ARMATURA

User Manual

OmniAC30

Date: January 2025

Version: 2.3

English

Copyright © 2025 ARMATURA LLC. All rights reserved.

Without the prior written consent of ARMATURA, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ARMATURA and its subsidiaries (hereinafter the "Company" or "ARMATURA").

Trademark

ARMATURA is a registered trademark of ARMATURA. 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 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 have 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 https://armatura.us/

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

ARMATURA Headquarters

Address 190 Bluegrass Valley Parkway Alpharetta, GA 30005

Phone +1-650-4556863

Email: sales@armatura.us

Website: www.armatura.us

About the Manual

This manual introduces the operation of user interfaces and menu functions of **OmniAC30**.

The pictures in this manual may not be exactly consistent with those of your product; the actual product's display shall prevail.

Not all the devices have the function with ★, which the real product prevails.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Table of Contents

Copyright © 2025 ARMATURA LLC. All rights reserved.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Copyright © 2025 ARMATURA LLC. All rights reserved.

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.

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.

Copyright © 2025 ARMATURA LLC. All rights reserved.

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.

Electrical Safety

- Before connecting an external cable to the device, complete grounding properly, and set up surge protection; otherwise, static electricity will damage the mainboard.
- Make sure that the power has been disconnected before you wire, install, or dismantle the device.
- Ensure that the signal connected to the device is a weak-current (switch) signal; otherwise, components of the device will get damaged.
- 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.
- In the case of power supply damage, return the device to the professional technical personnel or your dealer for handling.
- 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.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Operation Safety

- 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.
- Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.
- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.
- 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.
- 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.
- 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.

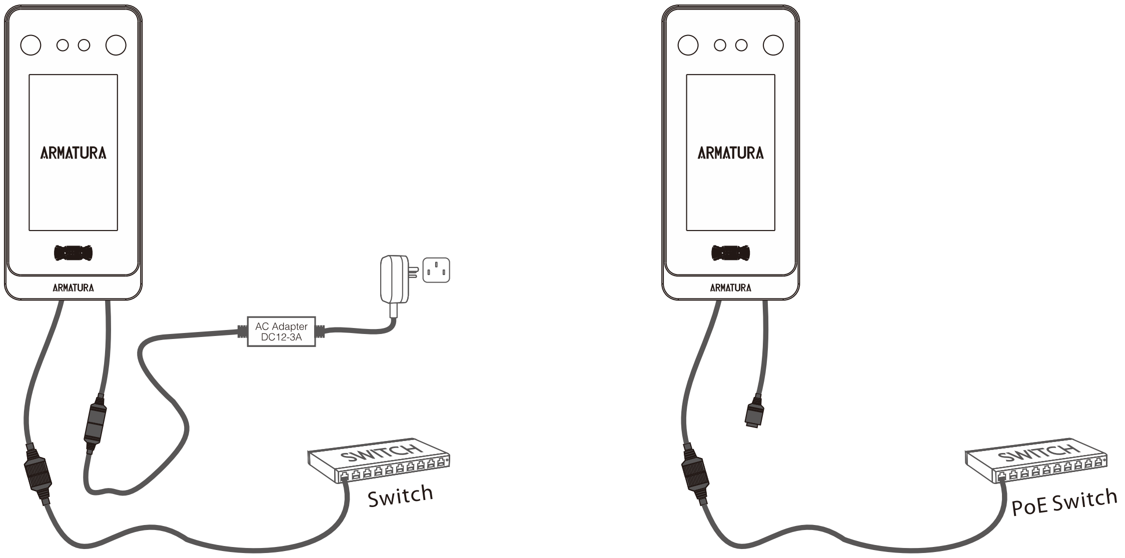
Copyright © 2025 ARMATURA LLC. All rights reserved.

1 Instruction for Use

To satisfy RF exposure requirements，a separation distance of 7.87inch (20cm) or more should be maintained between this device and persons during device operation.

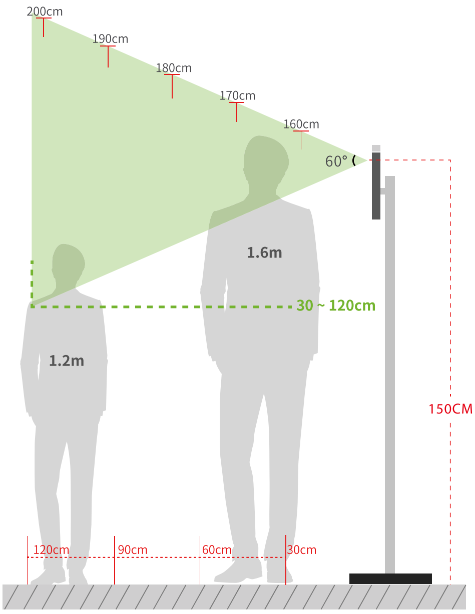
1.1 PoE Ready

Supports IEEEPower over Ethernet (PoE) 802.3at from power sourcing requirement (PSE).



1.2 Standing Position, Facial Expression and Standing Posture

Recommended Distance



The distance between the device and a user whose height is within 59.06 to 72.83inch (150 to 185cm) is recommended to be 11.81 to 78.74inch (30 to 200cm). Users may slightly move forwards and backwards to improve the quality of facial images captured.

Copyright © 2025 ARMATURA LLC. All rights reserved.

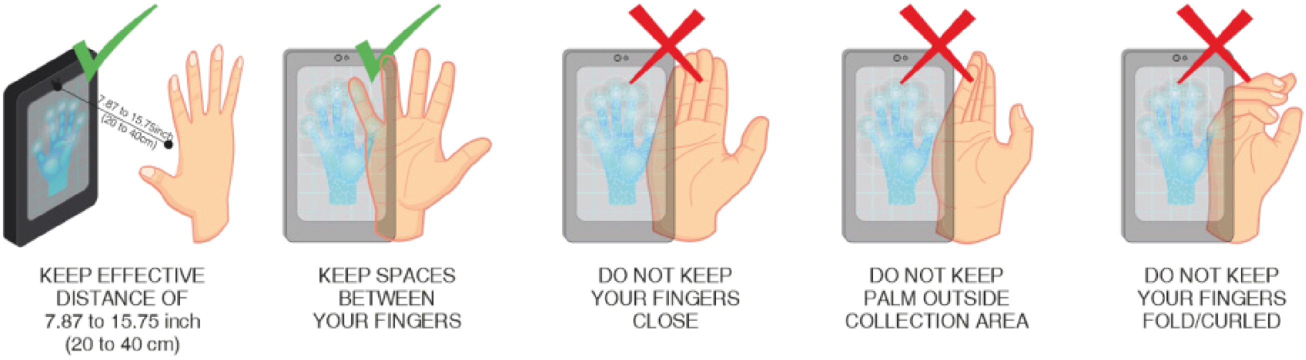
Facial Expression and Standing Posture

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

1.3 Palm Registration

Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device.

Make sure to keep space between your fingers.


7.87 to 15.75inch (20 to 40cm)
KEEP EFFECTIVE DISTANCE OF 7.87 to 15.75 inch (20 to 40 cm)
KEEP SPACES BETWEEN YOUR FINGERS
DO NOT KEEP YOUR FINGERS CLOSE
DO NOT KEEP PALM OUTSIDE COLLECTION AREA
DO NOT KEEP YOUR FINGERS FOLD/CURLED

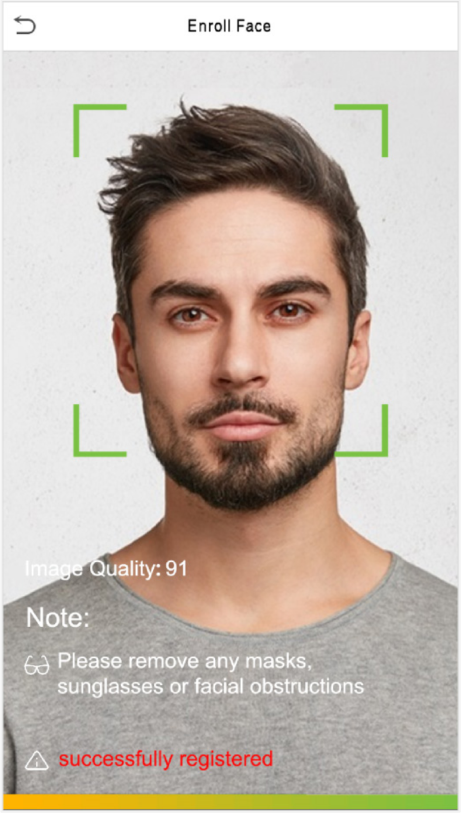
Note:

1. Place your palm within 7.87 to 15.75 inch (20 to 40 cm) of the device.
2. Place your palm in the palm collection area, such that the palm is placed parallel to the device.
3. Make sure to keep space between your fingers.
4. Please avoid direct sunlight when using the palm function outdoors. According to laboratory test, the palm recognition effect is best when the light intensity is not more than 10,000 lux.

Copyright © 2025 ARMATURA LLC. All rights reserved.

1.4 Face Registration

Try to keep the face in the center of the screen during registration. Please face the camera and stay still during face registration. The page looks like shown below:



Enroll Face

Image Quality: 91

Note:

Please remove any masks, sunglasses or facial obstructions

successfully registered

Face registration and authentication methods

<u>Instructions to Register a Face</u>

- When registering a face, maintain a distance of 15.75 to 31.5inch (40 to 80cm) between the device and the face.
- Be careful not to change the facial expression. (smiling, drawn, wink, etc.)
- If you do not follow the instructions on the screen, the face registration may take a longer time or may fail.
- Be careful to not cover the eyes or eyebrows.
- Do not wear hats, masks, sunglasses, or eyeglasses.
- Be careful to not display two faces on the screen. Register only one person at a time.
- It is recommended for a user wearing glasses to register both faces with and without glasses.

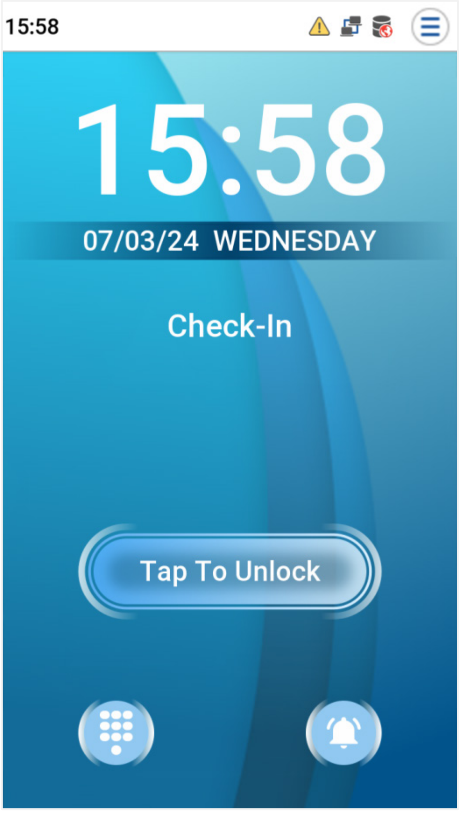
Copyright © 2025 ARMATURA LLC. All rights reserved.

Instructions to Authenticate a Face

- Ensure that the face appears inside the detection area displayed on the device screen.
- If eyeglasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses. If only the face with glasses has been registered, authenticate the face with the previously worn glasses again.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

1.5 Standby Interface

After connecting the power supply, the interface appears as shown below:



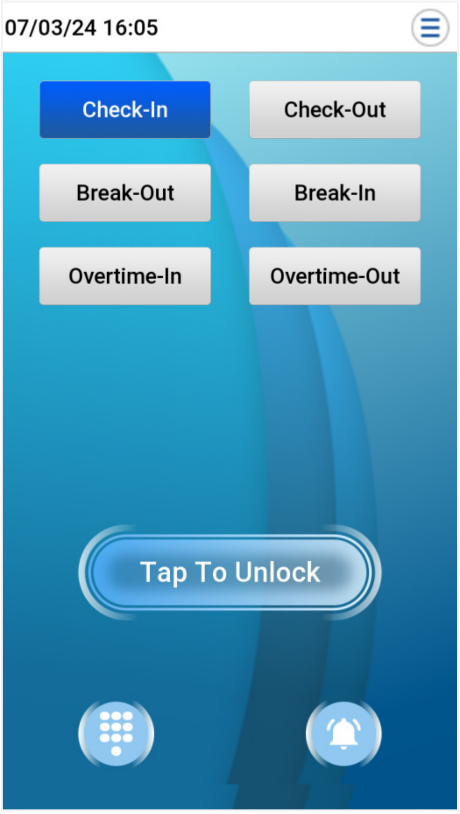
Note:

1. Tap ⠿ to open the interface to enter the User ID.
2. Tap Tap To Unlock to wake up the camera for auto-identification.
3. Visitors tap 🔔 to make a call and the phone will ring.

Copyright © 2025 ARMATURA LLC. All rights reserved.

4. When there is no super administrator registered in the device, tap ☰ to enter the menu. After setting the super administrator, it requires the super administrator's verification before entering the menu operation. For the security of the device, it is recommended to register a super administrator the first time you use the device.

5. The punch state options can also be displayed and used directly on the standby interface. Tap anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:

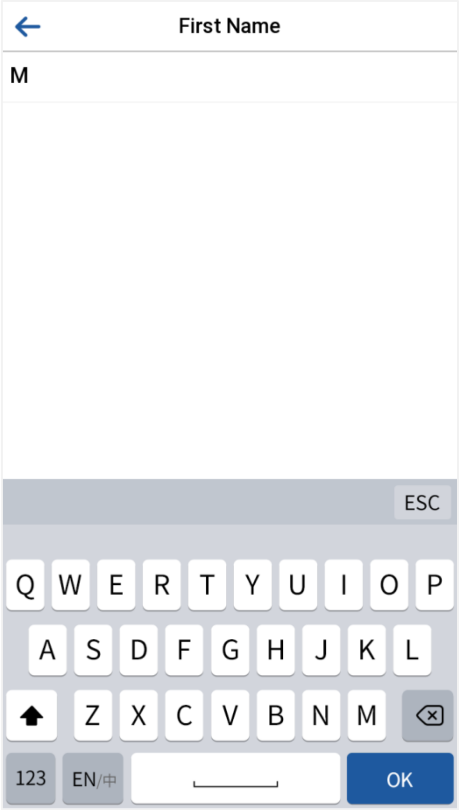


6. Press the corresponding punch state key to select your current punch state, which is displayed in blue. Please refer to "Shortcut Key Mappings" for the specific operation method.

   Note: The device type needs to be set as T&A PUSH, and the punch state options are off by default and need to select other mode options in the "Punch States Options" to get the punch state options on the standby screen.

Copyright © 2025 ARMATURA LLC. All rights reserved.

1.6 Virtual Keyboard



Note: The device supports the input of English characters, numbers and symbols. Tap [**123**] to switch to the numeric and special character keyboard, and tap [**ABC**] to return to the alphabetic keyboard. Tap the input box, and the virtual keyboard appears. Tap [**ESC**] to exit the keyboard screen.

1.7 Verification Mode

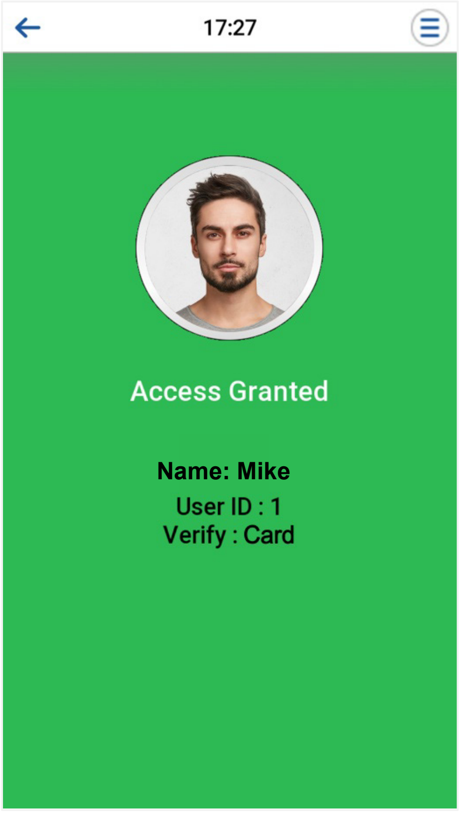
1.7.1 QR Code Verification

Static QR Code: In this verification mode, the device compares the QR code image collected by the QR code collector with all the QR code data available in the device.

Dynamic QR Code: Tap [**Credentials**] on the ARMATURA ID App, and the QR code will appear, which includes employee ID and card number information. The QR code can replace a physical card on a specific device to achieve contactless authentication. Please refer to the 14.2.3 Use of the Mobile Credentials.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Credentials
Personnel Code
1170562
ARMATURA ID
13:45
12/23/24 MONDAY
Tap To Unlock
ARMATURA



Access Granted

Name: Mike
User ID : 1
Verify : Card

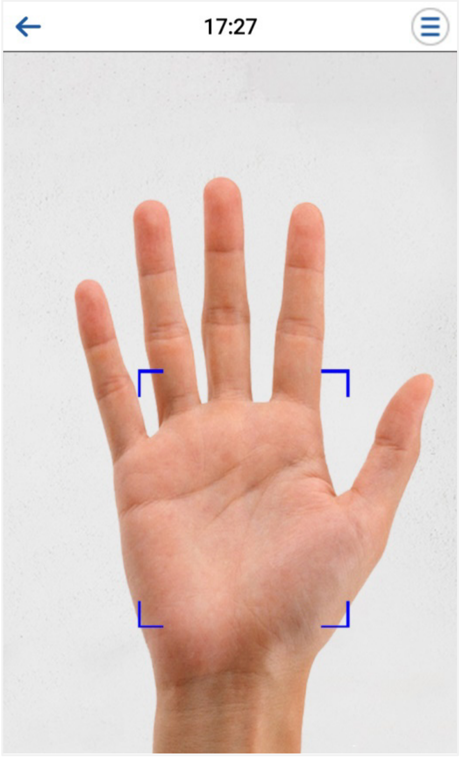
1.7.2 Palm Verification

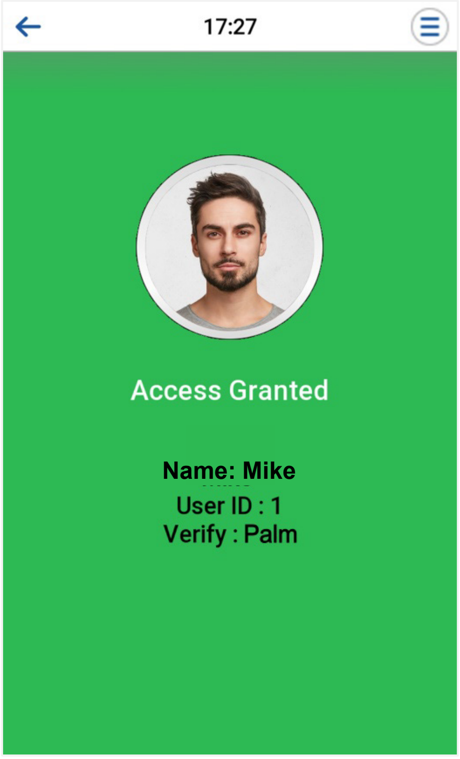
1:N Palm Verification Mode

This verification mode compares the palm image collected by the palm module with all the palm data template in the device.

The device will automatically distinguish between the palm and face verification mode. Place the palm in the area that can be collected by the palm module, so that the device will automatically switch to palm verification mode.

Copyright © 2025 ARMATURA LLC. All rights reserved.





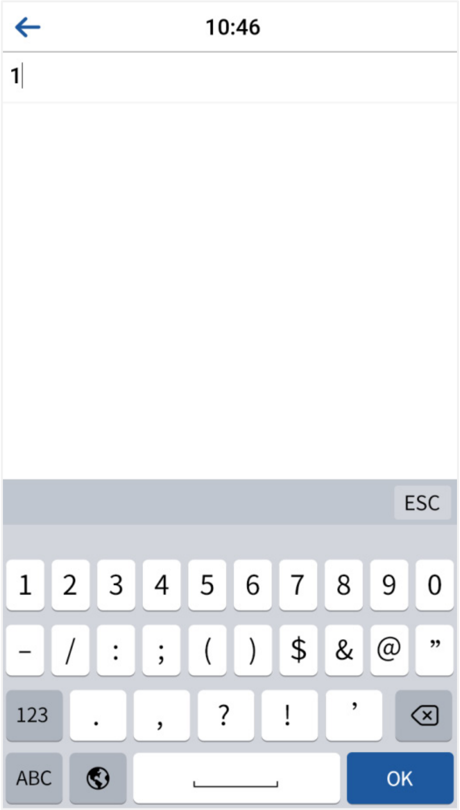
Access Granted

Name: Mike
User ID : 1
Verify : Palm

1:1 Palm Verification Mode

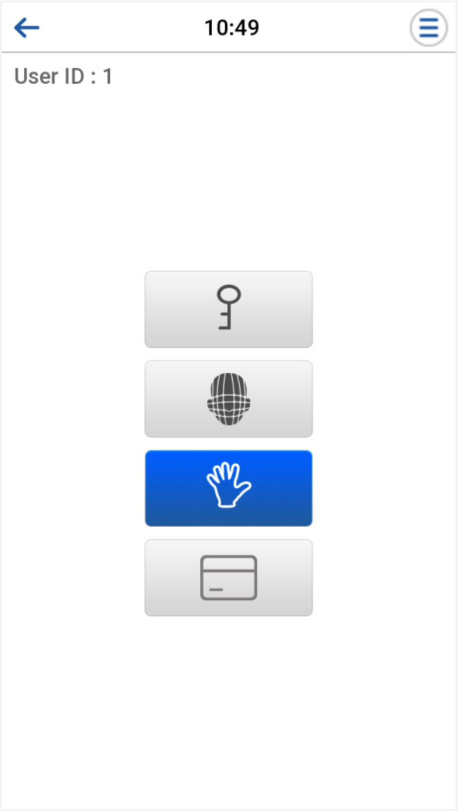
Tap the ▦ button on the main screen to open the 1:1 palm verification mode.

1. Input the user ID and tap **OK**.



Copyright © 2025 ARMATURA LLC. All rights reserved.

If the user has registered the card, face and password in addition to palm, and the verification method is set to Password/Card/Face/Palm, the following screen will appear. Select the palm icon ✋ to enter palm verification mode.



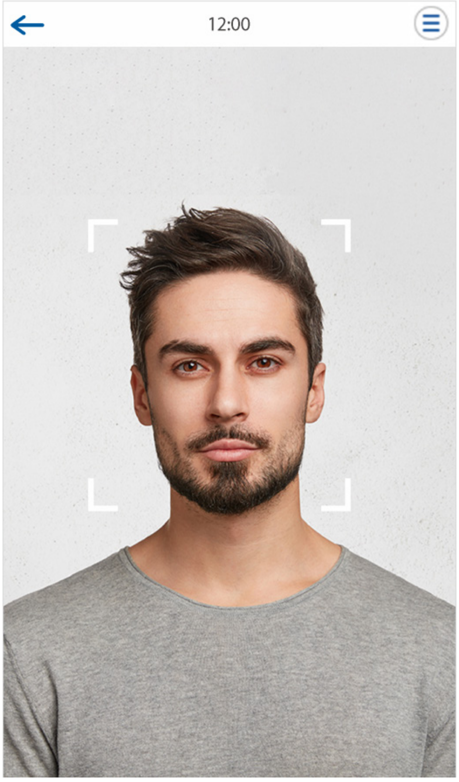
1.7.3 Facial Verification

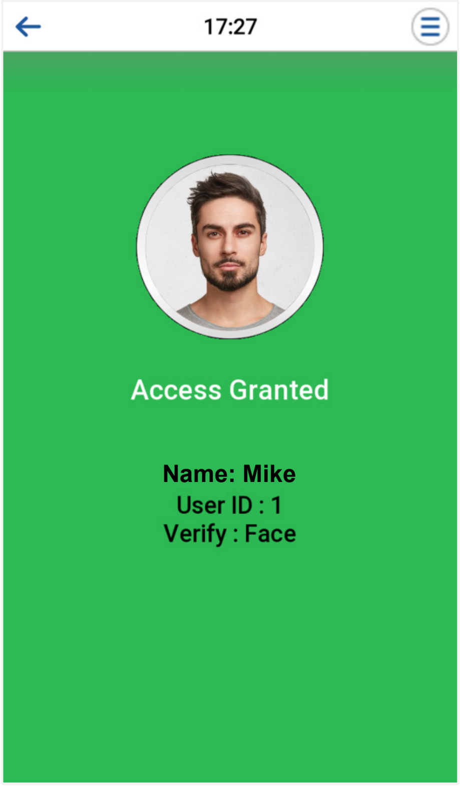
1:N Facial Verification

1. **Conventional Verification**

In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.

Copyright © 2025 ARMATURA LLC. All rights reserved.



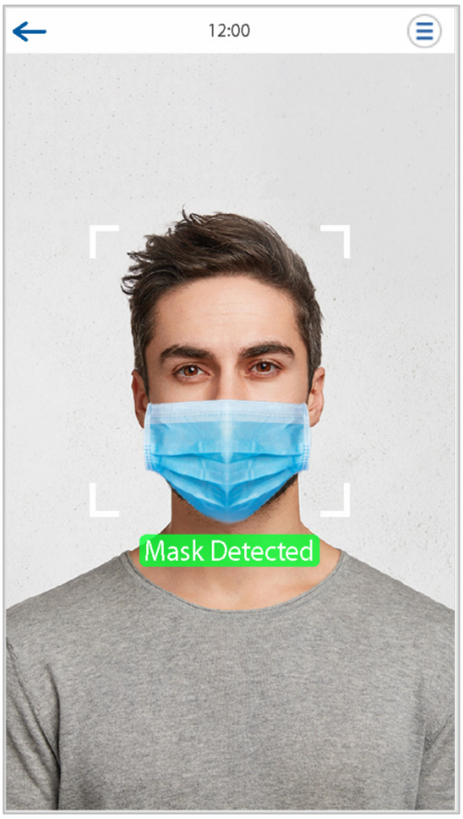


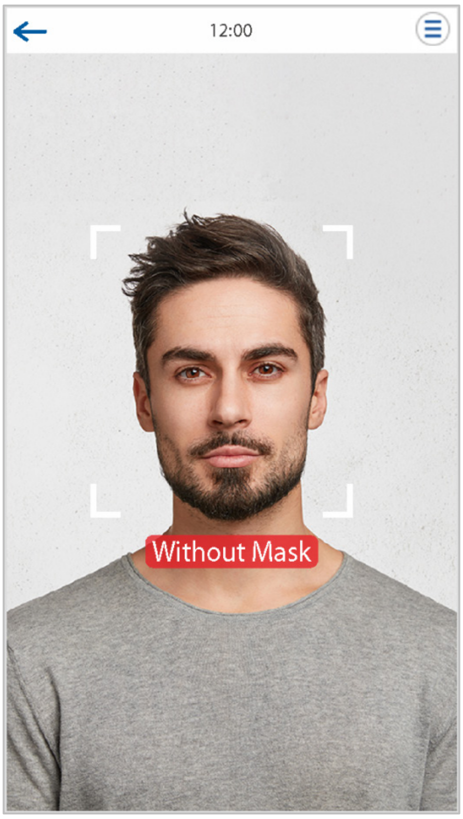
Access Granted

Name: Mike
User ID : 1
Verify : Face

2. Enable Mask Detection

When the user enables the **Mask Detection** function, the device identifies whether the user is wearing a mask while verification or not. The following are the popups of the comparison result prompt interface.

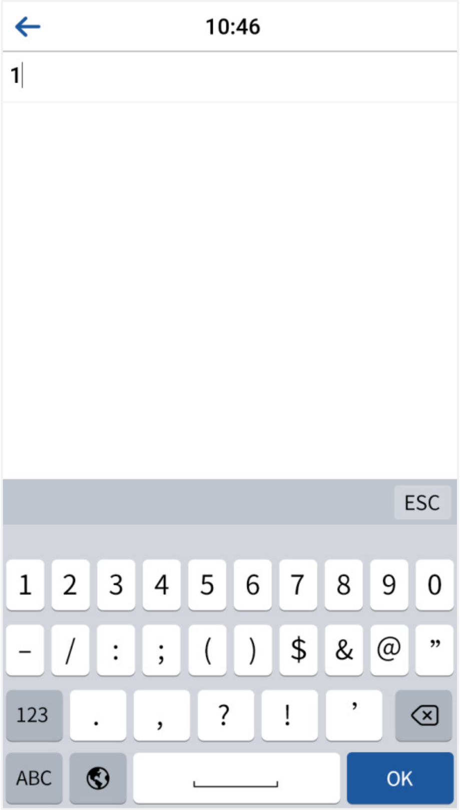




Copyright © 2025 ARMATURA LLC. All rights reserved.

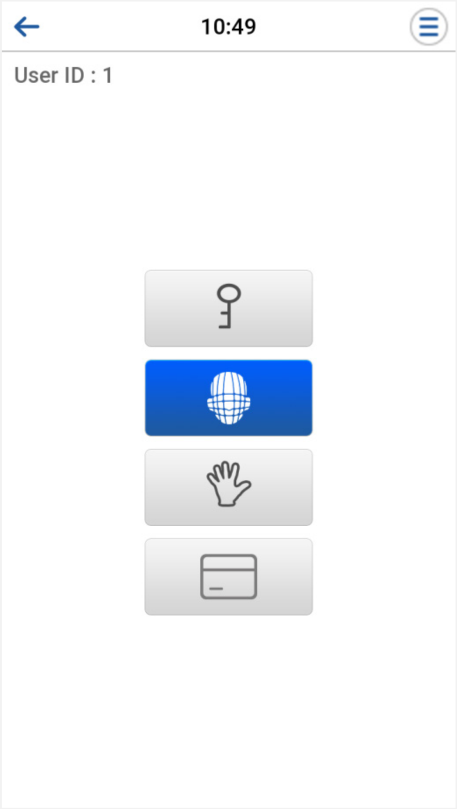
1:1 Facial Verification

In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Tap on the main interface and enter the 1:1 facial verification mode and enter the user ID and tap OK.

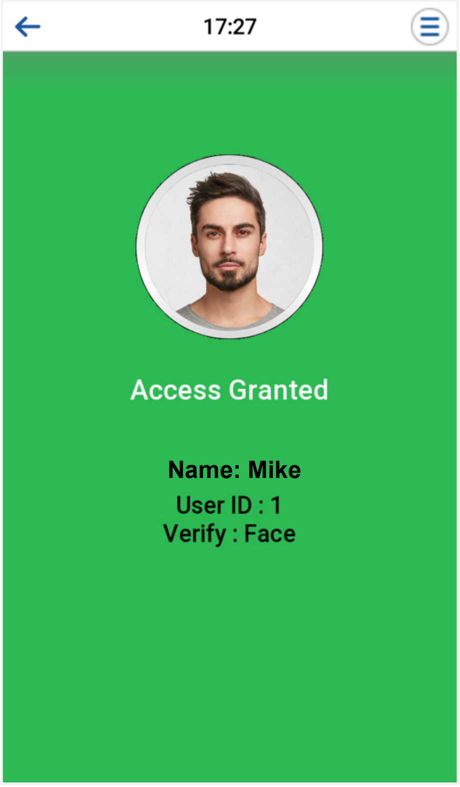


If the user has registered password, card and palm in addition to the face, and the verification method is set to Password/Card/Face/Palm verification, the following screen will appear. Select the icon to enter the face verification mode.

Copyright © 2025 ARMATURA LLC. All rights reserved.



After successful verification, the prompt box displays "**Access Granted**", as shown below:



Access Granted

Name: Mike

User ID : 1

Verify : Face

If the verification is failed, it prompts "**Unregistered person** ".

Copyright © 2025 ARMATURA LLC. All rights reserved.

1.7.4 Multi-face Verification

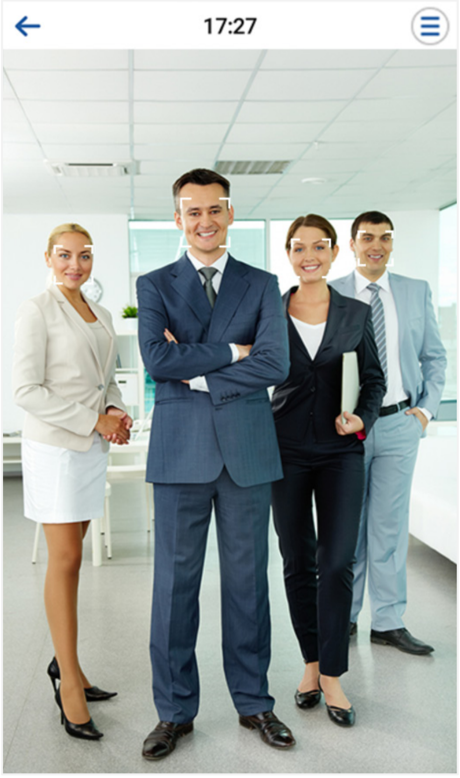
1: N Multi-face Verification

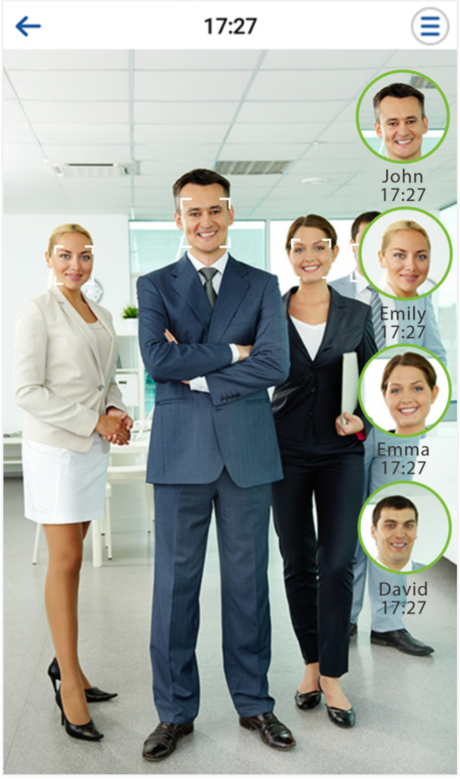
1. Conventional Verification

In this verification mode, the device compares the obtained multi-person facial images with all the face data stored in it. At the same time, the device can verify up to four people. The number of verification results displayed on the right side, can be customized. The image below depicts the pop-up prompt for a successful comparison result.

Tap System > Face > Recognition Settings > Multi-face Identifying > Count to Display to set the number of the verification results to be displayed.

Note: The Count to Display can be set between 1 to 4.

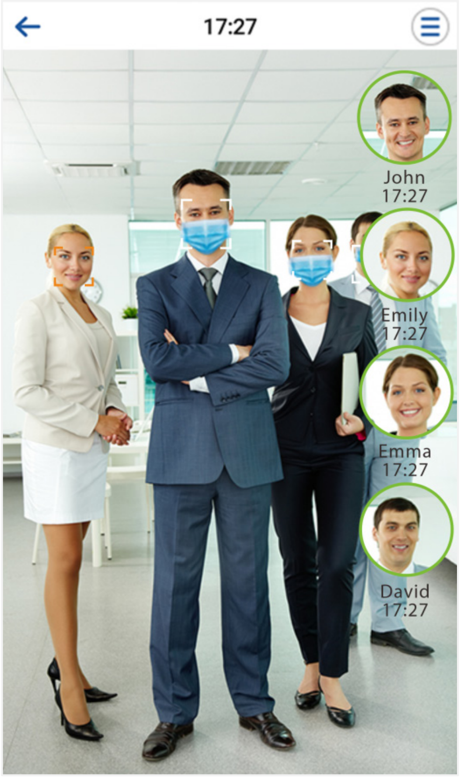




2. Enable Mask Detection

When the user enables the Mask Detection function, the device identifies whether the user is wearing a mask while verification or not. The following are the pop-ups of the comparison result prompt interface.

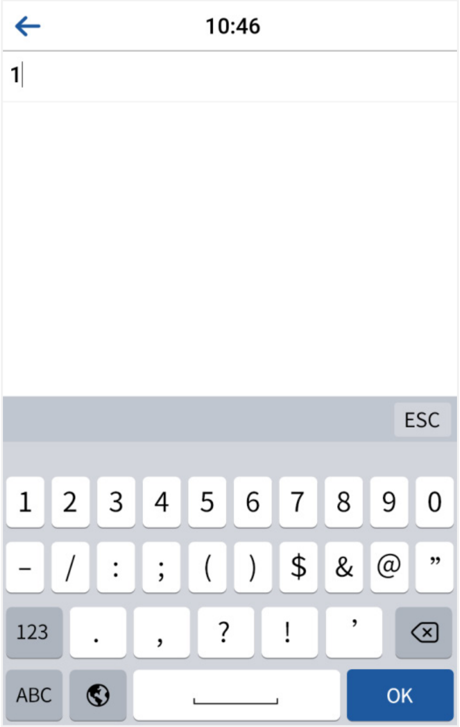
Copyright © 2025 ARMATURA LLC. All rights reserved.



Note: Not wearing a mask is displayed yellow box.

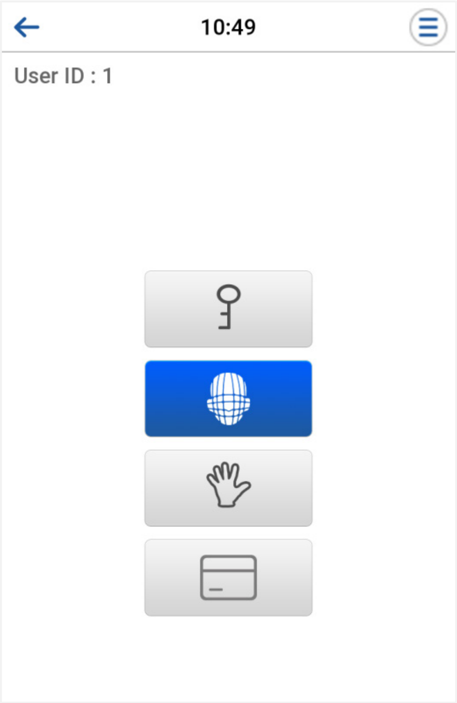
1:1 Multi-face Verification

In this verification mode, the device compares the face captured by the camera with the facial template associated to the entered user ID. Tap ⌨ on the main interface and select the 1:1 facial verification mode and enter the user ID and tap **OK**.

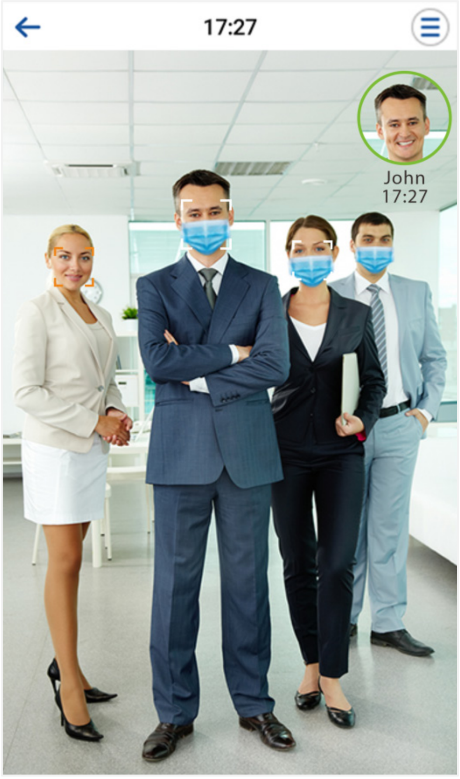


Copyright © 2025 ARMATURA LLC. All rights reserved.

If the user has registered password, card and palm in addition to the face, and the verification method is set to Password/Card/Face/Palm verification, the following screen will appear. Select the 🌐 icon to enter the face verification mode.



After successful verification, it prompts "**Access Granted**", as shown below:

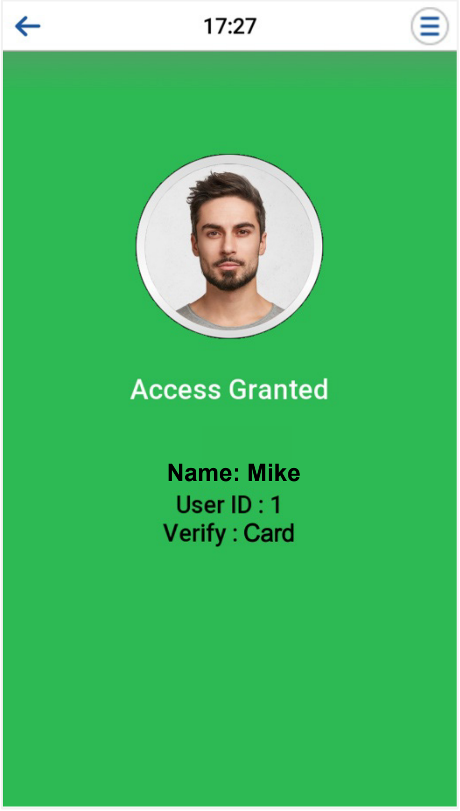


Copyright © 2025 ARMATURA LLC. All rights reserved.

1.7.5 Card Verification

1:N Card Verification

This verification mode compares the card number in the Card induction area with all the card number data registered in the device; the following is the card verification screen.



