ACFA Intellect

Control Readers Settings Guide

Last update 24/11/2020

Table of contents

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).

Intellect Client – a computer with *Intellect* software installed in a **Client** configuration.

Intellect Server – a computer with *Intellect* software installed in a **Server** configuration.

2 General information on control reader integration modules

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

Name	Vendor
HID OMNIKEY® 5321 CL SAM	**HID Global** 611 Center Ridge Drive Austin, TX 78753, U.S.A Tel.: (949) 732-2000, (800) 237-7769 https://www.hidglobal.com/
BioSmart FS80	**Prosoft Systems** 620102 Russia Yekaterinburg 194 A Vologodskaya str. Tel.: +7 (343) 376-2820; 356-5111 E-mail: 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	**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
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/

Modules licensing

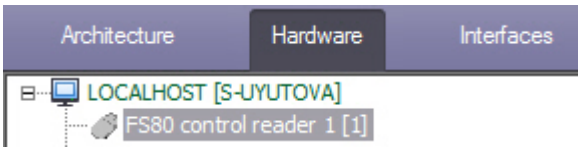
Control readers are available free of charge upon purchase of an *Access Manager* module license (see Access Manager Module Settings and Operation Guide).

4 Configuring control readers in the Intellect software

4.1 Configuring BioSmart FS80 control reader in the Intellect 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 *Intellect* software.

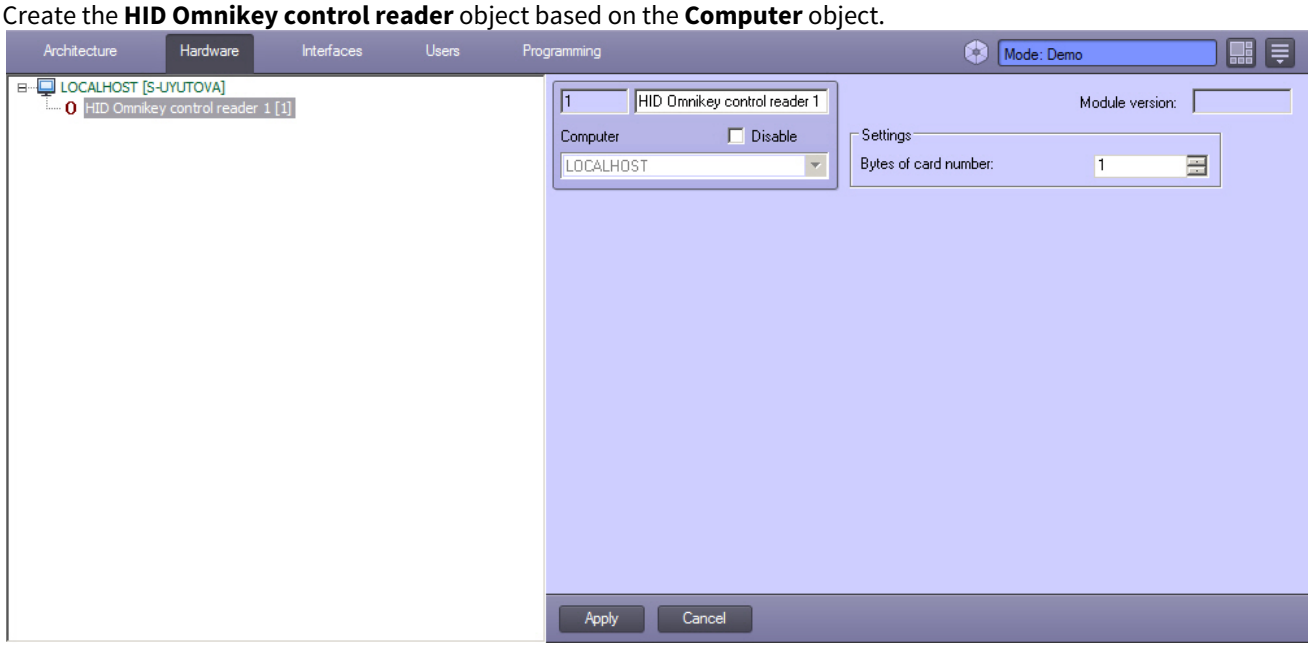


4.2 Configuring HID OMNIKEY control reader in the Intellect software

After connection of the *HID OMNIKEY® 5321 CL SAM* reader to a Server download and install driver from the manufacturer official web site.

To configure the *HID OMNIKEY* control reader in the *Intellect* software, do the following:

