Virdi Integration Module Settings Guide

ACFA PSIM 1.9

Last update 27/03/2026

Table of Contents

1 Introduction into Virdi Module Settings Guide

On the page:

1.1 Purpose of the document

This *Virdi Module Settings Guide* is a reference manual designed for *Virdi* 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 *Virdi* integration module;
2. configuration of the *Virdi* integration module;
3. working with the *Virdi* integration module.

1.2 General information about the Virdi integration module

The *Virdi* 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 *Virdi* hardware;
2. Interaction between the *Virdi hardware* and the *ACFA PSIM* Software System.

Note.

Detailed information about the *Virdi* ACS is presented in the official documentation for this system (manufactured by Union Community Co. Ltd).

Before configuration the *Virdi* ACS integration module, do the following:

1. Install the *Virdi* hardware on the protected territory (for details, see the *Virdi* guide).
2. Connect the *Virdi* ACS hardware to the *Axxon PSIM* Server (for details, see the *Virdi* guide).

2 Supported hardware and licensing of the Virdi integration module

Manufacturer	Union Community Co. Ltd 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea E-mail: sales@virditech.com Web site: https://www.virditech.com
Integration type	SDK
Equipment connection	Ethernet

Supported equipment

Equipment	Function	Features
MCP-040	Controller	• CPU: 32-bit RISC (ARM Cortex-M3 Core) • Memory: 8 MB • Zone Interface: 8 zones (each is a dual-use port) • Maximum number of schedules: 1024 • Maximum number of users: 50,000 • Network: 10/100M Ethernet • Maximum number of doors: 4 • Ringer Interface: Monitored Ringer/Siren Port (1 port) • Number of Events: 51,200 • Communication Port: RS485 Reader Port / Wiegand Input Ports • Programmable Inputs / Outputs
The terminals of AC series	Terminal	AC-7000 AC-5100 AC-2200 AC-2100 AC-2000 AC-1100 AC-6000 Detailed information is given in the official documentation of the corresponding terminal manufacturer (Union Community Co. Ltd).

Equipment	Function	Features
The terminals of UBio-X series	Terminal	UBio-X Pro Lite UBio-X Iris UBio-X Slim UBio-X Face UBio-X Pro2 UBio-X Pro Detailed information is given in the official documentation of the corresponding terminal manufacturer (Union Community Co. Ltd).
FOH02	Control reader	Fingerprints Cards: RF: 125KHz proximity card SC: 13. 56 MHz smart card

Licensing

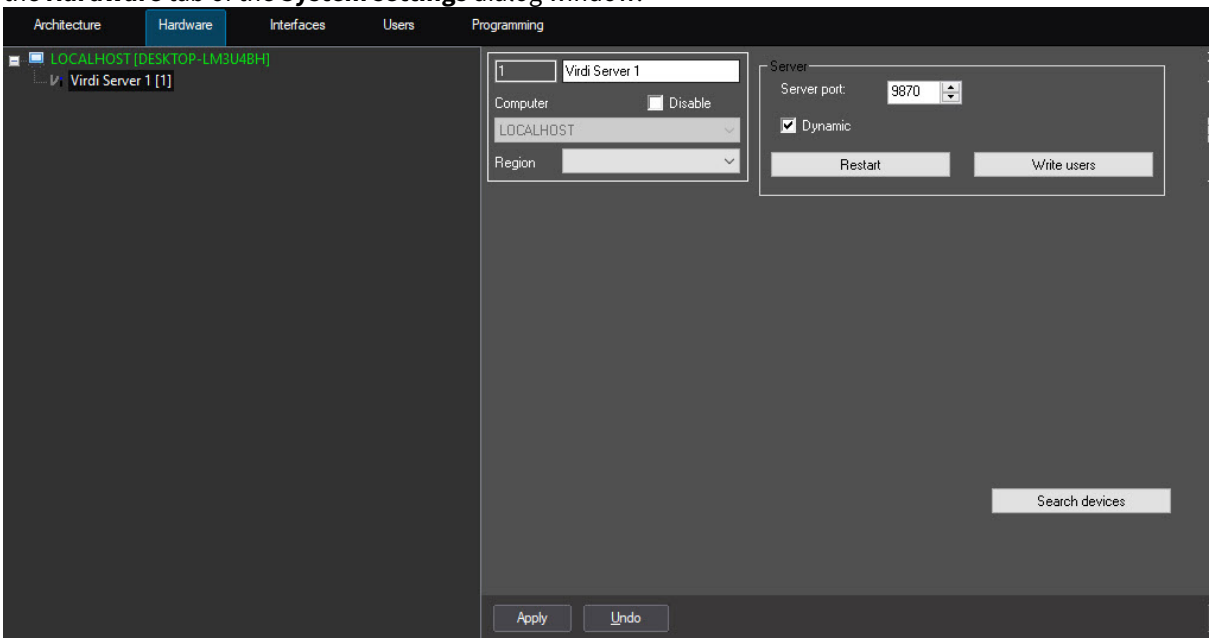
Per 1 controller/terminal.

3 Configuration of the Virdi integration module

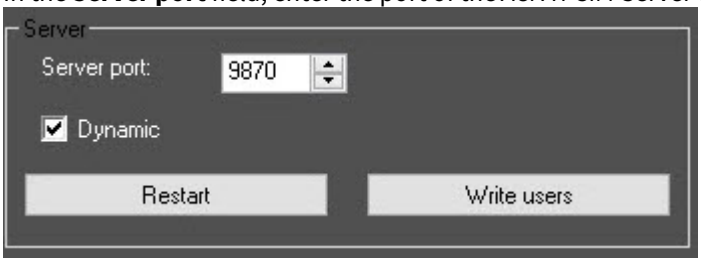
3.1 Configuring the Virdi ACS connection

The *Virdi* ACS connection is configured as follows:

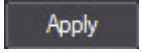
1. Go to the settings panel of the **Virdi Server** object, which is created on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog window.



2. In the **Server port** field, enter the port of the *ACFA PSIM* Server to which the *Virdi ACS* is connected.



3. Set the **Dynamic** checkbox if it is necessary to automatically send the changes in employees, access rights or time zones to the corresponding controllers and readers for which these changes are made.
4. Click the **Restart** button if it is necessary to reconnect to all controllers and readers.
5. Click the **Write users** button if it is necessary to write the users to all controllers and readers.
6. Click the **Search devices** 

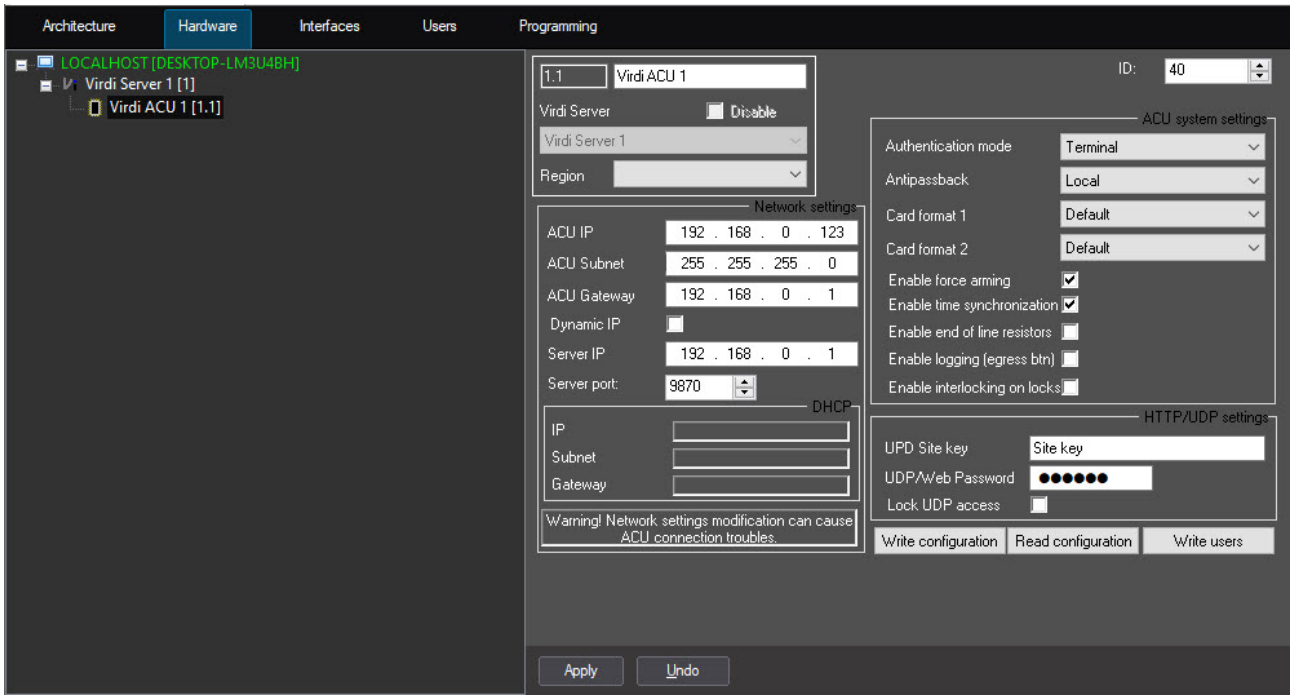
button to find all devices connected to the Server and build an objects tree corresponding to the configuration.
7. Click the **Apply** 

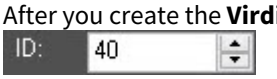
button to save the changes.

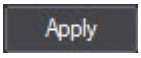
3.2 Configuring the Virdi Controller

3.2.1 Setting up the Virdi controller

The Virdi controller is set up on the settings panel of the **Virdi ACU** object, which is created on the basis of the **Virdi Server** object.



