Suprema Integration Module Settings Guide

ACFA PSIM 1.1

Last update 05/06/2024

Table of Contents

1 Introduction into Suprema Integration Module Settings Guide

On the page:

1.1 Purpose of the document

This *Suprema Module Settings Guide* is a reference manual designed for *Suprema* Module configuration technicians. This module is part of an access control system (ACS) built on the *ACFA PSIM* Software System.

This Guide presents the following materials:

1. general information about the *Suprema Biometrical ACS* module;
2. configuration of the *Suprema Biometrical ACS* module;
3. working with the *Suprema Biometrical ACS* module.

1.2 General information about the Suprema integration module

The *Suprema* Module is a component of an ACS built on the *ACFA PSIM* Software System. It was designed to perform the following functions:

1. Configuration of the *Suprema Biometrical* ACS (manufactured by Suprema Inc.);
2. Interaction between the *Suprema Biometrical* ACS and the *ACFA PSIM* Software System (monitoring, control).

Note:

Detailed information about the Suprema Biometrical ACS is presented in the official documentation for that system.

Before configuring the *Suprema* Module, the following actions must be performed:

1. Install the *Suprema Biometrical* ACS hardware on the protected territory (see the *Suprema* reference documentation).
2. Connect the *Supreme* ACS hardware to the Server.
3. Install *BioStar 1_8* onto the Server (available on the official website of the manufacturer of *Supreme* ACS).
4. Configure the connection of *Supreme* ACS to the *BioStar 1_8* Server (see the reference documentation for the configuration utility of the BioStar 1_8).

2 Supported hardware and licensing of the Suprema integration module

Manufacturer	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
XPass	Controller	Max. number of users: 40000 Inputs: 2 Relay: 1 Ethernet interface
X-Station		Max. number of users: 200000 Inputs: 2 Relay: 1
BioEntry Plus	Fingerprint scanner	Max. number of users: 5000 Inputs: 4 Relay: 1 Ethernet interface
SecureIO		

Protection
Per reader.

3 Configuration of the Suprema integration module

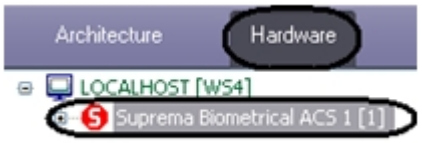
3.1 Procedure for configuration of the Suprema integration module

The *Suprema* module is configured in the following order:

1. Activate the *Suprema Biometrical ACS* integration module.
2. Configure the *Suprema Host Controller* object.
3. Configure the *Suprema Host Controller Input* object.
4. Configure the *Suprema Host Controller Door* object.
5. Configure the *Suprema Host Controller Reader* object.
6. Configure the *Suprema Secure IO* object.
7. Configure the *Suprema Secure IO Input* object.
8. Configure the *Suprema Secure IO Relay* object.
9. Configure the *Suprema Slave Controller* object.
10. Configure the *Suprema Slave Controller Door* object.
11. Configure the *Suprema Slave Controller Input* object.
12. Configure the *Suprema Slave Controller Reader* object.

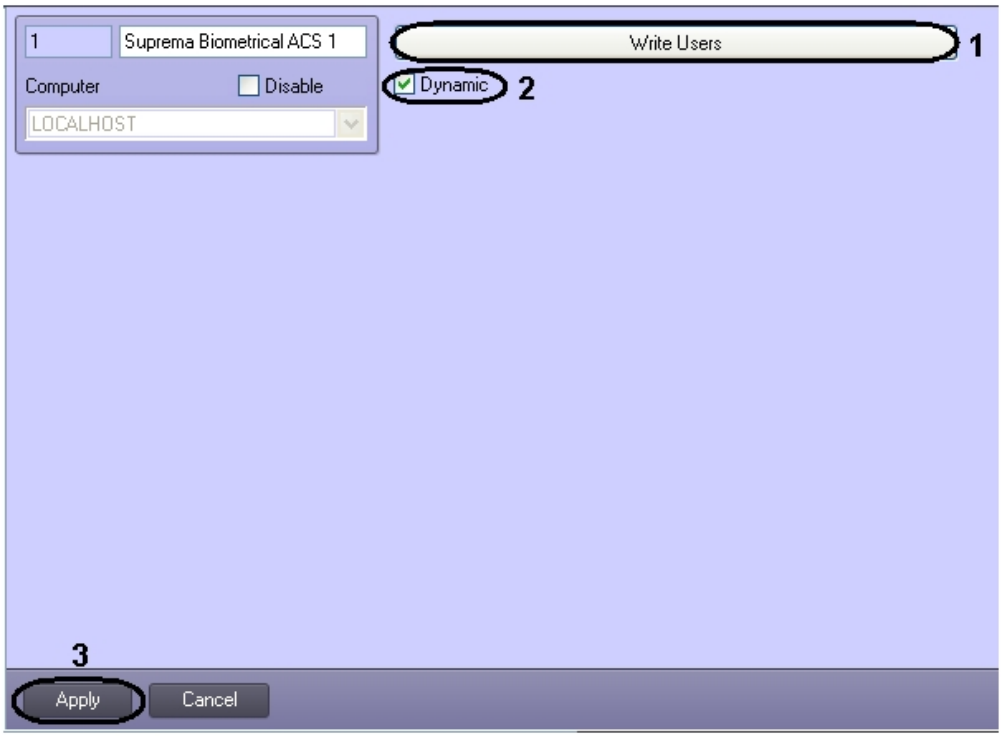
3.2 Activate the Suprema Biometrical ACS integration module

To activate the *Suprema Biometrical ACS* integration module, a **Suprema Biometrical ACS** object must be created based on a **Computer** object on the **Hardware** tab of the **System Settings** dialog.



3.3 Writing users to all Suprema controllers

To write users to all controllers click the **Write Users** button on the **Suprema Biometrical ACS** object's settings panel.

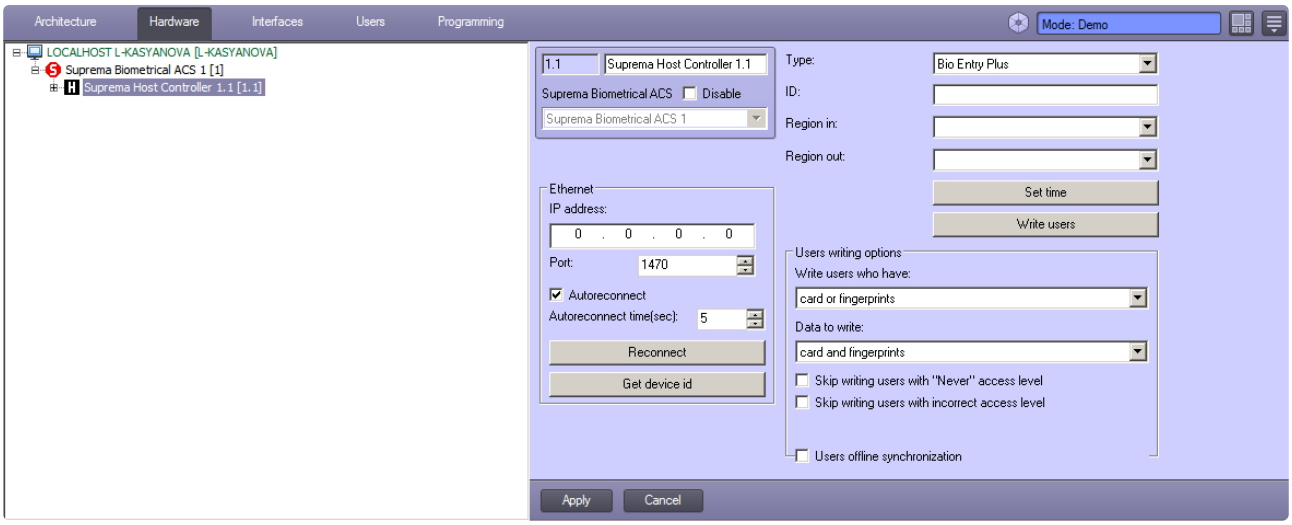


To enable the dynamical sending of users set the **Dynamic** checkbox (**2**).

To save changes click the **Apply** button (**3**).

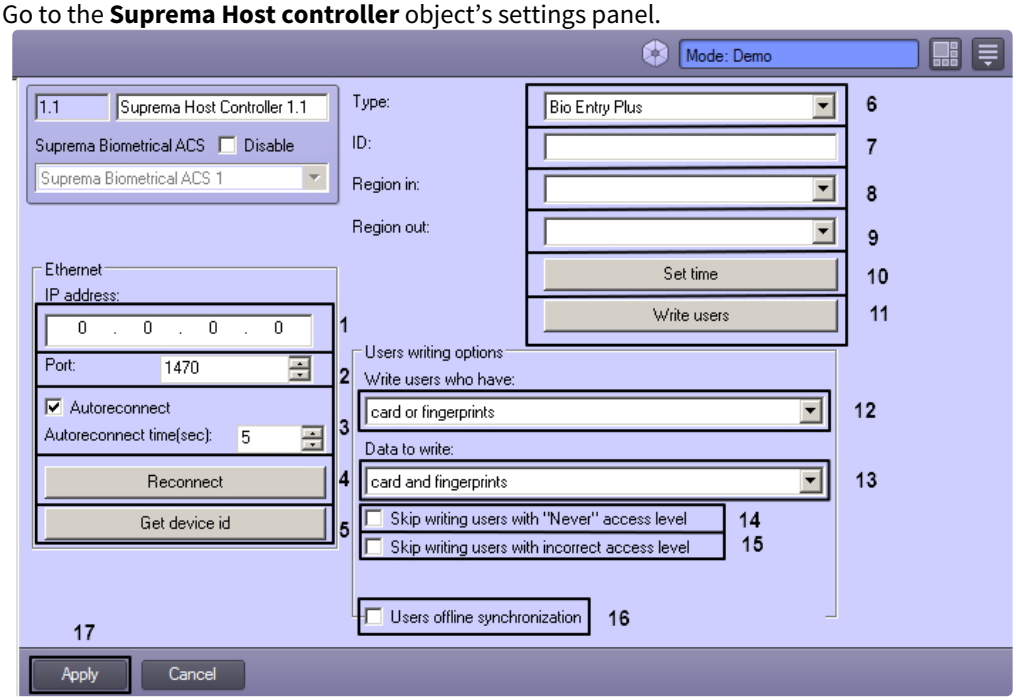
3.4 Configure the Suprema Host Controller object

The *Suprema Host Controller* object is configured on the **Suprema Host Controller** object's settings panel. This object is created based on a **Suprema Biometrical ACS** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Host Controller* do the following:

1. Go to the **Suprema Host controller** object's settings panel.



2. Enter the controller's IP address in the **IP-address:** field (**1**).
3. Enter the controller's connection port in the **Port** field (**2**).
4. Check the **Autoreconnect** box that enables automatic reconnect if the connection with the controller is lost in the time period specifed in the **Autoreconnect time** field (**3**).
5. Click the **Reconnect** button to reconnect controller by Ethernet (**4**).
6. To get the ID of controller connected via Ethernet click the **Get device id** button (**5**).
7. From the **Type:** drop-down list select the type of the controller (**6**). The following types are available:
    a. Bio Entry Plus – finger and card can be used;
    b. XPass – only card can be used;
    c. X-station – card and password can be used.
8. Enter the hardware address of a connected controller in the **ID:** field (**7**).
9. From the **Region In:** drop-down list select the Area located in the site of exit through this reader (**8**).
10. From the **Region Out:** drop-down list select the Area located in the site of entry through this reader (**9**).