1. Create the **HID Omnikey control reader** object based on the **Computer** object.



2. Specify the number of bytes of card number on the object settings panel.
3. Click **Apply**.

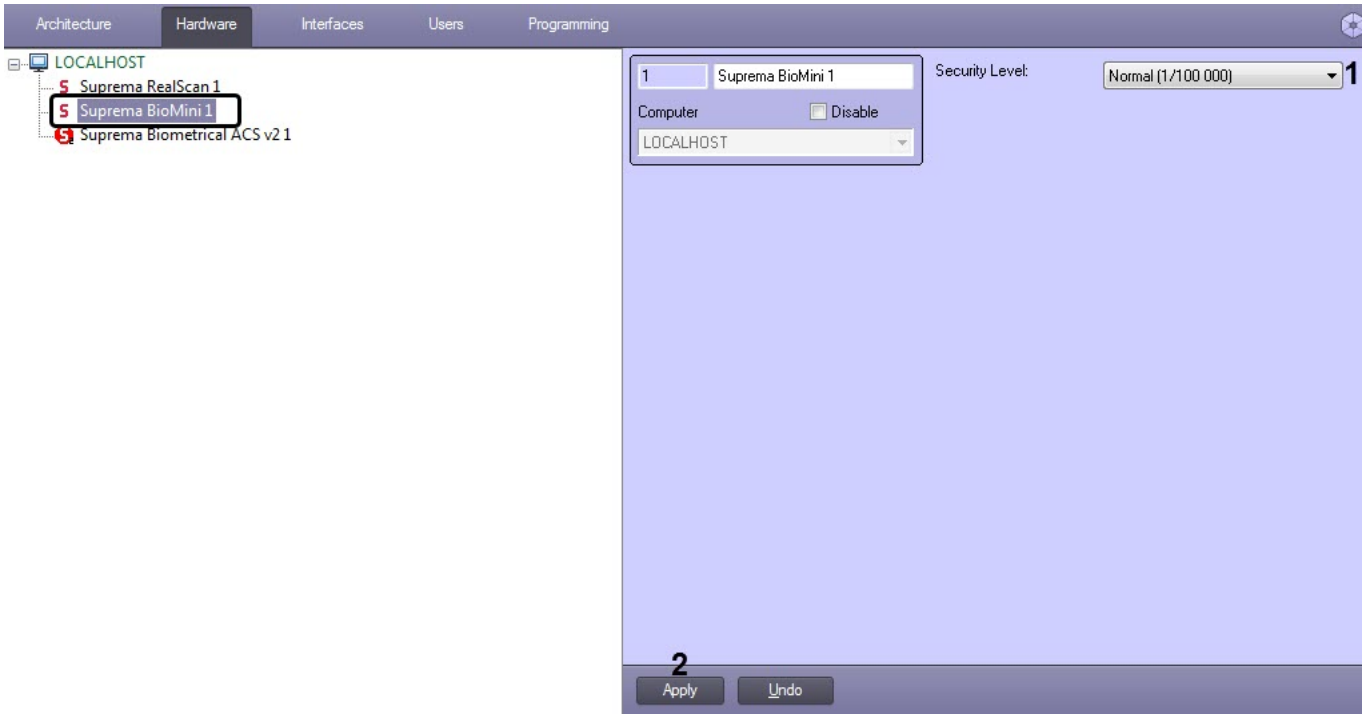
4.3 Configuring Suprema BioMini control reader

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 Suprema 2 Settings Guide.

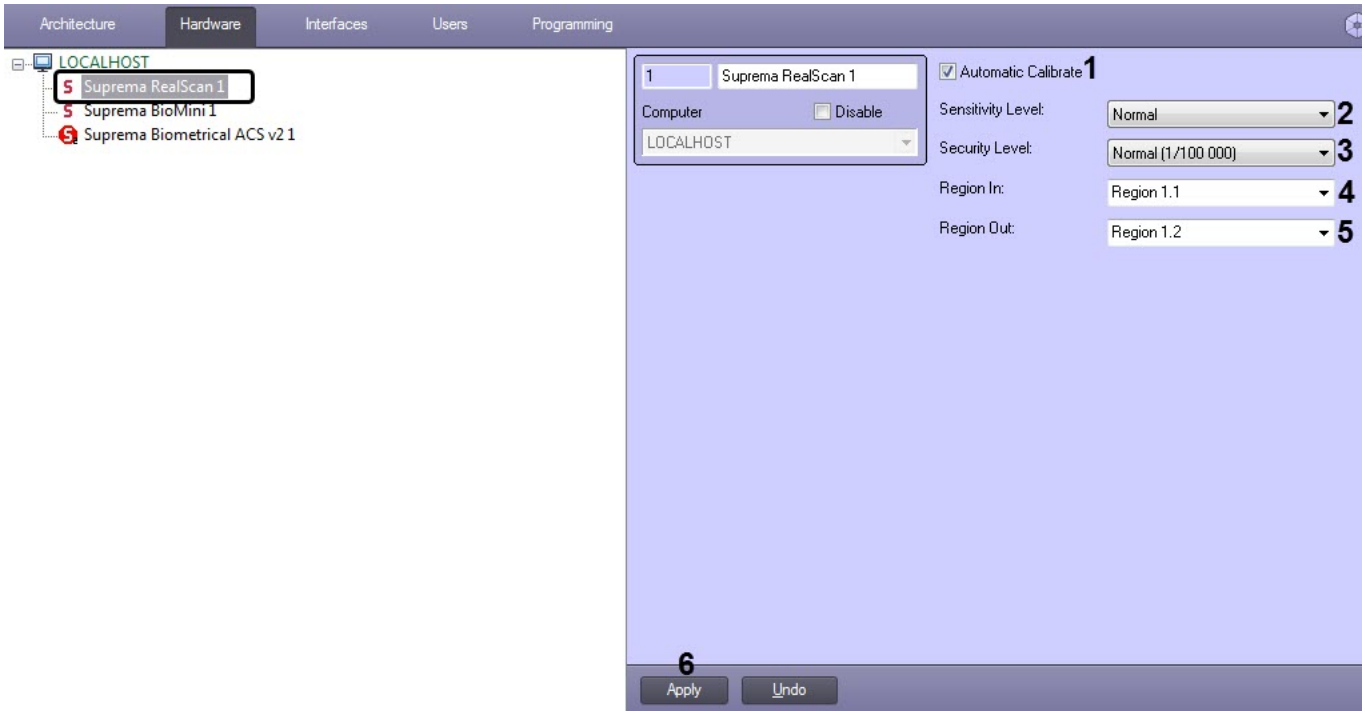
Configuring *Suprema BioMini* control reader is completed.

4.4 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.

