DS-KM9503 Main 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.

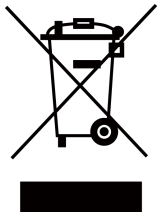
Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

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
Main Station	DS-KM9503

Contents

Chapter 1 Appearance

Front Panel

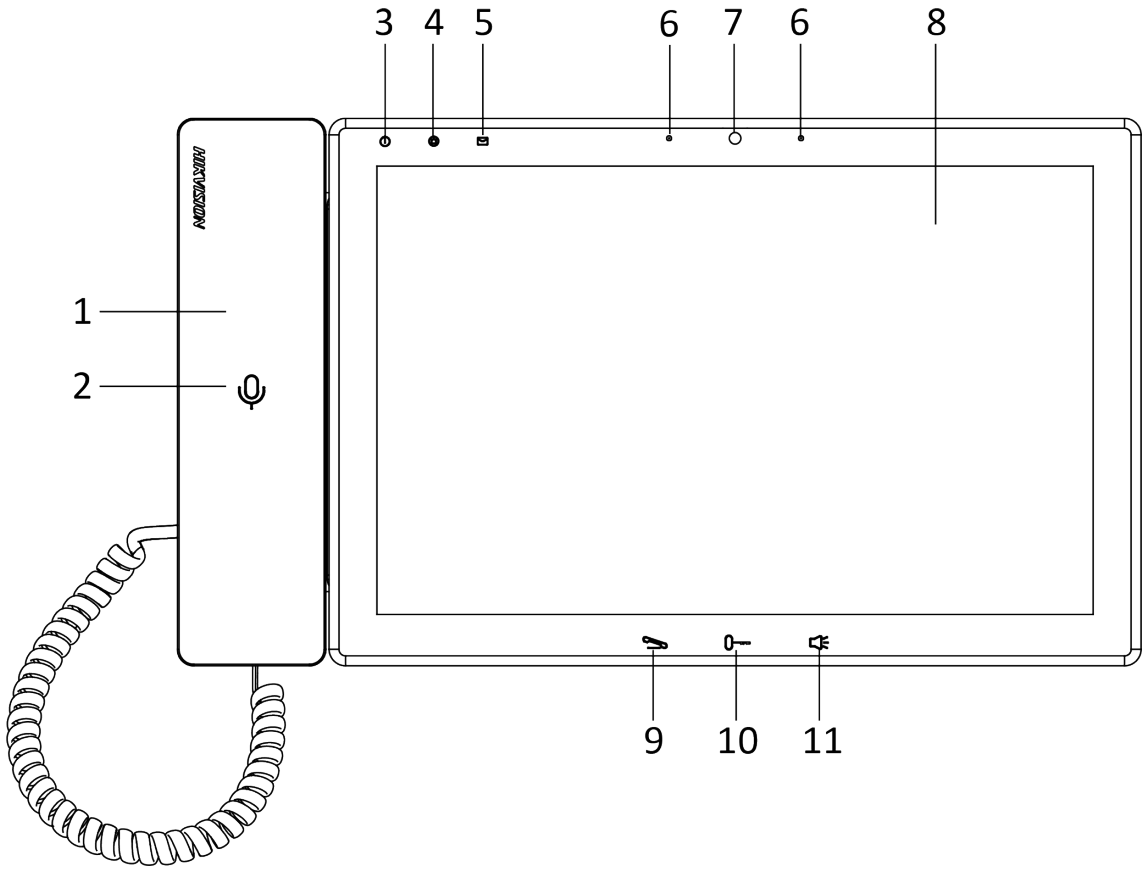


Figure 1-1 Front Panel

Table 1-1 Description

No.	Description	No.	Description
1	Phone	7	Camera
2	Phone Indicator(Reserved)	8	Screen
3	Power Indicator	9	Call/Hang Up Button
4	Alarm Indicator	10	Unlock Button
5	Information Indicator	11	Speaker Button
6	Microphone		

Note

You can hold the unlock button to unlock lock 1, and press the unlock button to unlock lock 2.

Top Panel and Rear Panel

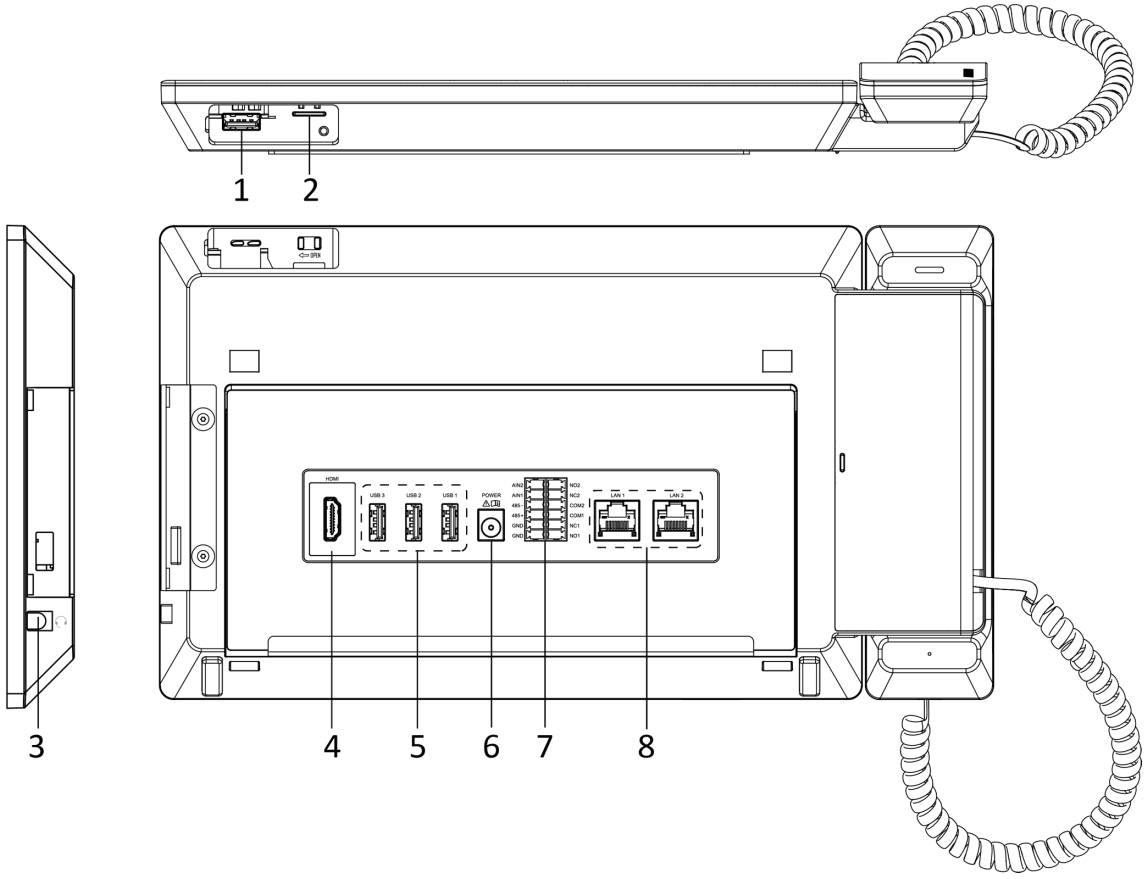


Figure 1-2 Top Panel and Rear Panel

Table 1-2 Description

No.	Description	No.	Description
1	Goose Neck Microphone Port	5	USB Interface
2	SD Card Slot	6	Power Interface
3	Earphone Interface	7	Terminals (Reserved)
4	HDMI	8	Network Interface

Speaker(Optional)

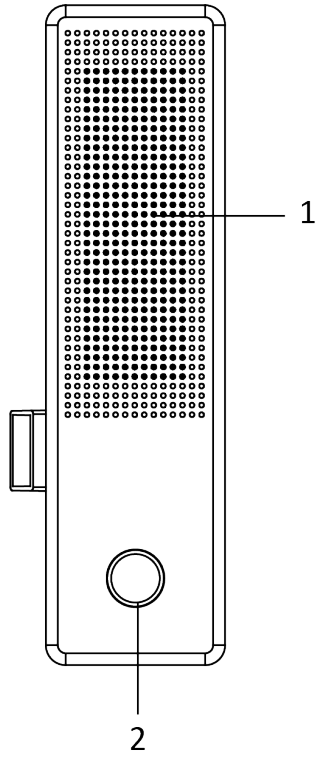


Figure 1-3 Speaker

Table 1-3 Description

No.	Description	No.	Description
1	Speaker	2	Fingerprint Module

Chapter 2 Terminal Description

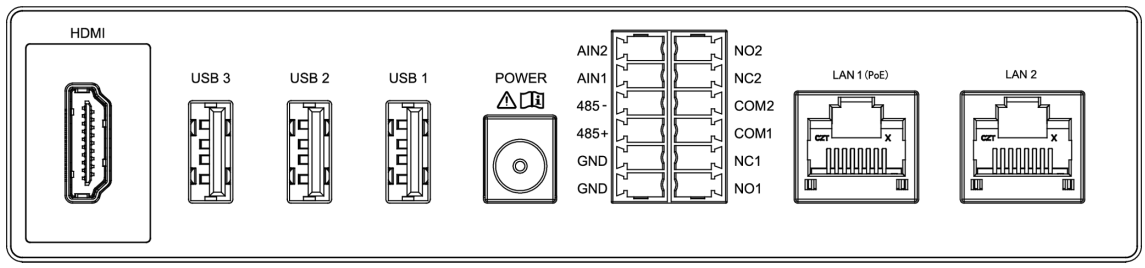


Figure 2-1 Terminal Description

Table 2-1 Terminal Description

Name	Interface	Description
Video Interface	HDMI	HDMI Signal Output
USB Interface	USB 1	USB Interface **Note** USB3 is used to debugging only. It cannot connect to USB flash drive.
	USB 2	
	USB 3	
Power Interface	POWER	12 VDC Power Input
Terminal (Reserved)	NO1	Alarm Output 1(NO)
	NC1	Alarm Output 1(NC)
	COM1	Common Interface
	NO2	Alarm Output 2(NO)
	NC2	Alarm Output 2(NC)
	COM2	Common Interface
	AIN1	Alarm Input 1
	AIN2	Alarm Input 2
	485+	RS-485 Communication Interfaces
	485-	
	GND	Grounding
	GND	Grounding

Name	Interface	Description
Network Interface	LAN1(PoE)	Network Interface (Support PoE)
	LAN2	Network Interface (Reserved)

Chapter 3 Installation

- Make sure the device in the package is in good condition and all the assembly parts are included.
- The power supply the door station support is 12 VDC. Please make sure your power supply matches your door station.
- Make sure all the related equipment is power-off during the installation.
- Check the product specification for the installation environment.

3.1 Table Bracket(Optional)

The device supports table mounting and wall mounting. The dimensions of the table bracket(optional) is shown as below.

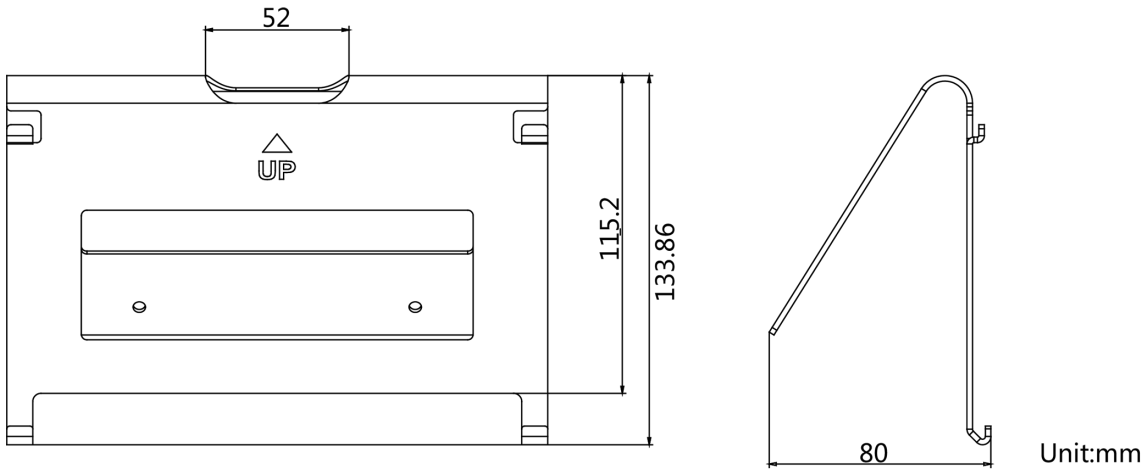


Figure 3-1 Table Bracket

3.2 Accessory Installation(Optional)

Before installing the device on the wall or on the table, you should install the accessories first.

Note

Ask our technique supports and sales and purchase mounting plate, speaker and goose neck microphone.

