Module Door Station

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

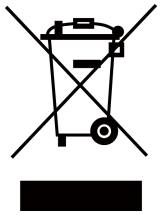
The symbols that may be found in this document are defined as follows.

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.

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.

Contents

Chapter 1 Appearance

Module Door Station

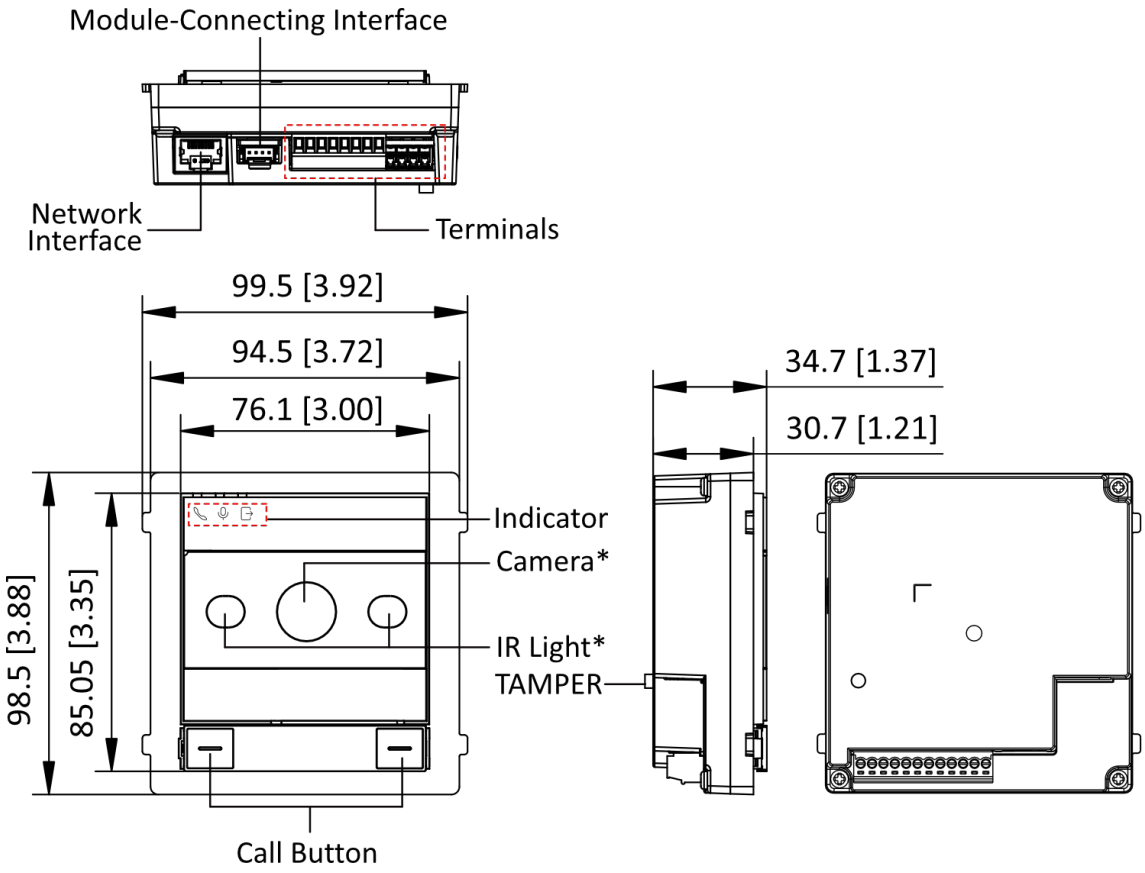


Figure 1-1 Module Door Station

Note

- The pictures here are for reference only.
- RS-485 interface is for module-connecting.
- Camera and IR lights are only supported by DS-KD9005 series module door station.

Chapter 2 Terminal and Wiring

2.1 Wiring

Wiring

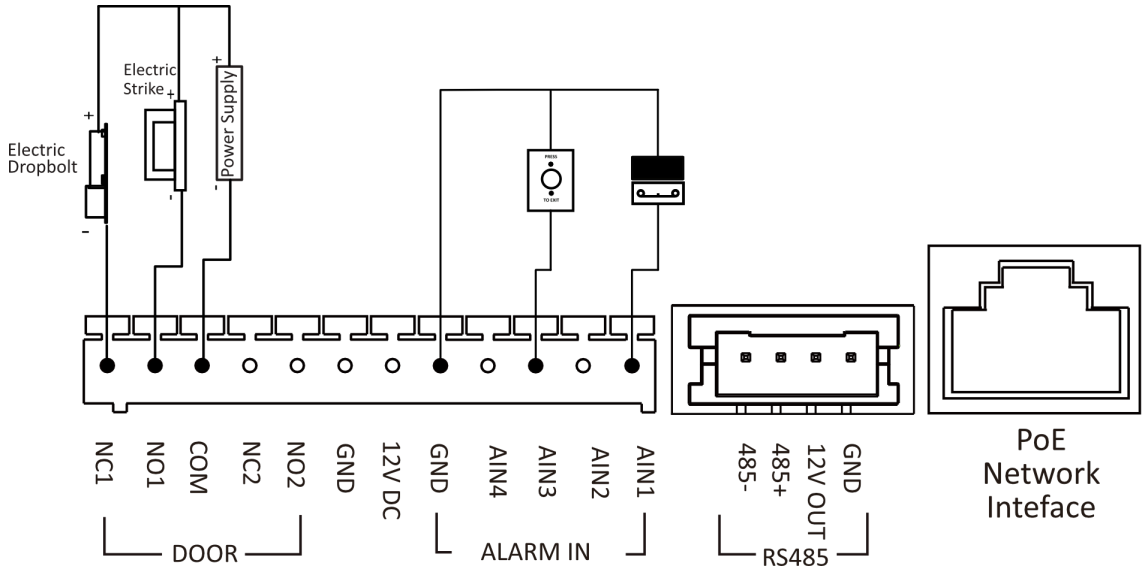


Figure 2-1 Wiring of Door Station

Note

- When the device is powered by PoE, the 12V DC interface can supply power to the lock. The total consumption cannot exceed 10.8 W.
- When you connect to 12V DC power input and PoE switch at the same time, the priority of 12 VDC is higher than PoE Switch. When the device is powered off, you should disconnect the network cable from PoE Switch before disconnecting the power cable.
- By default, AIN1 supports connecting door contact and AIN3 supports connecting exit button. You can set alarm input AIN1~AIN4 via Web Client according to your needs.
- The RS-485 interface is for module-connecting.
- You can connect locks via NC1/NO1 or NC2/NO2. Lock 2 (NC2/NO2) is disabled by default. You can set lock parameters via Web client.

Chapter 3 Installation

Note

- The module supports one-module, two-module and three-module installation. Here takes three-module installation as an example, the one module and two-module installation share 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.

3.1 Three-Module Installation

3.1.1 Surface Mounting

Before You Start

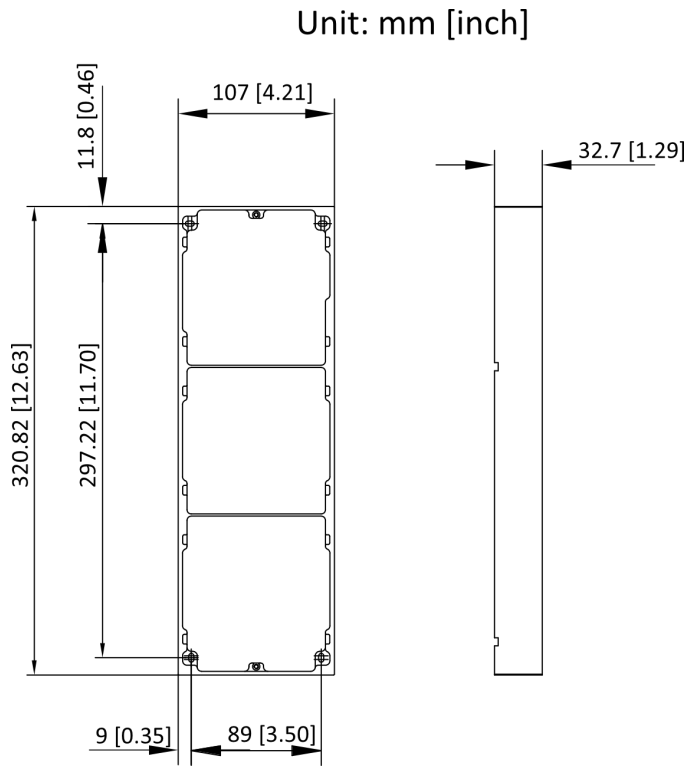


Figure 3-1 Mounting Frame

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.

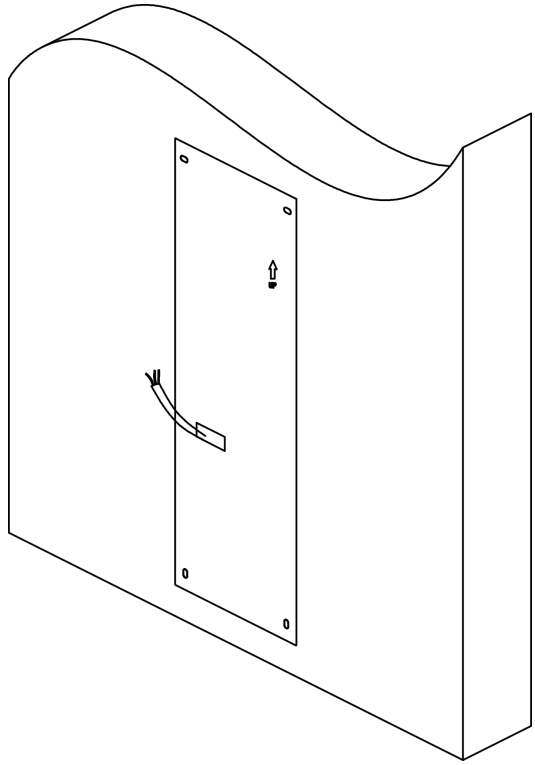


Figure 3-2 Stick the Sticker

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.

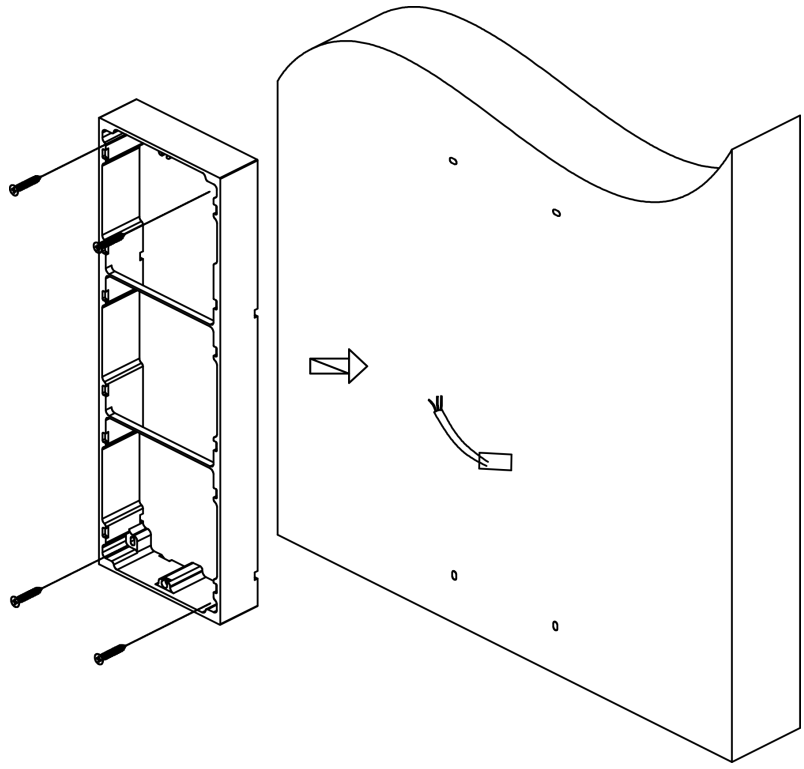


Figure 3-3 Fix the Mounting Frame

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

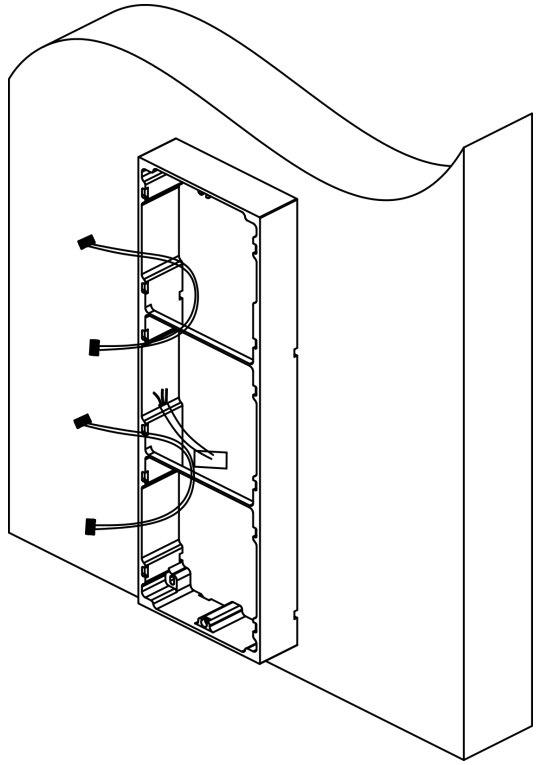


Figure 3-4 Thread the Module-Connecting Line

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.

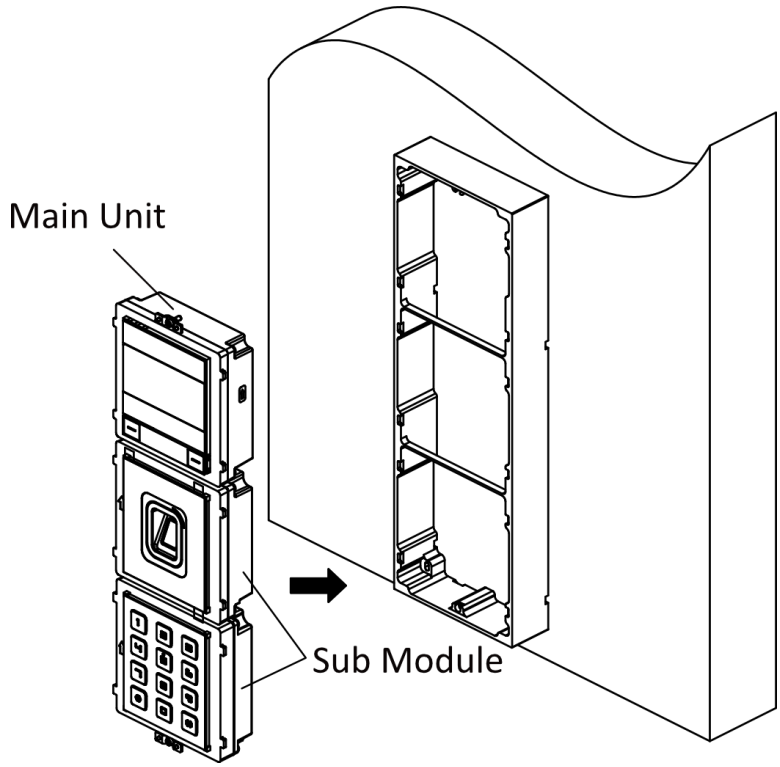


Figure 3-5 Fix Modules to the Frame

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

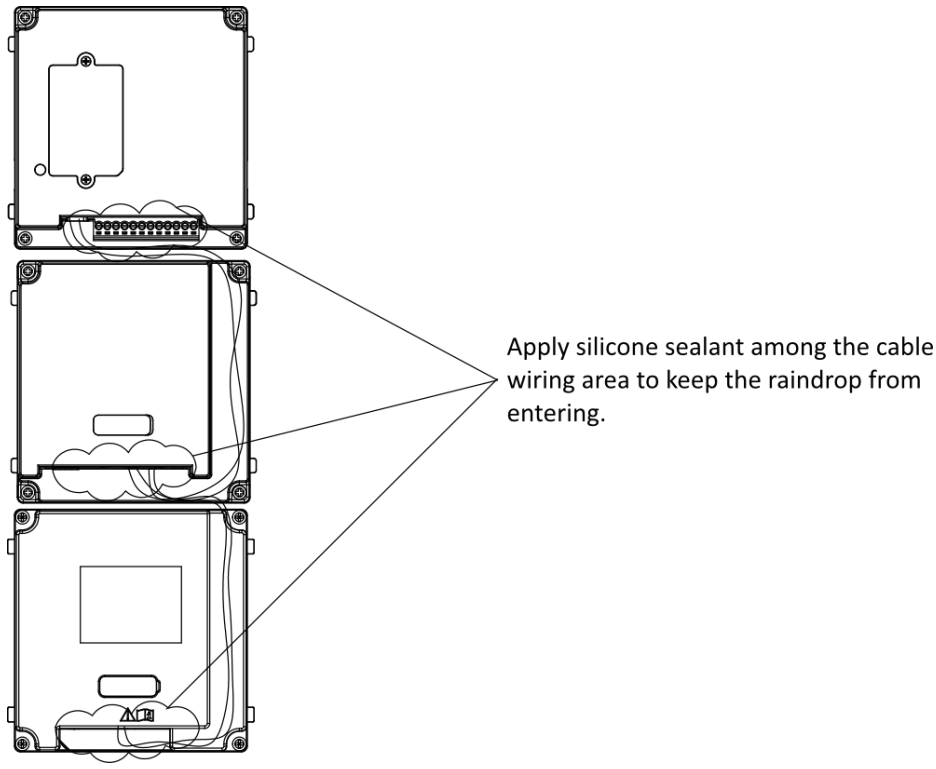


Figure 3-6 Apply Silicone Sealant

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

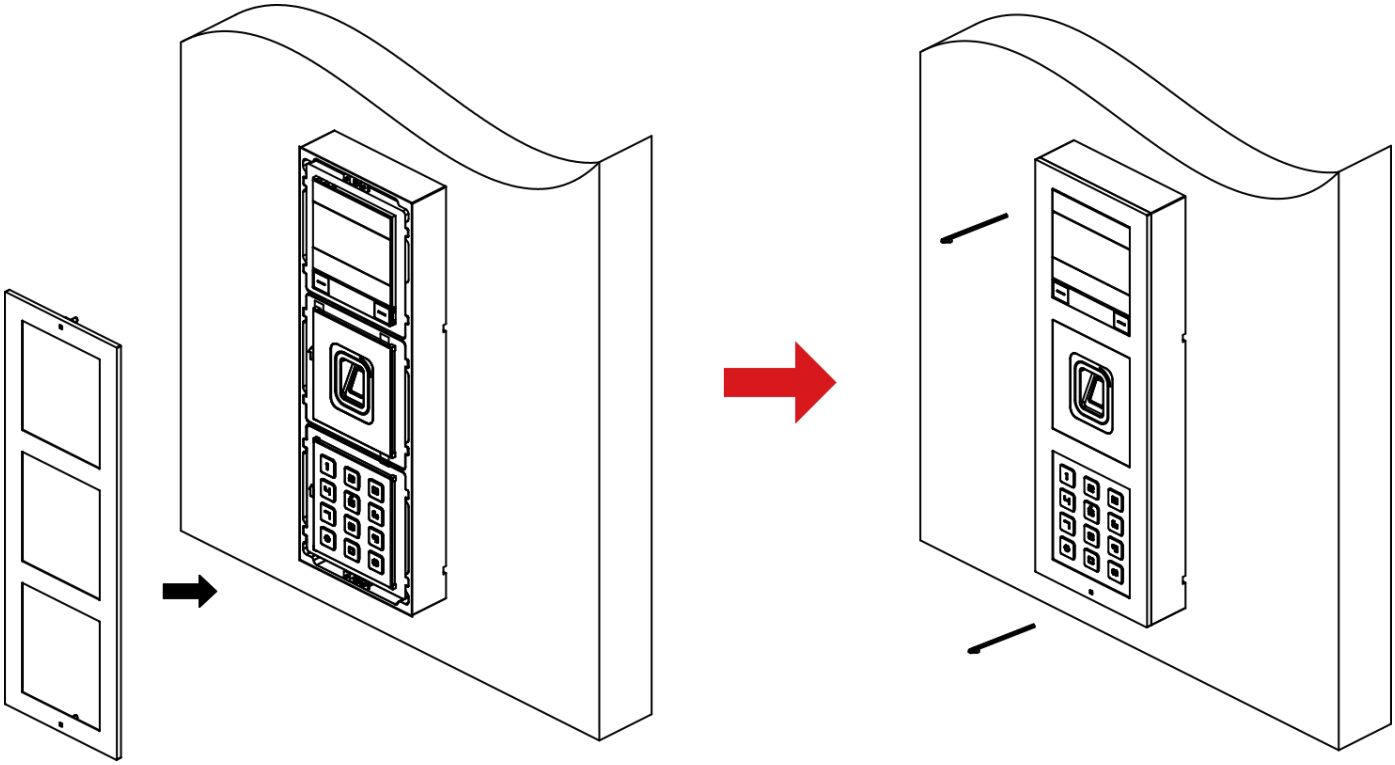


Figure 3-7 Fix the Cover

3.1.2 Flush Mounting

Before You Start

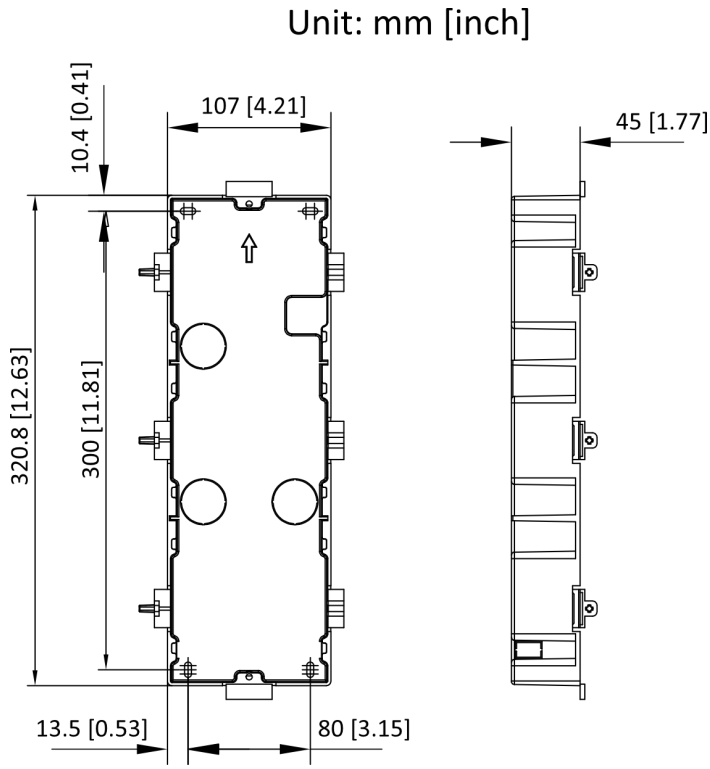


Figure 3-8 Mounting Box

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.

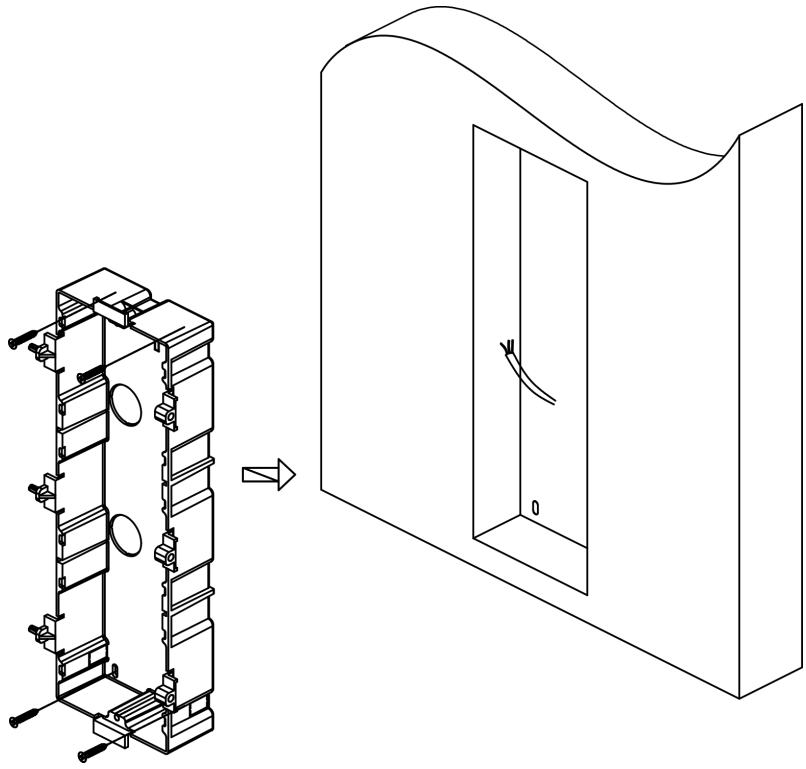


Figure 3-9 Drill the Installation Hole

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

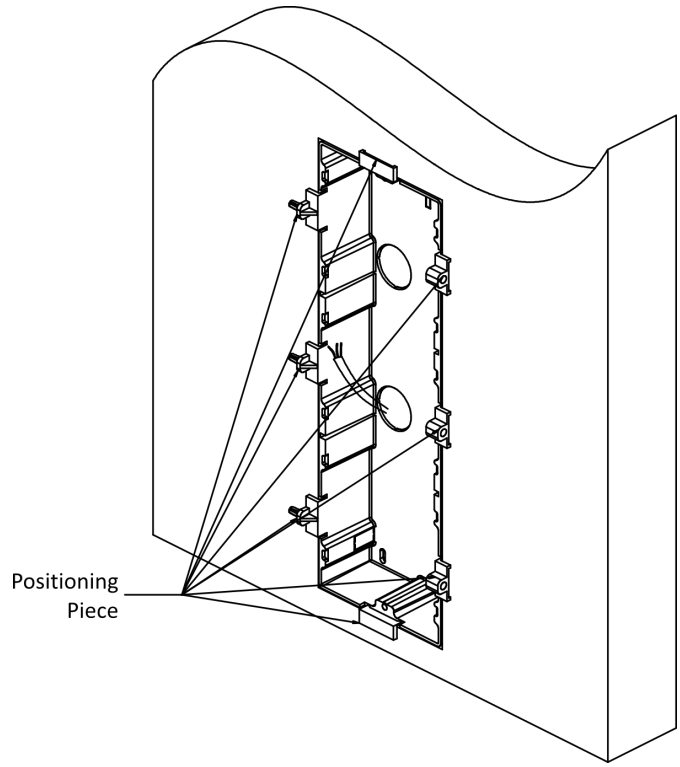


Figure 3-10 Fix the Mounting Box

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.

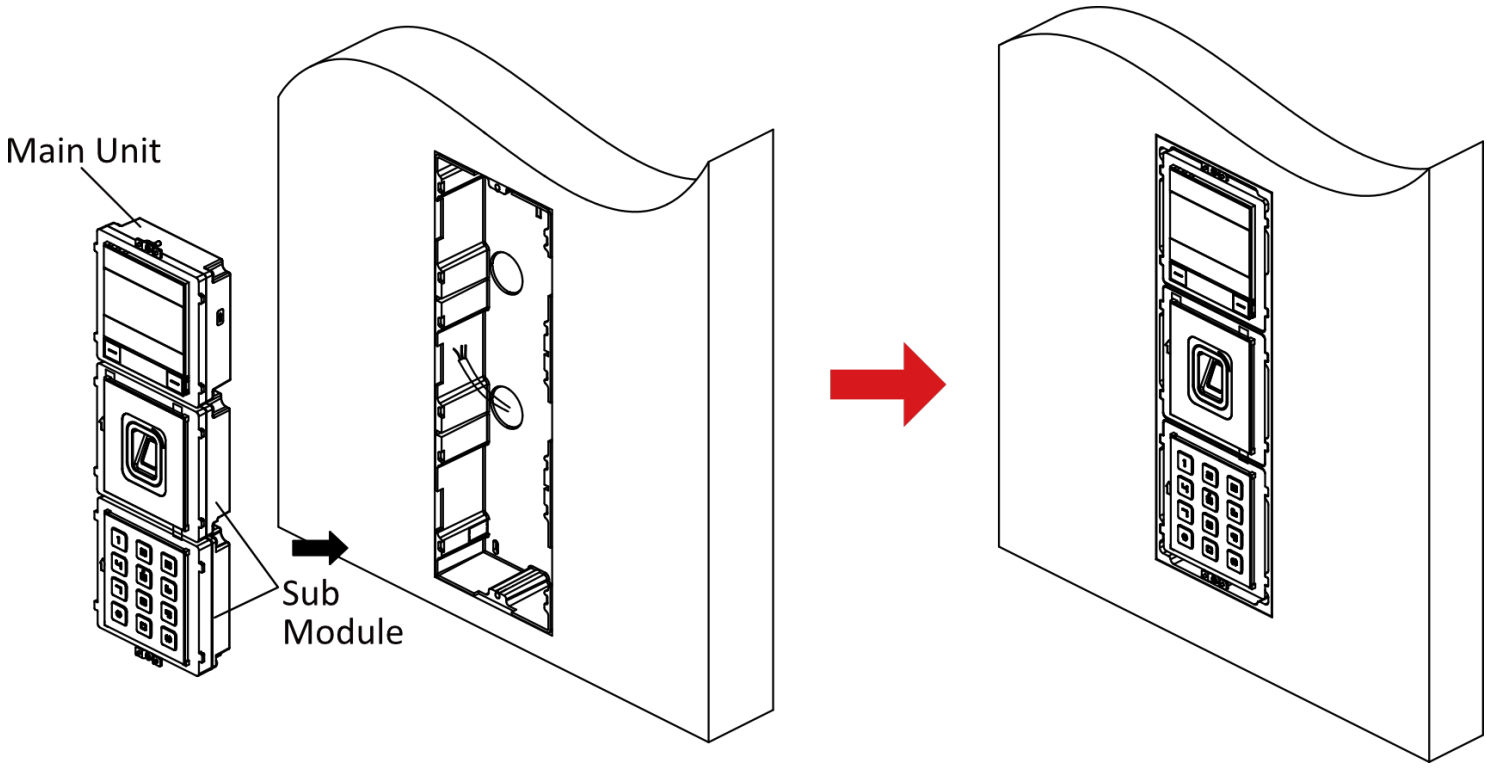


Figure 3-11 Fix Modules to the Mounting Box

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

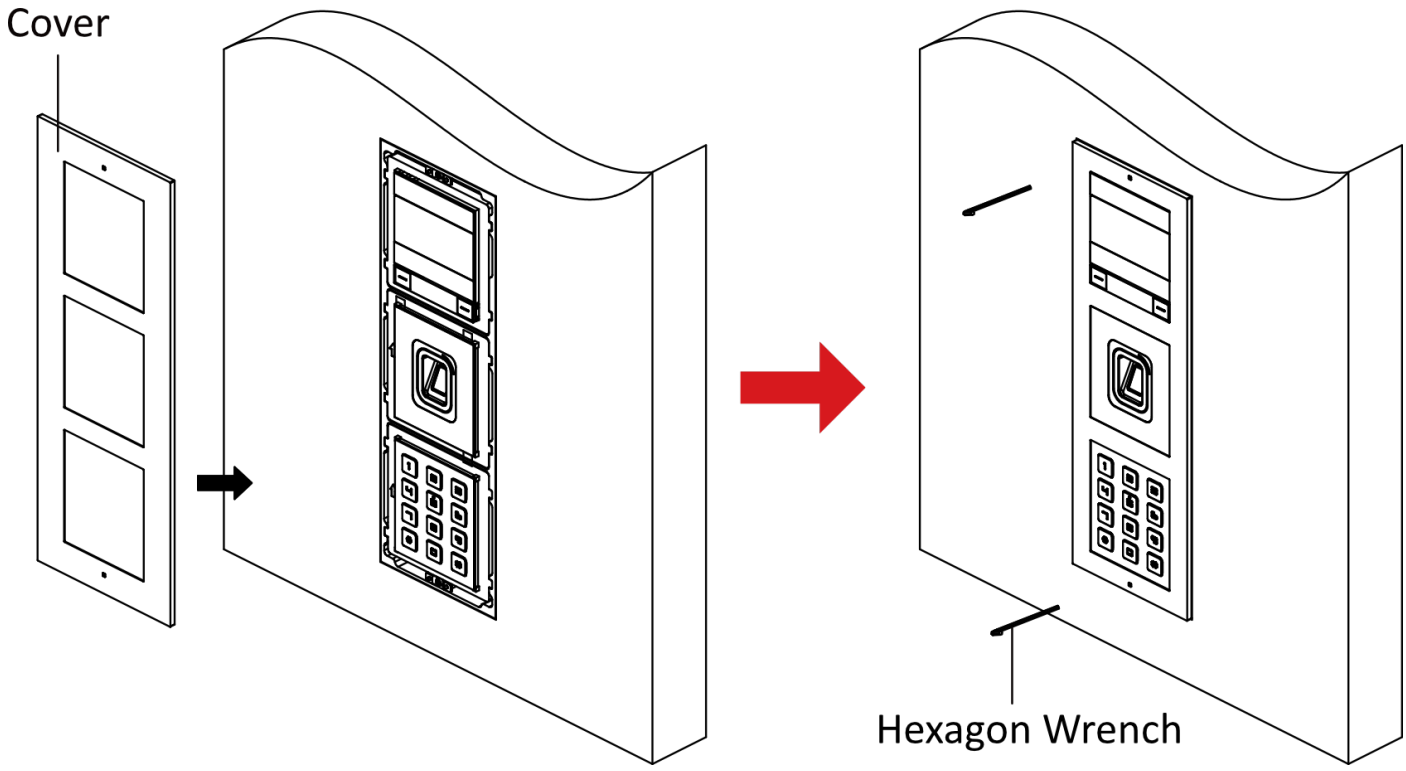


Figure 3-12 Fix the Cover

Chapter 4 Activation

4.1 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

Note

Make sure the device IP address and the computer's should be in the same IP segment.

2. Create a new password (admin password) and confirm the password.

Caution

- The password should be 8 to 16 characters.
- The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
- Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
- The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product. Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
- (If the device supports AP mode, after the admin password is changed, the password of AP hotspot will be changed simultaneously.)

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

4.2 Activate Device via iVMS-4200 Client Software

For some devices, you are required to create the password to activate them before they can be added to the iVMS-4200 software and work properly.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

   Caution

   - The password should be 8 to 16 characters.
   - The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
   - Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
   - The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product. Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
   - (If the device supports AP mode, after the admin password is changed, the password of AP hotspot will be changed simultaneously.)

   Note

   Characters containing admin and nimda are not supported to be set as activation password.
7. Click **OK** to activate the device.

Chapter 5 Quick Operation via Web Browser

5.1 Select Language

You can select a language for the device system.

Click in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

5.2 Time Settings

Click in the top right of the web page to enter the wizard page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

5.3 Administrator Settings

Steps

1. Click on the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **Administrator Settings** page.
2. Enter the employee ID and name of the administrator.
3. Add card. Click **+** to enter the Card No. or click **read** to present the card on the card reading area to read the card No. automatically.

Note

Up to 5 cards can be supported.

4. Click **Next** .

5.4 No. and System Network

Steps

1. Click in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and Network System Network** settings page.
2. Set the device type.

Note

- If set the device type as **Door Station**, you can set the**Community No.**, **Building No.**, **Unit No.**, **Floor No.** and **Door Station No.**.
- If set the device type as **Outer Door Station**, you can set**Outer Door Station No.** and **Community No.**.
- If set the device type as **Doorphone**, you can set**Community No.**, **Building No.**, **Unit No.**.

Device Type

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed door station No.

Note

The main door station No. is 0, and the sub door station No. ranges from 1 to 99.

Outer Door Station No.

Set the device installed outer door station No.

Note

The No. ranges from 1 to 99.

3. Set the video intercom network parameters.

Note

The device type is selected as **Door Station** by default. If you select another type, you can reboot device and go to **Configuration → Intercom** for intercom settings.

Registration Password

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

Main Station IP

Enter the main station's IP address that used for communication.

Private Server IP

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

Enable Protocol 1.0

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

4. Click **Complete** to save the settings after the configuration.

Chapter 6 Operation via Web Browser

6.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

Make sure the device is activated.

Login via Web Browser

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

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click to enter the Configuration page.

6.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

Note

The function is supported when the PC/mobile phone is in the same network segment with the device.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

6.3 Overview

You can view the live video of the device, check linked devices, person information, network status, basic information, and device capacity.

Note

Only some devices support the function of viewing live videos.

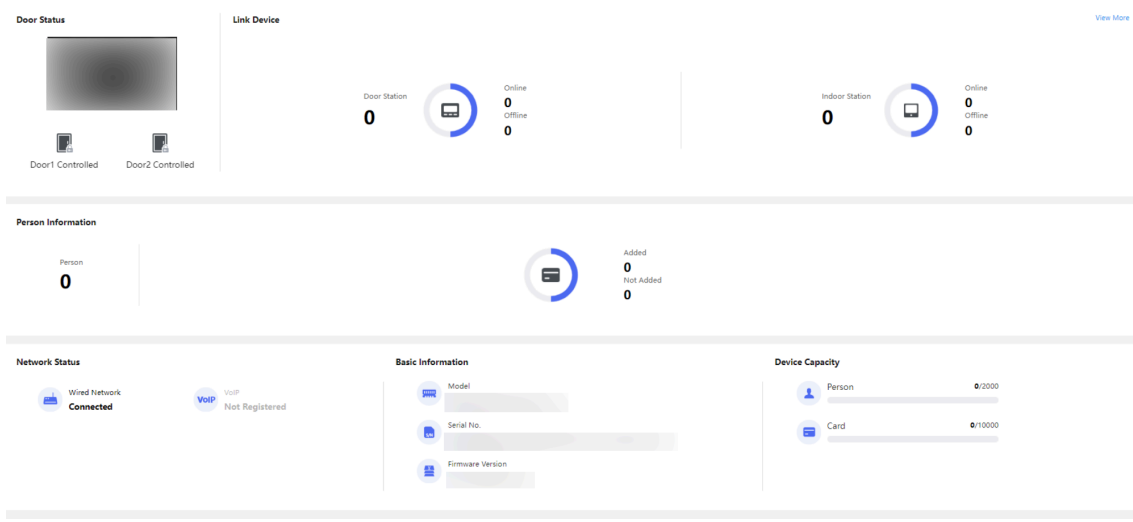


Figure 6-1 Overview Page

Function Descriptions:

Door Status

Click to view the device live view.

Set the volume when starting live view.

Note

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.

You can capture image when starting live view.

Select the streaming type when starting live view. You can select from the main stream and the sub stream.

Full screen view.

/ / /

To set the door status as unlock/remaining open or to restore the settings.

Device Status

View the other linked devices' status.

Person Information

You can view the added and not added information of person.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the person and card capacity.

6.4 Person Management

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, floor No., room No., 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.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
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.

6.5 Device Management

You can manage the linked device on the page.

Click **Device Management** to enter the settings page.

Figure 6-2 Device Management

Add Device

- Click **Add** to add the indoor station, decoder or sub door station. Enter the parameters and click **Save** to add.
- Click **Import**. Download the template and enter the information of the device in the template. Upload the template to import devices in batch.

Export

Click **Export** to export the device information to the PC.

Delete

Select the device and click **Delete** to remove the selected device from the list.

Refresh

Click **Refresh** to refresh the page.

Synchronization Settings

Click **Synchronization Settings** and enable **Synchronize** function. After enabled, the current device's settings will be synchronized to other devices.

Optional: Set Device Information.

- Click to edit device information.
- Click to set the parameters of the device.

- Click to delete device information from the list.
- Select **Status** and **Device Type** to search devices.

6.6 Search Event

Click **Access Control → Event Search** to enter the page.

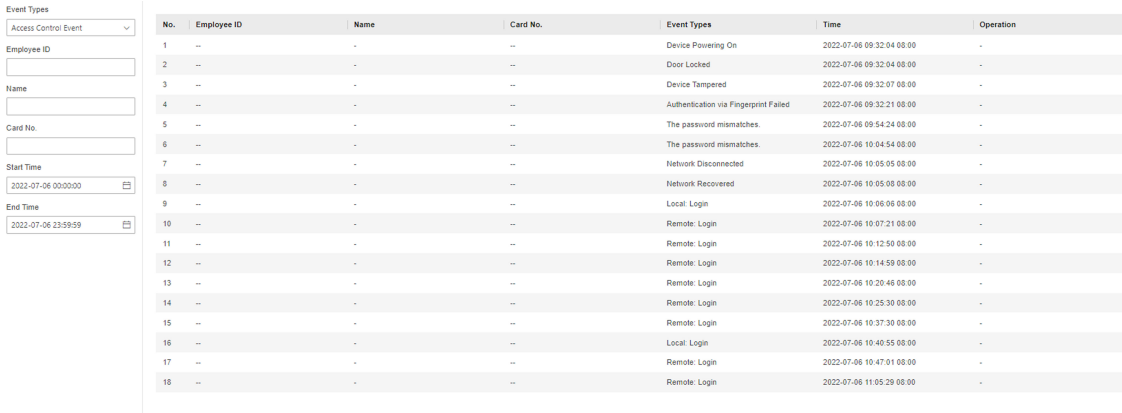


Figure 6-3 Search Event

Enter the search conditions, including the event type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

The results will be displayed on the right panel.

6.7 Configuration

6.7.1 View Device Information on PC Web

View the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

Click **Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can view the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

6.7.2 Set Time

Set the device's time, time zone, synchronization mode, server address, NTP port, and interval.

Click **Configuration → System → System Settings → Time Settings** .

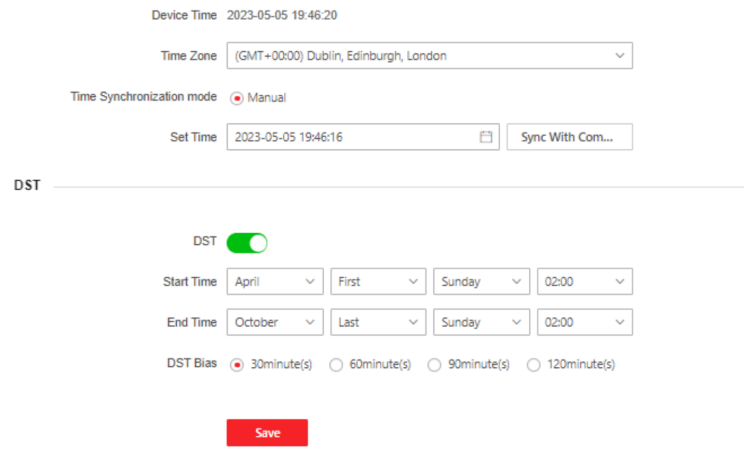


Figure 6-4 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.

6.7.3 Set DST

Steps

1. Click **Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

6.7.4 Change Administrator's Password

Steps

1. Click **Configuration → System → User Management** .
2. Click ✎ .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

Caution

- The password should be 8 to 16 characters.
- The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
- Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
- The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product. Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
- (If the device supports AP mode, after the admin password is changed, the password of AP hotspot will be changed simultaneously.)

6.7.5 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

6.7.6 View Device Arming/Disarming Information

View device arming type and arming IP address.

Click **Configuration → System → User Management → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

6.7.7 Elevator Control

Steps

1. Click **Configuration → Access Control → Elevator Control Parameters** .

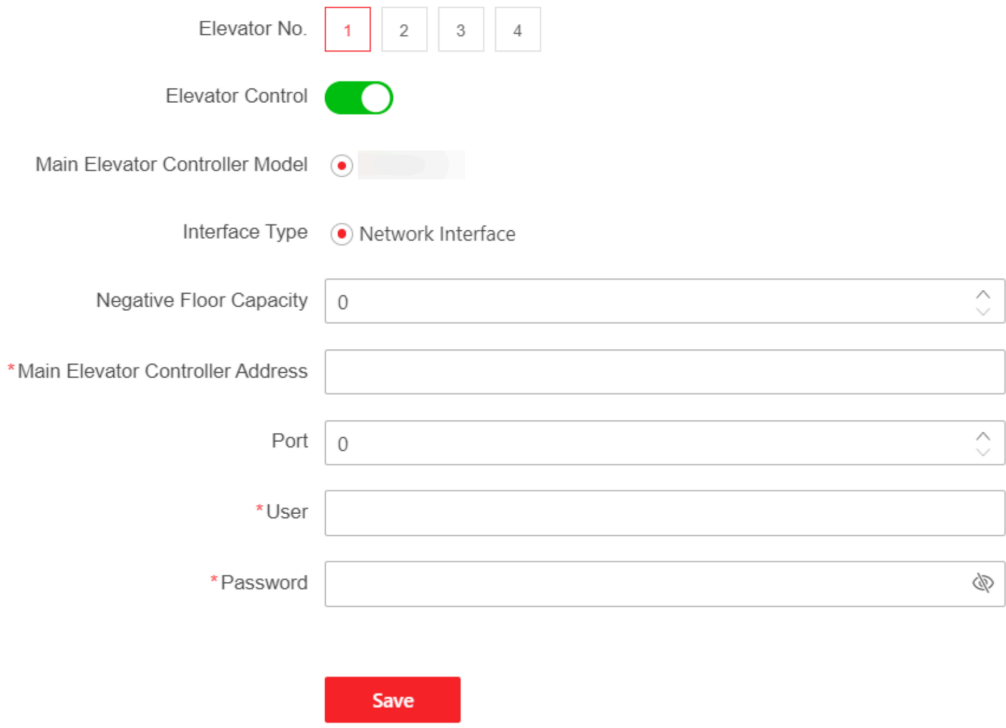


Figure 6-5 Elevator Control

2. Select **Elevator No.**
3. Click to enable **Elevator Control**.
4. Set the elevator parameters.

Elevator No.

Select an elevator No.

Main Elevator Controller Model

Select an elevator controller.

Interface Type

If you select **RS-485**, make sure you have connected the device to the elevator controller with RS-485 wire.

If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password for communication.

Negative Floor Capacity

Set the negative floor number.

Note

- Up to 4 elevator controllers can be connected to 1 device.
- Up to 10 negative floors can be added.
- Make sure the interface types of elevator controllers, which are connected to the same device, are consistent.

6.7.8 Set Secure Door Control Unit Parameters via PC Web

You can set secure door control unit parameters.

Steps

1. Click **System and Maintenance → Access Configuration → Secure Door Control Unit** .
2. Select door.

Note

Selecting door 1 means that the door will be controlled by secure door control unit. The same goes to the selection of door 2.

3. View secure door control unit status.
4. You can enable **Two-Door Interlocking**.

Note

If the function is enabled, the two doors cannot be opened at the same time.

6.7.9 Set I/O Parameters

You can set I/O Parameters on PC Web.

Steps

1. Click **Configuration → Video Intercom → I/O Settings** .
2. Select Input 2 as **Disable** or **Door Status**. Select Input 3 and Input 4 as **Disable** or **Exit Button**.

Note

The Input 1 is **Door Status** by default.

3. Select Output 2 as **Disable**, **Mechanical Doorbell** or **Electric Lock**.

Note

The Output 1 is **Electric Lock** by default.

6.7.10 Sub Module Configuration

Steps

1. Click **Intercom → Sub Module Configuration** , and you can view the sub module information, including No., module type, status, and version.
2. Click ⚙ to edit the sub module.

   Display Module

   - Slide to adjust **Screen Backlight Brightness**.
   - Slide **Enable Buzzer** to enable the function.

   Touch-Display Module

   - Slide to adjust **Screen Backlight Brightness**.
   - Slide **Enable Buzzer** to enable the function.
   - Select **Address Book Display Mode** according to actual needs.
   - Enable **Homepage Shortcut Dial**, you can tap contact on the main page to call.
   - Click **Add** to add custom buttons.

Note

- The module address is used to differentiate the sub modules. See *Configure Sub Module Address* for detailed configuration instructions.
- For the other sub modules (indicator module, keypad module and card reader module), it prompts **Not supported**.
- The room No. for the main unit's call button is 1 by default; and the room No. for the nametag modules call buttons are 2 to 7 by default.

6.7.11 Network Settings

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .

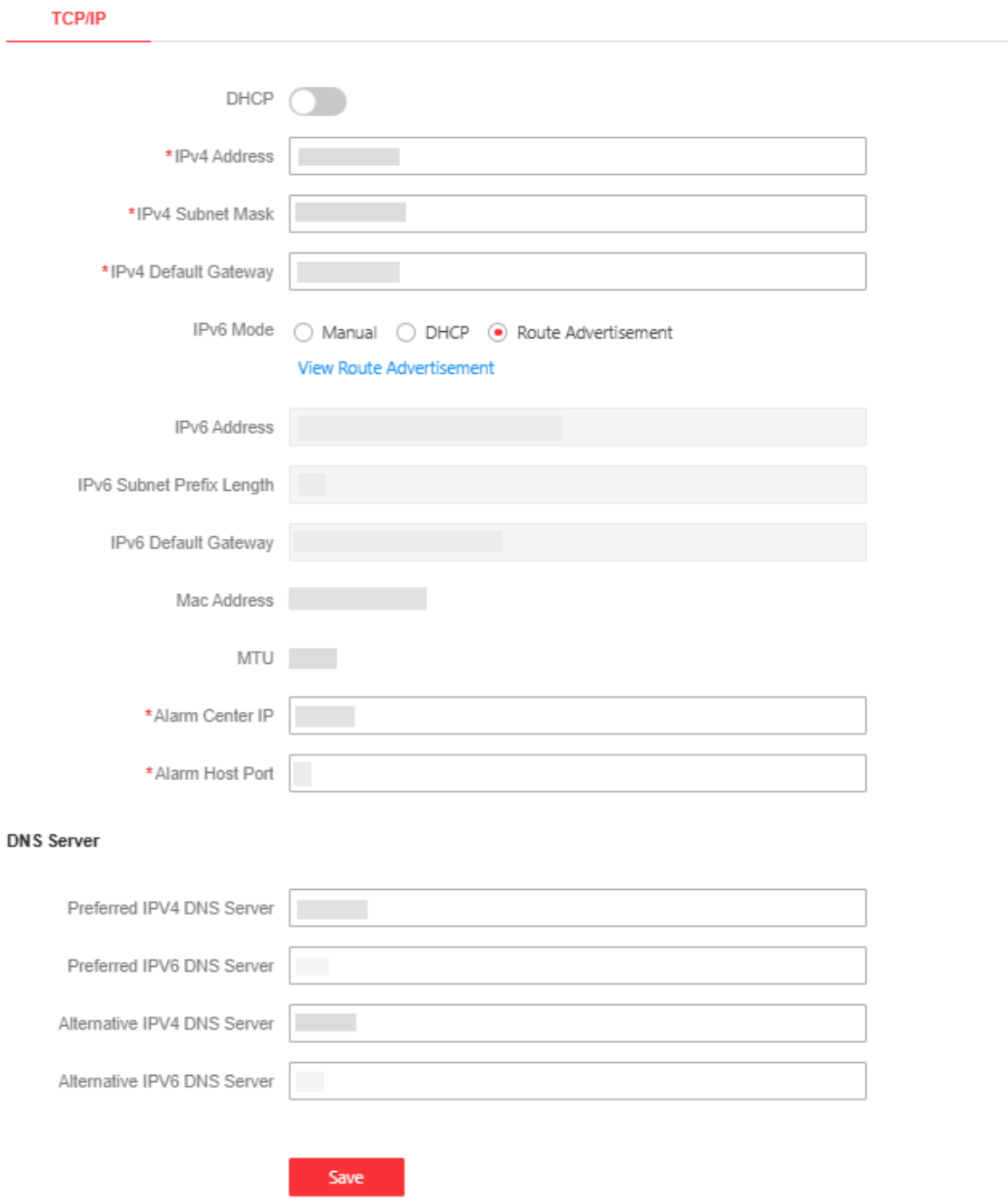


Figure 6-6 TCP/IP Settings

Set the parameters and click **Save** to save the settings.

DHCP

If disable the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, preferred DNS server and the Alternate DNS server.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway, preferred DNS server and the Alternate DNS server automatically.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Enter **IPv6 Address**, **IPv6 Prefix Length**, and **IPv6 Default Gateway**. Consult the network administrator for required information.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Port Parameters

Set the HTTP, HTTPS, RTSP and Server port parameters.

Click **Configuration → Network → Network Service → HTTP(S)** .

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

Click **Configuration → Network → Network Service → RTSP** .

RTSP

It refers to the port of real-time streaming protocol.

Click **Configuration → Network → Device Access → SDK Server** .

SDK Server

It refers to the port through which the client adds the device.

Platform Access via PC Web

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **System and Maintenance → System Configuration → Network → Device Access → Hik-Connect** to enter the settings page.

   Note

   Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. Click **View** to view device QR code. Scan the QR code to bind the account.

   Note

   8 to 32 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

6. Click **Save** to enable the settings.

FTP Settings

You can configure FTP (File Transfer Protocol) parameters.

Steps

1. Click **Network → Advanced → FTP** to enter the settings page.

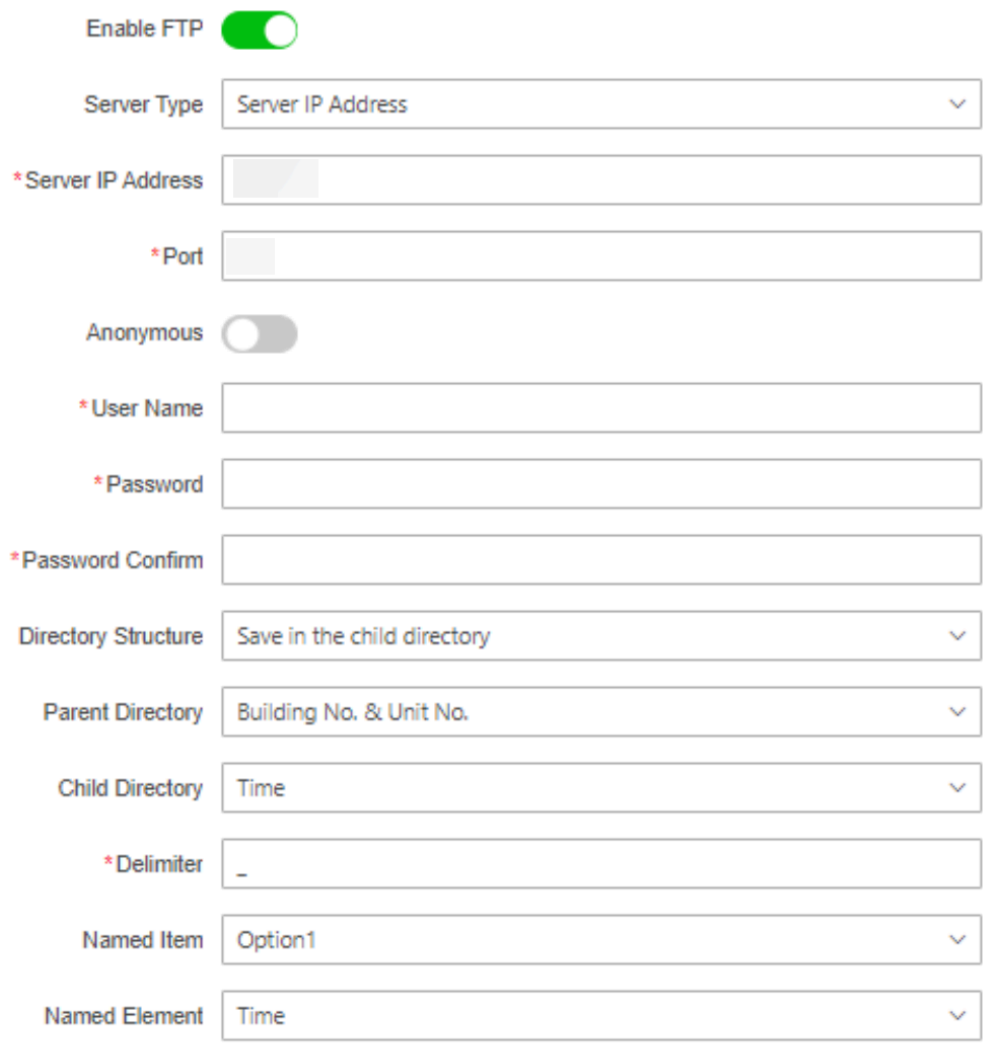


Figure 6-7 FTP Settings

2. Enable**FTP**.
3. Select **Server Type**.
4. Enter **Server IP Address** and **Port**.
5. Configure the FTP Settings, and the user name and password are required for the server login.

Note

If you enable **Anonymous**, you will not need to set user name and password.

6. Set the **Directory Structure**, **Parent Directory** and **Child Directory**.
7. Set naming rules.
8. Click **Save** to enable the settings.

Set Network Penetration Service

When the device is deployed on the LAN, penetration service can be enabled to achieve remote device management.

Steps

1. Click **Configuration → Network → Network Service → Network Penetration Service** .
2. Click to **Enable Penetration Service**.
3. Enter **Server IP Address** and **Server Port**.
4. Enter login **User Name** and **Password**.
5. Set **Heartbeat Timeout**. The range is1 to 6000.
6. Click **Save**.
7. You can view **Online Status**. Click **Refresh** to view the latest status.

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

Go to **System and Maintenance → System Configuration → Network → Network Service → WebSocket(s)** .

View WebSocket and WebSockets port.

6.7.12 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

Click **System and Maintenance → System Configuration → Video/Audio → Video** .

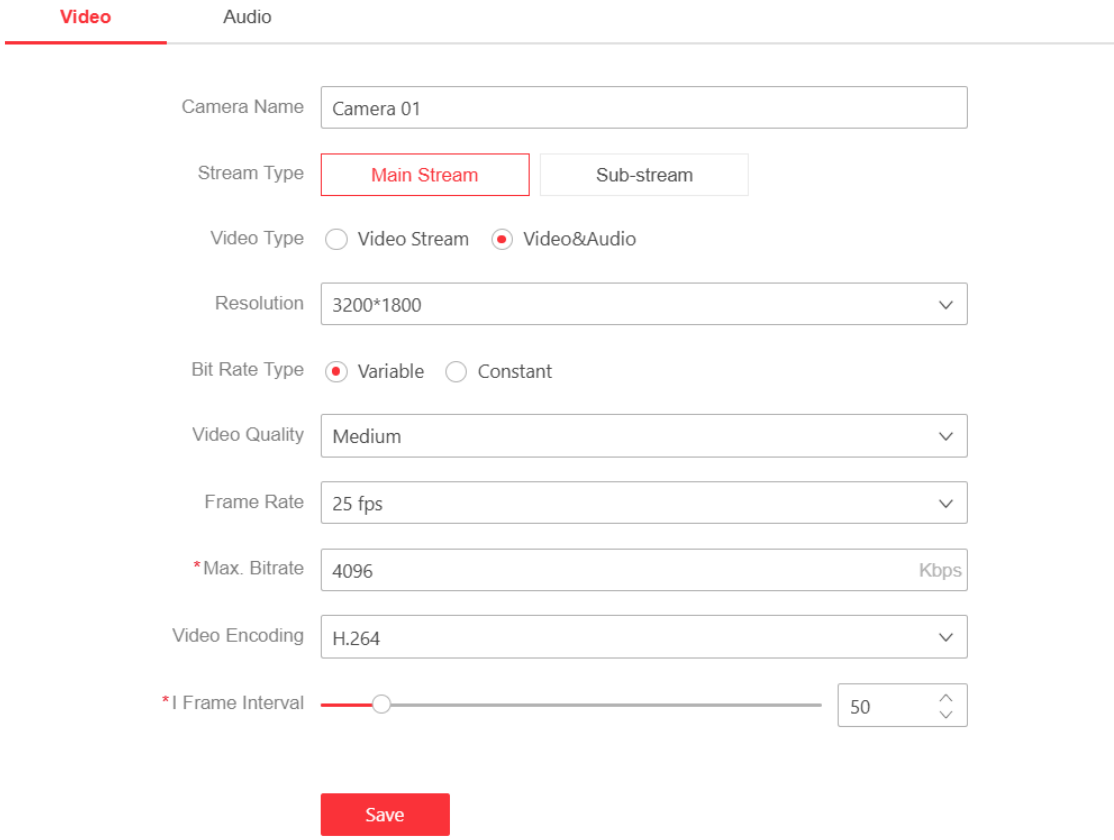


Figure 6-8 Video Settings Page

Set the stream type, the video type, the resolution, the Bit Rate type, the video quality, the frame rate, the Max. bitrate, the video encoding, and I Frame Interval.
Click **Save** to save the settings.

Note

The functions vary according to different models. Refers to the actual device for details.
Main Sream Resolution: 3200*1800, 1280*720 or 1920*1080.
Sub-Sream Resolution: 1280*720 or 640*480.

Set Audio Parameters

Click **System and Maintenance → System Configuration → Video/Audio → Audio** .

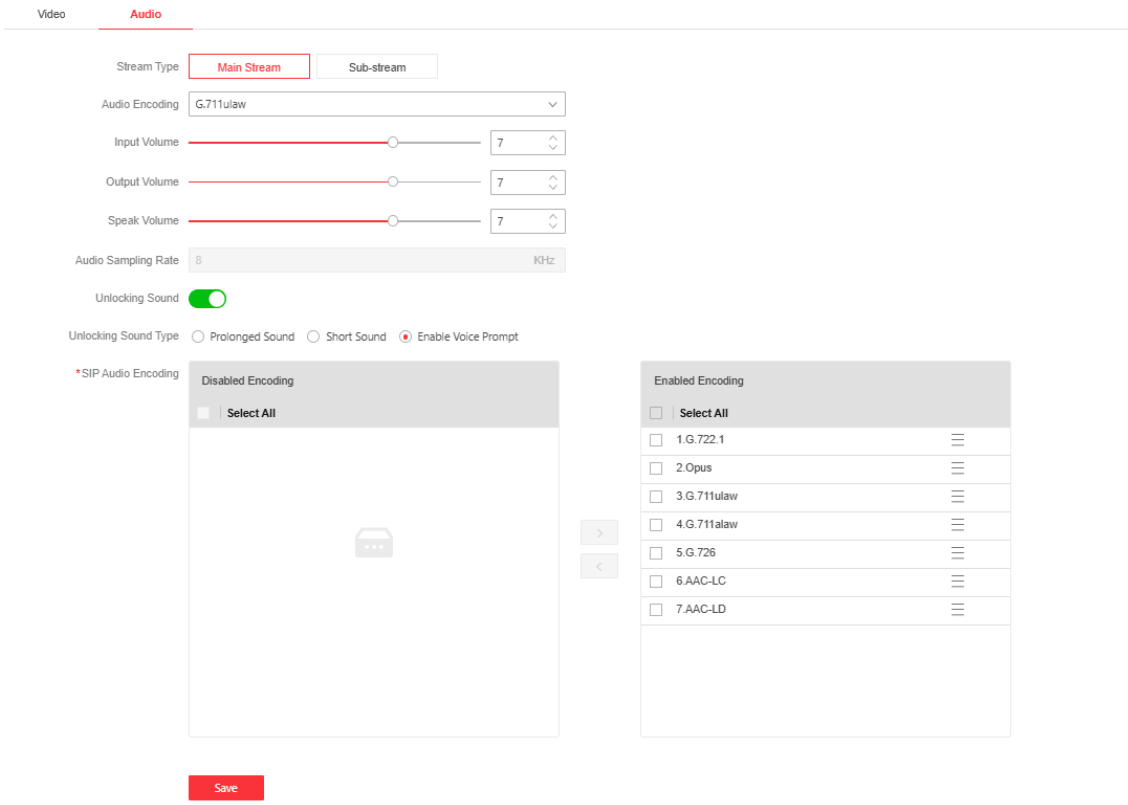


Figure 6-9 Audio Settings Page

Set audio encoding, input volume, output volume.

Slide to enable **Unlocking Sound** and choose unlocking sound type according to your actual need.

Note

The unlocking sound is enabled by default. If select unlocking sound type as **Enable Voice Prompt**, wou will hear "The door is open" when the door is unlcoked.

Check then click **<** or **>** to enable or disable **SIP Audio Encoding**.

Note

You can drag icon ☰ to adjust the order of the encoding.

Click **Save** to save the settings.

6.7.13 Adjust Display Settings

You can adjust image parameters, video parameters, supplement parameters, backlight, beauty etc..

Steps

1. To adjust display settings. Click **System and Maintenance → System Configuration → Image → Display Settings** .
2. Configure the parameters to adjust the image.

   Video Adjustment

   Set the video frame rate when performing live view remotely. After changing the video standard, you should reboot the device to take effect.

   PAL

   25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

   NTSC

   30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

   Image Adjustment

   Drag the block or enter the value to adjust the live video's brightness, contrast, saturation, and sharpness.

   Backlight

   - You can enable or disable the BLC function.
     If enabled, you can choose BLC as **Center**, **UP**, **Down**, **Left** or **Right**.
   - You can enable or disable the WDR function.
     When there are both very bright and very dark areas simultaneously in the view, WDR balances the brightness level of the whole image and provide clear images with details.

   Day/Night Switch

   You can choose Day/Night Switch as Auto, Schedule Switch, Night or Daytime mode.

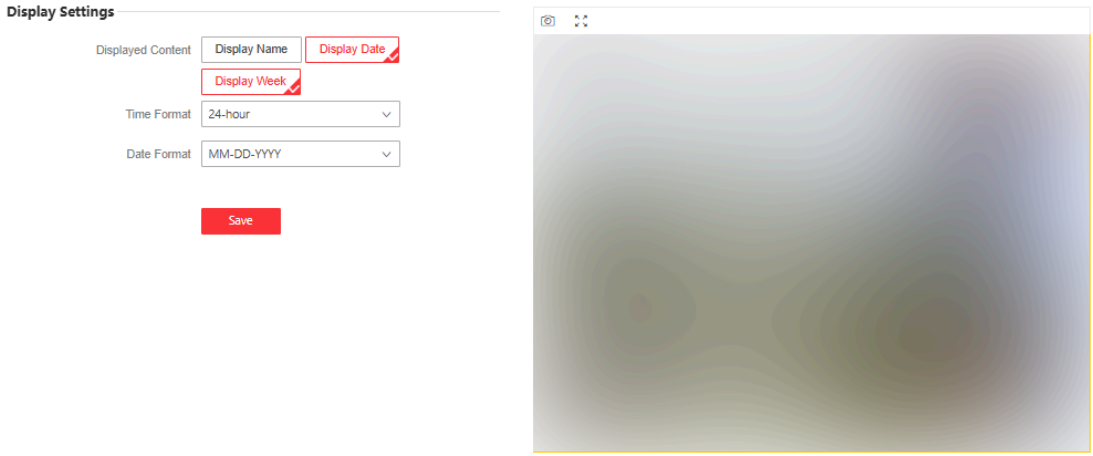
   When choose Day/Night Switch as Auto, you also need to select **Sensitivity** range from 1 to 7.
3. Click **Restore Default Settings** to restore the parameters to the default settings.

OSD Configuration

Steps

1. To adjust display settings. Click **System and Maintenance → System Configuration → Image → OSD Configuration** .

2. At **Displayed Content**, you can click to choose what to display.

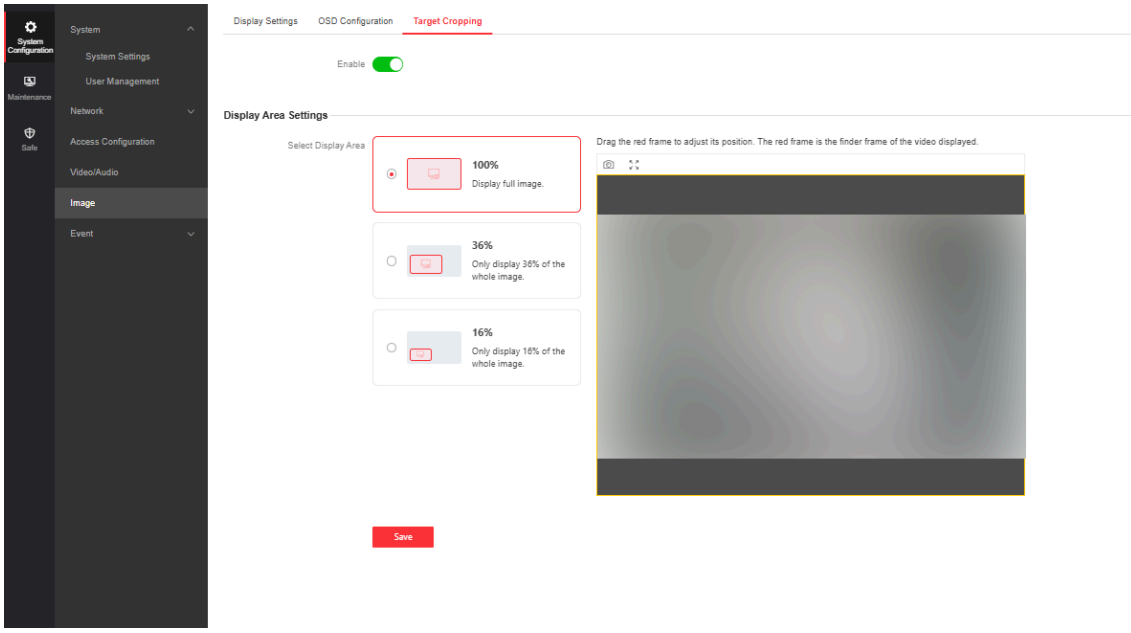


3. You can also choose **Time Format** and **Date Format** according to your actual needs.

Target Cropping

Steps

1. To adjust display settings. Click **System and Maintenance → System Configuration → Image → Target Cropping** .
2. Slide to enable this function.



3. Select **Display Area**.

Note

- Drag the red frame to adjust its position. The red frame is the finder frame of the video displayed.
- If select **100%**, the device will display the full image you can see on the right .
- If select **36%**, only 36% of the whole image will be display.
- If select **16%**, only 16% of the whole image will be display.

4. Click **Save**.

6.7.14 Event Settings

Set Motion Detection

After enable the function of motion detection, people or stuff enter the configured area will trigger alarm.

Steps

1. Click **Configuration → Event → Event Detection → Motion** .

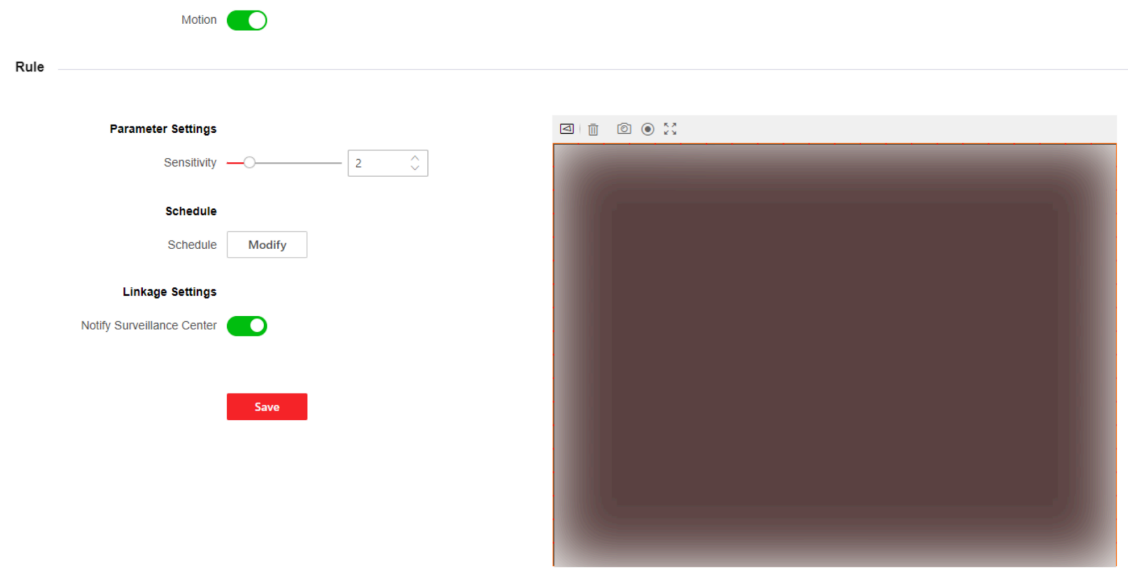


Figure 6-10 Motion Detection

2. Enable **Motion**.
3. Drag the process bar to adjust the **Sensitivity** parameter.
4. Enable **Notify Surveillance Center** according to your actual needs. After enabled, the alarm information is uploaded to the surveillance center when an alarm event is detected.
5. Click **Save**.

Note

The arming schedule is defaulted as all-day.

Linkage Settings

Configure the linkage parameters when an event is triggered, including regular linkage and upload to center.

Steps

1. Go to **Configuration → Event → Event Detection → Linkage Settings** .
2. Set the linkage method.

   Tampering Alarm

   Silde to enable. It's the basic form of alarm.

   Notify Surveillance Center

   Slide to enable. When an alarm occurs, upload the alarm information to the center platform.
3. Click **Save** to complete the configuration.

6.7.15 Access Control Settings

Configure Schedule Template

Holiday Schedule Template

Set official holidays or specified dates as holidays. The access level of set holidays is higher than the other basic access level.

Steps

1. Click **Access control → Permission Management → Access Plan Management → +Add**.
2. Enter holiday name in the right column.
3. **Optional:** Enable **Repeat Annually** according to actual demand. Once enabled, the template will take effect every year. No need to set again. Applicable to set official holidays.
4. Set Start Date and End Date.
5. Drag cursor on corresponding timestamp to map valid access period. People can access during valid access period.
6. **Optional:** Click **Clear** to adjust chosen time period. You can also click a certain time period then adjust it manually.
7. Click **Save**.

Set Door Parameters

Click **Configuration → Access Control → Door Parameters** .

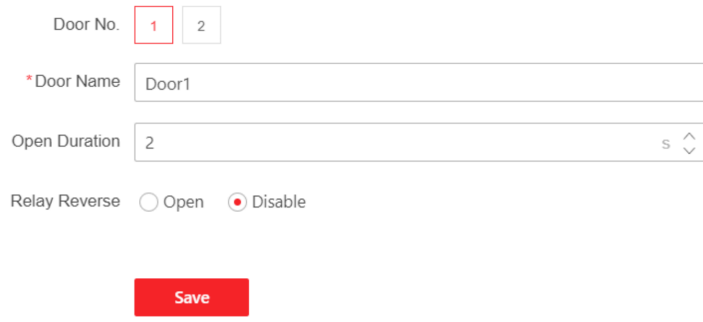


Figure 6-11 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select the device corresponded door No.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Relay Reverse

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Privacy Settings

You should set the privacy parameters, including the picture uploading and storage.

Select parameters according to your actual needs.

Upload Pic. When Auth. (Upload Captured Picture When Authenticating)

Upload the pictures captured when authenticating to the platform automatically.

Save Pic. When Auth. (Save Captured Picture When Authenticating)

If you enable this function, you can save the picture when Authenticating to the device.

Save Registered Pic. (Save Registered Picture)

The registered face picture will be saved to the system if you enable the function.

Upload Pic. After Linked Capture (Upload Picture After Linked Capture)

Upload the pictures captured by linked camera to the platform automatically.

Save Pic. After Linked Capture (Save Pictures After Linked Capture)

If you enable this function, you can save the picture captured by linked camera to the device.

Tap **Next** to complete the settings.

Set Card No. Authentication Parameters via Web

Set the card reading content when authenticate via card on the device.

Go to **Access Control → Parameter Settings → Card Settings** .

Select a card authentication mode and click **Save**.

Full Card No.

All card No. will be read.

3 bytes

The device will read card via read 3 bytes.

4 bytes

The device will read card via 4 bytes.

6.7.16 Video Intercom Settings

Search Notice

Steps

1. On the Video Intercom page, click **Notice** to enter the page.
2. Set the search conditions, including notice type, start time and end time.

   Type

   Select **Advertising Information**, **Property Information**, **Alarm Information** or **Notice Information** as **Type** according to your needs.

   Start Time/End Time

   Click the time icon to specify the start time and end time of a time period to search the logs.

   Reset the Settings Click **Reset** to reset all the configured search conditiions.
3. Click **Search** and the matched notice will display on this page.
4. **Optional:** Click **Export** to export the notices to your PC.

Device No. Settings

Steps

1. Click **Configuration → Intercom → Device No.** to enter the page.

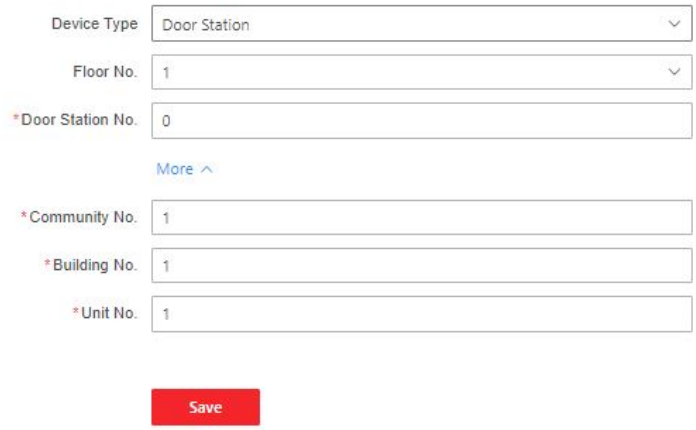


Figure 6-12 Device No. Settings

2. Select the device type from the drop-down list, and set the corresponding information including **Building No.**, **Floor No.**, **Door Station No.**, **Community No.** and **Unit No.**

Note

- When you select **Outer Door Station** as **Device Type**, only **Community No.** and **Outer Door No.** can be set.
- When you select **Doorphone** as **Device Type**, only **Community No.**, **Unit No.** and **Building No.** can be set.

3. Click **Save** to enable the device number configuration.

Linked Network Settings

Steps

1. Click **Intercom → Video Intercom Network** to enter the settings page.

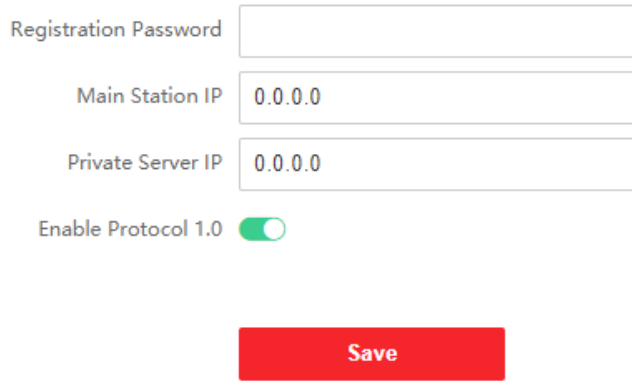


Figure 6-13 Session Settings

2. Set **Registration Password**.
3. Set **Main Station IP** and **Video Intercom Server IP**.
4. Enable Protocol 1.0.
5. Click **Save** to enable the settings.

Time Duration Settings

Set the Max. call duration.

Go to **Configuration → Intercom → Call Settings** .

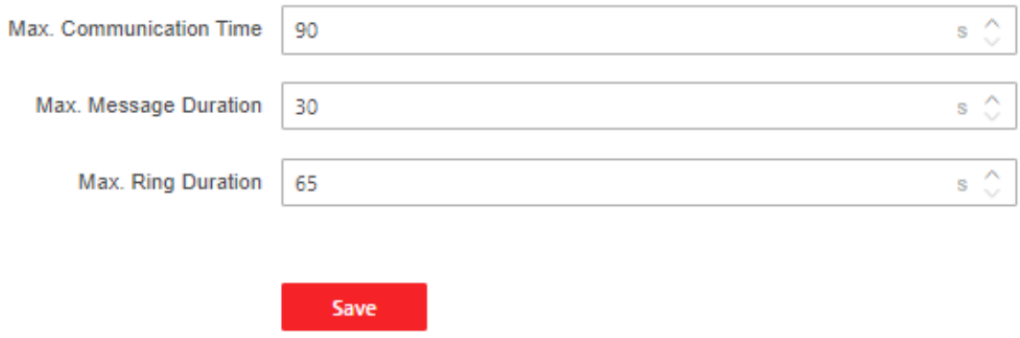


Figure 6-14 Call Settings

Set the **Max. Communication Time**, **Max. Message Duration**and **Max. Ring Duration** . Click **Save**.

Note

- The Max. communication time range is 90 s to 1800 s.
- The Max. message duration range is 30 s to 60 s.
- The Max. ring duration range is 65 s to 225 s.

Ringbacktone Settings

Steps

1. Click **Configuration → Intercom → Ringbacktone Settings** to enter the settings page.
2. Click to import new ringtone.

Note

The supported audio file type for importing is .wav. The file should be less than 800 KB.

Press Button to Call

Steps

1. Click **Intercom → Press Button to Call** to enter the settings page.
2. Set the parameters.
   - Check **Call Management Center**, **Specified Indoor Station**, **Indoor Station** or **APP** to set the button.

Note

If you check **Call Specified Indoor Station**, you should enter the specified indoor station No.

Call Priority

Enter a short description of your task here (optional).

Before You Start

Enter the prerequisites here (optional).
Enter the context of your task here (optional).

Steps

1. Click **Intercom → Call Priority** to enter the settings page.

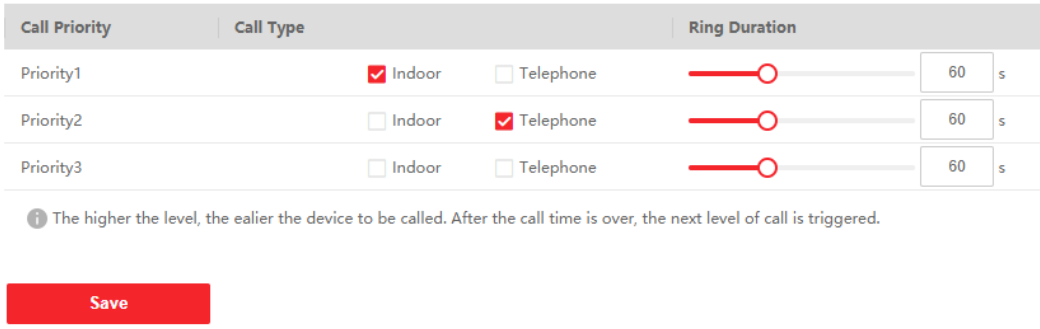


Figure 6-15 Call Priority

2. Check the **Call Type** and set the **Ring Duration** of each 3 priorities.
3. Click **Save** to enable the settings.

Note

The higher the level, the ealier the device to be called. After the call time is over, the next level of call is triggered.

Number Settings

Link the room No. and SIP numbers.

Click **Configuration → Intercom → Number Settings** to enter the page.

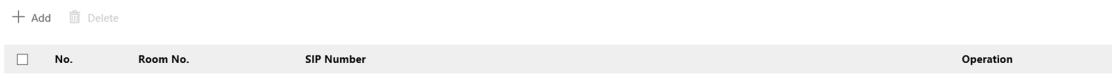


Figure 6-16 Number Settings

Click **+Add**, and set the **Room No.** and SIP numbers in the pop-up dialog box.

Click **Save** to save the settings.

6.8 Maintenance and Security

6.8.1 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **Maintenance and Security → Maintenance → Restart** .
Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

Note

Do not power off during the upgrading.

Restore Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the network parameters and the user information.

Import and Export Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.

Note

You can import the exported device parameters to another device.

Import

Click and select the file to import. Click **Import** to start import configuration file.

6.8.2 Device Debugging on PC Web

You can set device debugging parameters.

Steps

1. Click **Maintenance and Security → Maintenance → Device Debugging** .
2. You can set the following parameters.

   Enable SSH

   To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

   Print Log

   You can click **Export** to export log.

   Capture Network Packet

   You can set the **Capture Packet Duration**, **Capture Packet Size**, and click **Start** to capture.

6.8.3 Set Network Diagnosis

Enter the device IP address or domain name, you can perform PING settings. Debug the network according to the PING result.

Go to **Maintenance and Security → Maintenance → Network Diagnosis** .

Enter the device IP for PING operation, select the network connection mode, PING duration, and Ping data package size (default parameter is recommended.) Click **Diagnose**. The result will displayed in **PING Result**.

6.8.4 Set Protocol Testing

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **Maintenance and Security → Maintenance → Protocol Testing** .

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

6.8.5 Security Audit Log

Steps

1. Click **Maintenance and Security → Maintenance → Security Audit Log** to enter the page.
2. Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

3. The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

6.8.6 View Log via PC Web

You can search and view the device logs.

Go to **System and Maintenance → Maintenance → Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

6.8.7 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Import HTTPS Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **HTTPS Certificate** area, click **Create Certificate Request**.
3. Input certificate information and click **Save**.
   - Click **View** and the created certificate will be displayed.
   - The certificate will be saved automatically.
4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
   1) In the **Import Key** area, select a certificate from the local, and click **Import**.
   2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Create and Import SYSLOG Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **SYSLOG Certificate** area, click **Create Certificate Request**.
3. Input certificate information and click **Save**.

- Click **View** and the created certificate will be displayed.
- The certificate will be saved automatically.

4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
   1) In the **Import Key** area, select a certificate from the local, and click **Import**.
   2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **CA Certificate ID** area.

   Note

   The input certificate ID cannot be the same as the existing ones.

3. Upload a certificate file from the local.
4. Click **Import**.


See Far, Go Further