ACFA Intellect

Virdi Integration Module Settings Guide

Last update 27/04/2020

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 Intellect* 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 Intellect* 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 Intellect* 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 *Intellect* 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 sales@virditech.com 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 entire line of AC series terminals	Terminal	Detailed information is given in the official documentation of the corresponding terminal manufacturer (Union Community Co. Ltd).
UBio-X Pro Lite	Terminal	• Max Users 500,000 • Fingerprints (Templates) FP : 1,000,000 (1:1), 200,000 (1:N), Face : 500,000 (1:1), 35,000 (1:N) • Logs 10,000,000 • Images 20,000 • Smartcard option 125khz-EM, HID Prox, HID iclass, 13.56MHz Smart Card • Interfaces RS232/RS485, Wiegand In/Out

Licensing

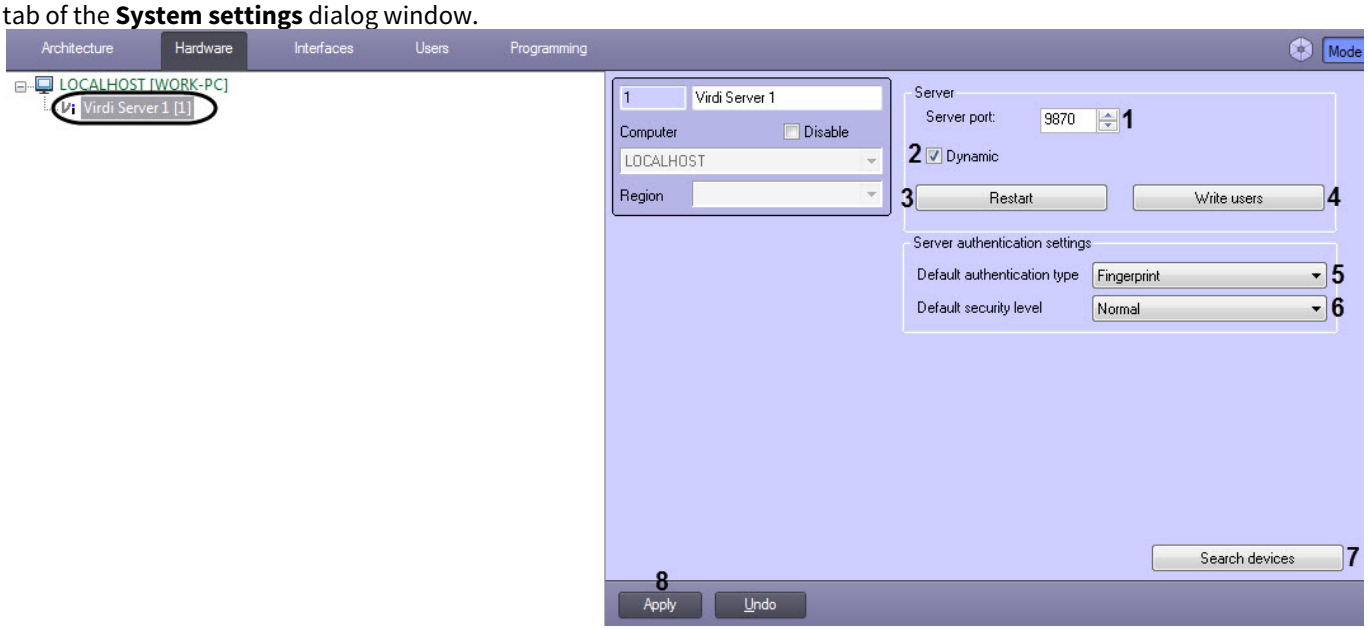
Per 1 controller/terminal.

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 (**1**), enter the port of the *ACFA-Intellect Server* to which the *Virdi ACS* is connected.
3. Set the **Dynamic** checkbox (**2**) 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. Press the **Restart** button (**3**) if it is necessary to reconnect to all controllers and readers.
5. Click the **Write users** button (**4**) if it is necessary to record the users to all controllers and readers.
6. From the **Default authentication type** drop-down list (**5**), select the default authentication type:
   - **Fingerprint** is only a fingerprint.
   - **Fingerprint in card (*)** is a fingerprint attached to the card.
   - **Fingerprint + Password** is a combination of a fingerprint and a password.
   - **Password, if Fingerprint failed** is a password if fingerprint authentication failed.
   - **Card + Password + Fingerprint** is a combination of a card, a password, and a fingerprint.
   - **Password** is a password only.
   - **Card** is only a card.
   - **Card or Fingerprint** is either a card or a fingerprint.
   - **Card + Fingerprint** is a combination of a card and a fingerprint.
   - **Card or password** is either a card or a password.
   - **Card + password** is a combination of a card and a password.
   - **(ID or Card) + Fingerprint** is a combination of a user ID or a card, and a fingerprint.
   - **(ID or Card) + Password** is a combination of a user ID or a card, and a password.
7. From the **Default security level** drop-down list (**6**), select the quality level of fingerprint verification from the lowest to the highest.
8. Click the **Search devices** button (**7**) to find all devices connected to the Server and build a tree of objects corresponding to the configuration.
9. Click the **Apply** button (**8**) to save the changes.

The Virdi ACS connection is configured.

3.2 Configuring the Virdi Controller

3.2.1 Setting up the Virdi Controller

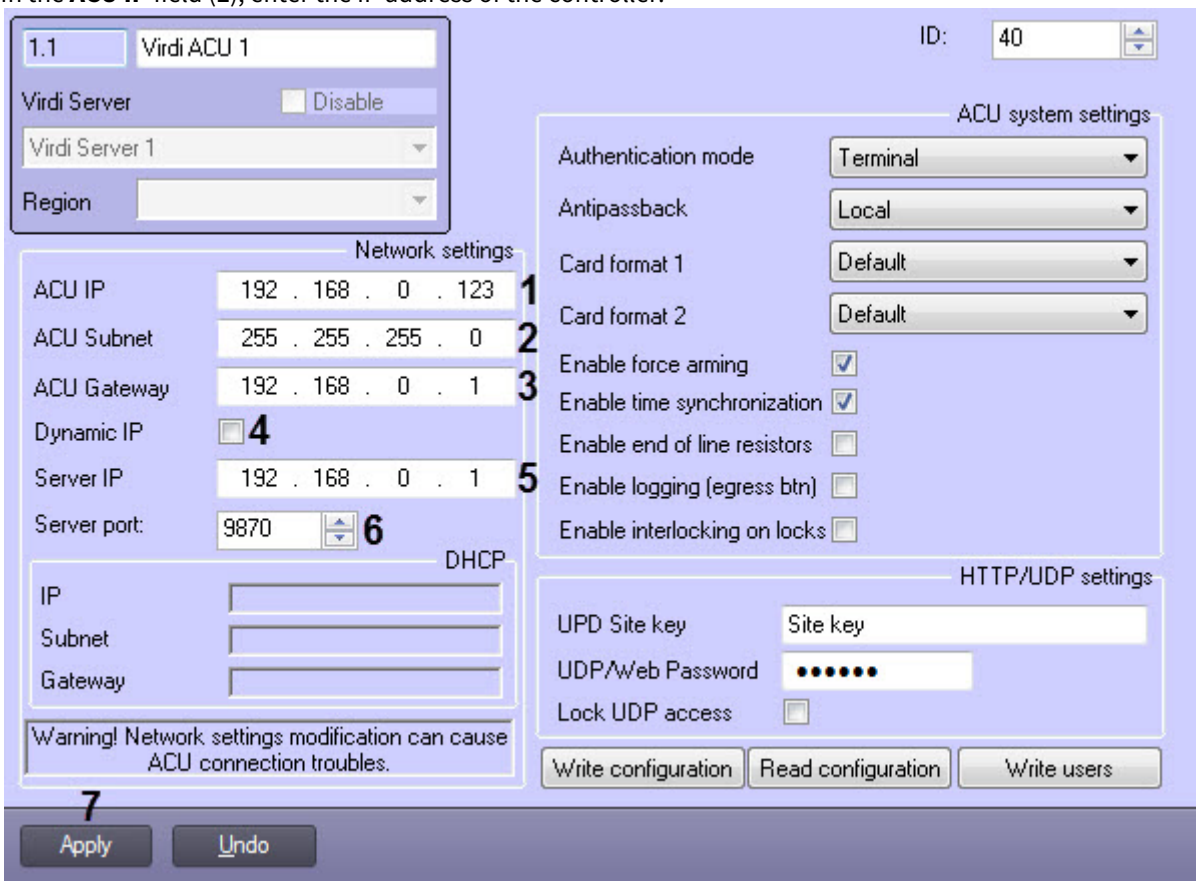
The Virdi controller is set up on the settings panel of the **Virdi ACU** object, which is created on the basis of the **Virdi Server** object.

