

The HIKVISION logo is displayed on a red horizontal bar with a white diagonal stripe on the left side. The text "HIKVISION" is written in a white, italicized, sans-serif font.

HIKVISION

Video Intercom Main Station

Configuration Guide

Legal Information

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 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 INSPECTION, 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 MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.




Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Symbol Conventions

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

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

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.



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



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

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

Contents

1 Appearance	1
2 Terminal Description	4
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 Wall Mounting	9
3.4 Table Mounting	10
4 Local Operation	11
4.1 Activate the Device	11
4.2 Basic Settings	11
4.2.1 Local Network Parameters	11
4.2.2 Linked Device Management	12
4.2.3 Set Device No.	14
4.2.4 Add Camera	15
4.3 User Management	16
4.4 Synchronize Time	17
4.5 Call Settings	18
4.6 Restore Main Station	19
4.7 Upgrade	20
4.8 Maintenance	21

4.9 Device Information	23
5 Remote Configuration via Web	24
5.1 Activate Device via Web	24
5.2 Device Management	24
5.3 Parameters Settings	26
5.3.1 System Settings	26
5.3.2 Network Settings	29
5.3.3 Video & Audio Settings	31
5.3.4 Intercom Settings	32
5.3.5 Grab Bag	33
5.3.6 The Third-Party APP Settings	33
6 Configuration via Client Software	35
6.1 Edit Network Parameters	35
6.2 Add Device	35
6.2.1 Add Online Device	35
6.2.2 Add Device by IP Address	36
6.2.3 Add Device by IP Segment	36
6.3 Remote Configuration	37
6.4 Device Management	37
6.5 Organization Management	37
6.5.1 Add Organization	37
6.5.2 Modify and Delete Organization	38
6.6 Video Intercom Settings	38
6.6.1 Receive Call from Door Station	38

6.6.2 Live View via Door Station	39
6.6.3 Release Notice	39
6.6.4 Search Video Intercom Information	40
A. Communication Matrix and Device Command	42

1 Appearance

Front Panel

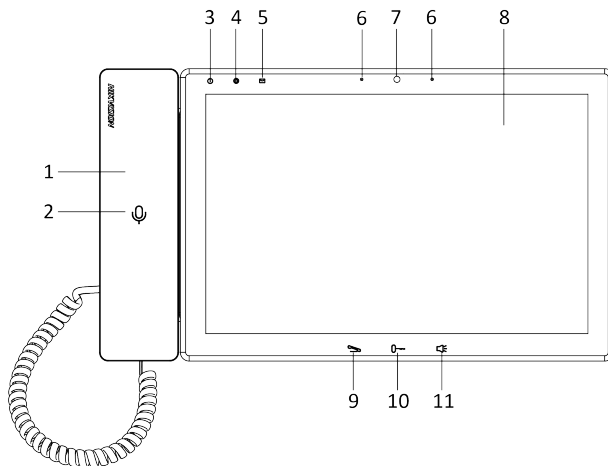


Figure 1-1 Front Panel

Table 1-1 Description

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

Note

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

Top Panel and Rear Panel

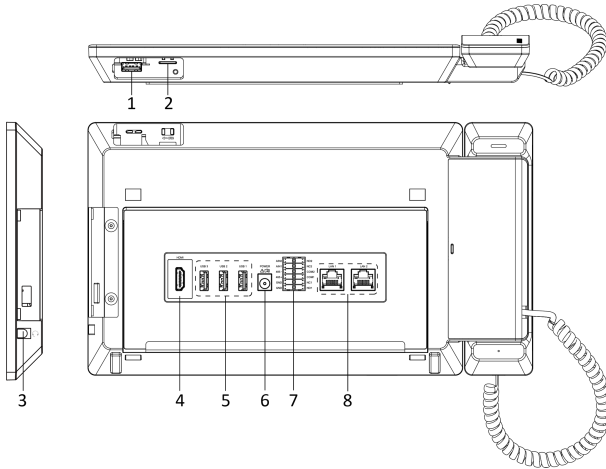


Figure 1-2 Top Panel and Rear Panel

Table 1-2 Description

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

Speaker(Optional)

