



Guide for configuring and working with the Suprema 2 integration module

ACFA PSIM 1.4

Last update 23/06/2025

Table of Contents

1	Introduction into the Guide for configuring and working with the Suprema 2 integration module	3
1.1	Purpose of the document	3
1.2	General information about the Suprema 2 integration module	3
2	Supported hardware and licensing of Suprema 2 integration module	4
3	Configuring Suprema 2 integration module.....	6
3.1	Activating Suprema 2 integration module.....	6
3.2	Configuring the Suprema 2 parent object	6
3.3	Configuring the Suprema 2 controller	7
3.4	Configuring the Suprema 2 scheduled lock/unlock zones	8
3.4.1	Configuring the scheduled lock/unlock zones	9
3.4.2	Features of adding holidays for the doors unlocking time zone	9
3.5	Configuring the Suprema 2 access point	10
3.6	Configuring the Suprema 2 reader	11
3.7	Configuring the Suprema 2 slave controller	12
3.8	Setting up additional user parameters in Suprema 2 integration.....	13
4	Operation of Suprema 2 integration module	17
4.1	General information about Suprema 2 operation.....	17
4.2	Managing Suprema 2 controller	17
4.3	Managing Suprema 2 Door object.....	17
4.4	Adding the Suprema 2 biometric parameters	20
4.4.1	Adding the Suprema 2 face template	20
4.4.2	Adding the Suprema 2 fingerprints	22
4.5	Working with QR codes	25

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

On the page:

- Purpose of the document
- General information about the Suprema 2 integration module

1.1 Purpose of the document

The *Guide for configuring and working with the Suprema 2 integration module* is a reference and information manual and is intended for configuration specialists and operators of the *Suprema 2* integration module. This module is a part of *Access Control* subsystem in *ACFA PSIM*.

The Guide has the following information:

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

1.2 General information about the Suprema 2 integration module

The *Suprema 2* integration module is the *ACFA PSIM*-based *ACS* component. The module is designed for *Suprema 2 ACS* interaction with *ACFA PSIM* (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)
BioStation 3	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.

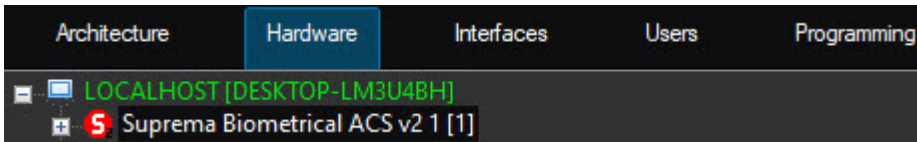
Module licensing

Per scanner/reader.

3 Configuring Suprema 2 integration module

3.1 Activating Suprema 2 integration module

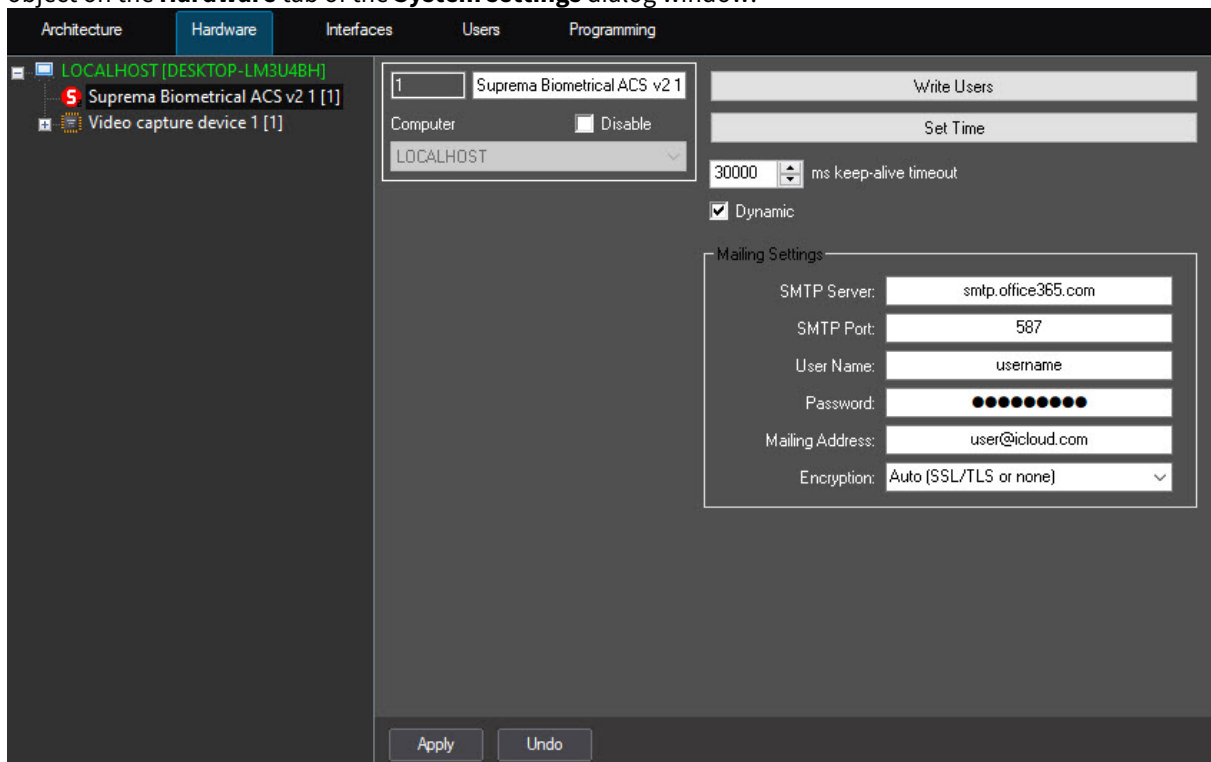
Create the **Suprema Biometrical ACS v2** object based on the **Computer** object in the **Hardware** tab of the **System settings** dialog box in order to activate *Suprema 2* integration module.



3.2 Configuring the Suprema 2 parent object

To configure the Suprema 2 parent 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 to write users to all controllers.
3. Click the **Set Time** button to synchronize the time of all controllers with the computer time.
4. Set the timeout in the **ms keep-alive timeout** field. The default value is **30000** ms.
5. Set the **Dynamic** checkbox for dynamic recording of the users access settings.
6. To email QR codes, set the following parameters:
 - a. In the **SMTP Server** field, enter the SMTP server address of the outgoing mail;
 - b. In the **SMTP Port** field, enter the port number used by the outgoing mail server;
 - c. In the **User Name** field, enter the name of the account used to send messages on the outgoing mail server;
 - d. In the **Password** field, enter the password of the account on the outgoing mail server;

- e. In the **Mailing Address** field, enter the email address from which the messages will be sent.
- f. From the **Encryption** drop-down list, select the type of encryption: **None**, **Auto (SSL/TLS or none)** (default), **SSL or TLS**, **STARTTLS**.

If you don't need to send QR codes, you can skip this step.

