



Panic Alarm 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.

© 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.

Contents

Chapter 1 About this Manual	1
Chapter 2 Activation	2
2.1 Activate via Device	2
2.2 Activate via Web Browser	2
2.3 Activate Device via iVMS-4200 Client Software	3
Chapter 3 Local Configuration and Operation	5
3.1 Local Configuration of Main Station	5
3.1.1 Activate the Device	5
3.1.2 Basic Settings	5
3.1.3 User Management	13
3.1.4 Synchronize Time	15
3.1.5 Call Settings	16
3.1.6 Broadcast Configuration	18
3.1.7 Restore Main Station	19
3.1.8 Upgrade	20
3.1.9 Maintenance	21
3.1.10 Device Information	24
3.2 Local Operation of Main Station	25
3.2.1 Call Settings	25
3.2.2 Live View	27
3.2.3 Broadcast Operation	29
3.2.4 The Third-Party App Settings	30
3.2.5 Information Management	31
3.2.6 One-Touch Screen Off	32
3.2.7 Change Calling Sequence	32
Chapter 4 Operation via Web Browser	33

4.1 Login	33
4.2 Overview	33
4.3 Quick Operation via Web Browser	34
4.3.1 Time Settings	34
4.4 Device Management	34
4.5 Camera Management	35
4.6 Partition Settings	36
4.7 Video Intercom Settings	37
4.7.1 Call Settings	37
4.7.2 Set Ringtone	38
4.7.3 Call Forwarding Settings	38
4.7.4 Add Broadcast Materials	39
4.7.5 View Call Log	39
4.8 Configuration	39
4.8.1 View Device Information	39
4.8.2 Set Time	40
4.8.3 Change Administrator's Password	40
4.8.4 User Management	41
4.8.5 Network Settings	41
4.8.6 Storage Settings	45
4.8.7 Set Video and Audio Parameters	45
4.8.8 Alarm Settings	47
4.8.9 Event Task Settings	48
4.8.10 Set Open Platform	50
4.8.11 Upgrade and Maintenance	51
4.8.12 Device Debugging	52
4.8.13 Test Protocol via PC Web	53
4.8.14 Log	53

4.8.15 Certificate Management	54
4.9 Help	55
4.9.1 Open Source Software Licenses	55
4.9.2 View Online Help Document	56
4.10 Logout	56
Chapter 5 Other Platforms to Configure	57

Chapter 1 About this Manual

Product	Model
Main Station	DS-PEA4H-20

Chapter 2 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

2.1 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 be 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).
-

2.2 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.

2.3 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 3 Local Configuration and Operation

3.1 Local Configuration of Main Station

3.1.1 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.

3.1.2 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.

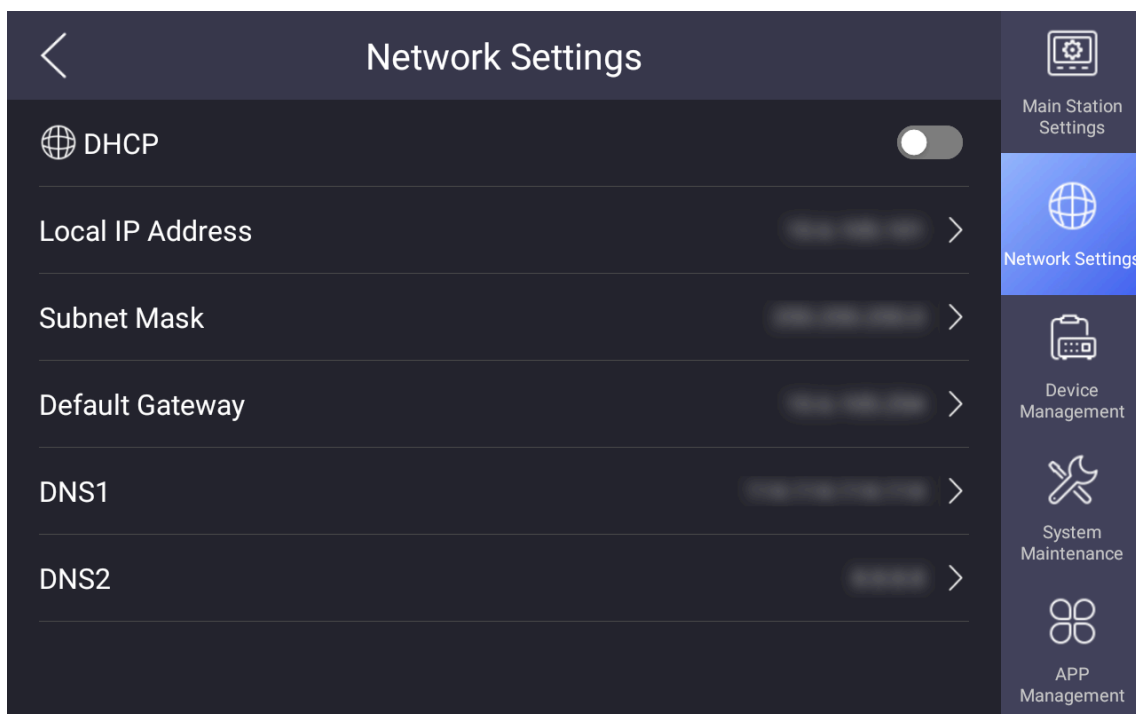


Figure 3-1 Network Settings

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, to which 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.

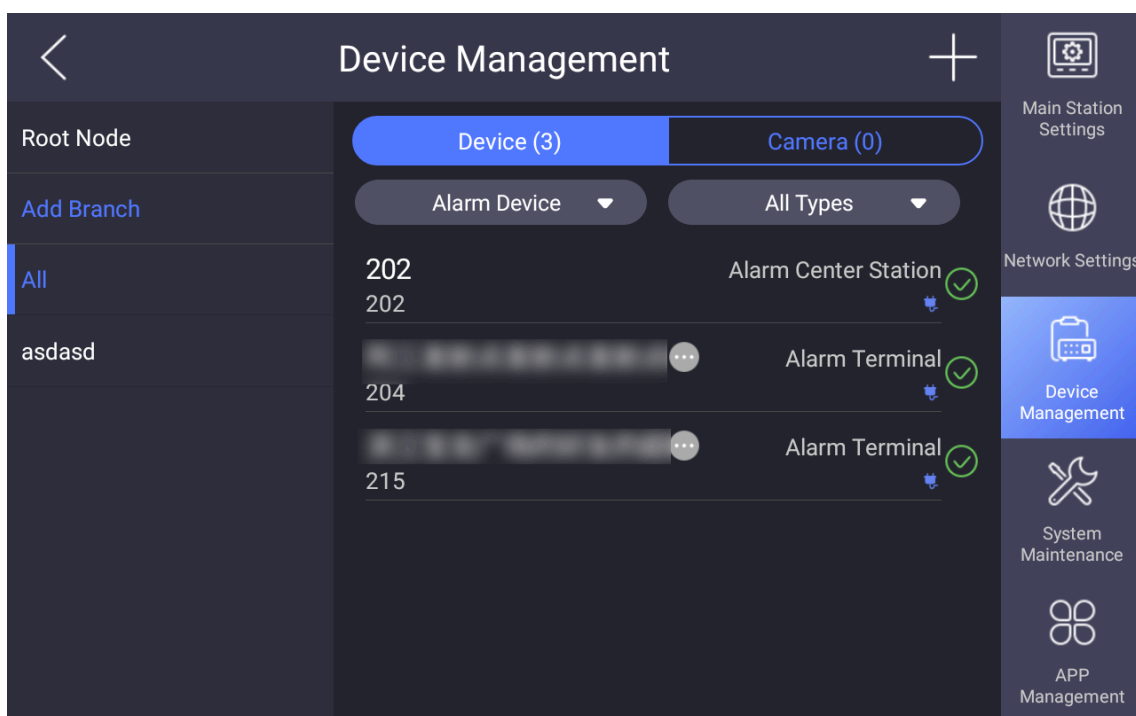


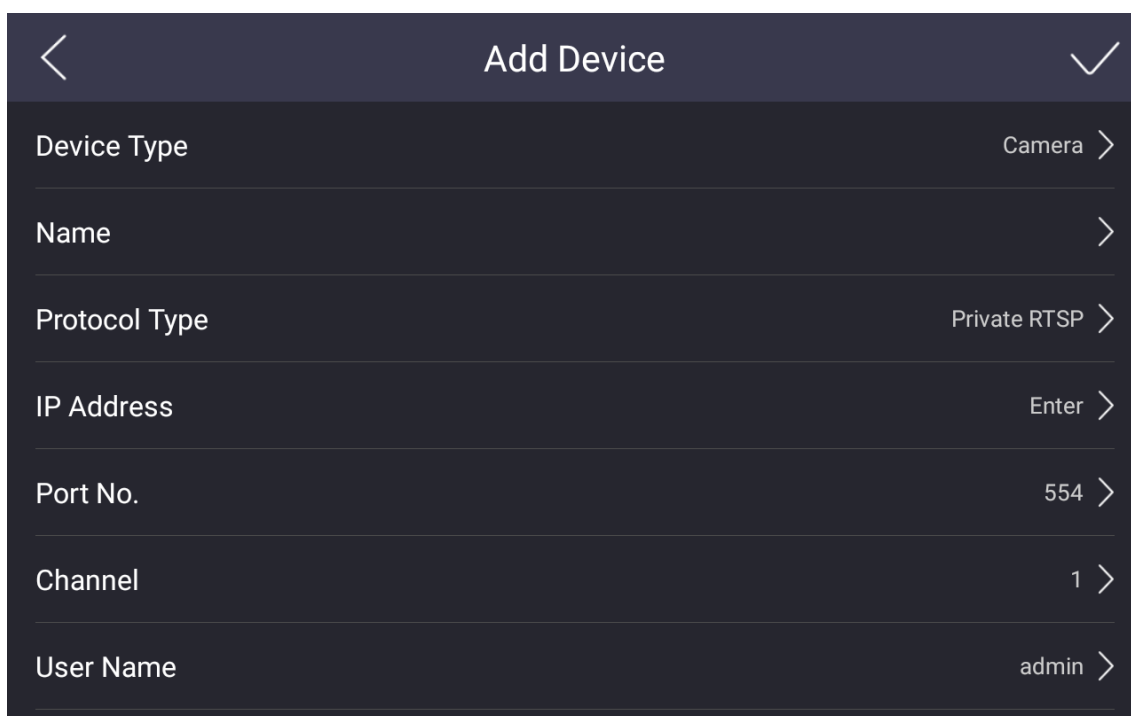
Figure 3-2 Device Management

3. Select device type from the drop-down list.
4. Tap **Add Branch** to create a panic alarm 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.



Add Device	
Device Type	Camera >
Name	>
Protocol Type	Private RTSP >
IP Address	Enter >
Port No.	554 >
Channel	1 >
User Name	admin >

Figure 3-3 Add Linked Device

6. Select the **Device Type**.
7. Set the linked device parameters.
8. Tap **V** to add.

Set Device No.

Main station No. can be dialed by other devices to call the main station in an panic alarm system.

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.

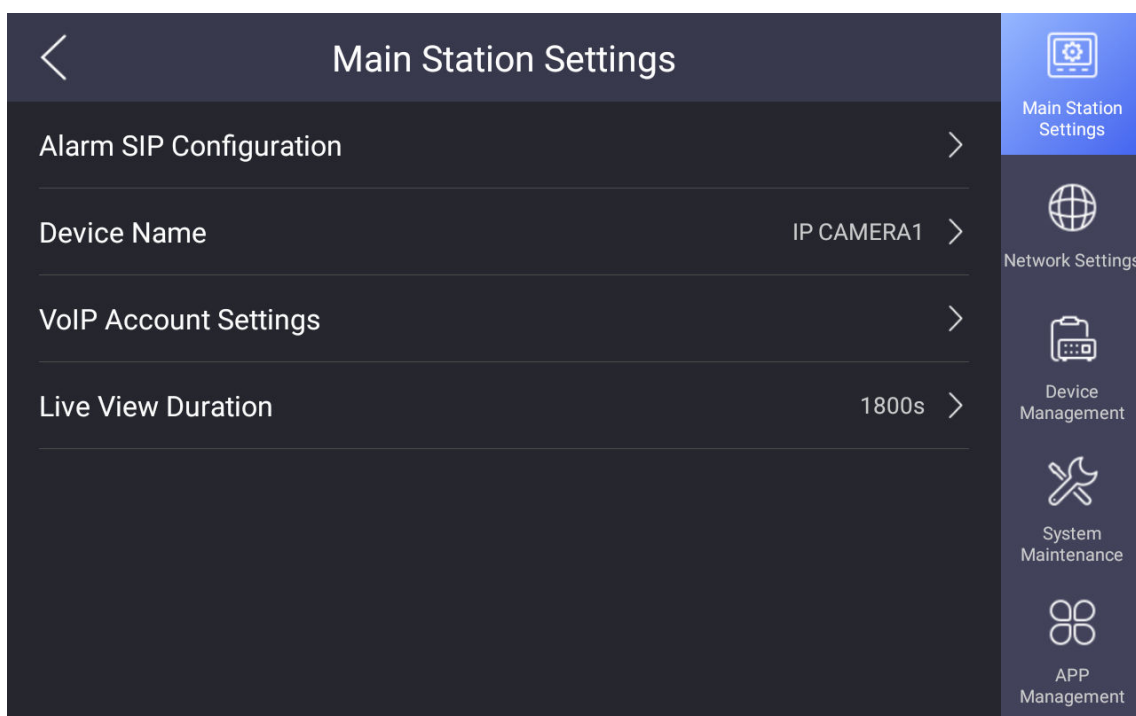


Figure 3-4 Device Settings

3. Set the following parameter.

Alarm SIP Configuration

Enable the SIP function and set the parameters. The SIP protocol enables communication between devices across different network segments. Without registration, devices can only communicate within the same network segment. After successful registration with the SIP server, devices can make calls by dialing using SIP IDs.

Server Address Type

Set the SIP server address as **IP Address** or **Domain Name**.

Server Address

You can enter the IP address of the management device that needs to communicate via SIP. In this case, the management device will function as a SIP server. Other devices must register with this SIP server address to enable mutual calling functionality.



Note

If main station 1 is configured as a SIP server, its wired network address must match the SIP server address; otherwise, main station 1 will not function as a SIP server.

Server Port

Set the SIP server port for communication.

Registration Period

Set the registration period. If the registration exceeds the period, the registration will be failed.

Registration Password

Enter the registration password for communication via SIP server.

Device Location

Set the device location name.

Device ID

Set this device's ID. If other alarm device wants to call the main station, dial the device ID to call.

Devie Name

Set the main station's name.

VoIP Account Settings

Account information for devices using VoIP communication.

You can edit VoIP account parameters. (Including user name, number, registered usered name, password, SIP server and private SIP.)

Live View Duration

Set the live duration. If the live video is played exceeds the configured duration, the live video will be stopped.

Add Camera

The main station can view the live video of 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.

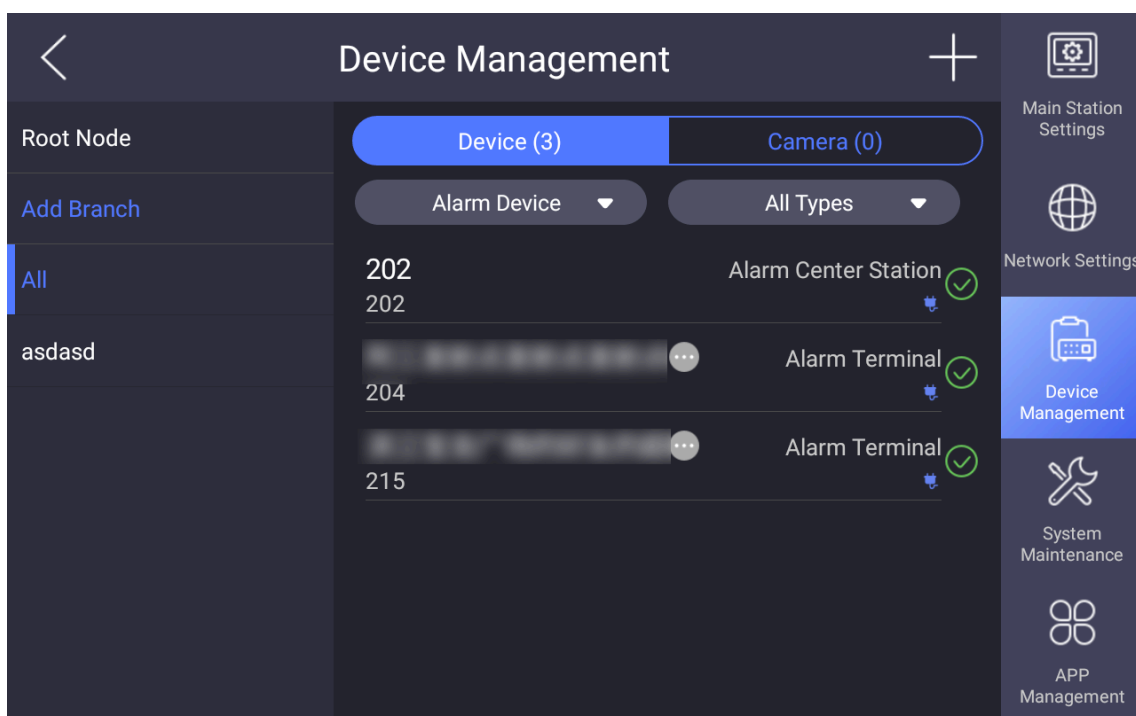


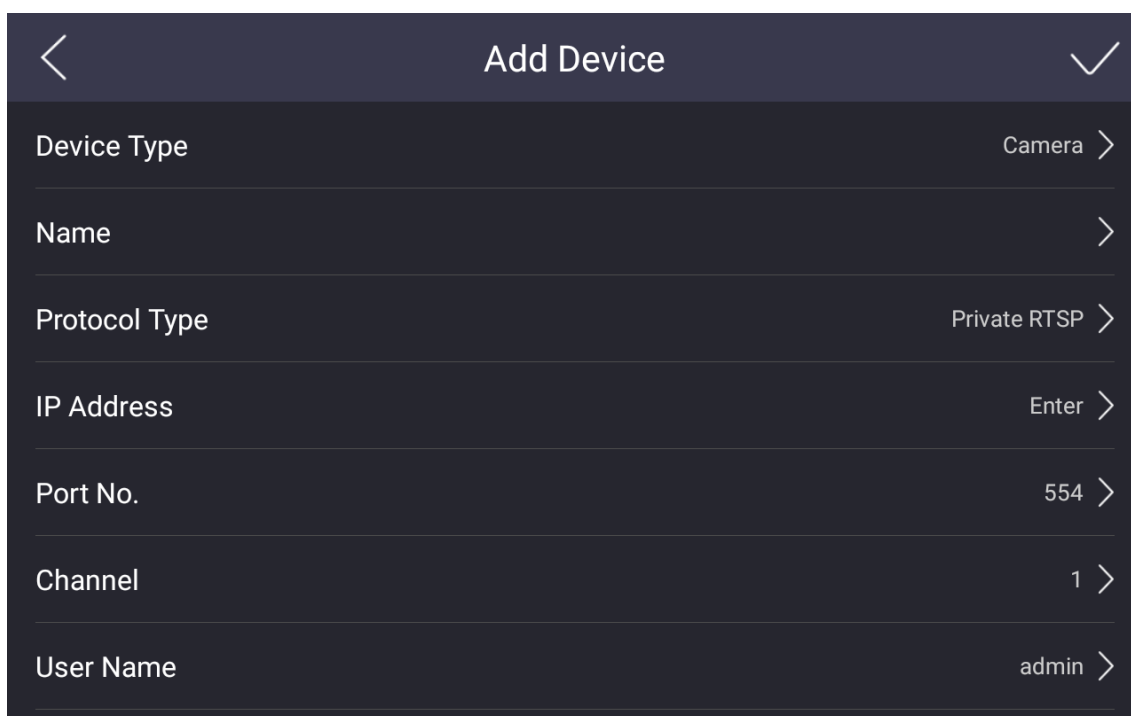
Figure 3-5 Device Management

3. Tap **Add Branch** to create an panic alarm 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.

4. Tap + to link the device.



Add Device	
Device Type	Camera
Name	
Protocol Type	Private RTSP
IP Address	Enter
Port No.	554
Channel	1
User Name	admin

Figure 3-6 Add Camera

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

Set Call Forwarding

Set call forwarding device and ring duration.

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.

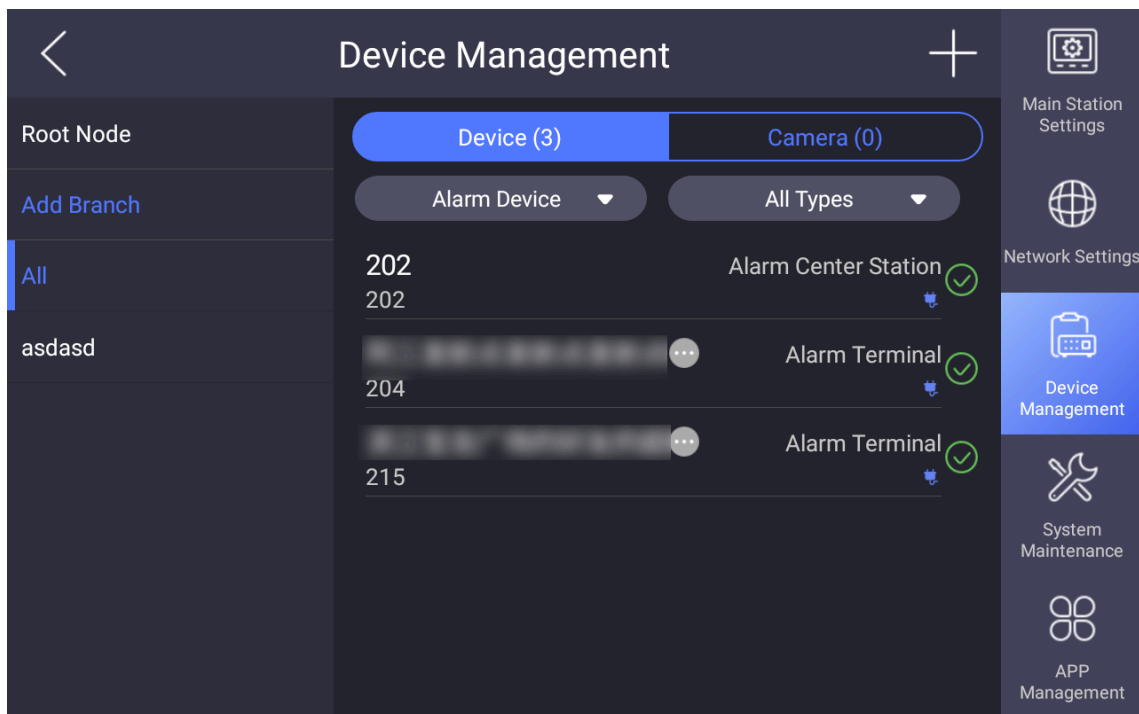


Figure 3-7 Device Management

3. Tap a device to enter the device details.
4. Tap **Call Forwarding** and set the parameters.

Enable Call Forwarding

Enable the function and if the call rings for the configured time, it will forward to the configured first, second, and third main stations by sequence.