After you create the **Virdi ACU** object, it is necessary to specify the identifier of this controller in the **ID** field (**1**) and click **Apply** (**2**).

3.2.1.1 Setting up the Virdi ACU network connection

The *Virdi ACU* connection is configured as follows:

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



2. In the **ACU Subnet** field (**2**), enter the subnet mask of the controller.
3. In the **ACU Gateway** field (**3**), enter the controller gateway.
4. Select the **Dynamic IP** check box (**4**) if the controller operates in a network with the DHCP protocol.
5. In the **Server IP** field (**5**), enter the IP address of the *ACFA-Intellect Server*.
6. In the **Server port** field (**6**), enter the port of the *ACFA-Intellect Server*.
7. Click the **Apply** button (**7**) to apply the settings.

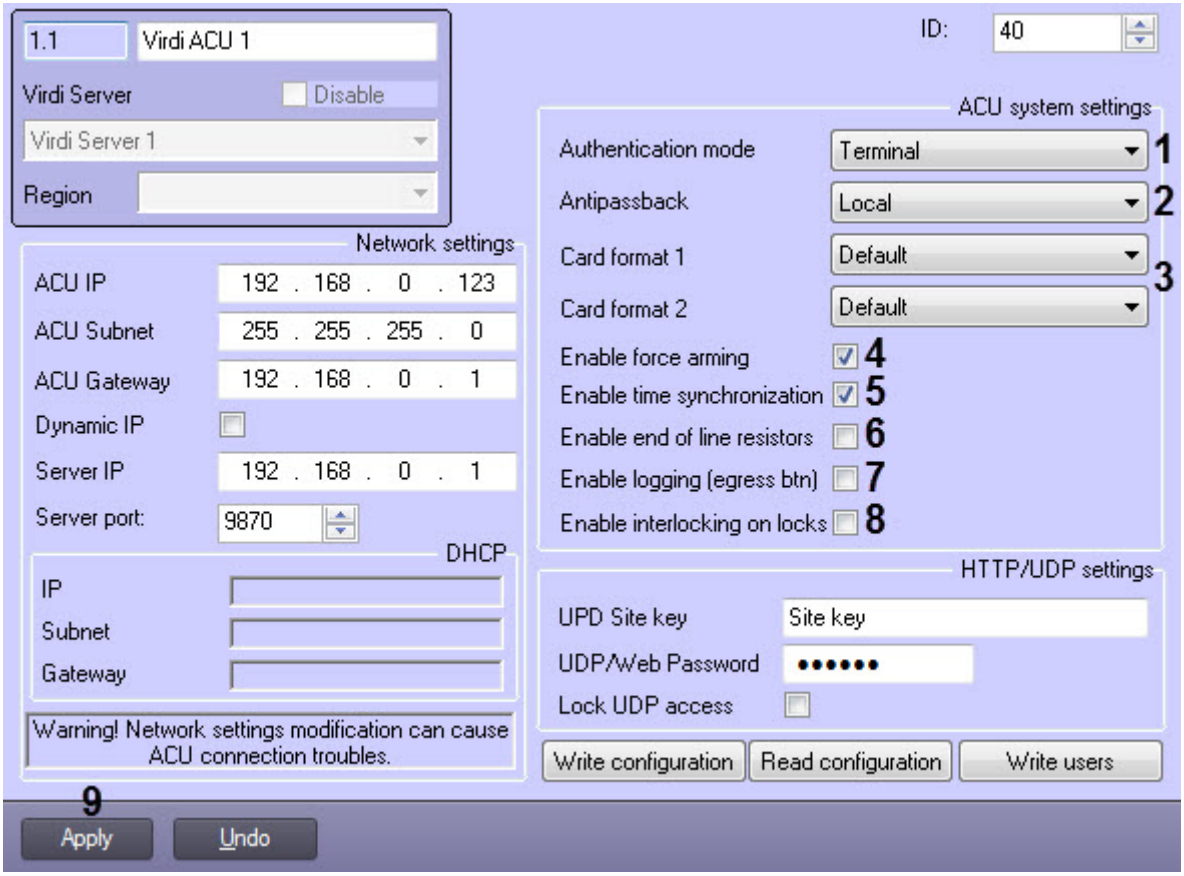
The *Virdi* controller connection is set up.

3.2.1.2 Virdi ACU system settings

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

1. From the **Authentication mode** drop-down list (**1**), 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-Intellect Server*.



