ARMATURA

User Manual

FT10CMQ

Date: October 2024

Version: 1.0

Copyright © 2024 ARMATURA LLC. All rights reserved.

Trademark

ARMATURA is a registered trademark of ARMATURA LLC. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the Armatura equipment. The copyright in all the documents, drawings, etc. in relation to the Armatura supplied equipment vests in and is the property of Armatura. The contents hereof should not be used or shared by the receiver with any third party without express written permission of Armatura.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact Armatura before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/ equipment. It is further essential for the safe operation of the machine/unit/ equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

Armatura offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. Armatura does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

Armatura does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

Armatura in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or

referenced by this manual, even if Armatura has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. Armatura periodically changes the information herein which will be incorporated into new additions/amendments to the manual. Armatura reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/ equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

Armatura shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.armatura.us.

If there is any issue related to the product, please contact us.

Armatura LLC. Co., Ltd.

Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005 USA

Phone: +1-650-4556863

For business related queries, please write to us at: sales@armatura.us.
To know more about our global branches, visit www.armatura.us.

About the Manual

This manual introduces the operations of **FT10CMQ**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

Table of Contents

1. Data Security Statement

ARMATURA, as a smart product supplier, may also need to know and collect some of your personal information in order to better assist you in using ARMATURA's goods and services, and will treat your privacy carefully by developing a Privacy Policy.

Please read and understand completely all the privacy protection policy regulations and key points that appear on the device before using ARMATURA products.

As a product user, you must comply with applicable laws and regulations related to personal data protection when collecting, storing, and using personal data, including but not limited to taking protective measures for personal data, such as performing reasonable rights management for devices, strengthening the physical security of device application scenarios, and so on.

1.1 Safety Measures

The below instructions intend to ensure that the user can use the product correctly to avoid danger or property loss. The following precautions are to keep users safe and prevent any damage. Please read carefully before installation.

⚠ Noncompliance with instructions could lead to product damage or physical injury (may even cause death).

1. **Read, follow, and retain instructions** - All safety and operational instructions must be properly read and followed before bringing the device into service.

2. **Do not ignore warnings** - Adhere to all warnings on the unit and in the operating instructions.

3. **Accessories** - Use only manufacturer-recommended or product-sold accessories. Please do not use any other components other than manufacturer suggested materials.

4. **Precautions for the installation** – Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.

5. **Service** - Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.

6. **Damage requiring service** - Disconnect the system from the Mains AC or DC power source and refer service personnel under the following conditions:

   - *When cord or connection control is affected.*
   - *When the liquid spilled, or an item dropped into the system.*
   - *If exposed to water or due to inclement weather (rain, snow, and more).*
   - *If the system is not operating normally, under operating instructions.*

   Just change controls defined in operating instructions. Improper adjustment of the controls may result in damage and involve a qualified technician to return the device to normal operation.

   And do not connect multiple devices to one power adapter as adapter overload can cause over-heat or fire hazard.

7. **Replacement parts** - When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.

8. **Safety check** - On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.

9. **Power sources** - Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.

10. **Lightning** - Can install external lightning conductors to protect against electrical storms. It stops power-ups from destroying the system.

    Recommended installing the devices in areas with limited access.

1.2 Electrical Safety

1. Before connecting an external cable to the device, complete grounding properly, and set up surge protection; otherwise, static electricity will damage the mainboard.

2. Make sure that the power has been disconnected before you wire, install, or dismantle the device.

3. Ensure that the signal connected to the device is a weak-current (switch) signal; otherwise, components of the device will get damaged.

4. Ensure that the standard voltage applicable in your country or region is applied. If you are not sure about the endorsed standard voltage, please consult your local electric power company. Power mismatch may cause a short circuit or device damage.

5. In the case of power supply damage, return the device to the professional technical personnel or your dealer for handling.

6. To avoid interference, keep the device far from high electromagnetic radiation devices, such as generators (including electric generators), radios, televisions, (especially CRT) monitors, or speakers.

1.3 Operation Safety

1. If smoke, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.

2. Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.

3. If the device has major defects that you cannot solve, contact your dealer as soon as possible.

4. Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.

5. Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.

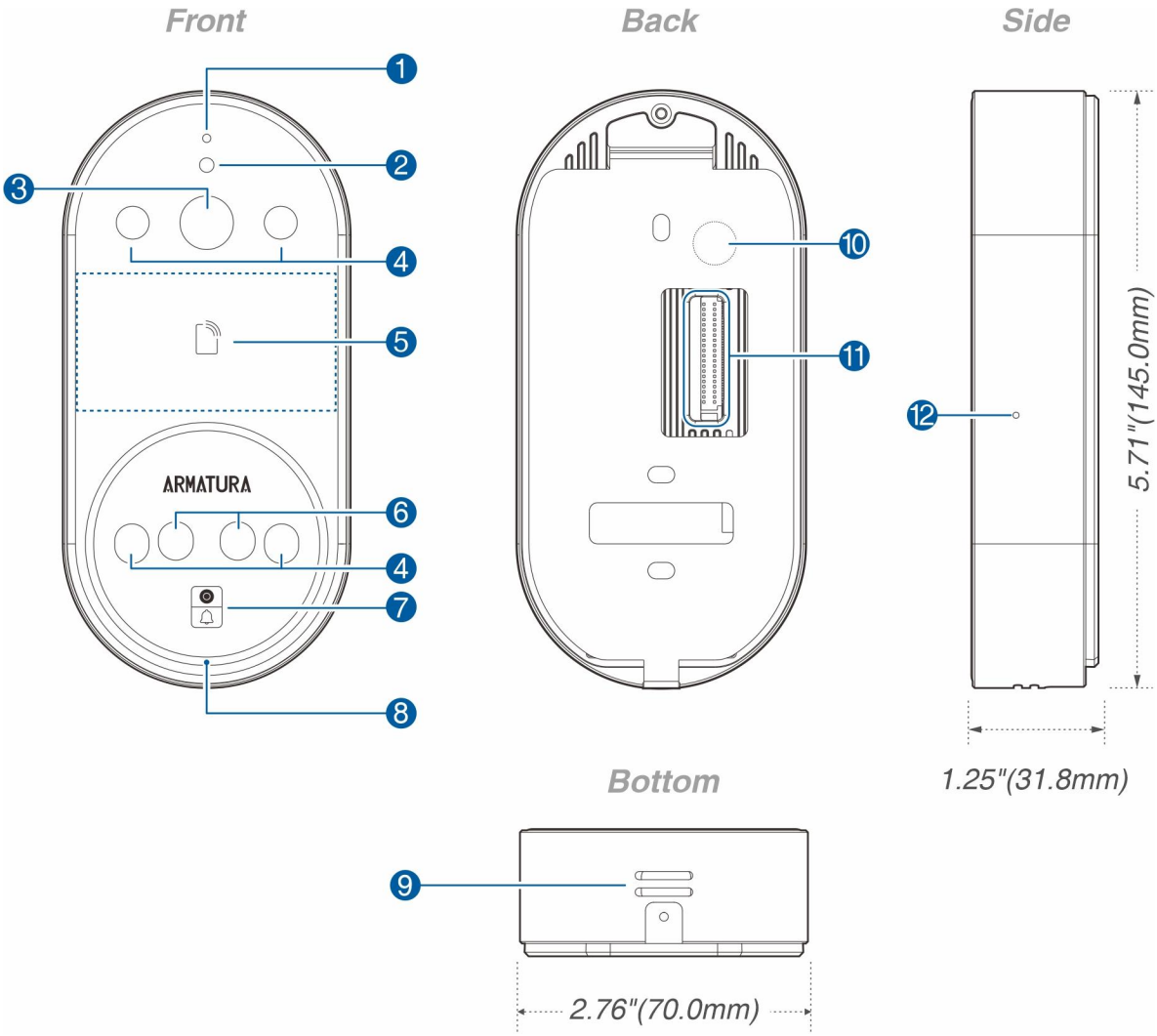
6. Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.

7. If you have any technical questions regarding usage, contact certified or experienced technical personnel.

Note:

- *Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.*
- *Make sure to connect the wires following the positive polarity and negative polarity shown on the device's nameplate.*
- *The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.*

2. Appearance

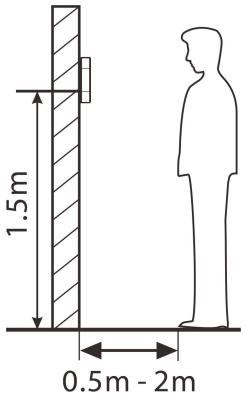


NO.	Descriptions	NO.	Descriptions
1	Microphone	7	Touch Doorbell
2	Proximity sensor	8	LED Indicator
3	Security Camera	9	Speaker
4	Near-Infrared Flash	10	Tamper Switch
5	Card Reading Area	11	Terminal Block
6	Binocular Camera	12	Reset

3. Instruction for Use

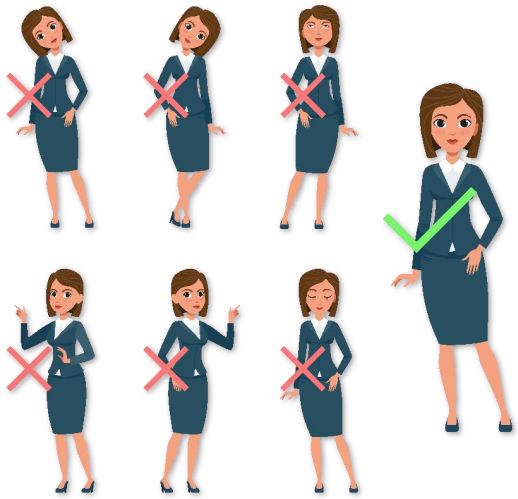
3.1 Standing Position, Posture and Facial Expression

The recommended distance



The distance between the device and a user whose height is in a range of 1.55 m to 1.85 m is recommended to be 0.5 m to 2 m. Users may slightly move forward or backward to improve the quality of facial images captured.

Recommended standing posture and facial expression:



Standing Posture

Facial Expression

Note: *During enrollment and verification, please remain natural facial expression and standing posture.*

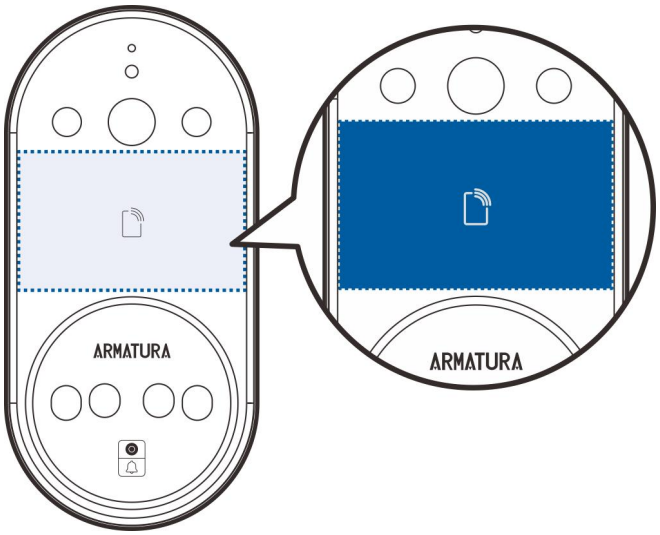
3.2 Recommended Palm Gestures

Note:

- *Place your palm within 200 to 400 mm of the device.*
- *Place your palm in the palm collection area, such that the palm is placed parallel to the device.*
- *Make sure to keep space between your fingers.*

3.3 Recommended Method for Swiping Card

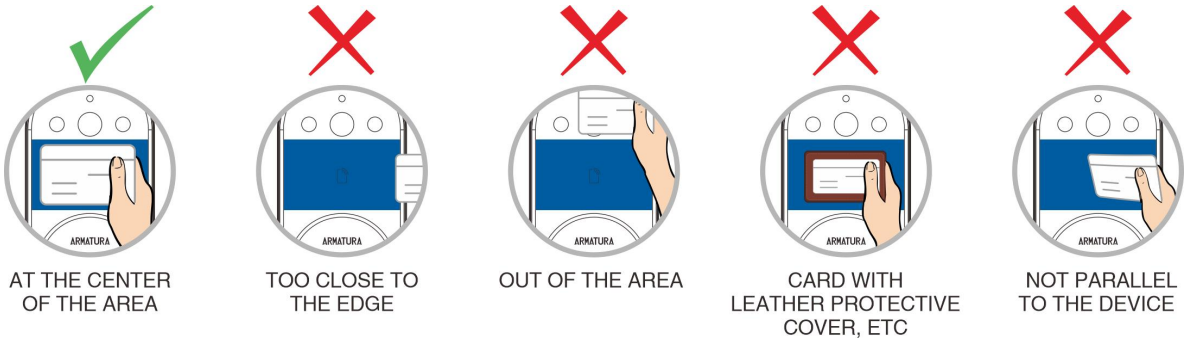
The Specific Range of Card Reading Area:



Notes for Swiping Card:

1. Supports card orientation in horizontal, vertical, and oblique directions.
2. The card should be placed parallel to the device.
3. Ensure that the card is at the center of the card reading area.

Frequency	Protocols	Card Types	Max Range
125KHz	\	EM4100	25mm
	\	HID Prox	30mm
13.56MHz	ISO14443A	MIFARE	20mm
		DESFire	15mm
		HID iCLASS SEOS	10mm
	ISO15693	HID iCLASS/SE/SR/Elite	50mm
	ISO18092	FeliCa	20mm



3.4 Tamper Switch

The tamper switch is pressed and held down with a rear cover. When the device is dismantled, the tamper switch will be lifted and then it will send an alarm signal to trigger an alarm.

Clear Alarm: The user can clear the alarm by putting the magnet back on the tamper switch.

Restore Factory Defaults: The factory defaults can be restored through the tamper switch.

After normal startup of the device, place the magnet (place and remove) on the tamper switch no less than **6** times, and then swipe the card. The interval between each movement of magnet and card swiping action should not be more than **10** seconds. After successful operation, the indicator light will flash amber color for **5** seconds. Then it means the restoration of factory settings is successful and the device will reboot.

Note:

- *The user data will be cleared including the administrator and ordinary users.*
- *The IP address of the device and the login password of the Webserver will be restored to default.*

4. Installation Set-up

Ensure that the device is installed following the provided installation instructions. Failure to do so may result in voiding of the devices warranty.

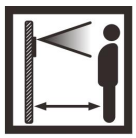
4.1 Installation Environment

Please refer to the following recommendations for installation.

KEEP DISTANCE

AVOID GLASS REFRACTION

AVOID DIRECT SUNLIGHT AND EXPOSURE



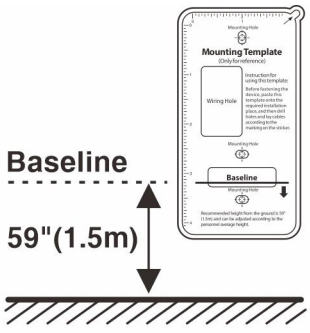
KEEP EFFECTIVE DISTANCE 0.5-2m

4.2 Installation Steps

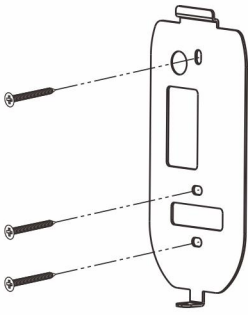
With Backplate:

1. Attach the mounting template sticker to the wall, and drill holes according to the mounting paper.
2. Fix the Backplate on the wall using wall mounting screws.
3. Attach the device to the Backplate.
4. Fasten the device to the Backplate with a security screw.