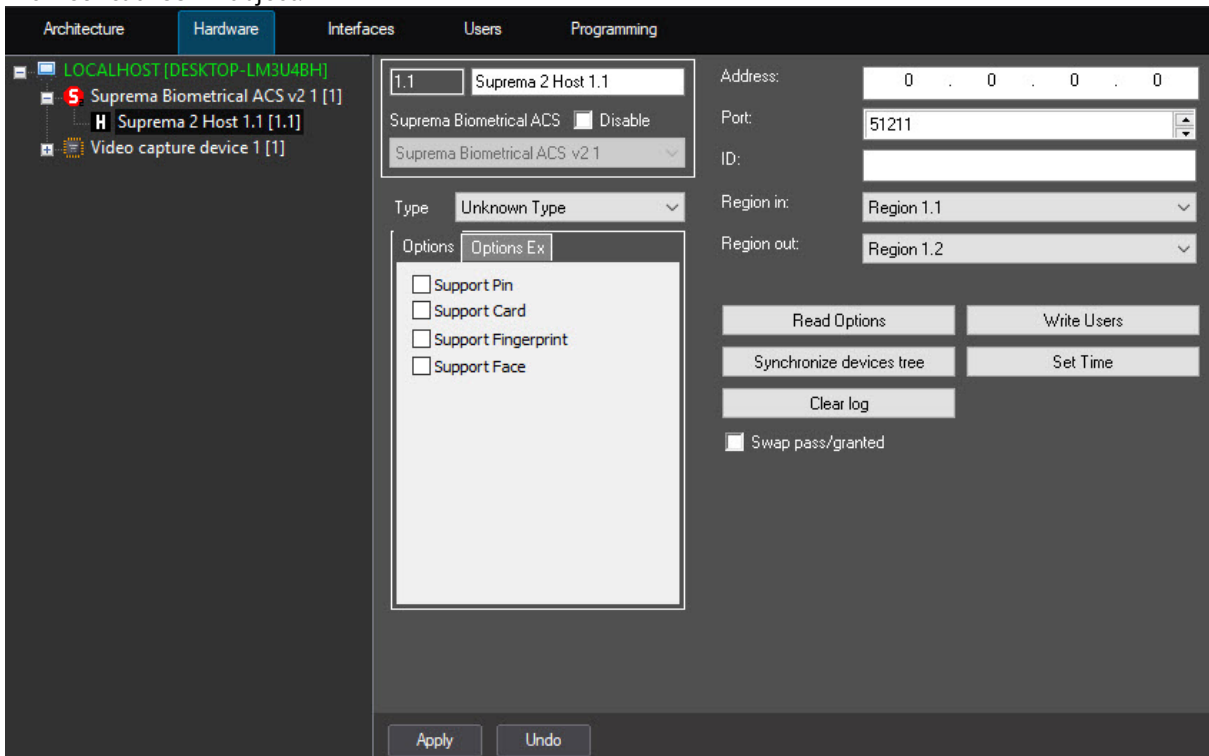
7. Click the **Apply** button to save the changes.

Configuration of the *Suprema 2* parent object is complete.

3.3 Configuring the Suprema 2 controller

The *Suprema 2* controller is configured as follows:

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



2. In the **Address** field, enter the IP address of the *Suprema 2* controller.
3. In the **Port** field, set the port of the *Suprema 2* controller.
4. In the **ID** field, specify the ID of the controller connected via Ethernet.
5. From the **Region in** drop-down list, select the Region corresponding to the area where the user will be located after entering.
6. From the **Region out** 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 must be selected if the *Time and Attendance* interface module is used. Otherwise, leave these fields empty.

7. Click the **Read Options** button to read the current options of the controller. The **Type** 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!

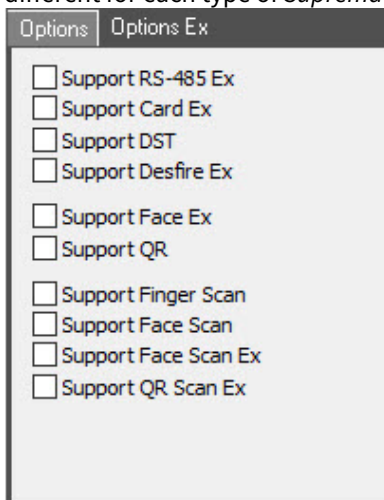
It is not recommended to change the **Type** setting manually.

8. Click the **Synchronize devices tree** button to automatically create a tree of devices connected to the controller in *ACFA PSIM*.
9. Click the **Clear log** button to clear the event log of the controller.
10. Click the **Write Users** button to write users to the controller.
11. Click the **Set Time** button to synchronize the controller time with the computer time.
12. Configure sending an event upon successful access: **Swap pass/granted**. 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.

13. When reading the options (step 7), the checkboxes are automatically set on the **Options** tab with the basic device features and on the **Options Ex** 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:



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

Configuring the *Suprema 2* controller is complete.

3.4 Configuring the Suprema 2 scheduled lock/unlock zones

On the page:

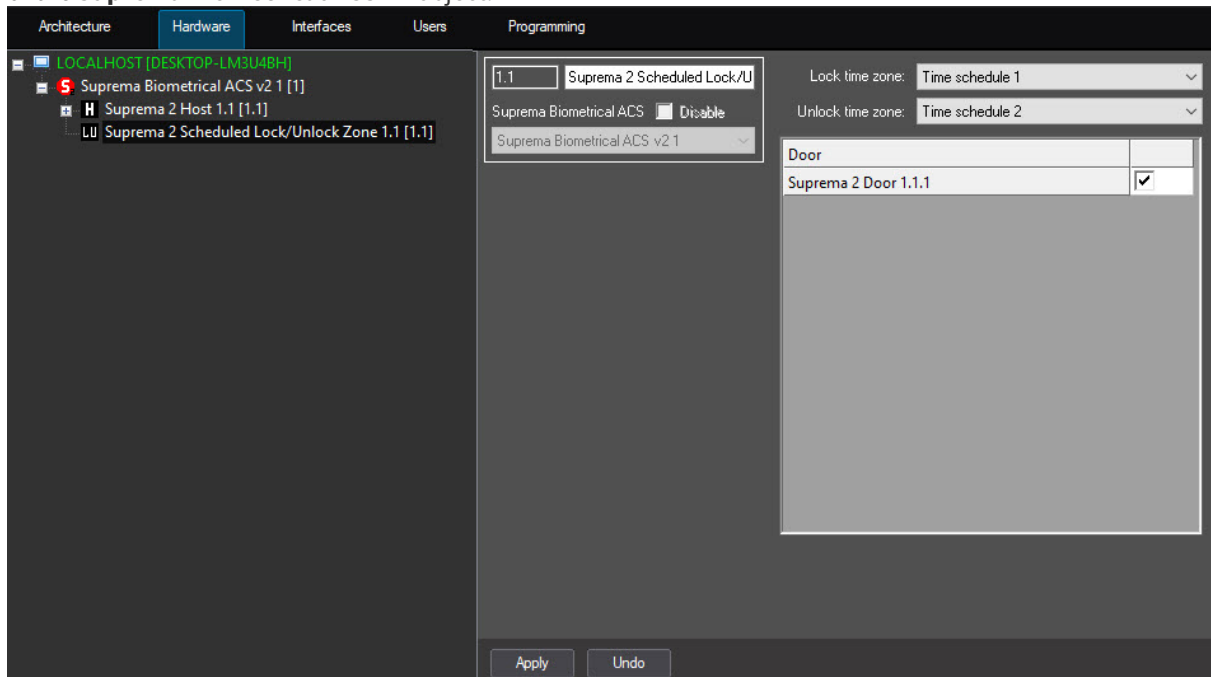
- [Configuring the scheduled lock/unlock zones](#)

- Features of adding holidays for the doors unlocking time zone

3.4.1 Configuring the scheduled lock/unlock zones

To configure the scheduled lock/unlock zones, do the following:

1. Go to the settings panel of the **Suprema 2 Scheduled Lock/Unlock Zone** object that is created on the basis of the **Suprema Biometrical ACS v2** object.



