



Control Readers Settings Guide

ACFA PSIM 1.10

Last update 05/06/2026

Table of Contents

1	Control Readers Settings Guide. List of terms.....	3
2	General information on control reader integration modules.....	4
3	Supported control readers and licensing	5
4	Configuring control readers in the Axxon PSIM software	7
4.1	Configuring BioSmart FS80 control reader in the Axxon PSIM software.....	7
4.2	Configuring Suprema BioMini control reader.....	7
4.3	Configuring Suprema RealScan control reader.....	8
4.4	Configuring Hikvision DS-K1F100 control reader in the Axxon PSIM software.....	9
4.5	Configuring a reader that supports the USB HID standard.....	10
4.6	Configuring a text reader	10
4.7	Configuring FOH02 control reader	13
4.8	Configuring a universal reader	13
5	Working with control readers in Axxon PSIM.....	15
5.1	Working with control readers for card number input	15
5.1.1	Special Feature of the Proxy-USB-MA Control Reader	15
5.2	Adding the Access Manager users fingerprints using Biosmart FS80.....	15
5.3	Capturing fingerprints of Access Manager users with Suprema BioMini	18
5.4	Working with Suprema RealScan control reader	22
5.4.1	Capturing fingerprints of Access Manager users with Suprema RealScan	22
5.4.2	Verification of user authentication using the Suprema RealScan control reader	26
5.5	Working with FOH02 control reader.....	29
5.5.1	Capturing fingerprints of Access Manager users with FOH02.....	29
5.5.2	Entering the card number with FOH02 control reader	32
5.6	Working with a universal reader.....	33
5.6.1	Virtual reader.....	34
5.6.2	Smart card reader	36

1 Control Readers Settings Guide. List of terms

Access Control System (ACS) – program and software complex designed to manage and control access to premises.

Readers – electronic devices designed to enter a code from a keyboard, read code information from system keys (identifiers), or read out user's biometric parameters (fingerprint, palm vein pattern).

Axxon PSIM Client – a computer with *Axxon PSIM* software installed in a **Client** configuration.

Axxon PSIM Server – a computer with *Axxon PSIM* software installed in a **Server** configuration.

2 General information on control reader integration modules

Control reader integration modules are components of *ACFA PSIM* software package. They are designed to process information received from readers integrated with the *ACFA PSIM* software.

Control readers shall be utilized to fill in user database with identifiers (codes, access cards, fingerprints, palm vein patterns). It is impossible to build an ACS based on control readers only.

Also, any reader from the ACS integration modules (see [ACS integration modules](#)) or FSA/ACS (see [ACFA Systems integration modules](#)) can act as a control reader.

3 Supported control readers and licensing

The following control readers are integrated with ACFA PSIM.

Name	Vendor
BioSmart FS80 <i>Note. This reader module is installed automatically together with the BioSmart integration module (see BioSmart Integration Module Configuration and Operation Manual (obsolete))</i>	Prosoft Systems 620102 Russia Yekaterinburg 194 A Vologodskaya str. Phone: +7 (343) 376-2820; 356-5111 Email: info@prosoftsystems.ru www.prosoftsystems.ru
Suprema BioMini	Suprema 17F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863 Republic of Korea www.supremainc.com
Suprema RealScan	Suprema 17F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863 Republic of Korea www.supremainc.com
DS-K1F100-D8E DS-K1F820-F <i>Note. This reader modules are installed automatically together with the Hikvision integration module (see Hikvision Integration Module Configuration and Operation Guide)</i>	Hikvision USA 18639 Railroad Street, City of Industry, California 91748 Phone: + 1-909-895-0400 Phone toll free: + 1-866-200-6690 (U.S. and Canada only) Technical Support: tel: 909-612-9039 or email: techsupport.usa@hikvision.com Sales Department: sales.usa@hikvision.com http://www.hikvision.com/us/
Proxy-USB-MA	Bolid innovation and research enterprise (ZAO NVP Bolid) Russia, 141074, Moscow Region, Korolev, Pionerskaya str, 4 Phone/fax: +7 (495) 775-71-55, 777-40-20 Email: info@bolid.ru , sales@bolid.ru https://bolid.ru

Name	Vendor
ST-CE321LR-WT	LLC "ARMO-Systems" Russia, Leningradsky prospect, 37A, building 14, BC "ARKUS-II" Phone: +7(495) 787-33-42 Email: cctv@smartec-s.com https://smartec-security.com/
PW-Desktop BLE	ProxWay Russia, 107023, Moscow, Malaya Semyonovskaya st., 3a Phone: +7 (495) 788-83-93 info@proxway-ble.ru https://proxway-ble.ru
Honeywell Voyager 1400g	Honeywell Charlotte, North Carolina, U.S. Phone: +001 (480) 353-3020 https://www.honeywellaidc.com/
All smart card readers supporting PC/SC standard	For a complete list of PC/SC compatible smart card reader manufacturers, visit: https://www.pcscworkgroup.com/members/member-list/ An example of such smart card readers: ACS ACR1252U (Advanced Card Systems Ltd., www.acs.com.hk)
FOH02	Union Community Co. Ltd 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea sales@virditech.com https://www.virditech.com
Dahua DHI-ASM202	Dahua Technology Co., Ltd. No.1199, Bin'an Road, Binjiang District, Hangzhou, China P.C: 310053 Phone: +86 571 8768 8883 Fax: +86 571 8768 8815 Email: overseas@dahuatech.com Website: https://www.dahuasecurity.com

Modules licensing

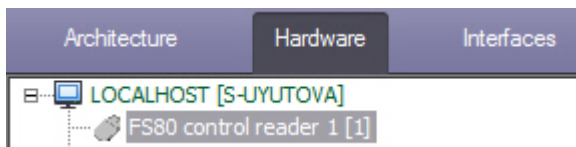
Control readers are available free of charge upon purchase of an *Access Manager* module license (see [Guide for configuring and working with the Access Manager module](#)).

4 Configuring control readers in the Axxon PSIM software

4.1 Configuring BioSmart FS80 control reader in the Axxon PSIM software

After connection of the *FS80* reader to a Server download and install driver from the manufacturer [official web site](#).

Then create the **FS80 control reader** object on the base of the **Computer** object in the *Axxon PSIM* software.



4.2 Configuring Suprema BioMini control reader

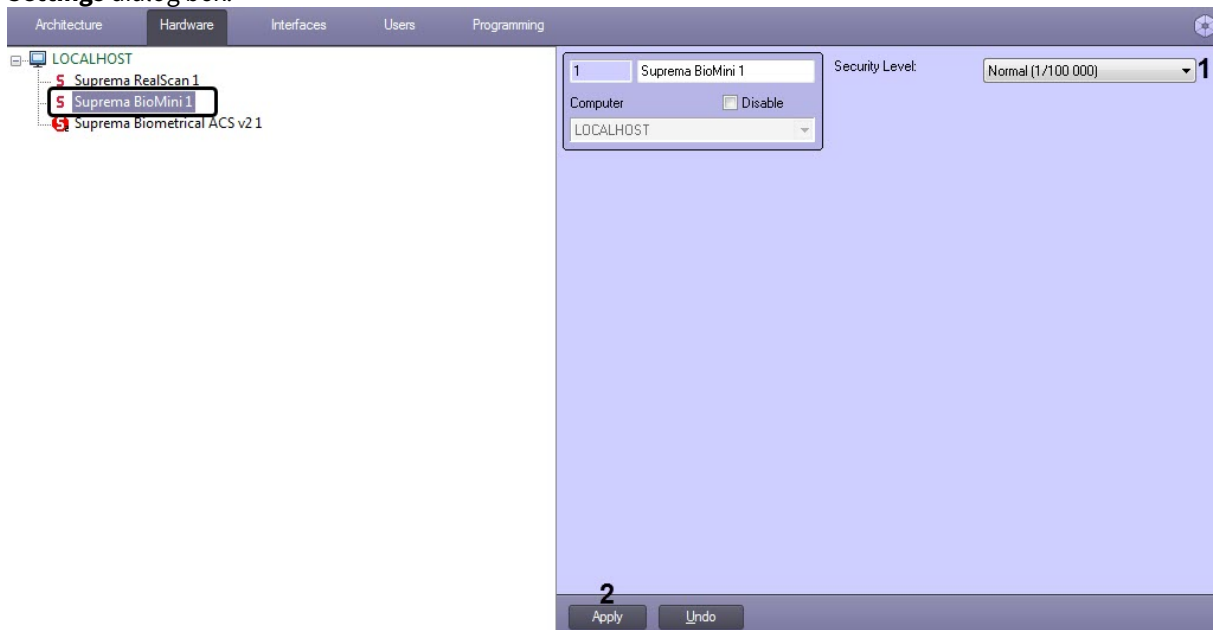
Configure the *Suprema BioMini* control reader as follows:

1. Connect the reader to a Server, download and install driver from the manufacturer's [official web site](#).

Note

Registration on this site is required for download.

2. Create the **Suprema BioMini** object based on the **Computer** object on the **Hardware** tab of the **System Settings** dialog box.



3. In the **Security Level** drop-down list (1) select the fingerprint verification quality level:
 - **Lowest (1/1000)** — the lowest level.
 - **Low (1/10 000)** — low level.
 - **Normal (1/100 000)** — average level.
 - **High - (1/1 000 000)** — high level.
 - **Highest (1/10 000 000)** — the highest level.
4. Click **Apply** (2) to save the settings.

Note

- Capturing fingerprints with this control reader in the *Access Manager* is described in the [Capturing fingerprints of Access Manager users with Suprema BioMini](#).
- The *Suprema RealScan* control reader is to be used only with the *Suprema 2* integration module — see [Guide for configuring and working with the Suprema 2 integration module](#).

Attention!

