Guide for configuring and working with the BioSmart integration module

ACFA PSIM 1.5

Last update 16/07/2025

Table of Contents

1 List of terms used in the Guide for configuring and working with the BioSmart integration module 5
2 Introduction into the Guide for configuring and working with the BioSmart integration module 6
2.1 Purpose of the document 6
2.2 General information about the BioSmart integration module 6
3 Supported hardware and licensing of the BioSmart module 7
4 Configuring the BioSmart integration module 9
4.1 Configuring the BioSmart parent object 9
4.2 Configuring biometric identification Server 9
4.3 Configuring the connection of the BioSmart controller or terminal to the ACFA PSIM server 10
4.4 Configuring interaction of the BioSmart integration module with the Access Manager module and Time and Attendance subsystem 12
4.4.1 Interaction with the Access Manager module 12
4.4.2 Interaction with the Time&Attendance subsystem 13
4.5 Managing the configuration of the BioSmart controllers/terminals 14
4.5.1 Managing the configuration of the BioSmart UniPass and Biosmart PV-WTC controllers 14
4.5.2 Managing the configuration of the BioSmart 4 and BioSmart 5M controllers 15
4.5.3 Managing the configuration of the BioSmart UniPass Pro and BioSmart UniPass Pro 2 controllers 17
4.5.4 Managing the configuration of the BioSmart Prox-E controller 18
4.5.5 Managing the configuration of the BioSmart Quasar terminal 20
4.5.6 Managing the configuration of the BioSmart Quasar 7 terminal 22
Managing the terminal configuration 22
Creating a user face template manually 23
4.5.7 Managing the configuration of the Biosmart KeyPass controller 23
4.6 Configuring the BioSmart PV-WTC terminal 24
4.7 Configuring the BioSmart 4 controller 26
4.7.1 Configuring the relay control button and access sensor 27
Configuring the relay control button 27
Configuring the access sensor 27

4.7.2 Configuring the number of user fingerprint templates ... 28
4.7.3 Configuring working with external hardware and exit relay ... 29
Configuring working with external hardware ... 29
Configuring working with exit relay ... 30
4.7.4 Setting up the BioSmart 4 network configuration ... 30
4.7.5 Configuring system parameters of the BioSmart 4 controller ... 31
4.7.6 Configuring operating scenarios for actuating devices of the BioSmart 4 controller ... 32
4.8 Setting up the BioSmart UniPass controller ... 34
4.8.1 Configuring the BioSmart UniPass controller ... 34
4.8.2 Configuring inputs, outputs and relays of the BioSmart UniPass controller ... 36
4.9 Setting up the BioSmart Prox-E controller ... 37
4.9.1 Setting up the BioSmart Prox-E network configuration ... 38
4.9.2 Configuring system parameters of the BioSmart Prox-E controller ... 38
4.9.3 Configuring the Multi-access mode of the BioSmart Prox-E controller ... 40
4.9.4 Configuring the Gateway mode of the BioSmart Prox-E controller ... 40
4.9.5 Configuring the Maintenance mode of the BioSmart Prox-E controller ... 41
4.9.6 Configuring the relay of the BioSmart Prox-E controller ... 41
4.9.7 Configuring the BioSmart Mini reader ... 42
General settings ... 42
Control ... 42
The Basic settings tab ... 43
The Biosmart Mini tab ... 44
4.9.8 Configuring the RFID reader ... 44
General settings ... 45
Control ... 45
The Basic settings tab ... 46
4.10 Setting up the BioSmart Quasar terminal ... 47
4.10.1 The Basic settings tab ... 47
4.10.2 The Advanced settings tab ... 48
4.10.3 The Wiegand 0 and Wiegand 1 tabs ... 48
4.11 Setting up the BioSmart UniPass Pro and BioSmart UniPass Pro 2 controllers ... 49
4.12 Configuring the BioSmart control readers ... 50
4.13 Configuring the BioSmart 5M controller ... 51
4.13.1 Configuring the number of fingerprint templates of the users of the BioSmart 5M controller ... 52

4.13.2 Configuring operating scenarios for actuating devices of the BioSmart 5M controller 53
4.13.3 General settings of the BioSmart 5M controller 55
The General 1 tab 56
The General 2 tab 57
4.13.4 Configuring working with external hardware and exit relay of the BioSmart 5M controller 57
Configuring working with external hardware 58
Configuring working with exit relay 58
4.13.5 Configuring discrete entrance of the BioSmart 5M controller 59
4.13.6 Network settings of the BioSmart 5M controller 60
5 Working with the BioSmart integration module 61
5.1 General information about working with the BioSmart integration module 61
5.2 Adding the BioSmart biometric parameters 61
5.2.1 Adding biometric parameters using the Biosmart PV-WTC terminal 61
5.2.2 Adding biometric parameters using the DCR-PV USB control reader 62
5.3 Managing the BioSmart terminals and controllers 65
5.4 Managing inputs, outputs and relays of the BioSmart UniPass controller and relay of the BioSmart 5M controller 66
5.5 Managing the BioSmart readers 67
5.6 Example of a configured macro of the BioSmart integration module 68

1 List of terms used in the Guide for configuring and working with the BioSmart integration module

BioSmart controller is a device used to work as part of a network access control and management system based on *BioSmart* ACS and *ACFA PSIM*.

BioSmart terminal is a device that combines the functions of a controller and a biometric reader, used to work as part of a network access control and management system based on *BioSmart* ACS and *ACFA PSIM*.

ACFA PSIM Server is a computer with *ACFA PSIM* installed and connected to the *BioSmart* controller.

Reader (control reader) is a device used to connect to the *BioSmart* controller and recognize users by the pattern of veins and capillaries on the palm. The reader can be used to read information from RFID cards as well.

Template is an image from the reader that contains biometric information about the location of veins and capillaries in the user's palm and used to identify them.

Biometric information (biometric data or biometrics) is a graphic representation of the pattern of veins and capillaries on the user's palm.

2 Introduction into the Guide for configuring and working with the BioSmart integration module

On the page:

- Purpose of the document
- General information about the BioSmart integration module

2.1 Purpose of the document

The *Guide for configuring and working with the BioSmart integration module* is a reference and informational guide intended for *BioSmart* configuration specialists. This module is a part of *ACFA PSIM*.

The Guide provides:

1. General information about the *BioSmart* module.
2. Configuring the *BioSmart* module.
3. Working with the *BioSmart* module.

2.2 General information about the BioSmart integration module

The *BioSmart* module is a component of the ACS implemented on the basis of *ACFA PSIM* and used to perform the following functions:

1. Configuring the *BioSmart* controllers and connected readers, as well as the *BioSmart* terminals.
2. Ensuring interaction between *BioSmart* ACS and *ACFA PSIM* (collecting biometric information, controlling access).

Note

Detailed information about *BioSmart* devices is given in the official documentation (manufacturer is Prosoft-Biometrics company).

Before configuring the *BioSmart* integration module, do the following:

1. Install the *BioSmart* hardware on the protected facility (see the official installation guide for the *BioSmart* controller and *BioSmart* terminal).
2. Connect the *BioSmart* ACS to the *ACFA PSIM* Server.

3 Supported hardware and licensing of the BioSmart module

Manufacturer	BioSmart LLC Address: 194A Volgogradskaya str., Ekaterinburg, 620102 Phone: 8-804-333-99-63 Website: https://www.biosmart-tech.com/ Email: info@bio-smart.ru
Integration type	SDK
Hardware connection	USB, Ethernet

Supported hardware

Hardware	Function
BioSmart UniPass/BioSmart UniPass-EX	Standalone access controller
BioSmart UniPass Pro	Standalone access controller
BioSmart UniPass Pro 2	Standalone access controller
BioSmart Prox-E	Standalone access controller
BioSmart BS 4	Standalone access controller
BioSmart 5M-O	Biometric access controller
BioSmart 5M-E	Biometric access controller
BioSmart KeyPass	Controller
BioSmart PV-WM	Reader. Works in tandem with access controllers
USB DCR-PV	Control reader
FS-80	Control reader
PALMJET (all versions)	Contactless palm vein reader
PALMJET 2	Contactless palm vein reader

Hardware	Function
BioSmart PV-WTC	Terminal
BIOSMART QUASAR	Terminal
BIOSMART QUASAR 7	Terminal

Module licensing

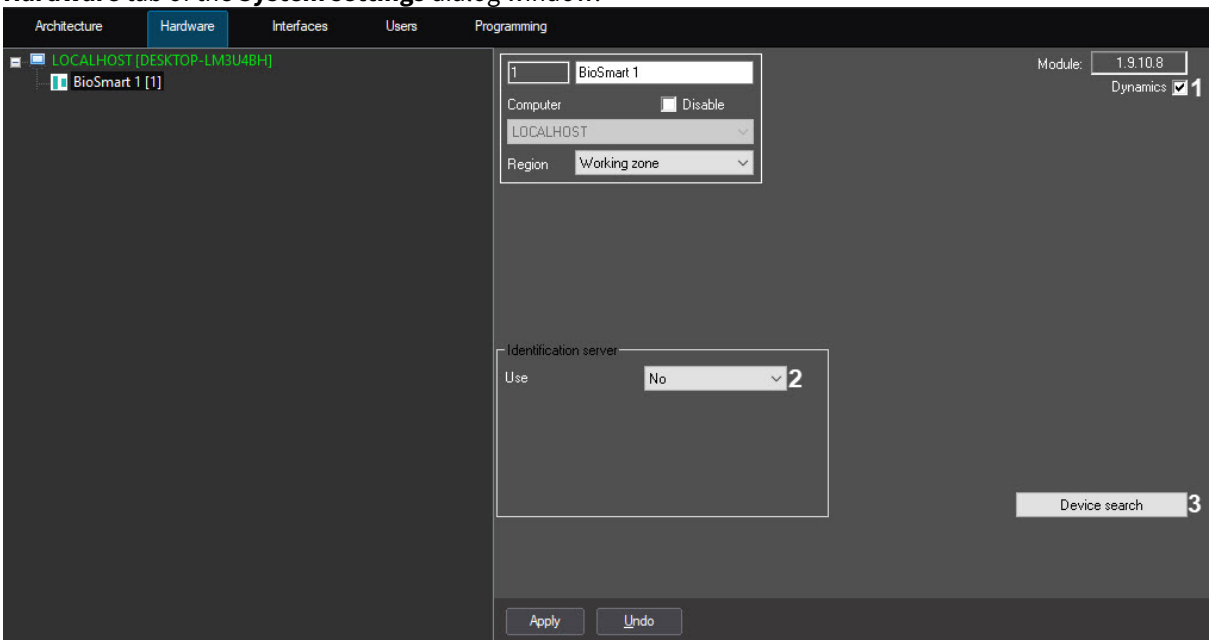
Per one controller/terminal.

4 Configuring the BioSmart integration module

4.1 Configuring the BioSmart parent object

To configure the *BioSmart* parent object, do the following:

1. Go to the settings panel of the **BioSmart** object that is created on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog window.



2. To automatically update the data of all devices, set the **Dynamics** checkbox (**1**).
3. From the **Use** drop-down list (**2**), select:
   - **No**—Identification server isn't connected. This is the default value;
   - **Yes**—Identification server is connected.
4. To find the devices connected to the parent object and automatically build the hardware tree, click the **Device search** button (**3**).
5. Click the **Apply** button to save the changes.

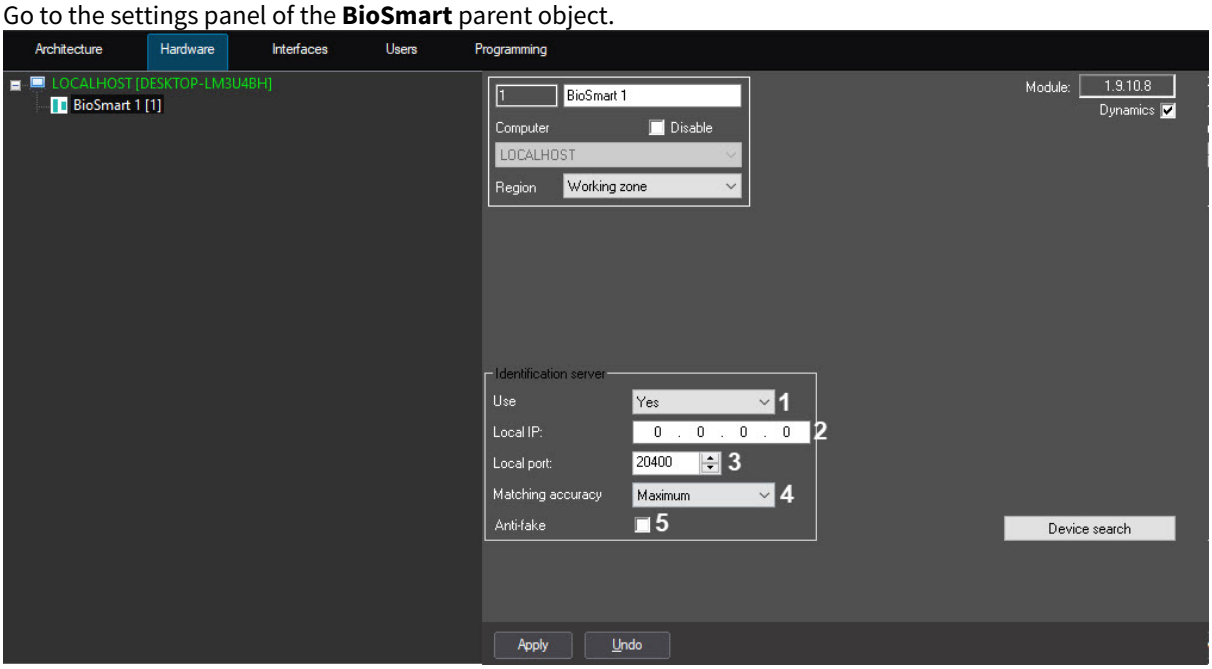
4.2 Configuring biometric identification Server

Configuring the *Axxon PSIM* biometric identification Server is required if the controller/terminal is configured for the **Server identification** system mode (see Configuring the BioSmart UniPass controller and Configuring the BioSmart PV-WTC terminal).

> **Attention!**
>
> The *Axxon PSIM* biometric identification Server works only with the BioSmart UniPass and BioSmart PV-WTC controllers.

To configure the *Axxon PSIM* biometric identification Server, do the following:

1. Go to the settings panel of the **BioSmart** parent object.



2. In the **Identification server** group, select **Yes** from the **Use** drop-down list (**1**).
3. In the **Local IP** field (**2**), enter the local IP address of the *Axxon PSIM* Biometric Identification server.
4. In the **Local port** field (**3**), select the local port number of the *Axxon PSIM* Biometric Identification server.
5. From the **Matching accuracy** drop-down list (**4**), select the matching accuracy of the palmprint and the palmprint stored in the controller/terminal: **Maximum** (default), **High**, **Normal**, **Low**, **Lower**, **Minimum**.

> **Note**
>
> The higher the matching accuracy, the longer it takes to check the matching of the palmprint, but the security is higher.

6. Set the **Anti-fake** checkbox (**5**) to enable protection of biometric readers from bringing objects other than the palm of the hand (so that the controller does not react, for example, on palm photo).
7. Click the **Apply** button to save the changes.

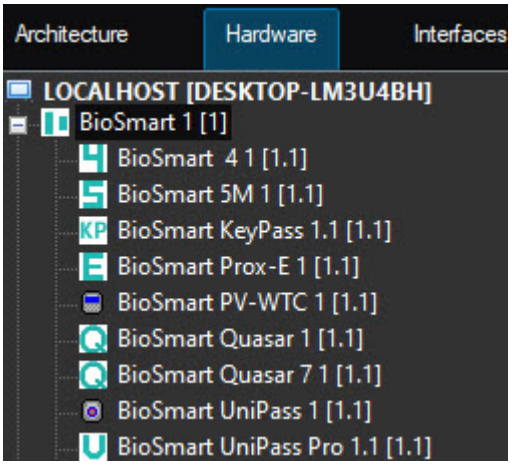
Configuration of the *Axxon PSIM* biometric identification Server is complete.

4.3 Configuring the connection of the BioSmart controller or terminal to the ACFA PSIM server

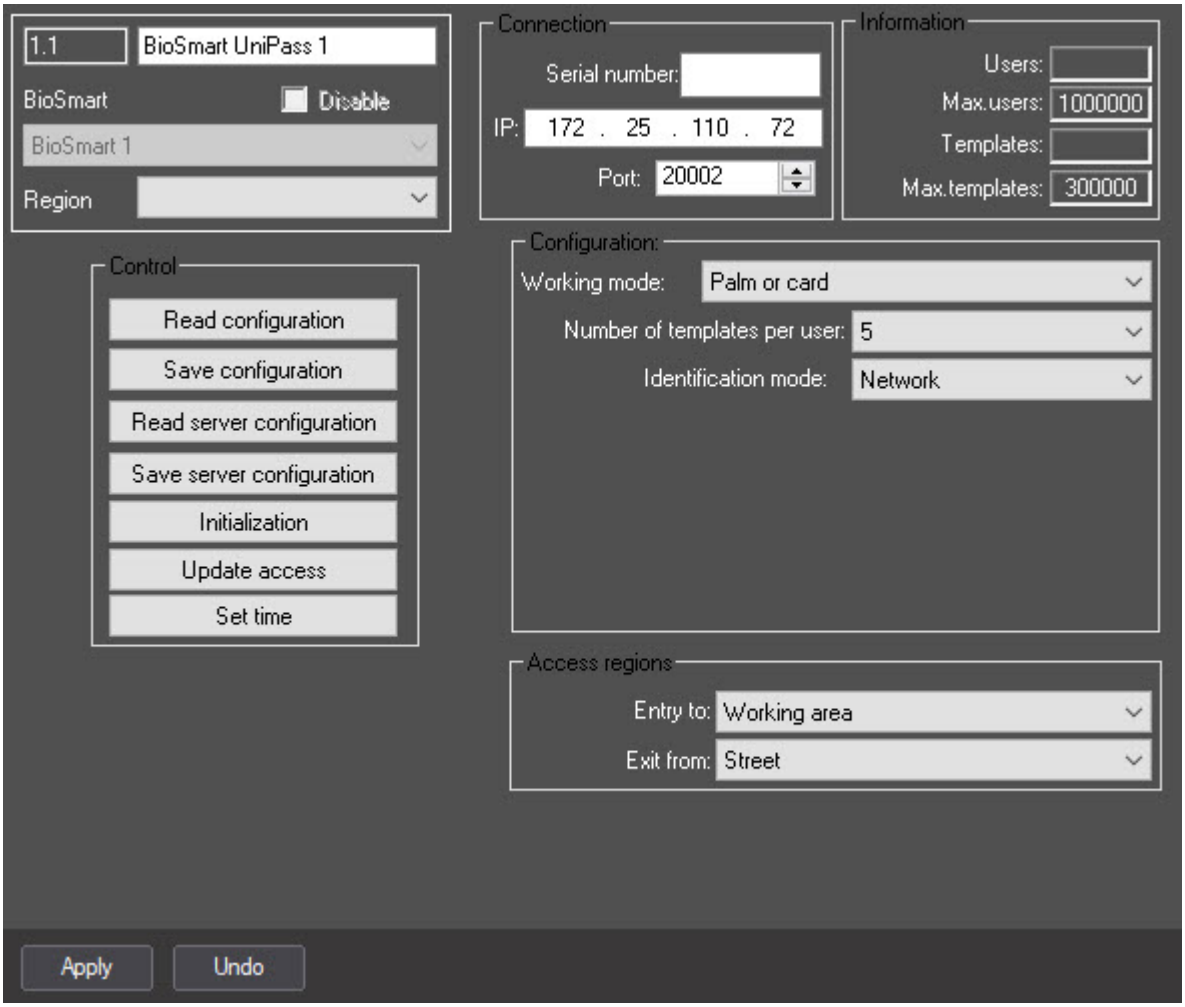
> **Attention!**
>
> These connection settings are ignored if the **Server identification** system mode is used (see Configuring the BioSmart UniPass controller).

If the *BioSmart* object tree is created automatically, you don't need to configure the connection of the BioSmart controller or terminal. If an object is created manually, do the following:

1. Go to the settings panel of the **BioSmart UniPass, BioSmart PV-WTC**, **BioSmart 4**, **BioSmart Prox-E**, **BioSmart Quasar**, **BioSmart Quasar 7**, **BioSmart UniPass Pro**, **BioSmart UniPass Pro 2**, **BioSmart 5M**, or **BioSmart KeyPass** object that is created on the basis of the **BioSmart** parent object.



2. In the **Serial number** field, enter the factory serial number of the device. The serial number is the name of the device on the network as well.



3. The **IP** field displays the device's IP address. The factory IP address is 172.25.110.72.
4. In the **Port** list, select the port number for connecting the device to the computer. Port **20002** is used by default.
5. Click the **Apply** button to save the settings.

Configuring the connection of the controller or the *BioSmart* terminal to the *ACFA PSIM* server is complete.

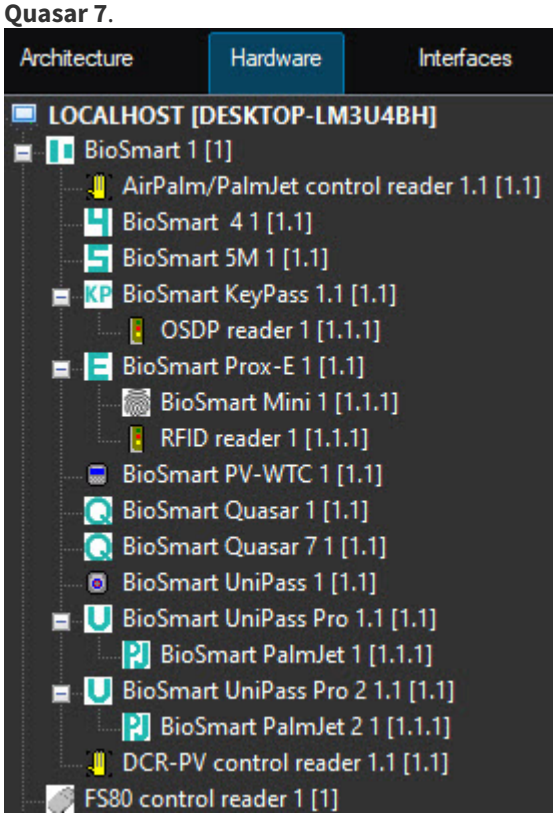
4.4 Configuring interaction of the BioSmart integration module with the Access Manager module and Time and Attendance subsystem

On the page:

- Interaction with the Access Manager module
- Interaction with the Time&Attendance subsystem

4.4.1 Interaction with the Access Manager module

The FS-80 control reader, the DCR-PV USB reader, the PalmJet contactless palm vein reader, the Biosmart PV-WTC reader (works in tandem with access controllers), as well as the Biosmart PV-WTC, BioSmart Quasar, and BioSmart Quasar 7 terminals, can be used as control readers in the *Access Manager* module (see Configuring control readers in the Access Manager). For this, you must create the corresponding objects: **FS80 control reader**, **AirPalm/ PalmJet control reader**, **DCR-PV control reader,** and/or **Biosmart PV-WTC**, **Biosmart Quasar**, and **BioSmart Quasar 7**.

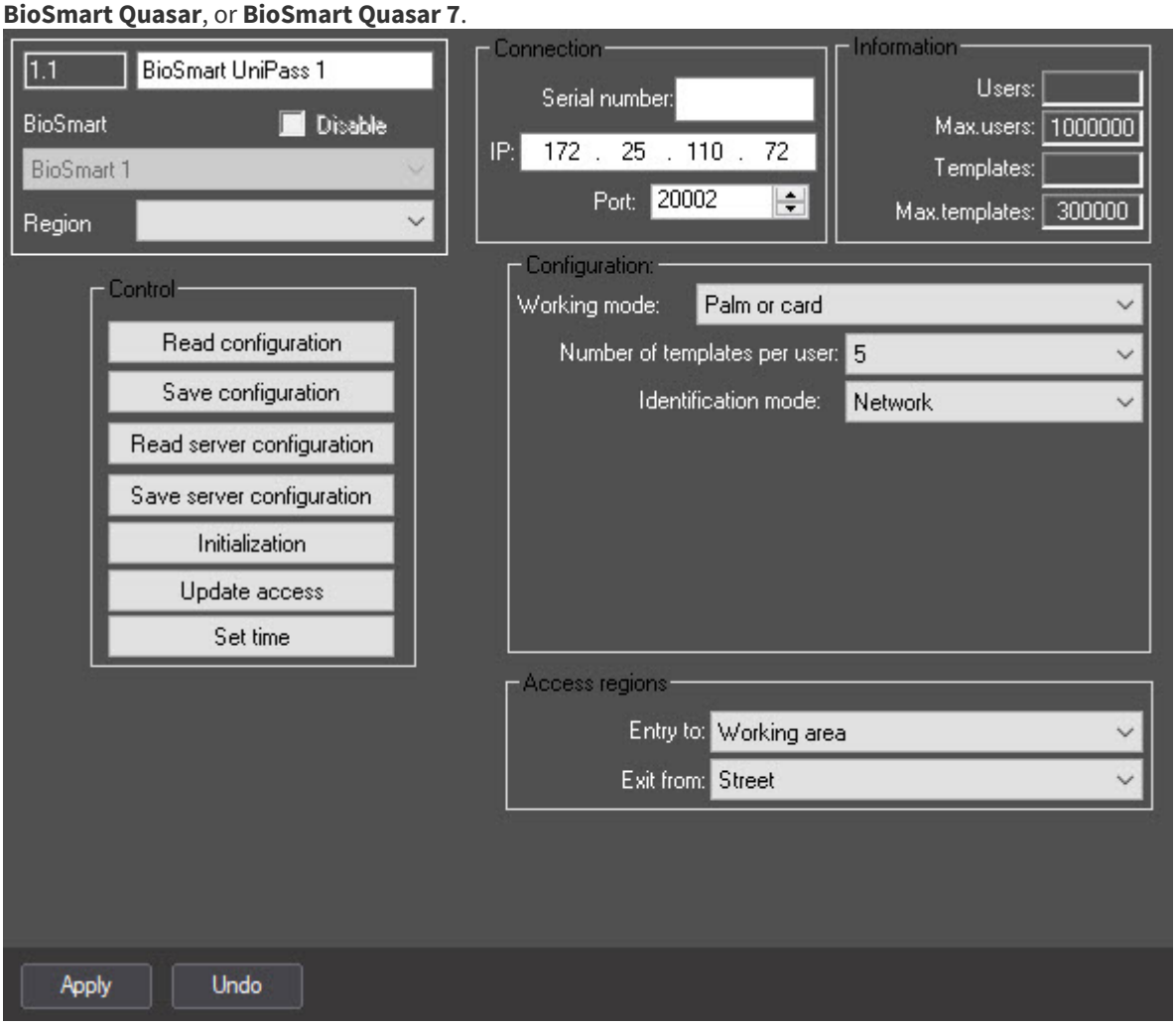


4.4.2 Interaction with the Time&Attendance subsystem

The readers of the BioSmart UniPass, BioSmart 4, BioSmart Prox-E, BioSmart UniPass Pro, BioSmart UniPass Pro 2, BioSmart 5M, BioSmart KeyPass controllers, as well as the BioSmart PV-WTC, BioSmart Quasar, and BioSmart Quasar 7 terminals, can be used to record working time in the *Time and Attendance* subsystem that is a part of the *Access Manager* module (see Guide for configuring and working with the Access Manager module).

