DS-KD-MFB Series Fingerprint & Card Reader Module

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE

PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

Warning

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Caution

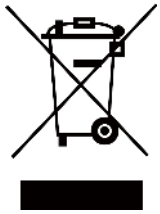
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.

- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type. If a power adapter is provided in the device package, use the provided adapter only.
- If no power adapter is provided, ensure the power adapter or other power supply complies with Limited Power Source. Refer to the product label for the power supply output parameters.

Regulatory Information

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

About this Manual

Get the manual and related software from or the official website (http://www.hikvision.com).

Product	Model
Module Door Station (Sub Module)	DS-KD-MFB
Module Door Station (Sub Module)	DS-KD-MFB/S

Contents

Chapter 1 Appearance

Fingerprint&Card Reader Module

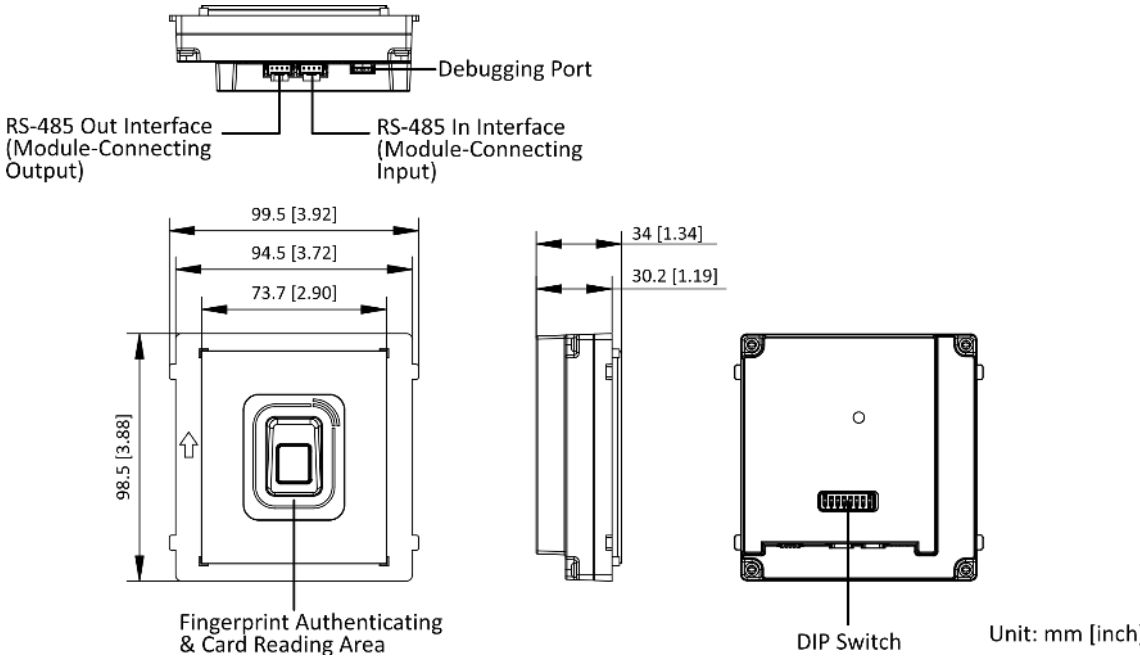


Figure 1-1 Fingerprint&Card Reader Module Appearance

Note

- The pictures here are for reference only.
- RS-485 interfaces are for module-connecting.
- The debugging port is for debugging use only.
- The device can be used for cascading. To avoid the risk of overload in the preceding power supply, it is necessary to use it in combination according to the output limit of the main unit.

Chapter 2 Configuration Flow of the Fingerprint & Card Reader Module

You can configure the fingerprint & card reader module through the following flow.

Table 2-1 Configuration Flow of the Fingerprint & Card Reader Module

Configuration Steps	Details
1. Set sub module address of the fingerprint & card reader module	Please refer to: ***Configure Sub Module Address***
2. Wiring and Installation of the Fingerprint & Card Reader Module	Please refer to: • ***Terminal and Wiring*** • ***Installation***
3. Configure the Fingerprint & Card Reader Module via the Web Client of the Main Unit or Client Software	• Configure the Fingerprint & Card Reader Module via Web 4.0: ***Configuration via Web 4.0*** • Configure the Fingerprint & Card Reader Module via PC Web 5.0 or Mobile Web: ***Configuration via PC Web 5.0 or Mobile Web*** • Configure the Fingerprint & Card Reader Module via Client Software: ***Configuration via Client Software of the Main Unit***
Unlock Door via Fingerprint & Card Reader Module	Please refer to: ***Unlock Door***

Chapter 3 Configure Sub Module Address

You need to set the sub module address via DIP switch before installation.

Steps

1. Remove the rubber cover on the rear panel of the sub module to expose the DIP switch.

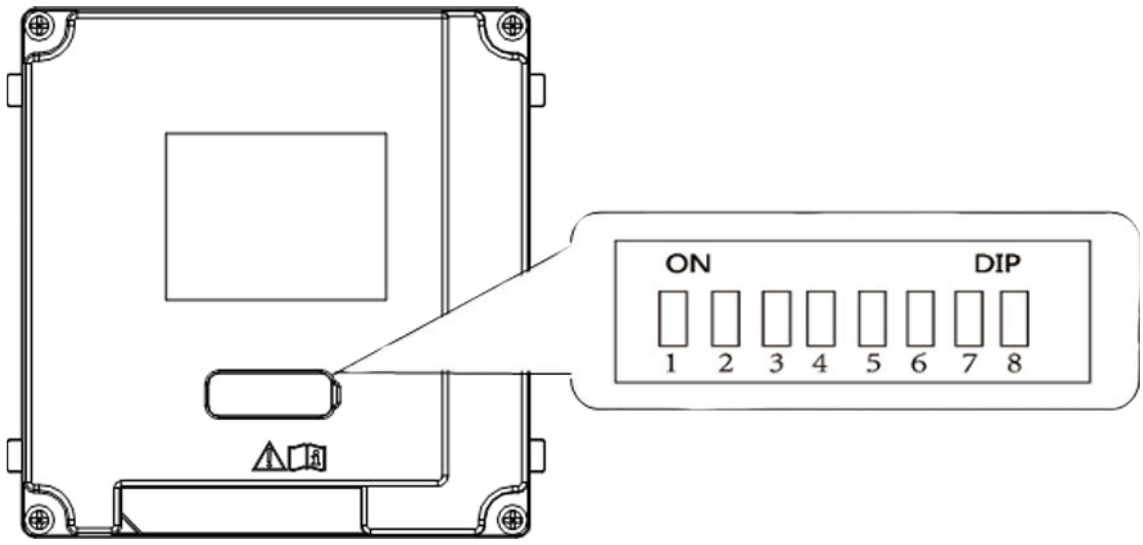


Figure 3-1 DIP Switch

2. Set the sub module address according to the DIP rules, and install the rubber cover back.

Note

- Valid sub module address is from 1 to 20. The address should be unique for connecting to the main unit.
  The sub module address and its corresponding switch status are displayed as below.

