
- **Sound**.

You can find detailed information in Tab. 5 on p. **27**.

## Password settings

In joint mode, password settings cannot be configured by means of Sobol. Settings can be configured by the tools, that operate in tandem with Sobol.

To find detailed information about password settings, see Tab. 7 on p. **31**.

### User management

In joint mode, the administrator is only allowed to view the user list and not allowed to modify it in any way, including modifying account settings.

User settings are managed via an information security tool that operates in tandem with Sobol.

### Change password and Secure ID

In joint mode, neither the administrator nor users can change a password and a Secure ID using Sobol.

You can perform these operations via software that operates in tandem with Sobol.

### Integrity check and checksums calculation

In joint mode, the administrator can choose an IC template volume and a folder, as well as calculate the checksums of IC objects. The other IC settings are configured via an information security tool that operates in tandem with Sobol.

In joint mode, you cannot choose software for IC template management.

IC template management can be performed using Sobol software or an information security tool that operates in tandem with Sobol.

**Note.**

- In joint mode, Sobol software allows you to add the following objects to IC templates:
  - in a Windows family OS– PCI devices and SMBIOS;
  - in a Linux family OS – files and hard drive sectors.
- The order according to which you should install and use Sobol software is given in document [**1**].

### Work with log

In joint mode, the following functions are disabled when working with the log:

- log clearing;
- setting **Maximum log size** and **Audit frequency**.

To make use of these functions, use the information security tools that operate in tandem with Sobol.

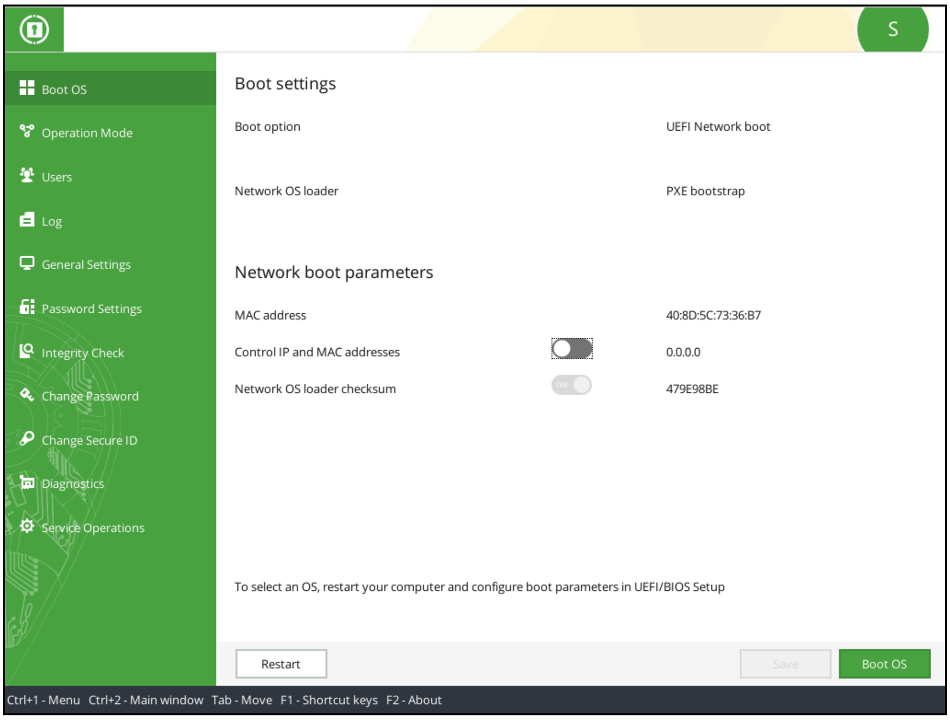
To find detailed information about Sobol log settings, see Tab. 6 on p. **30**.

### Specify identification numbers

In joint mode, the value of Secret Net Studio factory number is assigned to the parameter **Factory number**.

## The Sobol system settings in case of network boot

The **System Settings** window in case of network boot is displayed in the figure below.



Boot settings

Boot option: UEFI Network boot

Network OS loader: PXE bootstrap

Network boot parameters

MAC address: 40:8D:5C:73:36:B7

Control IP and MAC addresses: 0.0.0.0

Network OS loader checksum: 479E98BE

To select an OS, restart your computer and configure boot parameters in UEFI/BIOS Setup

The description of the settings is given in the table below.

**Boot option**

Displays the selected boot option.
To configure the parameter, restart your computer and configure boot parameters in UEFI/BIOS Setup

**Network OS loader**

Displays the name of the selected network OS loader.
To configure the parameter, restart a computer and configure boot parameters in UEFI/BIOS Setup

**MAC address**

Displays the MAC address of a boot network card.
To configure the parameter, restart a computer and configure boot parameters in UEFI/BIOS Setup

**Control IP and MAC addresses**

Displays the IP address of a boot network card, as well as allows controlling IP and MAC addresses thereof. Takes the following values:

- ON — control the MAC and IP addresses of a boot network card;
- OFF — do not control the MAC and IP addresses of a boot network card.

The default value is OFF

**Network OS loader checksum**

Displays the checksum of the selected network OS loader. The checksum is checked at Sobol start

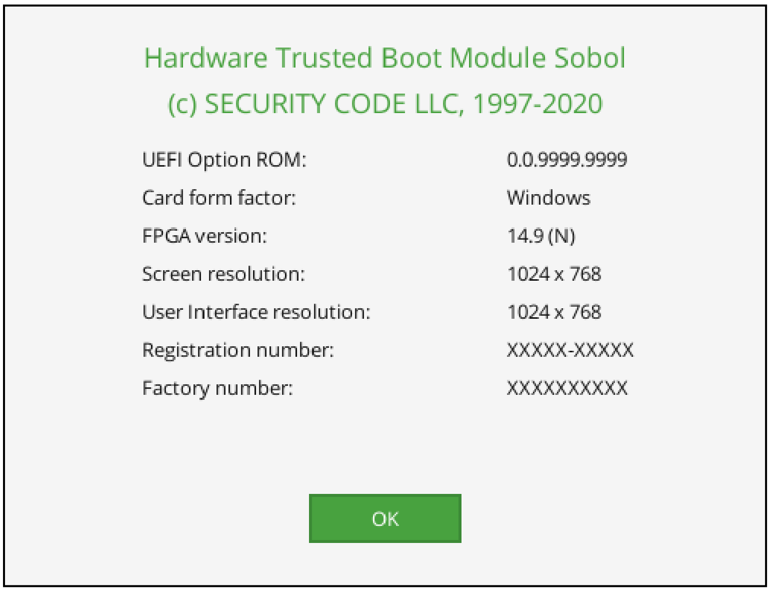
**System time and date**

Allows configuring the system time and date. Set the required time and date, if necessary

**Note.** This parameter is displayed only during Sobol initialization.

## Information window

To see Sobol information, press <F2>. A window appears as in the figure below.



Hardware Trusted Boot Module Sobol
(c) SECURITY CODE LLC, 1997-2020

| | |
|---|---|
| UEFI Option ROM: | 0.0.9999.9999 |
| Card form factor: | Windows |
| FPGA version: | 14.9 (N) |
| Screen resolution: | 1024 x 768 |
| User Interface resolution: | 1024 x 768 |
| Registration number: | XXXXX-XXXXX |
| Factory number: | XXXXXXXXXX |

The window contains the following information about Sobol:

| Parameter | Note |
|---|---|
| **UEFI Option ROM version** | The current version of UEFI Option ROM |
| **Card form factor** | Sobol card form factor |
| **FPGA version** | The current version of FPGA configuration |
| **Screen resolution** | The resolution of the screen |
| **User Interface resolution** | The resolution of the User Interface |
| **Registration number** | The registration number of your Sobol copy |
| **Factory number** | The factory number of your Sobol copy |

## Taking screenshots

While working with SobolSobol, you can take screenshots.

**To take screenshots:**

1. In the root directory of a removable device, create folder **sblscreenshots**.
2. Connect the removable device to a computer with SobolSobol.
3. To take a screenshot while working with Sobol, press <**F11**>.

   The screenshot is stored to the folder **sblscreenshots**.

# Documentation

1. Hardware Trusted Boot Module Sobol. Version 4. Administrator guide. Sobol Software.
2. Hardware Trusted Boot Module Sobol. Version 4. User guide. Basic Operations.