Terminal

BioSmart WTC2

Operating Manual
# CONTENTS

1. INTRODUCTION ................................................................................................................5

2. DESCRIPTION OF THE TERMINAL ...................................................................................6
   2.1 Front panel of the terminal ..........................................................................................7
   2.2 Indication and jumpers on the circuit board of the terminal ......................................8

3. OPERATION OF THE TERMINAL .....................................................................................9
   3.1 Connection ..................................................................................................................9
      3.1.1 Connecting power supply to the terminal using PoE ......................................... 11
      3.1.2 Connecting power supply to the terminal using power source ......................... 12
      3.1.3 Connecting the terminal to Ethernet ..................................................................13
      3.1.4 Connecting the lock to the terminal circuit board ............................................. 14
      3.1.5 Connecting the lock using BioSmart RCB ......................................................... 15
      3.1.6 Connecting the door sensor and control buttons .............................................. 16
      3.1.7 Connecting to external controller via Wiegand ................................................. 18
   3.2 Configuring and working with the terminal from BioSmart-Studio software ........... 19
   3.3 Configuring and working with the terminal using the keyboard ............................... 19
      3.3.1 “Settings” Menu ................................................................................................. 21
      3.3.2 “Employee” menu ............................................................................................. 33
      3.3.3 “Self-diagnosis” menu ...................................................................................... 37
Dear customers!

Thank you for purchasing our product. If you follow the below installation and operation rules, this device will serve you for many years.
1. INTRODUCTION

The present document describes operation of the «BioSmart WTC2» terminal.

Abbreviations used:
- **LCI** – liquid crystal indicator;
- **ACS** – access control system;
- **RCB** – relay control block;
- **OS** – operating system.
2. DESCRIPTION OF THE TERMINAL

The “BioSmart WTC2” terminal is designed to work as a part of the biometrical access control system BioSmart. The terminal allows for time management by identifying employees using fingerprints or contactless RFID cards, as well as provides managing of access control.

In the upper part of the screen there is a status panel displaying the following symbols:

- **Operating mode indication**
  - The blinking blue symbol signifies the terminal is ready for identification;
  - The blinking yellow symbol means the administration is in progress and identification is temporarily unavailable.

- **Output relay state**
  - Closed;
  - Opened.

- **BioSmart-Studio server connection status**
  - Connection is established;
  - No connection.

- **Other indicators**
  - Connection with the identification server is established;
  - The free pass mode is activated;
  - The terminal is blocked;
  - An error occurred during the operation of the terminal (the error state is displayed in the “Info” menu of the terminal).
2.1 Front panel of the terminal

The front panel of the BioSmart WTC2 terminal includes:

- **Serial number of the device**
- **Current date and time and the day of the week**
- **Menu** (In the “Menu” you can configure the device)
- **Info** (The menu displays all crucial information about the device state)
- **LCI** (Contactless card scanner)
- **Fingerprint scanner**
- **Keyboard**

**Screen navigation**

is performed using the keyboard buttons:

- **2** – go up in a list;
- **8** – go down in a list;
- **4** – go left or switch from a list to functional buttons. In the “Users” menu is used to scroll one page up;
- **6** – go right or switch from a list to functional buttons. In the “Users” menu is used to scroll one page down;
- **C** – either gets you back to a previous menu, or deletes the last entered symbol.
- **–** selects and confirms selection. All numeric settings are also typed using the keyboard.

*Figure 1. Front panel of the BioSmart WTC2 terminal*
2.2 Indication and jumpers on the circuit board of the terminal

The **RUN** LED shows if the fingerprint scanner circuit board is working. Normally, it should blink once in 20 seconds.

LED lights on the Ethernet connector display physical connection (Link, green light) and network activity (Activity, red light).

The **USB** LED lights up when the device is connected to a computer via the USB interface as long as the device driver is installed and the equipment is successfully identified by the OS.

The **POE** LED indicates POE power supply.