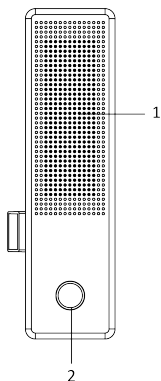


Figure 1-3 Speaker
Table 1-3 Description

Description	No.	Description
Speaker	2	Fingerprint Module

2 Terminal Description

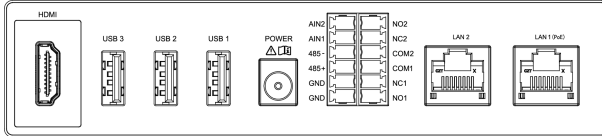



Figure 2-1 Terminal Description
Table 2-1 Terminal Description

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

Video Intercom Main Station Configuration Guide

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

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.

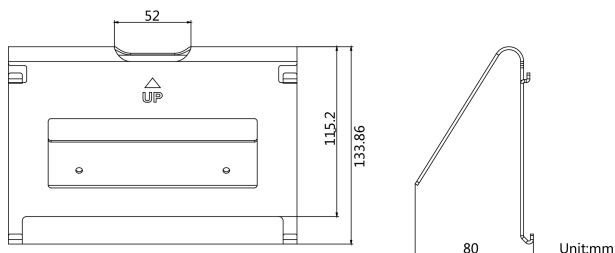


Figure 3-1 Table Bracket

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. Loosen 2 screws on the rear panel of the device.

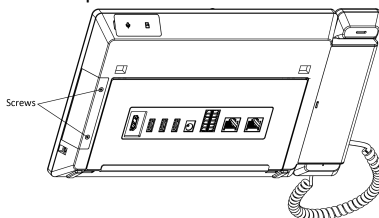


Figure 3-2 Loosen the screws

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

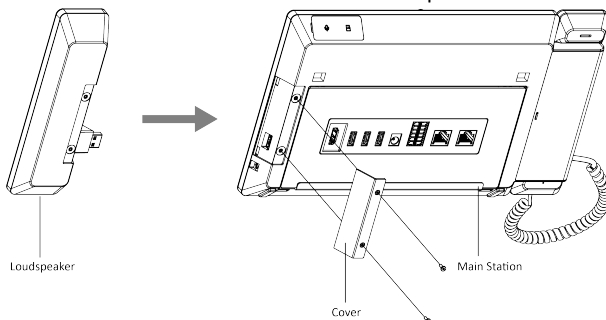


Figure 3-3 Install the Speaker

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

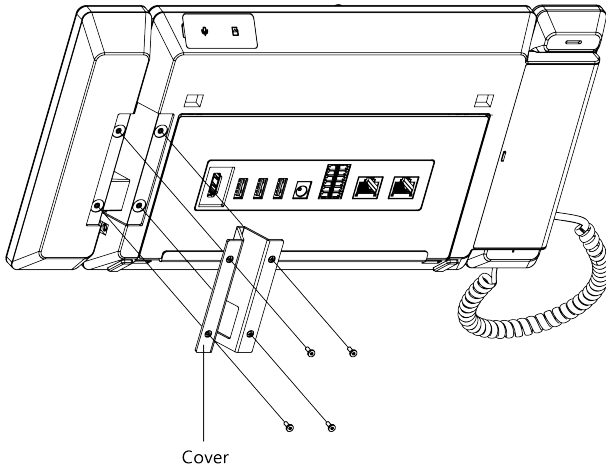


Figure 3-4 Secure the Speaker

Note

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

3.2.2 Install Goose Neck Microphone

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

Steps

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

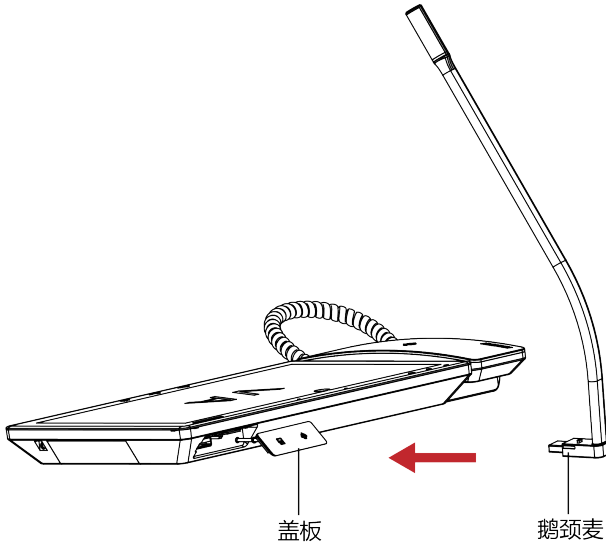


Figure 3-5 Install the Goose Neck Microphone

3.3 Wall Mounting

Before You Start

Note

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

Steps

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

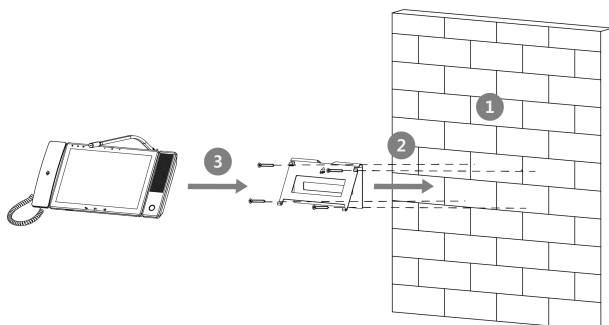


Figure 3-6 Wall Mounting

3.4 Table Mounting

Steps

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

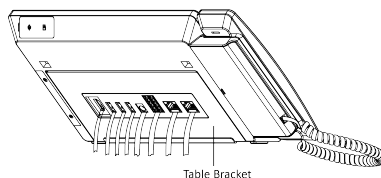


Figure 3-7 Smooth the Cable

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

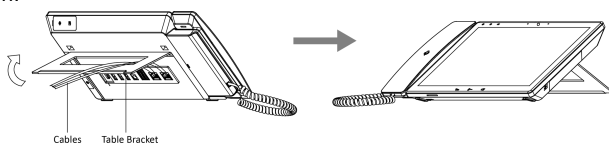


Figure 3-8 Adjust the Table Bracket

Note

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

4 Local Operation

4.1 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.

4.2 Basic Settings

4.2.1 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.

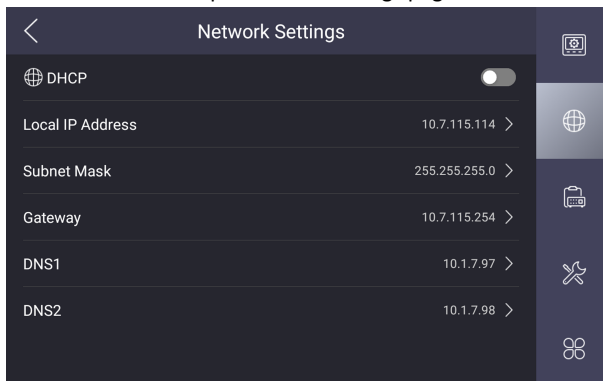


Figure 4-1 Network Settings

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.

