ARMATURA

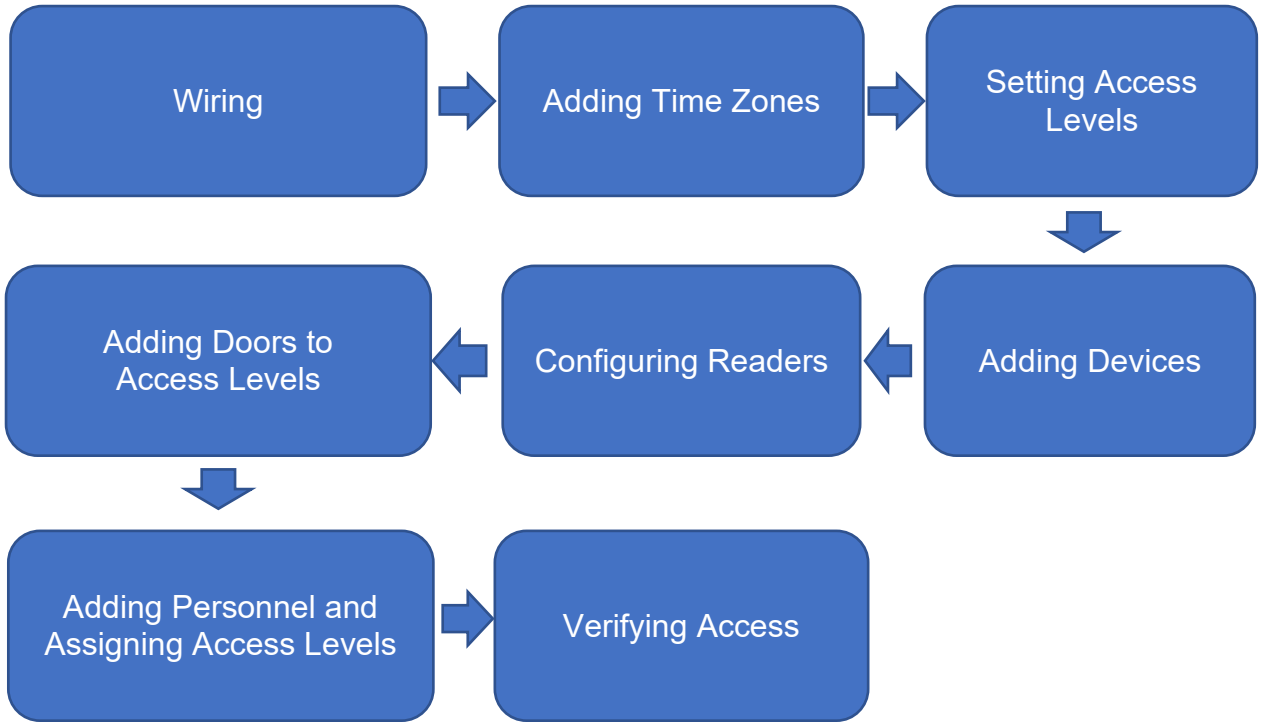
Armatura Horizon Series Access Controller QSG

Doc Version: 1.0.0

Contents

1 Horizon Series Panel Configuration and Setup

Configuration and Setup Flow Chart:



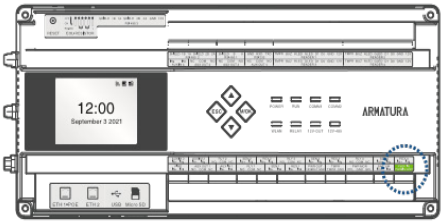
Based on your requirements, select the appropriate operation method below:

2 Access Controller Wiring

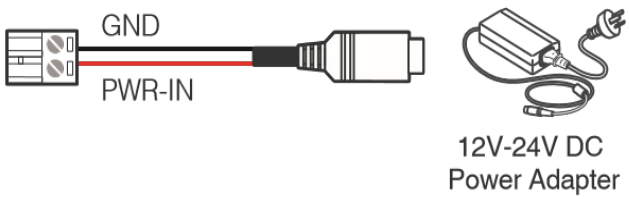
Please click on the corresponding option to view the device wiring guide based on your device type:

● Power

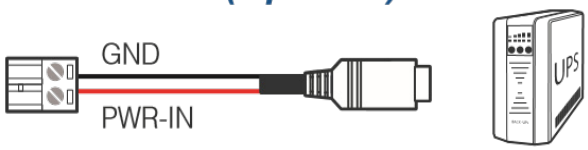
The Armatura Horizon Controller is powered through a 12V-24V DC power adapter or PoE, whichever is available. The wiring is as shown below:



1. Without UPS



2. With UPS (Optional)



Recommended Power Supply

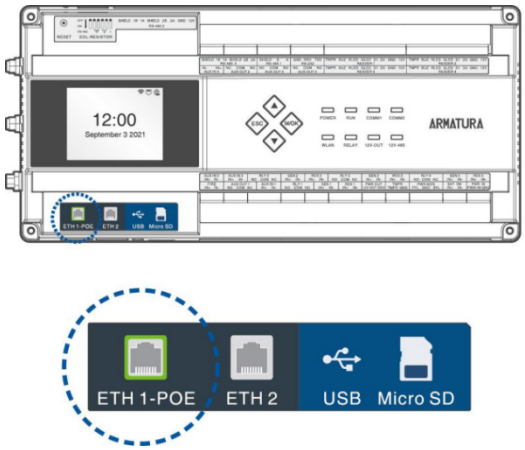
Note:

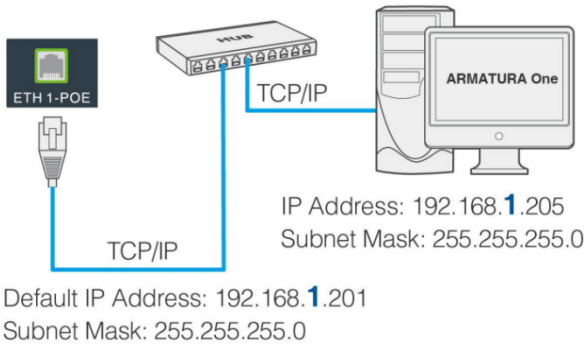
Recommended Power Supply: 12V-24V DC ±20%, minimum 1.5A.

Consider utilizing an AC adapter with a higher current rating to allocate power efficiently among multiple devices.

● Network

Connect the device to the software via Ethernet cable plugged into the network. An example is provided below:





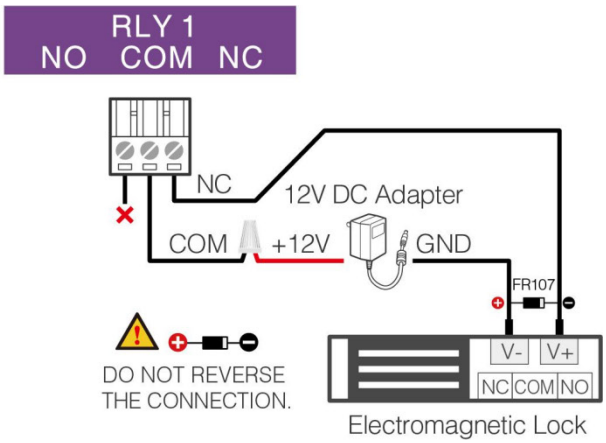
Important Notes:

1. When connecting to the ARMATURA One software in a LAN, ensure that the IP addresses of the server (PC) and the device are in the same network segment.

2. For dual Ethernet interfaces, the default IP address for the primary NIC is 192.168.1.201, and for the expansion NIC, it is 192.168.2.202.