The **IPRST** jumper allows resetting parameters to the factory values. To do this, close contacts of the jumper and wait until LINK and Activity LEDs are off. After that, disconnect the jumper.

The **BOOT** jumper is intended to switch the terminal to the bootloader mode. This mode allows to restore operation of the terminal in case the built-in firmware is damaged.

To switch to the bootloader mode:
1. Turn off the power supply of the terminal;
2. Close the **BOOT** jumper;
3. Turn on the power supply of the terminal.
4. Wait for 2 seconds and disconnect the jumper.

There should be the “BOOT” message on the display of the terminal.
3. OPERATION OF THE TERMINAL

3.1 Connection

The layout of the terminal circuit board is shown on the Figure 2. The list of circuit board contacts is summarized into Table 1.

Figure 2. Layout of the terminal circuit board
**Table 1. Terminal circuit board contacts**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>485+</td>
<td>+ of the RS485 RCB connection interface</td>
<td>RCB +485 contact</td>
</tr>
<tr>
<td>485-</td>
<td>- of the RS485 RCB connection interface</td>
<td>RCB -485 contact</td>
</tr>
<tr>
<td>IN</td>
<td>Discrete input</td>
<td>Door sensor output, relay control key</td>
</tr>
<tr>
<td>+IN</td>
<td>+12V output for discrete input</td>
<td>Relay control key</td>
</tr>
<tr>
<td>WO0</td>
<td>DATA0 output of the Wiegand interface</td>
<td>DATA0 input of the third-party controller Wiegand interface</td>
</tr>
<tr>
<td>WO1</td>
<td>DATA1 output of the Wiegand interface</td>
<td>DATA1 input of the third-party controller Wiegand interface</td>
</tr>
<tr>
<td>REL</td>
<td>Output of the normally opened contact #1 of the relay (DC 1A, 12V)</td>
<td>Control input of the actuating device</td>
</tr>
<tr>
<td>REL</td>
<td>Output of the normally opened contact #2 of the relay (DC 1A, 12V)</td>
<td>Power supply output of the actuating device</td>
</tr>
<tr>
<td>+12 V</td>
<td>Power supply, +12V</td>
<td>“+” of the power supply 12V</td>
</tr>
<tr>
<td>GND</td>
<td>Power supply, ground</td>
<td>Ground of 12V power supply</td>
</tr>
<tr>
<td>USB</td>
<td>Mini-USB jack to configure the terminal via the BioSmart Manager software</td>
<td>USB port of the PC</td>
</tr>
<tr>
<td>Ethernet</td>
<td>RJ45(8P8C) Ethernet connector</td>
<td>Network device</td>
</tr>
<tr>
<td>DC IN</td>
<td>5.5 x 2.5 socket for pin power supply connector. Central pin +12V.</td>
<td>Power supply 12VDC</td>
</tr>
</tbody>
</table>

**Cable types to connect the terminal are listed in Table 2.**

**Table 2. Cable types used:**

<table>
<thead>
<tr>
<th>Cable #</th>
<th>Cable connection</th>
<th>Max. length</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ethernet (IEEE 802.3) - terminal</td>
<td>100 m</td>
<td>Four Category 5 twisted pairs with section at least 0.2 mm²</td>
</tr>
<tr>
<td>2</td>
<td>Power supply - terminal</td>
<td>50 m</td>
<td>Duplex cable with section at least 0.75 mm²</td>
</tr>
<tr>
<td>3</td>
<td>Terminal – lock, RCB - lock</td>
<td>20 m</td>
<td>Duplex cable with section at least 0.75 mm²</td>
</tr>
<tr>
<td>4</td>
<td>Terminal – RCB BioSmart</td>
<td>20 m</td>
<td>Four Category 5 twisted pairs with section at least 0.2 mm²</td>
</tr>
<tr>
<td>5</td>
<td>Terminal, IN, IN+ contacts – external devices.</td>
<td>10 m</td>
<td>CQR-6 or RAMCRO-6 cables</td>
</tr>
<tr>
<td>6</td>
<td>Terminal, WO0, WO1 contacts – external devices.</td>
<td>60 m</td>
<td>Four Category 5 twisted pairs with section at least 0.2 mm²</td>
</tr>
</tbody>
</table>
3.1.1 Connecting power supply to the terminal using PoE