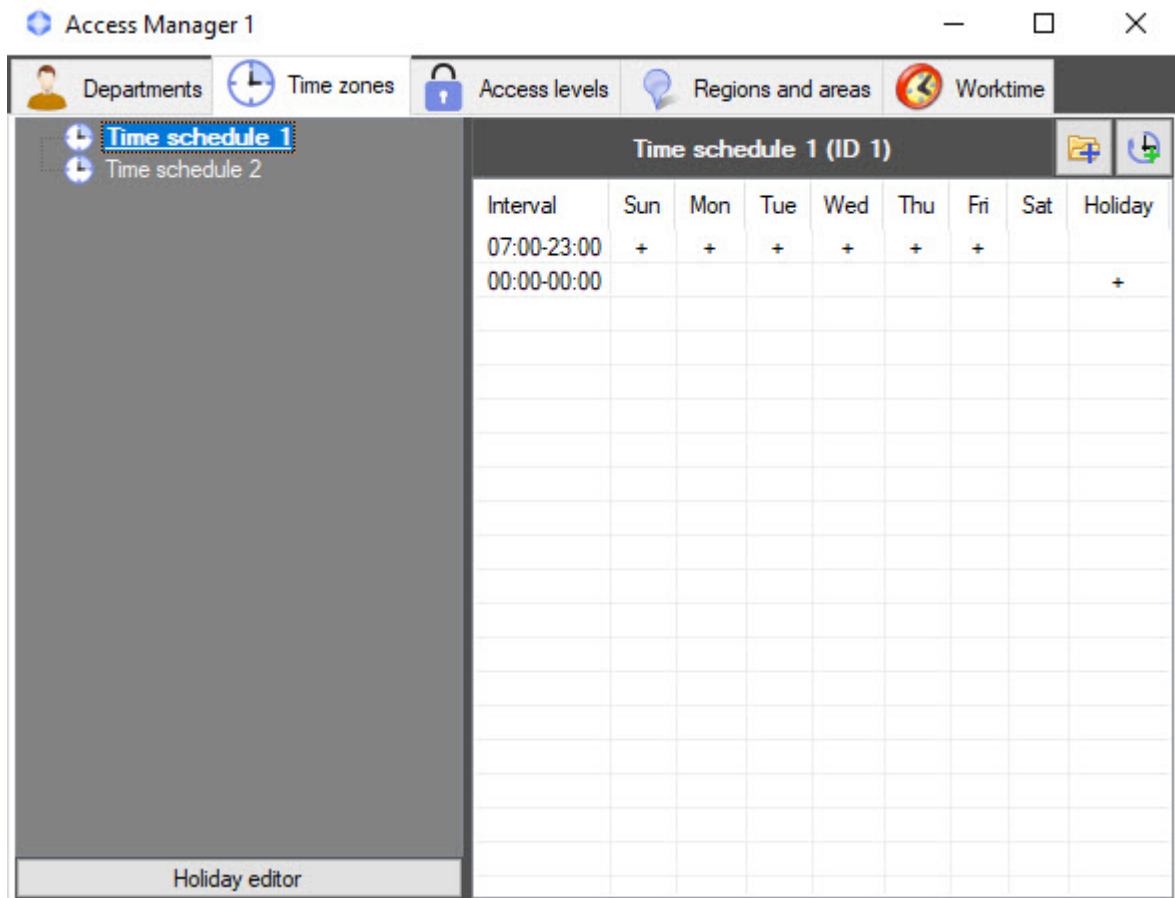
2. From the **Lock time zone** drop-down list, select the time schedule for locking the specified doors.
3. From the **Unlock time zone** drop-down list, select the time schedule for unlocking the specified doors.
4. Select the doors that you want to lock/unlock by the time schedule by setting the corresponding checkboxes.
5. Click the **Apply** button to save the changes.
6. Go to the settings panel of the **Suprema 2 Host** object.
7. Click the **Write Users** button to write users to the controller (see [Configuring the Suprema 2 controller](#)).

Configuring the scheduled lock/unlock zones is complete.

3.4.2 Features of adding holidays for the doors unlocking time zone

To add holidays to the doors unlocking time zone, do the following:

1. Create the time schedule with two intervals, the first of which is the main working one, and the second is an empty holiday interval, as follows:



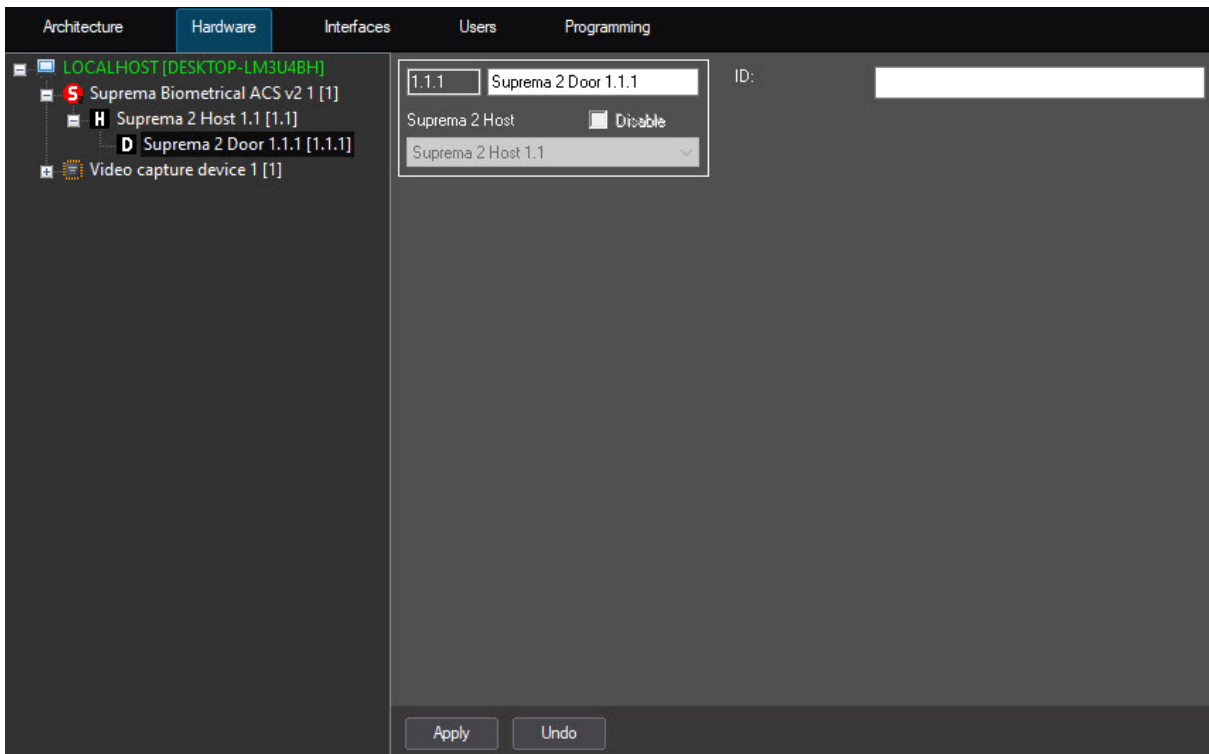
2. Add the created time schedule as the unlocking one (**Unlock time zone** parameter) on the settings panel of the **Suprema 2 Scheduled Lock/Unlock Zone** object, and leave the unlocking schedule blank. With this setting, the system doesn't unlock the door on that day if it is determined to be a holiday.