● Locks

The panel supports both Normally Opened (NO) and Normally Closed (NC) locks. For NO Lock, it is connected to the 'NO' and 'COM' terminals, while the NC Lock is connected to the 'NC' and 'COM' terminals. Importantly, the device does not share power with the lock. Below is an example of how the NC Lock is connected:



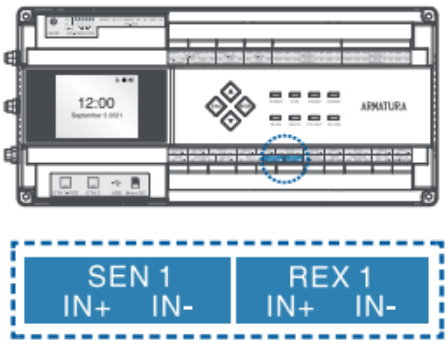
Note:

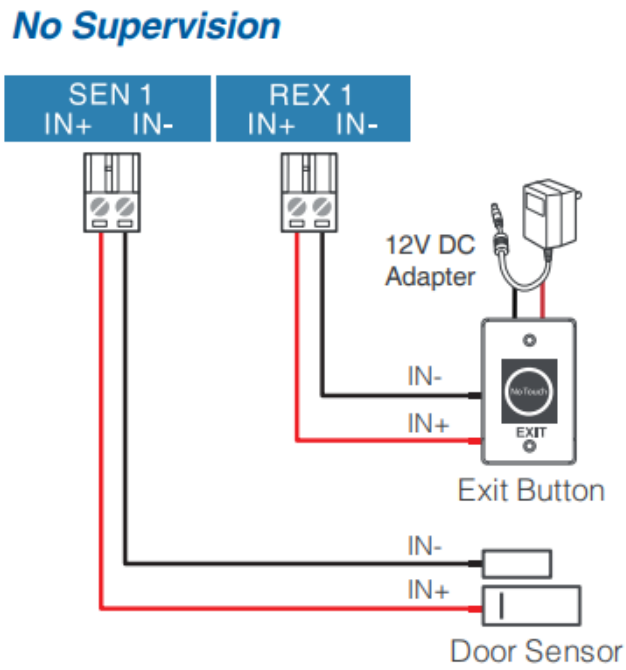
To safeguard the access control panel against self-induced electromotive force produced by an electronic lock during switching off/on, it is crucial to connect a diode in parallel (please use FR107 provided with the system) with the electronic lock. This diode will dissipate the self-induced electromotive force during onsite connection, ensuring the secure application of the access control system.

Exit Button and Door Sensor

1. A door sensor is employed to detect the open/close status of a door. This sensor switch enables the access control panel to identify door openings and activate an alarm output when necessary.

2. An exit button serves as a switch specifically designed to effortlessly open a door. When activated, the door promptly swings open. Typically, the exit button is conveniently installed at a height of approximately 55.12 inches (1.4m) above the ground, providing easy access for users.





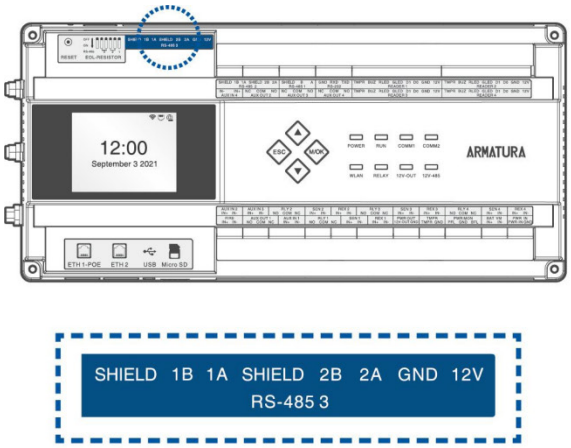
Readers

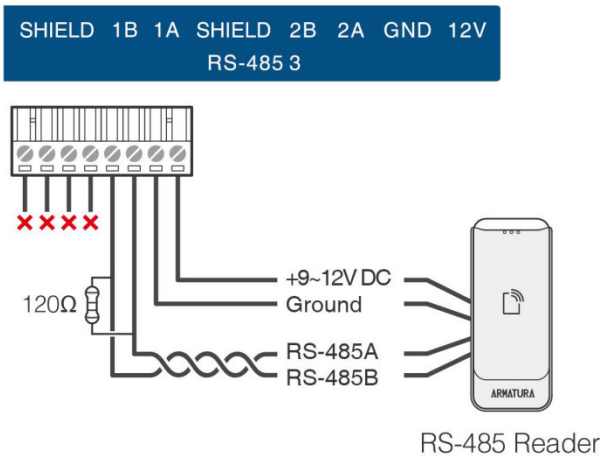
Select the Reader Connection Method Based on the Respective Device Type:

1. RS-485/OSDP

2. Wiegand

RS-485/OSDP





RS-485 Reader

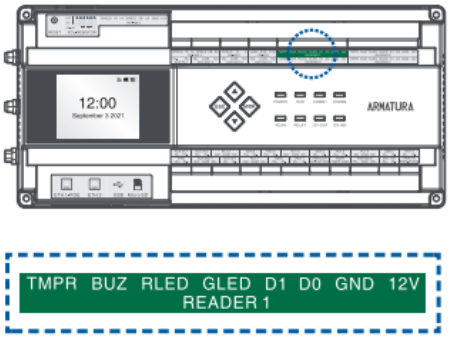
Note:

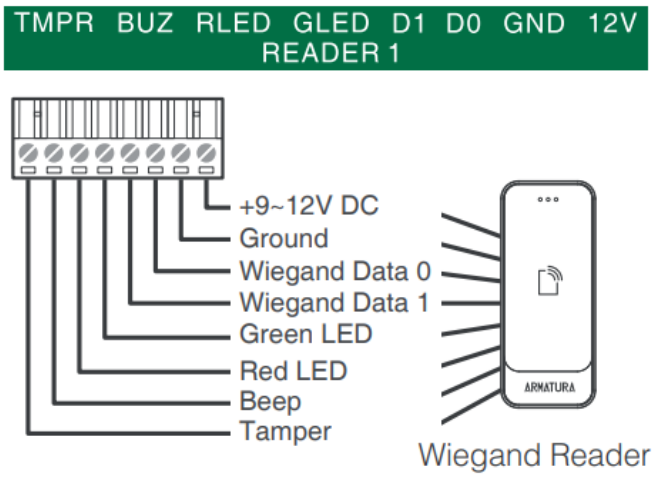
For communication distances greater than or equal to 984ft (300m), follow these steps to ensure proper functioning:

1. Configure the EOL resistor of 485 using the dip switch to enable the terminal.

2. Additionally, connect a 120-ohm terminal matching resistor between the 485+ and 485- terminals of the last terminal device.

Wiegand





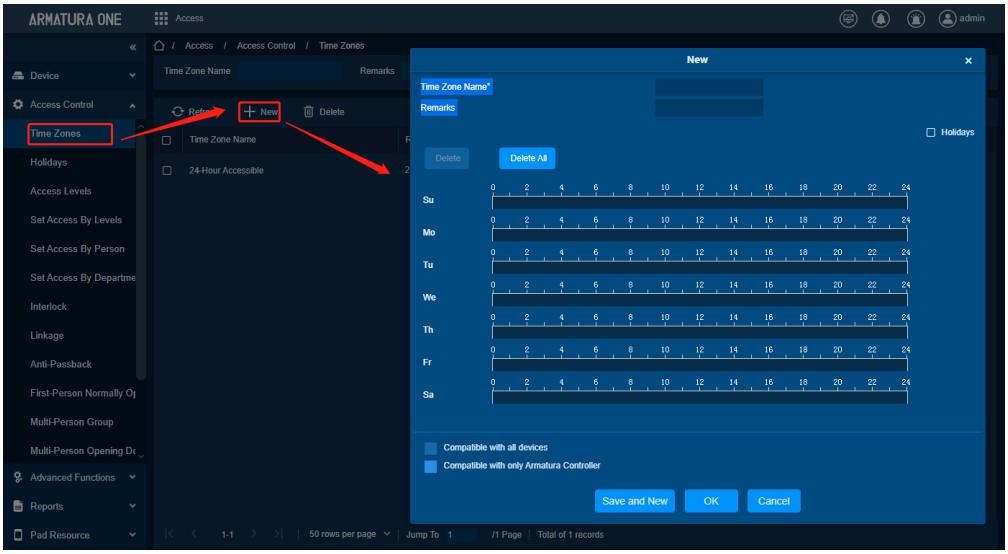
Wiegand Reader

3 Adding Time Zones

The system offers a default access control time zone named [24 Hours Accessible], but you also have the flexibility to create a new time zone based on your specific requirements. See the options below:

1. Click on [Access Control] > [Time Zones] > [New] to access the time zone setting interface.

2. After making the desired settings, click [OK] to save, and it will be displayed in the list.



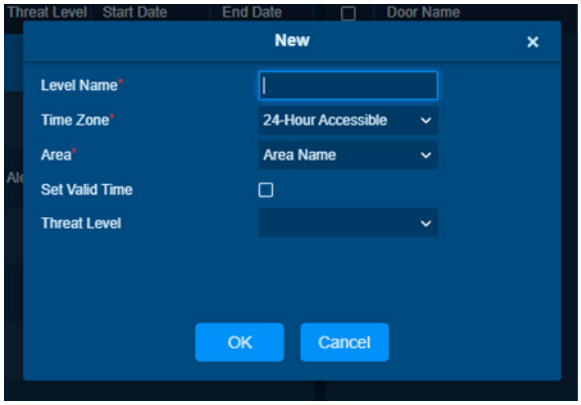
4 Setting Access Levels

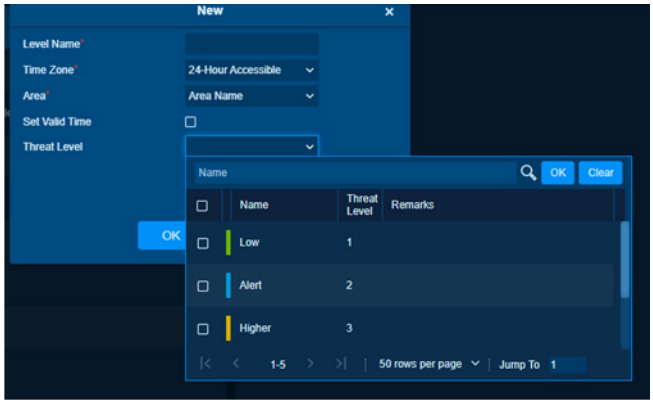
The system includes an access level named [General], and users also have the option to create a new access level based on their specific requirements. See the example below:

1. Click on [Access Control], then select [Access Levels], and click [New] to access the Add Levels editing interface.

2. Define the Threat Level for this access level.

3. Click [OK] to prompt the system to 'Immediately add doors to the current Access Control Level'. Next, click [OK] to add doors, or click [Cancel] to return to the access levels list. The newly added access level will be displayed in the list.

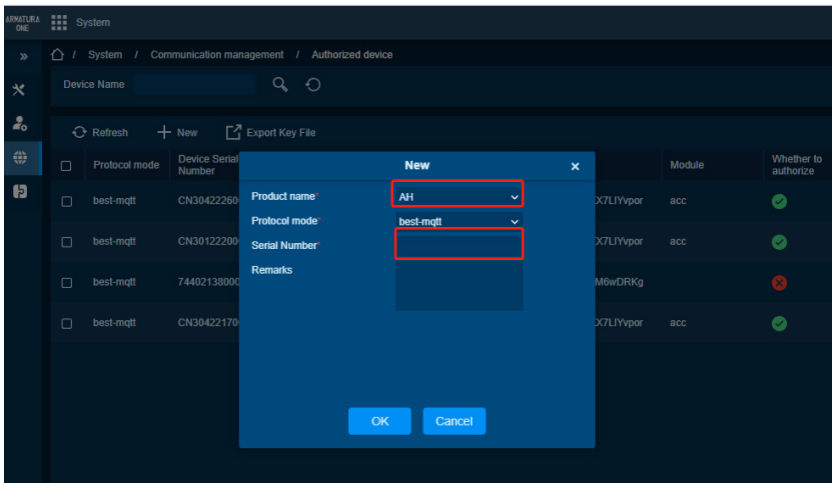




5 Adding Devices

Authorized Devices

In the [System] > [Communication Management] > [Authorized Device] section, click the [New] button to add a new authorized device. Input the serial number and then click the [OK] button to confirm.

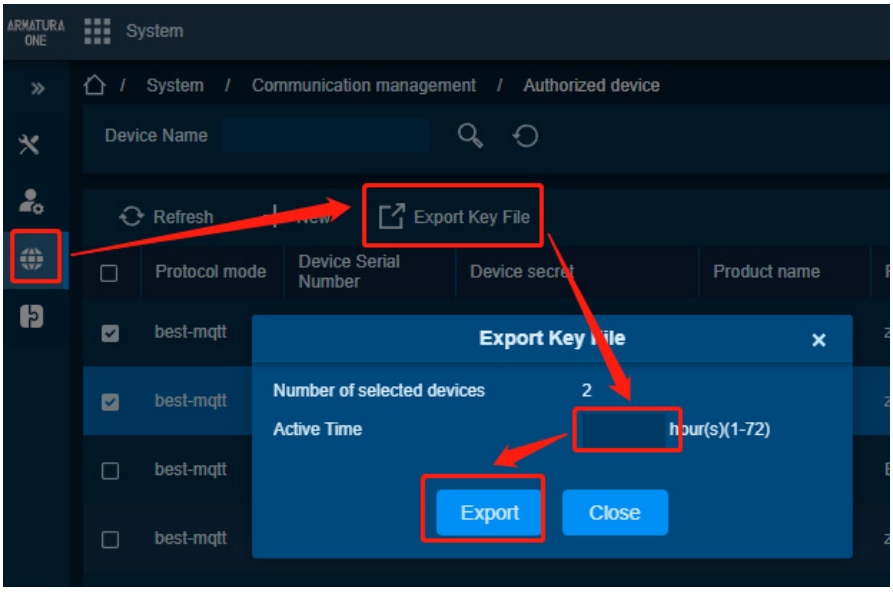


Export Key File

1. In the [System] > [Communication Management] > [Authorized Device], click [Export Key File] Button.

2. Active Time Key File Validity: Key value can be set between 1 and 72 Hours.

3. After clicking the Export button, the browser will initiate the download of a .zip file.



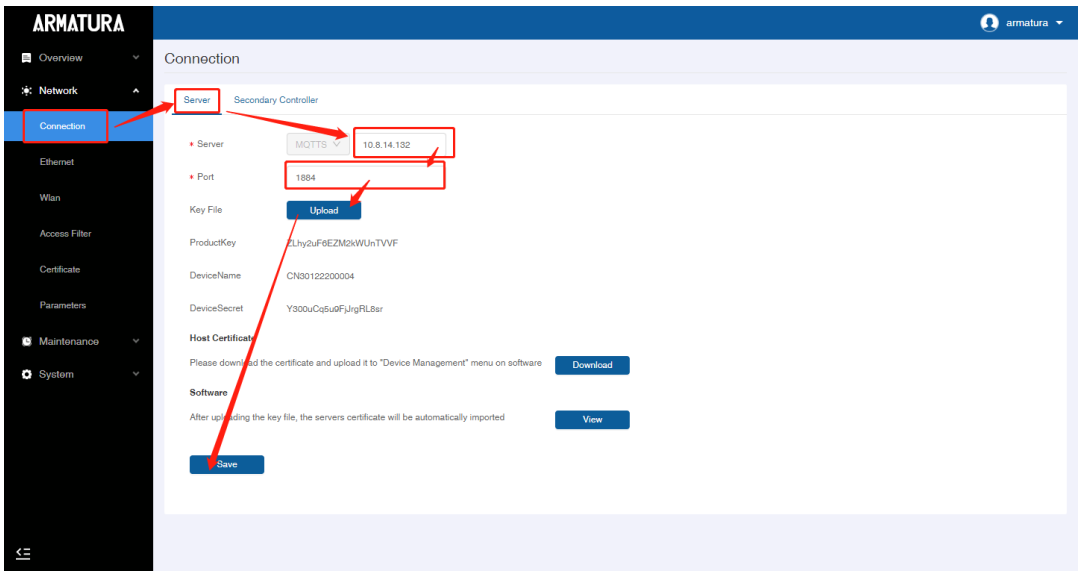
Importing Key File to the Controller

1. Open your web browser and enter the controller's IP address in the URL bar as follows: https://" [controller's IP address]".