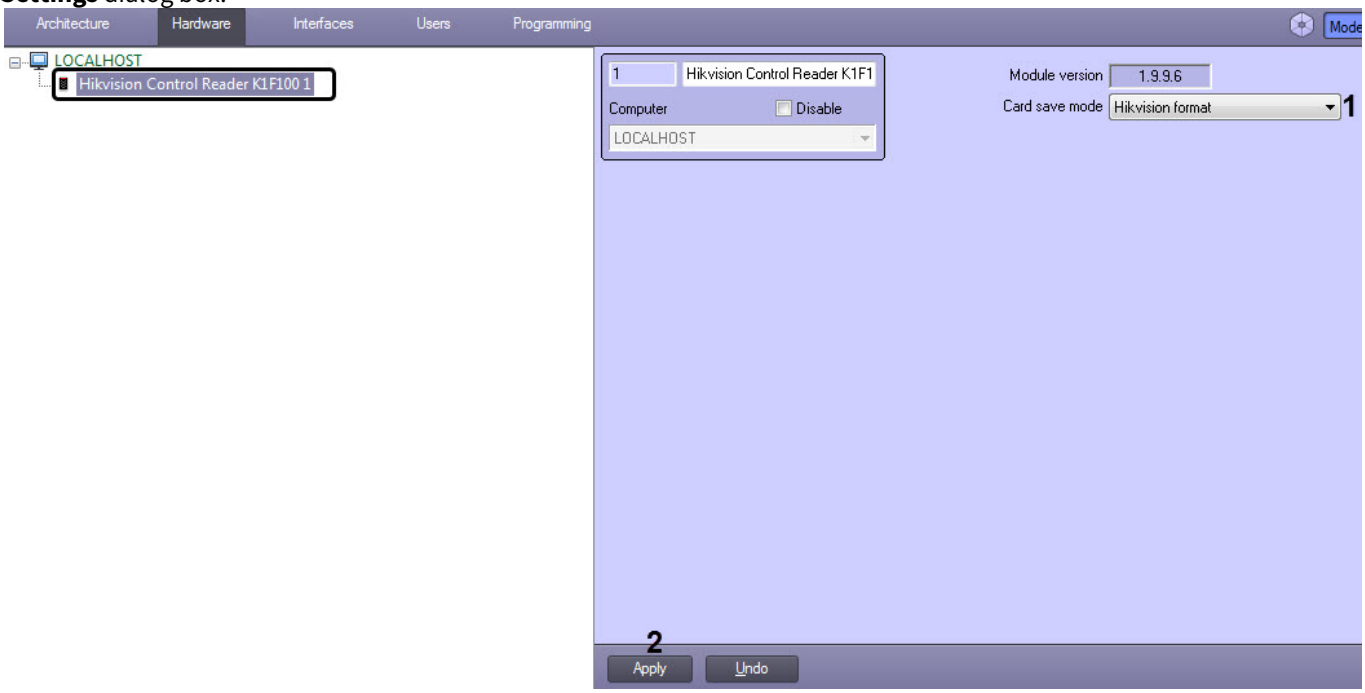
> **Note**
>
> - Capturing fingerprints with this control reader in the *Access Manager* is described in the Capturing fingerprints in Access Manager with Suprema RealScan.
> - The *Suprema RealScan* control reader is to be used only with the *Suprema 2* integration module – see Suprema 2 Settings Guide.

Configuring *Suprema RealScan* control reader is completed.

4.5 Configuring Hikvision DS-K1F100 control reader in the Intellect 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.

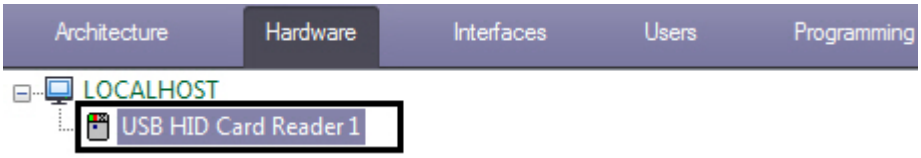
   > **Attention!**
   >
   > **Card + Facility code** only works for EM-Marine Wiegand-26 access cards. Other types of cards will be saved in Hikvision format.

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

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

4.6 Configuring Proxy-USB-MA and ST-CE321LR-WT control readers in the Intellect software

After connection of the *Proxy-USB-MA* and *ST-CE321LR-WT* readers to a Server create the **USB HID Card Reader** object on the base of the **Computer** object in the *Intellect* software.



5 Working with control readers in the Intellect software

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

The biometric control readers integration modules are designer 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 the *ACFA Intellect* software:

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

Information on how to configure the **Event Viewer** interface object is given in Intellect software package: Administrator's Guide.

Information on how to use the **Event Viewer** interface object is given in Intellect software package:Operator's Guide.

Information on how to use the **Access Manager** interface object is given in Access Manager Module Settings and Operation Guide.

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 Input of 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.

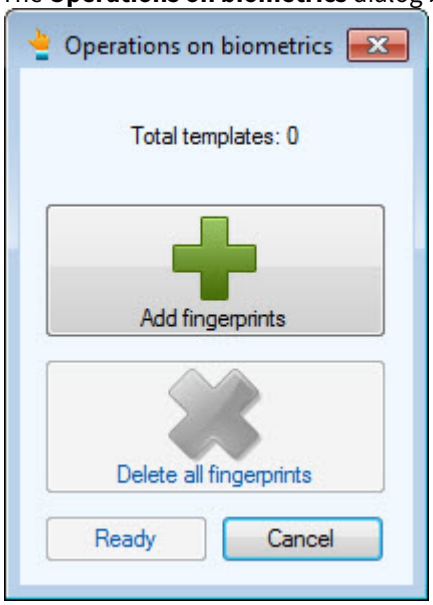
5.2 Adding the Access Manager users fingerprints using Biosmart FS80

> **Important!**
>
> The *FS80* control reader is to be used only with the BioSmart integration module (see BioSmart Integration Module Configuration and Operation Manual).

