ACFA Intellect

Suprema 2 Settings Guide

Last update 28/01/2022

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* software package.

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. It is designed for *Suprema 2* ACS monitoring and control in *ACFA Intellect* software.

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 Server (to download it, go to the manufacturer's web site)
4. Configure *Suprema 2* ACS connection with the *BioStar 2* server (configuration of *BioStar 2* is described in the official documentation for it).

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
Equipment connection	Ethernet

Supported equipment

Equipment	Function	Features
BioStation A2 (BSA2-OEPW)	Biometric terminal (scanner)	• 1 GHz 4-core CPU • 8 GB flash, 1 GB RAM • Built-in 2 MP camera, face detection + video intercom • Standards of proximity cards: RFID (125 kHz EM) • Number of templates: 1,000,000 templates, 1:1 verification, 1:N identification • Number of users: 500,000 users, 1:1 verification; 100,000 users, 1: N identification • Event memory capacity: 5,000,000 events (50,000 with image) • I/O ports Wiegand, TCP/IP, Wi-Fi, USB, TTL I/O, RS 485, SD-Card, PoE
FaceStation 2	Biometric terminal (scanner)	• 1.4GHz Quad Core CPU • 1 GB RAM + 8 GB Flash • Built-in camera, face detection, photo saving in event log, video intercom • Standards of proximity cards: FS2-D: 125kHz EM & 13.56MHz Mifare, Mifare Plus, Desfire/EV1, FeliCa, NFC, FS2- AWB: 125kHz EM, HID Prox & 13.56 MHz Mifare, Mifare Plus, Desfire/EV1, FeliCa, iCLASS SE/ SR, NFC, BLE • Number of templates: 900,000 (1:1), 90,000 (1:N) • Number of users: 30,000 • Events memory capacity 5,000,000 / 50,000 wit photo Interfaces TCP/IP, Wiegand, 1-channel RS485 (Host or Slave), 2 TTL inputs, 1 output, USB 2.0 Host
BioStation 2	Biometric terminal (scanner)	• 1 GHz CPU • 128 MB RAM + 8 GB Flash • Camera, face recognition + video intercom • Standards of proximity cards: 125KHz EM, 125KHz HID Prox, 13.56MHz Mifare/DesFire/DesFire EV1/ Felica/NFC, 13.56MHz iClass SE • Number of templates: 1,000,000 (1:1), 40,000 (1:N) • Number of users: 500,000 (1:1), 20,000 (1:N)

		• Events memory capacity: 3,000,000 (text) • Enclosure rating IP65 • Interfaces TCP/IP, Wiegand, RS485, RS232, TTL I/O, Wi-Fi, output
BioEntry W2	Biometric terminal (scanner)	• 533 MHz DSP CPU • 8 MB RAM + 8 MB Flash • Standards of proximity cards: (EM), HID Prox, Mifare/DesFire, iClass SE • Recognition rate in the identification mode (1:N) 1:2,000 templates per second • Number of templates: 10,000 (1:1), 10,000 (1:N) • Number of users: 5,000 (1:1), 5,000 (1:N) • Events memory capacity: 50,000 • I/O ports: TCP/IP, Wiegand, RS485, RS232, TTL I/O, output, PoE
CoreStation	Controller	• 1.4 GHz Octa Core CPU • 8 GB Flash + 1 GB RAM • Number of templates: 500,000 (1:1), 100,000 (1:N) • Events memory capacity: 5,000,000 (text) • Interfaces: Ethernet, RS-485, Wiegand • Number of Relays: 4 • Max. Slave Devices (RS-485): 64 devices (Max. 31 devices per port) • Max. Wiegand Devices: 132 devices (with DM-20) • Number of supervised Inputs: 8 (TTL input selectable) • Number of TTL Outputs: 8 • Number of AUX Inputs: 2
BioEntry P2	Biometric device (scanner)	• 1 GHz CPU • 2 GB Flash + 64 MB RAM • Supported card formats: BEP2-OD: 125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, NFC BEP2-OA**:** 125kHz EM, HID Prox & 13.56MHz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, iCLASS SE/SR, iCLASS SEOS, NFC • Maximum number of users: 10,000 (1:1) 10,000 (1:N) • Maximum number of templates: 20,000 (1:1) 20,000 (1:N) * Two templates per each fingerprint • Number of events (text): 1,000,000 • Connection interfaces: Ethernet (10/100 Mbps, auto MDI/MDI-X) RS-485 (1 Host or Slave channel) Wiegand (1 input or 1 output) TTL (2 inputs) Relay (1 relay)
XPass 2	Reader	• CPU: 1 GHz

		• Memory: 4 GB Flash + 64 MB RAM • RF Option: 125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa • Mobile Card: NFC, BLE • Maximum number of users: 200,000 • Text Log: 1,000,000 • Connection interfaces: Ethernet 10/100 Mbps, auto MDI / MDI-X, RS485 (OSDP support, 1 channel Master or Slave), Wiegand (input or output), relay