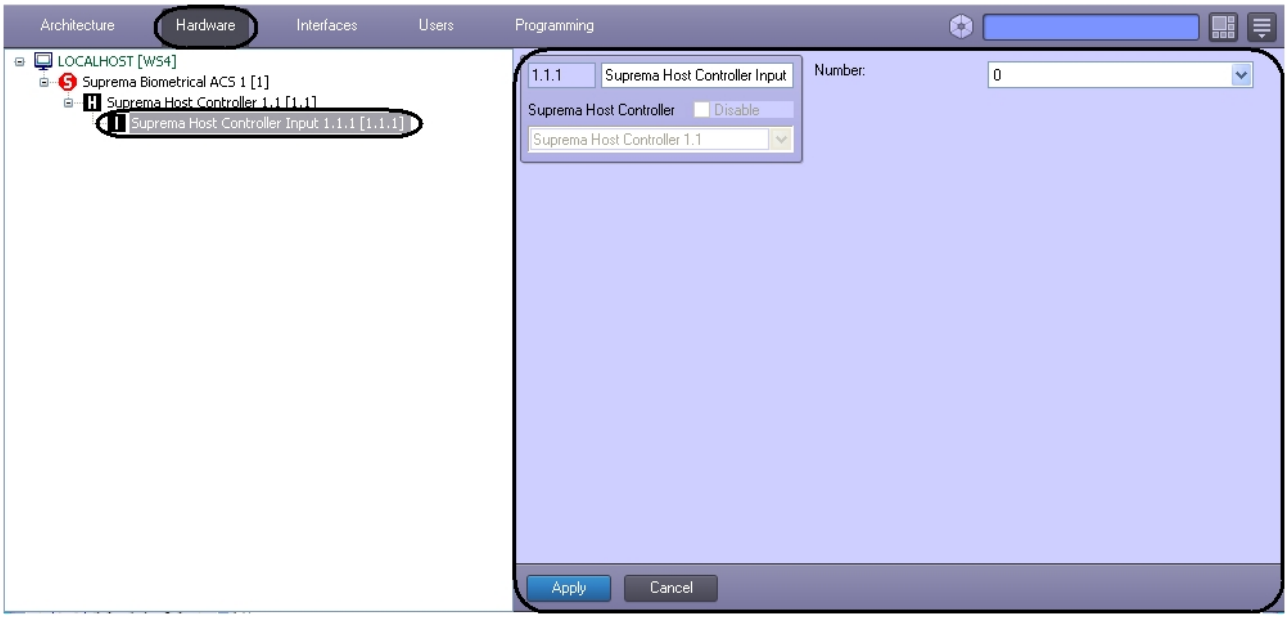
> **Note.**
>
> **Region In** and **Region Out** fields must be filled if the *Time and Attendance* interface module is used. Otherwise, leave these fields empty.

11. Click the **Set time** button to set time to the controller (**10**).
12. Click the **Write Users** button to write users to the controller (**11**).
13. Specify options of users writing:
    a. From the **Write users who have:** drop-down list select a parameter by which users for writing will be selected (**12**).
    b. From the **Data to write:** drop-down list select data which will be written (**13**).
    c. Set the **Skip writing users with "Never" access level** checkbox to write users with the "Never" access level (**14**).
    d. Set the **Skip writing users with incorrect access level** checkbox to write users with invalid or missed access level (**15**).
    e. Set the **Offline synchronization** checkbox to maintain the current information about users in controller in spite of breaking the connection (**16**).
14. To save changes click the **Apply** button (**17**).

This completes the configuration of the *Suprema Host Controller* object.

3.5 Configure the Suprema Host Controller Input object

The *Suprema Host Controller Input* object is configured on the **Suprema Host Controller Input** object's settings panel. This object is created based on a **Suprema Host Controller** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Host Controller Input* do the following:

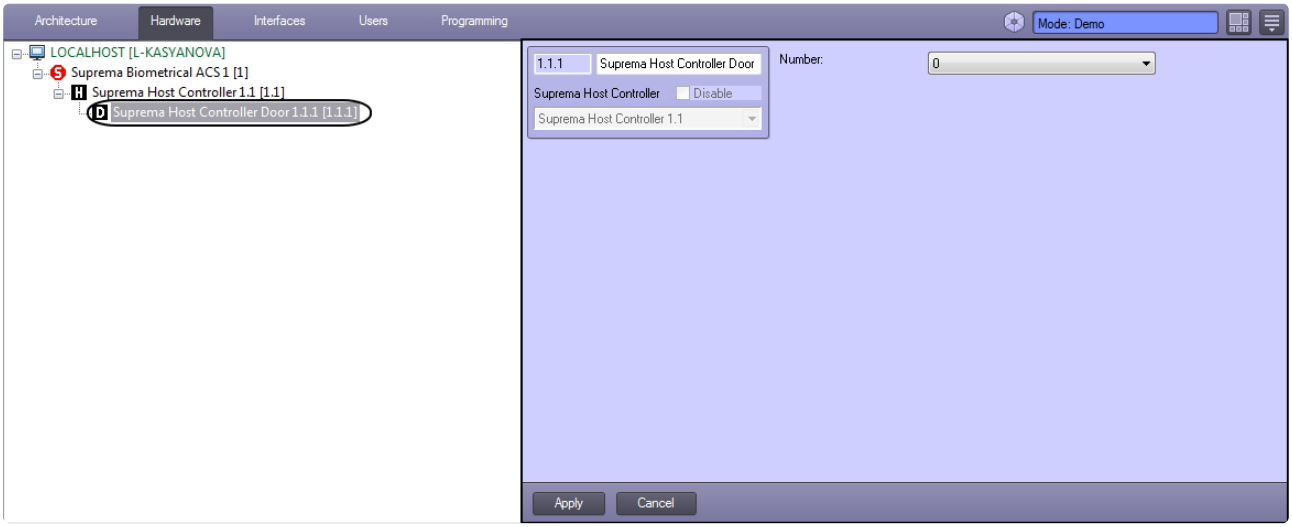
1. Go to the **Suprema Host Controller Input** object's settings panel.

2. From the **Number:** drop-down list select the number of the controller input (**1**).
3. To save changes click the **Apply** button (**2**).

This completes the configuration of the *Suprema Host Controller Input* object.

3.6 Configure the Suprema Host Controller Door object

The *Suprema Host Controller Door* object is configured on the **Suprema Host Controller Door** object settings panel. This object is created based on a **Suprema Host Controller** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Host Controller Door* do the following:

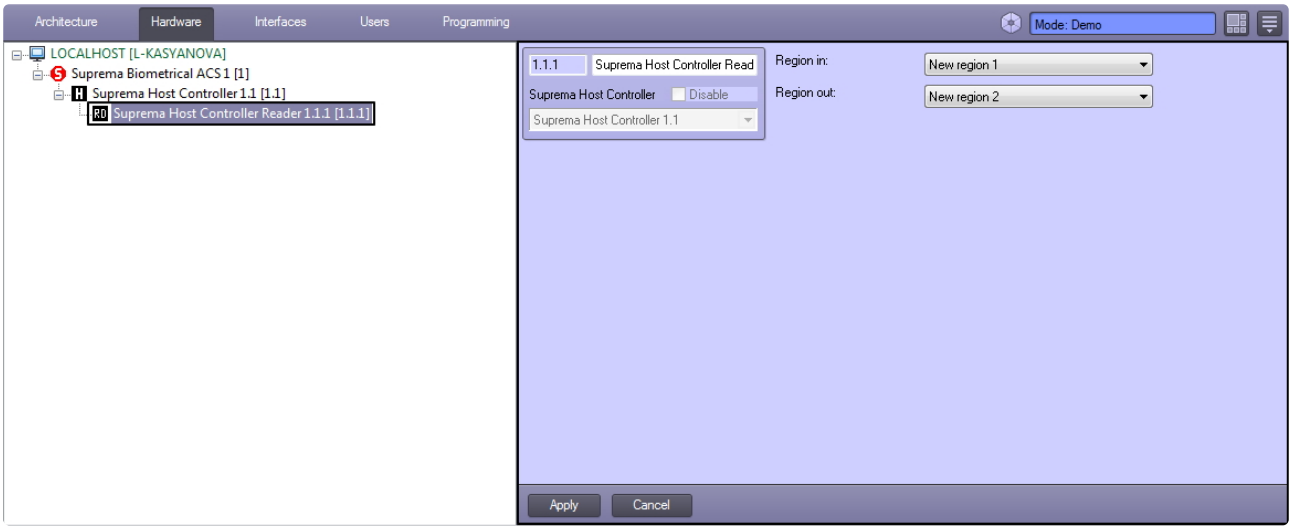
1. Go to the **Suprema Host Controller Door** object settings panel.

2. From the **Number:** drop-down list select the number of the door (**1**).
3. To save changes click the **Apply** button (**2**).