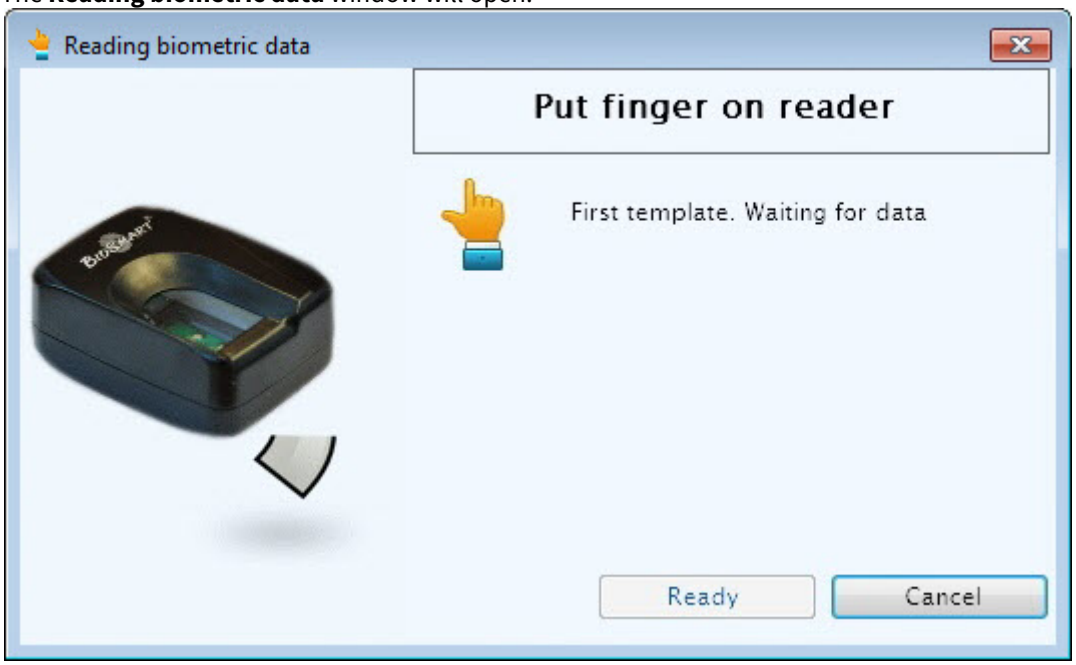
To add the biometric parameters (fingerprints) of users from the *Access Manage*r module using the *BioSmart FS80* biometric control reader, do the following:

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.

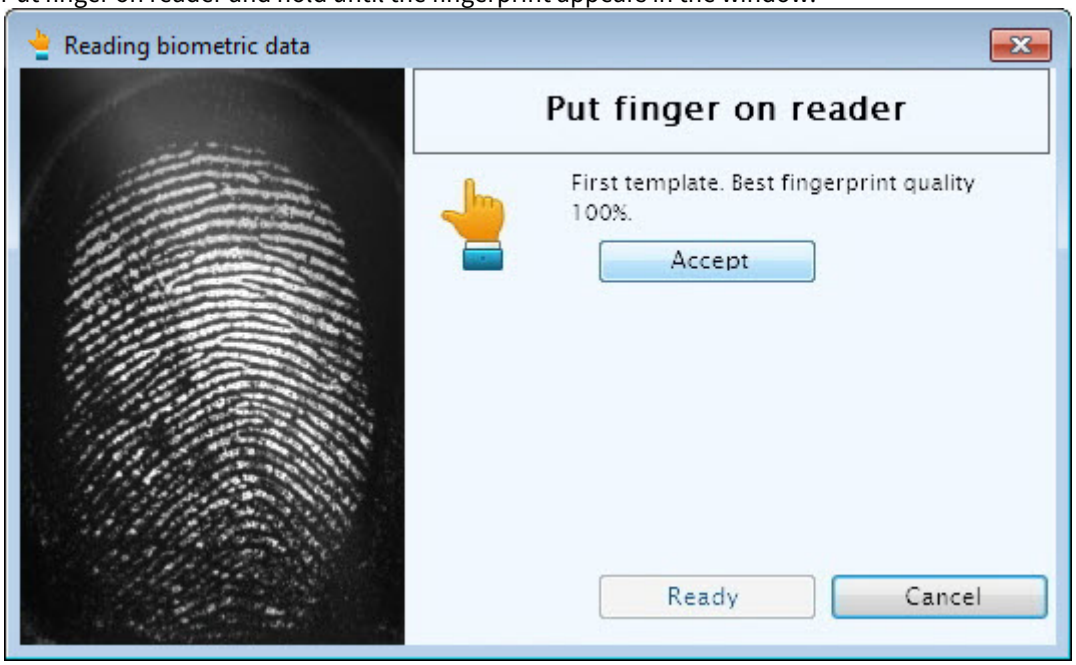
3. The **Operations on biometrics** dialog box will open. To add a new fingerprint, click the **Add fingerprints** button.



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



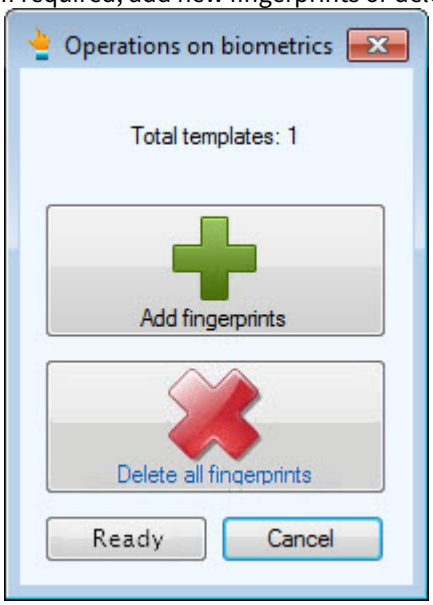
4. Put finger on reader and hold until the fingerprint appears in the window.



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

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

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



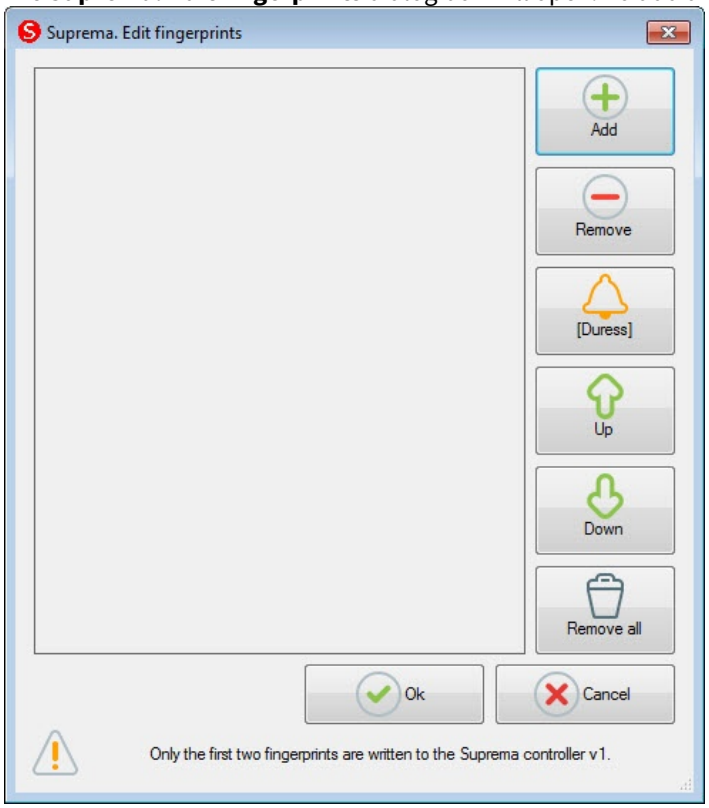
9. Click **Ready** and then save the user parameters.