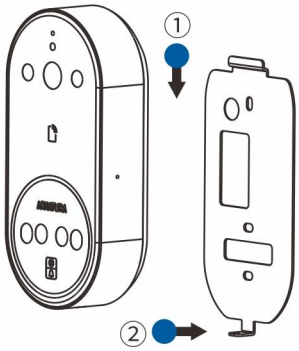
❶



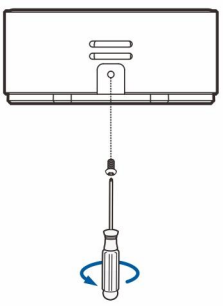
❷



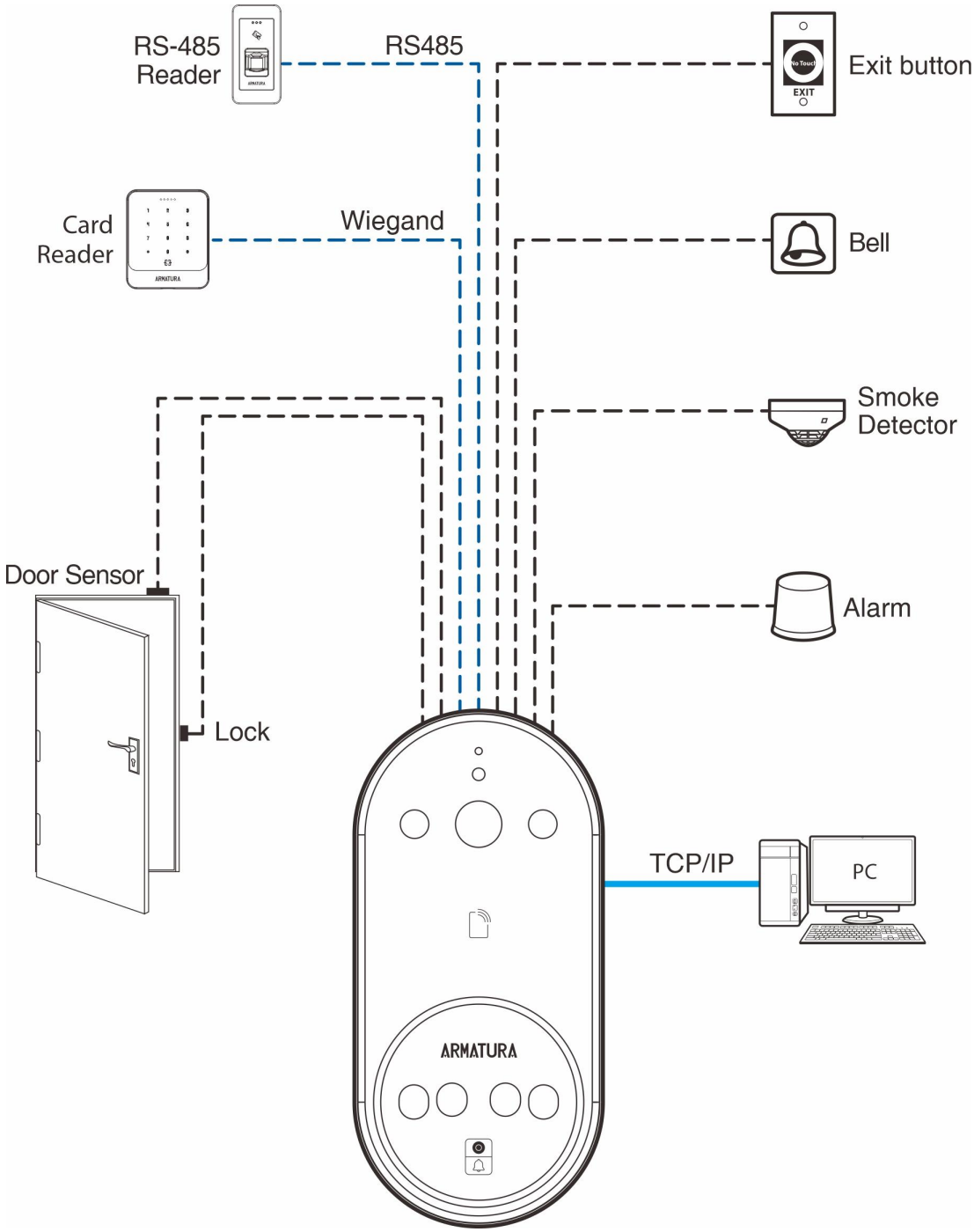
❸



❹

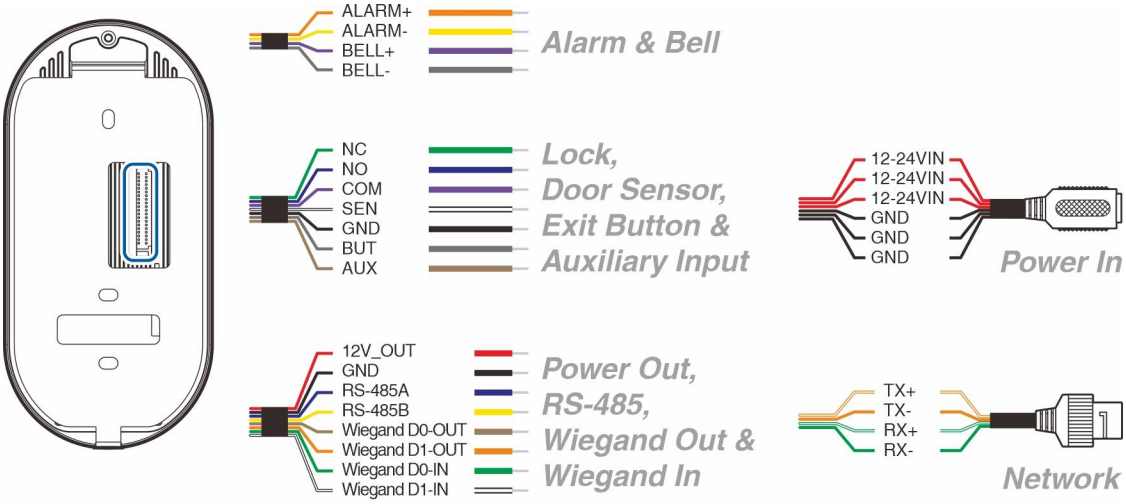


5. Standalone Installation



6. Terminal and Wiring Description

6.1 Terminal Description



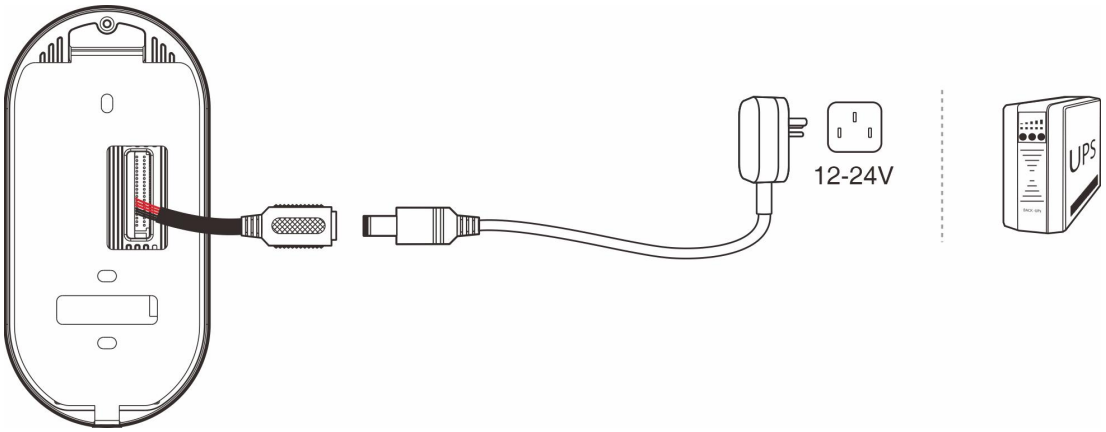
Name	Interface	Colour	Description
Alarm	ALARM+	Orange	Alarm Input (For the access of Door Contact)
	ALARM-	Yellow	
Door Bell	BELL+	Purple	Door Bell Input
	BELL-	Gray	
Lock	NC	Green	Door Lock Relay Output (NC)
	NO	Blue	Door Lock Relay Output (NO)
	COM	Purple	Common Interface
Door Sensor	SEN	White	Door Sensor Input
	GND	Black	
Exit Button	BUT	Gray	Exit Button Input
Auxiliary Input	AUX	Brown	Auxiliary Input
Power Output	12V-OUT	Red	12V DC Output
	GND	Black	
RS-485	RS-485A	Blue	RS-485 Communication Interface
	RS-485B	Yellow	

Wiegand Out	Wiegand D0-OUT	Brown	Wiegand Output
	Wiegand D1-OUT	Orange	
Wiegand In	Wiegand D0-IN	Green	Wiegand Input
	Wiegand D1-IN	White	
Power Input	12-24VIN	Red	12-24V DC Input It can be powered using either a 12V DC power adapter or PoE, depending on availability. ***Note:*** 1. Recommended AC adapter:**12V, 3A / 24V, 1.5A** 2. To share the power with other devices, use an AC Adapter with higher current ratings.
	12-24VIN	Red	
	12-24VIN	Red	
	GND	Black	
	GND	Black	
	GND	Black	
Ethernet	TX+	Orange White	Network Interface Support PoE, IEEE802.3at Version
	TX-	Orange	
	RX+	Green White	
	RX-	Blue	

6.2 Wiring Description

6.2.1 Power Wiring

The device can be powered using either a 12-24V DC power adapter or PoE, depending on availability.

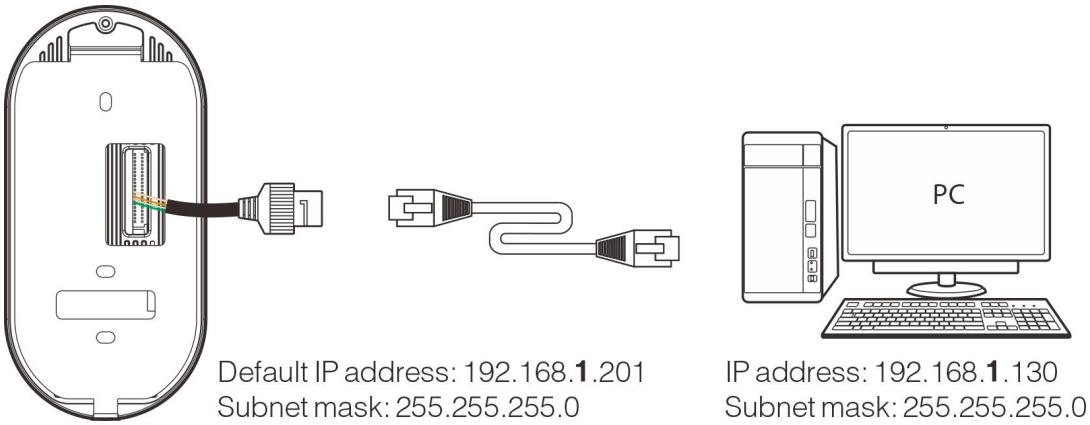


Recommended AC Adapter:

- *12V, 3A / 24V, 1.5A.*
- *To share the power with other devices, use an AC Adapter with higher current ratings.*

6.2.2 Network Wiring

Establish the connection between the device and the software using an Ethernet cable. An illustrative example is provided below:

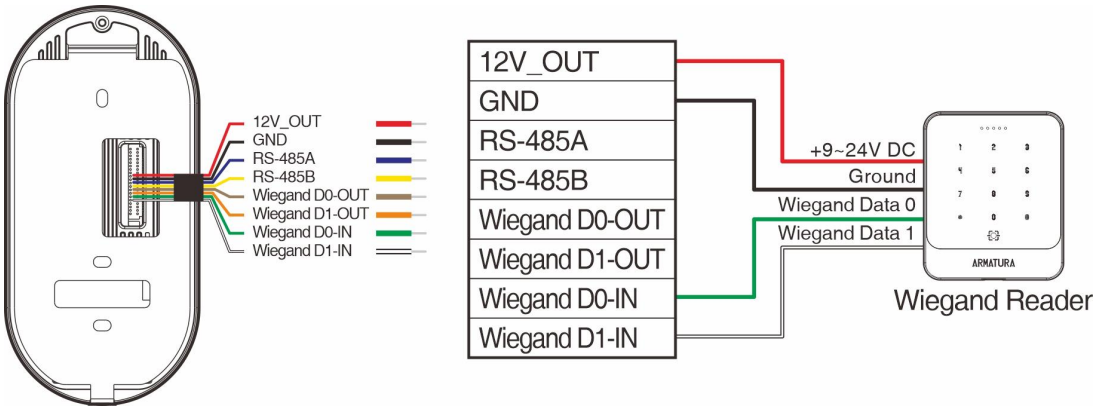


Note:

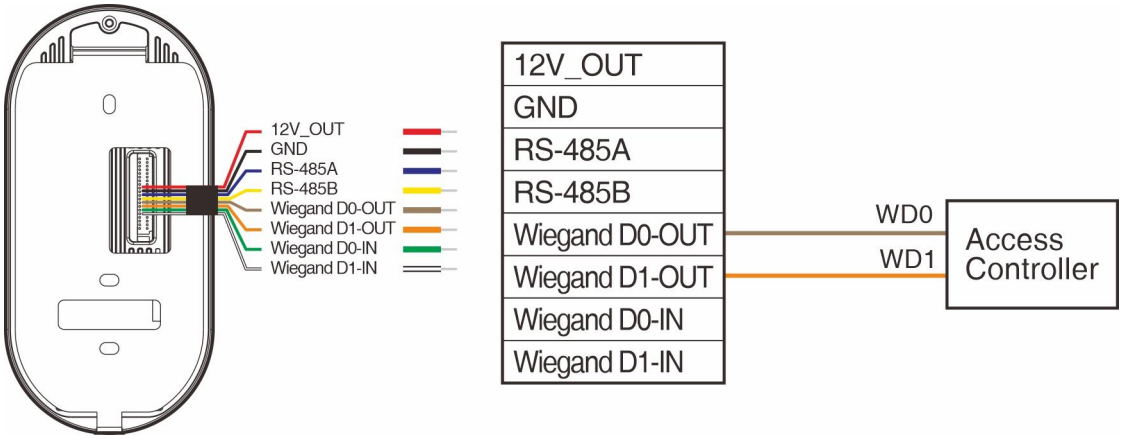
- *On the Webserver, click [**Advanced Settings**] > [**COMM.**] > [**IP Address**] to input the IP address.*
- *In LAN, the IP addresses of the server (PC) and the device must be in the same network segment when connecting to the **ARMATURA One** software.*

6.2.3 Wiegand Reader Wiring

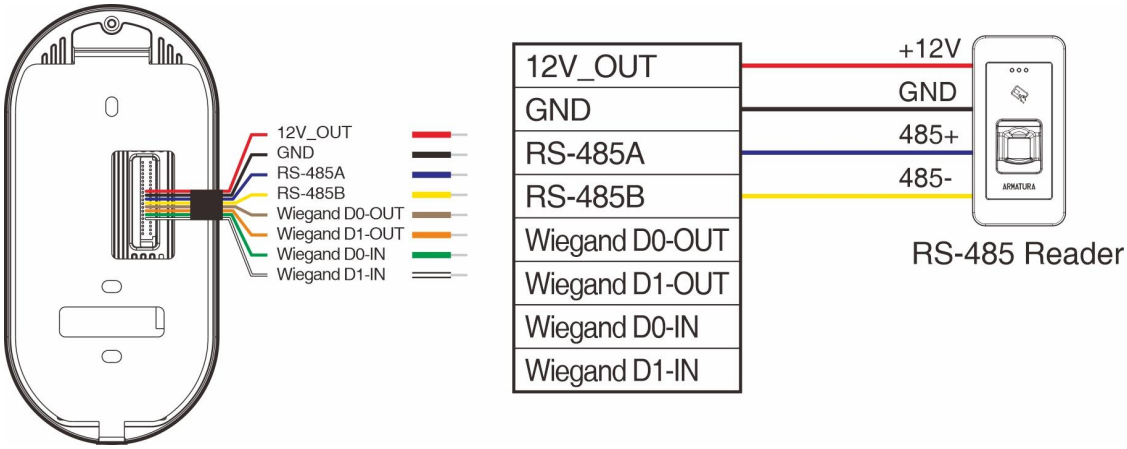
When the device is connected to a Wiegand reader, the wiring diagram is shown below.



When the device is connected to the controller as a Wiegand reader, the wiring diagram is shown below.



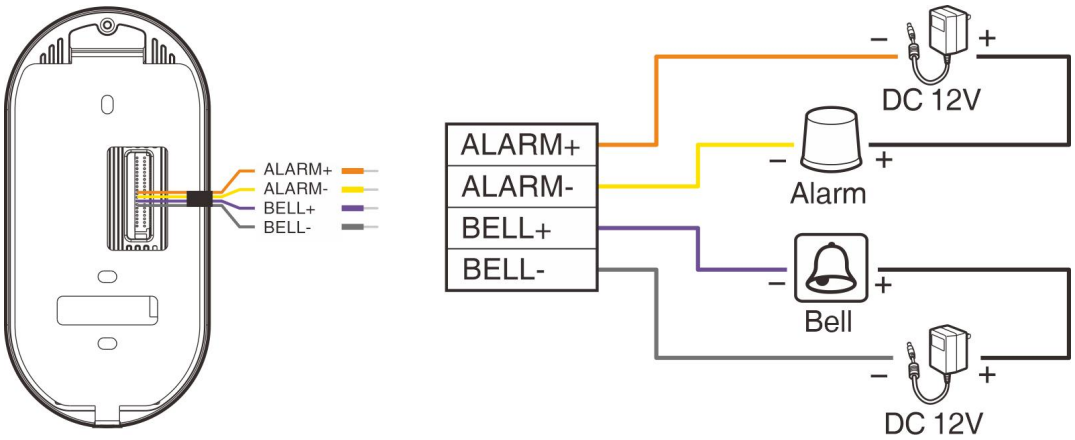
6.2.4 RS-485 Reader Wiring



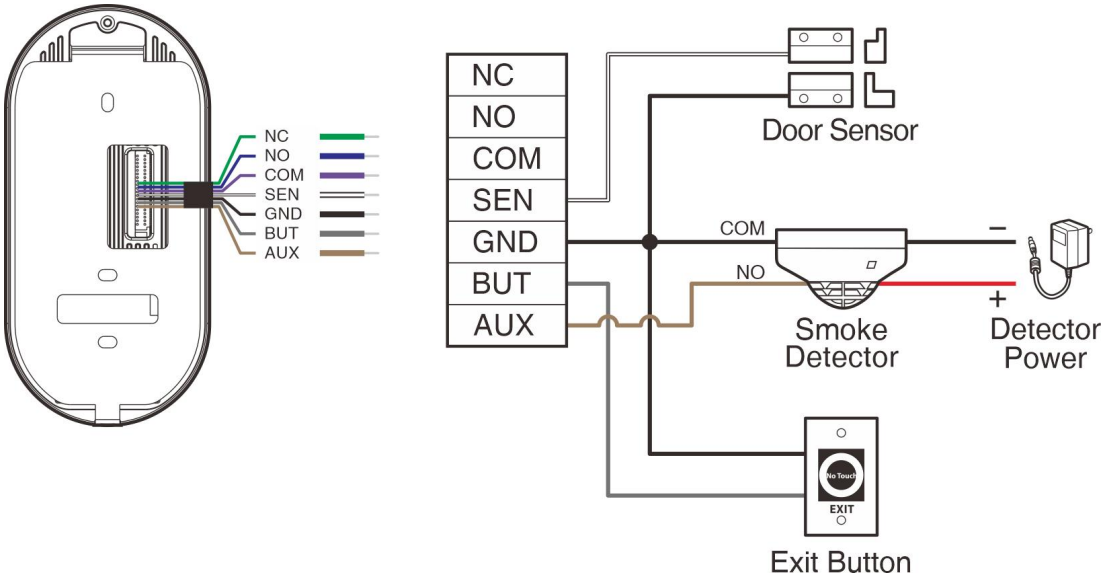
Note:

- *RS-485A and RS-485B can be connected to the Barrier gate or the RS-485 Reader, separately, but cannot be connected to the gate and reader at the same time.*