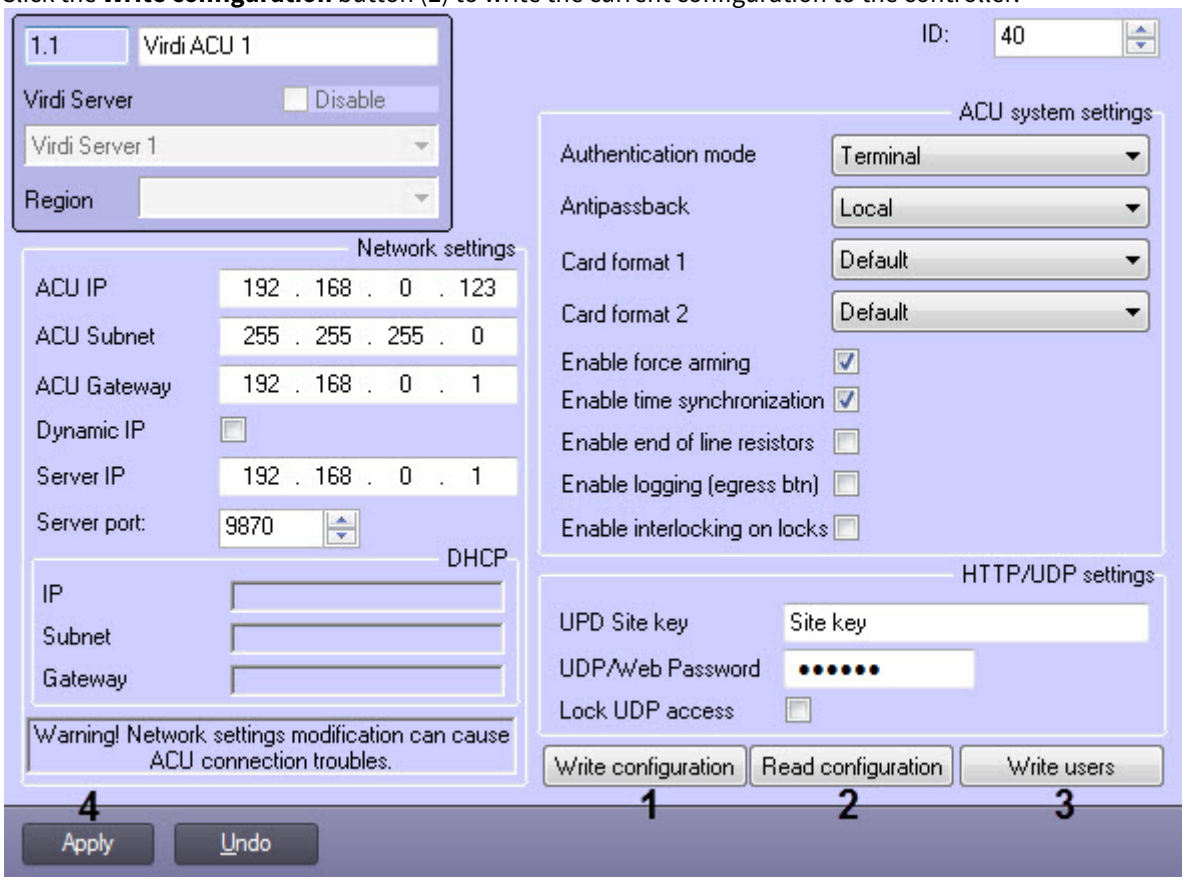
2. From the **Antipassback** drop-down list (**2**), select the double-entry control mode:
   - **Local** - the antipassback is controlled by the controller.
   - **Server** - the antipassback is controlled by the Server.
3. From the **Card format 1** and **Card format 2** drop-down lists (**3**), select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

The system settings of the Virdi controller are set up.

3.2.1.3 Managing the Virdi ACU configuration

Virdi controller configuration is managed as follows:

1. Click the **Write configuration** button (**1**) to write the current configuration to the controller.



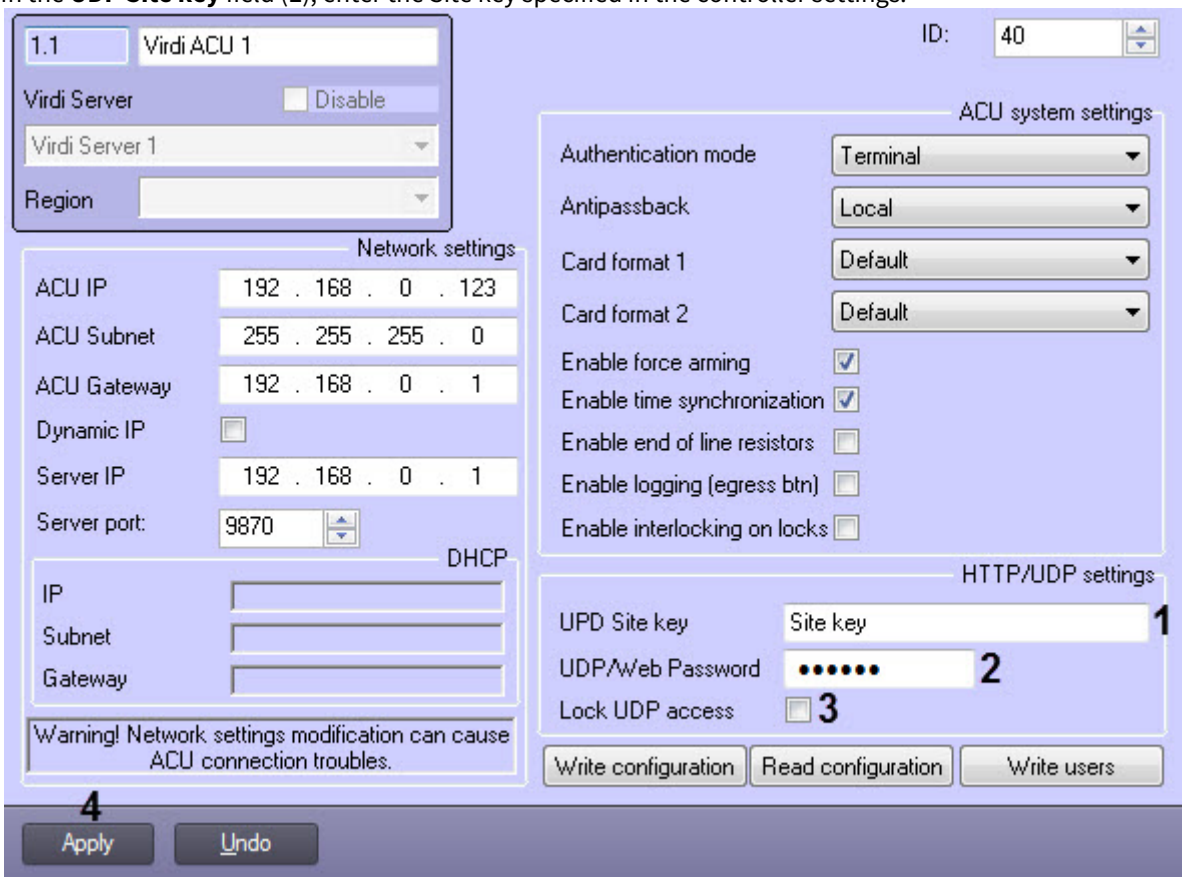
2. Click the **Read configuration** button (**2**) to read the controller configuration.
3. Click the **Write users** button (**3**) to send the users to the controller.
4. Click the **Apply** button (**4**) to apply the settings.

Virdi controller configuration management is complete.

3.2.1.4 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 (**1**), enter the Site key specified in the controller settings.



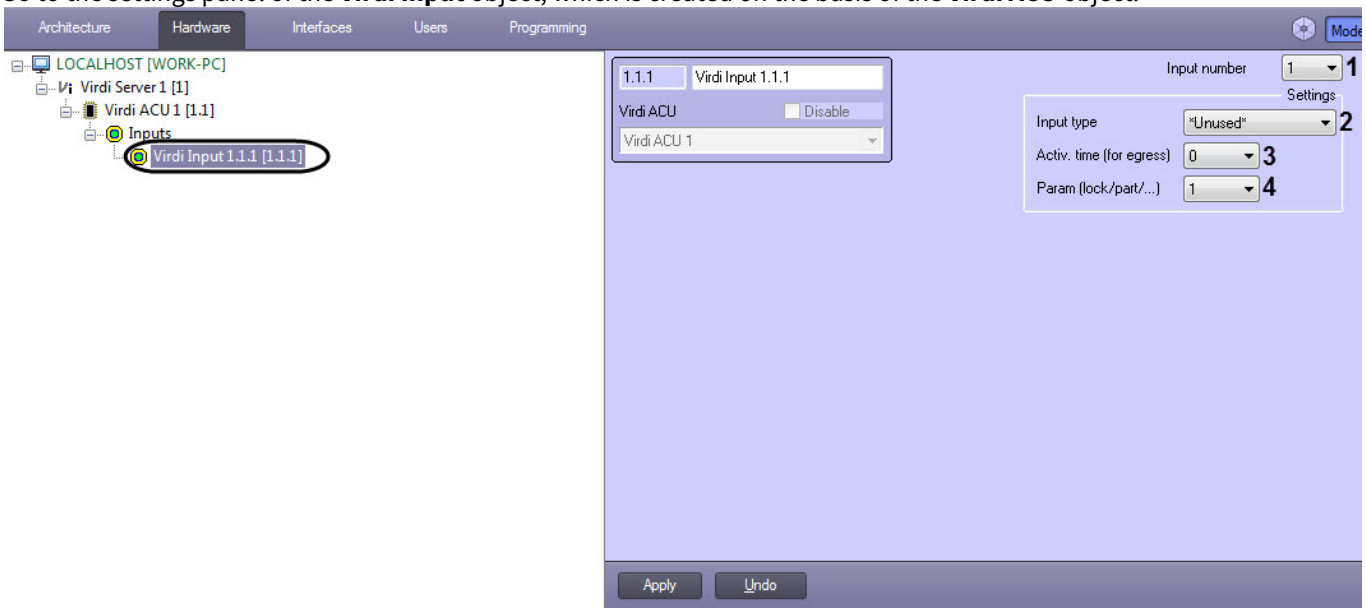
2. In the **UDP/Web Password** field (**2**), enter the controller password.
3. Set the **Lock UDP access** checkbox (**3**) if it is necessary to disable the ability to set up the controller via the Web interface.
4. Click the **Apply** button (**4**) to apply the settings.