For this, do the following:

1. Go to the settings panel of the **BioSmart UniPass**, **BioSmart 4**, **BioSmart 5M**, **RFID Reader**, or **BioSmart Mini** (created on the basis of the **BioSmart Prox-E** object), **OSDP reader** (created on the basis of the **BioSmart KeyPass** object), **BioSmart PalmJet** (created on the basis of the **BioSmart UniPass Pro** object), **BioSmart PalmJet 2** (created on the basis of the **BioSmart UniPass Pro 2** object), **BioSmart PV-WTC**, **BioSmart Quasar**, or **BioSmart Quasar 7**.



2. From the **Entry to** drop-down list, select the region corresponding to the area located on the side of the exit through the reader/terminal.
3. From the **Exit from** drop-down list, select the region corresponding to the area located on the side of the entrance through the reader/terminal.
4. Click the **Apply** button.

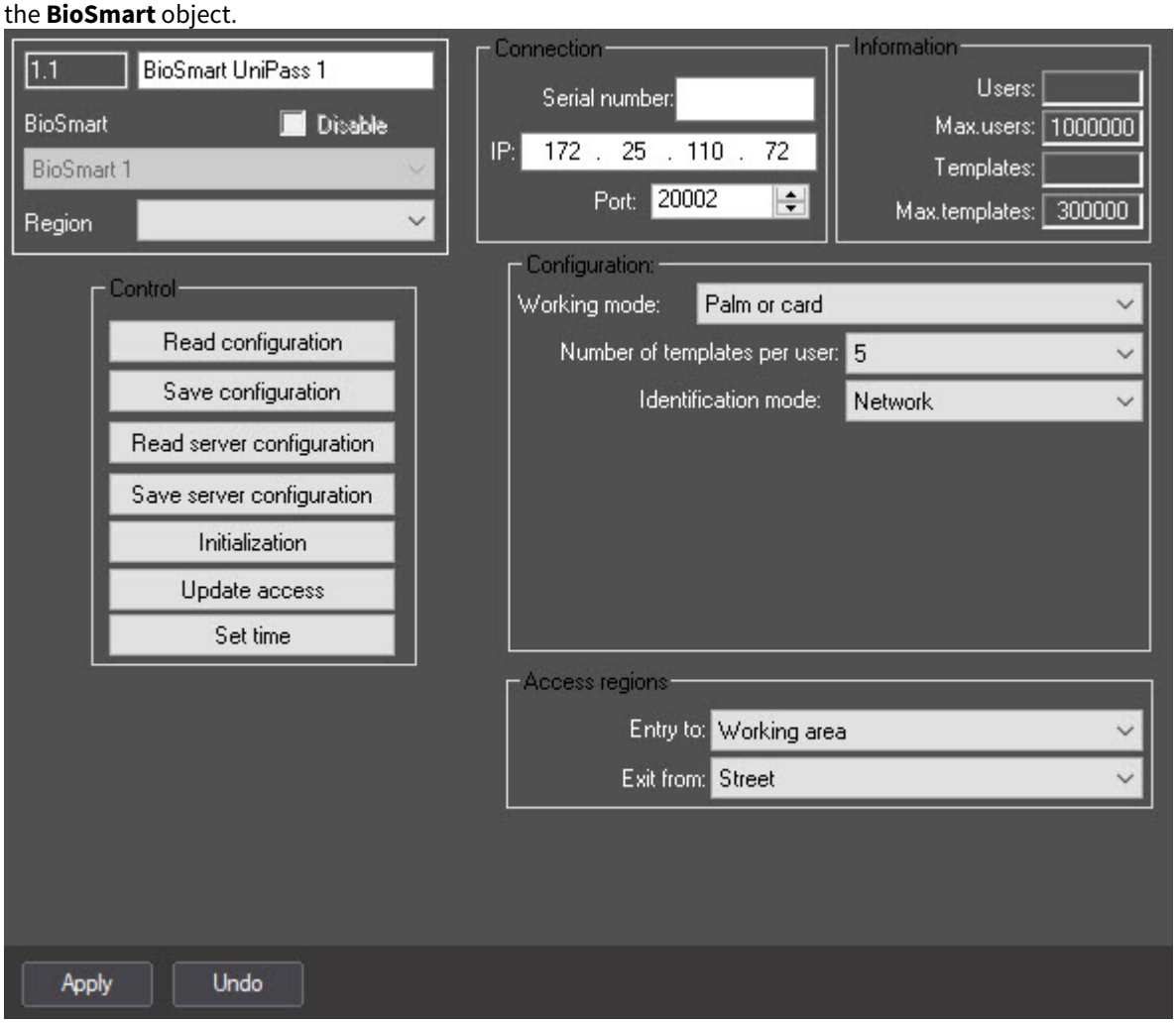
Configuring the interaction of the *BioSmart* integration module with the *Access Manager* module and the *Time and Attendance* subsystem is complete.

4.5 Managing the configuration of the BioSmart controllers/terminals

4.5.1 Managing the configuration of the BioSmart UniPass and Biosmart PV-WTC controllers

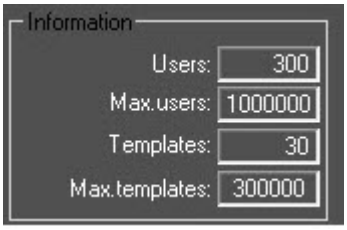
To manage the configuration of the BioSmart UniPass and BioSmart PV-WTC controllers, do the following:

1. Go to the settings panel of the **BioSmart UniPass** or **BioSmart PV-WTC** object that is created on the basis of the **BioSmart** object.



2. Click the **Read configuration** button to read the configuration of the controller.

> **Note**
>
> After reading the configuration, the **Information** block on the settings panel will be filled. It is for reference only and displays how many users are allowed to enter and how many vein templates are registered for them, as well as the factory maximum settings.



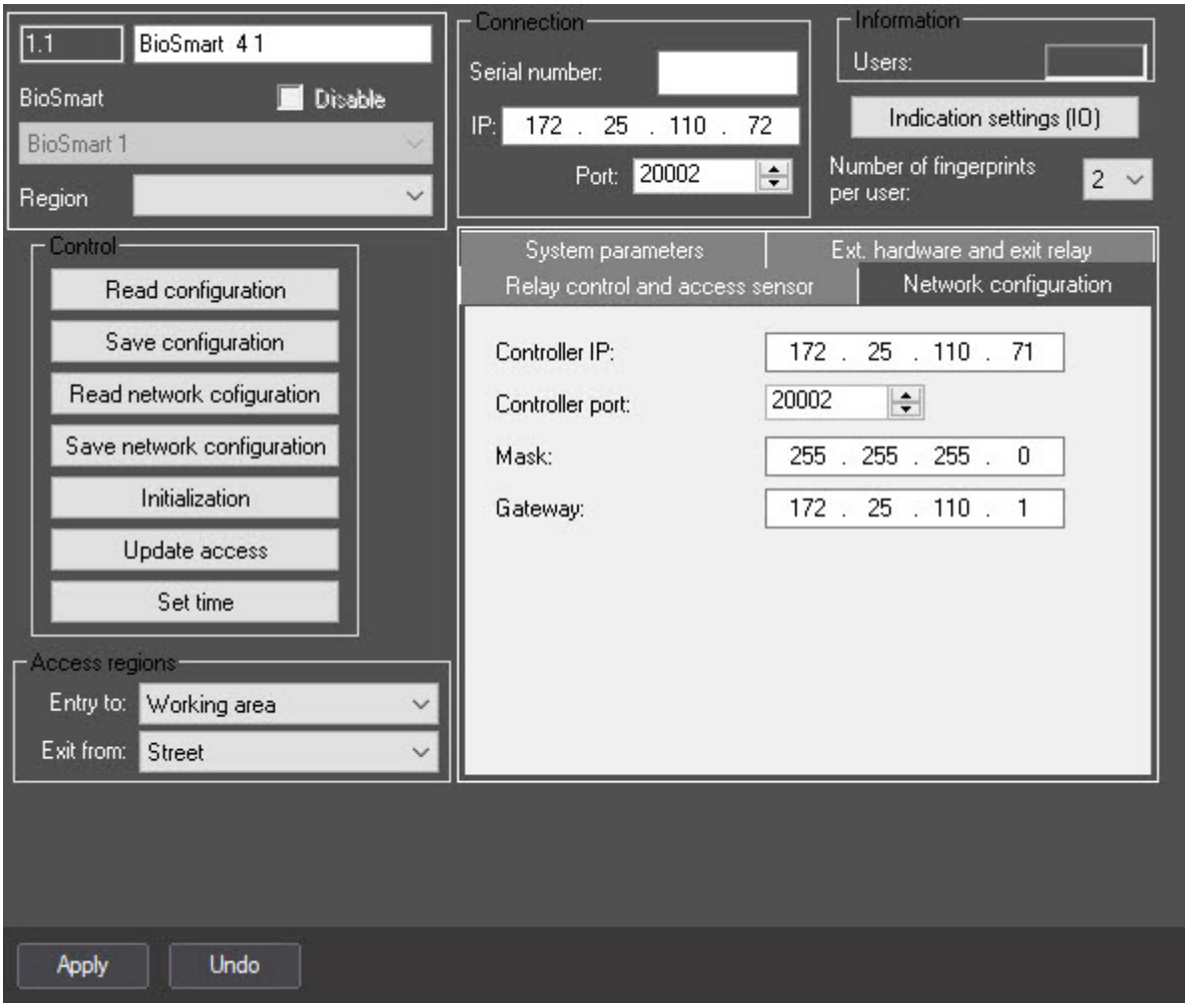
3. Click the **Save configuration** button to save the configuration changes to the controller.
4. Click the **Read server configuration** button to read the data of the system server operating mode from the controller.
5. Click the **Save server configuration** button to save the changes of the system server operating mode to the controller.
6. Click the **Initialization** button to delete all data on users, access cards, palm vein templates, and time schedules.
7. Click the **Update access** button to save access data (data on palm vein templates, access cards, time schedules, users, and so on) to the controller.
8. Click the **Set time** button to synchronize the time of the controller/terminal and the *ACFA PSIM* Server to which the controller/terminal is connected.
9. Click the **Apply** button to save the changes.

Managing the configuration of the BioSmart UniPass and BioSmart PV-WTC controllers is complete.

4.5.2 Managing the configuration of the BioSmart 4 and BioSmart 5M controllers

To manage the configuration of the BioSmart 4 and BioSmart 5M controllers, do the following:

1. Go to the settings panel of the **BioSmart 4** or **BioSmart 5M** object that is created on the basis of the **BioSmart** object.



2. Click the **Read configuration** button to read the configuration of the controller.

> **Note**
>
> After reading the configuration, the **Information** block on the settings panel will be filled. It is for reference only and displays how many users are allowed to enter.

3. Click the **Save configuration** button to save the configuration changes to the controller.
4. Click the **Read network configuration** button to read the data of the system network operating mode from the controller.
5. Click the **Save network configuration** button to save the changes of the system network operating mode to the controller.
6. Click the **Initialization** button to delete all data on users, access cards, palm vein templates, and time schedules.
7. Click the **Update access** button to save access data (data on palm vein templates, access cards, user time schedules, and so on) to the controller.

> **Note**
>
> BioSmart 4 controllers support 255 time schedules, that is, the id of the time schedule must be in the range 1-255.

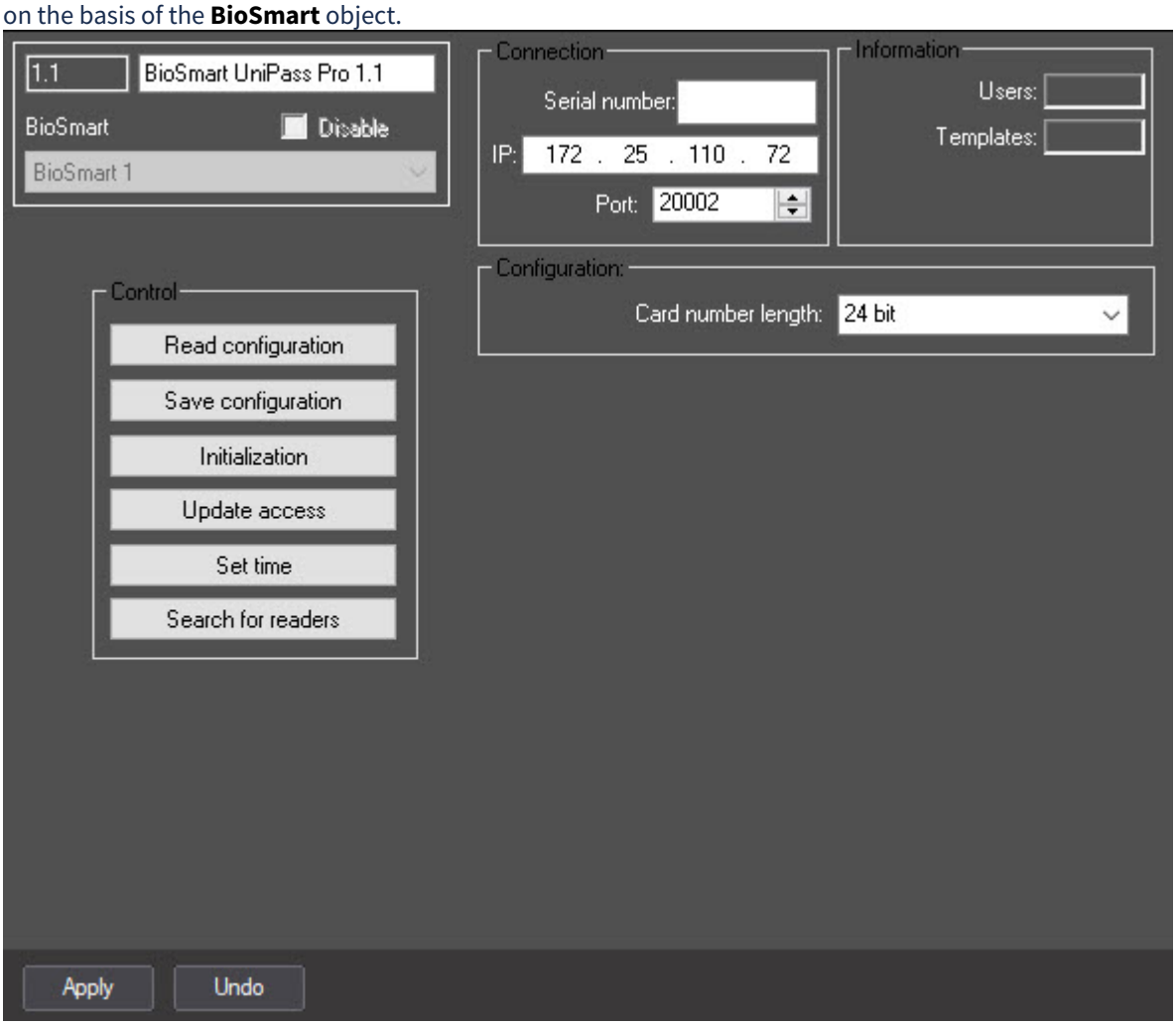
8. Click the **Set time** button to synchronize the time of the controller and the *ACFA PSIM* Server to which the controller is connected.
9. Click the **Apply** button to save the changes.

Managing the configuration of the BioSmart 4 and BioSmart 5M controllers is complete.

4.5.3 Managing the configuration of the BioSmart UniPass Pro and BioSmart UniPass Pro 2 controllers

To manage the configuration of the BioSmart UniPass Pro and BioSmart UniPass Pro 2 controllers, do the following:

1. Go to the settings panel of the **BioSmart UniPass Pro** or **BioSmart UniPass Pro 2** objects that are created on the basis of the **BioSmart** object.



2. Click the **Read configuration** button to read the configuration of the controller.

> **Note**
>
> After reading the configuration, the **Information** block on the settings panel will be filled. It is for reference only and displays how many users are allowed to enter and how many vein templates are registered for them.

3. Click the **Save configuration** button to save the configuration changes to the controller.

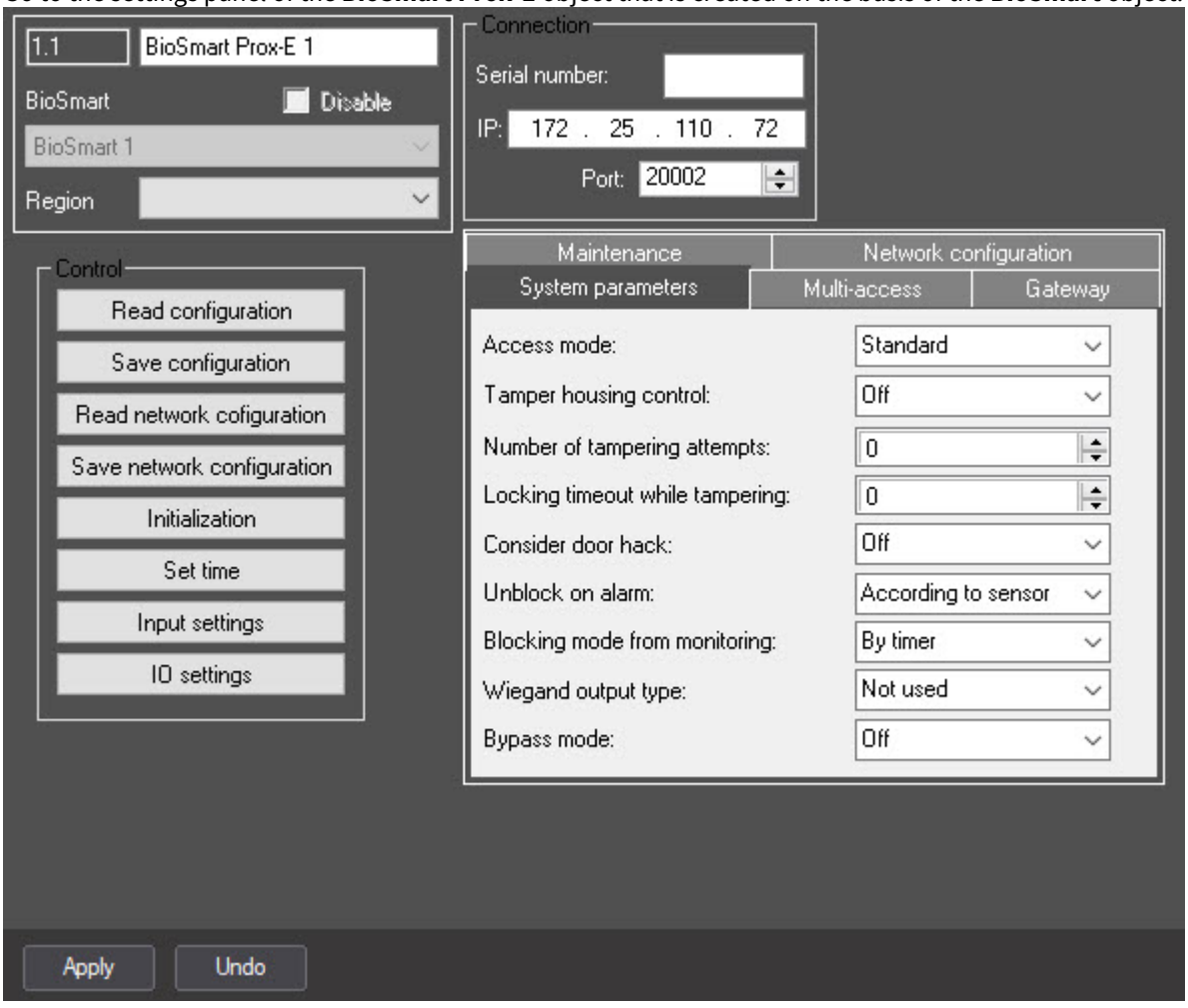
4. Click the **Initialization** button to delete all data on users, access cards, palm vein templates, and time schedules.
5. Click the **Update access** button to save access data (data on palm vein templates, access cards, user time schedules, and so on) to the controller.
6. Click the **Set time** button to synchronize the time of the controller and the *ACFA PSIM* server to which the controller is connected.
7. Click the **Search for readers** button to find all readers connected to the controller and build the hardware tree.
8. Click the **Apply** button to save the changes.

Managing the configuration of the BioSmart UniPass Pro and BioSmart UniPass Pro 2 controllers is complete.

4.5.4 Managing the configuration of the BioSmart Prox-E controller

To manage the configuration of the BioSmart Prox-E controller, do the following:

1. Go to the settings panel of the **BioSmart Prox-E** object that is created on the basis of the **BioSmart** object.

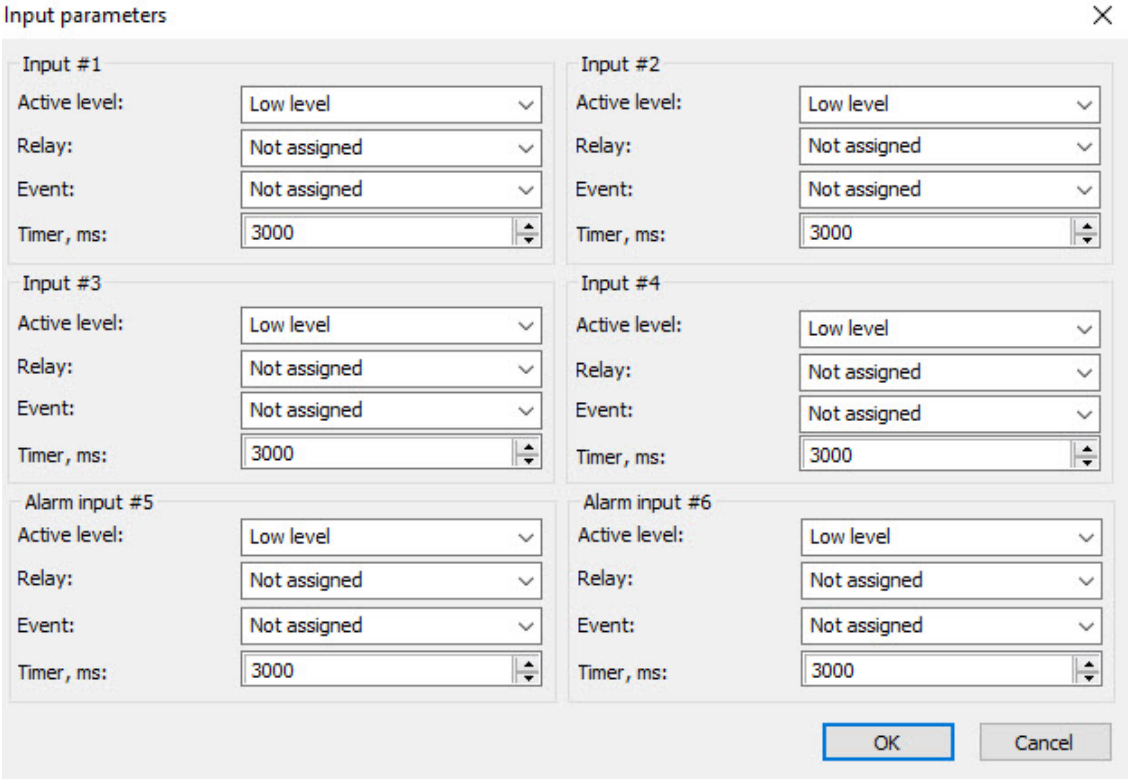


2. Click the **Read configuration** button to read the configuration of the controller.
3. Click the **Save configuration** button to save the configuration changes to the controller.
4. Click the **Read network configuration** button to read the data of the system network operating mode from the controller.
5. Click the **Save network configuration** button to save the changes of the system network operating mode to the controller.

6. Click the **Initialization** button to delete all data on users, access cards, palm vein templates, and time schedules.