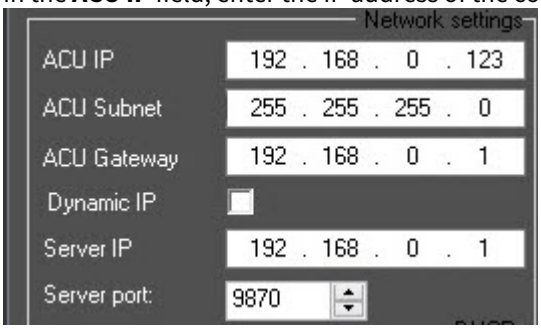
1. After you create the **Virdi ACU** object, it is necessary to specify the identifier of this controller in the **ID** field.


2. Click the **Apply** 

button.

Setting up the Virdi ACU network connection

The *Virdi ACU* connection is configured as follows:

1. In the **ACU IP** field, enter the IP address of the controller.


2. In the **ACU Subnet** field, enter the subnet mask of the controller.
3. In the **ACU Gateway** field, enter the controller gateway.
4. Set the **Dynamic IP** checkbox if the controller operates in a network with the DHCP protocol.
5. In the **Server IP** field, enter the IP address of the *ACFA PSIM* Server.

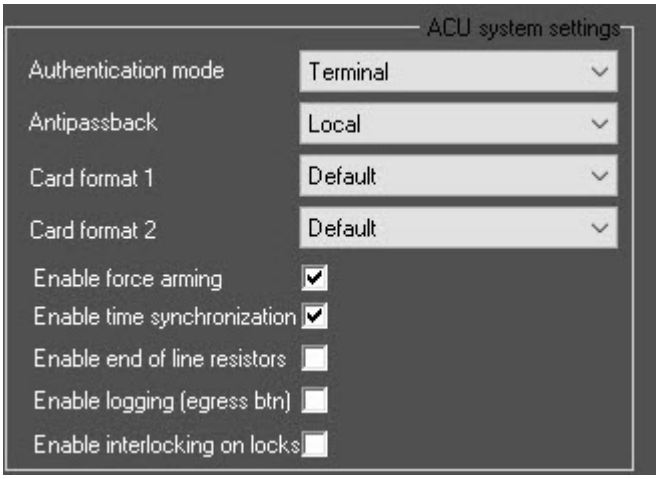
6. In the **Server port** field, enter the port of the *ACFA PSIM* Server.
7. Click the **Apply** Apply button to apply the settings.

Virdi ACU system settings

The system settings of the *Virdi* controller are set up as follows:

1. From the **Authentication mode** drop-down list, select the mode of authentication and controller operation:
   - **Server/Terminal**—the decisions are made by the Server, and if it is not available, then by the controller.
   - **Terminal/Server**—the decisions are made by the controller, and if it is not available, then by the Server.
   - **Server**—the decisions are made by the Server.
   - **Terminal**—the decisions are made by the controller.
   - **Offline mode**—the offline mode of the controller.

   > **Note**
   >
   > In the offline mode, the controller cannot be managed from the *ACFA PSIM* Server.

2. From the **Antipassback** drop-down list, select the double-entry control mode:
   - **Local**—the antipassback is controlled by the controller.
   - **Server**—the antipassback is controlled by the Server.
3. From the **Card format 1** and **Card format 2** drop-down lists, select the format for displaying the access cards data:
   - **Default**—standard.
   - **Hexademical**—hexadecimal.
   - **Decimal**—decimal.
   - **3:5 Decimal**—3 or 5 decimal digits.
4. Set the **Enable force arming** checkbox if it is necessary to enable the forced arming of the zone, even if the zone has open doors.
5. Set the **Enable time synchronization** checkbox if it is necessary to enable the time synchronization on the Server and controller.
6. Set the **Enable end of line resistors** checkbox if it is necessary to enable the terminal resistors.
7. Set the **Enable logging (egress btn)** checkbox if it is necessary to log all events by clicking the EXIT buttons.
8. Set the **Enable interlocking on locks** checkbox if it is necessary to activate the dual locking of all doors.
9. Click the **Apply** Apply button to apply the settings.

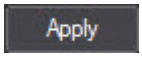
Managing the Virdi ACU configuration

The *Virdi* controller configuration is managed as follows:

1. Click the **Write configuration** 

button to write the current configuration to the controller.
2. Click the **Read configuration** 

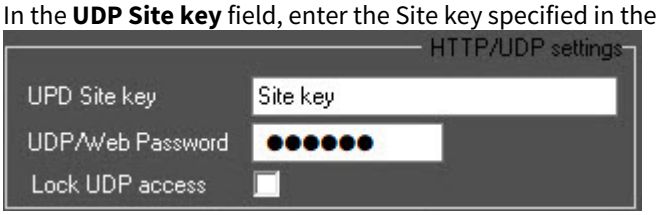
button to read the controller configuration.
3. Click the **Write users** 

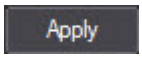
button to send the users to the controller.
4. Click the **Apply** 

button to apply the settings.

Setting up the Web-Server connection of the Virdi ACU

The *Virdi* ACU connection to the Web-Server is configured as follows:

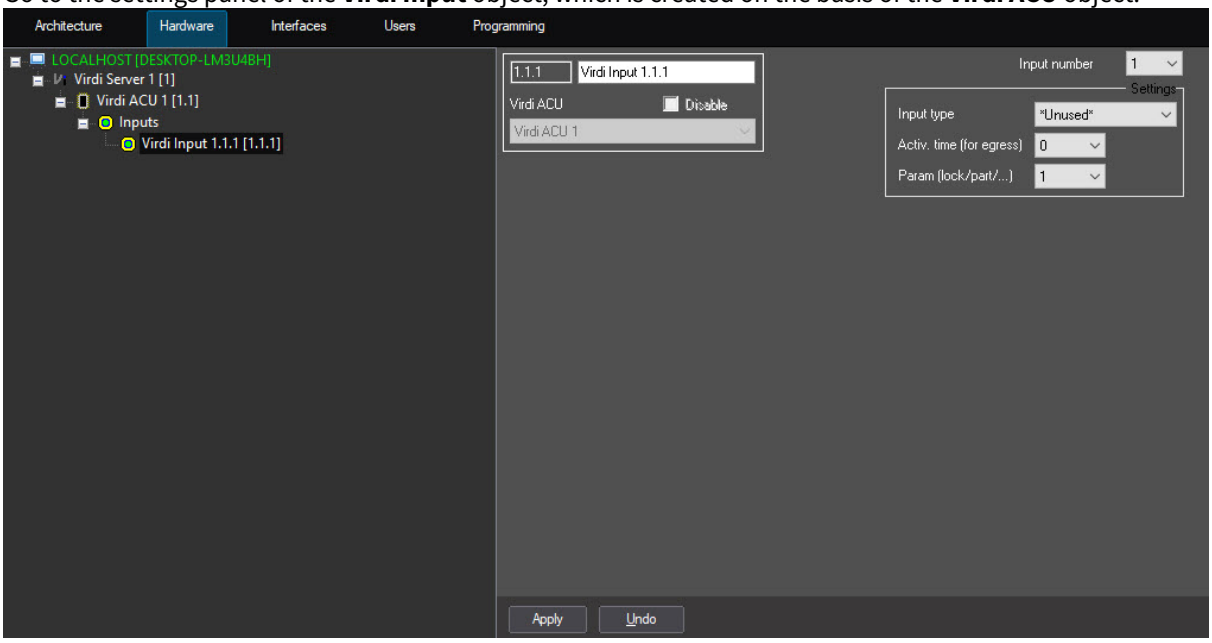
1. In the **UDP Site key** field, enter the Site key specified in the controller settings.


2. In the **UDP/Web Password** field, enter the controller password.
3. Set the **Lock UDP access** checkbox if it is necessary to disable the ability to set up the controller via the Web-Interface.
4. Click the **Apply** 

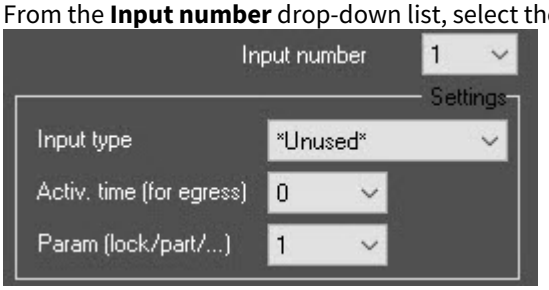
button to apply the settings.

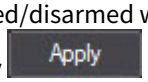
3.2.2 Setting up the Virdi Input

The *Virdi* input is configured as follows:

1. Go to the settings panel of the **Virdi Input** object, which is created on the basis of the **Virdi ACU** object.


2. From the **Input number** drop-down list, select the input number from **1** to **4**.



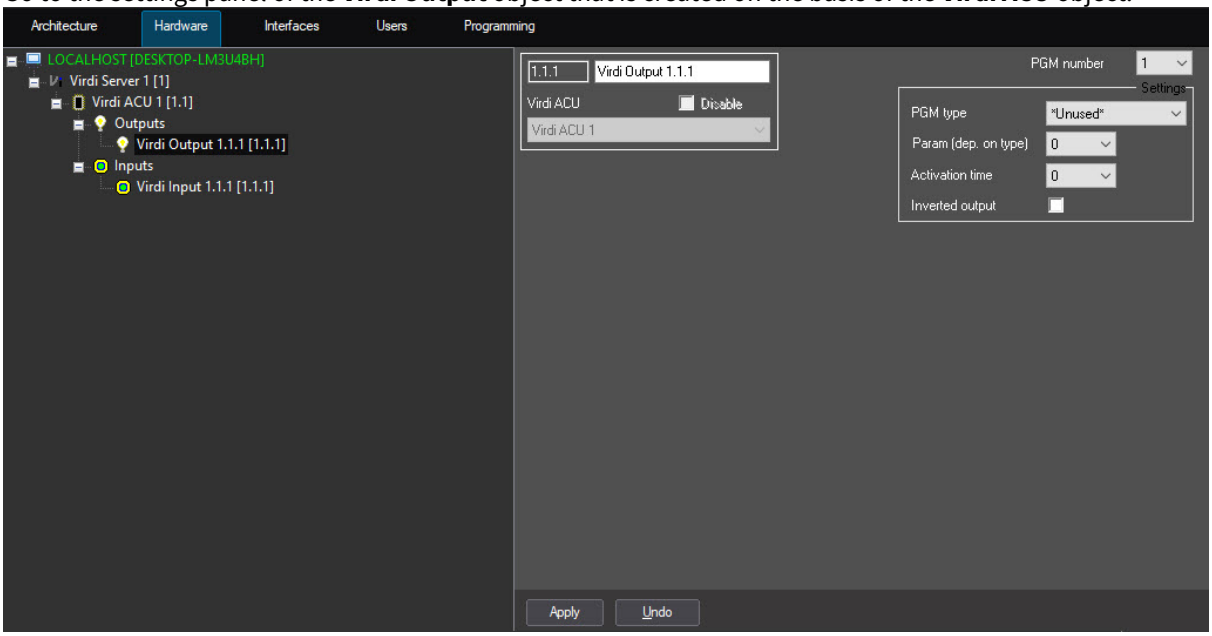
3. From the **Input type** drop-down list, select the input type:
   - **Unused**—not used.
   - **Egress (NC)**—input with normally-closed contacts.
   - **Egress (NO)**—input with normally-open contacts.
   - **Fire (NC)**—fire input with normally-closed contacts.
   - **Fire (NO)**—fire input with normally-open contacts.
   - **Security (NC)**—security input with normally-closed contacts.
   - **Security (NO)**—security input with normally-open contacts.
4. From the **Activ. time (for egress)** drop-down list, select the time in seconds during which the door will be opened when the **Egress (NC)** or **Egress (NO)** input is triggered: from **0** to **255**.
5. In the **Param (lock/part/...)** drop-down list:
   - If the input type **Egress (NC)** or **Egress (NO)** is selected, then select the number of the door that will be opened when this input is activated: from **1** to **4**.
   - If the input type **Fire (NC)** or **Fire (NO)** is selected, then select the section number in which the fire alarm will be triggered when this input is activated: from **1** to **4**.
   - If the input type **Security (NC)** or **Security (NO)** is selected, then select the partition number that will be armed/disarmed when this input is activated: from **1** to **4**.
6. Click the **Apply** 

button to apply the settings.

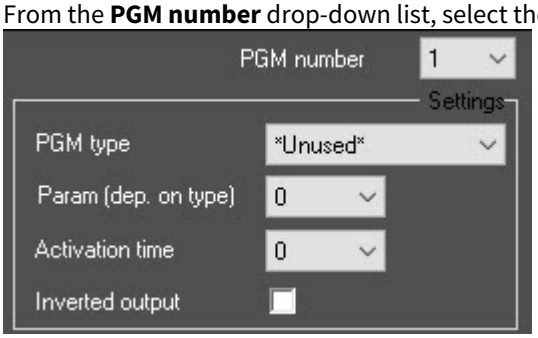
3.2.3 Setting up the Virdi Output

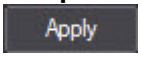
The *Virdi* output is configured as follows:

1. Go to the settings panel of the **Virdi Output** object that is created on the basis of the **Virdi ACU** object.



2. From the **PGM number** drop-down list, select the output number from **1** to **8**.



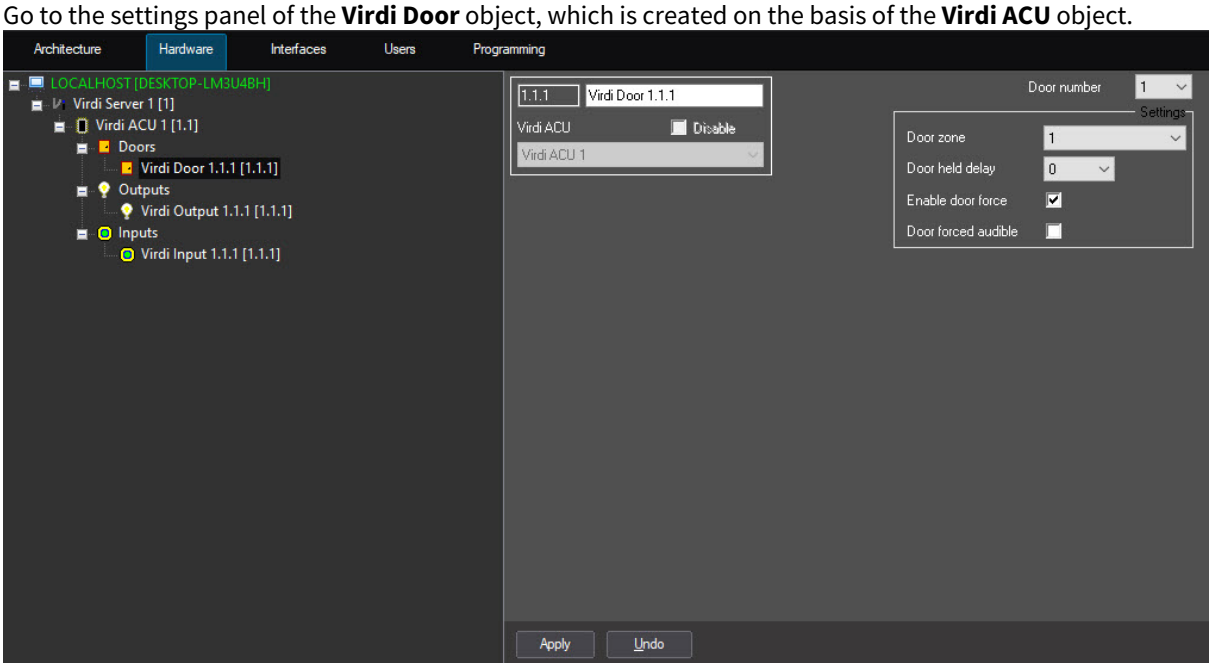
3. From the **PGM type** drop-down list, select the output type:
   - **Unused**—not used.
   - **Matching success**—triggers after successful authorization of a user.
   - **Matching failed**—triggers after an unsuccessful authorization of a user.
   - **Scheduled output**—works according to the assigned schedule.
   - **Alarm output**—triggers when an alarm is activated.
   - **System troubles**—triggers when a problem occurs in the system, for example, a problem with the battery, a problem with the reader, and so on.
   - **Arm/disarm status**—triggers when a region becomes armed/disarmed.
   - **Fire alarm**—triggers when a fire alarm is activated.
   - **Silent alarm**—triggers when a silent alarm is activated.
   - **Open too long**—triggers when the door is open for too long.
   - **Door forced**—triggers when the door is held by force.
4. In the **Param (dep. on type)** drop-down list:
   - if the **Matching success** or **Matching failed** output type is selected, then select the door number that will be opened when the corresponding output is triggered: from **1** to **4**.
   - if the **Alarm output**, **Fire alarm**, or **Silent alarm** output type is selected, then select the section number in which the alarm will be triggered when the corresponding output is triggered: from **1** to **4**.
   - if the **Scheduled output** output type is selected, then select the schedule number according to which the corresponding output will operate: from **0** to **255**.
5. From the **Activation time** drop-down list, select the time in seconds for which the output will be activated: from **0** to **255**.
6. Set the **Inverted output** checkbox if it is necessary to invert the output.
7. Click the **Apply** 

button to apply the settings.

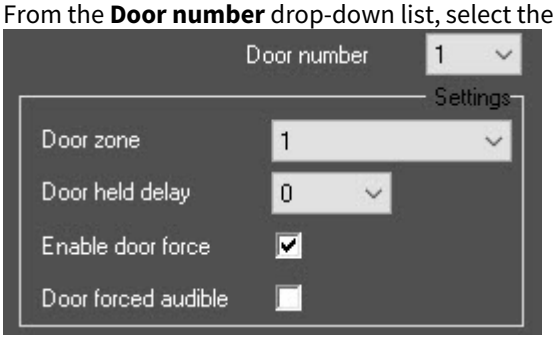
3.2.4 Setting up the Virdi Door

The *Virdi* door is configured as follows:

1. Go to the settings panel of the **Virdi Door** object, which is created on the basis of the **Virdi ACU** object.

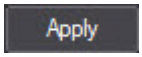


2. From the **Door number** drop-down list, select the entry number from **1** to **4**.



3. From the **Door zone** drop-down list, select the zone to which this door will belong:
   - ***Unassigned***—zone is not assigned.
   - from **1** to **8**.
4. From the **Door held delay** drop-down list, select the time in seconds after which the open door will be considered as held: from **0** to **255**.

> **Note**
>
> - The total time until the door hold alarm is activated is considered as follows: **Open time** (see Setting up the Virdi Reader) + **Door held delay** time.
> - To receive this alarm, the type of zone to which this door belongs must be **Exit1**, **Exit2**, **Instant**, or **Interior**.