6.2.5 Alarm, Bell Wiring



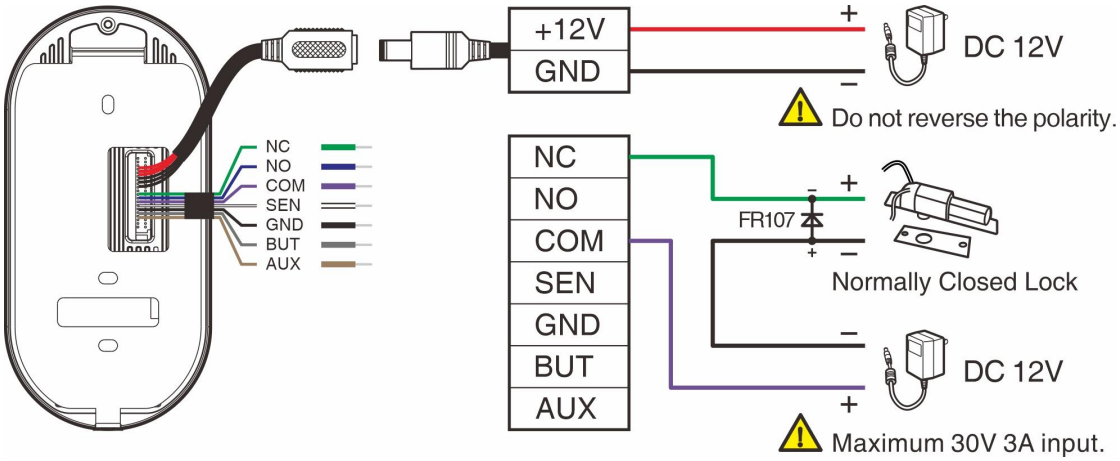
6.2.6 Door Sensor, Exit Button, Auxiliary Wiring



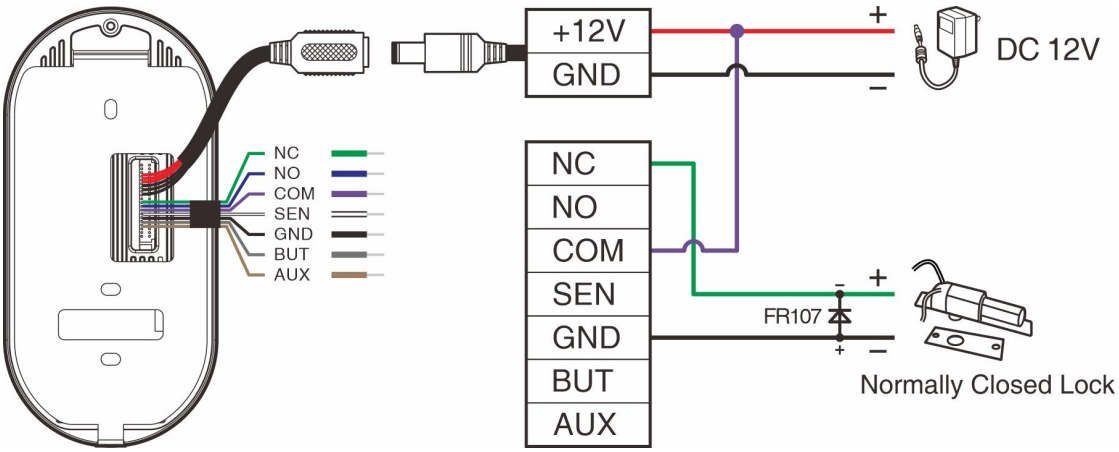
6.2.7 Lock Relay Wiring

The system supports **Normally Opened Lock** and **Normally Closed Lock**. The **NO LOCK** (normally unlocked when power-on) is connected with '**NO**' and '**COM**' terminals, and the **NC LOCK** (normally locked when power-on) is connected with '**NC**' and '**COM**' terminals. Take NC Lock as an example below:

1) Device not sharing power with the lock

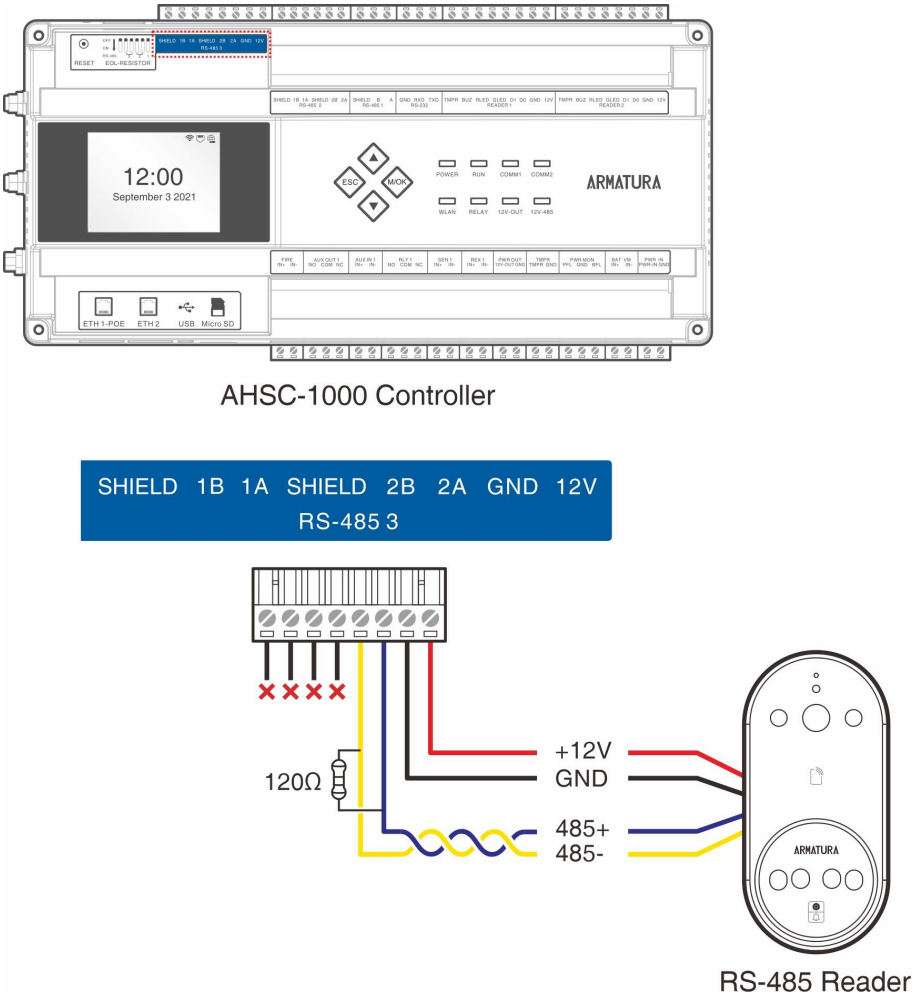


2) Device sharing power with the lock



6.2.8 Controller Wiring

The device can be used as a reader and connected to the AHSC-1000 controller via RS-485.



7. Connect to the Armatura Connect / ID App

7.1 Download the Armatura Connect / ID App

Search for the "**Armatura Connect**" and "**Armatura ID**" App in the iOS App Store or the Google Play Store. Install and log in to the installer account.

Armatura ID

Armatura Connect

Download on the App Store

ANDROID APP ON Google play

7.2 Activate your credentials on the Armatura ID App

When you register as a user of Armatura ID, you will receive an email with activation code from Armatura. Please activate your mobile credential according to the following steps.

1. Click the link on the email to activate.
2. Or scan the QR code or input the activation code in the email on the App to activate.
3. Activate successfully, enjoy with your Mobile Credentials.

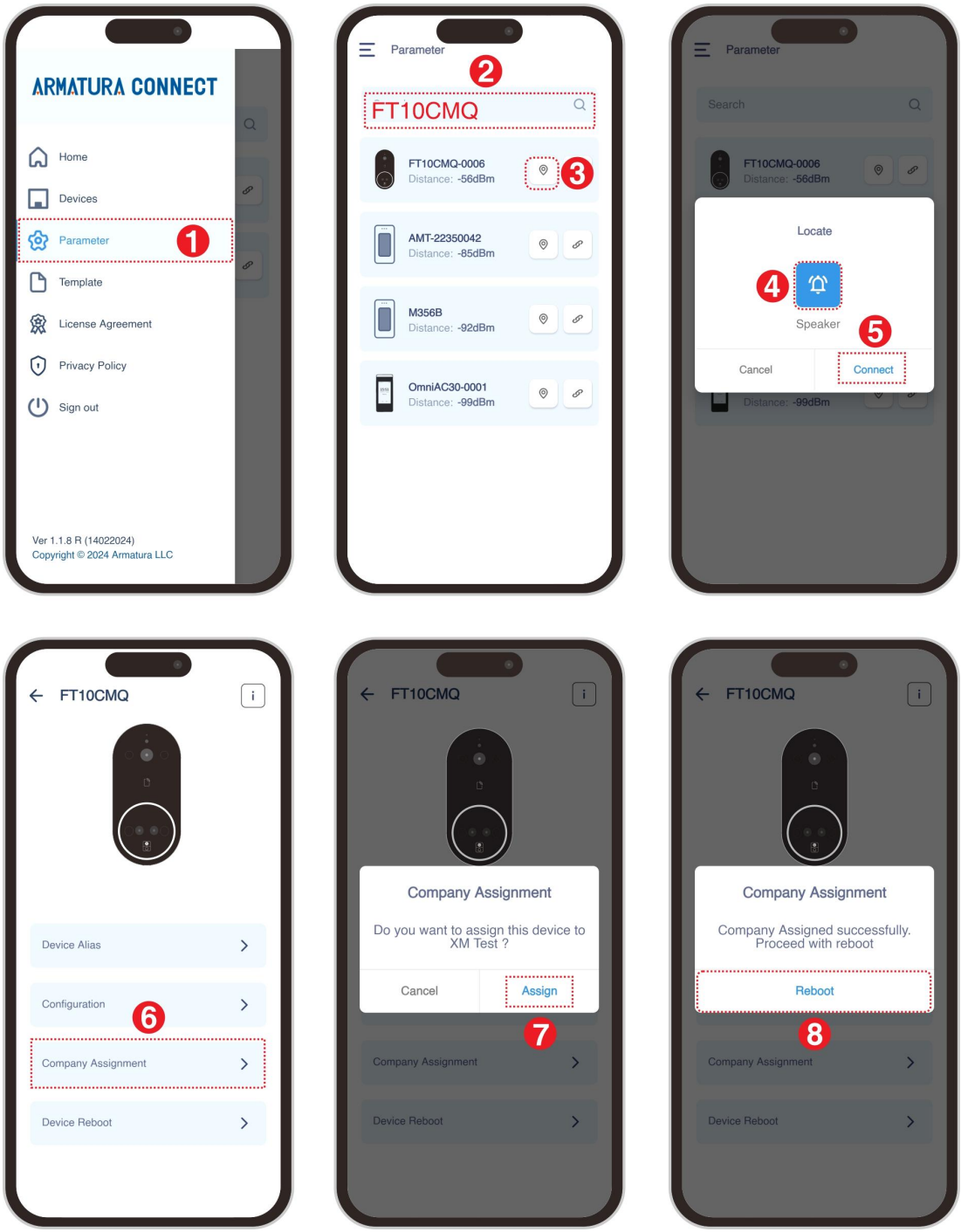
7.3 Login to the Armatura Connect App

1. Open the Armatura Connect App and enter the installer account and password.
2. Click [Sign In] to log into the Armatura Connect App.
3. After entering the Welcome Home page, users can search device, set the parameters and set the template.

7.3.1 Company Assign

1. Click icon > [**Parameter**] to enter the parameter interface.
2. Turn on the bluetooth function of the mobile phone. Click icon to search the reader.
3. Find the reader closest to you and click icon to open the locate window. Click button to confirm the reader. Then click [**Connect**] to connect the reader.
4. Click [**Company Assignment**] and select the company in the popup window.
5. Click [**Assign**] to assign the reader to the specified company.

6. After successfully assigning the company, click [**Reboot**] to restart the device.



Note:

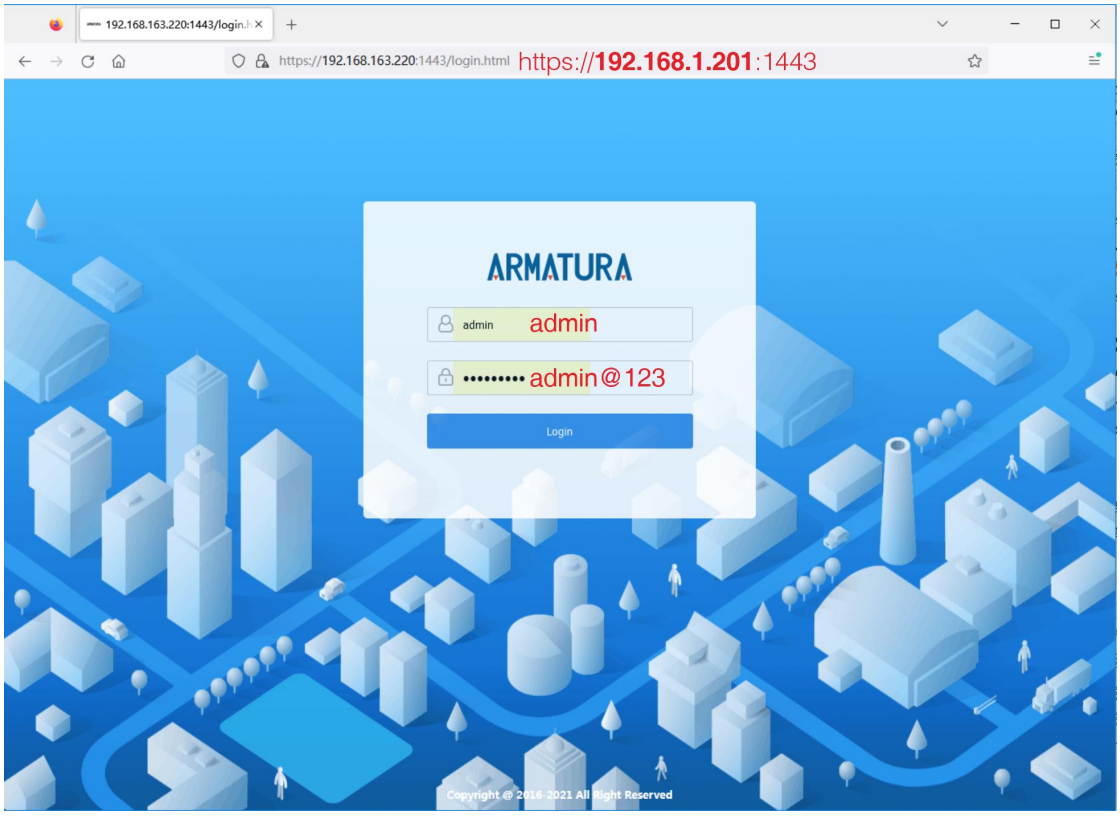
- *For more information, refer to the relevant user manual.*

8. Webserver

8.1 Login to the Webserver

After the device is powered on, connect the device using a network cable. Access the WebServer by entering the IP address and server port in the address bar of your browser. The IP address is set as: https://device IP address:1443.

- The IP address is **https://192.168.1.201:1443** by default.
- The default user name is [**admin**] and the password is [**admin@123**].



Note:

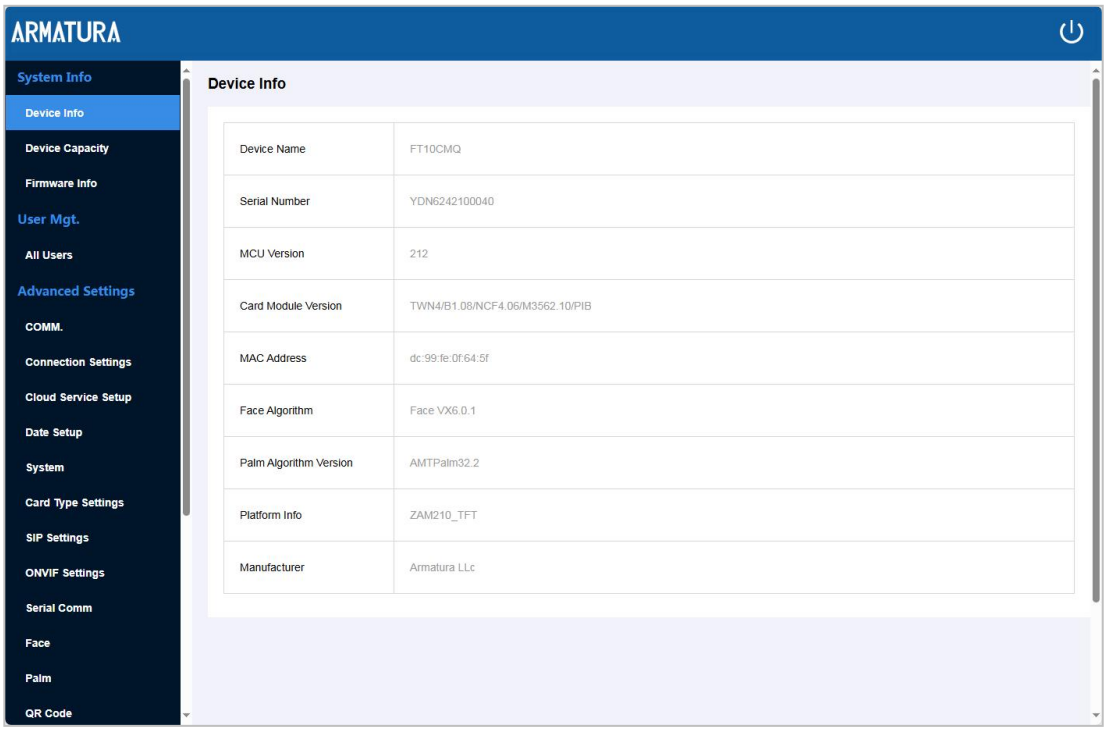
- In *LAN, IP addresses of the server (PC) and the device must be in the same network segment.*

8.2 System Information

8.2.1 Device Information

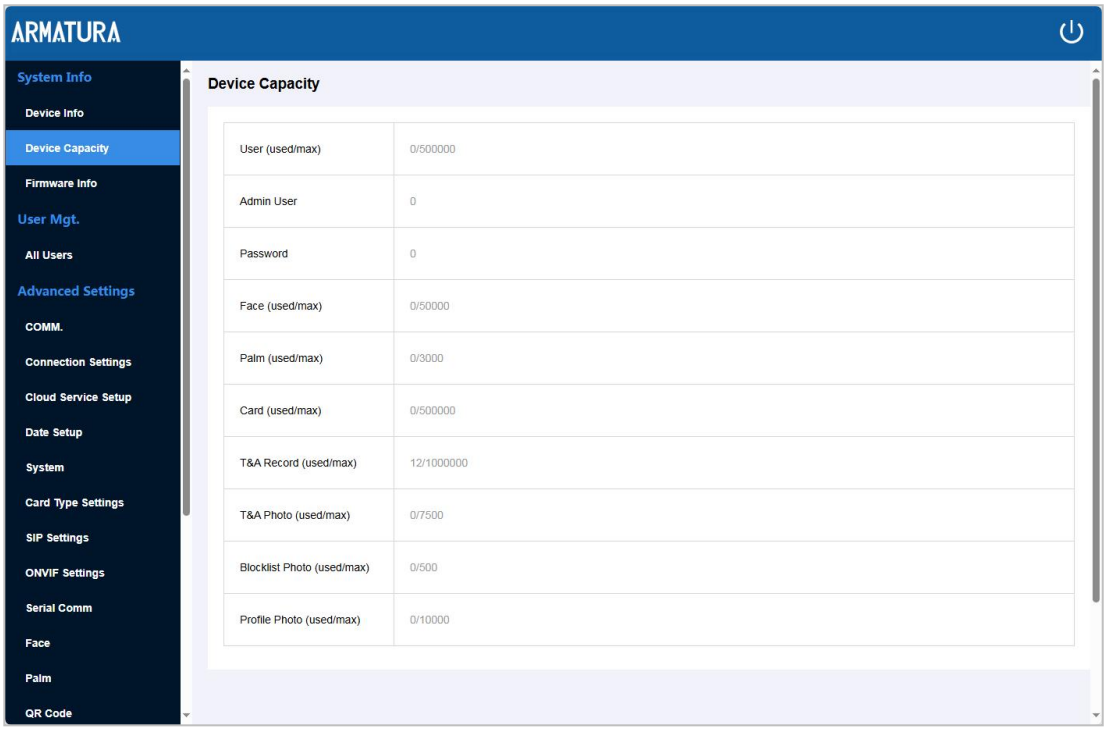
Click [**Device Info**] to view the Device name, Serial number, MCU Version, Card Module Version, MAC address, Face Algorithm, Palm Algorithm Version, Platform Information and Manufacturer of the

current device.