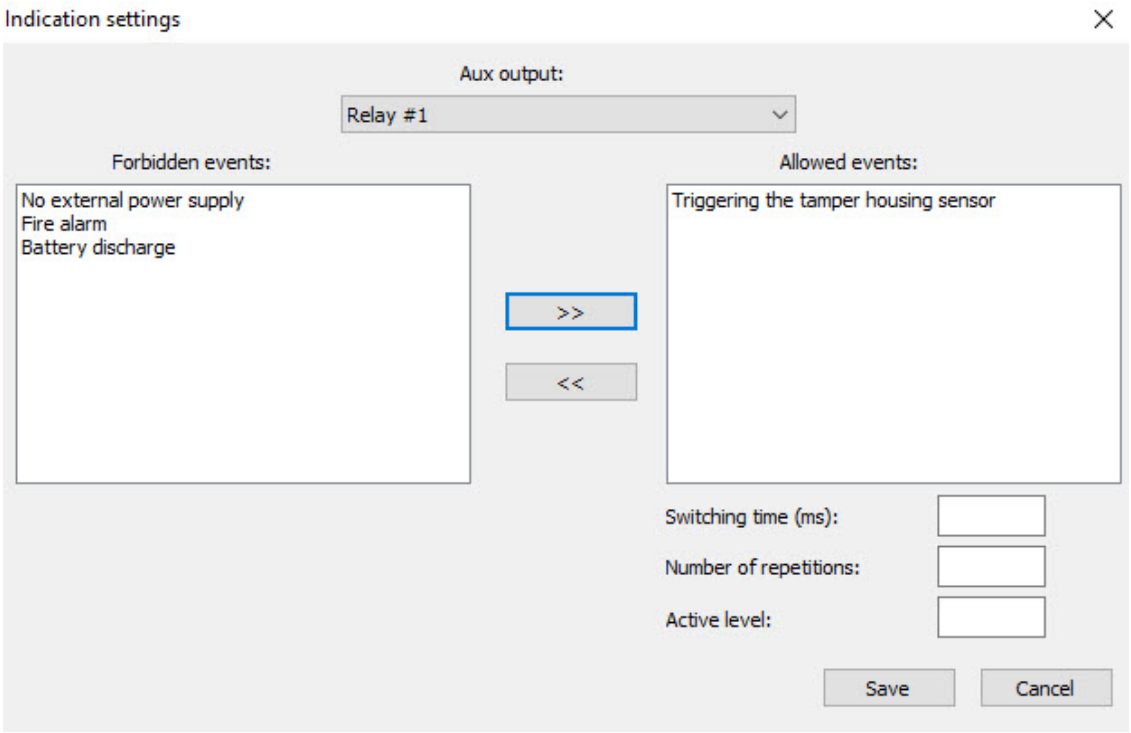
> **Note**
>
> BioSmart Prox-E controllers support 255 time schedules, that is, the id of the time schedule must be in the range 1-255.

7. Click the **Set time** button to synchronize the time of the controller and the *ACFA PSIM* Server to which the controller is connected.
8. Click the **Input settings** button.
   a. In the **Input parameters** window, configure the controller input parameters:



   b. Click the **OK** button to save the changes.
9. Click the **IO settings** button.

a. In the **Indication settings** window, configure the indication settings of the aux outputs of the controller:



b. Click the **Save** button to save the changes.

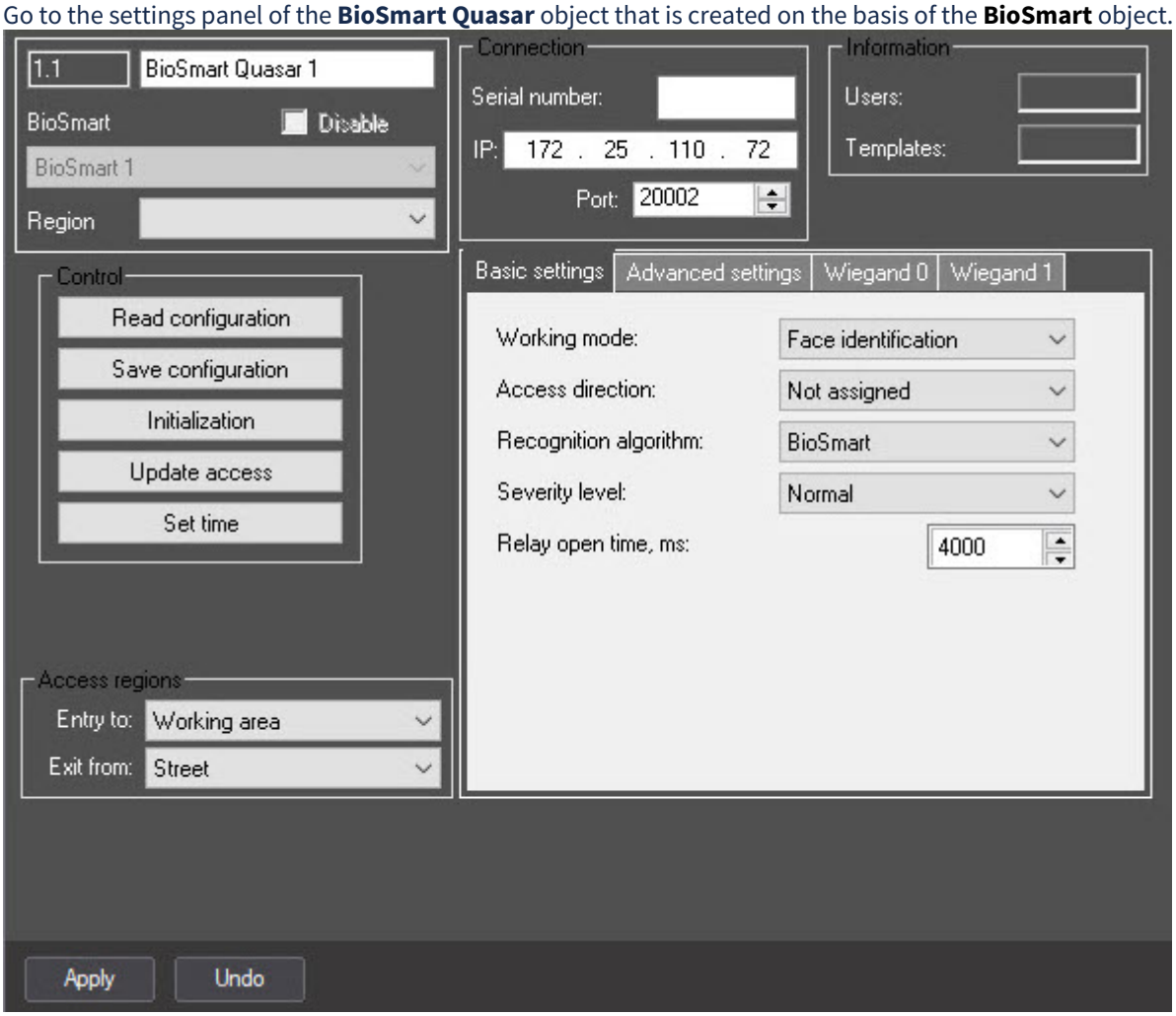
10. Click the **Apply** button to save the changes.

Managing the configuration of the BioSmart Prox-E controllers is complete.

4.5.5 Managing the configuration of the BioSmart Quasar terminal

To manage the configuration of the BioSmart Quasar terminal, do the following:

1. Go to the settings panel of the **BioSmart Quasar** object that is created on the basis of the **BioSmart** object.



2. Click the **Read configuration** button to read the configuration of the terminal.

> **Note**
>
> After reading the configuration, the **Information** block on the settings panel will be filled. It is for reference only and displays how many users are allowed to enter and how many vein templates are registered for them.

3. Click the **Save configuration** button to save the configuration changes to the terminal.
4. Click the **Initialization** button to delete all data on users, access cards, palm vein templates, and time schedules.
5. Click the **Update access** button to save access data (data on palm vein templates, access cards, user time schedules, and so on) to the terminal.
6. Click the **Set time** button to synchronize the time of the terminal and the *ACFA PSIM* Server to which the terminal is connected.
7. Click the **Apply** button to save the changes.

Managing the configuration of the BioSmart Quasar terminal is complete.

4.5.6 Managing the configuration of the BioSmart Quasar 7 terminal

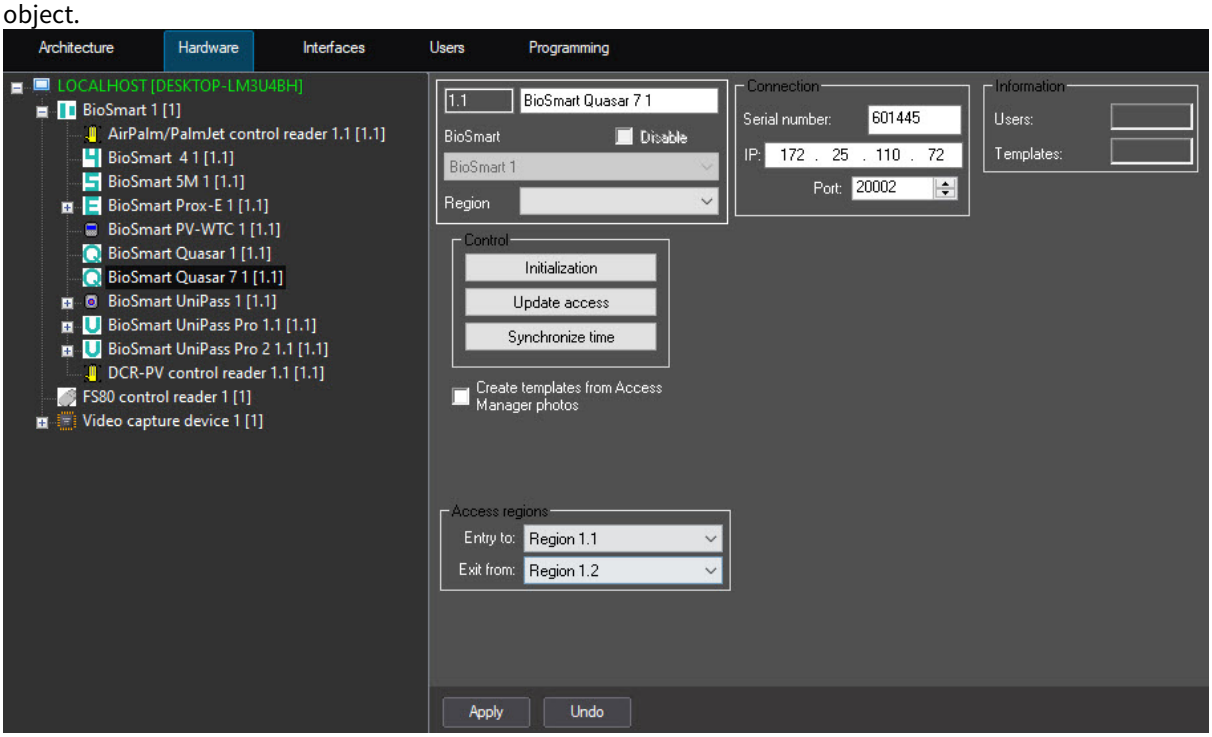
On the page:

- Managing the terminal configuration
- Creating a user face template manually

Managing the terminal configuration

To manage the configuration of the *BioSmart Quasar 7* terminal, do the following:

1. Go to the settings panel of the **BioSmart Quasar 7** object that is created on the basis of the **BioSmart** object.



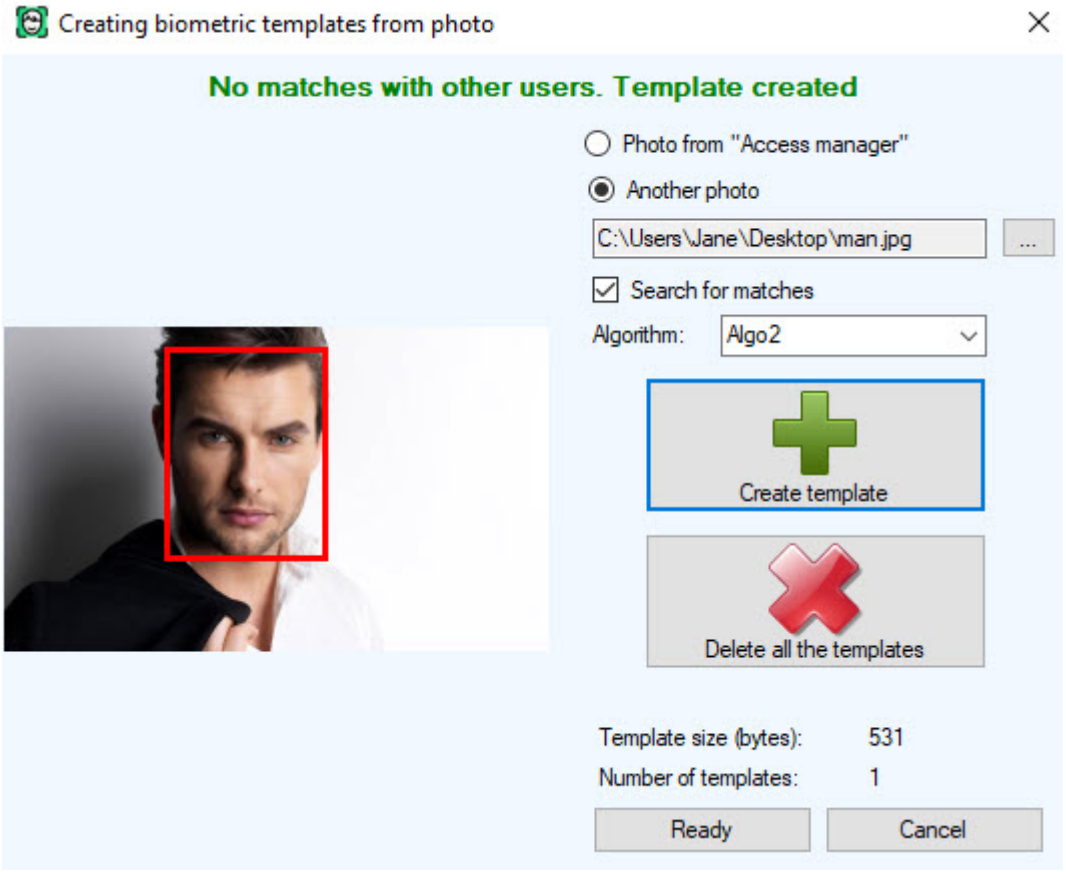
2. Click the **Initialization** button to delete all data on users, access cards, palm vein templates, and time schedules.
3. Click the **Update access** button to write access data (data on palm vein templates, access cards, user time schedules, and so on) to the terminal.
4. Click the **Synchronize time** button to synchronize the time of the terminal and the *ACFA PSIM* server to which the terminal is connected.
5. Set the **Create templates from Access Manager photos** checkbox so that face templates are created automatically when users are fully written or, if the **Dynamics** checkbox is set (see Configuring the BioSmart parent object), via the ALGO5 algorithm. If you don't set the checkbox, the face templates are created manually via the *BioSmart* extension in the *Access Manager*. See below on the page for more details.
6. Click the **Apply** button to save the settings.

Managing the configuration of the *BioSmart Quasar 7* terminal is complete.

Creating a user face template manually

To add a face template manually, do the following:

1. Open the user settings in editing mode.
2. Right-click the user photo and select the *BioSmart* parent object as the extension (for the information on how to work with extensions, see Adding biometric parameters).
3. Select a location for uploading the photo:
   a. **Photo from "Access Manger"**.
   b. **Another photo**.



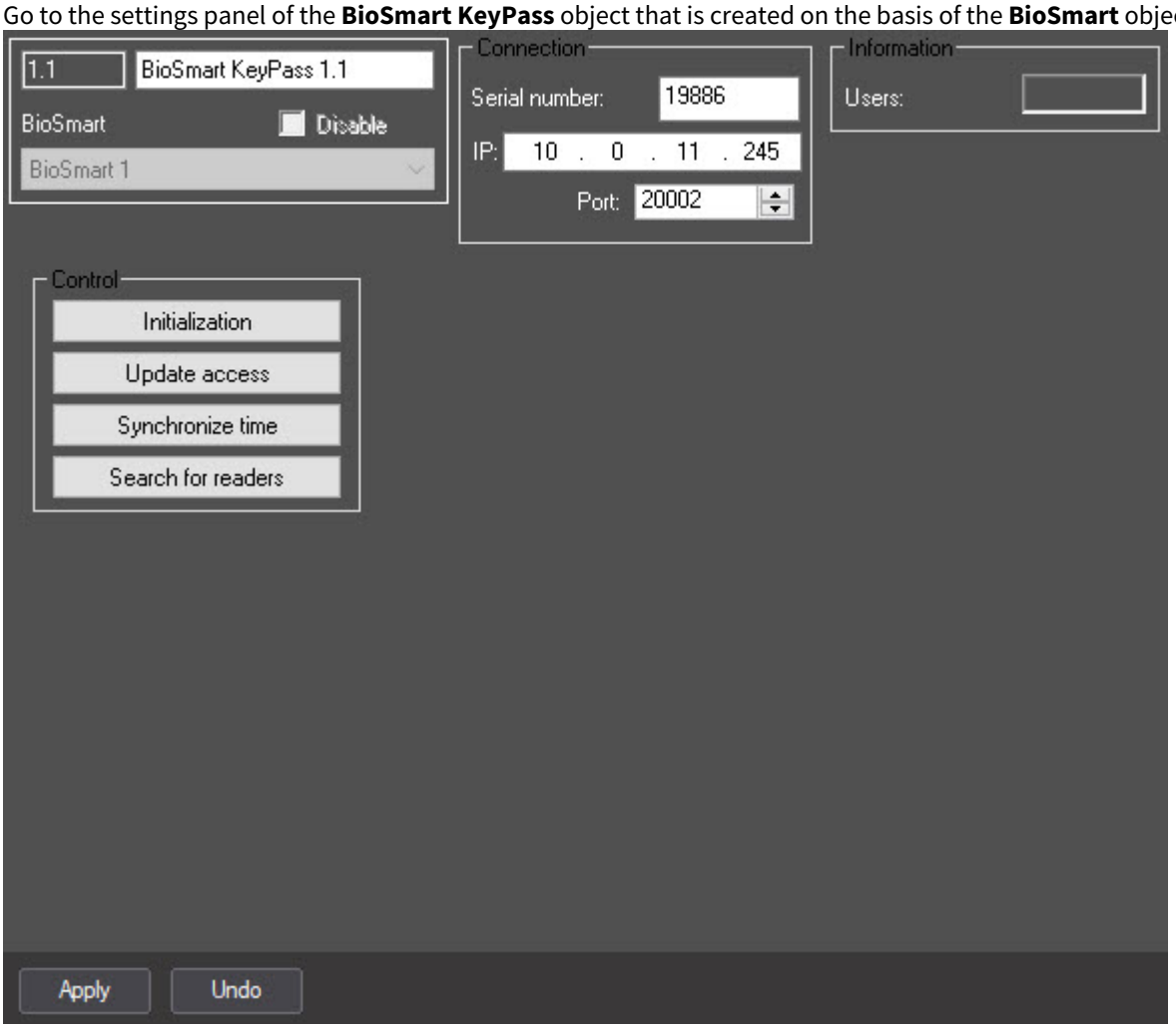
4. Select **Algo5** from the **Algorithm** drop-down list.
5. Click the **Create template** button.
6. To save the template, click the **Ready** button.

Creating a user face template manually is complete.

4.5.7 Managing the configuration of the Biosmart KeyPass controller

To manage the configuration of the BioSmart KeyPass controller, do the following:

1. Go to the settings panel of the **BioSmart KeyPass** object that is created on the basis of the **BioSmart** object.



2. Click the **Initialization** button to remove all data about users, maps, palm vein patterns, and time schedule data.
3. Click the **Update access** button to update all data about users, maps, palm vein patterns, and time schedule data.
4. Click the **Synchronize time** button to synchronize the time of the controller and the *ACFA PSIM* server to which it is connected.
5. Click the **Search for readers** button to find all readers connected to the controller.

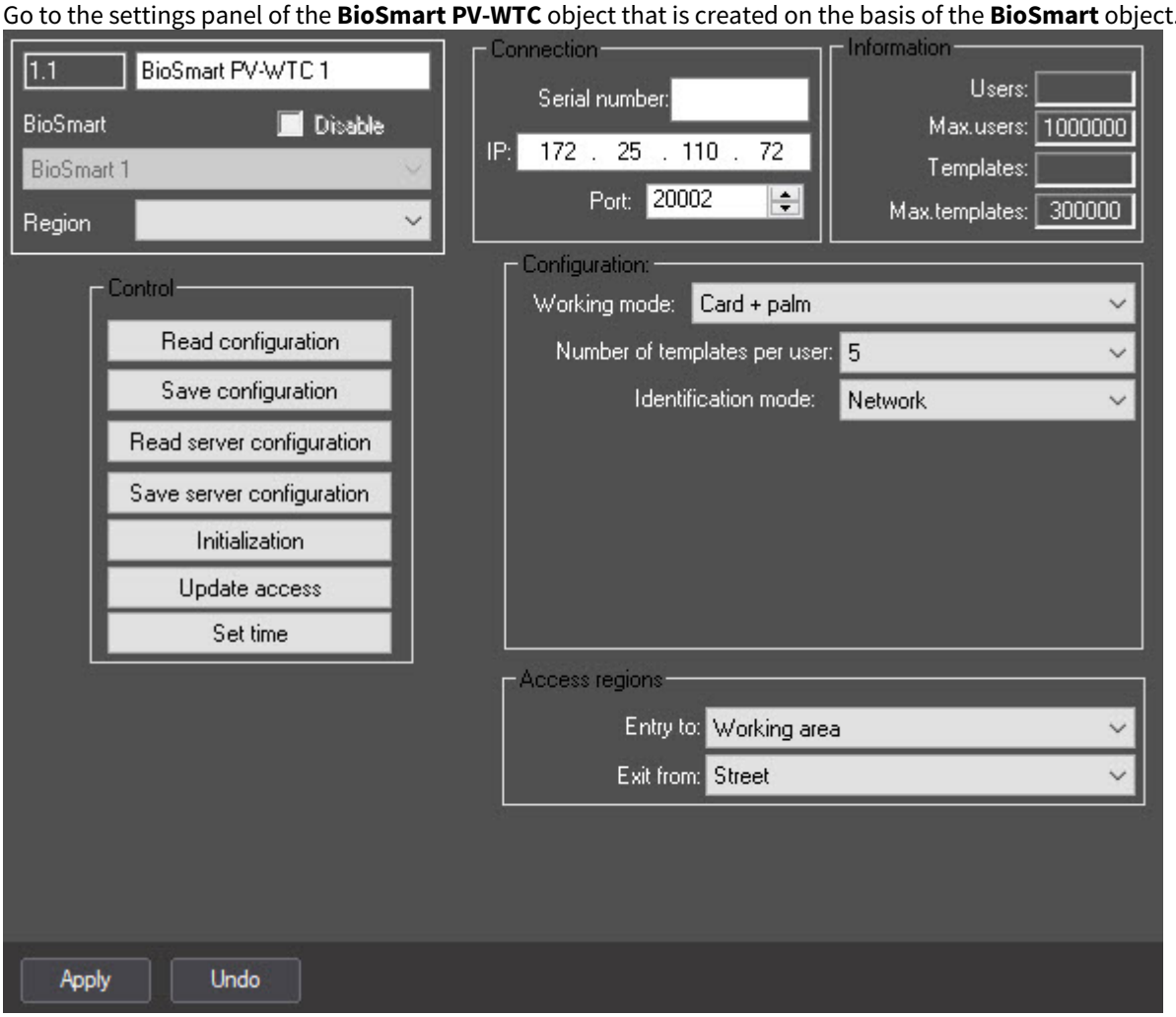
Managing the configuration of the BioSmart KeyPass controller is complete.

4.6 Configuring the BioSmart PV-WTC terminal

You can configure the BioSmart PV-WTC terminal both when objects are created automatically and manually.

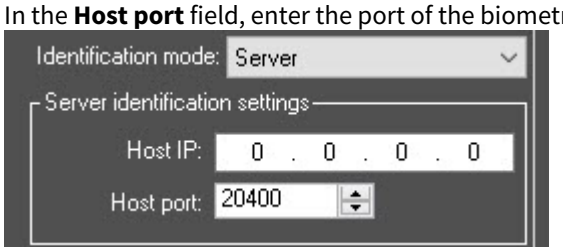
For this, do the following:

1. Go to the settings panel of the **BioSmart PV-WTC** object that is created on the basis of the **BioSmart** object.



2. From the **Working mode** drop-down list, select the terminal operation mode that corresponds to the serial number of the terminal operation model in the web interface.
3. From the **Number of templates per user** drop-down list, select the number of possible templates of the user's palm vein pattern in the range 1-10. Templates are saved in the controller and used for user identification. If the number of templates saved in the *Access Manager* is greater than the specified number, only the number specified in the **Number of templates per user** parameter is saved to the controller. The default value is **5**.
4. From the **Identification mode** drop-down list, select the system operation mode:
    a. **Network**—operation mode in which access to the terminal is assigned from the manufacturer's software BioSmart Studio. Palm templates are stored in the terminal memory.
    b. **Local**—standalone operation mode of BioSmart PV-WTC terminal. Differs from the **Network** operation mode by the database storage logic.
    c. **Server identification**—operation mode in which palm templates are stored on an external biometric identification server instead of the terminal local memory. In this mode, comparison of biometric data is performed on an external server, which allows you to expand the number of templates and increase the speed of identification. The following parameters of the external biometric identification Server must be specified:
        i. In the **Host IP** field, enter the IP address of the biometric identification Server.

ii. In the **Host port** field, enter the port of the biometric identification Server.