PoE (Power over Ethernet) is a technology to power up a remote device through the same twisted pair Ethernet cable as used for data transmission. According to the IEEE 802.3af-2003 standard the technology provides active current at rated voltage of 48V (min = 36V, max = 57V) and maximum current of 400mA for peak power of 15W, through two pairs of conductors in one four-pair cable. Power supply with this technology requires PSE (Power Sourcing Equipment).

Connection must be made as shown on Figure 3.

**Connection:**
- Use cable #1 (see Table 2) to connect the terminal via PoE. Connect one end of the cable to the “DATA INPUT” connector on the PSE device, and connect the other end of the cable to a computer, a switcher or a router.
- Use cable #1 (see Table 2) to connect the PSE device (VDC + DATA OUTPUT connector) to the terminal (the Ethernet connector);
- Power up the PSE device.

![Figure 3. Connecting using PoE](image-url)
3.1.2 Connecting power supply to the terminal using power source

Connection of an external power source to the terminal must be made in accordance with connection diagrams shown on Figure 4. Use cable #2 for connection (see Table 2).

Figure 4. Power supply connection using the terminal bus
3.1.3 Connecting the terminal to Ethernet

Connection to Ethernet must be made as shown on Figure 5.

Crimping of the cable cap must be done in compliance with the TIA/EIA-568-B standard.
3.1.4 Connecting the lock to the terminal circuit board

Connection of the electromechanical lock to the terminal must be made as shown on Figure 6. Use cable #3 for connection (see Table 2).

Figure 6. Connecting the electromechanical lock
3.1.5 Connecting the lock using BioSmart RCB

Connection of the electromechanical lock via the BioSmart RCB must be made in accordance with the diagram shown on Figure 7. Use cables #3 and #4 for connection (see Table 2).

Connection and configuration of RCB are described thoroughly in the BioSmart RCB operation manual. You can find all necessary information at www.bio-smart, the “Technical support” section.

Figure 7. Connecting the electromechanical lock using RCB
3.1.6 Connecting the door sensor and control buttons

The door sensor and the room exit button can be connected directly to the on-board discrete input BioSmart WTC2 (Figure 8).

Figure 8. Connecting the door sensor or the button to the on-board discrete input

Use cable #5 for connection (see Table 2).
If access control implies usage of both the door sensor and the room exit button, the connection must be made using BioSmart RCB (Figure 9).

Connection and configuration of BioSmart RCB are described thoroughly in the BioSmart RCB operation manual. You can find all necessary information at [www.bio-smart](http://www.bio-smart), the “Technical support” section.

![Figure 9. Connecting the door sensor and the button using BioSmart RCB](image)

Use cables #4 and #5 for connection (see Table 2).
3.1.7 Connecting to external controller via Wiegand

Connection of the terminal to an external ACS controller via the Wiegand interface must be made as shown on Figure 10.

Figure 10. Connecting the terminal to an external controller via the Wiegand interface

Use cable #6 for connection (see Table 2).
3.2 Configuring and working with the terminal from BioSmart-Studio software

The detailed description of work with the BioSmart-WTC2 terminal from BioSmart-Studio software can be found in BioSmart-Studio v5 Administrator manual, section 9.5.10.

3.3 Configuring and working with the terminal using the keyboard

Screen menu navigation is performed with keys on the keyboard (see Figure 2). You can find the description of navigation keys in the section 3.1 of the present manual. From there, the phrase “go to the menu ***” will omit the detailed step-by-step description of this process.

⚠️ **Factory setting of the administrator password is the empty password.**

After you enter the configuration mode for the first time, it is recommended that you set a new password to prevent unauthorized access to settings of the terminal in the future.
Figure 14 shows typical screens of the terminal in various work modes.

