ACFA Intellect

Suprema 2 Settings Guide

Last update 26/01/2023

Table of contents

1 Introduction into Suprema 2 Settings Guide

On the page:

1.1 Purpose of the Document

Suprema 2 Settings Guide is a reference and information guide meant for *Suprema 2* configuration specialists. This module is a part of Access Control subsystem in *ACFA Intellect*.

The guide provides the following:

1. General information about *Suprema 2* integration module;
2. Configuration of *Suprema 2* integration module;
3. Operation of *Suprema 2* integration module.

1.2 General information about Suprema 2 integration module

Suprema 2 integration module is the *ACFA Intellect*-based *ACS* component. The module is designed for *Suprema 2 ACS* interaction with *ASFA Intellect* (monitoring, control).

> **Note**
>
> For more information about *Suprema 2 ACS*, please refer to official documentation for this system (manufacturer Suprema Inc.)

Before configuring *Suprema 2* integration module do the following:

1. Install *Suprema 2 ACS* hardware on site.
2. Connect *Suprema 2* hardware to the Server.
3. Install *BioStar 2* software on the Server (to download the software, go to the manufacturer's website)
4. Configure *Suprema 2 ACS* connection to the *BioStar 2* Server (configuration of *BioStar 2* utility is described in the official documentation).

2 Supported hardware and licensing of Suprema 2 integration module

Vendor	Suprema 17F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863 Republic of Korea www.supremainc.com
Integration type	SDK
Hardware connection	Ethernet

Supported hardware

Hardware	Function
BSA2-OEPW	Biometric terminal (scanner)
FaceStation 2	Biometric terminal (scanner)
BioStation 2	Biometric terminal (scanner)
BioEntry W	Biometric terminal (scanner)
CoreStation	Controller
BioEntry P2	Biometric device (scanner)
XPass 2	Reader
FaceStation F2 (all models)	Biometric terminal (scanner) with an option to receive temperature from Suprema Thermal Camera
X-Station 2 (all models)	Terminal (scanner) with an option to work with QR codes
XPass S2	Reader

Note.

All devices supporting SDK v.2 can be connected. The table lists those tested by AxxonSoft QA department.

Module licensing

Per scanner/reader.

3 Configuring Suprema 2 integration module

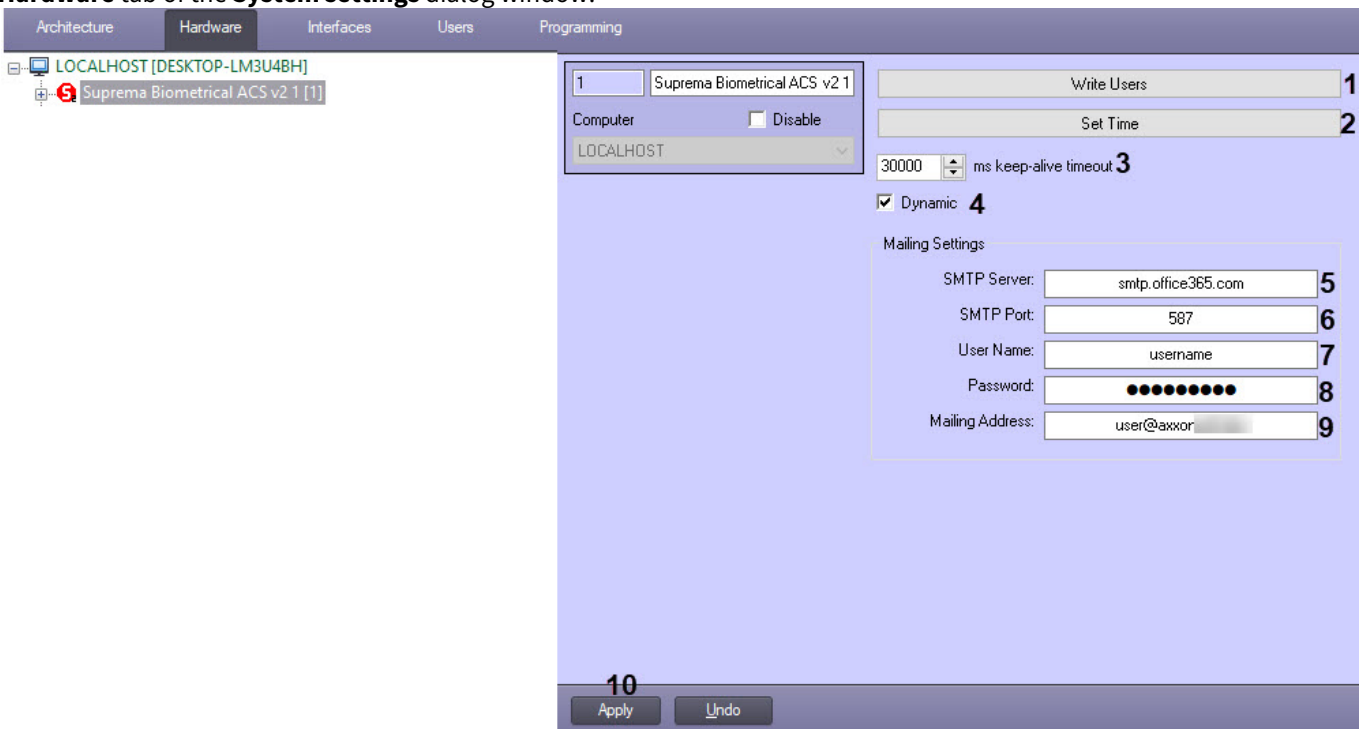
3.1 Activating Suprema 2 integration module

Create the **Suprema Biometrical ACS v2** object based on the **Computer** object in the **Hardware** tab of the **System settings** dialog box in order to activate *Suprema 2* integration module.

3.2 Configuring the Suprema 2 head object

To configure the Suprema 2 head object, do the following:

1. Go to the settings panel of the **Suprema Biometrical ACS v2** object, created on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog window.