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

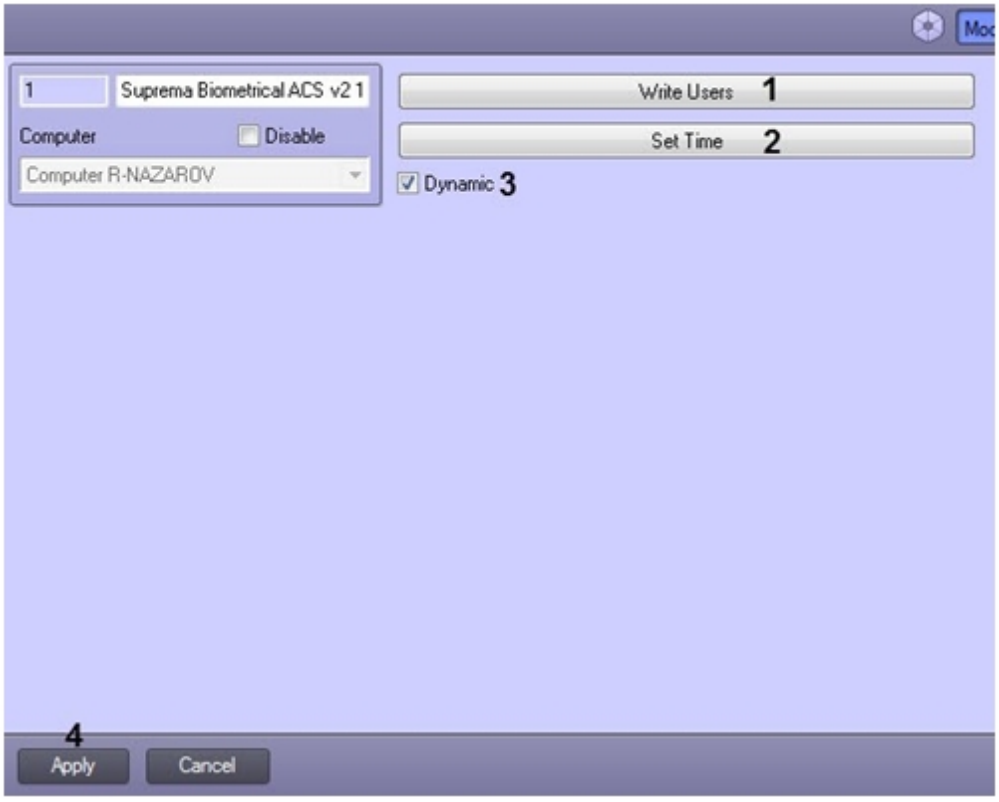
3.1 Activating Suprema 2 integration module

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 Writing users and time synchronization in Suprema 2

To send the users to all connected controllers, click the **Write Users** (**1**) button on the **Suprema Biometrical ACS v2** object settings panel.

To synchronize all controllers' time with the Server time, click the **Set Time** (**2**) button on the **Suprema Biometrical ACS v2** object settings panel.



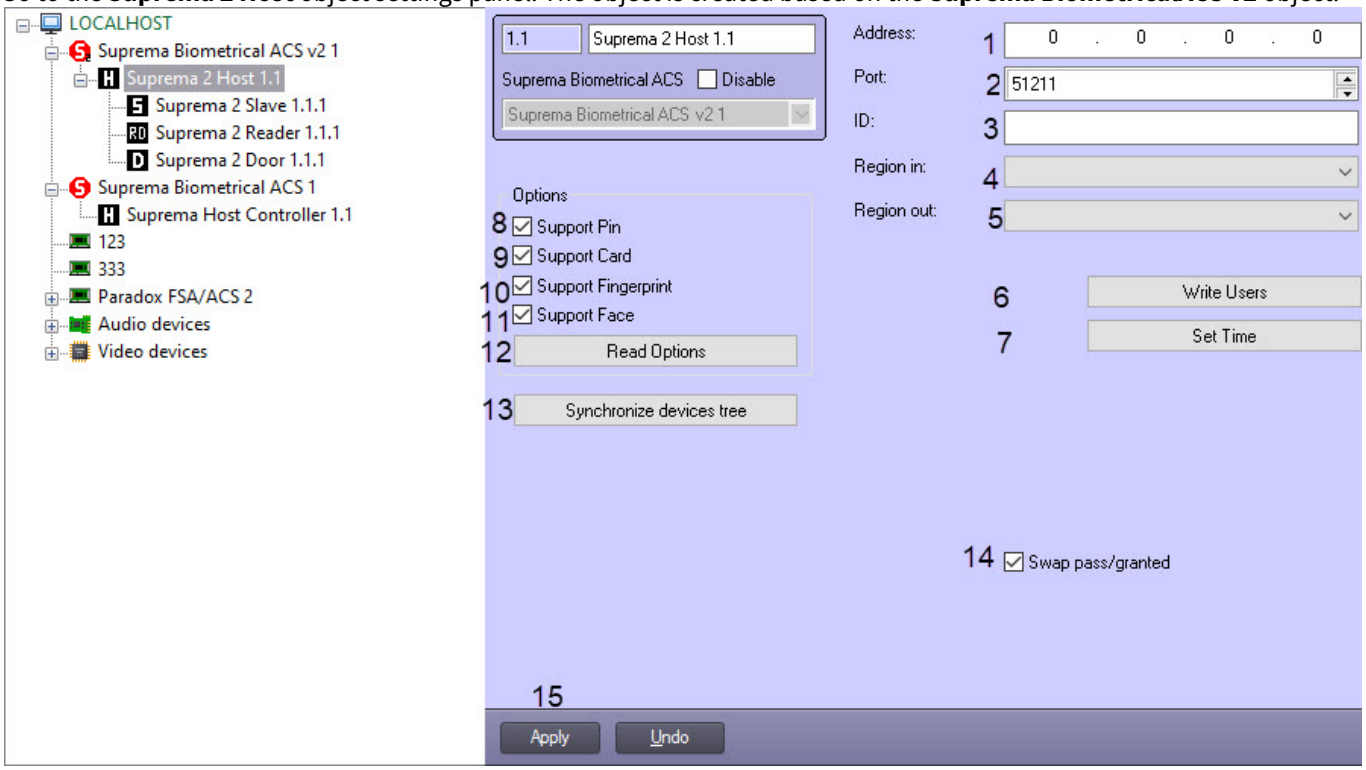
Set the **Dynamic** (**3**) checkbox in order to enable the dynamic sending of users and time.