3.2.1 Install Speaker

Steps

1. Loose 2 screws on the rear panel of the device.

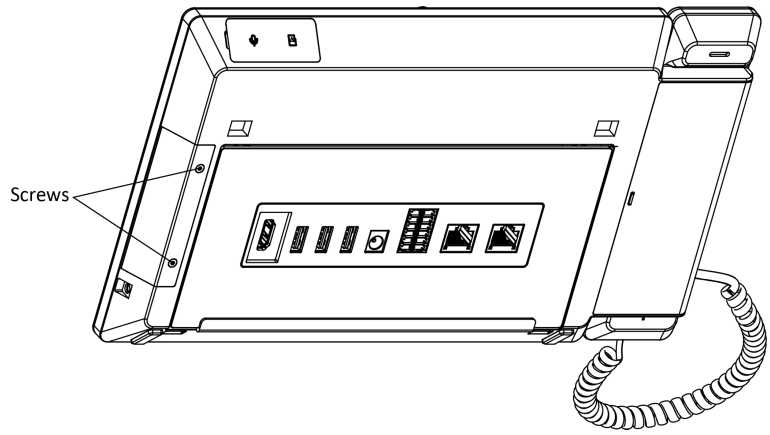


Figure 3-2 Loose the screws

2. Remove the cover from the device and install the speaker to the main station.

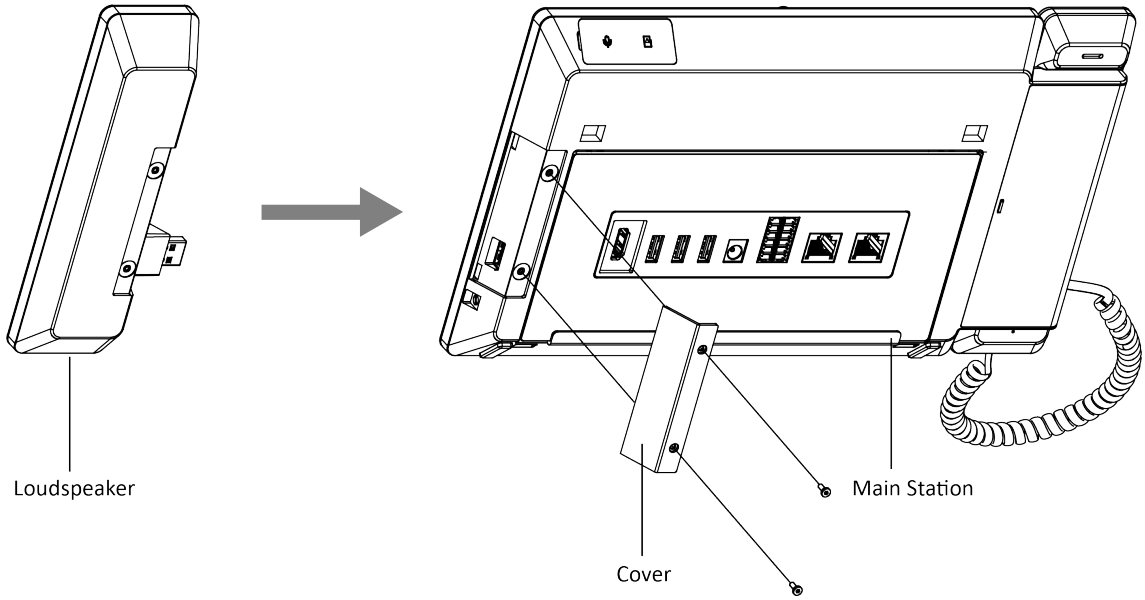


Figure 3-3 Install the Speaker

3. Use 4 screws to secure the speaker to the main station with the cover.

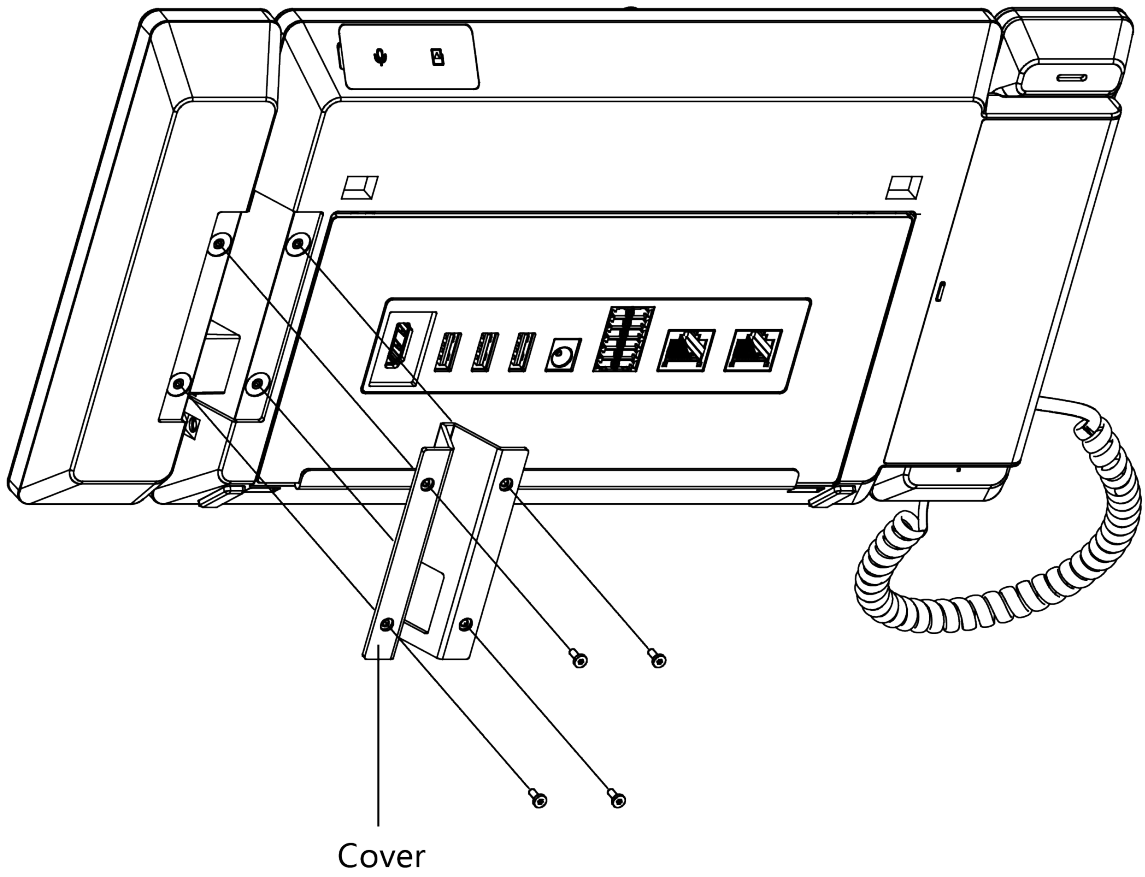


Figure 3-4 Secure the Speaker

Note

- The speaker and earphone can not be used at the same time. If you want to use the earphone, you should remove the speaker.
- When using earphones, the small size of the earphone plug should be selected. The size of the plug should be smaller than 7 mm.

3.2.2 Install Goose Neck Microphone

If you want to use the goose neck microphone to create two-way audio communication.

Steps

1. Remove the cover of the device on the top panel.
2. Insert the goose neck microphone to the interface.

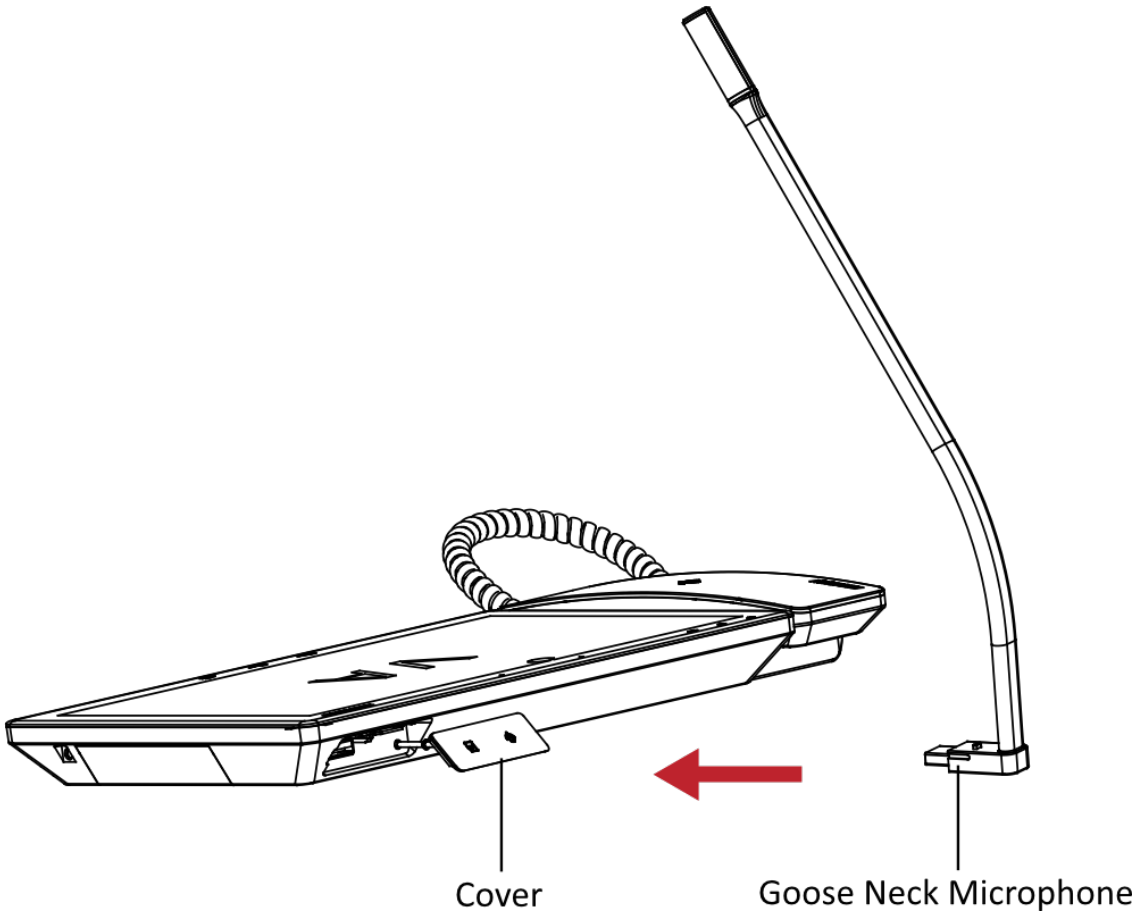


Figure 3-5 Install the Goose Neck Microphone

3.3 Wall Mounting

Before You Start

Note

- Tools that you need to prepare for installation: Drill (6).
- Make sure all the related equipment is power-off during the installation.

Steps

1. Place the table bracket on the wall. Mark the screw holes' position with a marker, and take out the the table bracket. Drill 4 holes according to the marks on the wall, and insert the expansion sleeves into the screw holes.
2. Secure the table bracket on the wall with 4 screws.
3. Hook the device to the table bracket tightly by inserting the hooks into the slots on the rear panel of the device,during which the lock catch will be locked automatically.

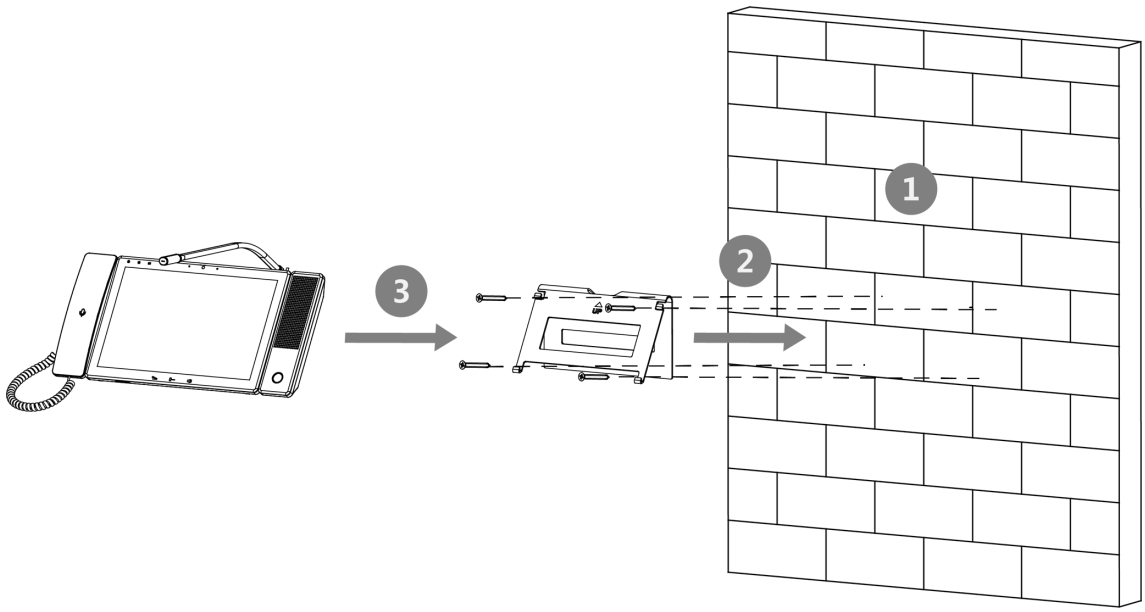


Figure 3-6 Wall Mounting

3.4 Table Mounting

Steps

1. Wiring the device and smooth the cables across the cable hole.

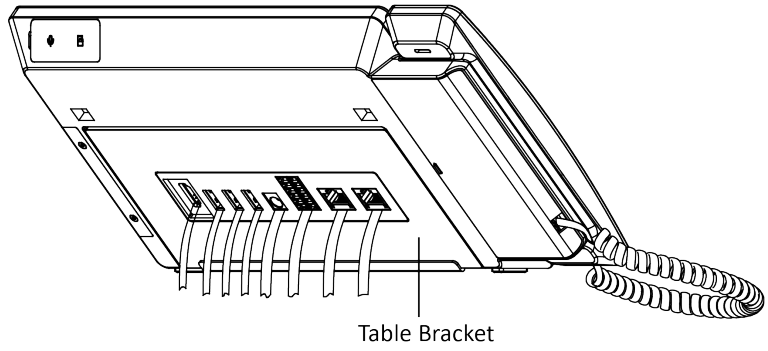


Figure 3-7 Smooth the Cable

2. Adjust the table bracket to the right angle and put the device on the right position.

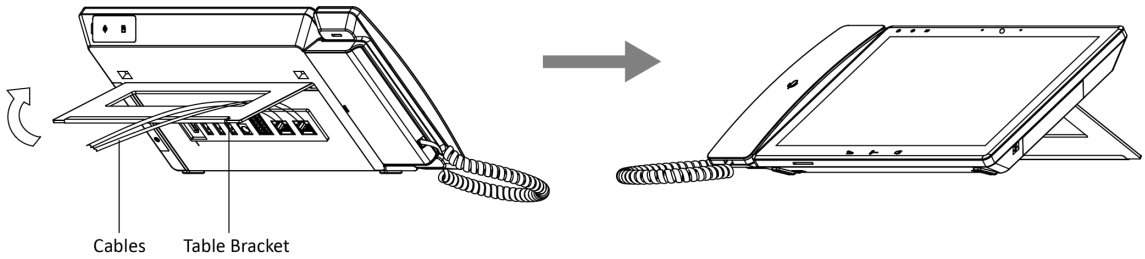


Figure 3-8 Adjust the Table Bracket

Note

Recommend the use of the table bracket: the maximum opening angle used.

Chapter 4 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

4.1 Activate via Device

If the device is not activated, you can activate the device after it is powered on.

On the Activate Device page, create a password and confirm the password. Tap **Activate** and the device will activated.

Caution

- The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.
- 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.
- Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

4.2 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 strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.
- 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.
- Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

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.

4.3 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 strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

Note

Characters containing admin and nimda are not supported to be set as activation password.

7. Click **OK** to activate the device.

Chapter 5 Local Configuration and Operation

5.1 Local Configuration of Main Station

5.1.1 Activate the Device

You can only configure and operate the main station after creating a password for the device activation.

Steps

1. Power on the device. It will enter the activation page automatically.
2. Create a password and confirm it.
3. Tap **OK** to activate the main station.

Note

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

5.1.2 Basic Settings

Local Network Parameters

Network connection is mandatory for the use of the main station. Set the network parameters parameters after activating the main station. Only when the IP address of the device is in the same network segment as other devices, it can work properly in the same system.

Two ways are available for you to set IP address: DHCP, and set IP address manually.

Steps

Note

The default IP address of the main station is 192.0.0.64.

1. Tap **Configuration** → → **Configuration** and enter the admin password to enter the settings page.

Note

Default admin password is the activation password.

2. Tap to enter the network parameters settings page.

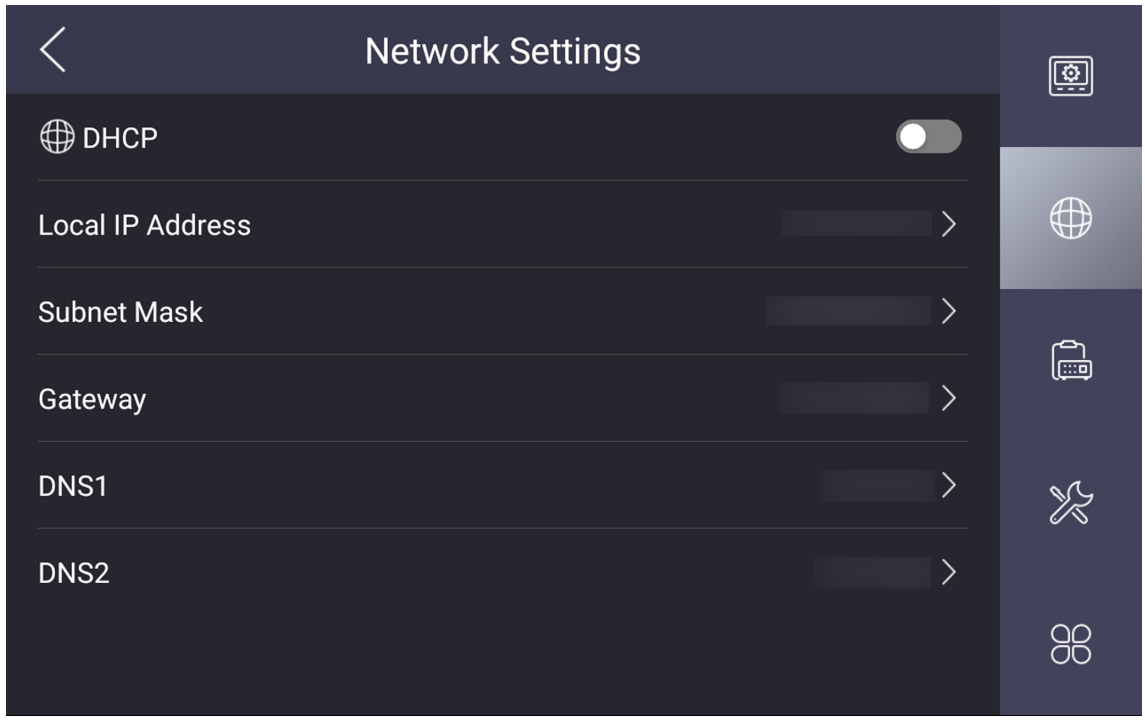


Figure 5-1 Network Settings

3. Edit the local network parameters.
- Set the **Local IP Address**, **Subnet Mask**, **Gateway** and DNS address manually.
- Enable **DHCP**, then the device can search and get an IP address automatically.

Linked Device Management

Linked network parameters refers to the network parameters of device (like indoor station, door station, doorphone, etc.), to whick the main station is linked.

Steps

1. Tap **Configuration →** → **Configuration** , and enter the admin password to enter the settings page.

Note

Default admin password is the activation password.

2. Tap to enter the device management page.

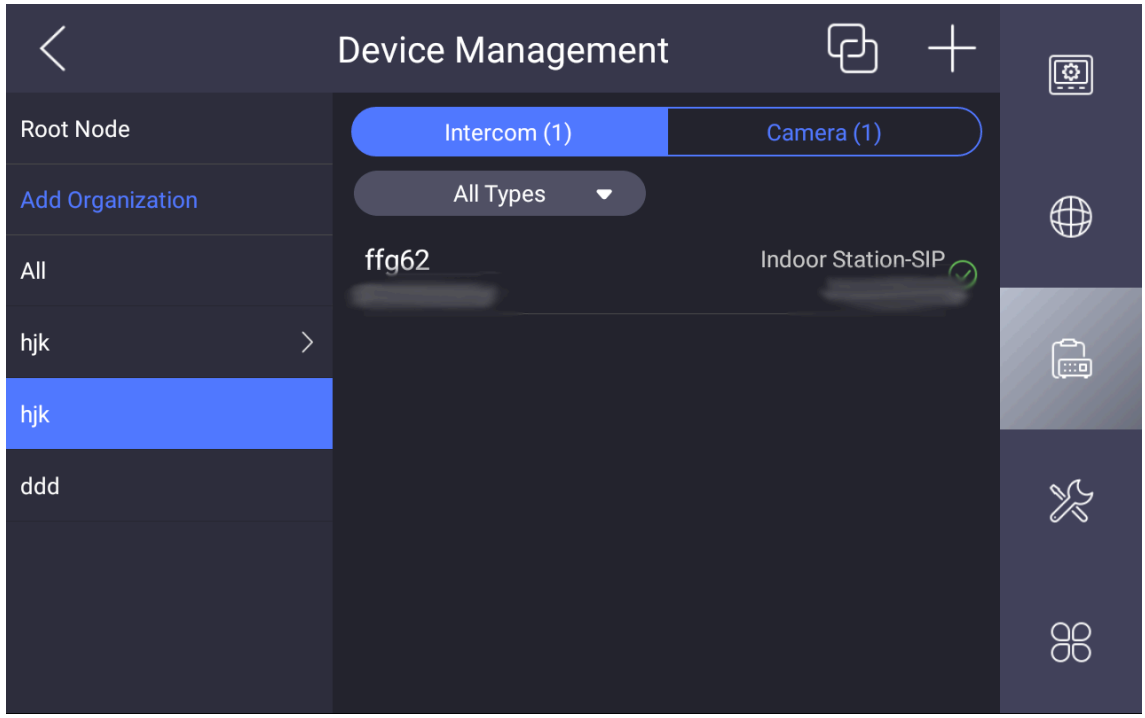


Figure 5-2 Device Management

3. Tap **Intercom**.
4. Tap **Add Organization** to create video intercom system.

   Example

   If the device is located in Phase 1 Building 1 Unit 1, you should tap **Add Organization** and create Phase 1 Building 1 Unit 1. First, tap **Add Organization** and enter the Phase 1 to add first level. Second, select the Phase 1 and tap **Add Organization** to add the Building 1 as the sub level. Repeat the steps above to add the last level.
5. Tap **+** to link the device.

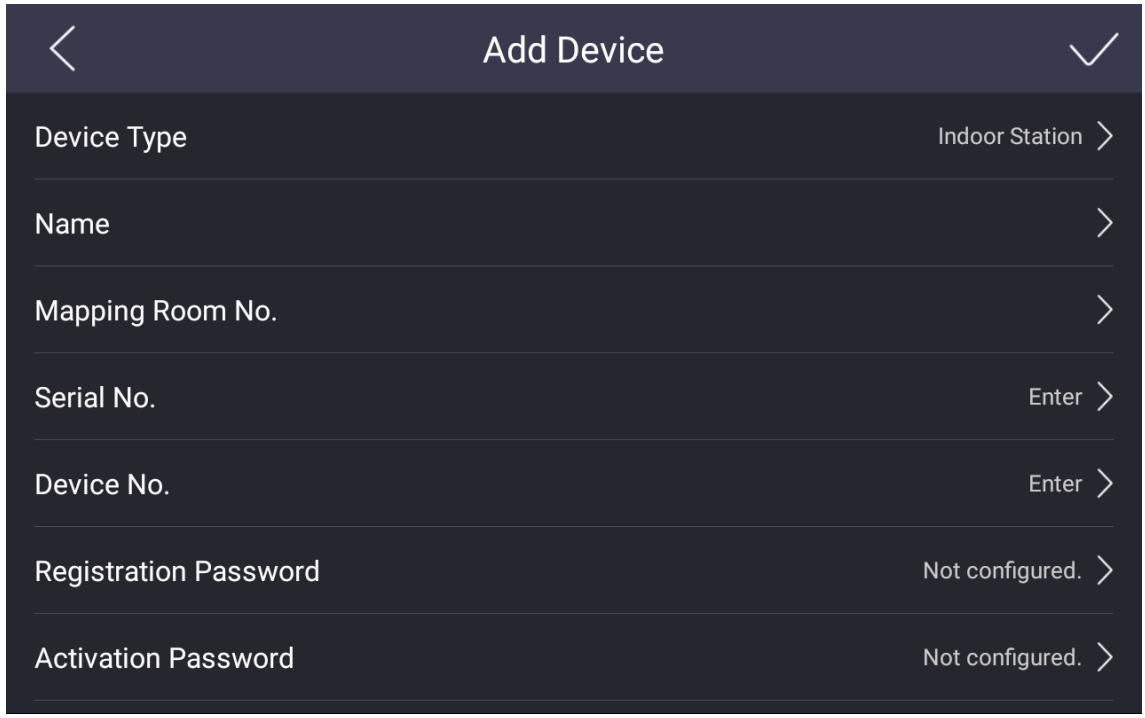


Figure 5-3 Add Linked Device

6. Select the **Device Type** as indoor station, outer door station, main station, door station or camera.
7. Set the **Serial No.**, **SIP Account**, **SIP Password**, **Activation Password**, **Device IP Address** and **Subnet Mask**.
8. Tap **√** to add.

Set Device No.

Main station No. can be dialed by other devices to call the main station in an intercom system. The main station No., is composed of the phase No. and No.

Steps

1. Tap **Configuration** → → **Configuration** , and enter the admin password to enter the settings page.

Note

Default admin password is the activation password.

2. Tap to enter the Main Station Settings page.

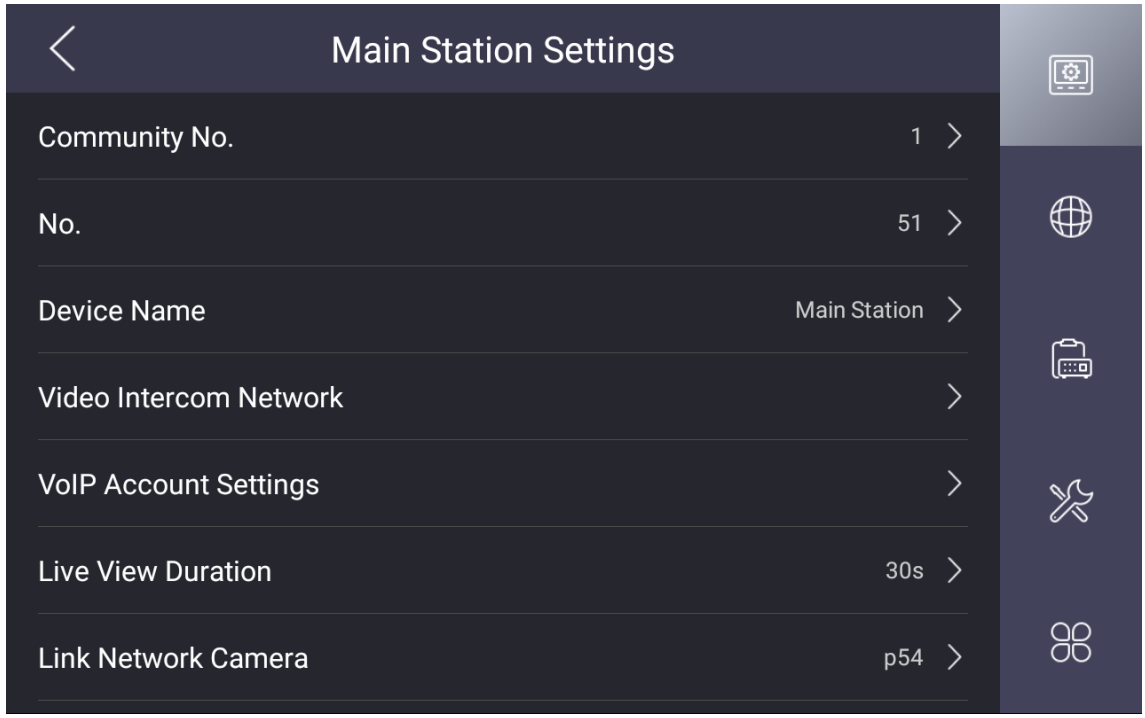


Figure 5-4 Device Settings

3. Edit the **Community No.** and **No.** of the device.
4. Tap **Video Intercom Network** to set the SIP server parameters. (Including registration password, private server IP, private SIP server port.)

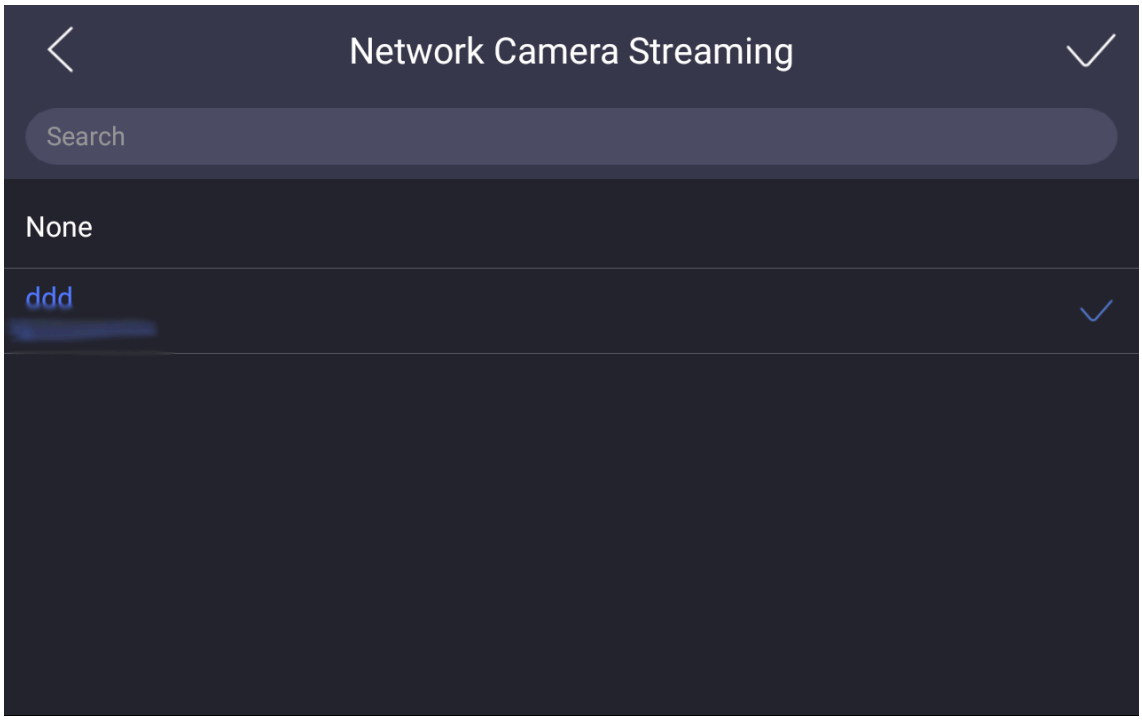
   Registration Password

   Enter the registration password for communication via SIP server.

   Private Server IP

   Enter the main station's IP address that used for VoIP communication. At this time, the main station is ussed as a SIP server. Other intercome devices should registered to this server address to realize communication.
5. Tap **VoIP Account Settings** and enable VoIP. Then you can edit VoIP account parameters. (Including user name, number, registered usered name, password, SIP server and private SIP.)
6. Set the **Live View Duration**.

7. Configure the **Link Network Camera**.



Note

You need to add IPC first. Then you can select the IPC you want from the list while doing configuration.

Add Camera

The main station can monitor via the camera. You should add cameras first.

Steps

1. Tap **Configuration** → → **Configuration** , and enter the admin password to enter the settings page.

Note

Default admin password is the activation password.