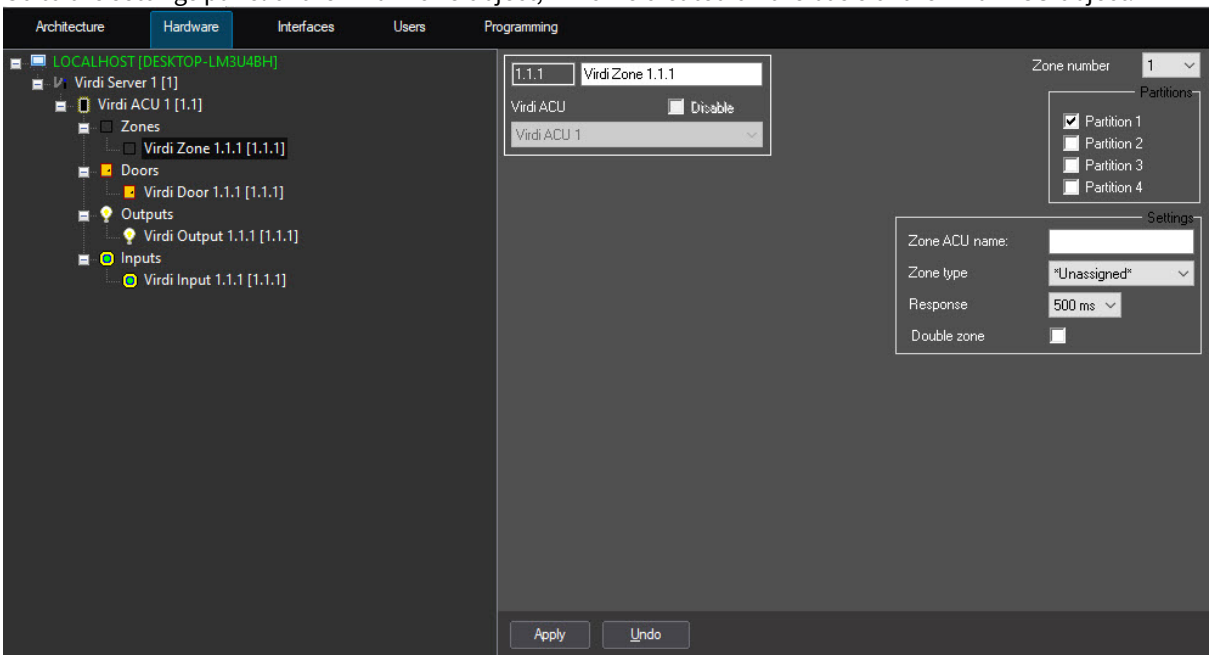
5. Set the **Enable door force** checkbox if it is necessary to monitor the holding of the door.
6. Set the **Door forced audible** checkbox if it is necessary to generate a visual and audible alarm on the reader of this door if the door is held.
7. Click the **Apply** 

button to apply the settings.

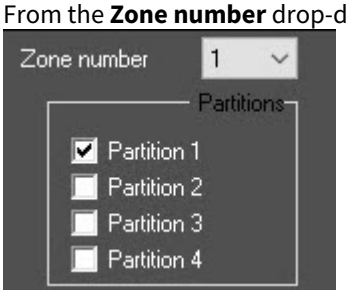
3.2.5 Setting up the Virdi Zone

The *Virdi* zone is configured as follows:

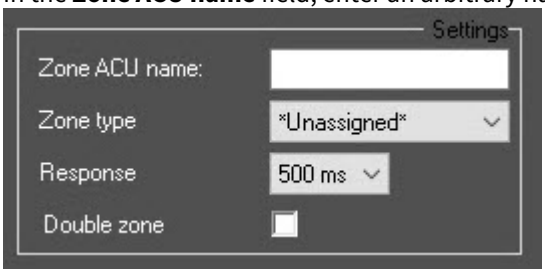
1. Go to the settings panel of the **Virdi Zone** object, which is created on the basis of the **Virdi ACU** object.



2. From the **Zone number** drop-down list, select the zone number from **1** to **8**.



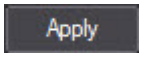
3. Set the checkboxes next to the partitions that must be included in this zone.
4. In the **Zone ACU name** field, enter an arbitrary name for this zone (no more than 10 characters).



5. From the **Zone type** drop-down list, select the zone type:
   - ***Unused***—not used.
   - **Exit1**—this zone type has a time delay for entry and exit, which is set on the *Virdi* partition settings panel in the **Entry delay 1** and **Exit delay 1** parameters respectively (see Setting up the Virdi Partition).
   - **Exit2**—this zone type has a time delay for entry and exit, which is set on the *Virdi* partition settings panel in the **Entry delay 2** and **Exit delay 2** parameters respectively (see Setting up the Virdi Partition).
   - **Instant**—this zone type is used when monitoring the zone perimeter. This zone type has no time delay and will immediately activate an alarm if the zone partition is armed and the zone is open.
   - **Interior**—this zone type is used when monitoring the internal area of the zone and has a time delay for entry and exit, which is set on the *Virdi* partition settings panel in the **Entry delay** and **Exit delay**

parameters, respectively. If the partition is armed and there is no delay for entry and exit, this zone will immediately activate an alarm.

- **24H Emergency**—this zone type is always active, regardless of whether the partition is armed or not. This zone type is intended for alarming and monitoring.
- **24H Silent panic**—this zone type is always active, regardless of whether the partition is armed or not. This zone type is intended for monitoring purposes only.
- **Fire**—this zone type monitors the fire alarms and malfunctions. A fire alarm occurs if the fire zone is closed, and a malfunction occurs if the fire zone is disabled.
- **Arm/Disarm**—when this zone is open or closed, the controller can be armed/disarmed using the external button or a signal.
- ***Unassigned***—not assigned.

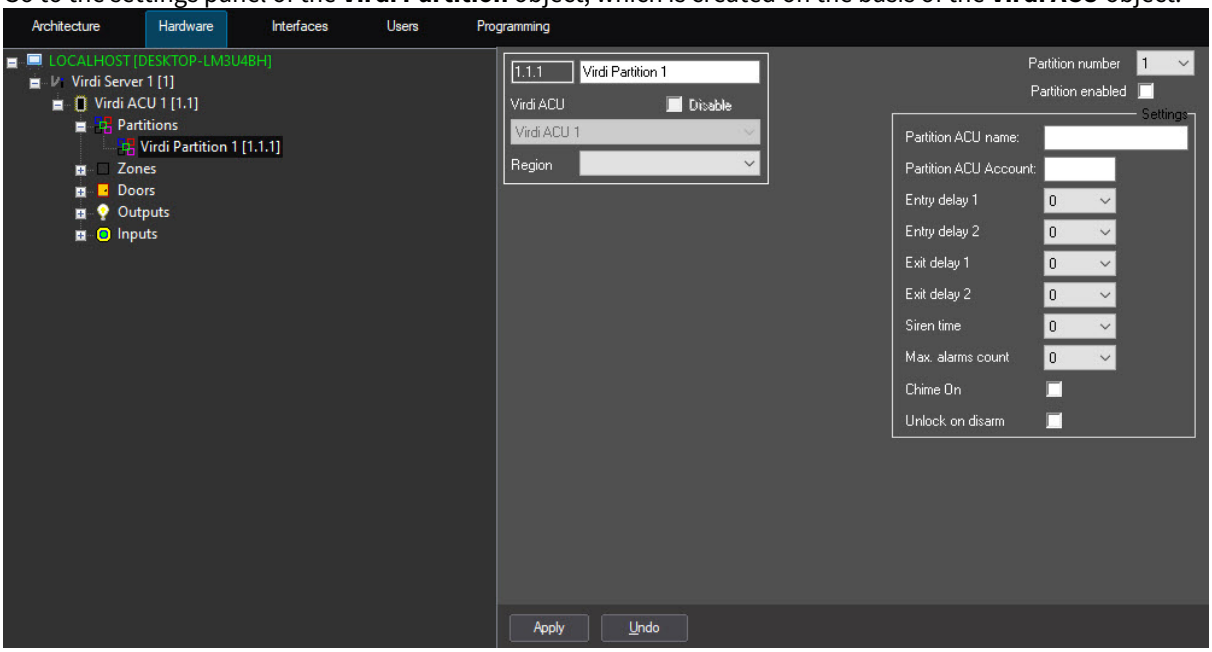
6. From the **Response** drop-down list, select the response time of the zone status change in seconds. If the zone becomes open/closed within this time, then the state of the zone will change: **500 ms** or **100 ms**.
7. Set the **Double zone** checkbox if the zones require more than four hardware inputs.
8. Click the **Apply** 

button to apply the settings.

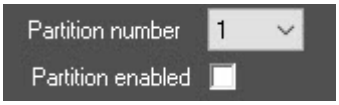
3.2.6 Setting up the Virdi Partition

The *Virdi* Partition is configured as follows:

1. Go to the settings panel of the **Virdi Partition** object, which is created on the basis of the **Virdi ACU** object.

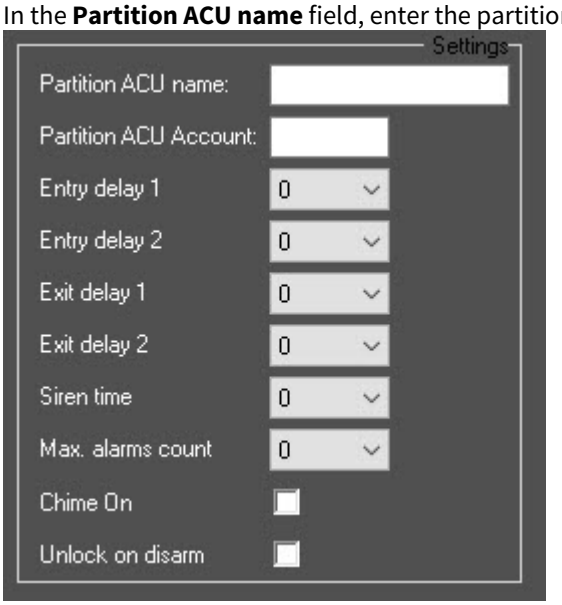


2. From the **Partition number** drop-down list, select the partition number from **1** to **4**.



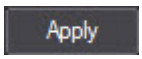
3. Set the **Partition enabled** checkbox to activate this partition.

4. In the **Partition ACU name** field, enter the partition name (maximum 16 characters).



5. In the **Partition ACU Account** field, enter the partition account number in the form of four hexadecimal digits. By default, the account number matches the controller ID.
6. From the **Entry delay 1** and **Entry delay 2** drop-down lists, select the time delay in seconds for the entry: from **0** to **255**.
7. From the **Exit delay 1** and **Exit delay 2** drop-down lists, select the time delay in seconds for the exit: from **0** to **255**.

> **Note**
>
> - **Entry delay 1** and **Exit delay 1** affect all zones of **EXIT1** type.
> - **Entry delay 2** and **Exit delay 2** affect all zones of **EXIT2** type.