Click **Apply** to save changes (**4**).

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 based on the **Suprema BiometricalACS v2** object.



2. In the **Address** (**1**) field, set 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 identification number of the controller connected via Ethernet.
5. From the **Region in** (**8**) drop-down list, select the Region corresponding to the area located at side of exit through the reader.
6. From the **Region out** (**9**) drop-down list, select the Region corresponding to the area located at side of entrance through the reader.

> **Note.**
>
> The **Region in** and **Region out** are to be selected if *Time&Attendance* interface module is in use. Otherwise, leave these fields empty.

7. Click **Write Users** (**6**) to send users to the controller.
8. Click **Set Time** (**7**) to synchronize controller time with Server time.
9. Enable controller options:
   a. Set the **Support Pin** (**8**) check box if the controller supports authorization by password.
   b. Set the **Support Card** (**9**) check box if the controller supports authorization by card.
   c. Set the **Support Fingerprint** (**10**) check box if the controller supports authorization by fingerprint.
   d. Set the **Support Face** (**11**) check box if the controller supports authorization by face.

   > **Note.**
   >
   > Only set the check boxes for options supported by the *Suprema 2* controller.

10. Click **Read Options** (**12**) to read supported options from the controller.
11. Click **Synchronize devices tree** (**13**) to automatically create objects in ACFA Intellect hardware tree according to the devices connected to the controller.

12. Configure sending an event upon successful access: **Swap pass/granted** (**14**). 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.

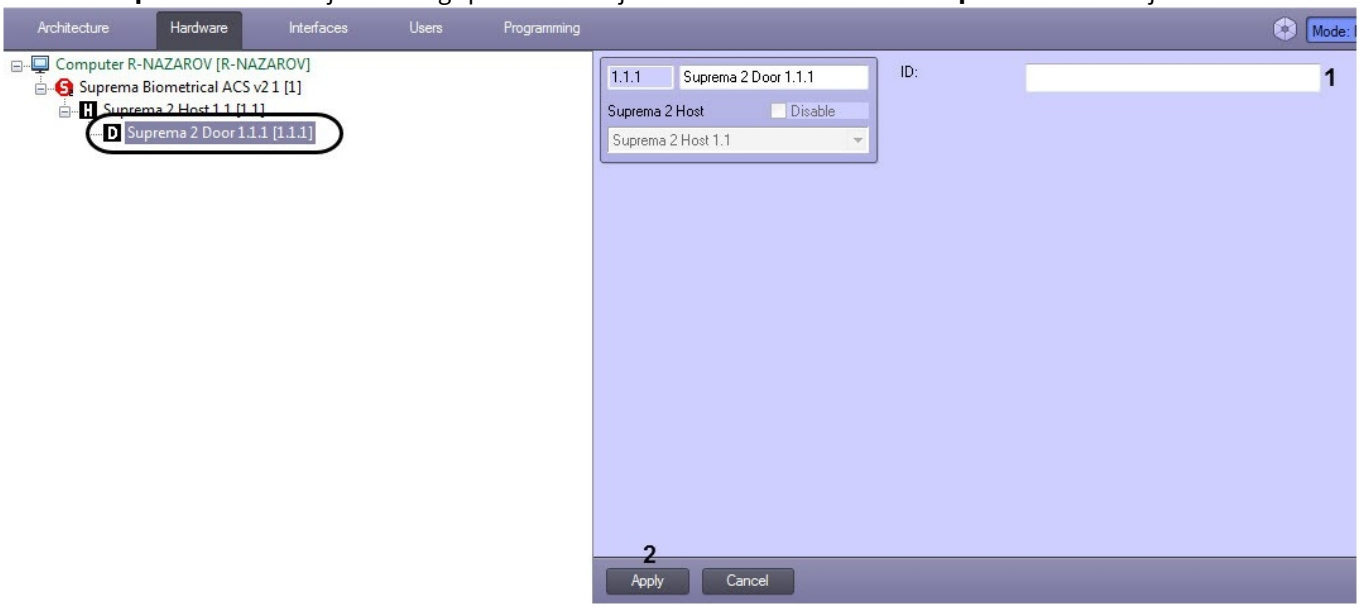
13. Click **Apply** to save changes (**15**).