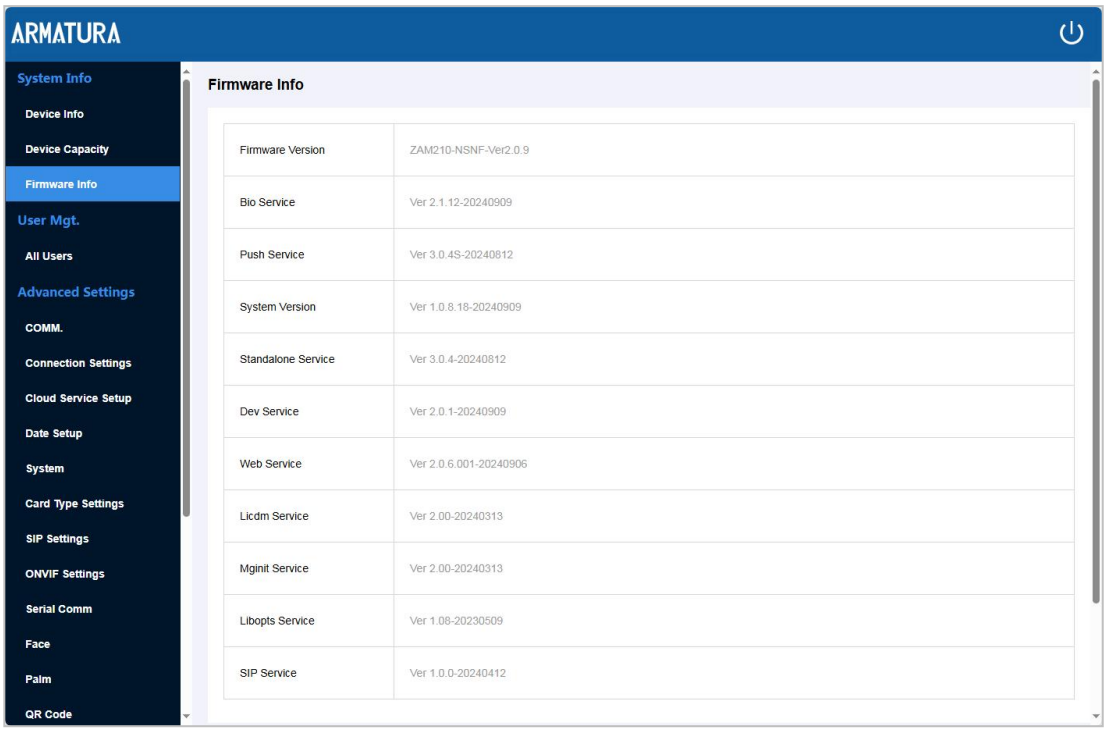
8.2.2 Device Capacity

Click [**Device Capacity**] to view the capacity information of the current device.



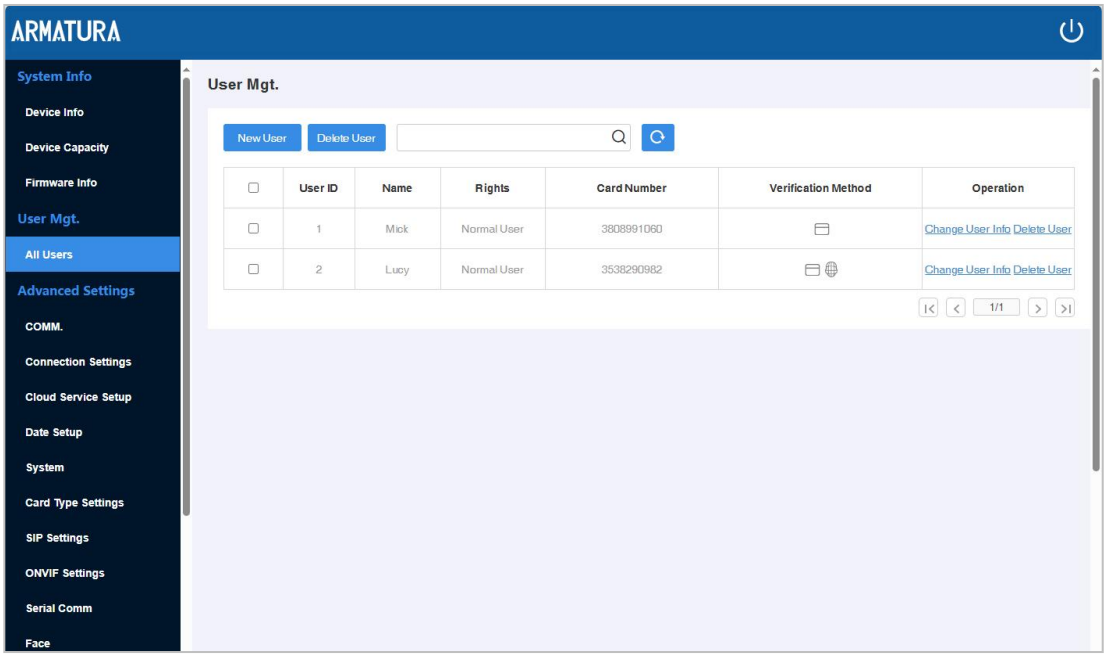
8.2.3 Firmware Information

Click [**Firmware Info**] to view the firmware information of the current device.



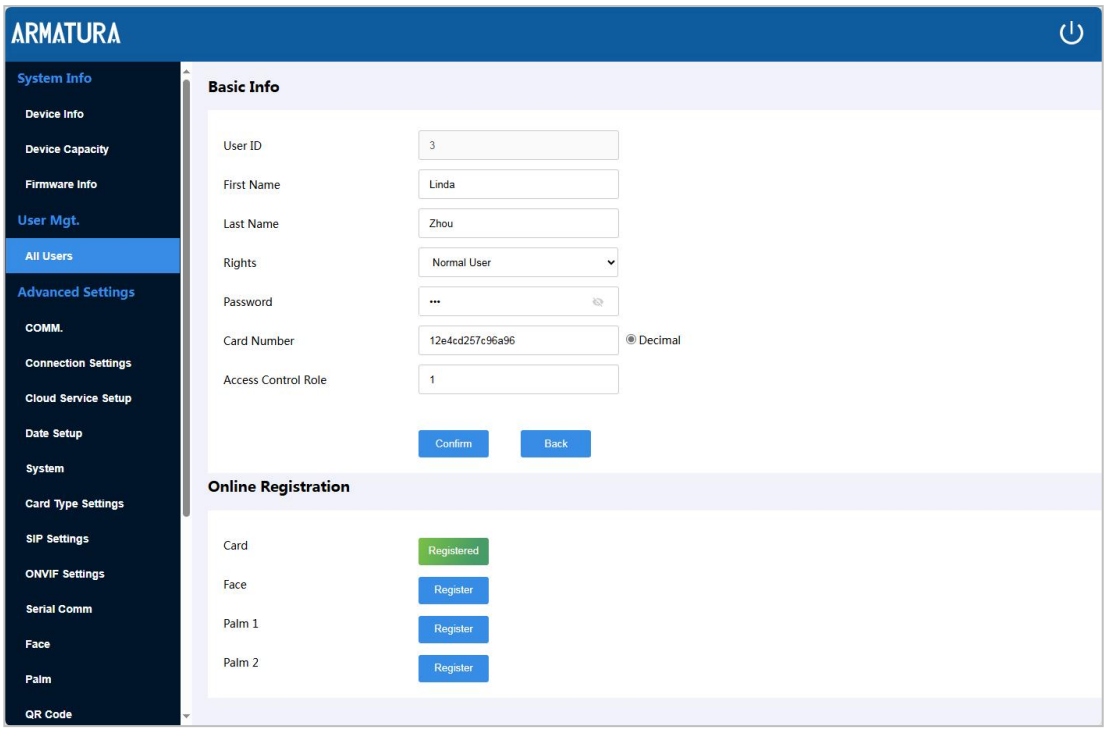
8.3 User Management

You can manage the basic information of the registered users, including User ID, Name, Rights, Card Number, and Verification Method in the User Management.



8.3.1 Add User

Click [**User Mgt.**] > [**All Users**] > [**New User**]:



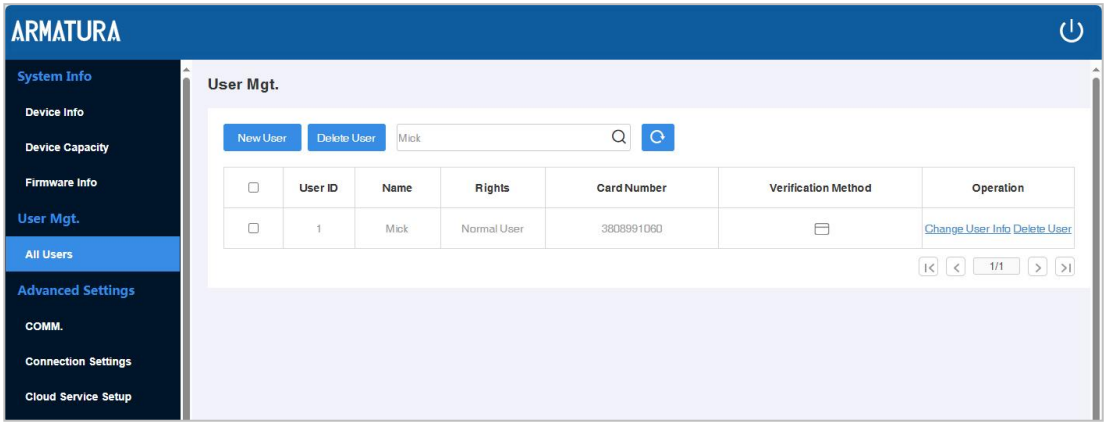
8.3.2 Delete User

Click [**User Mgt.**] > [**All Users**] to enter the user list, then select a person, and click [**Delete User**] > [**Confirm**] to delete.

Note: *All relevant information about the user will be deleted.*

8.3.3 Search a User

Tap the search bar on the user's list and enter the retrieval keyword. Then click icon to search.

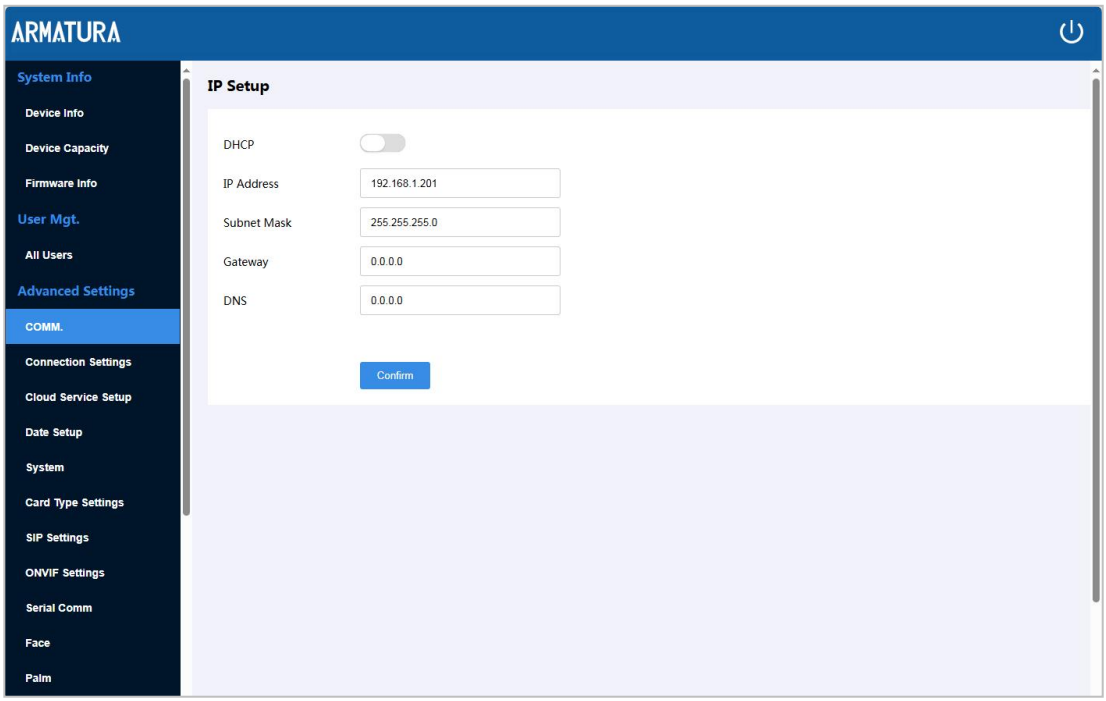


8.4 Advanced Settings

8.4.1 Comm. Settings

When the device needs to communicate with the network, you need to configure the IP settings.

Click [**Advanced Settings**] > [**COMM.**] to set the network parameters.



The fields description is as follows:

DHCP: DHCP (Dynamic Host Configuration Protocol) dynamically allocates the IP addresses for clients via server. If DHCP is enabled, IP addresses cannot be set manually.

IP Address: The default value is192.168.1.201, it can be modified according to the available network parameters.

Subnet Mask: The default value is 255.255.255.0, it can be modified according to the available network parameters.

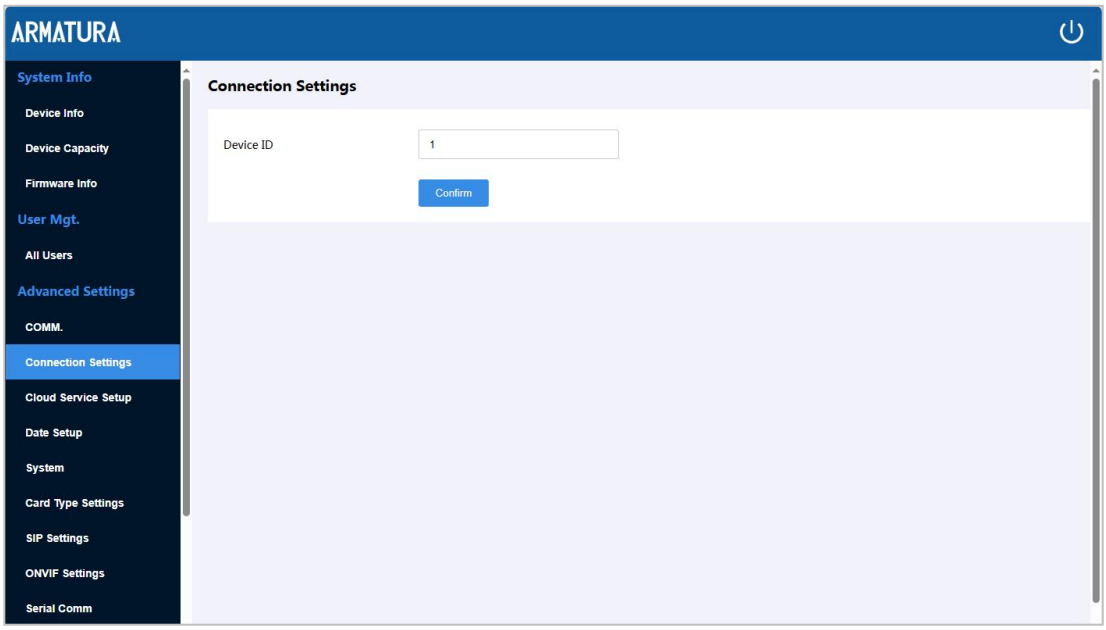
Gateway: The default value is 192.168.1.1, it can be modified according to the available network parameters.

DNS: The default DNS address is 0.0.0.0. It can be modified according to network availability.

8.4.2 Connection Settings

Comm Key facilitates to improve the security of the data by setting up the communication between the device and the PC. Once the Comm Key is set, a password is required to connect the device to the PC software.

Click [**Advanced Settings**] > [**Connection Settings**] to configure the communication settings.