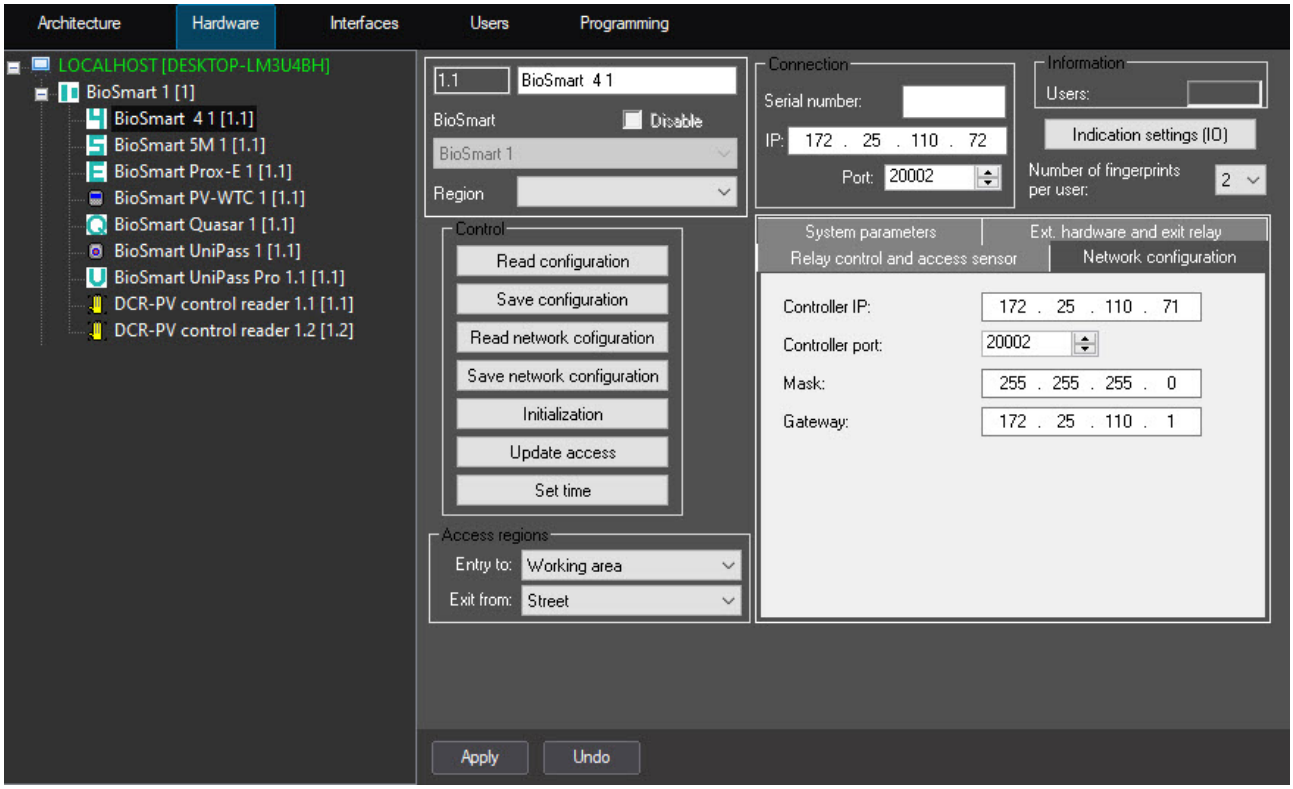
> **Attention!**
>
> If the **Server identification** mode is used, then the biometric identification Server must be configured on the parent object (see Configuring the biometric identification Server).

5. Click the **Save configuration** button to write the settings to the terminal.
6. Click the **Apply** button.

Configuring the BioSmart PV-WTC terminal is complete.

4.7 Configuring the BioSmart 4 controller

The BioSmart 4 controller is configured on the settings panel of the **BioSmart 4** object created on the basis of the **BioSmart** object.

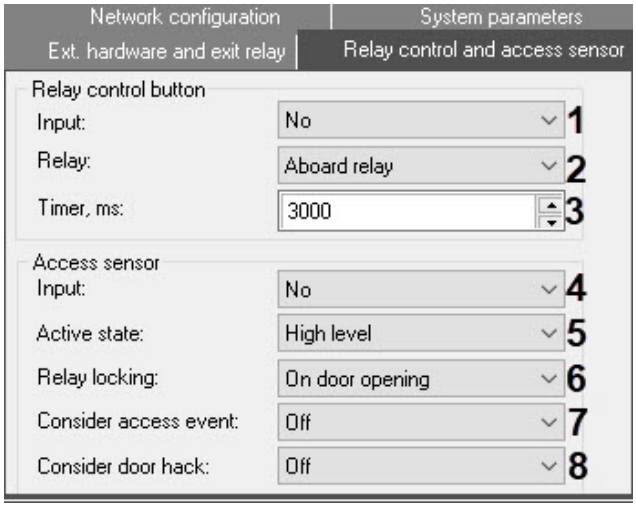


4.7.1 Configuring the relay control button and access sensor

On the page:

- Configuring the relay control button
- Configuring the access sensor

A relay control button or an access sensor can be connected to the discrete input of the BioSmart 4 controller. To configure them, go to the **Relay control and access sensor** tab on the settings panel of the BioSmart 4 controller.



Configuring the relay control button

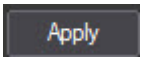
In the corresponding parameter group, configure the relay control button:

1. From the **Input** drop-down list (**1**), select the input to which the button is connected: **Aboard input**, **Input #1 RCU**, **Input #2 RCU**, **Input #3 RCU**, **Input #4 RCU**. If the button isn't connected, select the **No** value. In this case, further configuration isn't relevant.
2. From the **Relay** drop-down list (**2**), select the type of relay that will trigger by clicking the control buttons:
   a. **Aboard relay**—controller relay.
   b. **Relay #1 RCU**—relay 1 of *BioSmart* RCU (relay control unit).
   c. **Relay #2 RCU**—relay 2 of *BioSmart* RCU.
3. In the **Timer, ms** field (**3**), enter the time of the active state of the relay after clicking the relay control button in milliseconds. The default value is **3000**.

Configuring the access sensor

In the corresponding parameter group, configure the access sensor:

1. From the **Input** drop-down list (**4**), select the input to which the access sensor is connected: **Aboard input**, **Input #1 RCU**, **Input #2 RCU**, **Input #3 RCU**, **Input #4 RCU**. If the access sensor isn't connected, select the **No** value. In this case, further configuration isn't relevant.

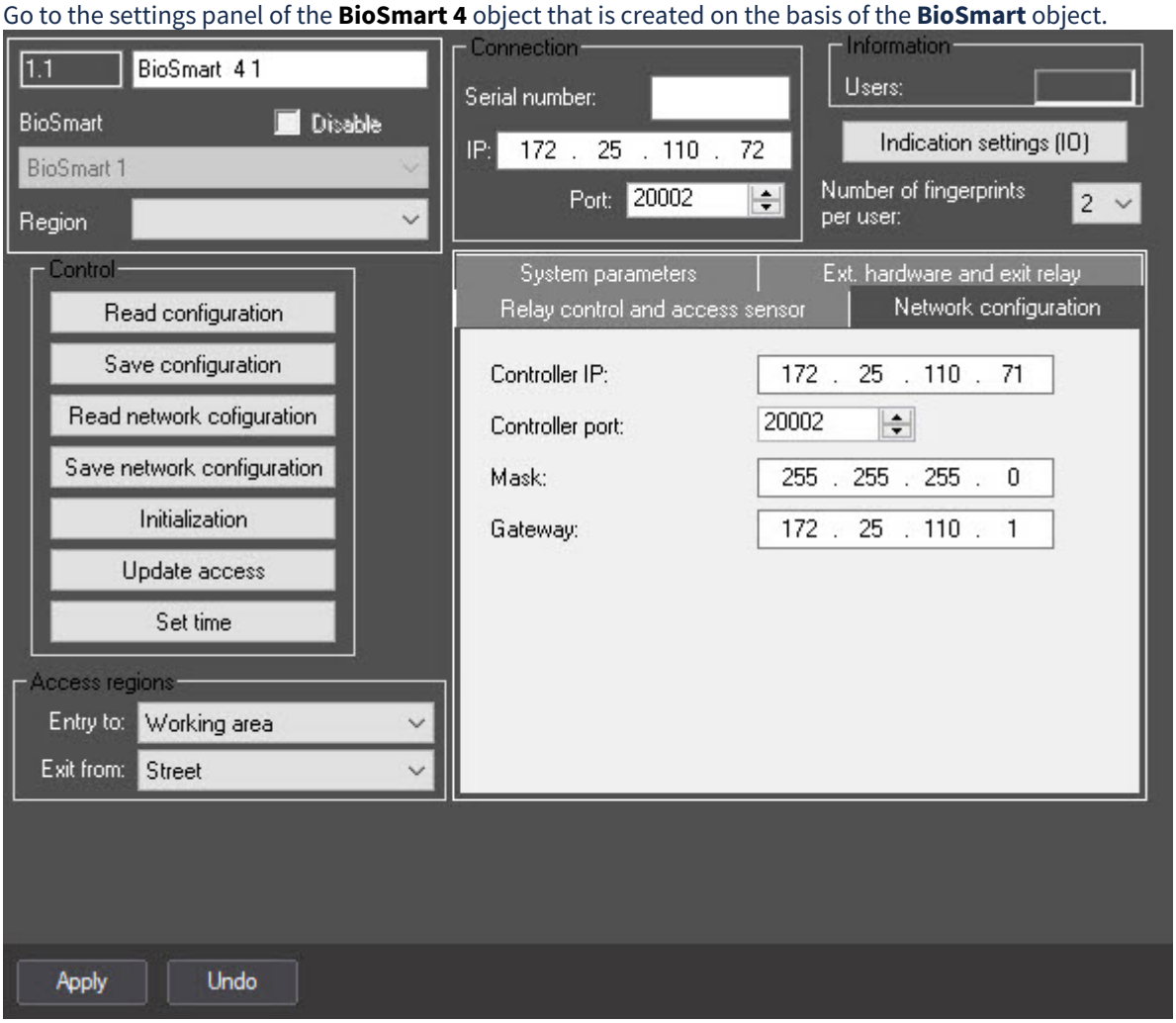
2. From the **Active state** drop-down list (**5**), select **Low level** or **High level** of the signal that appears on the discrete input, at which the access sensor triggering is detected.
3. From the **Relay locking** drop-down list (**6**), select the relay locking mode when the access sensor triggering is detected. **On door opening**—relay is disabled when the access sensor is triggered. **On door closing**—relay is disabled when the access sensor returns to its initial state.
4. If it is necessary to consider an access event, select the **On** value from the **Consider access event** drop-down list (**7**). The default value is **Off**.
5. If it is necessary to consider a door hack, select the **On** value from the **Consider door hack** drop-down list (**8**). The default value is **Off**.
6. Click the **Apply** 

button to save the changes.

4.7.2 Configuring the number of user fingerprint templates

To configure the number of user fingerprint templates, do the following:

1. Go to the settings panel of the **BioSmart 4** object that is created on the basis of the **BioSmart** object.



2. From the **Number of fingerprints per user** drop-down list, select the maximum number of templates of the user's fingerprints in the range 0-5. Templates are saved in the BioSmart 4 controller and used for user identification. If the number of templates saved in the *Access Manager* is greater than the specified number, only the number specified in the **Number of fingerprints per user** parameter is saved to the controller. The default value is **2**.

3. Click the **Apply** button to save the changes.

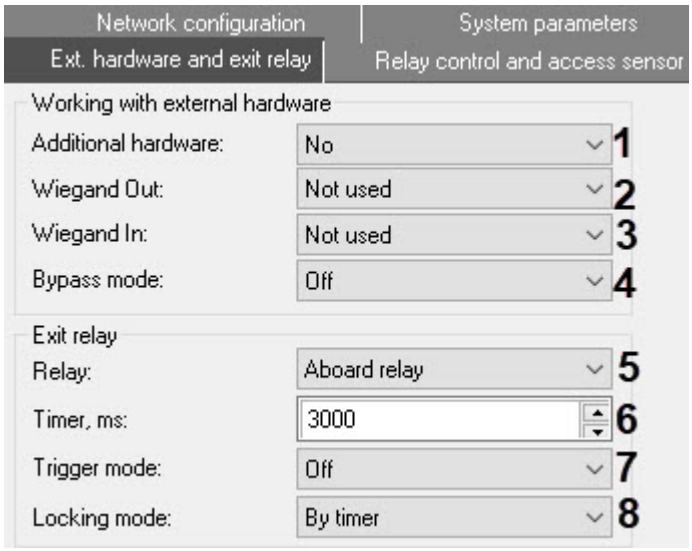
Configuring the number of user fingerprint templates is complete.

4.7.3 Configuring working with external hardware and exit relay

On the page:

- Configuring working with external hardware
- Configuring working with exit relay

You can connect external hardware to the BioSmart 4 controller. To configure interaction with external hardware, as well as configure the exit relay, go to the **Ext. hardware and exit relay** tab on the settings panel of the BioSmart 4 controller.



Configuring working with external hardware

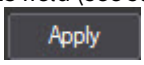
In the corresponding parameter group, configure working with external hardware:

1. From the **Additional hardware** drop-down list (**1**), select the type of hardware connected to the BioSmart 4 controller:
   a. **No**—additional hardware isn't connected.
   b. **BioSmart RCU**—the *BioSmart* relay control unit (RCU) is connected to the controller.
   c. **CK-24**—key dispenser is connected to the controller.
   d. **Kronwerk**—controller works in the integration mode with the *Kronwerk* ACS under the *Kronwerk* software control.
   e. **BioSmart BOX**—the BioSmart BOX cell monitoring hardware is connected to the controller.
   f. **Perco**—controller works in the integration mode with the *Perco* ACS under the *Perco* software control.

2. From the **Wiegand Out** drop-down list (**2**), select the protocol type of the Wiegand output interface of the BioSmart 4 controller:
    a. **Not used**—the Wiegand output interface of the BioSmart 4 controller isn't used.
    b. **Wiegand-26 (W/P)**—hardware that uses the Wiegand 26 protocol with parity check bits is connected to the Wiegand output of the BioSmart 4 controller.
    c. **Wiegand-32**—hardware that uses the Wiegand 32 protocol is connected to the Wiegand output of the BioSmart 4 controller.
3. From the **Wiegand In** drop-down list (**3**), select the protocol type of the Wiegand input interface of the BioSmart 4 controller:
    a. **Not used**—the Wiegand input interface of the BioSmart 4 controller isn't used.
    b. **Wiegand-26**—reader that uses the Wiegand 26 protocol is connected to the Wiegand input of the BioSmart 4 controller.
    c. **Wiegand-26 (W/P)**—reader that uses the Wiegand 26 protocol with parity check bits is connected to the Wiegand input of the BioSmart 4 controller.
    d. **Wiegand-32**—reader that uses the Wiegand 32 protocol is connected to the Wiegand input of the BioSmart 4 controller.
4. If you want to enable the bypass mode, select the **On** value from the **Bypass mode** drop-down list (**4**). In this case, the access card not registered in the *ACFA PSIM* database will be available for transmission to the external ACS controller via the Wiegand output of the Biosmart 4 controller. The default value is **Off**.

Configuring working with exit relay

In the corresponding parameter group, configure working with exit relay:

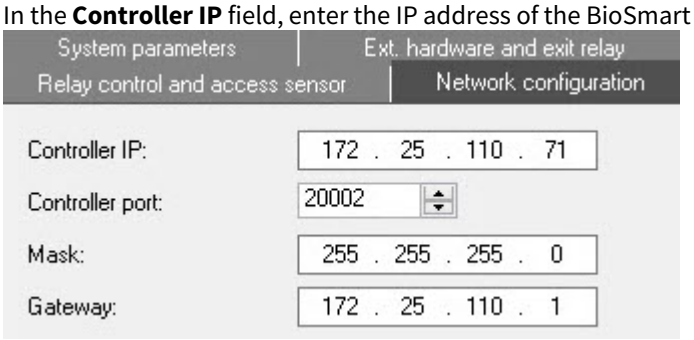
1. From the **Relay** drop-down list (**5**), select the type of relay that will trigger at access: **Aboard relay**, **Relay #1 RCU**, **Relay #2 RCU**.
2. In the **Timer, ms** field (**6**), enter the time in milliseconds of the active state of the relay after clicking the relay control button. The default value is **3000**.
3. To enable the trigger mode, from the **Trigger mode** drop-down list (**7**), select the **On** value. In this case, the relay will change its state each time the access is successful. When the controller power is on after an emergency shutdown, the relay will return to the state it was in when the power was off. The default value is **Off**.
4. If you select the **Manual** mode from the **Locking mode** drop-down list (**8**), locking is enabled when the **Open** button is enabled. Locking is disabled on the **Close** command.
   By timer—locking is enabled when the **Open** button is enabled. Locking is disabled after the time specified in the **Timer, ms** field (see step 2 of configuring working with exit relay).
5. Click the **Apply** 

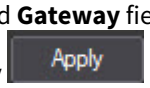
button to save the changes.

4.7.4 Setting up the BioSmart 4 network configuration

The BioSmart 4 controller network parameters are configured on the **Network configuration** tab on the settings panel of the **BioSmart 4** object.

1. In the **Controller IP** field, enter the IP address of the BioSmart 4 controller.



2. In the **Controller port** field, enter the controller port number. The default number is **20002**.
3. In the **Mask** and **Gateway** fields, enter the addresses of the network mask and gateway, respectively.
4. Click the **Apply** 

button to save the changes.

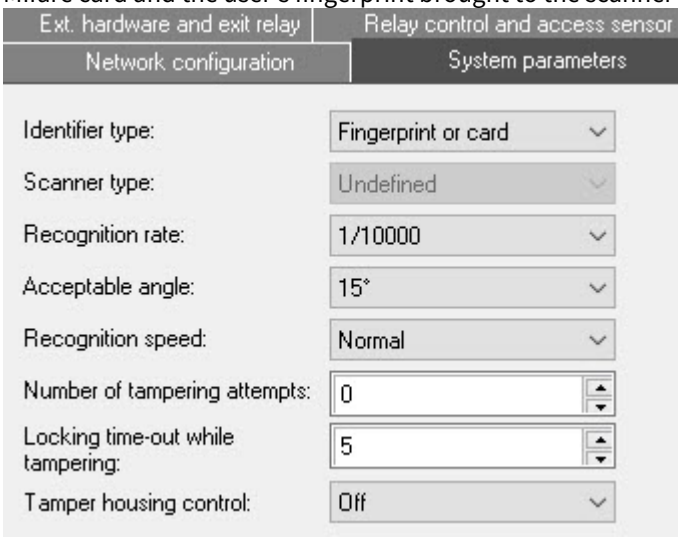
The BioSmart 4 controller network parameters are configured.

4.7.5 Configuring system parameters of the BioSmart 4 controller

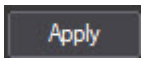
You can configure system parameters of the BioSmart 4 controller on the **System parameters** tab on the settings panel of the **BioSmart 4** object.

> **Attention!**
>
> You must set only the recommended parameter values. You can set other values only after consultation with the manufacturer of the *BioSmart* ACS. For these parameter values to take effect, the configuration must be saved to the controller (see Managing the configuration of the BioSmart 4 and BioSmart 5M controllers).

1. From the **Identifier type** drop-down list, select the access mode for this controller:
   a. **Fingerprint or card**—access is granted when a fingerprint is scanned or access card is brought to the scanner.
   b. **Card and fingerprint**—access is granted when the access card is brought to the scanner and the fingerprint is scanned within 10 seconds after the card is brought to the scanner.
   c. **Fingerprint on card**—access is granted after a positive comparison of the fingerprint template on the Mifare card and the user's fingerprint brought to the scanner within 10 seconds after the Mifare card.



> **Note**
>
> The **Scanner type** parameter is filled in automatically.

2. From the **Recognition rate** drop-down list, select the probability of false identification by fingerprint. The recommended value is **1/100000**.
3. Select the maximum acceptable angle of rotation of the fingerprint from the scanner axis in degrees. The recommended value is **30°**.
4. From the **Recognition speed** drop-down list, select the fingerprint recognition algorithm. The higher the recognition speed, the higher the probability of false access denial. It is recommended to use the **Auto** value. In this mode, the speed is determined automatically depending on the number of fingerprint templates in the controller database.
5. In the **Number of tampering attempts** field, enter the number of unsuccessful access attempts by any identifier, beyond which the controller will be locked for the **Locking time-out while tampering** (see step 6).
6. In the **Locking time-out while tampering** field, enter the controller locking time-out in seconds when the **Number of tampering attempts** parameter is exceeded.
7. From the **Tamper housing control** drop-down list, select the **On** value to enable tamper housing control. In this case, when the controller housing is tampered, the corresponding event is received and alarm signals are emitted. The default value is **Off**.
8. Click the **Apply** 

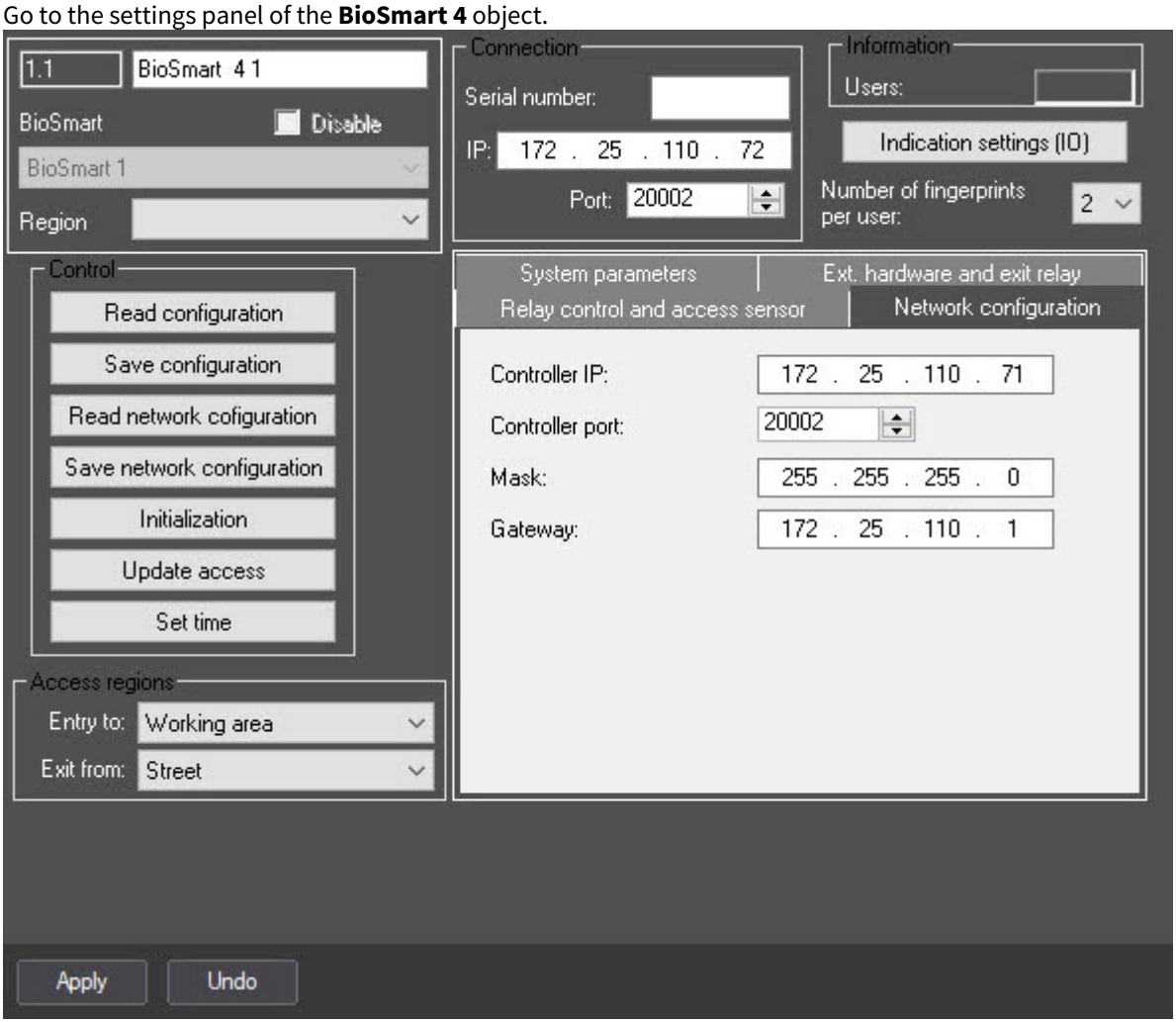
button to save the changes.

System parameters of the BioSmart 4 controller are configured.

4.7.6 Configuring operating scenarios for actuating devices of the BioSmart 4 controller

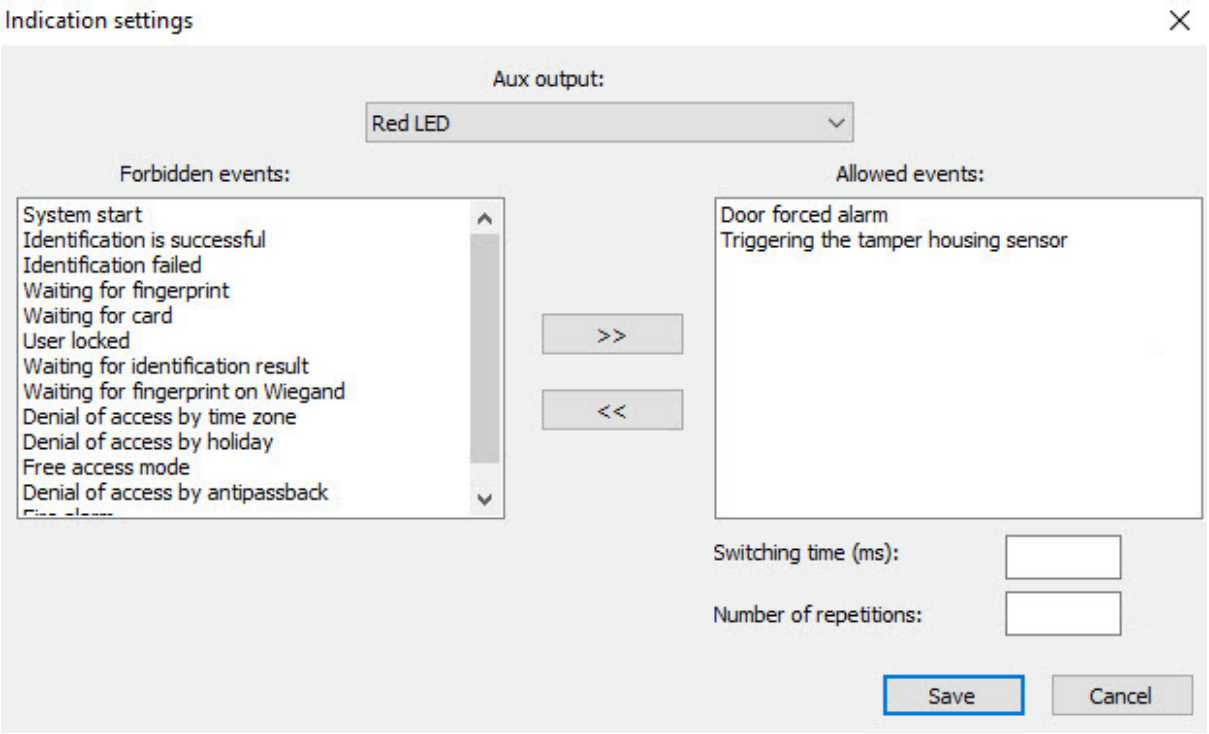
In *ACFA PSIM*, you can configure the reaction of actuating devices of the BioSmart 4 controller to certain events. For this, do the following:

1. Go to the settings panel of the **BioSmart 4** object.



2. Click the **Indication settings** button.

As a result, the **Indication settings** window opens.