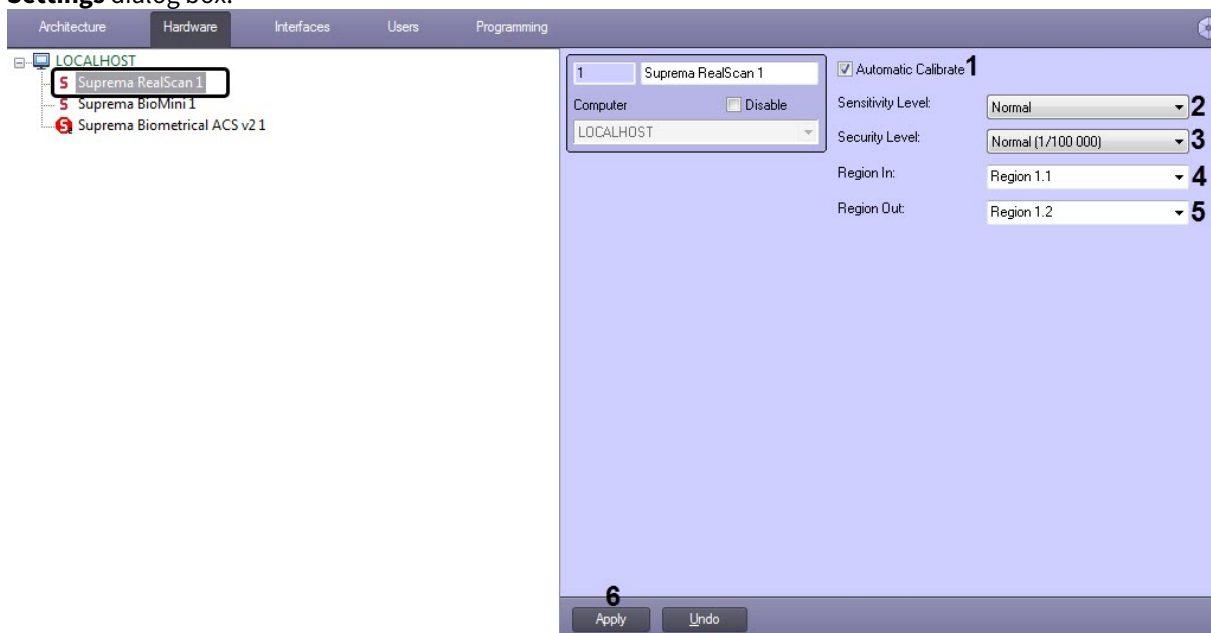
The module requires the 32-bit version of the Microsoft Visual C++ 2008 redistributable package to be installed. If this component is not installed in your system, use the `redist/en/x86/vc90redist.exe` installer provided in the *ACFA PSIM* installation package.

Configuring *Suprema BioMini* control reader is completed.

4.3 Configuring Suprema RealScan control reader

Configure the *Suprema RealScan* control reader as follows:

1. Connect the reader to a Server, download and install driver from the manufacturer's [official web site](#).
2. Create the **Suprema RealScan** object based on the **Computer** object on the **Hardware** tab of the **System Settings** dialog box.



3. Uncheck the **Automatic Calibrate** check box (1) if it is necessary to disable the automatic calibration of the reader.

Note

It is recommended not to unset this check box.

4. In the **Sensitivity Level** drop-down list (2) select the sensitivity level:
 - **Normal** - average sensitivity.
 - **High** - high sensitivity.
 - **Higher** - the highest sensitivity.

- **Disabled** - disabled.
5. In the **Security Level** drop-down list (3) select the fingerprint verification quality level:
 - **Lowest (1/1000)** - the lowest level.
 - **Low (1/10 000)** - low level.
 - **Normal (1/100 000)** - average level.
 - **High - (1/1 000 000)** - high level.
 - **Highest (1/10 000 000)** - the highest level.
 6. In the **Region In** field (4) specify the input region.
 7. In the **Region Out** field (5) specify the output region.
 8. Click **Apply** (6) to save the settings.

Note

- Capturing fingerprints with this control reader in the *Access Manager* is described in the [Capturing fingerprints in Access Manager with Suprema RealScan](#).
- The *Suprema RealScan* control reader is to be used only with the *Suprema 2* integration module – see [Guide for configuring and working with the Suprema 2 integration module](#).

Attention!

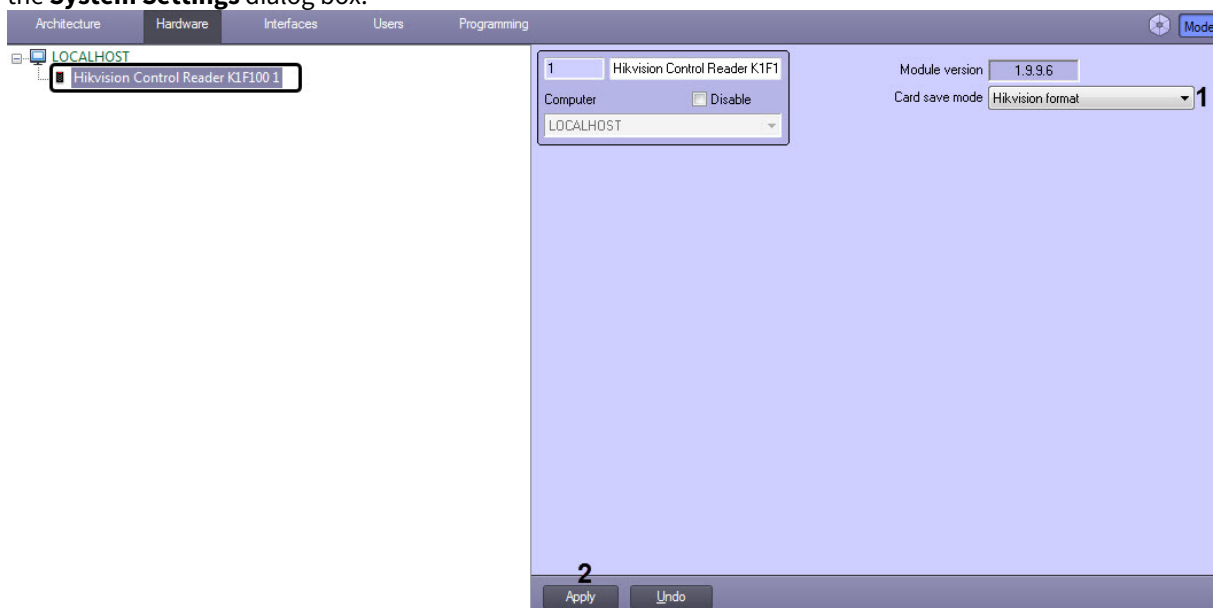
The module requires the 32-bit version of the Microsoft Visual C++ 2008 redistributable package to be installed. If this component is not installed in your system, use the `redist/en/x86/vc90redist.exe` installer provided in the *ACFA PSIM* installation package.

Configuring *Suprema RealScan* control reader is completed.

4.4 Configuring Hikvision DS-K1F100 control reader in the Axxon PSIM software

The *Hikvision DS-K1F100* control reader is configured as follows:

1. Create a **Hikvision Control Reader K1F100** object based on the **Computer** object on the **Hardware** tab of the **System Settings** dialog box.



2. From the **Card save mode** drop-down list (1), select the format for saving the facility code and card code:
 - **Hikvision format** - saves all access cards in the Hikvision format (the facility code contains a fixed H character, the card code is a decimal number up to 32-bits).
 - **Hikvision W26 text format** - saves all access cards in Hikvision format, and the original facility code is added to the beginning of the card code.
 - **Card + Facility code** - saves EM-Marine access cards in Wiegand-26 format.

⚠ Attention!

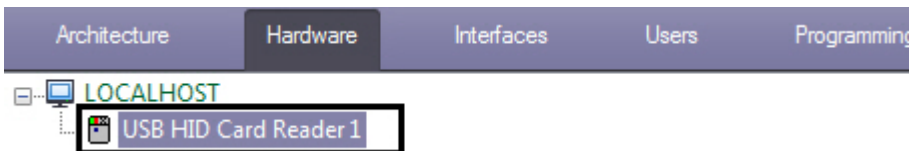
Card + Facility code only works for EM-Marine Wiegand-26 access cards. Other types of cards will be saved in Hikvision format.

3. Click the **Apply** button (3) to save the settings.

The configuration of the *Hikvision DS-K1F100* control reader is completed.

4.5 Configuring a reader that supports the USB HID standard

After you connect a reader that supports the USB HID standard, for example Proxy-USB-MA or ST-CE321LR-WT, to the Server, it is necessary to create the **USB HID Card Reader** object on the basis of the **Computer** object in *Axxon PSIM*.



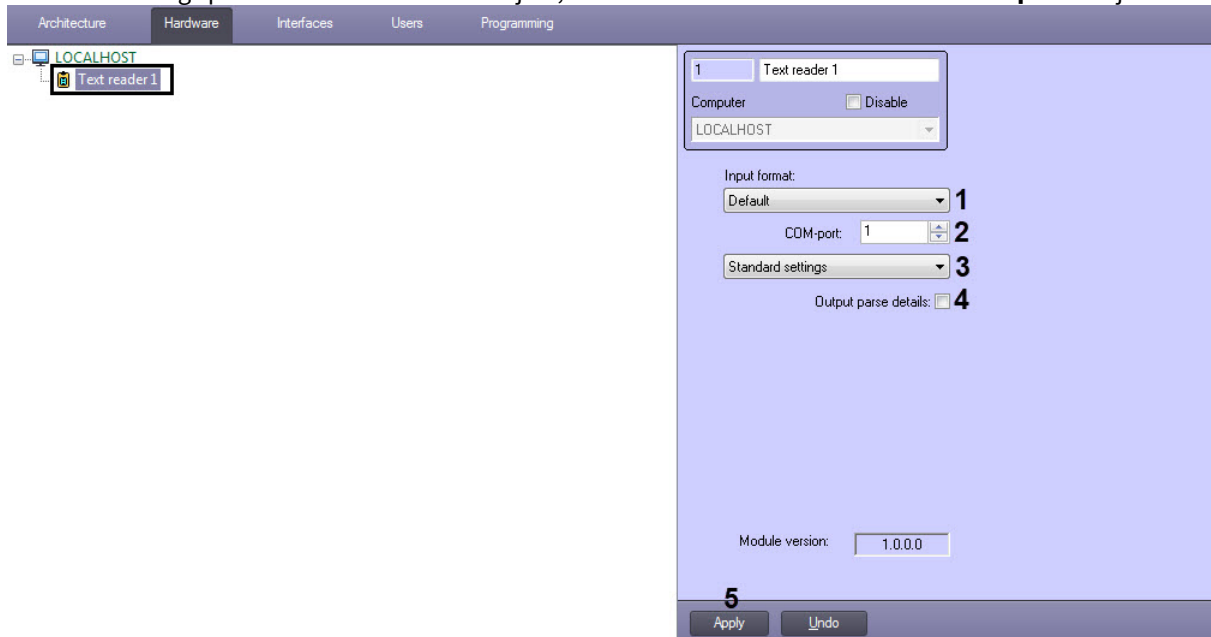
4.6 Configuring a text reader

⚠ Attention!