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 based on the **Suprema 2 Host** object.



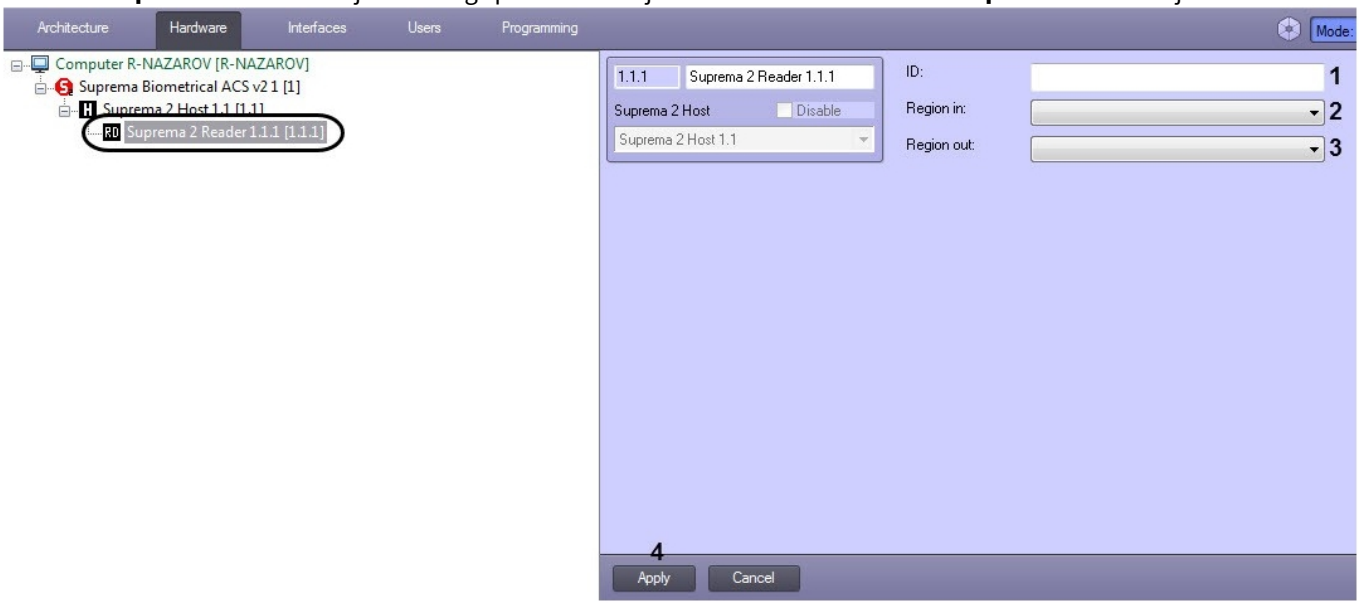
2. In the **ID** (**1**) field, specify the access point identification number.
3. Click **Apply** to save changes (**2**).

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 based on 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 located at side of exit through the reader.
4. From the **Region out** (**3**) drop-down list, select the Region corresponding to the area located at side of entrance through the reader.