The configuration of the *Suprema Host Controller Door* object is complete.

3.7 Configure the Suprema Host Controller Reader object

The *Suprema Host Controller Reader* object is configured on the **Suprema Host Controller Reader** object settings panel. This object is created based on a **Suprema Host Controller** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Host Controller Reader* do the following:

1. Go to the **Suprema Host Controller Reader** object settings panel.

2. From the **Region in:** drop-down list select the region which the user enters (**1**).
3. From the **Region out:** drop-down list select the section from which the user enters (**2**).
4. To save changes click the **Apply** button (**3**).

The configuration of the *Suprema Host Controller Reader* object is complete.

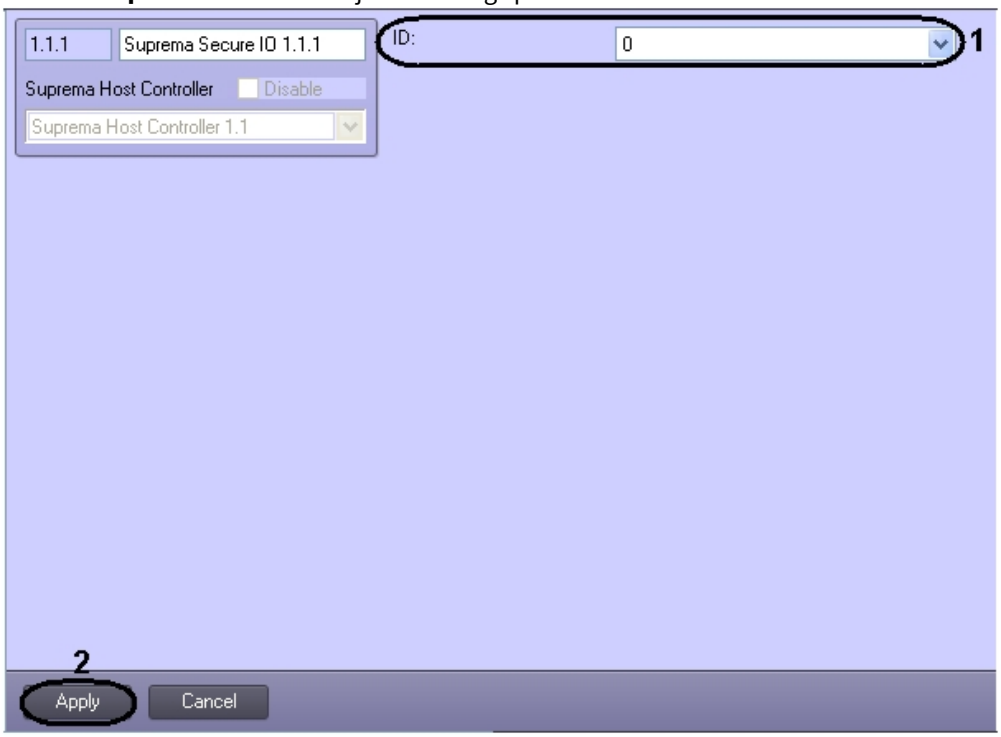
> **Note**
>
> The **Suprema Host Controller Reader** can be configured to work with the **Access Manager** module, see Configure the interaction between the Suprema Biometrical ACS and the Access Manager module.

3.8 Configure the Suprema Secure IO object

The *Suprema Secure IO* object is configured on the **Suprema Secure IO** object's settings panel. This object is created based on a **Suprema Host Controller** object on the **Hardware** tab of the **System Settings** dialog.

To configure the *Suprema Secure IO* do the following:

1. Go to the **Suprema Secure IO** object's settings panel.

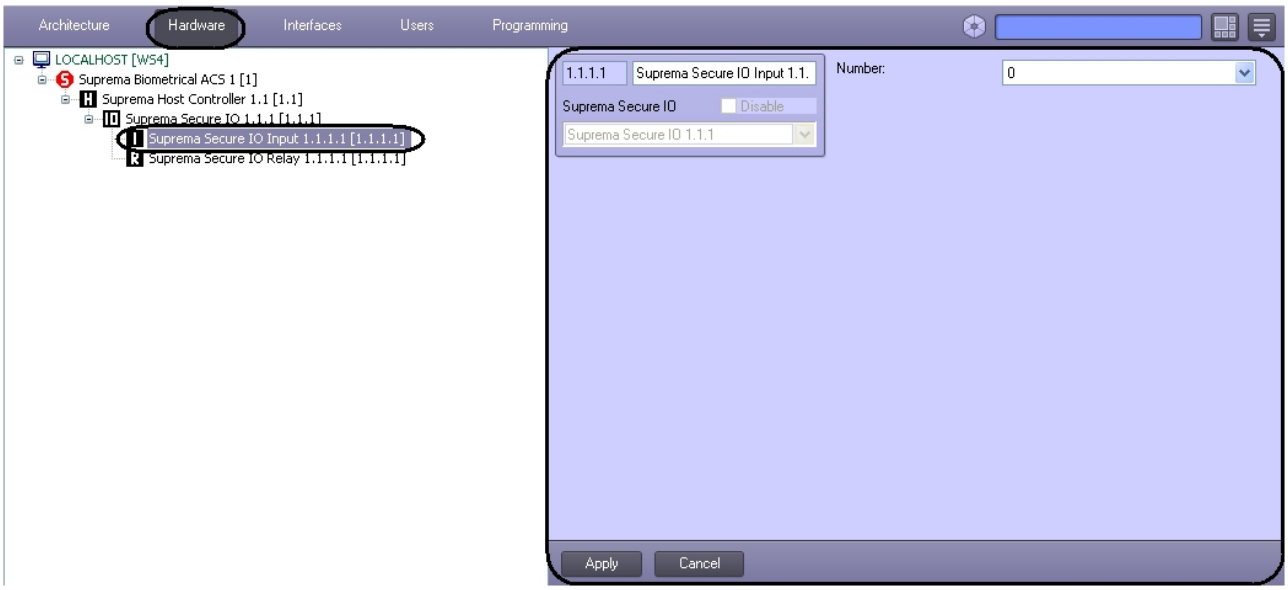


2. From the **Number:** drop-down list select the number of the controller (**1**).
3. To save changes click the **Apply** button (**2**).

This completes the configuration of the *Suprema Secure IO* object.

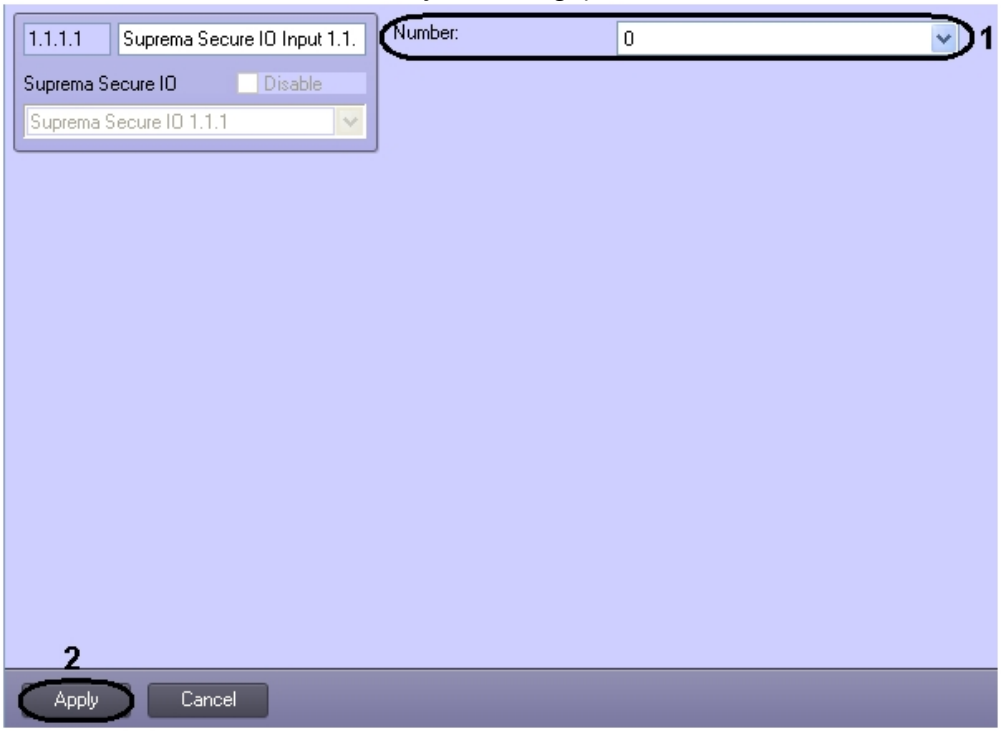
3.9 Configure the Suprema Secure IO Input object

The *Suprema Secure IO Input* object is configured on the **Suprema Secure IO Input** object's settings panel. This object is created based on a **Suprema Secure IO** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Secure IO Input* do the following:

1. Go to the **Suprema Secure IO Input** object's settings panel.

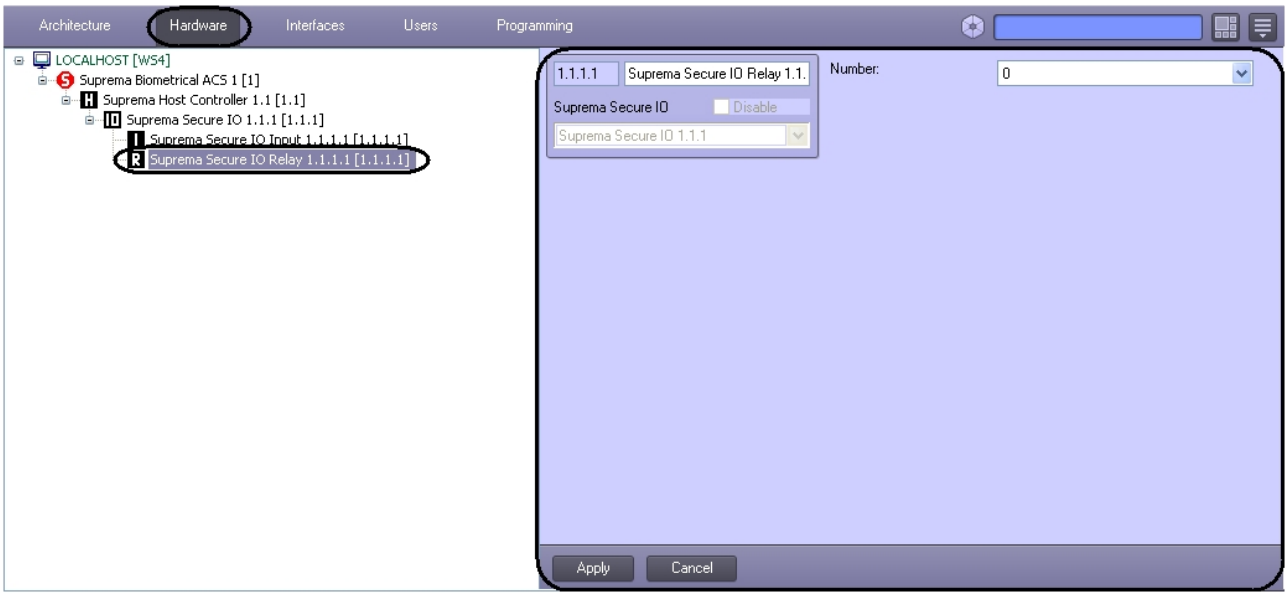


2. From the **Number:** drop-down list select the number of the controller input (**1**).
3. To save changes click the **Apply** button (**2**).