3. From the **Aux output** drop-down list, select the actuating devices, which response to the event you need to configure.
4. From the **Forbidden events** list, move those events that must trigger this actuating device to the **Allowed events** list using the buttons.
5. In the **Switching time (ms)** field, enter the time in milliseconds that must pass after receiving the selected event before the actuating device is activated.
6. In the **Number of repetitions** field, enter the number of the actuating device responses when the selected event is received.
7. Repeat steps 3-6 for all required types of actuating devices.
8. Click the **Save** button. As a result, the **Indication settings** window closes.
9. Click the **Apply** button to save the changes.

The reaction of actuating devices of the BioSmart 4 controller to certain events is configured.

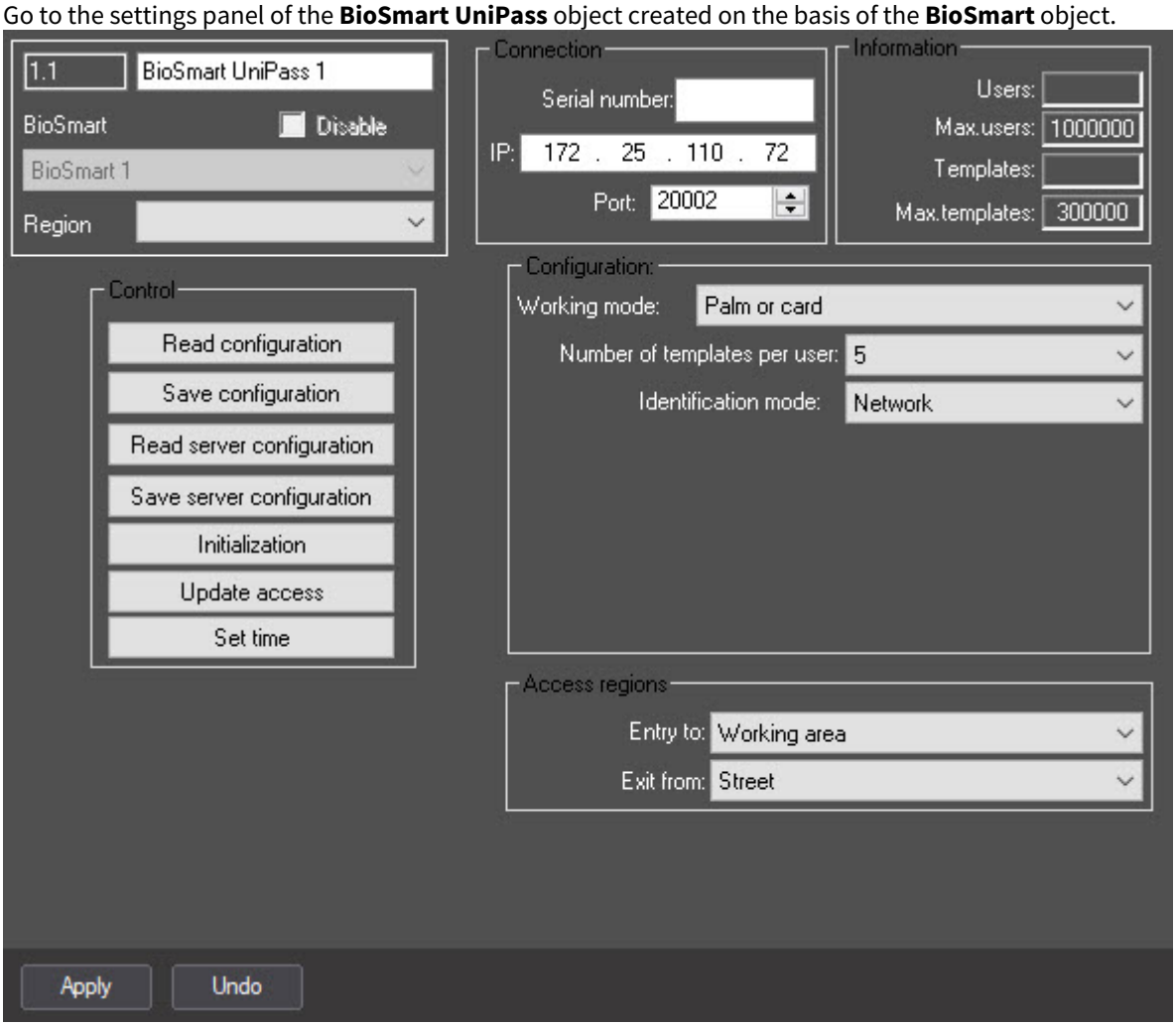
4.8 Setting up the BioSmart UniPass controller

4.8.1 Configuring the BioSmart UniPass controller

You can configure the BioSmart UniPass controller both when objects are created automatically and manually.

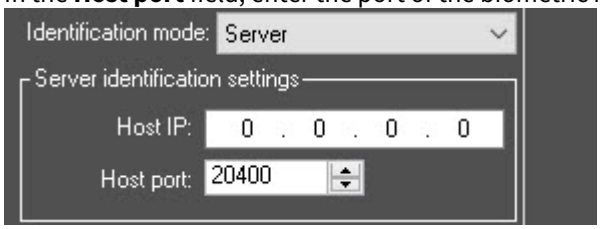
For this, do the following:

1. Go to the settings panel of the **BioSmart UniPass** object created on the basis of the **BioSmart** object.



2. From the **Working mode** drop-down list, select the controller working mode that corresponds to the serial number of the working model in the controller web interface:
    a. **Palm or card**—for a successful access, it is necessary to put a palm or a card to the reader. It is used to control one door in both directions, entrance by palm/card and exit by button.
    b. **Simplified turnstile**—for a successful access, it is necessary to put a palm or a card to the reader. It is used to control two doors, turnstile in both directions, entrance and exit by button without access sensors.
    c. **Turnstile with sensors**—for a successful access, it is necessary to put a palm or a card to the reader. It is used to control two doors, turnstile in both directions, entrance and exit by button with access sensors.
    d. **Card + palm**—for a successful access, it is necessary to put a card to the reader and then put a palm. It is used to control two doors, turnstile in both directions, entrance and exit by button without access sensors.
    e. **Template on card**—for a successful access, it is necessary to put a card with biometric template to the reader.
    f. **Custom 1**—user configurable model 1.
    g. **Custom 2**—user configurable model 2.
    h. **Custom 3**—user configurable model 3.
    i. **Custom 4**—user configurable model 4.
    j. **Custom 5**—user configurable model 5.

3. From the **Number of templates per user** drop-down list, select the number of possible templates of the user's palm vein pattern in the range 1-10. Templates are saved in the controller and used for user identification. If the number of templates saved in the *Access Manager* is greater than the specified number, only the number specified in the **Number of templates per user** parameter is saved to the controller. The default value is **5**.
4. From the **Identification mode** drop-down list, select the system operation mode:
    a. **Network**—operation mode in which access to the controller is assigned from the manufacturer's software BioSmart Studio. Palm templates are stored in the controller memory.
    b. **Local**—operation mode of the BioSmart UniPass controller that differs from the **Network** operation mode by the database storage logic.
    c. **Server identification**—operation mode in which palm templates are stored on an external biometric identification server instead of the controller local memory. In this mode, comparison of biometric data is performed on an external server, which allows you to expand the number of templates and increase the speed of identification. The following parameters of the external Biometric Identification Server must be specified:
        i. In the **Host IP** field, enter the IP address of the biometric identification Server.
        ii. In the **Host port** field, enter the port of the biometric identification Server.



> **Attention!**
>
> If the **Server identification** mode is used, then the biometric identification Server must be configured on the parent object (see Configuring the biometric identification Server).

5. Click the **Save configuration** button to write the settings to the controller (see Managing the configuration of the BioSmart UniPass and Biosmart PV-WTC controllers).
6. Click the **Apply** button.

Configuring the BioSmart UniPass controller is complete.

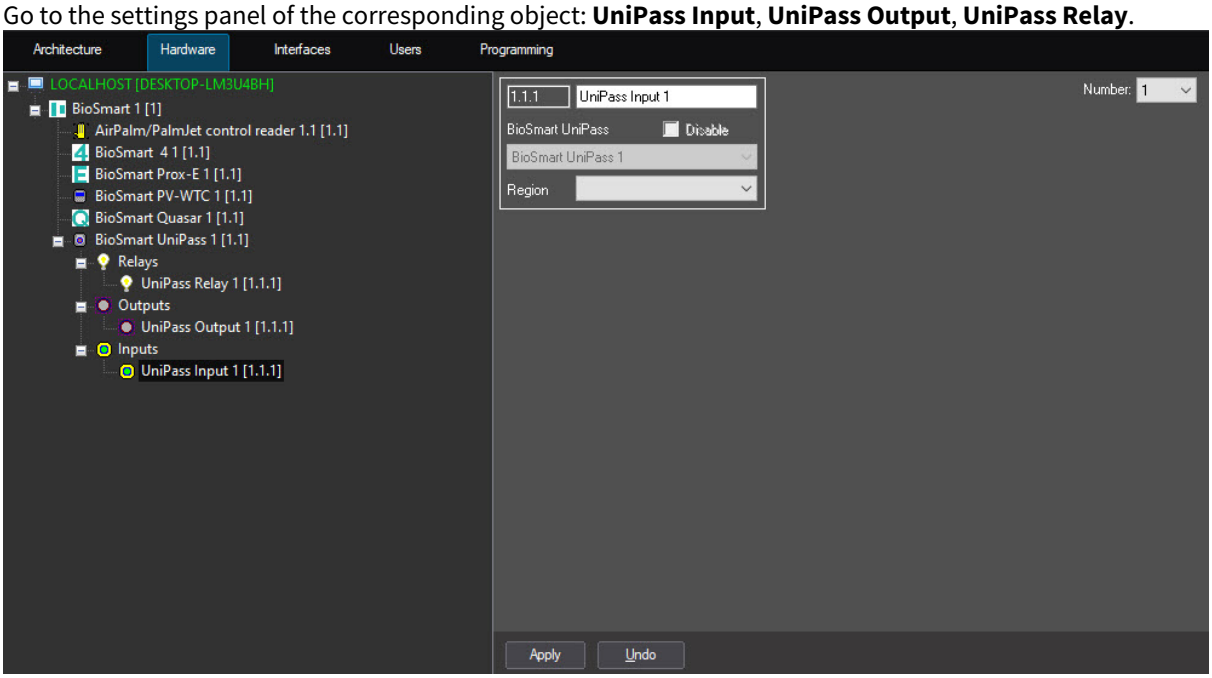
4.8.2 Configuring inputs, outputs and relays of the BioSmart UniPass controller

Inputs, outputs, and relays of the BioSmart UniPass controller in the *ACFA PSIM* system are represented by the **UniPass Input**, **UniPass Output**, and **UniPass Relay** objects, respectively. You can create these objects in the following ways:

- automatically from the **BioSmart UniPass** object settings (see Managing the configuration of the BioSmart UniPass and Biosmart PV-WTC controllers);
- manually on the basis of the **BioSmart UniPass** object.

Input, output, and relay of the BioSmart UniPass controller are configured in the same way:

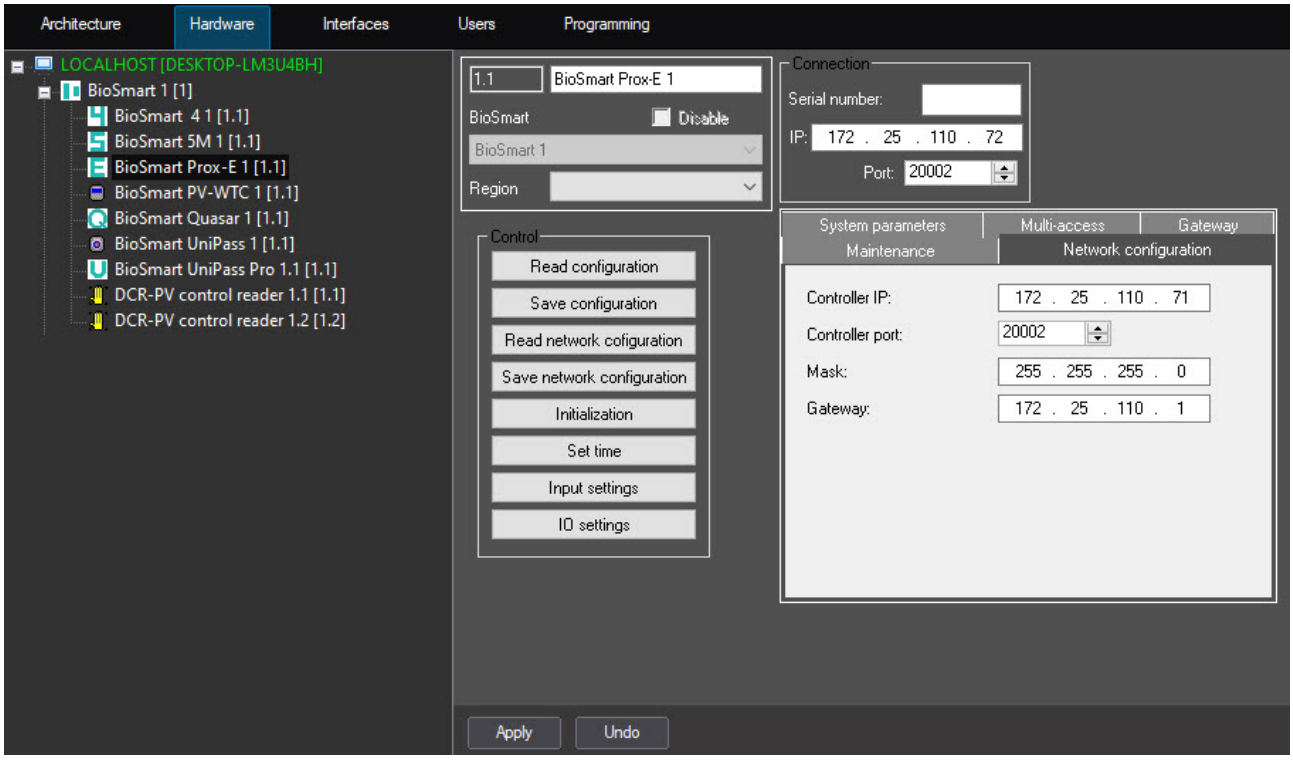
1. Go to the settings panel of the corresponding object: **UniPass Input**, **UniPass Output**, **UniPass Relay**.



2. From the **Number** drop-down list, select the number of the controller input or output in the range from 1 to 6. Select the number of the relay from 1 to 2.
3. Click the **Apply** button.

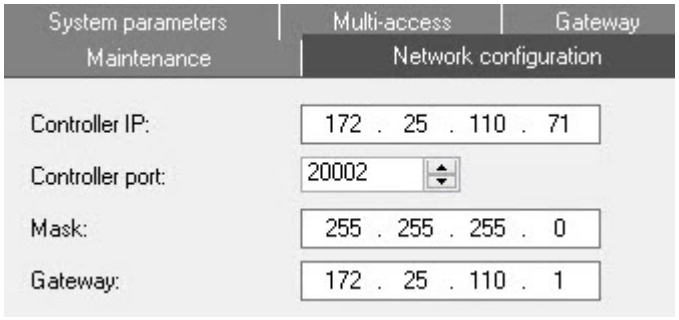
4.9 Setting up the BioSmart Prox-E controller

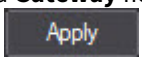
You can configure the BioSmart Prox-E controller on the settings panel of the **BioSmart Prox-E** object created on the basis of the **BioSmart** object.



4.9.1 Setting up the BioSmart Prox-E network configuration

The BioSmart Prox-E controller network parameters are configured on the **Network configuration** tab on the settings panel of the **BioSmart Prox-E** object.

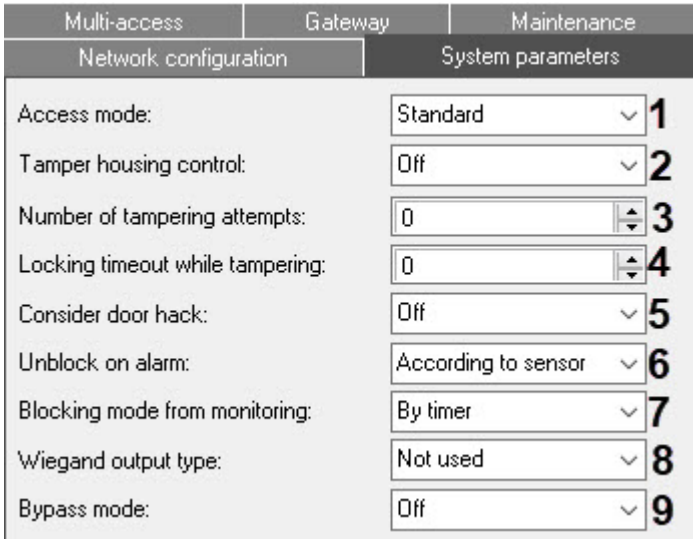


1. In the **Controller IP** field, enter the IP address of the BioSmart Prox-E controller.
2. In the **Controller port** field, enter the controller port number. The default number is **20002**.
3. In the **Mask** and **Gateway** fields, enter the addresses of the network mask and gateway, respectively.
4. Click the **Apply**  button to save the changes.

The BioSmart Prox-E controller network parameters are configured.

4.9.2 Configuring system parameters of the BioSmart Prox-E controller

You can configure system parameters of the BioSmart Prox-E controller on the **System parameters** tab on the settings panel of the **BioSmart Prox-E** object.



1. From the **Access mode** drop-down list (**1**), select the controller operating mode:
    a. **Standard**—access by fingerprint or access card.
    b. **Multi-access**—access to the premises only when different employees simultaneously scan fingerprints (simultaneously put access cards to the scanner) on different readers. To work in this mode, it is necessary to connect at least two readers to the controller.
    c. **Gateway**—access to a pass-through room. The second door cannot be opened until the first door is closed.
    d. **Maintenance**—access to the premises only when two employees, who are assigned access to this reader, are successfully identified in turn on one reader.
2. From the **Tamper housing control** drop-down list (**2**):
    a. Select the **On** value to enable the tamper housing control. When the controller housing is tampered, the corresponding event will be received and the alarm will be activated.
    b. Select the **Off** value to disable the tamper housing control. When the controller housing is tampered, the corresponding event won't be received and the alarm won't be activated.
3. In the **Number of tampering attempts** field (**3**), enter the number of unsuccessful access attempts by any identifier. When this number is exceeded, the controller will be locked for the time specified in the **Locking timeout while tempering** field (see step 4).
4. In the **Locking timeout while tempering** field (**4**), enter the time in seconds, for which the controller will be locked when the number of unsuccessful access attempts is exceeded (see step 3).
5. From the **Consider door hack** drop-down list (**5**) select the **On** value to enable the door hack control, so that the controller generates a "Door hack" event when there is an active signal from the door sensor without a preceding "Identification successful" event. The default value is **Off**.
6. From the **Unblock on alarm** drop-down list (**6**), select the mode of door unblocking in case of an alarm **According to sensor** or **Once**.
7. From the **Blocking mode from monitoring** drop-down list (**7**), select the algorithm by which the controller relay will be disabled after it is enabled with the **Open** button:
    a. **By timer**—the relay will be disabled after the time specified in the input/output setting of the reader working with the controller;
    b. **Manual**—the relay will be disabled only when the **Close** button is clicked.
8. From the **Wiegand output type** drop-down list (**8**), select the protocol type of the Wiegand output interface of the BioSmart Prox-E controller. It is used for integration with the third-party ACS.
    a. **Not used**—third-party device isn't connected to the Wiegand output of the BioSmart Prox-E controller.
    b. **Wiegand-26 (W/P)**—third-party ACS controller using the Wiegand 26 protocol with parity check bits is connected to the Wiegand output of the BioSmart Prox-E controller.

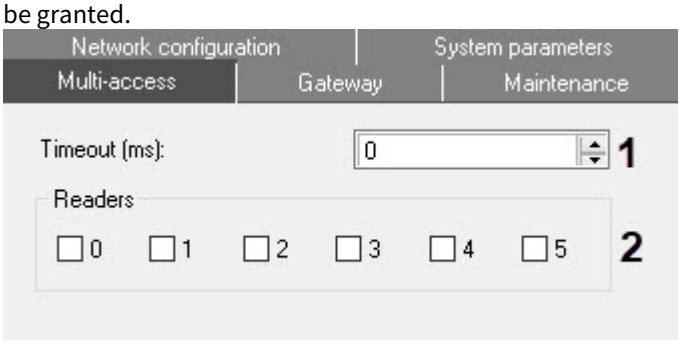
c. **Wiegand-32**—third-party ACS controller using the Wiegand 32 protocol is connected to the Wiegand output of the BioSmart Prox-E controller.

9. From the **Bypass mode** drop-down list (**9**), select the **On** value to enable the bypass mode. In this case, the card not registered in the *ACFA PSIM* database will be available for transmission to the third-party ACS controller via the Wiegand output of the Biosmart Prox-E controller. The default value is **Off**.
10. Click the **Apply** Apply button to save the changes.

4.9.3 Configuring the Multi-access mode of the BioSmart Prox-E controller

You can configure the Multi-access mode of the BioSmart Prox-E controller on the **Multi-access** tab of the settings panel of the **BioSmart Prox-E** object.

1. In the **Timeout (ms)** field (**1**), enter the maximum possible time in seconds between scanning fingerprints (putting access cards to the scanner) from different sides of the door. If this time is exceeded, access won't be granted.

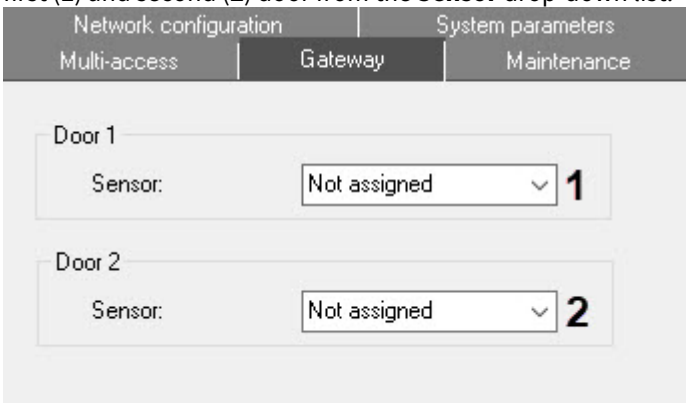


2. In the **Readers** field (**2**), select the readers through which the maintainer will access.
3. Click the **Apply** Apply button to save the changes.

4.9.4 Configuring the Gateway mode of the BioSmart Prox-E controller

You can configure the Gateway mode of the BioSmart Prox-E controller on the **Gateway** tab of the settings panel of the **BioSmart Prox-E** object.

1. Match the door sensors to the controller discrete outputs by selecting the required controller output for the first (**1**) and second (**2**) door from the **Sensor** drop-down list.

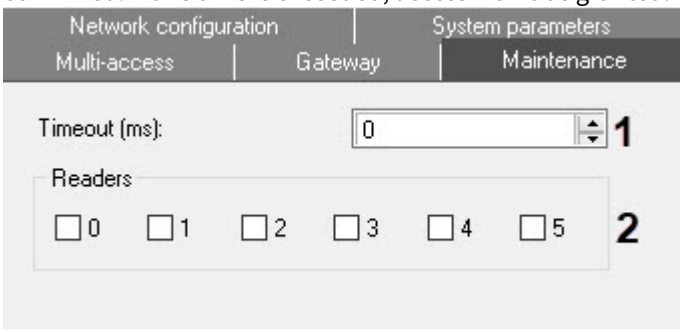


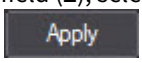
2. Click the **Apply** Apply button to save the changes.

4.9.5 Configuring the Maintenance mode of the BioSmart Prox-E controller

You can configure the Maintenance mode of the BioSmart Prox-E controller on the **Maintenance** tab of the settings panel of the **BioSmart Prox-E** object.

1. In the **Timeout (ms)** field (**1**), enter the time in milliseconds, during which the maintainer access must be confirmed. If this time is exceeded, access won't be granted.

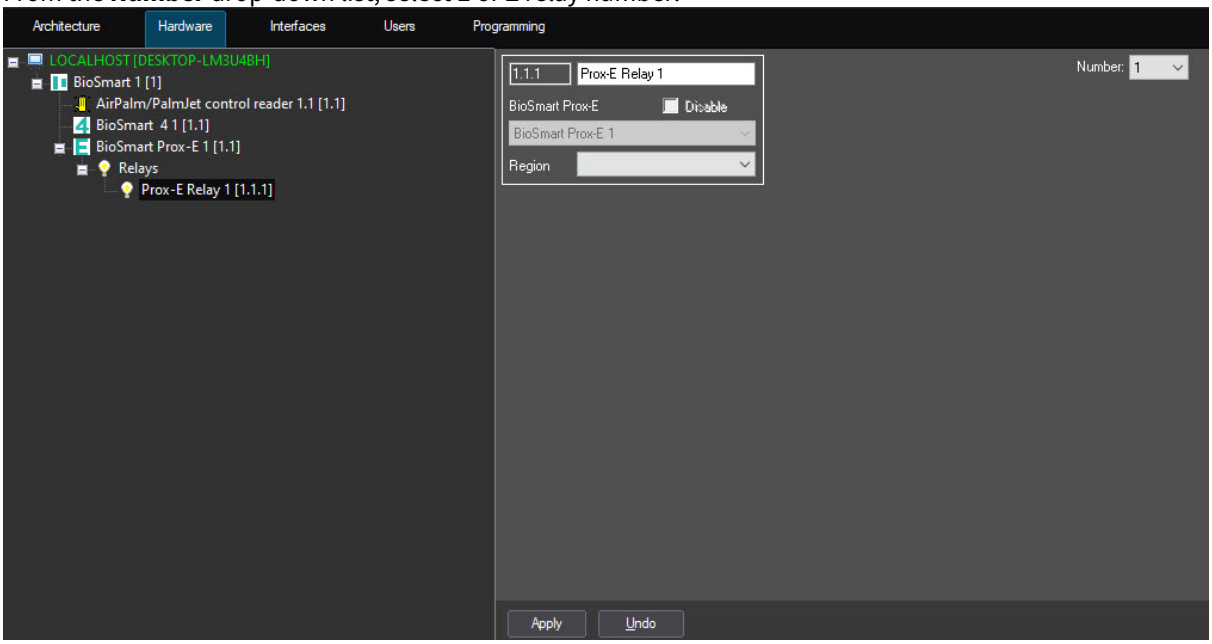


2. In the **Readers** field (**2**), select the readers through which the maintainer will access.
3. Click the **Apply**  button to save the changes.