After you connect a text reader to the Server, it is necessary to install the driver for the particular model, for example for *Honeywell Voyager 1400g*, *PW-Desktop BLE*. The driver can be downloaded from the vendors official websites.

To configure the text reader, do the following:

1. Go to the settings panel of the **Text reader** object, which is created on the basis of the **Computer** object.



2. From the **Input format** drop-down list (1) select the input card format:
 - **Default** – standard format for readers.
 - **Honeywell** – format of the *Honeywell* two-dimensional code reader (8 characters, where the first 3 characters are the decimal value of the facility code, and the last 5 characters are the decimal value of the card code).
3. In the **COM-port** field (2) enter the number of the COM port that is used for connecting the control reader.
4. From the drop-down list (3) select the operation mode of the control reader:
 - **Standard settings** – the reader will receive the facility and card codes as they are.
 - **Custom settings** – custom setting for parsing facility and card codes.
5. Set the **Output parse details** checkbox (4), if it is necessary to display the parsing of the facility code and the card code in the *Event viewer*.
6. Click the **Apply** button (5).

If the custom setting for parsing facility and card codes was selected:

1. Set the **Full hexadecimal mode** checkbox (1) if it is necessary to use the entire card number in hexadecimal notation.

2. Set the **Full decimal mode** checkbox (2) if it is necessary to use the entire card number in decimal notation.
3. In the **Get bit range from card data** group, set the settings for the received card data:
 - a. Set the length in bits of the card data (3).
 - b. Set the offset in bits of the card data (4).
 - c. Set the **Invert byte order** checkbox (5), if it is necessary to invert the byte order of the card data.
 - d. Set the **Invert bit values** checkbox (6) if it is necessary to invert the bits of the card data.
 - e. Set the **Add high bit** checkbox (7) if it is necessary to add the high-order bit to the received data, and select the type of the high-order bit to be added from the drop-down list.
 - f. Set the **Add low bit** checkbox (8) if it is necessary to add the low-order bit to the received data, and select the type of the low-order bit to be added from the drop-down list.
4. In the **Get card code from range** group, set the settings for the received card code:
 - a. Set the length in bits of the card code (9).
 - b. Set the offset in bits of the card code (10).
 - c. Set the **Invert byte order** checkbox on (11) if it is necessary to invert the byte order of the card code.
 - d. Set the **Invert bit order** checkbox (12) if it is necessary to invert the bit order of the card code.
5. In the **Get facility code from range** group, set the settings for the received facility code of the card:
 - a. Set the length of the facility code in bits (13).
 - b. Set the offset of the facility code in bits (14).
 - c. Set the **Invert byte order** checkbox (15) if it is necessary to invert the byte order in the facility code.
 - d. Set the **Invert bit order** checkbox (16) if it is necessary to invert the bit order of the facility code.
6. In the **Facility code** field (17), if necessary, enter the facility code, which will be automatically assigned to all access cards.
7. Click **Apply** (18).

The configuration of the text reader is now complete.

4.7 Configuring FOH02 control reader

In order to work with the *FOH02* control reader, a pre-created and configured *Virdi* server is required (see [Configuring the Virdi ACS connection](#)).

Once connected, the *Virdi* reader is not created in the hardware tree like other control readers.

4.8 Configuring a universal reader

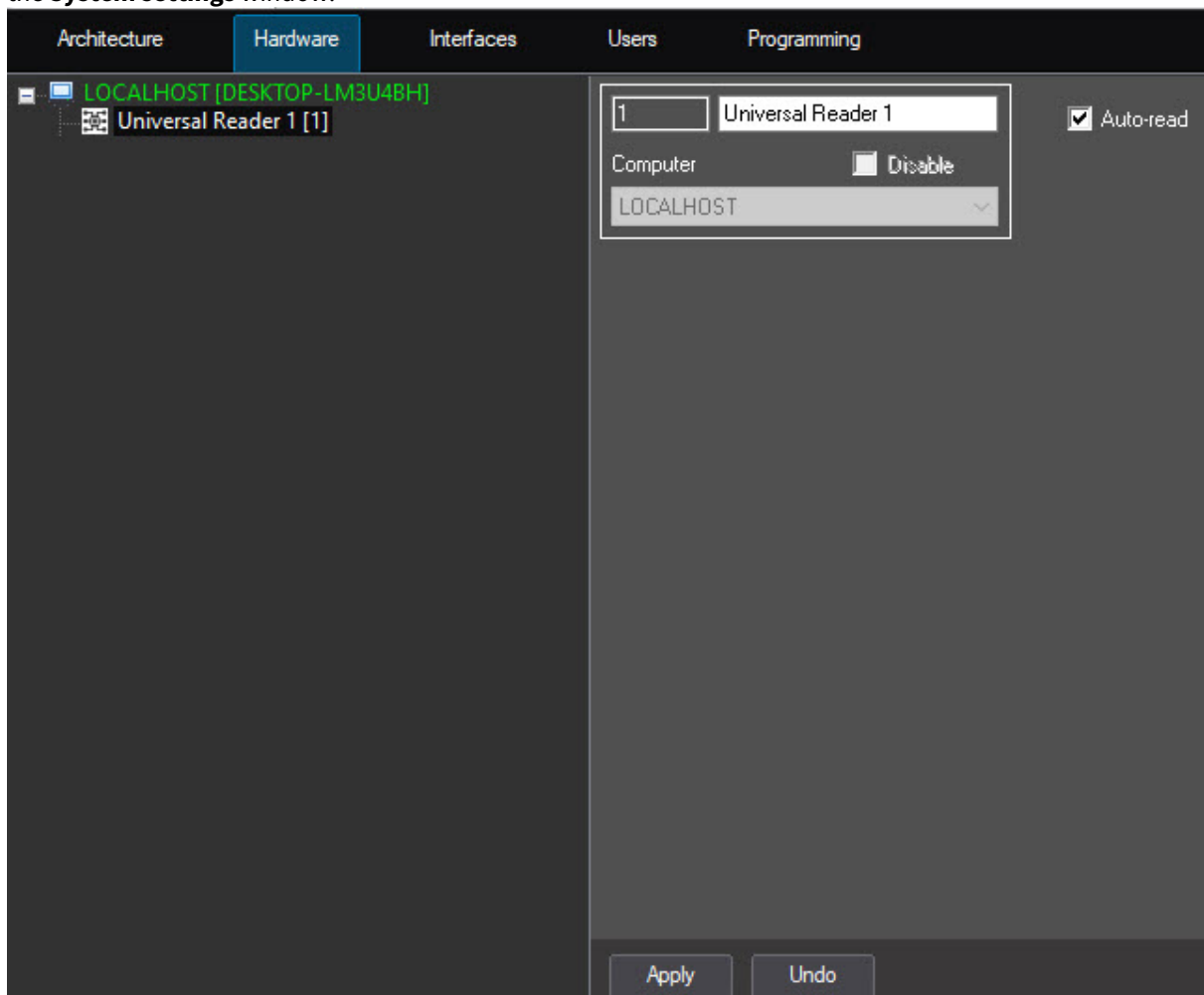
Note

Universal reader is installed together with the control readers. You must select it when you install *ACFA PSIM* by setting the corresponding checkbox.

Starting with *ACFA PSIM* 1.6, if there is a remote client in the distributed system, the logs of a universal reader are located at %ProgramData%\AxxonSoft\AxACFA.

To configure a universal reader, do the following:

1. Create the **Universal Reader** object on the basis of the **Computer** object on the **Hardware** tab of the **System settings** window.



2. Clear the **Auto-read** checkbox. Otherwise you cannot specify the reader settings in step 4.
3. Click the **Apply** button to save the settings.
4. Specify the reader settings (for more information, see [Working with a universal reader](#)).
5. Set the **Auto-read** checkbox to use the reader settings already specified in the previous step. If the checkbox is clear, the settings window opens every time the access card is read.
6. Click the **Apply** button to save the settings.

Configuring a universal reader is complete.

5 Working with control readers in Axxon PSIM

Control readers integration modules are designed for registration of events and automatic assigning users with card numbers.

The biometric control readers integration modules are designed for enrollment of user biometric parameters such as fingerprints (see subsections).

The following interface objects can be used to work with the control readers integration modules in *ACFA PSIM*:

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

Information on how to configure the **Event Viewer** interface object is given in *Axxon PSIM* software package. [Administrator's Guide](#).

Information on how to use the **Event Viewer** interface object is given in *Axxon PSIM*. [Operator's Guide](#).

Information on how to use the **Access Manager** interface object is given in [Guide for configuring and working with the Access Manager module](#).

5.1 Working with control readers for card number input

You can work with control readers for card number input as follows:

1. Open the **Access Manager** window (see [Starting and stopping the Access Manager module](#)).
2. Go to editing the required user (see [Going to user editing](#)).
3. Enter the card number using the control reader (see [Entering an access card number using a control reader](#)).

5.1.1 Special Feature of the Proxy-USB-MA Control Reader

The **Proxy-USB-MA** reader is designed for card input with the conversion of the original TouchMemory format to Wiegand 26 format.

If it is necessary to convert the original format of the TouchMemory reader to the Wiegand 26 format, then you can work with this reader in the same way as with other readers for card number input.

If it is necessary to enter card numbers in the original TouchMemory format, then:

- Do not create the **USB HID Card Reader** object.
- Enter the card number manually (see [Manual input of access card number](#)). Note that the **Proxy-USB-MA** reader is considered a HID (Human Interface Device) in the system, and when the card is presented to the reader, the number will be entered as from the keyboard.

Attention!

The TouchMemory format represents the HEX key code and may contain characters A, B, C, D, E, F. You can enter a card number only using the Latin keyboard layout. If you change the layout to a different one from the Latin alphabet, then the characters will not be read correctly and such a card will not work.

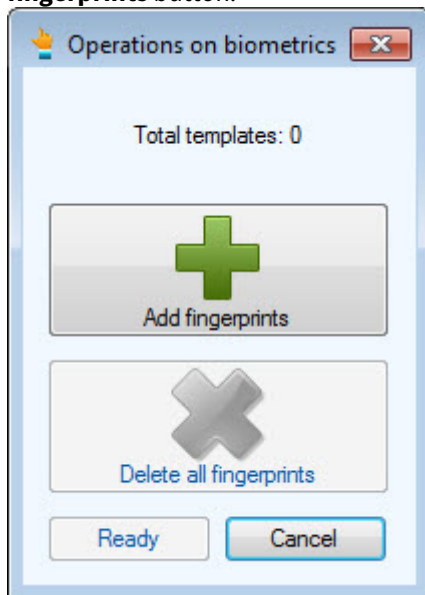
5.2 Adding the Access Manager users fingerprints using Biosmart FS80

Attention!