Figure 14. Standard screens

Enter the main menu of the terminal using navigation buttons and select “Settings” (Figure 15)

Figure 15. Selecting the “Settings” menu
3.3.1 “Settings” menu

3.3.1.1 “System”

Select the “System” menu using navigation buttons (Figure 16).

Figure 16. Selecting the system settings

This menu allows configuring system parameters of the terminal (Figure 17).

Figure 17. System settings
3.3.1.1 Identifier type

- **Fingerprint or card** – identification mode using fingerprints or plastic cards is asserted, the “Successful identification” event is produced and recorded in the event log.

- **Card + Fingerprint** – the card is verified using the fingerprint. At first, a card must be placed to the card reader. Then, during 10 seconds, a finger must be placed to the fingerprint scanner.

- **Code + Fingerprint** – the code is verified using the fingerprint. At first, a four-digit code must be entered on the keyboard. Then, during 10 seconds, a finger must be placed to the fingerprint scanner.

- **Mifare card fingerprint** – this mode verifies Mifare smart-card data using the fingerprint. Fingerprints are preliminarily recorded to the Mifare smart-card. At first, a Mifare Smart-card must be placed to the card reader. Then, during 10 seconds, a finger must be placed to the fingerprint scanner.

3.3.1.1.2 Operation mode

- **Standalone** – fingerprints are stored in the own memory of the terminal.

- **Server** – fingerprints are stored on the external biometrical identification server. No fingerprints are stored in the local memory of the terminal. In this mode, comparison of biometric data is performed by the external server which results in larger volumes of stored fingerprints and faster identification.

3.3.1.1.3 Pass direction

Sets pass direction that triggers the working time recording (entry, exit). If the terminal is to be used for passing in both directions, set the option to the “Not set” value.

3.3.1.1.4 Entry/exit with buttons

Keyboard buttons “1” (Entry) and “3” (Exit) set the direction of the pass for working time recording. When entering/exiting using buttons, the fingerprint scanner and the card reader are turned off in the standby mode. At first, press the appropriate button, “1” (Entry) or “3” (Exit), then put a finger or a card to the scanner.
3.3.1.1.5 Identification confirmation

Allows confirming identification from the BioSmart Studio software in the “Monitoring” window after the “Open” button is clicked. This mode allows a system administrator to confirm passage of an employee manually.

3.3.1.1.6 Scanner type

This parameter cannot be edited. It shows the type of the fingerprint scanner used.

3.3.1.1.7 Recognition quality (FAR)

FAR (False authorization rate) is a probability that the biometrical identification system mistakenly authorizes the fingerprint of a non-registered employee. This option is only available for the “Standalone” mode (see 3.3.1.1.2). In the “Server” mode, this option is set in the identification server settings. Possible values are between 1/10 000 and 1/100 000 000. The Table 3 below show FAR values depending on the number of fingerprints in the database. We recommend setting the “automatic mode” here. In this case, the FAR value changes automatically to meet the actual number of fingerprints in the database.

<table>
<thead>
<tr>
<th>Automatic mode:</th>
<th>Identification 1 to X</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X=(1~9)</td>
</tr>
<tr>
<td>Normal mode</td>
<td>1/10 000</td>
</tr>
<tr>
<td>Strict mode</td>
<td>1/100 000</td>
</tr>
<tr>
<td>Strictest mode</td>
<td>1/1 000 000</td>
</tr>
</tbody>
</table>
3.3.1.1.8 Fingerprint rotation angle

This parameter sets the maximum allowed for successful identification fingerprint rotation angle from the axis, in degrees. Increasing the angle also increases both probability of successful identification and identification time. The recommended value is 30°.

3.3.1.1.9 Recognition speed

This parameter sets the fingerprint recognition algorithm. The faster the algorithm works, the higher is the false rejection rate (FRR). At the same time, processing speed significantly improves in larger databases.