4.9.6 Configuring the relay of the BioSmart Prox-E controller

To configure the relay of the BioSmart Prox-E controller, do the following:

1. Go to the settings panel of the **Prox-E Relay** object created on the basis of the **BioSmart Prox-E** object.
2. From the **Number** drop-down list, select **1** or **2** relay number.



3. Click the **Apply** button to save the changes.

4.9.7 Configuring the BioSmart Mini reader

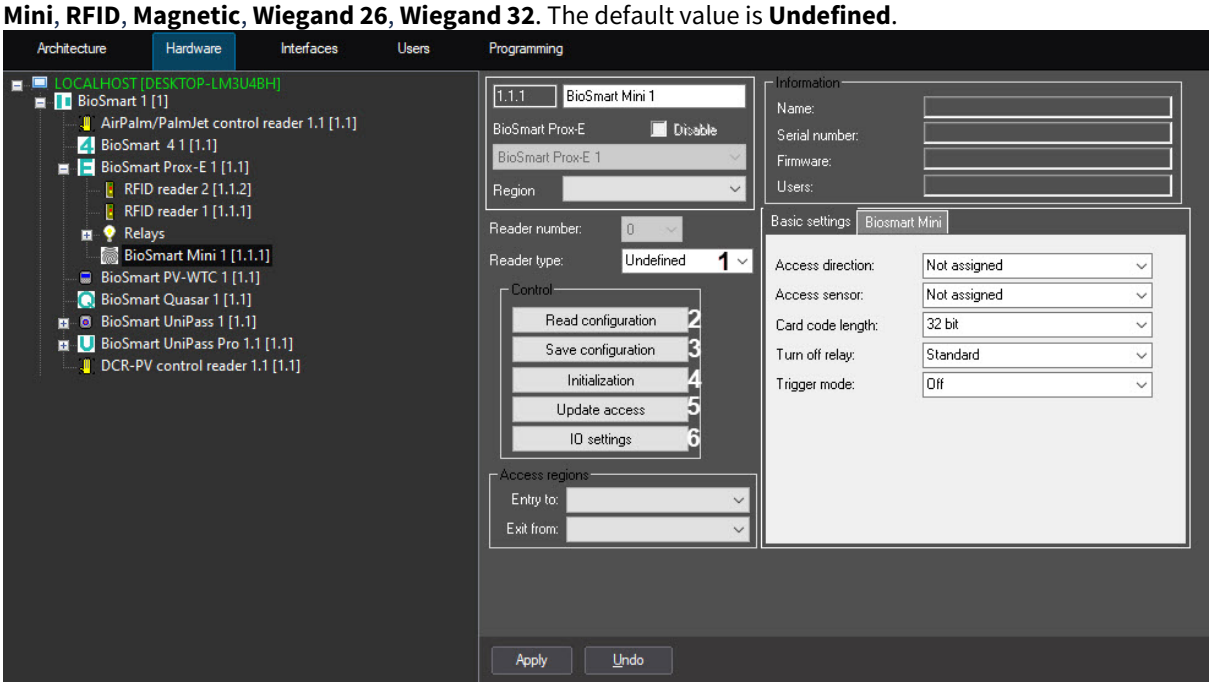
On the page:

- General settings
- Control
- The Basic settings tab
- The Biosmart Mini tab

You can configure the BioSmart Mini reader of the BioSmart Prox-E controller on the settings panel of the **BioSmart Mini** object created on the basis of the **BioSmart Prox-E** object.

General settings

1. From the **Reader type** drop-down list (**1**), select the reader type: **Wiegand Converter**, **BioSmart Mini**, **RFID**, **Magnetic**, **Wiegand 26**, **Wiegand 32**. The default value is **Undefined**.

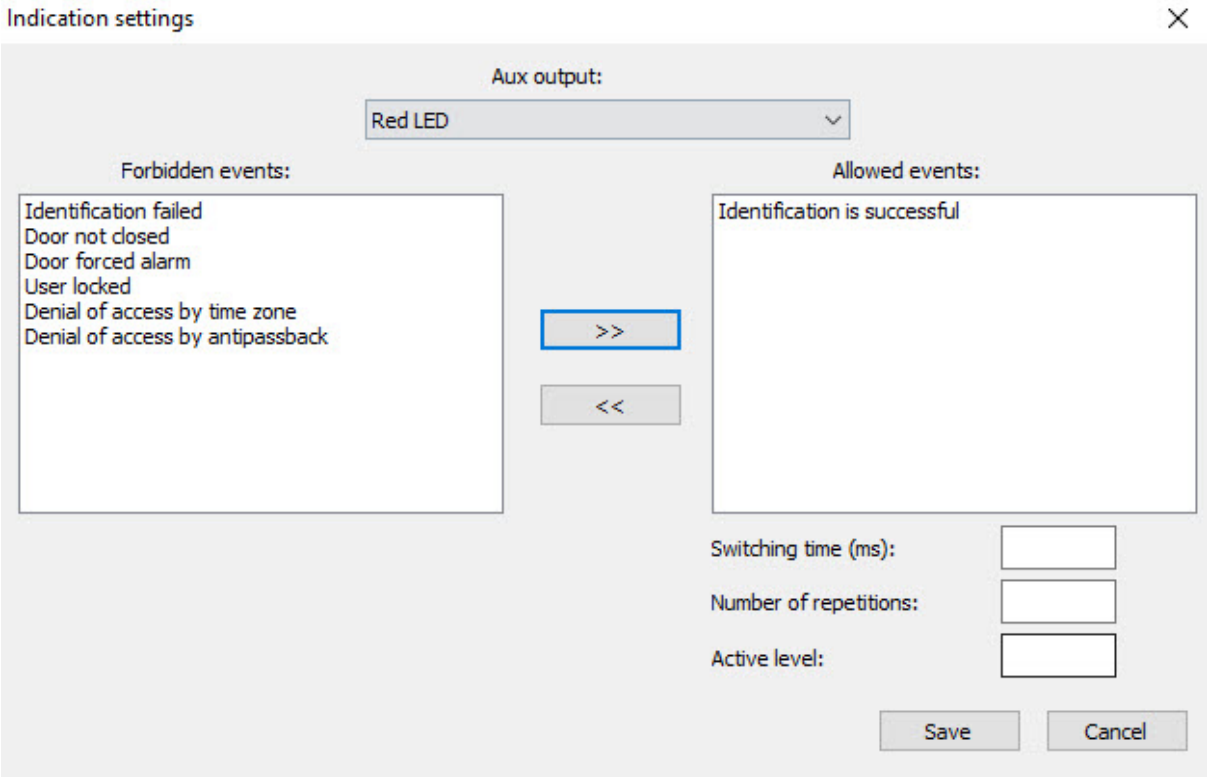


> **Note**
>
> The **Reader number** parameter is filled in automatically.

Control

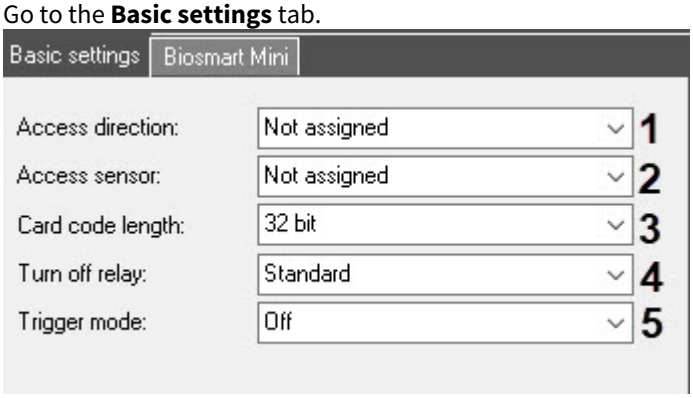
1. Click the **Read configuration** button (**2**) to read the configuration from the BioSmart Prox-E controller.
2. Click the **Save configuration** button (**3**) to save the configuration to the BioSmart Prox-E controller.
3. Click the **Initialization** button (**4**) to delete all data on users, access cards, palm vein templates, and time schedules.
4. Click the **Update access** button (**5**) to write access data (palm vein templates, access cards, user time schedules, and so on) to the controller.

5. Click the **IO settings** button (**6**), if you want to configure operating scenarios for the actuating devices of the BioSmart Prox-E controller for certain events.
   As a result, the **Indication settings** window will open, where you can configure the operating scenarios (see Configuring operating scenarios for actuating devices of the BioSmart 4 controller).



The Basic settings tab

1. Go to the **Basic settings** tab.

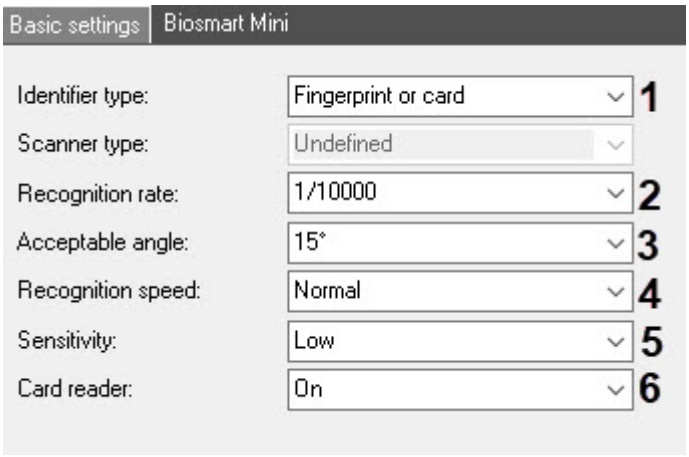


2. From the **Access direction** drop-down list (**1**), select the **Input**, **Output** or **Not assigned** (default) value.
3. From the **Access sensor** drop-down list (**2**), select a discrete input of the BioSmart Prox-E controller or the BioSmart Prox-E RCU, to which the access sensor will be connected: **Input #1**, **Input #2**, **Input #3**, **Input #4**, **Input #1 RCU**, **Input #2 RCU**, **Input #3 RCU**, **Input #4 RCU**.
4. From the **Card code length** drop-down list (**3**), select the length of the RFID card code that is read by the embedded card reader: **32 bit** (default) or **24 bit**.
5. From the **Turn off relay** drop-down list (**4**), select the operating mode of locking the actuating device after the employee's access:
   a. **Standard** (default)—locking by timer for four seconds.

   b. **On door opening**—locking happens on door opening/at the beginning of turnstile rotation.
   c. **On door closing**—locking happens on door closing/at the end of turnstile rotation.
6. From the **Trigger mode** drop-down list (**5**), select the **On** value to enable the trigger mode, so that the relay changes its state every time the access is successful. The default value is **Off**.

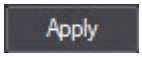
The Biosmart Mini tab

1. Go to the **Biosmart Mini** tab.



2. From the **Identifier type** drop-down list (**1**), select which identification algorithms will be used by the reader: **Fingerprint or card** (default), **Card and fingerprint**, **Fingerprint or SmartID card**.

> **Note**
>
> The **Scanner type** parameter is filled in automatically and isn't editable.

3. From the **Recognition rate** drop-down list (**2**), select the probability of false identification by fingerprint: **1/10000**, **1/100000**, **1/1000000**, **1/10000000**, **1/100000000**, **Auto. Normal mode**, **Auto. Strict mode**, **Auto. The strictest mode**. The recommended value is **1/100000**.
4. From the **Acceptable angle** drop-down list (**3**), select the maximum acceptable angle of rotation of the fingerprint from the scanner axis in degrees: **15°**, **30°**, **45°**, **60°**, **75°**, **90°**. The default value is **15°**, the recommended value is **30°**.
5. From the **Recognition speed** drop-down list (**4**), select the algorithm of fingerprint recognition: **Normal**, **Fast Mode 1**, **Fast Mode 2**, **Fast Mode 3**, **Fast Mode 4**, **Fast Mode 5**, **Auto**. The higher the recognition speed, the greater the probability of false access denial. It is recommended to use the **Auto** value. In this mode the speed will be determined automatically depending on the number of fingerprint templates in the controller database.
6. From the **Sensitivity** drop-down list (**5**), select the sensitivity level of the scanner when scanning fingerprints: **Low**, **Normal**, **High**.
7. From the **Card reader** drop-down list (**6**), select the **Off** value to disable the embedded RFID card reader. By default, the reader is enabled (**On**).
8. Click the **Apply** 

button to save the changes.

4.9.8 Configuring the RFID reader

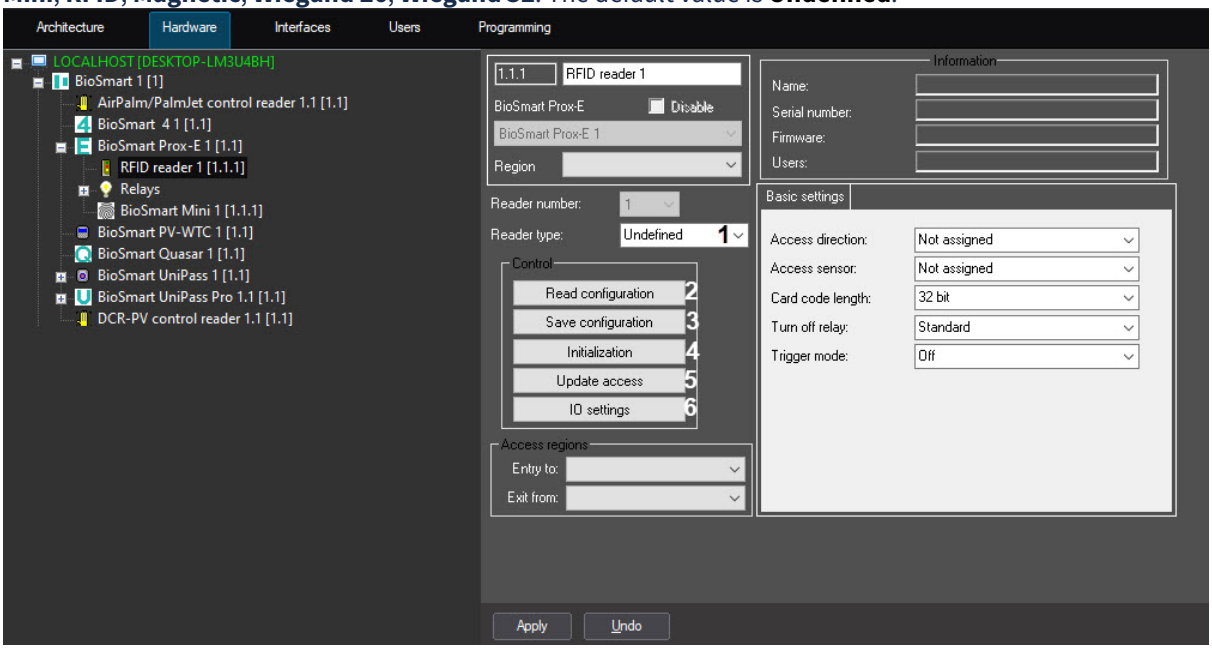
On the page:

- General settings
- Control
- The Basic settings tab

You can configure the RFID reader of the BioSmart Prox-E controller on the settings panel of the **RFID reader** object created on the basis of the **BioSmart Prox-E** object.

General settings

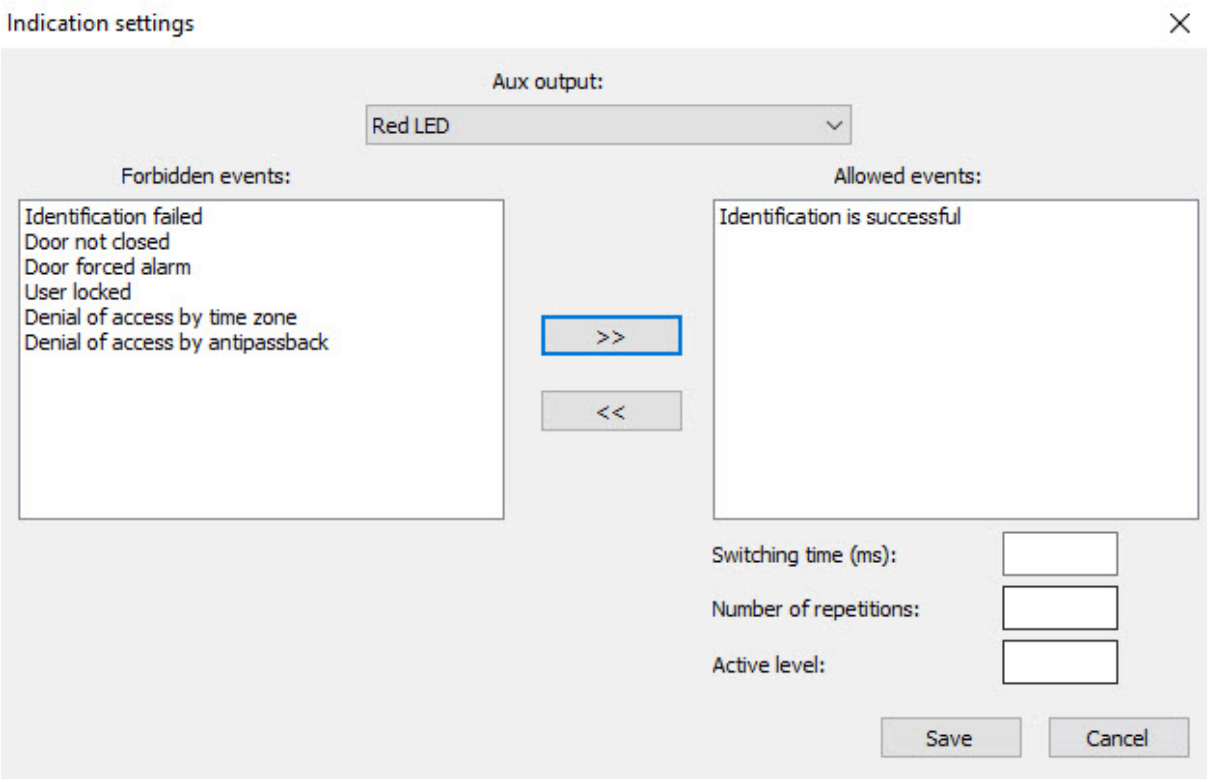
1. From the **Reader type** drop-down list (**1**), select the reader type: **Wiegand Converter**, **BioSmart Mini**, **RFID**, **Magnetic**, **Wiegand 26**, **Wiegand 32**. The default value is **Undefined**.



> **Note**
>
> The **Reader number** parameter is filled in automatically.

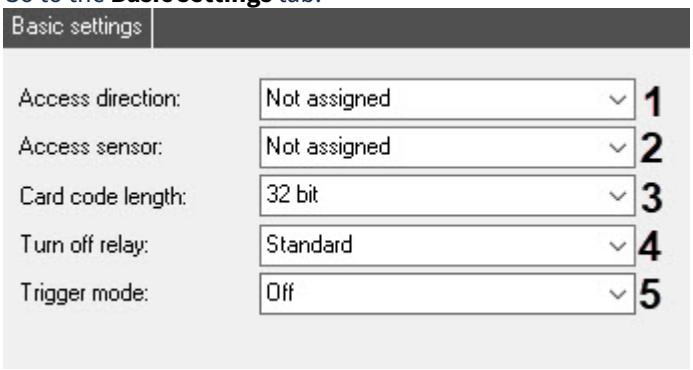
Control

1. Click the **Read configuration** button (**2**) to read the configuration from the BioSmart Prox-E controller.
2. Click the **Save configuration** button (**3**) to save the configuration to the BioSmart Prox-E controller.
3. Click the **Initialization** button (**4**) to delete all data on users, access cards, palm vein templates, and time schedules.
4. Click the **Update access** button (**5**) to write access data (palm vein templates, access cards, user time schedules, and so on) to the controller.
5. Click the **IO settings** button (**6**), if you want to configure operating scenarios for the actuating devices of the BioSmart Prox-E controller for certain events.
   As a result, the **Indication settings** window will open, where you can configure the operating scenarios (see Configuring operating scenarios for actuating devices of the BioSmart 4 controller).

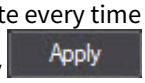


The Basic settings tab

1. Go to the **Basic settings** tab.



2. From the **Access direction** drop-down list (**1**), select the **Input**, **Output** or **Not assigned** (default) value.
3. From the **Access sensor** drop-down list (**2**), select a discrete input of the controller or the *BioSmart* RCU, to which the access sensor will be connected: **Input #1**, **Input #2**, **Input #3**, **Input #4**, **Input #1 RCU**, **Input #2 RCU**, **Input #3 RCU**, **Input #4 RCU**.
4. From the **Card code length** drop-down list (**3**), select the length of the RFID card code that is read by the embedded card reader: **32 bit** (default) or **24 bit**.
5. From the **Turn off relay** drop-down list (**4**), select the operating mode of locking the actuating device after the employee's access:
    a. **Standard** (default)—locking by timer for four seconds.
    b. **On door opening**—locking happens on door opening/at the beginning of turnstile rotation.
    c. **On door closing**—locking happens on door closing/at the end of turnstile rotation.

6. From the **Trigger mode** drop-down list (**5**), select the **On** value to enable the trigger mode, so that the relay changes its state every time the access is successful. The default value is **Off**.
7. Click the **Apply** 

button to save the changes.

4.10 Setting up the BioSmart Quasar terminal

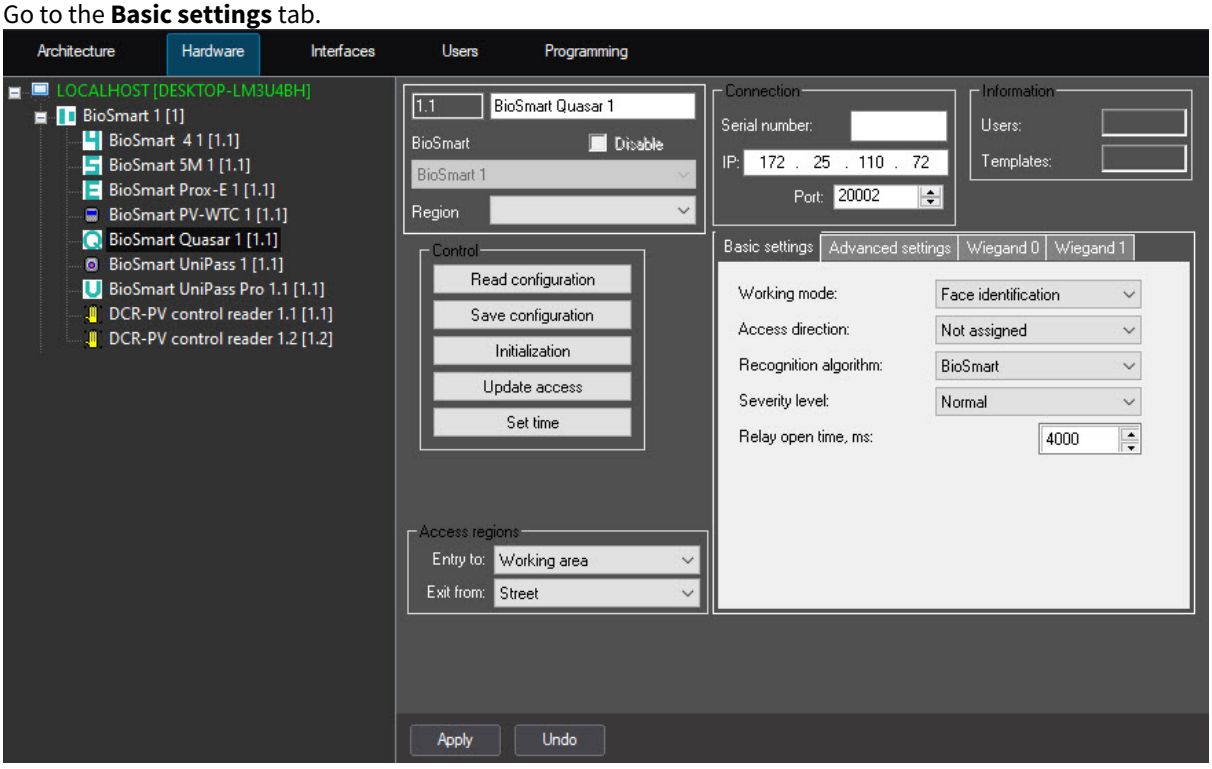
On the page:

- The Basic settings tab
- The Advanced settings tab
- The Wiegand 0 and Wiegand 1 tabs

You can configure the BioSmart Quasar terminal on the settings panel of the **BioSmart Quasar** object created on the basis of the **BioSmart** object.