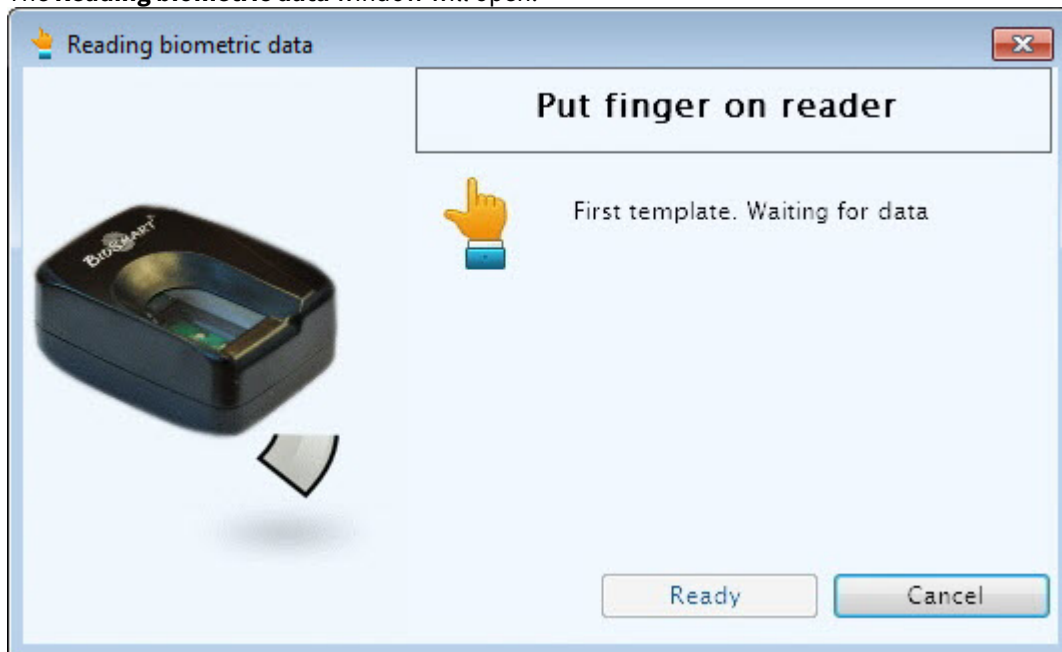
The FS80 control reader is to be used only with the BioSmart integration module (see [BioSmart Integration Module Configuration and Operation Manual \(obsolete\)](#)).

To add the biometric parameters (fingerprints) of users from the *Access Manager* module using the *BioSmart FS80* biometric control reader, do the following:

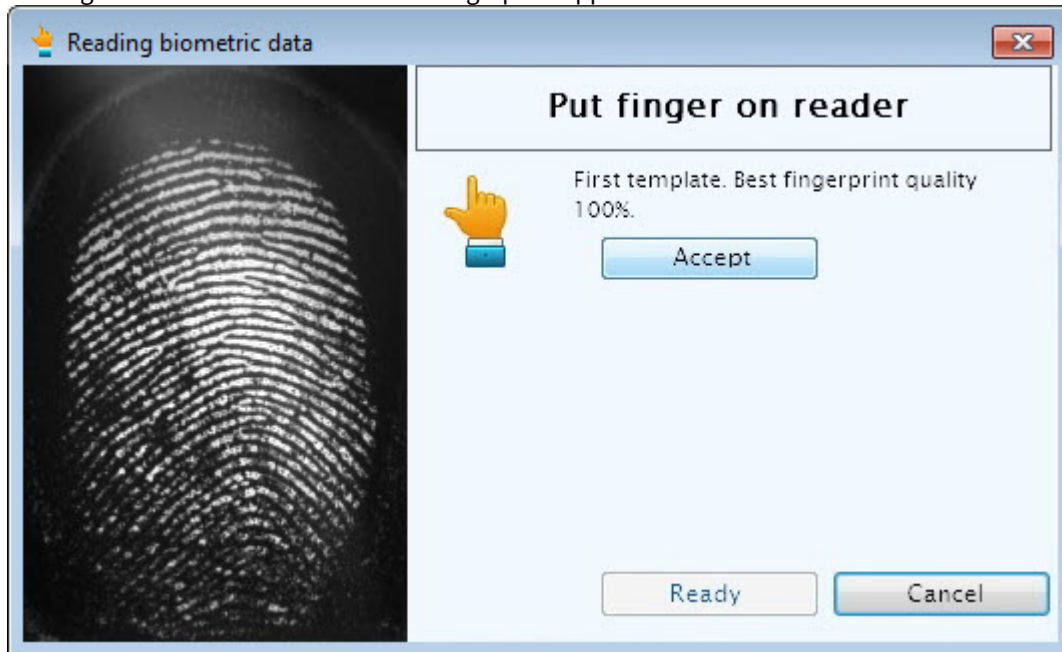
1. Go to adding biometric data in the *Access Manager* window (see [Adding biometric parameters](#)).
2. Select the **(Suprema/Biosmart) FS80 control reader** extension that corresponds to the FS80 biometric control reader.
3. The **Operations on biometrics** dialog box will open. To add a new fingerprint, click the **Add fingerprints** button.



The **Reading biometric data** window will open.



- Put finger on reader and hold until the fingerprint appears in the window.

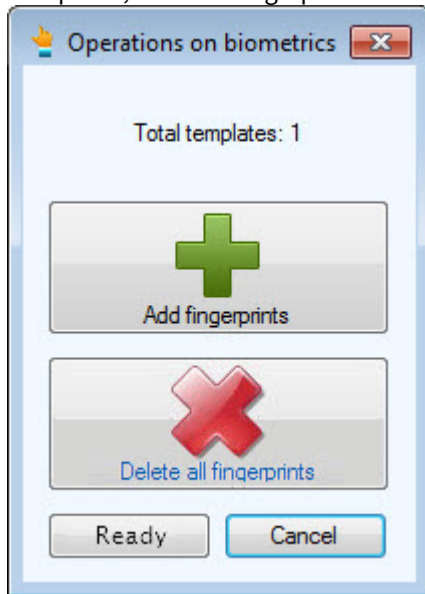


- Click the **Apply** button and repeat the procedure with the same finger.
- If the procedure was carried out properly, and the fingerprints match, the **Biometric data is valid** message will be displayed.



- Click **Ready** to save the fingerprint.

8. If required, add new fingerprints or delete all added fingerprints.



9. Click **Ready** and then save the user parameters.

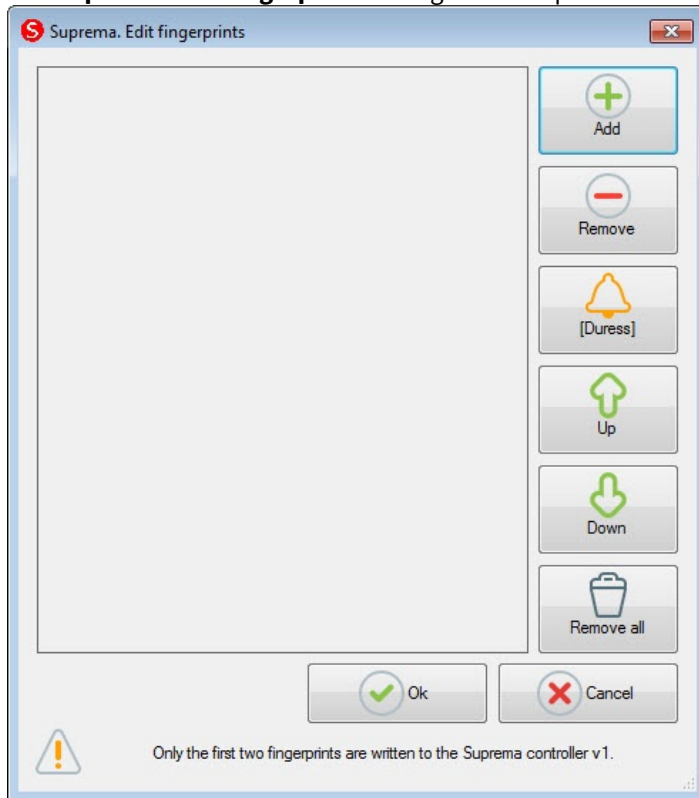
The biometric parameters (fingerprints) of users from the *Access Manager* module are added using the *BioSmart FS80* biometric control reader.

5.3 Capturing fingerprints of Access Manager users with Suprema BioMini

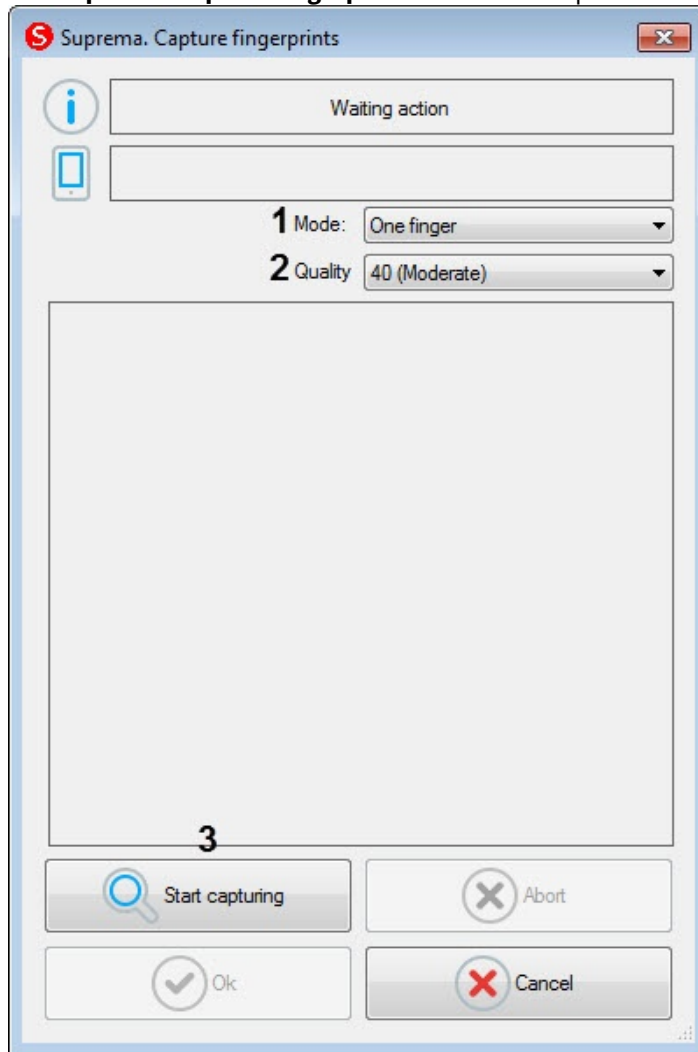
Adding fingerprints of users from the *Access Manager* using the *Suprema BioMini* biometric control reader is carried out as follows:

1. Go to adding biometric data in the *Access Manager* window (see [Adding biometric parameters](#)).
2. Select the **(Edit Fingerprints) Suprema BioMini** extension that corresponds to the *Suprema BioMini* control reader.