2. Open [Network] > [Connection].

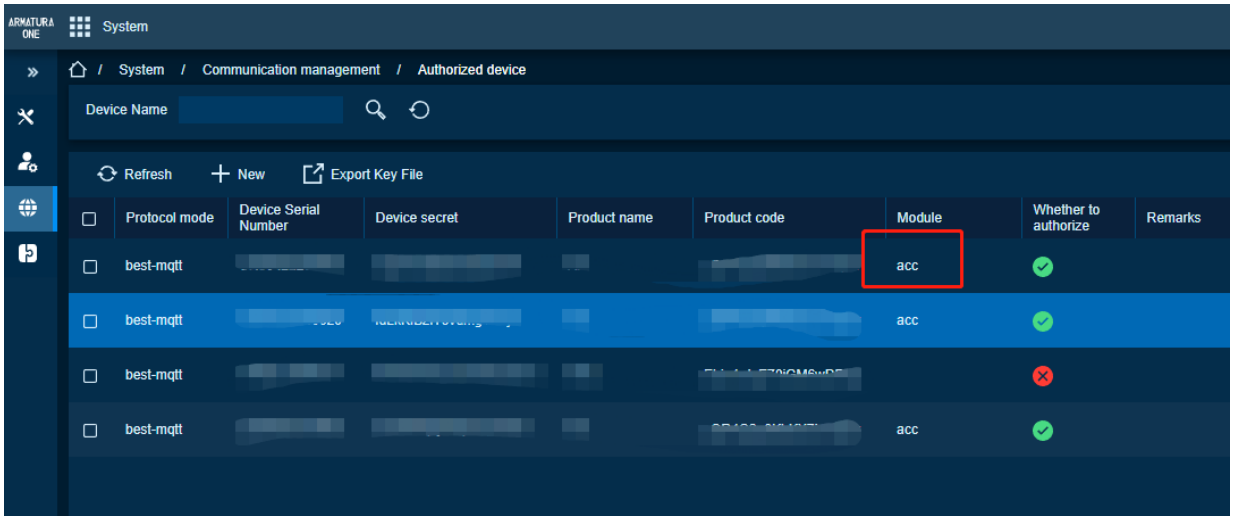
3. Click on the [Server] Tab: The default protocol for the server is MQTTs, and the address is the server address. The default port is 1884.

4. Click the [Upload] button to upload the .zip file downloaded in [Step 2]. Once the upload is complete, you will receive a prompt indicating the operation has succeeded. Finally, click the [Save] button to save the changes.



Check Authorization

1. After successful connection via MQTT, the Module column will display 'acc'.

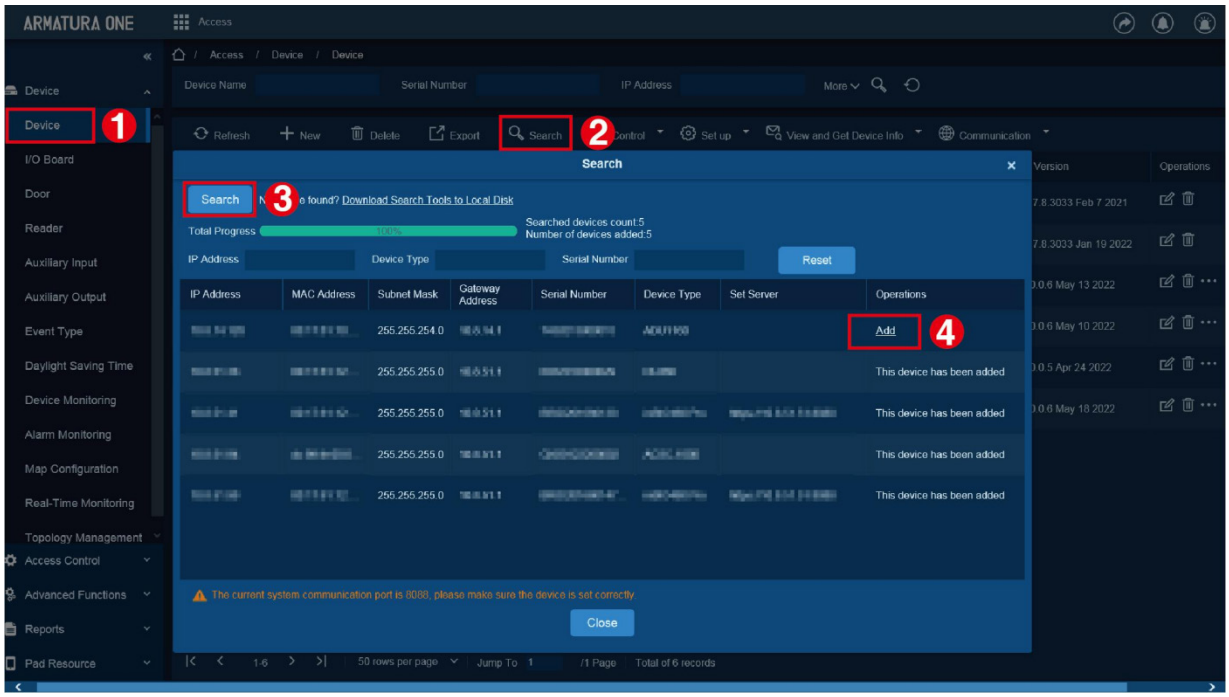


Adding a Device to the Software

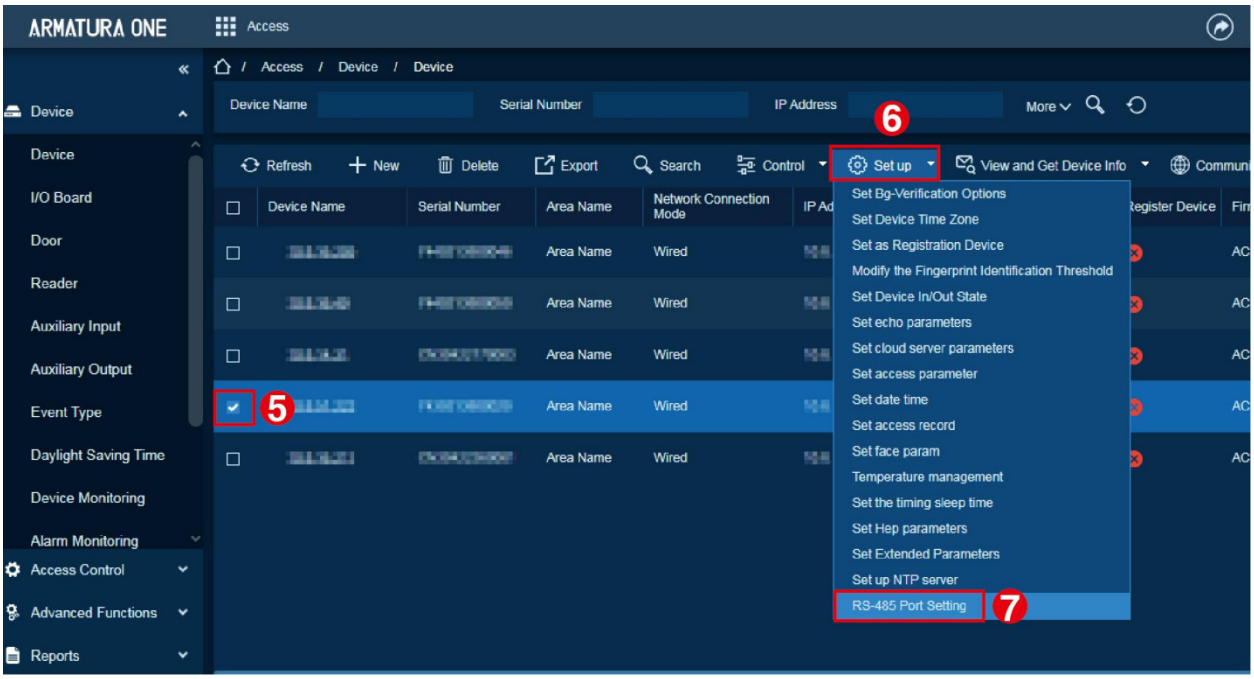
1. Click on [Access] > [Device] > [Device] > [Search] to open the Search interface.