2. Click the **Write users** button (**1**) to write users to all controllers.
3. Click the **Set Time** button (**2**) to synchronize the time of all controllers with the computer time.
4. Set the timeout in the **ms keep-alive timeout** field (**3**). The default value is 30000 ms.
5. Set the **Dynamic** checkbox (**4**) for dynamic recording of the users access settings.
6. To email QR codes, set the following parameters:
    a. In the **SMTP Server** field (**5**), enter the SMTP Server address of the outgoing mail;

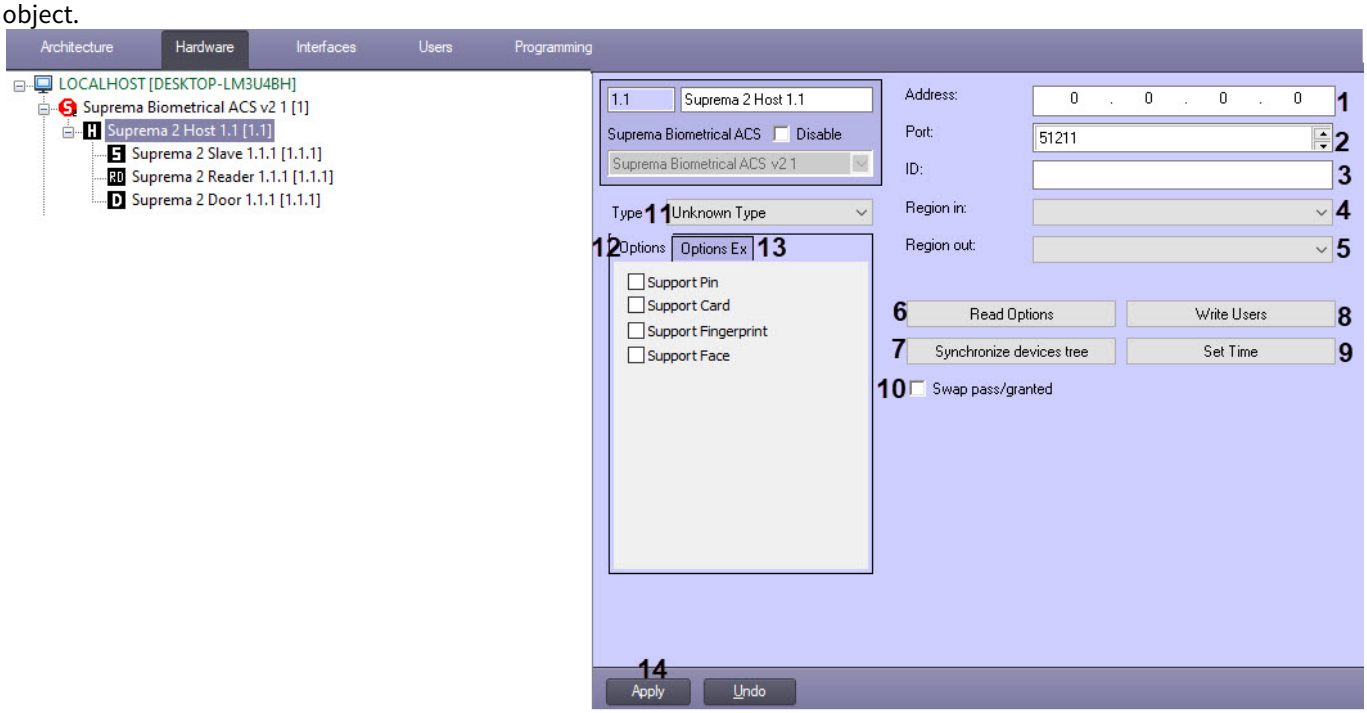
b. In the **SMTP Port** field (**6**), enter the port number used by the outgoing mail server;
c. In the **User Name** field (**7**), enter the name of the account used to send messages on the outgoing mail server;
d. In the **Password** field (**8**), enter the password of the account on the outgoing mail server;
e. In the **Mailing Address** field (**9**), enter the email address from which the messages will be sent.
If you don't need to send QR codes, you can skip this step.

7. Click the **Apply** button (**10**) to save the changes.

3.3 Configuring the Suprema 2 controller

The *Suprema 2* controller is configured as follows:

1. Go to the **Suprema 2 Host** object settings panel. The object is created on the basis of the **Suprema BiometricalACS v2** object.



2. In the **Address** (**1**) field, enter the IP address of the *Suprema 2* controller.
3. In the **Port** (**2**) field, set the port of the *Suprema 2* controller.
4. In the **ID** (**3**) field, specify the ID of the controller connected via Ethernet.
5. From the **Region in** (**4**) drop-down list, select the Region corresponding to the area where the user will be located after entering.
6. From the **Region out** (**5**) drop-down list, select the Region corresponding to the area where the user will be located after exiting.

> **Note**
>
> The **Region in** and **Region out** fields should be selected if *Time and Attendance* interface module is used. Otherwise, leave these fields empty.

7. Click the **Read Options** (**6**) button to read the current options of the controller. The **Type** (**11**) of the controller is determined automatically. The controller work features change depending on its specific type. For example, for Xpass S2 type controllers, the functionality of the module for reading events and writing users changes. This happens because with the usual functionality the events come with a delay, and it takes a long time to write users.

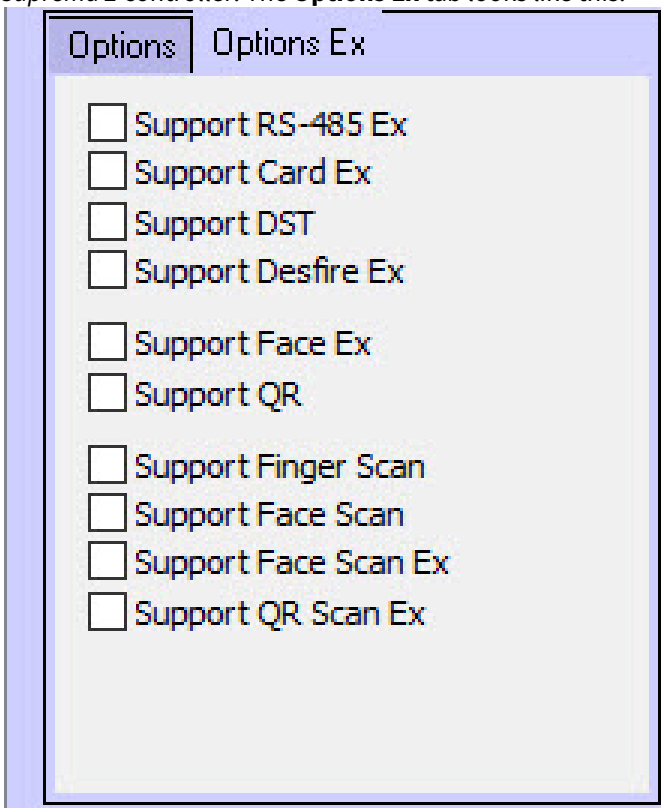
> **Attention!**
>
> It is not recommended to change the **Type** setting manually.

8. Click the **Synchronize devices tree** (**7**) button to automatically create a tree of devices connected to the controller in *ASFA Intellect*.

9. Click the **Write Users** (**8**) button to write users to the controller.
10. Click the **Set Time** (**9**) button to synchronize the controller time with the computer time.
11. Configure sending an event upon successful access: **Swap pass/granted** (**10**). If the checkbox is cleared, the **Pass** event is generated, otherwise, the **Access granted** event is generated.