Access Granted

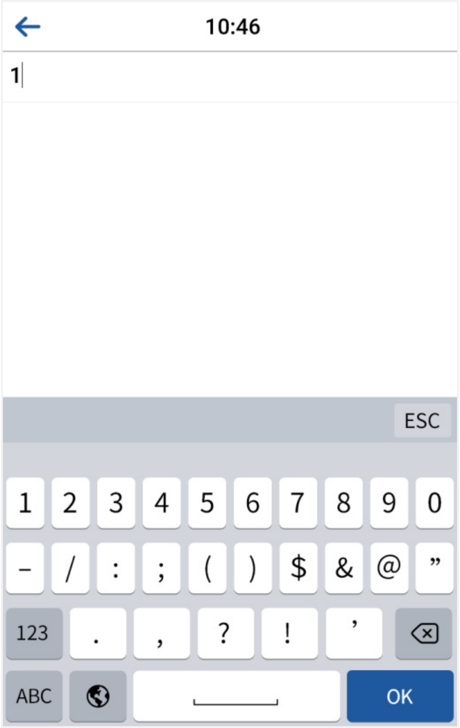
Name: Mike
User ID : 1
Verify : Card

1:1 Card Verification

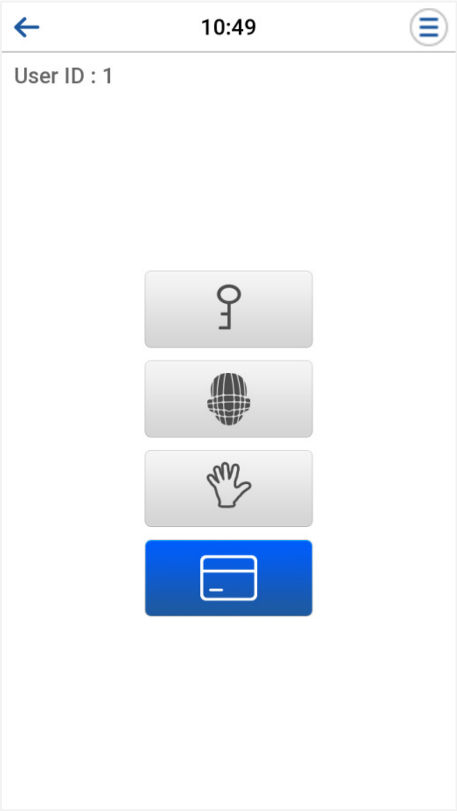
Tap the ⌨ button on the main screen to open the 1:1 Card verification mode.

1. Input the user ID and tap **OK**.

Copyright © 2025 ARMATURA LLC. All rights reserved.

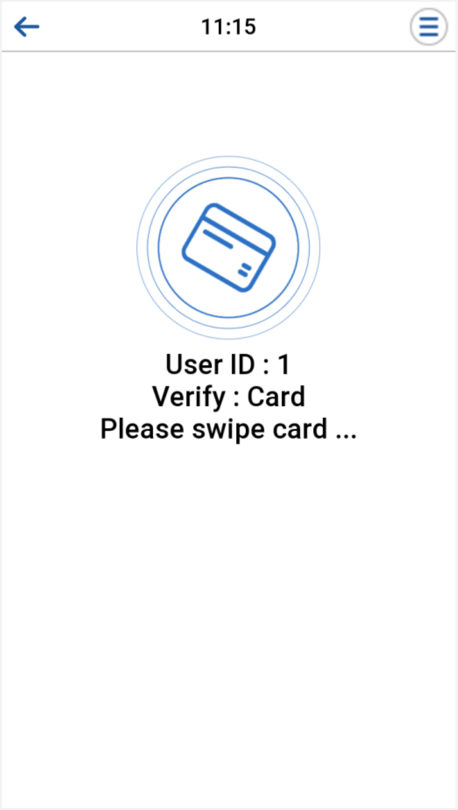


If an employee registers palm, face and password in addition to card, and the verification method is set to Password/Card/Face/Palm, the following screen will appear. Select the ▭ icon to enter the card verification mode.



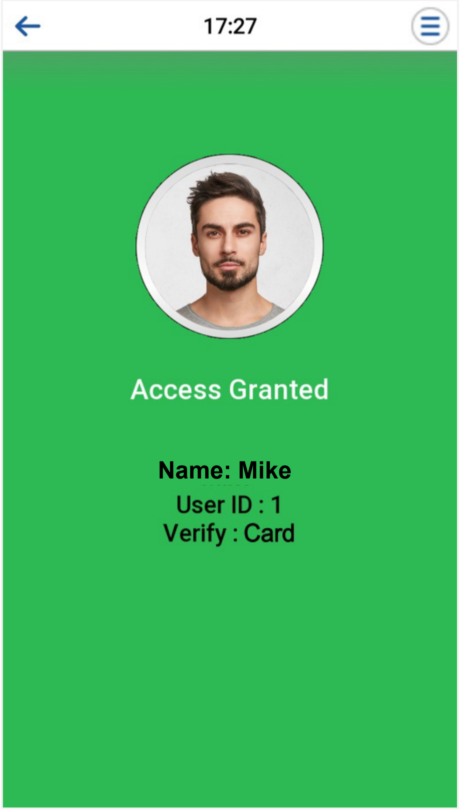
Copyright © 2025 ARMATURA LLC. All rights reserved.

2. Swipe the card above the card area (the card must be registered first).



User ID : 1
Verify : Card
Please swipe card ...

Successful Verification:



Access Granted

Name: Mike
User ID : 1
Verify : Card

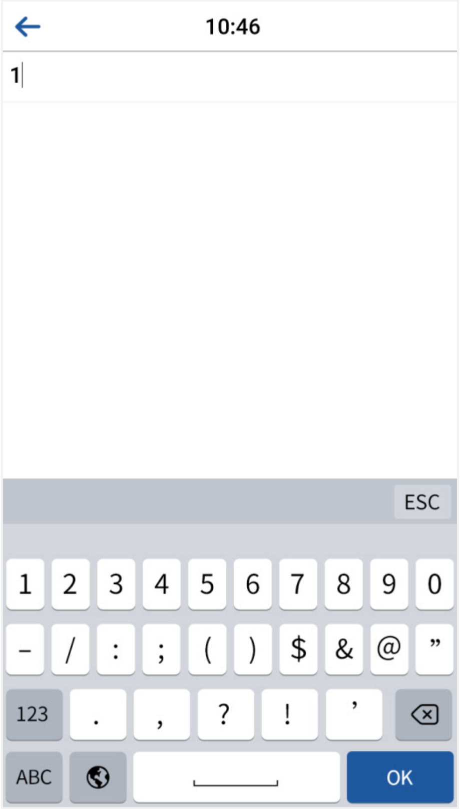
Copyright © 2025 ARMATURA LLC. All rights reserved.

1.7.6 Password Verification

The Password Verification mode compares the entered password with the registered User ID and Password.

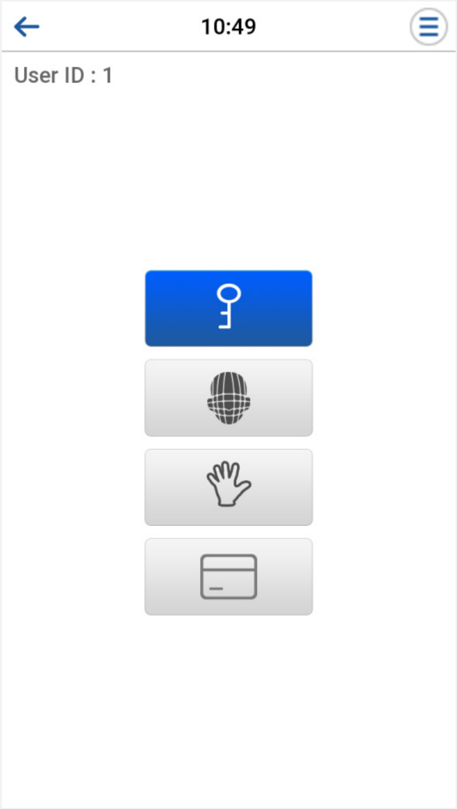
Tap the button on the main screen to open the 1:1 password verification mode.

1. Input the user ID and tap **OK**.

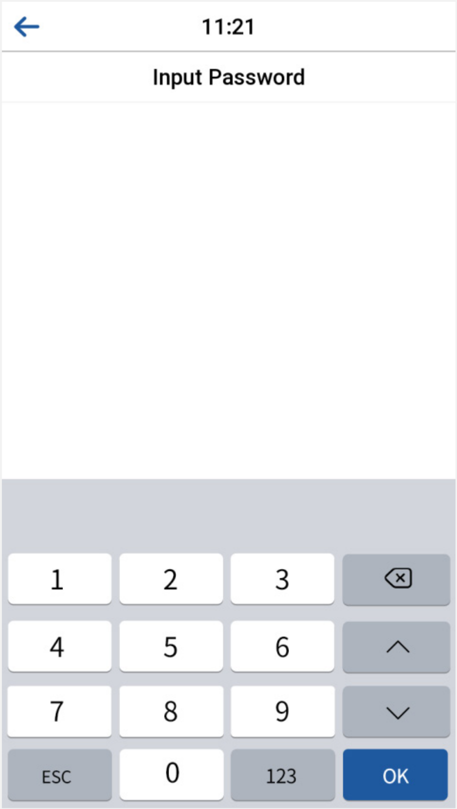


If an employee registers palm, card and face in addition to password, and the verification method is set to Password/Card/Face/Palm, the following screen will appear. Select the icon to enter the password verification mode.

Copyright © 2025 ARMATURA LLC. All rights reserved.

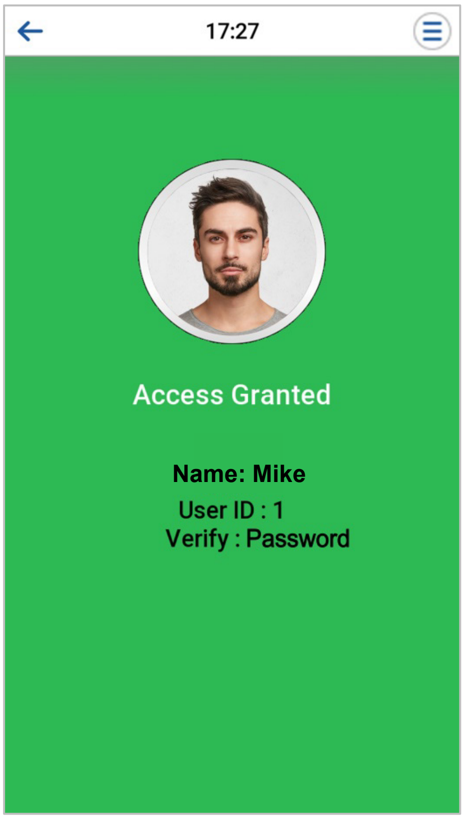


2. Input the password and tap **OK**.



Copyright © 2025 ARMATURA LLC. All rights reserved.

Successful Verification:

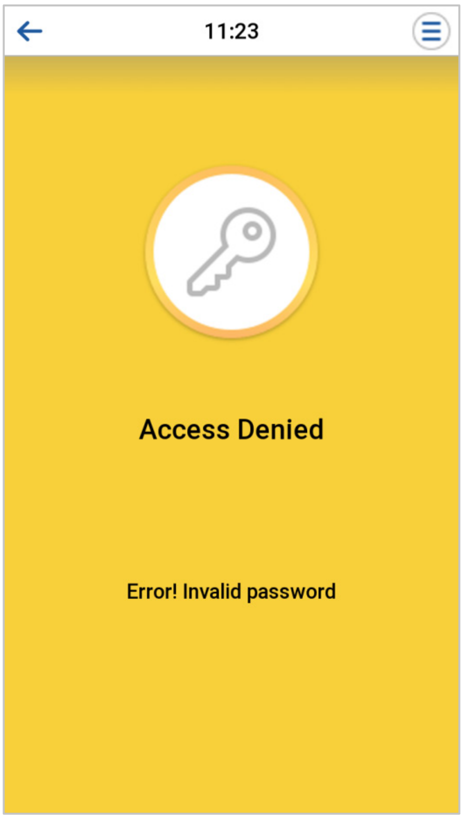


17:27

Access Granted

Name: Mike
User ID : 1
Verify : Password

Failed Verification:



11:23

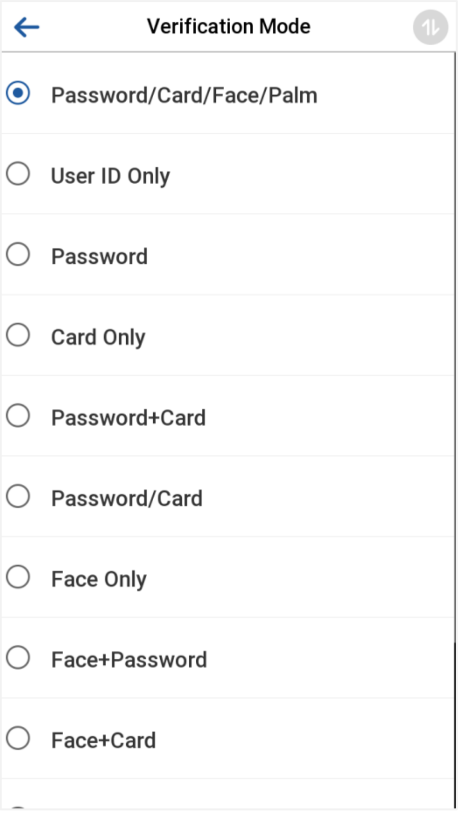
Access Denied

Error! Invalid password

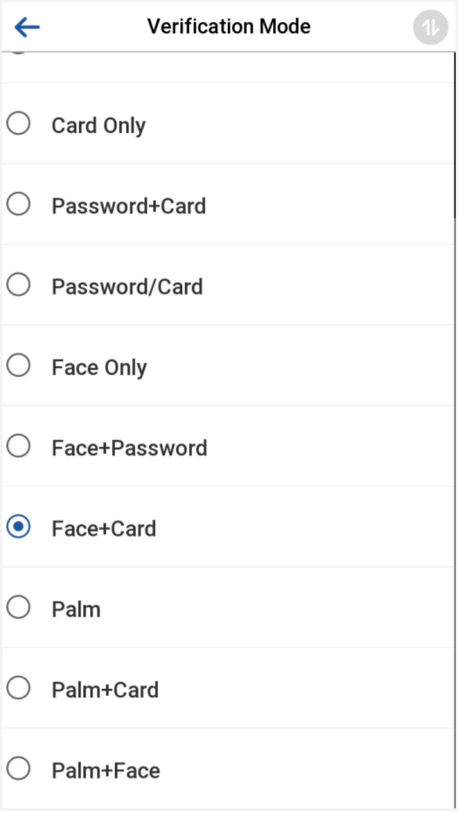
Copyright © 2025 ARMATURA LLC. All rights reserved.

1.7.7 Combined Verification

To increase the security, this device offers the option of using multiple forms of verification methods. A total of 12 different verification combinations can be used, as shown below:


Verification Mode

● Password/Card/Face/Palm
○ User ID Only
○ Password
○ Card Only
○ Password+Card
○ Password/Card
○ Face Only
○ Face+Password
○ Face+Card


Verification Mode

○ Card Only
○ Password+Card
○ Password/Card
○ Face Only
○ Face+Password
● Face+Card
○ Palm
○ Palm+Card
○ Palm+Face

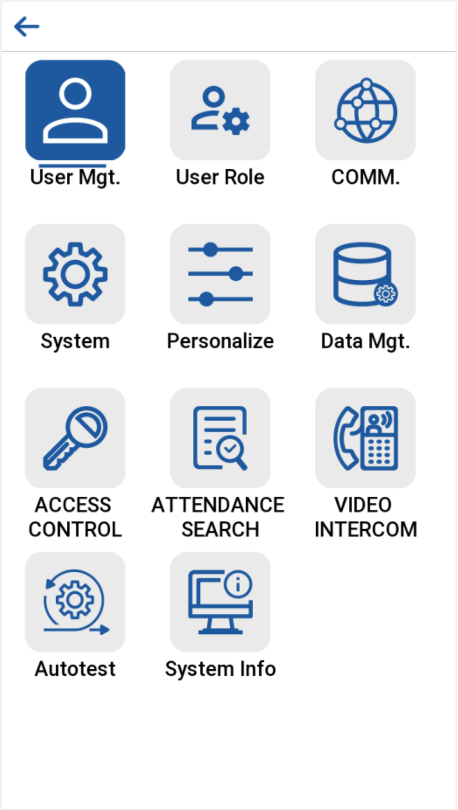
Note:

1. "/" means "or", and "+" means "and".
2. You must register the required verification information before using the combination verification mode, otherwise, the verification may fail. For example, if a user uses Face Registration but the verification mode is Face + Password, this user will never pass verification.

Copyright © 2025 ARMATURA LLC. All rights reserved.

2 Main Menu

Tap ☰ on the initial interface to enter the main menu, as shown below:

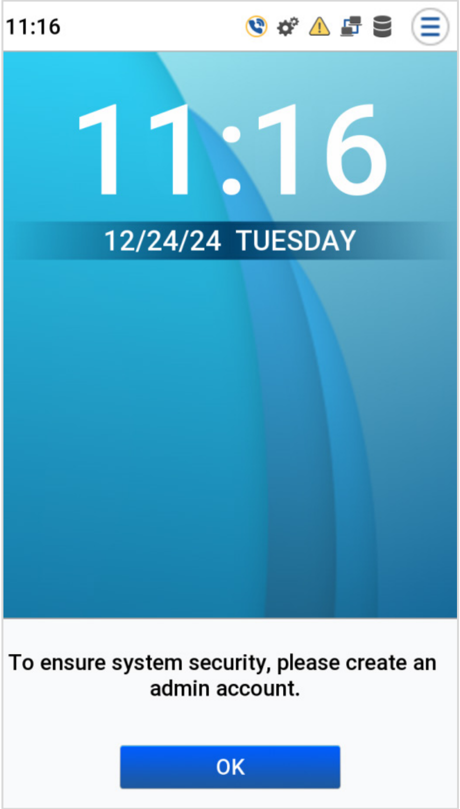


Menu	Description
User Mgt.	To add, edit, view, and delete the basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of the network, Serial Comm, PC Connection, Cloud Server and Wiegand, Network Diagnosis.
System	To set the parameters related to the system, including Date Time, Tap-To-Unlock, Attendance/Access Logs, Facial and Palm templates, QR Code, Card Management, Doorbell Setting, Resetting to factory settings, Security Settings, Device Type Settings and Health Protection.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete all the relevant data in the device.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time Rule Setting, Holiday Settings, Access Groups, Combine Verification, Anti-passback Setup and Duress Option Settings.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Attendance Search	To query the specified Attendance/Event Logs, check Attendance Photos and Blocklist attendance photos.
Video Intercom	To set the parameters related to the SIP.
Autotest	To automatically test whether each module functions properly, including the screen, audio, microphone, camera, real-time clock and Card.
System Info	To view the data capacity, device and firmware information and privacy policy of the device.

Note: When users use the product for the first time, they should operate it after setting administrator privileges. Tap **User Mgt.** to add an administrator or edit user permissions as a super administrator. If the product does not have an administrator setting, the system will show an administrator setting command prompt every time you enter the device menu.



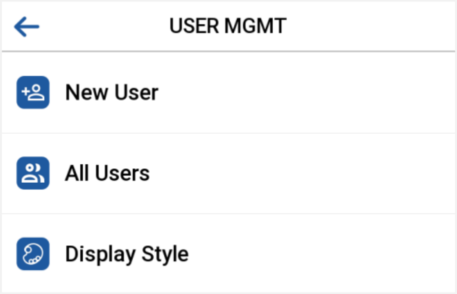
To ensure system security, please create an admin account.

Copyright © 2025 ARMATURA LLC. All rights reserved.

3 User Management

3.1 Add Users

Tap User Mgt. on the main menu.



USER MGMT

New User

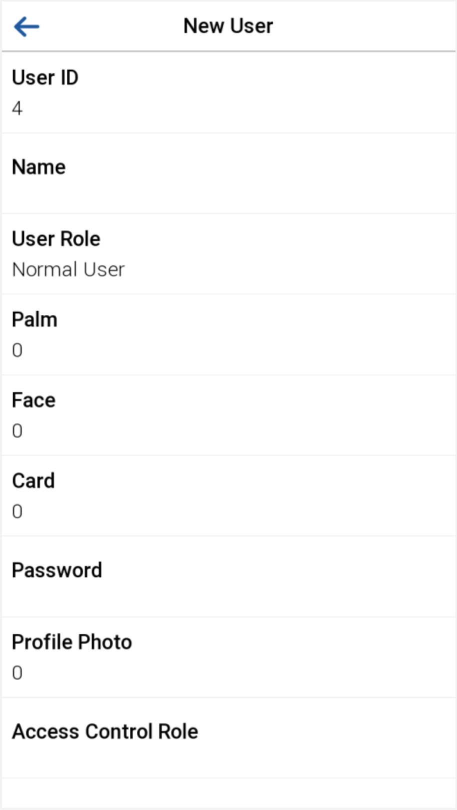
All Users

Display Style

Tap New User.

3.1.1 Register a User ID and Name

Tap New User and enter the User ID and Name.



New User

User ID
4

Name

User Role
Normal User

Palm
0

Face
0

Card
0

Password

Profile Photo
0

Access Control Role

Copyright © 2025 ARMATURA LLC. All rights reserved.

Note:

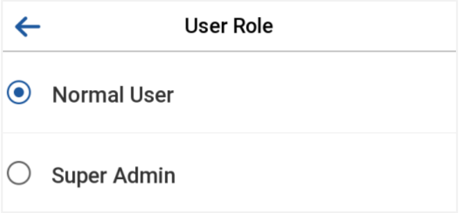
1. A username may contain 31 characters.
2. The user ID may contain 1 to 9 digits by default, supporting both numbers and alphabetic characters.
3. During the initial registration, you can modify your ID, which cannot be modified after registration.
4. If a message "**Duplicated**" pops up, you must choose another ID.

3.1.2 Setting the User Role

On the New User interface, tap on **User Role** to set the user's duty as either **Normal User or Super Admin**.

Tap **User Role** to select Normal User or Super Admin.

- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is registered already in the device, then the Normal Users will not have the privilege to manage the system and can only access authentic verifications.
- **User Defined Roles:** The Normal User can also be assigned custom roles with User Defined Role. The user can be permitted to access several menu options as required.



← User Role

● Normal User

○ Super Admin

Note: If the selected user role is the Super Admin, then the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered.

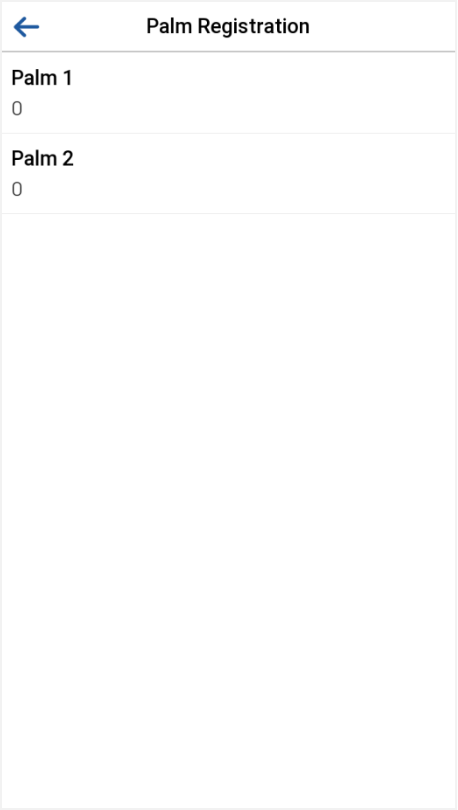
3.1.3 Register Palm

Tap **Palm** in the **New User** interface to enter the palm registration page.

- Support registration of two palms, select the palm to be enrolled.
- Please place your palm inside the guiding box and keep it still while registering.
- A progress bar shows up while registering the palm and a "**successfully registered**" is displayed as the progress bar completes.

If the palm is registered already then, the "**Palm repeated**" message shows up. The registration interface is as follows:

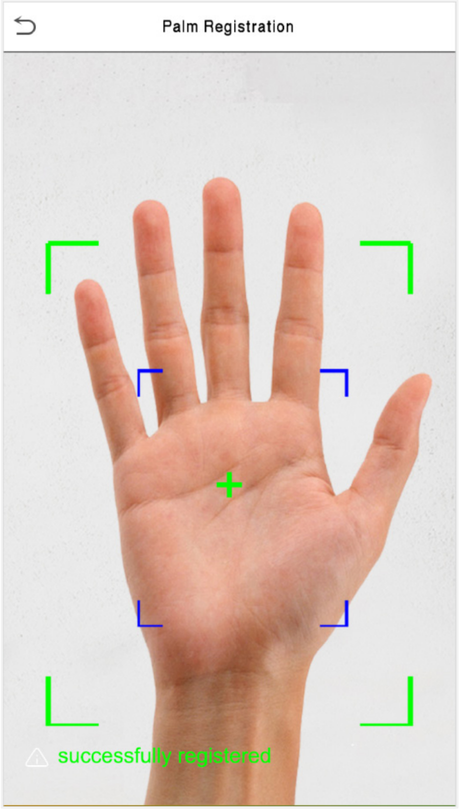
Copyright © 2025 ARMATURA LLC. All rights reserved.



Palm Registration

Palm 1
0

Palm 2
0



Palm Registration

successfully registered

3.1.4 Register Face

Tap **Face** in the **New User** interface to enter the face registration page.

- Please face towards the camera and place yourself in such a way that your face image fits inside the white guiding box and stays still during face registration.
- A progress bar shows up while registering the face and then "**successfully registered**" message is displayed as the progress bar completes.
- If the face is registered already then, the "**Duplicated Face**" message shows up. The registration interface is as follows:

Copyright © 2025 ARMATURA LLC. All rights reserved.

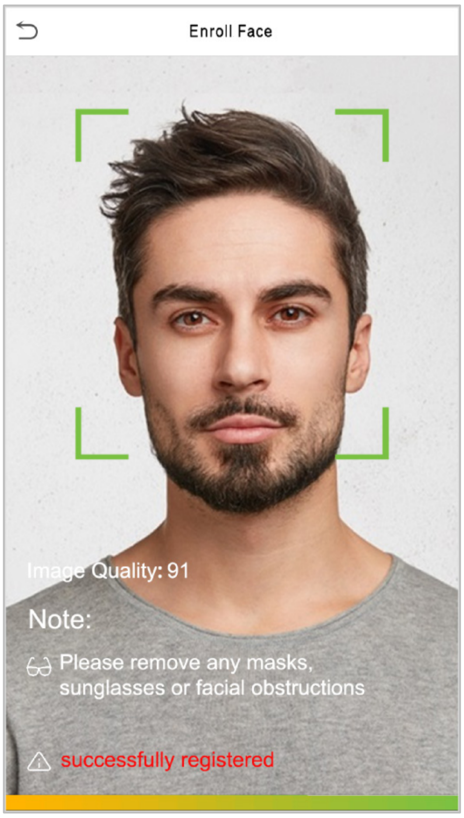


Image Quality: 91

Note:

Please remove any masks, sunglasses or facial obstructions

successfully registered

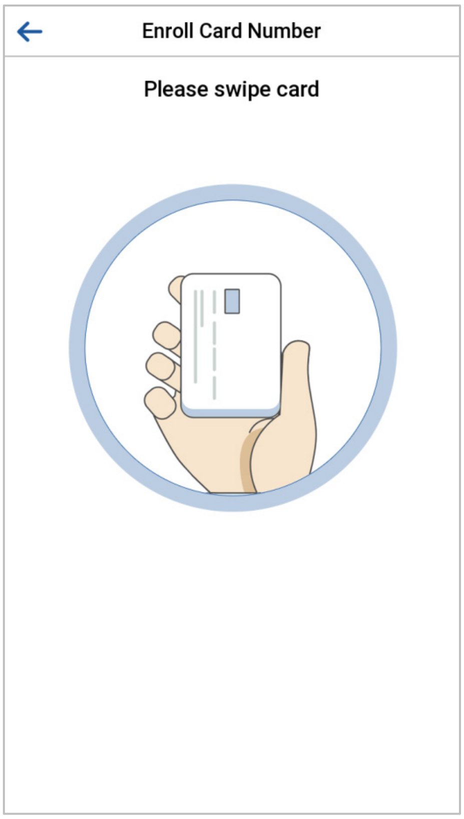
3.1.5 Register Card

Enroll Card

Tap **Card** in the **New User** interface to enter the card registration page.

- Swipe the card underneath the card reading area on the Card interface. The registration of the card will be successful.
- If the card has already been registered, the message "**Error! Card already enrolled**" appears. The registration interface looks like this:

Copyright © 2025 ARMATURA LLC. All rights reserved.

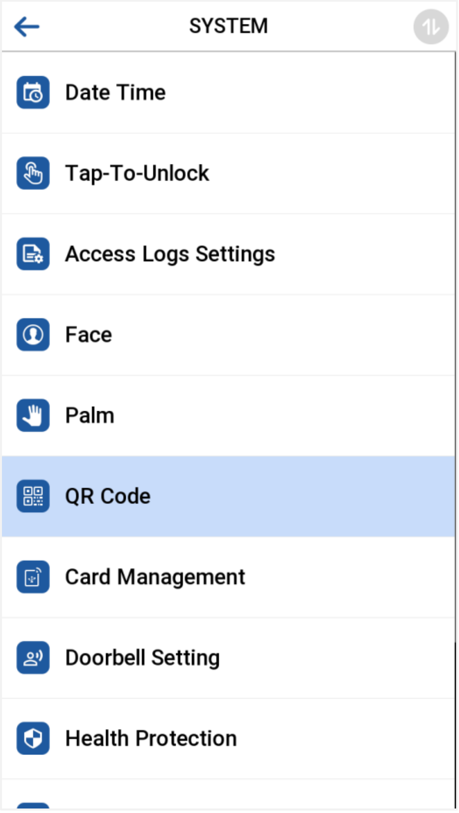


Enroll Card Number

Please swipe card

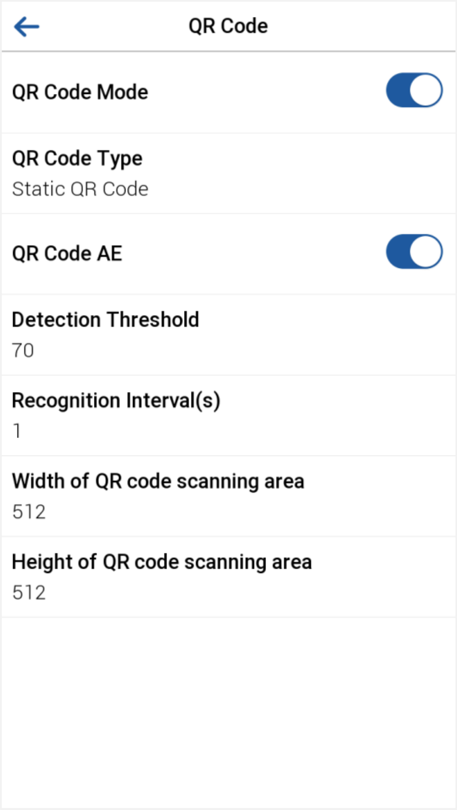
Enroll QR Code

Enable **QR Code Mode** in the **System** interface and select the **QR Code Type** as needed in the QR Code page.



SYSTEM

- Date Time
- Tap-To-Unlock
- Access Logs Settings
- Face
- Palm
- QR Code
- Card Management
- Doorbell Setting
- Health Protection



QR Code

QR Code Mode: on

QR Code Type: Static QR Code

QR Code AE: on

Detection Threshold: 70

Recognition Interval(s): 1

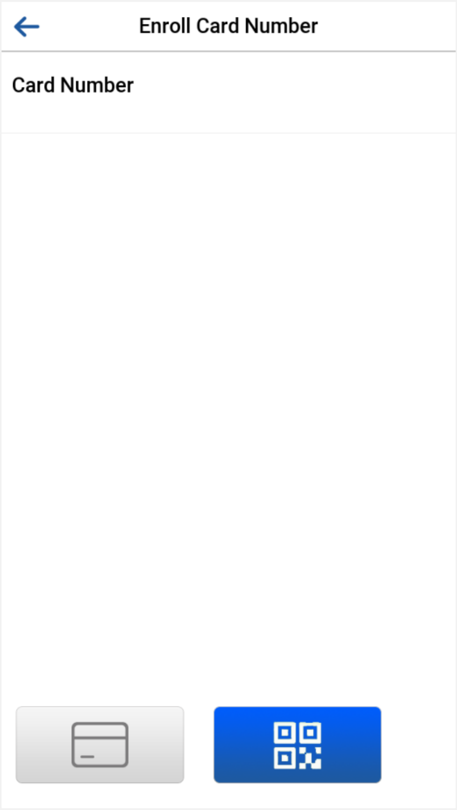
Width of QR code scanning area: 512

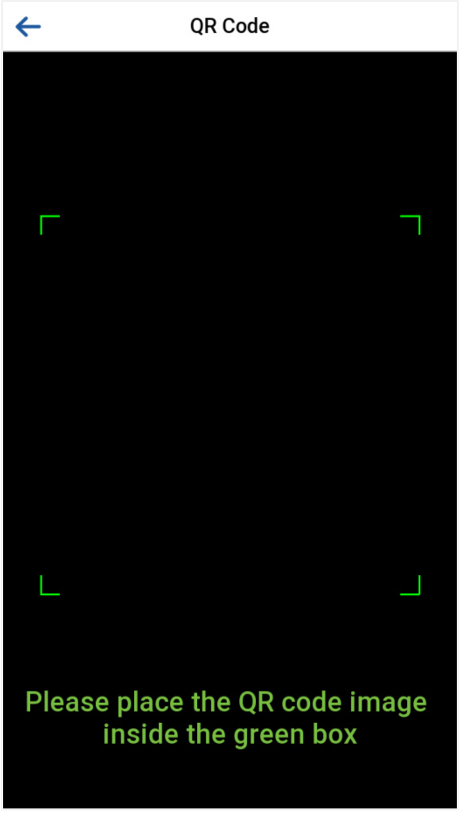
Height of QR code scanning area: 512

Copyright © 2025 ARMATURA LLC. All rights reserved.

Tap **Card** in the **New User** interface to enter the card registration page.

- On the Card interface, show the QR code in front of the camera. The QR code registration will be successful.
- If the QR code is registered already then the "**Error! Card already enrolled.**" message shows up. The registration interface is as follows:



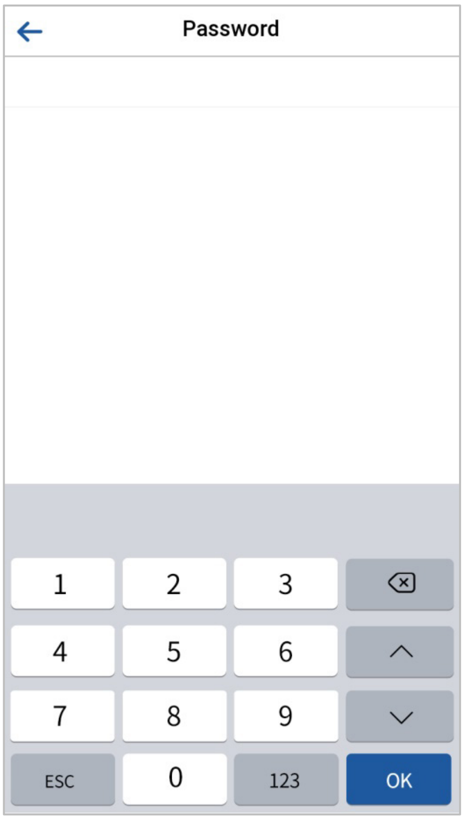


3.1.6 Register Password

Tap **Password** in the **New User** interface to enter the password registration page.

- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password does not match!**", where the user needs to re-confirm the password again.
- The password may contain 1 to 8 digits by default.

Copyright © 2025 ARMATURA LLC. All rights reserved.


Password

3.1.7 Register Profile Photo

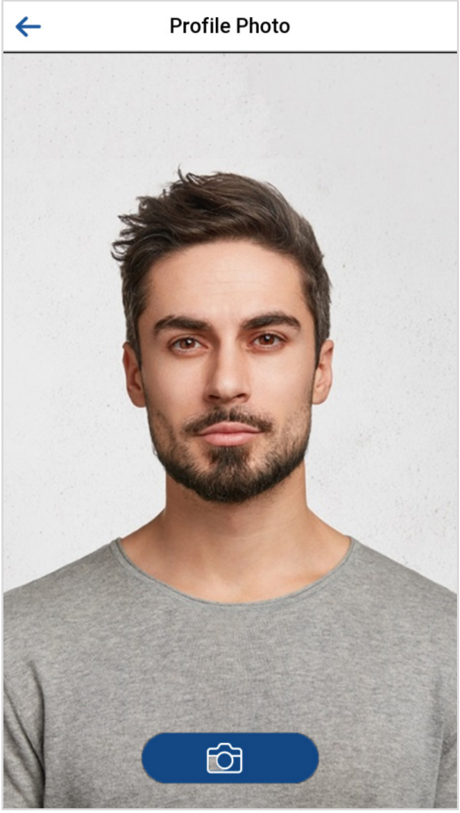
Tap **Profile Photo** in the **New User** interface to enter the profile photo registration page.

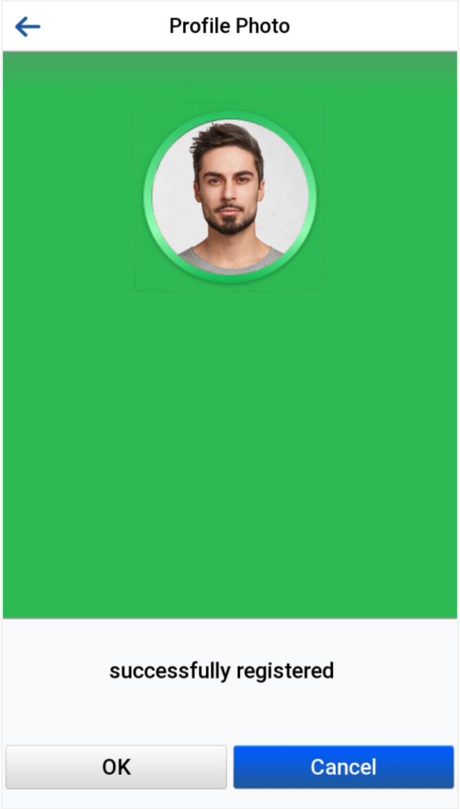
- When a user registered with a photo passes the authentication, the registered photo will be displayed.
- Tap **Profile Photo**, the device's camera will open, then tap the camera icon to take a photo. The captured photo is displayed on the top left corner of the screen and the camera opens up again to take a new photo, after taking the initial photo.

Note:

1. While registering a face, the system automatically captures a photo as the user photo. If you do not register a user photo, the system automatically sets the photo captured while registration as the default photo.
2. This function needs to be enabled in **System** > **Access Logs Settings/Attendance** > **Display User Photo**.

Copyright © 2025 ARMATURA LLC. All rights reserved.



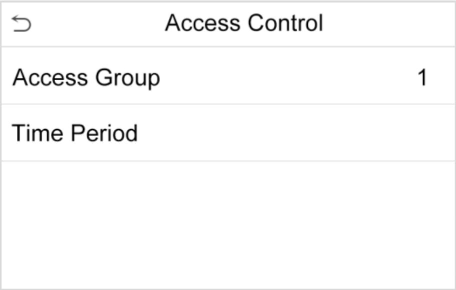


successfully registered

3.1.8 Access Control Role

The **Access Control Role** sets the door access privilege for each user. It includes the access group, verification mode and it facilitates setting the group access time period.

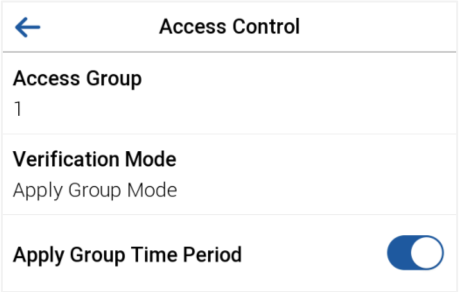
Access Control Terminal:



Access Group 1

Time Period

Time Attendance Terminal:



Access Group
1

Verification Mode
Apply Group Mode

Apply Group Time Period

- Tap **Access Control Role** > **Access Group** to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time to use.
- Select verification mode for the user, tap **Access Control Role** > **Verification Mode**.
- Select whether to apply the group time period for this user. It is enabled by default. If the group time period is not applied, you need to set the unlocking time for this user. The time period of this user does not affect the time period of any other member in this group. To set the unlocking

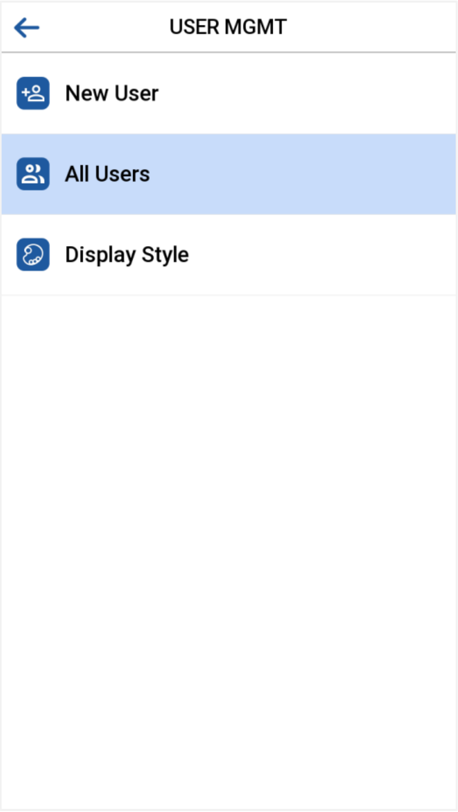
Copyright © 2025 ARMATURA LLC. All rights reserved.

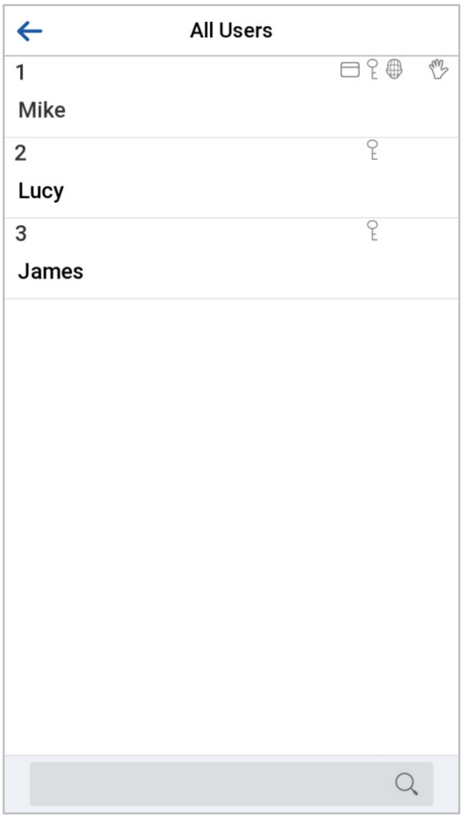
time for this user, tap **Apply Group Time Period > Time Period 1**. Enter the Time Period number and tap **OK**. 50 time periods can be set in the device and three time periods can be set for each user. For details, see Time Schedule Settings.