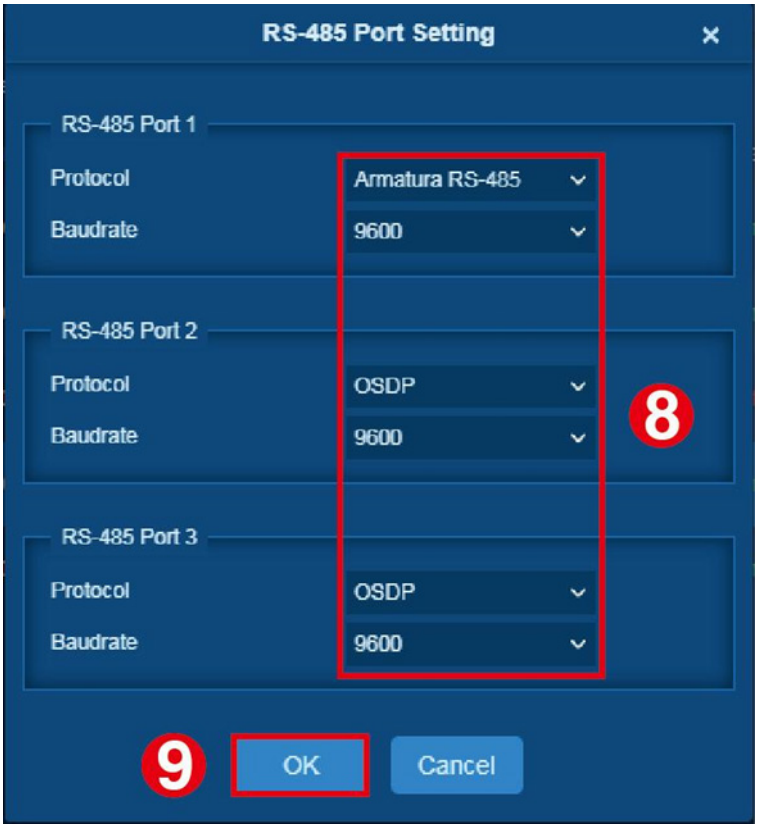
2. After clicking [Search], the list of Access Control Devices along with the total count will be displayed.

3. Click the [Add] button next to the Device to add it.



4. Click on [Set up] > [RS-485 Port Setting] to configure the RS-485 port of the device.

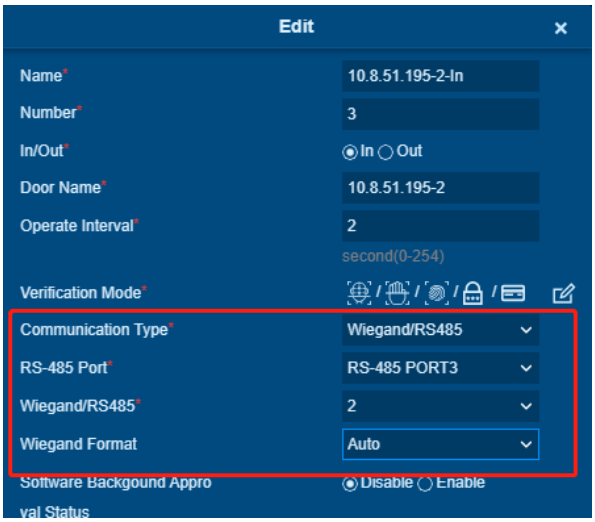




6 Configuring Readers

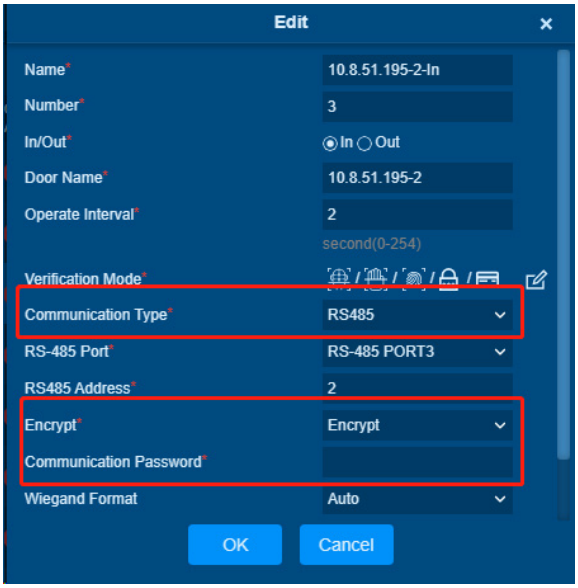
● Configure the Reader Parameters Using the Armatura One Software

To configure the parameters of the reader, click [Access] > [Device] > [Reader], as shown in the figure below.



Note:

If the reader is not encrypted, the default communication type is Wiegand/RS485. In this case, only the port and Wiegand/RS485 address need to be configured.



Note:

To ensure proper encryption of the reader, set the communication type to either Wiegand or RS485, depending on the actual wiring configuration. The encryption option should be selected as either the default password or encryption and remember to set a secure password.

Download and Install the App

ARMATURA CONNECT

1. Make sure your mobile device is connected to the internet through either a mobile data or Wi-Fi network.

2. Open Google Play (Android) or the App Store (iOS) on your mobile device.

3. Search for the ARMATURA CONNECT app.

4. Download and install the app on your mobile device.

5. After completing the account activation process, you can log in to the ARMATURA CONNECT App using your account and password.

Note:

For instructions on obtaining an account and password, kindly refer to the ACMS User Manual.

Viewing the Reader Information

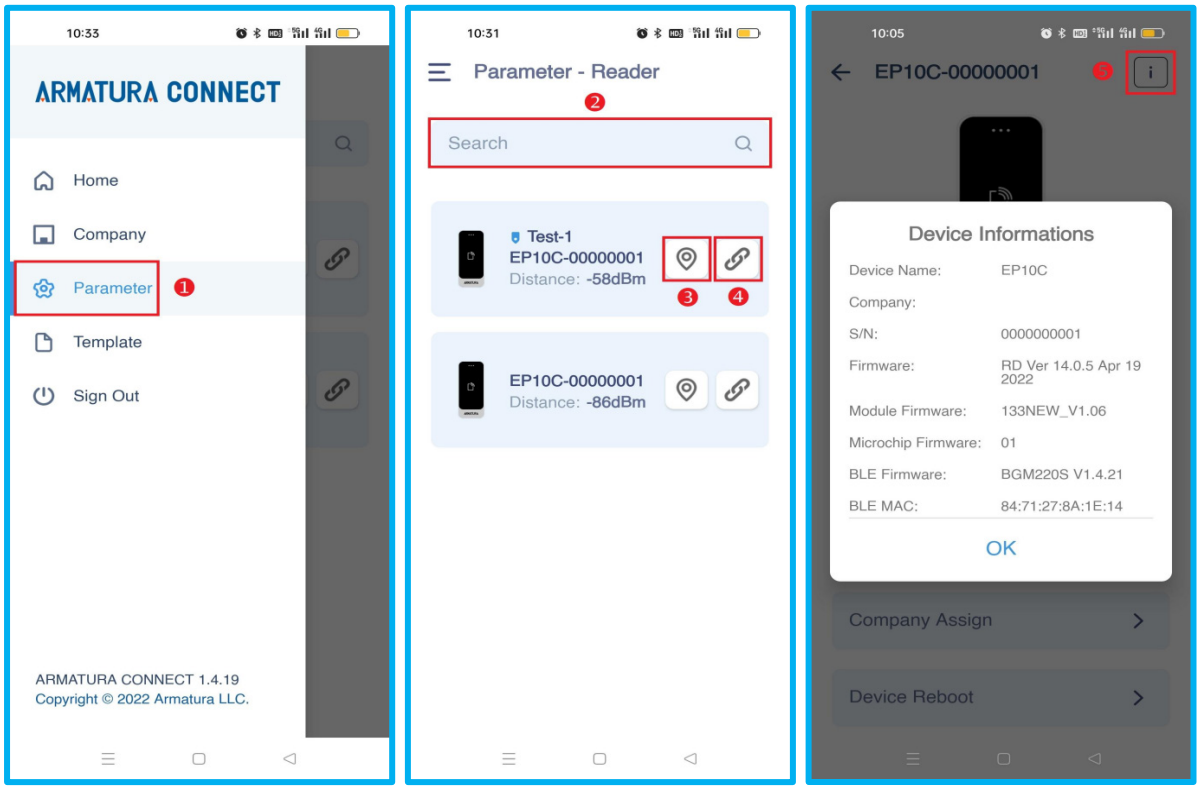
1. Make sure Bluetooth is enabled on your mobile device.