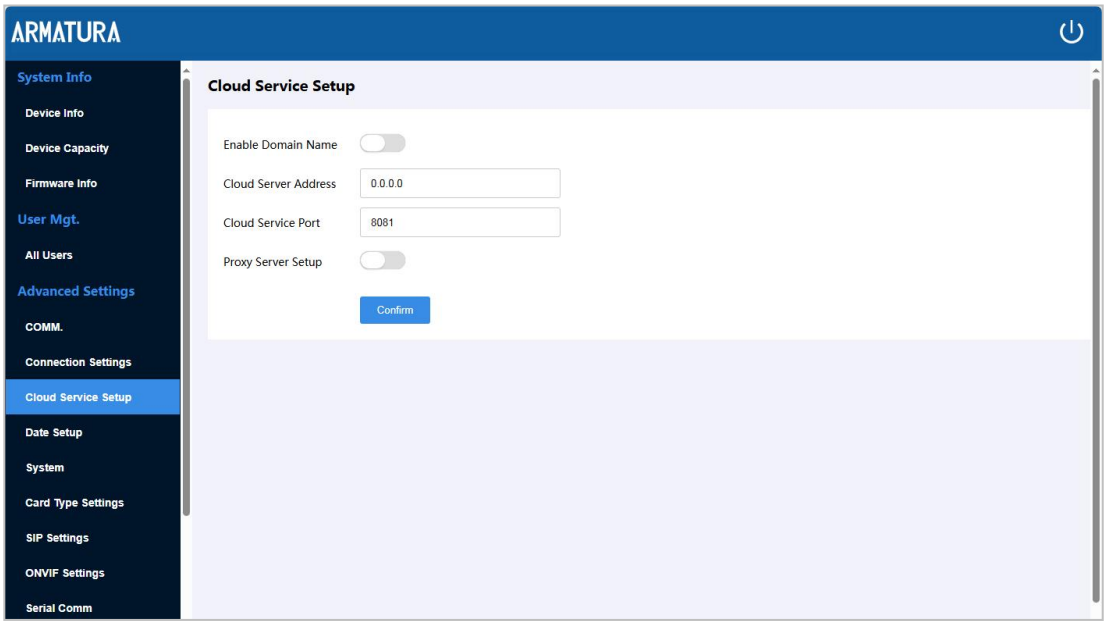
The fields description is as follows:

Device ID: It is the identification number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.

8.4.3 Cloud Service Setting

We can connect to the Cloud server by configuring the Cloud Server Settings.

Click [**Advanced Settings**] > [**Cloud Service Setup**] to set the server address and server port, that is, the IP address and port number of the server after the software is installed.



The fields description is as follows:

Enable Domain Name: When this function is enabled, the domain name mode “https://...” is used, such as https://www.XYZ.com (XYZ denotes the domain name). When this mode is turned OFF, you need to enter the IP address and port to connect to the webserver.

Cloud Server Address: The IP address of the server.

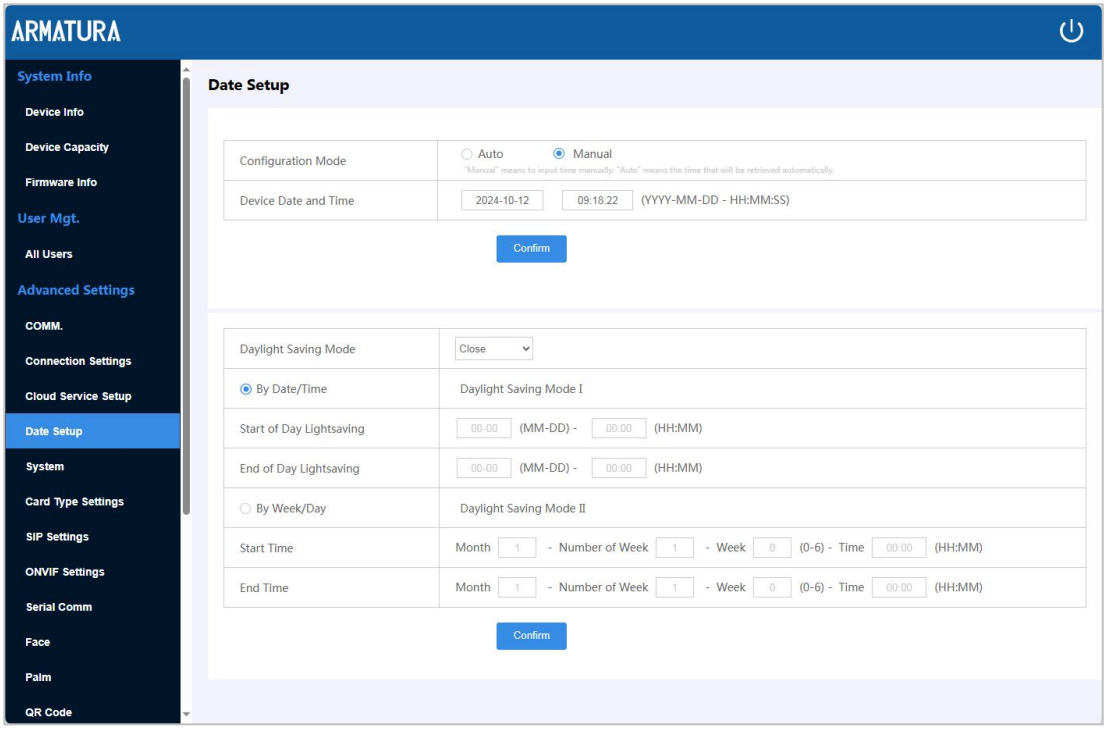
Cloud Server Port: The port of the server.

Proxy Server Setup: The IP address and the port number of the proxy server are set manually when the proxy is enabled.

8.4.4 Date Setup

This function customizes the related settings of the date and time, and Daylight Saving Mode.

Click [**Advanced Settings**] > [**Date Setup**] to set the date and time.



The fields description is as follows:

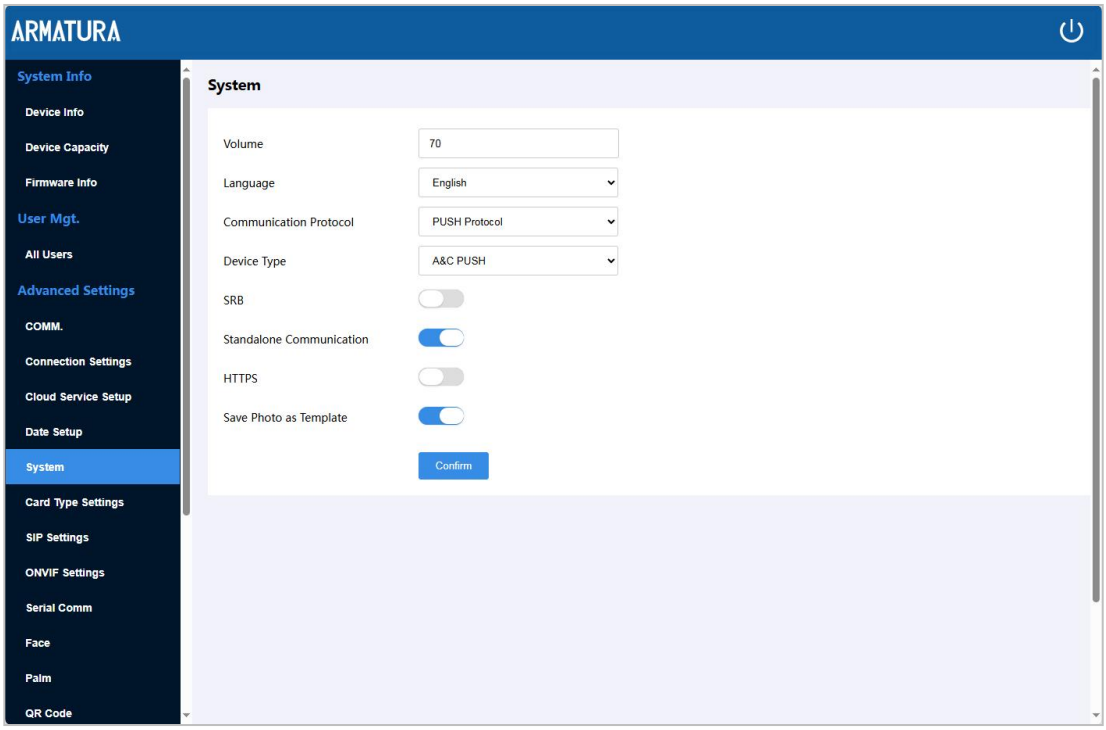
Configuration Mode: Select **Auto** to enable automatic time synchronization based on the service address you enter. Select **Manual** to manually set the date and time and then tap to Confirm and save.

Daylight Saving Mode: Tap **Daylight Saving Mode** to open or close the function. If enabled, tap Daylight Saving Mode to select a daylight-saving mode.

8.4.5 System Settings

The System Settings define the system parameters to optimize the performance of the device.

Click [**Advanced Settings**] > [**System**] to set the system parameters.



The fields description is as follows:

Volume: Set the volume of the device.

Language: Select the language of the device and WebServer interface as required.

Communication Protocol: Set the communication protocol to PUSH protocol.

Device Type: Set the device as T&A PUSH or A&C PUSH.

SRB: When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.

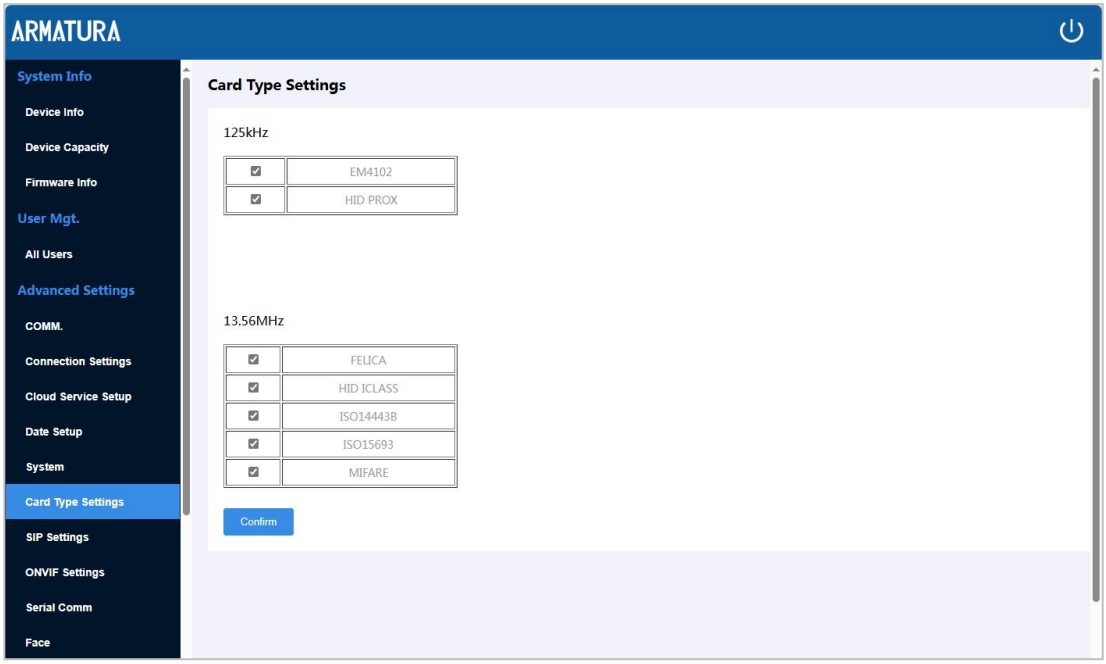
Standalone Communication: To avoid being unable to use when the device is offline, you can download the C/S software on your computer in advance for offline use.

HTTPS: Based on HTTP, transmission encryption and identity authentication ensures the security of the transmission process. **Note:** The device will reboot after modifying this setting and submitting it.

Save Photo as Template: After disable this function, face re-registration is required after an algorithm upgrade.

8.4.6 Card Type Settings

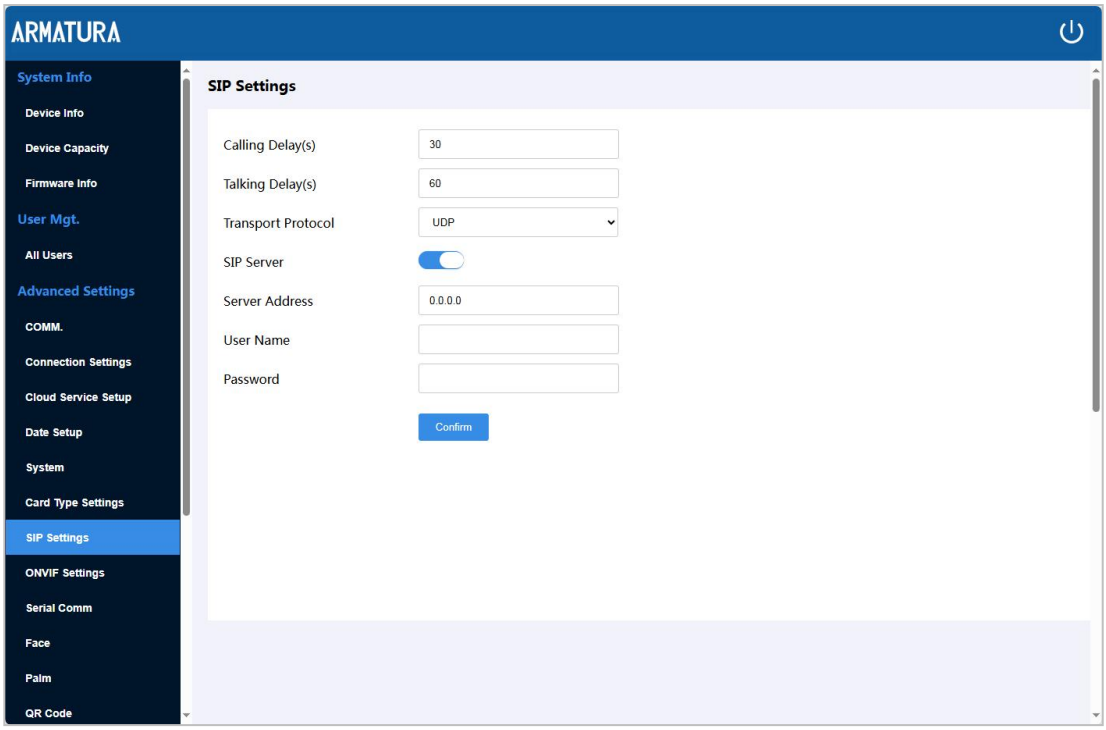
Click [**Advanced Settings**] > [**Card Type Settings**] to set the card type.



8.4.7 SIP Settings

Note: *This function needs to be used with the indoor station.*

Click [**Advanced Settings**] > [**SIP Settings**] to go to the SIP parameter settings.



The fields description is as follows:

Calling Delay(s): Set the time of call, valid value 30 to 60 seconds.

Talking Delay(s): Set the time of intercom, valid value 60 to 120 seconds.

Transport Protocol: Set the transmission protocol between the device and indoor unit. UDP, TCP and TLS options are available..

SIP Server: Select whether to enable the server address. Once you have connected to the server, you can call it by entering the username of the indoor station.

Server Address: Enter the server address.

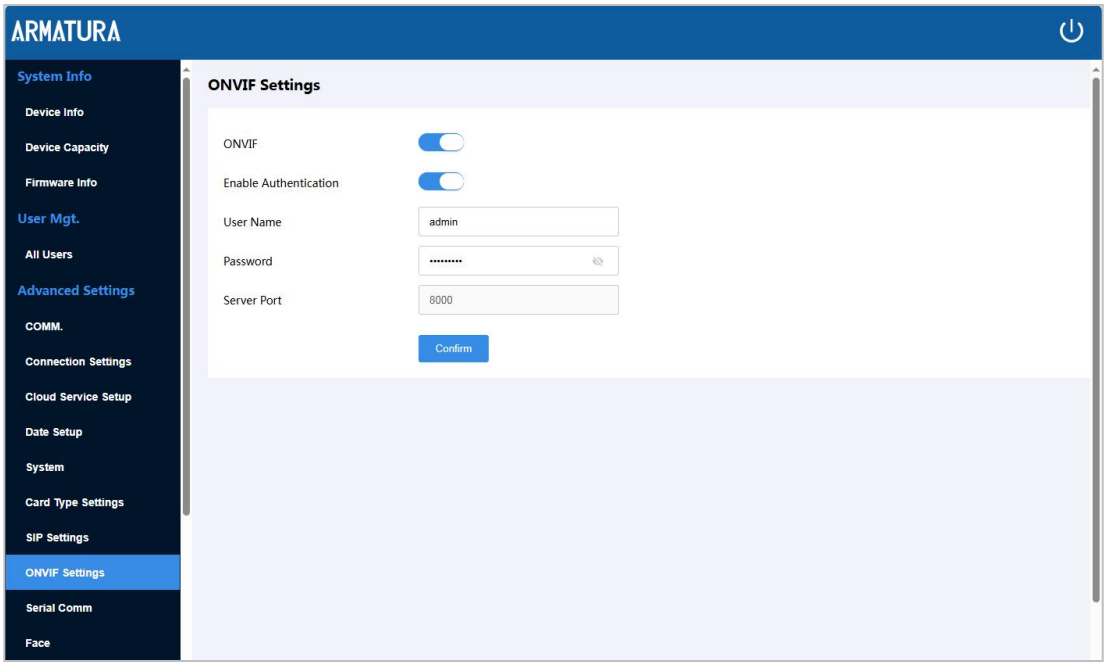
User Name: Enter the Username of server.

Password: Enter the password of server.

8.4.8 ONVIF Settings

Note: *This function needs to be used with the network video recorder (NVR).*

Click [**Advanced Settings**] > [**ONVIF Settings**] to enter the setting interface.



The fields description is as follows:

ONVIF: Enable/Disable the ONVIF function. **Note:** The device will reboot after modifying this setting and submitting it.

Enable Authentication: Enable/Disable the Authentication Function. When it is disabled, there is no need to input the User Name and Password when adding the device to the NVR.

User Name: Set the User Name. The default is admin.