The *Virdi* ACU connection to the web server is configured.

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.



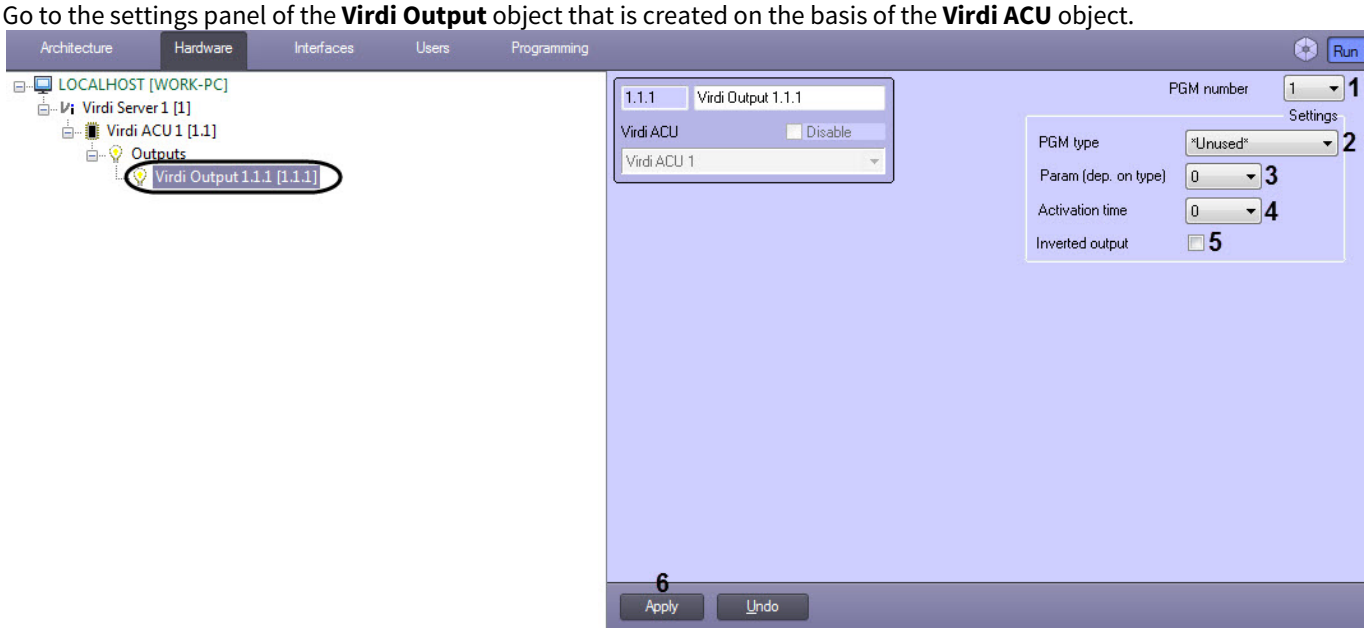
2. From the **Input number** drop-down list (**1**), select the input number from **1** to **4**.
3. From the **Input type** drop-down list (**2**), select the input type:
   - **Unused** - not used.
   - **Egress (NC)** - input with normally-closed contacts.
   - **Egress (NO)** - input with normally-open 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 (**3**), 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 (**4**):
   - 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 (**5**) to apply the settings.

The *Virdi* input is now configured.

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 (**1**), select the output number from **1** to **8**.
3. From the **PGM type** drop-down list (**2**), select the output type:
   - **Unused** - not used.
   - **Matching success** - is triggered after successful authorization of a user.
   - **Matching failed** - is triggered after an unsuccessful authorization of a user.
   - **Scheduled output** - works according to the assigned schedule.
   - **Alarm output** - is triggered when an alarm is activated.
   - **System troubles** - is triggered when a problem occurs in the system, for example, a problem with the battery, a problem with the reader, etc.
   - **Arm/disarm status** - is triggered when a region becomes armed/disarmed.
   - **Fire alarm** - is triggered when a fire alarm is activated.

- **Silent alarm** - is triggered when a silent alarm is activated.
- **Open too long** - is triggered when the door is open for too long.
- **Door forced** - is triggered when the door is held by force.

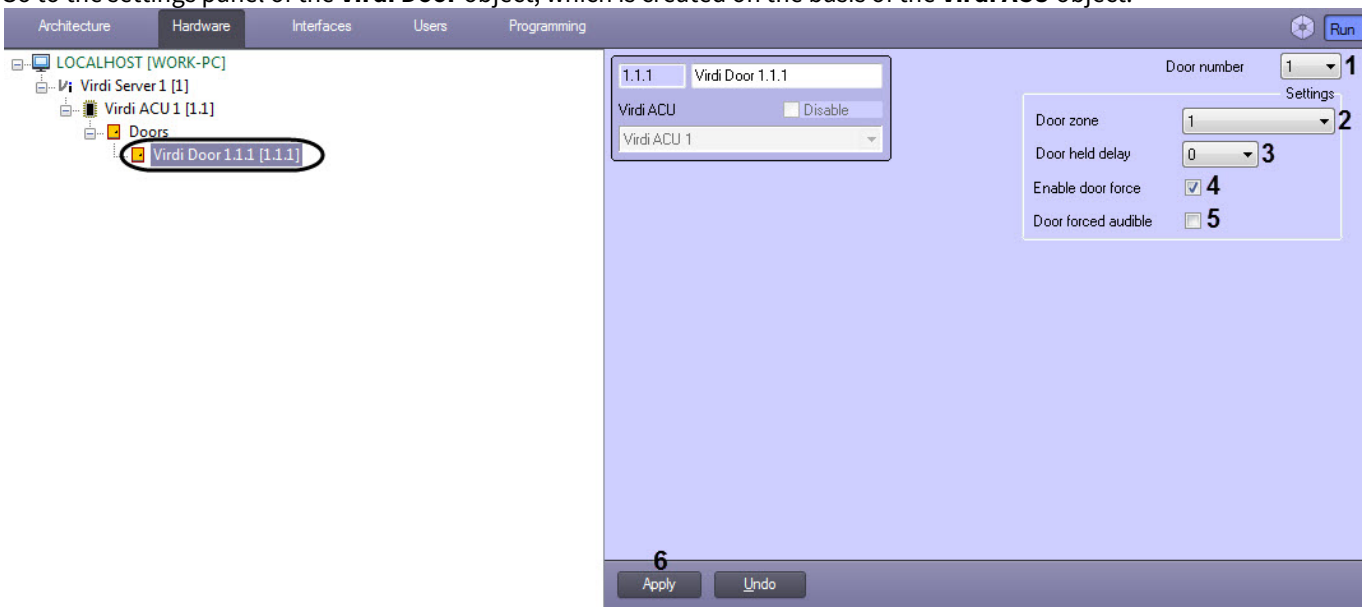
4. In the **Param (dep. on type)** drop-down list (**3**):
   - if the output type **Matching success** or **Matching failed** is selected, then select the door number that will be opened when the corresponding output is triggered: from **1** to **4**.
   - if the output type **Alarm output**, **Fire alarm**, or **Silent alarm** 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 output type **Scheduled output** 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 (**4**), select the time in seconds within which the output will be activated: from **0** to **255**.
6. Set the **Inverted output** check box (**5**) if it is necessary to invert the output.
7. Click the **Apply** button (**6**) to apply the settings.