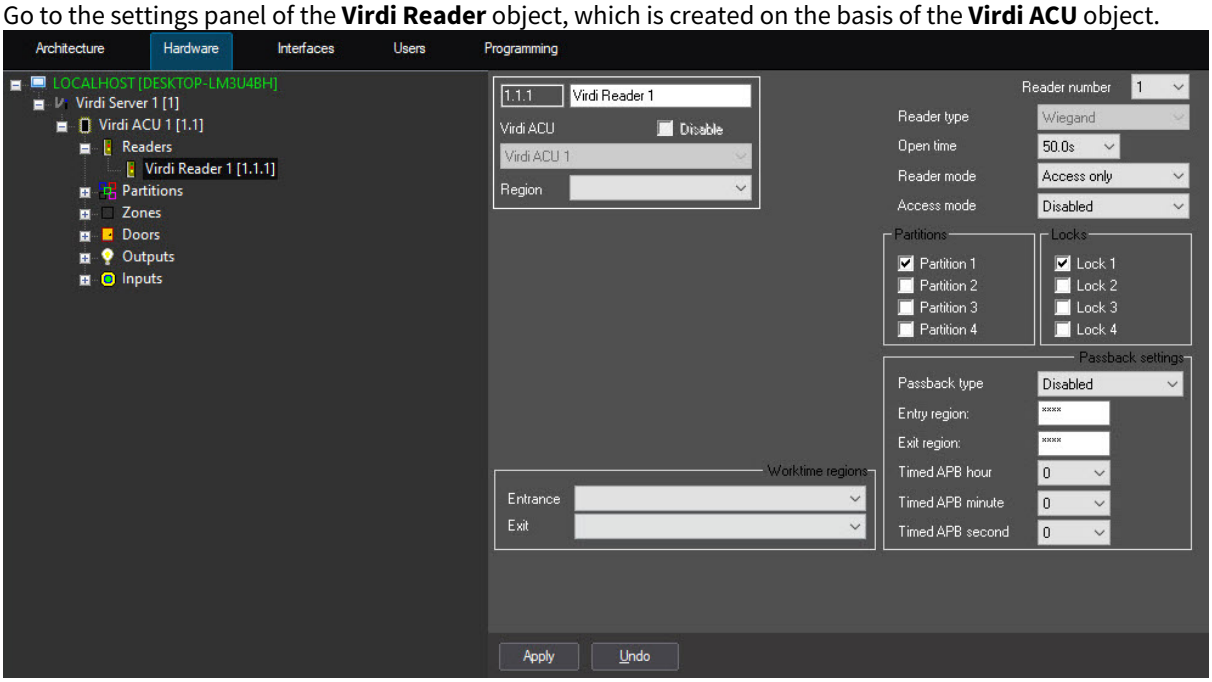
8. From the **Siren time** drop-down list, select the duration of the siren signal in seconds when an alarm occurs in the alarm section: from **0** to **255**.
9. From the **Max. alarms count** drop-down list, select the maximum number of the siren repetitions when an alarm occurs in the alarm section: from **0** to **255**.
10. Set the **Chime On** checkbox if it is necessary for the reader to make two short beeps when opening a zone such as **EXIT1**, **EXIT2**, or **INSTANT** and the partitions assigned to them. This can be used as an indicator of door opening, but not as an alarm indicator.
11. Set the **Unlock on disarm** checkbox if it is necessary for the doors belonging to this partition to be automatically unlocked when the partition is disarmed. Doors will remain open until the partition is armed again.
12. Click the **Apply** 

button to apply the settings.

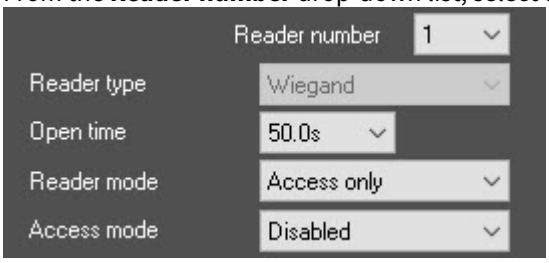
3.2.7 Setting up the Virdi Reader

The *Virdi* reader is configured as follows:

1. Go to the settings panel of the **Virdi Reader** object, which is created on the basis of the **Virdi ACU** object.



2. From the **Reader number** drop-down list, select the reader number from **1** to **12**.



> **Note**
>
> The **Reader type** drop-down list indicates the type of reader. This parameter value cannot be changed.

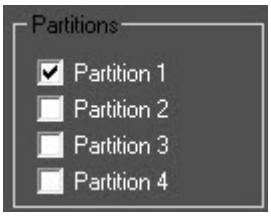
3. From the **Open time** drop-down list, select the time in seconds for which the door will be open after successful user authentication: from **1s** to **255s**.
4. From the **Reader mode** drop-down list, select the access grant mode:
   - **Access only**—after successful user authentication, the door assigned to the reader will be open for the time specified in the **Open time** parameter.
   - **Access + Security**—after successful user authentication, the door assigned to the reader will be open for the time specified in the **Open time** parameter. If the F1 key is pressed on the controller, then after successful user authentication, the partition assigned to the reader and user will be automatically armed. If the partition is already armed, it will be automatically disarmed and the door will be unlocked.

     > **Note**
     >
     > If the **Access + Security** mode is selected, then user authentication will be performed in **Offline mode**, regardless of the specified controller authentication mode (see Virdi ACU system settings).

5. From the **Access mode** drop-down list, select the access mode:

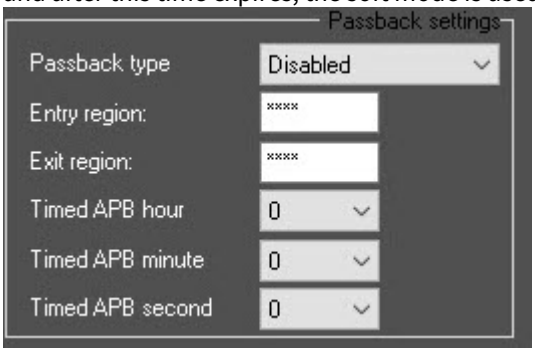
- **Disabled**—mode is disabled.
- **Enter**—enter.
- **Exit**—exit.
- **Out**—from the territory.
- **In**—to the territory.

6. Set the checkboxes next the partitions to which this reader will belong.



7. Set the checkboxes next to the doors to which this reader will belong.

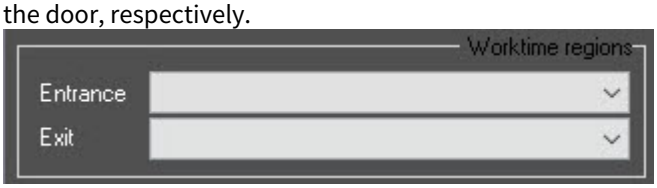
8. From the **Passback type** drop-down list, select the antipassback control mode:
   - **Disabled**—mode is disabled.
   - **Hard Passback** (strict)—re-entering the zone is prohibited until one leaves the zone.
   - **Soft Passback** (soft)—repeated access is not prohibited, but in this case, a corresponding event is generated.
   - **Timed Passback** (temporary)—strict mode is used during the specified time after entering the zone, and after this time expires, the soft mode is used.

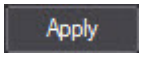


> **Note**
>
> **Timed Passback** is not available if antipassback is controlled by the Server (see Virdi ACU system settings).

9. In the **Entry region** field, enter an arbitrary name of the region for the entering (maximum four characters). Depending on the selected antipassback control mode, the user will be prohibited or allowed to enter the specified region again (it is necessary for this region name to be indicated at least in two readers).
10. In the **Exit region** field, enter an arbitrary name of the region for the exiting (maximum four characters). Depending on the selected antipassback control mode, the user will be prohibited or allowed to leave the specified region again (it is necessary for this region name to be indicated at least in two readers).
11. If the **Timed Passback** antipassback control mode is selected, then from the **Timed APB hour** drop-down list, select the time in hours during which the strict mode will be used.

12. If the **Timed Passback** antipassback control mode is selected, then from the **Timed APB minute** drop-down list, select the time in minutes during which the strict mode will be used.
13. If the **Timed Passback** antipassback control mode is selected, then from the **Timed APB second** drop-down list, select the time in seconds during which the strict mode will be used.
14. From the **Entrance** and **Exit** drop-down lists, select the partitions located on the entrance and exit sides of the door, respectively.