> **Note**
>
> The setting is required for the *Time and Attendance Module* operation with one access terminal.

12. When reading the options (step 7), the checkboxes are automatically set on the **Options** (**12**) tab with the basic device features and on the **Options Ex** (**13**) tab with the advanced device features. These tabs are not editable and show the functional features of a specific type of *Suprema 2* controller. The set of supported features is different for each type of *Suprema 2* controller. The **Options Ex** tab looks like this:



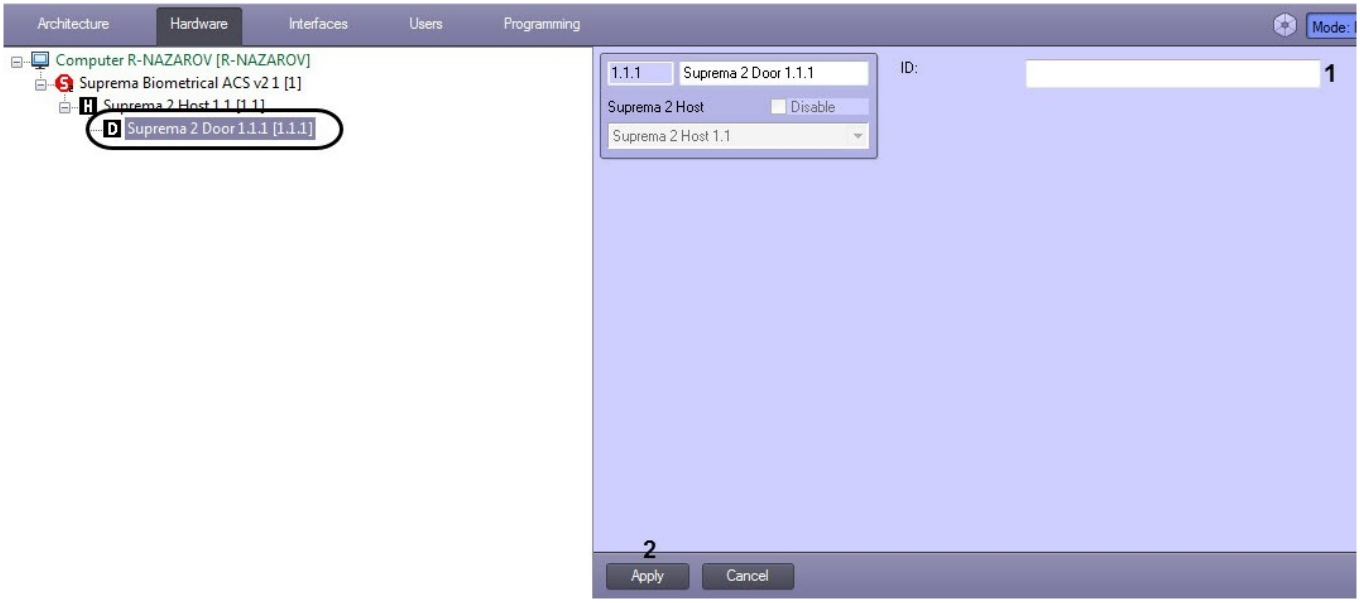
13. Click the **Apply** button (**14**) to save changes.

Configuring the *Suprema 2* controller is completed.

3.4 Configuring the Suprema 2 access point

To configure the *Suprema 2* access point, do the following:

1. Go to the **Suprema 2 Door** object settings panel. The object is created on the basis of the **Suprema 2 Host** object.



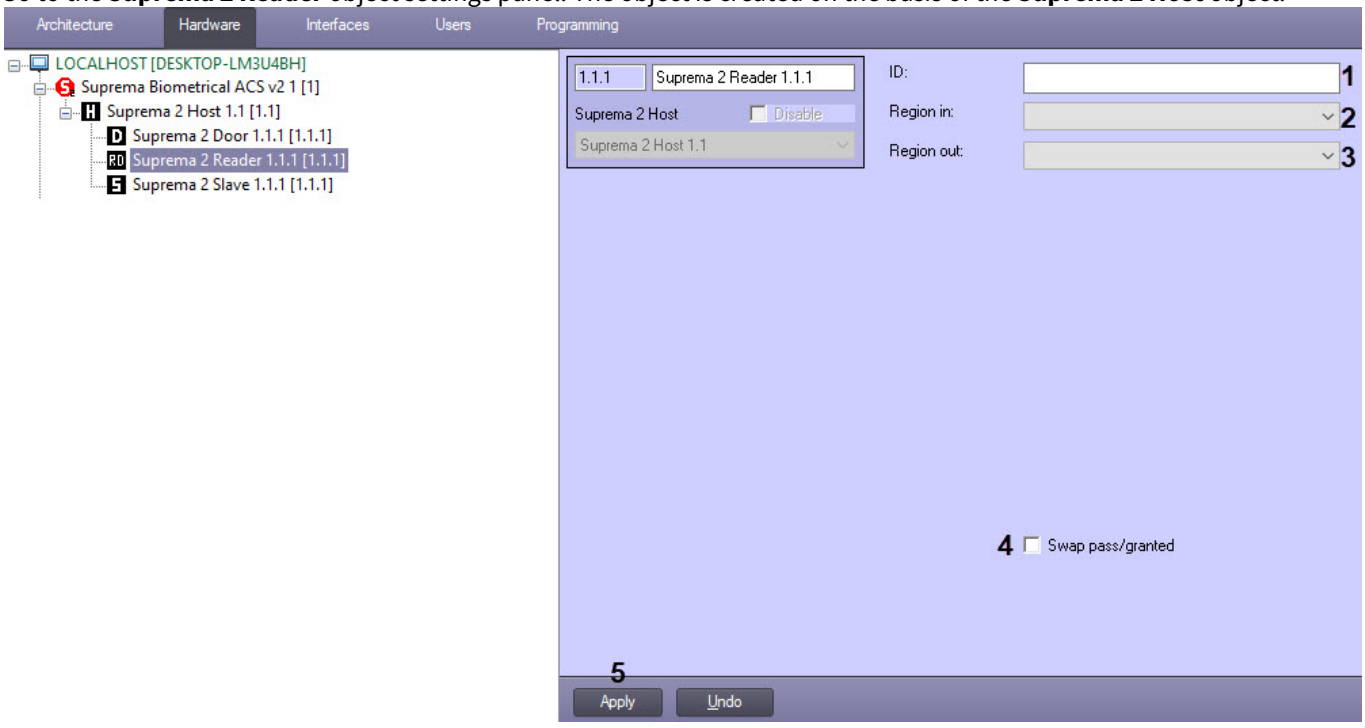
2. In the **ID** (**1**) field, specify the access point identification number.
3. Click the **Apply** (**2**) button to save changes.