Adding a holiday to the doors unlocking time zone is complete.

3.5 Configuring the Suprema 2 access point

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

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



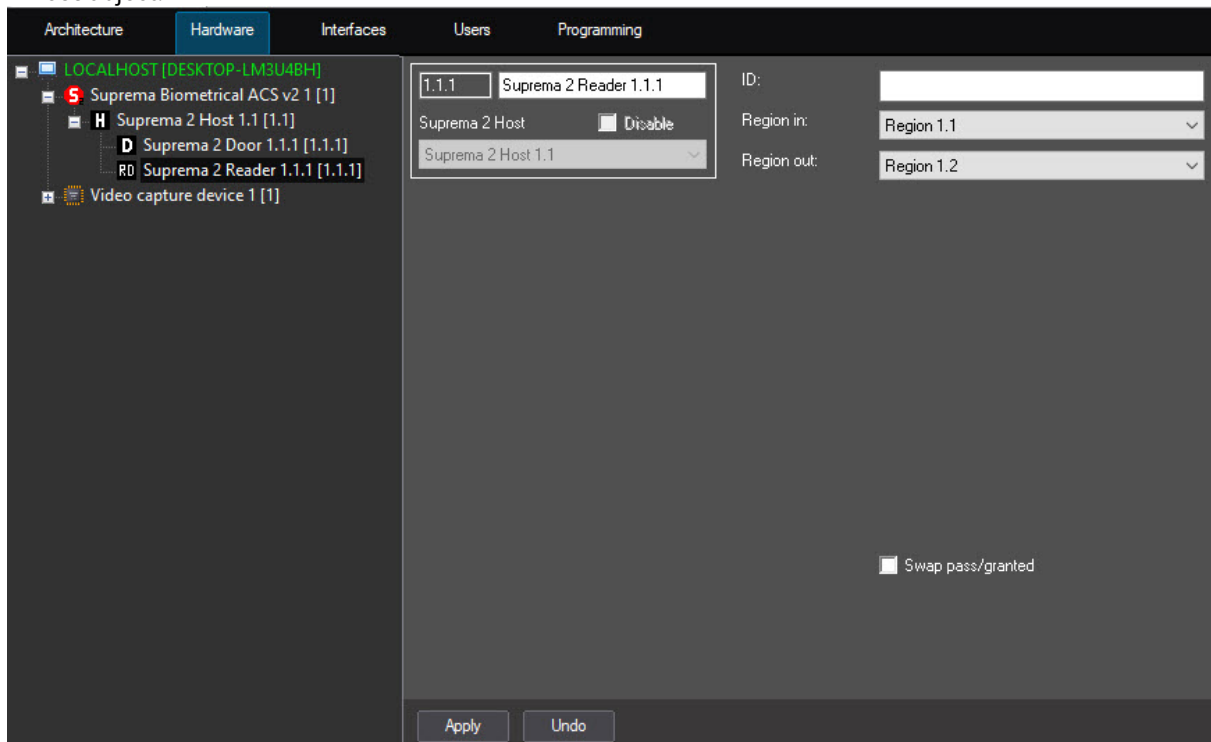
2. In the **ID** field, specify the identification number of the access point.
3. Click the **Apply** button to save changes.

Configuring the *Suprema 2* access point is complete.

3.6 Configuring the Suprema 2 reader

The *Suprema 2* reader is configured as follows:

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



2. In the **ID** field, specify the identification number of the reader.
3. From the **Region in** drop-down list, select the Region corresponding to the area where the user will be located after entering.
4. From the **Region out** 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 must be selected if the *Time and Attendance* interface module is used. Otherwise, leave these fields empty.

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

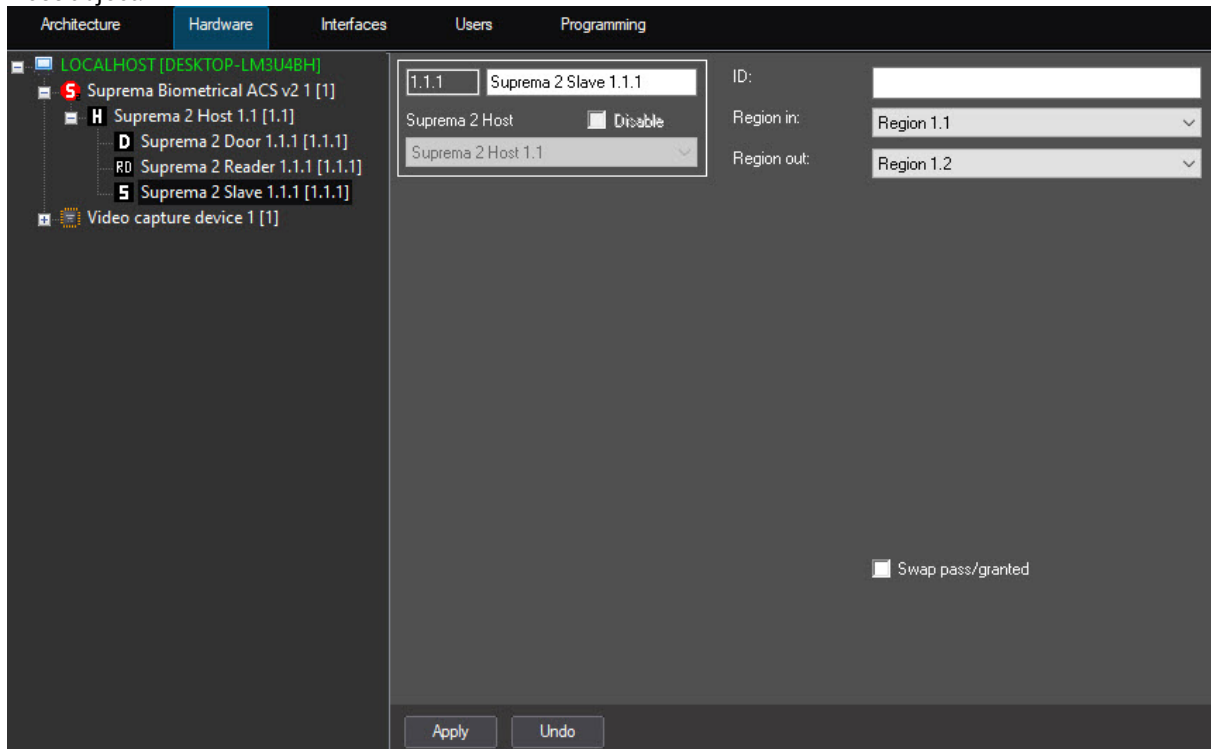
Configuring the *Suprema 2* reader is complete.

3.7 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, manufacturer is Suprema Inc.).

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

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



2. In the **ID** field, specify the identification number of the controller.
3. From the **Region in** drop-down list, select the Region corresponding to the area where the user will be located after entering.
4. From the **Region out** 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 must be selected if the *Time and Attendance* interface module is used. Otherwise, leave these fields empty.

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

Configuring the *Suprema 2* slave controller is complete.