2. Click ☰ > [Parameter] to enter the parameter setting interface.

3. Click to locate the reader. This will make the reader beep so you can locate it.

4. Click to access the reader parameter settings screen, where you can configure relevant reader parameters.

5. Click [i] to view reader information, including device name, company, serial number (S/N), firmware versions, module firmware, microchip firmware, BLE firmware, and BLE MAC address.

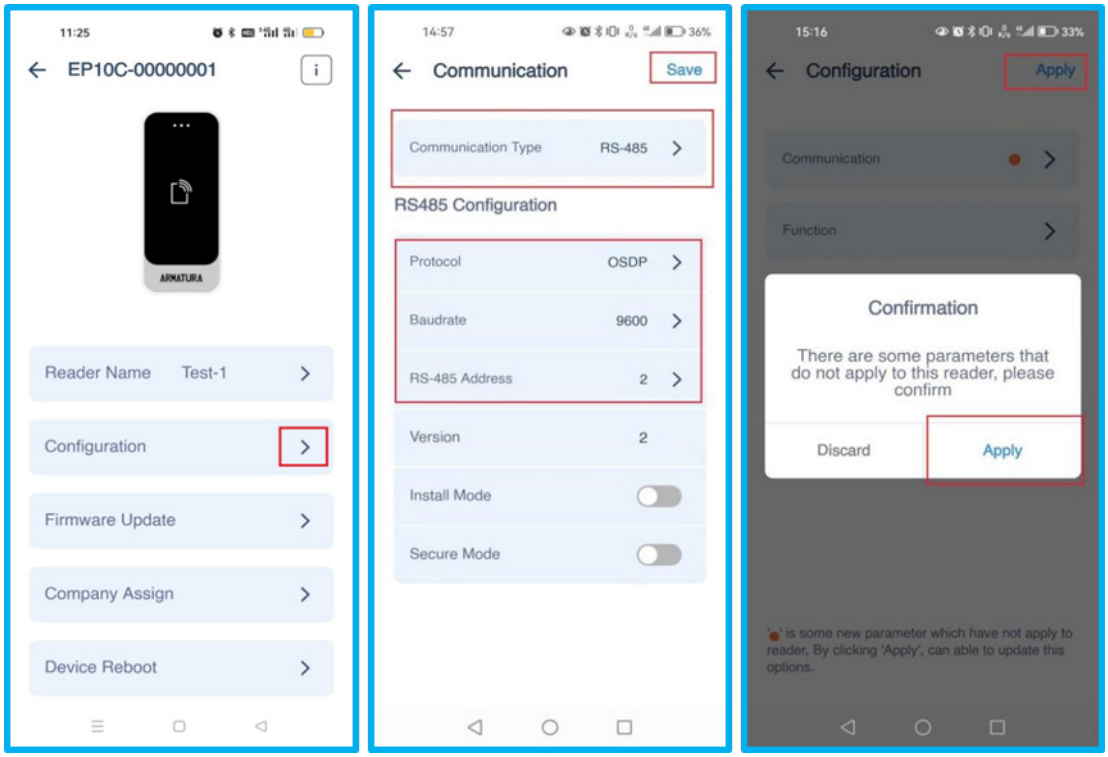


Configure the Reader Parameters Using the App

1. Click on [Configuration] and then navigate to [Communication].

2. Configure the Communication Type, Protocol, Baud Rate, and RS-485 Address options to match the parameters set in the Armatura One software.

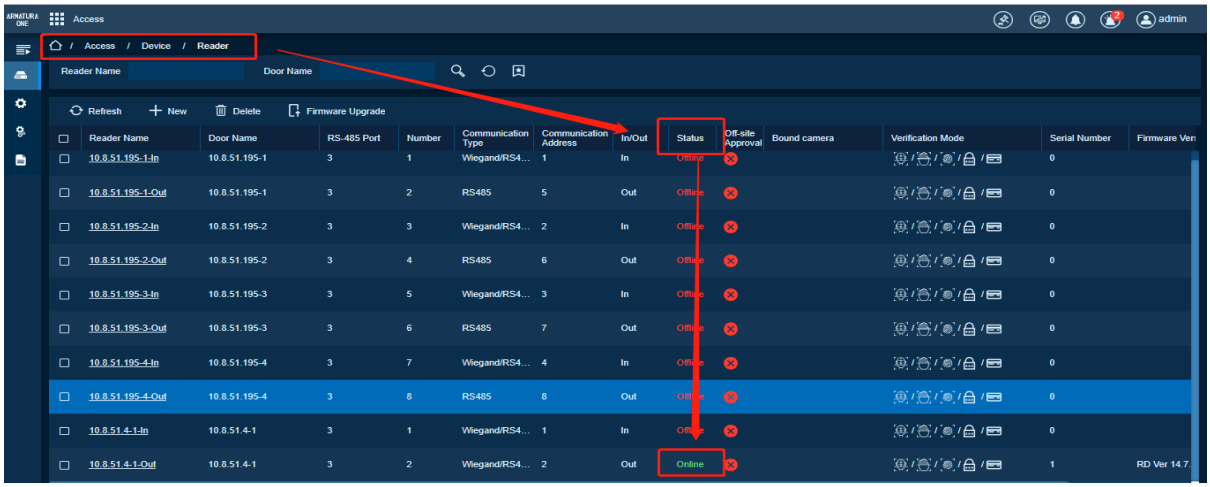
3. To save the reader configuration parameters, click [Save], then click [Apply].



Monitoring the Reader Status in the Armatura One Software

1. After completing the reader configuration, log into the Armatura One software.

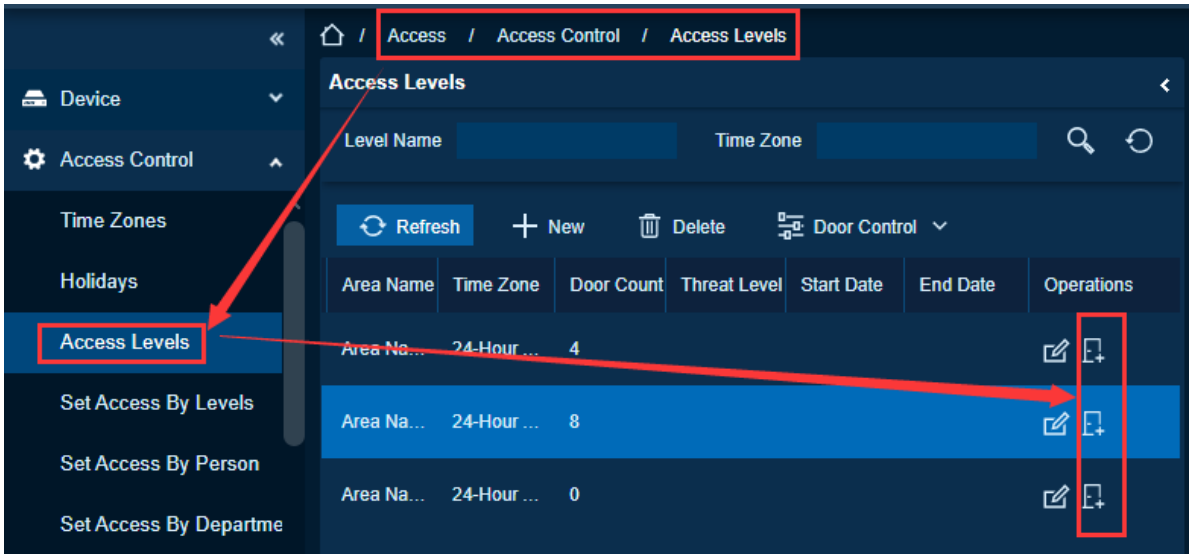
2. To check the reader status, click on [Access] > [Device] > [Reader]. If the reader status displays as online, it means the reader is ready for normal usage.