2. Tap to enter the device management page.

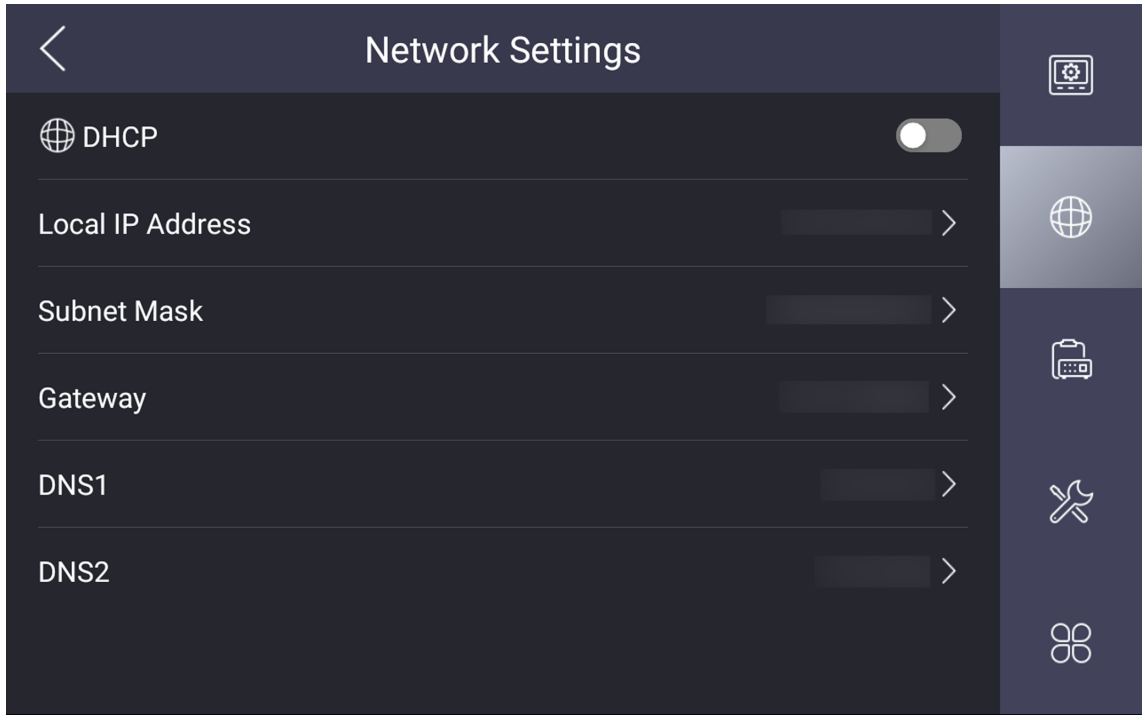


Figure 5-5 Device Management

3. Tap **Intercome**.
4. Tap **Add Branch** to create video intercom system.

   Example

   If the device is located in Phase 1 Building 1 Unit 1, you should tap **Add Branch** and create Phase 1 Building 1 Unit 1. First, tap **Add Branch** and enter the Phase 1 to add first level. Second, select the Phase 1 and tap **Add Branch** to add the Building 1 as the sub level. Repeat the steps above to add the last level.
5. Tap **+** to link the device.

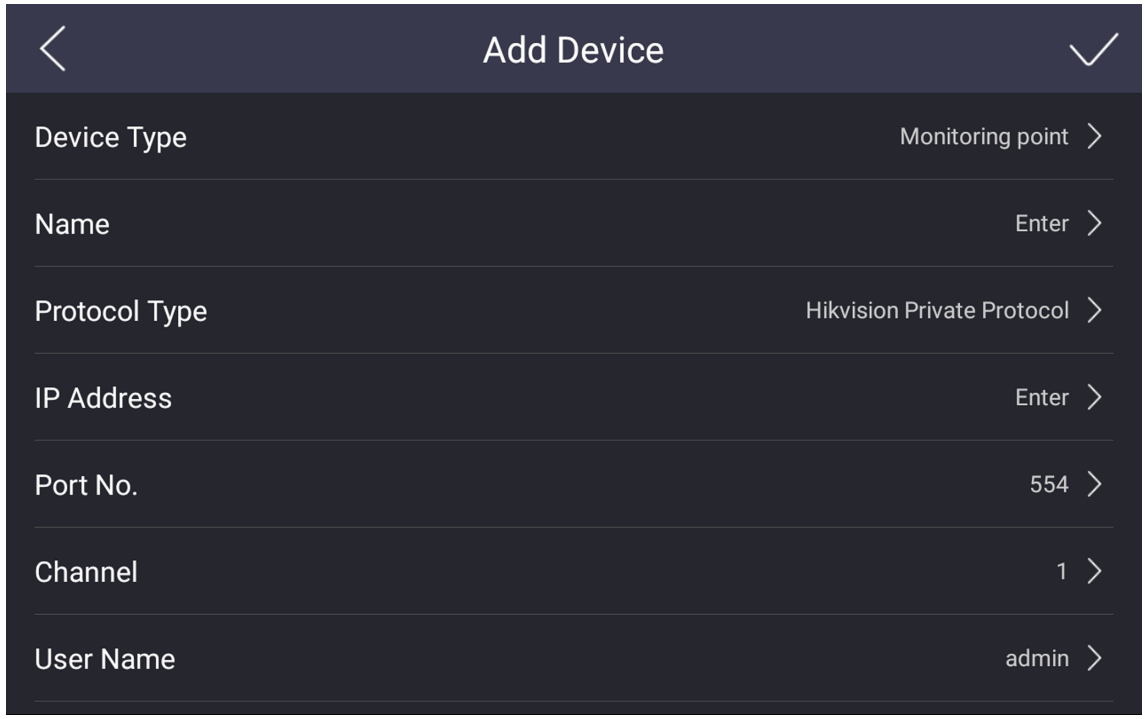


Figure 5-6 Add Camera

6. Select the **Device Type** as camera.
7. Set **Name**, **Protocol Type**, **IP Address**, **Port No.**, **Channel**, **User Name** and **Password** of the camera.
8. Tap **√** to add.

5.1.3 User Management

You can view the information of the user.

Steps

1. Tap **Configuration** → to enter the user management page.

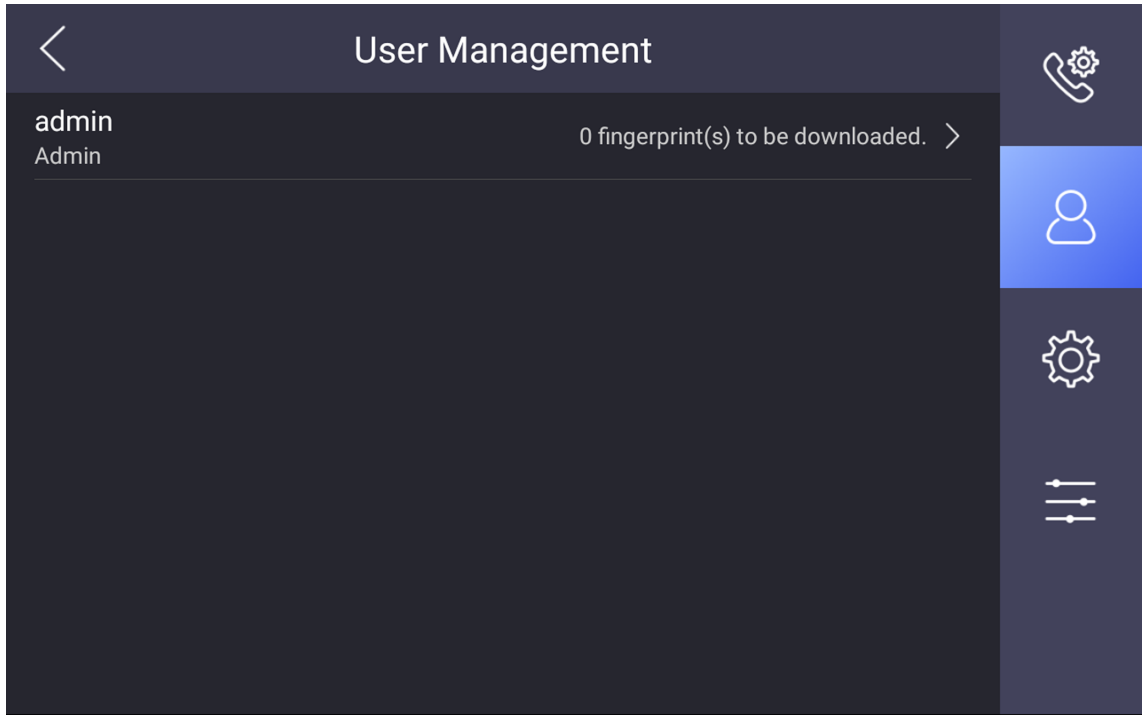


Figure 5-7 User Management

2. Tap **admin** and enter the admin password to view the details.

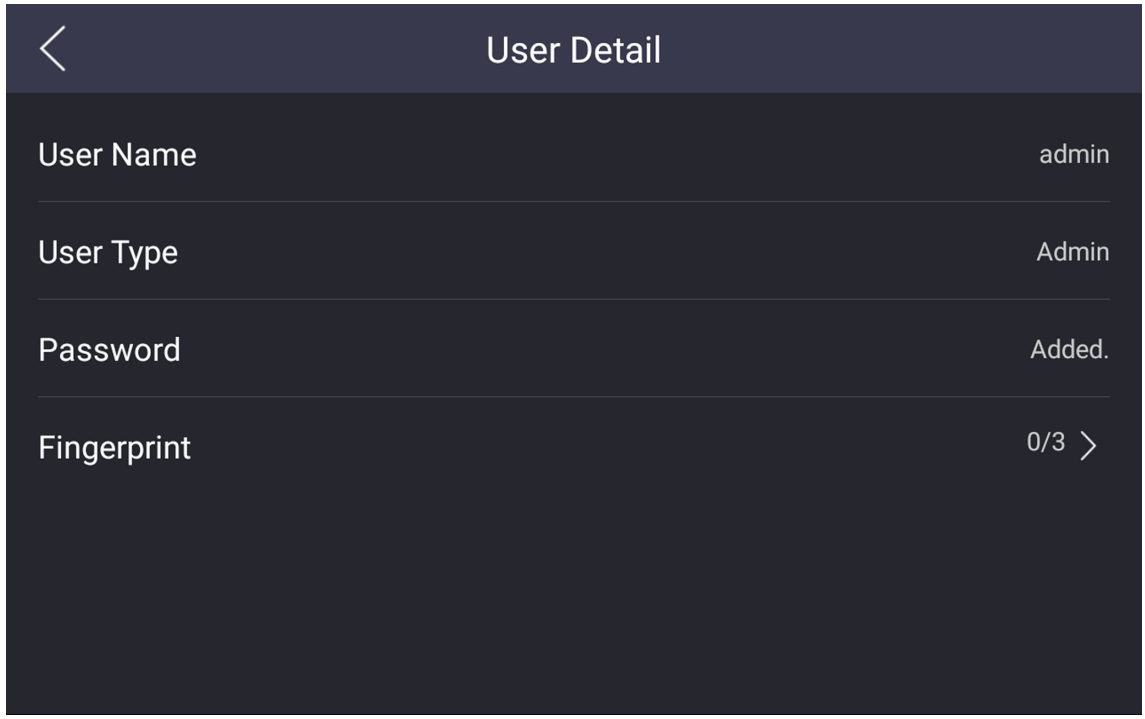


Figure 5-8 Details

3. Tap **Fingerprint** → **+** to add fingerprints refers to the tips on the page.

Note

Up to 3 fingerprints can be added.
Only when the fingerprint module is plugged in, can this function be used.

5.1.4 Synchronize Time

On the main page, tap the time displayed area to synchronize time manually. Here takes synchronizing time via local configuration for example.

Steps

1. Tap **Configuration** → ⚙ → **Time and Date** to enter the settings page.

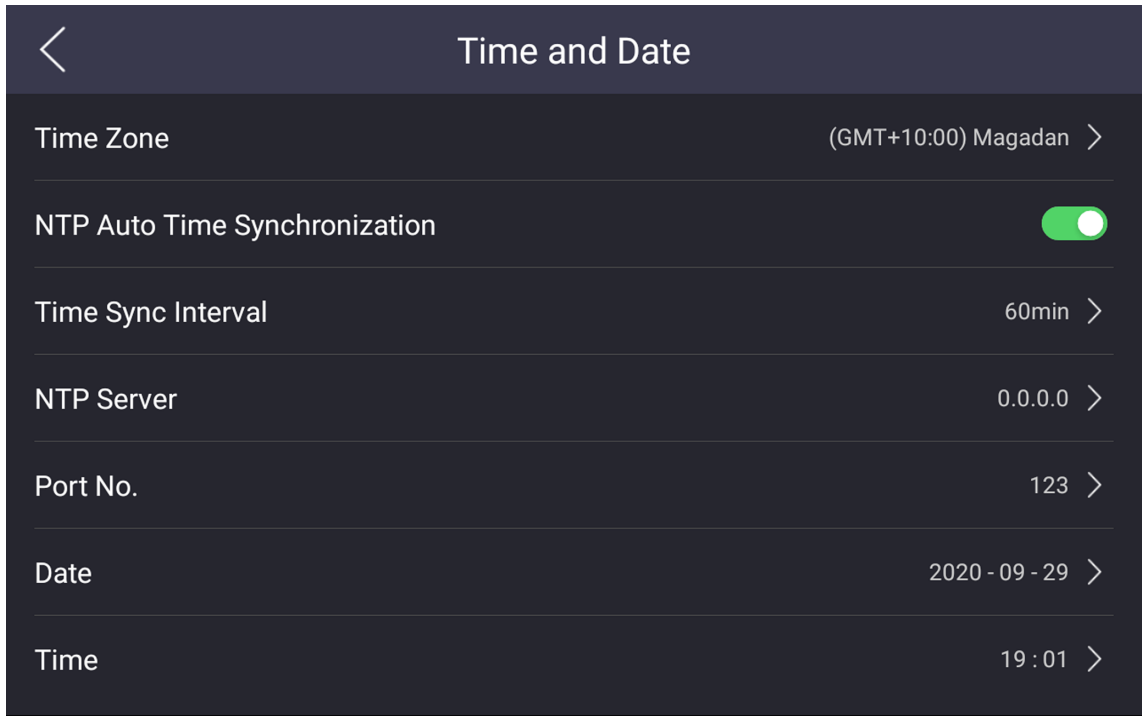


Figure 5-9 Time and Date

2. Select the **Time Zone**.
3. Synchronize time.
   - Configure the **Date** and **Time** manually.
   - Slide the slider to enable the **NTP Auto Time Synchronization** function.

     Set the synchronizing interval, enter the IP address of NTP server and port No.

5.1.5 Call Settings

You can set the ringtone, ring duration, call volume, notification volume and enable the group call and microphone functions.

Steps

1. Tap **Configuration** → to enter the call settings page.

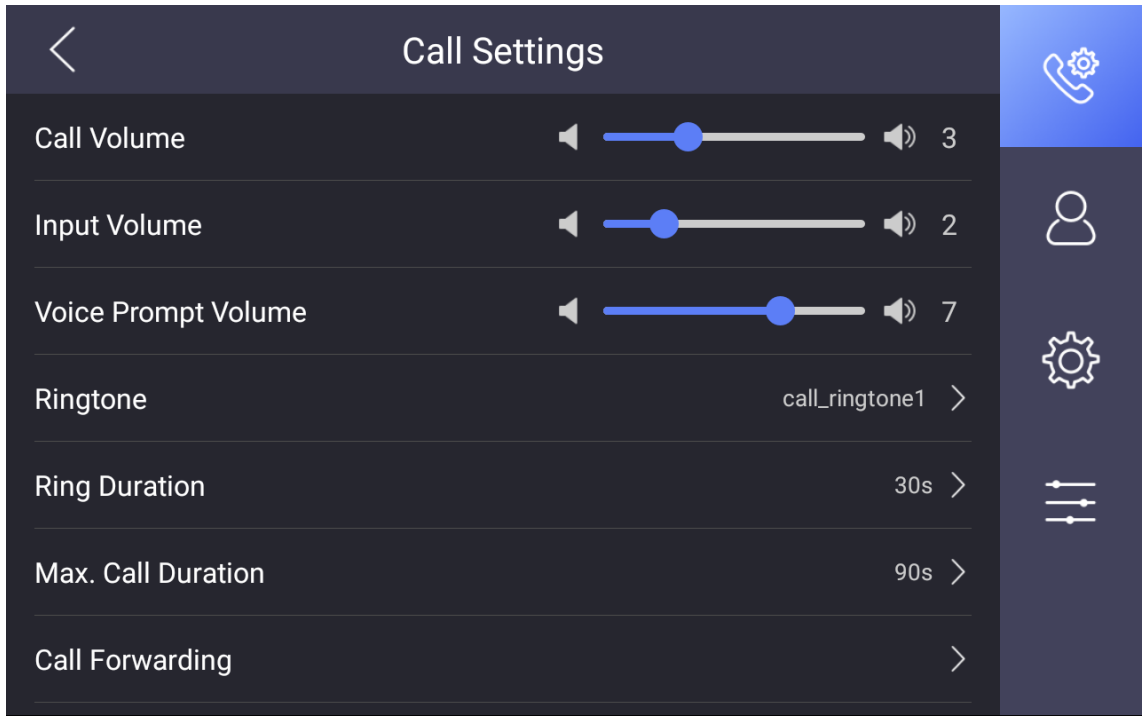


Figure 5-10 Call Settings

2. Set corresponding parameters.

Ringtone

There are 3 ringtones by default, and you can custom and import at most 4 ringtones via Batch Configuration Tool or **iVMS-4200** Client Software.

Ringtone Duration: The maximum duration of main station when it is called without being accepted. Ringtone duration ranges from 30 s to 60 s.

Volume Settings

Adjust the call volume, input volume and voice prompt volume.

Max. Call Duration

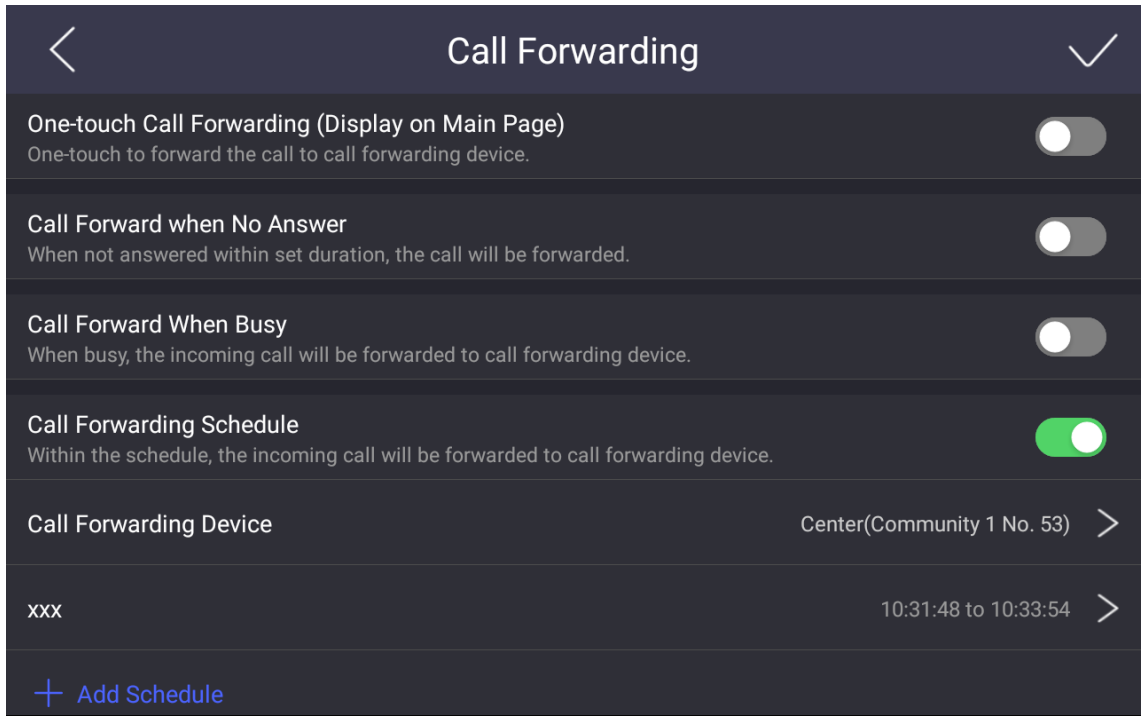
The maximum duration of calling between main station and other devices. It ranges from 90 s to 120 s.

Group Call

Slide to enable the group call function, then the device can receive more than 2 devices calling at the same time.

Call Forwarding

Slide to enable one-touch call forwarding, call forward when no answer, call forward when busy or call forwarding schedule.



One-touch Call Forwarding (Display on Main Page)

One-touch to forward the call to call forwarding device.

Call Forward when No Answer

When busy, the incoming call will be forwarded to call forwarding device.

Call Forwarding Schedule

Within the schedule, the incoming call will be forwarded to call forwarding device.

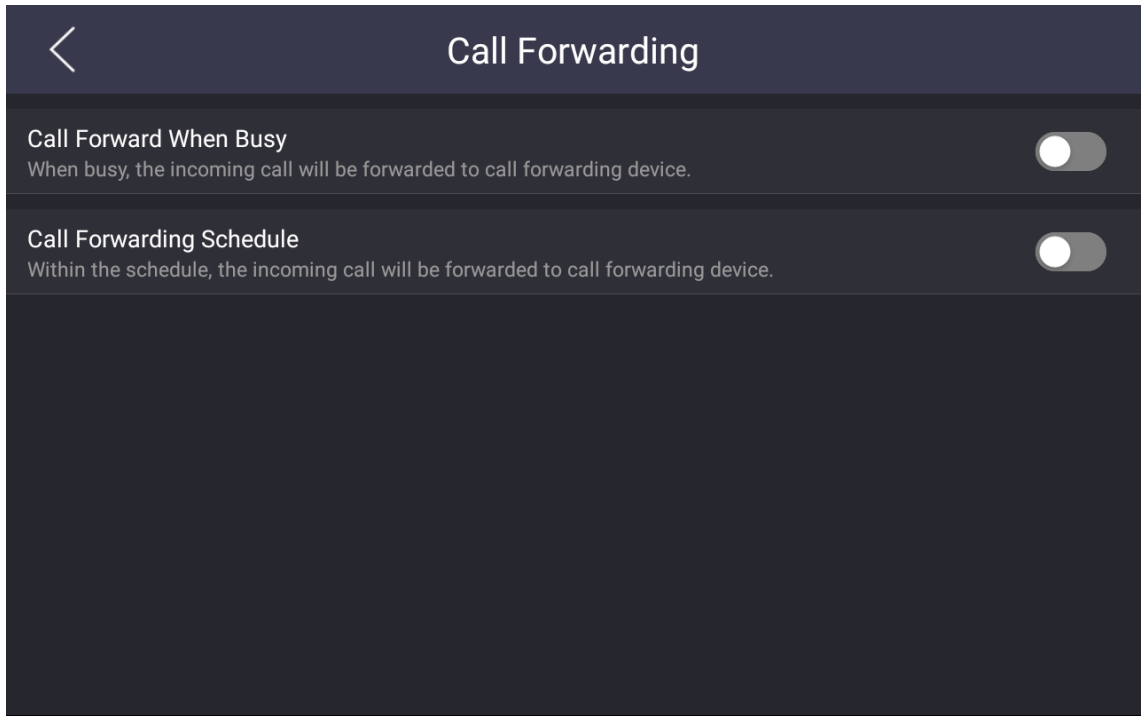
Call Forward When Busy

When busy, the incoming call will be forwarded to call forwarding device.

Note

You can also visit the call forwarding setting page when trying to add device.

- Go to **Cofiguration → Advanced Settings → Configuration →**  .
- Tap the device you want to configure.
- Click **Call Forwarding** to enable call forward when busy or call forwarding schedule.



VoIP Contact

Add VoIP contact and view them in the list. Hold one of the contacts to edit or delete the selected contact.

5.1.6 Restore Main Station

Steps

1. Tap **Configuration →** ☰ **→ Configuration** and enter the admin password to enter the settings page.

Note

Default admin password is the activation password.

2. Tap ⚙ to enter the system maintenance page.

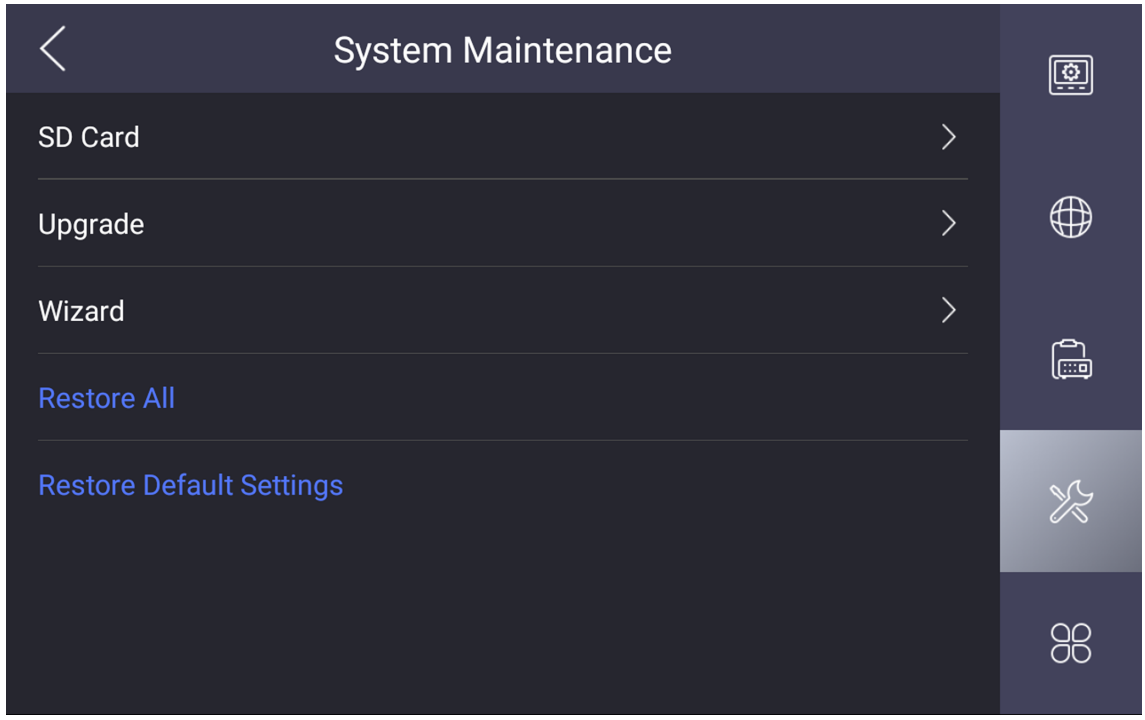


Figure 5-11 Maintenance

3. Restore All and Restore Default Settings.

Restore All

Tap Restore All to restore all parameters and reboot the system.

Restore Default Settings

Tap Restore Default Settings to restore the default settings and reboot the system.

5.1.7 Upgrade

Before You Start

Plug in a USB flash driver or an SD card with upgrading package.

Steps

1. Tap **Configuration** → → **Configuration** and enter the admin password to enter the settings page.

Note

Default admin password is the activation password.

2. Tap to enter the system maintenance page.

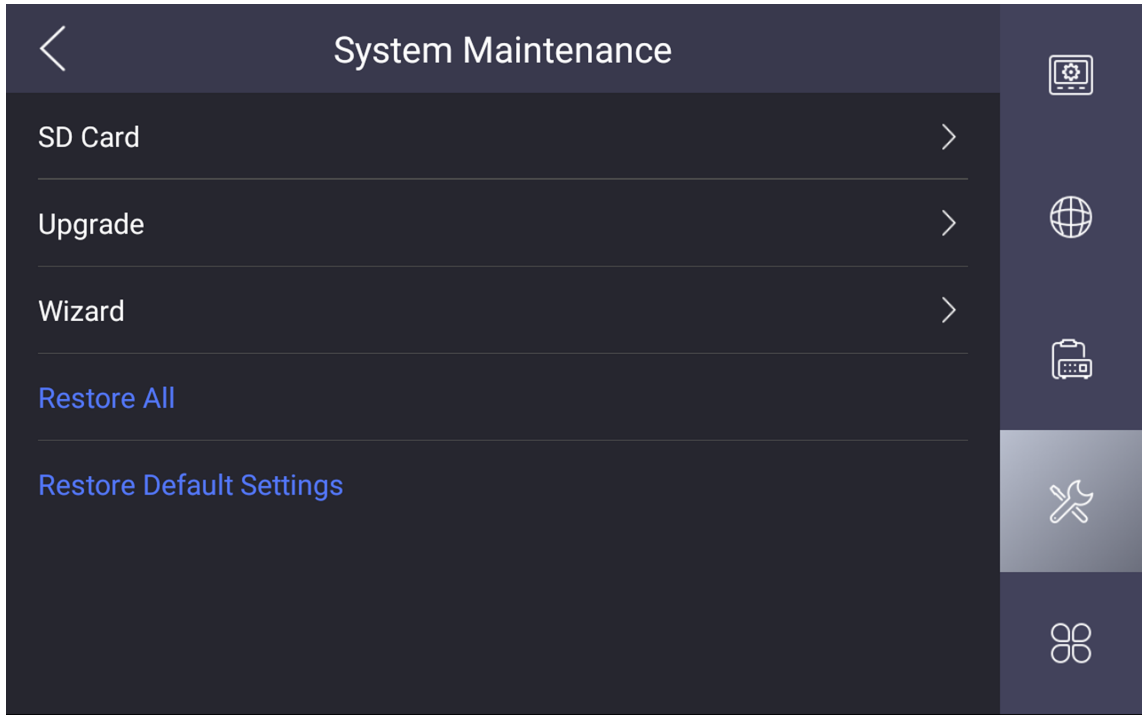


Figure 5-12 Maintenance

3. Tap **Upgrade** to get the upgrading package to upgrade the device.

5.1.8 Maintenance

SD Card

Tap **Configuration** → → **Configuration** and enter the admin password to enter the settings page. Tap to enter the maintenance page.