3.8 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 [Guide for configuring and working with the Access Manager module](#)). To do this, in the user editing mode, specify the following additional parameters:

1. **Suprema 2 Card Auth Mode**—determines the system behavior logic:

- **Default**—the default behavior set in the device settings;
- **Only card**—the user can get access only by card;
- **Card And Fingerprint**—the user can get access if they first present a card and then a fingerprint;
- **Card and Pin**—the user can get access if they first presents a card and then enter a PIN code;
- **Fingerprint Or Pin After Card**—the user can get access if they first present a card and then either present a fingerprint or enter a PIN code;
- **Card And Fingerprint And Pin**—the user can get access if they present a card, then a fingerprint and then enter a PIN code in this exact sequence;
- **Cannot use**—the user always gets access by card.

Suprema 2 Card Auth Mode	<input type="checkbox"/>	Default
Suprema 2 Ex Card Auth Mode	<input type="checkbox"/>	Default
Suprema 2 Ex Face Auth Mode	<input type="checkbox"/>	Default
Suprema 2 Ex Finger Auth Mode	<input type="checkbox"/>	Default
Suprema 2 Ex Id Auth Mode	<input type="checkbox"/>	Default
Suprema 2 Faces	<input type="checkbox"/>	0
Suprema 2 Finger Auth Mode	<input type="checkbox"/>	Default
Suprema 2 Id Auth Mode	<input type="checkbox"/>	Default
Suprema 2 Operator Level	<input type="checkbox"/>	None
Suprema 2 QR Code	<input type="checkbox"/>	
Suprema Bypass Card	<input type="checkbox"/>	No
Suprema(2) Fingerprints	<input type="checkbox"/>	0
Suprema(2) Security Level	<input type="checkbox"/>	Default

2. **Suprema 2 Ex Card Auth Mode**—determines the logic of authorization by an access card:

- **Default**—the default behavior set in the device settings;
- **Card**—the user can get access by card;
- **Card → Face**—the user can get access if they first present a card and then pass a face check to match the stored photo;
- **Card → Fingerprint**—the user can get access if they first present a card and then a fingerprint;
- **Card → Pin**—the user can get access if they first presents a card and then enter a PIN code;
- **Card → Face or Fingerprint**—the user can get access if they first present a card and then pass a face check to match the stored photo or present a fingerprint;
- **Card → Face or Pin**—the user can get access if they first present a card and then pass a face check to match the stored photo or enter a PIN code;
- **Card → Fingerprint or Pin**—the user can get access if they first present a card and then a fingerprint or enter a PIN code;
- **Card → Face or Fingerprint or Pin**—the user can get access if they first present a card and then pass a face check to match the stored photo or present a fingerprint or enter a PIN code;
- **Card → FaceFingerprint**—the user can get access if they first present a card, then pass a face check to match the stored photo, and then present a fingerprint;
- **Card → Face → Pin**—the user can get access if they first present a card, then pass a face check to match the stored photo, and then enter a PIN code;
- **Card → Fingerprint → Face**—the user can get access if they first present a card and then a fingerprint, and after that pass a face check to match the stored photo;
- **Card → Fingerprint → Pin**—the user can get access if they first present a card and then a fingerprint, and after that enter a PIN code;
- **Card → Face or Fingerprint → Pin**—the user can get access if they first present a card, then pass a face check to match the stored photo or present a fingerprint, and then enter a PIN code;

- **Card → Face → Fingerprint or Pin**—the user can get access if they first present a card, then pass a face check to match the stored photo, then present a fingerprint or enter a PIN code;
 - **Cannot Use**—the user always gets access by card.
3. **Suprema 2 Ex Face Auth Mode**—determines the logic of authorization by checking a face to match the stored photo:
- **Default**—the default behavior set in the device settings;
 - **Face**—the user can get access if they pass a face check to match the stored photo;
 - **Face → Fingerprint**—the user can get access if they first pass a face check to match the stored photo and then present a fingerprint;
 - **Face → Pin**—the user can get access if they first pass a face check to match the stored photo, and then enter a PIN code;
 - **Face → Fingerprint or Pin**—the user can get access if they first pass a face check to match the stored photo, then present a fingerprint or enter a PIN code;
 - **Face → Fingerprint → Pin**—the user can get access if they first pass a face check to match the stored photo, then present a fingerprint, and after that enter a PIN code;
 - **Cannot Use**—the user always gets access if they pass a face check to match the stored photo.
4. **Suprema 2 Ex Finger Auth Mode**—determines the logic of authorization by fingerprint:
- **Default**—the default behavior set in the device settings;
 - **Fingerprint**—the user can get access by fingerprint;
 - **Fingerprint → Face**—the user can get access if they first present a fingerprint, and after that pass a face check to match the stored photo;
 - **Fingerprint → Pin**—the user can get access if they first present a fingerprint, and then enter a PIN code;
 - **Fingerprint → Face or Pin**—the user can get access if they first present a fingerprint, then pass a face check to match the stored photo or enter a PIN code;
 - **Fingerprint → Face → Pin**—the user can get access if they first present a fingerprint, then pass a face check to match the stored photo, and after that enter a PIN code;
 - **Cannot Use**—the user always gets access by fingerprint.
5. **Suprema 2 Ex Id Auth Mode**—determines the logic of authorization by a unique user identifier (id):
- **Default**—the default behavior set in the device settings;
 - **Id → Face**—the user can get access if they first enter their id and then pass a face check to match the stored photo;
 - **Id → Fingerprint**—the user can get access if they first enter their id and then present a fingerprint;
 - **Id → Pin**—the user can get access if they first enter their id and then enter a PIN code;
 - **Id → Face or Fingerprint**—the user can get access if they first enter their id and then pass a face check to match the stored photo or present a fingerprint;
 - **Id → Face or Pin**—the user can get access if they first enter their id, and then pass a face check to match the stored photo or enter a PIN code;
 - **Id → Fingerprint or Pin**—the user can get access if they first enter their id, and then present a fingerprint or enter a PIN code;
 - **Id → Face or Fingerprint or Pin**—the user can get access if they first enter their id, and then pass a face check to match the stored photo, or present a fingerprint or enter a PIN code;
 - **Id → Face → Fingerprint**—the user can get access if they first enter their id, and then pass a face check to match the stored photo, and after that present a fingerprint;
 - **Id → Face → Pin**—the user can get access if they first enter their id, and then pass a face check to match the stored photo, and then enter a PIN code;
 - **Id → Fingerprint → Face**—the user can get access if they first enter their id, then present a fingerprint, and after that pass a face check to match the stored photo;
 - **Id → Fingerprint → Pin**—the user can get access if they first enter their id, then present a fingerprint, and after that enter a PIN code;
 - **Id → Face or Fingerprint → Pin**—the user can get access if they first enter their id, then pass a face check to match the stored photo or present a fingerprint, and after that enter a PIN code;

- **Id → Face → Fingerprint or Pin**—the user can get access if they first enter their id, then pass a face check to match the stored photo, and after that present a fingerprint or enter a PIN code;
 - **Id → Fingerprint → Face or Pin**—the user can get access if they first enter their id, then present a fingerprint, and after that pass a face check to match the stored photo or enter a PIN code;
 - **Cannot Use**—the user always gets access by id.
6. **Suprema 2 Faces**—displays the number of face vectors assigned to the current user.
 7. **Suprema 2 Finger Auth Mode**—determines the logic of authorization by fingerprint:
 - **Default**—the default behavior set in the device settings;
 - **Only Fingerprint**—the user can get access only by presenting a fingerprint;
 - **Fingerprint And Pin**—the user can get access if they first present a fingerprint and then enter a PIN code;
 - **Cannot use**—the user always gets access by fingerprint.
 8. **Suprema 2 Id Auth Mode**—determines the logic of authorization by id:
 - **Default**—the default behavior set in the device settings;
 - **Fingerprint After Id**—the user can get access if they first enter their id, and then presents a fingerprint;
 - **Pin After Id**—the user can get access if they first enter their id, and then enter a PIN code;
 - **Fingerprint Or Pin After Id**—the user can get access if they first enter their id, and then present a fingerprint or enter a PIN code;
 - **Fingerprint And Pin After Id**—the user can get access if they first enter their id, and then present a fingerprint and enter a PIN code;
 - **Cannot use**—the user always gets access by id.
 9. **Suprema 2 Operator Level**—determines access to the controller settings from its keyboard:
 - **None**—the default value. The user doesn't have access to the settings;
 - **Admin**—the user has full access to the settings;
 - **System settings**—the user has access to the system settings, but not to the user settings;
 - **User information**—the 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 that, the device requires you to present a fingerprint, a card, or id.