The *Virdi* output is now configured.

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 (**1**), select the entry number from **1** to **4**.
3. From the **Door zone** drop-down list (**2**), select the zone to which this door should belong:
   - ***Unassigned*** - zone is not assigned.
   - from **1** to **8**.
4. From the **Door held delay** drop-down list (**3**), select the time in seconds after which the open door will be considered as held: from **0** to **255**.

   Notes

   - 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 should be **Exit1**, **Exit2**, **Instant**, or **Interior**.
5. Set the **Enable door force** check box (**4**) if it is necessary to monitor the holding of the door.

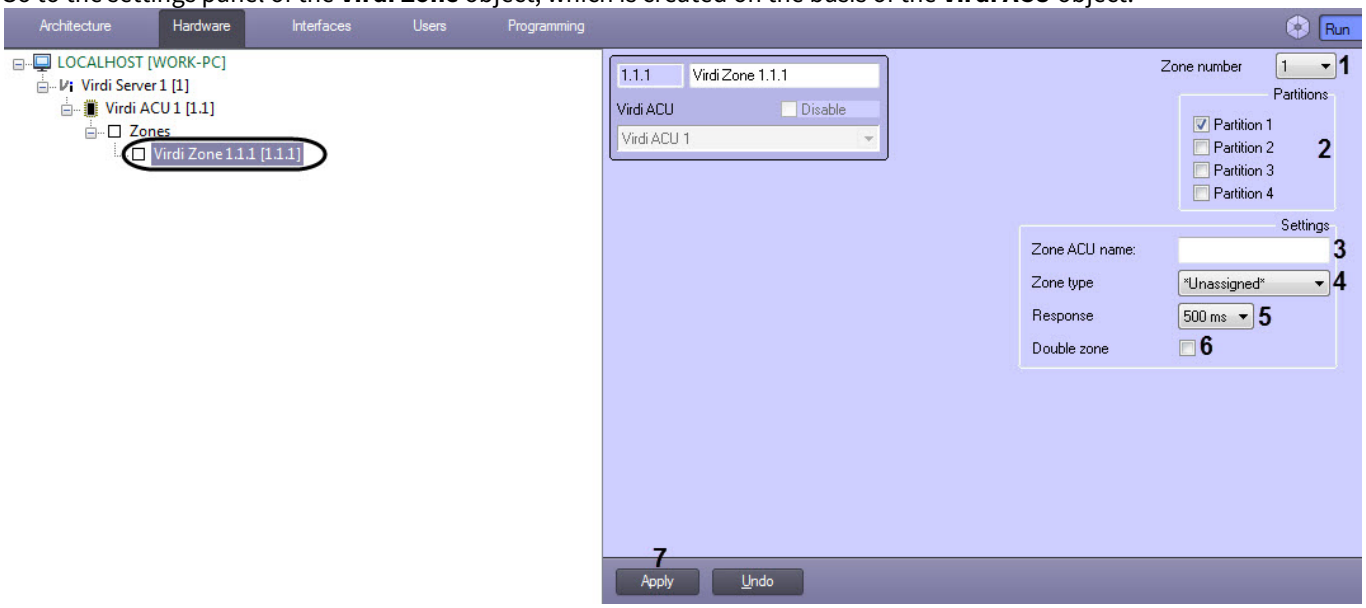
6. Set the **Door forced audible** check box (**5**) if it is necessary to generate a visual and audible alarm on the reader of this door if the door is held.
7. Click the **Apply** button (**6**) to apply the settings.

The *Virdi* door is now configured.

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 (**1**), select the zone number from **1** to **8**.
3. Set the checkboxes next to the partitions (**2**), which should be included in this zone.
4. In the **Zone ACU name** field (**3**), enter an arbitrary name for this zone (no more than 10 characters).
5. From the **Zone type** drop-down list (**4**), 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 (**5**), 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** check box (**6**) if the zones require more than 4 hardware inputs.
8. Click the **Apply** button (**7**) to apply the settings.

The *Virdi* zone is now configured.

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 (**1**), select the input number from **1** to **4**.
3. Set the **Partition enabled** checkbox (**2**) to activate this partition.
4. In the **Partition ACU name** field (**3**), enter the partition name (maximum 16 characters).
5. In the **Partition ACU Account** field (**4**), enter the partition account number in the form of 4 hexadecimal digits. By default, the account number matches the controller ID.
6. From the **Entry delay 1** and **Entry delay 2** drop-down lists (**5**), 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 (**6**), select the time delay in seconds for the exit: from **0** to **255**.

> **Notes**
>
> - **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.

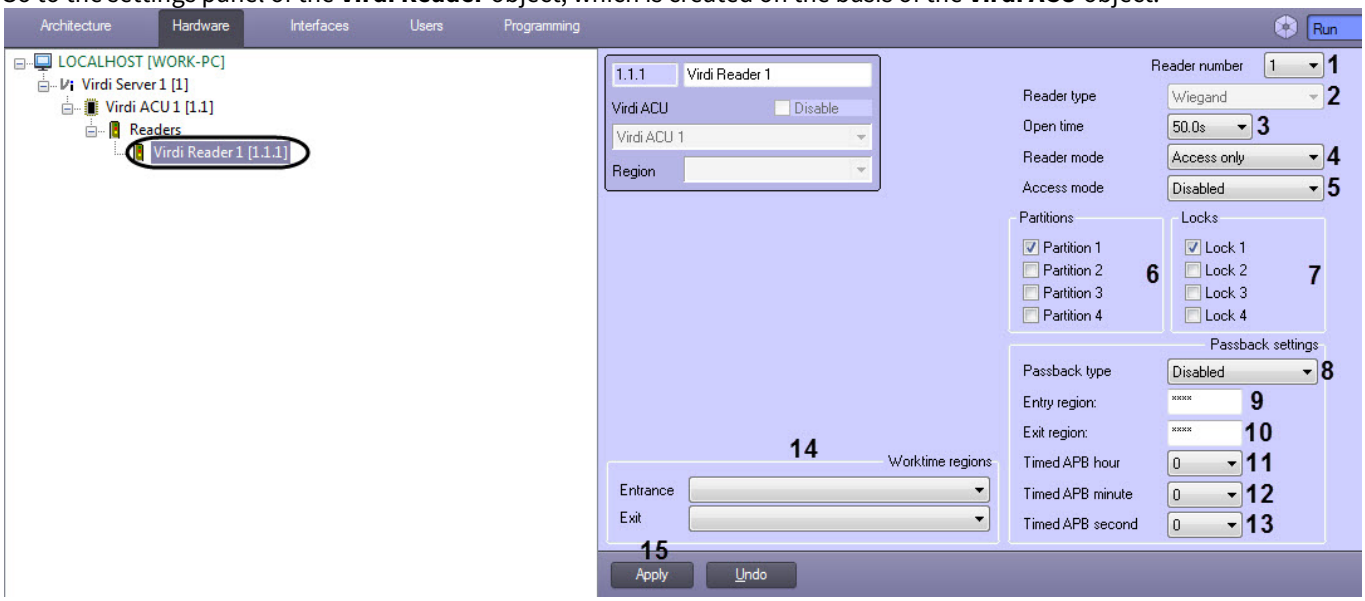
8. From the **Siren time** drop-down list (**7**), select the duration of the siren signal in seconds when an alarm occurs in the alarm section: from **0** to **255**.
9. From the **Max. alarms count** drop-down list (**8**) select the maximum number of the siren repetitions when an alarm occurs in the alarm section: from **0** to **255**.
10. Set the **Chime On** checkbox (**9**) if it is necessary for the reader to make 2 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 (**10**) 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 (**11**) to apply the settings.