3.2 Search for Users

On the **Main Menu**, tap **User Mgt.**, and then tap **All Users** to search a User.

- On the **All-Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.

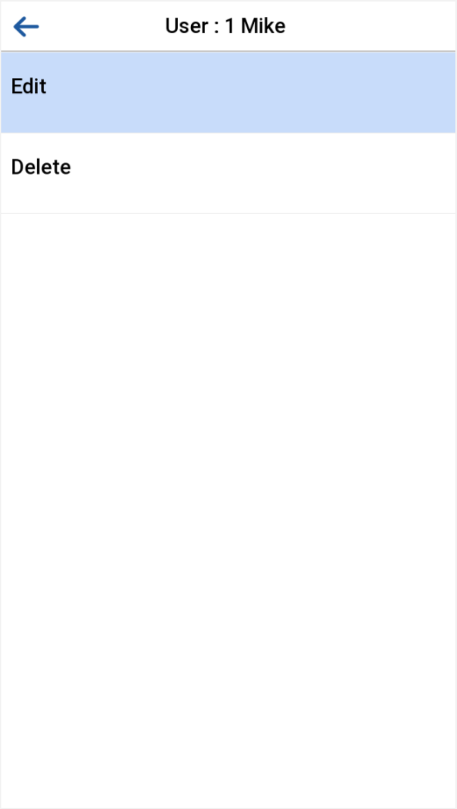


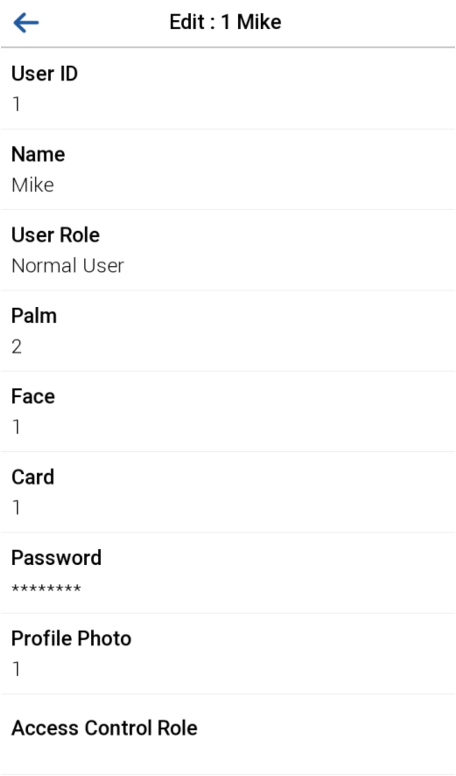


3.3 Edit Users

On the **All-Users** interface, tap on the required user from the list and tap **Edit** to edit the user information.

Copyright © 2025 ARMATURA LLC. All rights reserved.




Edit : 1 Mike

User ID
1

Name
Mike

User Role
Normal User

Palm
2

Face
1

Card
1

Password
****

Profile Photo
1

Access Control Role

Note: The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user. For further details, refers "3.1 Add Users".

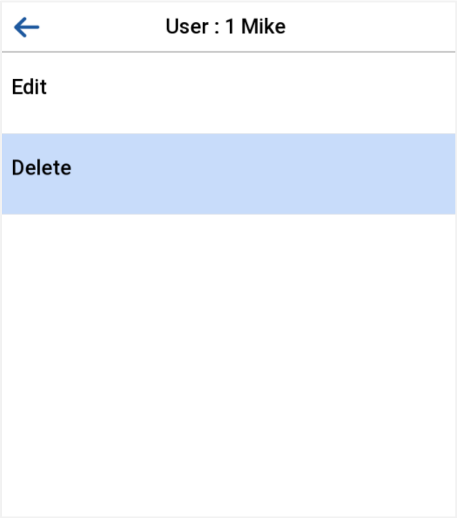
3.4 Delete Users

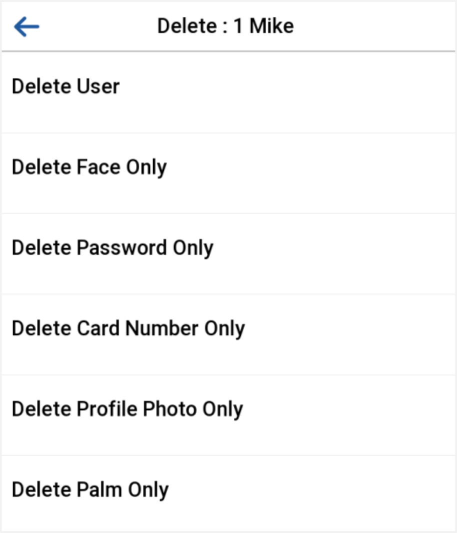
On the **All-Users** interface, tap on the required user from the list and tap **Delete** to delete the user or specific user information from the device. On the **Delete** interface, tap on the required operation, and then tap **OK** to confirm the deletion.

Delete Operations

- **Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.
- **Delete Face Only:** Deletes the face information of the selected user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete Card Only:** Deletes the card information of the selected user.
- **Delete Profile Photo Only:** Deletes the profile photo of the selected user.
- **Delete Palm Only:** Deletes the palm information of the selected user.

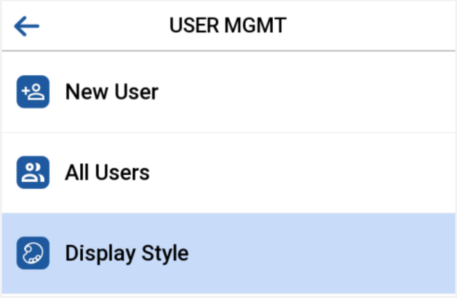
Copyright © 2025 ARMATURA LLC. All rights reserved.

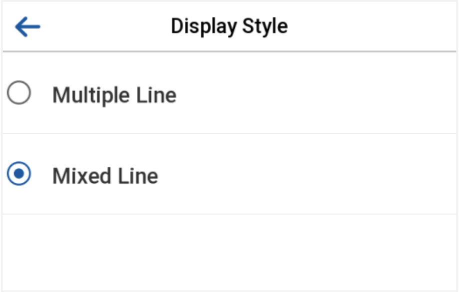




3.5 Display Style

On the **Main Menu**, tap **User Mgt.**, and then tap **Display Style** to enter Display Style setting interface.



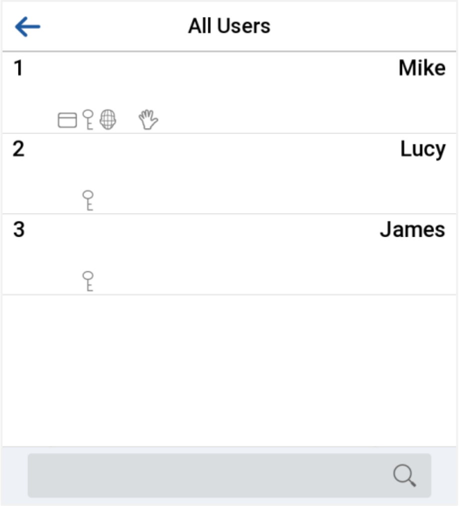

Display Style

○ Multiple Line

● Mixed Line

All the Display Styles are shown as below:

Multiple Line:

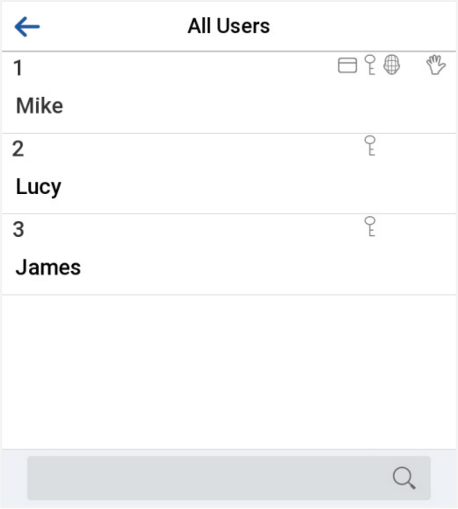

All Users

1 Mike

2 Lucy

3 James

Mixed Line:


All Users

1 Mike

2 Lucy

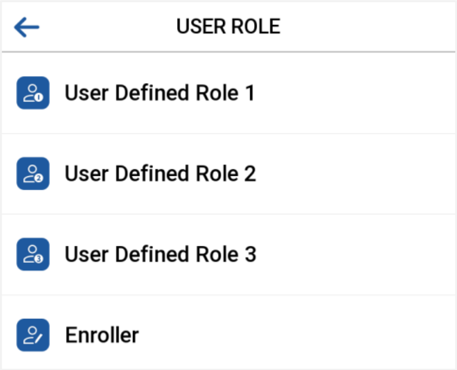
3 James

Copyright © 2025 ARMATURA LLC. All rights reserved.

4 User Role

User Role facilitates to assign some specific permissions to certain users, based on the requirement.

- On the **Main** menu, tap **User Role**, and then tap on the **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.


USER ROLE

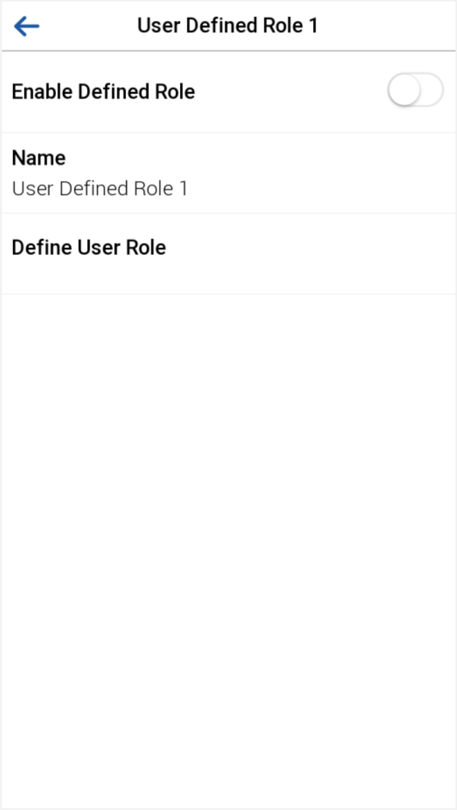
User Defined Role 1

User Defined Role 2

User Defined Role 3

Enroller

- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.


User Defined Role 1

Enable Defined Role

Name
User Defined Role 1

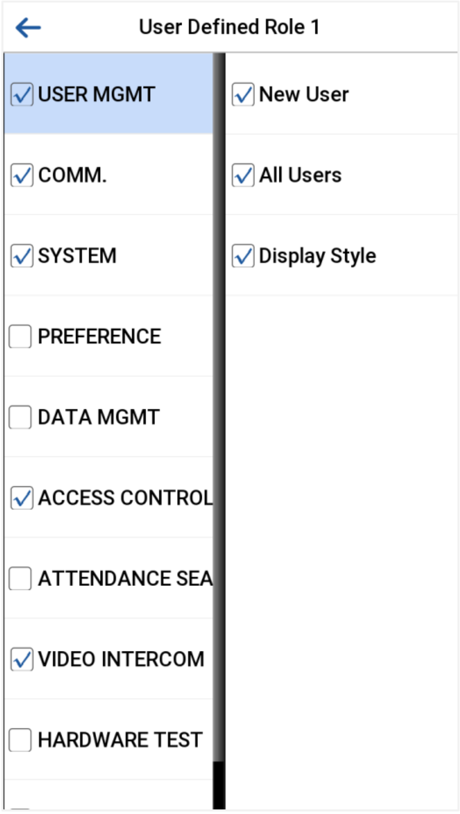
Define User Role

- Then, by tapping on Define User Role, select the required privileges for the new role, and then

Copyright © 2025 ARMATURA LLC. All rights reserved.

tap the Return button.

- During privilege assignment, the main menu function names will be displayed on the left and its sub-menus will be listed on the right.
- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.



User Defined Role 1

☑ USER MGMT	☑ New User
☑ COMM.	☑ All Users
☑ SYSTEM	☑ Display Style
□ PREFERENCE	
□ DATA MGMT	
☑ ACCESS CONTROL	
□ ATTENDANCE SEA	
☑ VIDEO INTERCOM	
□ HARDWARE TEST	

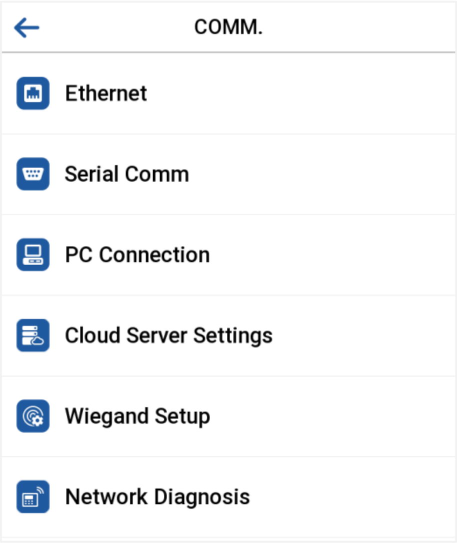
Note: If the User Role is enabled for the Device, tap on **User Mgt.** > **New User** > **User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "**Please enroll super admin first!**" when enabling the User Role function.

Copyright © 2025 ARMATURA LLC. All rights reserved.

5 Communication Settings

Communication Settings are used to set the parameters of the Network, Serial Comm, PC connection, Cloud server, Wiegand and Network Diagnosis.

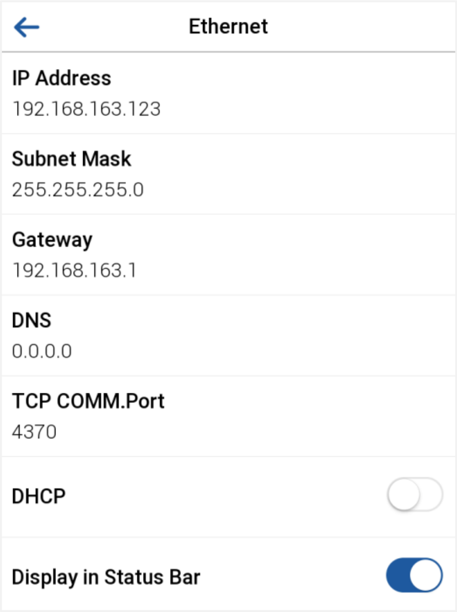
Tap **COMM.** on the main menu.



5.1 Network Settings

When the device needs to communicate with a PC over the Ethernet, you need to configure network settings and ensure that the device and the PC are connecting to the same network segment.

Tap **Ethernet** on the **COMM.** Settings interface.



IP Address
192.168.163.123

Subnet Mask
255.255.255.0

Gateway
192.168.163.1

DNS
0.0.0.0

TCP COMM.Port
4370

DHCP ○

Display in Status Bar ●

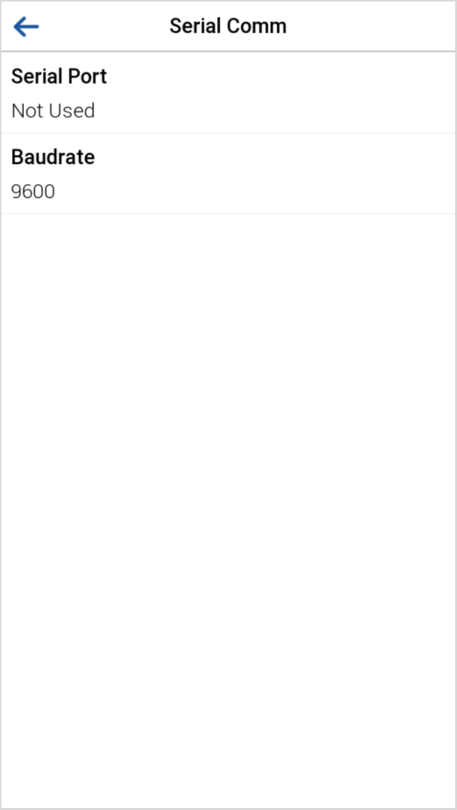
Copyright © 2025 ARMATURA LLC. All rights reserved.

Menu	Description
IP Address	The factory default value is 192.168.1.201. Please set the IP Address as per the requirements.
Subnet Mask	The factory default value is 255.255.255.0. Please set the value as per the requirements.
Gateway	The factory default address is 0.0.0.0. Please set the value as per the requirements.
DNS	The factory default address is 0.0.0.0. Please set the value as per the requirements.
TCP COMM. Port	The factory default value is 4370. Please set the value as per the requirements.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.
Display in Status Bar	To set whether to display the network icon on the status bar.

5.2 Serial Comm

Serial Comm function establishes communication with the device through a serial port (Control Unit/ OSDP Unit/ DM10).

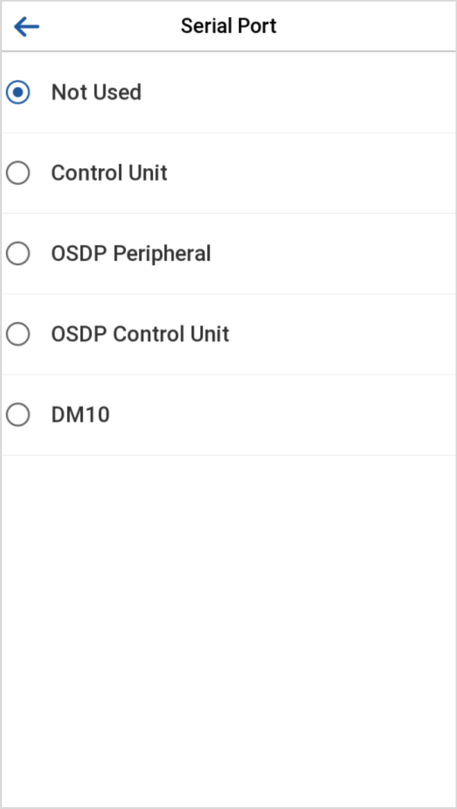
Tap **Serial Comm.** on the **COMM.** Settings interface.



Serial Comm

Serial Port
Not Used

Baudrate
9600



Serial Port

● Not Used

○ Control Unit

○ OSDP Peripheral

○ OSDP Control Unit

○ DM10

Copyright © 2025 ARMATURA LLC. All rights reserved.

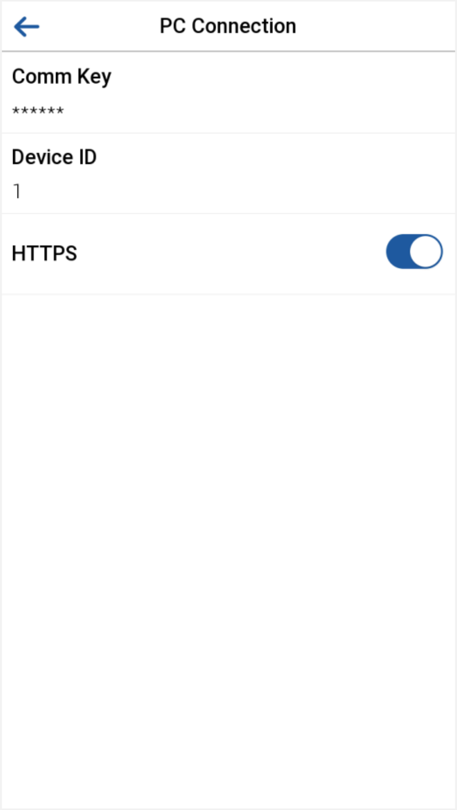
Menu	Description
Serial Port	**Not Used:** No communication with the device through the serial port. **Control Unit:** When RS485 is used as the function of "**Control Unit**", it can be connected to a card reader. **OSDP Peripheral:** Communicate with the device through the OSDP output. **OSDP Control Unit:** Communicate with the device through the OSDP output. **DM10:** When RS485 is used as the function of **"DM10"**, it can be connected to DM10 to control the lock relay.
Baudrate	There are 5 baud rate options at which the data communicates with PC. They are: 115200 (default), 57600, 38400, 19200 and 9600. The higher the baud rate, the faster is the communication speed, but also 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 is more reliable.

5.3 PC Connection

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.

Tap **PC Connection** on the **COMM.** Settings interface.

Copyright © 2025 ARMATURA LLC. All rights reserved.


PC Connection

Comm Key
******

Device ID
1

HTTPS

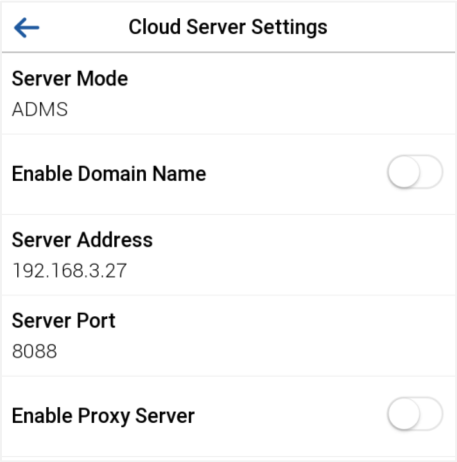
Menu	Description
Comm Key	The Comm Key must be 6 digits.
Device ID	The identity number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.
HTTPS	To increase the security of software access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication. This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will display a security prompt and restart.

5.4 Cloud Server Setting

This represents the settings used for connecting the ADMS server.

Tap **Cloud Server Setting** on the **COMM.** Settings interface.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Cloud Server Settings

Server Mode
ADMS

Enable Domain Name ○

Server Address
192.168.3.27

Server Port
8088

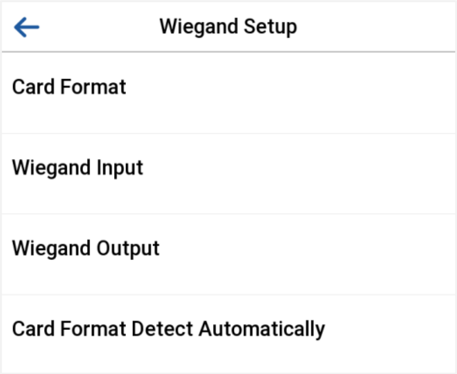
Enable Proxy Server ○

Menu		Description
Enable Domain Name	Server Address	When this function is enabled, the domain name mode "https://... "will be used, such as https://armatura.one:8088.
Disable Domain Name	Server Address	IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

5.5 Wiegand Setup

The menu is used to set the Wiegand Input & Output parameters, Card Format and Custom Card Format.

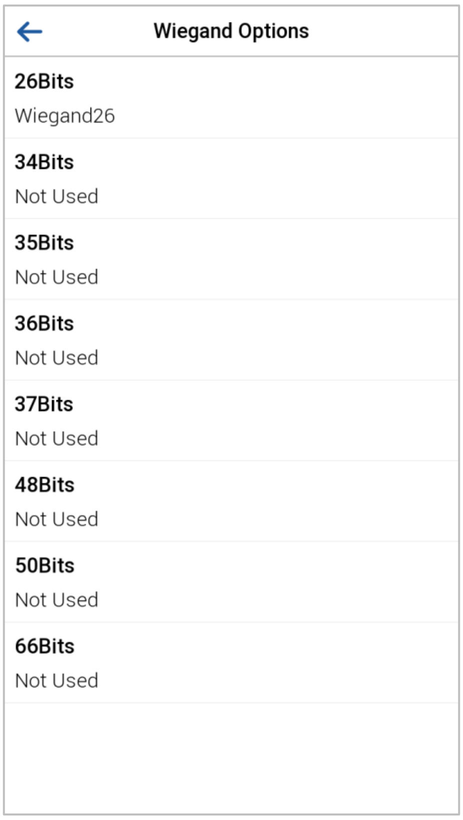
Tap **Wiegand Setup** on the **COMM.** Settings interface.



Card Format

Set the card format for this device. Support 26 bits, 34 bits, 35 bits, 36 bits, 37 bits, 48 bits, 50 bits and 66Bits.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Wiegand Options

26Bits
Wiegand26

34Bits
Not Used

35Bits
Not Used

36Bits
Not Used

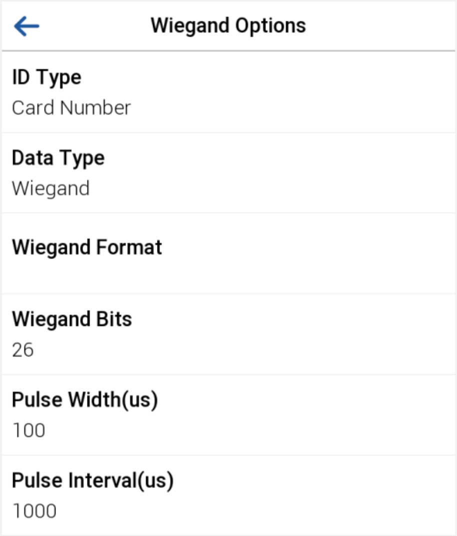
37Bits
Not Used

48Bits
Not Used

50Bits
Not Used

66Bits
Not Used

Wiegand Input



Wiegand Options

ID Type
Card Number

Data Type
Wiegand

Wiegand Format

Wiegand Bits
26

Pulse Width(us)
100

Pulse Interval(us)
1000

Menu	Descriptions
ID Type	Select between the User ID and Card number.
Data Type	Select between the Wiegand and Raw.
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.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default,

Copyright © 2025 ARMATURA LLC. All rights reserved.

	which can be adjusted within the range of 20 to 400 microseconds.
Pulse Interval(us)	The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.

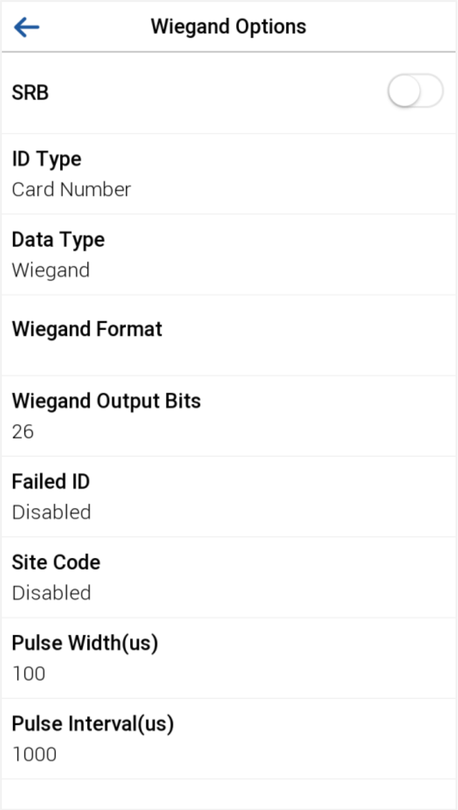
Definitions of various common Wiegand formats:

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits is the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits is the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME It consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits is the device codes. The 18th to 33rd bits is the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO It consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE It consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO It consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 14th bits is the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits is the site codes, and the 18th to 49th bits are the card numbers.
"C" denotes the card number; "E" denotes the even parity bit; "O" denotes the odd parity bit; "F" denotes the facility code; "M" denotes the manufacturer code; "P" denotes the parity bit; and "S" denotes the site code.	

Wiegand Output



Wiegand Options

SRB

ID Type
Card Number

Data Type
Wiegand

Wiegand Format

Wiegand Output Bits
26

Failed ID
Disabled

Site Code
Disabled

Pulse Width(us)
100

Pulse Interval(us)
1000

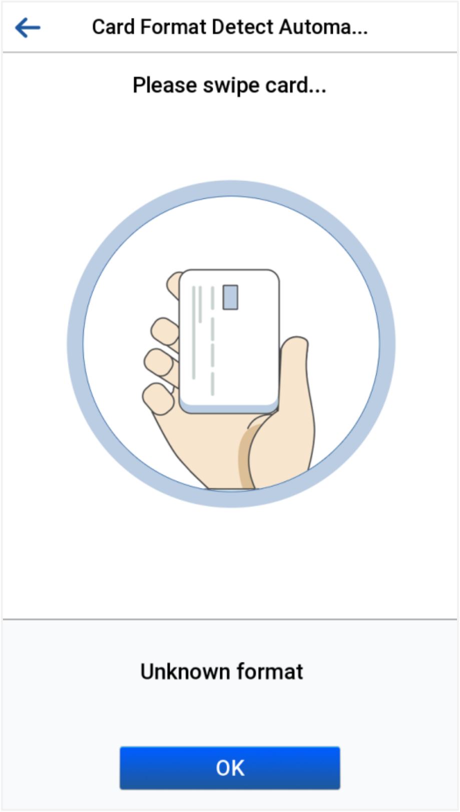
Menu	Descriptions
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
ID Type	The default selection is card number.
Data Type	Select between the Wiegand and Raw.
Wiegand Format	Values range from 26 bits, 34 bits, 35 bits, 36 bits, 37 bits, 48 bits, 50 bits, and 66Bits.
Wiegand Output Bits	After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new ones.
Site Code	It is similar to the Device ID. The difference is that a site code can be set

Copyright © 2025 ARMATURA LLC. All rights reserved.

	manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	Pulse width refers to the duration of the signal's highstate during transmission.
Pulse Interval(us)	The time interval between pulses.

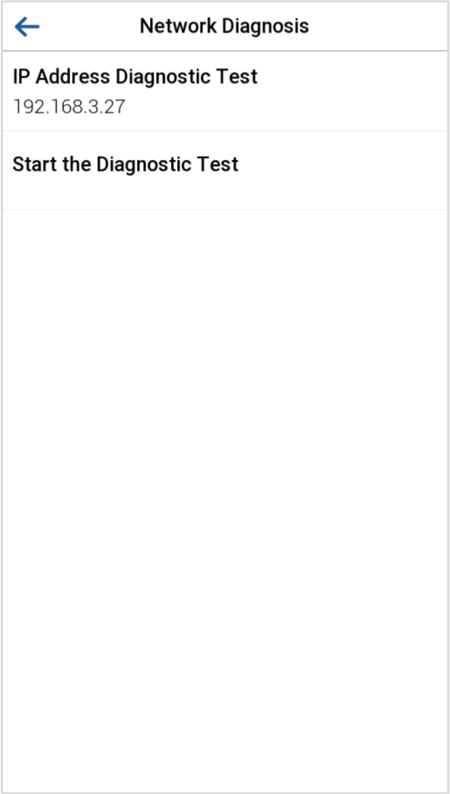
Card Format Detect Automatically

Detect the card format name, wiegand bits, Site code, card number, even parity and odd parity.



Copyright © 2025 ARMATURA LLC. All rights reserved.

5.6 Network Diagnosis



Network Diagnosis

IP Address Diagnostic Test
192.168.3.27

Start the Diagnostic Test

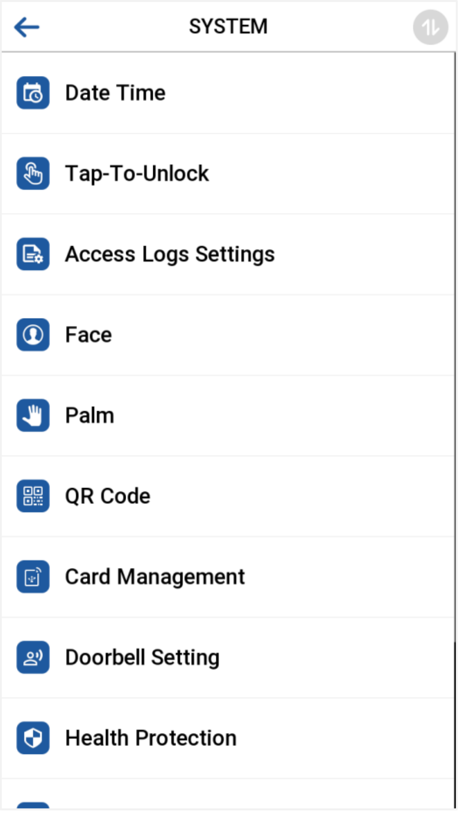
Menu	Description
IP Address Diagnostic Test	The factory default address is 0.0.0.0. Please set the value as per the requirements.
Start the Diagnostic Test	Tap start to automatically diagnose the network.

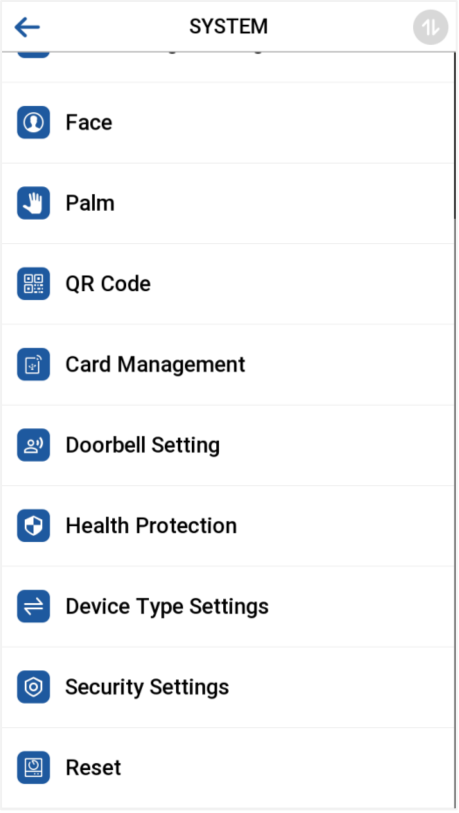
Copyright © 2025 ARMATURA LLC. All rights reserved.

6 System Settings

The System Settings is used to set the related system parameters to optimize the performance of the device.

Tap **System** on the main menu interface.

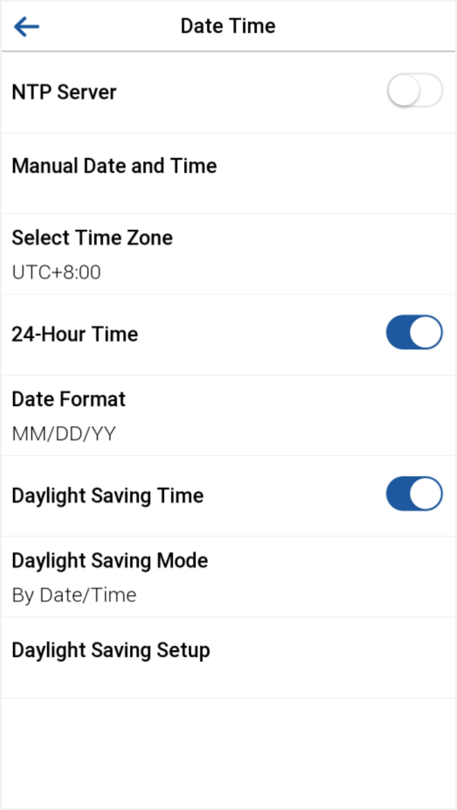




6.1 Date and Time

Tap **Date Time** on the **System** interface.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Date Time

NTP Server

Manual Date and Time

Select Time Zone
UTC+8:00

24-Hour Time

Date Format
MM/DD/YY

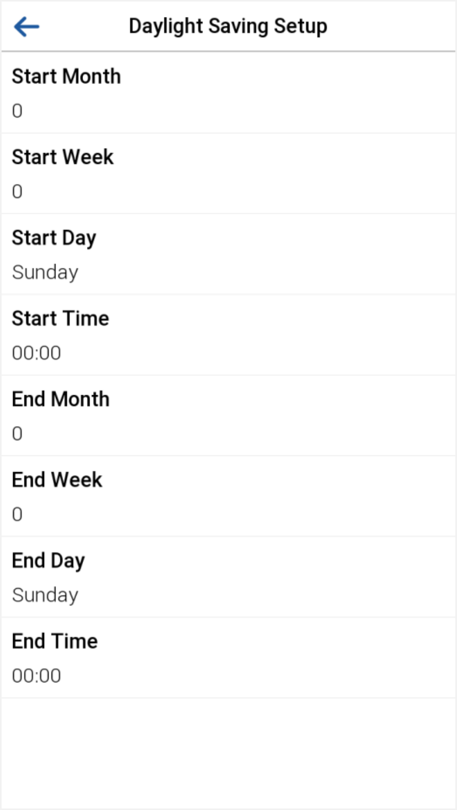
Daylight Saving Time

Daylight Saving Mode
By Date/Time

Daylight Saving Setup

- Tap **NTP Server** to enable automatic time synchronization based on the service address you enter.
- Tap **Manual Date and Time** to manually set the date and time and then tap to **Confirm** and save.
- Tap **Select Time Zone** to manually select the time zone where the device is located.
- Enable or disable this format by tapping 24-Hour Time. If enabled, then select the **Date Format** to set the date.
- Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set up the switch time.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Daylight Saving Setup

Start Month
0

Start Week
0

Start Day
Sunday

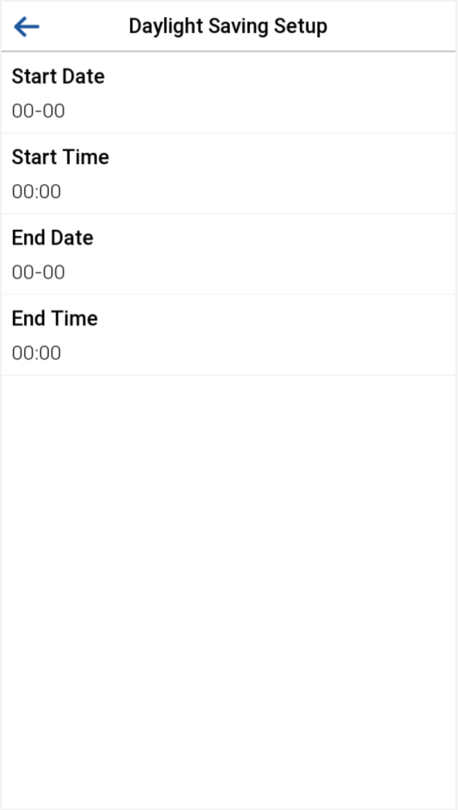
Start Time
00:00

End Month
0

End Week
0

End Day
Sunday

End Time
00:00



Daylight Saving Setup

Start Date
00-00

Start Time
00:00

End Date
00-00

End Time
00:00

Week Mode Date Mode

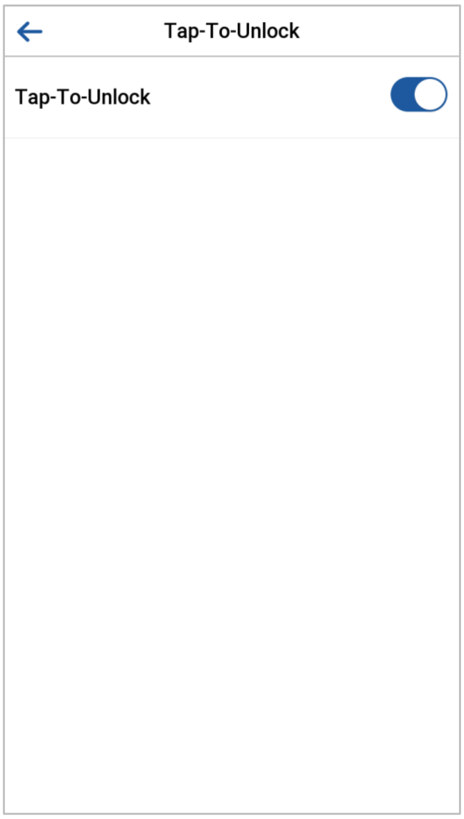
Note: For example, the user sets the time of the device (18:35 on March 15, 2020) to 18:30 on January 1, 2021. After restoring the factory settings, the time of the device will change to 18:30, January 1, 2021.

6.2 Tap-To-Unlock

Enable **Tap-To-Unlock**, and it will take effect after the device restarts. After the function takes effect, it will turn off the sensing function of camera auto-identification, and only touching the device screen can wake up the camera for auto-identification.

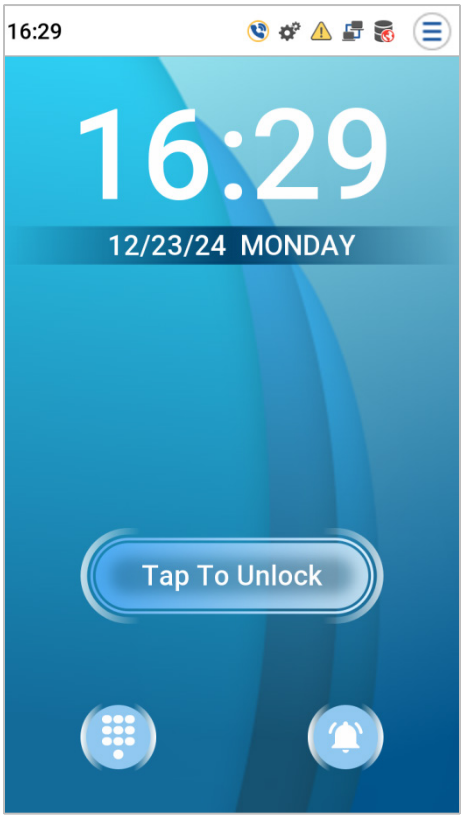
Tap **Tap-To-Unlock** on the System interface to enable this function.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Tap-To-Unlock

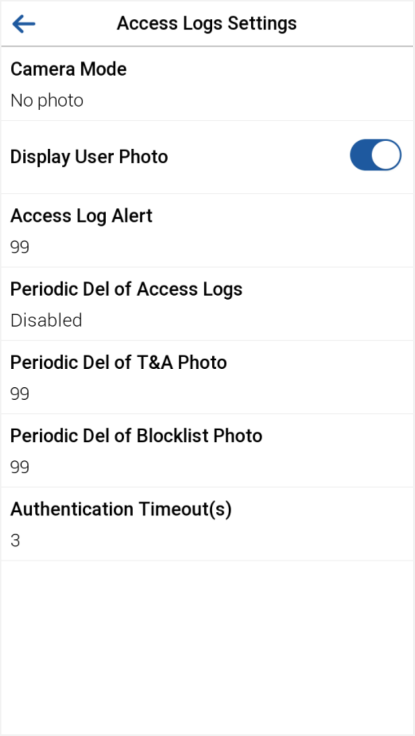
Tap-To-Unlock ●



6.3 Access Log Settings/Attendance

Tap Access Logs Settings/Attendance on the System interface.