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

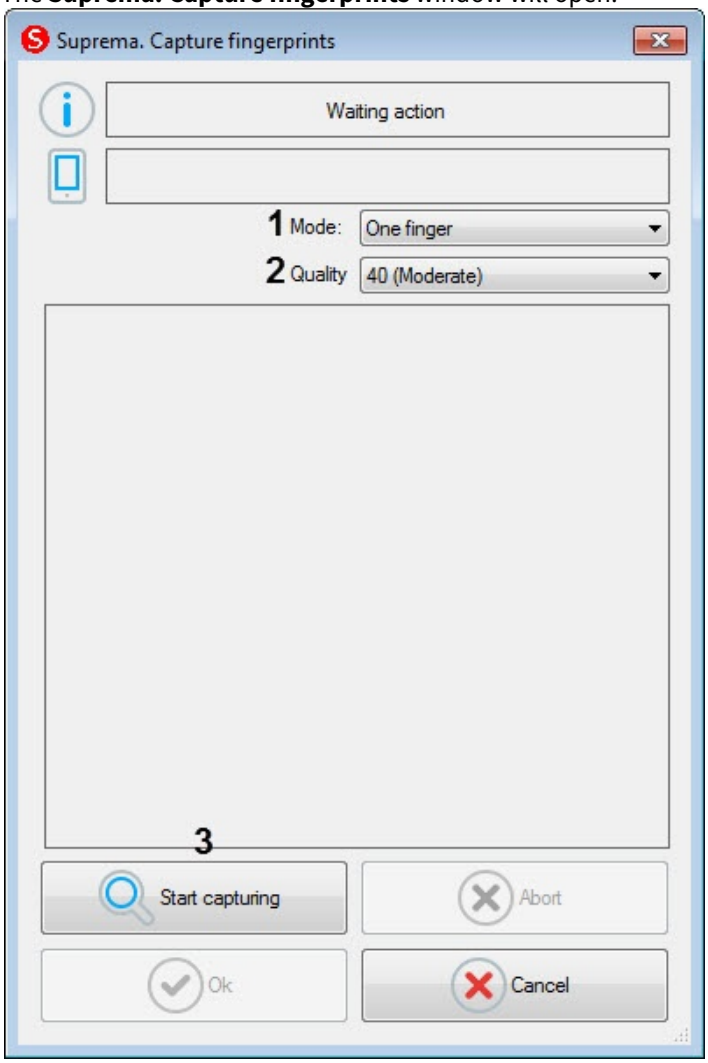
5.3 Capturing fingerprints of Access Manager users with Suprema BioMini

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.



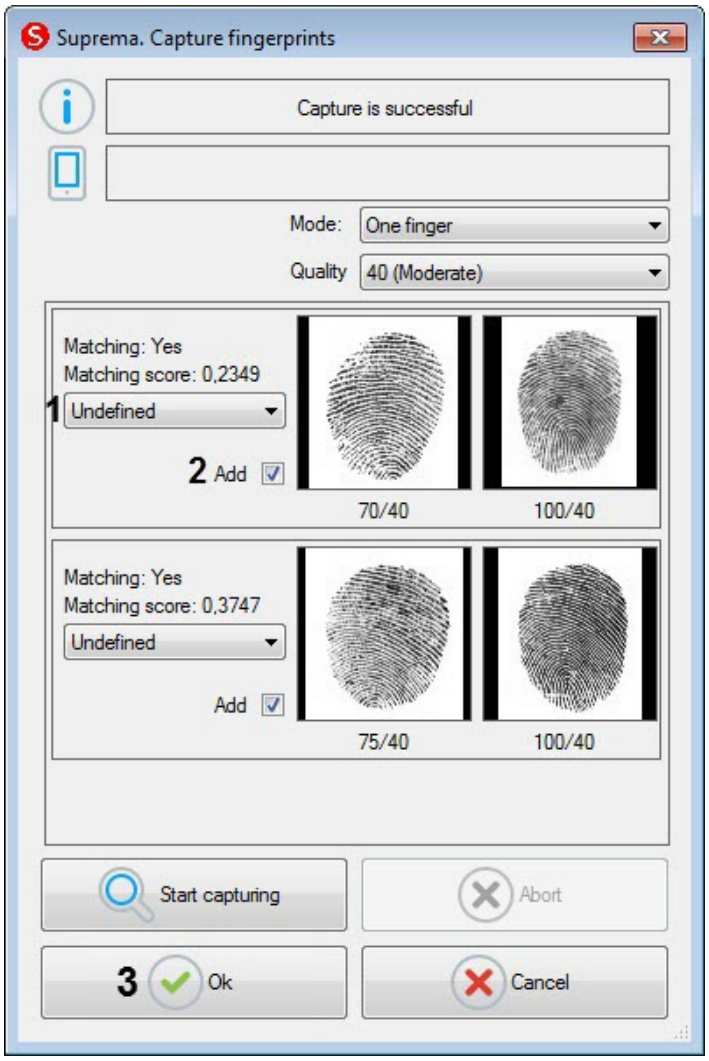
4. From the **Mode** drop-down list (**1**) select the fingerprint **One finger** capture mode.
5. From the **Quality** drop-down list (**2**) select the fingerprint capture quality:
   - **20 (Weak)** - low quality.
   - **40 (Moderate)** - average quality (default).
   - **60 (Strong)** - high quality.
   - **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.