The recommended value is Auto. In this mode the speed is set automatically depending on the number of fingerprint templates in the database of the terminal.

3.3.1.1.10 Sensor sensitivity

This option defines sensor sensibility while scanning fingerprints. Increased sensibility allows capturing low-quality fingerprints, but also increases false rejection rate (FRR) and leads to possible attempts of the scanner to scan grease marks left from fingers when exposed to direct light.

3.3.1.1.11 Hack attempts

This parameter defines the number of consequential unsuccessful identification attempts for any identifier. When the number of allowed attempts depletes, the controller is blocked for the time specified in “Blocking timeout”.

3.3.1.1.12 Blocking timeout

This parameter specifies time in seconds the terminal stays blocked after a hack attempt. The “Module is blocked. Fingerprint/card hack attempt” message is recorded to the event log.

3.3.1.1.13 Case tamper control

This option controls if the case was tampered. If the case of the terminal was tampered during operation, an alarm event “case tamper” is produced. Sound and visual indication can be configured in “IO” parameters.
3.3.1.1.14 Built-in card reader
This parameter configures the operation of the built-in card reader (on/off).

3.3.1.1.15 Administrator password
Sets the numeric password to access the settings menu of the terminal.

3.3.1.1.16 Card code length
The parameter sets the code length of the built-in card reader. Can be set to 24 or 32 bits, corresponding to Wiegand 26 and Wiegand 32 standards.

3.3.1.1.17 Fingerprint-free pass
In the verification mode (card + fingerprint) the identification uses the card data only as long as there are no fingerprints of the employee in the database. If the database contains the card ID and the fingerprint, both identifiers are required to pass.

3.3.1.1.18 Manual module block
This parameter allows blocking the module for card and fingerprint identification. Unblocking is performed manually then.

3.3.1.1.19 Host connection analysis
This parameter checks network connection to the server. If there is no connection with the server for 24 hours, the terminal is blocked. The terminal is unblocked automatically when the network connection is restored.

3.3.1.2 “Access Control”
Go to the “Access control” menu using navigation buttons. This menu allows configuring operation parameters of various actuating devices, as well as parameters of discrete inputs of the terminal.
3.3.1.2.1 Output relay

3.3.1.2.1.1 Relay
This parameter allows choosing the type of the output relay that should actuate on the “Successful identification” event. The dropdown list contains the following elements:

- On-board relay – on the “Successful identification” event, the on-board relay actuates (normally opened contacts REL of the terminal);
- RCB Relay 1 - on the “Successful identification” event, the relay #1 of the ACB actuates;
- Реле 2 БУР - on the “Successful identification” event, the relay #2 of the ACB actuates.

3.3.1.2.1.2 Timer
This parameter sets the time the output relay stays in the active state, in milliseconds.

3.3.1.2.1.3 Trigger mode
Makes the output relay change its state (open/closed) on every “successful identification” event. After the terminal is reset or power supply is restored, the last state of the output relay is preserved.

3.3.1.2.1.4 Software blocking
This parameter sets the operation mode when the “Open” command from the “Monitoring” window of the BioSmart-Studio software is received. The dropdown list of the setting contains the following elements:

- Manual – when the “Open” command from the “Monitoring” window of the software comes to the terminal, the output relay actuates and stays active until the “Close” command from the “Monitoring” window of the BioSmart-studio software comes;
- By timer – when the “Open” command from the “Monitoring” window of the software comes to the terminal, the output relay actuates and stays active for the time specified in the “Output relay timer” parameter.
3.3.1.2.2 Relay control button

3.3.1.2.2.1 Input

The parameter sets the number of the discrete input to connect the relay control button. The dropdown list of the parameter contains the following elements:

- Disabled – a control button is not connected;
- On-board input – the control button is connected to the on-board discrete input of the terminal (IN, +IN contacts);
- RCB Input #1,2,3,4 – the control button is connected to the discrete input RCB #1,2,3,4 respectively.