 **Attention!**

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

10. **Suprema QR Code** contains the value of the QR code assigned to the user.
11. **Suprema Bypass Card**—if this card is presented, access will be granted and an alarm event will be generated. This card can be used by the user under duress.
12. **Suprema(2) Fingerprints**—displays the number of fingerprints assigned to the current user.
13. **Suprema(2) Security Level**—determines the quality level of the fingerprints. 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 [Axxon PSIM Administrator's Guide](#).

For a detailed description of using these interface objects, refer to the [Axxon PSIM 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:

SUPREMA_2_HOST 1.1[1.1] 	Connected
SUPREMA_2_HOST 1.1[1.1] 	Connected but not synchronized
SUPREMA_2_HOST 1.1[1.1] 	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.



Suprema 2 Door 1.1.1[1.1.1]
Show last events
Unlock
Release
Reset alarms
Open
Lock

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

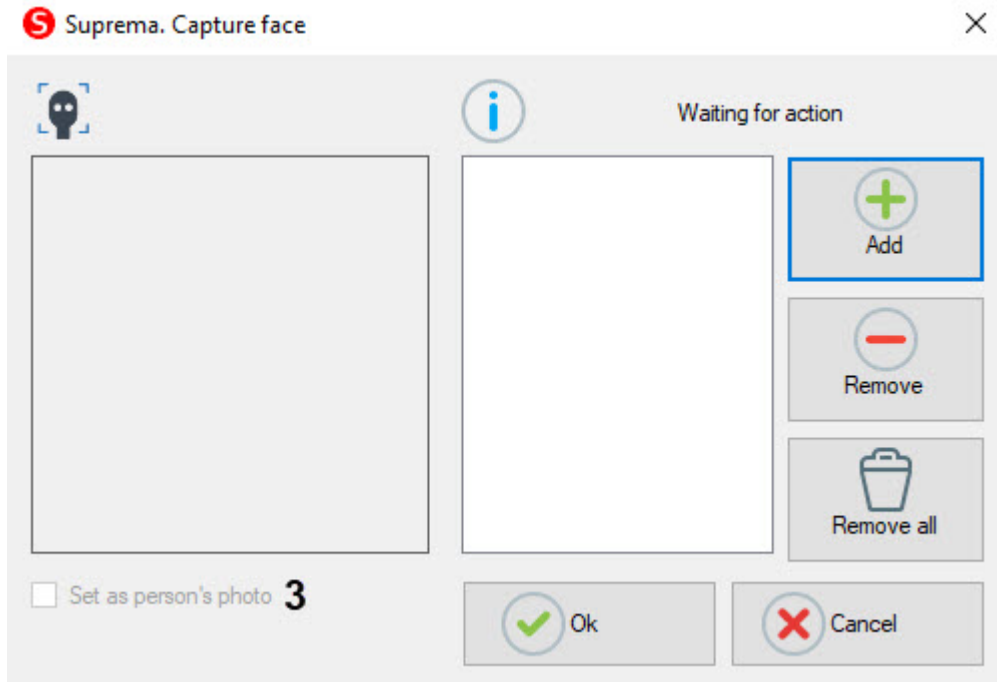
<p>SUPREMA_2_DOOR 1.1.1[1.1.1]</p> 	<p>Alarm held open</p>
<p>SUPREMA_2_DOOR 1.1.1[1.1.1]</p> 	<p>Alarm forced open</p>
<p>SUPREMA_2_DOOR 1.1.1[1.1.1]</p> 	<p>Lock (scheduled)</p>
<p>SUPREMA_2_DOOR 1.1.1[1.1.1]</p> 	<p>Lock (operator)</p>
<p>SUPREMA_2_DOOR 1.1.1[1.1.1]</p> 	<p>Lock (emergency)</p>
<p>SUPREMA_2_DOOR 1.1.1[1.1.1]</p> 	<p>Unlock (scheduled)</p>
<p>SUPREMA_2_DOOR 1.1.1[1.1.1]</p> 	<p>Unlock (operator)</p>
<p>SUPREMA_2_DOOR 1.1.1[1.1.1]</p> 	<p>Unlock (emergency)</p>
<p>SUPREMA_2_DOOR 1.1.1[1.1.1]</p> 	<p>Alarm APB</p>

4.4 Adding the Suprema 2 biometric parameters

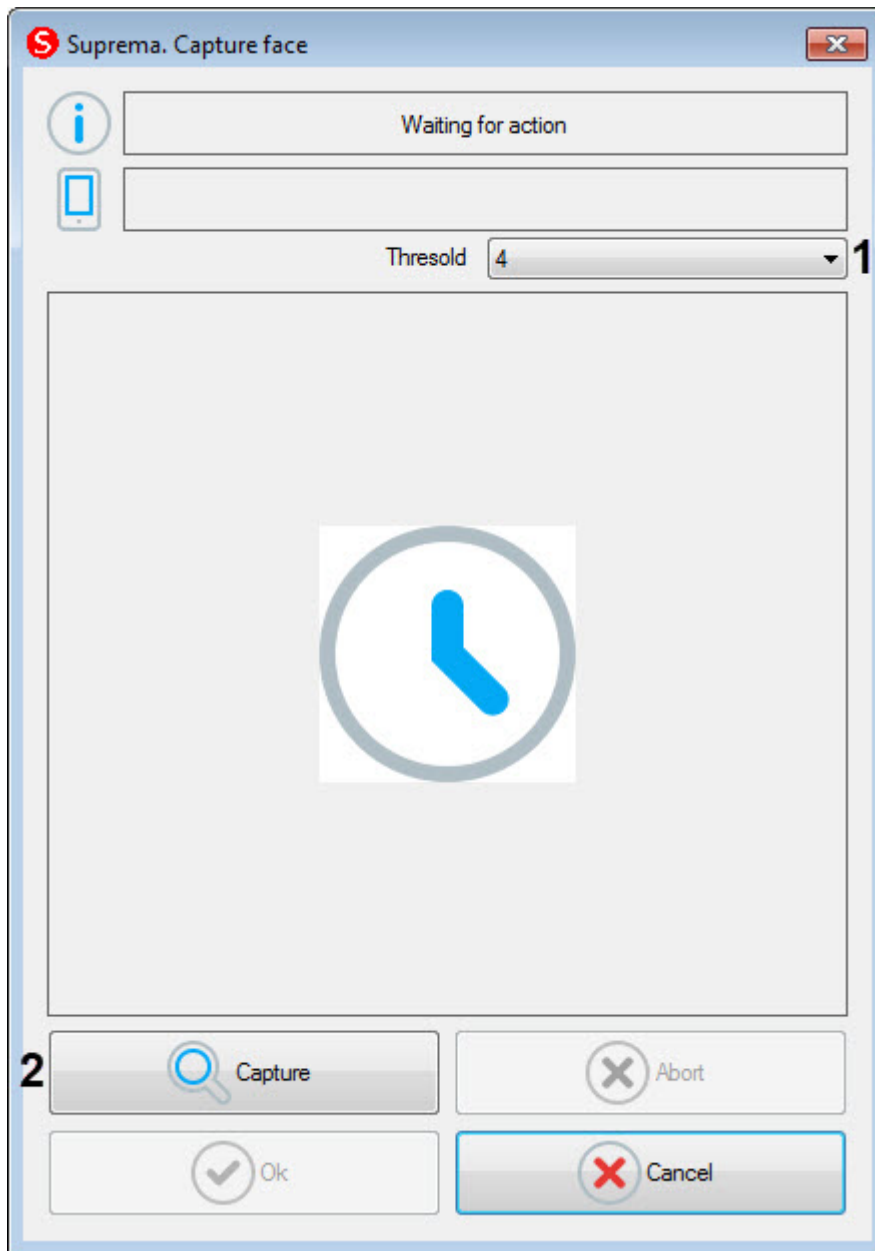
4.4.1 Adding the Suprema 2 face template