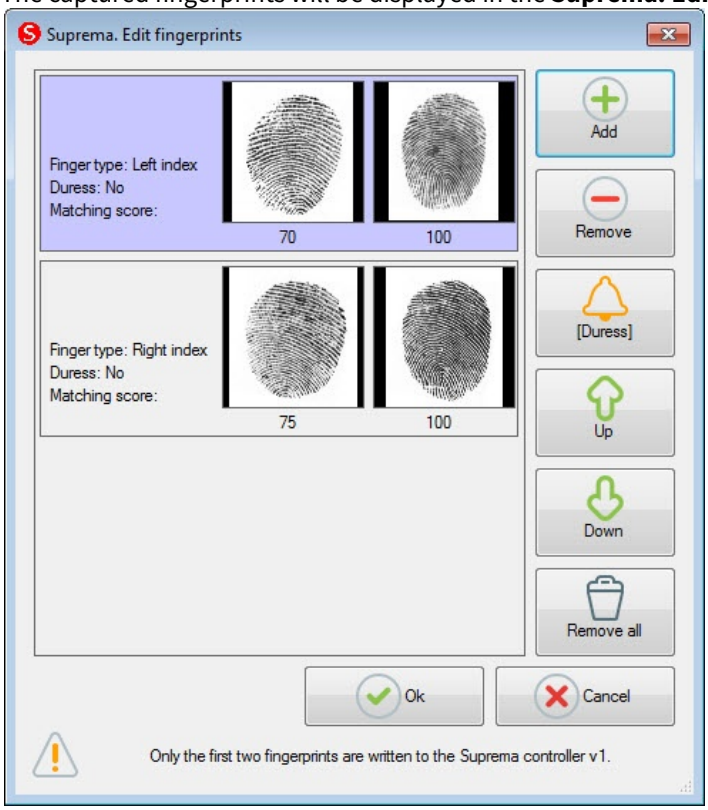
7. After the fingerprint capture is completed, select the type of scanned finger for each fingerprint in the drop-down list (**1**):
   - **Undefined** - undefined.
   - **Left thumb** - thumb of the left hand.
   - **Left index finger** - index finger of the left hand.
   - **Left middle finger** -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

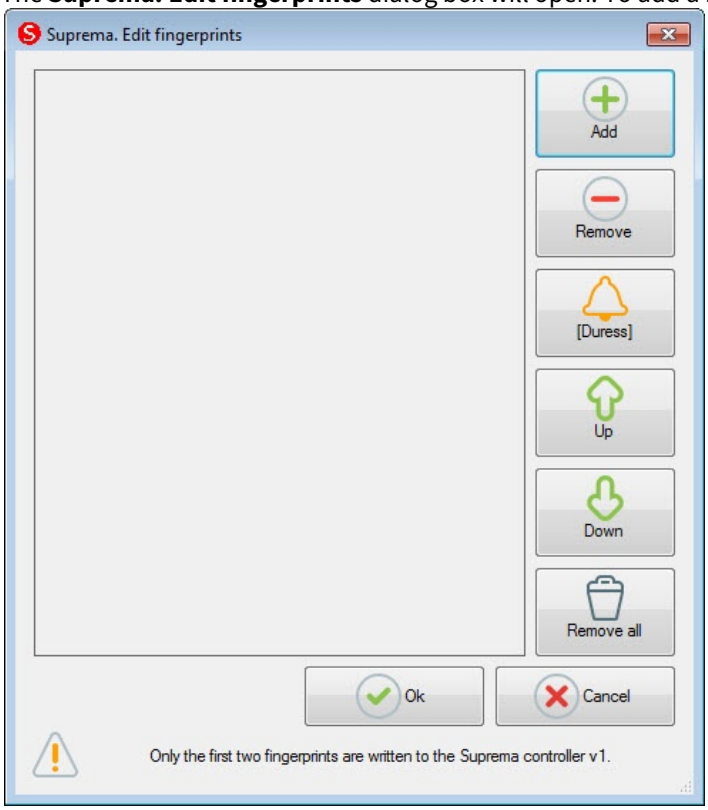
5.4 Working with Suprema RealScan control reader

5.4.1 Capturing fingerprints of Access Manager users with Suprema RealScan

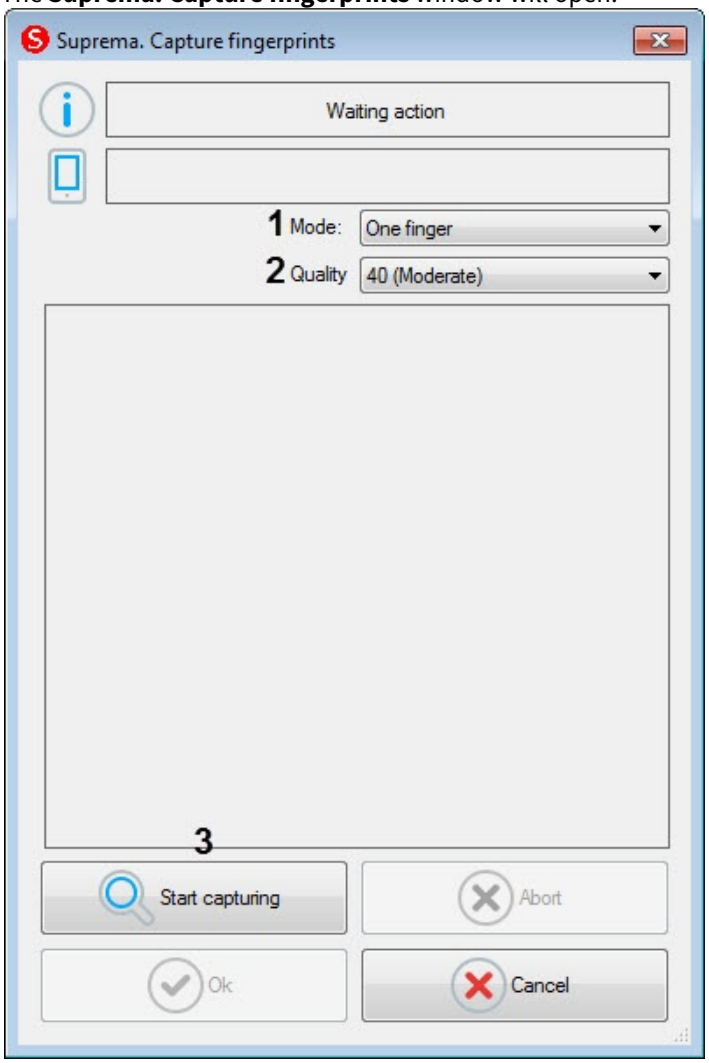
Adding fingerprints of the *Access Manager* users via the *Suprema RealScan* control reader is performed as follows:

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.



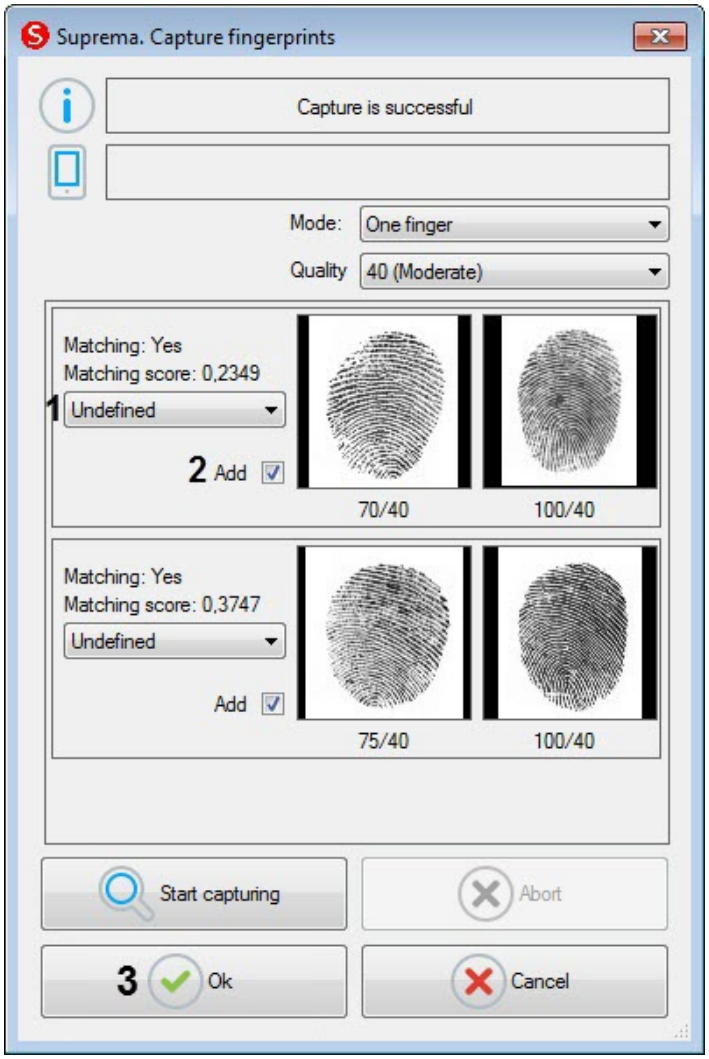
The **Suprema. Capture fingerprints** window will open.



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.

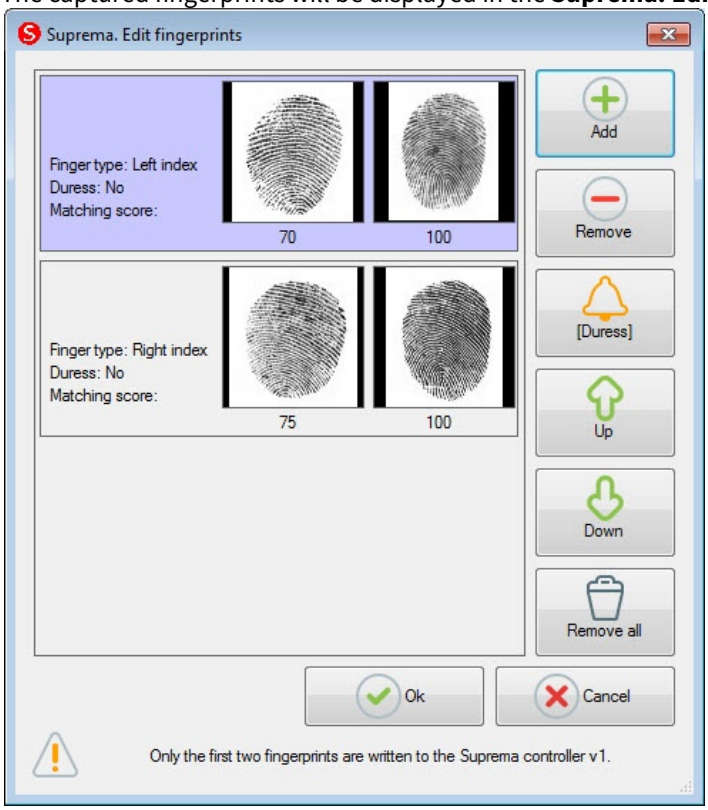
> **Note**
>
> To capture fingerprints, each finger or group of fingers should be placed on the reader twice with 5 seconds delay after pressing the **Start capturing** button and after the first capture.

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**.