Access Control Terminal:



Access Logs Settings

Camera Mode
No photo

Display User Photo ●

Access Log Alert
99

Periodic Del of Access Logs
Disabled

Periodic Del of T&A Photo
99

Periodic Del of Blocklist Photo
99

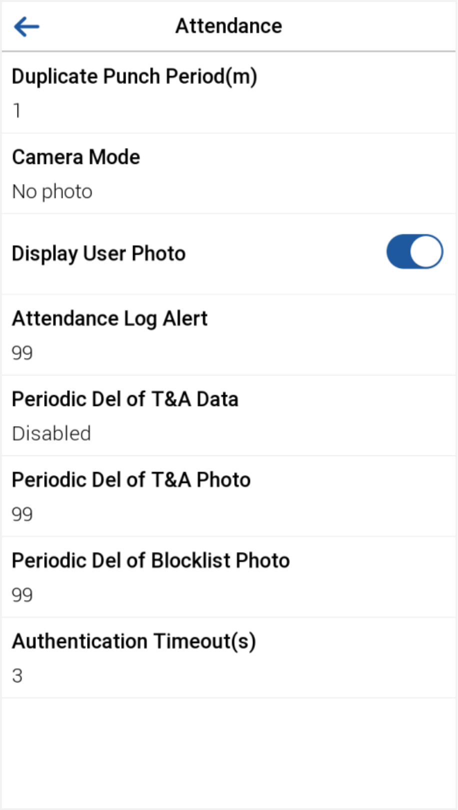
Authentication Timeout(s)
3

Copyright © 2025 ARMATURA LLC. All rights reserved.

Function Name	Description
Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but not saved during verification. **Take photo and save:** All the photos taken during verification is saved. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved only for each failed verification.
Display User Photo	This function is disabled by default. When enabled, a security prompt will pop-up.
Access Log Alert	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of Access Logs	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Time Attendance Terminal:



Attendance

Duplicate Punch Period(m)
1

Camera Mode
No photo

Display User Photo

Attendance Log Alert
99

Periodic Del of T&A Data
Disabled

Periodic Del of T&A Photo
99

Periodic Del of Blocklist Photo
99

Authentication Timeout(s)
3

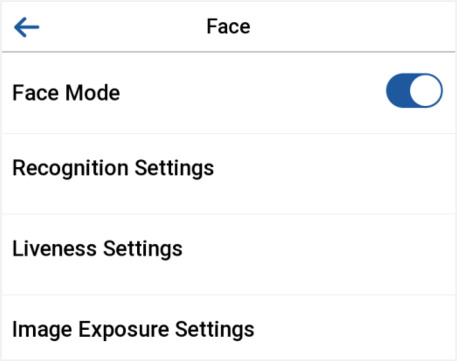
Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: No Photo: No photo is taken during user verification. Take photo, no save: Photo is taken but not saved during verification. Take photo and save: All the photos taken during verification is saved. Save on successful verification: Photo is taken and saved for each successful verification. Save on failed verification: Photo is taken and saved only for each failed verification.
Display User Photo	This function is disabled by default. When enabled, a security prompt will pop-up.
Attendance Log Alert	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Periodic Del of T&A Data	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

6.4 Face Parameters

Tap **Face** on the **System** interface.



Menu	Description
Face Mode	Whether to enable face function, when disable, the face feature is hidden and facial registration is not supported, nor is facial recognition (even if the person has previously registered a face).
Recognition Settings	**1: N Threshold:** Used to compare the similarity between the collected facial images and all registered facial templates in the device, with higher values being more stringent. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and higher is the rejection rate, and vice versa. It is recommended to set the default value of 88.
	1:1 Threshold: Used to verify whether the current face is consistent with the face template bound to the input user ID or other personal identifiers (such as card numbers). The higher the value, the higher the requirement for similarity and the stronger the security, but the user experience may be slightly affected.

Copyright © 2025 ARMATURA LLC. All rights reserved.

	The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher is the rejection rate, and vice versa. It is recommended to set the default value of 88.	
	Minimum Face Size: The minimum face size is used to limit the face size recognized by the device, thereby eliminating background interference or misjudgment. This parameter is usually related to the distance from the camera to the 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 of distance of faces. When the value is 0, the face comparison distance is not limited.	
	Occlusion ratio: It is the proportion of the obscured part of the face to the whole face, if the value is big, more obscured can pass the live detection, if the value is small, there may be a big beard these people can't pass the live. It is a parameter used for anti-counterfeiting, such as taking photos and real people together to deceive the anti-counterfeiting detection.	
	Recognition Interval(s): After the interval identifying is clicked (selected), for example, if the comparison 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.	
	Identifying Mode	**Tracking Identification:** The same face can only be recognized once. To recognize it again, you must leave the face recognition area and re-enter it before it can be recognized again.
		Multi-face Identifying: When it is toggled on, the device can identify multiple faces at once. The Content Mode to Display, and Count to Display can be configured only if it is toggled on.
		Content Mode to Display: You can select the content displayed below the user photo in the interface after the face verification is successful. Such as display the User ID, Name, User ID + Name, Timestamp, User ID + Timestamp, Name + Timestamp, User ID.
		Count to Display: You can choose the number of face verification results to be displayed in the interface at once, e.g., if set to 3, the interface displays up to 3 successful user verifications at once. *Note:* The Count to Display can be set from 1 to 4 users.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Liveness Settings	**Single-lens Liveness:** It uses visible light images to detect spoofing attempts and assess whether the biometric source sample provided is of a real person (a live human being) or a false representation. **Single-lens Liveness Threshold:** It facilitates judging whether the captured visible image is of a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light. **Dual-lens Liveness:** It uses near-infrared spectra imaging to identify and prevent fake photos and video attacks. **Dual-lens Liveness Threshold:** It is convenient to judge whether the near-infrared spectral imaging is a fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging. *Note:* Single-lens Liveness and Dual-lens Liveness are mutually exclusive options. Enabling Single-lens Liveness will automatically disable Dual-lens Liveness, and vice versa. When the option is turned on or off, the device reboots automatically to execute the function.
Image Exposure Settings	**Face AE:** Face Auto Exposure, 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. **WDR:** Wide Dynamic Range (WDR) balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments. **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.

Note:

1. Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.
2. Face AE and Multi-face Identifying are mutually exclusive options. Enabling Multi-face Identifying will automatically disable Face AE, and vice versa.
3. Recognition Interval and Tracking Identification are mutually exclusive options. Enabling Tracking Identification will automatically disable Recognition Interval, and vice versa.

Process to modify the Facial Recognition Accuracy

- On the **System** interface, tap on **Face** > **Liveness Settings** and then toggle to enable Single-lens Liveness or Dual-lens Liveness to set the liveness settings.
- Then, on the **Main Menu**, tap **Autotest** > **Test Camera** and perform the face test.
- Tap three times for the scores on the left upper corner of the screen, and the red rectangular

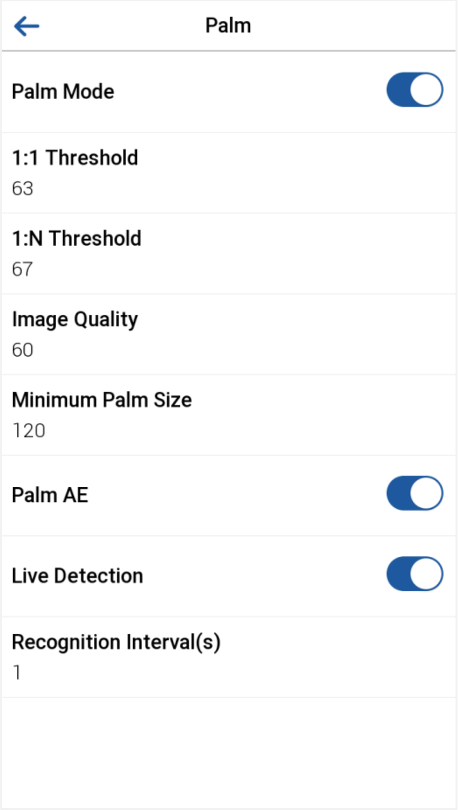
Copyright © 2025 ARMATURA LLC. All rights reserved.

box appears to start adjusting the mode.

- Keep one arm distance between the device and the face. It is recommended not to move the face in a wide range.

6.5 Palm Parameters

Tap **Palm Parameter** on the **System** interface.



Palm

Palm Mode: on

1:1 Threshold: 63

1:N Threshold: 67

Image Quality: 60

Minimum Palm Size: 120

Palm AE: on

Live Detection: on

Recognition Interval(s): 1

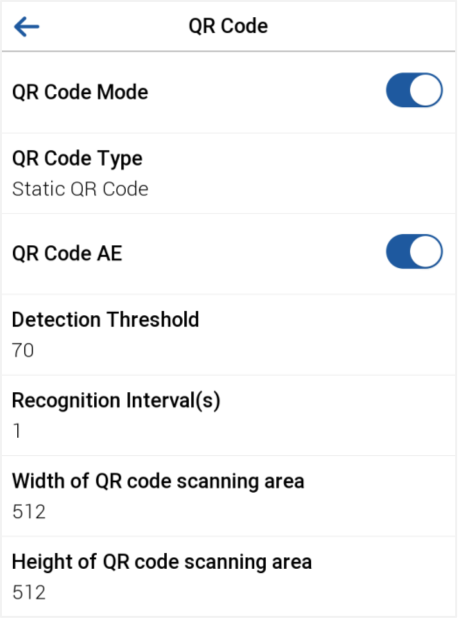
Menu	Description
Palm Mode	Whether to enable palm function, when disable, the palm feature is hidden and palm registration is not supported, nor is palm recognition (even if the person has previously registered the palm).
1:1 Threshold	Used to verify whether the current palm is consistent with the palm template bound to the input user ID or other personal identification (such as card number). The higher the value, the higher the requirement for similarity and the stronger the security, but the user experience may be slightly affected.
1:N Threshold	Used to compare the similarity between the collected palm images and all registered palm templates in the device, with higher values being more stringent.
Image Quality	Image quality for palm registration and comparison. The higher the value, the clearer the image requires.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Minimum Palm Size	The minimum palm size is used to limit the palm size recognized by the device, thereby eliminating background interference or misjudgment. This parameter is usually related to the distance from the camera to the palm. This value can be understood as the palm comparison distance. The farther the person is, the smaller the palm is, and the smaller the palm pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of palms. When the value is 0, the palm comparison distance is not limited.
Palm AE	Palm Auto Exposure, 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.
Liveness 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.
Recognition Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison 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.

6.6 QR Code

Tap **QR Code** on the **System** interface.



QR Code

QR Code Mode

QR Code Type
Static QR Code

QR Code AE

Detection Threshold
70

Recognition Interval(s)
1

Width of QR code scanning area
512

Height of QR code scanning area
512

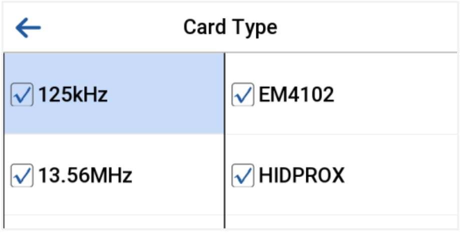
Menu	Description
QR Code Mode	Whether to enable QR Code function, when disable, the QR Code feature is hidden and QR Code registration is not supported, nor is QR Code recognition (even if the person has previously registered the QR Code).

Copyright © 2025 ARMATURA LLC. All rights reserved.

QR Code Type	Select the mode of QR Code. Static and Dynamic are supported.
QR Code AE	When the QR code is in front of the camera, the brightness of the QR code area increases, while other areas become darker.
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.
Recognition Interval(s)	After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the QR Code recognition will verify the QE Code every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals.
Width of QR code scanning area	Adjust the width of the QR code scanning area of the device, valid values are 50 to 720, default value is 512.
Height of QR code scanning area	Adjust the height of the QR code scanning area of the device, valid values are 50 to 1280, default value is 512.

6.7 Card Management

Tap **Card Management** on the **System** interface.


Card Type

☑ 125kHz | ☑ EM4102

☑ 13.56MHz | ☑ HIDPROX

- During card management, the main menu card type will be displayed on the left and its sub-menus will be listed on the right.
- First tap on the required card type, and then select its required sub-menus from the list.

Best plug'n play and high-performance full NFC solution, a full NFC controller solution with integrated firmware and NCI interface designed for contactless communication at 13.56 MHz. It is compatible with NFC forum requirements.

Designed based on learnings from previous NXP NFC device generation. It is the ideal solution for rapidly integrating NFC technology in any application, especially those running O/S environment like Linux and Android, reducing Bill of Material (BOM) size and cost, thanks to:

- Full NFC forum compliancy with small form factor antenna.
- Embedded NFC firmware providing all NFC protocols as pre-integrated feature.
- Direct connection to the main host or microcontroller, by I^{2}C-bus physical and NCI protocol.
- Ultra-low power consumption in polling loop mode.

Copyright © 2025 ARMATURA LLC. All rights reserved.

- Highly efficient integrated power management unit (PMU) allowing direct supply from a battery.

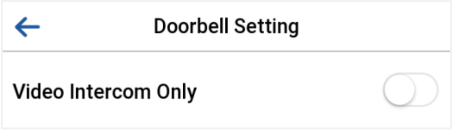
Embeds a new generation RF contactless front-end supporting various transmission modes according to NFCIP-1 and NFCIP-2, ISO/IEC 14443, ISO/IEC 15693, MIFARE Classic IC-based card and FeliCa card specifications. It embeds an ARM Cortex-MO microcontroller core loaded with the integrated firmware supporting the NCI 1.0 host communication. It also allows to provide a higher output power by supplying the transmitter output stage from 3.0 V to 4.75 V.

The contactless front-end design brings a major performance step-up with on one hand a higher sensitivity and on the other hand the capability to work in active load modulation communication enabling the support of small antenna form factor.

For contactless card functionality, the device can act autonomously if previously configured by the host in such a manner. Device integrated firmware provides an easy integration and validation cycle as all the NFC real-time constraints, protocols and device discovery (polling loop) are being taken care internally. In a few NCI commands, host SW can configure the device to notify for card or peer detection and start communicating with them.

6.8 Doorbell Setting

Tap **Doorbell Setting** on the **System** interface to set the doorbell.



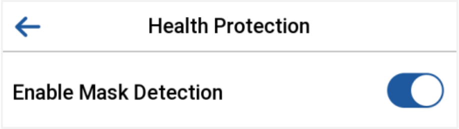
Doorbell Setting

Video Intercom Only ○

Menu	Description
Video Intercom Only	When enabled, the doorbell icon will be displayed in the standby interface, and video intercom will also appear in the main menu interface, which allows you to set the video intercom.

6.9 Health Protection

Tap **Health Protection** on the **System** interface to configure the health protection settings.



Health Protection

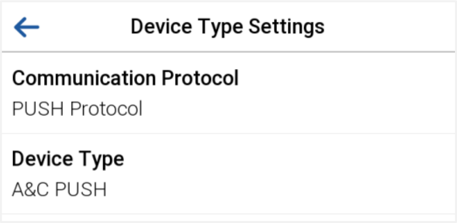
Enable Mask Detection ●

Copyright © 2025 ARMATURA LLC. All rights reserved.

Menu	Description
Enable Mask Detection	It enables or disables the mask detection function. When enabled, the device identifies whether the user is wearing a mask or not during verification.

6.10 Device Type Setting

Tap **Device Type Settings** on the **System** interface to configure the device type setting settings.



Communication Protocol
PUSH Protocol

Device Type
A&C PUSH

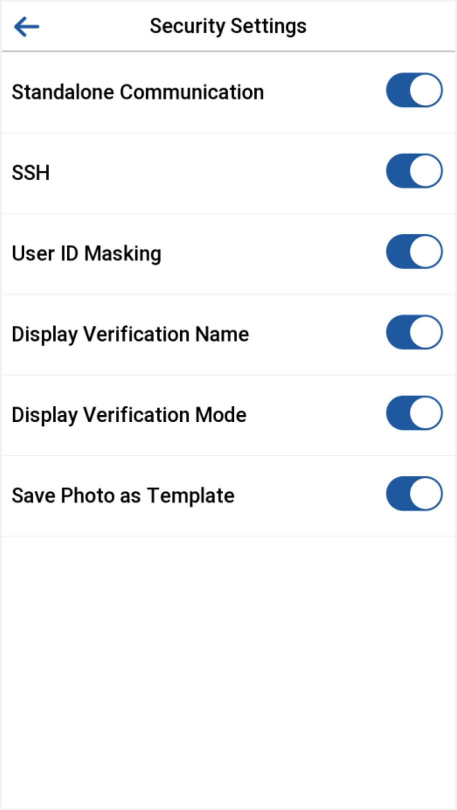
Menu	Description
Communication Protocol	Set the PUSH protocol.
Device Type	Set the device as an access control terminal or attendance terminal.

Note: After changing the device type, the device will delete all the data and restart, and some functions will be adjusted accordingly.

6.11 Security Settings

Tap **Security Settings** on the **System** interface.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Security Settings

Standalone Communication

SSH

User ID Masking

Display Verification Name

Display Verification Mode

Save Photo as Template

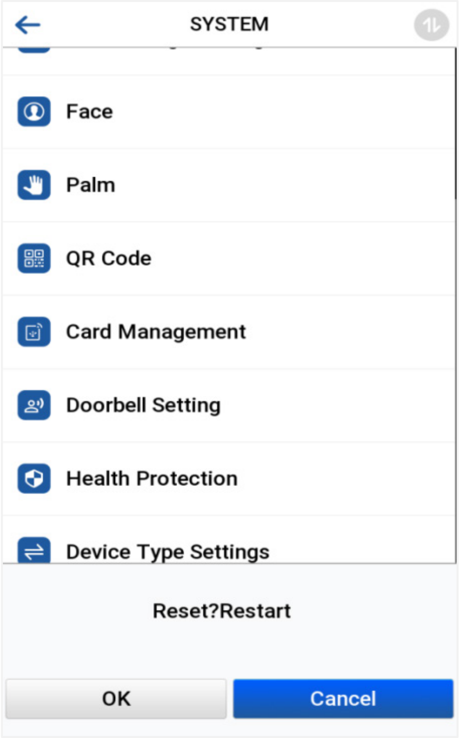
Function Name	Description
Standalone Communication	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.
SSH	The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation.
User ID Masking	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
Display Verification Name	After enabled, the user's name will be displayed after the personnel verification result. The verification result will not display the name when this option is disabled.
Display Verification Mode	After enabled, the personnel verification result will show the user's verification mode. The verification result will not display the mode when this option is disabled.
Save Photo as Template	After disable this function, face re-registration is required after an algorithm upgrade.

Copyright © 2025 ARMATURA LLC. All rights reserved.

6.12 Factory Reset

This option restores the device, such as communication settings and system settings, to factory settings (does not clear registered user data).

Tap **Reset** on the **System** interface.



Reset?Restart

Tap **OK** to reset.

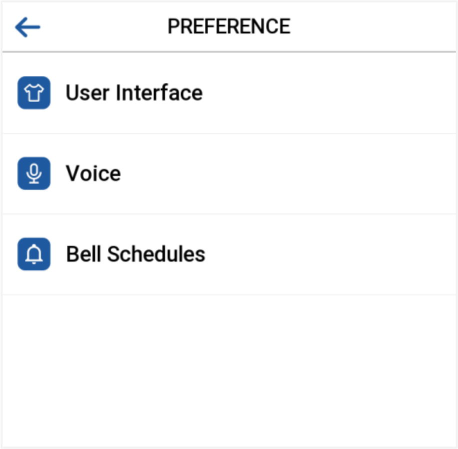
Copyright © 2025 ARMATURA LLC. All rights reserved.

7 Personalize Settings

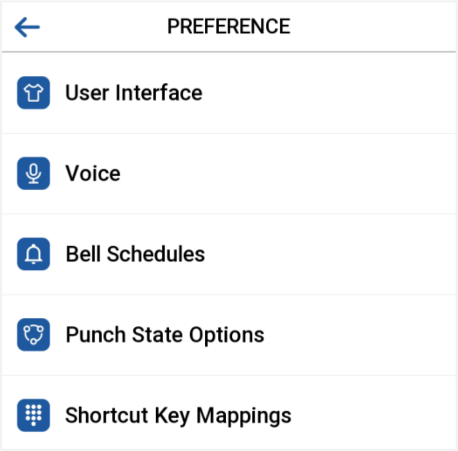
You may customize the interface settings, audio, and bell.

Tap **Personalize** on the main menu interface.

Access Control Terminal:



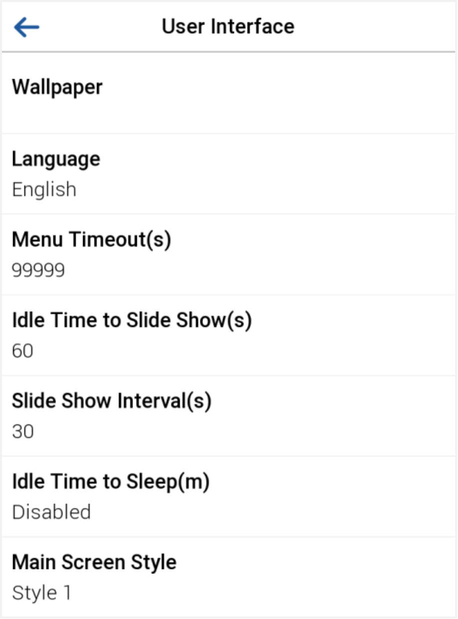
Time Attendance Terminal:



7.1 Interface Settings

You can customize the display style of the main interface.

Tap **User Interface** on the Personalize interface.



User Interface

Wallpaper

Language
English

Menu Timeout(s)
99999

Idle Time to Slide Show(s)
60

Slide Show Interval(s)
30

Idle Time to Sleep(m)
Disabled

Main Screen Style
Style 1

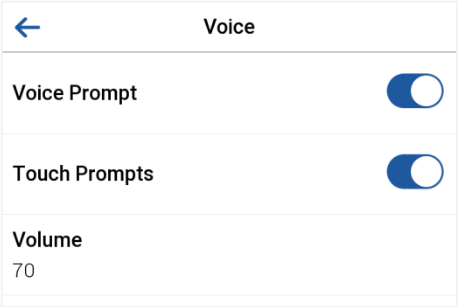
Menu	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	To select the language of the device.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Menu Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.
Idle Time to Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. It can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	This refers to the time interval switching different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time To Sleep (m)	If you have activated the sleep mode, when there is no operation, the device will enter the standby mode. You can disable this function or set a value within 1-999 minutes.
Main Screen Style	To select the main screen style according to your personal preference.

7.2 Voice Settings

Tap **Voice** on the Personalize interface.


Voice

Voice Prompt

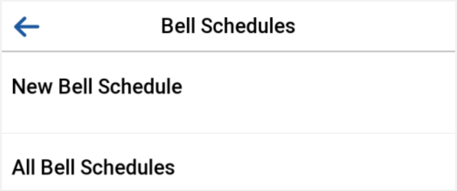
Touch Prompts

Volume
70

Menu	Description
Voice Prompt	Select whether to enable voice prompts during operation.
Touch Prompts	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0 to 100.

7.3 Bell Schedules

Tap **Bell Schedules** on the Personalize interface.


Bell Schedules

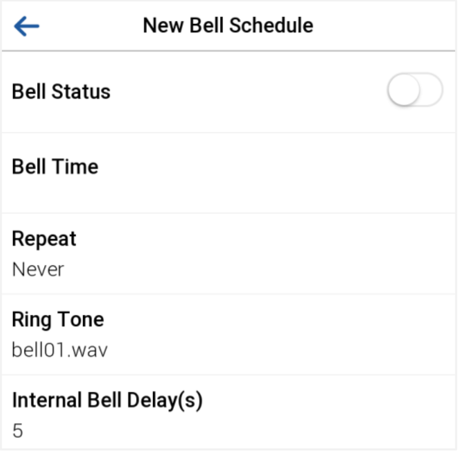
New Bell Schedule

All Bell Schedules

Copyright © 2025 ARMATURA LLC. All rights reserved.

Add a Bell

1. Tap **New Bell Schedule** to enter the adding interface:



New Bell Schedule

Bell Status

Bell Time

Repeat
Never

Ring Tone
bell01.wav

Internal Bell Delay(s)
5

Menu	Description
Bell Status	Set whether to enable the bell status.
Bell Time	At this time of day, the device automatically rings the bell.
Repeat	Set the repetition cycle of the bell.
Ring Tone	Select a ring tone.
Internal Bell Delay (s)	Set the duration of the internal bell. Valid values range from 1 to 999 seconds.

2. Back to the Bell Schedules interface; tap **All Bell Schedules** to view the newly added bell.

Edit a Bell

On the All Bell Schedules interface, tap the bell to be edited.

Tap **Edit**, the editing method is the same as the operations of adding a bell.

Delete a Bell

On the All Bell Schedules interface, tap the bell to be deleted.

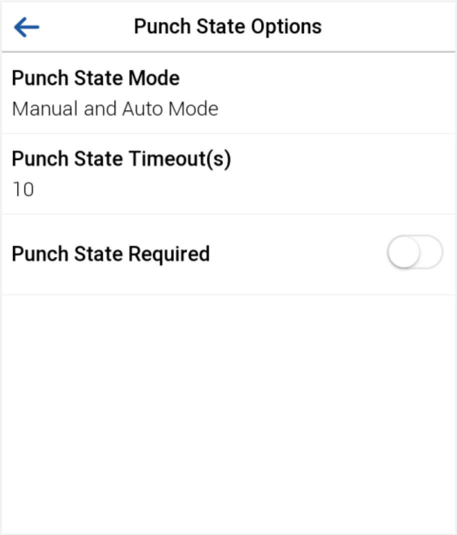
Tap **Delete** and select **Yes** to delete the bell.

7.4 Punch States Options

Tap **Punch States Options** on the **Personalize** interface to configure the punch state settings.

Note: This function only for Time Attendance Terminal.

Copyright © 2025 ARMATURA LLC. All rights reserved.

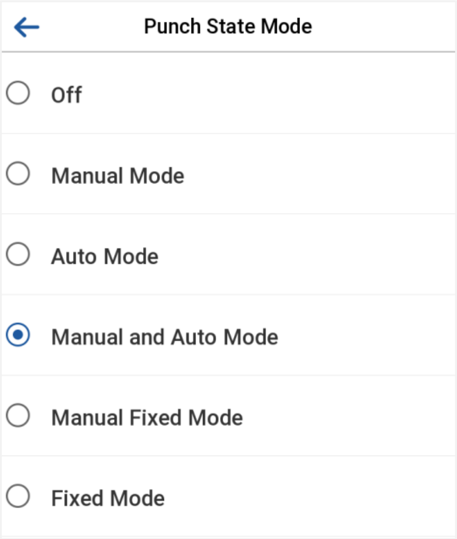


Punch State Options

Punch State Mode
Manual and Auto Mode

Punch State Timeout(s)
10

Punch State Required



Punch State Mode

○ Off

○ Manual Mode

○ Auto Mode

● Manual and Auto Mode

○ Manual Fixed Mode

○ Fixed Mode

Menu	Description
Punch State Mode	Off: Disable the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will become invalid. Manual Mode: Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout. Auto Mode: The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings. Manual and Auto Mode: The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key. Manual Fixed Mode: After the punch state key is set manually to a particular punch status, the function will remain unchanged until it is being manually switched again. Fixed Mode: Only the manually fixed punch state key will be shown. Users cannot change the status by tapping any other keys.
Punch State Timeout(s)	It is the amount of time for which the punch state is displayed. The value ranges from 5~999 seconds.
Punch State Required	To choose whether an attendance state needs to be selected during verification.

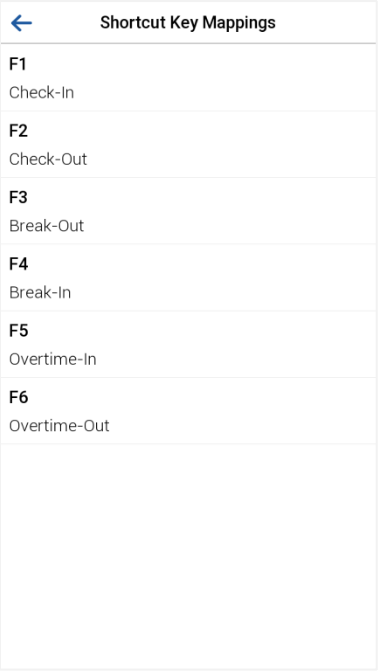
Copyright © 2025 ARMATURA LLC. All rights reserved.

7.5 Shortcut Key Mappings

Users may define shortcut keys for attendance status and for functional keys which will be defined on the main interface. So, on the main interface, when the shortcut keys are taped, the corresponding attendance status or the function interface will be displayed directly.

Note: This function only for Time Attendance Terminal.

Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



Shortcut Key Mappings

F1
Check-In

F2
Check-Out

F3
Break-Out

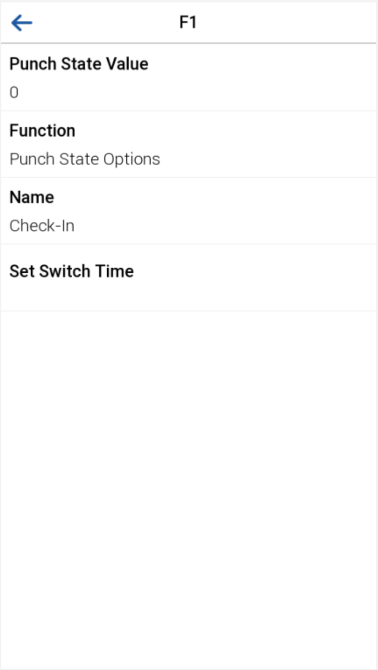
F4
Break-In

F5
Overtime-In

F6
Overtime-Out

- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key** (that is "F1") interface, tap **Function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key is defined as a function key (such as New user, All users, etc.), the configuration is completed as shown in the image below.

Copyright © 2025 ARMATURA LLC. All rights reserved.

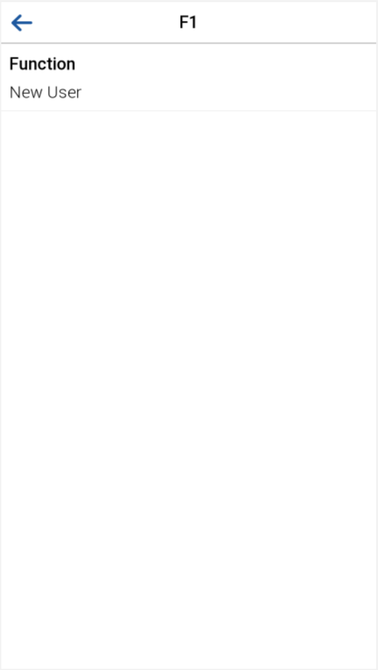


Punch State Value
0

Function
Punch State Options

Name
Check-In

Set Switch Time



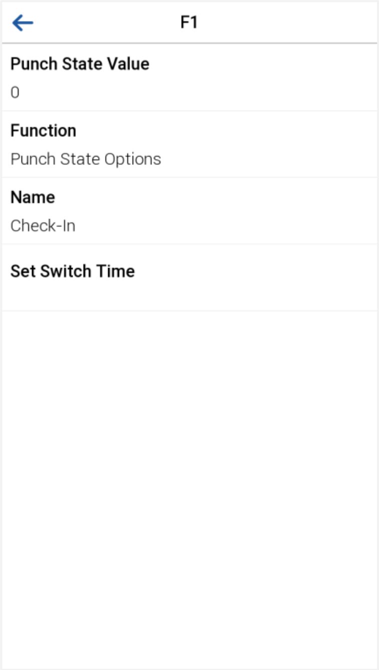
Function
New User

- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0~250), name.

Set the switch time

- The switch time is set in accordance with the punch state options.
- When the **Punch State Mode** is set to **Auto Mode**, the switch time should be set.
- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday, etc.) as shown in the image below.

Copyright © 2025 ARMATURA LLC. All rights reserved.



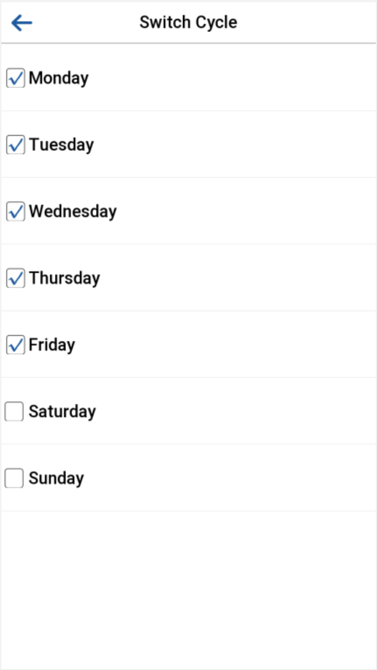
F1

Punch State Value
0

Function
Punch State Options

Name
Check-In

Set Switch Time



Switch Cycle

☑ Monday

☑ Tuesday

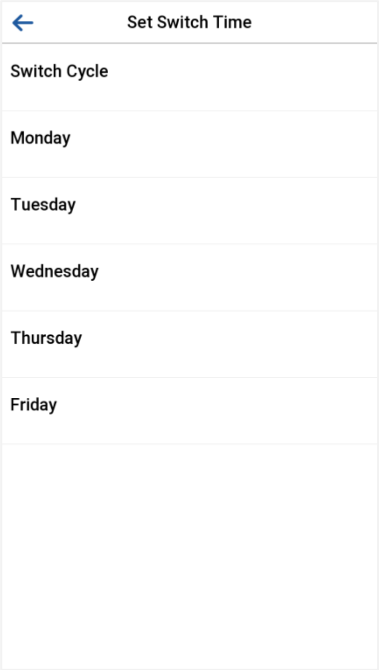
☑ Wednesday

☑ Thursday

☑ Friday

☐ Saturday

☐ Sunday



Set Switch Time

Switch Cycle

Monday

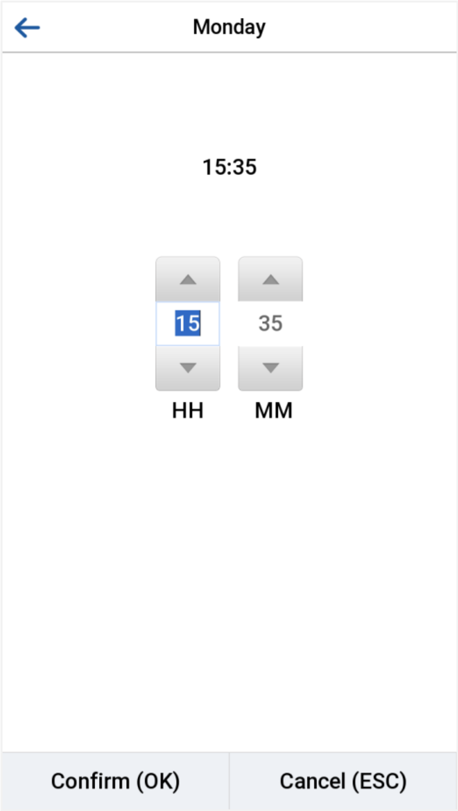
Tuesday

Wednesday

Thursday

Friday

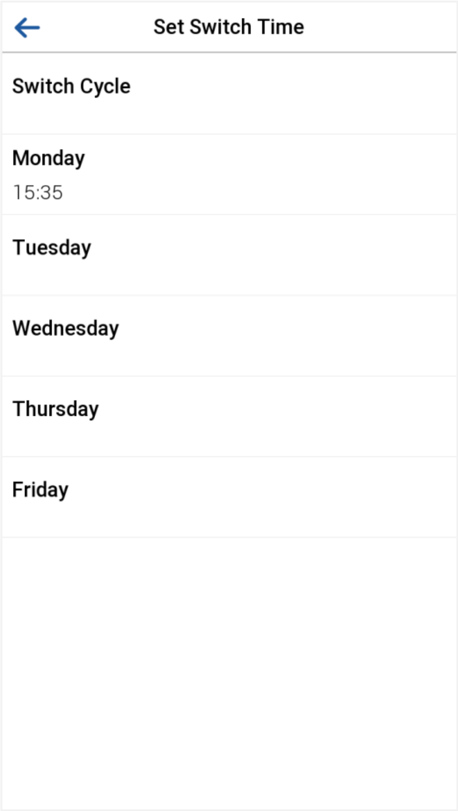
- Once the Switch cycle is selected, set the switch time for each day, and tap OK to confirm, as shown in the image below.



Monday

15:35

HH: 15
MM: 35



Set Switch Time

Switch Cycle

Monday
15:35

Tuesday

Wednesday

Thursday

Friday

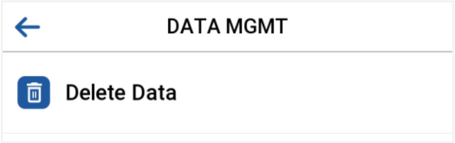
Note: When the function is set to Undefined, the device will not enable the punch state key.

Copyright © 2025 ARMATURA LLC. All rights reserved.

8 Data Management

The Data Management is used to delete the relevant data in the device.

Tap **Data Mgt.** on the main menu interface.

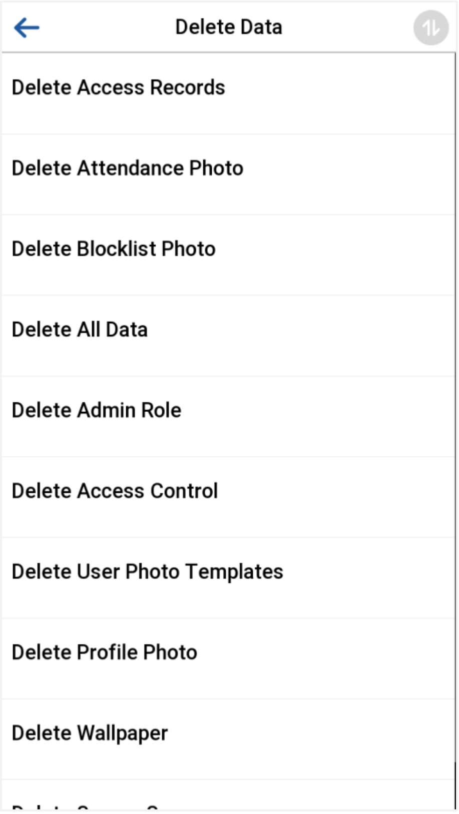


DATA MGMT

Delete Data

8.1 Delete Data

Tap **Delete Data** on the Data Mgt. interface.



Delete Data

Delete Access Records

Delete Attendance Photo

Delete Blocklist Photo

Delete All Data

Delete Admin Role

Delete Access Control

Delete User Photo Templates

Delete Profile Photo

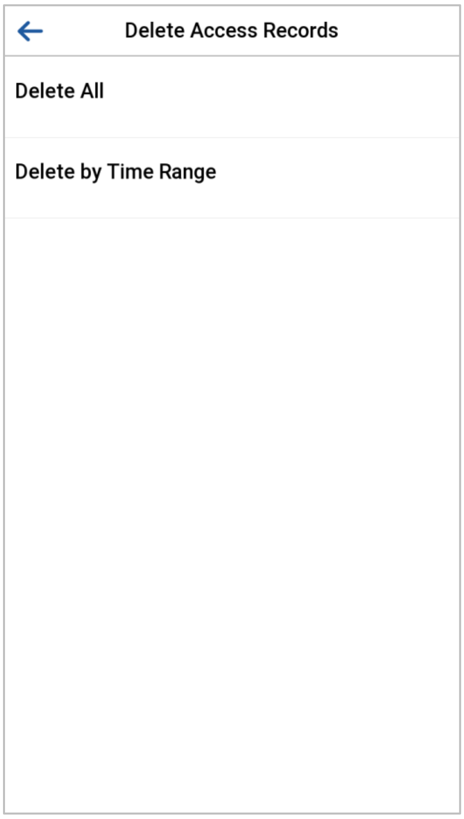
Delete Wallpaper

Function Name	Description
Delete Access Records/Delete Attendance Data	To delete attendance data/access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete information and attendance logs/access records of all registered users.

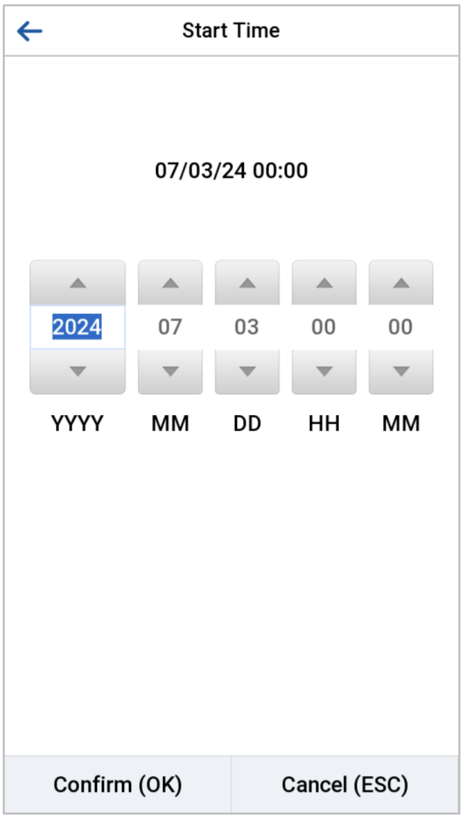
Copyright © 2025 ARMATURA LLC. All rights reserved.

Delete Admin Role	To remove all administrator privileges.
Delete Access Control	To delete all access data.
Delete User Photo Templates	To delete user photo templates in the device. When deleting template photos, there is a risk reminder: "Face re-registration is required after an algorithm upgrade."
Delete Profile Photo	To delete all user photos on the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.

The user may select Delete All or Delete by Time Range when deleting the access records, attendance photos or block listed photos. Selecting Delete by Time Range, you need to set a specific time range to delete all data within a specific period.



Select Delete by Time Range



Set the time range and tap OK

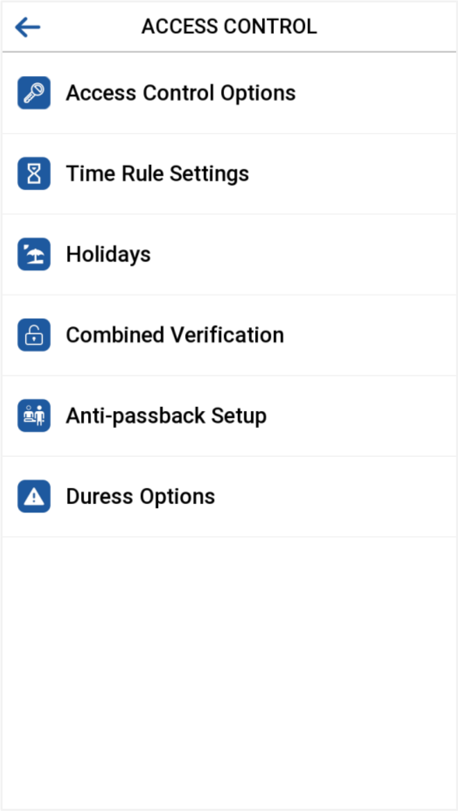
Copyright © 2025 ARMATURA LLC. All rights reserved.

9 Access Control

Access Control is used to set the schedule of a door opening, locks control and other parameter settings related to access control.

Tap Access Control on the main menu interface.

Access Control Terminal:


ACCESS CONTROL

Access Control Options

Time Rule Settings

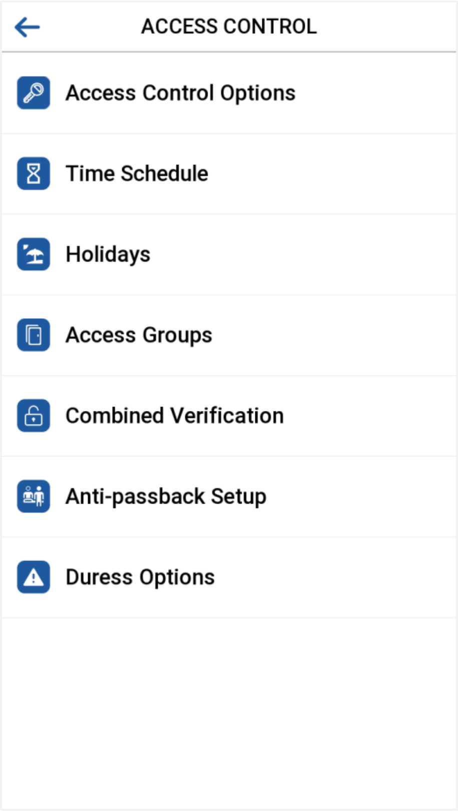
Holidays

Combined Verification

Anti-passback Setup

Duress Options

Time Attendance Terminal:


ACCESS CONTROL

Access Control Options

Time Schedule

Holidays

Access Groups

Combined Verification

Anti-passback Setup

Duress Options

To gain access, the registered user must meet the following conditions:

1. The current door unlock time should be within any valid time zone of the user time period.
2. The user's group must be in the door unlock combination (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).

In default settings, new users are allocated into the first group with the default group time zone and access combo as "1" and set in an unlocking state.

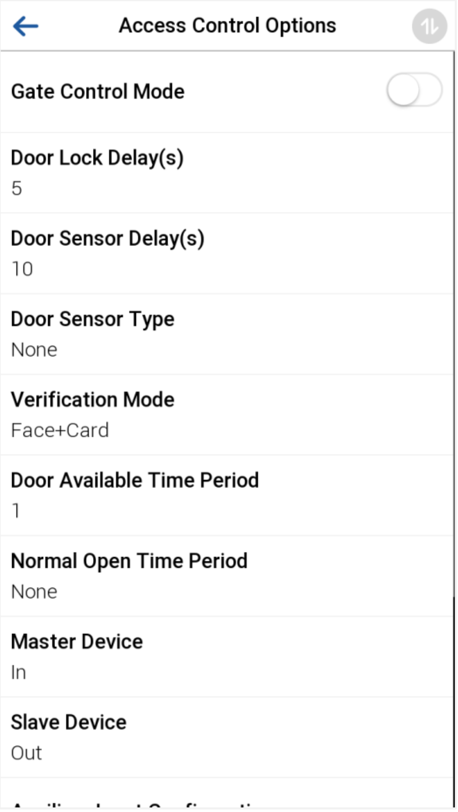
Copyright © 2025 ARMATURA LLC. All rights reserved.

9.1 Access Control Options

This option is used to set the parameters of the control lock of the device and the related parameters.

Tap **Access Control Options** on the Access Control interface.

Access Control Terminal:



Access Control Options

Gate Control Mode ○

Door Lock Delay(s)
5

Door Sensor Delay(s)
10

Door Sensor Type
None

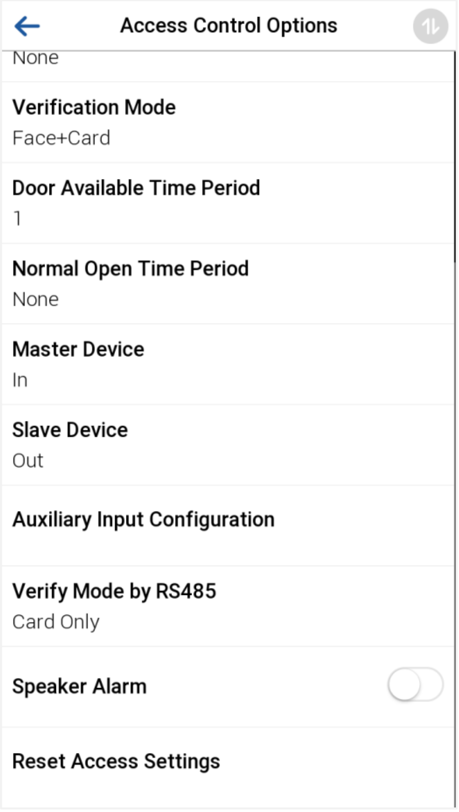
Verification Mode
Face+Card

Door Available Time Period
1

Normal Open Time Period
None

Master Device
In

Slave Device
Out



Access Control Options

None

Verification Mode
Face+Card

Door Available Time Period
1

Normal Open Time Period
None

Master Device
In

Slave Device
Out

Auxiliary Input Configuration

Verify Mode by RS485
Card Only

Speaker Alarm ○

Reset Access Settings

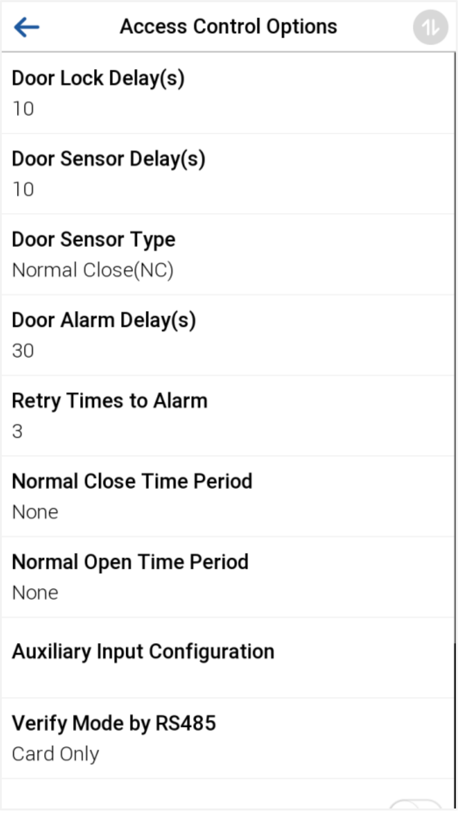
Function Name	Description
Gate Control Mode	It toggles between **ON** or **OFF** switch to get into gate control mode or not. When set to **ON**, the interface removes the Door lock relay, Door sensor relay, and Door sensor type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1 to 99 seconds; 0 seconds represents disabling the function.
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.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Door Sensor Type	There are three Sensor types: **None, Normal Open,** and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open(NO):** It means the door is always left open when electric power is on. **Normally Closed(NC):** It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Password/Card/Face/Palm, User ID Only, Password, Card Only, Password + Card, Password/Card, Face Only, Face + Password, Face + Card, Palm, Palm + Card and Palm + Face.
Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
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.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify Mode by RS485	The verification mode is used when the device is used either as a host or secondary. The supported verification mode includes Card only, and Card + Password.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, alarm and so on. However, erased access control data in Data Mgt. is excluded.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Time Attendance Terminal:



Door Lock Delay(s)
10

Door Sensor Delay(s)
10

Door Sensor Type
Normal Close(NC)

Door Alarm Delay(s)
30

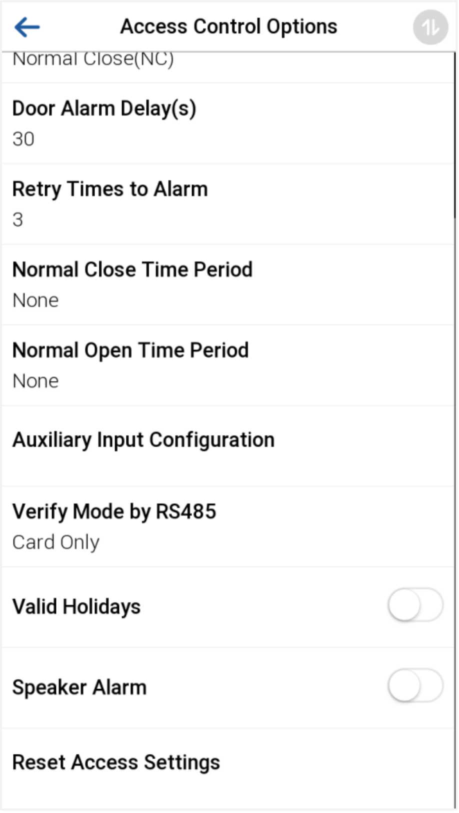
Retry Times to Alarm
3

Normal Close Time Period
None

Normal Open Time Period
None

Auxiliary Input Configuration

Verify Mode by RS485
Card Only



Normal Close(NC)

Door Alarm Delay(s)
30

Retry Times to Alarm
3

Normal Close Time Period
None

Normal Open Time Period
None

Auxiliary Input Configuration

Verify Mode by RS485
Card Only

Valid Holidays ○

Speaker Alarm ○

Reset Access Settings

Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1 to 10 seconds; 0 seconds represents disabling the function.
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 Closed. None: It means the door sensor is not in use. Normally Open(NO): It means the door is always left open when electric power is on. Normally Closed(NC): It means the door is always left closed when electric power is on.
Door Alarm Delay (s)	When the state of the door sensor is inconsistent with the door sensor type, an alarm will be triggered after a specified time period, i.e. the Door Alarm Delay. The valid value ranges from 1 to 999 seconds.
Retry Times To Alarm	When the number of failed verification reaches the set value (value ranges from 1 to 9 times), an alarm will be triggered. If the set value is None, the alarm will not be triggered after failed verification.
Normal Close Time Period	To set time period for Normally Closed mode, so that no one can access during this period.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Normal Open Time Period	To set time period for Normally Open, so that the door is always unlocked during this period.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify Mode by RS485	The verification mode is used when the device is used either as a primary or secondary. The supported verification mode includes Card only, and Card + Password.
Valid Holidays	To set if **Normal Close Time Period** or **Normal Open Time Period** settings are valid in set holiday time period. Choose [**ON**] to enable the set **Normal Close** or **Normal Open** time period in holiday.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, alarm and so on. However, erased access control data in Data Mgt. is excluded.

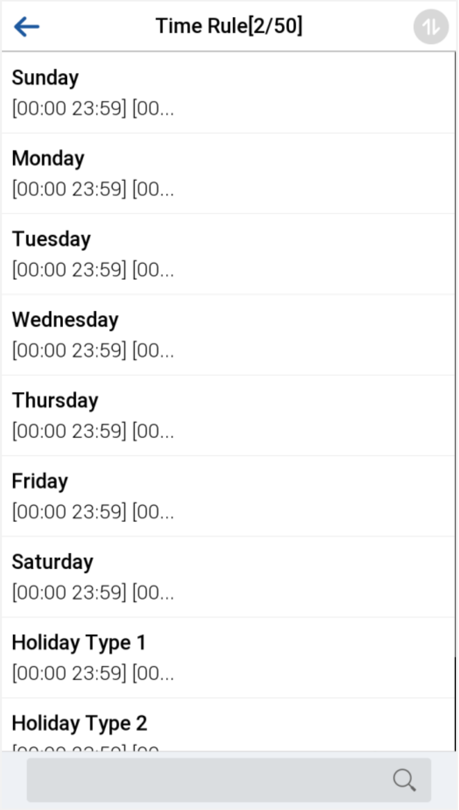
9.2 Time Rule Settings/Time Schedule

Tap **Time Rule Setting/Time Schedule** on the Access Control interface to configure the time settings.

- The entire system can define up to 50 Time Rules.
- Each time-period represents **10** Time Zones, i.e., **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time-period.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time-periods is "**OR**". Thus, when the verification time falls in any one of these time-periods, the verification is valid.
- The Time Zone format of each time-period is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

Tap the grey box to search the required Time Rule and specify the required Time Rule number (maximum up to 50 rules).

Copyright © 2025 ARMATURA LLC. All rights reserved.



Time Rule[2/50]

Sunday
[00:00 23:59] [00...

Monday
[00:00 23:59] [00...

Tuesday
[00:00 23:59] [00...

Wednesday
[00:00 23:59] [00...

Thursday
[00:00 23:59] [00...

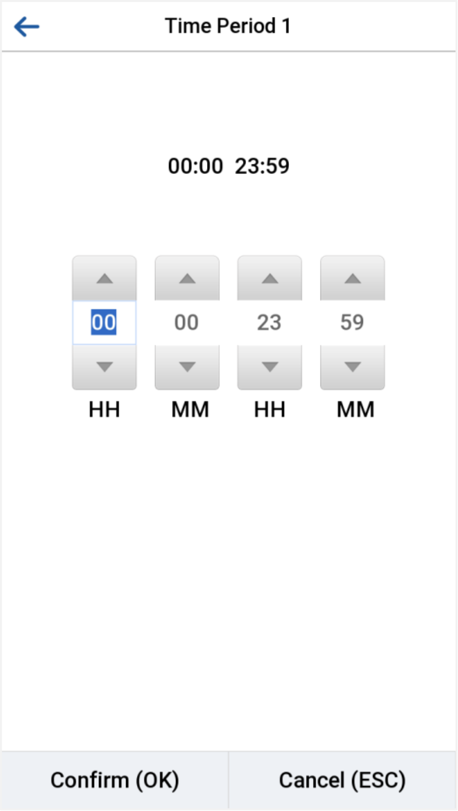
Friday
[00:00 23:59] [00...

Saturday
[00:00 23:59] [00...

Holiday Type 1
[00:00 23:59] [00...

Holiday Type 2

On the selected Time Rule number interface, tap on the required day (that is Monday, Tuesday, etc.) to set the time.



Time Period 1

00:00 23:59

HH	MM	HH	MM
00	00	23	59

Specify the start and the end time, and then tap OK.

Copyright © 2025 ARMATURA LLC. All rights reserved.

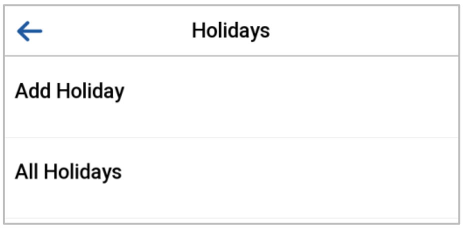
Note:

1. The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as 23:57~23:56).
2. It is the time interval for valid access when the End Time occurs after the Start Time (such as 08:00~23:59).
3. The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is 00:00 and End Time is 23:59).
4. The default Time Rule 1 indicates that the door is open all day long.

9.3 Holiday Settings

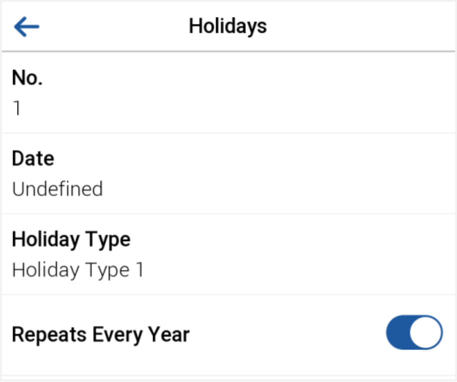
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which applies to all the employees, and the user will be able to open the door during the holidays.

Tap **Holidays** on the Access Control interface.



Add a New Holiday

Tap **Add Holiday** on the Holidays interface and set the holiday parameters.



No.
1

Date
Undefined

Holiday Type
Holiday Type 1

Repeats Every Year

Edit a Holiday

On the Holidays interface, select a holiday item to be modified. Tap **Edit** to modify holiday parameters.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Delete a Holiday

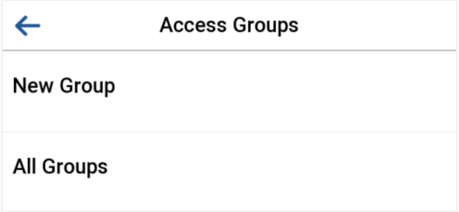
On the Holidays interface, select a holiday item to be deleted and tap **Delete**. Tap **OK** to confirm the deletion. After deletion, this holiday is no longer displayed on All Holidays interface.

9.4 Access Groups

Grouping is to manage users in groups, only for time attendance terminal.

The default time zone for group members is the group time zone, while users can set their personal time zone. When the group verification mode and the user verification mode overlap, the user verification mode takes priority. Each group can set a maximum of 3 time zones; as long as one of them is valid, the group can be successfully verified. The newly enrolled user is assigned to Access Group 1 by default, but can be assigned to another access group.

Tap **Access Groups** on the Access Control interface.

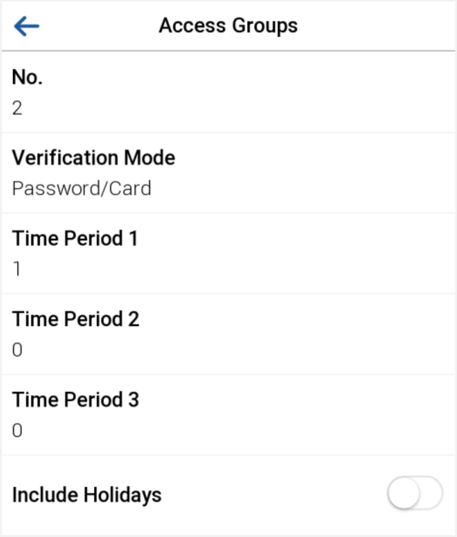

Access Groups

New Group

All Groups

Add a New Holiday

Tap **New Group** on the Access Group interface.


Access Groups

No.
2

Verification Mode
Password/Card

Time Period 1
1

Time Period 2
0

Time Period 3
0

Include Holidays ○

- The system has a default access group numbered 1, which cannot be deleted but can be modified.
- A number cannot be modified again after being set.
- When the holiday is set to be valid, the personnel in a group can open the door only when group time period overlaps with the holiday time period.

Copyright © 2025 ARMATURA LLC. All rights reserved.

- When the holiday is set to be invalid, the access control time of the personnel in this group is not affected by holidays.

Edit Group

On the **All Group** interface, tap to select the access group item to be modified. Tap **Edit** to modify group parameters.

Delete a Group

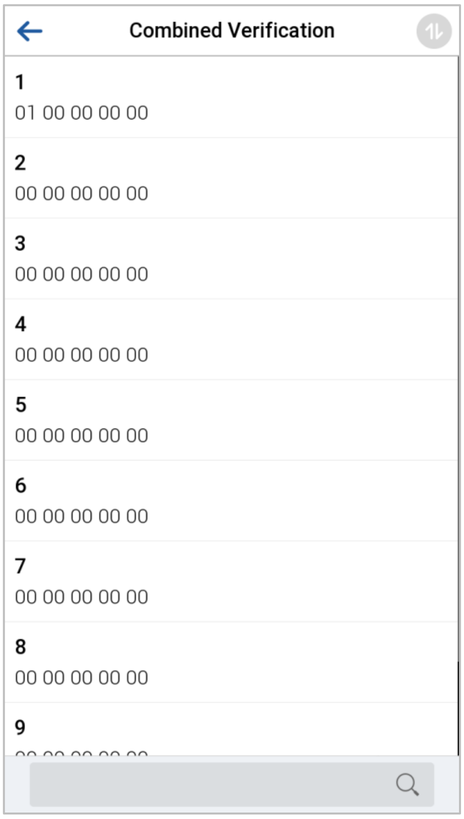
On the **All Group** interface, select a access group item to be deleted and tap **Delete**. After deletion, this group does not display on the **All Group** interface.

9.5 Combined Verification Settings

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen security.

In a door-unlocking combination, the range of the combined number N is 0 ⩽ N ⩽ 5, and the number of members N may all belong to one access group or may belong to five different access groups.

Tap **Combined Verification** on the Access Control interface.



Combined Verification

1
01 00 00 00 00

2
00 00 00 00 00

3
00 00 00 00 00

4
00 00 00 00 00

5
00 00 00 00 00

6
00 00 00 00 00

7
00 00 00 00 00

8
00 00 00 00 00

9

Tap the door-unlocking combination to be set. Tap the up and down arrows to input the combination number, then tap **OK**.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Examples:

- The **Door-unlocking combination 1** is set as (**01 03 05 06 08**), indicating that the unlocking combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, **Access Control Group 1** (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.
- The **Door-unlocking combination 2** is set as (**02 02 04 04 07**), indicating that the unlocking combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.
- The **Door-unlocking combination 3** is set as (**09 09 09 09 09**), indicating that there are 5 people in this combination; all of which are from AC group 9.
- The **Door-unlocking combination 4** is set as (**03 05 08 00 00**), indicating that the unlocking combination 4 consists of three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

Delete a Door-unlocking Combination

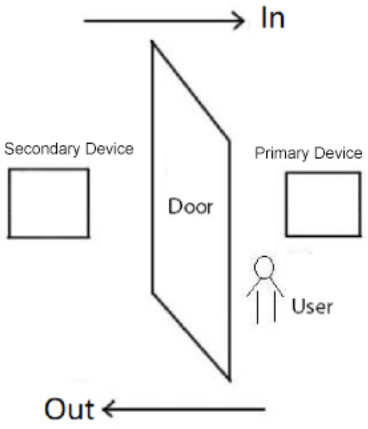
Set all the group numbers as 0 if you want to delete door-unlocking combinations.

9.6 Anti-passback Setup

A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent pattern.

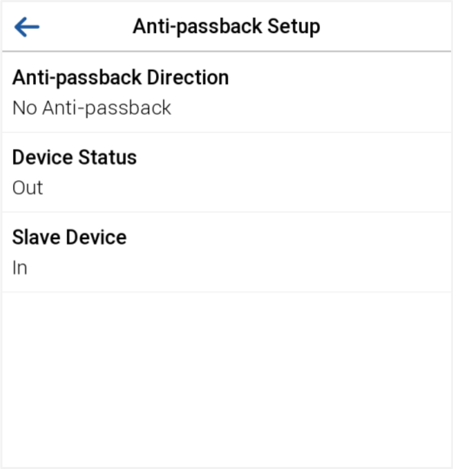
This function requires two devices to work together:

One device is installed on the indoor side of the door (primary device), and the other one is installed on the outdoor side of the door (the secondary device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID / Card Number) adopted by the primary device and secondary device must be consistent.



Tap **Anti-passback Setup** on the **Access Control** interface.

Copyright © 2025 ARMATURA LLC. All rights reserved.

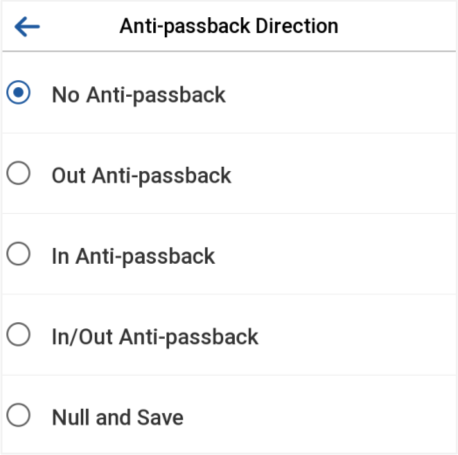


Anti-passback Setup

Anti-passback Direction
No Anti-passback

Device Status
Out

Slave Device
In



Anti-passback Direction

● No Anti-passback

○ Out Anti-passback

○ In Anti-passback

○ In/Out Anti-passback

○ Null and Save

Function Name	Description
Anti-passback Direction	**No Anti-passback:** The Anti-passback function is disabled, which means successful verification through either the primary device or secondary device can unlock the door. The attendance state is not saved in this option. **Out Anti-passback:** The user can check-out only if the last record is a check-in record otherwise an alarm is raised. However, the user can check-in freely. **In Anti-passback:** The user can check-in again only if the last record is a check-out record otherwise an alarm is raised. However, the user can check-out freely. **In/Out Anti-passback:** In this case, a user can check-in only if the last record is a check-out or the user can check-out only if the last record is a check-in otherwise the alarm is triggered.
Device Status	Set the device to in/out/none. **Note:** This function only for Time Attendance Terminal.
Slave Device	Set the slave device to in/out/none. **Note:** This function only for Time Attendance Terminal.

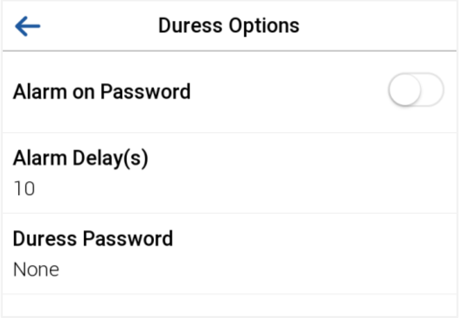
9.7 Duress Options Settings

If a user activated the duress verification function with specific authentication method(s), when he/she is under coercion during authentication with such method, the device will unlock the door as usual, but at the same time a signal will be sent to trigger the alarm.

Tap **Duress Options** on the Access Control interface.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Access Control Terminal:



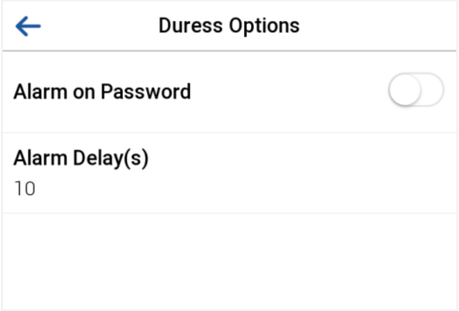
Duress Options

Alarm on Password ○

Alarm Delay(s)
10

Duress Password
None

Time Attendance Terminal:



Duress Options

Alarm on Password ○

Alarm Delay(s)
10

Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal is generated only when the password verification is successful otherwise there is no alarm signal.
Alarm Delay (s)	The alarm signal does not transmit until the alarm delay time elapses. The value ranges from 1 to 999 seconds.
Duress Password	Set the 6-digit duress password. When the user enters this duress password for verification, an alarm signal is generated.

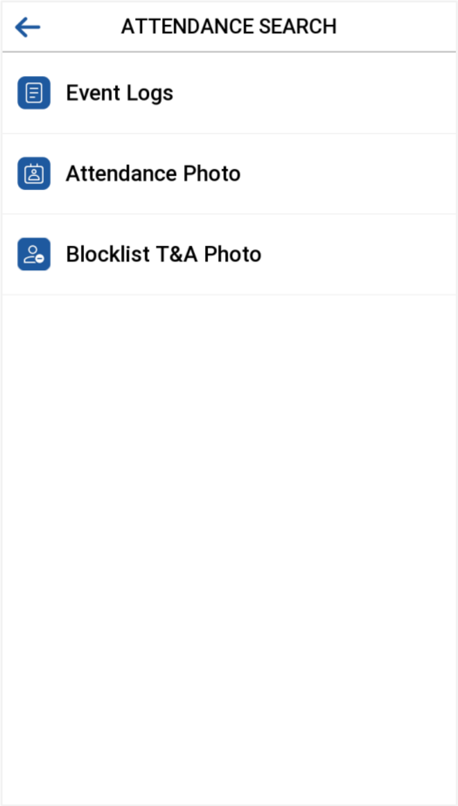
Copyright © 2025 ARMATURA LLC. All rights reserved.

10 Attendance Search

Once the identity of a user is verified, the access record is saved in the device. This function enables users to check their event logs.

Select **Attendance Search** on the **Main Menu** interface to search for the required event logs.

Access Control Terminal:



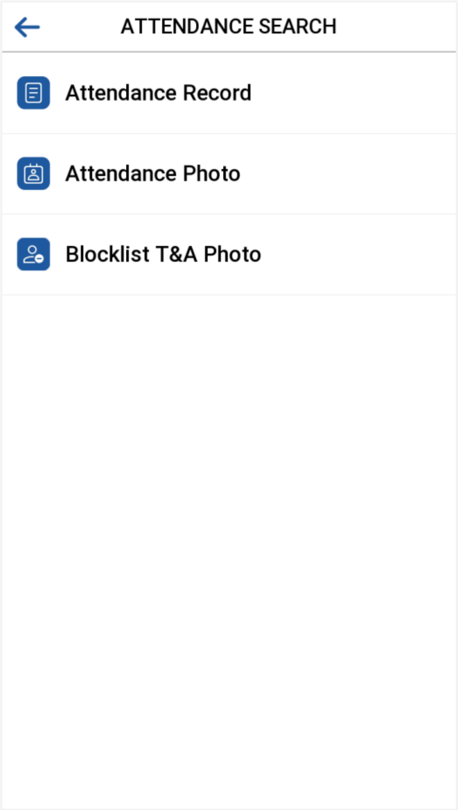
ATTENDANCE SEARCH

Event Logs

Attendance Photo

Blocklist T&A Photo

Time Attendance Terminal:



ATTENDANCE SEARCH

Attendance Record

Attendance Photo

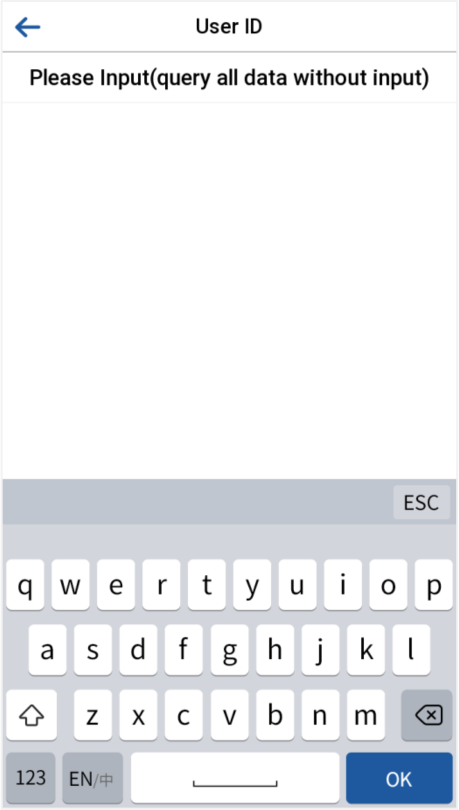
Blocklist T&A Photo

The process of searching for attendance and blocklist photos is similar to that of searching for event logs. The following is an example of searching for event logs.

On the **Attendance Search** interface, tap **Event Logs/Attendance Record** to search for the required record.

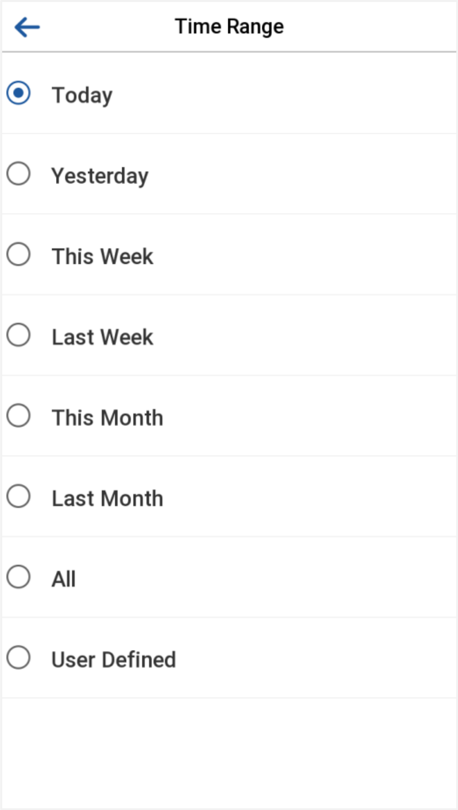
Copyright © 2025 ARMATURA LLC. All rights reserved.

1. Enter the user ID to be searched and tap OK. If you want to search for records of all users, tap OK without entering any user ID.


User ID

Please Input(query all data without input)

2. Select the time range in which the records you want to search for.


Time Range

● Today

○ Yesterday

○ This Week

○ Last Week

○ This Month

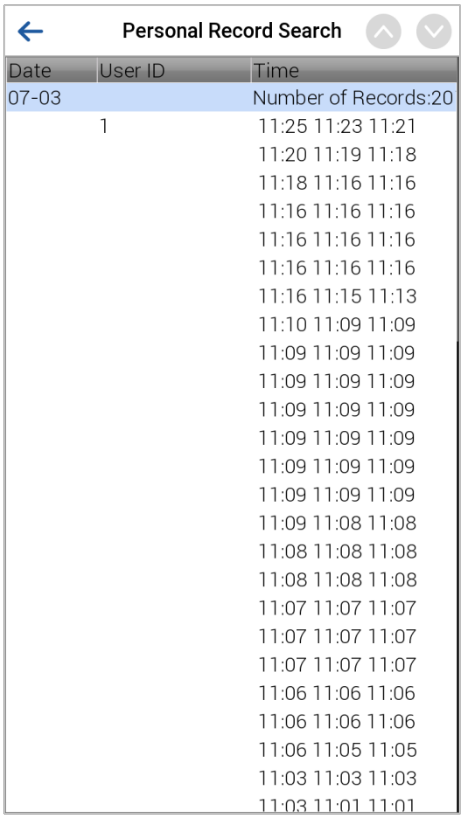
○ Last Month

○ All

○ User Defined

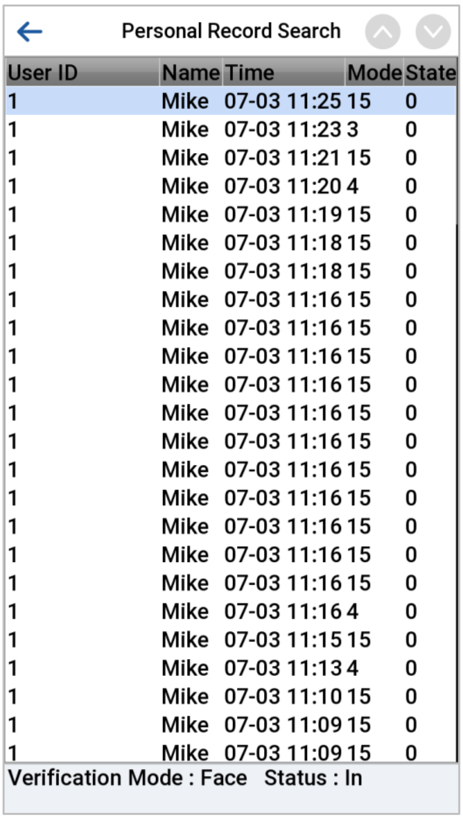
Copyright © 2025 ARMATURA LLC. All rights reserved.

3. The record search succeeds. Tap the record in green to view its details.



Date	User ID	Time
07-03		Number of Records:20
	1	11:25 11:23 11:21
		11:20 11:19 11:18
		11:18 11:16 11:16
		11:16 11:16 11:16
		11:16 11:16 11:16
		11:16 11:16 11:16
		11:16 11:15 11:13
		11:10 11:09 11:09
		11:09 11:09 11:09
		11:09 11:09 11:09
		11:09 11:09 11:09
		11:09 11:09 11:09
		11:09 11:09 11:09
		11:09 11:09 11:09
		11:09 11:08 11:08
		11:08 11:08 11:08
		11:08 11:08 11:08
		11:07 11:07 11:07
		11:07 11:07 11:07
		11:07 11:07 11:07
		11:06 11:06 11:06
		11:06 11:06 11:06
		11:06 11:05 11:05
		11:03 11:03 11:03
		11:03 11:01 11:01

4. The below figure shows the details of the selected record.



User ID	Name	Time	Mode	State
1	Mike	07-03 11:25	15	0
1	Mike	07-03 11:23	3	0
1	Mike	07-03 11:21	15	0
1	Mike	07-03 11:20	4	0
1	Mike	07-03 11:19	15	0
1	Mike	07-03 11:18	15	0
1	Mike	07-03 11:18	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	15	0
1	Mike	07-03 11:16	4	0
1	Mike	07-03 11:15	15	0
1	Mike	07-03 11:13	4	0
1	Mike	07-03 11:10	15	0
1	Mike	07-03 11:09	15	0
1	Mike	07-03 11:09	15	0

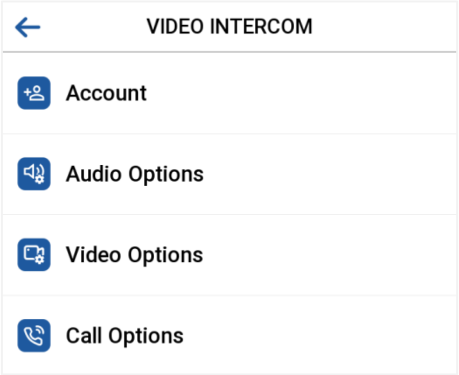
Verification Mode : Face   Status : In

Copyright © 2025 ARMATURA LLC. All rights reserved.

11 Video Intercom

Tap **Video Intercom** on the main menu interface to get into its menu options.

Note: This function needs to be enabled in **System** > **Doorbell Setting** > **Video Intercom Only**. And it needs to be used in conjunction with the Armatura One software. For more specific operations, please refer to 15 Video Intercom.



Function Name		Description
Account	SIP Server	Select whether to enable the SIP server. After enabling, it is necessary to set the server address, user name, verify ID, Password.
	Server Address	Enter the server address.
	User Name	Enter the username of server.
	Verify ID	Enter the verify ID of server.
	Password	Enter the password of server.
	Transport Protocol	Set the transport protocol between the device and indoor station.
	Verify TLS certificate	Select whether to enable the verify TLS certificate.
Audio Options	**Echo Cancellation:** Select whether to enable the echo cancellation. It is used to eliminate echoes caused by sound returning from the speaker to the microphone during a call. **Encoder:** Select the audio encoder for intercom. Both PCMU and PCMA provide better voice quality, but they take up more bandwidth, requiring 64kbps.	

Copyright © 2025 ARMATURA LLC. All rights reserved.

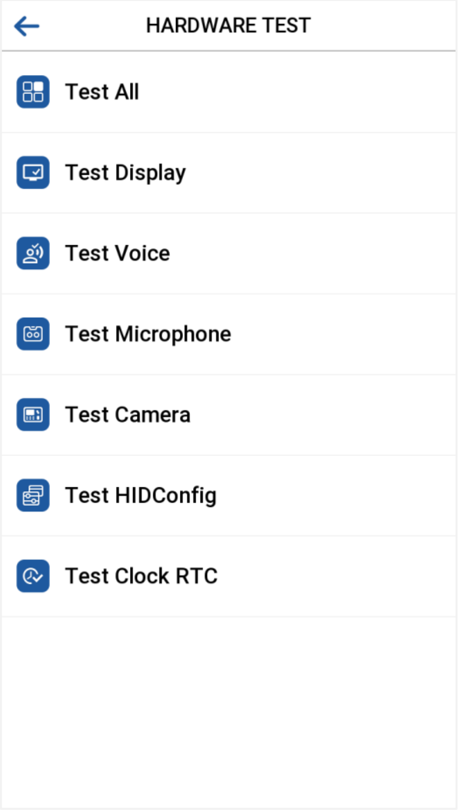
Video Options	**Video Resolution:** Select the video resolution of the intercom. **Video Frame Rate:** Refers to the number of frames per second of the intercom video display, the larger the value the smoother, the device defaults to 25Hz, does not support modification. **Video Code Stream:** Select the video code stream of the intercom, the larger the value, the higher the picture and sound quality of the video, and the greater the network requirements. **Encoder:** Whether to enable H264 Encoder.	
Call Options	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.
	Mode	Select the mode of the call, which supports direct dial and directory.
	Auto Answer	When dials the device successfully, it is automatically connected within the set answer time.
	Organization Search	Organization search is a user management method provided by video intercom that allows users to tag video intercom personnel into different categories for better management and location. Through Organization Search, users can find video intercom personnel they need to contact more easily and improve communication efficiency.
	Organization Input Method	Select the input method to use organization search, which supports both alphabet and number methods.

Copyright © 2025 ARMATURA LLC. All rights reserved.

12 Autotest

To automatically test whether all modules in the device function properly, which include the LCD, Audio, microphone, Camera, real-time clock (RTC), and HID Config.

Tap **Autotest** on the main menu interface.



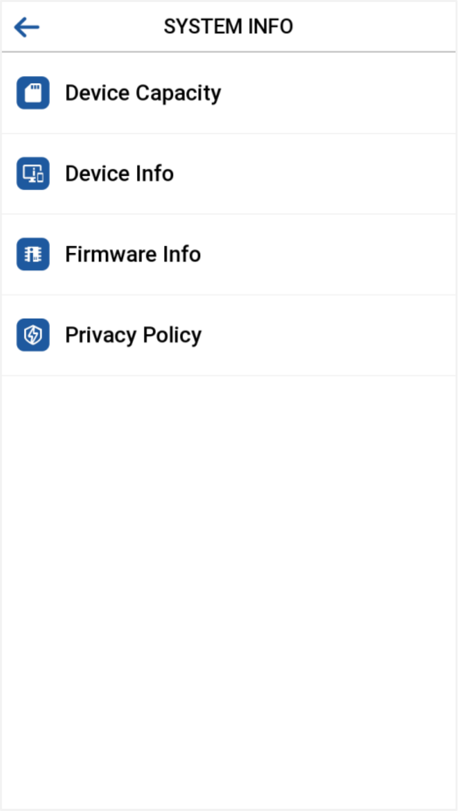
Menu	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test Display	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays the colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Microphone	To test if the microphone is working properly by speaking into the microphone.
Test Camera	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test HID Config	To test if the card is working properly by swiping into the card reading area.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and tap it again to stop counting.