3. The **Suprema. Edit fingerprints** dialog box will open. To add a new fingerprint, click the **Add** button.



The **Suprema. Capture fingerprints** window will open.



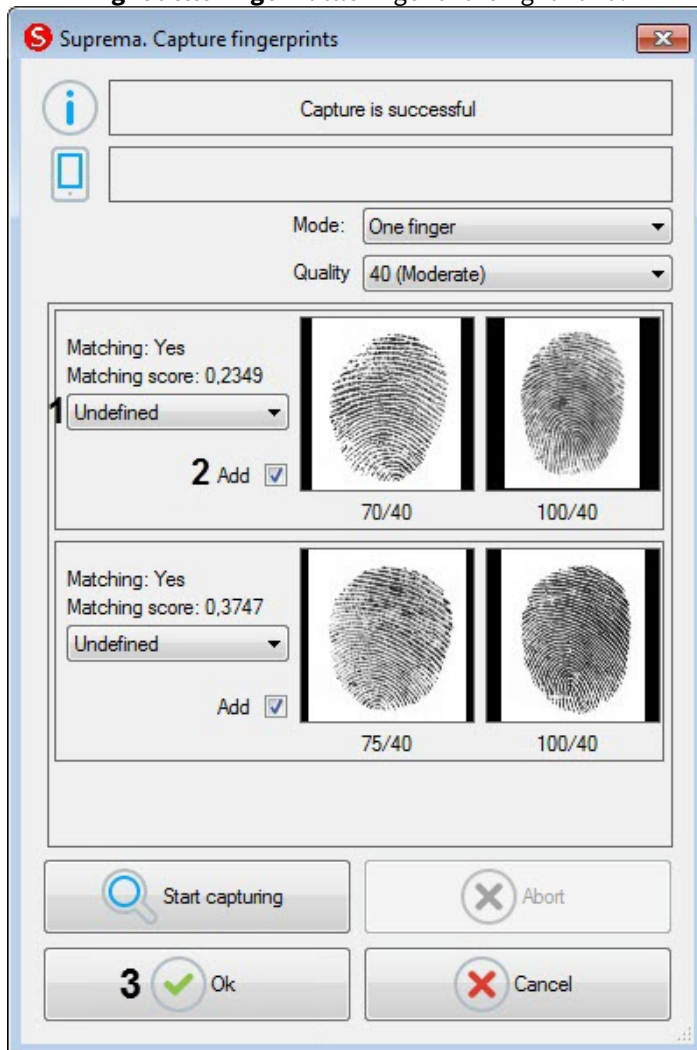
4. From the **Mode** drop-down list (1) select the fingerprint **One finger** capture mode.
5. From the **Quality** drop-down list (2) select the fingerprint capture quality:
 - **20 (Weak)** - low quality.
 - **40 (Moderate)** - average quality (default).
 - **60 (Strong)** - high quality.
 - **80 (Strongest)** - the highest quality.
6. To start capturing fingerprints, click the **Start capturing** button (3) and follow the instructions displayed at the top of the **Suprema. Capture fingerprints** window.

Note

To capture fingerprints, each finger or group of fingers should be placed on the reader twice with 5 seconds delay after pressing the **Start capturing** button and after the first capture.

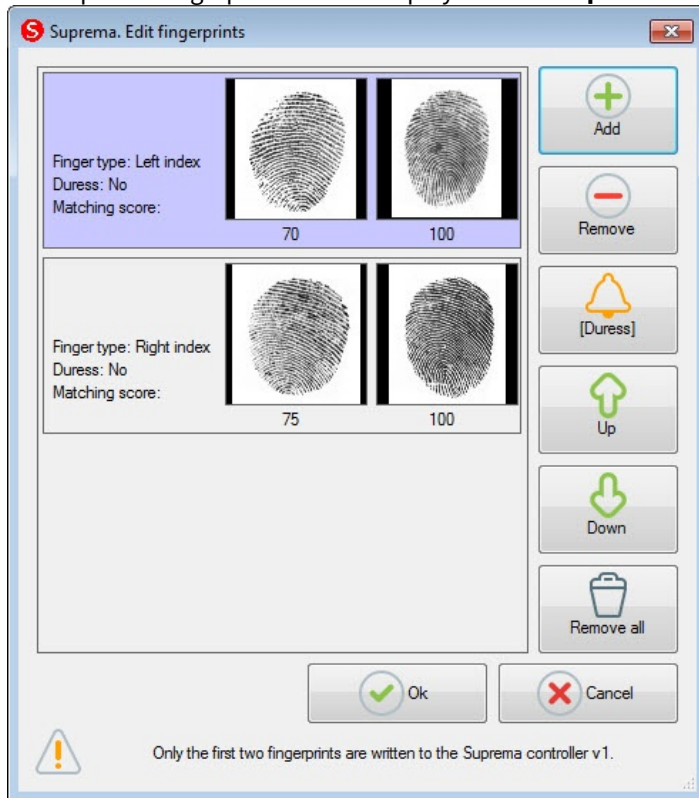
7. After the fingerprint capture is completed, select the type of scanned finger for each fingerprint in the drop-down list (1):
 - **Undefined** - undefined.
 - **Left thumb** - thumb of the left hand.
 - **Left index finger** - index finger of the left hand.
 - **Left middle finger** - middle finger of the left hand.

- **Left ring finger** - ring finger of the left hand.
- **Left little finger** - little finger of the left hand.
- **Right thumb** - thumb of the right hand.
- **Right index finger** - index finger of the right hand.
- **Right middle finger** - middle finger of the right hand.
- **Right ring finger** - ring finger of the right hand.
- **Right little finger** - little finger of the right hand.



8. Uncheck the **Add** check box (2) if it is not necessary to add the fingerprint to the user.
9. Click **OK** (3) to save the result.

10. The captured fingerprints will be displayed in the **Suprema. Edit fingerprints** window.



11. To remove one fingerprint, select it and click **Remove**.

Note

To remove all fingerprints, click **Remove all**.

12. To mark a fingerprint as captured "Under duress", select it and click the **[Duress]** button.

Note

As a result, a silent alarm will be generated when reading this fingerprint.

13. To move a fingerprint up or down in the list, select it and click the **Up** or **Down** button.
 14. To finish entering fingerprints, click **OK**.

Adding fingerprints of users from the *Access Manager* using the *Suprema BioMini* biometric control reader is completed.

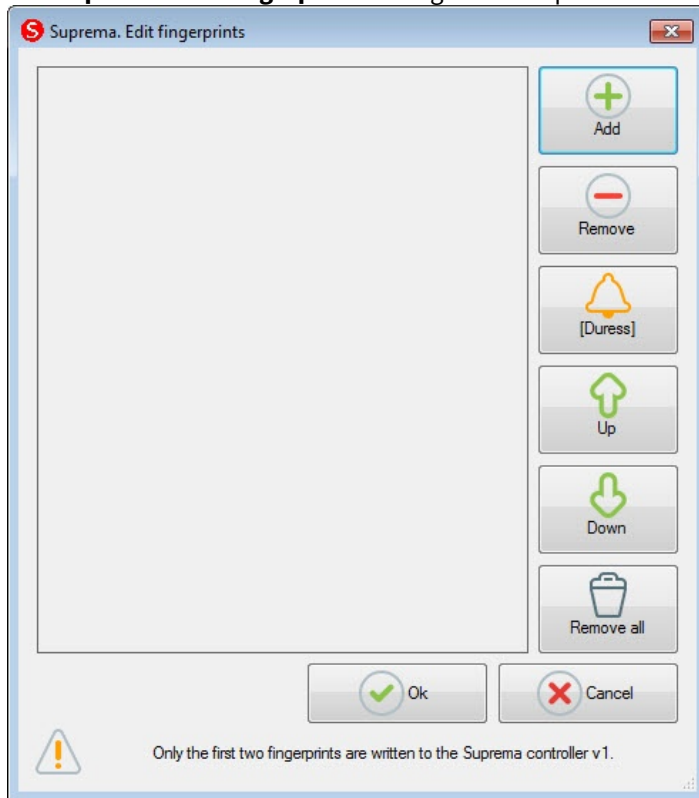
5.4 Working with Suprema RealScan control reader

5.4.1 Capturing fingerprints of Access Manager users with Suprema RealScan

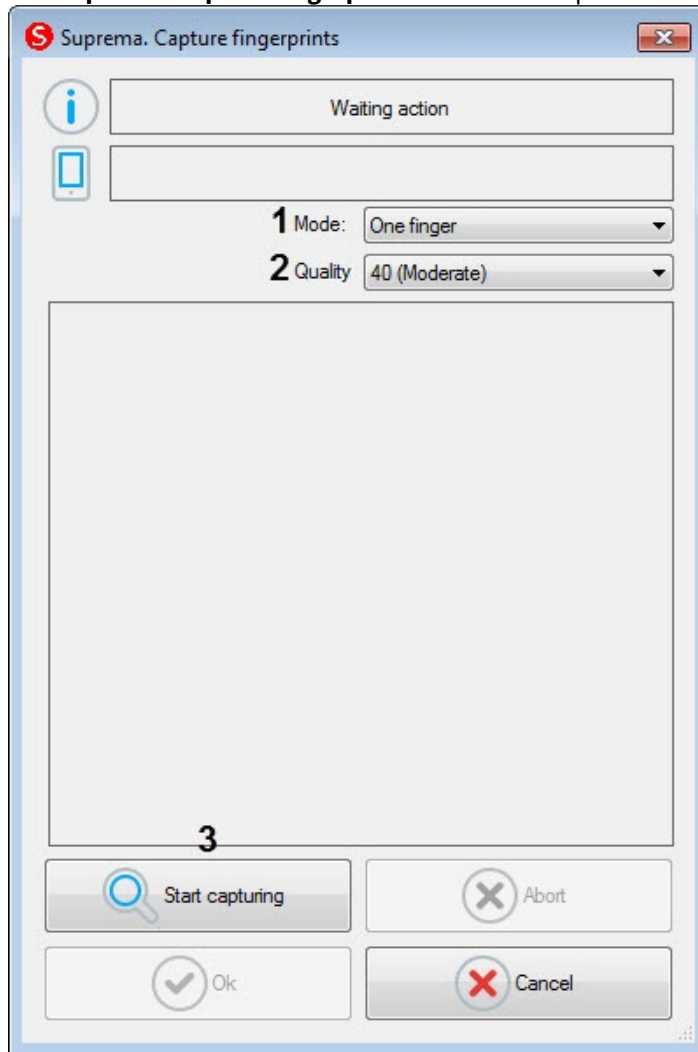
Adding fingerprints of the *Access Manager* users via the *Suprema RealScan* control reader is performed as follows:

1. Go to adding biometric data in the *Access Manager* window (see [Adding biometric parameters](#)).
2. Select the **(Edit Fingerprints) Suprema RealScan** extension that corresponds to the *Suprema RealScan* control reader.