Configuring the *Suprema 2* access point is completed.

3.5 Configuring the Suprema 2 reader

The *Suprema 2* reader is configured as follows:

1. Go to the **Suprema 2 Reader** object settings panel. The object is created on the basis of the **Suprema 2 Host** object.



2. In the **ID** (**1**) field, specify the identification number of the reader.
3. From the **Region in** (**2**) drop-down list, select the Region corresponding to the area where the user will be located after entering.
4. From the **Region out** (**3**) drop-down list, select the Region corresponding to the area where the user will be located after exiting.

> **Note**
>
> The **Region in** and **Region out** fields should be selected if *Time and Attendance* interface module is used. Otherwise, leave these fields empty.

5. Configure sending an event upon successful access: **Swap pass/granted** (**4**). If the checkbox is cleared, the **Pass** event is generated, otherwise, the **Access granted** event is generated.
6. Click the **Apply** (**5**) button to save changes.

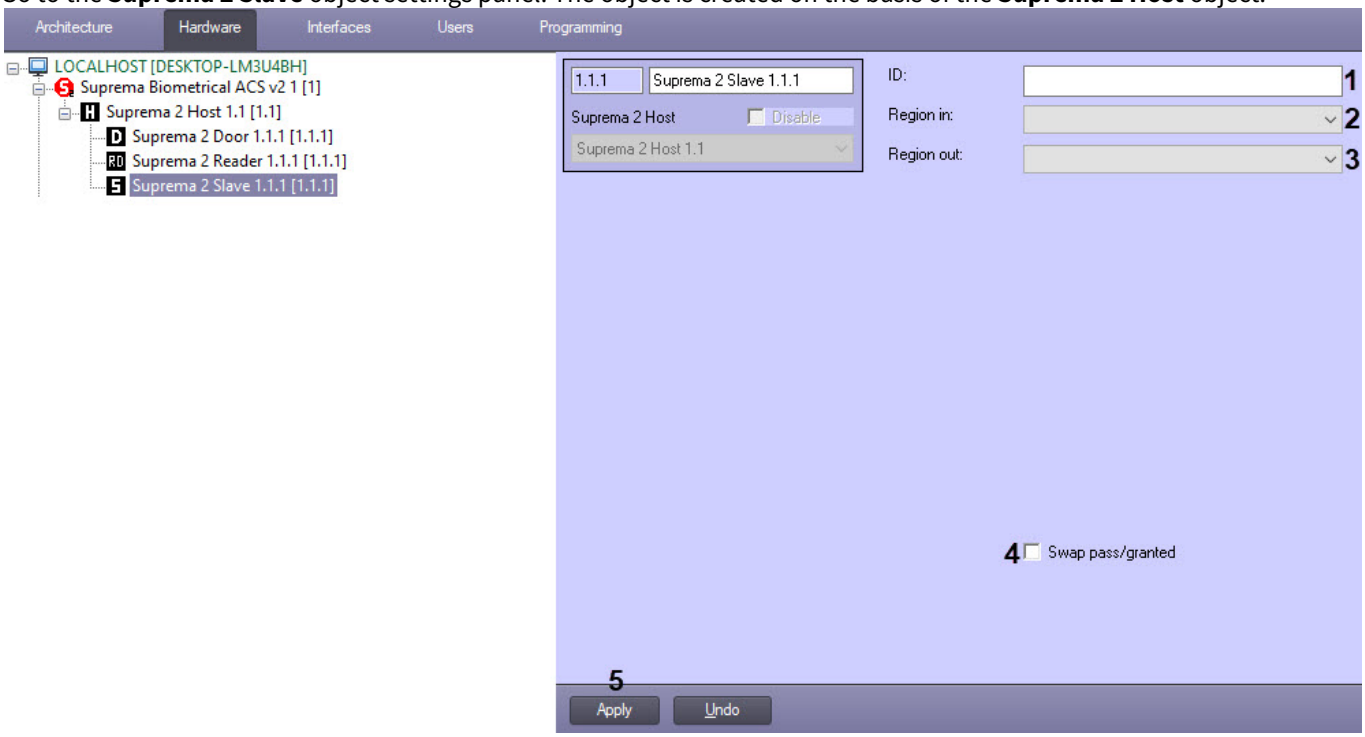
Configuring the *Suprema 2* reader is completed.

3.6 Configuring the Suprema 2 slave controller

One or several controllers can be connected to the *Suprema 2* controller. As a result, the Master-Slave mode is created, where the slave controller acts as a reader, and the Master controller makes the decision to grant access (for details, see the official reference documentation for the system by the Suprema Inc. manufacturer).

The *Suprema 2* slave controller is configured as follows:

1. Go to the **Suprema 2 Slave** object settings panel. The object is created on the basis of the **Suprema 2 Host** object.



2. In the **ID** (**1**) field, specify the identification number of the controller.
3. From the **Region in** (**2**) drop-down list, select the Region corresponding to the area where the user will be located after entering.
4. From the **Region out** (**3**) drop-down list, select the Region corresponding to the area where the user will be located after exiting.

> **Note**
>
> The **Region in** and **Region out** fields should be selected if *Time and Attendance* interface module is used. Otherwise, leave these fields empty.

5. Configure sending an event upon successful access: **Swap pass/granted** (**4**). If the checkbox is cleared, the **Pass** event is generated, otherwise, the **Access granted** event is generated.
6. Click the **Apply** (**5**) button to save changes.

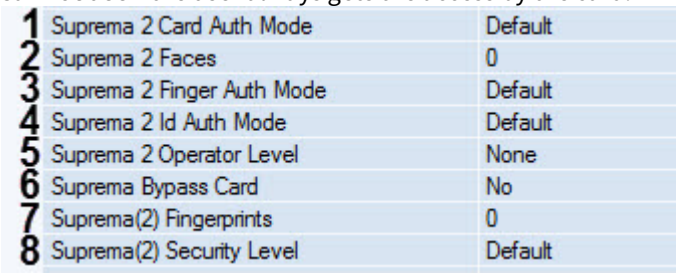
Configuring the *Suprema 2* slave controller is completed.

3.7 Setting up additional user parameters in Suprema 2 integration

> **Attention!**
>
> When you create an access level in the *Access Manager* module, select the **Suprema 2 Door** objects of the corresponding controllers as a required access point (see Working with access levels in the Access Manager software module). If you select **Suprema 2 Host** objects as an access point, this access level will not work.