Copyright © 2025 ARMATURA LLC. All rights reserved.

13 System Information

With the system information option, you can view the storage status, the version information of the device, and so on.

Tap **System Info** on the main menu interface.



Menu	Description
Device Capacity	Displays the current device's user storage, password, palm, face and card storage, administrators, access/attendance records, attendance and blocklist photos, and Profile photos.
Device Info	Displays the Device's name, Serial number, MAC Address, Face and Palm algorithm version information, platform information, MCU Version, card module version, manufacturer and manufacture Date.
Firmware Info	Displays the Firmware version and other version information of the device.
Privacy Policy	The privacy policy control will appear when the gadget turns on for the first time. After tapping "**Read and Accept**," the customer can use the product regularly. Tap **System Info** -> **Privacy Policy** to view the content of the privacy policy. The privacy policy's content does not allow for U disc export. **Note:** The current privacy policy's text is only available in Simplified Chinese/English. However, translation of other multi-language content is underway, with more iterations.

Copyright © 2025 ARMATURA LLC. All rights reserved.

14 Connecting to ACMS★

ACMS (Armatura Credential Management System) facilitates integrators to use the ARMATURA CONNECT APP with OmniAC30. The ACMS can be used by customers & integrators to manage & issue credentials.

14.1 ARMATURA CONNECT

14.1.1 Download and Install the APP

1. Ensure your mobile device is connected to the internet via a mobile or Wi-Fi network.
2. Search for the ARMATURA CONNECT APP in the Apple APP Store (for iOS devices), Google Play Store (for Android devices) or scan the QR code below to download the APP on your mobile phone.

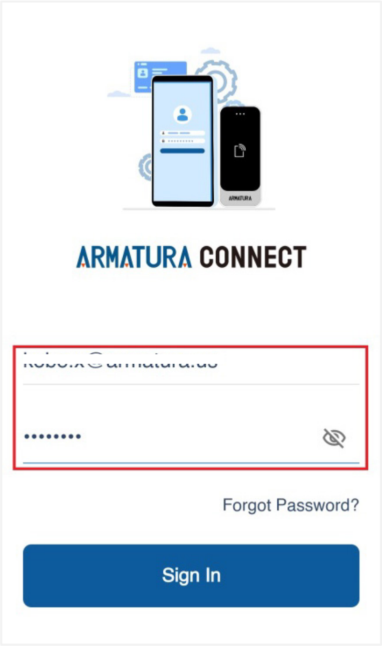
iOS Android

14.1.2 Log in the APP

After the account activation process is complete, you can log in to the ARMATURA CONNECT APP with your account and password.

1. Enter the account and the password. Click **Sign In** to log into the ARMATURA CONNECT APP. The password is set when the account was activated.
2. If you have forgotten your login password, tap **Forgot Password?**. Enter your email address and tap **Send Link**. Your password will be reset through the ACMS mailbox.

Copyright © 2025 ARMATURA LLC. All rights reserved.

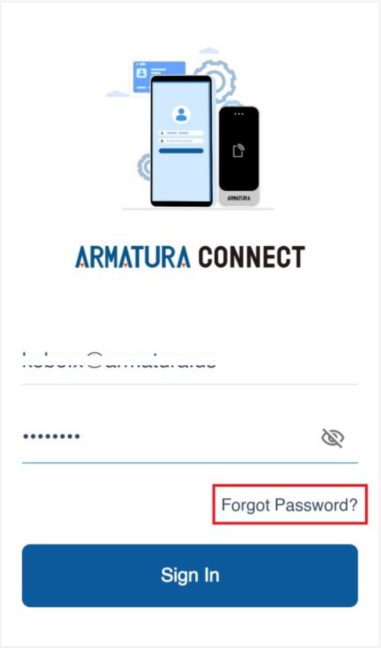


ARMATURA CONNECT

kobe.x@armatura.us

••••••••

Forgot Password?

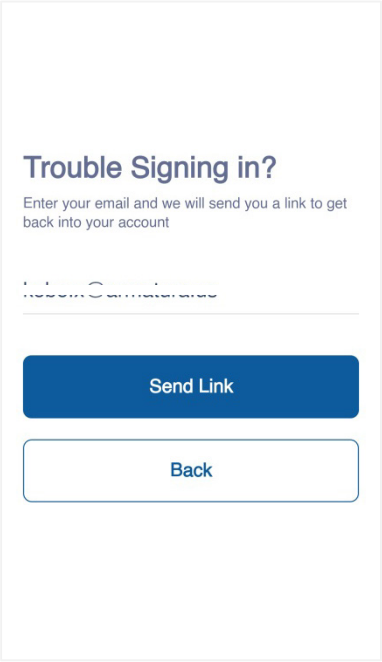


ARMATURA CONNECT

kobe.x@armatura.us

••••••••

Forgot Password?



Trouble Signing in?

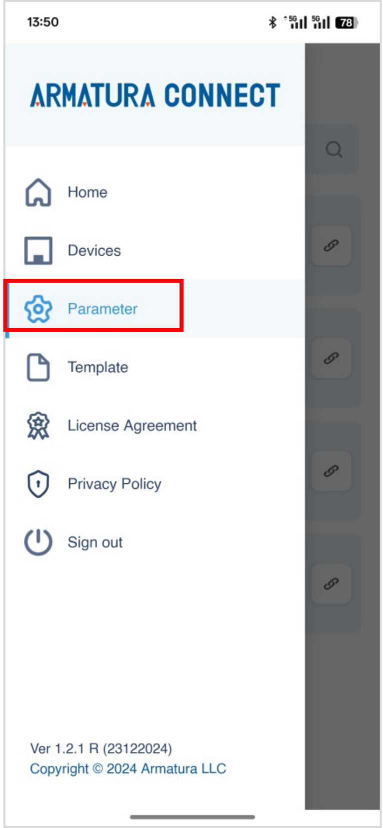
Enter your email and we will send you a link to get back into your account

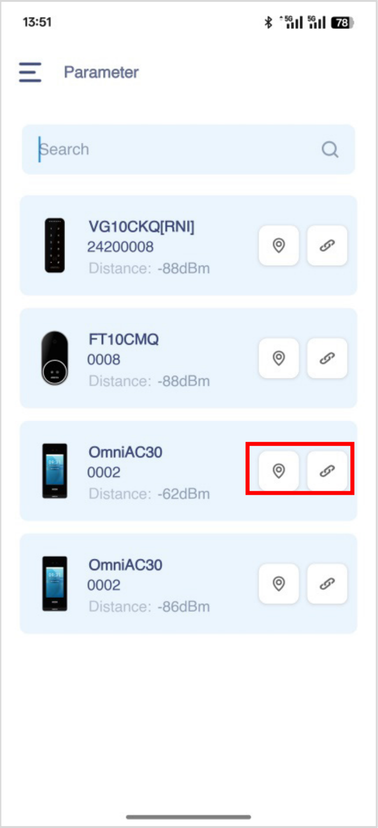
kobe.x@armatura.us

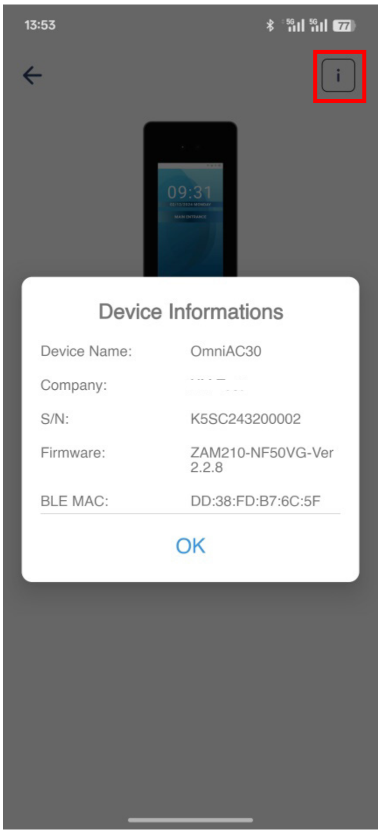
14.1.3 Bind Device

1. Click ☰ > **Parameter** to enter the parameter setting screen.
2. Turn on the Bluetooth function of the mobile device, and click 🔍 to search for the device. All searched devices will be displayed in the list.
3. Click 📍 to confirm your device.
4. Click 🔗 to enter the device parameter setting screen. Here you can set the relevant parameters of the device.

Copyright © 2025 ARMATURA LLC. All rights reserved.







Device Informations

Device Name: OmniAC30

Company: [redacted]

S/N: K5SC243200002

Firmware: ZAM210-NF50VG-Ver 2.2.8

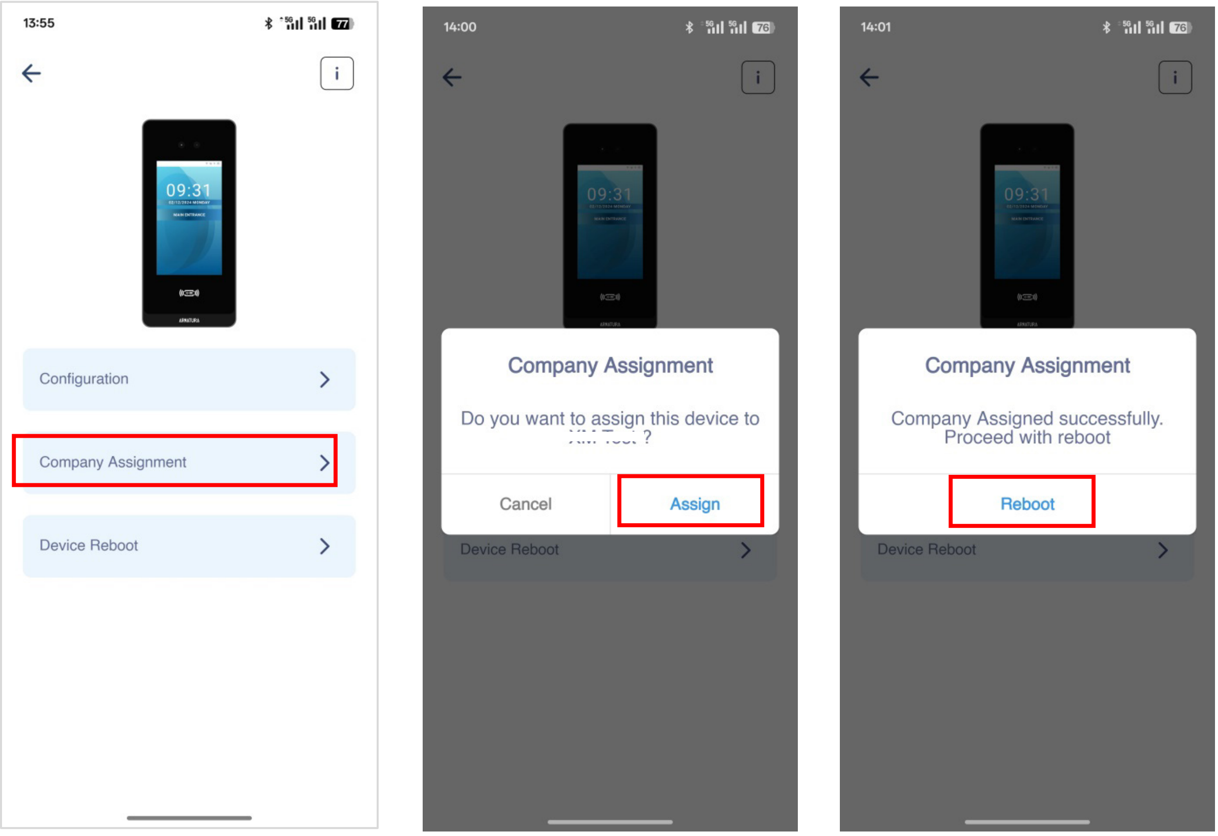
BLE MAC: DD:38:FD:B7:6C:5F

14.1.4 Company Assign

This function is used to assign the device to the company. The Bluetooth function of the mobile device needs to be turned on before operation.

1. Click **Company Assignment** and the Assignment window will pop up. Click **Assign** to assign the device to the current company.
2. Click **Reboot** when prompted that the assignment is successful.
3. After completing the above steps, please wait for the device to reboot.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Company Assignment

Do you want to assign this device to XM Test ?

Company Assignment

Company Assigned successfully. Proceed with reboot

After the device configuration is complete, employees of the company can use the mobile credentials to operate on the Armatura ID APP.

14.2 ARMATURA ID

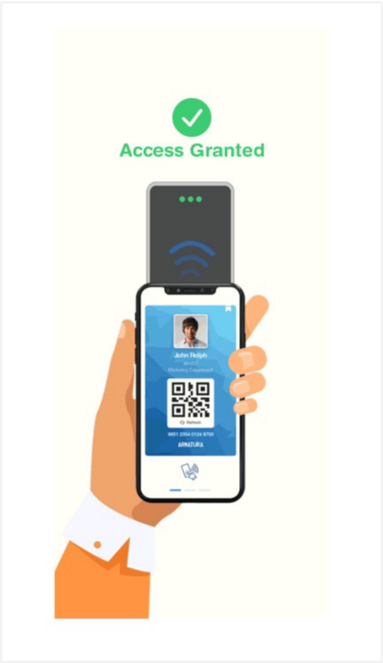
ARMATURA ID allows end users to use their mobile devices (smartphones) to securely and conveniently enter the workplace by extending access control capabilities to smart devices.

When the user approaches the OmniAC30, the following interaction modes can be performed through their mobile device to access:

- Card Mode: When using this mode, the end user's mobile device is brought very close to, or touching the reader (a similar user experience to using a physical credential).
- Remote Mode: This mode allows end users to use mobile devices to perform remote control within the set range.
- QR Code Mode: This mode allows end users to swipe the QR code on the mobile phone on the OmniAC30.

Note: The effective distance of Card Mode is 0 to 20 inches (0 to 50 centimeters). The effective distance of Remote Mode is 0 to 394 inches (0 to 1000 centimeters).

Copyright © 2025 ARMATURA LLC. All rights reserved.



Card Mode

Access Granted

Remote Mode

Credentials
Personnel Code
1170562
ARMATURA ID
13:45
12/23/24 MONDAY
Tap To Unlock
ARMATURA

QR Code Mode

14.2.1 Download the ARMATURA ID APP

Ensure the mobile device is connected to the internet (either via mobile data network or Wi-Fi) during device registration and Mobile ID delivery. Both Android and iOS versions are available, please download the APP according to the following instructions.

1. Search for the ARMATURA ID APP in the Apple APP Store (for iOS devices), Google Play Store (for Android devices) or scan the QR code below to download the APP on your mobile phone.

iOS Android

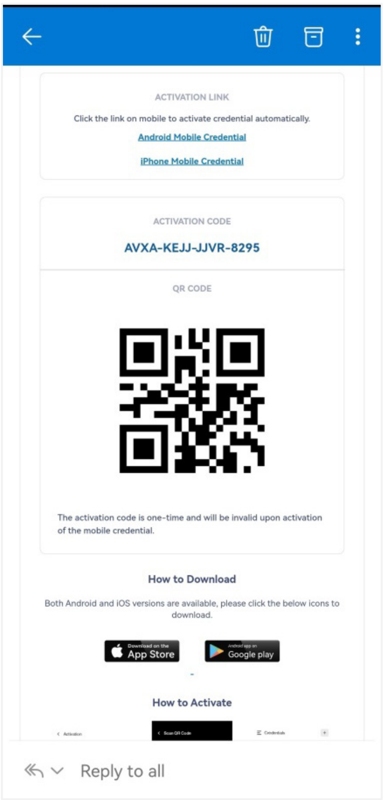
2. You can also download the APP by clicking on the store icons in the activation code email sent by the server mailbox Armatura Credential Management System.

14.2.2 Activate the Credentials

After completing the installation of the APP, you first need to activate the credentials. There are three ways to activate the credentials: click the activation link to activate automatically, enter the activation code to activate, and scan the QR code to activate. The specific operation steps are as follows.

Copyright © 2025 ARMATURA LLC. All rights reserved.

First, please open the activation code email sent by Armatura Credential Management System. It is sent by the site administrator of your company via ACMS.



ACTIVATION LINK

Click the link on mobile to activate credential automatically.

Android Mobile Credential

iPhone Mobile Credential

ACTIVATION CODE

AVXA-KEJJ-JJVR-8295

QR CODE

The activation code is one-time and will be invalid upon activation of the mobile credential.

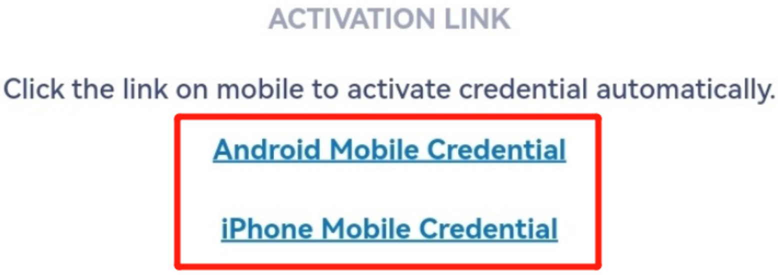
How to Download

Both Android and iOS versions are available, please click the below icons to download.

How to Activate

Click the Activation Link to Activate

Click the link on mobile to activate credential automatically. Follow the prompts.



ACTIVATION LINK

Click the link on mobile to activate credential automatically.

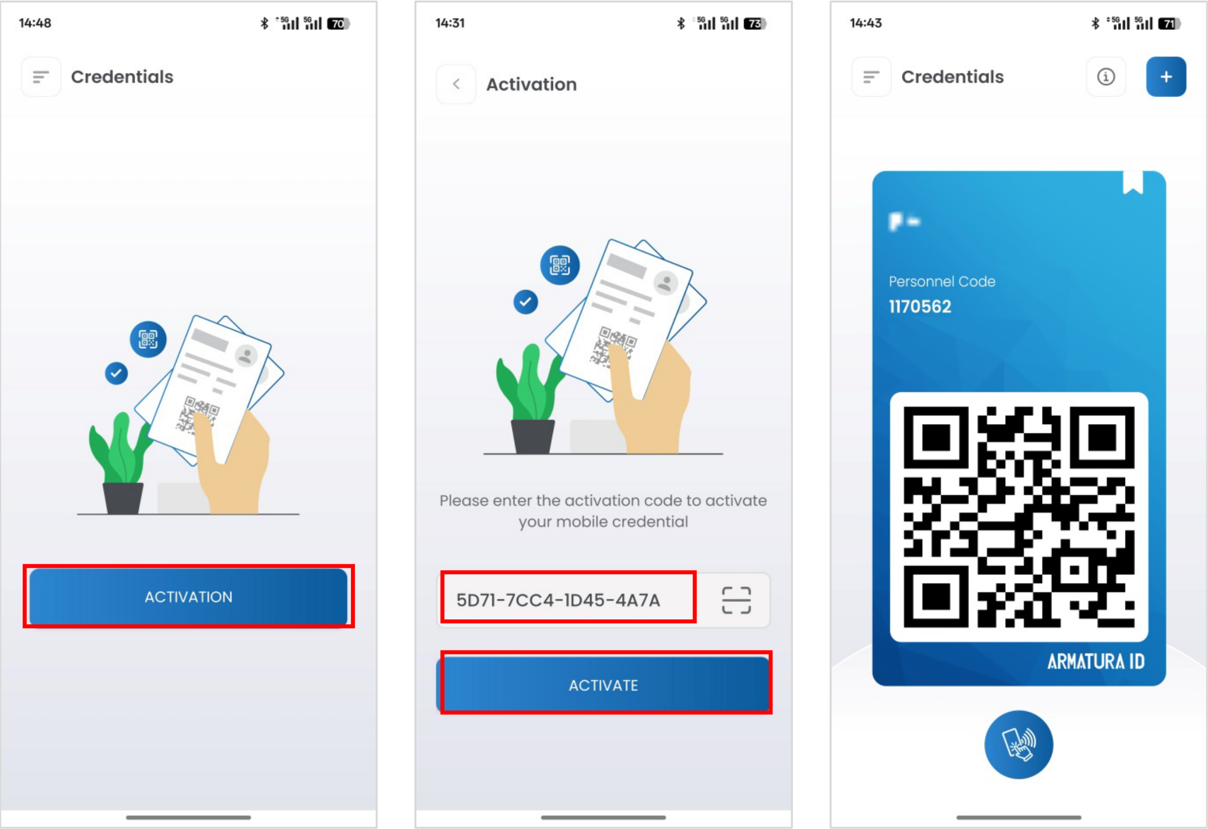
Android Mobile Credential

iPhone Mobile Credential

Enter the Activation Code to Activate

1. Open the ARMATURA ID APP and enter the Credentials interface. Click **ACTIVATION**.
2. Manually enter the activation code from the email in the input field.
3. Click **ACTIVATE** on the Activation interface.
4. A mobile credential will be displayed after successful activation.

Copyright © 2025 ARMATURA LLC. All rights reserved.



14:48

Credentials

ACTIVATION

14:31

Activation

Please enter the activation code to activate your mobile credential

5D71-7CC4-1D45-4A7A

ACTIVATE

14:43

Credentials

Personnel Code

1170562

ARMATURA ID

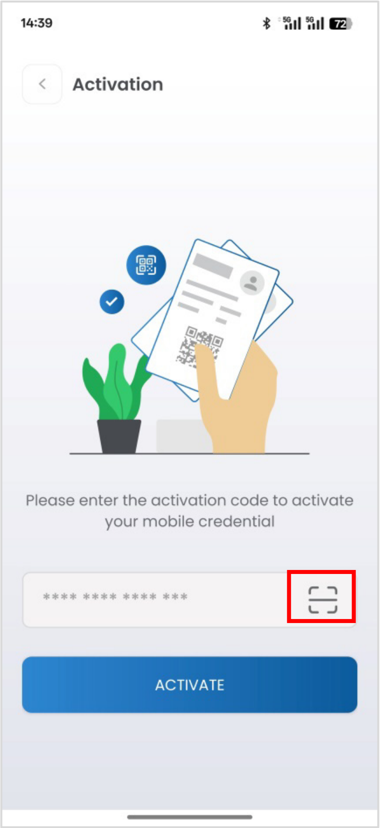
Scan the QR Code to Activate

1. Open the ARMATURA ID APP and enter the Credentials interface. Click ACTIVATION.
2. Click ⛶ to scan the QR code on the email. And the system will automatically enter the activation code.
3. Then click ACTIVATE to activate the credential.
4. A mobile credential will be displayed after successful activation.

Note:

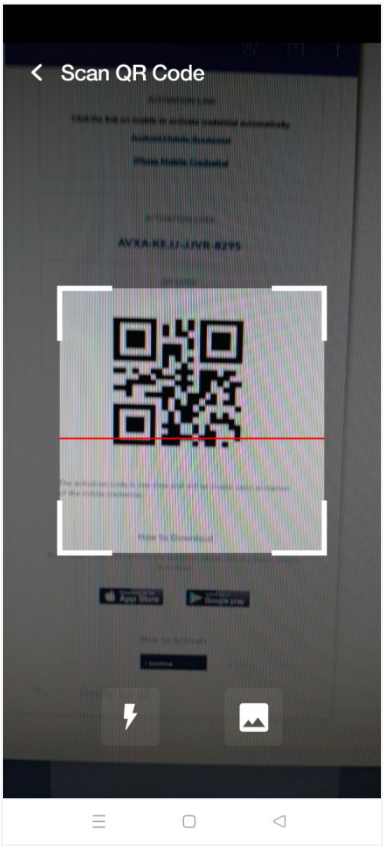
1. Please turn on the Bluetooth function of your mobile phone before scanning.
2. In order to allow access for users' devices, the site administrators need to assign devices under their company beforehand.

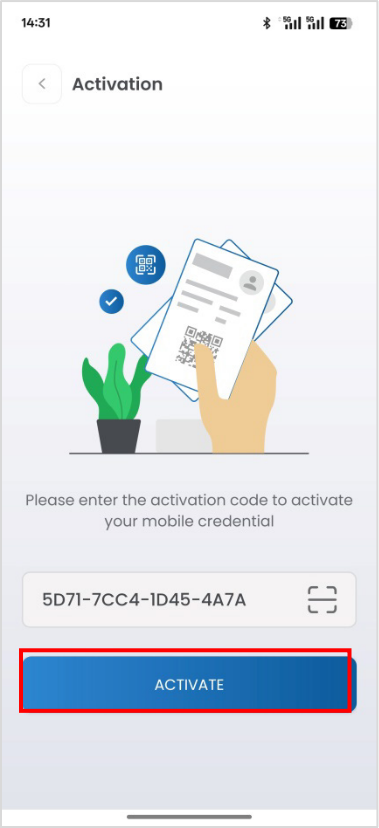
Copyright © 2025 ARMATURA LLC. All rights reserved.



Please enter the activation code to activate your mobile credential

**** **** **** ***





Please enter the activation code to activate your mobile credential

5D71-7CC4-1D45-4A7A

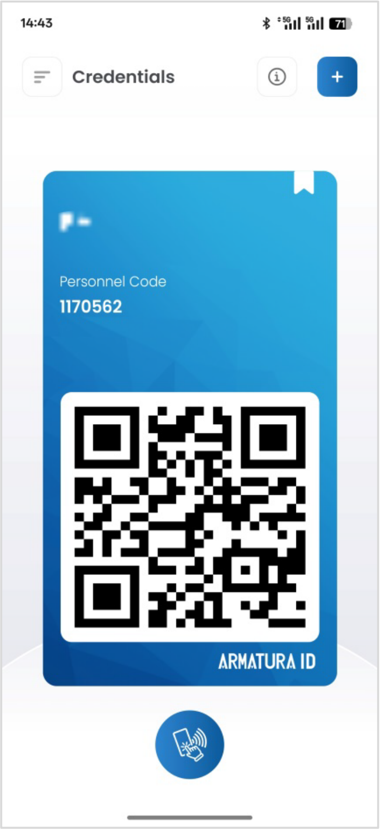
14.2.3 Use of the Mobile Credentials

The end users can swipe their cards through QR code, NFC and Bluetooth.

Swipe the card through QR code

The dynamic QR code can be seen directly on the card. You just need to swipe the QR code on your mobile phone on the OmniAC30 to open the door.

Copyright © 2025 ARMATURA LLC. All rights reserved.

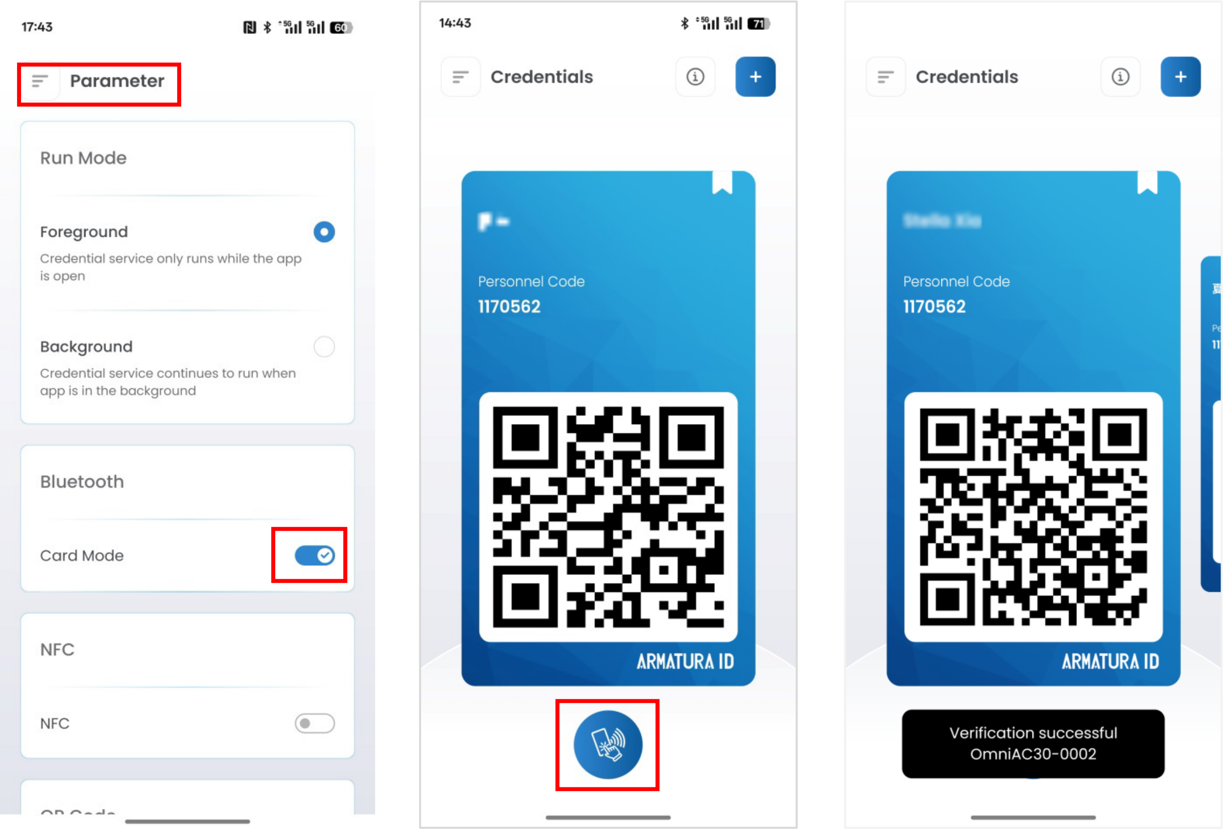


Swipe the card through Bluetooth

Card mode functions requires the end user to hold the mobile device close to the card reader to swipe the card. Remote mode functions like a remote control. With the remote mode, you don't need to swipe the card on the reader, just get close to the reader within the effective range.

1. Turn on the **Bluetooth** functions on your mobile phone.
2. Click **Parameter** on the **Main Menu** screen to enter the parameter setting interface.
3. Click of the **Card Mode** to enable the function.
4. Then you can swipe the card with the mobile phone close to the reader, or click of the card to swipe the card remotely within the set range.

Copyright © 2025 ARMATURA LLC. All rights reserved.



17:43

Parameter

Run Mode

Foreground ●
Credential service only runs while the app is open

Background ○
Credential service continues to run when app is in the background

Bluetooth

Card Mode ☑

NFC

NFC ○

14:43

Credentials

Personnel Code
1170562

ARMATURA ID

Credentials

Personnel Code
1170562

ARMATURA ID

Verification successful
OmniAC30-0002

Note: For other specific operations, please refer to *Armatura CONNECT User Manual* and *Armatura ID User Manual*.

Copyright © 2025 ARMATURA LLC. All rights reserved.

15 Video Intercom

The video intercom feature needs to be used in conjunction with the Armatura One server and the Armatura ICS mobile APP.

15.1 Connect to Armatura One Software

Device Side

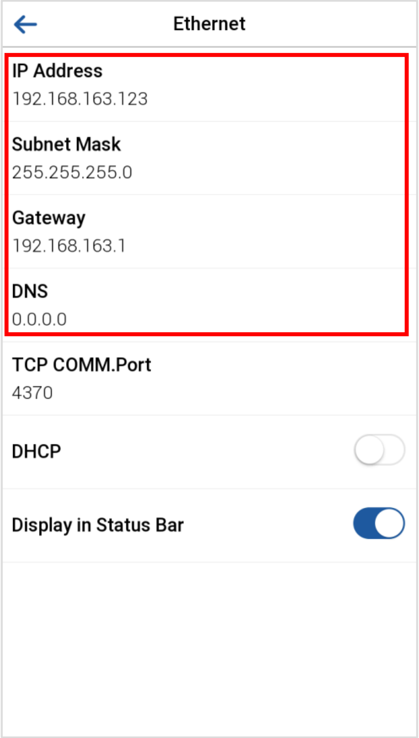
1. Tap COMM. > Ethernet in the main menu to set the IP address and gateway of the device.

   Note: Please ensure that the IP address is in the same network segment as the server address and can communicate with the Armatura One server.

2. In the main menu, tap COMM. > Cloud Server Settings to set the server address and server port.

   Server Address: Set the IP address as of Armatura One server.

   Server Port: Set the server port as of Armatura One.



Ethernet

IP Address
192.168.163.123

Subnet Mask
255.255.255.0

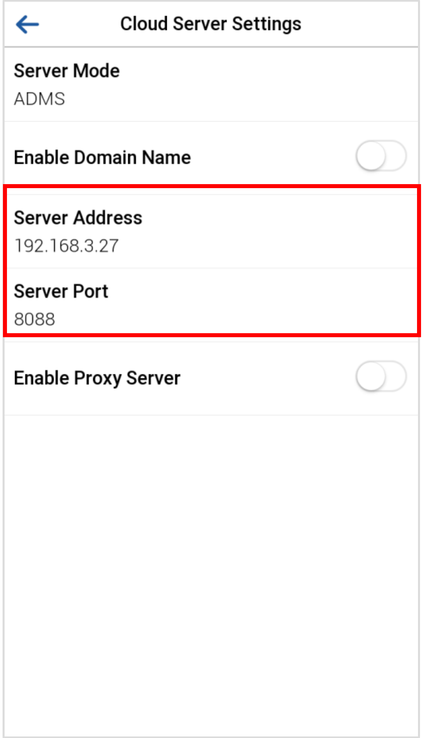
Gateway
192.168.163.1

DNS
0.0.0.0

TCP COMM.Port
4370

DHCP

Display in Status Bar



Cloud Server Settings

Server Mode
ADMS

Enable Domain Name

Server Address
192.168.3.27

Server Port
8088

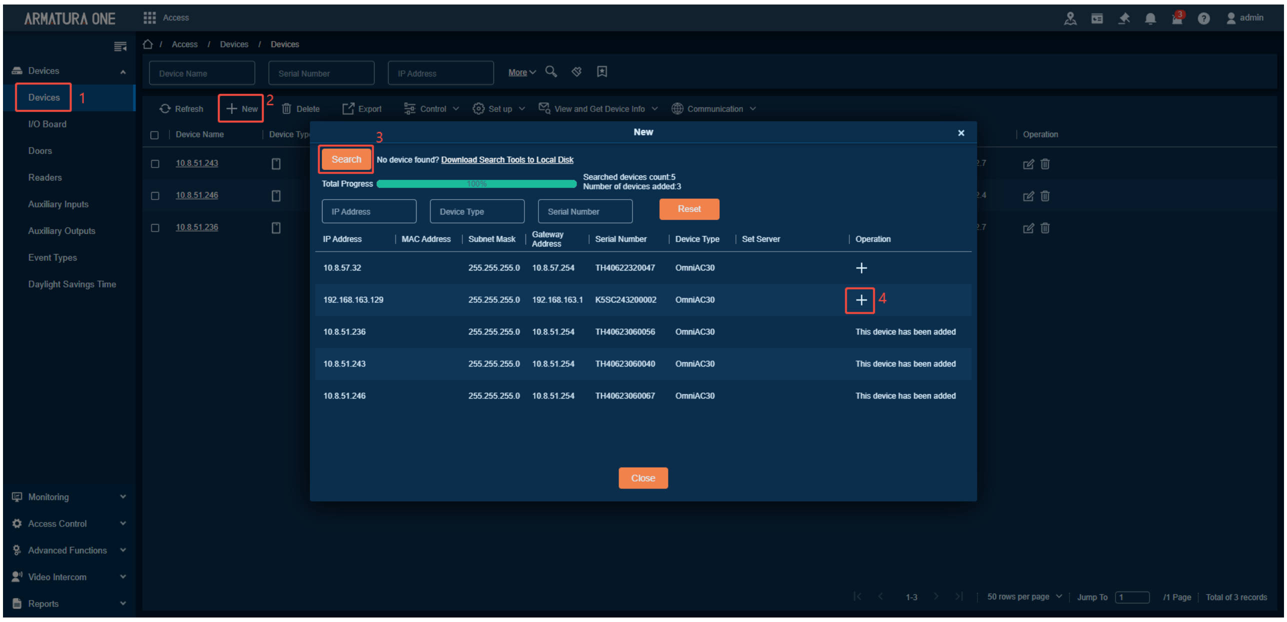
Enable Proxy Server

Copyright © 2025 ARMATURA LLC. All rights reserved.

Software Side

Login to Armatura One software, add the device by searching. The process is as follows:

1. Click **Access** > **Device** > **Device** > **+New**, to open the search interface in the software.
2. Click **Search**, and it will prompt searching…….
3. After searching, the list and total number of access controllers will be displayed.



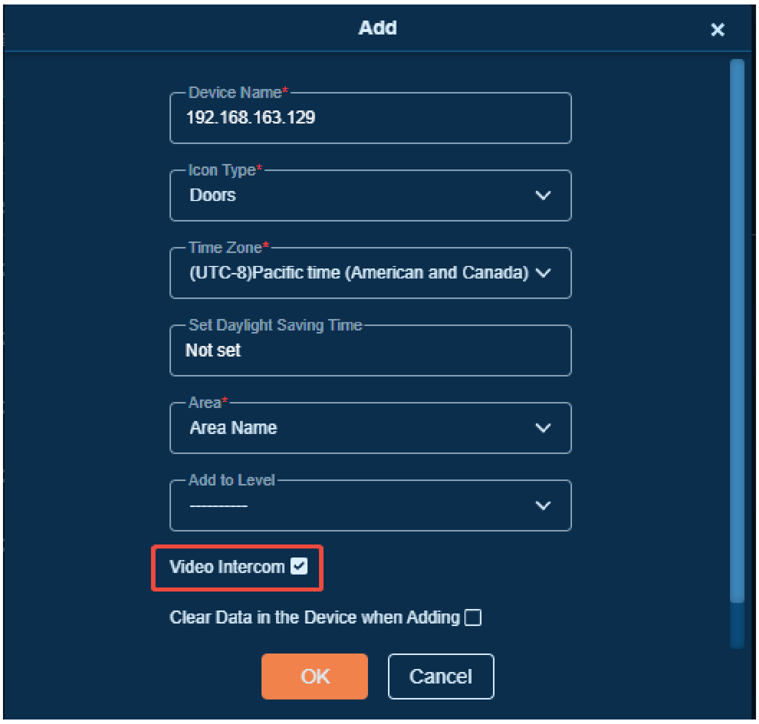
No device found? Download Search Tools to Local Disk

Total Progress 100%

Searched devices count:5
Number of devices added:3

IP Address	MAC Address	Subnet Mask	Gateway Address	Serial Number	Device Type	Set Server	Operation
10.8.57.32		255.255.255.0	10.8.57.254	TH40622320047	OmniAC30		+
192.168.163.129		255.255.255.0	192.168.163.1	K5SC243200002	OmniAC30		+
10.8.51.236		255.255.255.0	10.8.51.254	TH40623060056	OmniAC30		This device has been added
10.8.51.243		255.255.255.0	10.8.51.254	TH40623060040	OmniAC30		This device has been added
10.8.51.246		255.255.255.0	10.8.51.254	TH40623060067	OmniAC30		This device has been added

4. Click **+** in operation column, a new window will pop-up. Set the Device Name, Icon Type, Time Zone, Area, Add to Level, and enable Video Intercom, finally click **OK** to add the device.



Device Name*: 192.168.163.129

Icon Type*: Doors

Time Zone*: (UTC-8)Pacific time (American and Canada)

Set Daylight Saving Time: Not set

Area*: Area Name

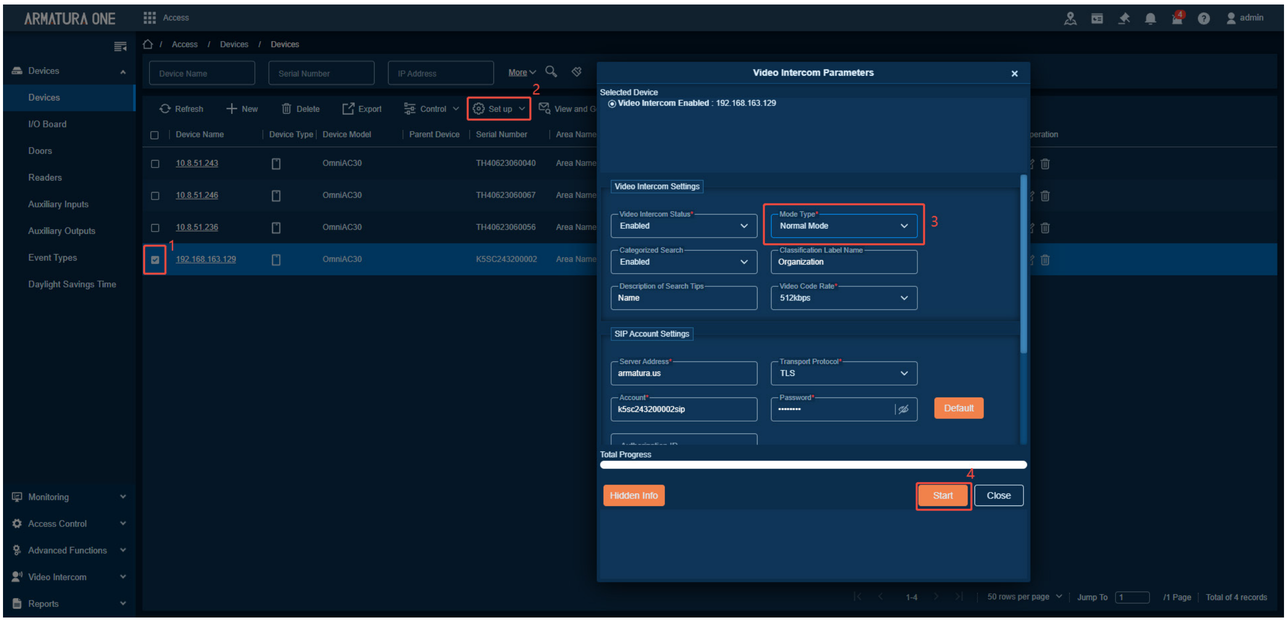
Add to Level: ---------

Video Intercom ☑

Clear Data in the Device when Adding □

Copyright © 2025 ARMATURA LLC. All rights reserved.