Sub Module Address	DIP 1	DIP 2	DIP 3	DIP 4	DIP 5	DIP 6	DIP 7	DIP 8
Module 1	ON	OFF	OFF	OFF	OFF	OFF	OFF	OFF
Module 2	OFF	ON	OFF	OFF	OFF	OFF	OFF	OFF
Module 3	ON	ON	OFF	OFF	OFF	OFF	OFF	OFF
Module 4	OFF	OFF	ON	OFF	OFF	OFF	OFF	OFF
Module 5	ON	OFF	ON	OFF	OFF	OFF	OFF	OFF
Module 6	OFF	ON	ON	OFF	OFF	OFF	OFF	OFF

Sub Module Address	DIP 1	DIP 2	DIP 3	DIP 4	DIP 5	DIP 6	DIP 7	DIP 8
Module 7	ON	ON	ON	OFF	OFF	OFF	OFF	OFF
Module 8	OFF	OFF	OFF	ON	OFF	OFF	OFF	OFF

Chapter 4 Terminal and Wiring

4.1 Terminals

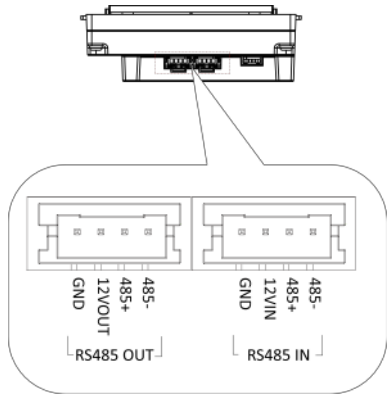


Figure 4-1 RS-485 Module-Connecting Interfaces

4.2 Module Door Station Wiring

4.2.1 Wiring with the Main Unit

The fingerprint & card reader module can connect to IP module door station (main unit) and Two-Wire module door station via RS-485 module-connecting interfaces. After connecting with the main unit, you need to go to the Web Client of the main unit to add fingerprint and card information. After the setting, you can authenticate via fingerprint or swipe card to unlock the door. For more information about setting call buttons, please refer to **Configuration and Operations** chapter.

Note

For more information about setting call buttons, please refer to **Configuration and Operations** chapter. ***Configuration and Operation***

Wiring with IP Module Door Station

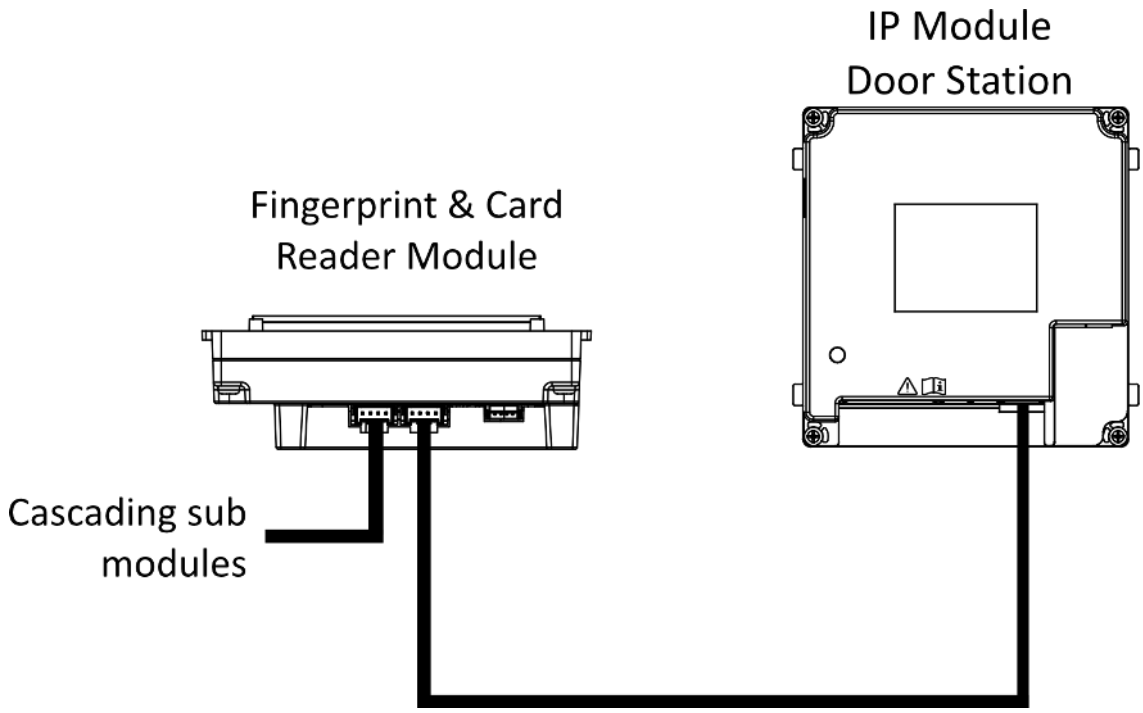


Figure 4-2 Wiring with IP Module Door Station

Wiring with Two-Wire Module Door Station

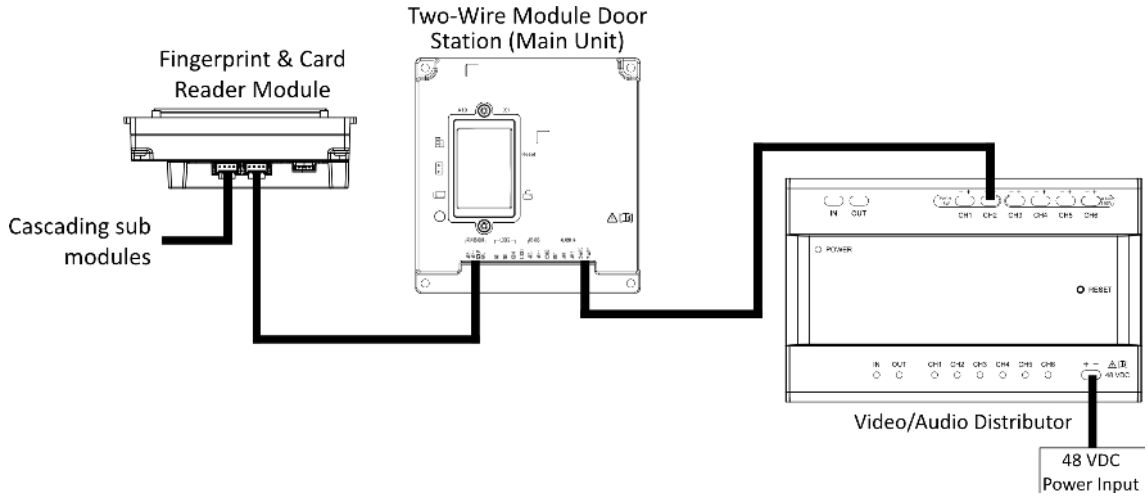


Figure 4-3 Wiring with Two-Wire Module Door Station

Chapter 5 Installation

Note

- The sub module supports two-module and three-module installation. Here takes three-module installation as an example, the two-module installation shares the same approach as the three module installation.
- Sub module must work along with the main unit.
- Sub modules share the same approach of the installation. The sub modules in installation images are for reference only.
- Make sure the device in the package is in good condition and all the assembly parts are included.
- Set the sub module address before start the installation steps.
- Make sure the place for surface mounting is flat.
- Make sure all the related equipment is power-off during the installation.
- Tools that you need to prepare for installation:
  Drill (ø6), cross screwdriver (PH1*150 mm), and gradienter.