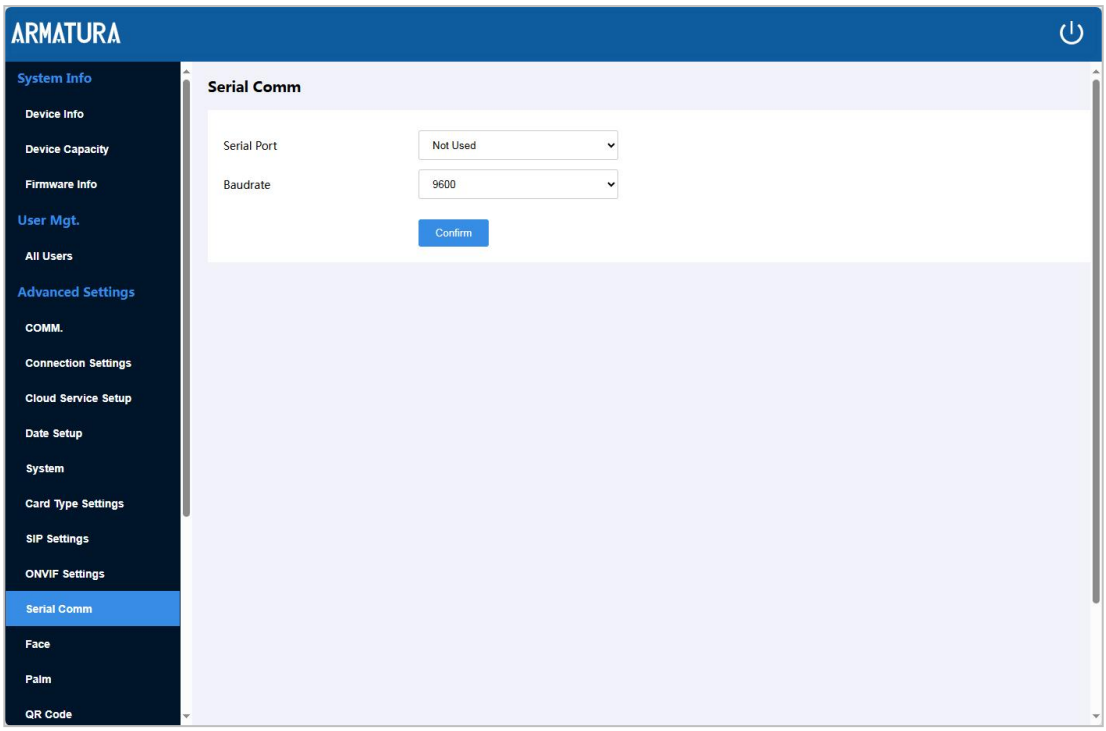
Password: Set the password. The default is admin.

Server Port: The default is 8000, and cannot be modified.

8.4.9 Serial Comm Settings

Serial Comm function facilitates to establish communication with the device through a serial port.

Click [**Advanced Settings**] > [**Serial Comm**] to enter the setting interface.



The fields description is as follows:

Serial Port:

- ✧ **Not Used:** Do not communicate with the device through the serial port.
- ✧ **Control Unit:** Communicates with the device through control unit.
- ✧ **OSDP Peripheral:** Communicates with the device through OSDP peripheral.
- ✧ **OSDP Control Unit:** Communicates with the device through OSDP control unit.
- ✧ **DM10:** Communicates with the device through DM10.

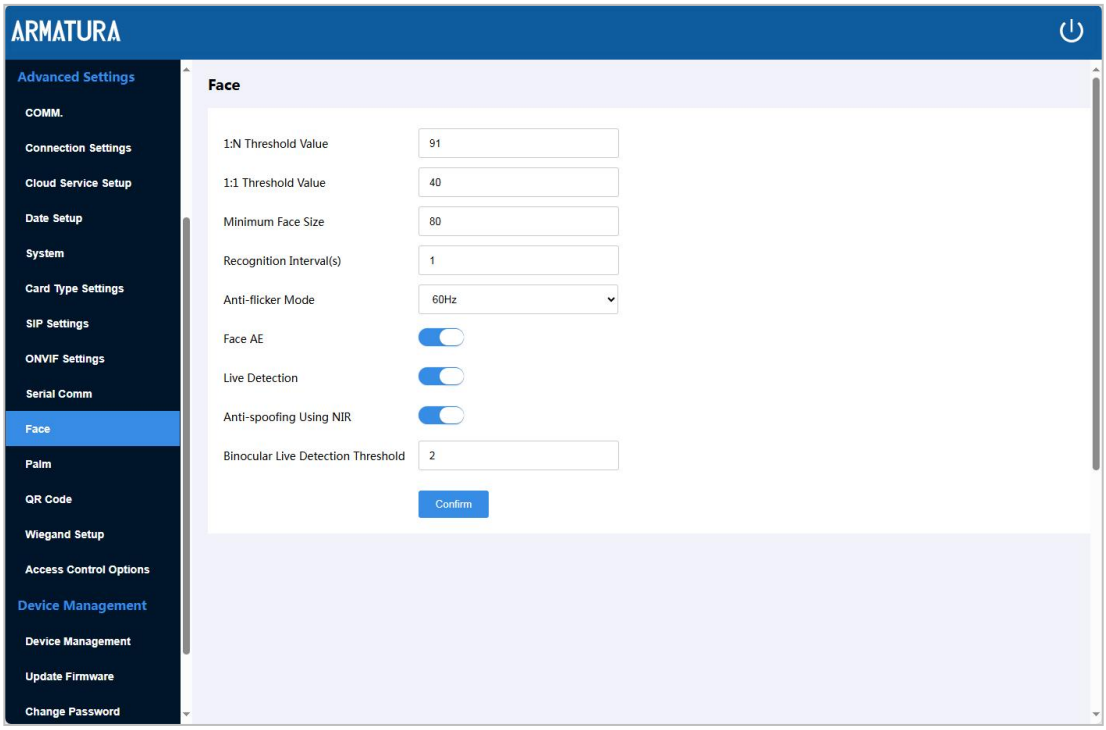
Baudrate:

The rate at which the data is communicated with PC, there are 5 options of baud rate: 115200 (default), 57600, 38400, 19200, and 9600. The higher is the baud rate, the faster is the communication speed, but also the less reliable.

Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.

8.4.10 Face Template Parameters

Click [**Advanced Settings**] > [**Face**] to go to the face template parameter settings.



The fields description is as follows:

1:N Threshold Value: Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value.

The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 88.

1:1 Threshold Value: Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value.

The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 88.

Minimum Face Size: It sets the minimum face size required for facial registration and comparison.

If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face.

This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.

Recognition Interval(s): After the interval identifying is clicked (selected), for example, if the recognition interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

Anti-flicker Mode: It is used when WDR is turned off. It helps to reduce flicker when the device's screen flashes at the same frequency as the light.

Face AE: When the face is in front of the camera in Face AE mode, the brightness of the face area increases, while other areas become darker.

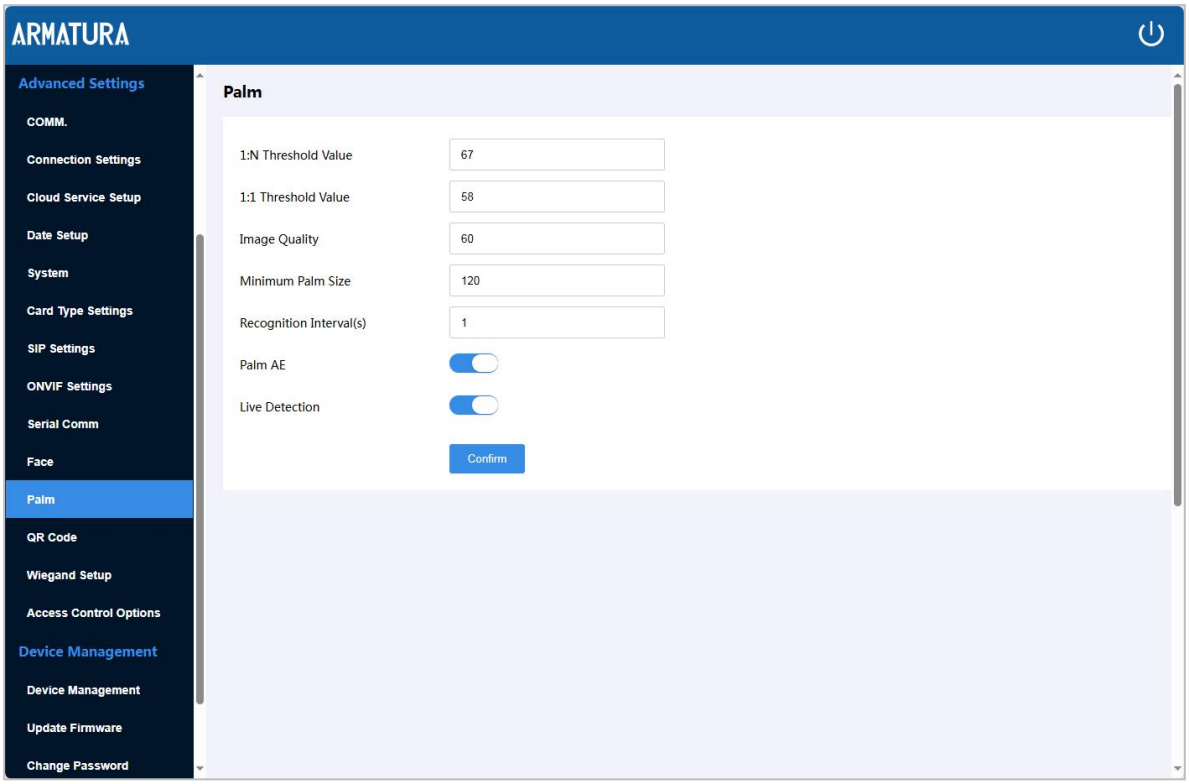
Live Detection: It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.

Anti-spoofing Using NIR: Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.

Binocular Live Detection Threshold: It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.

8.4.11 Palm Template Parameters

Click [**Advanced Settings**] > [**Palm**] to go to the palm template parameter settings.



The fields description is as follows:

1:N Threshold Value: In 1: N Verification Method, only when the similarity between the verifying palm and all the registered palm is greater than this value can the verification succeed.

1:1 Threshold Value: In 1:1 Verification Method, only when the similarity between the verifying palm and the user's registered palm is greater than this value can the verification succeed.

Image Quality: Image quality for palm registration and comparison. The higher the value, the clearer the image requires.

Minimum Palm Size: It sets the minimum palm size required for palm registration and comparison.

If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a palm.

This value can also be interpreted as the palm comparison distance. The farther the individual is, the smaller the palm, and the smaller number of pixels of the palm obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of palms. When the value is 0, the palm comparison distance is not limited.

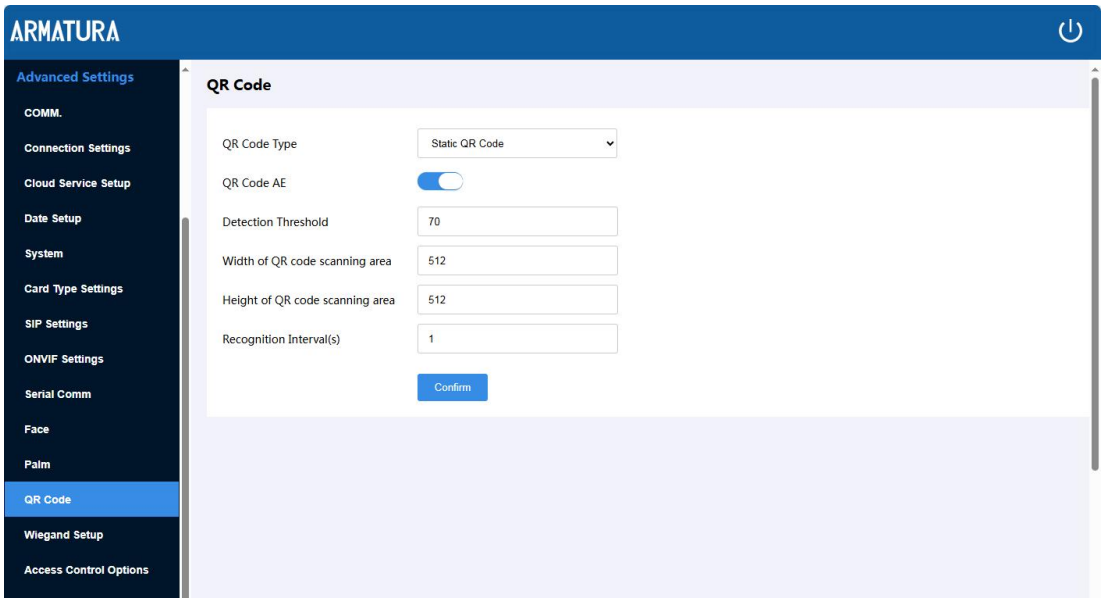
Recognition Interval(s): After the interval identifying is clicked (selected), for example, if the recognition interval is set to 5 seconds, then the palm recognition will verify the palm every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

Palm AE: When the palm is in front of the camera in Palm AE mode, the brightness of the palm area increases, while other areas become darker.

Live Detection: It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.

8.4.12 QR Code

Click [**Advanced Settings**] > [**QR Code**] to set the QR code parameters.



The fields description is as follows:

QR Code Type: To select the type of QR code, there are Static QR Code and Dynamic QR Code.

QR Code AE: When the QR code is in front of the camera in QR Code AE mode, the brightness of the QR code area increases, while other areas become darker.

Detection Threshold: This is the threshold value that determines whether an object is detected as a QR code or not. The lower the threshold value, the more likely to misjudge and detect

non-QR code objects as QR code; while the higher the threshold value, the more likely to miss the detection, which may result in the real QR code not being detected. A suitable detection threshold should be set. It is recommended to set the default value of 70. Range 0~100.

Width of QR code scanning area: The width of the scanned area of the QR code in the image. The range is 300 to the maximum width of the image. Subject to the image width of the specific device.

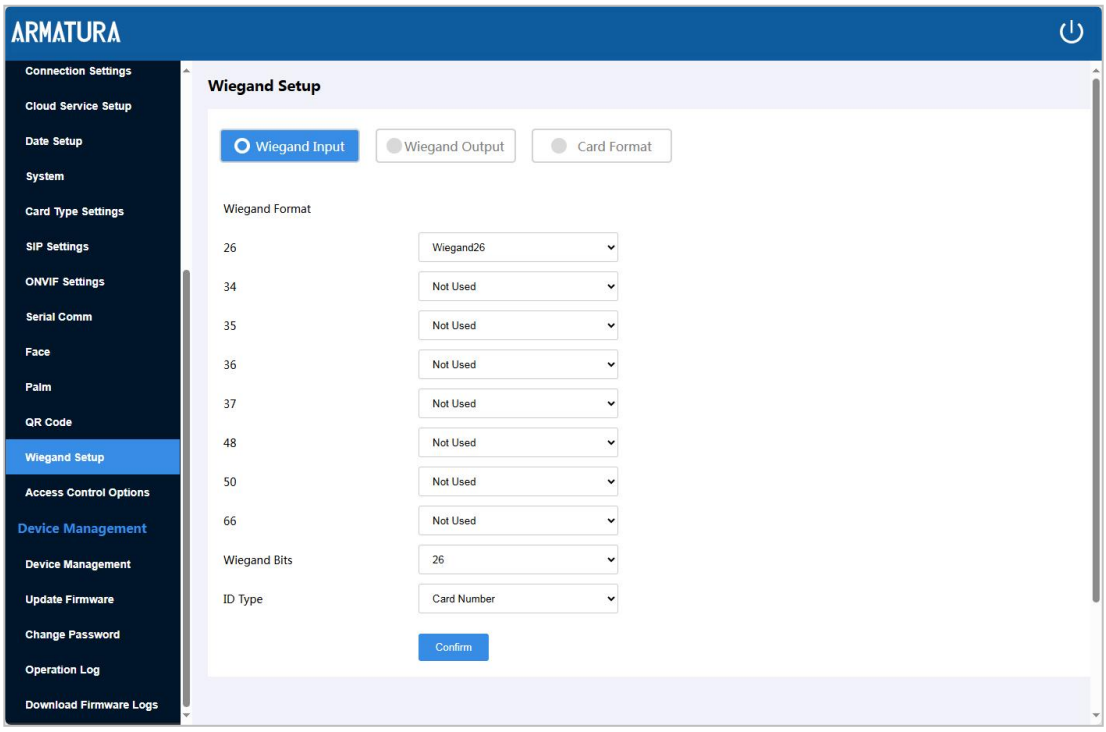
Height of QR code scanning area: The height of the scanned area of the QR code in the image. The range is 300 to the maximum width of the image. Subject to the image height of the specific device.

Recognition Interval(s): After the interval identifying is clicked (selected), for example, if the recognition interval is set to 5 seconds, then the QR code recognition will verify the QR code every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.

8.4.13 Wiegand Setup

To set the Wiegand input, Wiegand output and card format parameters.

Click [**Advanced Settings**] > [**Wiegand Setup**] to set the relevant parameters.



The fields description is as follows:

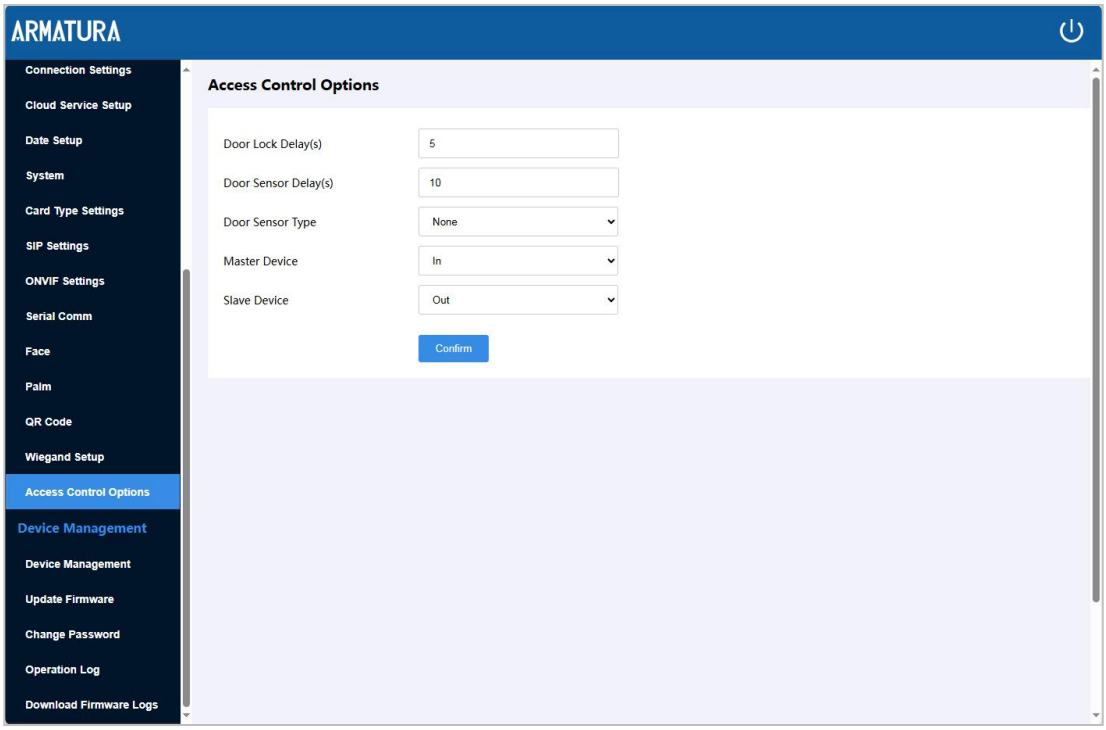
Wiegand Format: Values range from 26 Bits, 34 Bits, 35 Bits, 36 Bits, 37 Bits, 48 Bits, 50 Bits and 66Bits.