5. The video intercom mode is Direct Call Mode by default. You can switch to Normal Mode in **Set up > Video Intercom Parameters**.



Device Name	Device Type	Device Model	Parent Device	Serial Number	Area Name
10.8.51.243		OmniAC30		TH40623060040	Area Name
10.8.51.246		OmniAC30		TH40623060067	Area Name
10.8.51.236		OmniAC30		TH40623060056	Area Name
192.168.163.129		OmniAC30		K5SC243200002	Area Name

Video Intercom Parameters

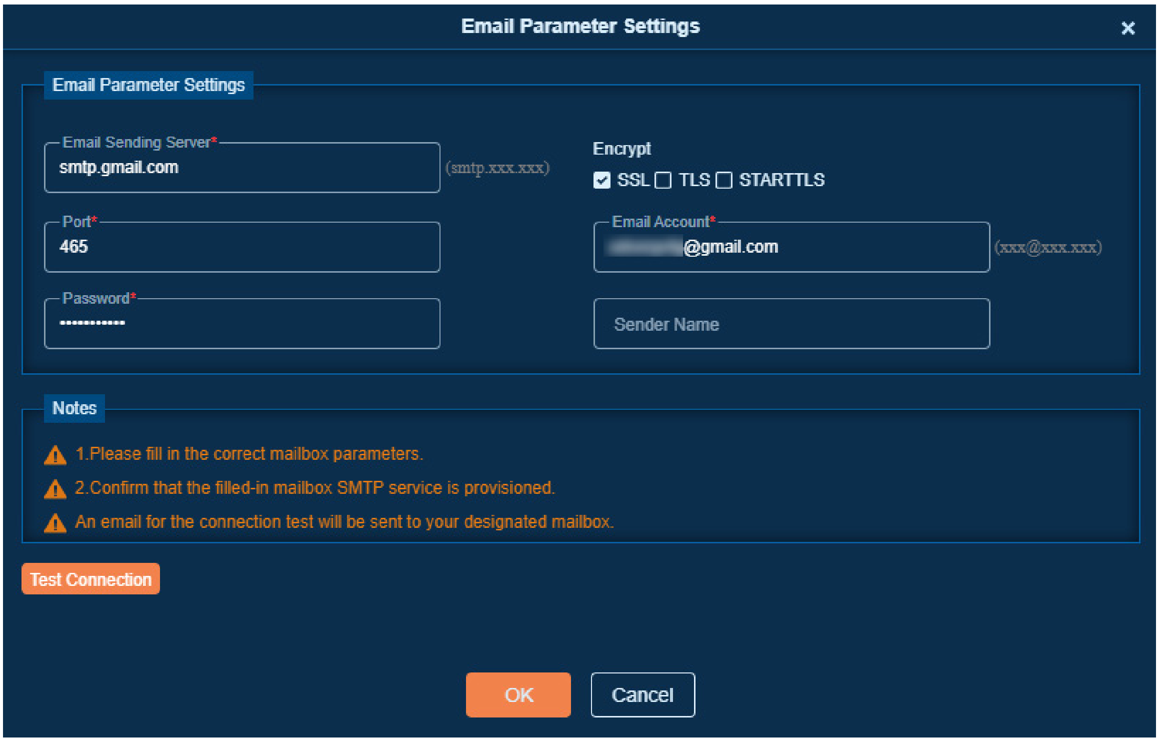
Selected Device
● Video Intercom Enabled : 192.168.163.129

Video Intercom Settings
Video Intercom Status*: Enabled
Mode Type*: Normal Mode
Categorized Search: Enabled
Classification Label Name: Organization
Description of Search Tips: Name
Video Code Rate*: 512kbps

SIP Account Settings
Server Address*: armatura.us
Transport Protocol*: TLS
Account*: k5sc243200002sip
Password*: ••••••••

15.2 Set up Email SMTP Service

1. Set up email functionality from Armatura One server for users. In the Armatura One software, click System > Integrations > E-mail Management > Email Parameter Settings.



Email Parameter Settings

Email Parameter Settings

Email Sending Server*: smtp.gmail.com (smtp.xxx.xxx)
Port*: 465
Password*: ••••••••••••
Encrypt: ☑ SSL ☐ TLS ☐ STARTTLS
Email Account*: [redacted]@gmail.com (xxx@xxx.xxx)
Sender Name

Notes

1.Please fill in the correct mailbox parameters.
2.Confirm that the filled-in mailbox SMTP service is provisioned.
An email for the connection test will be sent to your designated mailbox.

2. In the **[Email Parameter Settings]** interface, configure the necessary parameters for the SMTP server.

Copyright © 2025 ARMATURA LLC. All rights reserved.

The field description is as follows:

[Email Sending Server]: the format is **[smtp.xxxx.xxx]**. If you are using Gmail, please fill in [smtp.gmail.com].

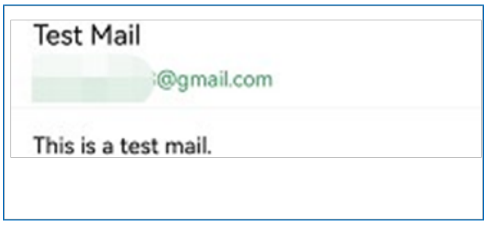
[Port]: the available options are **[SSL:465]** or **[TLS:587]**. If you are using Gmail, please select [SSL:465].

[Email Account]: please enter the email address that you used to generate the app password.

[Password]: please enter the app password.

[Sender Name]: feel free to set a name of your choice. The system will use this name to send emails in the future.

3. Click on the **[Test Connection]** button to perform a test. The system will send a test email to your email, please do not reply.



Test Mail

[redacted]@gmail.com

This is a test mail.

4. Once the system prompt success, you can click on the **[OK]** button to complete the email parameter setup process.

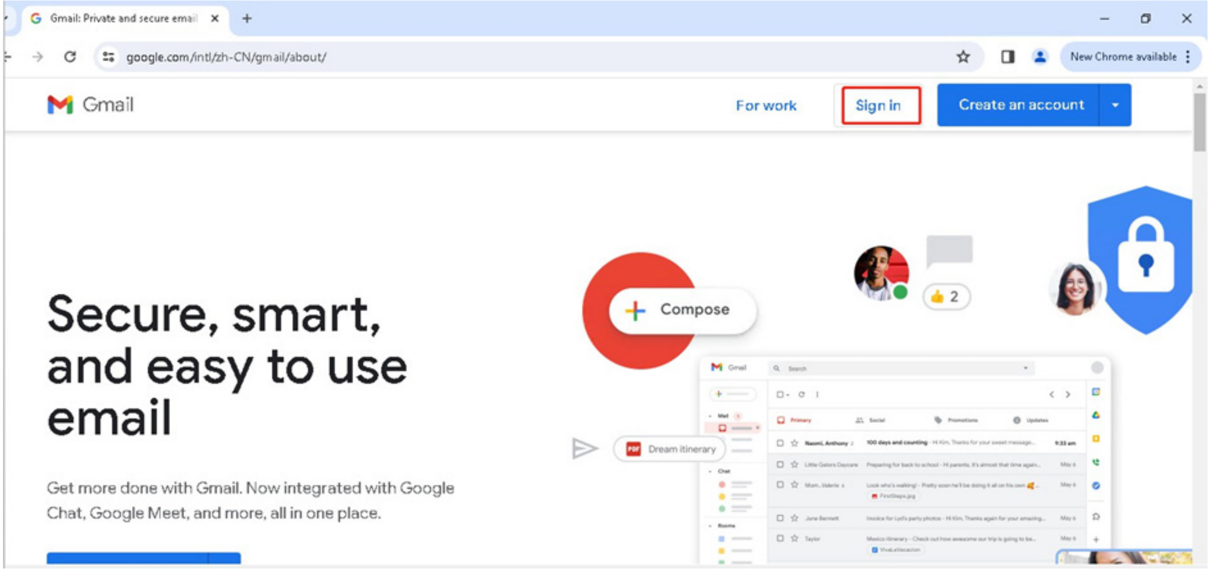
App Password Setup (Take Gmail as an example)

Step 1: Log in to Your Gmail Email Account

1. Open a web browser and go to the Gmail website (www.gmail.com).

2. On the Gmail login page, locate the sign-in section.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Secure, smart, and easy to use email

Get more done with Gmail. Now integrated with Google Chat, Google Meet, and more, all in one place.

3. Enter your Gmail email address in the provided field.

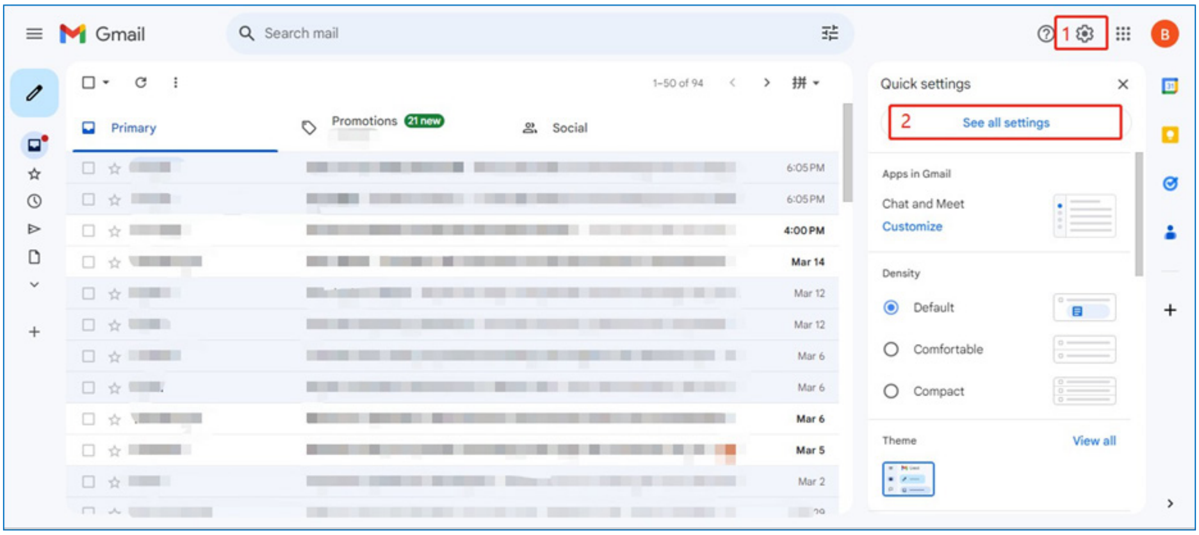
4. Click on the **[Next]** button.

5. On the next page, enter your password associated with your Gmail account.

6. Click on the **[Sign In]** button.

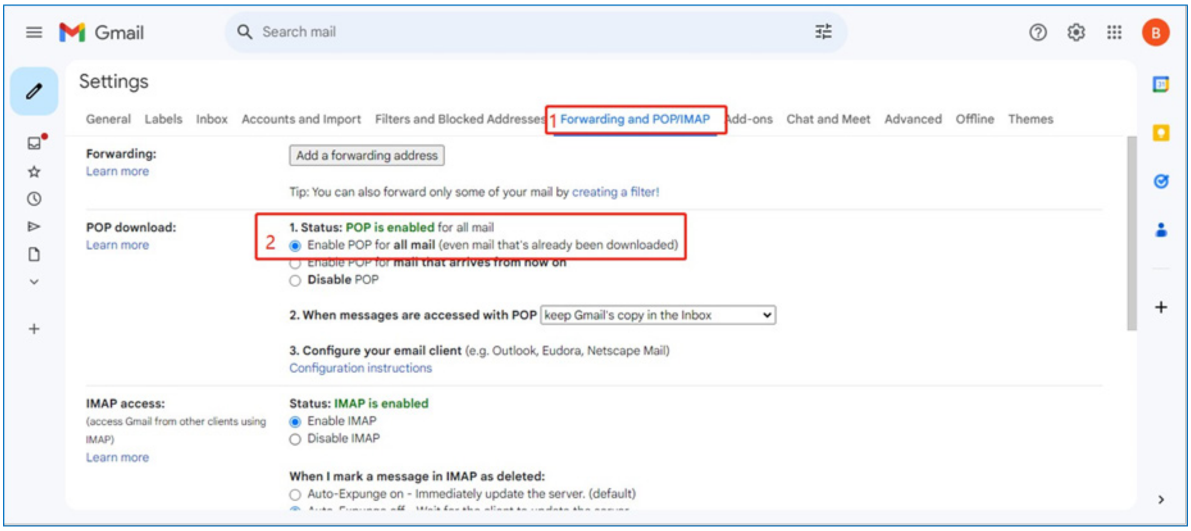
Step 2: Generate an App Password

1. Click on Setting ⚙ icon and then click **[See all settings]**.



2. Select the **Forwarding and POP/IMAP**, then enable the POP for all mail.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Forwarding:
Learn more

Tip: You can also forward only some of your mail by creating a filter!

POP download:
Learn more

1. Status: POP is enabled for all mail
● Enable POP for **all mail** (even mail that's already been downloaded)
○ Enable POP for **mail that arrives from now on**
○ **Disable** POP

2. When messages are accessed with POP: keep Gmail's copy in the Inbox

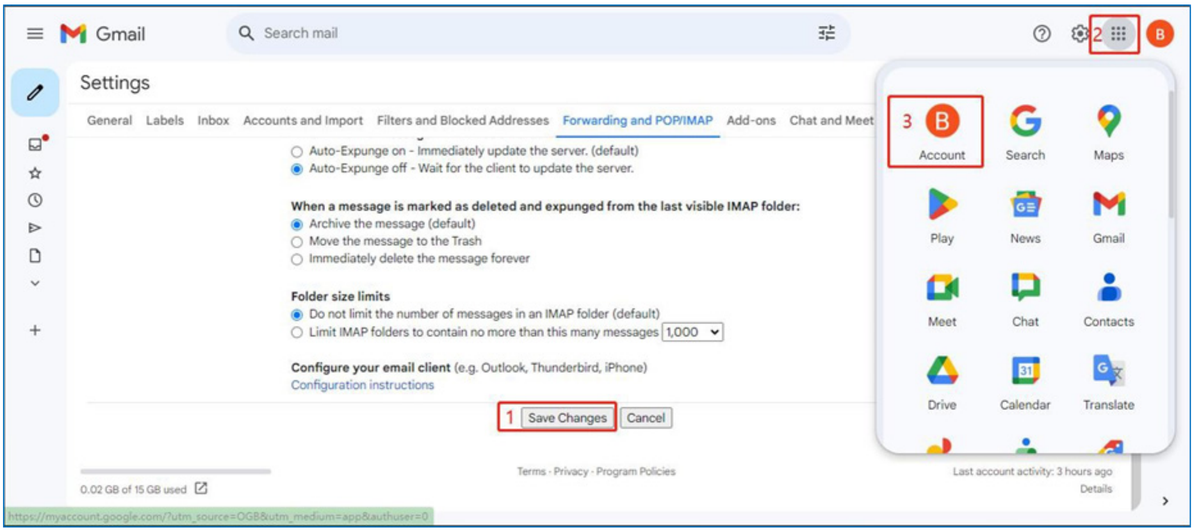
3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)
Configuration instructions

IMAP access:
(access Gmail from other clients using IMAP)
Learn more

Status: IMAP is enabled
● Enable IMAP
○ Disable IMAP

When I mark a message in IMAP as deleted:
○ Auto-Expunge on - Immediately update the server. (default)

3. After enabling all services set **[save changes]** and then click on the menu ⋮⋮⋮ icon and select the [Account].



○ Auto-Expunge on - Immediately update the server. (default)
● Auto-Expunge off - Wait for the client to update the server.

When a message is marked as deleted and expunged from the last visible IMAP folder:
● Archive the message (default)
○ Move the message to the Trash
○ Immediately delete the message forever

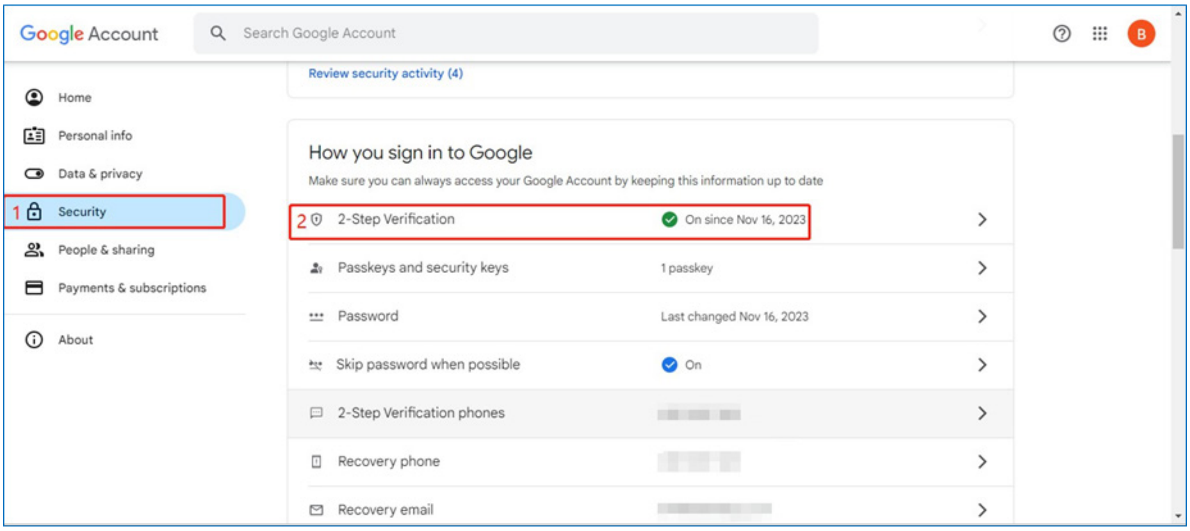
Folder size limits
● Do not limit the number of messages in an IMAP folder (default)
○ Limit IMAP folders to contain no more than this many messages 1,000

Configure your email client (e.g. Outlook, Thunderbird, iPhone)
Configuration instructions

0.02 GB of 15 GB used
Terms · Privacy · Program Policies
Last account activity: 3 hours ago
Details
https://myaccount.google.com/?utm_source=OGB&utm_medium=app&authuser=0

4. In Account, select the **[Security]> [2-Step Verification]**.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Google Account | Search Google Account

Review security activity (4)

- Home
- Personal info
- Data & privacy
- 1 Security
- People & sharing
- Payments & subscriptions
- About

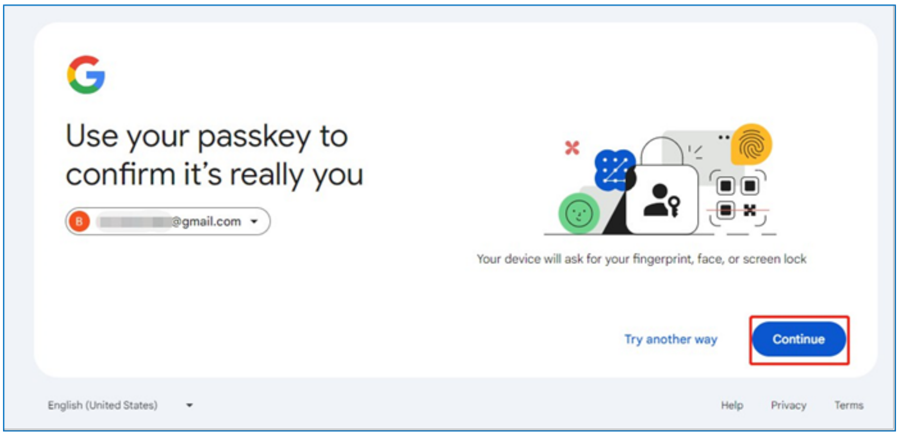
How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date

2 2-Step Verification	On since Nov 16, 2023
Passkeys and security keys	1 passkey
Password	Last changed Nov 16, 2023
Skip password when possible	On
2-Step Verification phones	[redacted]
Recovery phone	[redacted]
Recovery email	[redacted]

5. In the new interface, click on [Continue] to start the Google Two-Step Verification process.

6. You can choose to receive a verification code via a text message or a phone call to your registered mobile number. The code will be sent to you, and you can enter it during the Google Two-Step Verification process.



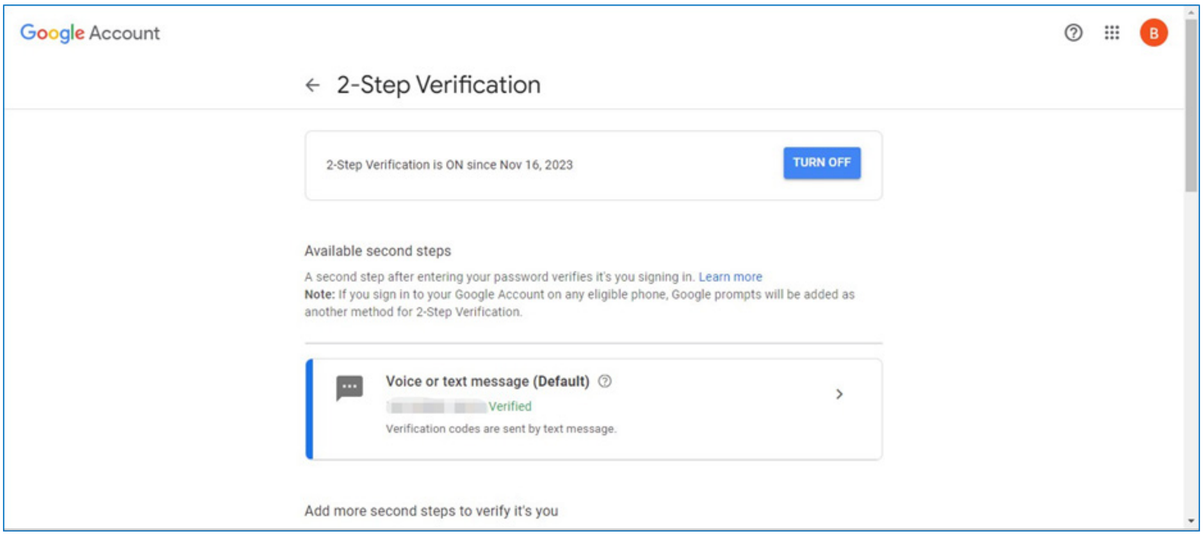
Use your passkey to confirm it's really you

B [redacted]@gmail.com

Your device will ask for your fingerprint, face, or screen lock

7. Once you enter the correct verification code, Google will verify it and grant you access to your account.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Google Account

2-Step Verification

2-Step Verification is ON since Nov 16, 2023

Available second steps

A second step after entering your password verifies it's you signing in. Learn more

Note: If you sign in to your Google Account on any eligible phone, Google prompts will be added as another method for 2-Step Verification.

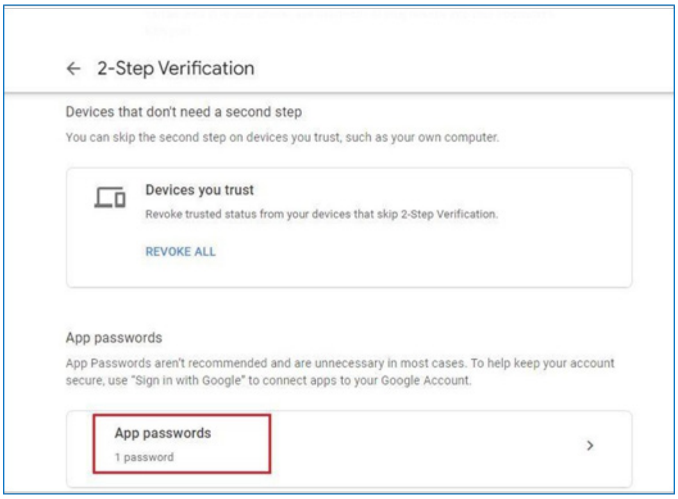
Voice or text message (Default)

Verified

Verification codes are sent by text message.

Add more second steps to verify it's you

8. Once the 2-Step Verification is done, you can find the **[App Passwords]** below.



2-Step Verification

Devices that don't need a second step

You can skip the second step on devices you trust, such as your own computer.

Devices you trust

Revoke trusted status from your devices that skip 2-Step Verification.

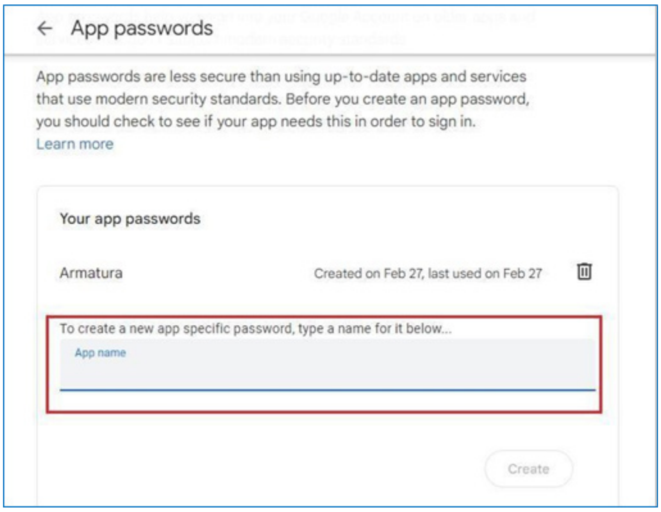
App passwords

App Passwords aren't recommended and are unnecessary in most cases. To help keep your account secure, use "Sign in with Google" to connect apps to your Google Account.

App passwords

1 password

9.Click on **[App passwords]** and fill the application name to generate the password to use it on SMTP services.



App passwords

App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.

Learn more

Your app passwords

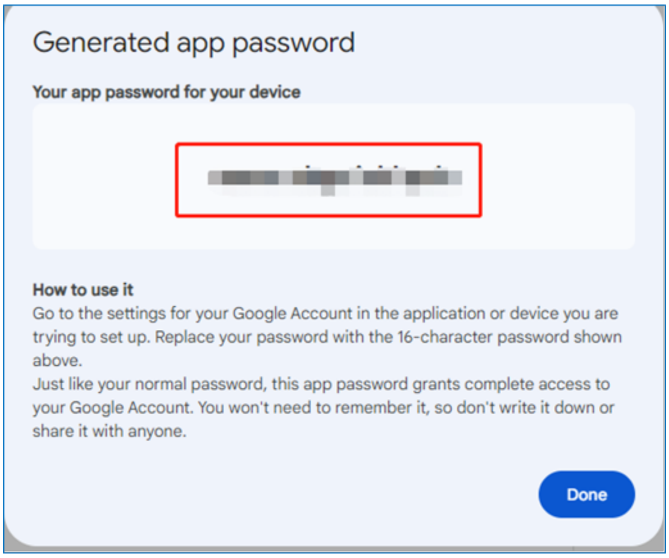
Armatura Created on Feb 27, last used on Feb 27

To create a new app specific password, type a name for it below...

App name

Copyright © 2025 ARMATURA LLC. All rights reserved.

10. Copy the App password, it will be used in the subsequent Armatura ONE SMTP service configuration process.



Generated app password

Your app password for your device

[redacted]

How to use it

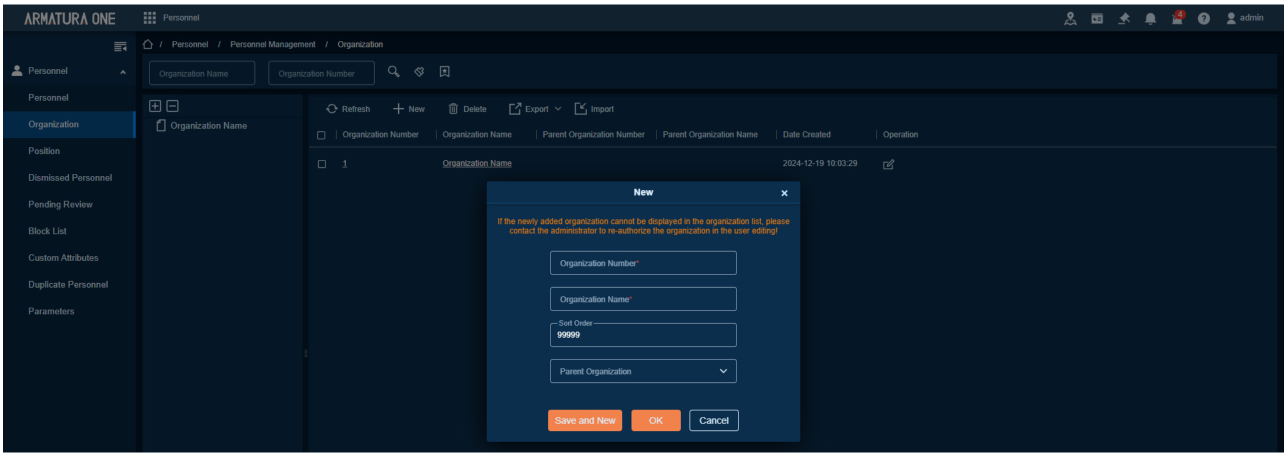
Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above.

Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

15.3 Add Personnel on the Software

Add the Organization

Click **Personnel > Personnel > Organization > +New** on the Armatura One.



If the newly added organization cannot be displayed in the organization list, please contact the administrator to re-authorize the organization in the user editing!

Organization Number*

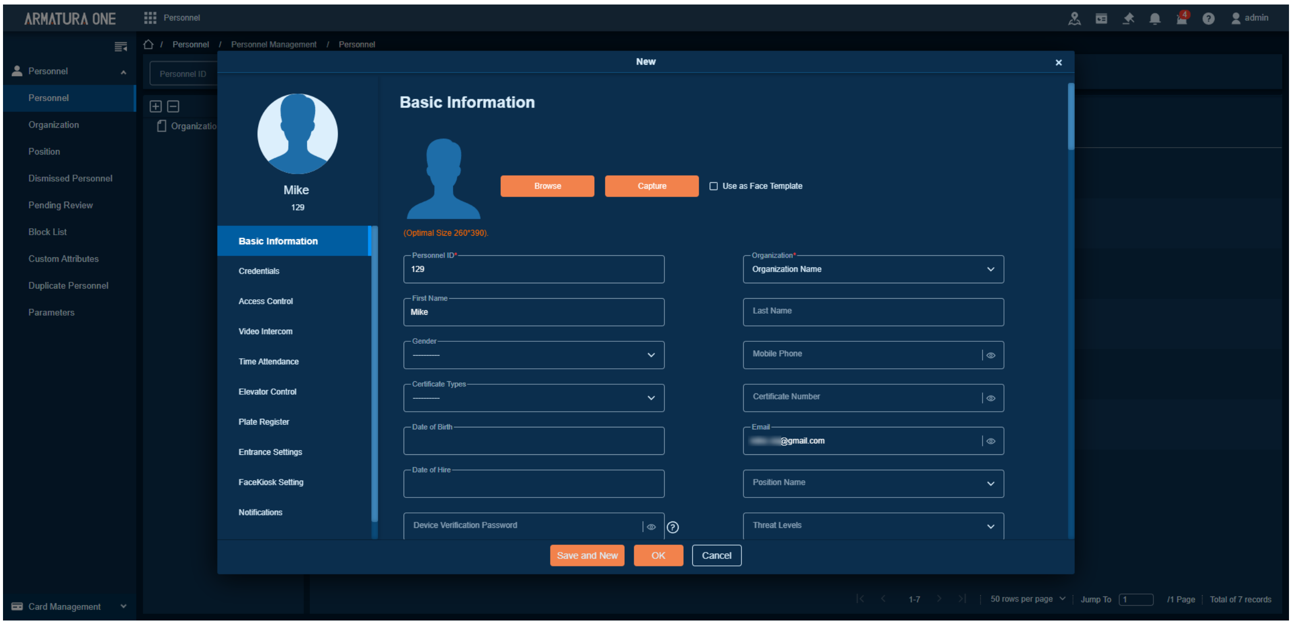
Organization Name*

Sort Order: 99999

Parent Organization

Add the Personnel

1. Click **Personnel > Personnel > Personnel > +New** and enter information about the person in the **Basic information** pop-up.



Basic Information

☐ Use as Face Template

(Optimal Size 260*390).

Personnel ID*: 129

Organization*: Organization Name

First Name: Mike

Last Name

Gender: ---------

Mobile Phone

Certificate Types: ---------

Certificate Number

Date of Birth

Email: [redacted]@gmail.com

Date of Hire

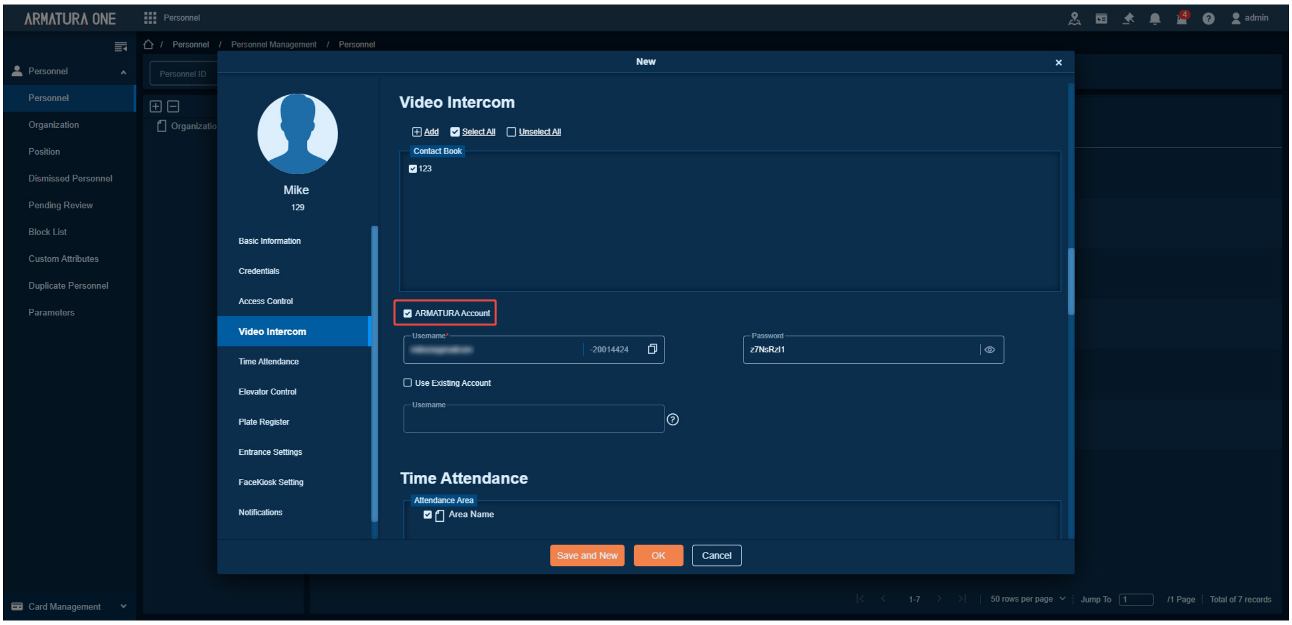
Position Name

Device Verification Password

Threat Levels

2. On the current page, click **ARMATURA Account** on the left side to enable intercom function for the changed user. After clicking **Save and New**, the system will automatically send a message to the new user.

Copyright © 2025 ARMATURA LLC. All rights reserved.



Video Intercom

Contact Book

☑ 123

☑ ARMATURA Account

Username*: [redacted] -20014424

Password: z7NsRzI1

☐ Use Existing Account

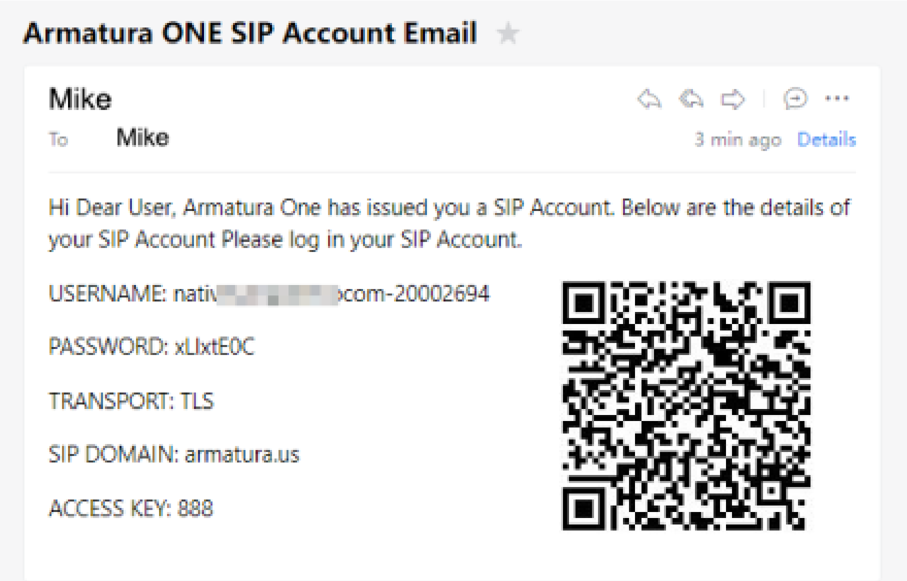
Username:

Time Attendance

Attendance Area

☑ Area Name

3. At this point, the user's e-mail address will receive the account number and password for the video intercom.



Armatura ONE SIP Account Email

Mike

To Mike

3 min ago Details

Hi Dear User, Armatura One has issued you a SIP Account. Below are the details of your SIP Account Please log in your SIP Account.

USERNAME: nativ[redacted]com-20002694

PASSWORD: xLIxtE0C

TRANSPORT: TLS

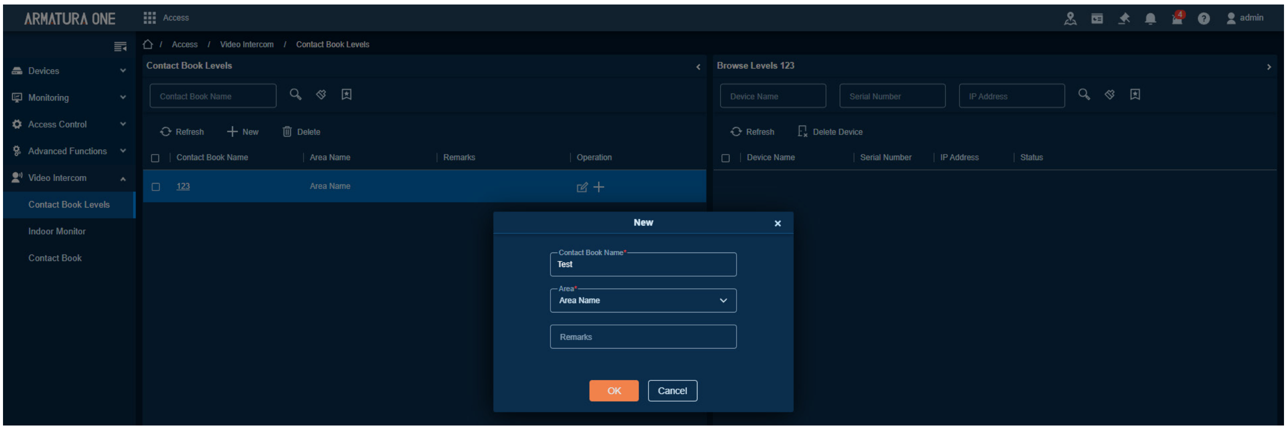
SIP DOMAIN: armatura.us

ACCESS KEY: 888

15.4 Configure Contact Book for the Device

1. On Armatura One, click **Access** > **Video Intercom** > **Contact Book Levels** > **+New**, enter the contact book name. Finally, click **OK**.

Copyright © 2025 ARMATURA LLC. All rights reserved.



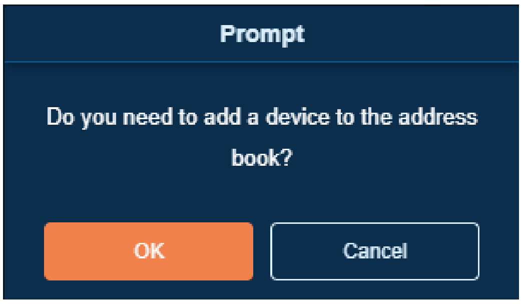
□	Contact Book Name	Area Name	Remarks	Operation
□	123	Area Name		

New

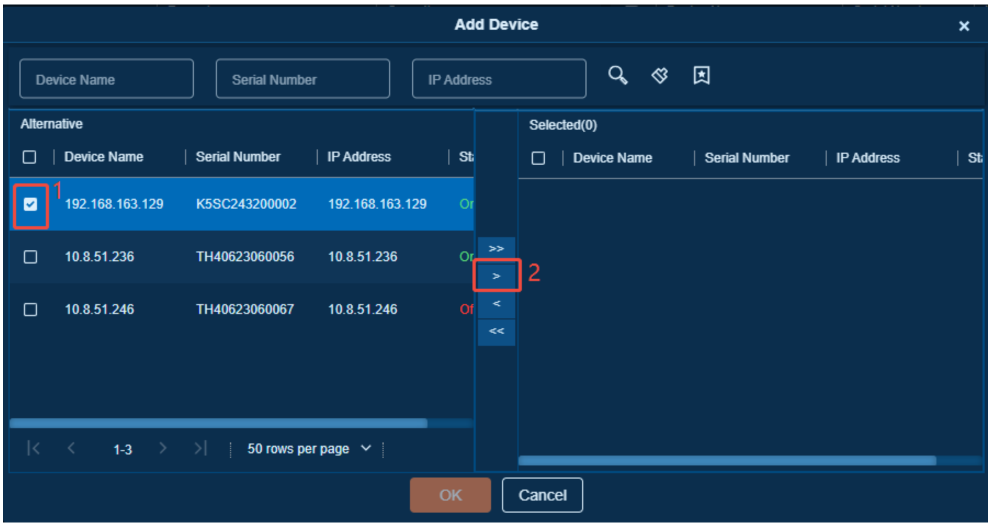
Contact Book Name*: Test

Area*: Area Name

2. On the pop-up page, click **OK** and then select the device you just added.


Prompt

Do you need to add a device to the address book?