4.10.1 The Basic settings tab

1. Go to the **Basic settings** tab.



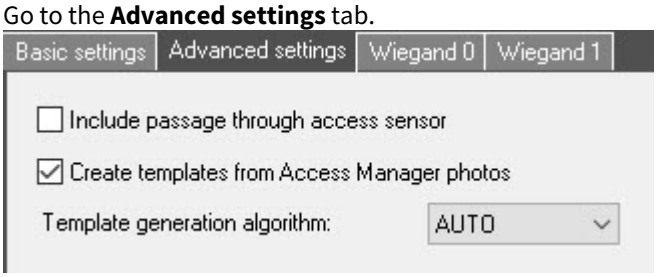
2. From the **Working mode** drop-down list, select the working mode of the terminal:
   a. **Face identification**—automatic identification of an employee by face.
   b. **Entry/exit by button**—the terminal waits for an employee to press the Enter or Exit button, after that it starts employee identification.

c. **Card + face**—the terminal waits for the RFID card to be put to the terminal reader. If the card code is found, the terminal scans the biometric data of the employee's face and compares it with the biometric template corresponding to the presented card.
d. **RT identification**—the terminal reads the biometric data of the face and sends it to the Rt Lab server for identification.
e. **Visitors check**—the terminal waits for a visitor to present a QR code confirming the presence of a COVID certificate of vaccination or past medical history. After that, the terminal verifies the authenticity and validity period of the certificate. If the verification is successful, a message appears on the screen asking to wear a mask. Identification is considered successful only if a valid QR code is presented and the mask is put on the face.
f. **REST server mode**—the terminal is a server that receives requests for identification.
g. **Entry/exit + room**—the terminal waits for an employee to press the Entry, Exit or Room button, after that it starts employee identification. Operation of the terminal in the **Entry/exit + room** mode is similar to the operation in the **Entry/exit by button** mode, but an additional **Room** button is displayed on the screen. After pressing the **Room** button and successful identification, the employee is granted access to their profile, which contains information about the employee.

3. From the **Access direction** drop-down list, select the **Input**, **Output** or **Not assigned** (default) value.
4. From the **Recognition algorithm** drop-down list, select the recognition algorithm that will be used: **BioSmart** (default) or **3DiVi**—image processing algorithm from the 3DiVi company.
5. From the **Severity level** drop-down list, select the level of identification severity: **Normal** (default), **Higher**, **High**, **Lower**, **Low**. The parameter determines how accurately the biometric data of the user's face, received from the camera, must match the biometric template stored in the database.
6. In the **Relay open time, ms** field, enter the time in milliseconds during which the terminal relay will be opened.

4.10.2 The Advanced settings tab

1. Go to the **Advanced settings** tab.

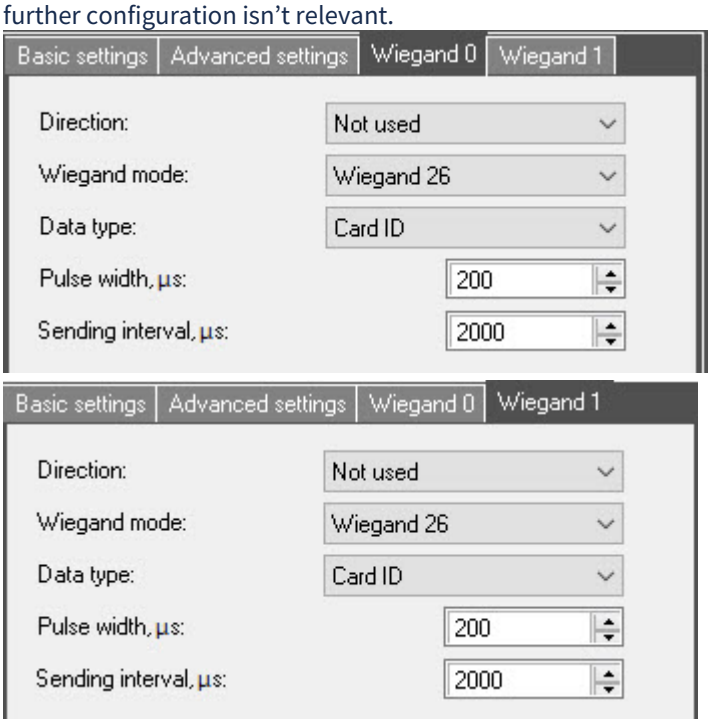


2. Set the **Include passage through access sensor** checkbox to take into account employee passages through door sensor.
3. Set the **Create templates from Access Manager photos** checkbox, so that when a user is written to the *Access Manager* and if they have a photo, a biometric template is also created according to the selected algorithm (see step 3) and written to the BioSmart Quasar terminal.
4. From the **Template generation algorithm** drop-down list, select an algorithm for creating a user biometric template: **AUTO**, **ALGO2**, or **ALGO5**. When you select **ALGO2** or **ALGO5**, templates are created on *Axxon PSIM* side and are ready to be written to the terminal. If you select **AUTO**, a user photo is saved to the terminal and a template is created on the terminal side according to the algorithm configured in it.

4.10.3 The Wiegand 0 and Wiegand 1 tabs

1. Go to the **Wiegand 0** or **Wiegand 1** tab.
2. From the **Direction** drop-down list, select the direction of information transfer via the Wiegand interface:
   a. **Wiegand Out**—used to transfer information to external devices.
   b. **Wiegand In**—used to receive information from external devices.

c. **Not used**—the Wiegand interface isn't used to transfer information (default). If you select this value, further configuration isn't relevant.



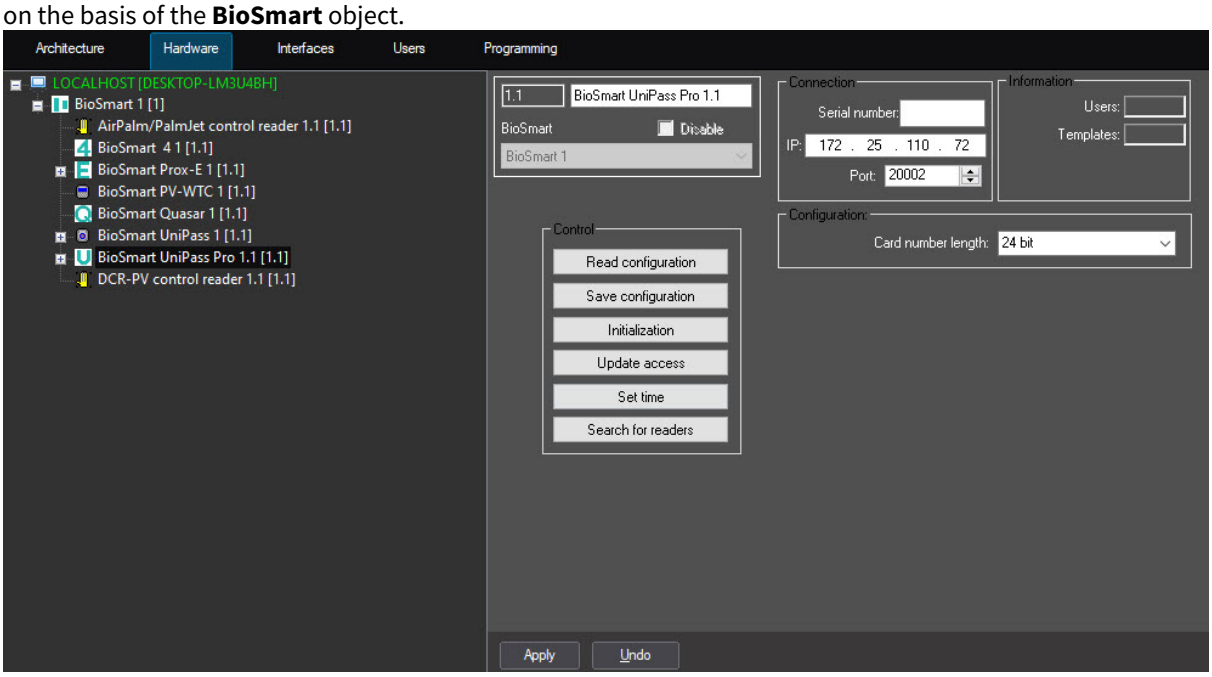
3. From the **Wiegand mode** drop-down list, select the operation mode of the Wiegand interface: **Wiegand 26**, **Wiegand 32**, **Wiegand 34**, **Wiegand 37**, **Wiegand 40**, **Wiegand 42**, **Wiegand 48**, **Wiegand 64**.
4. From the **Data type** drop-down list, select the type of the transferred data: **Card ID**—transfer of the RFID card code (default) or **Employee ID**—transfer of the employee code (ID).
5. From the **Pulse width, µs** drop-down list and **Sending interval, µs** drop-down list, select the values of the data transfer parameters via the Wiagand interface. Default values: **Pulse width, µs**—**200 µs**, **Sending interval, µs**—**2000 µs**.
6. Click the **Apply** button to save the changes.

Configuring the BioSmart Quasar terminal is complete.

4.11 Setting up the BioSmart UniPass Pro and BioSmart UniPass Pro 2 controllers

To set up the configuration of the BioSmart UniPass Pro and BioSmart UniPass Pro 2 controllers, do the following:

1. Go to the settings panel of the **BioSmart UniPass Pro** or **BioSmart UniPass Pro 2** objects that are created on the basis of the **BioSmart** object.



2. From the **Card number length** drop-down list, select **24 bit**, **32 bit**, or **64 bit**. The default value is **24 bit**.
3. Click the **Apply** button to save the changes.

Configuration of the BioSmart UniPass Pro and BioSmart UniPass Pro 2 controllers is complete.

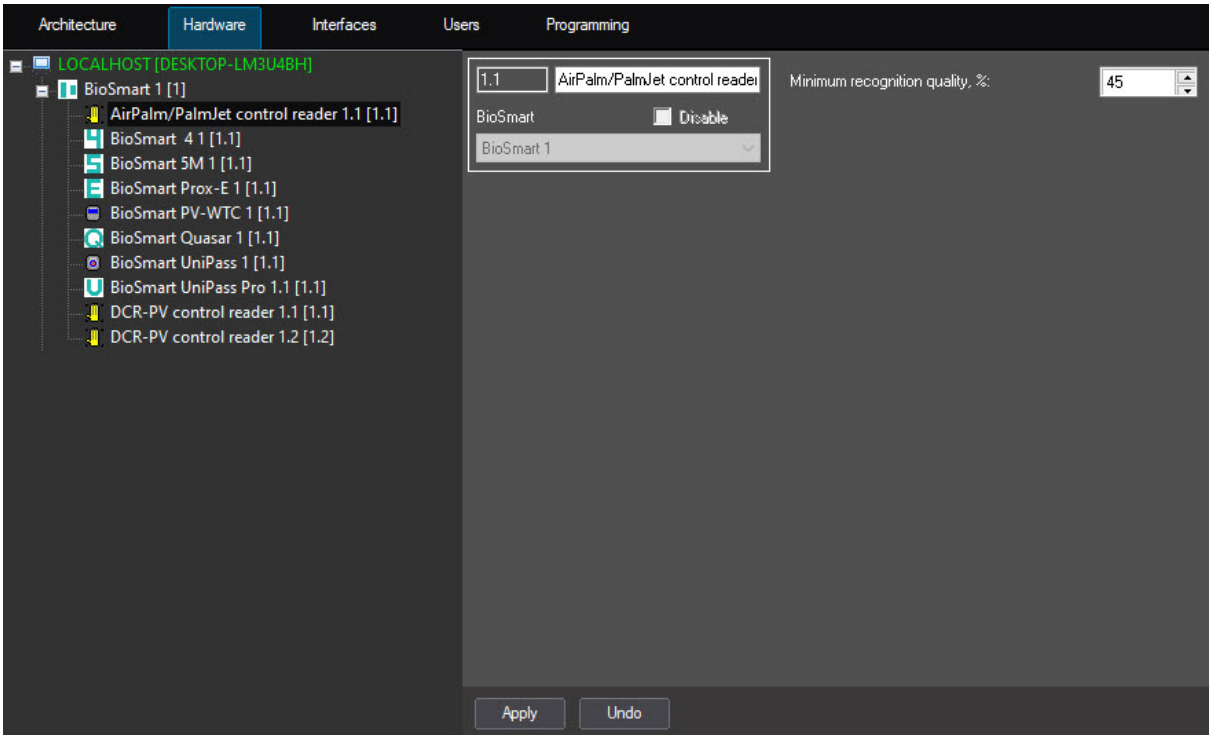
4.12 Configuring the BioSmart control readers

The AirPalm/PalmJet and DCR-PV *BioSmart* biometric readers are used for scanning palm vein patterns and transferring the obtained image to the *BioSmart* controller. On their basis, digital biometric templates of palm veins are created.

The **AirPalm/PalmJet control reader** and the **DCR-PV control reader** are created on the basis of the *BioSmart* parent object.

You can configure the AirPalm/PalmJet control reader and the DCR-PV control reader in the same way. For this, do the following:

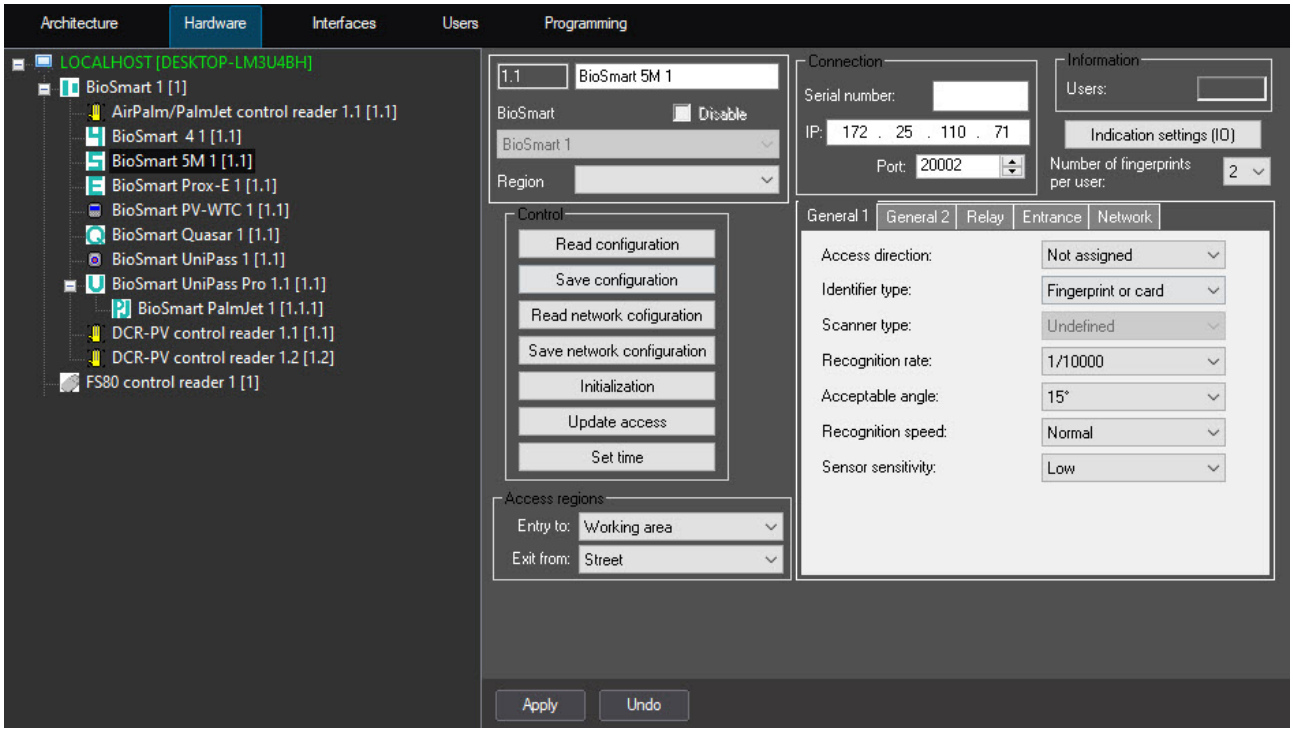
1. Go to the settings panel of the corresponding object.
2. In the **Minimum recognition quality, %** field, specify the minimum quality of palm vein templates recognition in percent. The default value is **45**%.



3. Click the **Apply** button to save the changes.

4.13 Configuring the BioSmart 5M controller

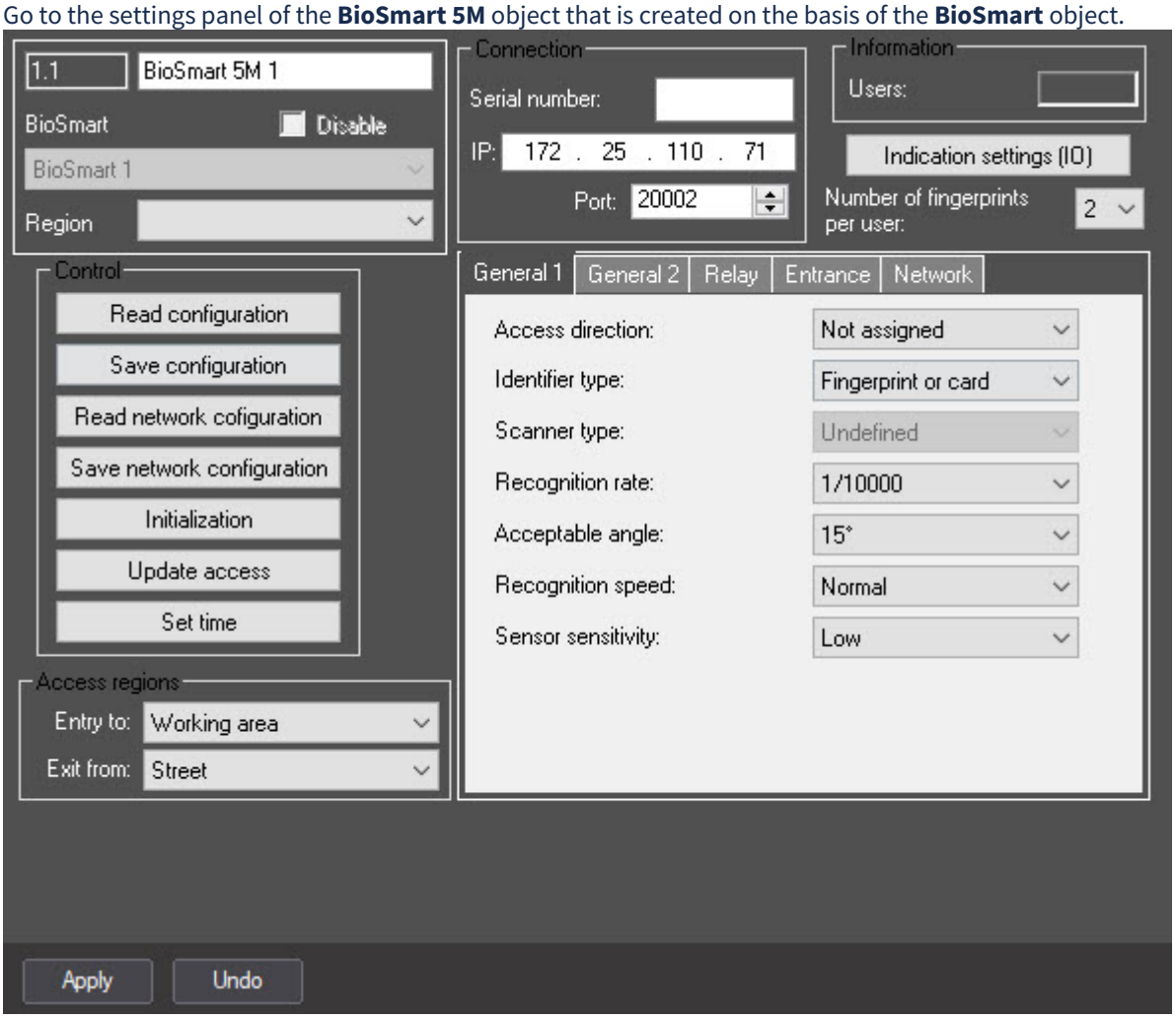
You can configure the BioSmart 5M controller on the settings panel of the **BioSmart 5M** object that is created on the basis of the **BioSmart** object as a result of device search (see Configuring the BioSmart parent object) or manually (see Configuring the connection of the BioSmart controller or terminal to the ACFA PSIM server).



4.13.1 Configuring the number of fingerprint templates of the users of the BioSmart 5M controller

To configure the number of user fingerprint templates, do the following:

1. Go to the settings panel of the **BioSmart 5M** object that is created on the basis of the **BioSmart** object.



2. From the **Number of fingerprints per user** drop-down list, select the maximum number of templates of the user's fingerprints in the range 0-5. Templates are saved in the BioSmart 5M controller and used for user identification. If the number of templates saved in the *Access Manager* is greater than the specified number, only the number specified in the **Number of fingerprints per user** parameter is saved to the controller. The default value is **2**.
3. Click the **Apply** button to save the changes.

Configuring the number of user fingerprint templates is complete.

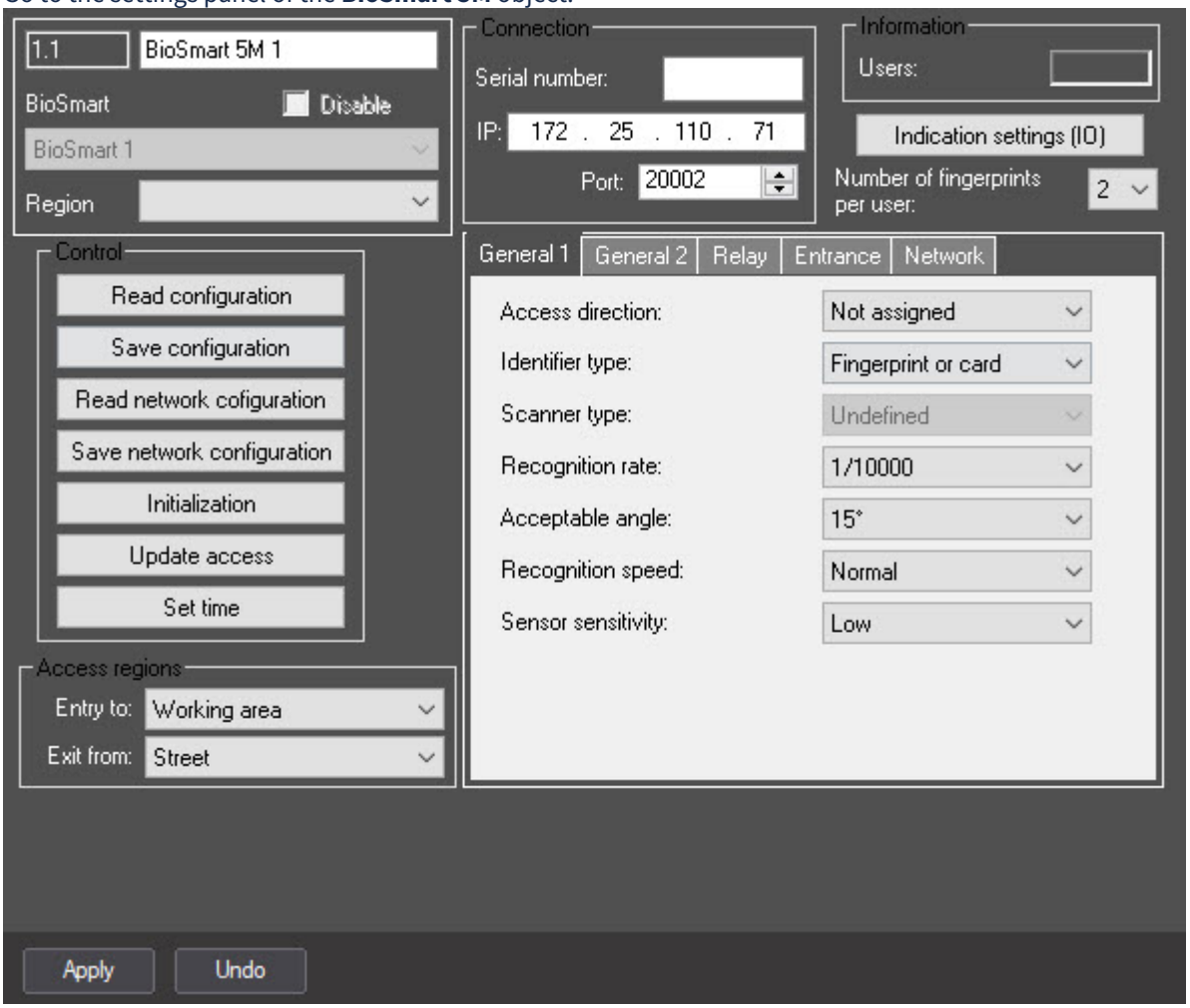
4.13.2 Configuring operating scenarios for actuating devices of the BioSmart 5M controller

Attention!

You must set only the recommended parameter values. You can set other values only after consultation with the manufacturer of the *BioSmart* ACS. For these parameter values to take effect, the configuration must be saved to the controller (see Managing the configuration of the BioSmart 4 and BioSmart 5M controllers).

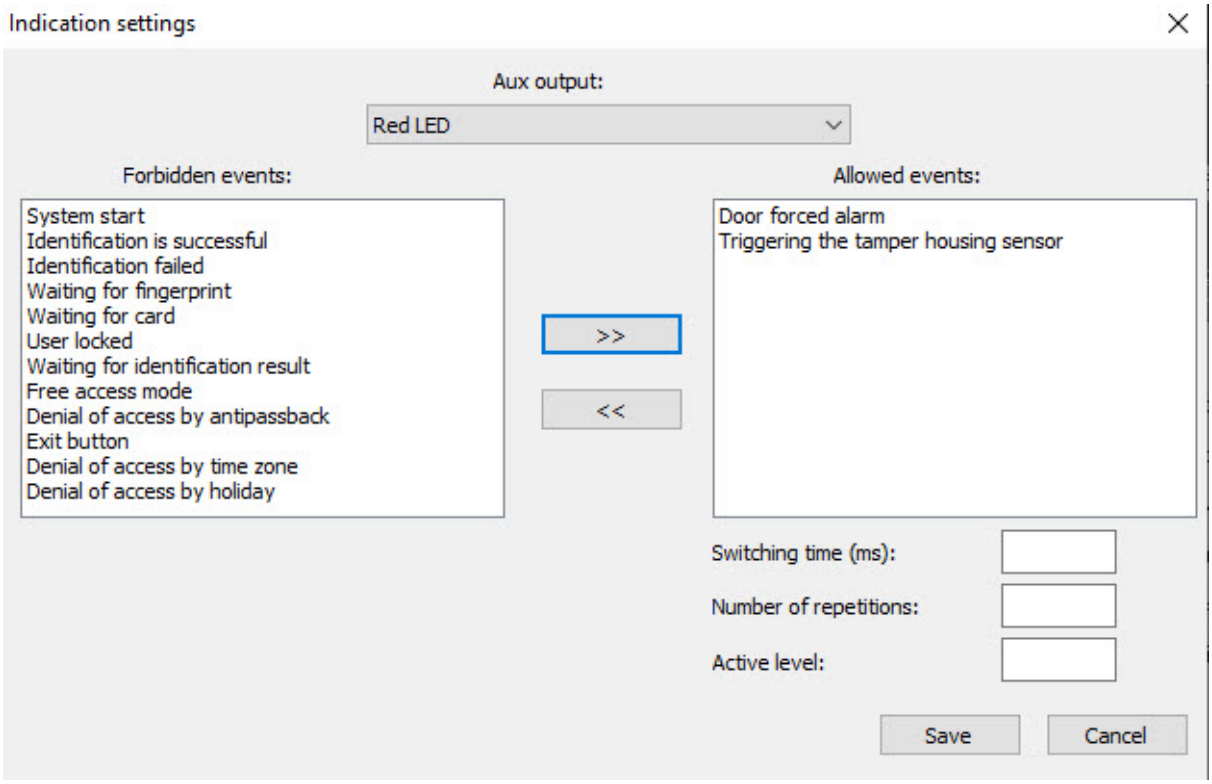
In *ACFA PSIM*, you can configure the reaction of actuating devices of the BioSmart 5M controller to certain events. For this, do the following:

1. Go to the settings panel of the **BioSmart 5M** object.



2. Click the **Indication settings** button.

As a result, the **Indication settings** window opens.