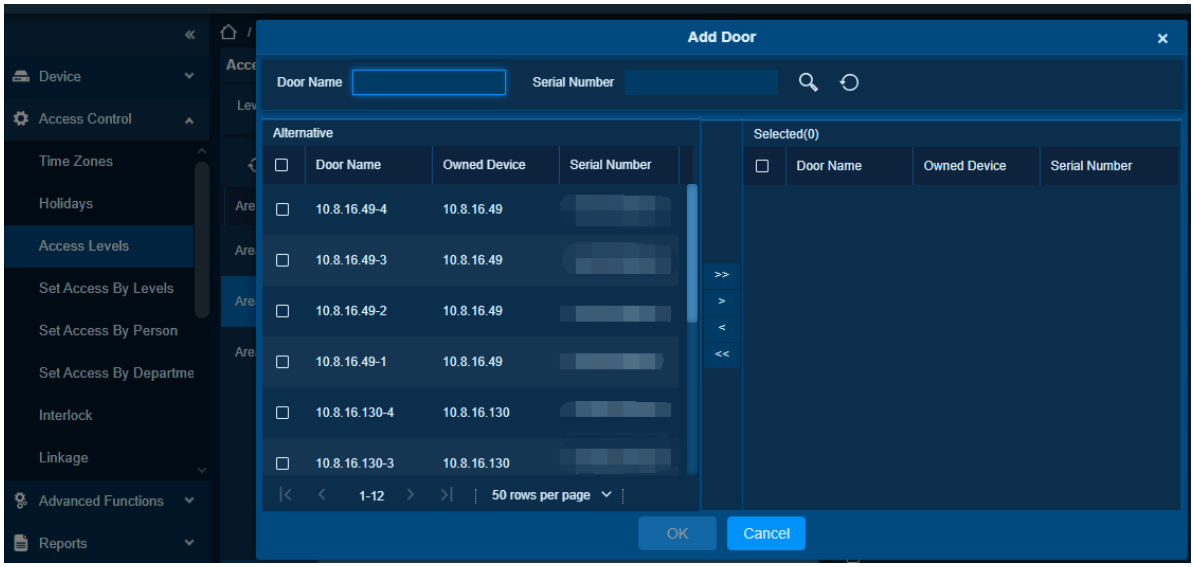


7 Adding Doors to Access Levels

1. To reach the access levels interface, click on [Access] > [Access Control] > [Access Levels].

2. Select the appropriate access levels and click [Add Door] to assign them to the respective door.

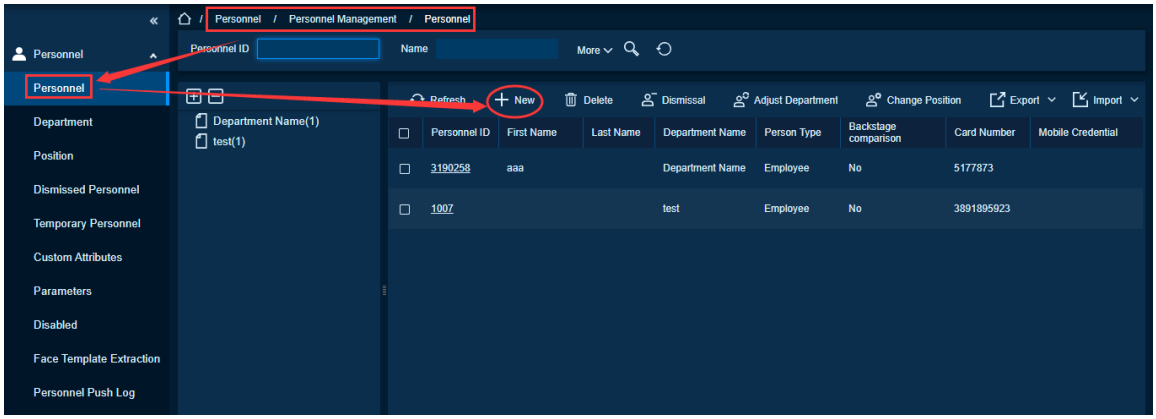




8 Adding Personnel and Assigning Access Levels

Add Personnel in the Software

1. To add personnel, select: [Personnel] > [Personnel Management] > [Personnel] > [New].



2. In the new personnel interface, input the Personnel ID, Department, First Name, Last Name, and other relevant details.

3. You can select one or any of the following verification methods:

• Face

• Card

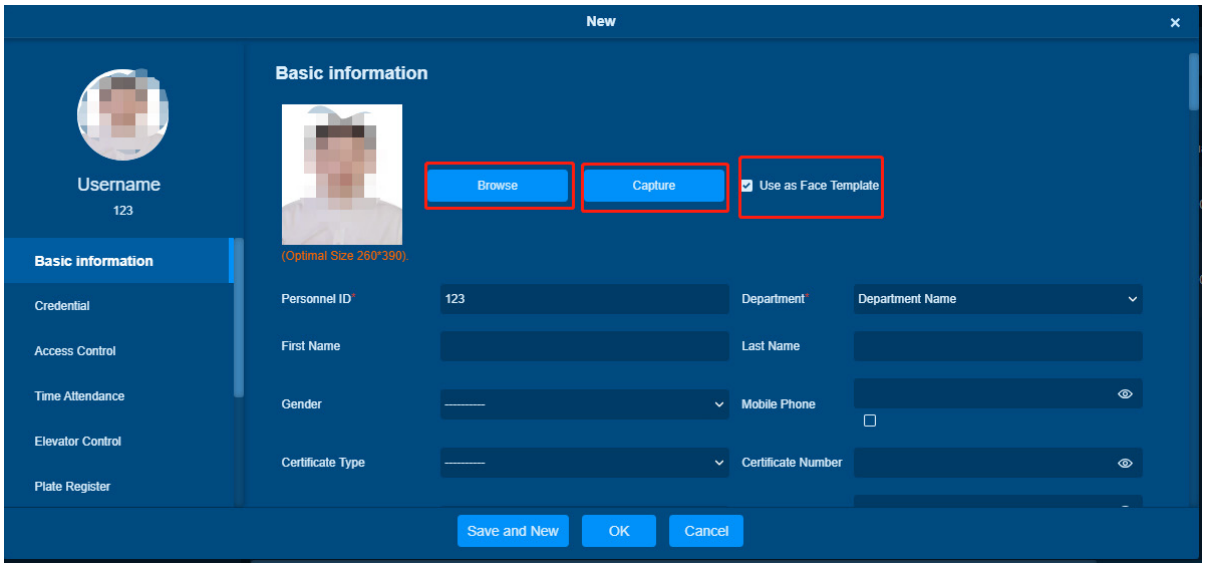
• Fingerprint

Adding Face

• [Browse]: Click [Browse] to select a local photo to upload.

• [Capture]: Capture a facial image using the webcam or device as enrollment reader.

• [Use as Face Template]: Enable this option to use as a face template by checking the box.