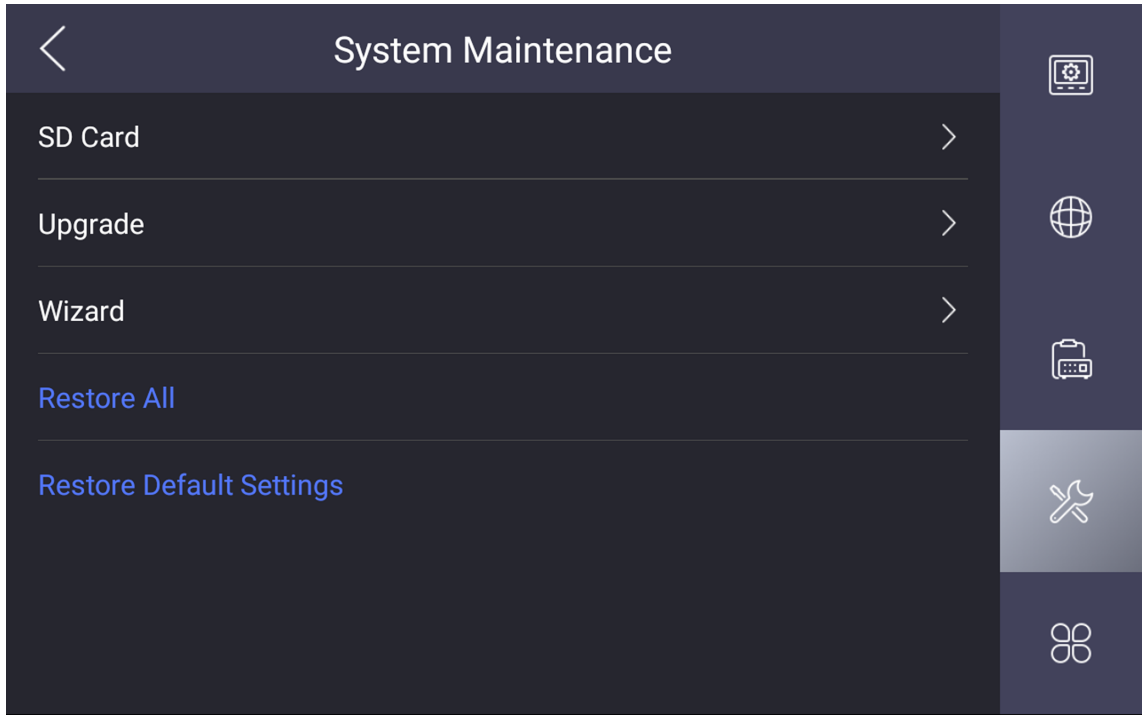


Figure 5-13 Maintenance

Tap **SD Card** to view the capacity of the SD card. You can format and uninstall the SD card.

Wizard

Tap **Configuration** → → **Configuration** and enter the admin password to enter the settings page.
Tap to enter the maintenance page.
Tap **Wizard** to configure the system quickly.

Permission Verification

Tap **Configuration** → to enter the settings page.

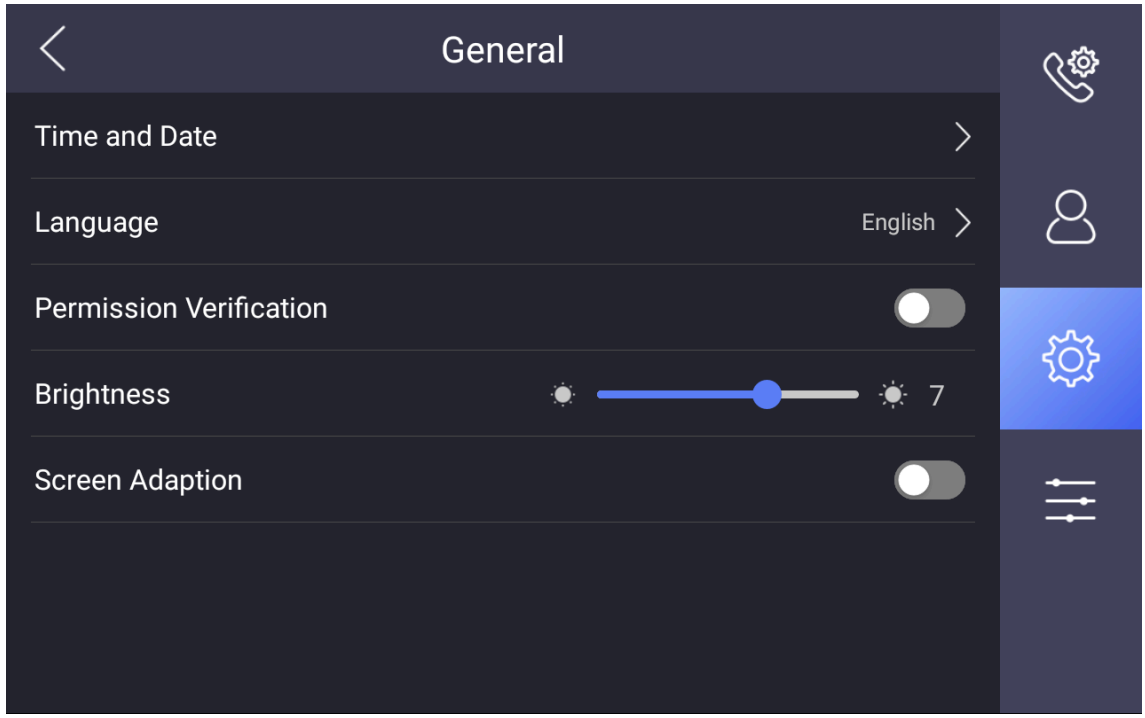


Figure 5-14 General Settings

Slide to enable the permission verification and screen adaption function.

Screen Adaption

After enable screen adaption function, the page will automatically adapt to the screen size of the device.

Permission Verification

After enable permission verification, you need to enter your user name and password to awake the device.

Brightness Adjustment

Tap **Configuration** → to adjust the brightness.

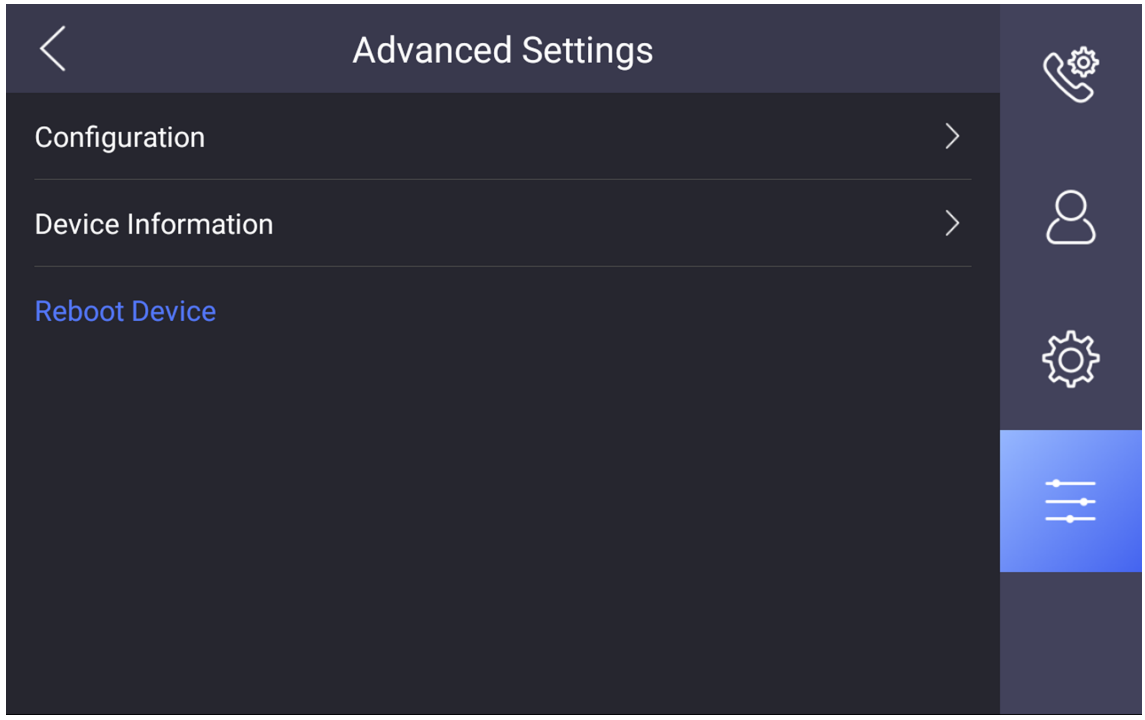


Figure 5-15 Advanced Settings

Tap **Configuration** → to enter the settings page.
Tap **Reboot Device** to reboot the system.

Note

Please do not cut the power during rebooting.

5.1.9 Device Information

View the device information, including the version information, model, serial No., LAN2 IP address, LAN2 Mac address and open source disclaimer.

Steps

1. Tap **Configuration** → → **Device Information** to enter the Device Information page.
2. View the version information, model, serial No., LAN2 IP address, LAN2 Mac address and open source disclaimer.
3. **Optional:** Tap **Open Source Disclaimer** to view the OSS statement.

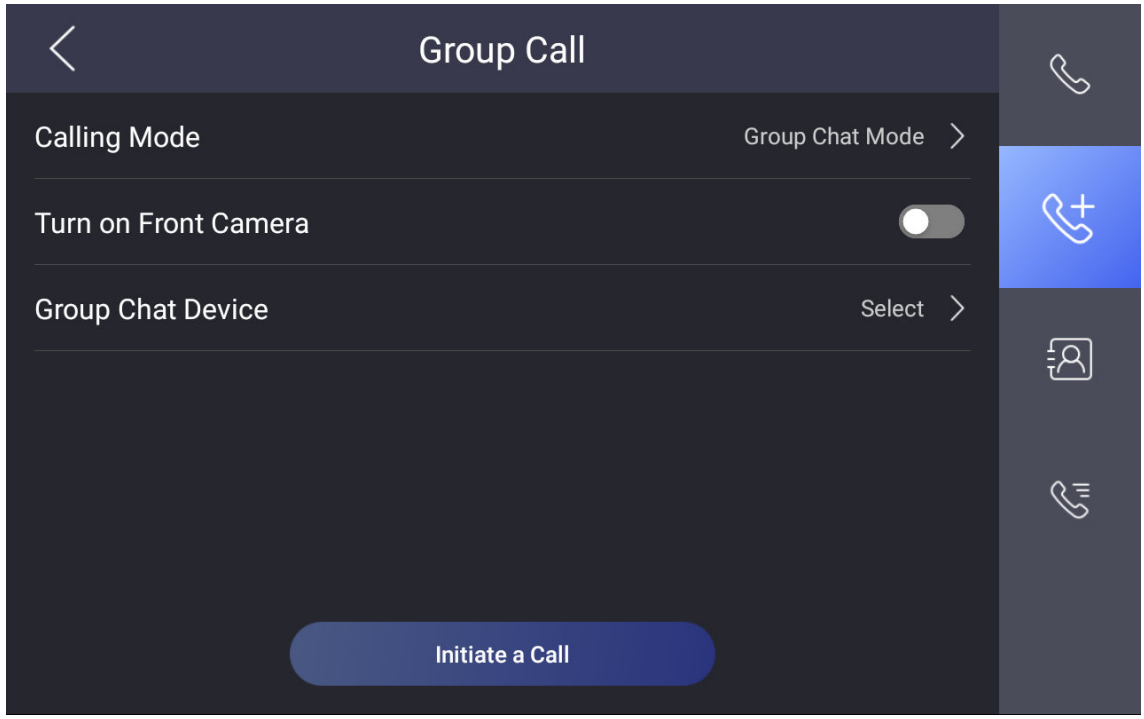
5.2 Local Operation of Main Station

5.2.1 Call Settings

Group Call Settings

You can initiate group call with more than 2 devices via the main station. The device can also receive more than 2 devices calling at the same time.

1. Tap **Call** → on the main page.



2. You can select calling mode and group chat device. Slide to enable turn on front camera.
3. Tap **Initiate a Call**.

Call Resident

Call the indoor station via the main station.

Steps

1. Tap **Call** → to enter the call page.

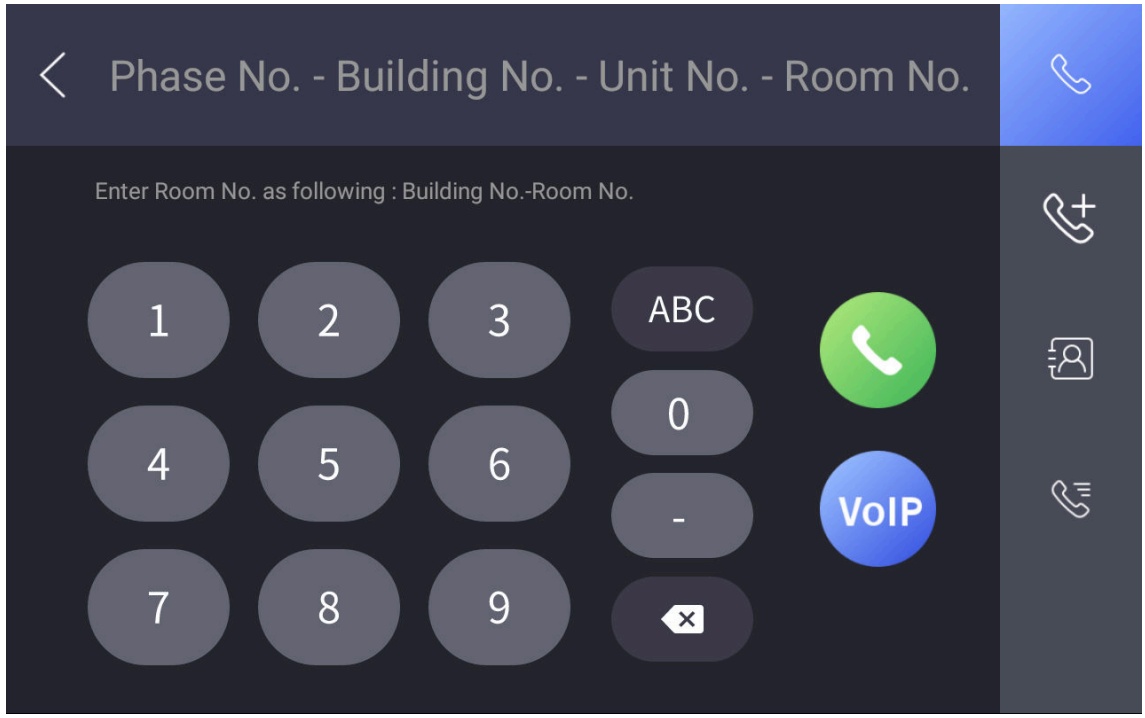


Figure 5-17 Call Page

2. Enter the calling number to call.

Note

- The calling number format should be x-x-x-xxx. For example, the calling number of Community 1, Building 2, Unit 3, and Room 405 is 1-2-3-405. Tap the call button to start an audiovisual call.
- The community No. can be omitted.

Receive Call

The main station can receive the call from the indoor station, the door station, and the other main station.

When the main station receives the call from the other device, tap the receive call button to receive the call. Or tap the hang up button to end the call.

During the call, you can tap the unlock button to unlock the door remotely.

Note

The maximum call duration between the main station and the indoor station is 120 s.

View Call Logs

View call logs of the main station.

Steps

1. Tap **Call** → on the main page.

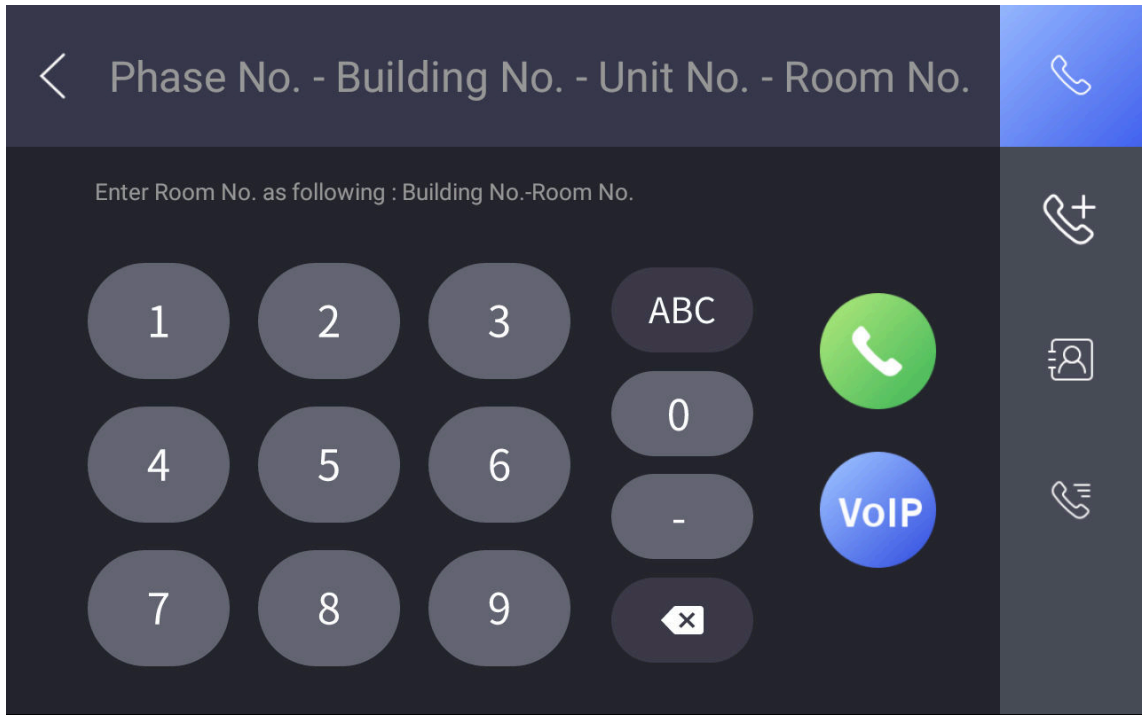


Figure 5-18 Call Log Page

2. View the call logs.

Note

Up to 2000 call logs can be viewed.

3. **Optional:** Hold one of the call logs to clear all call logs or delete the select call log.

5.2.2 Live View

View the live videos of other devices from the main station.

Steps

1. Tap **Live View** on the main page.

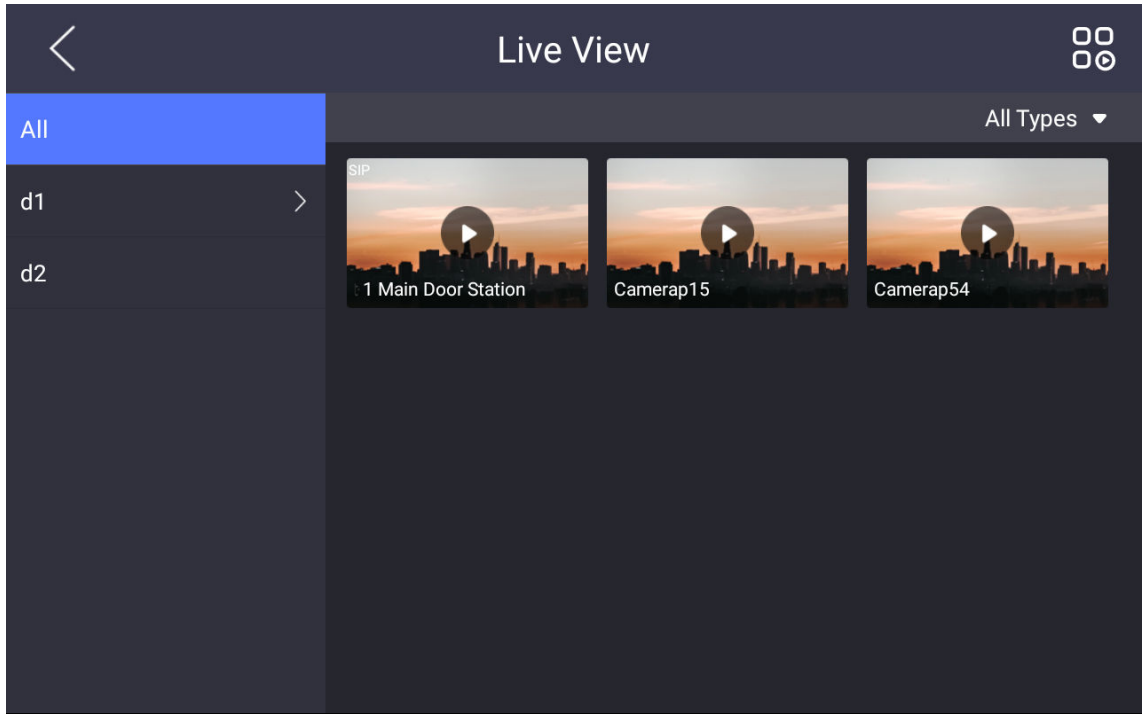


Figure 5-19 Live View Page

2. View the live videos of other devices.
3. **Optional:** Tap the unlock button to unlock the door.

5.2.3 The Third-Party App Settings

Install the App

Install the third-party App to your device.

Steps

1. Tap **Configuration** → → **Configuration** .
2. Enter the configuration password.

Note

By default, the configuration password is the activation password.

3. Tap to view the third-party apps.

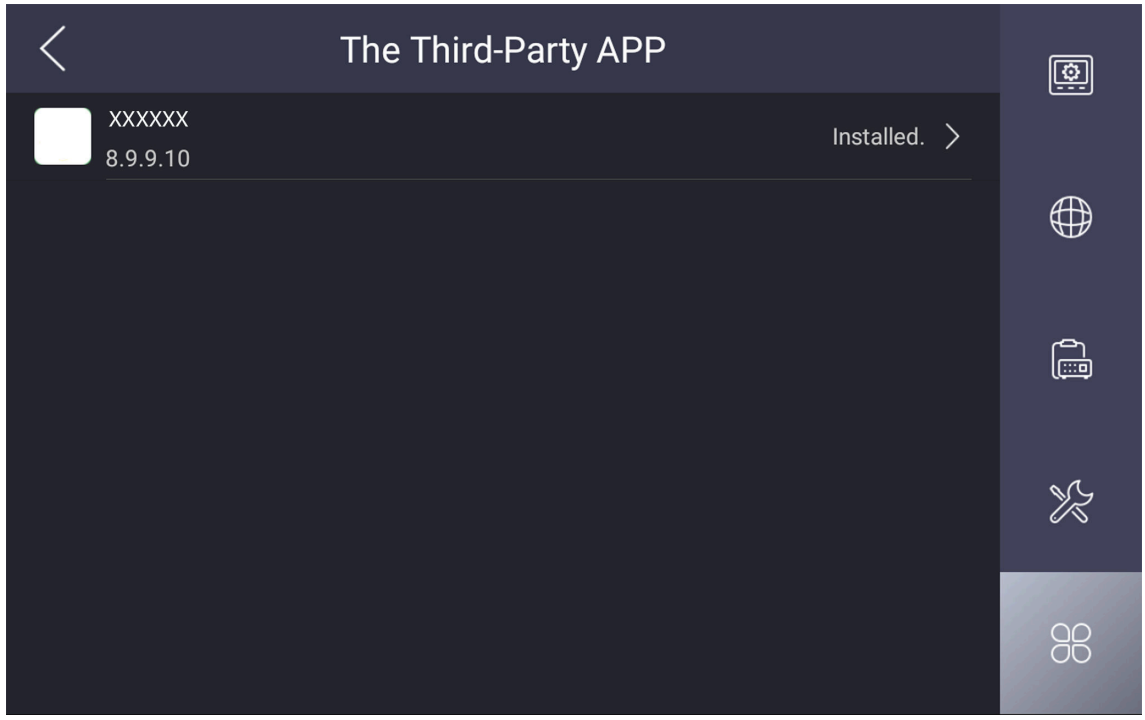


Figure 5-20 Add the Third-Party Apps

4. Tap **New APP** to view the details.
5. **Optional:** Tap the added third-party app, and tap **Clear Memory** to clear the app's memory or uninstall the app.

Uninstall the App

Steps

1. Tap **Configuration** → ☰ → **Configuration**
2. Enter the configuration password.

Note

By default, the configuration password is the activation password.

3. Tap ⁘ to view the third-party apps.
4. Select an App and tap **Uninstall Application**.

Note

You can also uninstall the Apps via client software remotely.

5.2.4 Information Management

You can view the received alarm logs, captured pictures, recorded videos, and recorded audios.

Take viewing alarm logs as an example. Tap **Message** → and you can view all received alarm logs.

Hold one of the logs to clear all logs or delete the selected log.

Note

Up to 200 alarm logs, 200 captured pictures, 200 recorded videos, 200 recorded audios can be viewed.

Chapter 6 Quick Operation via Web Browser

6.1 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.

Note

After you change the system language, the device will reboot automatically.

6.2 Time Settings

Click in the top right of the web page to enter the wizard page. After setting device language, you can click **Next** to enter the **Time Settings** 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.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

6.3 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 device No.

Community No.

Set the device community No.

No.

Set the main station No.

Note

The No. should be 51~99.

3. Set the video intercom network parameters.

Registration Password

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

Private SIP Server Port

Refers to the SIP server Port.

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

Chapter 7 Operation via Web Browser

7.1 Login

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

Note

Make sure the device is activated. For detailed information about activation, see ***Activate 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**.

Note

5 failed password enterings will lock the device. You should try again after 30 min.

7.2 Device Management

You can manage the linked device on the page.

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

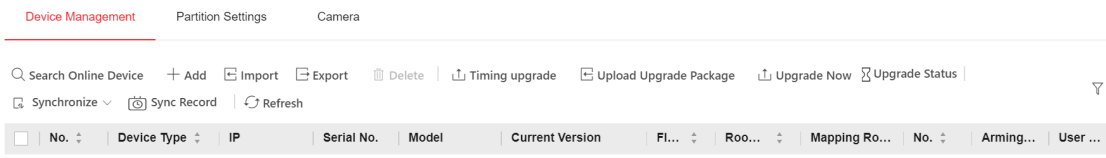


Figure 7-1 Device Management

Add Device

- Click **Add** to add the indoor station or sub door station. Enter the parameters and click **OK** to add.
- Click **Import**. Enter the information of the device in the template to import devices in batch.

Export

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

Delete

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

Synchronization Settings

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

Upgrade

Timing Upgrade

You can choose to **Enable Upgrading Device Automatically** or set upgrade time so that the device will upgrade within the time. Click **Save**.

Upload Upgrade Package

You can import upgrading package from local and select device type. Click **OK** to upgrade.

Upgrade Now

Check the device you would like to upgrade and click **OK** to upgrade.

Upgrade Status

You can view the upgrade status of linked devices.

Refresh

Click **Refresh** to get the device information.

Optional: Set Device Information.

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

7.3 Camera Management

You can add, edit or delete the cameras through the camera management operation.

7.4 Overview

You can view linked devices, network status and basic information.

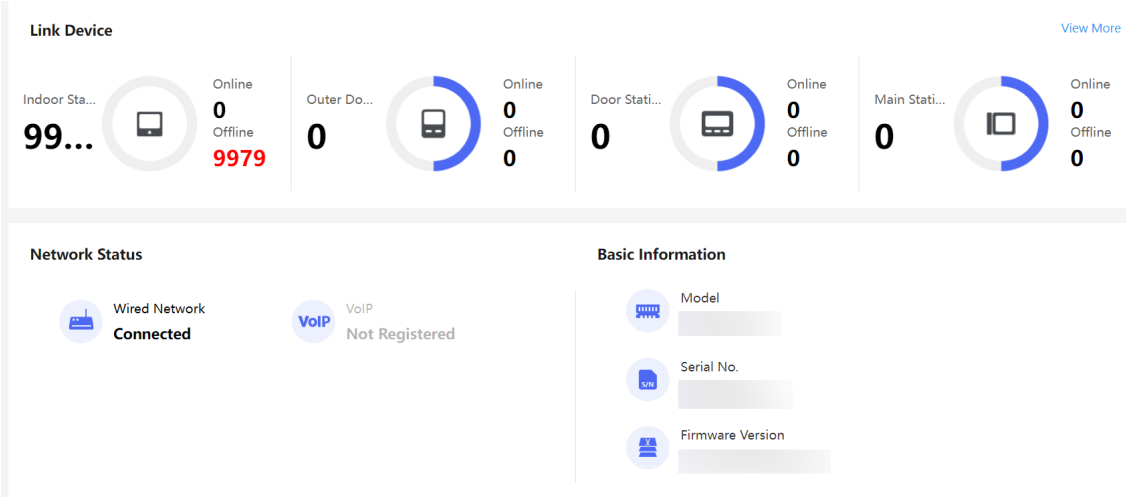


Figure 7-2 Overview Page

Function Descriptions:

Linked Device

You can view linked devices and their online status.

Network Status

You can view the connected and registered status of wired network, wireless network, ISUP and cloud service.

Basic Information

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

View More

You can click **View More** to enter the page of **Device Management**.

7.5 Configuration

7.5.1 View Device Information

View the device name, language, model, serial No., version, available cameras, IO input, IO output, Lock, Local RS-485,alarm input, alarm output, and device capacity, etc.

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

You can view device name, language, model, serial No., version, available cameras, IO input, IO output, Lock, Local RS-485,alarm input, alarm output, and device capacity, etc.

7.5.2 Set Time

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

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

Device Time

Display the device time in real time.

Time Zone

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

Time Synchronization Mode

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.

DST

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

7.5.3 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 strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

7.5.4 View Device Arming/Disarming Information

View device arming type and arming IP address.

Go to **Configuration → User Management → Arming/Disarming Information** .

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

7.5.5 Partition (Area)

1. The platform shall support displaying partition (area) information including partition (area) name, area, device, linked zone, partition (area) No., IP address and port No., auto-detected device No., and device resource type.
2. The platform shall support searching for partitions by partition (area) name, device name, and IP address.
3. The platform shall support editing partitions (areas).
4. The platform shall support customizing displayed columns.
5. The platform shall support linking a partition (area) to another zone.