This completes the configuration of the *Suprema Secure IO Input* object.

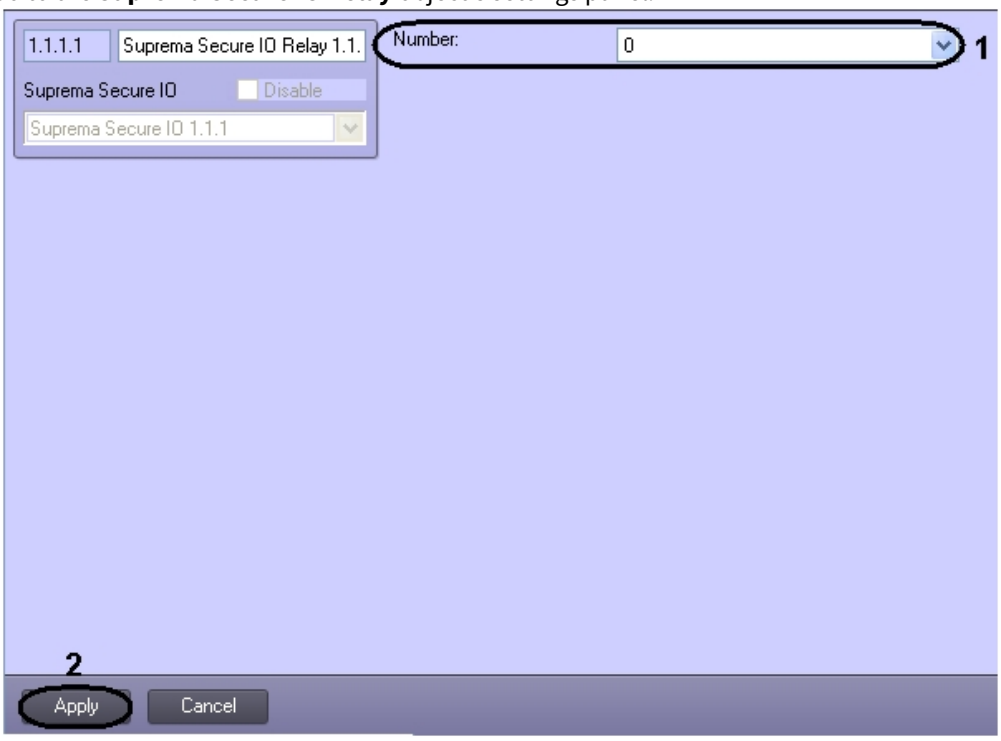
3.10 Configure the Suprema Secure IO Relay object

The *Suprema Secure IO Relay* object is configured on the **Suprema Secure IO Relay** object's settings panel. This object is created based on a **Suprema Secure IO** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Secure IO Relay* do the following:

1. Go to the **Suprema Secure IO Relay** object's settings panel.

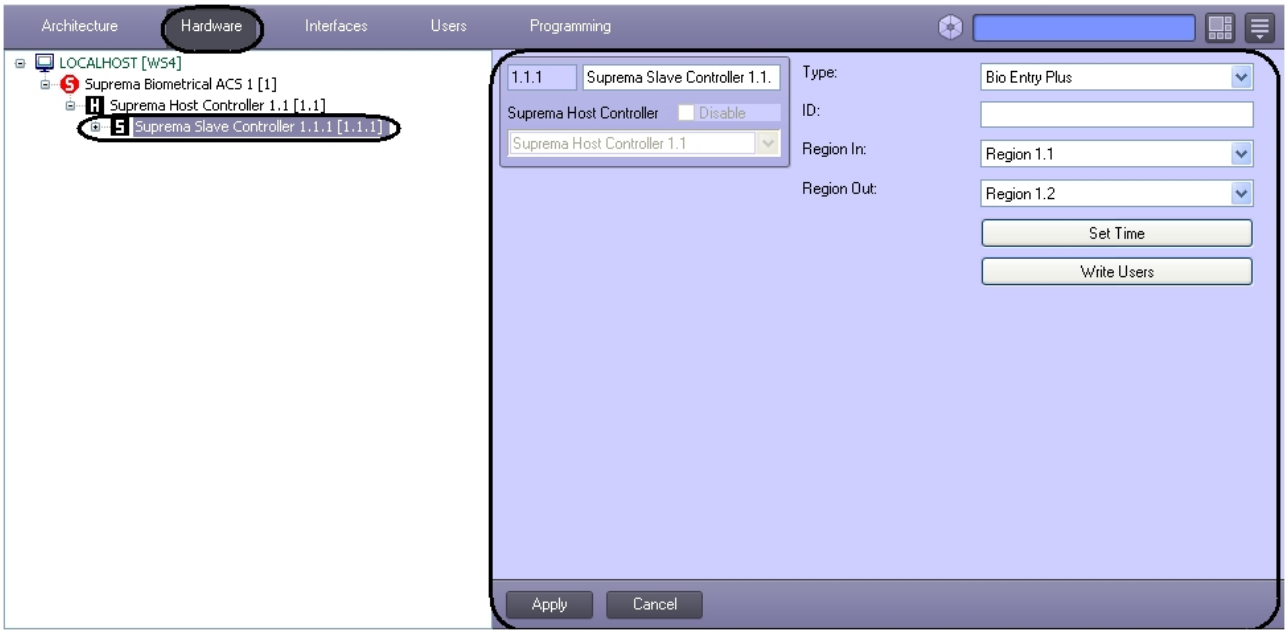


2. From the **Number:** drop-down list select the number of the controller input (**1**).
3. To save changes click the **Apply** button (**2**).

This completes the configuration of the *Suprema Secure IO Relay* object.

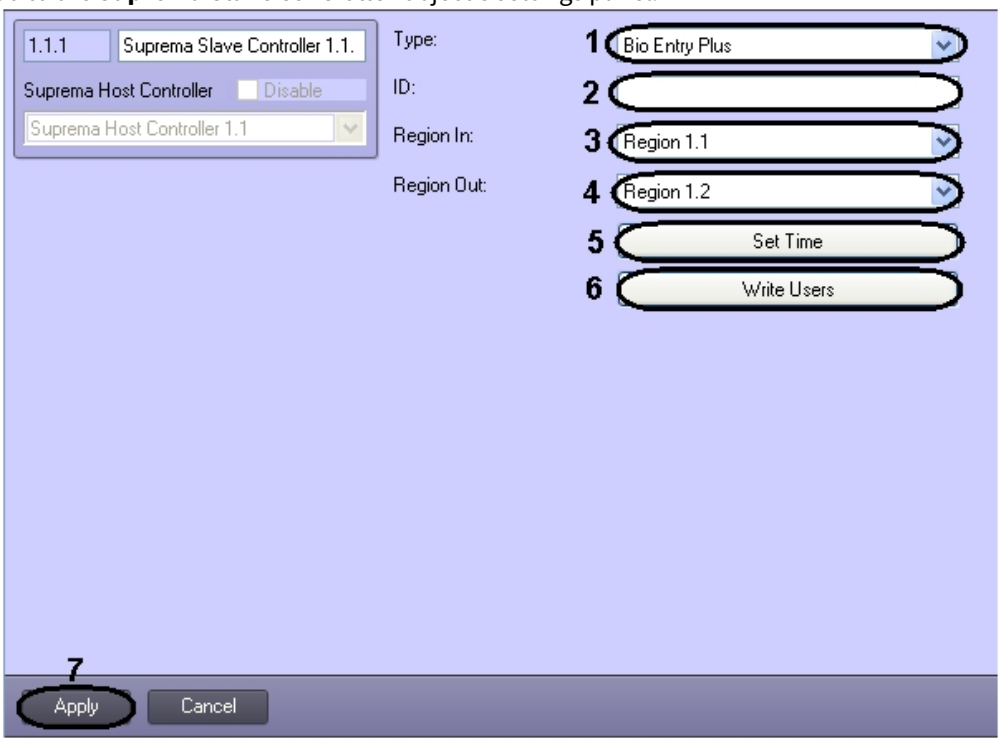
3.11 Configure the Suprema Slave Controller object

The *Suprema Slave Controller* object is configured on the **Suprema Slave Controller** object's settings panel. This object is created based on a **Suprema Host Controller** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Slave Controller* do the following:

1. Go to the **Suprema Slave controller** object's settings panel.

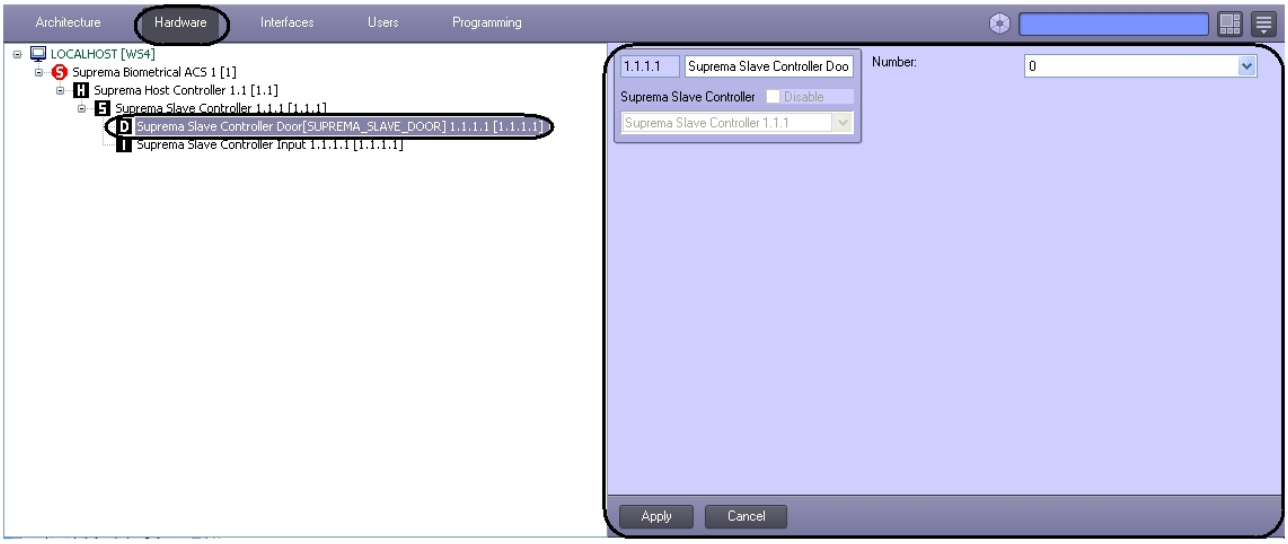


2. From the **Type:** drop-down list select the type of the controller (**1**). The following types are available:
   a. Bio Entry Plus – finger and card can be used;
   b. XPass – only card can be used
   c. X-station – card and password can be used.
3. Enter the hardware address of a connected controller in the **ID:** field (**2**).
4. From the **Region In:** drop-down list select the Area located in the site of exit through this reader (**3**).
5. From the **Region Out:** drop-down list select the Area located in the site of entry through this reader (**4**).
6. Click the **Set time** button to set time to the controller (**5**).
7. Click the **Write Users** button to write users to the controller (**9**).
8. To save changes click the **Apply** button (**10**).

This completes the configuration of the *Suprema Slave Controller* object.

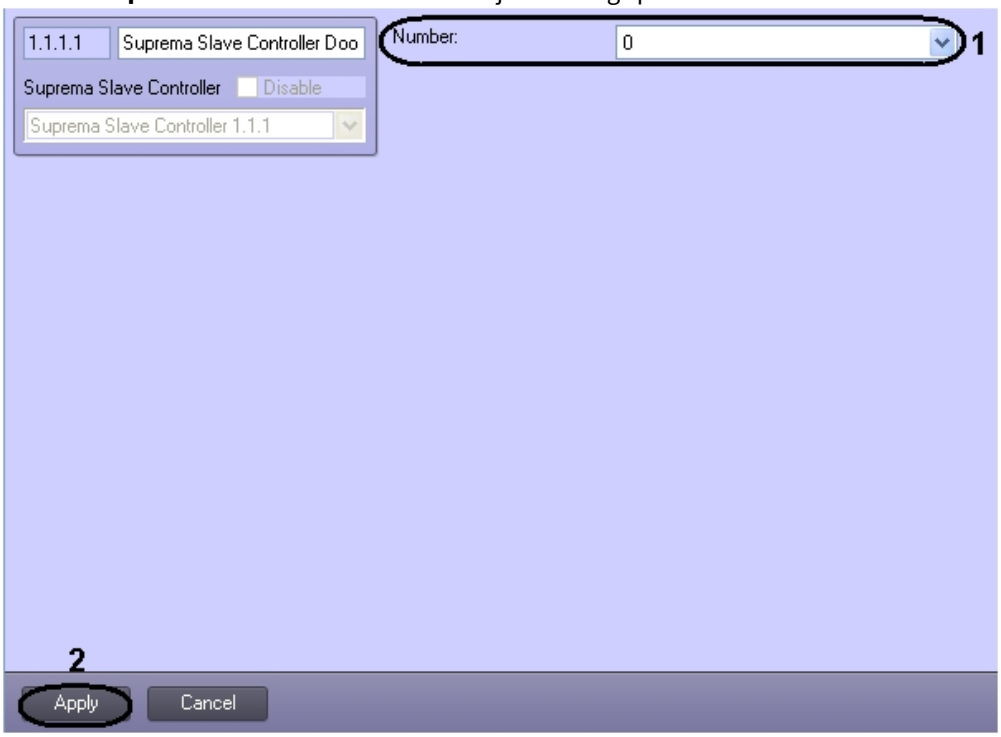
3.12 Configure the Suprema Slave Controller Door object

The *Suprema Slave Controller Door* object is configured on the **Suprema Slave Controller Door** object settings panel. This object is created based on a **Suprema Slave Controller** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Slave Controller Door* do the following:

1. Go to the **Suprema Slave Controller Door** object settings panel.

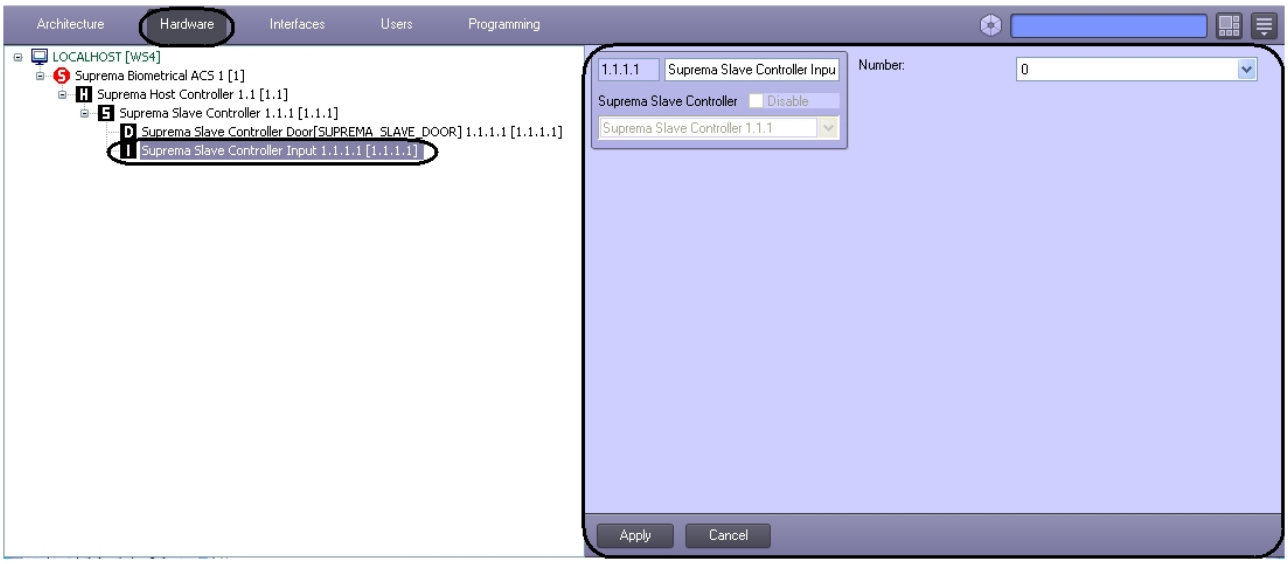


2. From the **Number:** drop-down list select the number of the door (**1**).
3. To save changes click the **Apply** button (**2**).

The configuration of the *Suprema Slave Controller Door* object is complete.

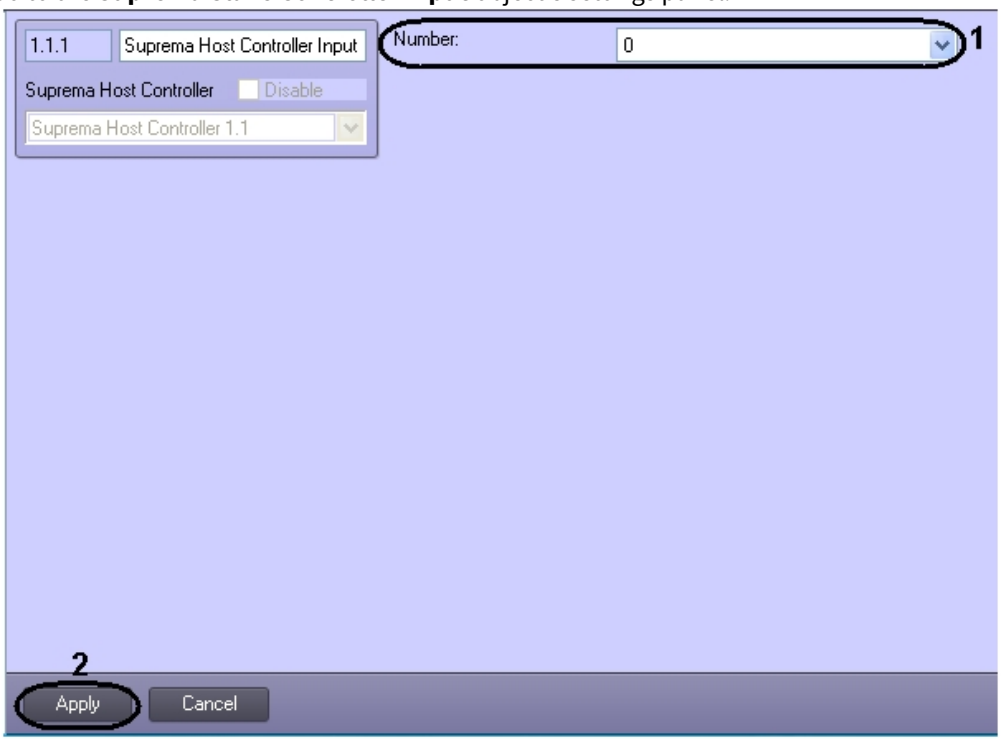
3.13 Configure the Suprema Slave Controller Input object