3. From the **Aux output** drop-down list, select the actuating devices, which response to the event you need to configure.
4. From the **Forbidden events** list, move those events that must trigger this actuating device to the **Allowed events** list using the buttons.
5. In the **Switching time (ms)** field, enter the time in milliseconds that must pass after receiving the selected event before the actuating device is activated.
6. In the **Number of repetitions** field, enter the number of the actuating device responses when the selected event is received.
7. Repeat steps 3-6 for all required types of actuating devices.
8. Click the **Save** button. As a result, the **Indication settings** window closes.
9. Click the **Apply** button to save the changes.

The reaction of actuating devices of the BioSmart 5M controller to certain events is configured.

4.13.3 General settings of the BioSmart 5M controller

On the page:

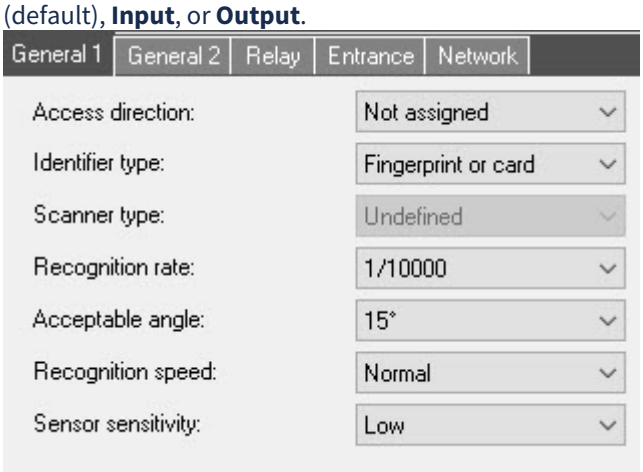
- The General 1 tab
- The General 2 tab

> **Attention!**
>
> You must set only the recommended parameter values. You can set other values only after consultation with the manufacturer of the *BioSmart* ACS. For these parameter values to take effect, the configuration must be saved to the controller (see Managing the configuration of the BioSmart 4 and BioSmart 5M controllers).

You can configure the general settings of the BioSmart 5M controller on the **General 1** and **General 2** tabs on the settings panel of the **BioSmart 5M** object.

The **General 1 tab**

1. From the **Access direction** drop-down list, select the access direction through this controller: **Not assigned** (default), **Input**, or **Output**.



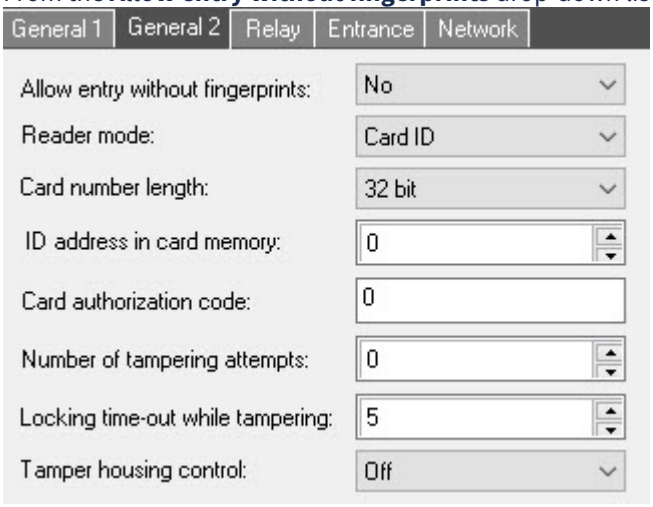
2. From the **Identifier type** drop-down list, select the access mode through this controller:
   a. **Fingerprint or card**—access is granted when a fingerprint or access card is scanned.
   b. **Card and fingerprint**—access is granted after scanning an access card and scanning the fingerprint within 10 seconds after scanning a card.

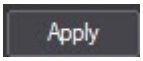
   > **Note**
   >
   > The **Scanner type** parameter is filled in automatically.

3. From the **Recognition rate** drop-down list, select the probability of false identification by fingerprint. The recommended value is **1/100000**.
4. From the **Acceptable angle** drop-down list, select the maximum allowable angle of rotation of the fingerprint from the scanner axis in degrees. The recommended value is **30°**.
5. From the **Recognition speed** drop-down list, select the fingerprint recognition algorithm. The higher the recognition speed, the higher the probability of false access denial. We recommend using the **Auto** value. In this mode the speed is determined automatically depending on the number of fingerprint templates in the controller database.
6. From the **Sensor sensitivity** drop-down list, select the sensor sensitivity level: **Low** (default), **Medium**, **High**.

The **General 2 tab**

1. From the **Allow entry without fingerprints** drop-down list, select **Yes** or **No** (default).



2. From the **Reader mode** drop-down list, select the reader operation mode: **Card ID** (default), **Disabled**, **KABA UID**, **User ID from memory**, **Data from memory**.
3. From the **Card number length** drop-down list, select the length of an access card: **32 bit** (default) or **24 bit**.
4. In the **ID address in card memory** field, specify the ID address in a card memory.
5. In the **Card authorization code** field, specify the card authorization code.
6. In the **Number of tampering attempts** field, specify the number of unsuccessful access attempts by any identifier, beyond which the controller will be locked for the **Locking time-out while tampering** (see step 7).
7. In the **Locking time-out while tampering** field, specify the controller locking time-out in seconds when the **Number of tampering attempts** parameter is exceeded.
8. From the **Tamper housing control** drop-down list, select the **On** value to enable tamper housing control. In this case, when the controller housing is tampered, the corresponding event is received and alarm signals are emitted. The default value is **Off**.
9. Click the **Apply** 

button to save the changes.

General settings of the BioSmart 5M controller are configured.

4.13.4 Configuring working with external hardware and exit relay of the BioSmart 5M controller

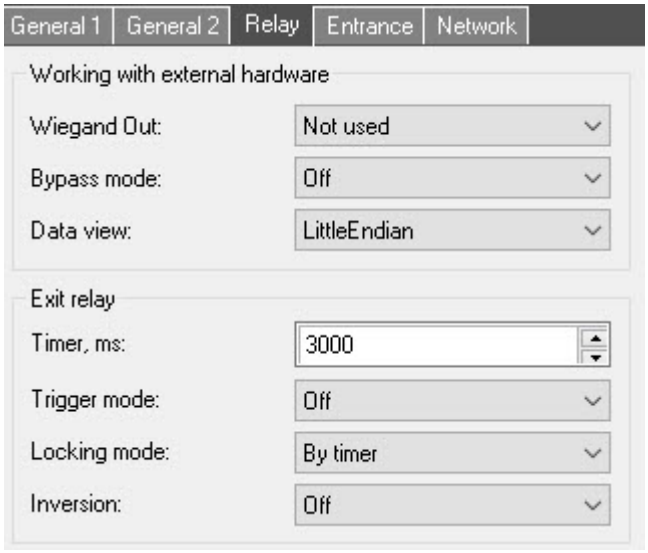
On the page:

- Configuring working with external hardware
- Configuring working with exit relay

Attention!

You must set only the recommended parameter values. You can set other values only after consultation with the manufacturer of the *BioSmart* ACS. For these parameter values to take effect, the configuration must be saved to the controller (see Managing the configuration of the BioSmart 4 and BioSmart 5M controllers).

You can connect external hardware to the BioSmart 5M controller. To configure interaction with external hardware, as well as configure the exit relay, go to the **Relay** tab on the settings panel of the BioSmart 5M controller.



Configuring working with external hardware

In the corresponding parameter group, configure working with external hardware:

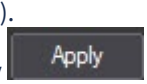
1. From the **Wiegand Out** drop-down list, select the protocol type of the Wiegand output interface of the BioSmart 5M controller:
   a. **Not used**—the Wiegand output interface of the BioSmart 5M controller isn't used.
   b. **Wiegand-26 (W/P)**—hardware that uses the Wiegand 26 protocol with parity check bits is connected to the Wiegand output of the BioSmart 5M controller.
   c. **Wiegand-32**—hardware that uses the Wiegand 32 protocol is connected to the Wiegand output of the BioSmart 5M controller.
2. If you want to enable the bypass mode, select the **On** value from the **Bypass mode** drop-down list. In this case, the access card not registered in the *ACFA PSIM* database will be available for transmission to the external ACS controller via the Wiegand output of the BioSmart 5M controller. The default value is **Off**.
3. From the **Data view** drop-down list, select **LittleEndian** (default) or **BigEndian**.

Configuring working with exit relay

In the corresponding parameter group, configure working with exit relay:

1. In the **Timer, ms** field, enter the time in milliseconds of the active state of the relay after clicking the relay control button. The default value is **3000**.
2. To enable the trigger mode, from the **Trigger mode** drop-down list, select the **On** value. In this case, the relay changes its state each time the access is successful. When the controller power is on after an emergency shutdown, the relay returns to the state it was in when the power was off. The default value is **Off**.
3. From the **Locking mode** drop-down list, select the **Manual** mode. Locking is enabled when the **Open** button is enabled. Locking is disabled on the **Close** command.

By timer—locking is enabled when the **Open** button is enabled. Locking is disabled after the time specified in the **Timer, ms** field (see step 1 of configuring working with exit relay).

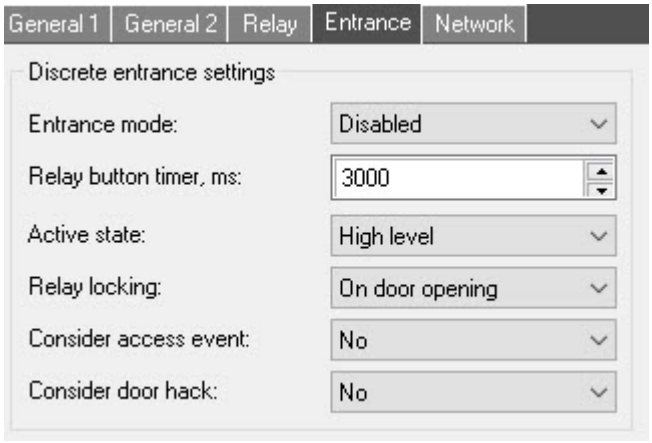
4. From the **Inversion** drop-down list, select **On** to enable the inversion mode. By default, inversion is disabled (**Off** is selected).
5. Click the **Apply**  button to save the changes.

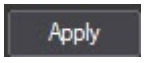
Configuring working with external hardware and exit relay is complete.

4.13.5 Configuring discrete entrance of the BioSmart 5M controller

> **Attention!**
>
> You must set only the recommended parameter values. You can set other values only after consultation with the manufacturer of the *BioSmart* ACS. For these parameter values to take effect, the configuration must be saved to the controller (see Managing the configuration of the BioSmart 4 and BioSmart 5M controllers).

You can connect the relay control button, access sensor or fire alarm sensor to the discrete entrance of the BioSmart 5M controller. To configure them, go to the **Entrance** tab on the settings panel of the BioSmart 5M controller.



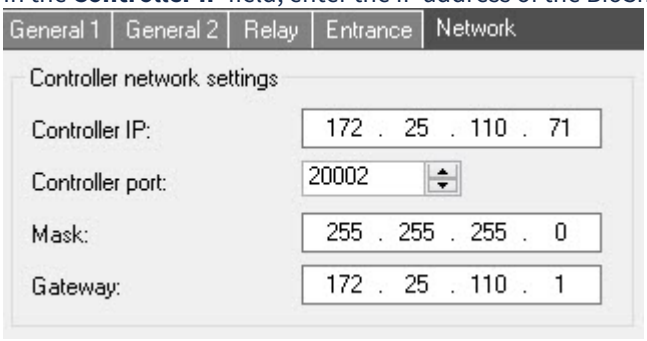
1. From the **Entrance mode** drop-down list, select the operation mode of the discrete entrance: **Relay control button**, **Access sensor**, or **Fire alarm sensor**. If no button or sensor is connected, select **Disabled**. In this case, further configuration isn't relevant.
2. In the **Relay button timer, ms** field, specify the time in milliseconds of active relay state after pressing the relay control button. The default value is **3000**.
3. From the **Active state** drop-down list, select **Low level** or **High level** (default) of the signal that appears on the discrete entrance, at which the access sensor triggering is detected.
4. From the **Relay locking** drop-down list, select the relay locking mode when the access sensor triggering is detected. **On door opening**—relay is disabled when the access sensor is triggered. **On door closing**—relay is disabled when the access sensor returns to its initial state.
5. If it is necessary to consider an access event, select the **On** value from the **Consider access event** drop-down list. The default value is **Off**.
6. If it is necessary to consider a door hack, select the **On** value from the **Consider door hack** drop-down list. The default value is **Off**.
7. Click the **Apply**  button to save the changes.

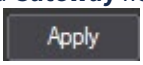
Configuring discrete entrance of the BioSmart 5M controller is complete.

4.13.6 Network settings of the BioSmart 5M controller

You can configure the network parameters of the BioSmart 5M controller on the **Network** tab on the settings panel of the **BioSmart 5M** object.

1. In the **Controller IP** field, enter the IP address of the BioSmart 5M controller.



2. In the **Controller port** field, enter the controller port number. The default number is **20002**.
3. In the **Mask** and **Gateway** fields, enter the addresses of the network mask and gateway, respectively.
4. Click the **Apply**  button to save the changes.

The network parameters of the BioSmart 5M controller are configured.

5 Working with the BioSmart integration module

5.1 General information about working with the BioSmart integration module

The following interface objects are used to work with the *BioSmart* module:

1. **Map**.
2. **Event Viewer**.
3. **Access Manager**.

For the information on configuring these interface objects, see the *Axxon PSIM* Administrator's Guide.

For the information on working with these interface objects, see the *Axxon PSIM* Operator's Guide.

Configuration and operation of the *Access Manager* module is described in the Guide for configuring and working with the Access Manager module.

5.2 Adding the BioSmart biometric parameters

To get the *BioSmart* biometric parameters for the *Access Manager* module:

- from the BioSmart parent object, a biometric face template from the *Access Manager* photo or other image file is added that is suitable for the BioSmart Quasar terminal;
- from the DCR-PV control reader, a biometric template of palm veins is added that is suitable for the PV-WTC terminal and the UniPass controller;
- from the Biosmart PV-WTC terminal, a biometric template of palm veins is added that is suitable for the PV-WTC terminal and the UniPass controller;
- from the PalmJet reader, working with Unipass Pro, a biometric template of palm veins is added that is suitable for the PalmJet reader;
- from the AirPalm/PalmJet control reader (from AirPalm via USB or PalmJet via Ethernet, if PalmJet is connected directly to the local network and not to Unipass Pro) a biometric template of palm veins is added that is suitable for the AirPalm/PalmJet reader;
- from the BioSmart Quasar terminal, a biometric face template is added;
- from the Biosmart 4 controller, a biometric fingerprint template is added that is suitable for the Biosmart 4 controller and the Biosmart Mini reader (under the control of the Prox-E controller);
- from the FS-80 control reader, a biometric fingerprint template is added that is suitable for the Biosmart 4 controller and the Biosmart Mini reader (under the control of the Prox-E controller).

Before you start, you need to configure the interaction of the reader connected to the *BioSmart* controller, or the interaction of the *BioSmart* terminal with the *Access Manager* module (see Configuring interaction of the BioSmart integration module with the Access Manager module and Time and Attendance subsystem).

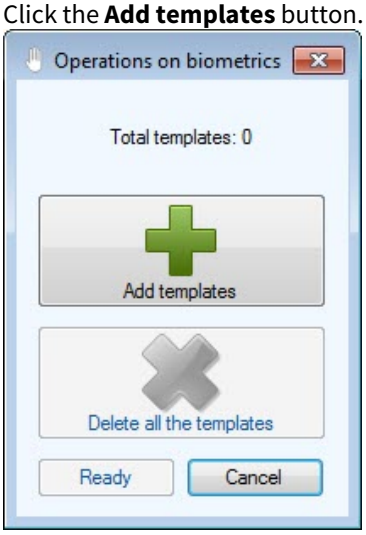
Below you can see an example of adding biometric parameters using the Biosmart PV-WTC terminal and DCR-PV USB control reader.

5.2.1 Adding biometric parameters using the Biosmart PV-WTC terminal

To add biometric parameters using the Biosmart PV-WTC terminal, do the following:

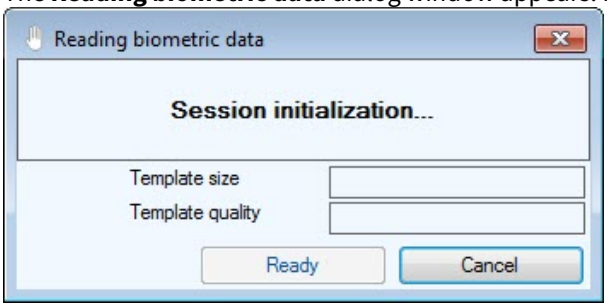
1. Go to adding biometric data in the **Access Manager** window (see Adding biometric parameters).
2. Select the corresponding extension: **(Biosmart Biometrics) PV-WTC**. The **Operations on biometrics** dialog window will open.

3. Click the **Add templates** button.

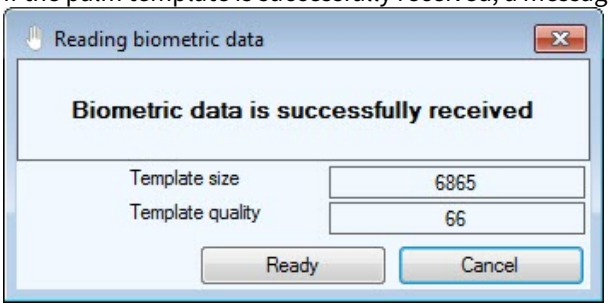


> **Note**
>
> The **Delete all the templates** button removes all palm templates that you added earlier.

4. The **Reading biometric data** dialog window appears. Follow the instructions on the terminal screen.



5. If the palm template is successfully received, a message will be displayed.



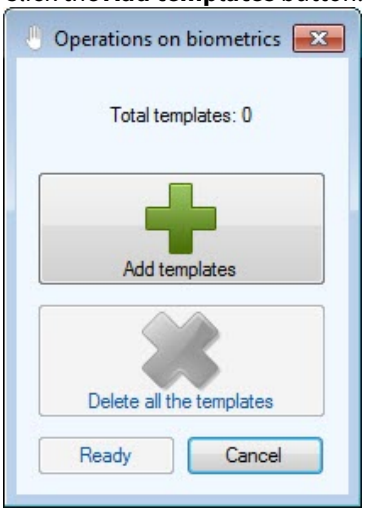
6. Click the **Ready** button to save the template.
7. Similarly, you can add as many templates as the terminal configuration allows (see Configuring the BioSmart PV-WTC terminal). The **Operations on biometrics** window displays the number of saved templates.

5.2.2 Adding biometric parameters using the DCR-PV USB control reader

To add biometric parameters using the DCR-PV USB control reader, do the following:

1. Go to adding biometric data in the **Access Manager** window (see Adding biometric parameters).

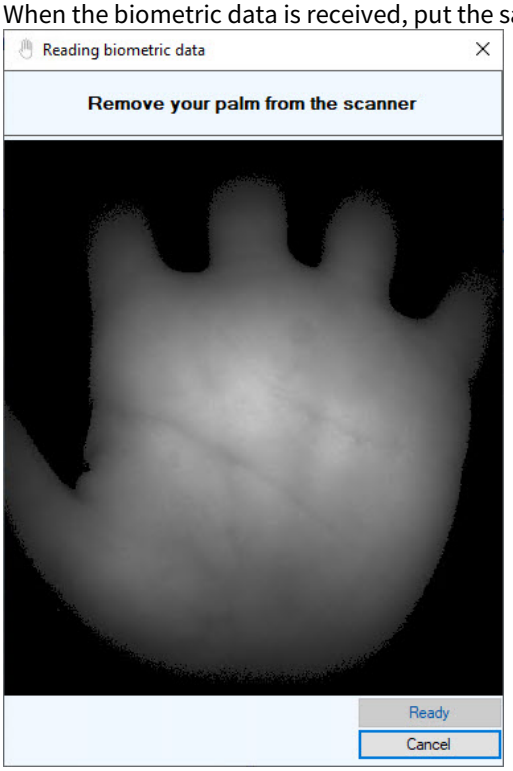
2. Select the corresponding extension: **(Biosmart Biometrics) DCR-PV control reader**. The **Operations on biometrics** dialog window will open.
3. Click the **Add templates** button.



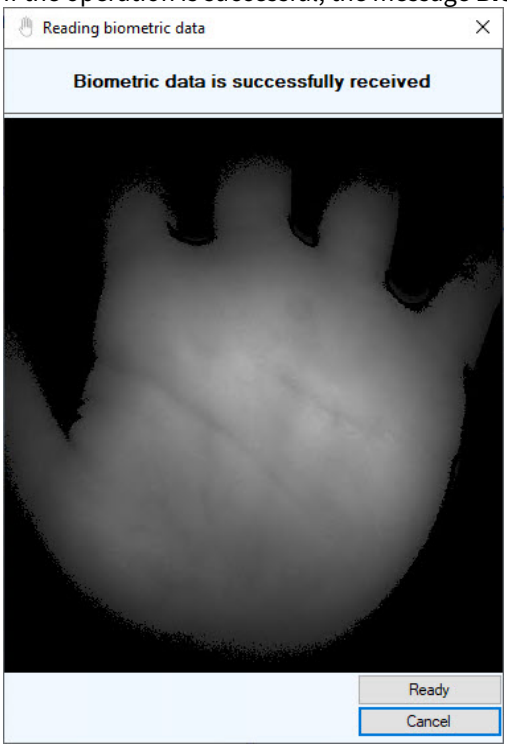
> **Note**
>
> The **Delete all the templates** button removes all palm templates that you added earlier.

4. The **Reading biometric data** dialog window will open. Put your palm to the reader.

5. When the biometric data is received, put the same palm to the reader again.



6. If the operation is successful, the message **Biometric data is successfully received** will appear.



7. Click the **Ready** buttton to save the template.

5.3 Managing the BioSmart terminals and controllers

You can manage the BioSmart PV-WTC, BioSmart Quasar, BioSmart Quasar 7 terminals by the BioSmart 4, BioSmart UniPass, BioSmart Prox-E, BioSmart 5M, BioSmart UniPass Pro 2 controllers in the **Map** interactive window using the function menu of the **Biosmart PV-WTC**, **Biosmart Quasar**, **BioSmart 4**, **BioSmart UniPass**, **BioSmart Prox-E, BioSmart 5M**, and **BioSmart UniPass Pro 2** objects, respectively. You cannot manage the BioSmart UniPass Pro, BioSmart KeyPass controllers, and the Quasar 7 terminal in the **Map** window.

> **Note**
>
> To open the function menu of an object, right-click the object's icon.

The description of the controller/terminal function menu commands is given in the table below.

Function menu command	Function
Open	Open an access point
Close	Close an access point

The following states of the BioSmart PV-WTC terminal are possible:

	Terminal is offline
	Terminal is online

The following states of the BioSmart Quasar and BioSmart Quasar 7 terminal are possible:

	Terminal is offline
	Terminal is online

The following states of the BioSmart 4 controller are possible:

	Controller is offline
	Controller is online

The following states of the BioSmart UniPass, BioSmart UniPass Pro, BioSmart UniPass Pro 2, and BioSmart KeyPass controllers are possible:

	Controller is offline
	Controller is online

The following states of the BioSmart Prox-E controller are possible:

	Controller is offline
	Controller is online

The following states of the BioSmart 5M controller are possible:

	Controller is offline
	Controller is online

5.4 Managing inputs, outputs and relays of the BioSmart UniPass controller and relay of the BioSmart 5M controller

You cannot manage inputs, outputs and relays of the BioSmart UniPass controller in the **Map** interactive window.

The following input states are possible:

	Activated
	Deactivated

The following output states are possible:

	Activated

	Deactivated

The following relay states are possible:

	On
	Off

5.5 Managing the BioSmart readers

You can work with the BioSmart Mini reader (under the control of the BioSmart Prox-E controller), the RFID Reader (under the control of the BioSmart Prox-E controller), and the BioSmart PalmJet 2 reader (under the control of the BioSmart UniPass Pro 2) in the **Map** window using the function menu of the **BioSmart Mini**, **RFID Reader**, and **BioSmart PalmJet 2** objects, respectively. You cannot manage the BioSmart PalmJet reader in the **Map** window.

The description of the reader menu commands is given in the table below.

Function menu command	Function
Open	Open an access point
Close	Close an access point

The following states of the BioSmart Mini reader are possible:

	Controller is offline
	Controller is online

The following states of the RFID Reader are possible:

	Controller is offline
	Controller is online

The following states of the BioSmart PalmJet and BioSmart PalmJet 2 readers are possible:

	Controller is offline
	Controller is online

5.6 Example of a configured macro of the BioSmart integration module

Creating and using macros
Examples of macros

When working with the *BioSmart* integration module, you can configure a macro that will trigger when an event is received from a *BioSmart* device.

Example of a configured macro: