Nurse 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.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

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.
- HDMI The terms HDMI, HDMI High-Definition Multimedia Interface, HDMI Trade dress and the HDMI Logos are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.

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.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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

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
Nurse Station	DS-KHM9503X DS-KHM9803X

Contents

Chapter 1 Appearance 1

Chapter 2 Terminal Description 4

Chapter 3 Installation 6

3.1 Table Bracket(Optional) 6

3.2 Accessory Installation(Optional) 6

3.2.1 Install Speaker 6

3.2.2 Install Goose Neck Microphone 8

3.3 Table Mounting 9

Chapter 4 Activation 11

4.1 Activate via Device 11

Chapter 5 Local Configuration and Operation 12

5.1 Local Configuration of Main Station 12

5.1.1 Activate the Device 12

5.1.2 Quick Operation 12

5.1.3 Basic Settings 13

5.1.4 Set Basic Settings for Broadcast 14

Chapter 6 Quick Operation via Web Browser 15

6.1 Select Language 15

6.2 Time Settings 15

6.3 No. and System Network 16

Chapter 7 Operation via Web Browser 18

7.1 Login 18

7.2 Device Management 18

7.3 Camera Management 19

7.4 Overview 20

7.5 Configuration 21

7.5.1 View Device Information 21
7.5.2 Set Time 21
7.5.3 Change Administrator's Password on PC Web 22
7.5.4 View Device Arming/Disarming Information via PC Web 23
7.5.5 Partition Settings 23
7.5.6 Add Contact 23
7.5.7 Network Settings 26
7.5.8 Set Video and Audio Parameters 27
7.5.9 Call Settings 30
7.5.10 Add Broadcast Materials 33
7.5.11 Broadcast Plans 34
7.5.12 View Call Log 35
7.5.13 Set Open Platform 35
7.5.14 Upgrade and Maintenance 37
7.5.15 Device Debugging 38
7.5.16 Log 38
7.5.17 Security Mode Settings 38
7.5.18 Certificate Management 39
Chapter 8 Other Platforms to Configure 40

Chapter 1 Appearance

Front Panel

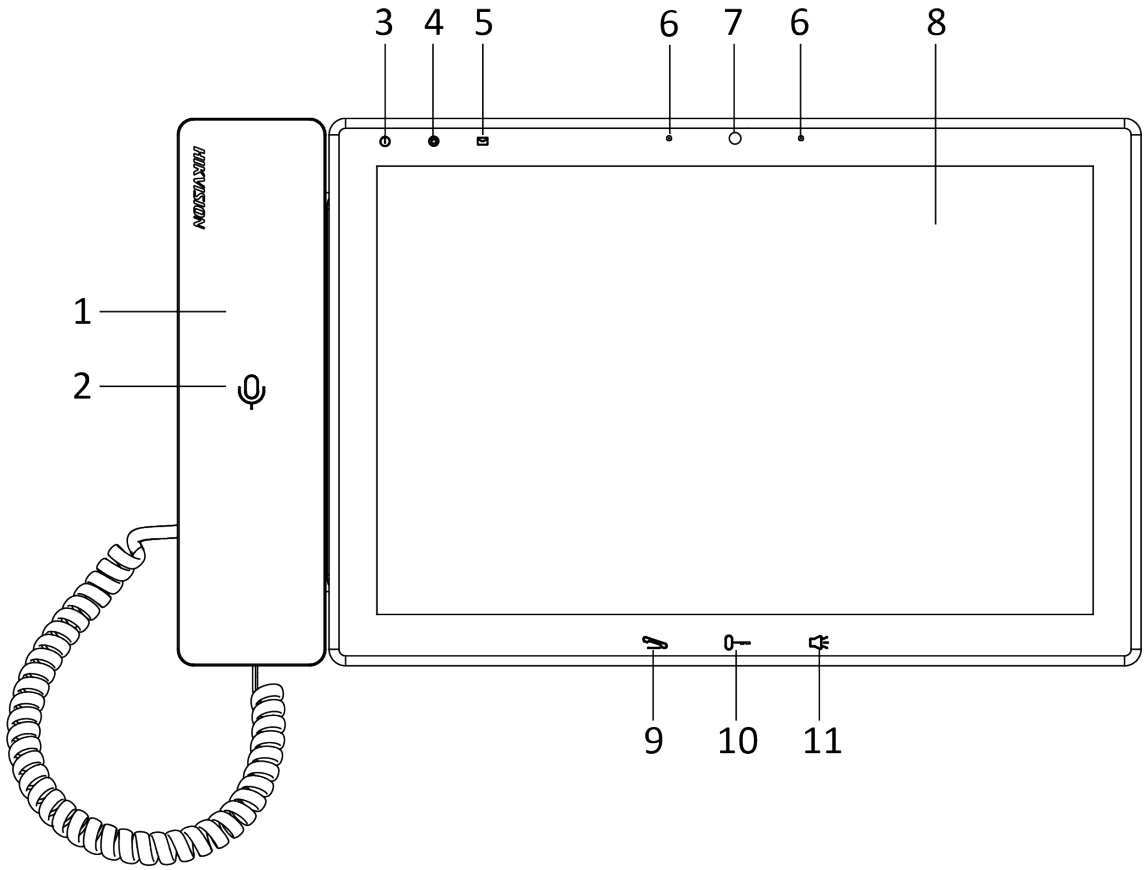

Figure 1-1 Front Panel

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

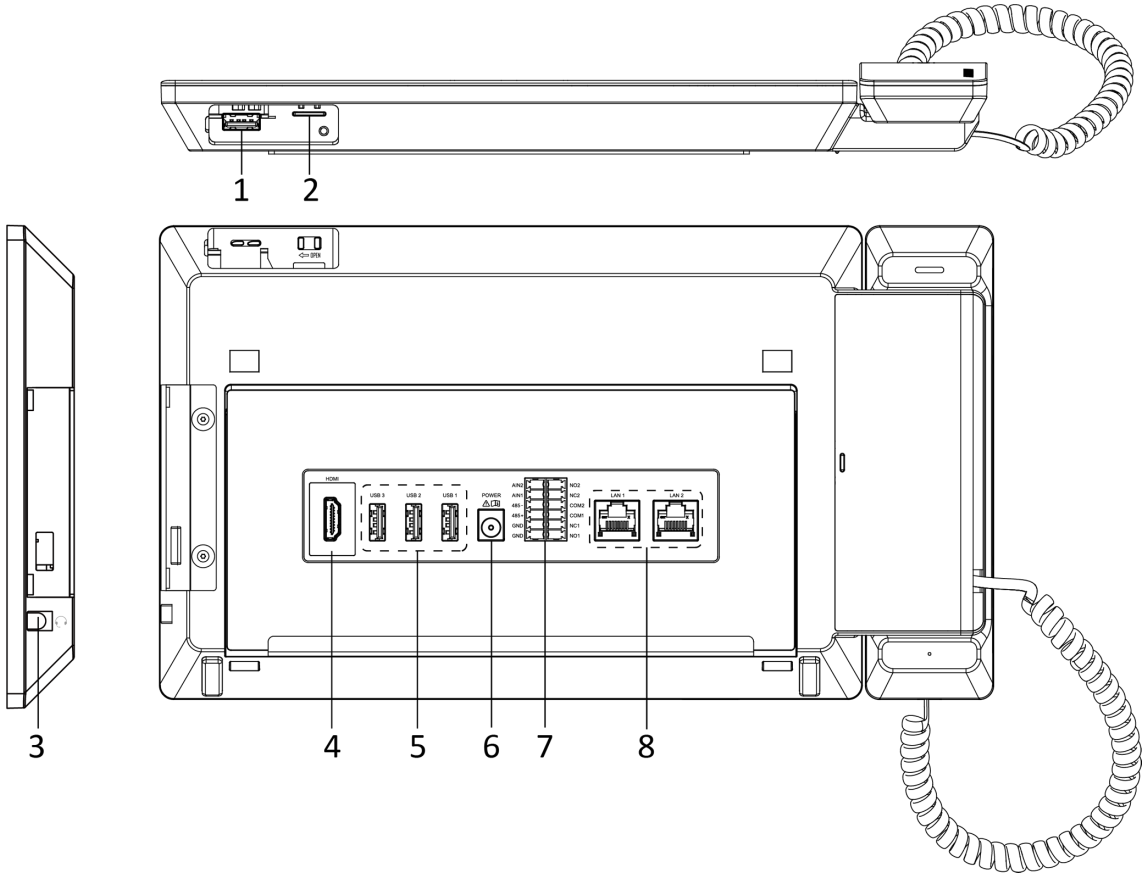

Figure 1-2 Top Panel and Rear Panel

Table 1-2 Description

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

Speaker(Optional)

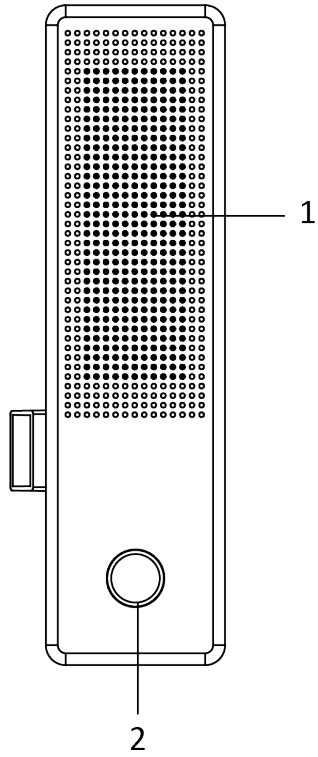

Figure 1-3 Speaker

Table 1-3 Description

No.	Description	No.	Description
1	Speaker	2	Fingerprint Module

Chapter 2 Terminal Description

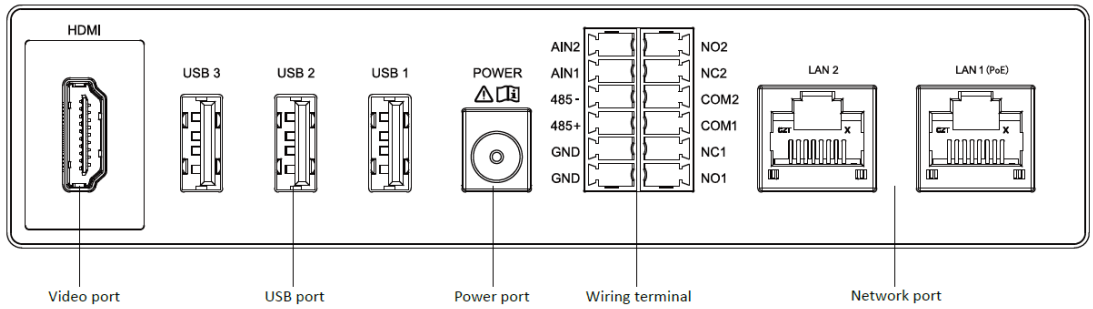

Figure 2-1 Terminal Description

Table 2-1 Terminal Description

Name	Interface	Description
Video Port	HDMI	HDMI Signal Output
USB Port	USB 1	USB Port **Note** USB3 is used to debugging only. It cannot connect to USB flash drive.
	USB 2	
	USB 3	
Power Port	POWER	12 VDC Power Input
Wiring Terminal	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

Name	Interface	Description
	GND	Grounding
Network Port	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.

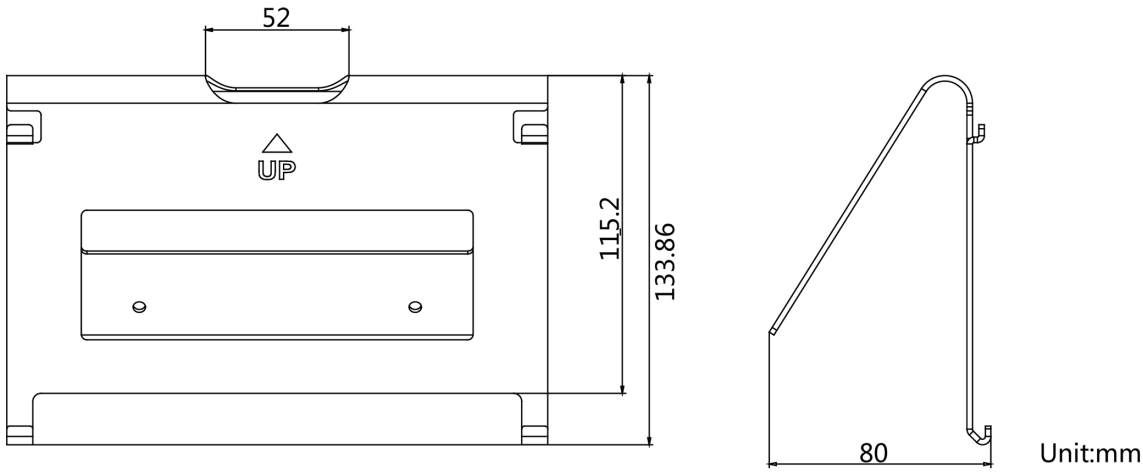

Figure 3-1 Table Bracket

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.