The *Suprema Slave Controller Input* object is configured on the **Suprema Slave Controller Input** object's settings panel. This object is created based on a **Suprema Slave Controller** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Slave Controller Input* do the following:

1. Go to the **Suprema Slave Controller Input** object's settings panel.

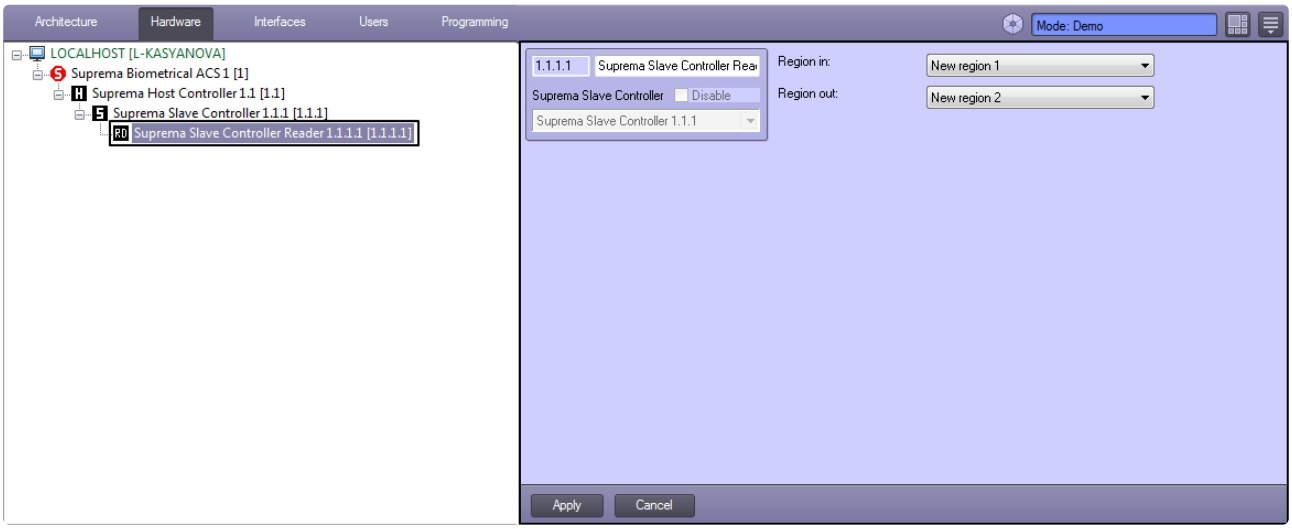


2. From the **Number:** drop-down list select the number of the controller input (**1**).
3. To save changes click the **Apply** button (**2**).

This completes the configuration of the *Suprema Slave Controller Input* object.

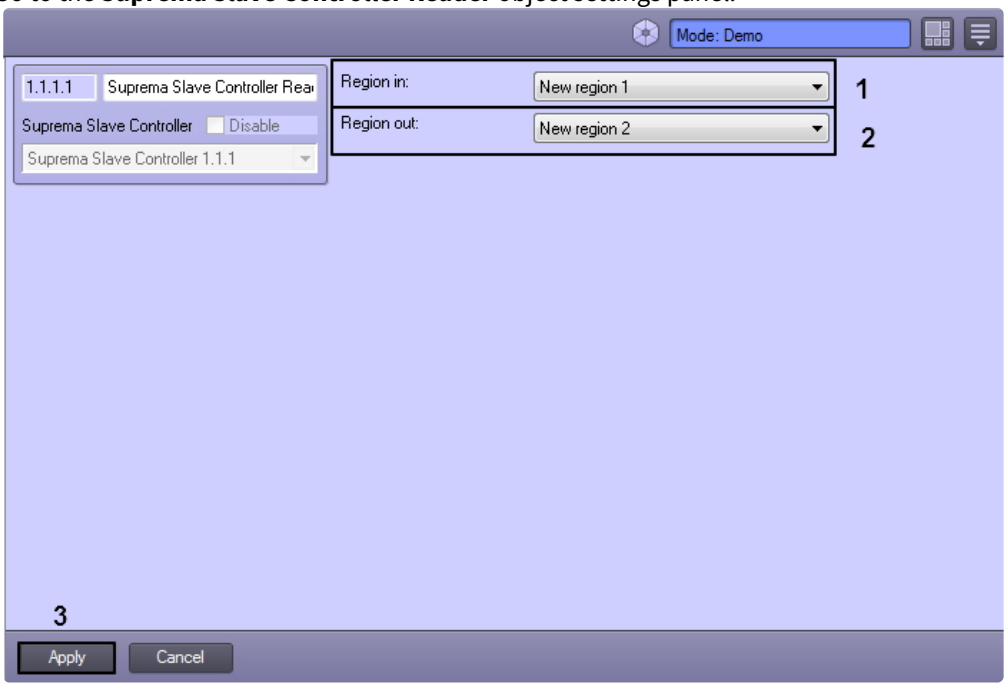
3.14 Configure the Suprema Slave Controller Reader object

The *Suprema Slave Controller Reader* object is configured on the **Suprema Slave Controller Reader** object settings panel. This object is created based on a **Suprema Slave Controller** object on the **Hardware** tab of the **System Settings** dialog.



To configure the *Suprema Slave Controller Reader* do the following:

1. Go to the **Suprema Slave Controller Reader** object settings panel.



2. From the **Region in:** drop-down list select the region which the user enters (**1**).
3. From the **Region out:** drop-down list select the section from which the user enters (**2**).
4. To save changes click the **Apply** button (**3**).

The configuration of the *Suprema Slave Controller Reader* object is complete.

Note

The **Suprema Slave Controller Reader** can be configured to work with the **Access Manager** module, see Configure the interaction between the Suprema Biometrical ACS and the Access Manager module.

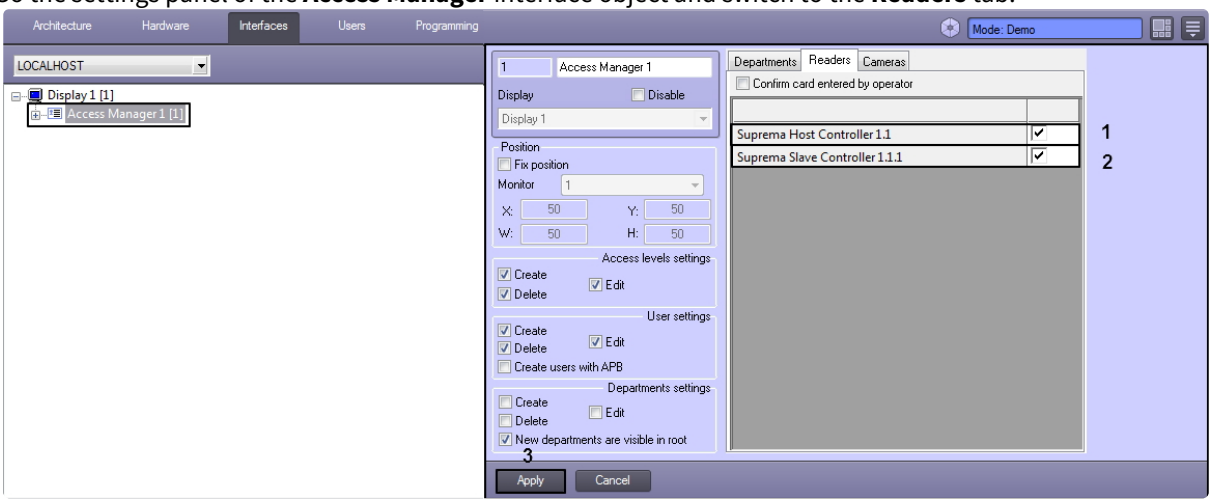
3.15 Configure the interaction between the Suprema Biometrical ACS and the Access Manager module

The readers connected to the Suprema controllers may be configured to supply fingerprints to the **Access Manager** service module. For information on the **Access Manager** module, see Guide for Configuring and Working with the ACFA PSIM Service Modules.

The interaction between **Suprema Biometrical ACS** and the **Access Manager** module is configured on the **Access Manager** interface object settings panel on the **Interfaces** tab of the **System Settings** dialog.

To configure the interaction between the Suprema module and the Access Manager module, do the following:

1. Go the settings panel of the **Access Manager** interface object and switch to the **Readers** tab.



2. Check the **Suprema Host Controller** to enable the readers connected to the **Suprema Host Controller** (**1**).
3. Check the **Suprema Slave Controller** to include the readers connected to the **Suprema Slave Controller** (**2**).
4. Click **Apply** to save the changes (**3**).

Configuring the interaction between the Suprema Biometrical ACS and the Access Manager module is complete.

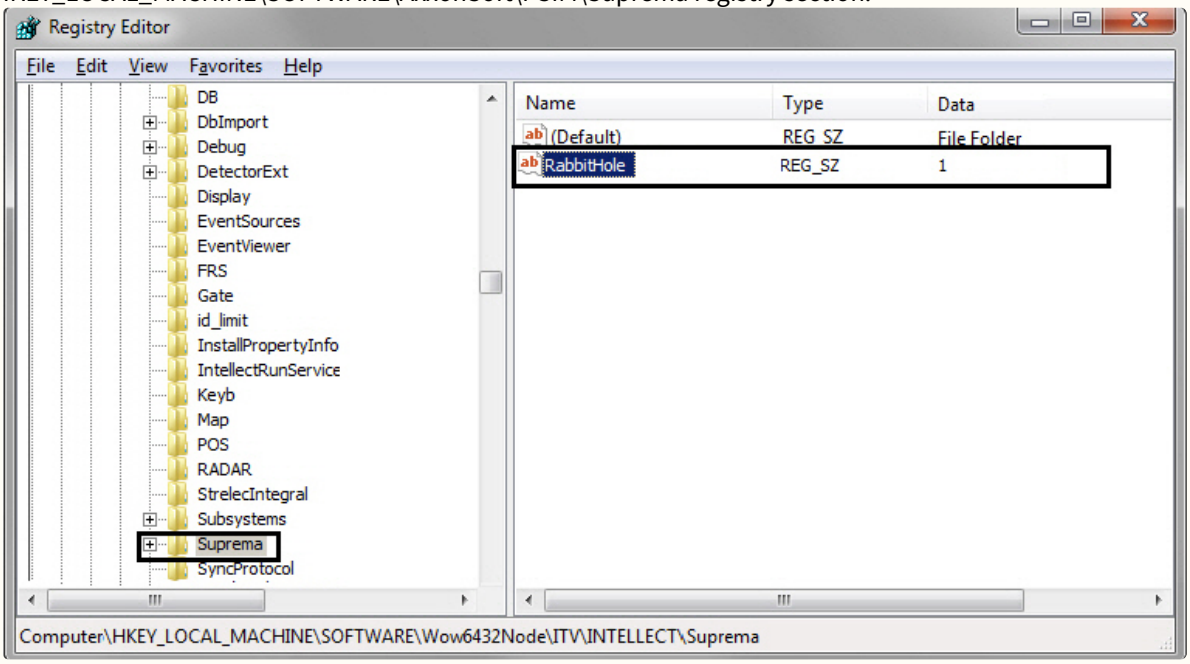
The procedure for fingerprint scanning using the Suprema readers is described in detail in Adding the Suprema fingerprints section.