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.

- 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.

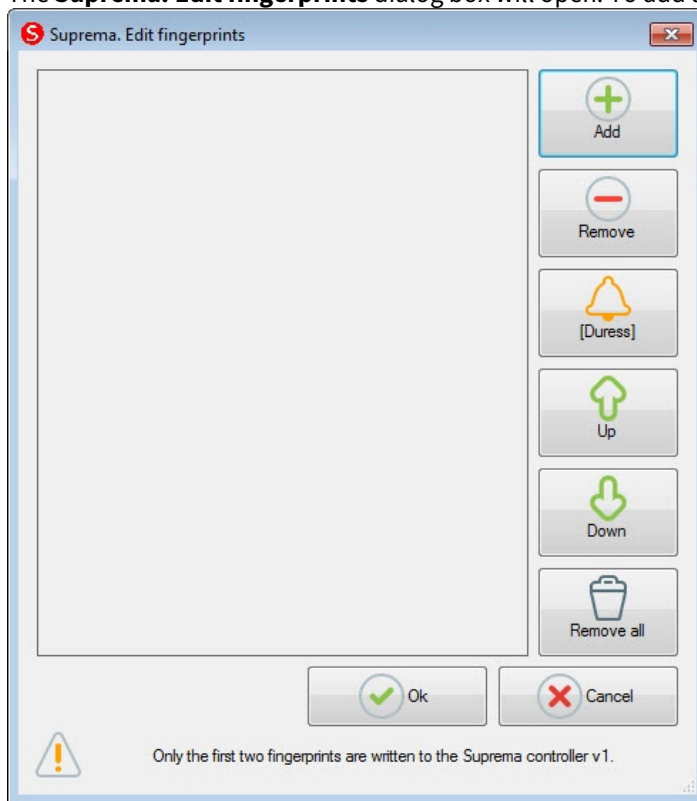
- Click the **OK** button to save the face template.

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

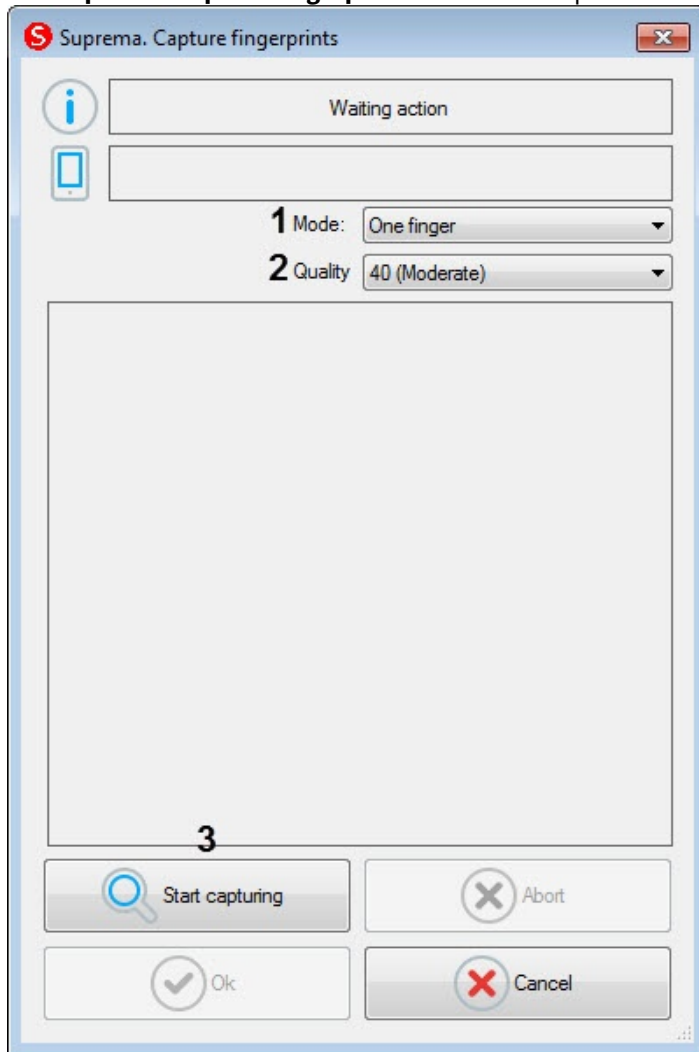
4.4.2 Adding the Suprema 2 fingerprints

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

- Go to adding biometric data in the *Access Manager* window (see [Adding biometric parameters](#)).
- Select the **(Edit Fingerprints) Suprema 2 Host** extension that corresponds to the controller with the biometric fingerprint reader connected to it.
- The **Suprema. Edit fingerprints** dialog box will open. To add a new fingerprint, click the **Add** button.