The *Virdi* Partition is now configured.

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 (**1**), select the reader number from **1** to **12**.

> **Note**
>
> The **Reader type** drop-down list (**2**) indicates the type of reader. This parameter value cannot be changed.

3. From the **Open time** drop-down list (**3**), 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 (**4**), 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 (**4**), select the access mode:
   - **Disabled** - mode is disabled.
   - **Enter** - enter.
   - **Exit** - exit.
   - **Out** - from the territory.
   - **In** - to the territory.
6. Set the checkboxes near the partitions (**6**) to which this reader will belong.
7. Set the flags opposite the doors (**7**) to which this reader will belong.
8. From the **Passback type** drop-down list (**8**), 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).

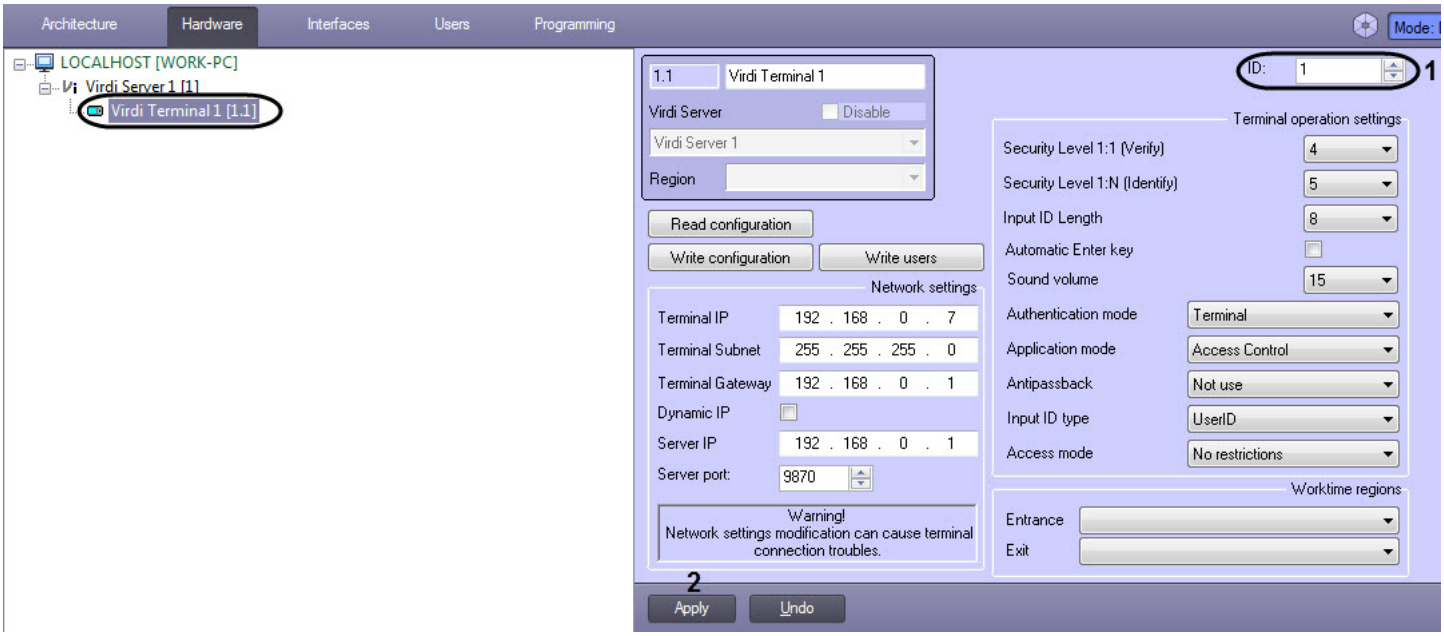
9. In the **Entry region** field (**9**), enter an arbitrary name of the region for the entering (maximum 4 characters). Depending on the selected antipassback control mode, the user will be prohibited or allowed to enter the specified region again (it is necessary for this region name to be indicated at least in 2 readers).
10. In the **Exit region** field (**10**), enter an arbitrary name of the region for the exiting (maximum 4 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 2 readers).
11. If the **Timed Passback** antipassback control mode is selected, then from the **Timed APB hour** drop-down list (**11**), 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 (**12**), 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 (**13**), select the time in seconds during which the strict mode will be used.
14. From the **Entrance** and **Exit** drop-down lists (**14**), select the partitions located on the entrance and exit sides of the door, respectively.
15. Click the **Apply** button (**15**) to apply the settings.

The *Virdi* reader is now configured.

3.3 Configuring the Virdi Terminal

The *Virdi* terminal is configured on the settings panel of the **Virdi Terminal** object, which is created on the basis of the **Virdi Server** object.

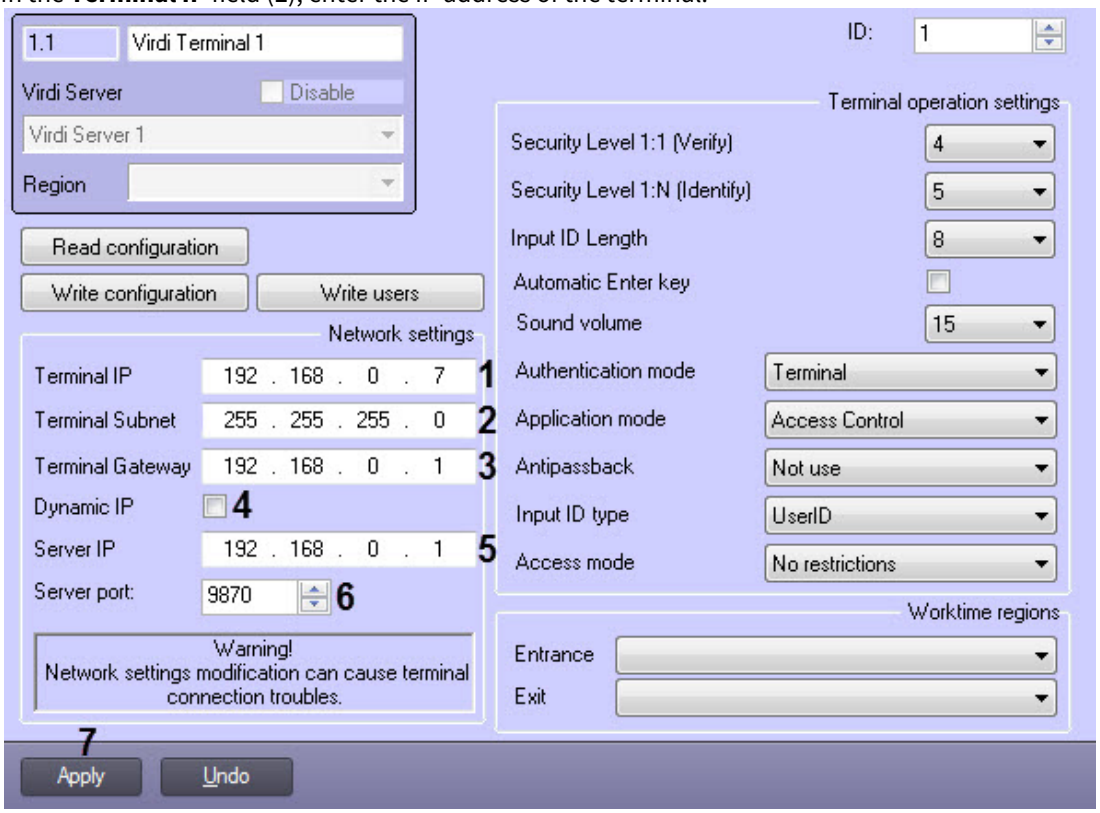
After creating the **Virdi Terminal** object, it is necessary to specify the identifier of this terminal in the **ID** field (**1**) and click the **Apply** button (**2**).