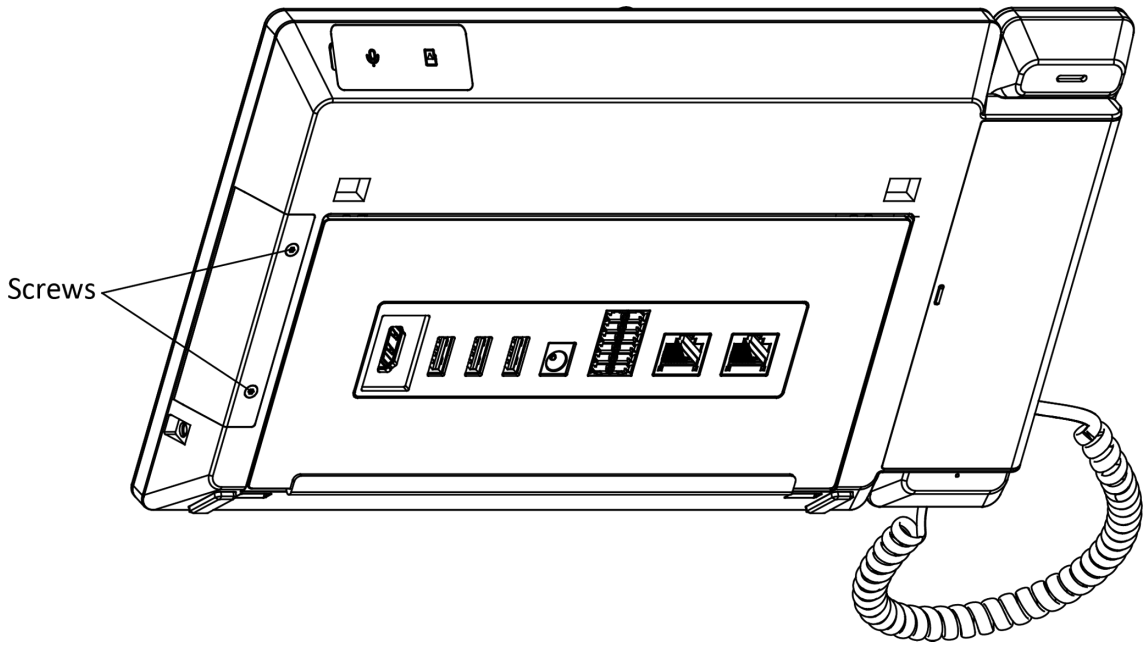

Figure 3-2 Loose the screws

2. Remove the cover plate from the device and install the USB connector of the speaker into the port.

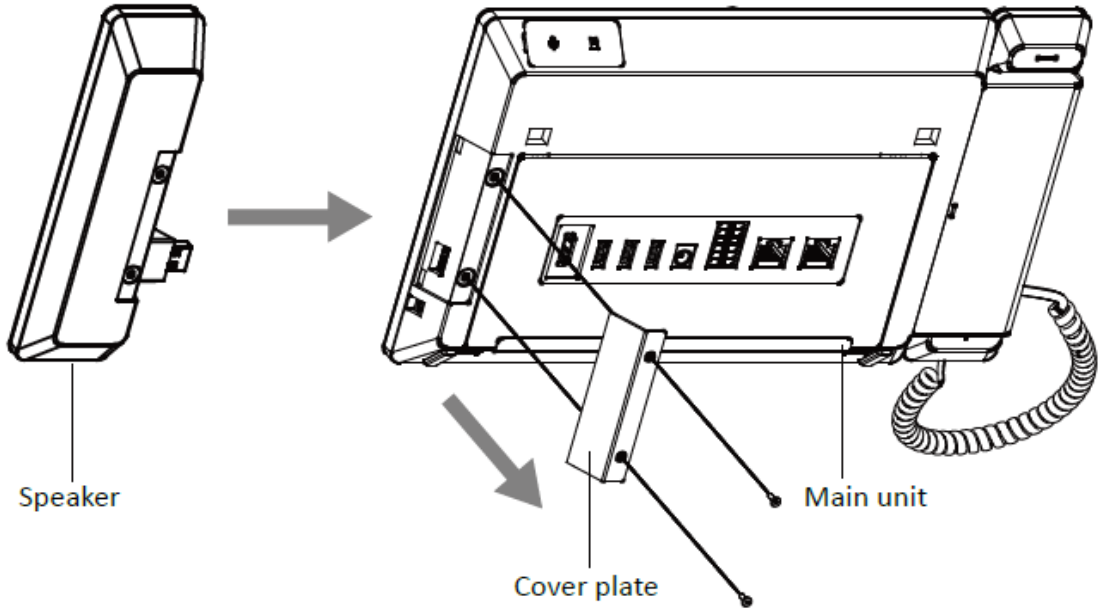

Figure 3-3 Install the Speaker

3. Fasten the cover plate of the speaker to the device with four screws.

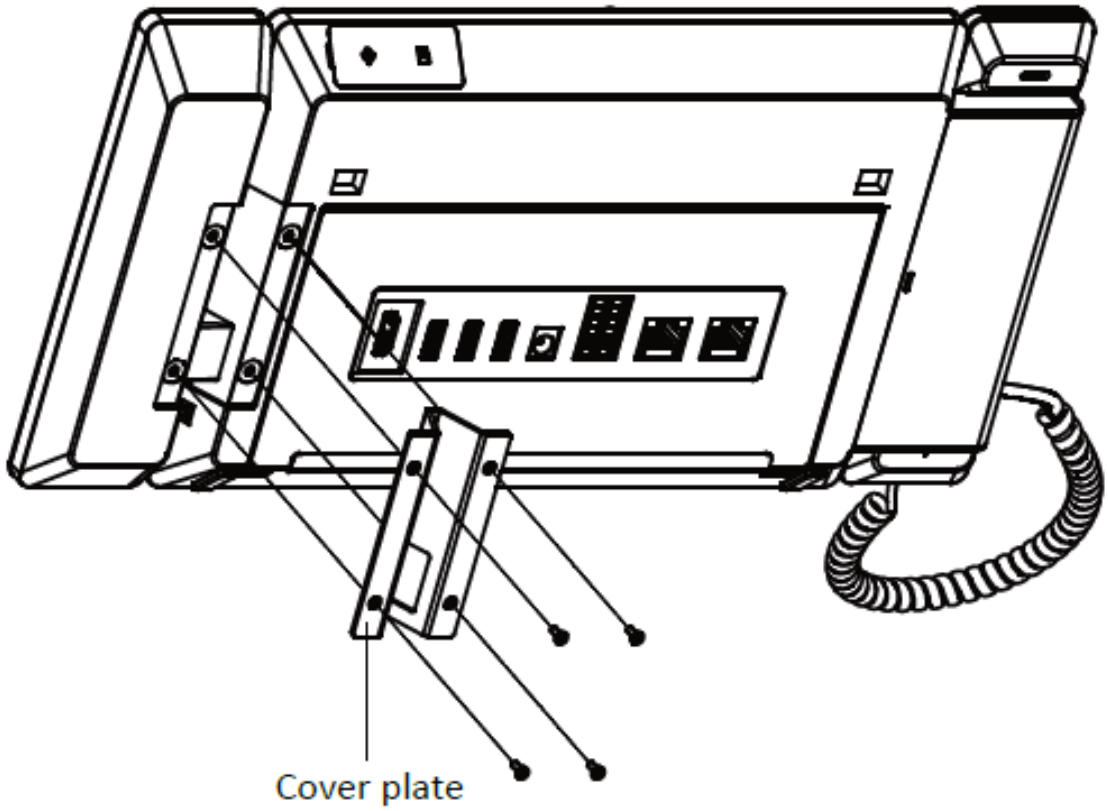

Figure 3-4 Secure the Speaker

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.