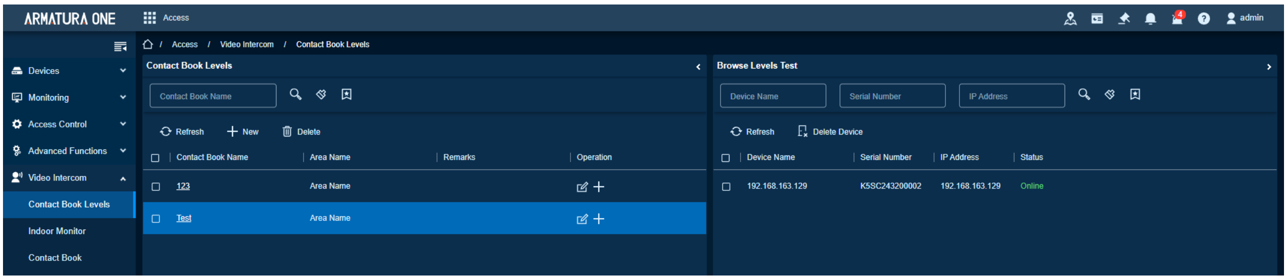

Add Device

Alternative

□	Device Name	Serial Number	IP Address	St
☑	192.168.163.129	K5SC243200002	192.168.163.129	Or
□	10.8.51.236	TH40623060056	10.8.51.236	Or
□	10.8.51.246	TH40623060067	10.8.51.246	Of

Selected(0)

□	Device Name	Serial Number	IP Address	St

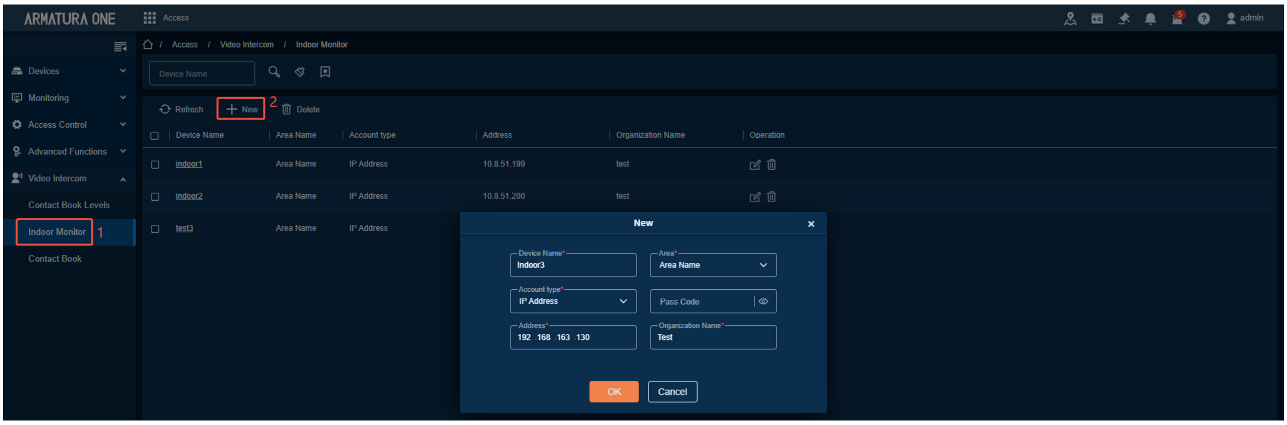


□	Contact Book Name	Area Name	Remarks	Operation
□	123	Area Name		
□	Test	Area Name		

□	Device Name	Serial Number	IP Address	Status
□	192.168.163.129	K5SC243200002	192.168.163.129	Online

3. Click **Indoor Monitor > +New** on the current page. You can manually enter the IP Address or SIP Account of the indoor monitor to add the indoor monitor.

Copyright © 2025 ARMATURA LLC. All rights reserved.

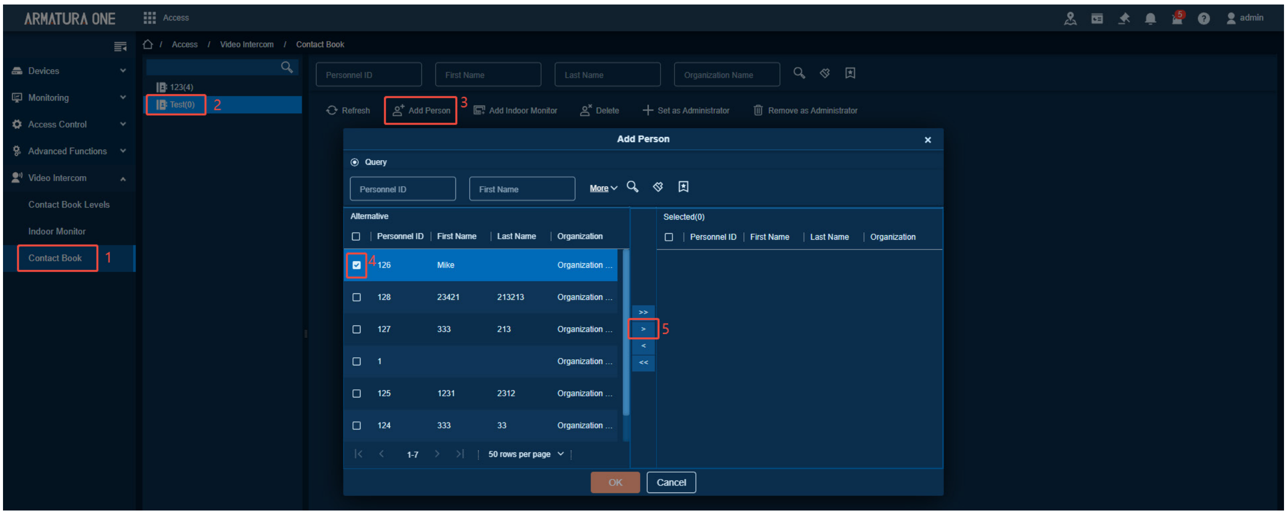


Device Name	Area Name	Account type	Address	Organization Name	Operation
indoor1	Area Name	IP Address	10.8.51.199	test	
indoor2	Area Name	IP Address	10.8.51.200	test	
test3	Area Name	IP Address			

New

Device Name*: Indoor3
Area*: Area Name
Account type*: IP Address
Pass Code
Address*: 192 .168 .163 .130
Organization Name*: Test

4. Click **Contact Book** on the current page to assign video intercom personnel and indoor monitors to the created contact book levels. Personnel and indoor monitors are automatically sent down to the device.

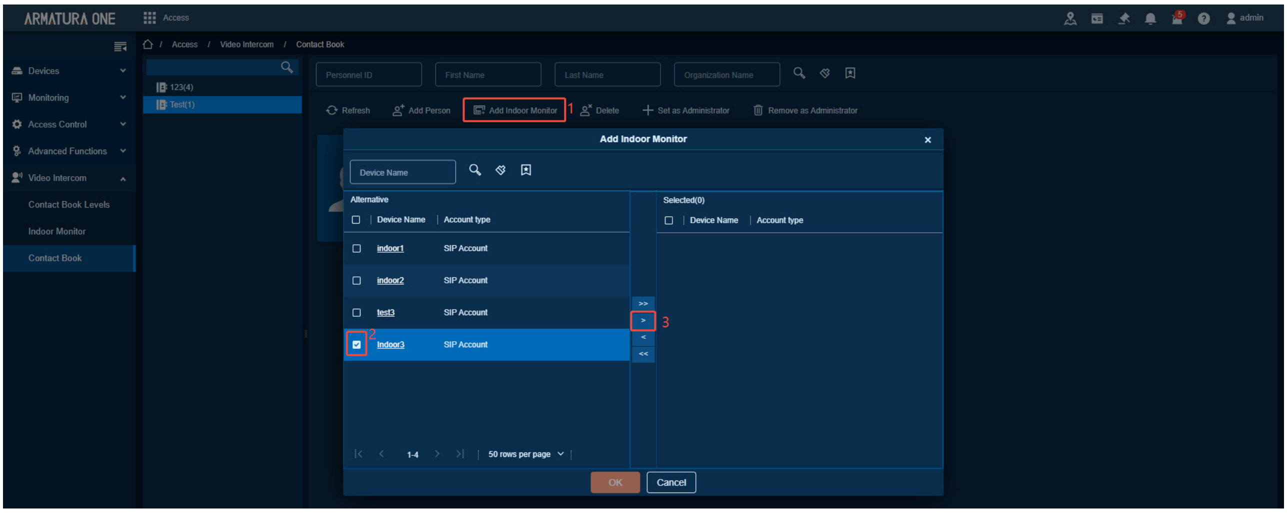


Alternative

Personnel ID	First Name	Last Name	Organization
126	Mike		Organization ...
128	23421	213213	Organization ...
127	333	213	Organization ...
1			Organization ...
125	1231	2312	Organization ...
124	333	33	Organization ...

Selected(0)

Personnel ID	First Name	Last Name	Organization



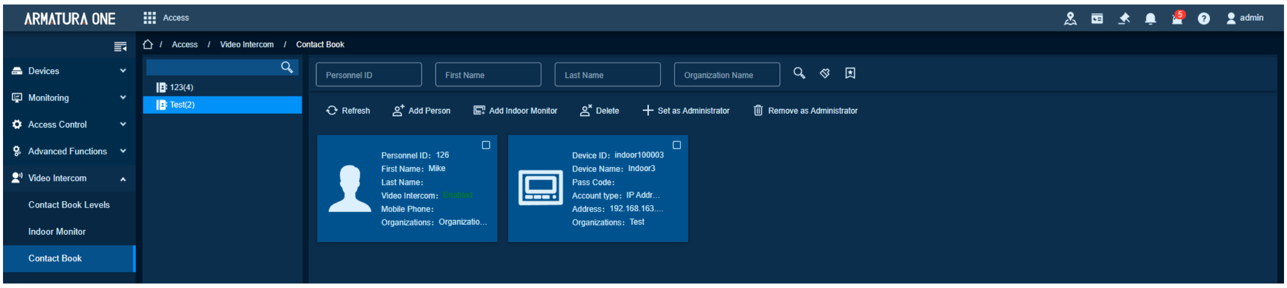
Alternative

Device Name	Account type
indoor1	SIP Account
indoor2	SIP Account
test3	SIP Account
Indoor3	SIP Account

Selected(0)

Device Name	Account type

Copyright © 2025 ARMATURA LLC. All rights reserved.



Personnel ID: 126
First Name: Mike
Last Name:
Video Intercom: Enabled
Mobile Phone:
Organizations: Organizatio...

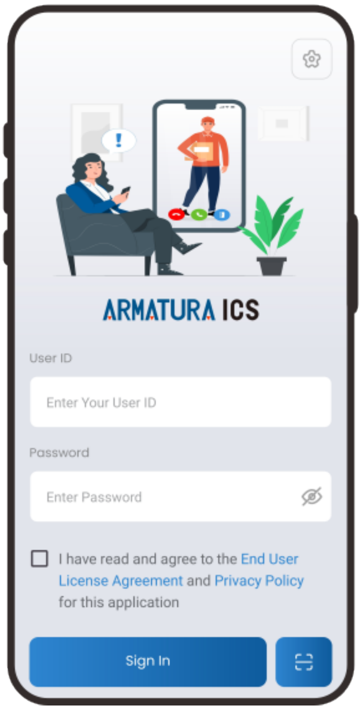
Device ID: indoor100003
Device Name: Indoor3
Pass Code:
Account type: IP Addr...
Address: 192.168.163....
Organizations: Test

15.5 Download and Login the APP

1. Ensure your mobile device is connected to the internet via a mobile or Wi-Fi network.
2. Search for the ARMATURA ICS APP in the Apple APP Store (for iOS devices), Google Play Store (for Android devices) or scan the QR code below to download the APP on your mobile phone.

iOS Android

3. Users can manually enter their video intercom account and password on the ARMATURA ICS APP, or they can choose to scan the code to log in.



□ I have read and agree to the End User License Agreement and Privacy Policy for this application

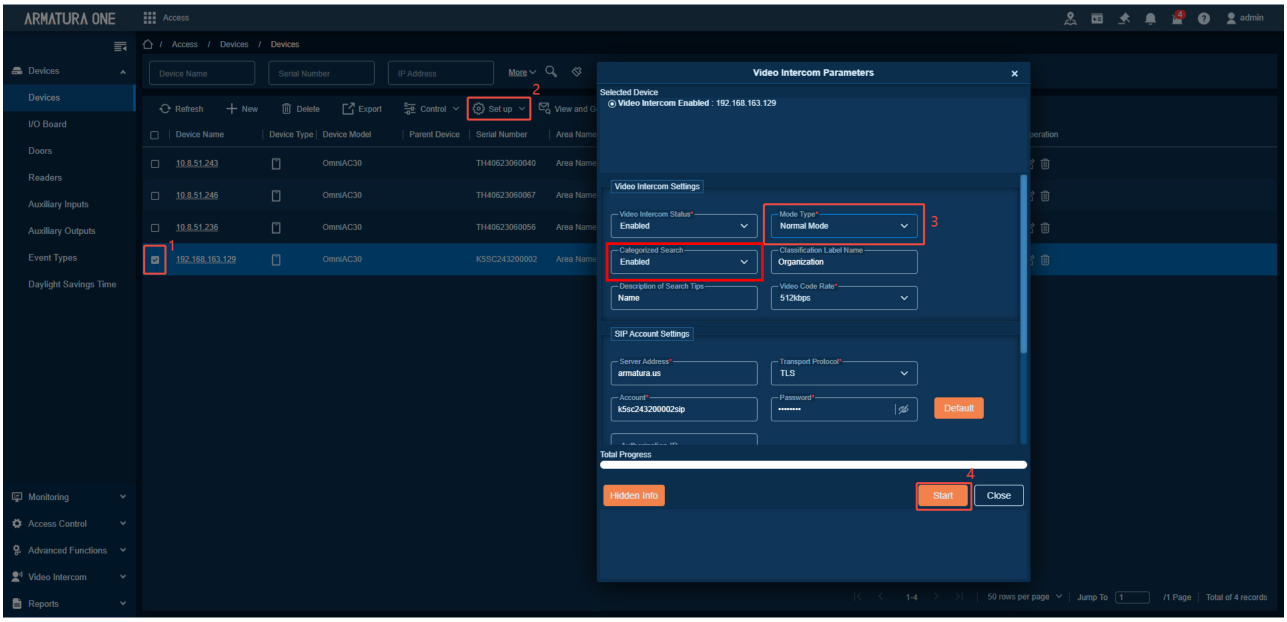
Copyright © 2025 ARMATURA LLC. All rights reserved.

15.6 Device Call the Phone/Indoor Monitor

15.6.1 Normal Mode with Categorization Search Enabled

This mode supports entering numbers, organizations, and names for calling.

1. Click **Access** > **Device** > **Device** > **Set up**> **Video Intercom Parameters** > **Mode Type** > **Normal Mode**, and set the Categorization search as **Enabled**.



☐	Device Name	Device Type	Device Model	Parent Device	Serial Number	Area Name
☐	10.8.51.243		OmniAC30		TH40623060040	Area Name
☐	10.8.51.246		OmniAC30		TH40623060067	Area Name
☐	10.8.51.236		OmniAC30		TH40623060056	Area Name
☑	192.168.163.129		OmniAC30		K5SC243200002	Area Name

Video Intercom Parameters

Selected Device
● Video Intercom Enabled : 192.168.163.129

Video Intercom Settings

Video Intercom Status*: Enabled
Mode Type*: Normal Mode
Categorized Search: Enabled
Classification Label Name: Organization
Description of Search Tips: Name
Video Code Rate*: 512kbps

SIP Account Settings

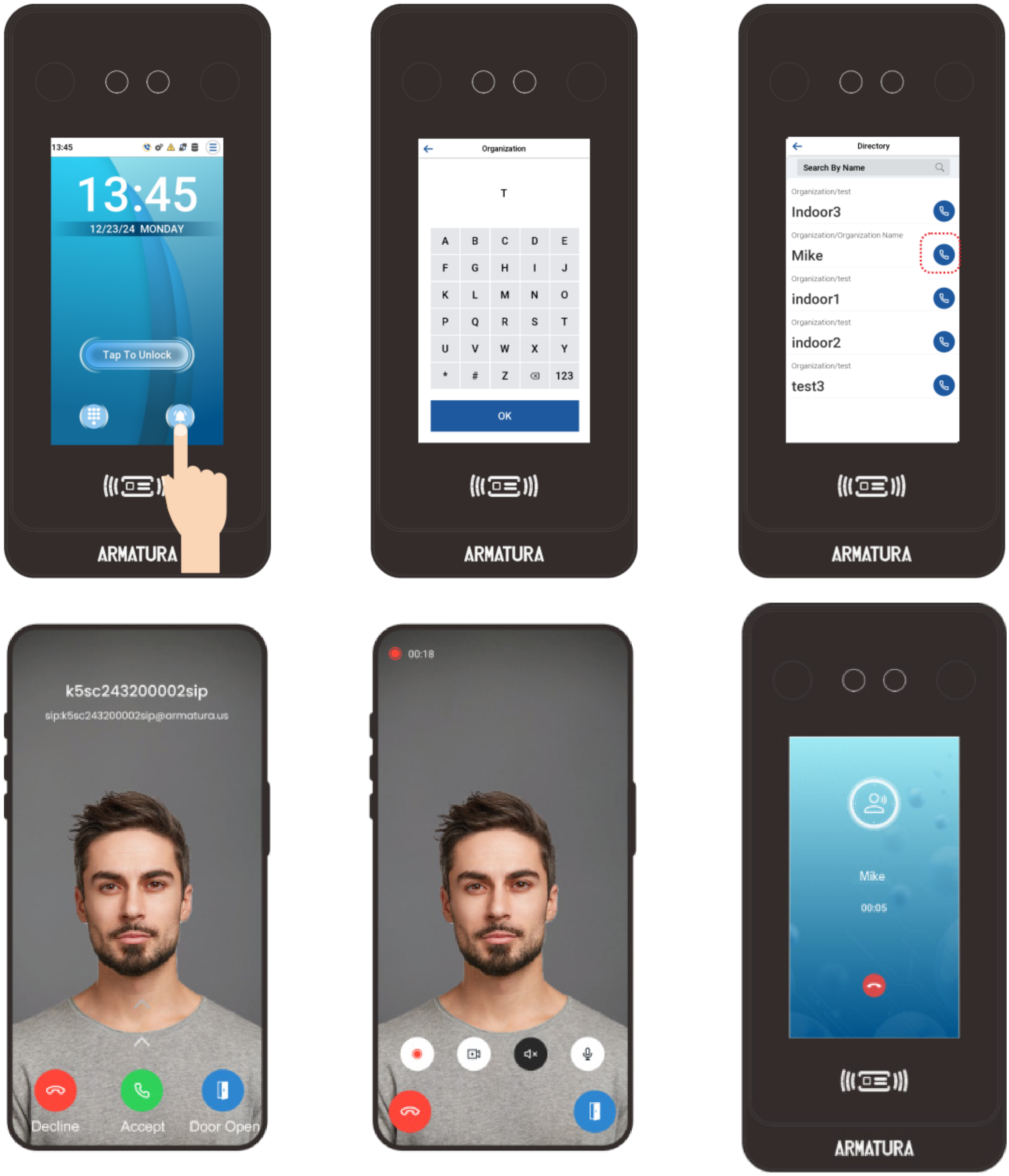
Server Address*: armatura.us
Transport Protocol*: TLS
Account*: k5sc243200002sip
Password*: ••••••••

Total Progress

2. In the standby screen of the device, tap the icon, enter the organization number or name in the pop-up screen. This manual takes inputting the name as an example for illustration, input the organization name, click **OK**, the device will show all the personnel and indoor monitors of the organization, click the icon behind the personnel or indoor monitor to carry out video intercom.

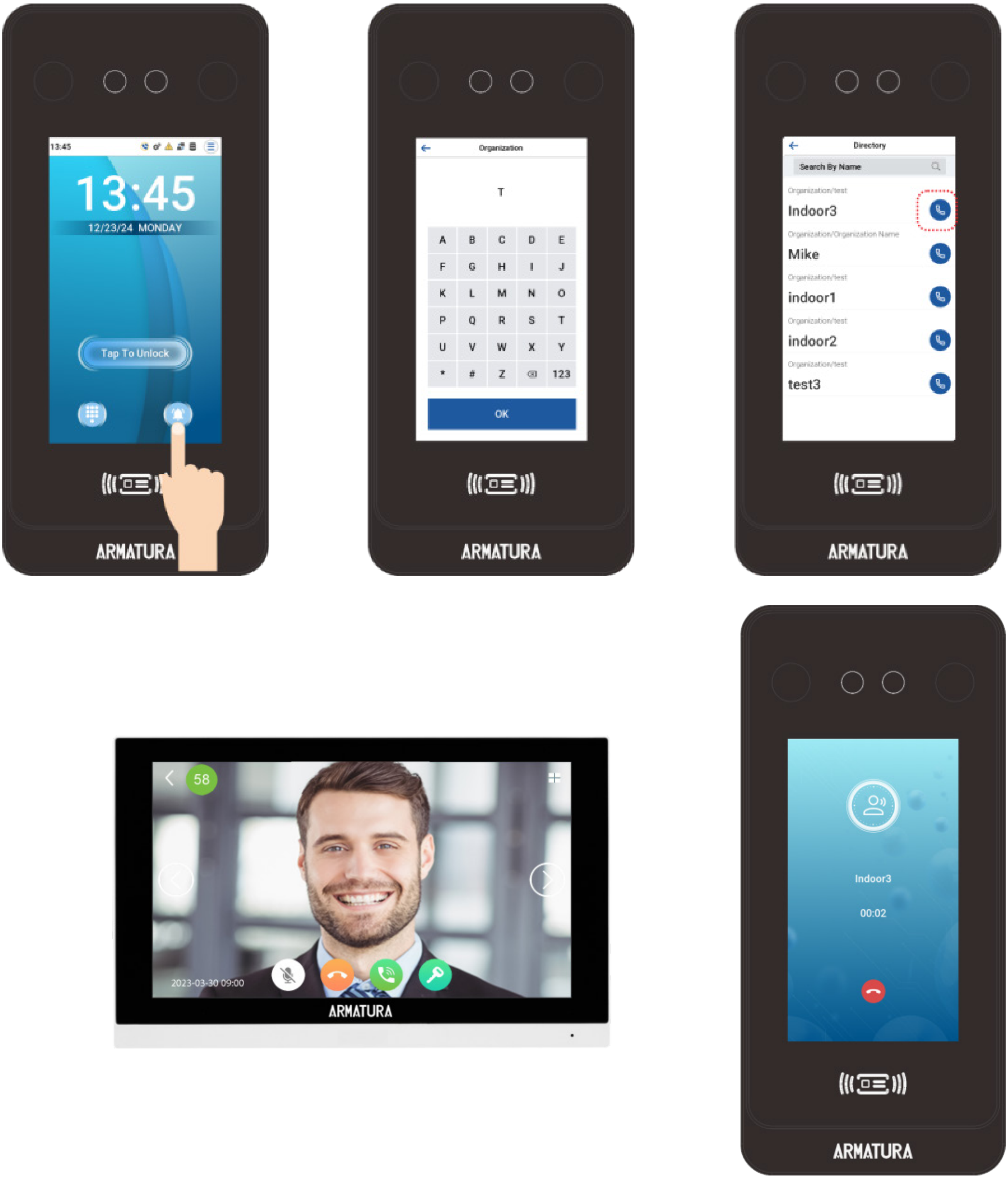
Copyright © 2025 ARMATURA LLC. All rights reserved.

Device call the phone:



Copyright © 2025 ARMATURA LLC. All rights reserved.

Device call the indoor monitor:



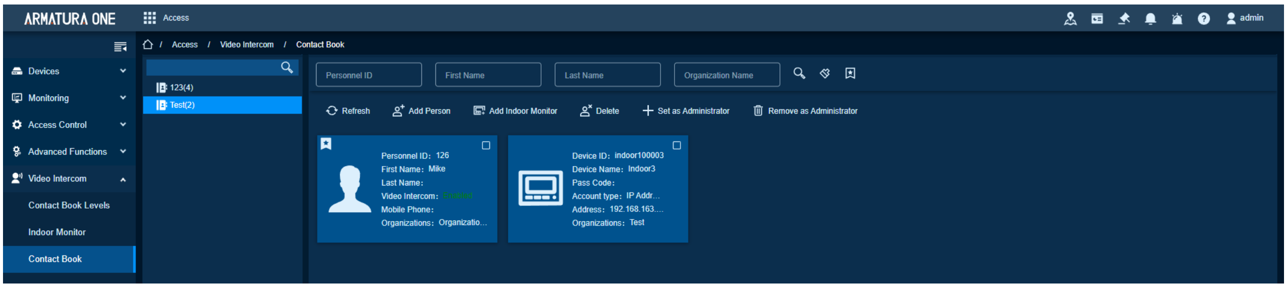
15.6.2 Direct Call Mode

No need to enter a number or organization and name, etc. on the device, tap 🔔 to call directly. The person or indoor monitor needs to be set as administrator on Armatura One.

Copyright © 2025 ARMATURA LLC. All rights reserved.

1. Click **Access** > **Video Intercom** > **Contact Book**, select the person or indoor monitor and click **Set As Administrator**.

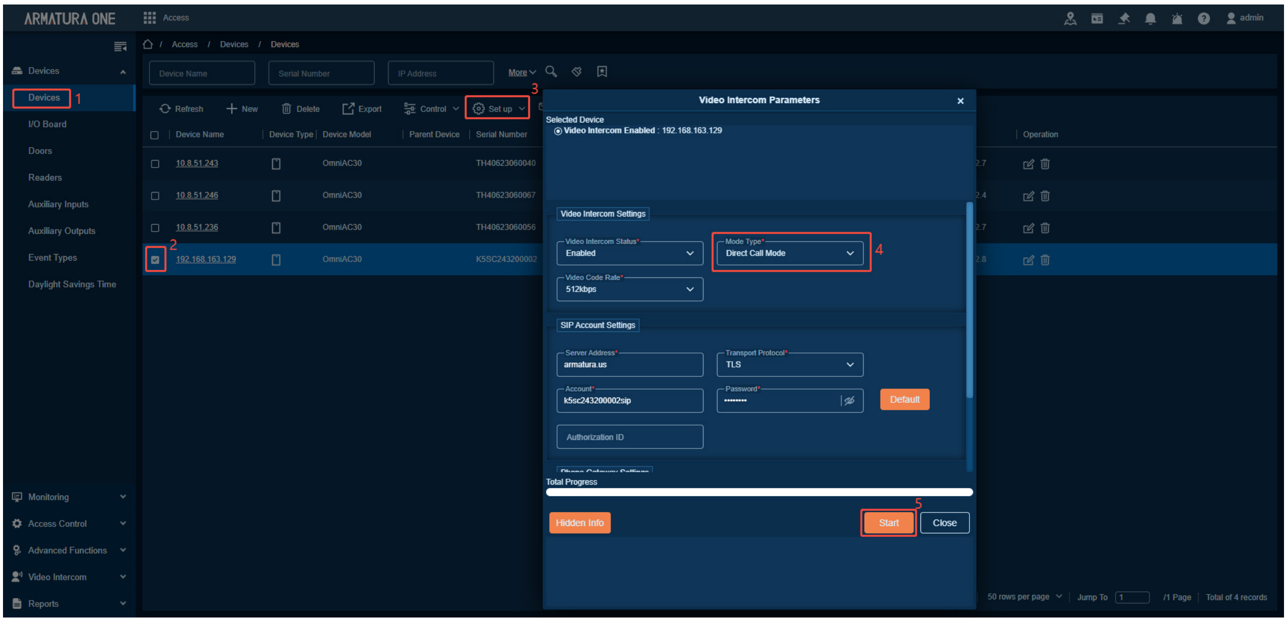
   Note: An address book only supports marking one administrator.



Personnel ID: 126
First Name: Mike
Last Name:
Video Intercom: Enabled
Mobile Phone:
Organizations: Organizatio...

Device ID: indoor100003
Device Name: Indoor3
Pass Code:
Account type: IP Addr...
Address: 192.168.163....
Organizations: Test

2. Then change the calling mode of the device to direct call, click **Access** > **Device** > **Device** > **Set up** > **Video Intercom Parameters** > **Mode Type** > **Direct Call Mode**.



Device Name	Device Type	Device Model	Parent Device	Serial Number
10.8.51.243		OmniAC30		TH40623060040
10.8.51.246		OmniAC30		TH40623060067
10.8.51.236		OmniAC30		TH40623060056
192.168.163.129		OmniAC30		K5SC243200002

Video Intercom Parameters

Selected Device
● Video Intercom Enabled : 192.168.163.129

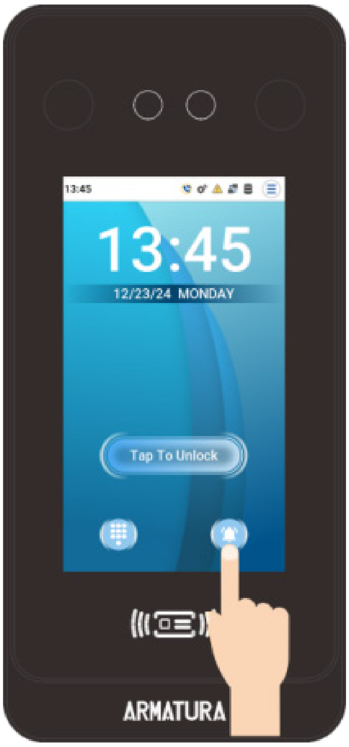
Video Intercom Settings
Video Intercom Status*: Enabled
Mode Type*: Direct Call Mode
Video Code Rate*: 512kbps

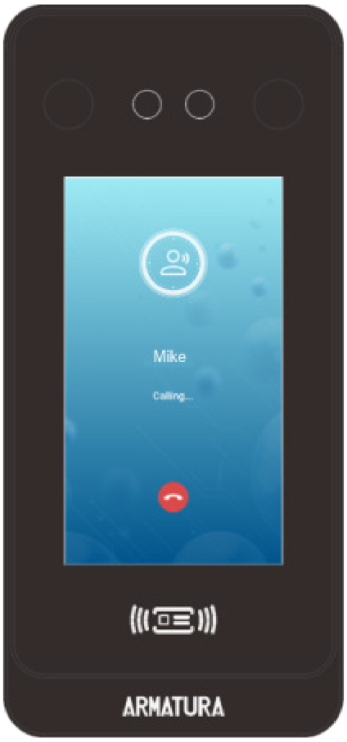
SIP Account Settings
Server Address*: armatura.us
Transport Protocol*: TLS
Account*: k5sc243200002sip
Password*: ••••••••
Authorization ID

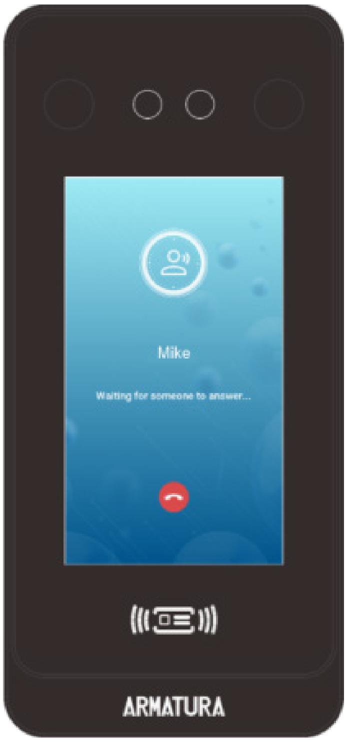
Total Progress

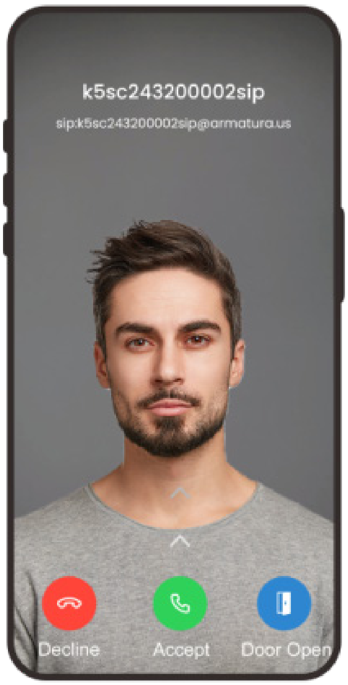
Hidden Info | Default | Start | Close

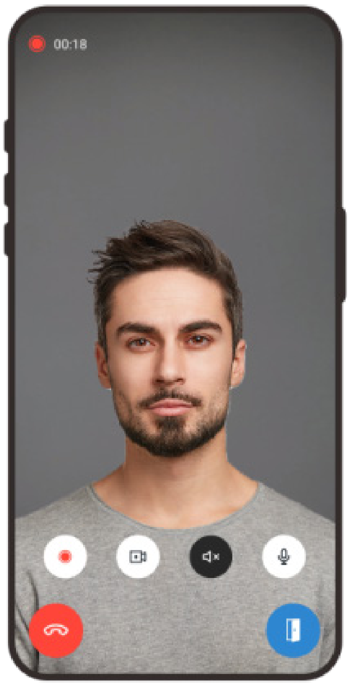
Copyright © 2025 ARMATURA LLC. All rights reserved.

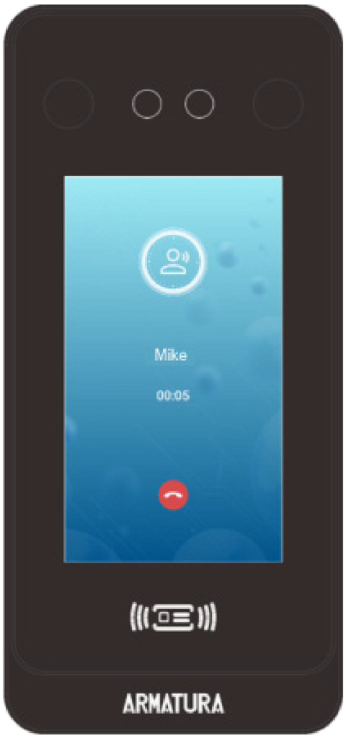








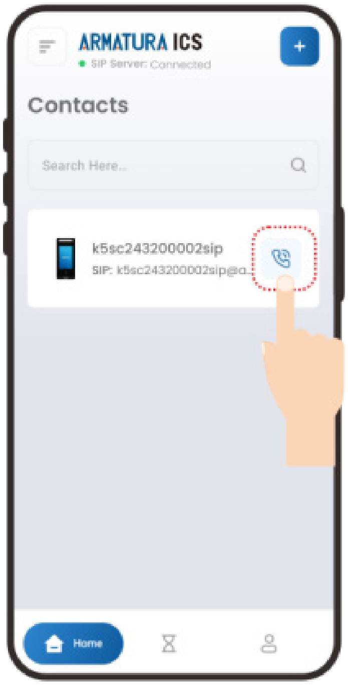


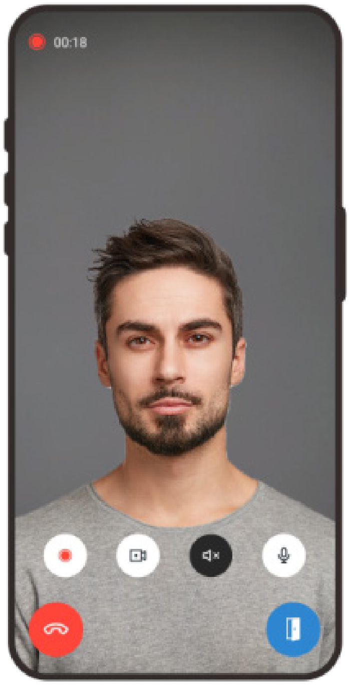


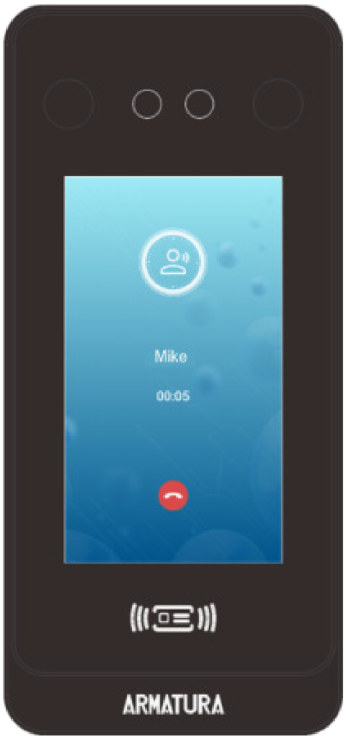
Copyright © 2025 ARMATURA LLC. All rights reserved.

15.7 Phone Call the Device

After the device calling the phone, the device will be automatically saved in the Armatura ICS App, click on the ☎ icon behind the device to perform video intercom with the device.







ARMATURA ICS APP

Function Name	Description
☎	Dialing key.
🔴	It is the Hang up key. After hanging up, immediately end the current call.
🟢	It is the answer key, the user can tap to answer the current call. After answering, enter the window during the call, and turn on audio and video by default.
🔵	It is the Remote Open key, used to open the door remotely. The default lock drive time is 5 seconds.
◉	Record video button, support to record current screen.
▣	Turning it off prevents you from seeing the live feed captured by the device's camera.
🔇	Speaker key, turn on to receive sound from the device.

Copyright © 2025 ARMATURA LLC. All rights reserved.

🎙	Microphone key, turn on for voice intercom.

Device

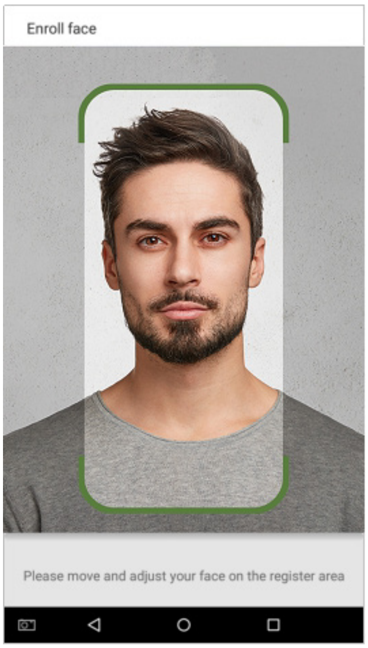
Function Name	Description
☎	It is the Hang up key. After hanging up, immediately end the current call.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Appendix 1

Requirements for Live Collection and Registration of Visible Light Face Templates

1) It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.
2) Do not shoot towards outdoor light sources like door or window or other strong light sources.
3) Dark-color apparels which are different from the background color are recommended for registration.
4) Please show your face and forehead, and do not cover your face and eyebrows with your hair.
5) It is recommended to show a plain facial expression. Smile is acceptable, but do not close your eyes, or incline your head to any orientation. Two images are required for persons with eyeglasses, one image with eyeglasses and one other without.
6) Do not wear accessories like scarf or mask that may cover your mouth or chin.
7) Please face right towards the capturing device, and locate your face in the image capturing area as shown in Image 1.
8) Do not include more than one face in the capturing area.
9) 19.69 to 31.5inch (50 to 80cm) is recommended for capturing distance adjustable subject to body height.



Please move and adjust your face on the register area

Image1 Face Capture Area

Copyright © 2025 ARMATURA LLC. All rights reserved.

Requirements for Visible Light Digital Face Template Data

Digital photo should be straightly edged, colored, half-portrayed with only one person, and the person should be uncharted and not in uniform. Persons who wear eyeglasses should remain to put on eyeglasses for photo capturing.

- Eye Distance

200 pixels or above are recommended with no less than 115 pixels of distance.

- Facial Expression

Plain face or smile with eyes naturally open are recommended.

- Gesture and Angle

Horizontal rotating angle should not exceed ±10°, elevation should not exceed ±10°, and depression angle should not exceed ±10°.

- Accessories

Masks and colored eyeglasses are not allowed. The frame of the eyeglasses should not shield eyes and should not reflect light. For persons with thick eyeglasses frame, it is recommended to capture two images, one with eyeglasses and the other one without.

- Face

Complete face with clear contour, real scale, evenly distributed light, and no shadow.

- Image Format

Should be in BMP, JPG or JPEG.

- Data Requirement

Should comply with the following requirements:

1) White background with dark-colored apparel.
2) 24bit true color mode.
3) JPG format compressed image with not more than 20kb size.
4) Definition rate between 358 x 441 to 1080 x 1920.
5) The vertical scale of head and body should be 2:1.
6) The photo should include the captured person's shoulders at the same horizontal level.
7) The captured person should be eyes-open and with clearly seen iris.
8) Plain face or smile is preferred, showing teeth is not preferred.
9) The captured person should be clearly seen, natural in color, and without image obvious twist, no shadow, light spot or reflection in face or background, and appropriate contrast and lightness level.

Copyright © 2025 ARMATURA LLC. All rights reserved.

Appendix 2

Privacy Policy

Notice:

To help you better use the products and services of Armatura LLC, and its affiliates, hereinafter referred 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**

Copyright © 2025 ARMATURA LLC. All rights reserved.

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.

Copyright © 2025 ARMATURA LLC. All rights reserved.

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.

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)	Hexavalen t Chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

Copyright © 2025 ARMATURA LLC. All rights reserved.

This table is prepared in accordance with the provisions of SJ/T 11364.

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in GB/T 26572.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in GB/T 26572.

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.

Copyright © 2025 ARMATURA LLC. All rights reserved.

FCC Warning

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.

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.

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.

FCC RF Radiation Exposure Statement:

- This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This equipment should be installed and operated with a minimum distance of 7.87 inch (20 cm) between the radiator and your body.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IMPORTANT! Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Copyright © 2025 ARMATURA LLC. All rights reserved.

ARMATURA

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

Copyright © 2025 ARMATURA LLC. All rights reserved.