7.5.6 Add Contact

You can add contact to the indoor station.

Steps

1. Press to enter the contact list page.
2. Press **Add Contact** to pop up the contact adding dialogue box.
3. Enter the name and room number of the contact.
4. Press to save the settings.

Note

Up to 200 contacts can be added.

5. **Optional:** You can hold an added contact to open the contact handling menu, and do the following operations :

Call	Press **Call** to start the video call with the contact.
Edit	Press **Edit** to modify the contact information.
Delete	Press **Delete** to delete the contact.
Clear	Press **Clear** to delete all contacts added in the indoor station.

7.5.7 Network Settings

Set Basic Network Parameters

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

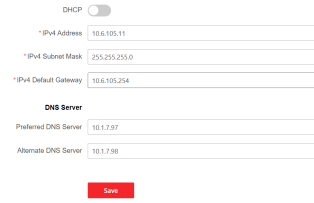


Figure 7-3 TCP/IP Settings

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.

DNS Server

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

VoIP Account Settings

You can realize voice call by network.

Steps

1. Go to **System and Maintenance → System Configuration → Network → Device Access → VoIP**.
2. Enable **VoIP Gateway**.
3. Set **Register User Name**、**Registration Password**、**Server IP Address**、**Server Port**、**Expiry Time**、**Register Status**、**Number**、**Display User Name.**

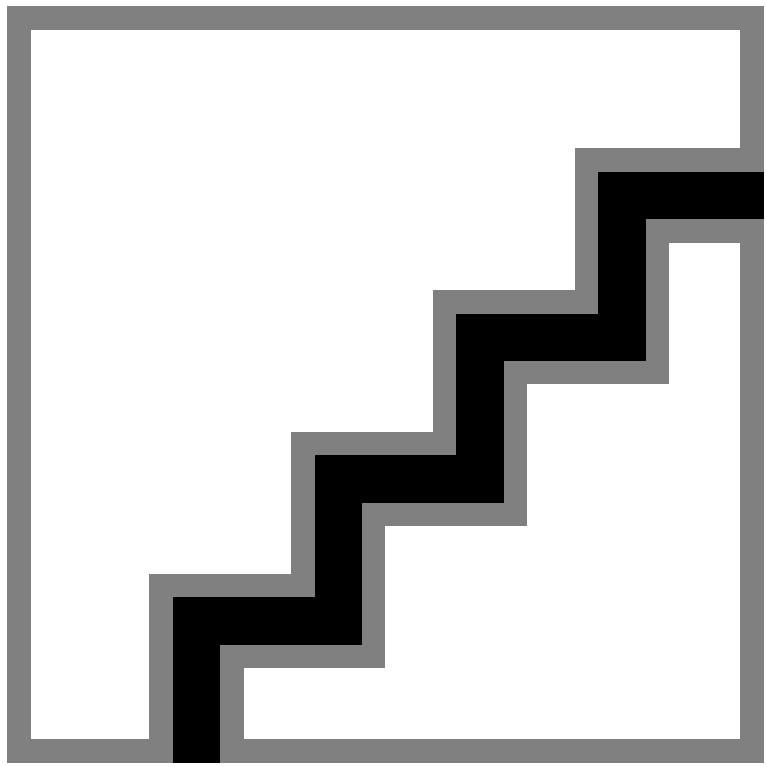


Figure 7-4 VoIP Account Settings

Registration Password

Enter the registration password for communication via SIP server. The registration password for the SIP server is configured usually in the main station's SIP settings.

Server IP Address

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

Number / Display User Name

The device displayed call number and user name.

4. Click **Save**.

Set Port Parameters

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

Click **Configuration → Network → Advanced Configuration → 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 → Advanced Configuration → 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.

7.5.8 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

Click **Configuration → Video/Audio → Video** .

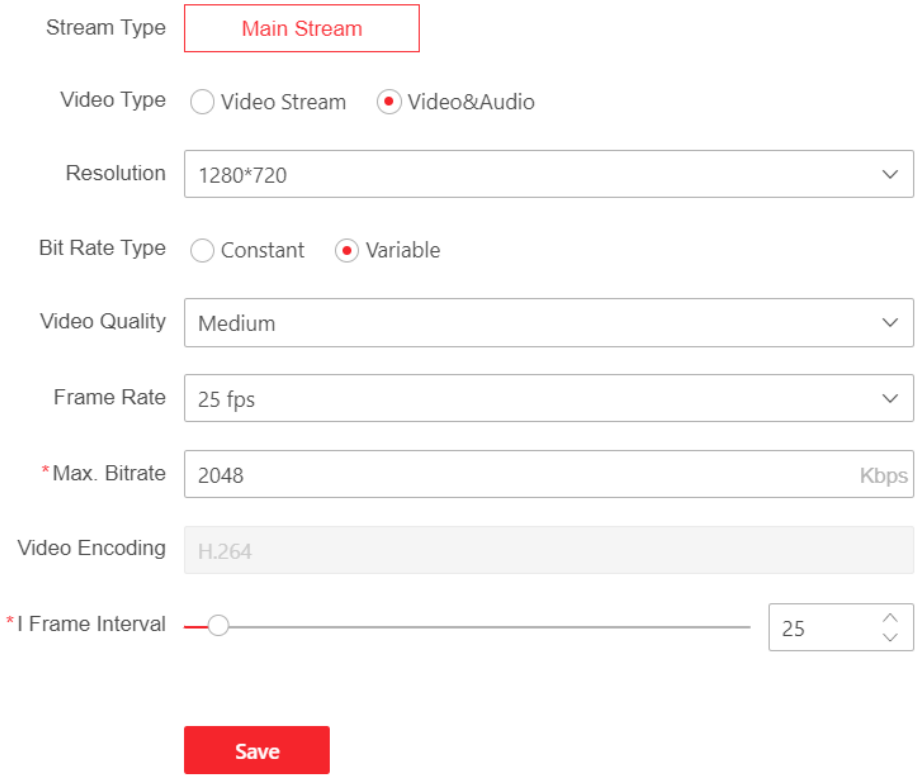


Figure 7-5 Video Settings Page

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.

Set Audio Parameters

Click **Configuration → Video/Audio → Audio** .

Figure 7-6 Audio Settings Page

Set the stream type, audio encoding, input volume, output volume, speak volume and audio sampling rate.
Click **Save** to save the settings.

7.5.9 Call Settings

Device No. Settings

Steps

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

Figure 7-7 Device No. Settings

2. Set the corresponding information including **Door Station No.** and **No.**
3. Click **Save** to enable the device number configuration.

Linked Network Settings

Steps

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

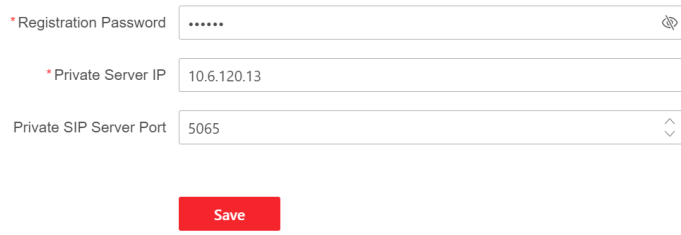


Figure 7-8 Session Settings

2. Set **Registration Password**.
3. Set **Private Server IP** and **Private SIP Server Port**.
4. Click **Save** to enable the settings.

Custom No. and Name on PC Web

Steps

1. Click **Video Intercom → Call Parameters → Custom No and Name** to enter this page.
2. Click on the **Device Type** dropdown menu and choose the appropriate category that defines the primary function of the device.
3. The **Industry Type** will change automatically based on the device type you select.
4. Then you can edit the **Custom Name**.

Set Communication Time via PC Web

Set the max. communication time.

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

Enter the **Max. Communication Time**. Click **Save**.

Note

The Max. Communication time range is 90 s to 120 s.

7.5.10 Add Broadcast Material

Add broadcast material to material library.

Steps

1. Go to **Broadcast Settings → Material Library** .
2. Click **New Material Library**.
3. Enter **Material Library Name**.
4. Click **OK**.
5. Click the corresponding material library.
6. Click **Batch Add**.
7. Check the folder as your needs.
8. Click **Add**.
9. Check the broadcast material.
10. Click **Add**.
11. Click to edit **Material Library Name**.
12. Click **OK**.

7.5.11 Broadcast Plans

Add scheduled broadcast tasks to make devices broadcast according to the schedule.

Steps

1. Click **Video Intercom → Broadcast Settings → Broadcast Plans** to enter the broadcast schedule configuration interface.
2. Click **+ Add** to create a broadcast task.
3. Enter the task name.
4. Select the task type as Daily Schedule or Weekly Schedule.

   Daily Schedule

   The broadcast task will be played at fixed time every day.

   Weekly Schedule

   Specify the days of the week when the broadcast task needs to be played.
5. **Optional:** If there are existing plans that can be reused, click **Copy From** to select the plan to be copied.
6. Configure the validity period of the broadcast schedule. The broadcast will be played within the validity period.
7. Configure broadcast rules in **Playing Settings**.
   1) Add terminal devices for broadcasting. Click **+ Add**, check the devices that need to play the broadcast, then click **OK**.

   Note

   If needed, you can click to delete a single device or check multiple devices and click **Delete** to batch delete devices.

   2) Add play time and broadcast content. Click **+ Add**, select broadcast start time, configure audio source, select or add audio, configure broadcast level and play mode.

Start Time

Configure the time to start broadcasting.

Audio Source

Audio File

If materials have been added to the broadcast material database, audio files from the database will appear directly in the audio file list.

If there are no materials in the database, click **+ Add** → **+ Add Material**, select audio from local computer, then click **Add**.

Check audio files from the list as broadcast materials.

Delete terminal devices (optional): Click to delete a single terminal device. Or check multiple devices and click **Delete** to batch delete devices.

Voice Synthesis

Enter voice content and select synthesis parameters as male or female voice.

Local Microphone

The broadcast content is the voice sent through the device.

Broadcast Ratings

Drag the slider to configure the playback priority of this broadcast. 0 is the highest priority and 15 is the lowest.

Play Mode

Play Once

Play in the order of the audio list, each audio is played only once.

Loop

Note

When selecting Weekly Plan as the task type, you need to select the **Cycle** period.

Play in order and loop.

8. Click **Save** to complete the configuration.

7.5.12 View Call Log

The indoor station supports saving call logs from door station, outer door station, management center and other indoor stations. You can view the call logs on the indoor station.

Steps

1. Press on the main page of the indoor station.
2. **Optional:** Press **Missed Call** to view the missed call logs.
3. **Optional:** Press **All Calls** to view all call logs, including calling logs, called logs, and missed call logs.
4. Hold a piece of call log to open the call log handing menu.

1) Press **View** to display the live view page for getting the live view of the call.
2) Press **Delete** to delete the piece of call log.
3) Press **Clear** to delete all pieces of call logs.

7.5.13 Set Open Platform

If the device supports HEOP protocol, you can upload the third-party application to the device from this page.

Before You Start
Make sure the device contains the HEOP program.

Steps
1. Click **Configuration → Open Platform** .
2. If it is the first time to use the function, you should read the Disclaimer and make sure that the application you want to install fit the following conditions.
   - Each application has its own exclusive name.
   - The FLASH memory space that the application takes up is less than the available FLASH memory space of the device.
   - The memory and computing power of the application is less than that available memory and computing power of the device.
3. Import license.
   - If the application package has a license, click and select the license file from your local computer. Click **Import**.
   - If the application package does not have a license, enter ***https://tpp.hikvision.com/*** in the web browser to get a license.
4. Click **Import Application** to complete the installation.

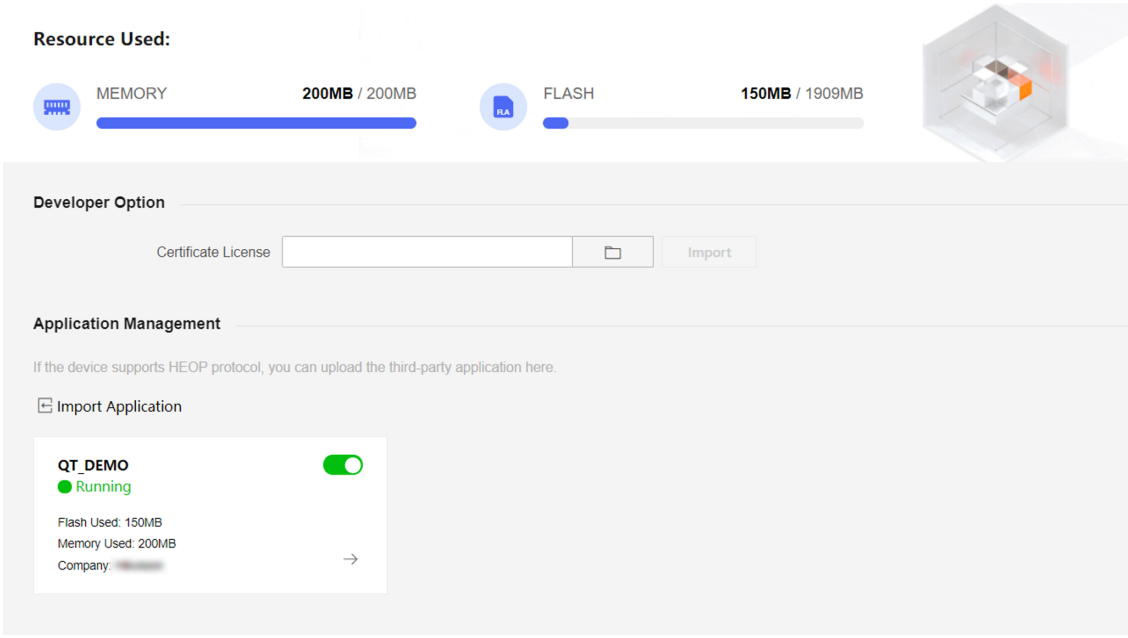


Figure 7-9 Open Platform

The installed applications and their related information are displayed in **Application Management** area. You can select to enable/disable the application. You

Click → to view the details about the application, including the application name, version, manufacturer, introduction, license status, system memory, flash, and disclaimer.

5. **Optional:** Set other functions.

	Enable or disable the application.
	Delete the application.
··· → **Download Log**	download the log.

7.5.14 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.

If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.

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 device IP address 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.

7.5.15 Device Debugging

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.

ADB

Enable **ADB Remote Control** for actual needs.

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 Capture** to capture network data.

3. Click **Save**.

7.5.16 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.

7.5.17 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click **Maintenance and Security → Security → Security Service** .

Select a security mode, and click **Save**.

Security Mode

High security level for user information verification when logging in the client software.

Compatible Mode

The user information verification is compatible with the old client software version when logging in.

7.5.18 Certificate Management

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

Note

The function is only supported by certain device models.

Import Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Before You Start

You should send the asking file to a certification authority for signature. Then save the authorized certificate locally.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. 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**.

Chapter 8 Other Platforms to Configure

You can also configure the device via iVMS-4200 Client Software or HikCentral Access Control. For details, see the platforms' user manual.

iVMS-4200 Client Software

Click/tap the link to view the client software's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247

HikCentral Access Control (HCAC)

Click/tap the link to view the HCAC's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42


See Far, Go Further