Note:

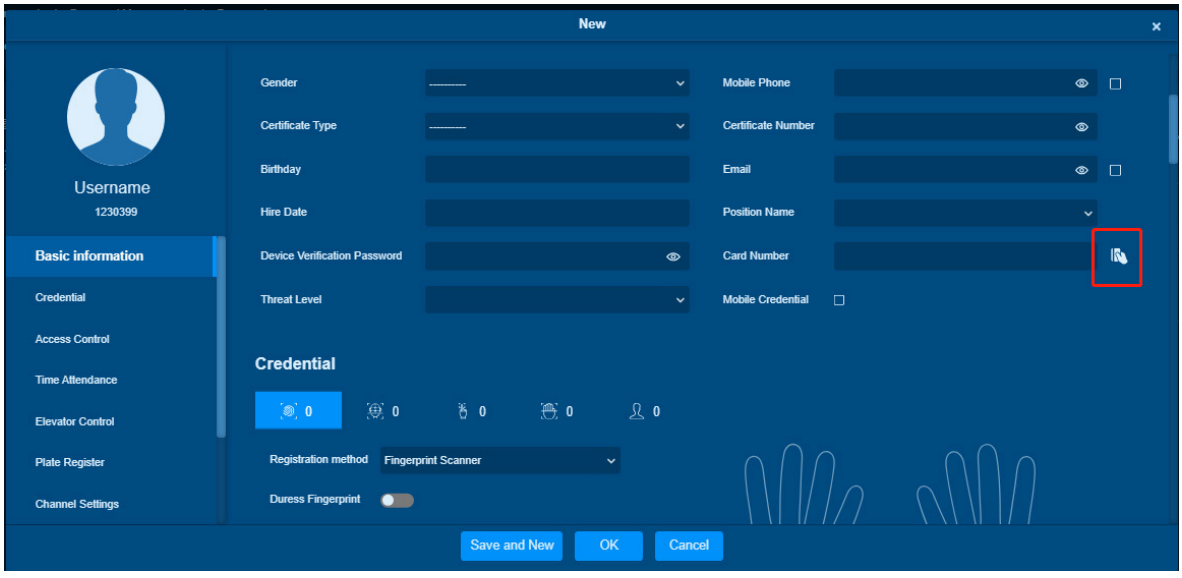
Personnel Images: The software offers an image preview function that supports various common picture formats, including JPG, JPEG, BMP, PNG, GIF, etc. To ensure the best display, we recommend using an image size of 120×140 pixels.

● Adding Card

If you know the card number, you can manually enter the card. Otherwise, click on the button to select a reader. Swipe the card at the selected reader to input the card number.

Note:

This reader should be connected to the panel via Wiegand/RS-485/OSDP.



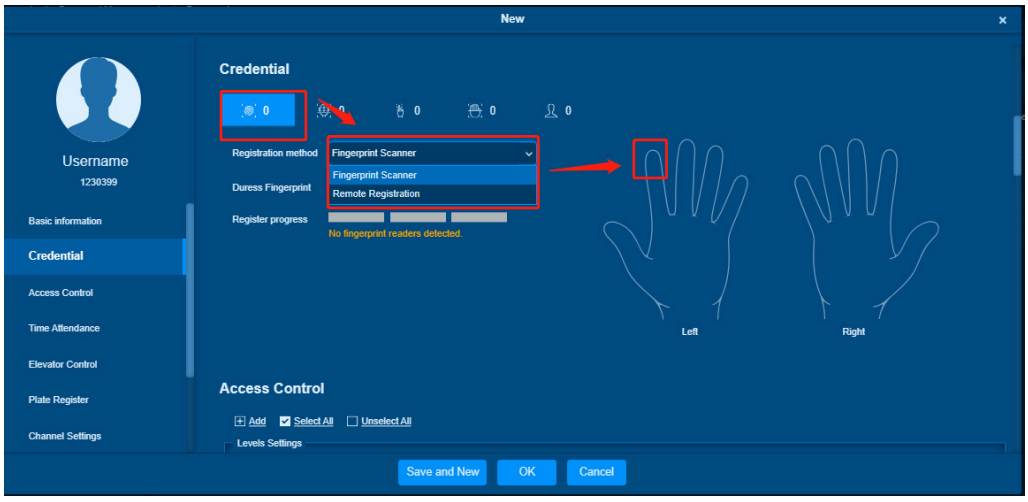
Registering a Fingerprint

1. Move the cursor to the fingerprint icon position. A registration pop-up or driver download box will appear. Click on [Register].

2. Click [Fingerprint Scanner] if using a fingerprint reader; otherwise, click '[Remote Registration]' for using remote standalone device.

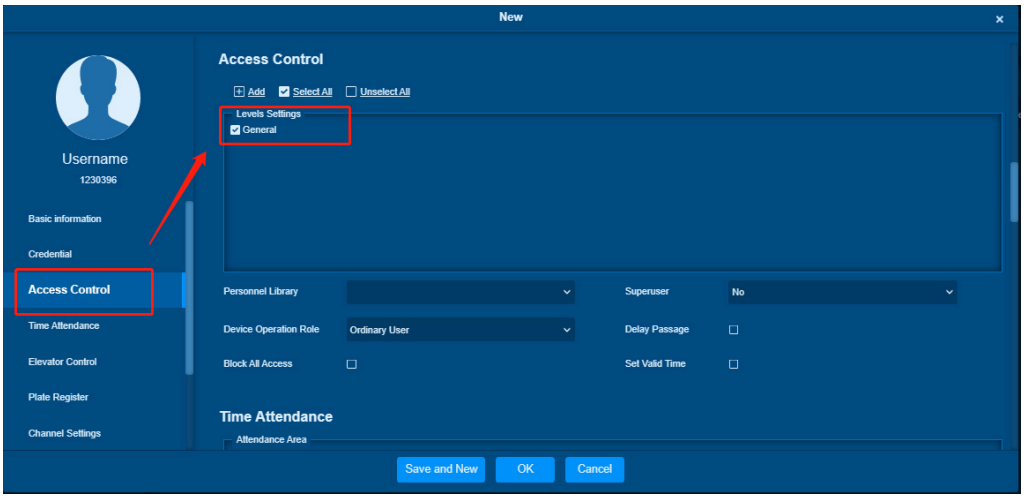
3. Select a finger and press it on the sensor three times. Once the fingerprint is successfully registered, a message 'Fingerprint registered successfully' will appear on the interface.

4. Click [OK] to finalize the registration process.



5. To configure Personnel Permission Settings, click on [Access Control], then select [General].

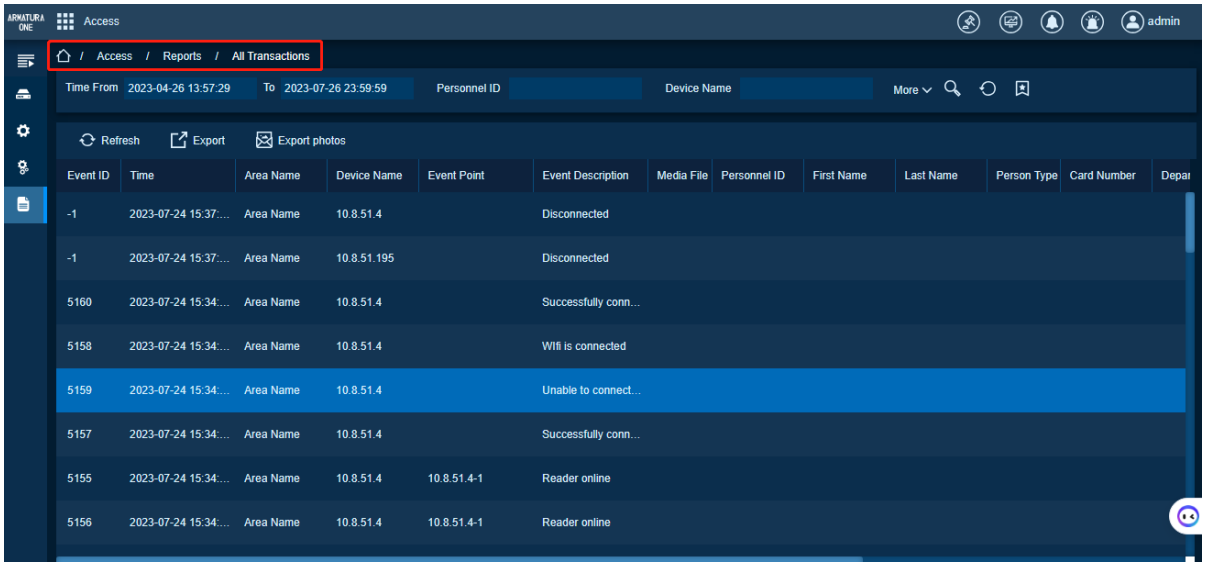
6. Click [OK] to save the settings.



9 Verifying Access

1. Use your configured permissions for door access: Swipe your card, perform a face scan, or verify your fingerprint on the device to gain access to the door.

2. If access is granted, you can view the event log in the software by navigating to [Access] > [Reports] > [All Transactions].



ARMATURA

ARMATURA LLC www.armatura.us E-mail:sales@armatura.us