Additional user parameters are configured in the *Access Manager* module (for details, see Access Manager Module Settings and Operation Guide). To do this, in the user editing mode, specify the following additional parameters:

1. **Suprema 2 Card Auth Mode** (**1**)—defines the system behavior logic:
   - **Default**—the default behavior set in the device settings.
   - **Only card**—the user can get the access only by the card.
   - **Card And Fingerprint**—the user can get the access if he first presents a card and then a fingerprint.
   - **Card and Pin**—the user can get the access if he first presents a card and then enters a PIN code.
   - **Fingerprint Or Pin After Card**—the user can get the access if he first presents a card and then either presents a fingerprint or enters a PIN code.
   - **Card And Fingerprint And Pin**—the user can get the access if he presents a card, then a fingerprint and then enters a PIN code in this exact sequence.
   - **Cannot use**—the user always gets the access by the card.



1	Suprema 2 Card Auth Mode	Default
2	Suprema 2 Faces	0
3	Suprema 2 Finger Auth Mode	Default
4	Suprema 2 Id Auth Mode	Default
5	Suprema 2 Operator Level	None
6	Suprema Bypass Card	No
7	Suprema(2) Fingerprints	0
8	Suprema(2) Security Level	Default

2. **Suprema 2 Faces** (**2**)—displays the number of face vectors assigned to the current user.
3. **Suprema 2 Finger Auth Mode** (**3**)—defines the authorization behavior logic using a fingerprint:
   - **Default**—the default behavior set in the device settings.
   - **Only Fingerprint**—the user can get the access only by presenting a fingerprint.
   - **Fingerprint And Pin**—the user can get the access if he first presents a fingerprint and then enters a PIN code.
   - **Cannot use**—the user always gets the access by presenting a fingerprint.
4. **Suprema 2 Id Auth Mode** (**4**)—defines the authorization behavior logic using the ID:
   - **Fingerprint After Id**—the user can get the access if he first enters his ID (not a PIN code!), and then presents a fingerprint.
   - **Pin After Id**—the user can get the access if he first enters his ID, and then the PIN code.
   - **Fingerprint Or Pin After Id**—the user can get the access if he first enters his ID, and then either presents a fingerprint or enters a PIN code.
   - **Fingerprint And Pin After Id**—the user can get the access if he first enters his ID, and then presents both a fingerprint and enters a PIN code.
   - **Cannot use**—the user always gets access by entering his ID.
5. **Suprema 2 Operator Level** (**5**)—defines access to the controller settings from its keyboard:
   - **None**—the default value. The user does not have the access to the settings.
   - **Admin**—the user has full access to the settings.
   - **System settings**—the user has the access to the system settings, but not to the user settings.
   - **User information**—a user has the read-only access to the user information, but cannot change anything.

> **Note**
>
> You can get the access to the controller settings by pressing the **Esc** button on the controller's keyboard. After you press **Esc**, the device requires you to present a fingerprint, a card, or ID.

> **Attention!**

There should be at least one administrator level user. Otherwise, this feature is disabled.

6. **Suprema Bypass Card** (**6**)—if this card is presented, the access will be granted and an alarm event will be generated. This card can be used by the user under duress.
7. **Suprema (2) Fingerprints** (**7**)—displays the number of fingerprints assigned to the current user.
8. **Suprema (2) Security level** (**8**)—determines the fingerprint quality level. For the proper configuration, refer to the official reference guide for this system.

Additional user parameters in *Suprema 2* integration are now configured.

4 Operation of Suprema 2 integration module

4.1 General information about Suprema 2 operation

The following interface objects are applied to work with the *Suprema 2* integration module:

1. **Map**.
2. **Event Viewer**.

For a detailed description of configuring these interface objects, refer to the Intellect Administrator's Guide.

For a detailed description of using these interface objects, refer to the Intellect Operator's Guide.

4.2 Managing Suprema 2 controller

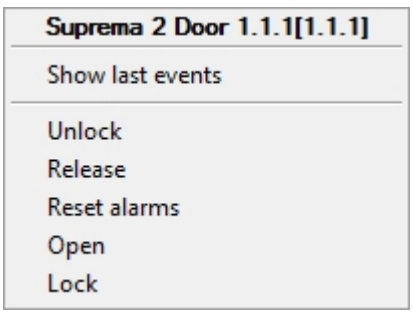
The *Suprema 2* controller is not managed in the **Map** interface window.

The following *Suprema 2* controller states are possible:

	Connected
	Connected but not synchronized
	Disconnected

4.3 Managing Suprema 2 Door object

The **Suprema 2 Door** object is managed in the **Map** interface window with the **Suprema 2 Door** object function menu.



Commands to manage **Suprema 2 Door** are given in the table.

Menu command	**Function**
Unlock	Unlock the door

Release	Standby mode
Reset alarms	Alarm reset by Operator
Open	Open the door
Lock	Lock the door

The following **Suprema 2 Door** object states are possible:

SUPREMA_2_DOOR 1.1.1[1.1.1] 	Locked
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Unlocked
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Connection lost
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Closed
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Opened
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Held open
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Alarm held open
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Alarm forced open

	Lock (scheduled)
	Lock (operator)
	Lock (emergency)
	Unlock (scheduled)
	Unlock (operator)
	Unlock (emergency)
	Alarm APB

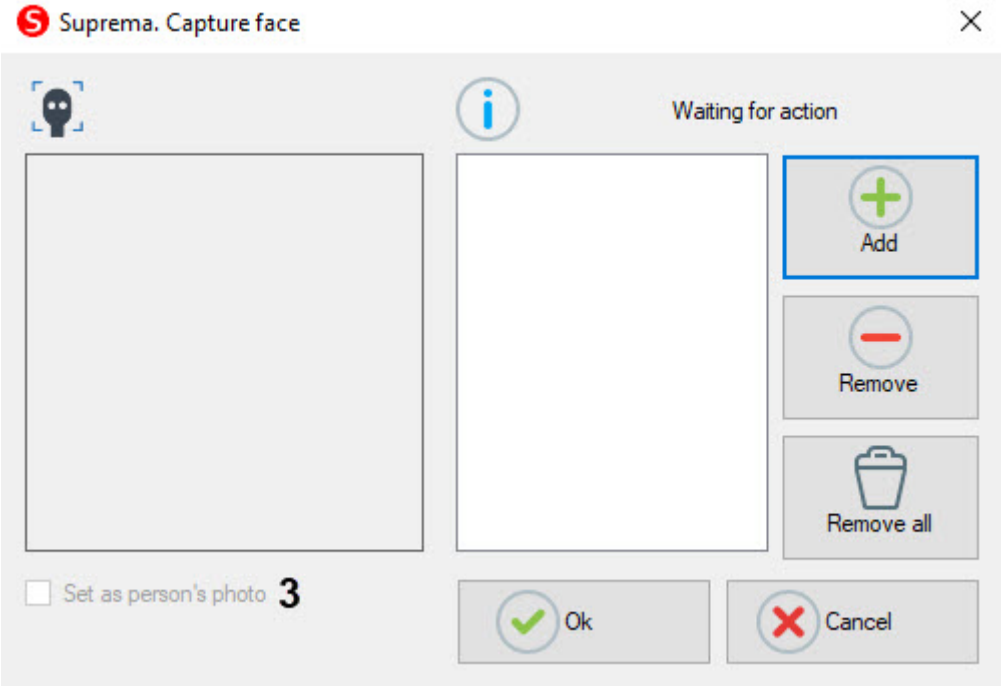
4.4 Adding the Suprema 2 biometric parameters