5.1 Surface Mounting

Before You Start

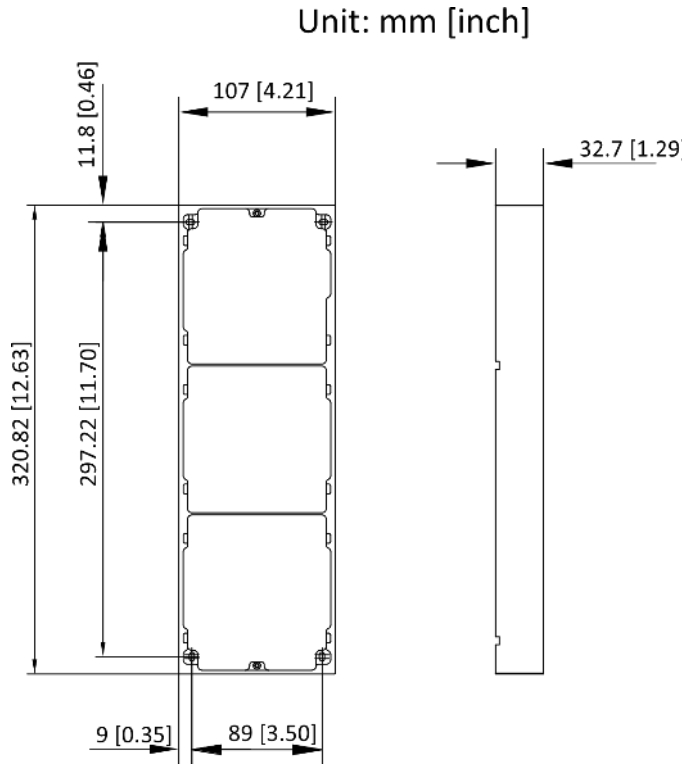


Figure 5-1 Mounting Frame

Note

- The suggested depth of the installation hole is 33 mm.
- The dimensions above are for reference only. The actual size can be slightly different from the theoretical dimension.

Steps

1. Stick the mounting sticker to the wall. The suggested length of cables left outside is 270 mm.

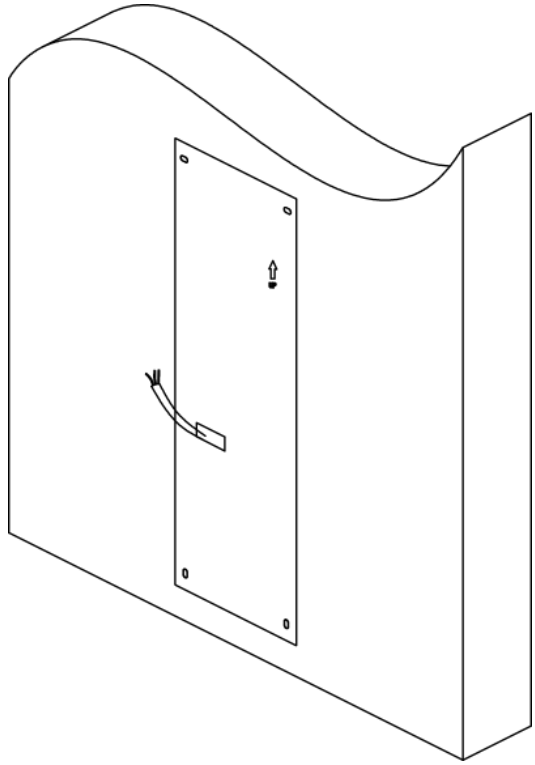


Figure 5-2 Stick the Sticker

2. Drill 4 holes of 25 mm deep according to the marks on the sticker and insert the expansion sleeves into the screw holes. Remove the mounting sticker and fix the mounting frame to the wall with 4 expansion bolts.

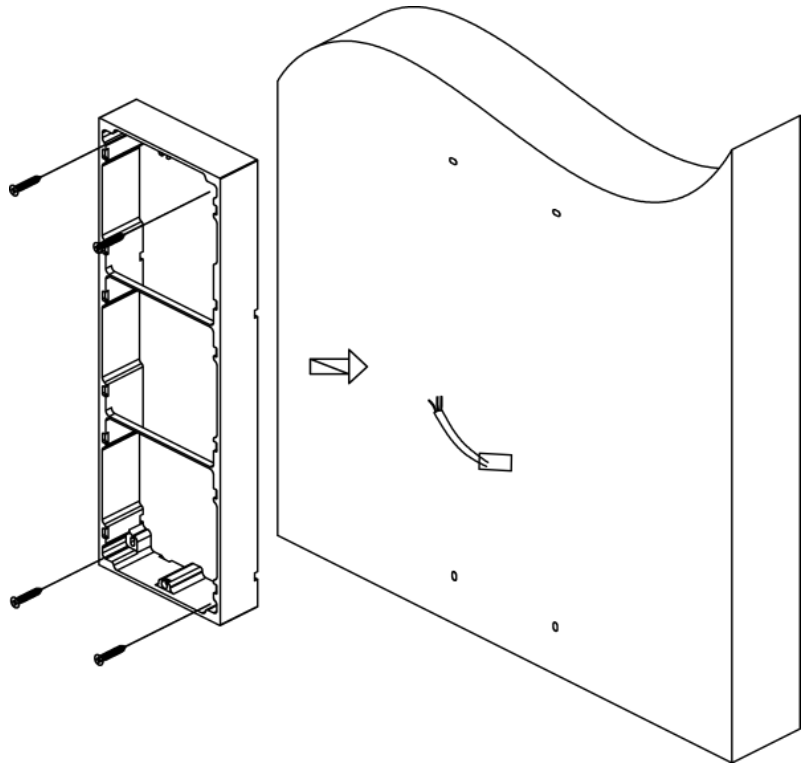


Figure 5-3 Fix the Mounting Frame

3. Thread the module-connecting line across the thread holes of the frame.

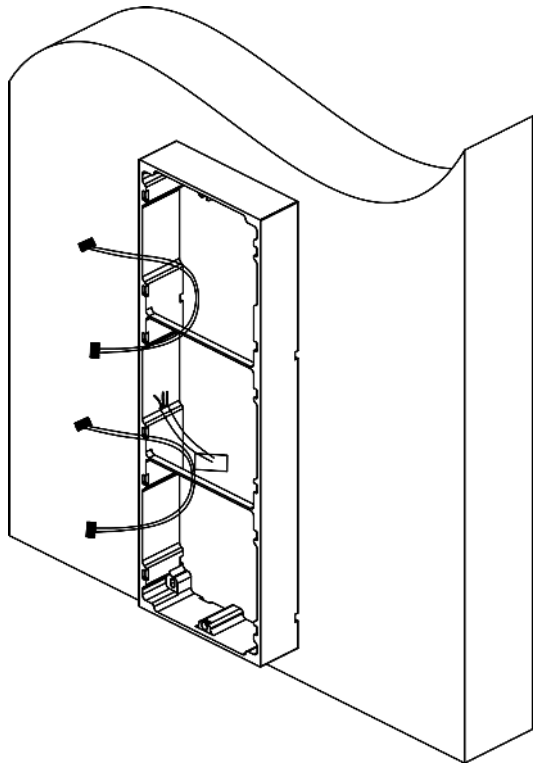


Figure 5-4 Thread the Module-Connecting Line

4. Pass the main unit connecting line across the thread hole to the top grid and connect the cables. Insert the modules into the frame after wiring. The main unit must be placed in the top grid.

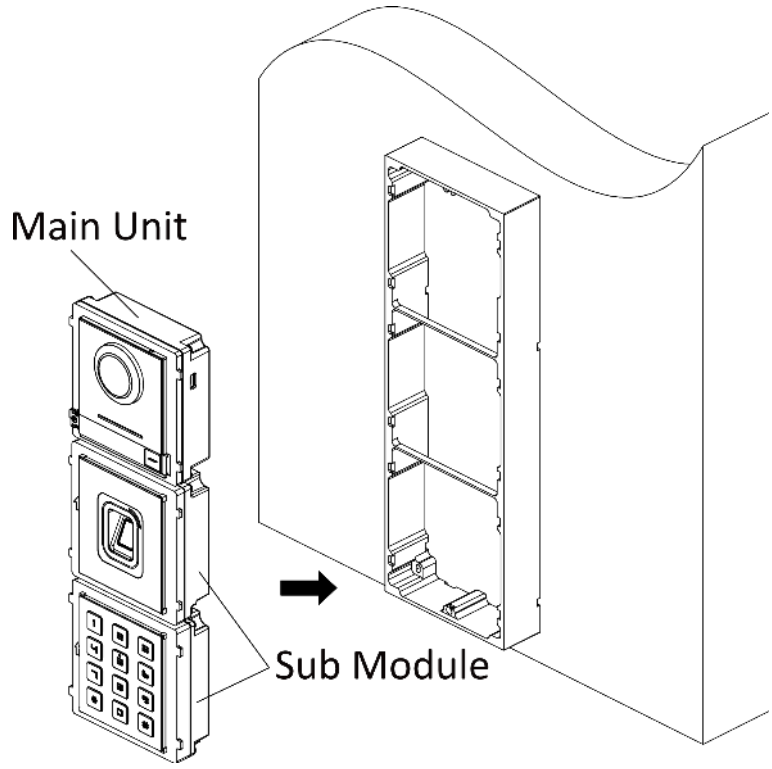


Figure 5-5 Fix Modules to the Frame

5. Apply silicone sealant among the cable wiring area to keep the raindrop from entering.

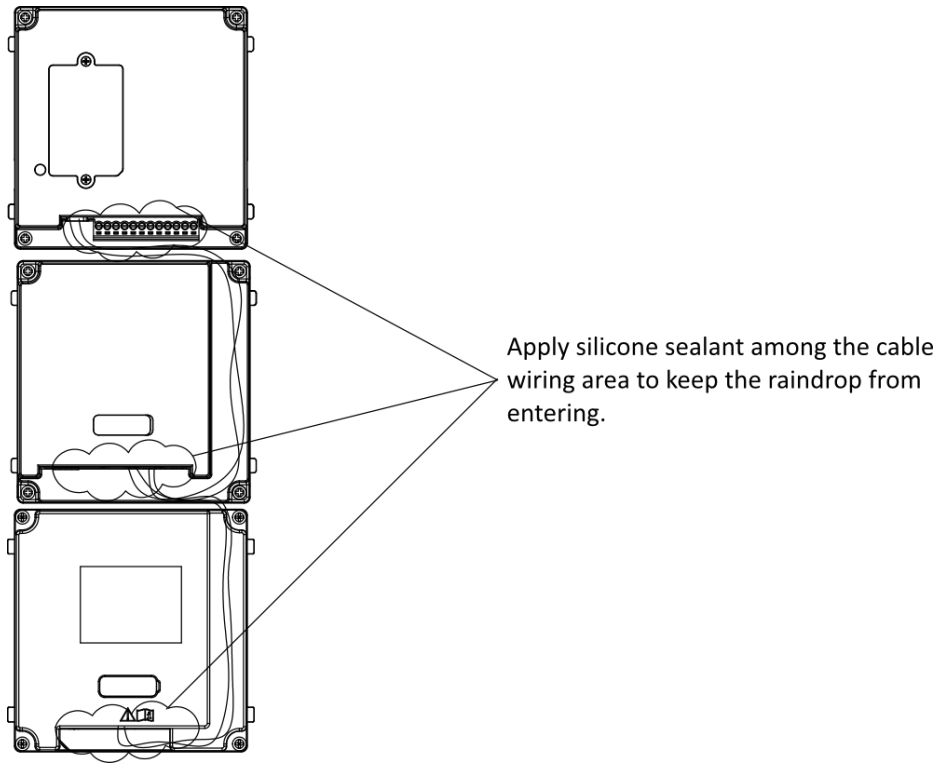


Figure 5-6 Apply Silicone Sealant

6. Use the hexagon wrench in the package to fix the cover onto the frame.

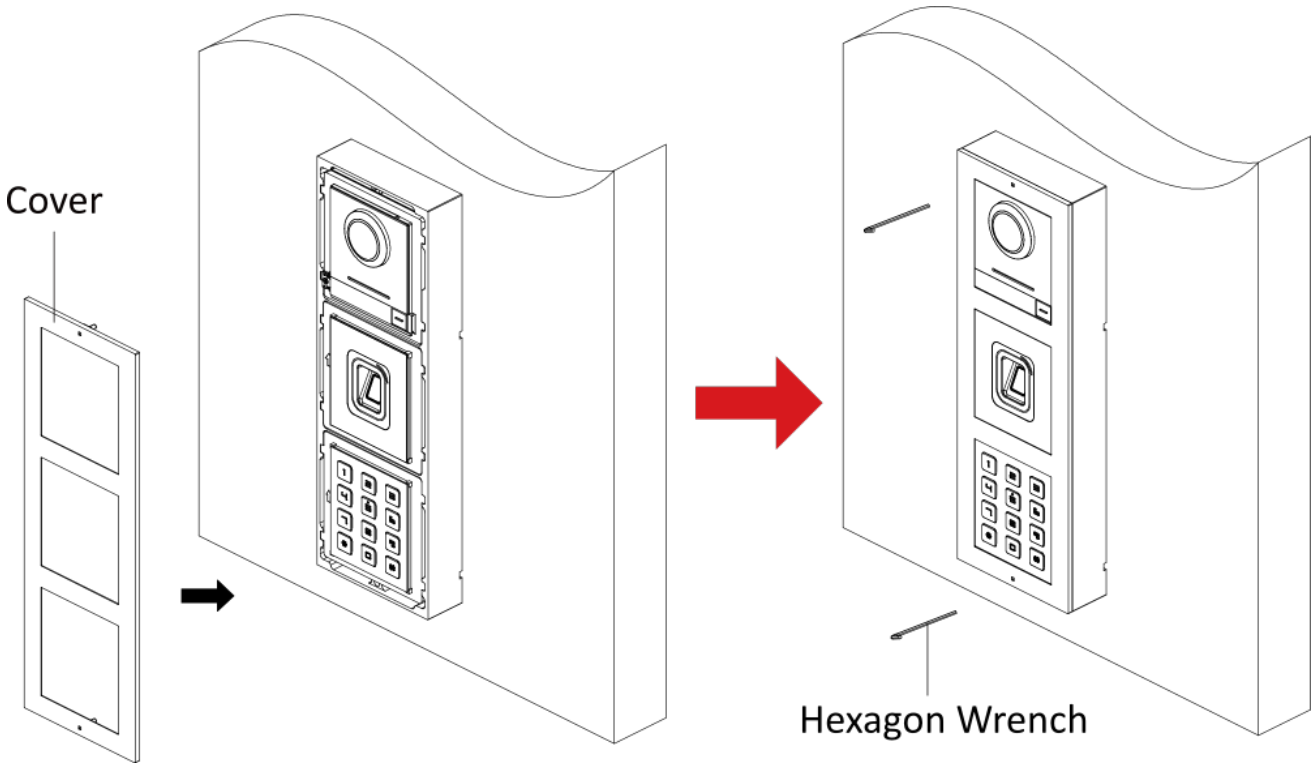


Figure 5-7 Fix the Cover

5.2 Flush Mounting

Before You Start

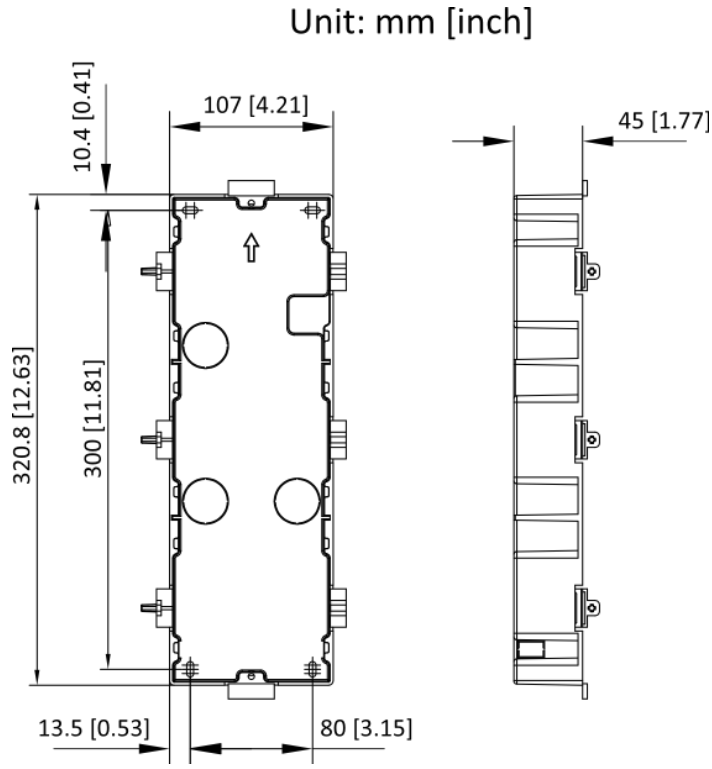


Figure 5-8 Mounting Box

Note

The dimensions above are for reference only. The actual size can be slightly different from the theoretical dimension.

Steps

1. Stick the mounting sticker to the wall and cave the installation hole according to the sticker. Pull the cable out. Stick the mounting sticker to the installation hole and drill 4 holes of 25 mm deep according to the marks on the sticker and insert the expansion sleeves into the screw holes.

   Note

   - The suggested depth of the hole is 44.5 mm.
   - The suggested length of cables left outside is 270 mm.

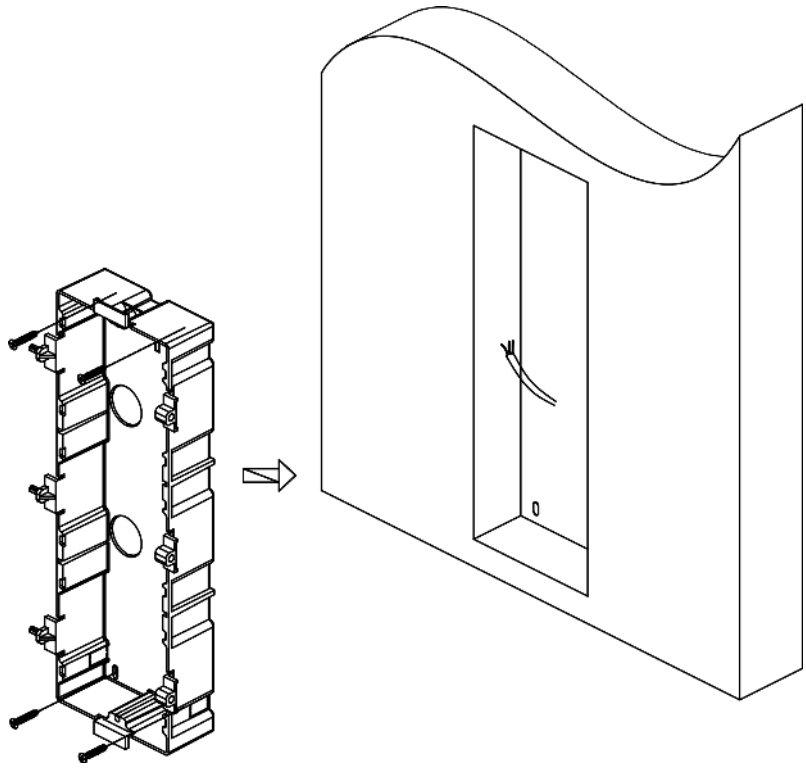


Figure 5-9 Drill the Installation Hole

2. Fix the mounting box to the installation with 4 expansion bolts. Remove the positioning piece of the mounting box.

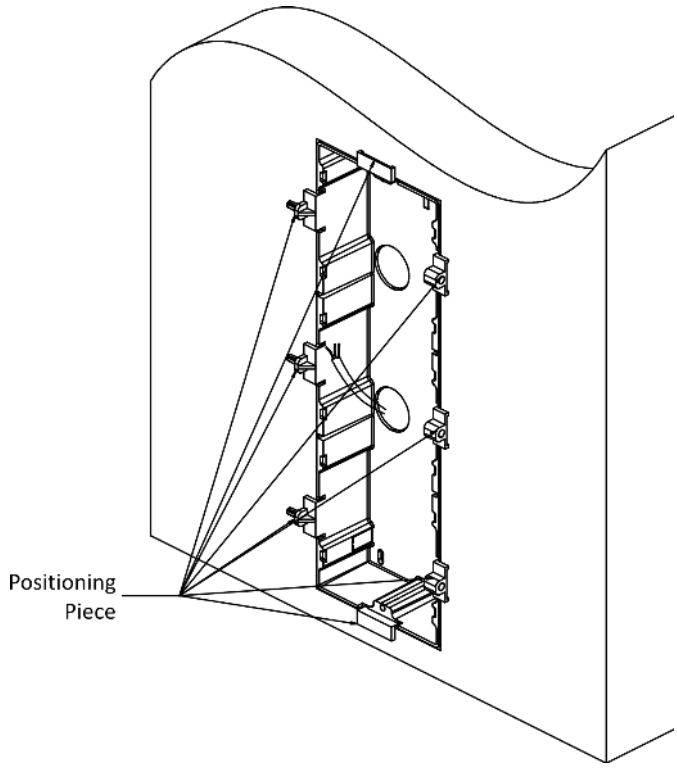


Figure 5-10 Fix the Mounting Box

3. Connect cables of the main unit and other modules and insert the modules to the mounting box.

Note

Apply silicone sealant on the top and sides of the mounting box. Do not apply silicone sealant on the bottom of the box.

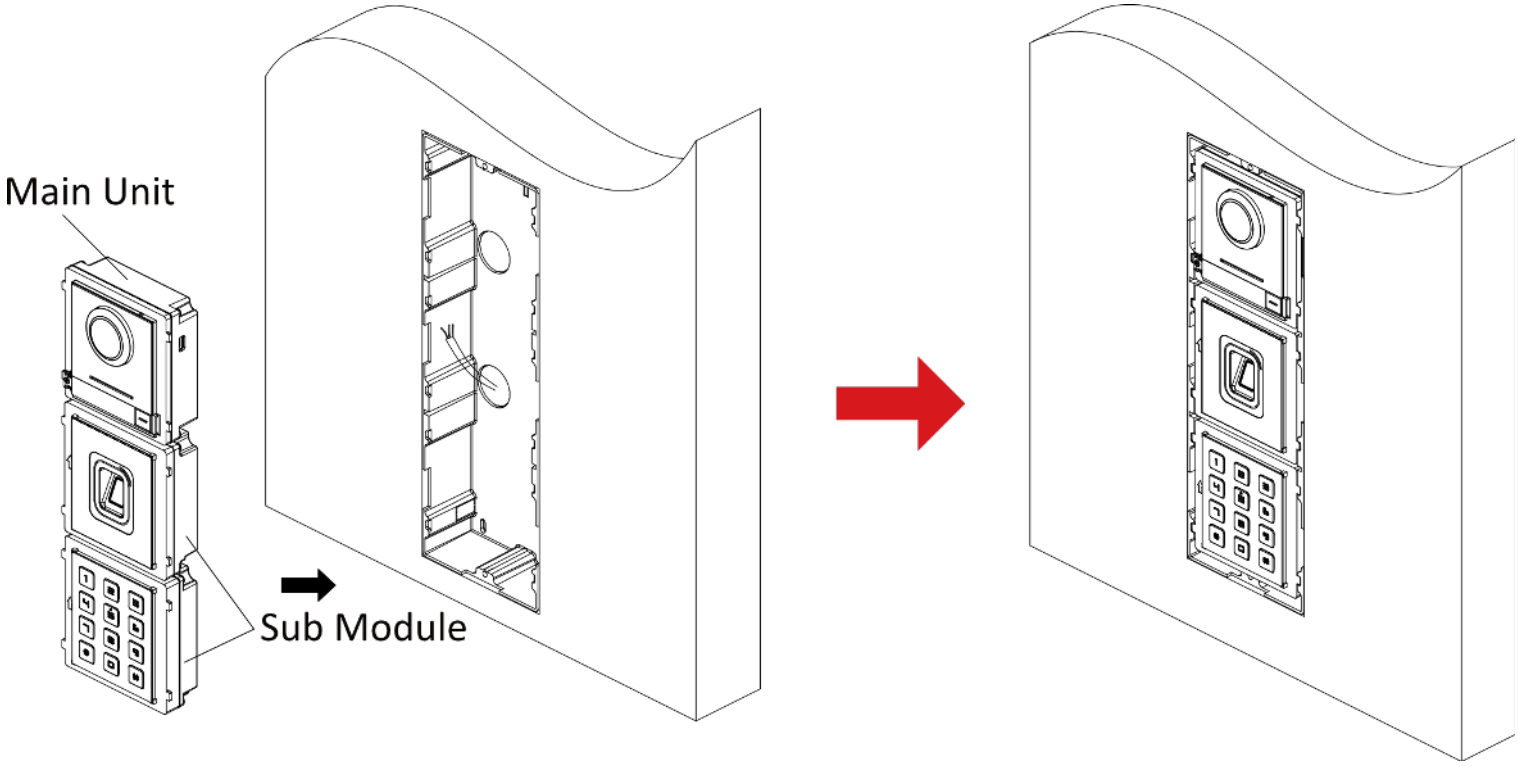


Figure 5-11 Fix Modules to the Mounting Box

4. Fix the cover with 2 socket head cap screws by using a hexagon wrench.

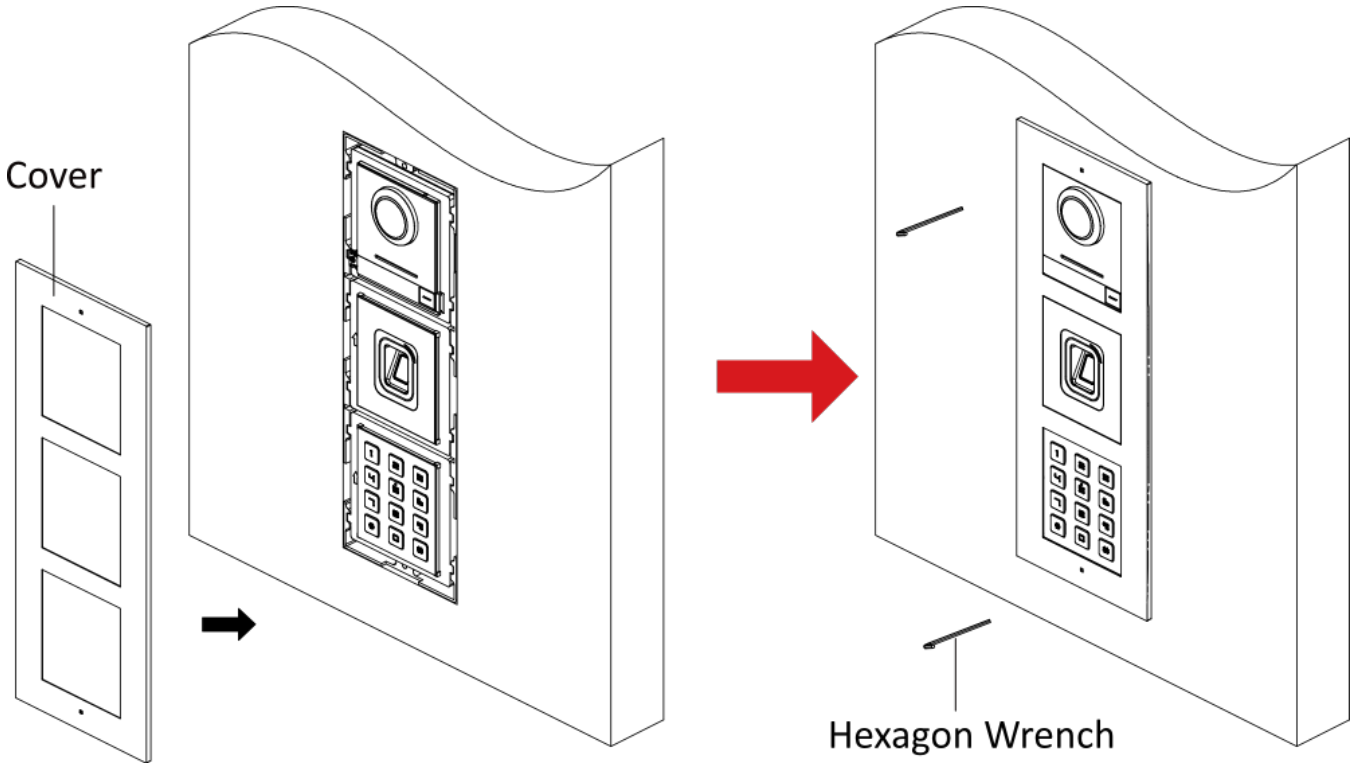


Figure 5-12 Fix the Cover

Chapter 6 Issue Card

You can issue card via main card or via Web client of the main unit.

Note

- M1 card and DESFire card are supported.
- If the amount of sub cards exceeds 6000, no more sub cards can be issued.
- You can only issue card via the main card or the Web Client.

Issue Card via Main Card

1. Swipe the main card on the card reading area, and hear two beeps.
2. Swipe the unauthorized sub cards in turn after hearing a beep.
3. Swipe the main card again to end the card issuing process.

Issue Card via Web Client

For more information about adding card via Web client please refer to:

- Web 4.0: ***Person Management***
- Web 5.0 (PC Web): ***Person Management on PC Web***
- Web 5.0 (Mobile Web): ***Person Management on Mobile Web***

Chapter 7 Add Fingerprint

You can add fingerprint information via Web client of the main unit.

Note

Up to 1,000 fingerprints can be added.

Add Fingerprint via Web Client

For more information about adding fingerprint via Web client, please refer to:

- Web 4.0: ***Person Management***
- Web 5.0 (PC Web): ***Person Management on PC Web***
- Web 5.0 (Mobile Web): ***Person Management on Mobile Web***

Chapter 8 Configuration and Operation

You can configure the sub module via the Web Client and Client Software of the main unit.

8.1 Configuration via Web Client of the Main Unit

8.1.1 Configuration via Web 4.0

Login Web Browser

You can log into the Web browser for device configuration.

Before You Start
The sub module needs to be connected with the main unit before you can set the sub module via the web client of the main unit. For more details, please refer to ***Wiring with the Main Unit***

Steps
1. Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
2. Enter the device user name and the password. Click **Login** to login to the page.

Person Management

Click and add the person's information, including the basic information, authentication mode and credentials. And you can also edit user information, view user picture and search user information in the user list.

Click **User → Add** to enter the page of **Add User**.

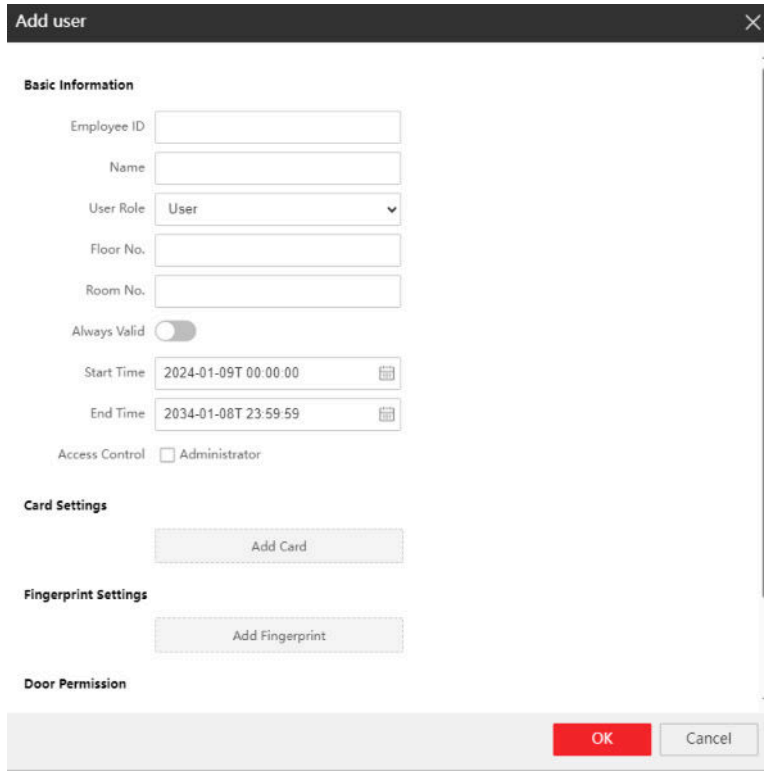


Figure 8-1 Add User

Add Basic Information

Add the person's basic information, including **Employee ID**, **Name**, **Floor No.** and **Room No.** . You also need to select the **User Role**.
Click **OK** to save the settings.

Set Permission Time

Set **Start Time** and **End Time** and the person can only have the permission within the configured time period. If you enable **Always Valid**, then the user can have the permanent permission and you do not need to set **Start Time** and **End Time**.
Click **OK** to save the settings.

Note

You can check **Administrator** to set the user as the Administrator.

Add Card

Click **Add Card**, enter the **Card No.** or click **Read** to read card No. from the card reader module.
Select **Property**, and click **OK** to add the card.
Click **OK** to save the settings.

Add Fingerprint

Click **Add Fingerprint**, and press your finger on the fingerprint module to add your fingerprint. Click **Complete** to save the settings.

Set Card Security

Click **Configuration → General → Card Security** to enter the settings page.

You can check to enable DESFire card and click to enable DESFire Card Read Content. Click **Save** to save the settings.

Enable DESFire Card

The device can read the data from DESFire card when enabling the DESFire card function.

DESFire Card Read Content

After enable the DESFire card content reading function, the device can read the DESFire card No.

View Information of Sub Module

You can view the sub module address, module type, status, and version of the sub module.

Steps

1. Click **Configuration → Intercom → Sub Module Configuration** to enter the page.
2. View the sub module information, including No. (sub module address), module type, status, and version.

Note

- The module address is used to differentiate the sub modules.
- The room No. for the main unit's call button is 1 by default; and the room No. for other call buttons will start with 2. The number will increase continuously. For example, the room No. of the first sub module range from 2~7, the room No. of next sub module will range from 8~13.

8.1.2 Configuration via PC Web 5.0 or Mobile Web

Login Web Browser

You can log into the Web browser for device configuration.

Before You Start

The sub module needs to be connected with the main unit before you can set the sub module via the web client of the main unit. For more details, please refer to ***Wiring with the Main Unit***

Steps

1. Connect your mobile devices or PCs to the main unit's hotspot.
2. Enter the user name and the activation password. Click **Login**.

   Note

   The main unit will be activated automatically after powered on. You can check the activation password via the label on the surface of the main unit.
3. For the first-time login, you need to change the activation password: Click **admin → Modify Password** on the upper right of the Web browser page. Enter the old and new password and confirm the new password. Click **Save** to save the setting.

   Note

   The hotspot password will be changed simultaneously after the activation password is changed.

Person Management

You can manage person information on PC Web and mobile Web.

- ***Person Management on PC Web***
- ***Person Management on Mobile Web***

Person Management on Mobile Web

You can add, edit, delete, and search users via mobile Web browser.

Steps

1. Tap → **Person Management** to enter the settings page.
2. Add user.
   1) Tap**+**.
   2) Set the following parameters.

   Employee ID

   Enter the employee ID. The Employee ID cannot be 0 or exceed 32 characters. It can be a combination of uppercase, lowercase letters and numbers.

   Name

   Enter your name. The name supports numbers, uppercase and lowercase English, and characters. The name is recommended to be within 32 characters.

   Room No.

   Enter the Room No.

   Note

   The room No. refers to the mapping room No. which you can custom the No. on your own.

Long-Term Effective User

Set the user permission as long-term effective.

Start Date/End Date

Set **Start Date** and **End Date** of user permission.

Administrator

If the user needs to be set as administrator, you can enable **Administrator**.

User Role

Select your user role.

Card

Add card. Tap **Add Card**. Enter the **Card No.**, or present the card on the device and tap **Read**, and select the **Property**. Tap **Save** to add the card.

Fingerprint

Add fingerprint. Tap **Fingerprint**, then tap **+**, and add fingerprint via the fingerprint module.

3) Tap **Save**.

3. Tap the user that needs to be edited in the user list to edit the information.

4. Tap the user that needs to be deleted in the user list, and tap to delete the user.

5. You can search the user by entering the employee ID or name in the search bar.

Person Management on PC Web

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, person type, etc.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.
Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.
Click **Save** to save the settings.

Add Administrator

Click **Person Management → Add** to enter the Add Person page.
Tap to enable **Administrator**, and the person you add will be administrator.
Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.
Click **Save** to save the settings.

Add Fingerprint

Click **Person Management → Add** to enter the Add Person page.
Click **Add Fingerprint**, and press your finger on the fingerprint module of the device to add your fingerprint.
Click **Save** to save the settings.

Set Room No.

Click **Person Management → Add** to enter the Add Person page.
Click **Add**, enter the **Room No.** to add the room.

Note

The room No. refers to the mapping room No. which you can custom the No. on your own.

Click **Save** to save the settings.

Set Door Permission

Click **Person Management → Add** to enter the Add Person page.
Select Door 1 or Door 2, to configure the door permission of the person.
Click **Save** to save the settings.

View/edit Person

Click **Person Management → Add** to enter the Add Person page.
You can filter a person by entering the employee ID, name or card No.
You can view added people under the mode of card or list. You can click the card of the person or the editing icon to edit the information of the person.
Click **Save** to save the settings.

Sub Module Configuration

View Sub Module Information via Mobile Web

You can view information of the sub module on mobile Web of the main unit.

Steps

1. Tap → **Intercom → Sub Module Configuration** to enter the page.
2. View the version and online status of connected sub modules.

View Sub Module Information via PC Web

You can view the information of the sub module via PC Web Client of the main unit.

Steps

1. Click **Configuration → Intercom → Sub Module Configuration** to enter the page.
2. View the sub module information, including No. (sub module address), module type, online status, and version.

Card Settings

Set Card Security

Tap → **Access Control → Card Security** to enter the configuration page.

Set the parameters and tap **Save**.

Enable DESFire Card

The device can read the data from DESFire card when enabling the DESFire card function.

DESFire Card Read Content

After enable the DESFire card content reading function, the device can read the DESFire card No.

Set Card Security on PC Web

Click **Configuration → Card Settings → Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable DESFire Card

The device can read the data from DESFire card when enabling the DESFire card function.

DESFire Card Read Content

After enable the DESFire card content reading function, the device can read the DESFire card No.

Set Fingerprint Security Level

Set Fingerprint Security Level on PC Web

Click **Configuration → Smart → Smart** .

Fingerprint Security Level

Select the fingerprint security level.
The higher is the security level, the lower is the false acceptance rate (FAR).
The higher is the security level, the higher is the false rejection rate (FRR).

Set Fingerprint Security Level on Mobile Web

Set fingerprint security level.

Tap → **Smart** → **Fingerprint Parameters** .

Fingerprint Security Level

Select the fingerprint security level.
The higher is the security level, the lower is the false acceptance rate (FAR).
The higher is the security level, the higher is the false rejection rate (FRR).

8.2 Configuration via Client Software of the Main Unit

8.2.1 Device Management

Device management includes device activation, adding device, editing device, and deleting device, and so on.

After running the iVMS-4200, video intercom devices should be added to the client software for remote configuration and management.

Add Online Device

Before You Start

Make sure the device to be added is in the same subnet with your computer. Otherwise, please edit network parameters first.

Steps

1. Click **Online Device** to select an active online device.
2. Click **Add**.
3. Enter corresponding information, and click **Add**.

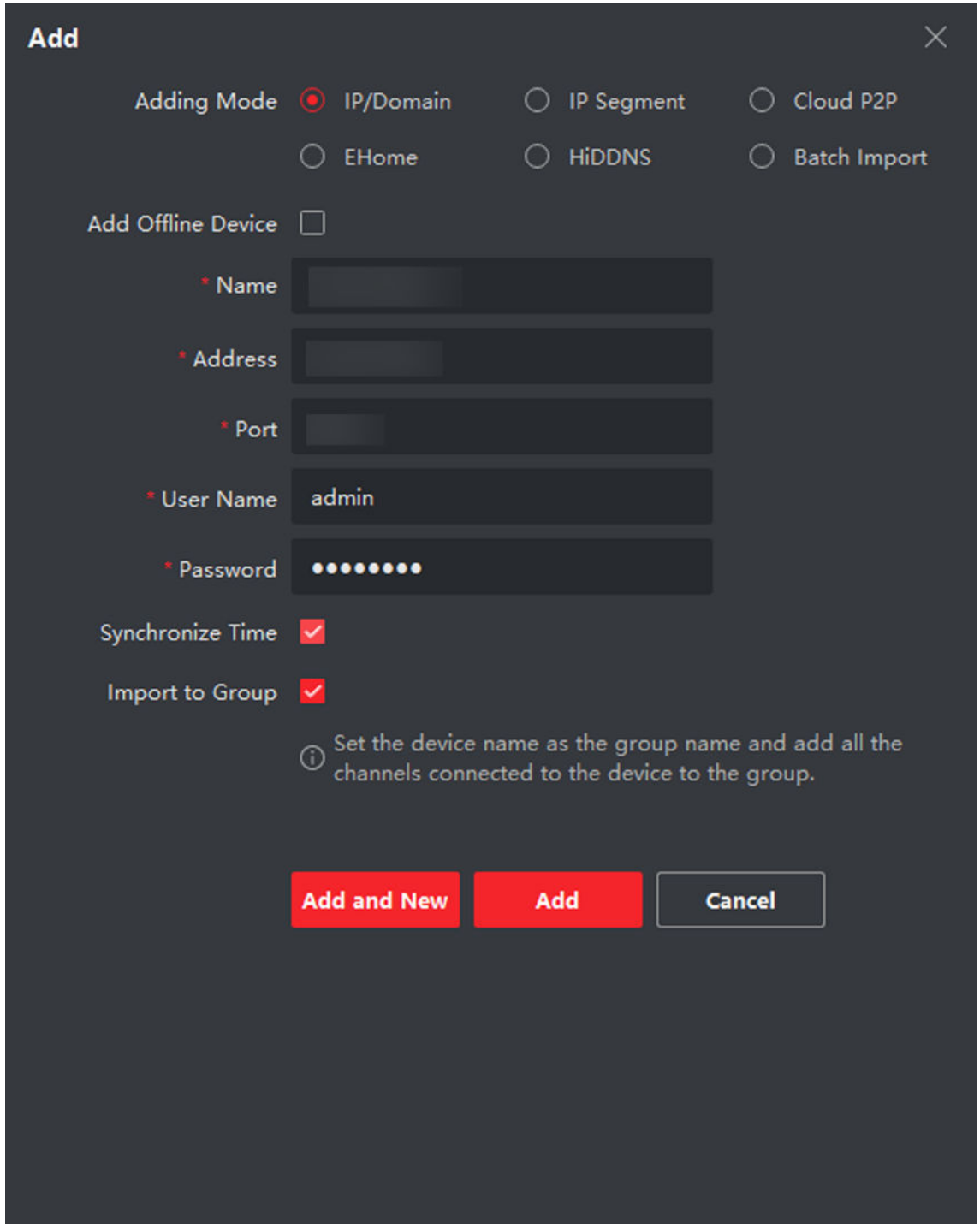


Figure 8-2 Add to the Client

Add Device by IP Address

Steps

1. Click **+Add** to pop up the adding devices dialog box.
2. Select **IP/Domain** as **Adding Mode**.
3. Enter corresponding information.
4. Click **Add**.

Add Device by IP Segment

You can add many devices at once whose IP addresses are among the IP segment.

Steps

1. Click **+Add** to pop up the dialog box.
2. Select **IP Segment** as **Adding Mode**.
3. Enter corresponding information, and click **Add**.

8.2.2 Remote Configuration

After login to the Client Software and add main units to the Client, you can click to set the parameters of the device.

Note

It will automatically jump to the Web configuration page of the main unit. For more information of Web configuration, please refer to ***Configuration via Web Client of the Main Unit*** .
Run the browser, click → **Internet Options** → **Security** to disable the Protected Mode.

Chapter 9 Unlock Door

You can swipe card or use fingerprint to unlock door.

After adding card and fingerprint information to the device via Web client of the main unit, you can swipe card or authenticate via fingerprint to unlock the door.

Note

For more information about adding card and fingerprint, please refer to:

- Web 4.0: ***Person Management***
- Web 5.0 (PC Web): ***Person Management on PC Web***
- Web 5.0 (Mobile Web): ***Person Management on Mobile Web***


See Far, Go Further