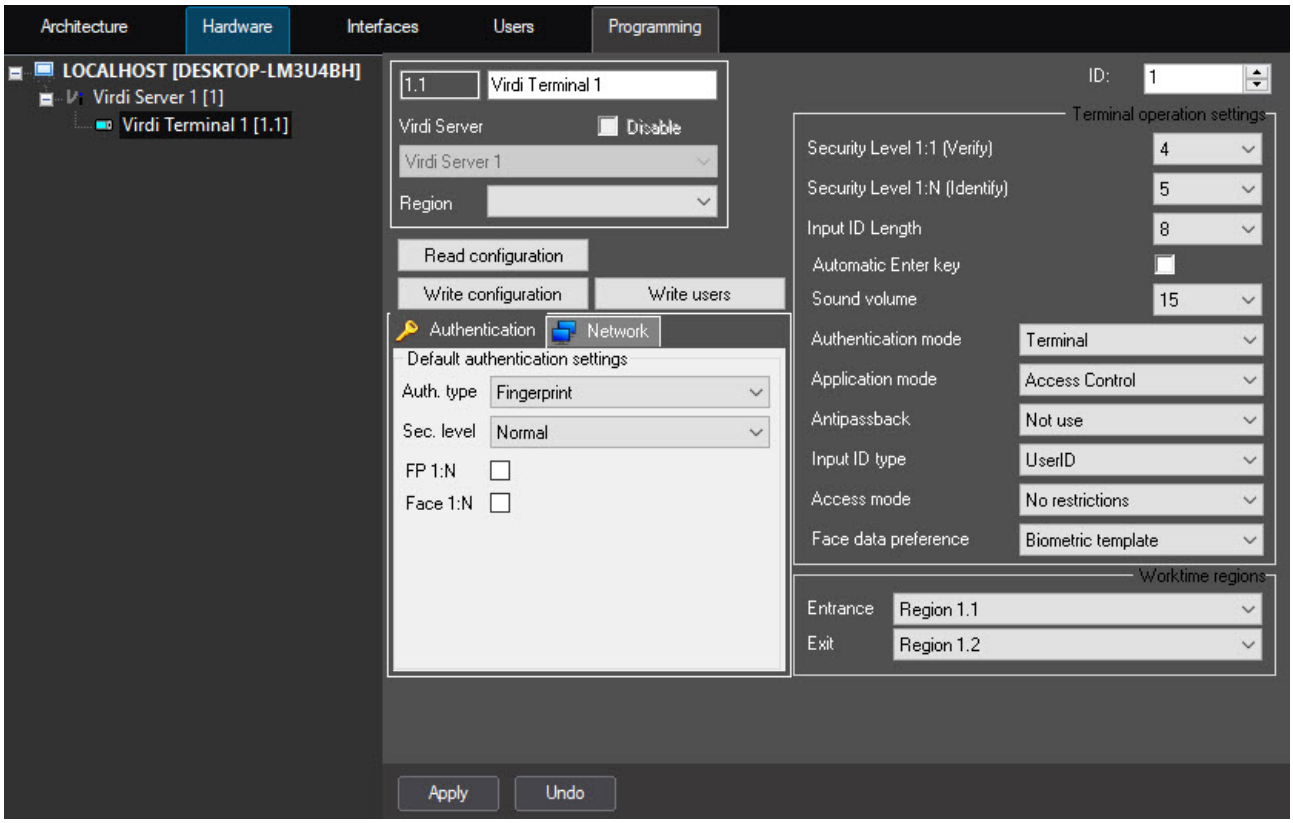


15. Click the **Apply**  button to apply the settings.

3.3 Configuring the Virdi Terminal

You can configure the *Virdi* terminal on the settings panel of the **Virdi Terminal** object that is created on the basis of the **Virdi Server** object.

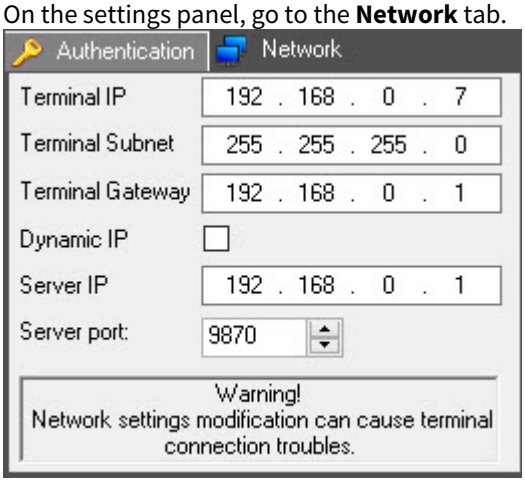
After you create the **Virdi Terminal** object, you must specify the identifier of this terminal in the **ID** field and click the **Apply** button.

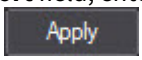


3.3.1 Setting up the network connection of the Virdi Terminal

The *Virdi* terminal connection is configured as follows:

1. On the settings panel, go to the **Network** tab.



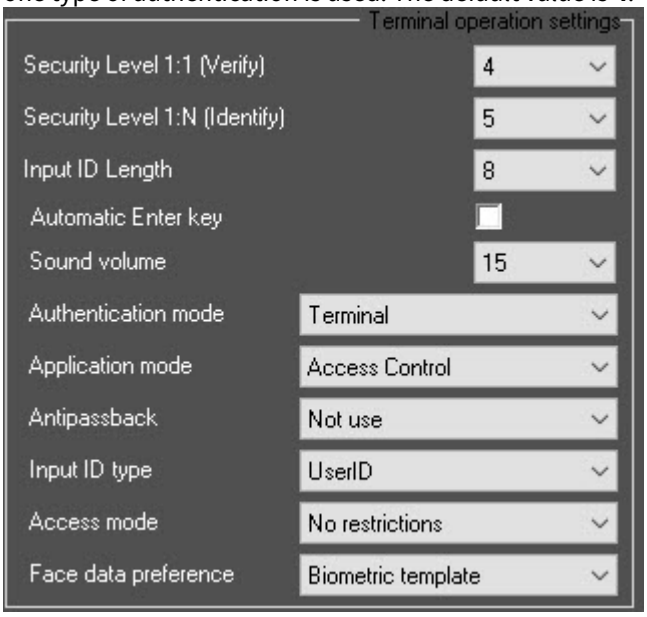
2. In the **Terminal IP** field, enter the IP address of the terminal.
3. In the **Terminal Subnet** field, enter the terminal subnet mask.
4. In the **Terminal Gateway** field, enter the terminal gateway.
5. Set the **Dynamic IP** checkbox if the terminal operates in a network with the DHCP protocol.
6. In the **Server IP** field, enter the IP address of the *ACFA PSIM* server.
7. In the **Server port** field, enter the port of the *ACFA PSIM* server.
8. Click the **Apply**  button to apply the settings.

Setting up the network connection of the Virdi Terminal is complete.

3.3.2 The system settings of the Virdi Terminal

The system settings of the *Virdi* Terminal are configured as follows:

1. From the **Security Level 1:1 (Verify)** drop-down list, select the verification quality level from **1** to **9** if only one type of authentication is used. The default value is **4**.



2. From the **Security Level 1:N (Identify)** drop-down list, select the authentication quality level from **1** to **9** if several authentication types are used. The default value is **5**.
3. From the **Input ID Length** drop-down list, select the user ID length from **4** to **8** characters.

> **Attention!**
>
> To ensure the terminal operation with *ACFA PSIM*, it is necessary to select **8**. Also, the **Input ID Length** must be set to **8** in the terminal.

4. Set the **Automatic Enter key** checkbox to enable the automatic key entry from the terminal keyboard (F1-F4 buttons).
5. From the **Sound volume** drop-down list, select the terminal speaker volume level from **0** to **20**.
6. From the **Authentication mode** drop-down list, select the mode of authentication and terminal operation:
   - **Server/Terminal**—the decisions are made by the server, and if it is not available, then by the terminal.
   - **Terminal/Server**—the decisions are made by the terminal, and if it is not available, then by the server.
   - **Server**—the decisions are made by the server.
   - **Terminal**—the decisions are made by the terminal.
   - **Offline mode**—the offline mode of the terminal.

   > **Note**
   >
   > In the offline mode, the terminal cannot be managed from the *ACFA PSIM* server.
7. From the **Application mode** drop-down list, select the terminal operating mode:
   - **Access Control**—access point mode.

     > **Attention!**
     >
     > To ensure the terminal operation with *ACFA PSIM*, it is necessary to select the **Access Control** operation mode.
   - **Time/Attendance**—working time tracking mode.
   - **Drinking Water**—breathalizers compatibility mode.
8. From the **Antipassback** drop-down list, select the double-entry control mode:
   - **Not use**—not used.
   - **Access when disconnected**—allow entry if the connection with the server is lost.
   - **Prohibit when disconnected**—prohibit entry if the connection with the server is lost.
9. From the **Input ID type** drop-down list, select the type of user identifiers:
   - **UserID**—custom user identifiers.
   - **UniqueID**—unique user identifiers specified in the terminal.
10. From the **Access mode** drop-down list, select the access mode provided by the terminal if there is no keyboard for entering numbers on the terminal:
    - **No restrictions**—no restrictions.
    - **Only fingers and password**—only fingerprints and password.
11. From the **Face data preference** drop-down list, select the preferred data for biometric user authentication. If the required data isn't available, other data is used.
    - **Biometric template**—the saved biometric template of the user is used.
    - **Person photo**—the photo of the user's face from the *Access Manager* is used.

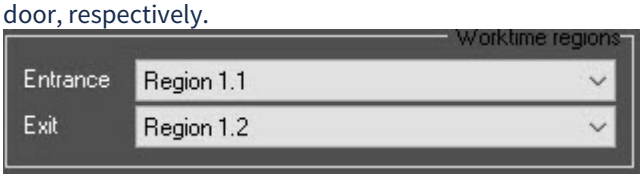
    > **Note**
    >
    > Not all terminal models support the feature of selecting data for biometric user authorization.
12. Click the **Apply** button to apply the settings.

Configuration of the system settings of the *Virdi* Terminal is complete.

3.3.3 Setting up the Virdi Terminal worktime regions

The *Virdi* Terminal worktime regions are configured as follows:

1. From the **Entrance** and **Exit** drop-down lists, select the regions located on the entrance and exit sides of the door, respectively.



2. Click the **Apply** button to apply the settings.

Setting up the *Virdi* Terminal worktime regions is complete.

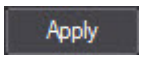
3.3.4 Managing the configuration of the Virdi Terminal

The *Virdi* Terminal configuration is managed as follows:

1. Click the **Read configuration** 

button to read the terminal configuration.
2. Click the **Write configuration** 

button to write the current configuration to the terminal.
3. Click the **Write users** 

button to send the users to the terminal.
4. Click the **Apply** 

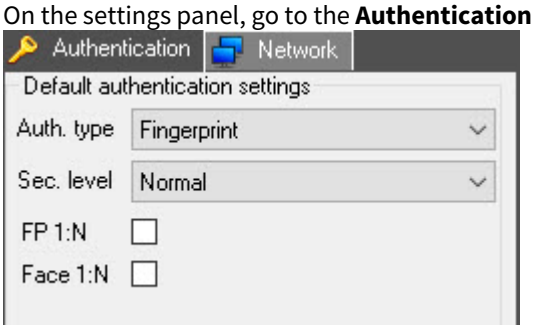
button to apply the settings.