4.4.1 Adding the Suprema 2 face template

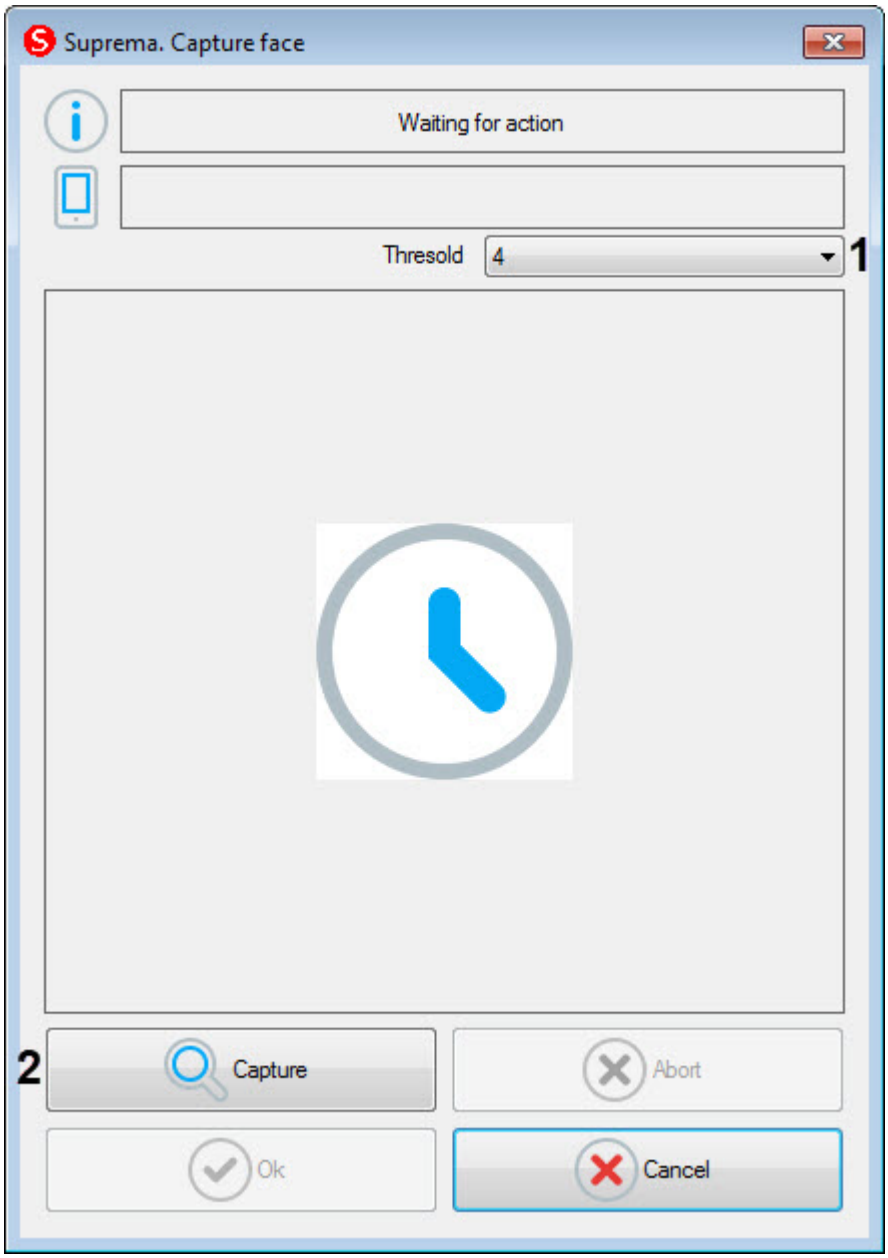
To add a *Suprema 2* face template in the *Access Manager* module, do the following:

1. Go to adding biometric data in the **Access Manager** window (see Adding biometric parameters).
2. Select the extension **(Edit Face) Suprema 2 Host** that corresponds to the controller with the biometric face reader connected to it, or to the terminal.

3. The **Suprema. Capture face** dialog box will open. To add a new face template, click the **Add** button.



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



4. From the **Threshold** drop-down list (**1**), select the sensitivity for capturing a face image: from **0** (low) to **8** (maximum).
5. To start capturing, click the **Capture** button (**2**) and then follow the instructions displayed at the top of the **Suprema. Capture face** window. In case of successful face capture, the resulting photo will be displayed, and the template of this photo will be saved.

> **Attention!**
>
> Arbitrary photos (from files, cameras) cannot be sent to the terminals. If there are many terminals, you can capture a face from any of them. Then this image will be sent to other terminals with different access attributes.

6. Set the **Set as person's photo** checkbox (**3**) to assign the face captured by the terminal as the user photo.
7. Click the **OK** button to complete adding a face template. Click the **Cancel** button to cancel the operation.
8. To delete a face template, select it in the list of templates and click the **Remove** button.

> **Note**
>
> To delete all face templates, click the **Remove all** button.

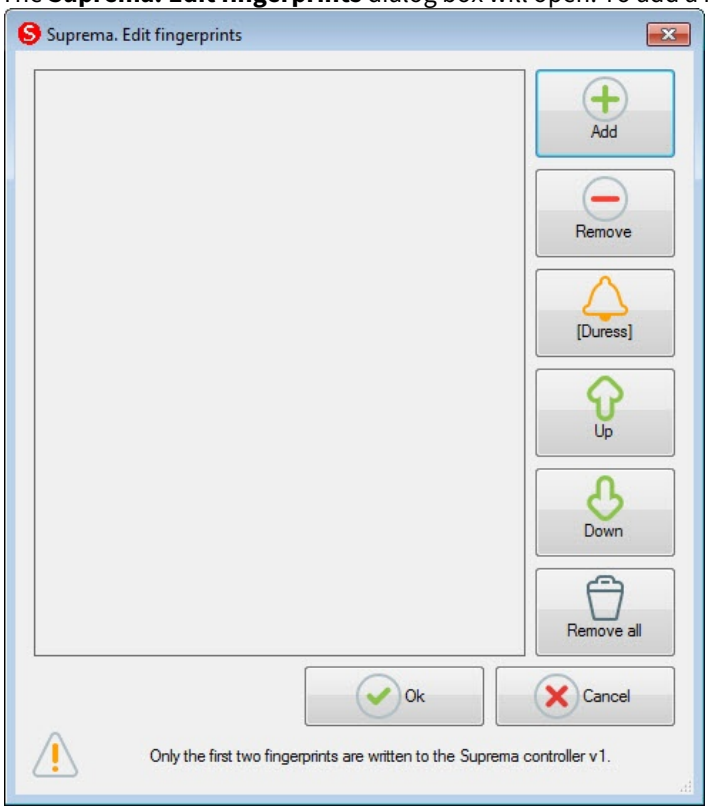
9. Click the **OK** button to save the face template.