3.16 Reading of users and events from Suprema database to the ACFA PSIM software

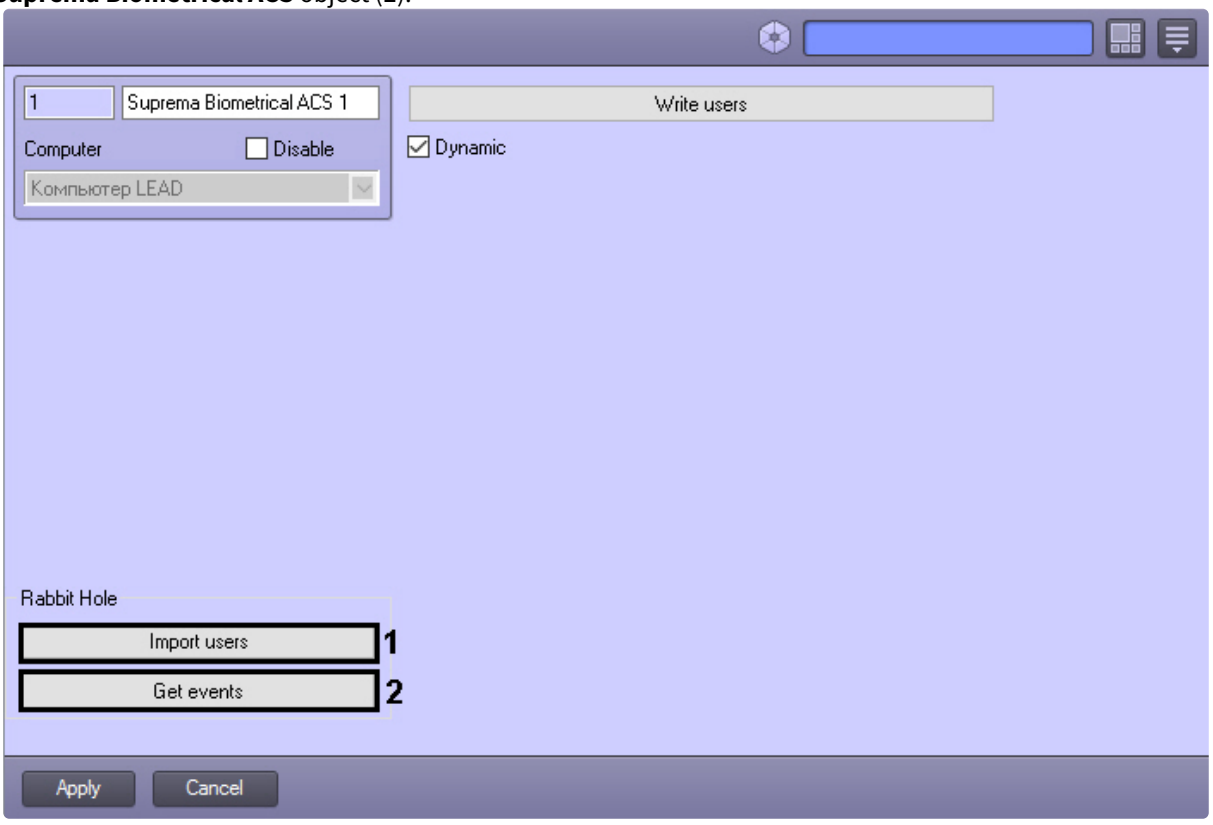
It's possible to import users and get events from the *Suprema* vendor software.

Attention!

Buttons for import of users and getting of events from the *Suprema* database are hidden on default. To display these buttons create the string parameter with the RabbitHole name and with value 1 in the HKEY_LOCAL_MACHINE\SOFTWARE\AxxonSoft\PSIM\Suprema registry section.

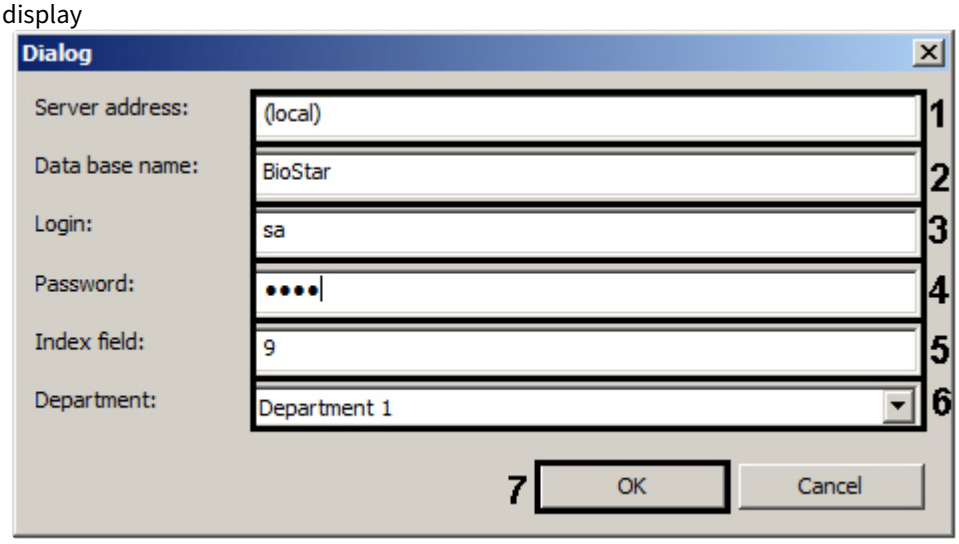


1. To import users from the *Suprema* database click the **Import users** button on the settings panel of the **Suprema Biometrical ACS** object (**1**).



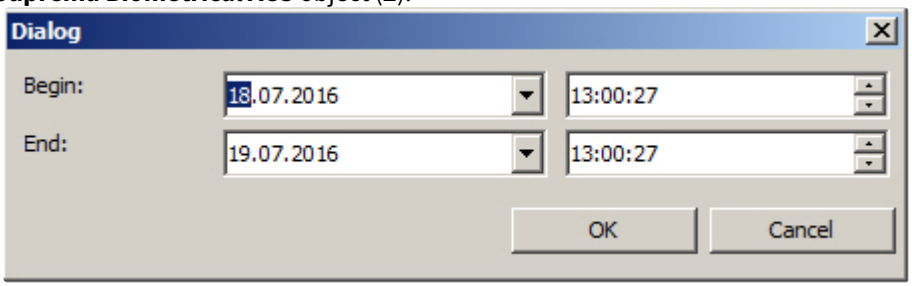
As a result the dialog window for specifying parameters of connection to the vendor software database will

display



a. In the **Server address:** field enter a server address of vendor software database (**1**).
b. In the **Database name:** field enter a database name from which users will be imported (**2**).
c. In the **Login:** field enter a login for connecting to database (**3**).
d. In the **Password:** field enter a password for connecting to database (**4**).
e. In the **Index field:** enter a number of additional database field of vendor software in which there is the *Axxon PSIM ID* parameter (**5**).
f. From the **Department:** drop-down list select a department in which imported users will be added (**6**).
g. Click the **OK** button (**7**).

2. To get events from the vendor software database click the **Get events** button on the settings panel of the **Suprema Biometrical ACS** object (**2**).



In the opened dialog window specify the time interval during which events are to be read.
As a result of this operation all events from all controllers in the system for the specified time interval will be received. If it's required to get events from the specific controller, do actions described above from the settings panel of the corresponding object.

3. Click **Apply** to save changes.

Attention!

Careless using of these settings can result in loss of users or events in the system and further incorrect working of the system.

4 Working with the Suprema Module

The following interface objects are used to work with the *Suprema* module:

1. **Map**;
2. **Access Manager**;
3. **Event Log**.

Information about configuring these interface objects is contained in the Axxon PSIM Software package: Administrator's Guide.

Working with interface objects is described in detail in the Axxon PSIM Software package: Operator's Guide.

4.1 General information about Suprema operation

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

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

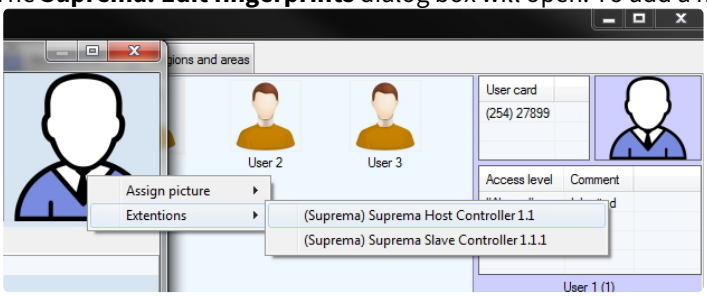
For a detailed description of configuring these interface objects, refer to the Axxon PSIM Administrator's Guide.