3.3.1 Setting up the Virdi Terminal network connection

The *Virdi* terminal connection is configured as follows:

1. In the **Terminal IP** field (**1**), enter the IP address of the terminal.



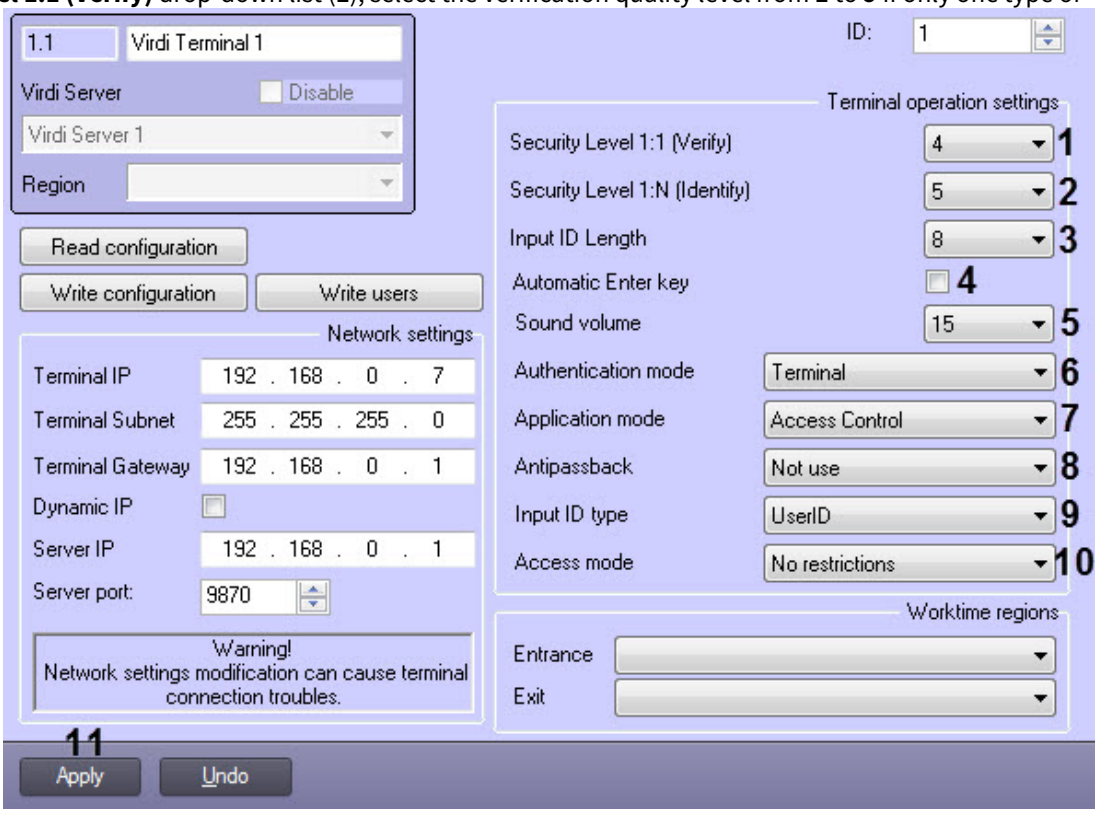
2. In the **Terminal Subnet** field (**2**), enter the terminal subnet mask.
3. In the **Terminal Gateway** field (**3**), enter the terminal gateway.
4. Set the **Dynamic IP** checkbox (**4**) if the terminal operates in a network with DHCP protocol.
5. In the **Server IP** field (**5**), enter the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

The *Virdi* terminal connection is now configured.

3.3.2 Virdi Terminal operation settings

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

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



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

> **Attention!**
>
> To ensure the terminal operation with *ACFA-Intellect*, it is necessary to select the **8** value. Also, the **Input ID Length** should be set to **8** in the terminal itself.

4. Set the **Automatic Enter key** check box (**4**) to enable the automatic key entry from the terminal keyboard (F1-F4 buttons).
5. From the **Sound volume** drop-down list (**5**), select the terminal speaker volume level: from **0** to **20**.
6. From the **Authentication mode** drop-down list (**6**), 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-Intellect Server*.

7. From the **Application mode** drop-down list (**7**), select the terminal operating mode:
   - **Access control** - access point mode.

   > **Attention!**
   >
   > To ensure the terminal operation with *ACFA-Intellect*, it is necessary to select the **Access control** operation mode.

- **Time/Attendance** - working time tracking mode.
- **Drinking Water** - breathalizers compatibility mode.