Adding the *Suprema 2* face template in the *Access Manager* module is completed.

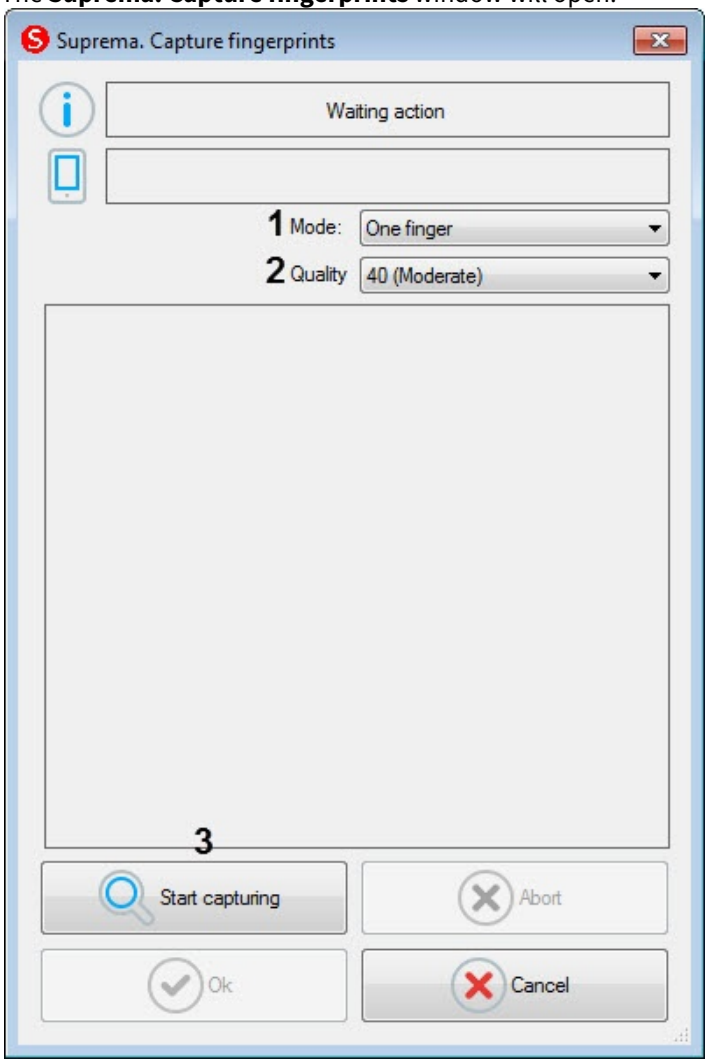
4.4.2 Adding the Suprema 2 fingerprints

To add *Suprema 2* fingerprints in the *Access Manager* module, do the following:

1. Go to adding biometric data in the *Access Manager* window (see Adding biometric parameters).
2. Select the **(Edit Fingerprints) Suprema 2 Host** extension that corresponds to the controller with the biometric fingerprint reader connected to it.
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.

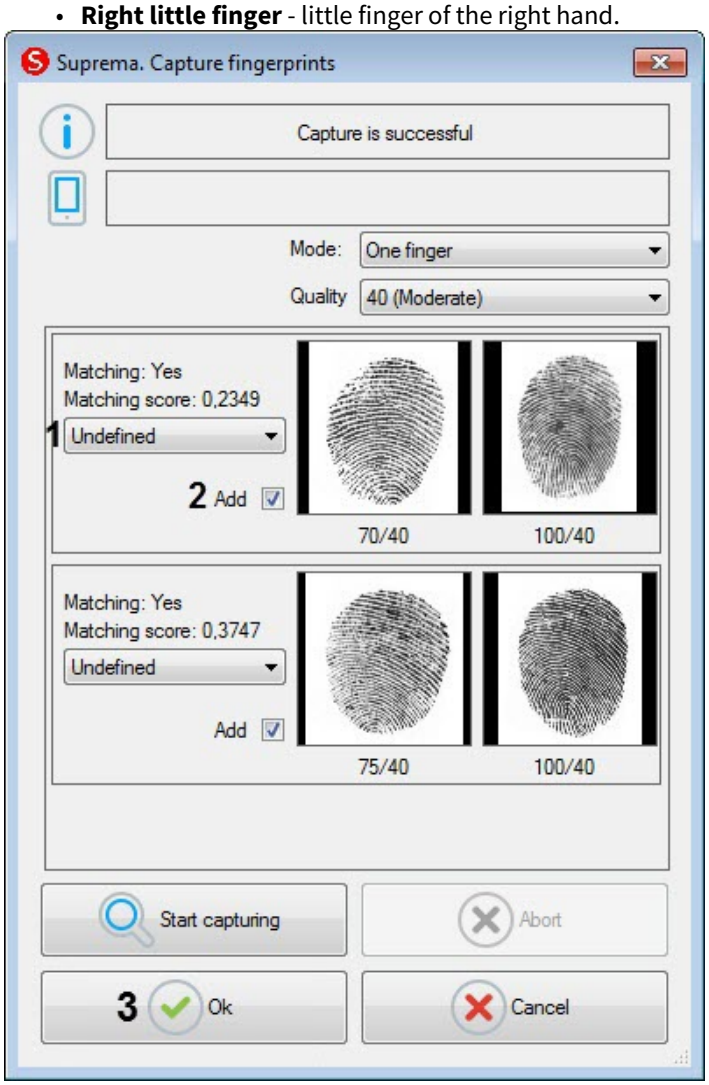


4. From the **Mode** drop-down list (**1**) select the fingerprint capture mode:
   - **One finger** - reading a single fingerprint.
   - **Two fingers** - reading two fingerprints.
   - **Two thumb fingers** - reading two thumb fingerprints.
   - **Left four fingers** - reading fingerprints of four 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.