Wiegand Bits: Number of bits of Wiegand data.

ID Type: Select between User ID and card number.

8.4.14 Access Control Options

Click [**Advanced Settings**] > [**Access Control Options**] to set the parameters of the control lock of the terminal and related equipment.



The fields description is as follows:

Door Lock Delay (s): The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~99 seconds.

Door Sensor Delay (s): If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.

Door Sensor Type: There are three Sensor types: None, Normal Open, and Normal Close.

- ✧ **None:** It means the door sensor is not in use.
- ✧ **Normal Open(NO):** It means the door is always left open when electric power is on.
- ✧ **Normal Closed(NC):** It means the door is always left closed when electric power is on.

Master Device: While configuring the master and slave devices, you may set the state of the master as **Out** or **In**.

- ✧ **Out:** A record of verification on the master device is a check-out record.
- ✧ **In:** A record of verification on the master device is a check-in record.

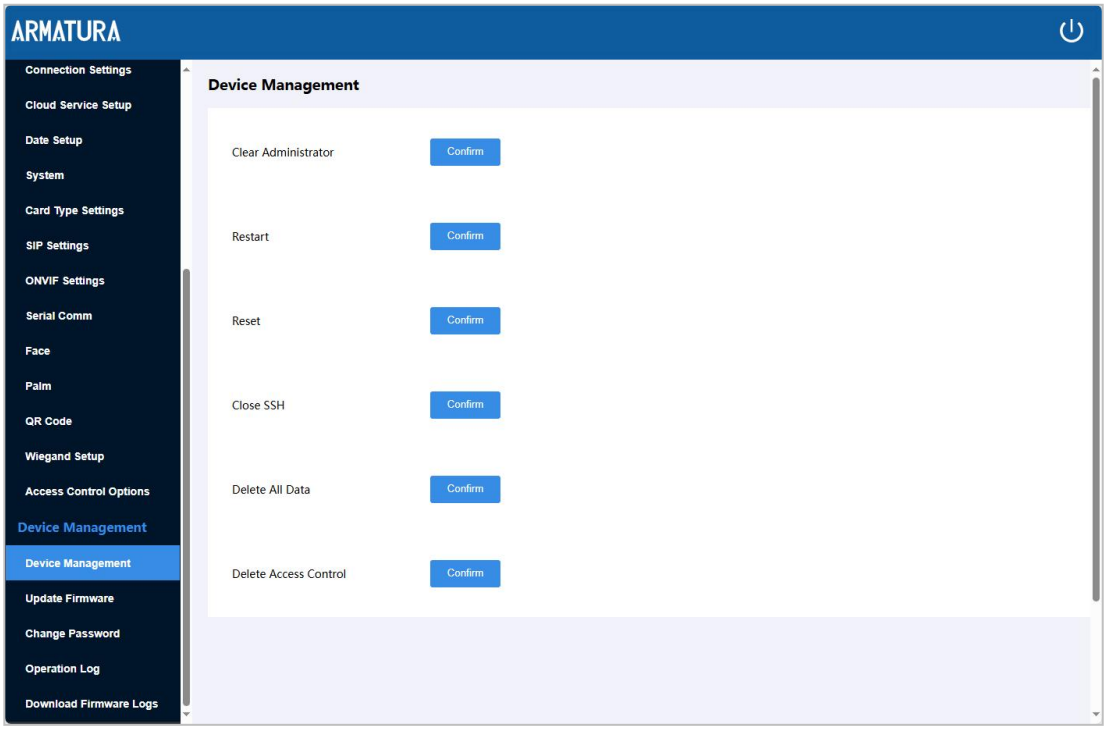
Slave Device: While configuring the master and slave devices, you may set the state of the slave as **Out** or **In**.

- ✧ **Out:** A record of verification on the slave device is a check-out record.
- ✧ **In:** A record of verification on the slave device is a check-in record.

8.5 Device Management

8.5.1 Device Management

Click [**Device Management**] > [**Device Management**] to set the parameters of the device.



The fields description is as follows:

Clear Administrator: To clear all the administrator.

Restart: To reboot the device.

Reset: To restore the factory settings. The function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

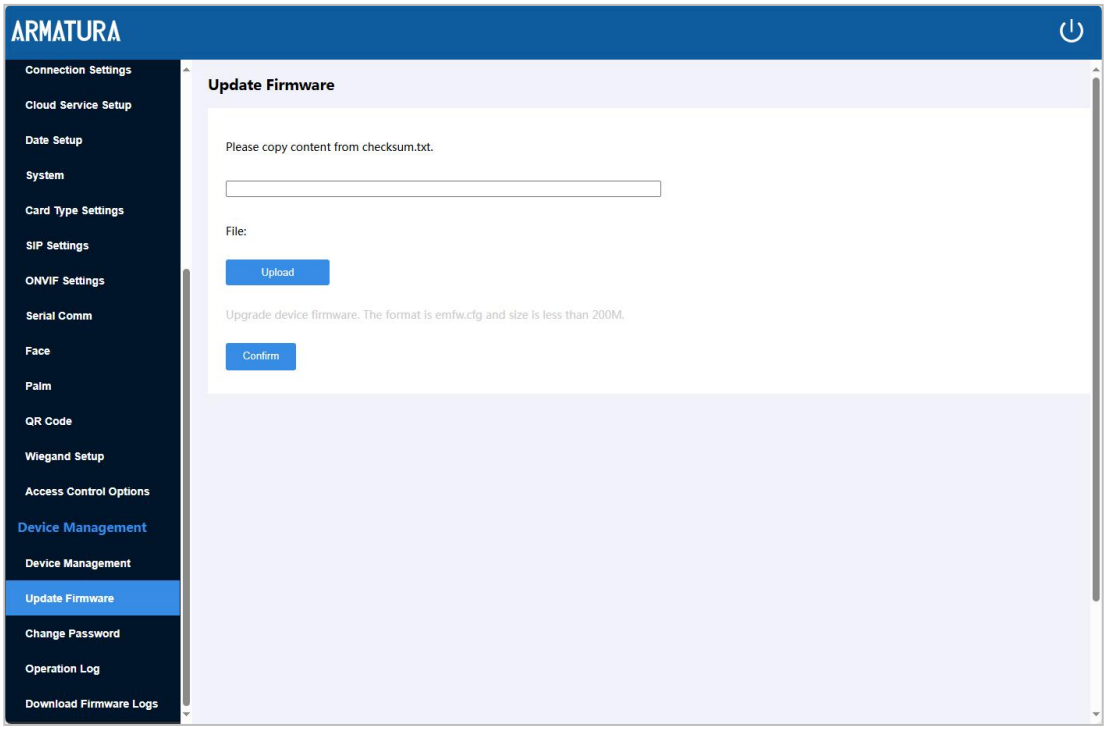
Close SSH: To close the SSH.

Delete All Data: To delete information and attendance logs/access records of all registered users.

Delete Access Control: To delete all access data.

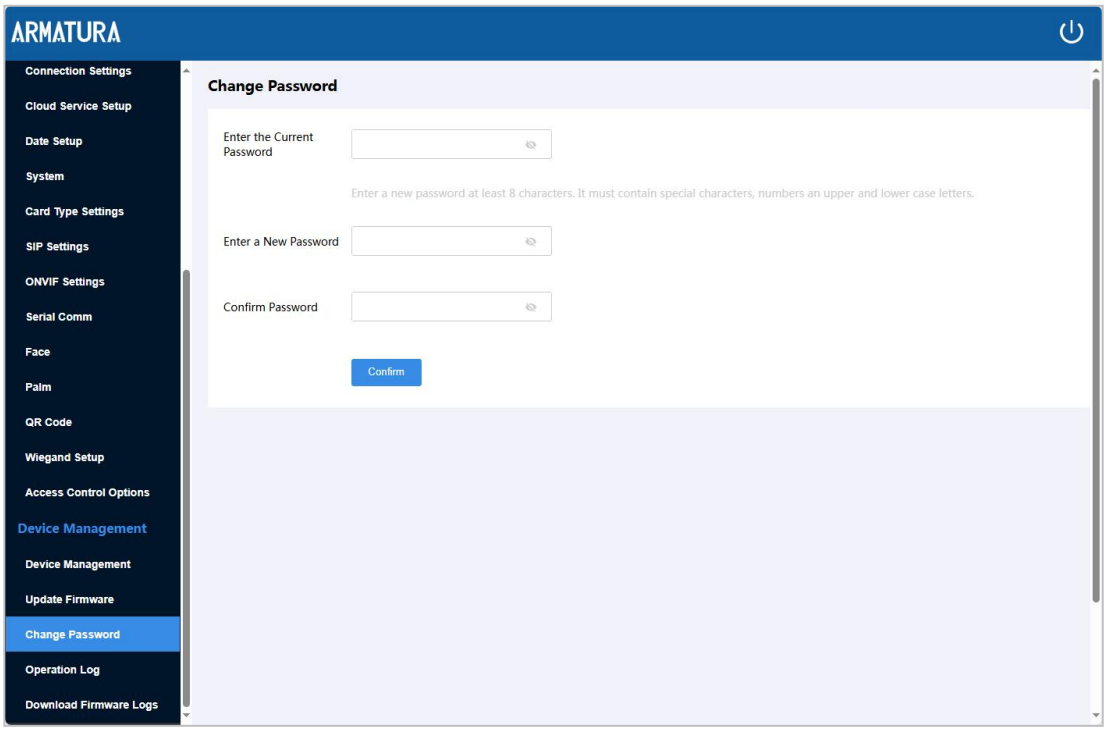
8.5.2 Update Firmware

Click [**Device Management**] > [**Update Firmware**] to update the firmware online.



8.5.3 Change Password

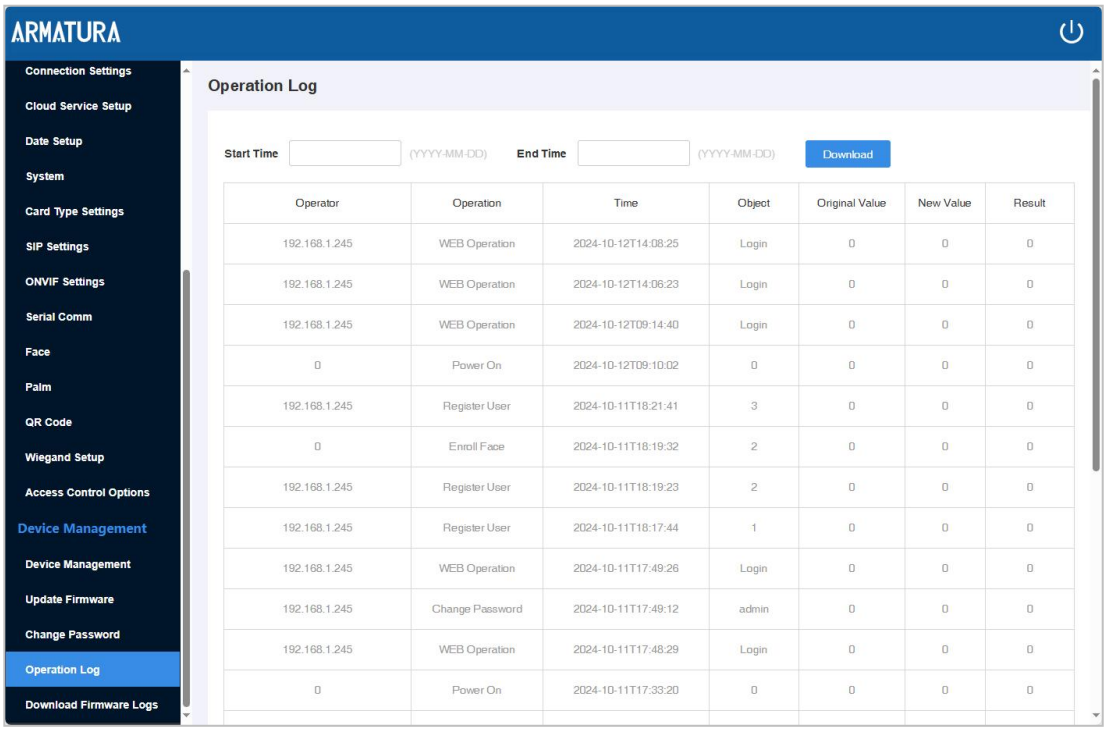
Click [**Device Management**] > [**Change Password**] to modify the user password.



Enter your **Previous password**, **New password** and **Confirm the password**, then click [**Confirm**].

8.5.4 Operation Log

Click [**Device Management**] > [**Operation Log**] to view all the device operation logs.

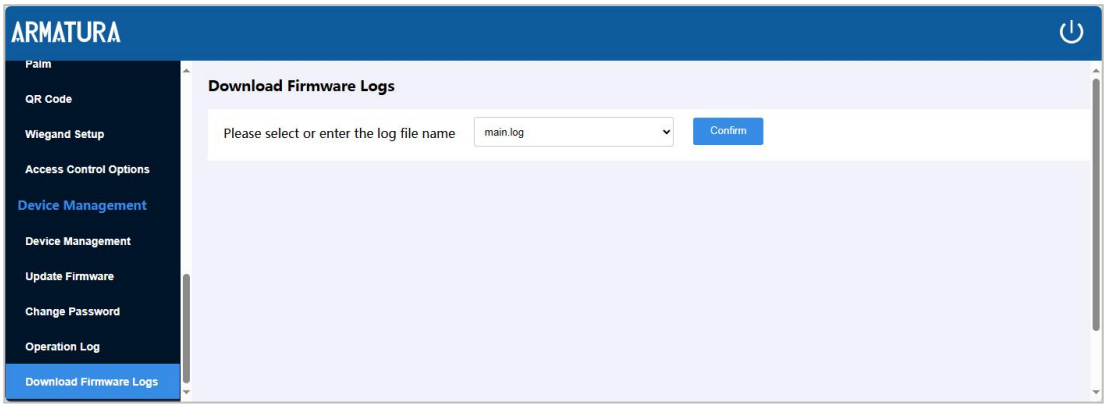


The fields description is as follows:

Download: Select the starting and ending time, and then click download, the operation log of the selected time will be automatically downloaded.

8.5.5 Download Firmware Logs

Click [**Device Management**] > [**Download Firmware Logs**] to download firmware logs.



Please select or enter the log file name, such as main.log, biometric.log or dev.log, and click [**Confirm**] to download firmware logs.

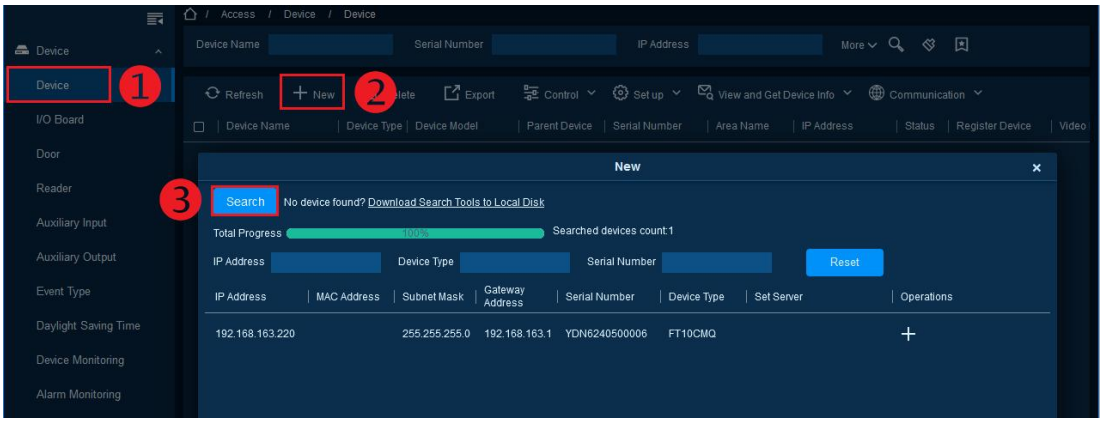
9. Connect to the ARMATURA One Software

Log in to the ARMATURA One software and perform the following steps.

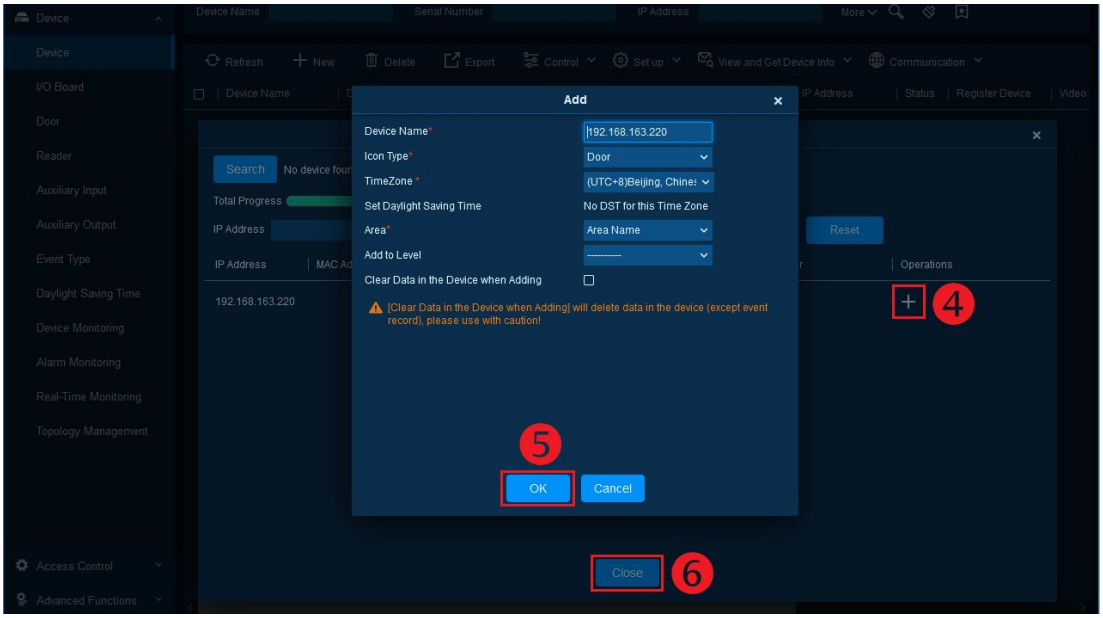
9.1 Add Device to the Software

The default IP address of the device is **192.168.1.201**. When connecting to the software, make sure that the IP addresses of the server (PC) and the device are in the same network segment. The IP address can be changed on the Webserver, see 8.4.1Comm. Settings for details.