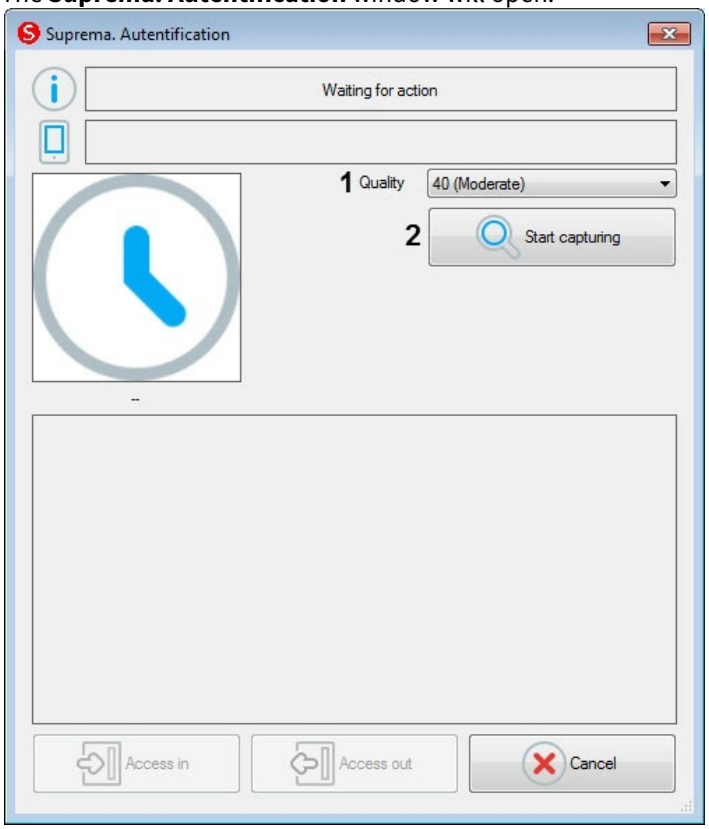
Capturing the fingerprints of the *Access Manager* users with *Suprema RealScan* is complete.

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.

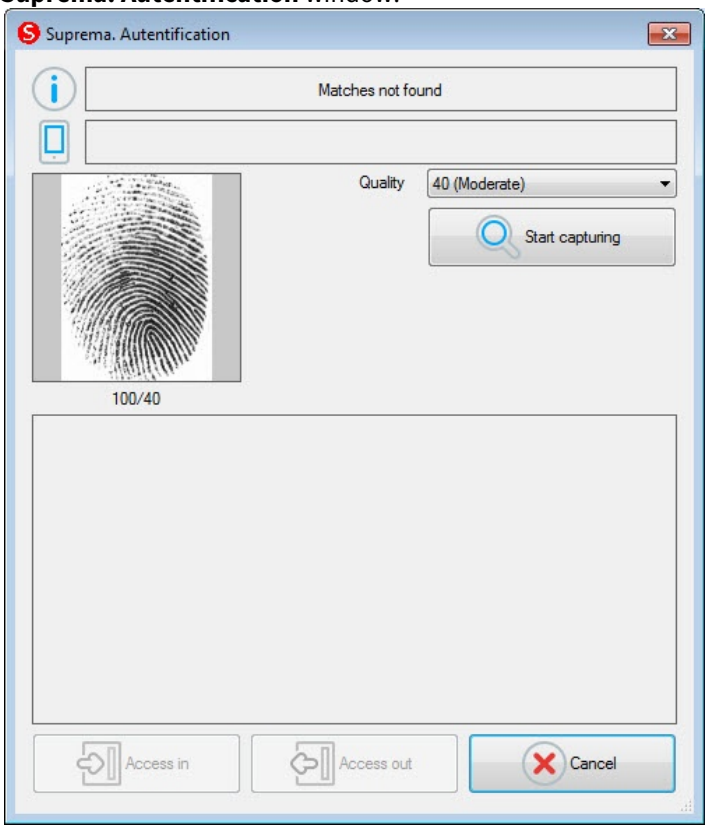
3. The **Suprema. Autentification** window will open.



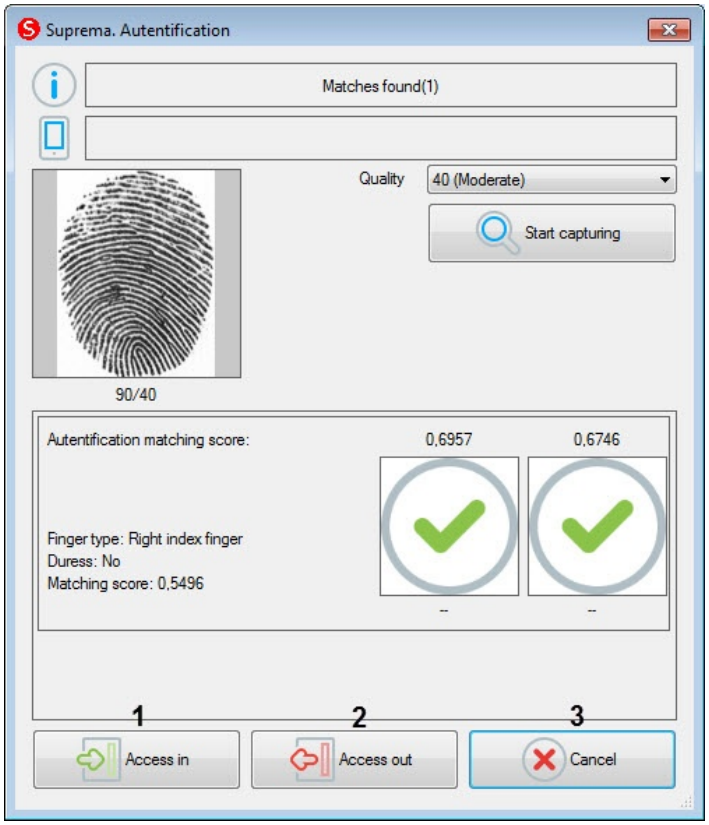
4. From the **Quality** drop-down list (**1**) select the fingerprint capture quality:
   - **20 (Weak)** - low quality.
   - **40 (Moderate)** - average quality (default).
   - **60 (Strong)** - high quality.
   - **80 (Strongest)** - the highest quality.
5. To start capturing fingerprints, click the **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.