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

5. Click **Apply** to save changes (**4**).

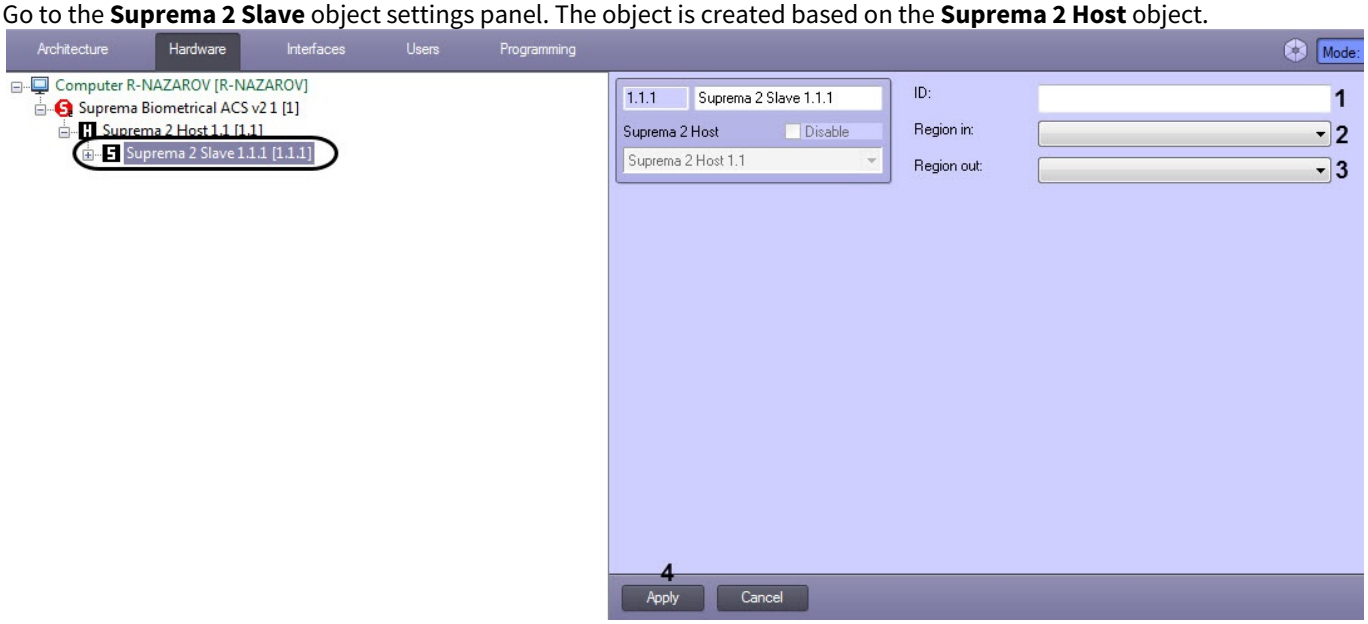
Configuring the **Suprema 2** reader is completed.

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 manufacturer Suprema Inc.).

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

1. Go to the **Suprema 2 Slave** object settings panel. The object is created based on 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 located at side of exit through the controller.
4. From the **Region out** (**3**) drop-down list, select the Region corresponding to the area located at side of entrance through the controller.

> **Note.**
>
> The **Region in** and **Region out** are to be selected if *Time&Attendance* interface module is in use. Otherwise, leave these fields empty.

5. Click **Apply** to save changes (**4**).

Configuring the **Suprema 2** slave controller is completed.

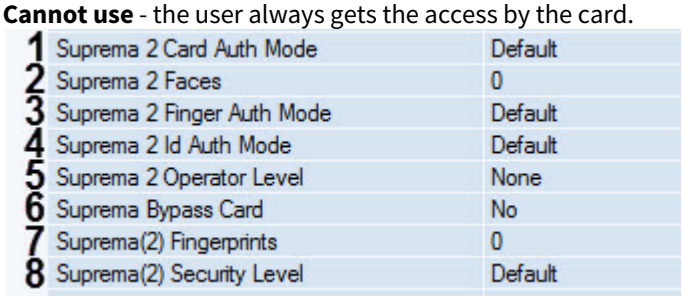
3.7 Setting up additional user parameters in Suprema 2 integration

> **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* module:

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

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

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

4.2 Controlling Suprema 2 Host object

Controlling the **Suprema 2 Host** object is performed in the Map interface window with the **Suprema 2 Host** object functional menu.

The **Suprema 2 Host** object functional menu commands are given in the table.

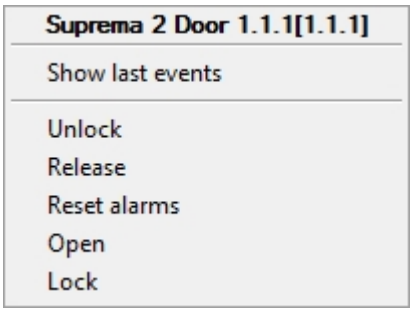
Menu command	Function
Show last events	Displays last 10 events received from the object.

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

	Connected
	Connected but not synchronized
	Disconnected

4.3 Controlling Suprema 2 Door object

Controlling the **Suprema 2 Door** object is performed in the Map interface window with the **Suprema 2 Door** object functional menu.