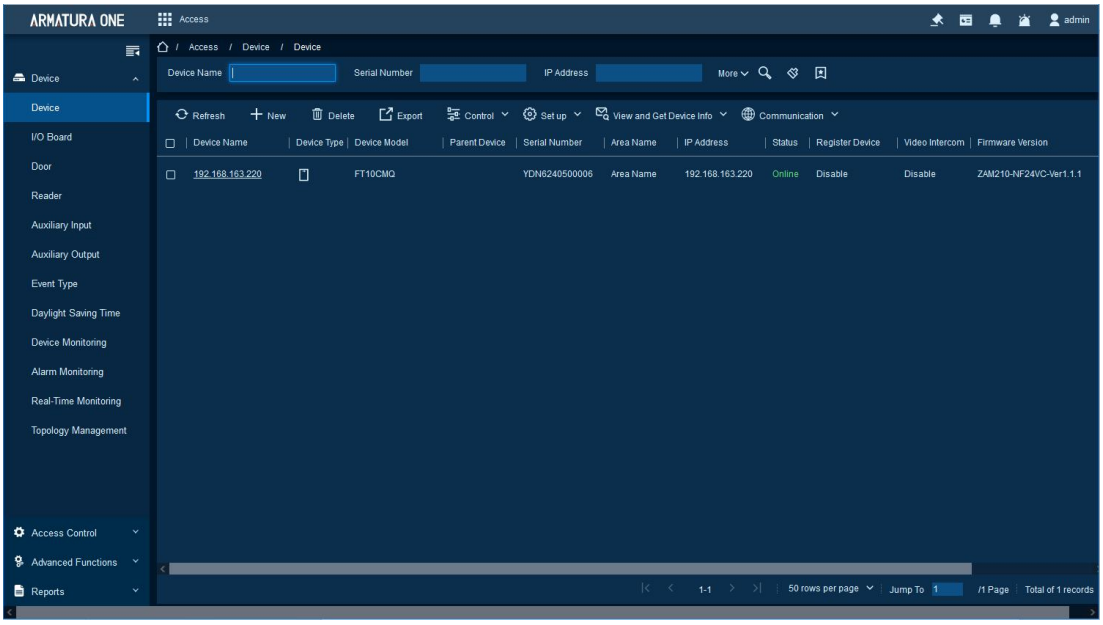
1. Log into the Armatura One software.
2. Click [**Access**] > [**Device**] > [**Device**] > [**New**] > [**Search**] to search the device on the software. When an appropriate server address and port is set on the device, the searched devices are displayed automatically.



3. Click [**+**] in operation column, the Add window will pop-up. Select Icon type, Area, and Add to Level from each dropdowns and click [**OK**] to add the device.

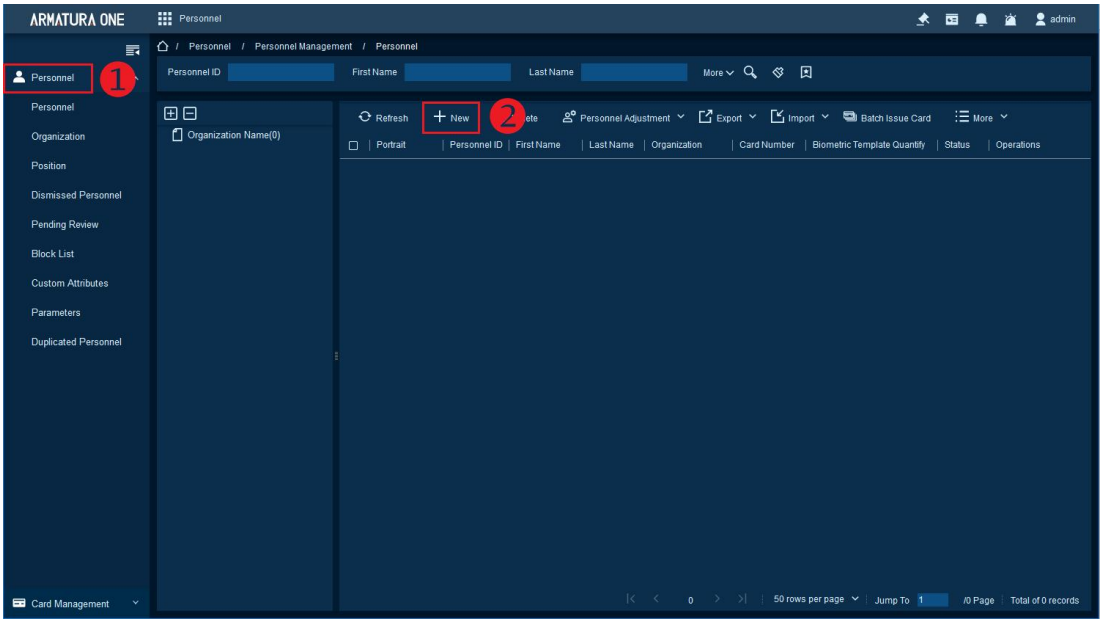


4. Once added, the device is displayed in the device list.

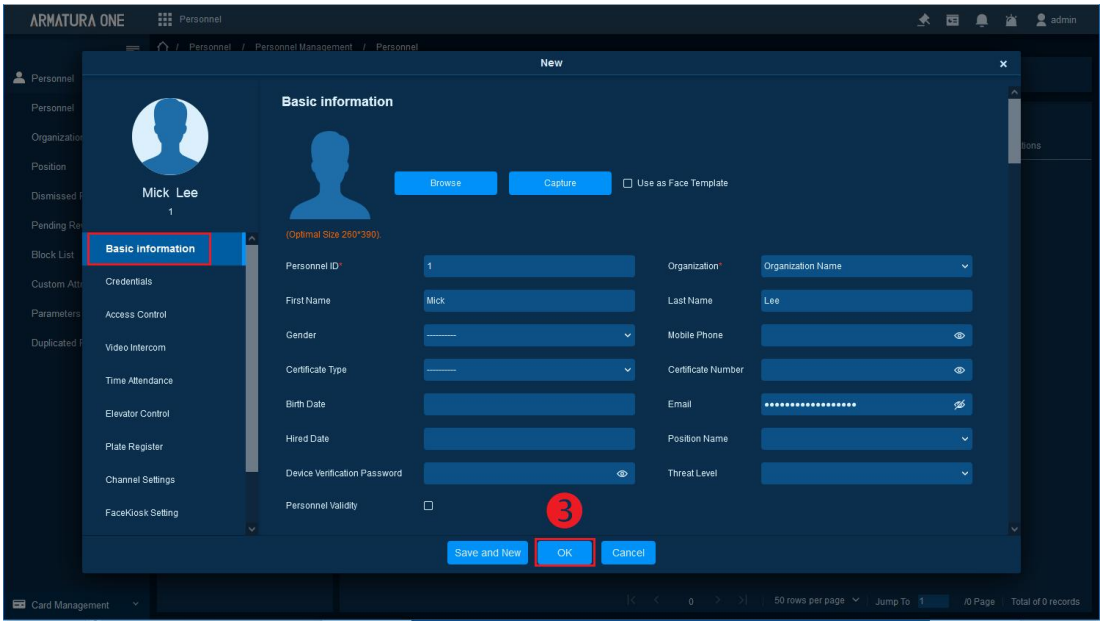


9.2 Add Personnel on the Software

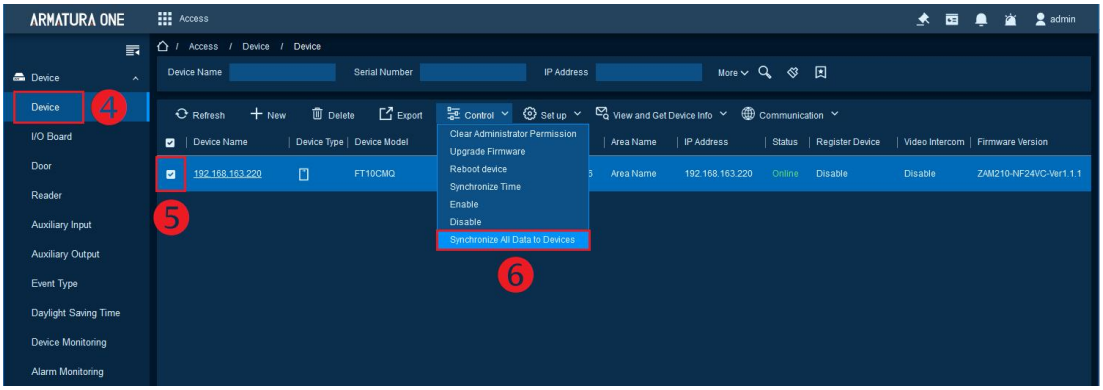
1. Click [**Personnel**] > [**Personnel**] > [**New**] to add a new personnel.

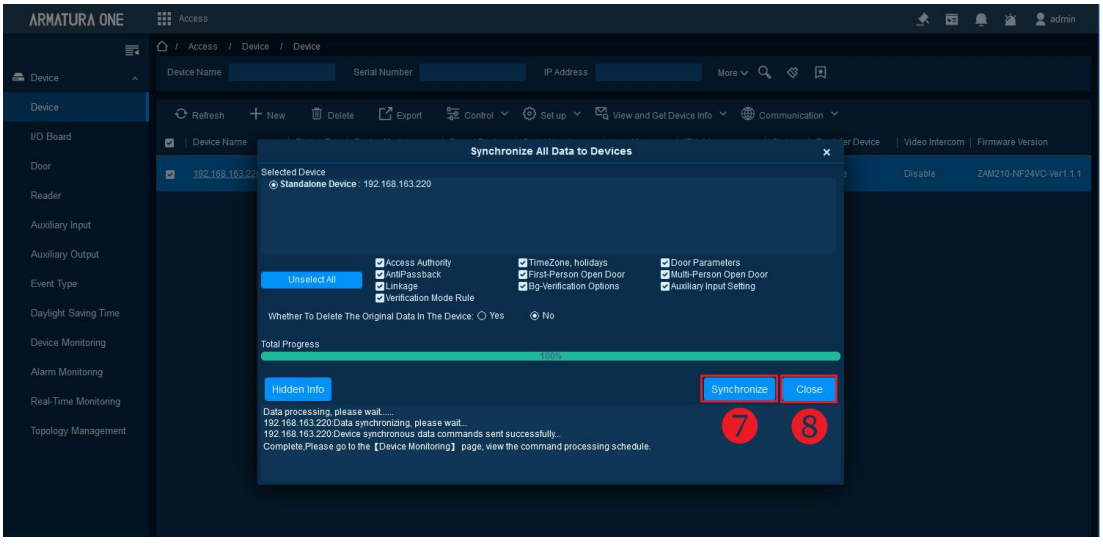


2. Fill in all the required fields and click [**OK**] to register a new user.



3. Click [**Access**] > [**Device**] > [**Control**] > [**Synchronize All Data to Devices**] to synchronize all the data to the device including the new users.



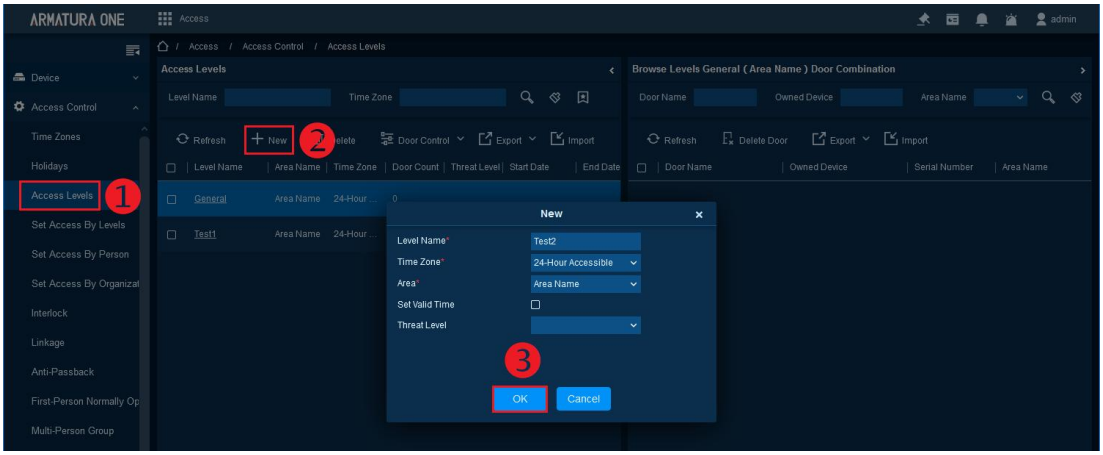


Note: *For other specific operations, please refer to the relevant software user manual.*

9.3 Set Access Levels

9.3.1 Add Access Levels Group

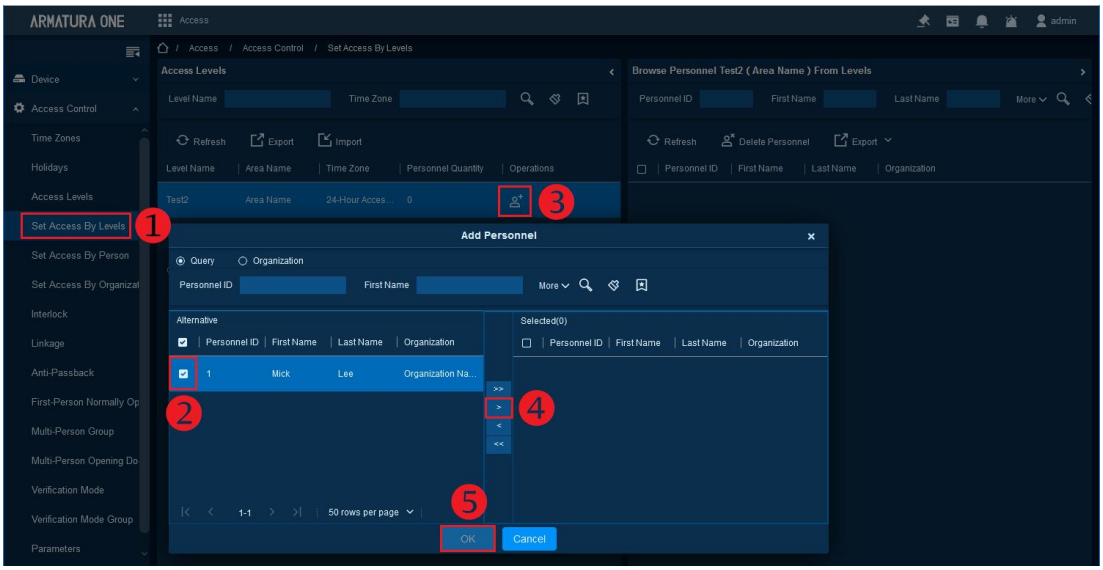
1. Click [**Access**] > [**Access Control**] > [**Access Levels**] to enter the setting interface.
2. Click [**New**] to add a new access control level group.
3. Enter the level name, time zones and setting area, then click [**OK**] to confirm and exit.



9.3.2 Set Access by Levels

Add personnel to the access control level group.

1. Click [**Access**] > [**Access Control**] > [**Set Access By Levels**] to enter the setting interface.
2. Check the levels group and click the [**Add Personnel**] icon in its bar to open the settings window.
3. Select the person and then click > to move it to the selected column on the right.
4. Click [**OK**] to confirm and exit.



10. Using Mobile Credential

Open the Armartura ID App. You can use mobile credentials in both Remote Mode and Card Mode.

10.1 Using Remote Mode

1. After enabling the **Remote Mode**, click ☰ icon > [**Credentials**] to enter the Credentials.
2. Directly click the  icon to swipe the card remotely within the valid range.
3. When the device beeps, the LED lights up red, and the interface prompts "Verication successful", it means that the card is swiped successfully.

10.2 Using Card Mode

1. After enabling the **Card Mode**, click ☰ icon > [**Credentials**] to enter the Credentials.
2. Click  icon to open Mobile Credentials.
3. Hold your mobile phone close to the reader until you hear a "beep" and the LED lights up red, indicating that the card is swiped successfully.

11. Appendix

11.1 Privacy Policy

Notice:

To help you better use the products and services of Armatura LLC, hereinafter referred to as "we", "our", or "us", the smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric

information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit www.armatura.us to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

11.2 Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

11.3 Attachment

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-- Consult the dealer or an experienced radio/TV technician for help.

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Supplier's Declaration of Conformity

Unique Identifier

Trade Name: ARMATURA

Model No.: AHSC-1000, AHDU-1160, AHDU-1260, AHDU-1460, AHDU-1860, AHDU-11660; AHEB-0808, AHEB-1602,AHEB-1616; EP10C, EP20, EP30CF, VG10, FT10CMQ.EP20/VG10 may be followed by C/CK/CQ/CKQ. All the readers may be followed by [LF]/[HF]/[LHF]/[NI]/[NP]/[NO]/[DF]/[SFMH]/[IDL]/[ICH]/[RNI]/[RNP]/[RNPL] /[NIH] /[NISH] /[NPL] /[NPSL] /[MNO]/[MNP] /[MNPSL], etc.

Responsible Party – U.S. Contact Information

US Company Name: Armatura LLC.

Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005 USA

Telephone number or internet contact information: 678-831-3345

"Hereby, Armatura LLC declares that this Product is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address: www.Armatura.us

The functions of Wireless Access Systems including Radio Local Area Networks(WAS/RLANs) within the band 5150-5350 MHz for this device are restricted to indoor use only within all European Union countries (BE/BG/CZ/DK/DE/EE/IE/EL/ES/FR/HR/ IT/CY/LV/LT/LU/HU/MT/NL/AT/PL/PT/RO/SI/SK/FI/SE/TR/N O/CH/IS/LI/UK(NI)

Customer: ZKTECO EUROPE SL

Customer Address: Crta.de Fuencarral 44. Edificio 1. Planta 2.28108, Alcobendas.

Madrid.SPAIN

ARMATURA

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