3. The **Suprema. Edit fingerprints** dialog box will open. To add a new fingerprint, click the **Add** button.



The **Suprema. Capture fingerprints** window will open.

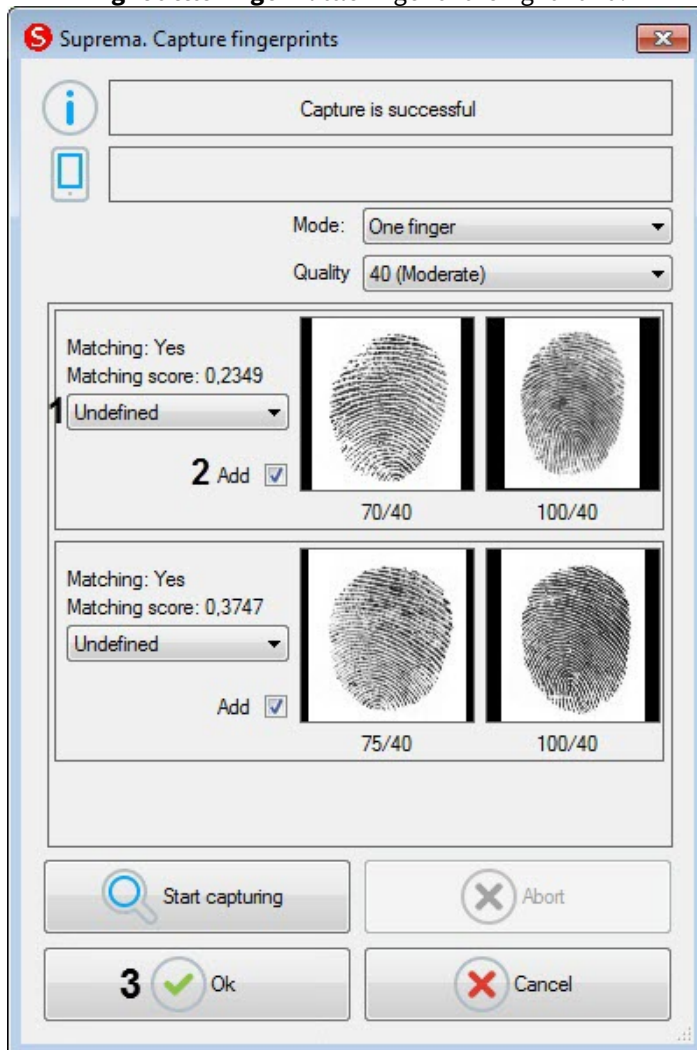


4. From the **Mode** drop-down list (1) select the fingerprint capture mode:
 - **One finger** - reading a single fingerprint.
 - **Two fingers** - reading two fingerprints.
 - **Two thumb fingers** - reading two thumb fingerprints.
 - **Left four fingers** - reading fingerprints of four fingers of the left hand.
 - **Right four fingers** - reading fingerprints of four fingers of the right hand.
 - **Ten fingers** - reading 10 fingerprints.
 - **Left palm** - reading the left palm print.
 - **Right palm** - reading the right palm print.
 - **One roll finger** - reading a single fingerprint with an offset.
5. From the **Quality** drop-down list (2) select the fingerprint capture quality:
 - **20 (Weak)** - low quality.
 - **40 (Moderate)** - average quality (default).
 - **60 (Strong)** - high quality.
 - **80 (Strongest)** - the highest quality.
6. To start capturing fingerprints, click the **Start capturing** button (3) and follow the instructions displayed at the top of the **Suprema. Capture fingerprints** window.

Note

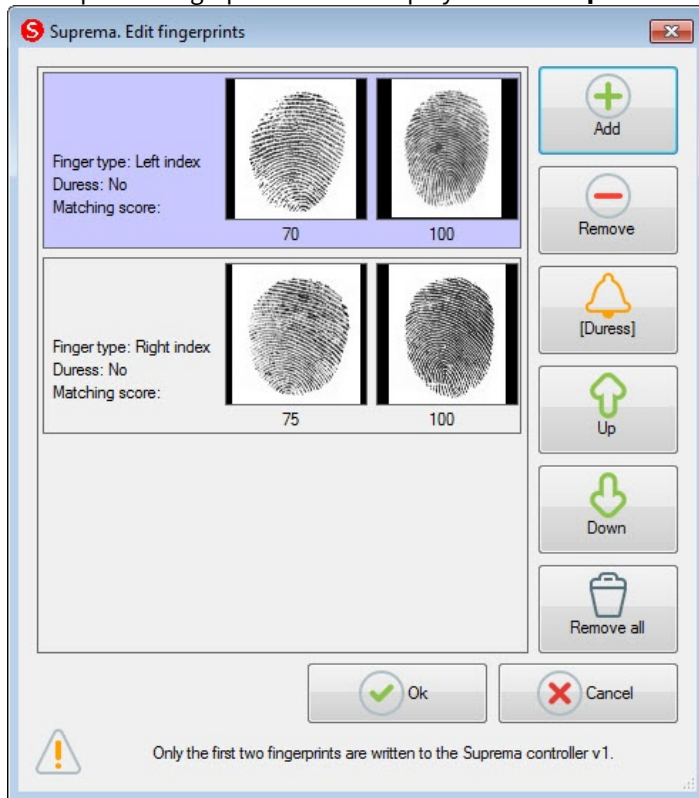
To capture fingerprints, each finger or group of fingers should be placed on the reader twice with 5 seconds delay after pressing the **Start capturing** button and after the first capture.

7. After the fingerprint capture is completed, select the type of scanned finger for each fingerprint in the drop-down list **(1)**:
 - **Undefined** - undefined.
 - **Left thumb** - thumb of the left hand.
 - **Left index finger** - index finger of the left hand.
 - **Left middle finger** - middle finger of the left hand.
 - **Left ring finger** - ring finger of the left hand.
 - **Left little finger** - little finger of the left hand.
 - **Right thumb** - thumb of the right hand.
 - **Right index finger** - index finger of the right hand.
 - **Right middle finger** - middle finger of the right hand.
 - **Right ring finger** - ring finger of the right hand.
 - **Right little finger** - little finger of the right hand.



8. Uncheck the **Add** check box **(2)** if it is not necessary to add the fingerprint to the user.
9. Click **OK** to save the result.

10. The captured fingerprints will be displayed in the **Suprema. Edit fingerprints** window.



11. To remove one fingerprint, select it and click **Remove**.

Note

To remove all fingerprints, click **Remove all**.

12. To mark a fingerprint as captured "Under duress", select it and click the **[Duress]** button.

Note

As a result, a silent alarm will be generated when reading this fingerprint.

13. To move a fingerprint up or down in the list, select it and click the **Up** or **Down** button.
 14. To finish entering fingerprints, click **OK**.

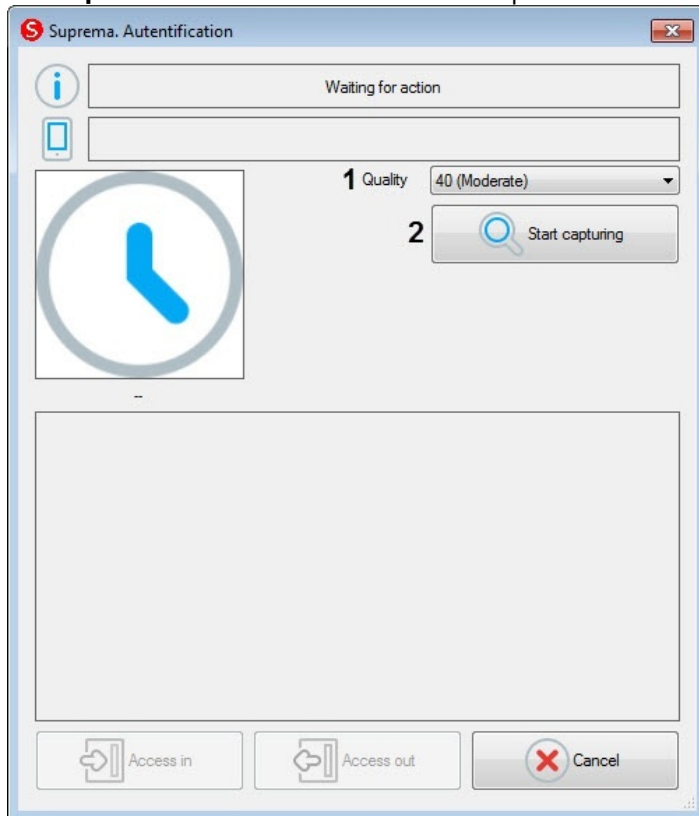
Capturing the fingerprints of the *Access Manager* users with *Suprema RealScan* is complete.

5.4.2 Verification of user authentication using the Suprema RealScan control reader

Verification of user authentication using the *Suprema RealScan* control reader is performed as follows:

1. Go to adding biometric data in the *Access Manager* window (see [Adding biometric parameters](#)).
2. Select the **(Fingerprint Authentication) Suprema RealScan** extension that corresponds to the *Suprema RealScan* control reader.