3.3.1.2.2.2 Relay

The parameter sets the type of the output relay controlled by the button. Can be activated using the “Exit by button” event in the system. The dropdown list of the parameter contains the following elements:

- On-board relay – when the “Exit by button” event occurs, the on-board relay actuates (normally opened contacts REL of the terminal);
- ACB relay 1 – when the “Exit by button” event occurs, the ACB relay #1;
- ACB relay 2 – when the “Exit by button” event occurs, the ACB relay #2.

3.3.1.2.2.3 Timer

The parameter sets the time the output relay stays in the active state when the “Exit by button” event occurs, in milliseconds.
3.3.1.2.3 Door sensor

3.3.1.2.3.1 Input

This parameter defines the discrete input of the terminal the door sensor is connected to. The dropdown list of the parameter contains the following elements:

- Disabled – a door sensor is not connected;
- On-board input – the door sensor is connected to the on-board discrete input of the terminal (IN, +IN contacts);
- RCB Input #1,2,3,4 – the door sensor is connected to the discrete input RCB #1,2,3,4 respectively.

3.3.1.2.3.2 Active state

This parameter sets the signal level at the discrete input during door sensor operation. Respectively, high (bridging the IN, +IN contacts of the terminal, applying +12V to IN1,2,3,4 RCB inputs) and low (opening the IN, +IN contacts of the terminal, removing +12V from IN1,2,3,4 RCB inputs).

3.3.1.2.3.3 Unblocking relay

The parameter sets the unblocking mode of the output relay upon the “Successful identification” event or the “Exit by button” event when the signal from the door sensor comes. The dropdown list of the parameter contains the following elements:

- On door open – the relay turns off on rising edge of the door sensor signal;
- On door close – the relay turns off on trailing edge of the door sensor signal.

3.3.1.2.3.4 Consider passage

This parameter sets the employee passage confirmation mode. When on, if an employee was successfully identified and the signal from the door sensor was received, the “Successful identification” event is recorded by the BioSmart system. If there is no signal from the door sensor after successful identification of an employee, the “Passage not registered” event is produced. The identification of the employee is not recorded by the BioSmart system.
3.3.1.2.3.5 Consider door hack
The parameter controls door state. The terminal produces the “Door hack” alarm event when the signal from the door sensor comes while the door is in the closed state.

3.3.1.3 “Integration” menu
Go to the “Integration” menu using navigation keys. In this menu you can configure third-party equipment, Wiegand output and so on.

3.3.1.3.1 Additional equipment
This parameter defines the type of a device connected via the RS485 interface to the terminal (contacts: «+», «−» 485). The dropdown list of the parameter contains the following elements:

- Disabled – additional equipment is not used;
- BioSmart RCB – the terminal works with a “Relay control block”.

3.3.1.3.2 Wiegand output
The parameter sets the type of the Wiegand output interface protocol of the terminal (contacts WO0 and WO1). The parameter is used to integrate the system to third-party ACS. The dropdown list of the parameter contains the following elements:

- Disabled – there are no third-party devices connected to the Wiegand output of the terminal;
- Wiegand-26 (W/P) – a third-party ACS controller is connected to the Wiegand output of the terminal; the Wiegand 26 parity control bits protocol is used;
- Wiegand-32 – a third-party ACS controller is connected to the Wiegand output of the terminal; the Wiegand 32 protocol is used.
3.3.1.3.3 Bypass mode
This parameter allows sending the ID of a card through the output Wiegand interface of the terminal when the given ID of a card is absent in the database. The mode is used to provide passage using cards and bypassing the BioSmart system when the third-party access control system is used.

3.3.1.3.4 Bypass timer
Sets the time in seconds to wait before the ID of the card is sent to the Weigand output of the terminal in the “Bypass” mode.

3.3.1.3.5 RCB address
Sets a network address for the relay control block. The terminal must have a unique address in the range between 0 and 3.

3.3.1.4 “Network” menu
Go to the “Network” menu using navigation keys. This menu displays current network settings of the terminal and allows editing them.

3.3.1.4.1 New IP address
Defines the IP address of the terminal. Factory value of the IP address is: 172.25.110.71.

3.3.1.4.2 New mask
Sets the network mask of the terminal. Factory value of the mask is: 255.255.0.0.

3.3.1.4.3 New gateway
Sets the gateway IP address of the terminal. Factory value of the gateway IP address is: 172.025.110.8.
3.3.1.4.4 IP address of the identification server
Sets the IP address of the identification server. Must be set if the “Server” identification mode is used.

3.3.1.5 “Screen” menu
Go to the “Screen” menu using navigation keys. This menu allows configuring information displayed on the screen, to change the background of the screen, to choose language and so on.

3.3.1.5.1 Language
Choose between Russian and English.

3.3.1.5.2 Keyboard blocking
Sets the keyboard blocking mode. When the keyboard is blocked, sequential pressing of “7” and “9” keys unblocks it for a while, and the display shows “Menu” and “Info” buttons.

3.3.1.5.3 Screen background
Allows choosing screen background:

- Standard;
- Standard, Ent/Ex;
- Custom.

A custom background can be uploaded to the terminal using the BioSmart Manager utility.
3.3.1.5.4 Standby mode

3.3.1.5.4.1 Screen off timer
Sets time in minutes after which the display of the terminal turns off. Pressing any key on the keyboard turns on the screen temporarily. When the specified times expires, the screen turns off again. If the value is “0”, the display is always on.

3.3.1.5.4.2 Turn on screen at given time
Turns on the display of the terminal at a certain time.

3.3.1.5.4.3 Time to turn on the screen, hh:mm
Sets the time the display of the terminal should on, in hours and minutes.

3.3.1.5.5 Display on the screen
Sets the type of information shown in the upper right corner of the screen: serial number of the terminal, passage direction.
3.3.2 “Employee” menu

Allows registering and deleting fingerprints and card identifiers for employees previously recorded by means of BioSmart-Studio v5. Select an employee from the list (Figure 18)

![Employee list](image1)

Figure 18. Employee list

3.3.2.1 Adding new fingerprints

Select “Update fingerprints” (Figure 19).

![Selection](image2)

Figure 19. Selection
You should hear short sound signals and see a message saying “Put the finger” (Figure 20).

Figure 20. Registering a fingerprint

Put the finger to the scanner as shown on Figure 21:

Figure 21. Correct placement of a finger to the fingerprint scanner

Finger cushion should fit tightly to the scanner surface. The contact area of the finger cushion with the scanner should be as large as possible, preferably covering the entire surface of the scanner.

The angle between the attached finger and the scanner surface must be near to zero.

If registration of the fingerprint is successful, you should hear a long sound signal. The screen displays the “Remove the finger” message.
Remove the finger. You should hear short sound signals, and the displays should say “Put the finger again” (Figure 22).

![Figure 22. Fingerprint registration continues](image)

Put the same finger to the scanner one more time. If the registration was successful, you should hear a long sound again. The screen shows the “Fingerprint saved” message, the name of the employee and the number of registered fingerprints (Figure 23).

![Figure 23. Fingerprint registration. Final stage](image)
3.3.2.2 Adding card ID

Select “Specify the card ID”. Short sounds are played, and the display shows “Put the card” (Figure 24).

Put the card to the card reader. If card ID registration was successful, a long sound rings, and the screen displays the “Card ID is set” message and the name of the employee (Figure 25).

Figure 24. Card ID registration process

Figure 25. Card ID registration process. Final stage
3.3.3 “Self-diagnosis” menu

Allows running a self-test of main elements of the terminal. Select “Self-diagnosis” (Figure 26).

Upon finishing of the self-diagnosis process, the following message appears on the screen (Figure 27).

Figure 26. “Self-diagnosis” menu selection

Figure 27. Self-diagnosis results