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

Menu command	**Function**
Show last events	Displays last 10 events received from the object.
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:

	Locked
	Unlocked
	Connection lost
	Closed
	Opened

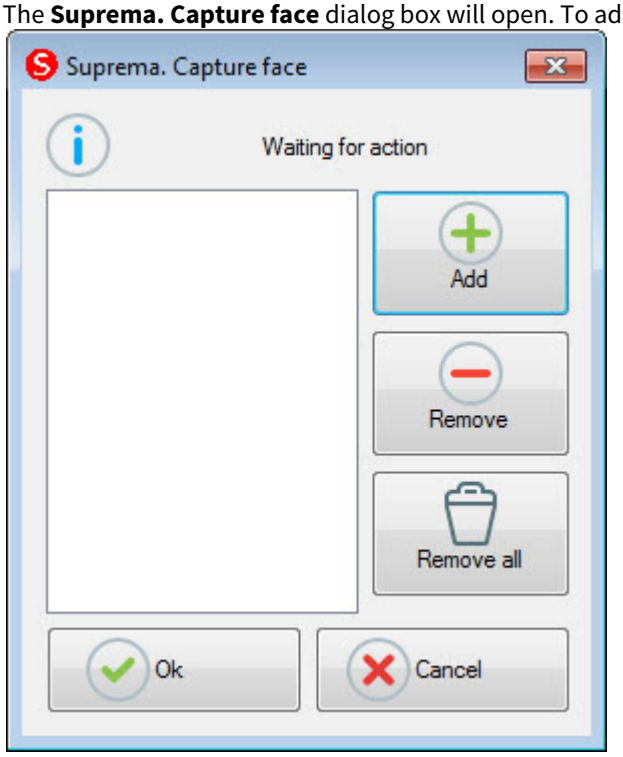
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Held open
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Alarm held open
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Alarm forced open
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Lock (scheduled)
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Lock (operator)
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Lock (emergency)
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Unlock (scheduled)
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Unlock (operator)
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Unlock (emergency)
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Alarm APB

4.4 Adding the Suprema 2 biometric parameters

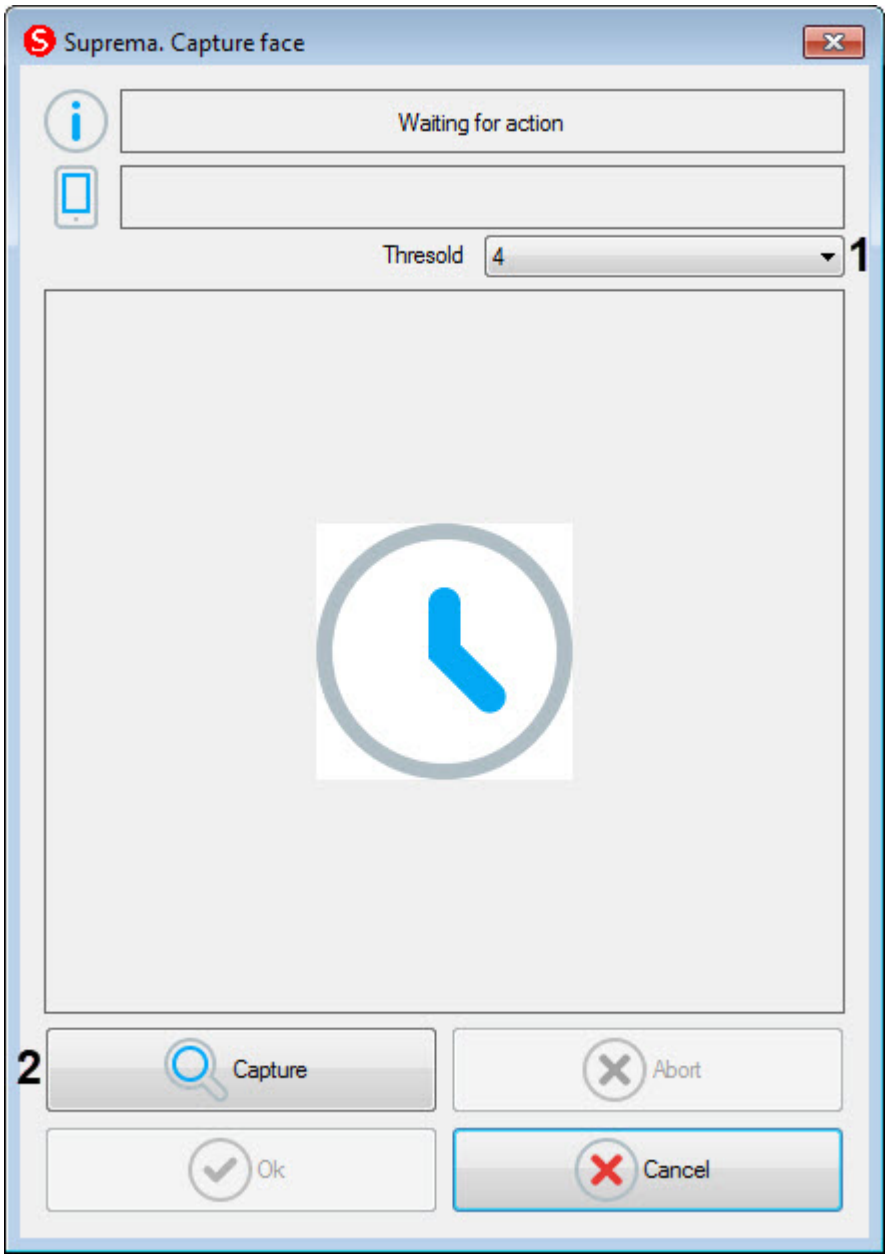
4.4.1 Adding the Suprema 2 face template

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.
6. Click **OK** to complete adding a face template.
7. 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.