3. The **Suprema. Autentification** window will open.

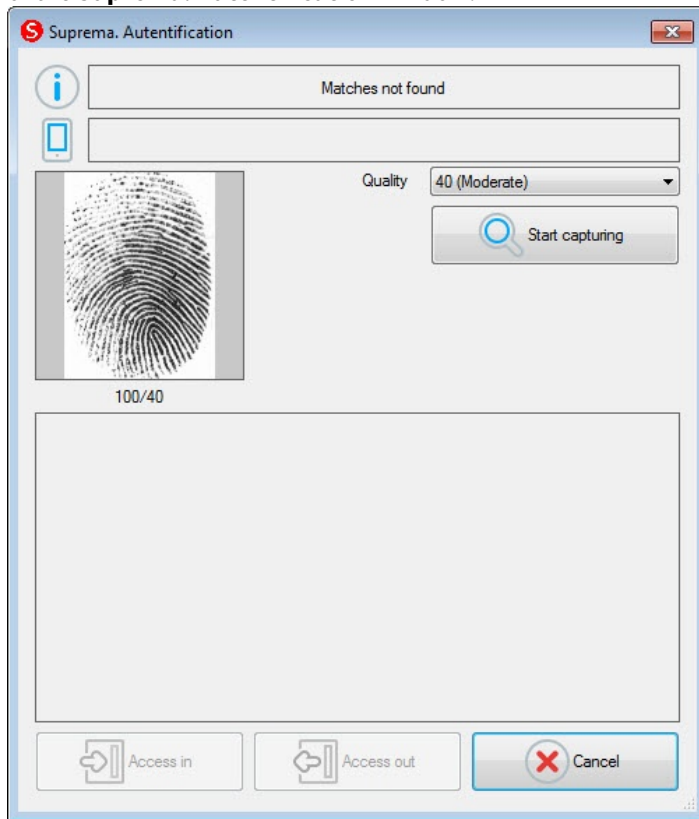


4. From the **Quality** drop-down list (1) select the fingerprint capture quality:
- **20 (Weak)** - low quality.
 - **40 (Moderate)** - average quality (default).
 - **60 (Strong)** - high quality.
 - **80 (Strongest)** - the highest quality.
5. To start capturing fingerprints, click the **Start capturing** button (2) and follow the instructions displayed at the top of the **Suprema. Autentification** window.

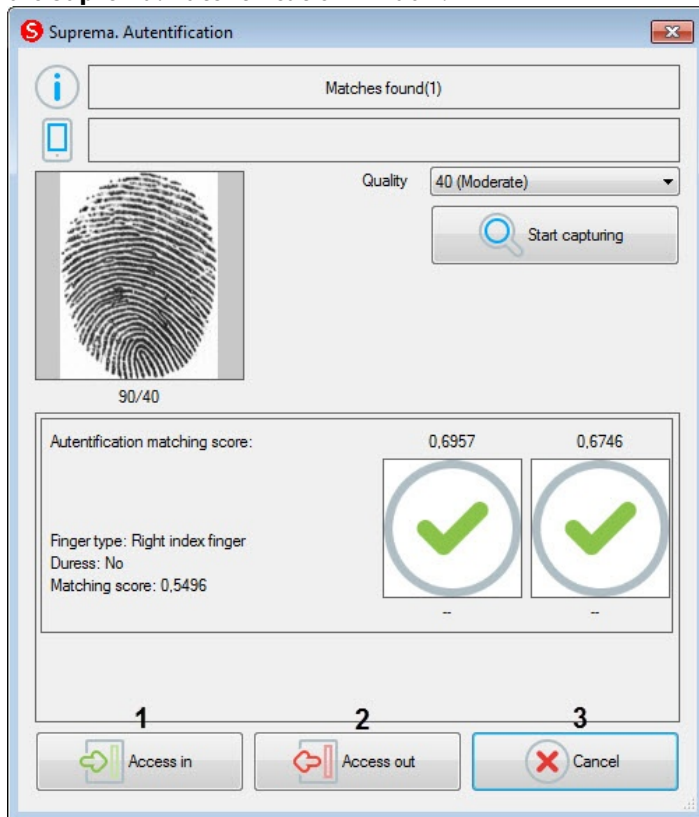
Note

The finger should be attached with 5 seconds delay after clicking the **Start capturing** button.

6. As a result, if there are no fingerprint matches, the **Matches not found** message will be displayed at the top of the **Suprema. Autentification** window.



If fingerprint matches are found, then the **Matches found** message will be displayed at the top of the **Suprema. Autentification** window.



7. To open the door for entrance, click the **Access in** button (1).
8. To open the door for exit, click the **Access out** button (2).
9. To close the **Suprema. Autentification** window, click **Cancel** (3).

Verification of user authentication using the *Suprema RealScan* control reader is completed.

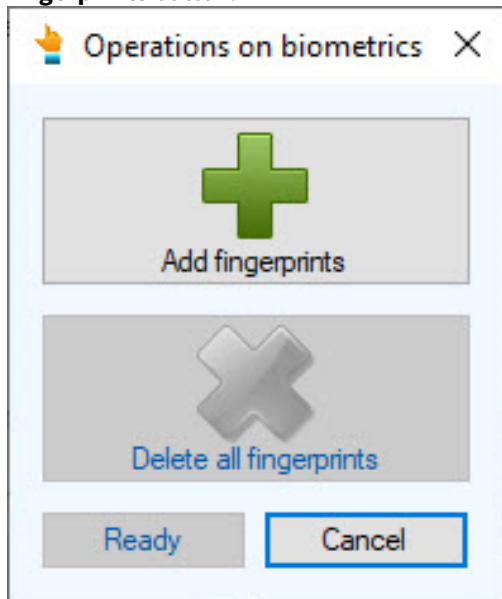
5.5 Working with FOH02 control reader

5.5.1 Capturing fingerprints of Access Manager users with FOH02

Adding fingerprints of the *Access Manager* users via the *FOH02* control reader is performed as follows:

1. Go to adding biometric data in the *Access Manager* window (see [Adding biometric parameters](#)).
2. Select the **(Virdi Fingerprints) Virdi Server** extension that corresponds to the *FOH02* control reader.

3. The **Operations on biometrics** dialog box will open. To add a new fingerprint, click the **Add fingerprints** button.



4. The **Virdi** window will open.



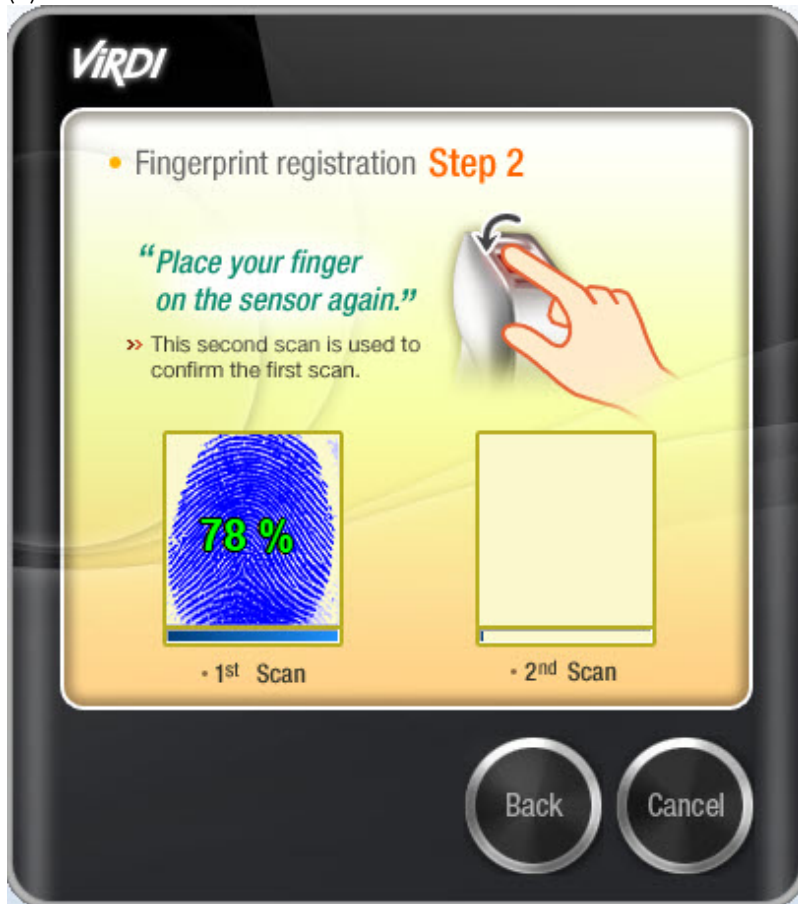
5. Click the **Next** button to start.

6. Select fingers for fingerprinting.



7. Place your finger on the reader to scan the fingerprint — the result will be displayed in the **1st Scan** window (1). Place your finger again to confirm the fingerprint. The result will be displayed in the **2nd Scan** window

(2).



8. In the **Operations on biometrics** window, click the **Ready** button, then save the user's settings.

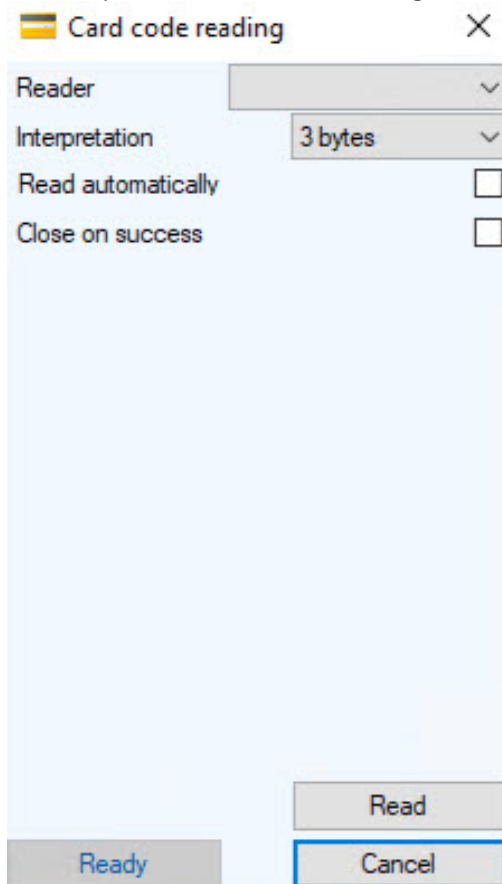
Capturing the fingerprints of the *Access Manager* users with *FOH02* is complete.