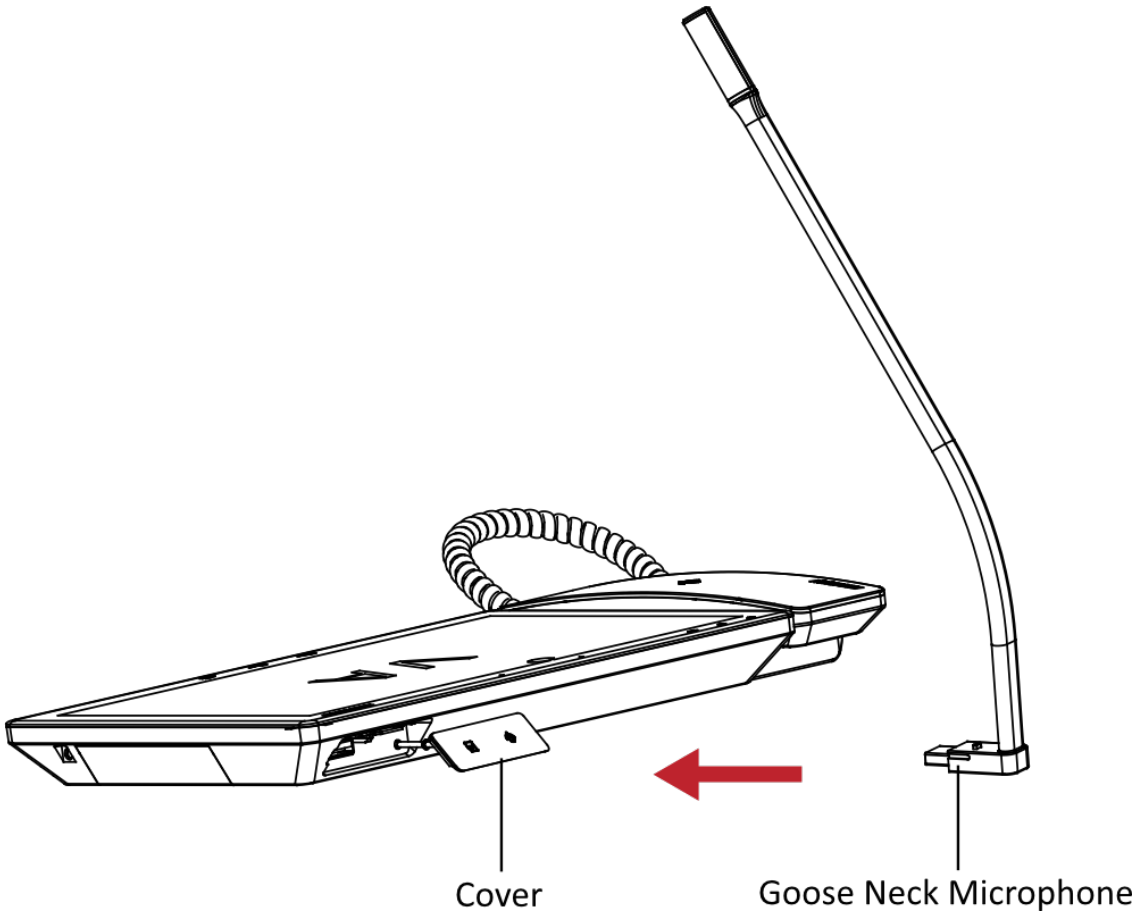

Figure 3-5 Install the Goose Neck Microphone

3.3 Table Mounting

Steps

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

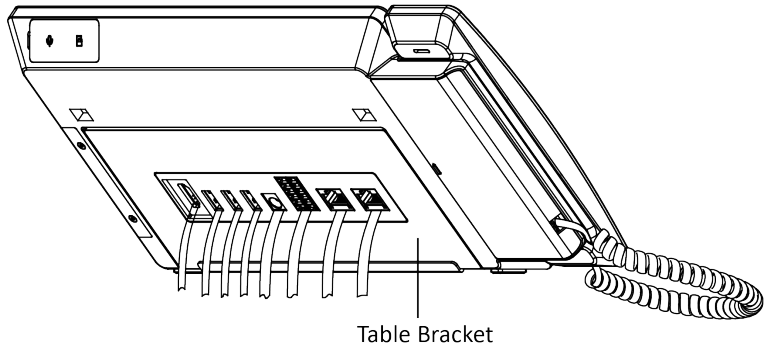

Figure 3-6 Smooth the Cable

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

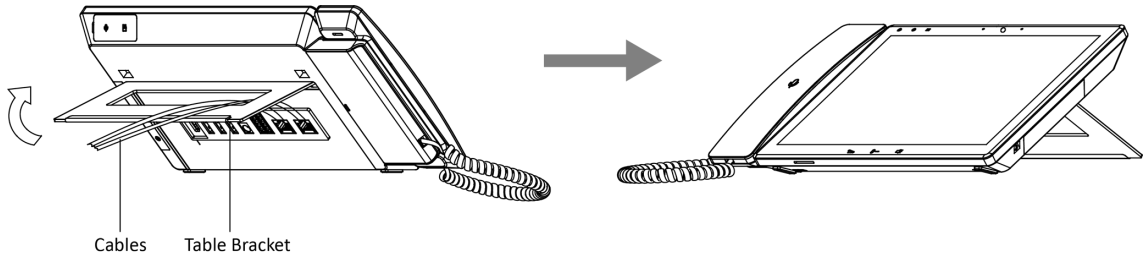

Figure 3-7 Adjust the Table Bracket

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).

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 device 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**. The device will automatically go to the Quick Setup interface.

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 Quick Operation

After device activation, the system will automatically enter the configuration wizard. You need to select the usage mode, configure Server Settings and Service Settings.

Steps

1. At Mode Selection, please select usage mode then tap **Next**.

   Note

   Demo mode is typically used by manufacturers to demonstrate device operation to users. For regular device usage, please select normal mode.
2. Configure the local IP address. Enter **Local IP**, **Subnet Mask** and **Gateway**, then click **Next**.
3. Configure the server.
   1) Enter the server address, port number and admin password.
   2) Tap **Next**.

   Note

   The admin password can be viewed and modified in HikCentral Professional.
   After server configuration is completed, the device will connect to HikCentral Professional.
4. Select department/ ward to complete the configuration.
5. Tap **Finish** to save the settings.

5.1.3 Basic Settings

Advanced Settings

Steps

1. Click **Settings → Advanced Settings** , then enter admin password to enter the page.
2. You can modify the local IP address, subnet mask, gateway, server IP, port number, department/ ward, and usage mode, and view the SIP service address.

General Settings

You can view the device's date, time, timezone, and configure screen brightness and screen-off time.

Click **Settings → Basic Settings** to enter the page.

View the device's date, time, and timezone.

Note

Device time can be configured on the web client. For details, refer to Set Device Time.

Slide the slider to adjust screen brightness.

Click **Screen-off Time**, select the desired duration based on actual needs, then click **OK** to save settings.

Call Settings

You can set the device call volume and notification volume, and enable the recording function.

Steps

1. Tap **Settings → Call Settings** to enter the call settings page.
2. Set corresponding parameters.

   Call Volume

   Drag the silder to adjust the call volume. Range: 1-10.

   Notification Volume

   Drag the silder to adjust the notification volume. Range: 1~10.

   Record

   Silde to enable the function of recording. Then the device will record calls receive automatically.

5.1.4 Set Basic Settings for Broadcast

You can select audio file for broadcasting or click to do a real-time broadcast.

On main the page, click **Broadcast** to enter the setting page.

Select the devices for broadcast playback, or click **Select All** in the upper-right corner of the interface to choose all devices.

Start broadcasting.

- For real-time broadcast: click the microphone icon to begin.
- For audio file broadcast: select the audio file to play before starting.

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

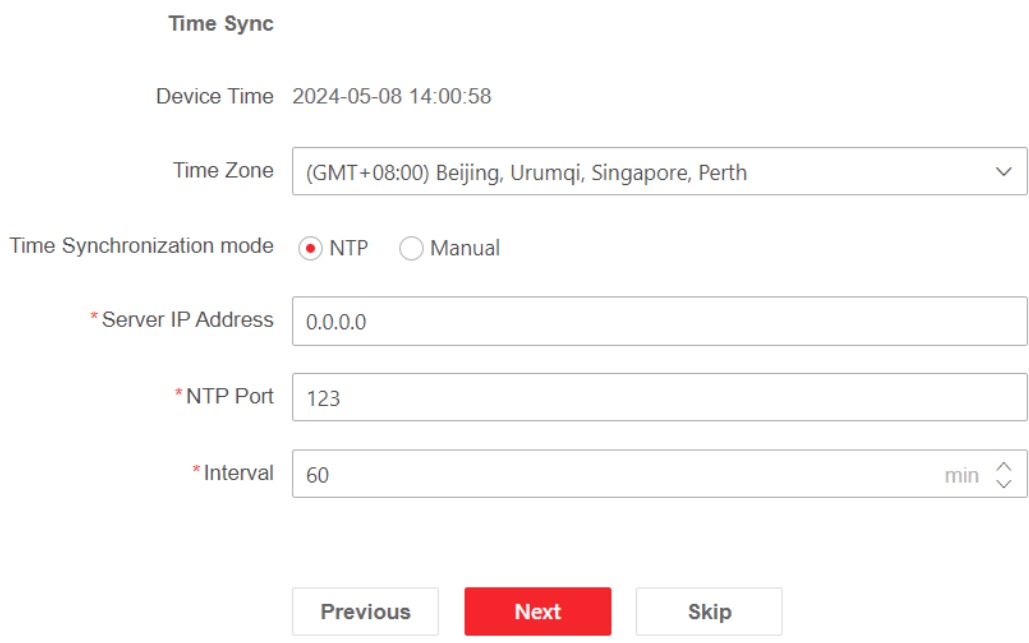

Figure 6-1 Set Time and DST

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.

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. Slide to **Enable Device No.** or **Enable Industry Rule No.**.

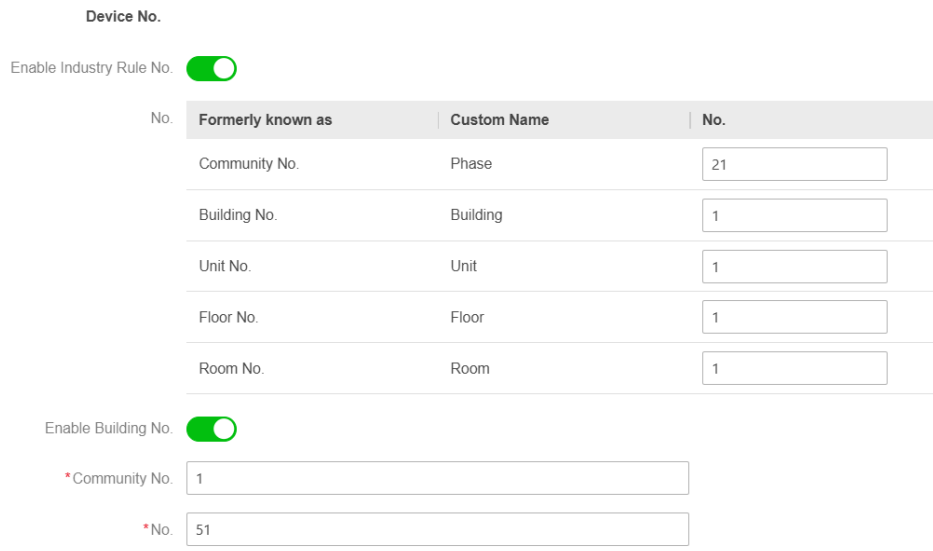

Figure 6-2 Device No.

Community No.

If you enabled Building No., then you need to set the device community No.

No.

If you enabled Building No., then you need to 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.

Advanced Two-way Audio Server IP

The server address that supports two-way audio intercom between nurse station and other terminals.

Advanced SIP Server Port

Extended-function SIP communication ports, typically used for special requirements or enhanced protocol support. Dedicated to transmitting high-fidelity audio streams, avoiding signaling congestion.

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 .

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.

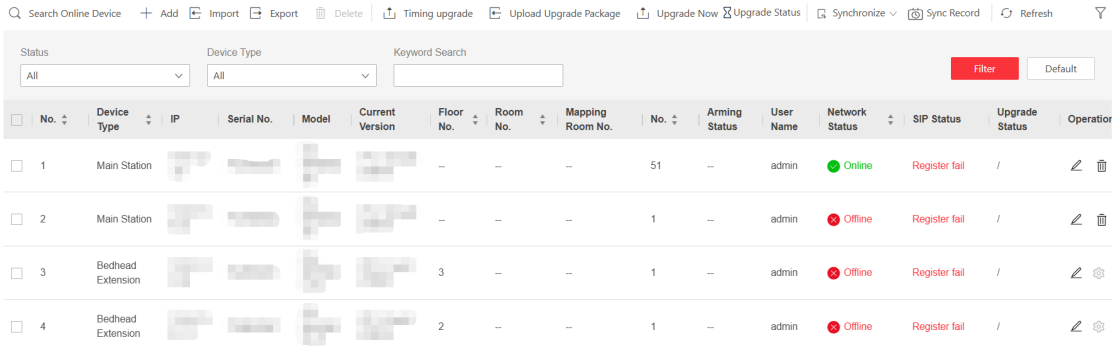

Figure 7-1 Device Management

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 **Synchronize** and select from **Apply Device Name**, **Obtain Device Name** or **Synchronize All**. If you want to synchronize record, just click **Sync Record**.

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.

Click **Device Management → Device Management → Camera** to enter this page.

Click **+Add** to add camera.

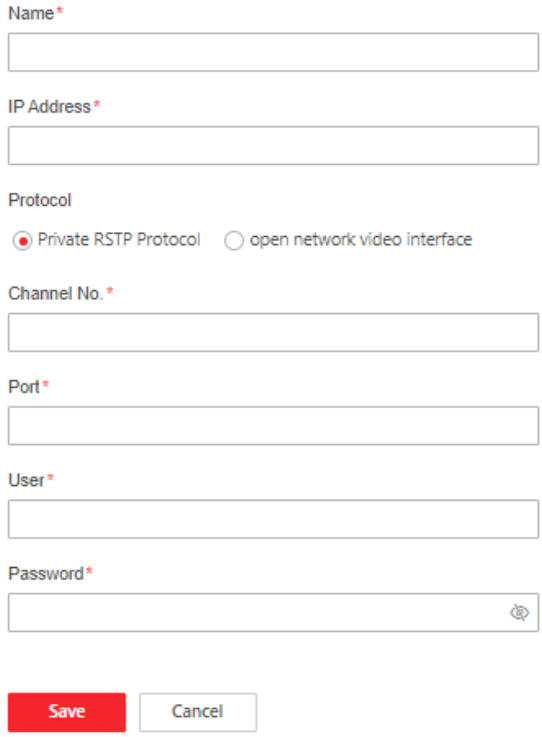

Figure 7-2 Add Camera

7.4 Overview

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

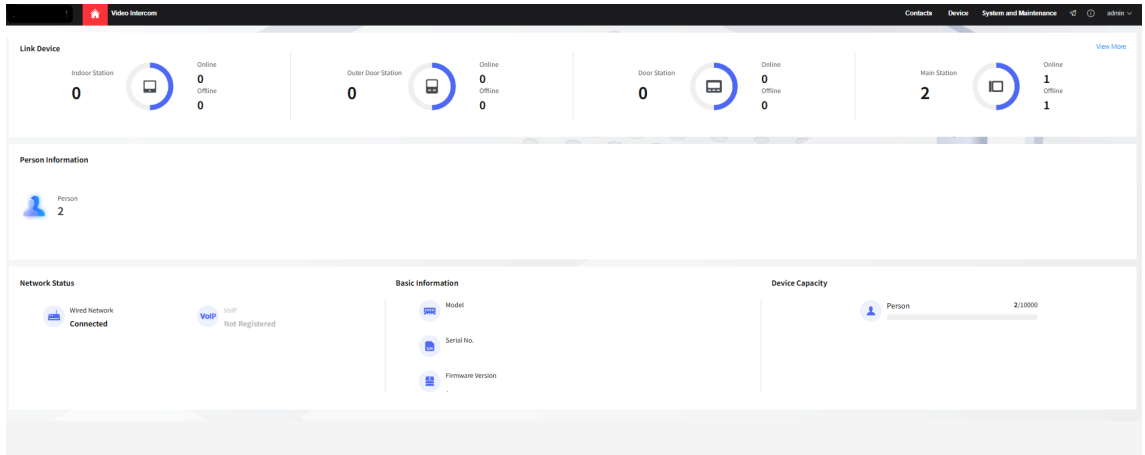

Figure 7-3 Overview Page

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 and VoIP.

Basic Information

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

Device Capacity

You can view person capacity.

Person Information

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

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, number of channels, IO input, IO output, alarm input, alarm output, and device capacity, etc.

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

You can view the language, model, serial No., version, IO input, IO output, Local RS-485, alarm input and alarm output number.

You can change **Device Name** and **Language** and click **Save**.

Click **Upgrade** to upgrade the firmware version.

You can view the device person capacity.

7.5.2 Set Time

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

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

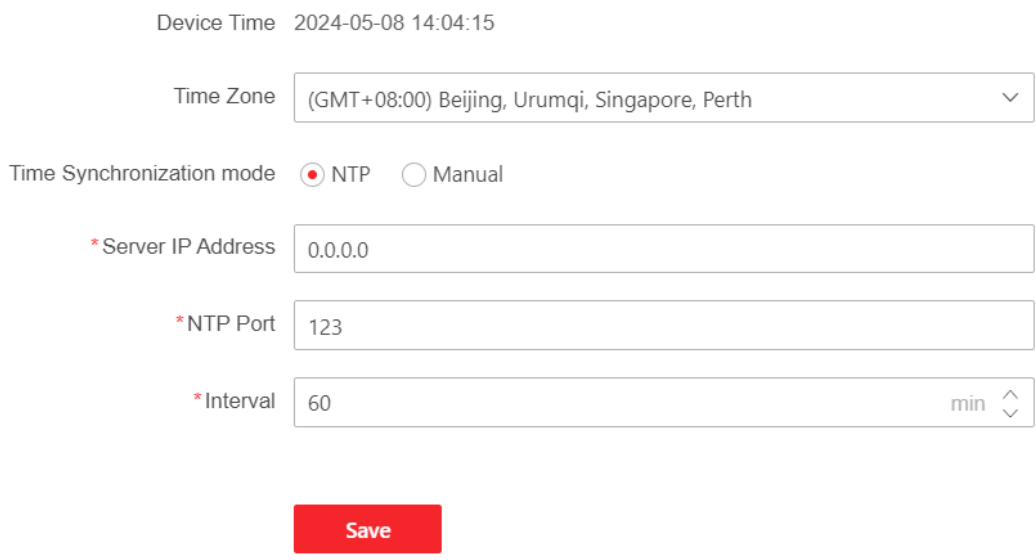

Figure 7-4 Time Settings

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.

7.5.3 Change Administrator's Password on PC Web

Steps

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

Note

- 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.
- (If the device supports AP mode, after the admin password is changed, the password of AP hotspot will be changed simultaneously.)

7.5.4 View Device Arming/Disarming Information via PC Web

View device arming type and arming IP address.

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

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

7.5.5 Partition Settings

Click **Device → Partition Settings** to enter this page.

Click **+** to add partition.

Enter **Partition Name** then select **Terminal**.

Click **OK** to finish adding.

7.5.6 Add Contact

You can add basic person and unauthorized person to the device.

Steps

1. On the main page, click **Contacts** to enter the contact list page.
2. Click **+ Add** to pop up the contact adding dialogue box.
3. If you choose the person type as **Basic Person**, then you'll need to enter the name, age, and select the gender of the person.

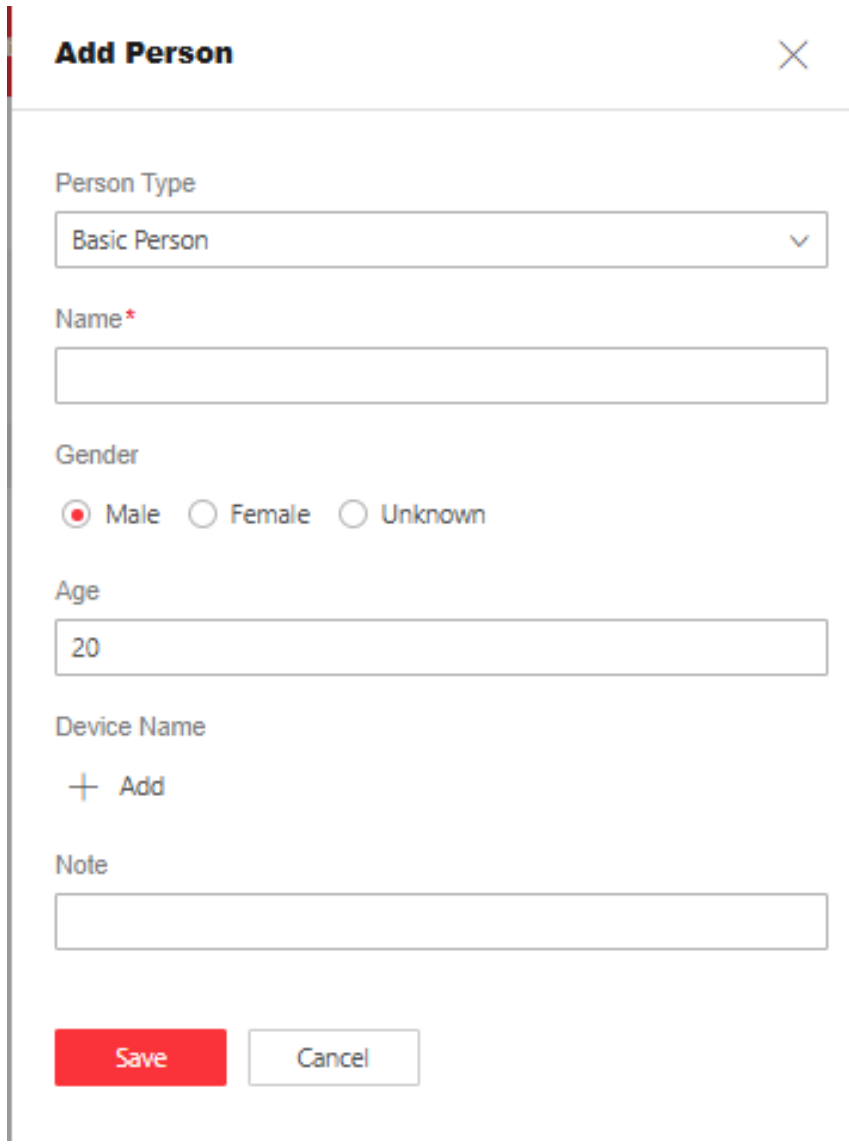

Figure 7-5 Add a Basic Person

Note

You can also enter note to hint some important things.

4. If you choose the person type as **Unauthorized Person**, you'll need to enter the name, age, assistant nurse, attending physician, medical advice and select the gender of the person.

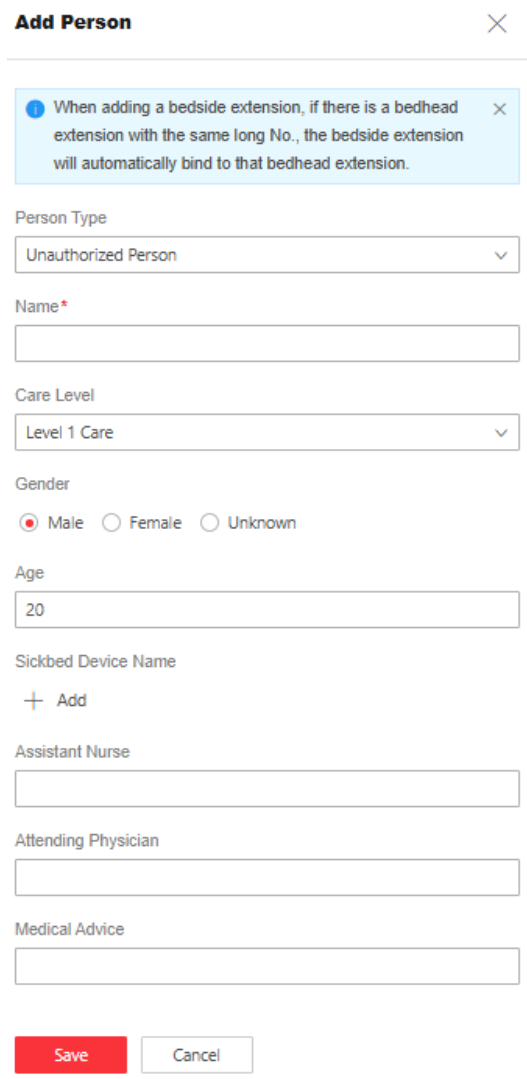

Figure 7-6 Add an Unauthorized Person

Note

When adding a bedside extension, if there is a bedhead extension with the same long No., the bedside extension will automatically bind to that bedhead extension.

5. Press **Save** to save the settings.

7.5.7 Network Settings

Set Basic Network Parameters via PC Web

Click **System and Maintenance → System Configuration → Network → Network Settings → TCP/IP** .

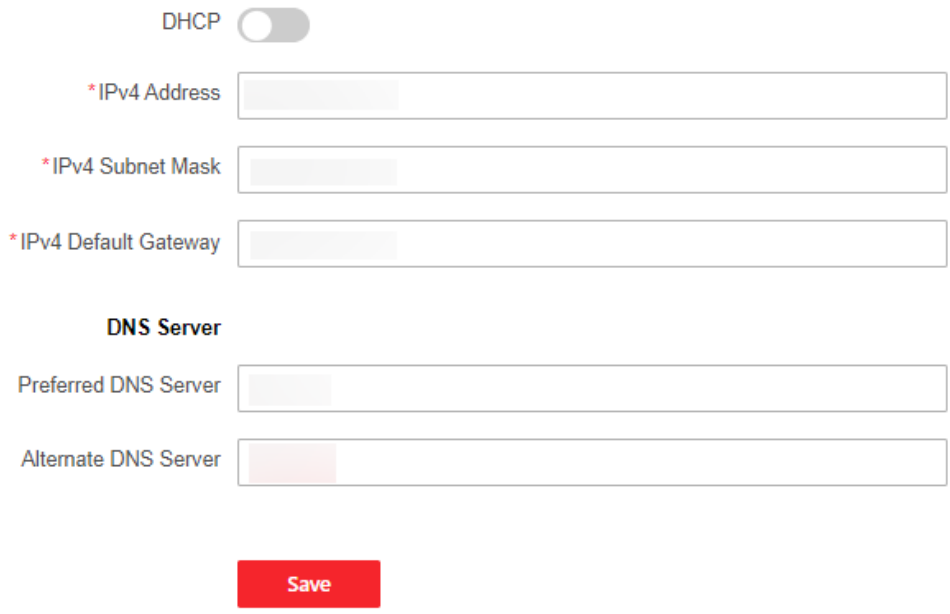

Figure 7-7 TCP/IP Settings Page

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

NIC Type

Select a NIC type from the drop-down list. By default, it is **Auto**.

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, Mac address, and MTU.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway 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. Silde to **Enable VoIP Gateway**.
3. Set **Register User Name**、**Registration Password**、**Server IP Address**、**Server Port**、**Expiry Time**、**Register Status**、**Number**、**Display User Name.** and **Center No.**
4. Click **Save**.

Set Port Parameters

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

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

RTSP

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

Click **System 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 Video Parameters

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

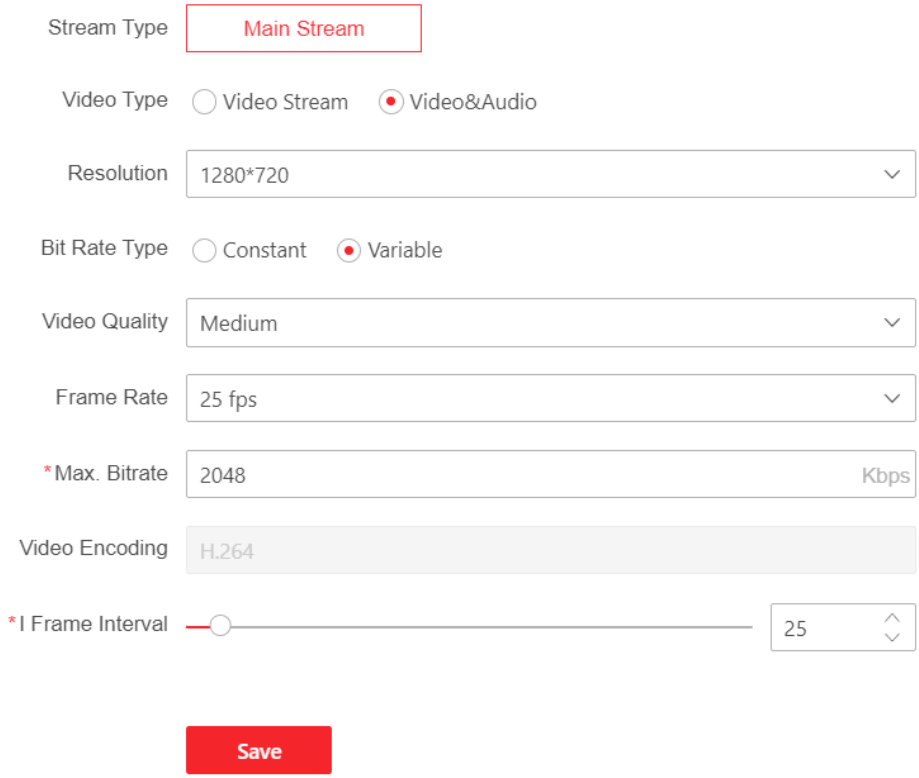

Figure 7-8 Video Settings Page

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.

Set Audio Parameters

Click **System and Maintenance → System Configuration → Video/Audio → Audio** .
You can complete **Input Method Configuration**, **Alarm Prompt Sound Configuration** and **Ringtone Configuration** at this page.

Note

Some models also support **Output Method Configuration**.
Please refer to your actual device.

Input Method Configuration

- Silde to enable **Custom Input Method**.
- Select **Audio Input Type** as **Handset microphone**, **Gooseneck Microphone** or **Local Microphone**.

Note

The default input priority order is handset microphone > gooseneck microphone > device speaker.

- Slide the slider to adjust input volume.

Output Method Configuration

Silde to enable **Custom Broadcast Output Method**, **Custom Audio Output Method** or **Customized Intercom Output Method**.

- **Custom Broadcast Output Method**: Select Broadcast Output Method from **3.5 mm Audio Output Port**, **USB Speaker** and **Device Interface**.

Note

The default input priority order is 3.5 mm Audio Output Port > USB Speaker > device speaker.

- **Custom Audio Output Method**: Select Audio Output Method from **3.5 mm Audio Output Port**, **USB Speaker** and **Device Interface**.

Note

The default input priority order is 3.5 mm Audio Output Port > USB Speaker > device speaker.

- **Customized Intercom Output Method**: Select Audio Output Method from **Handset Speaker**, **USB Speaker** and **Device Interface**.

Note

The default input priority order is handset speaker > USB Speaker > device speaker.

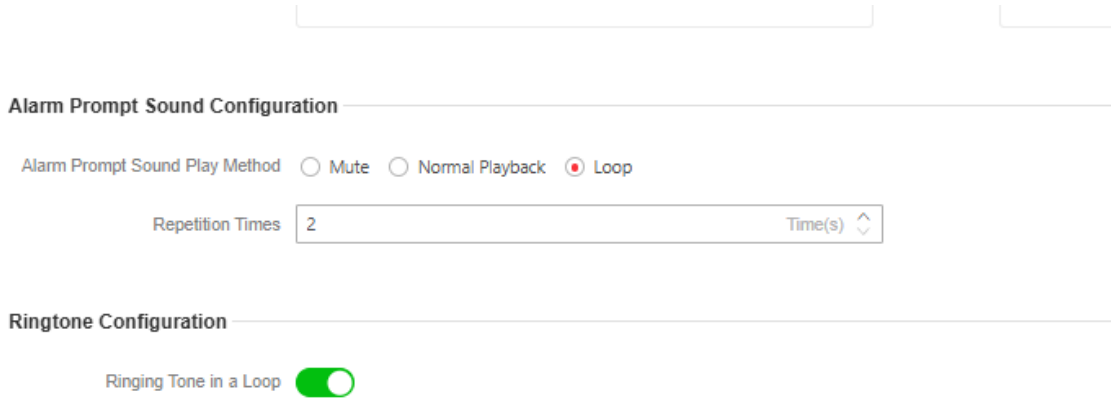

Figure 7-9 Alarm Prompt Sound Play Method and Ringtone Configuration

Alarm Prompt Sound Configuration

You can select **Alarm Prompt Sound Play Method** as **Mute**, **Normal Playback** or **Loop**.

Ringing Tone in a Loop

Silde to enable **Ringing Tone in a Loop**.

Set SIP Audio Encoding and Speak Volume.
Slide the slider to adjust speak volume.
Check the box and click **>/<** to enable or disable **SIP Audio Encoding**.

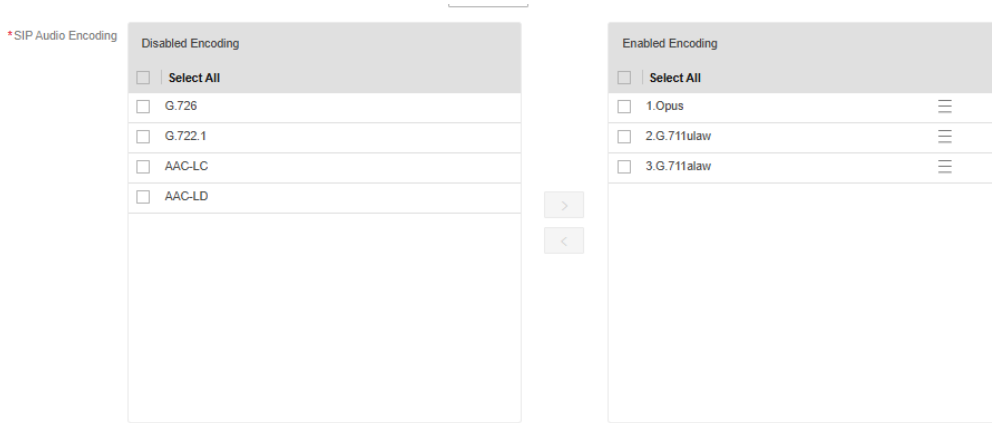

Figure 7-10 SIP Audio Encoding

Note

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

Click **Save** to save the settings.