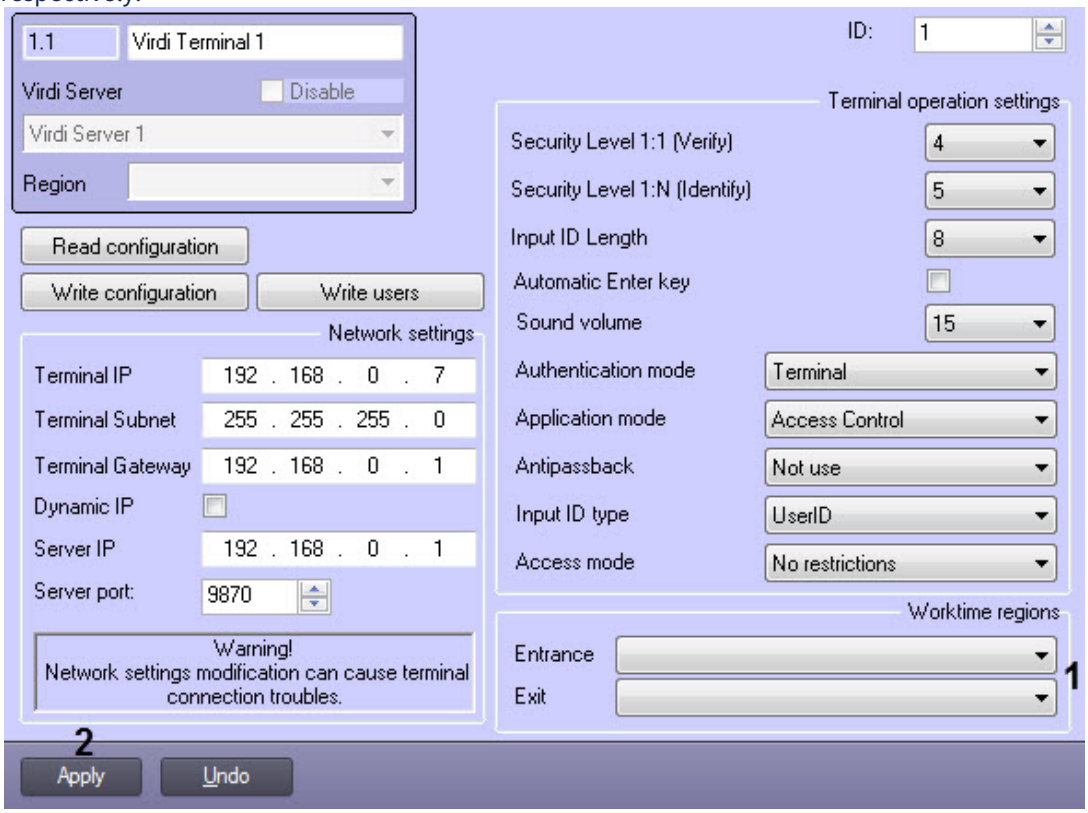
8. From the **Antipassback** drop-down list (**8**), select the double-entry control mode:
   - **Not use** - not used.
   - **Access when disconnected** - allow entry if the connection with the Server is lost.
   - **Prohibit when disconnected** - prohibit entry if the connection with the Server is lost.
9. From the **Input ID type** drop-down list (**9**), select the type of user identifiers:
   - **UserID type** - custom user identifiers.
   - **UniqueID** - unique user identifiers specified in the terminal.
10. From the **Access mode** drop-down list (**10**), 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. Click the **Apply** button (**11**) to apply the settings.

The operation settings of the *Virdi* Terminal are set up

3.3.3 Setting up the Virdi Terminal worktime regions

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

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



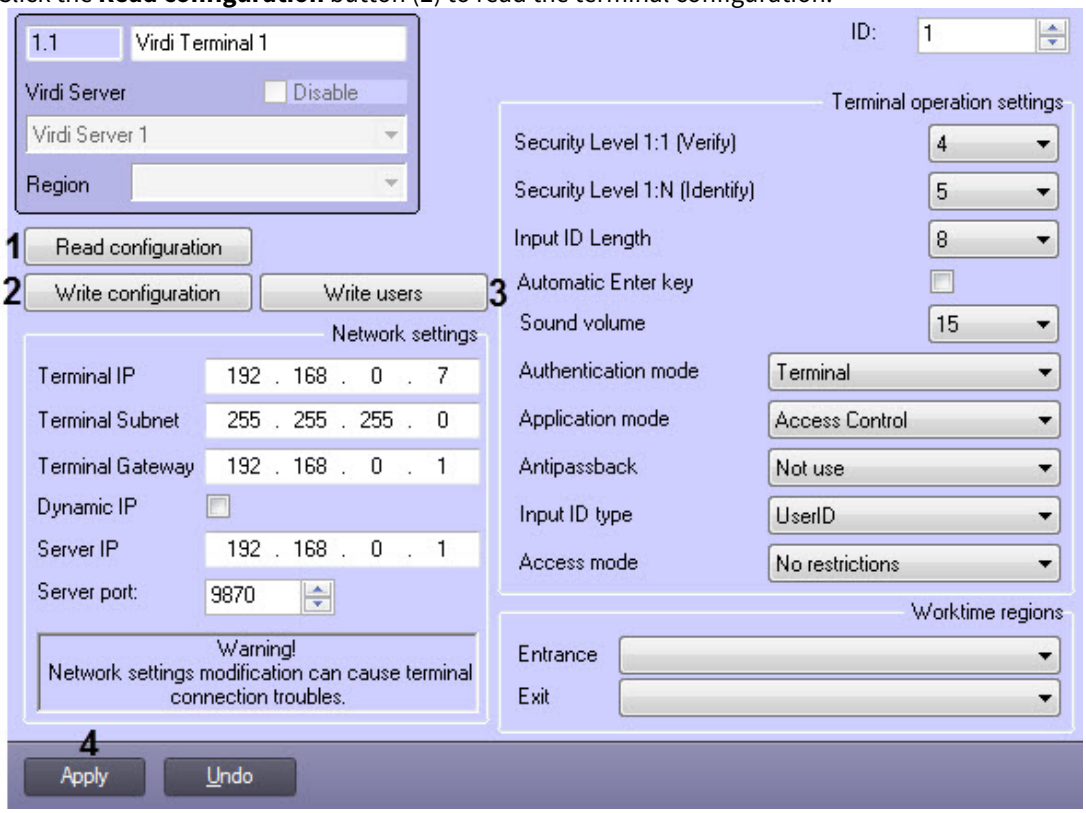
2. Click the **Apply** button (**2**) to apply the settings.

The *Virdi* Terminal worktime regions are now configured.

3.3.4 Managing the Virdi Terminal configuration

The *Virdi* Terminal configuration is managed as follows:

1. Click the **Read configuration** button (**1**) to read the terminal configuration.



2. Click the **Write configuration** button (**2**) to write the current configuration to the terminal.
3. Click the **Write users** button (**3**) to send the users to the terminal.
4. Click the **Apply** button (**4**) to apply the settings.

The *Virdi* Terminal configuration management is complete.

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 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 Managing the Virdi Terminal

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

The **Virdi Terminal** object functional 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 (continously)	The door is opened for a long time

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

Virdi Terminal 1 [1.1] 	The terminal body is force opened
Virdi Terminal 1 [1.1] 	Disconnected
Virdi Terminal 1 [1.1] 	Blocked
Virdi Terminal 1 [1.1] 	Closed

Virdi Terminal 1 [1.1] 	The door is force opened
Virdi Terminal 1 [1.1] 	The door is force held
Virdi Terminal 1 [1.1] 	Open
Virdi Terminal 1 [1.1] 	Connected

4.3 Managing the Virdi Partition

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

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

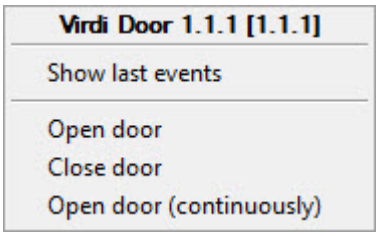
Menu command	Function performed
Arm	The partition is armed
Disarm	The partition is disarmed

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

Virdi Partition 1 [1.1.1] 	Disarmed
Virdi Partition 1 [1.1.1] 	Armed
Virdi Partition 1 [1.1.1] 	Alarm

4.4 Managing the Virdi Door

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



The **Virdi Door** object functional 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 (continously)	The door is opened until a command to close the door is given

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

	Closed
	Open

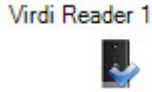
4.5 Managing the Virdi ACU, Reader, and Zone

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

The *Virdi* ACU can have the following states:

	Disconnected
	The body is force opened
	Connected

The *Virdi* Reader can have the following states:

	Normal
	Error on the RS485 line

Virdi Reader 1 [1.1.1] 	Unknown status

The *Virdi* Zone can have the following states:

Virdi Zone 1.1.1 [1.1.1] 	Normal
Virdi Zone 1.1.1 [1.1.1] 	Zone is open
Virdi Zone 1.1.1 [1.1.1] 	Malfunction