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

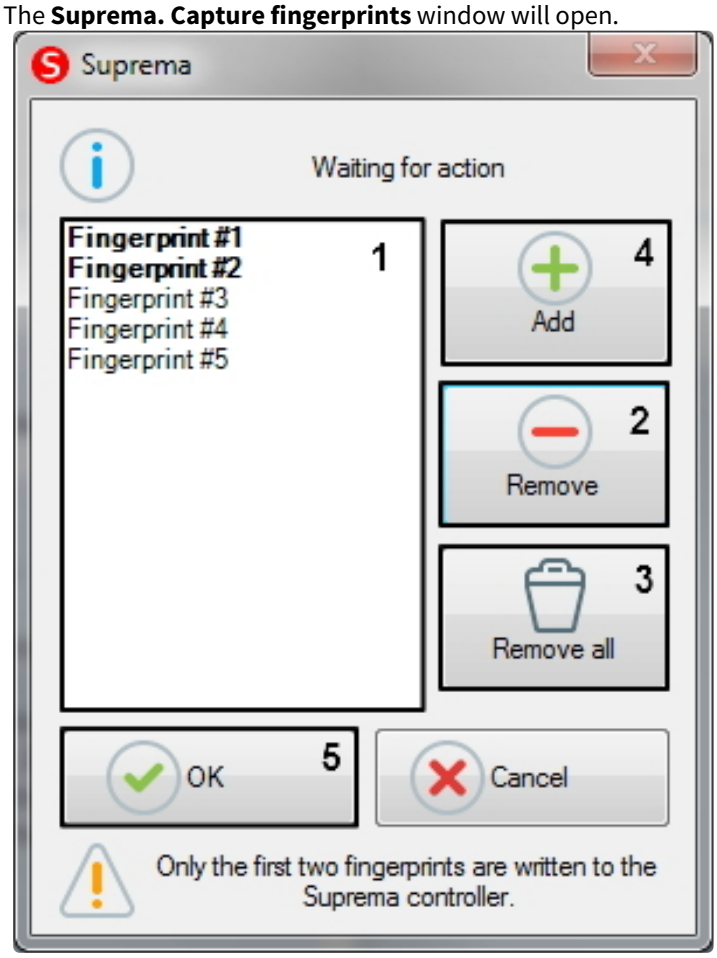
4.2 Adding the Suprema fingerprints

To add *Suprema* 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 Host Controller** or **Suprema Slave Controller** 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.



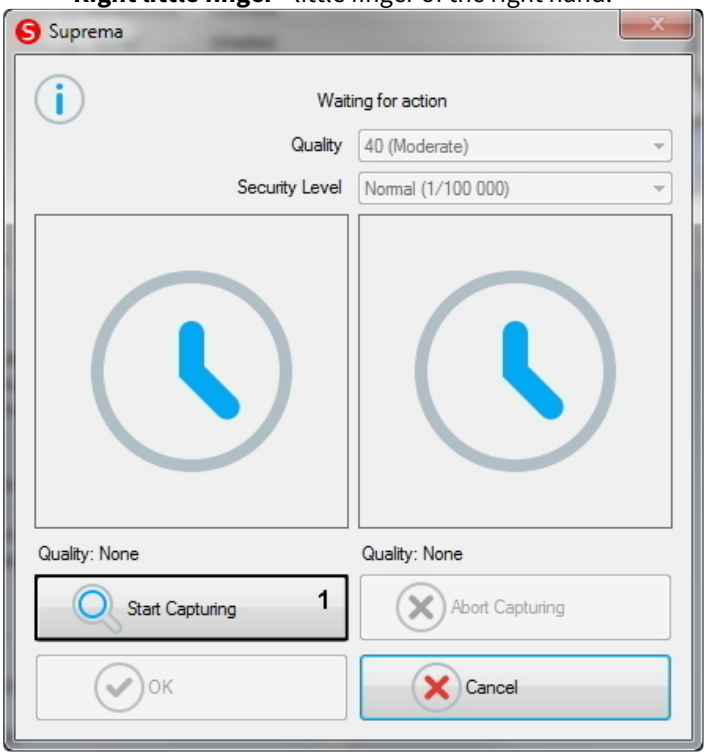
The **Suprema. Capture fingerprints** window will open.



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.

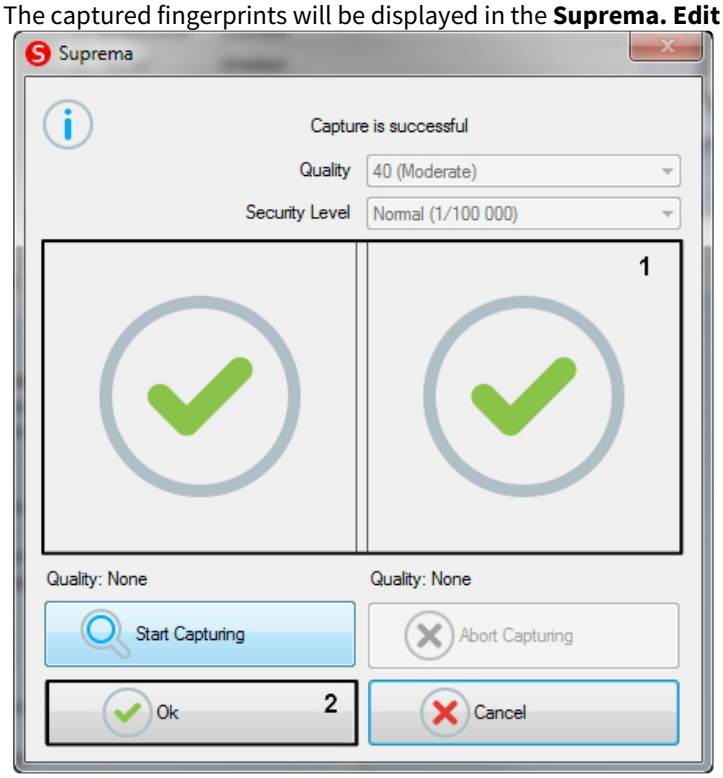
> **Note**
>
> To capture fingerprints, each finger or group of fingers should be placed on the reader twice with 5 seconds delay after pressing the **Start capturing** button and after the first capture.

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.

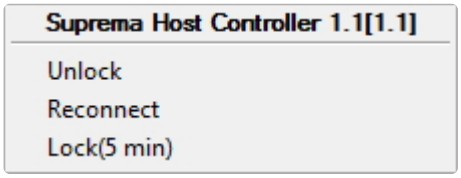
> **Note**
>
> As a result, a silent alarm will be generated when reading this fingerprint.

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* fingerprints are added.

4.3 Managing the Suprema Host Controller

The *Suprema Host Controller* is managed in the interactive **Map** window using the functional menu of the **Suprema Host Controller** object.

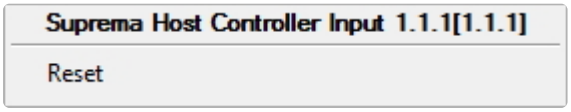


The commands of the functional menu are described in the table.

Command	Description
Unlock	Unlock the controller
Reconnect	Reconnect to the controller
Lock (5 min)	Lock the controller for 5 minutes

4.4 Managing the Suprema Host Controller Input

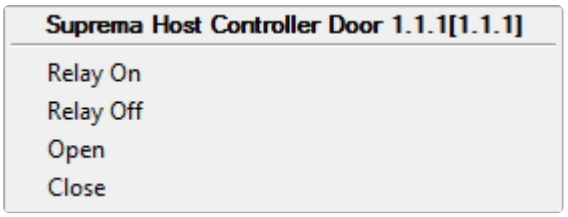
The *Suprema Host Controller Input* is managed in the interactive **Map** window using the functional menu of the **Suprema Host Controller Input** object.



Select the **Reset** command to reset the input.

4.5 Managing the Suprema Host Controller Door

The *Suprema Host Controller Door* is managed in the interactive **Map** window using the functional menu of the **Suprema Host Controller Door** object.

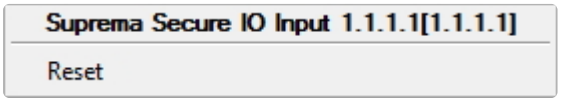


The commands of the functional menu are described in the table.

Command	Description
Relay On	Turn on the relay
Relay Off	Turn off the relay
Open	Open the door
Close	Close the door

4.6 Managing the Suprema Secure IO Input

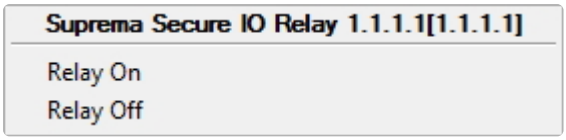
The *Suprema Secure IO Input* is managed in the interactive **Map** window using the functional menu of the **Suprema Secure IO Input** object.



Select the **Reset** command to reset the input.

4.7 Managing the Suprema Secure IO Relay

The *Suprema Secure IO Relay* is managed in the interactive **Map** window using the functional menu of the **Suprema Secure IO Relay** object.

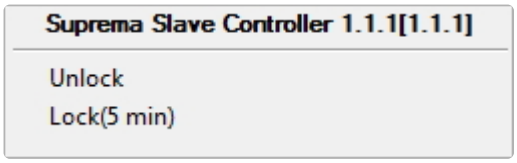


The commands of the functional menu are described in the table.

Command	Description
Relay On	Turn on the relay
Relay On	Turn off the relay

4.8 Managing the Suprema Slave Controller

The *Suprema Slave Controller* is managed in the interactive **Map** window using the functional menu of the **Suprema Slave Controller** object.



The commands of the functional menu are described in the table.

Command	Description
Unlock	Unlock the controller
Lock (5 min)	Lock the controller for 5 minutes

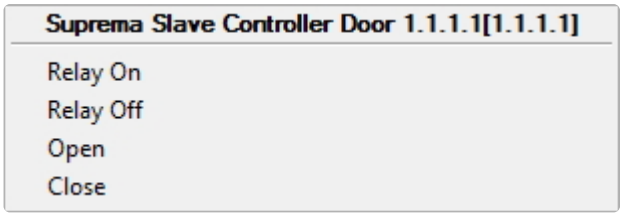
4.9 Managing the Suprema Slave Controller Input

The *Suprema Slave Controller Input* is managed in the interactive **Map** window using the functional menu of the **Suprema Slave Controller Input** object.

Select the **Reset** command to reset the input configuration.

4.10 Managing the Suprema Slave Controller Door

The *Suprema Slave Controller Door* is managed in the interactive **Map** window using the functional menu of the **Suprema Slave Controller Door** object.



The commands of the functional menu are described in the table.

Command	**Description**
Relay On	Turn on the relay
Relay Off	Turn off the relay
Open	Open the door
Close	Close the door