7.5.9 Call Settings

Device No. Settings

Steps

1. Click **Video Intercom → Call Parameters → Device No.** to enter the page.

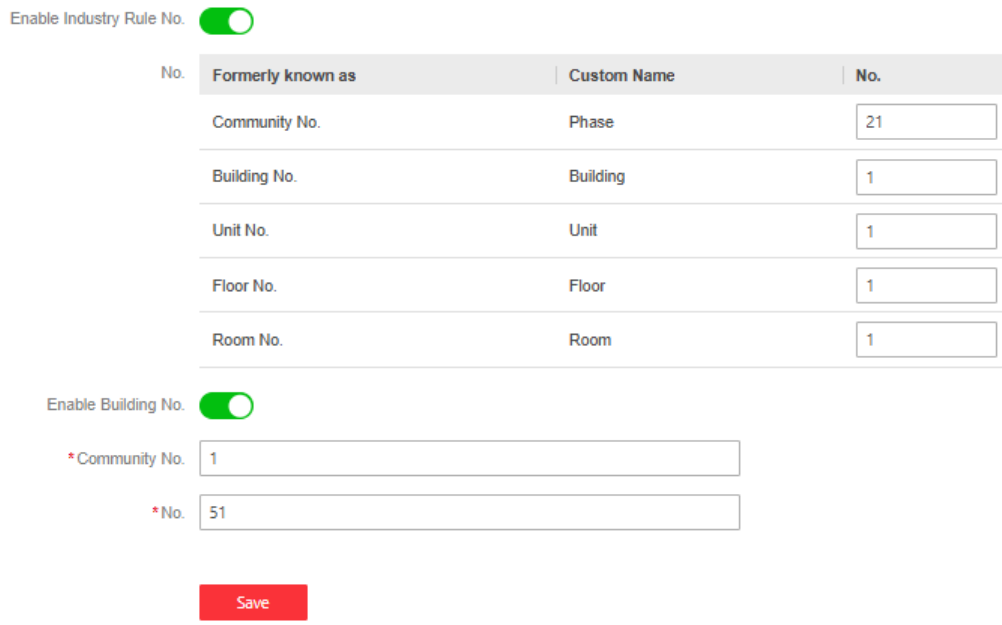

Figure 7-11 Device No. Settings

2. **Enable Industry Rule No.** is enabled by default. You can edit information including **Building No.**, **Floor No.**, **Room No.**, **Community No.** and **Unit No.**
3. If **Enable Building No.**, then you can set **Community No.** and **Unit No.**.
4. Click **Save** to enable the device number configuration.

Linked Network Settings

Steps

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

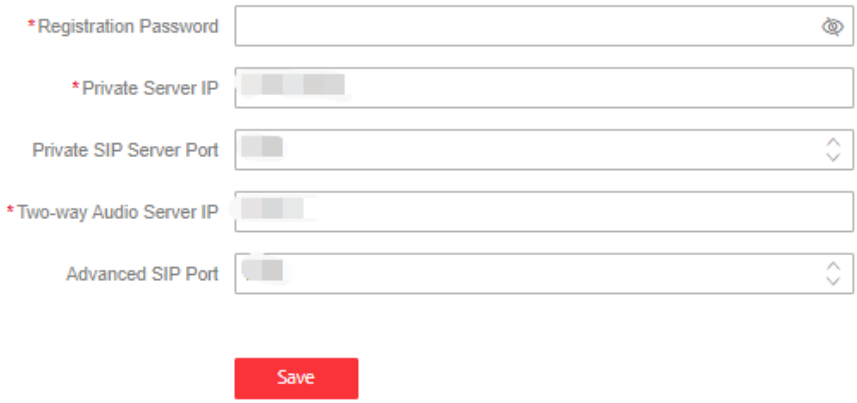

Figure 7-12 Session Settings

2. Set **Registration Password**.
3. Set **Two-way Audio Server IP**, **Private SIP Server Port**, **Advanced SIP Port** and **Private Server IP**.
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 Max. Intercom Duration via PC Web

You can finish time settings and call forwarding settings at this page.

Go to **Video Intercom → Call Parameters → Call Settings** .

Enter the **Max. Inercom Duration**.

Note

- The Max. intercom duration range is 90 s to 1800 s.
- When the audio is played via external speaker during a call, there may be an echo.

Enter the **Max. Live View Time** and **Max. Ring Duration**.

Note

- The Max. Live View Time range is 10 s to 1800 s.
- The Max. Ring Duration range is 30 s to 180 s.

You can also slide to **Enable Video Intercom Proxy Configuration** based on your actual needs.

Note

- If you select the **Industry Type** as Buidling, then you can configure phase, No. and proxy time period.
- If you select the **Industry Type** as General, you can configure phase, building, unit, floor, No. and proxy time period.

For **Call Forwarding Settings**, you can slide to enable **Call Forward when No Answer**, **Call Forwarding When Busy** or **Call Forwarding Schedule** based on your actual needs.

- **Call Forward when No Answer**: If enabled, you need to select **Call Forwarding Device**, set **Duration for No Answer Call Forwarding** and choose the start time and end time.

  Note

  The range of **Duration for No Answer Call Forwarding** is 10~60 s.
- **Call Forwarding When Busy**: If enabled, you need to select **Call Forwarding Device**.
- **Call Forwarding Schedule**: If enabled, you need to select **Call Forwarding Device** and click **+ Add** to create call forwarding schedule.

Click **Save**.

7.5.10 Add Broadcast Materials

You can add and delete broadcast materials in the Broadcast Material Database interface.

Steps

1. Click **Video Intercom → Broadcast Settings → Database** to enter the configuration interface.
2. Click **Batch Import** to select multiple broadcast materials from local storage.

   Note

   Each material should be less than 20 MB in MP3 or WAV format.
3. **Optional:** Click **Continue Import** to keep adding materials that need to be imported.
4. Click **OK**.
5. **Optional:** Check the broadcast materials that need to be deleted and click **Delete** to remove them.

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

Steps

1. Click **Video Intercom → Call Log** to enter this page.
2. Select the call type as **All**, **Incoming Call** or **Called**.
3. Select the call signaling as **All**, **SIP** or **VoIP**.
4. Click **Search** to find the records.
5. **Optional:** Click**Export All Record (s)** to export all the records.

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 **System and Maintenance → 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.

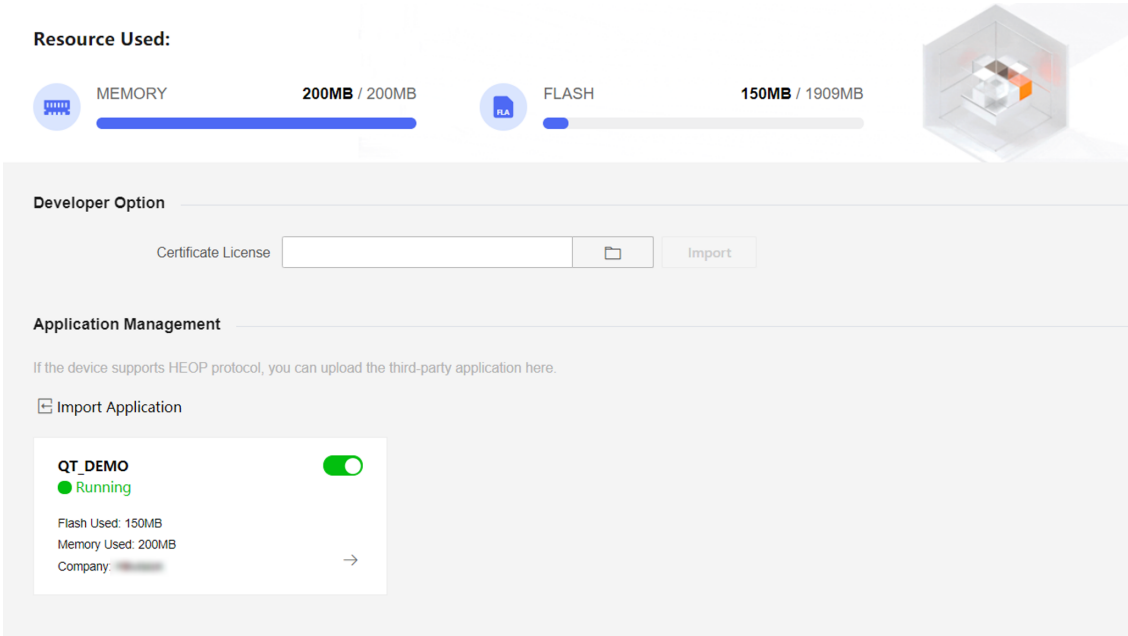

Figure 7-13 Open Platform

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** .
Upgrades include two types: device main program upgrades and touchscreen firmware upgrades. 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.

   Ping Network

   Enter the IP address to diagnose basic network issues.

   Capture Network Packet

   You can set the **Capture Packet Duration**, and click **Start Capture** to capture network data.
3. Click **Save**.

7.5.16 Log

Steps

1. Click **System and Maintenance → Maintenance → 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 HikCentral Professional Mobile Client. For details, see the platforms' user manual.

HikCentral Professional Mobile Client (HCP)

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

http://enpinfodata.hikvision.com/analysisQR/showQR/24cb4850

See Far, Go Further

UD43774B