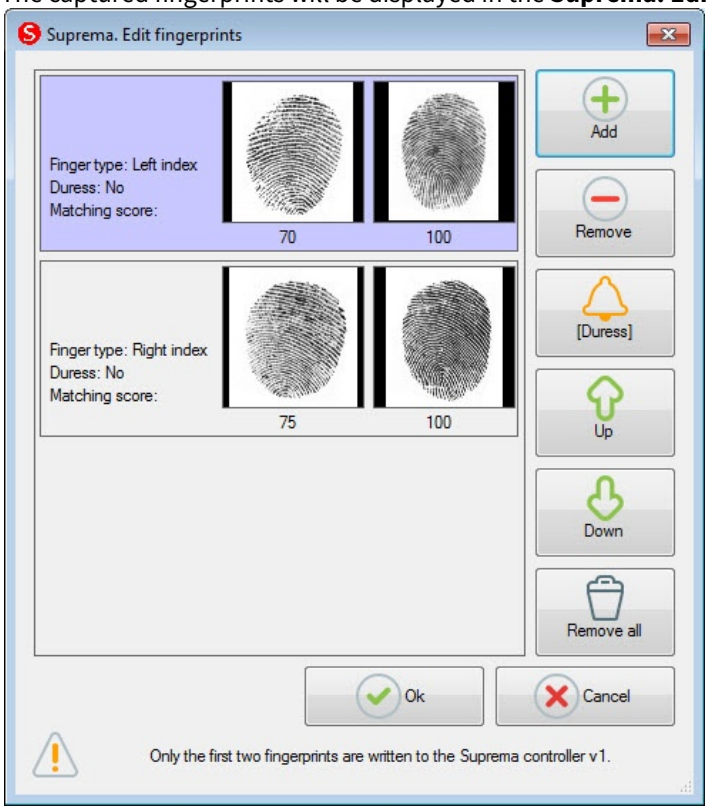
7. After the fingerprint capture is completed, select the type of scanned finger for each fingerprint in the drop-down list (**1**):

- **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.

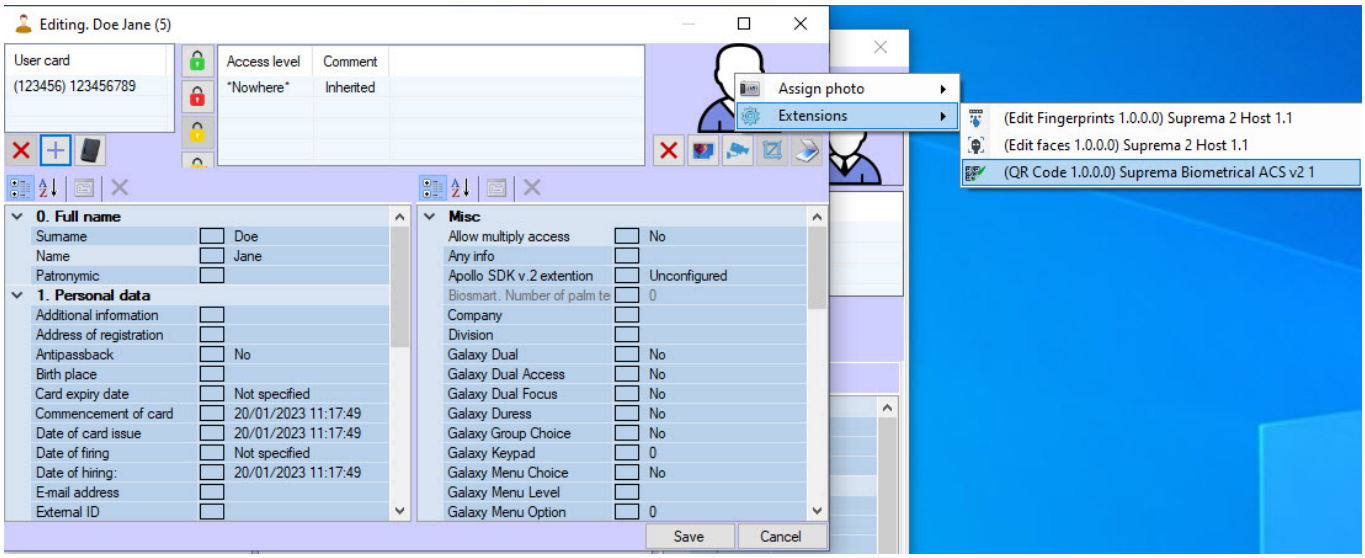
13. To move a fingerprint up or down in the list, select it and click the **Up** or **Down** button.
14. To finish entering fingerprints, click **OK**.

The *Suprema 2* fingerprints are added.

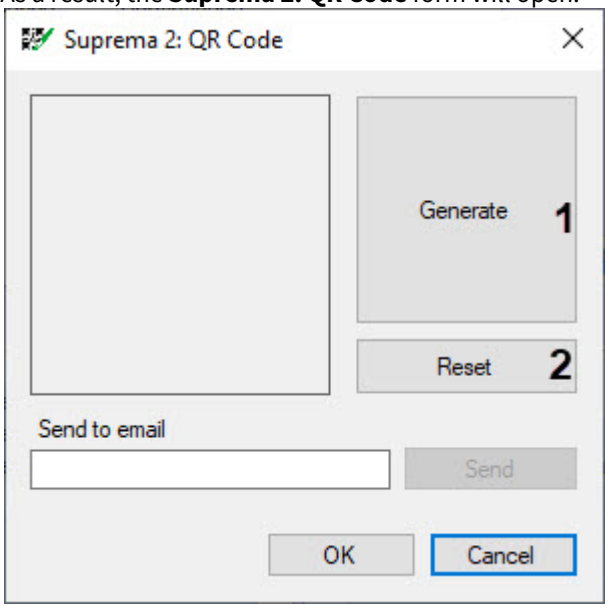
4.5 Working with QR codes

When you connect the X-Station 2 terminal, you can work with QR codes: generate a code, send it to the specified email address, and use it to pass through the terminal. For this, do the following:

1. Add the **Suprema Biometrical ACS v2** head object as a control reader (see Configuring control readers in the Access Manager).
2. Select the **(QR Code 1.0.0) Suprema Biometrical ACS v2** reader from the available **Extensions** buttons (see Adding biometric parameters).



As a result, the **Suprema 2: QR Code** form will open:



3. Click the **Generate** button (**1**) to generate a QR code. To cancel, click the **Reset** button (**2**).
4. In the **Send to email** field (**3**), enter the email address to which you want to send the QR code.

5. Click the **Send** button (**4**) to send the generated QR code to the email address specified in the previous step.
6. Click the **OK** button (**5**) to save the changes and return to the user editing form.
7. Click the **Save** button to save the QR code in the *Access Manager* in the user editing form.
   The QR code will be saved in the *Access Manager* and can be used by the user to pass through the terminal.