8. Click **OK** to save the face template.

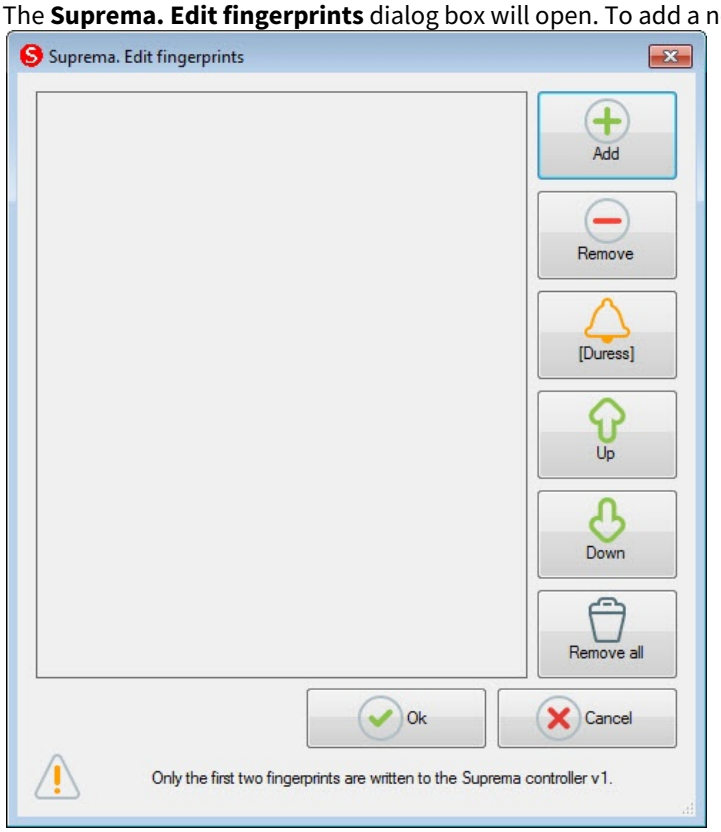
The *Suprema 2* face template is added.

4.4.2 Adding the Suprema 2 fingerprints

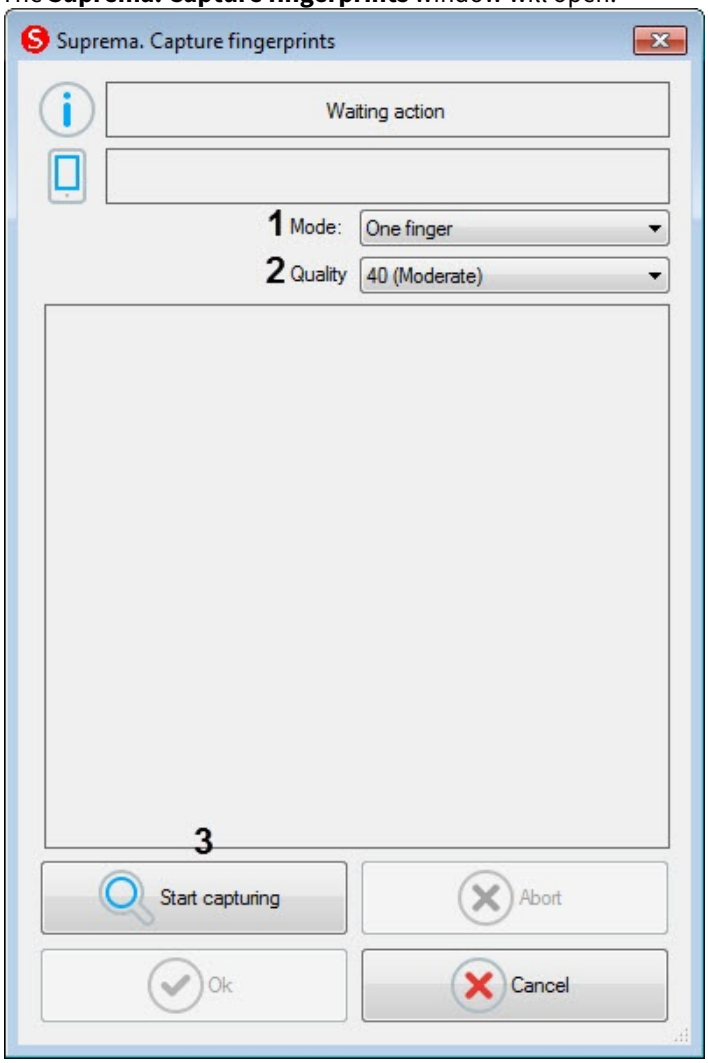
To add *Suprema 2* fingerprints in the *Access Manager* module, do the following:

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.