5.5.2 Entering the card number with FOH02 control reader

Entering the card number of the *Access Manager* users via the *FOH02* control reader is performed as follows:

1. Open the *Access Manager* window (see [Starting and stopping the Access Manager module](#)).
2. Go to editing the required user (see [Going to user editing](#)).

3. Enter the card number using the control reader (see [Entering an access card number using a control reader](#)). An example of the **Card code reading** window:



Entering the card number with *FOH02* control reader is completed.

Note

The specific feature of the *FOH02* reader is that you can choose different interpretations of the card code in order to work with other access control systems. To work with the *Virdi* ACS, use the standard settings.

5.6 Working with a universal reader

On the page:

- [Virtual reader](#)
- [Smart card reader](#)

Universal reader can read both the card number (see [Entering an access card number using a control reader](#)) and user data from the card.

You can work with a universal reader via a virtual reader or via a smart card reader that can be connected to any USB reader.

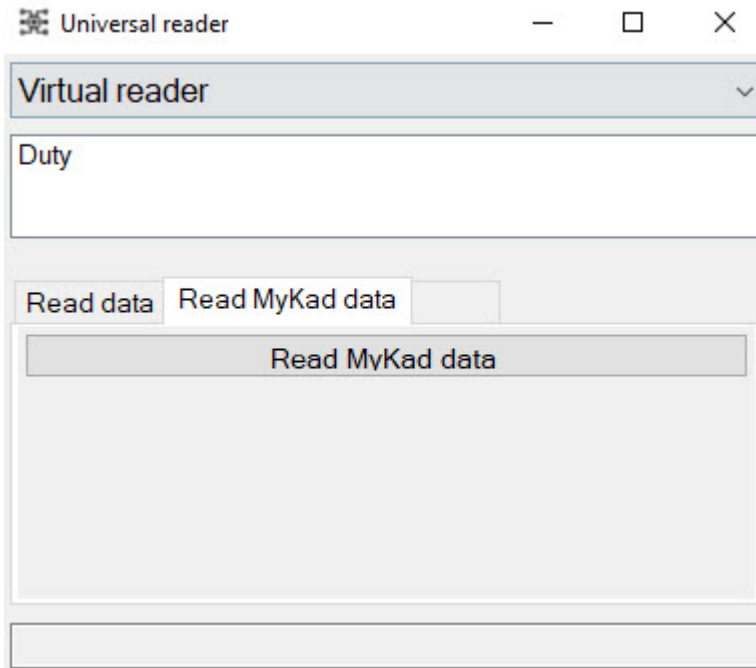
5.6.1 Virtual reader

1. To work with a virtual reader, select it from the reader drop-down list.

The screenshot shows a window titled "Universal reader" with standard window controls (minimize, maximize, close). Inside the window, there is a dropdown menu at the top currently set to "Virtual reader". Below this is a text field labeled "Duty". Further down, there are two tabs: "Read data" (which is selected) and "Read MyKad data". Under the "Read data" tab, there are three rows of controls: a "Block" dropdown menu set to "Digit", a "Key type" dropdown menu set to "B", and a "Key" text field containing "FFFFFFFFFFFF". At the bottom of these controls is a button labeled "Read data".

2. To read user data, go to the **Read data** tab.
 - a. From the **Block** drop-down list, select the format of the protected block of the card memory: **Digit** or **Hex**.
 - b. From the **Key type** drop-down list, select one of two types of access keys to the protected block of the card memory: **A** or **B**.
 - c. In the **Key** field, specify a key that protects access to the protected block of the card memory.
 - d. Click the **Read data** button. The process of reading the data of the access card starts.

3. To read the data of the MyKad identification card, go to the **Read MyKad data** tab.



The screenshot shows a window titled 'Universal reader' with standard Windows window controls (minimize, maximize, close). Inside the window, there is a dropdown menu at the top labeled 'Virtual reader'. Below this is a text input field labeled 'Duty'. A tabbed interface is present with two tabs: 'Read data' and 'Read MyKad data'. The 'Read MyKad data' tab is currently selected, and it contains a large, empty rectangular area for displaying data. At the bottom of the window is a single-line text input field.

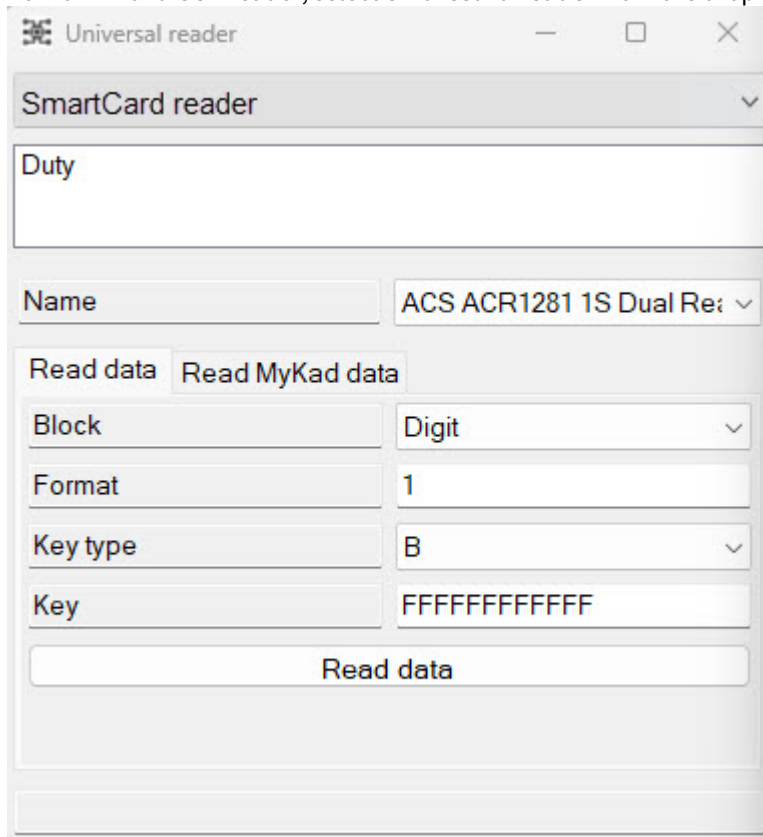
- a. Click the **Read MyKad data** button. The process of reading the data of the MyKad identification card starts.

**Note**

The MyKad card is used for identification in Malaysia. The MyKad card can be read using a universal reader. You can enter a card number in the corresponding user fields in the *Access Manager*. You can also enter the following user data: name, surname, address, photo.

5.6.2 Smart card reader

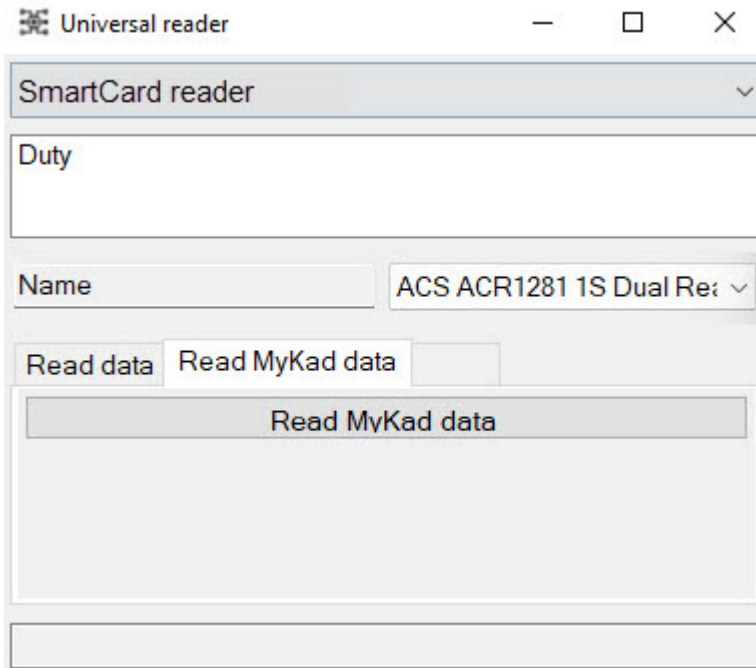
1. To work with a USB reader, select **SmartCard reader** from the drop-down list.



The screenshot shows a window titled "Universal reader" with a standard Windows-style title bar (minimize, maximize, close buttons). Inside the window, there is a drop-down menu at the top currently set to "SmartCard reader". Below this is a large text area labeled "Duty". Underneath the "Duty" area is a section with a "Name" label and a drop-down menu showing "ACS ACR1281 1S Dual Re". Below the "Name" section are two tabs: "Read data" (which is selected) and "Read MyKad data". Under the "Read data" tab, there are four rows of configuration fields: "Block" with a drop-down menu set to "Digit", "Format" with a text field containing "1", "Key type" with a drop-down menu set to "B", and "Key" with a text field containing "FFFFFFFFFFFF". At the bottom of this configuration section is a button labeled "Read data".

2. To read smart card data, remain on the **Read data** tab that is selected by default.
 - a. From the **Name** drop-down list, select the device for reading the access card data.
 - b. From the **Block** drop-down list, select the format of the protected block of the smart card memory.
 - c. In the **Format** field, enter the format of the smart card.
 - d. From the **Key type** drop-down list, select one of two types of access keys to the protected block of the smart card memory: **A** or **B**.
 - e. In the **Key** field, specify a key that protects access to the protected block of the smart card memory.
 - f. Click the **Read data** button. The process of reading the data of the smart card starts.

3. To read the data of the MyKad identification card, go to the **Read MyKad data** tab.



The screenshot shows a software window titled "Universal reader" with standard window controls (minimize, maximize, close). Inside the window, there is a dropdown menu at the top set to "SmartCard reader". Below it is a text field labeled "Duty". Underneath is a "Name" label followed by a dropdown menu currently showing "ACS ACR1281 1S Dual Re:". At the bottom, there are two tabs: "Read data" and "Read MyKad data", with the latter being the active tab. The content area of the "Read MyKad data" tab is mostly empty, with a faint "Read MyKad data" label at the top.

- a. From the **Name** drop-down list, select the device for reading the data of the MyKad identification card.
- b. Click the **Read MyKad data** button. The process of reading the data of the MyKad identification card starts.

Working with a virtual reader is complete.