First-Level/Second-Level/Third Level Transfer Main Station

Main Station

Select an added main station as the first forwarding device.



Note

You can add this device as the forwarding device.

Ring Duration

If the call rings for the configured time, it will forward to the configured main stations.

Delete

Tap to delete the forwarding item.

3.1.3 User Management

You can view the information of the user.

Steps

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

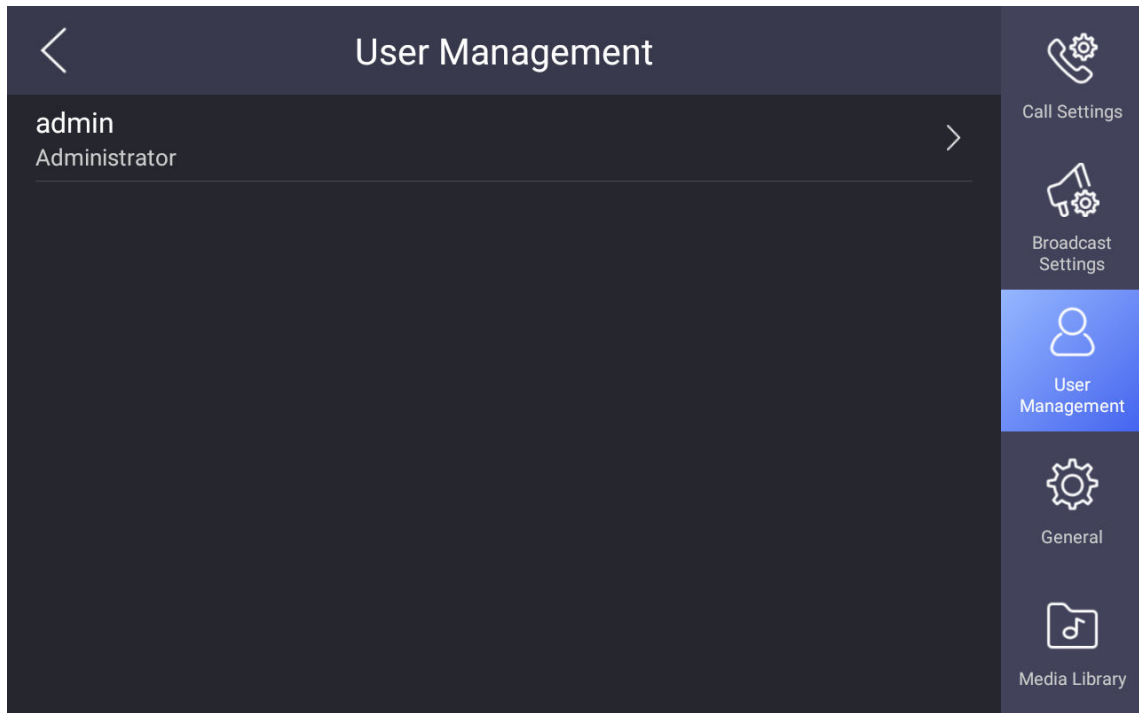


Figure 3-8 User Management

2. Tap **admin** to view the details.

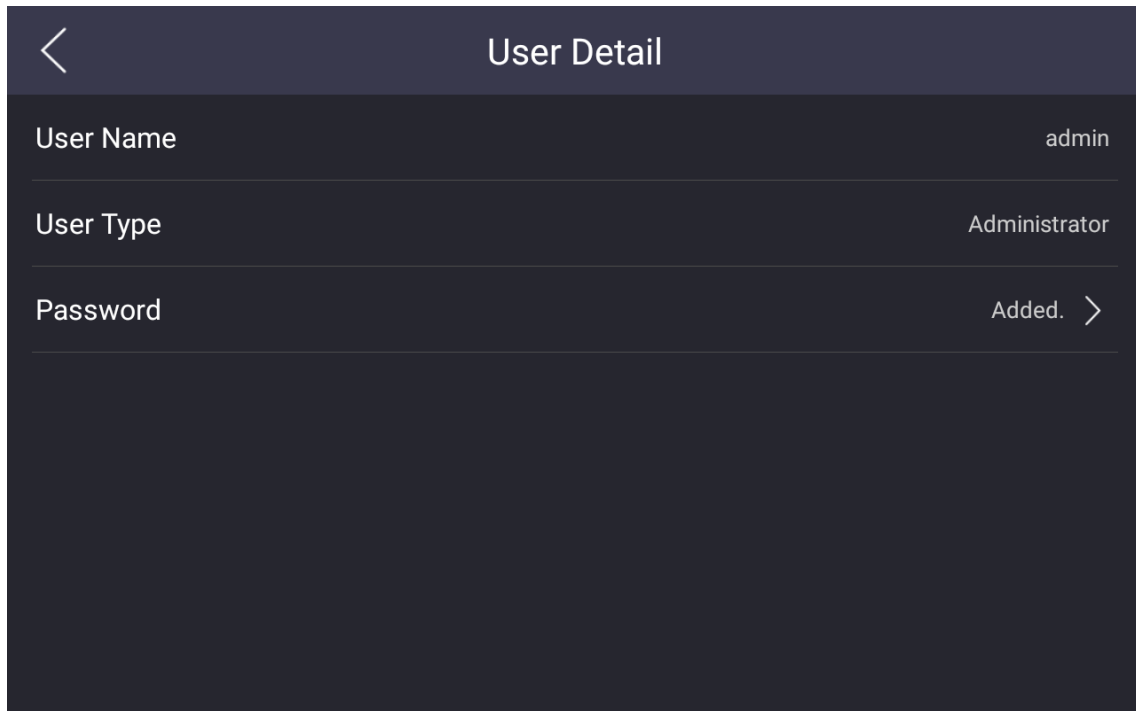


Figure 3-9 Details

3.1.4 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.

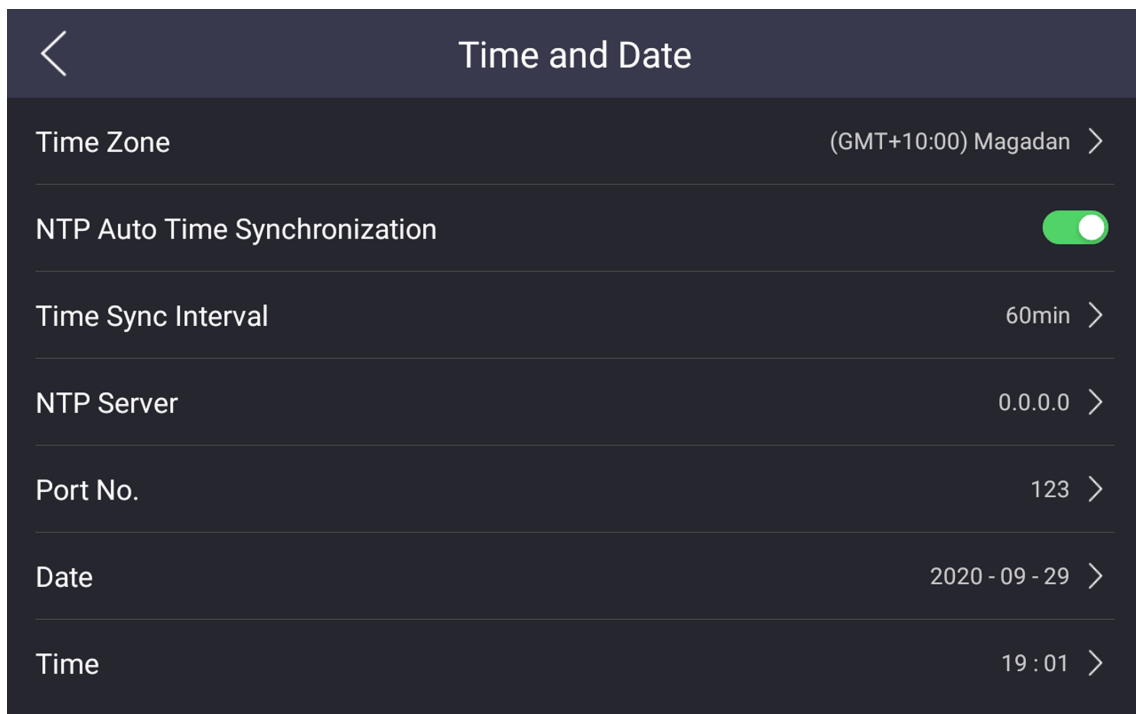


Figure 3-10 Time and Date

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.

3.1.5 Call Settings

You can set the call volume, input volume, voice prompt volume, ringtone, ring duration, microphone input, automatic recording, auto answer, and auto answer ring duration.

Steps

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

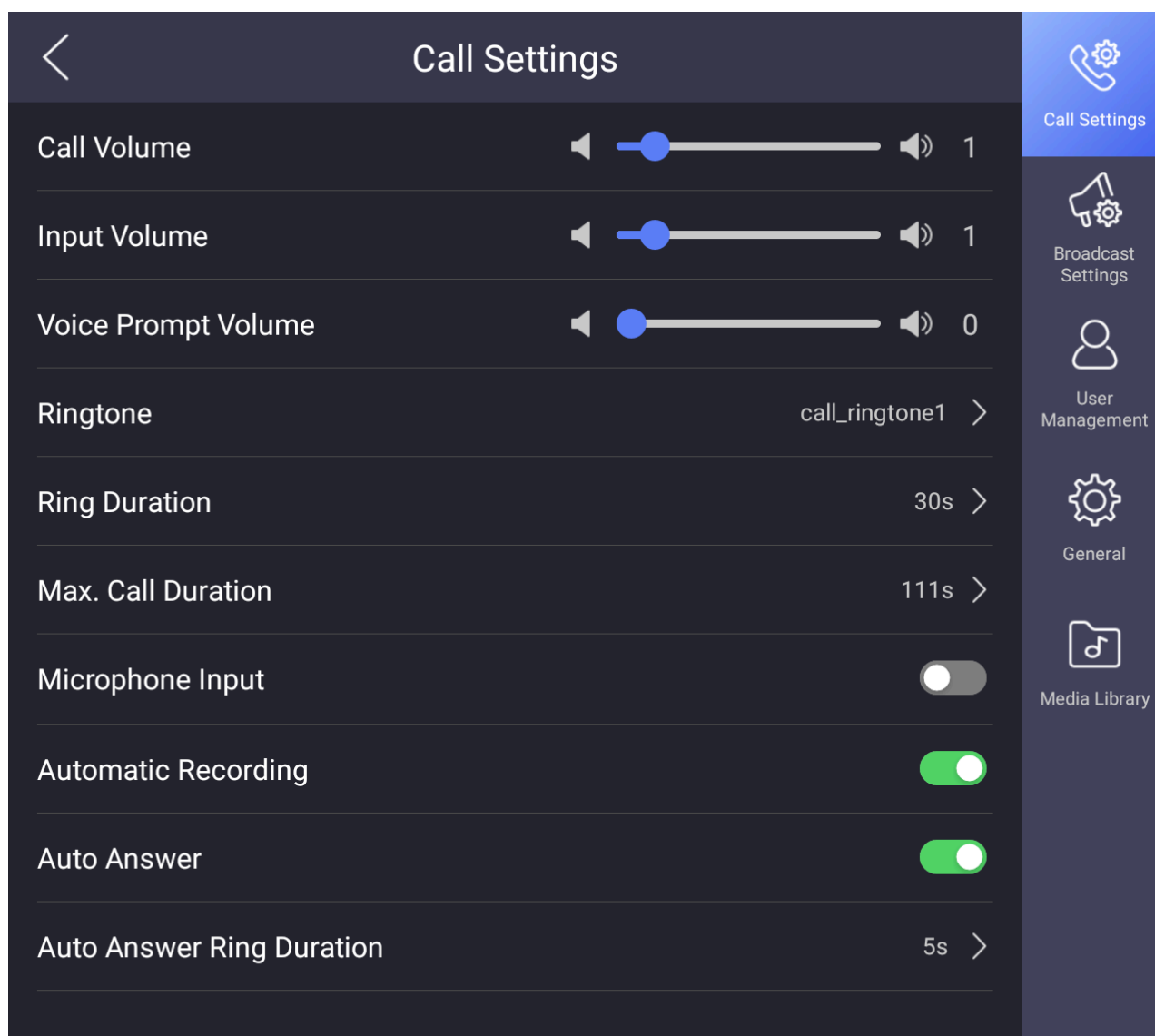


Figure 3-11 Call Settings

2. Set corresponding parameters.

Call Volume/Input Volume/Voice Prompt Volume

Set the volume.

Ringtone

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

Ring Duration

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

Max. Call Duration

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

Microphone Input

If the device has connected with a microphone, you should enable the function.

Automatic Recording

If enable the function, the device will auto recording the calling video and audio.

Auto Answer

If enable the function, the call will be auto answered.

Auto Answer Ring Duration

When another terminal calls this device and the calling device is set to auto answer, you can set the auto answer time. After the set time ends, this device will automatically answer.

3.1.6 Broadcast Configuration

Configure broadcast-related functions, including live broadcast priority and emergency broadcast function.

Steps

1. Click **Configuration** →  to enter the broadcast parameter settings page.

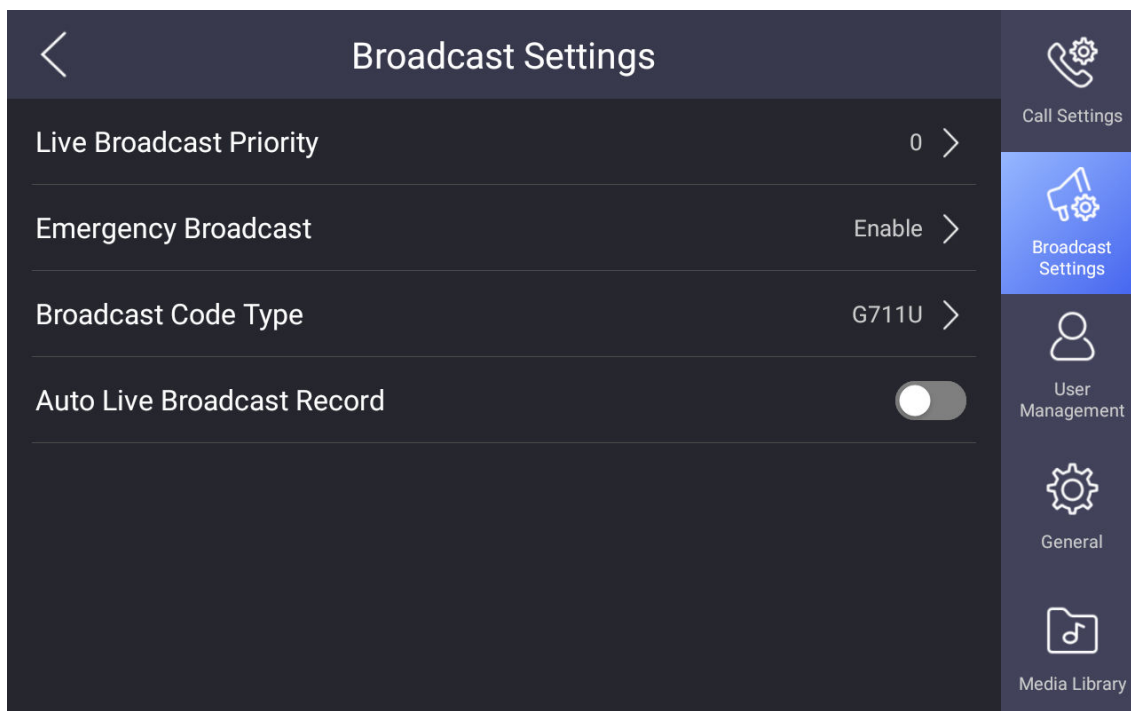


Figure 3-12 Broadcast Settings

2. Configure the relevant parameters.

Live Broadcast Priority

When multiple main stations are connected to the same broadcast device, you can set the live broadcast priority. The higher the number, the higher the priority. Devices with higher priority can interrupt devices with lower priority to broadcast first.



Note

The priority setting range is 0 to 15.

Emergency Broadcast

If there is an emergency requiring temporary broadcasting, the emergency broadcast function can be enabled.

Emergency Broadcast Trigger Method

Press: Short press the  button on the main page to trigger emergency broadcast.

Press and Hold: Hold the  button on the home page to trigger emergency broadcast.

Broadcast Terminal

Select the device for emergency broadcast.

Broadcast Code Type

Select the required broadcast encoding type. Alarm devices only support the **G711U** format. After enabling the emergency broadcast, you can short press/hold the  on the device home page to perform emergency broadcasting.

3.1.7 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.

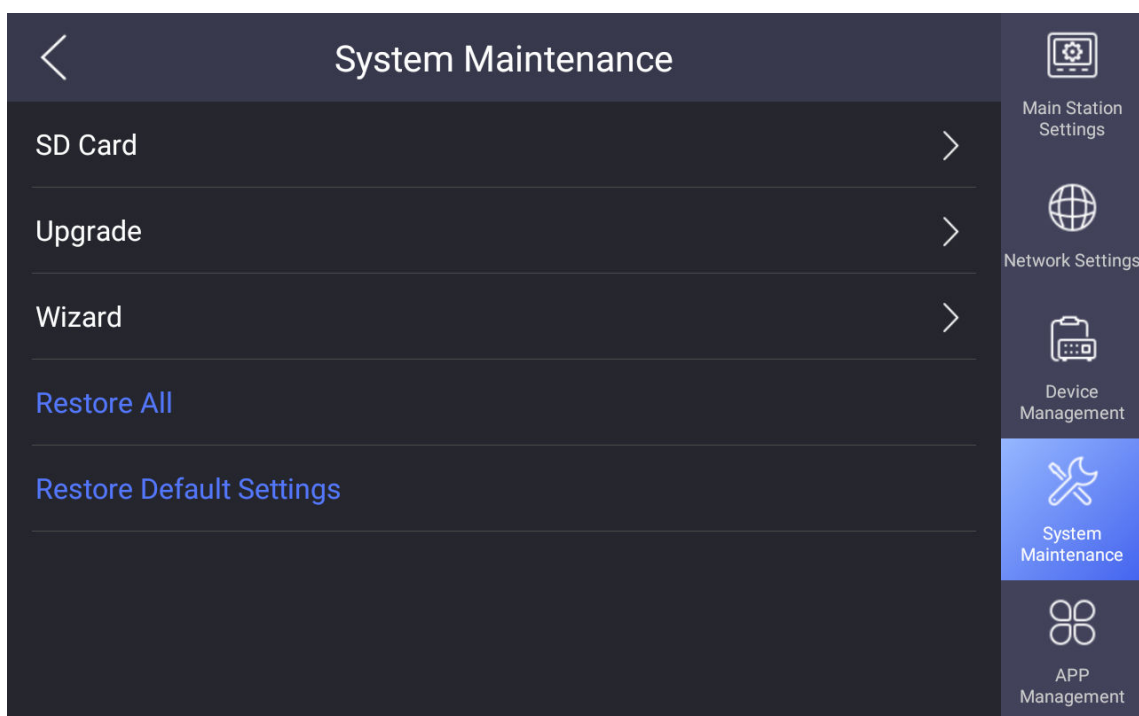


Figure 3-13 Maintenance

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.

3.1.8 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.

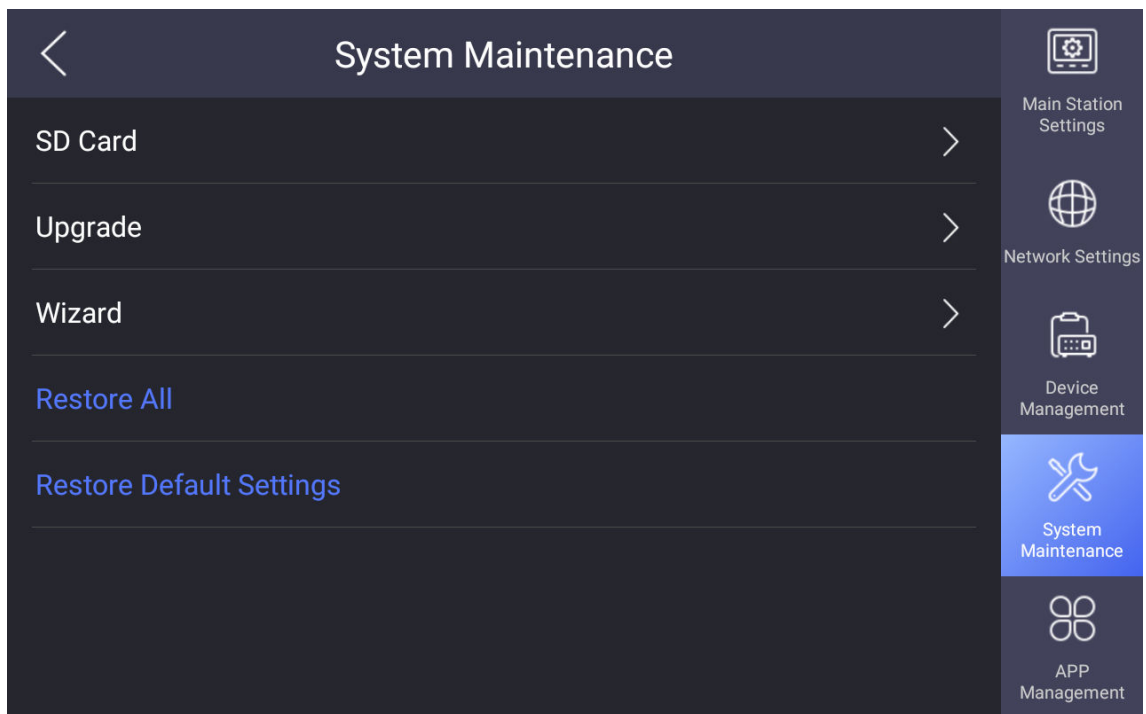


Figure 3-14 Maintenance

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

3.1.9 Maintenance

SD Card

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

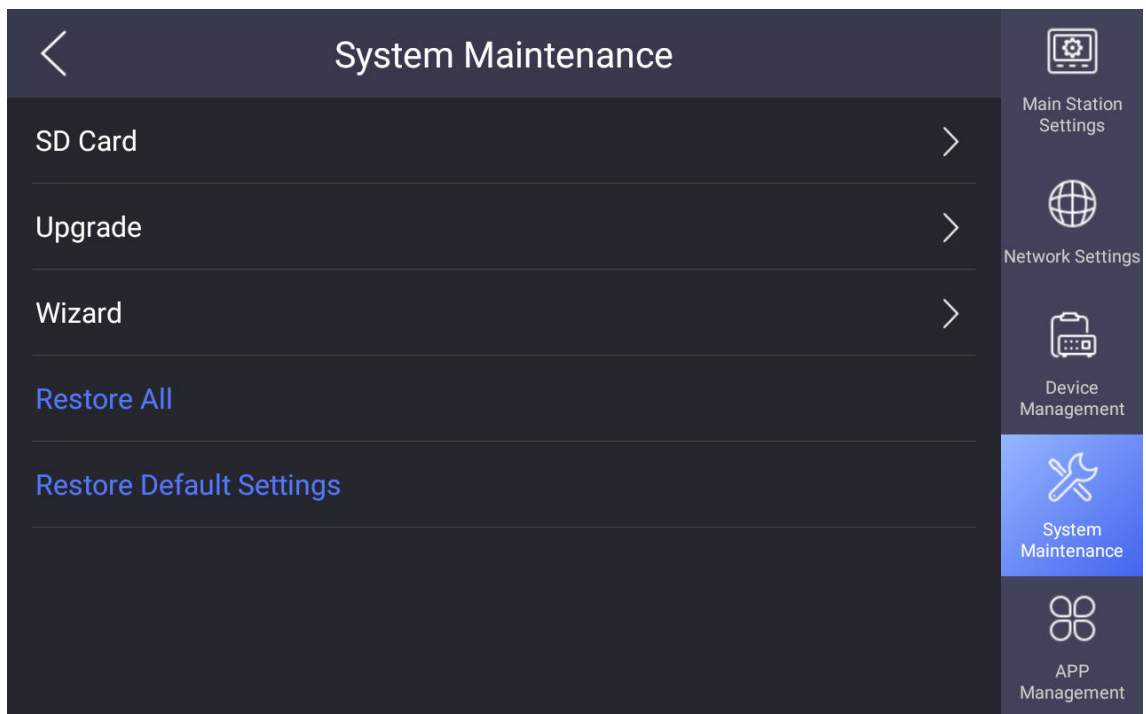


Figure 3-15 Maintenance

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.

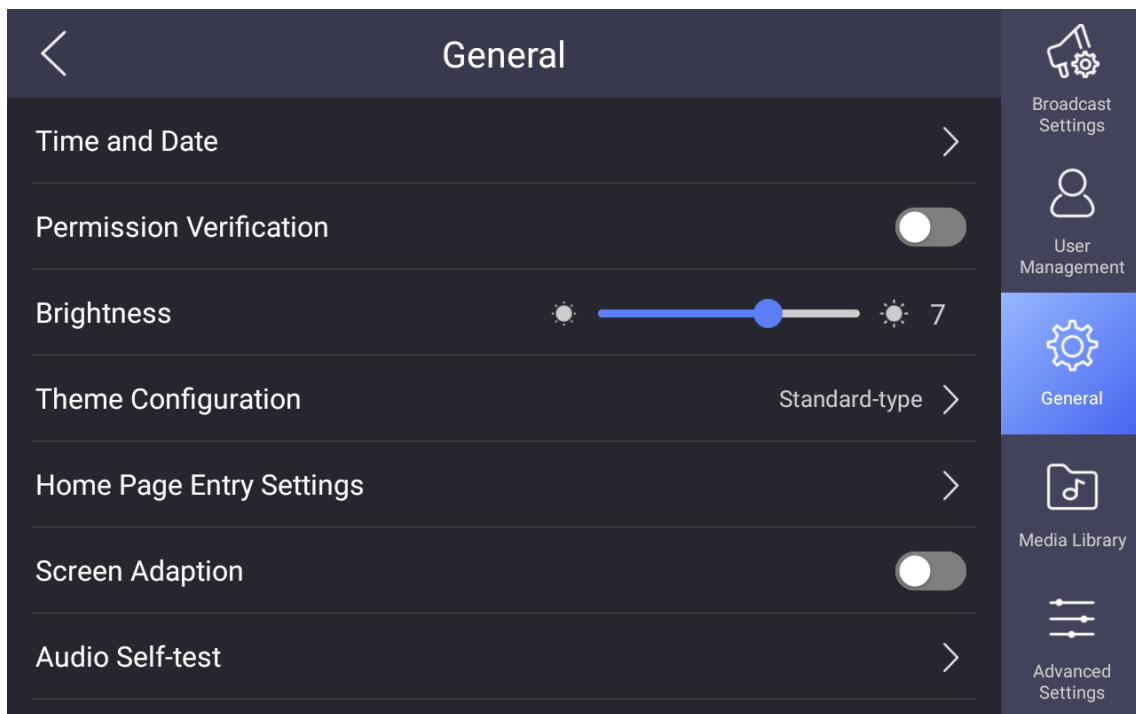


Figure 3-16 General Settings

Slide to enable the permission verification and screen adaption function.

Permission Verification

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

Brightness

Move the blocker to adjust the screen brightness.

Theme Configuration

Select the display theme.

Home Page Entry Settings

Custom the home page displayed shortcuts and their sequence.

Screen Adaption

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

Audio Self-test

Select the audio self-test device and the device will broadcast the test audio.

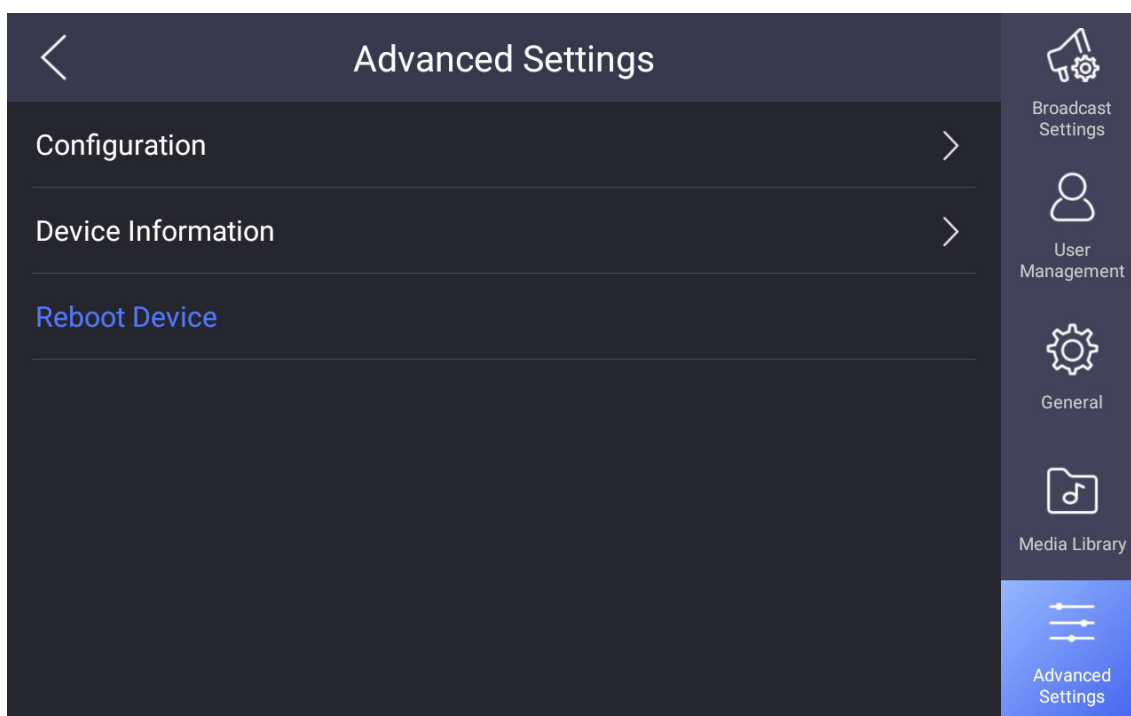


Figure 3-17 Advanced Settings

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

Tap **Reboot Device** to reboot the system.



Note

Please do not power of during rebooting.

3.1.10 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.

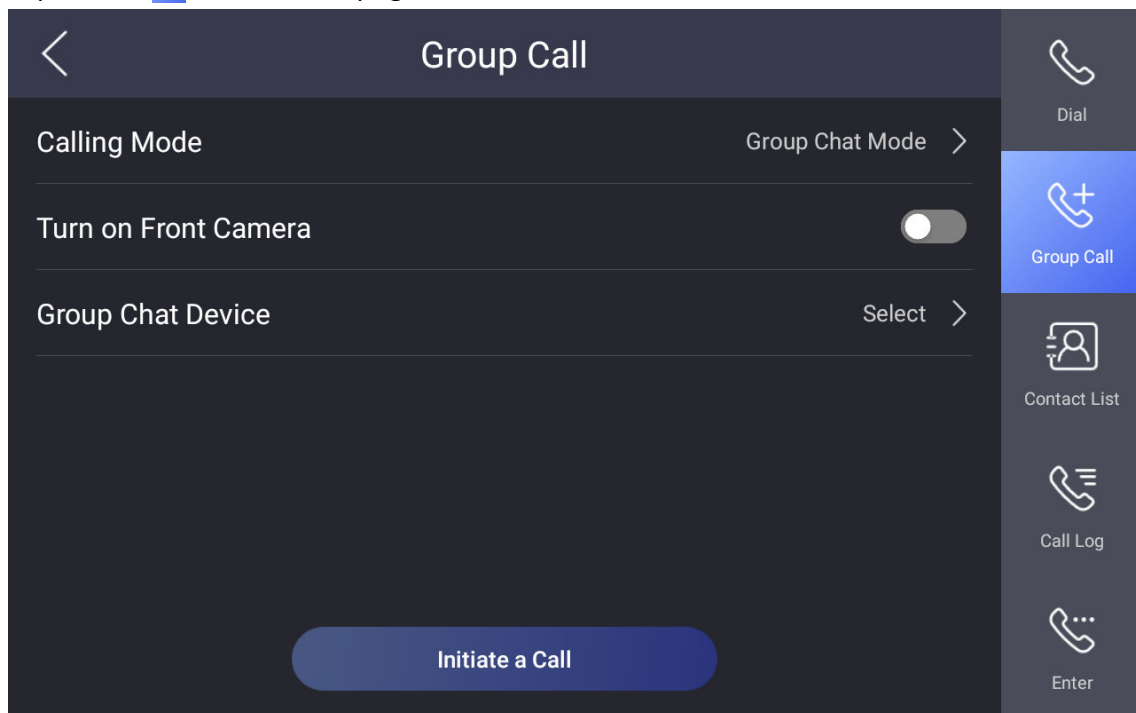
3.2 Local Operation of Main Station

3.2.1 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 other main stations or alarm devices.

Steps

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

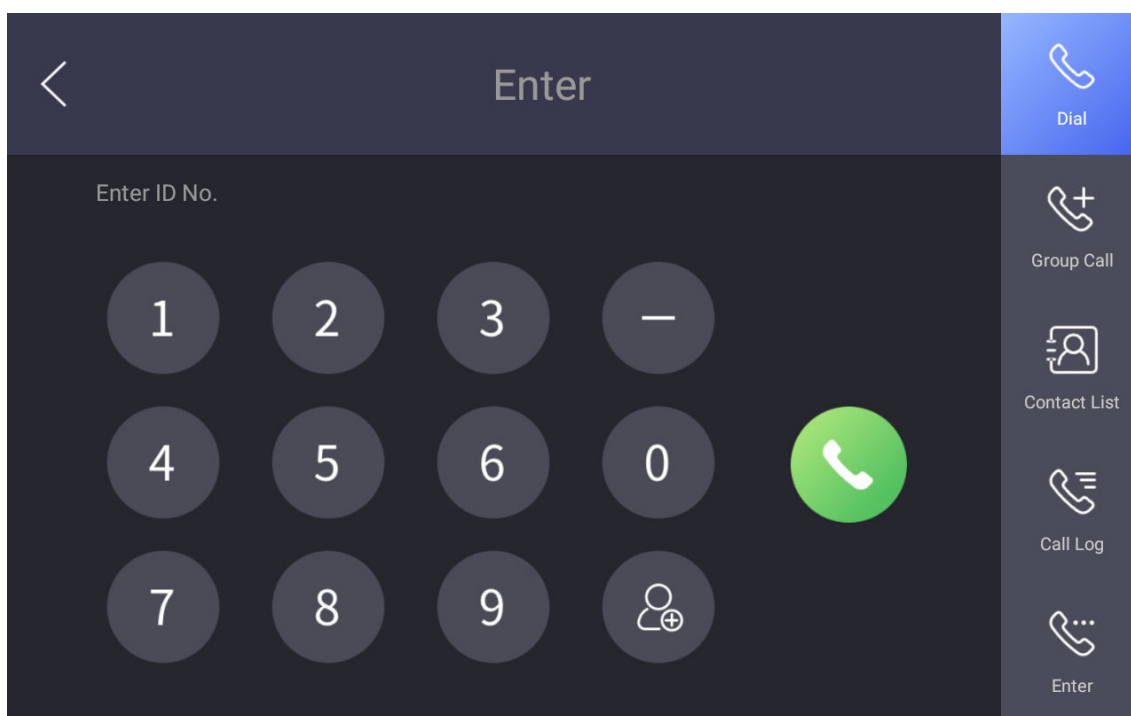


Figure 3-19 Call Page

2. Enter the device ID to call.

 Note

If you in the card mode, you can tap a resident card to call.

Receive Call

The main station can receive the call from other main stations or devices.

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.

 Note

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

You can also forward the call manually to other alarm devices.

If you have configured the call forwarding function, the call will automatically forward to other devices. For details, see

View Call Logs

View call logs of the main station.

Steps

1. Tap **Call** →  on the main page.

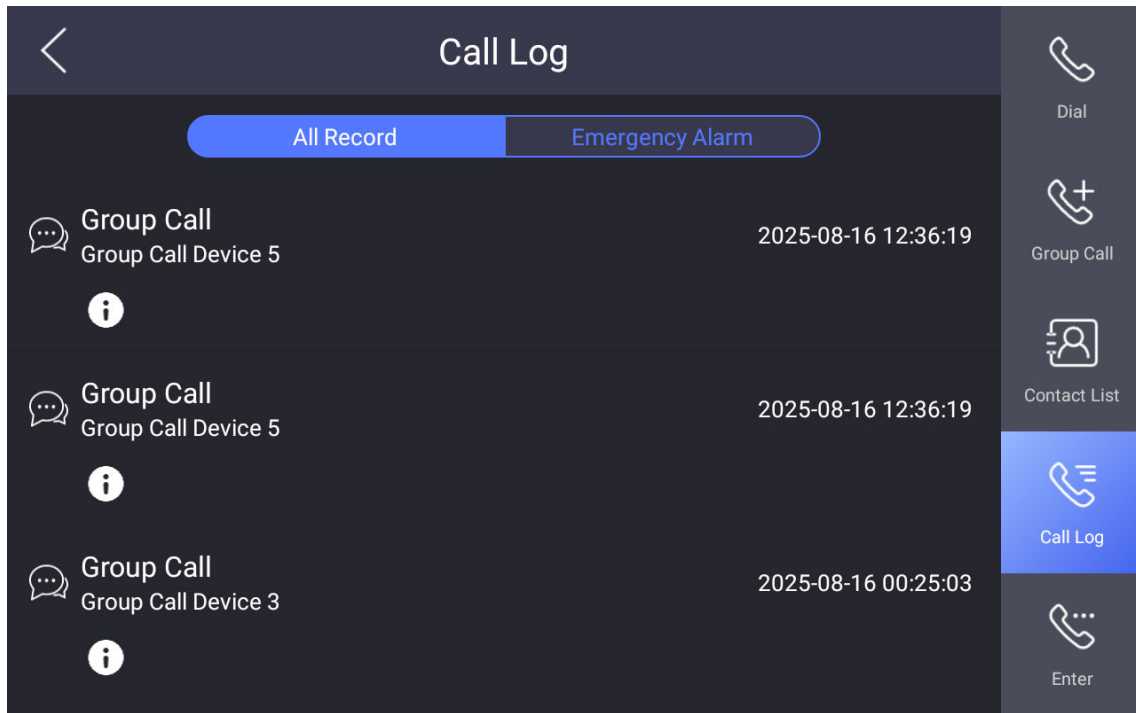


Figure 3-20 Call Log Page

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.

3.2.2 Live View

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

Steps

1. Tap **Live View** on the main page to enter the live view page.

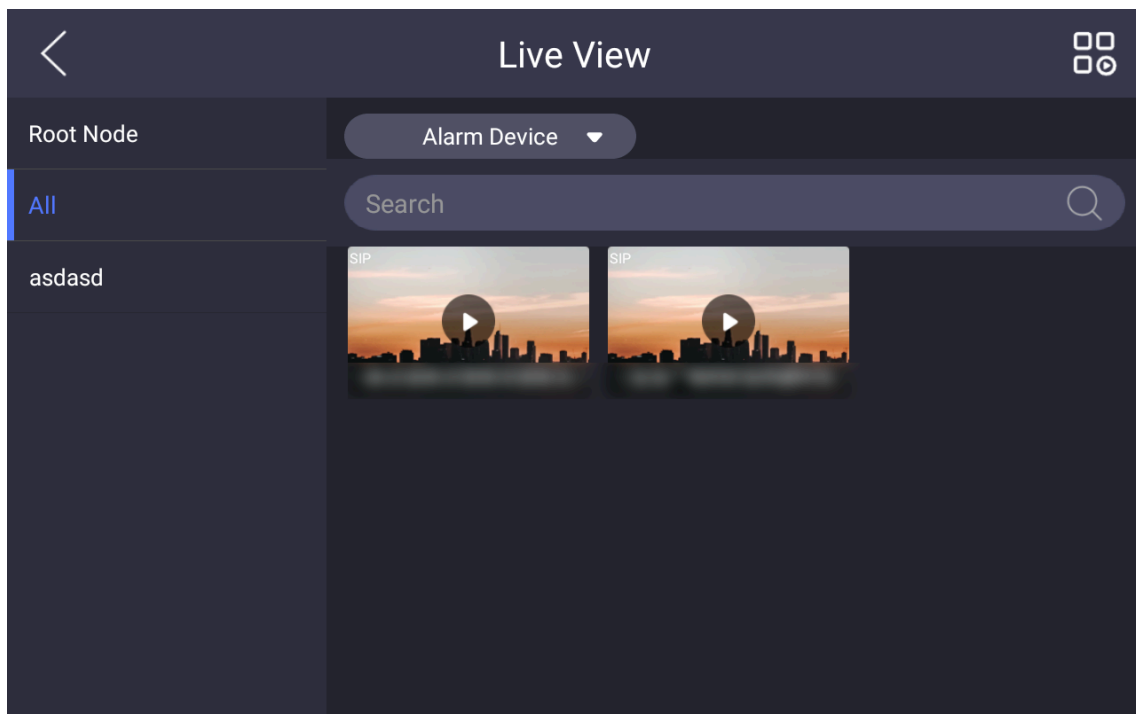


Figure 3-21 Live View Page

2. Tap one of the live videos to view the live videos of other devices.

3. **Optional:** You can do the following actions on the live view page.

Icon	Descriptions
	Add other alarm device for multi-window live view.
	If multiple calls is coming in, you can tap the button to select a call to answer.
	Speak with the current alarm device.
	Tap to show more functions.
	Record the video (except the audio).
	Capture the current picture.
	Listen the current alarm device.
	Control the auxiliary power supply.
	Control the alarm output device.
	Adjust the alarm device's volume.
	Adjust the alarm device's speaker's volume.

3.2.3 Broadcast Operation

Real-time Broadcasting

You can start real-time broadcasting from the main station.

Audio Source Settings

On the device home page, tap **Broadcast** →  → **Audio Source Control** to enter the audio source settings page.

Select the audio source as **File**, **Speech Synthesis**, **Microphone**, or **Local Sound Card**.

File

Play audio source files, with options for **Sequential Play** or **Loop Playback**.



Note

Audio source files are obtained from the media library. Media files need to be imported through the web page.

Speech Synthesis

Input voice content and select broadcast voice as male or female for broadcasting.



Note

The input character count for voice content cannot exceed 4096.

Microphone

Connect the local microphone for voice broadcasting.

Local Sound Card

Broadcast through the local sound card. After selecting this option, you need to enter **Third-party Applications** from the main page, open the application to be played, and select the file for playback. Then return to real-time broadcasting for playback configuration.

Start Broadcast

Select broadcast terminals to initiate real-time broadcasting.

Tap **Broadcast** →  → **Broadcast Terminal** to enter the configuration page.

Select a device from the list and tap  to start broadcasting.

Note

Real-time broadcasting cannot simultaneously select intercom devices and alarm devices for broadcasting.

View Broadcast Records

You can view the records of devices that have received broadcasts.

On the device home page, click **Broadcast** →  to enter the broadcast records page. You can view the records of devices that have received broadcasts.

Broadcast Device Status

View the status of added broadcast devices.

On the device home page, tap **Broadcast** →  to enter the broadcast device status viewing page. You can view the status of corresponding broadcast terminals by node, including the number of offline devices and the total number of devices.

3.2.4 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.

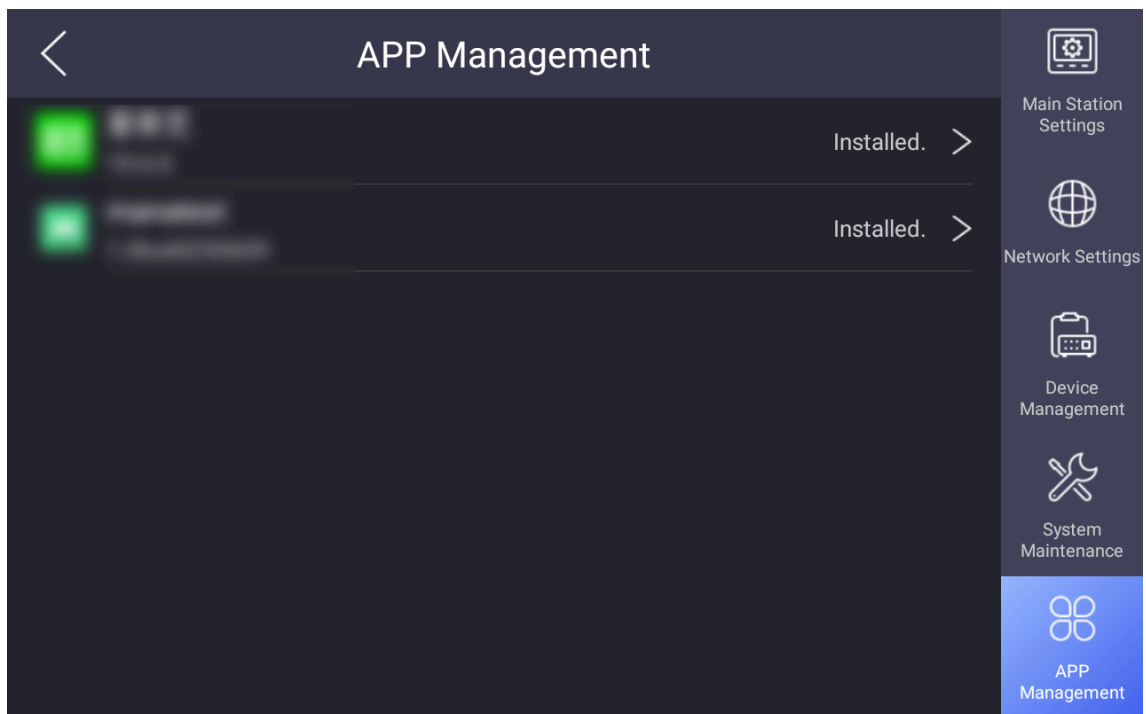


Figure 3-22 Add the Third-Party Apps

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.

3.2.5 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.

3.2.6 One-Touch Screen Off

The management device supports one-touch screen off function.

Steps

1. On the management device's main interface, tap  to perform screen off.

3.2.7 Change Calling Sequence

You can change the calling sequence in card-type mode.

On the home page, if you are in the card-type theme, you can tap **Order** on the upper right corner of the page and hold the card to change the sequence.

Note

For details about the theme change, see [**Maintenance**](#)

Chapter 4 Operation via Web Browser

4.1 Login

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



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**.



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

4.2 Overview

You can view linked device, network status and basic information. You can also click on related parameters to configure.

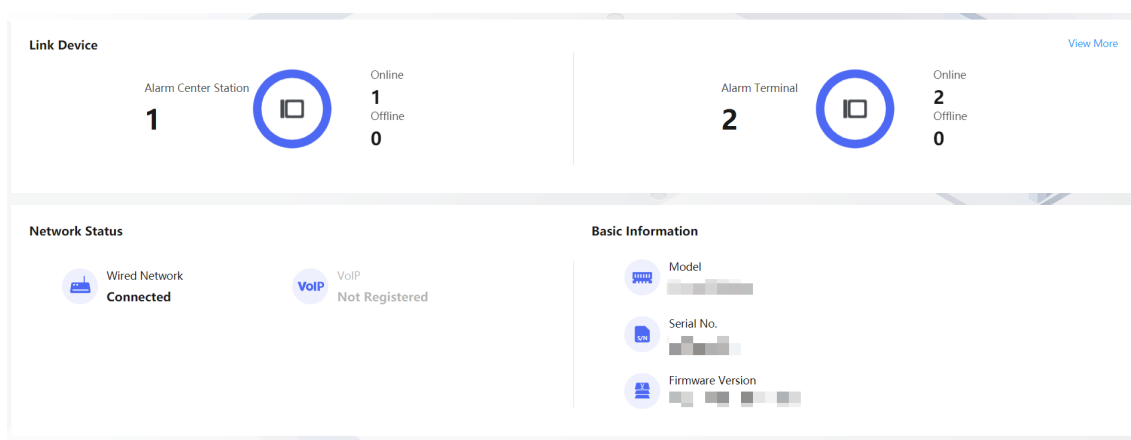


Figure 4-1 Overview

Function Descriptions:

Link Device

You can check if the device is working properly. You can also see online and offline device numbers.

Click **View More** to view the detailed component status. It will lead you to **Device Management** page.

Network Status

You can view the network connection status.



Note

Click on **Wired Network** or **VoIP** to configure.

Basic Information

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



Note

Click on related parameters to check detailed information.

4.3 Quick Operation via Web Browser

4.3.1 Time Settings

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address/NTP Port/Interval

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

DST

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

4.4 Device Management

You can manage the linked device on the page.

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

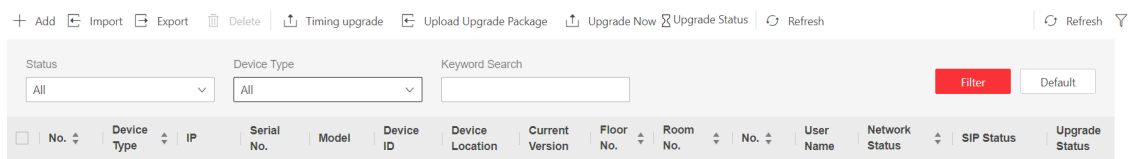


Figure 4-2 Device Management

Add Device

- Click **Add** to add the main 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 devices and click **Delete** to remove the selected device from the list.

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.

Set Device Information

- Click to edit device information.
- Click to delete device information from the list.
- Select **Status**, **Device Type**, enter **keyword**, and click **Filter** to search devices.

4.5 Camera Management

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

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

Click **Add** to add camera.

Name *

IP Address *

Protocol

☒ Private RTSP Protocol ☐ open network video interface

Channel No. *

Port *

User *

Password *

Add Cancel

Figure 4-3 Add Camera

4.6 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.

4.7 Video Intercom Settings

4.7.1 Call Settings

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

Set the parameters and click **Save**.

Max. Intercom Duration

Set the Max. intercom duration. If the call is exceed the duration, the call will be ended.



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.
-

Max. Ring Duration

Set the Max. ring duration. If the ringing time exceeds the duration, the ringing will be ended.



Note

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

Max. Live View Time

Set the Max. live view duration. If the live view time exceeds the duration, the live view will be ended.

Auto Answer

If enable the function, the call will be auto answered.

Auto Answer Time

When another terminal calls this device and the calling device is set to auto answer, you can set the auto answer time. After the set time ends, this device will automatically answer.

Alarm Proxy Configuration

If enable the function, the configured proxy main station will answer the call.

Alarm Proxy Configuration Main Station

Select the proxy main station.

Proxy Time Period

Set the time duration that the proxy main station can answer the call.

4.7.2 Set Ringtone

Steps

1. Click **Video Intercom** → **Call Parameters** → **Ringtone Configuration** .
2. Click **Add** →  and click **Import** to import new ringtone.



Note

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

3. You can enable the ringtone in the list or click  to delete the ringtone.

4.7.3 Call Forwarding Settings

Configure call forwarding rules to ensure emergency calls are transferred to backup main stations when the primary station cannot answer in time.

Before You Start

Make sure all main stations that need to call forwarding are added to this device.

Steps



Note

- Verify that all designated backup main stations are properly configured and operational.

1. Click **Video Intercom** → **Call Parameters** → **Call Forward Settings** .

Alarm Terminal ID	Default Transfer Host		First-Level Transfer			Second-Level Transfer			Third-Level Transfer			Transfer Status	Operation
	Main Station	Status	Main Station	First-Level Ring Duration	Status	Main Station	Second-Level Ring Duration	Status	Main Station	Third-Level Ring Duration	Status		
600	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
614	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
602	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
616	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
604	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
618	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
605	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
606	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
621	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
608	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
609	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
624	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
625	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 
612	--	--	--	--	--	--	--	--	--	--	--	❌ Disabled	 

Total: 250 20

< 1 2 3 4 5 6 ... 13 > 1 / 13 Go

Figure 4-4 Call Forwarding Settings

2. Select a main station in the list and click .
3. Configure the call forwarding parameters.

Call Forwarding

Enable the function and if the call rings for the configured time, it will forward to the configured first, second, and third main stations by sequence.

First-Level/Second-Level/Third Level Transfer Main Station

Select an added main station as the first forwarding device.



Note

You can add this device as the forwarding device.

Ring Duration

If the call rings for the configured time, it will forward to the configured main stations.

4. **Optional:** Click  and check the devices and click **OK** to copy the settings to other devices.

4.7.4 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.

4.7.5 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.

4.8 Configuration

4.8.1 View Device Information

View the device name, language, model, serial No., version, 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, available video channel, IO input, IO output, local RS-485, alarm input and alarm output number.

You can change **Device Name** and **Device No.** and click **Save**.

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

You can view the device capacity, including person, card, event, and palm print.

4.8.2 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** .

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address Type/Server Address/NTP Port/Interval

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

4.8.3 Change Administrator's Password

Steps

1. Click **System and Maintenance** → **System Configuration** → **System** → **User Management** → **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.

4.8.4 User Management

You can add operator on the page.

Steps

1. Click **System and Maintenance** → **System Configuration** → **System** → **User Management** → **User Management** to enter the page.
 2. Click **Add** and complete related information to add an operator, including **User Name**, **User Type**, **Password**, and **Confirm 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.

3. Delete or edit users.
 - Click  to delete user.
 - Click  to edit user information.
4. Input keywords in the bar and click  to search users, and the qualified users will be displayed on the result list.

4.8.5 Network Settings

Set Basic Network Parameters

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

DHCP ☐

*IPv4 Address

*IPv4 Subnet Mask

*IPv4 Default Gateway

DNS Server

Preferred DNS Server

Alternate DNS Server

Figure 4-5 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.

Port Settings

Set corresponding ports when accessing devices via network as needed.

HTTP Settings

Enter the device address in the browser, after logging in, click **System and Maintenance → System Configuration → Network → Network Service → HTTP(S)**.

HTTP Port

When logging in via browser, add the port number after the address. For example, when HTTP port is changed to 81, you need to enter `http://192.0.0.65:81`.

HTTP Listening

Device sends alarm information to target IP or domain via HTTP protocol, requiring the target IP/domain to support HTTP transmission. Enter target IP/domain, URL address and port, then select protocol type.

Click **Save** to complete configuration.

RTSP Settings

Enter the device address in the browser, after logging in, click **System and Maintenance → System Configuration → Network → Network Service → RTSP** to configure and view RTSP ports.

RTSP is Real Time Streaming Protocol port. You can view and configure RTSP ports.

Click **Save** to complete configuration.

SDK Service Port Settings

Enter the device address in the browser, after logging in, click **System and Maintenance → System Configuration → Network → Device Access → SDK Server** to configure and view SDK service ports. View and edit device service ports. Click **Save** to complete configuration.

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**.

Enable VoIP Gateway ☒

*Register User Name

*Registration Password

*Server IP Address

Server Port

Expiry Time min

Registration Status Not Registered [Refresh](#)

*Number

*Display User Name

Figure 4-6 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 Alarm Access

Alarm server enables communication between terminals across different network segments. Without registration, only terminals within the same segment can communicate. After successful server registration, terminals can dial calls by using device IDs.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **Alarm Access** to access the interface.

The screenshot shows the 'Server Settings' configuration page. At the top, there is an 'Enable' toggle switch which is turned on (green). Below it, the 'Registration Status' is 'Registered'. The 'Server Type' is set to 'ipv4' with a radio button. The form contains several input fields: '*IP' with the value '10.6.122.30', '*Server Port' with '5065', '*Registration Password' (masked with a lock icon), '*Device ID' with '220', '*Device Location' with 'Main Station 3', and '*Registration Period' with '10' and a unit of 'Minute(s)'. A red 'Save' button is at the bottom.

Figure 4-7 Server Settings

2. Check **Enable**.

3. Set server type as **IPv4** or **Domain Name**, then enter the server's IP or domain address.

4. Set **Server Port**, **Registration Password**, **Device ID**, **Device Location**, and **Registration Period**.

Note

The server can be main station or TS sever. If the server is main station, the port should be 5066. If the server is TS, the port should be 5065.

5. Click **Save** to complete configuration.

4.8.6 Storage Settings

TF Card Management

View TF card capacity information and format TF card.

Steps

1. Insert the TF card into the device.
2. Click **System and Maintenance** → **System Configuration** → **Storage Management** → **TF Card** .
3. View the current status and capacity of the TF card.
4. **Optional:** Click **Format** to format the current TF card. All content on the TF card will be erased after formatting.
5. Set storage quota including recording quota, audio quota, picture quota, and material quota.
6. Click **Save**.

Set Internal Storage

View internal storage capacity and format internal storage.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Storage Management** → **Internal Storage** .
2. View the current status and capacity of the internal storage.
3. **Optional:** Click **Format** to format the internal storage. All content on the internal storage will be erased after formatting.
4. Set storage quota including recording quota, audio quota, picture quota, and material quota.
5. Click **Save**.

4.8.7 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

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

Stream Type Main Stream

Video Type ☒ Video Stream ☐ Video&Audio

Resolution 1280*720 ▼

Bit Rate Type ☐ Constant ☒ Variable

Video Quality Medium ▼

Frame Rate 25 fps ▼

* Max. Bitrate 256 Kbps

Video Encoding H.264

* I Frame Interval 50 ⬆️ ⬆️

Save

Figure 4-8 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** .

Audio Encoding: G.711ulaw

Input Volume: 1

Output Volume: 0

Speak Volume: 1

Save

Figure 4-9 Audio Settings Page

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

4.8.8 Alarm Settings

Set alarm input and output's parameters.

Set Alarm Input Parameters

Click **System and Maintenance** → **System Configuration** → **Event** → **Alarm Input** .
Set parameters and click **Save**.

No.

Select **1** or **2** as the alarm input to configure.

Alarm Type

Select **Remain Open** or **Remain Closed** as the alarm input type.

Alarm Name

Create a name for the alarm input device.

Set Alarm Output Parameters

Click **System and Maintenance** → **System Configuration** → **Event** → **Alarm Output** .
Set parameters and click **Save**.

No.

Select **1** or **2** as the alarm output to configure.

Alarm Name

Create a name for the alarm output device.

Alarm Duration

Continuous Alarm

If the alarm output is triggered, an alarm will be triggered continuously.

Custom Alarm Duration

If the alarm output is triggered, the alarm will be triggered for the configured duration.

4.8.9 Event Task Settings

When the configured event is triggered, the linked action will be played according to the configured linkage relationship.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Event** → **Event Task** to enter the settings page.

+ Add

Linked Alarm Task (New)

Basic Information

*Task Name

Linked Alarm Task (New)

Task Type

Device Event

Fire Input Alarm

Alarm Output Settings

Link Alarm Output

Broadcast Settings

Broadcast Linkage

Linkage Source

+ Add

Delete

	id	Name	Operation

No data.

Broadcast Ratings

0

Broadcast Audio

Audio File

Speech Synthesis

Select Audio (0/1)

+ Add

Delete

	Name	Duration	Operation

No data.

Select Terminal

+ Add

Delete

	id	Name	Operation

No data.

Play Mode

Play Once

Loop

Save

Figure 4-10 Linkage Settings

- Click + .
- Set task name and task type. Select the linkage type as **Event Linkage**, **Card Linkage** or **Link Employee ID**.
 - Select **Task Type** as **Device Event**, you can select device event from the drop-down list.
 - Select **Task Type** as **Alarm Input Event**, you can select alarm input event from the drop-down list. And also, you should select an linkage source.
- Set linked alarm output action.
 - Enable **Link Alarm Output**.
 - Check the linked alarm output. The checked alarm output will perform the action.
- Set broadcast linkage. The linked broadcast audio will be played.
 - Enable **Broadcast Linkage** and set the parameters.

Broadcast Rating (Priority)

Set the priority of the broadcast.

Broadcast Audio

Audio File

If you select **Audio File** as **Broadcast Audio**, you can click **Add** and select the audio file from the list. You can add the audio file by clicking **Add Material**. For details, see [**Add Broadcast Materials**](#).

Speech Synthesis

Enter the content in the **Audio Content** and select the **Male** or **Female** as the audio. The content will be played in the broadcast.

Select Terminal

Click **Add** and check terminals that need to broadcast.

Play Mode

Select play mode as **Play Once** or **Loop**.

Play Once

The broadcast will be played only once.

Loop

The broadcast will be played on a loop.

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

4.8.10 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.

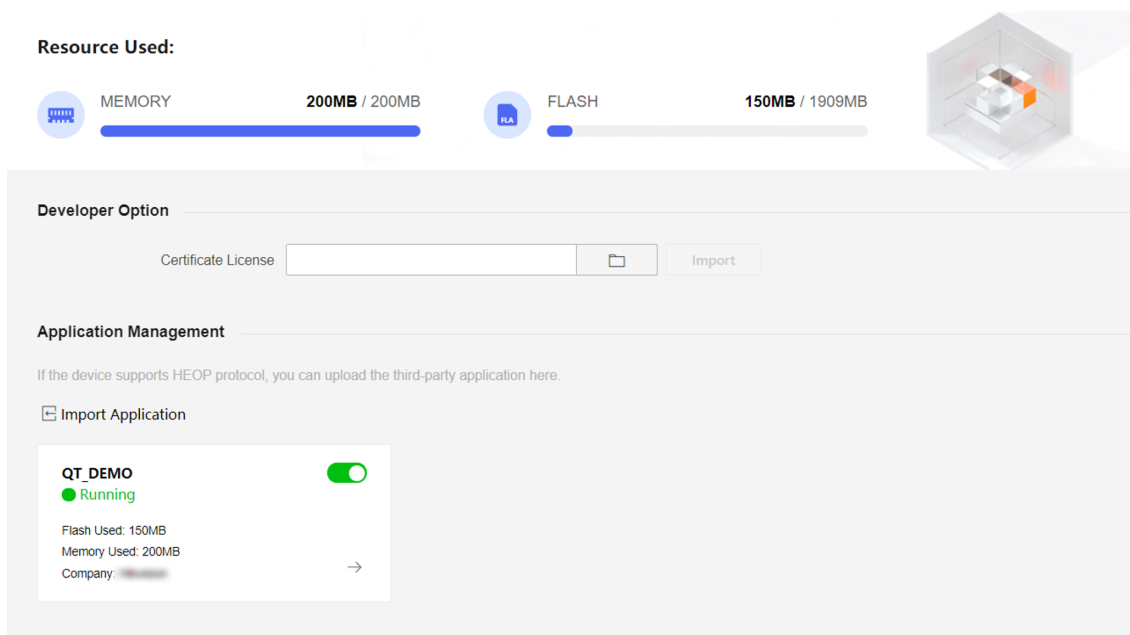


Figure 4-11 Open Platform

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.

4.8.11 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.

4.8.12 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**.

4.8.13 Test Protocol via PC Web

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

Go to **System and Maintenance** → **Maintenance** → **Device Debugging** → **Protocol Testing**.

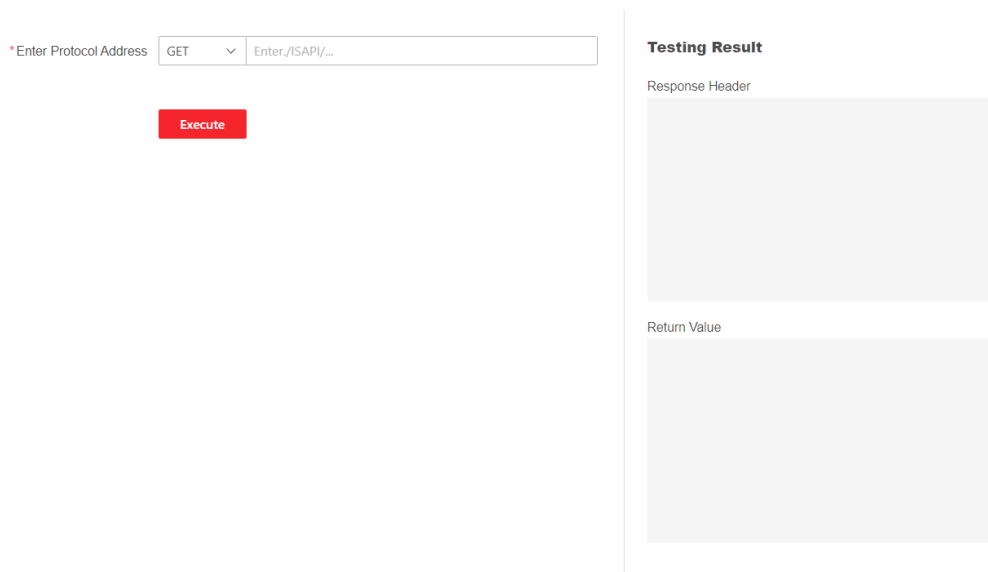


Figure 4-12 Protocol Testing

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

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

4.8.14 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.
4. **Optional:** Click **Network Service**, and set the network service information. The log will be uploaded to the configured service.

Log Upload Server

Enable **Log Upload Server** and set other parameters.

Encrypt Transmission

Enable the function and the log will be transmitted in encryption mode.

Log Server Address

Enter the log server address. The log will be transmitted to this server.

Log Server Port

Enter the log server port. The log will be transmitted to the server in this port.

4.8.15 Certificate Management

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



Note

The function is only supported by certain device models.

Security Management

Set security level when login the PC web.

Go to **System and Maintenance** → **Safe** → **Security Service** .

Security Mode

High security level when logging in and verify user information.

Compatible Mode

Compatible with old user verification method.

Click **Save**.

Install 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

Create a self-signed certificate.

Steps

1. Go to **Safe → Certificate Management**.
2. In the **HTTPS Certificate** and **SYSLOG Certificate** areas, select key and certificate from local PC.
3. Click **Import**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Safe → Certificate Management**.
2. In the **Import CA Certificate** in **SYSLOG Certificate** area, create an ID.



Note

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

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

Security Settings

To enhance network security, you can set IP address filtering function.

IP Address Filter

The device supports setting both a blocked IP address list and an allowed IP address list for communication. The device will not communicate with IP addresses in the block list. If an allow list is added, the device only communicates with IP addresses in the allowed list.

Enter the device address in the browser, after logging in, click **Maintenance & Security → Security → IP Address Filter** to access the configuration interface.

Slide the **Enable** switch. Select **Block List** or **Allow List**, click **Add**, enter the IP address, and click **OK**. Click **Save**.

4.9 Help

4.9.1 Open Source Software Licenses

You can view open source software licenses.

Click  → **Open Source Software Statement** on the upper-right corner to view the licenses.

4.9.2 View Online Help Document

You can view the help document for Web configuration.

Click  → **Online Document** on the upper right of the Web page to view the document.

4.10 Logout

Log out the account.

Click **admin** → **Logout** → **OK** to logout.

Chapter 5 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

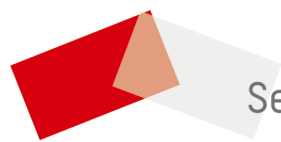
Click/tap the link to view the client software's user manual.

<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