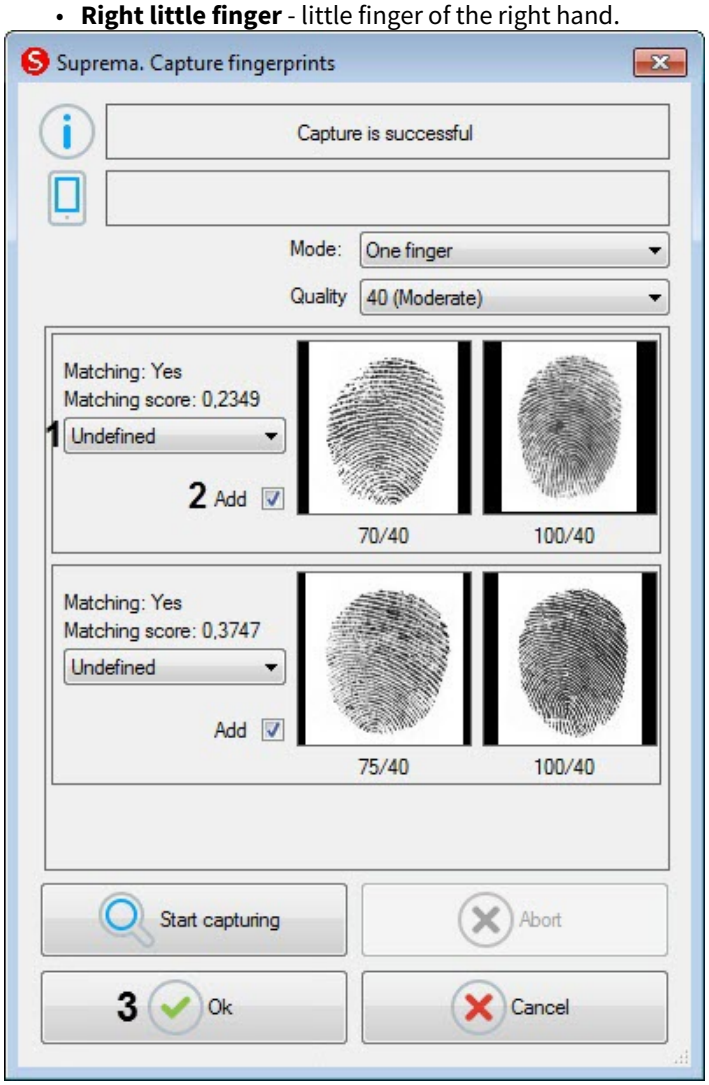


4. From the **Mode** drop-down list (**1**) select the fingerprint capture mode:
   - **One finger** - reading a single fingerprint.
   - **Two fingers** - reading two fingerprints.
   - **Two thumb fingers** - reading two thumb fingerprints.
   - **Left four fingers** - reading fingerprints of four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

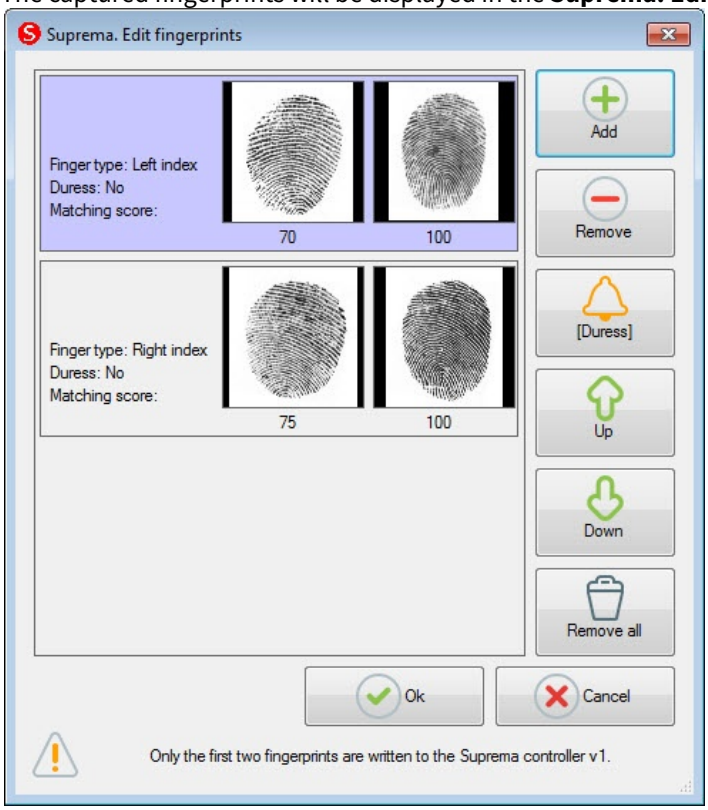
7. After the fingerprint capture is completed, select the type of scanned finger for each fingerprint in the drop-down list (**1**):

- **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.