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

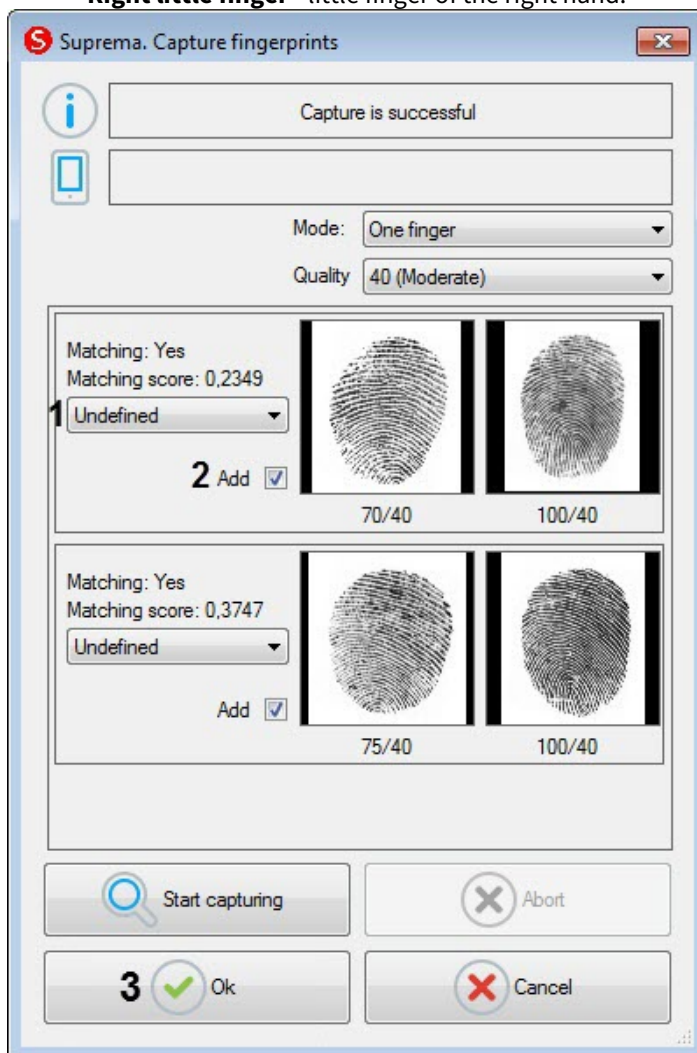


4. From the **Mode** drop-down list (1) select the fingerprint capture mode:
 - **One finger** - reading a single fingerprint.
 - **Two fingers** - reading two fingerprints.
 - **Two thumb fingers** - reading two thumb fingerprints.
 - **Left four fingers** - reading fingerprints of four fingers of the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

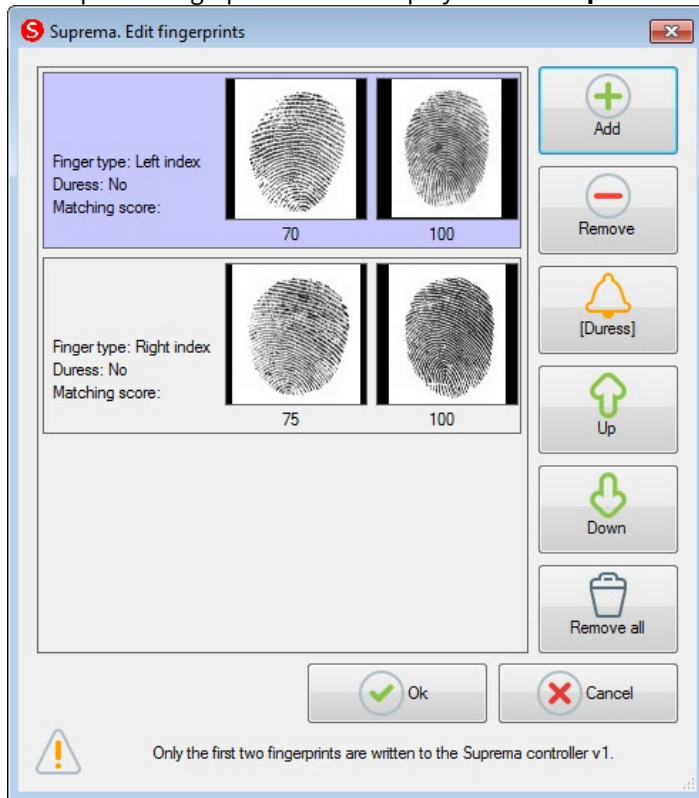
To capture fingerprints, each finger or group of fingers should be placed on the reader twice with 5 seconds delay after pressing the **Start capturing** button and after the first capture.

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.

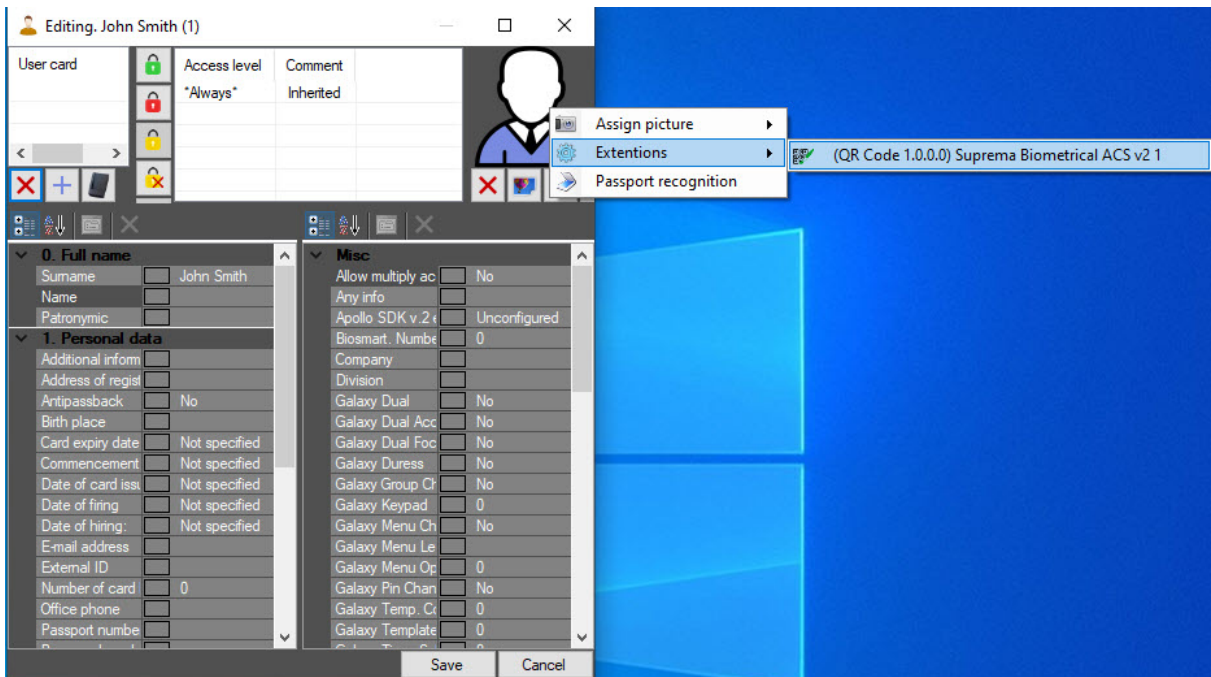
13. To move a fingerprint up or down in the list, select it and click the **Up** or **Down** button.
14. To finish entering fingerprints, click **OK**.

The *Suprema 2* fingerprints are added.

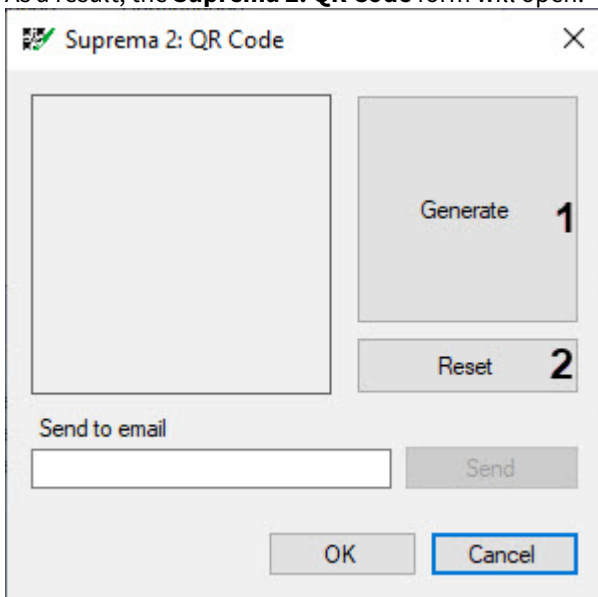
4.5 Working with QR codes

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.