> **Note**
>
> When users are sent to the terminal (step 3), they are assigned the default access type specified in the *Virdi* terminal settings on the **Authentication** tab (see Configuration of authentication). If the access type is changed, the change will take effect after writing the new configuration to the terminal (step 2) and updating the user/department with users with unassigned *Virdi* access types in the *Access Manager*. To update the user, open the edit mode and, without making any changes, click the **Save** button (see Going to user editing).

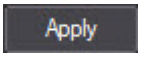
3.3.5 Configuration of authentication

The authentication parameters of the *Virdi* terminal user are configured as follows:

1. On the settings panel, go to the **Authentication** tab.



2. From the **Auth. type** drop-down list, select the default authentication type. The selected access type is used to write users to the *Virdi* terminal (see Managing the configuration of the Virdi Terminal).

3. From the **Sec. level** drop-down list, select the default required authentication quality level from **Lowest** to **Highest**.
4. Set the **FP 1:N** checkbox so that the fingerprint is requested first, and then it is checked against the entire fingerprint database of the device. The check can take a long time, depending on the number of fingerprints in the database.
5. Set the **Face 1:N** checkbox so that the face is recognized first, and then this face is checked against the entire face database of the device. The check can take a long time, depending on the number of faces in the database.
6. To save the changes, click the **Apply** 

button.

4 Working with the Virdi integration module

4.1 General information about working with the Virdi Module

The following interface objects are used for *Virdi* integration module operation:

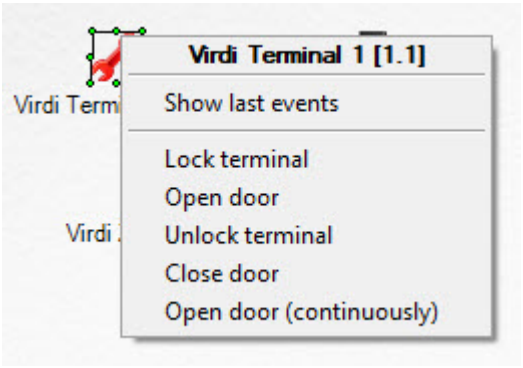
1. **Map**.
2. **Event Log**.

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 the Virdi Terminal

The *Virdi* Terminal is managed in the **Map** interactive window using the **Virdi Terminal** object function menu:



The **Virdi Terminal** object function menu commands description is given in the table.

Menu command	Function performed
Lock terminal	The terminal is locked
Open door	The door is opened
Unlock terminal	The terminal is unlocked
Close door	The door is closed
Open door (continuously)	The door is opened for a long time

The **Virdi Terminal** object can have the following states:

	Cover opened

	Disconnected
	Locked
	Closed
	Door cracked
	Door held
	Opened
	Connected

4.3 Managing the Virdi Partition

The *Virdi* Partition is managed in the **Map** interactive window using the **Virdi Partition** object function menu:

The **Virdi Partition** object function menu commands description is given in the table.

Menu command	Function performed
Arm	The partition is armed
Disarm	The partition is disarmed

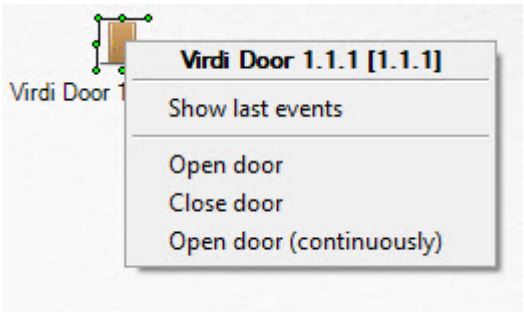
The **Virdi Partition** object can have the following states:

	Disarmed
	Armed

	Alarm

4.4 Managing the Virdi Door

The *Virdi* Door is managed in the **Map** interactive window using the **Virdi Door** object function menu:



The **Virdi Door** object function menu commands description is given in the table.

Menu command	Function performed
Open door	The door is opened
Close door	The door is closed
Open door (continuously)	The door is opened until a command to close the door is given

The **Virdi Door** object can have the following states:

	Closed
	Opened

4.5 Managing the Virdi ACU, Reader, and Zone

The *Virdi* ACU, Reader, and Zone are not managed in the **Map** interactive window.

The **Virdi ACU** object can have the following states:

	Cover opened
	Disconnected

	Connected

The **Virdi Reader** object can have the following states:

	Norm
	RS485 line error
	Unknown

The **Virdi Zone** object can have the following states:

	Norm
	Zone opened
	Zone trouble

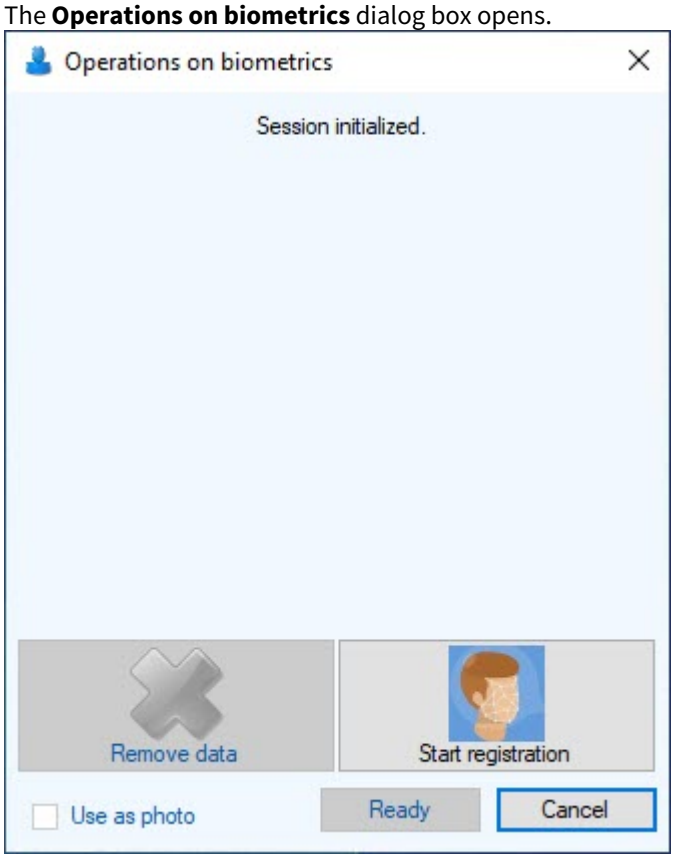
4.6 Adding the Virdi biometric parameters

4.6.1 Adding the Virdi face template

To add a *Virdi* 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 **(Virdi Faces) <Virdi Terminal Name>** that corresponds to a terminal with a biometric face reader.

3. The **Operations on biometrics** dialog box opens.



4. To add a new face template, click the **Start registration** button. Then follow the instructions on the terminal screen. In case of successful face capture, the resulting photo will be displayed, and the template of

this photo will be saved.

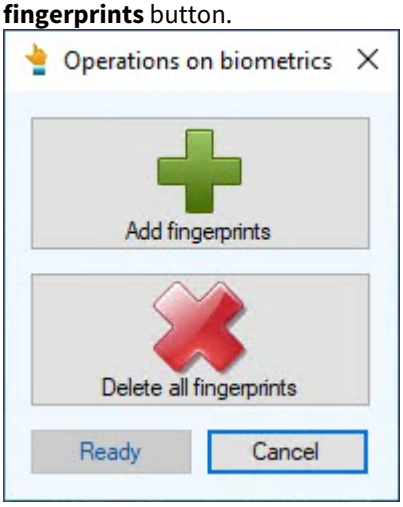
5. To use the resulting photo as a user photo, set the **Use as photo** checkbox (see Assigning a photograph to a user in the Access Manager software module).
6. To delete a face template, click the **Remove data** button.
7. Click the **Ready** button to save the face template.

4.6.2 Adding the Virdi fingerprints

To add *Virdi* 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 **(Virdi Fingerprints) <Virdi server/terminal name>** extension that corresponds to the controller with the biometric fingerprint reader connected to it, or to the terminal.

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



> **Note**
>
> To delete all fingerprint templates, click the **Delete all fingerprints** button. This button is active if there are any previously added fingerprint templates.

4. The **Virdi** dialog box will open. To continue, click the **Next** button.

5. Select the finger which you want to enroll.

6. Place your finger on the reader several times.

7. In case of successful capture, the fingerprint template will be automatically saved in the controller/terminal.

8. To add a new template, repeat the procedure. Fingers that already have a template are highlighted in green.

9. Click the **Next** button to finish adding fingerprint templates.

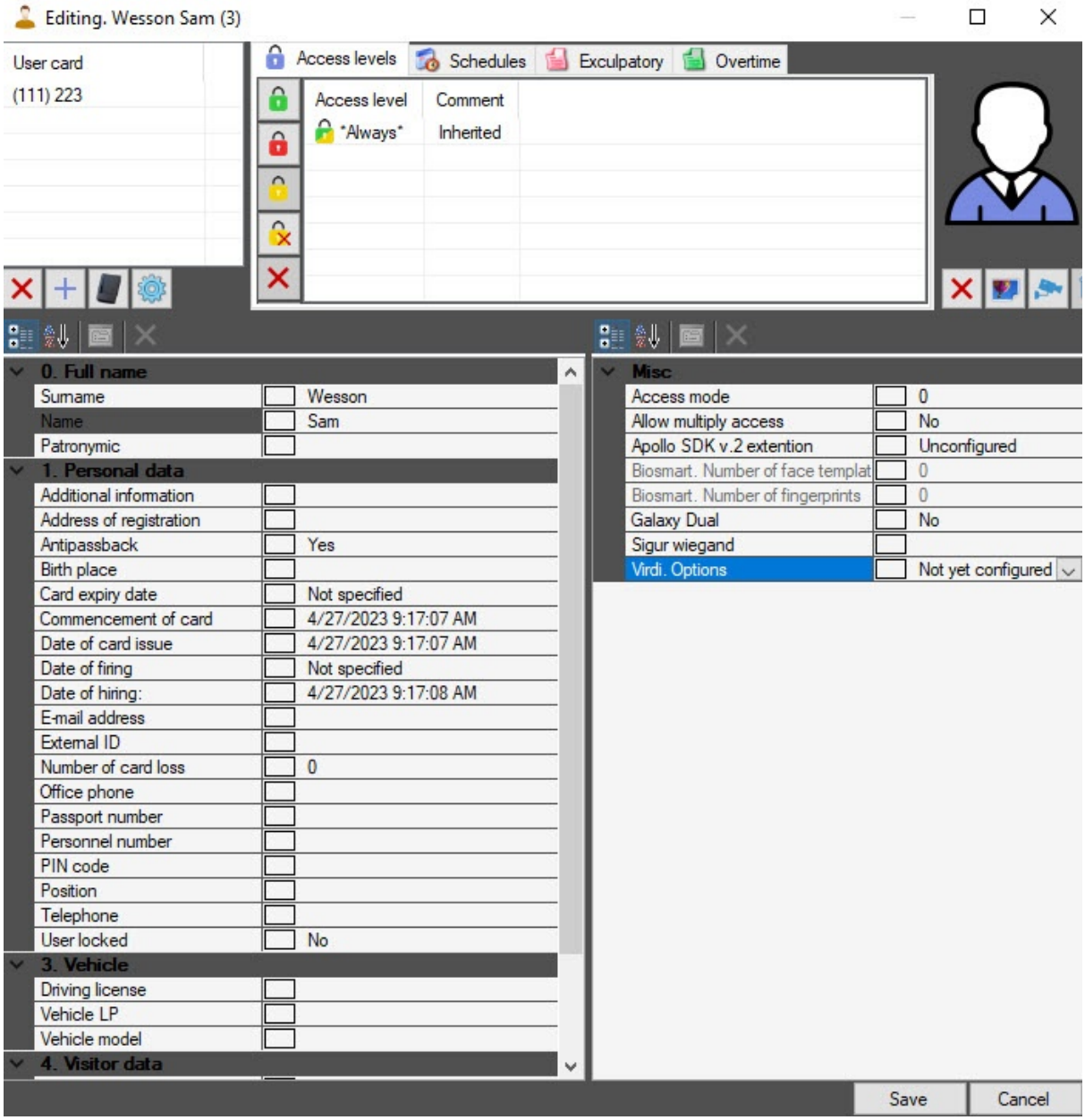
10. Click the **Finish** button to save the added fingerprints.

4.7 Working with Virdi user parameters

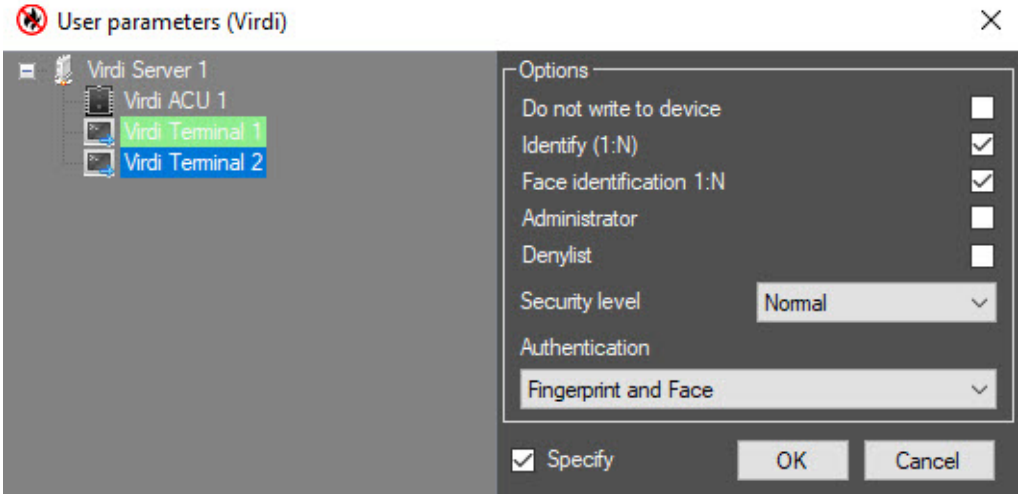
To configure the *Virdi* user parameters in *ACFA PSIM*, do the following:

1. In the *Access Manager* software module, open the user editing form (see Editing a user).

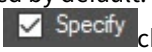
2. In the editing form that opens, select **Virdi. Options** and then click the button.



3. The **User parameters (Virdi)** form will open. In this form, select an object that you want to configure:



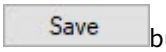
   a. **Virdi Server**;
   b. **Virdi ACU**;
   c. **Virdi Terminal**.

   Authorization of the **Virdi Server** object is enabled by default. To enable authorization of the **Virdi ACU** and **Virdi Terminal** objects, set the **Specify** 

checkbox. After that, the parameters of these objects can be set.

4. If you don't want to write the user to the device, set the **Do not write to device** checkbox. In this case, in the **Terminal** mode, the user will be considered an unknown user, and access for this user will be denied (see The system settings of the Virdi Terminal).
5. Set the **Identify (1:N)** checkbox to enable the recognition option. Depending on the selected authentication type, user biometric data can be checked with the device database during the recognition. The check may take a long time depending on the amount of data in the database.
6. Set the **Face identification 1:N** checkbox, so that the face is recognized first, and then this face is checked against the entire face database of the device. The check may take a long time depending on the number of faces in the database.
7. Set the **Administrator** checkbox to disable the settings on the device and allow only a user with the administrator role to change the settings.
8. Set the **Denylist** checkbox to enable the ability to block the user.
9. From the **Security level** drop-down list, select the required authentication quality level, from **Lowest** to **Highest**. The default value is **Normal**.
10. From the **Authentication** drop-down list, select the authentication type:
    - **Fingerprint**—only a fingerprint.
    - **Fingerprint inside card (*)**—a fingerprint attached to the card.
    - **Password**—a password only.
    - **Card**—only a card.
    - **Card or Fingerprint**—either a card or a fingerprint.
    - **Card + Fingerprint**—a combination of a card and a fingerprint.
    - **Card or Password**—either a card or a password.
    - **Card + Password**—a combination of a card and a password.
    - **(ID or Card) + Fingerprint**—a combination of a user ID or a card, and a fingerprint.
    - **(ID or Card) + Password**—a combination of a user ID or a card, and a password.
    - **Fingerprint + Password**—a combination of a fingerprint and a password.
    - **Password, if Fingerprint failed**—a password if fingerprint authentication failed.
    - **Card + Password + Fingerprint**—a combination of a card, a password, and a fingerprint.
    - **Face**—only a face.
    - **Face or Password**—either a face or a password.

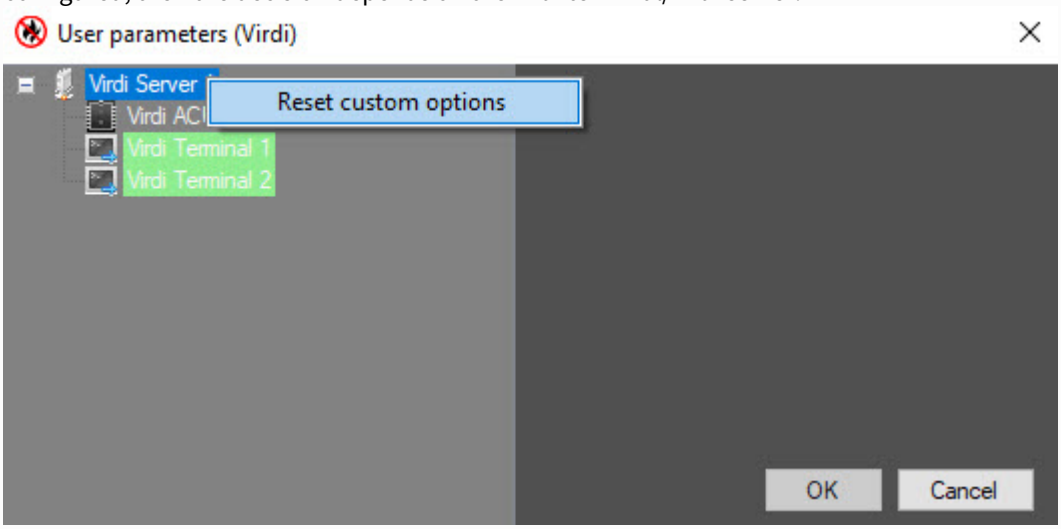
- **Card or Face**—either a card or a face.
- **Fingerprint or Face**—either a fingerprint or a face.
- **Card or Fingerprint or Face**—either a card or a fingerprint or a face.
- **Card + Face**—a combination of a card and a face.
- **(ID or Card) + Face**—a combination of a user ID or a card, and a face.
- **Fingerprint + Face**—a combination of a fingerprint and a face.
- **Face + Password**—a combination of a fingerprint and a password.
- **Card + Fingerprint + Face**—a combination of a card, a fingerprint, and a face.
- **Card + Face + Password**—a combination of a card, a face, and a password.
- **Fingerprint + Face + Password**—a combination of a fingerprint, a face, and a password.
- **Card + Fingerprint + Face + Password**—a combination of a card, a fingerprint, a face, and a password.

11. To save the changes, click the **OK** button.
12. In the *Access Manager,* in the user editing form, click the **Save** 

button to save the changes to the **Virdi. Options** parameter.

Note

Devices with user authentication settings are highlighted in green in the hardware tree in the *Access Manager.*
If the user authentication settings of the *Virdi* user are configured in the *Access Manager,* they will have priority over the settings of the *Virdi* terminal/*Virdi* server. If the settings in the *Access Manager* are not configured, then the decision depends on the *Virdi* terminal/*Virdi* server.



To cancel the user authentication settings for a specific device, select that device and clear the **Specify** checkbox for that device.