4.2.2 Linked Device Management


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

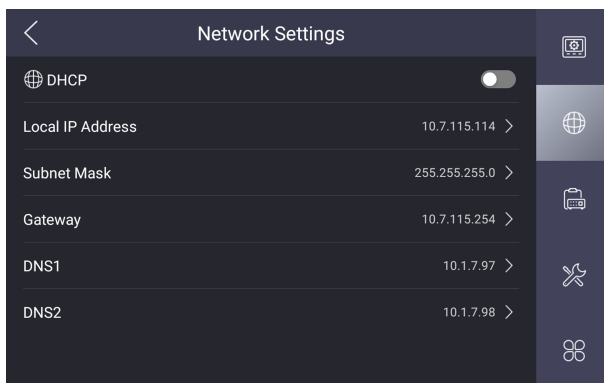


Figure 4-2 Device Management

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

Example

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

5. Tap + to link the device.

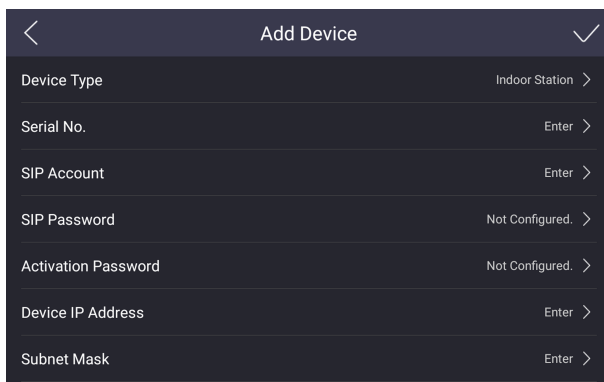



Figure 4-3 Add Linked Device

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

4.2.3 Set Device No.

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

Steps

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

Note

Default admin password is the activation password.

2. Tap  to enter the Main Station Settings page.

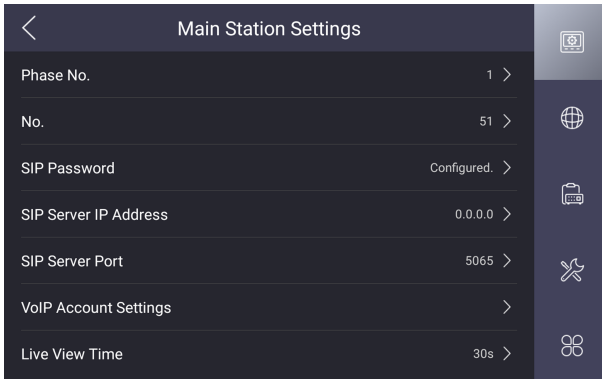



Figure 4-4 Device Settings

3. Edit the **Phase No.** and **No.** of the device.
4. Set the SIP server parameters. (Including SIP password, SIP server IP address, SIP server port and VoIP account settings.)
5. Set the **Live View Time**.

4.2.4 Add Camera


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

Steps

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

Note

Default admin password is the activation password.

2. Tap  to enter the device management page.

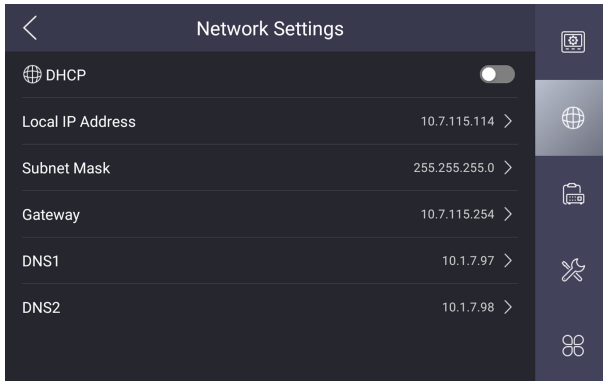


Figure 4-5 Device Management

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

Example

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

5. Tap + to link the device.

Add Device	
Device Type	Monitoring point >
Name	Enter >
Protocol Type	Hikvision Private Protocol >
IP Address	Enter >
Port No.	554 >
Channel	1 >
User Name	admin >

Figure 4-6 Add Camera

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


4.3 User Management

You can view the information of the user and add the fingerprints for admin.

Before You Start

Connect the fingerprint recognition module to the device first.

Steps

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

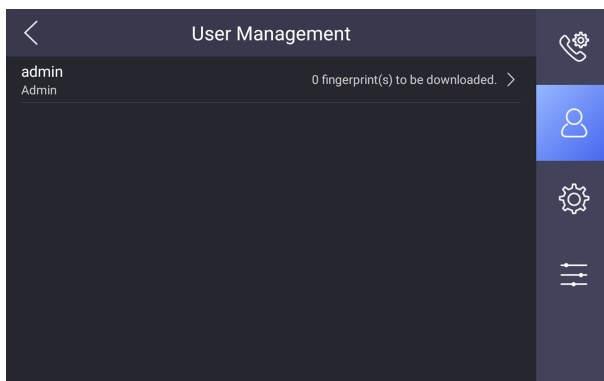


Figure 4-7 User Management

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

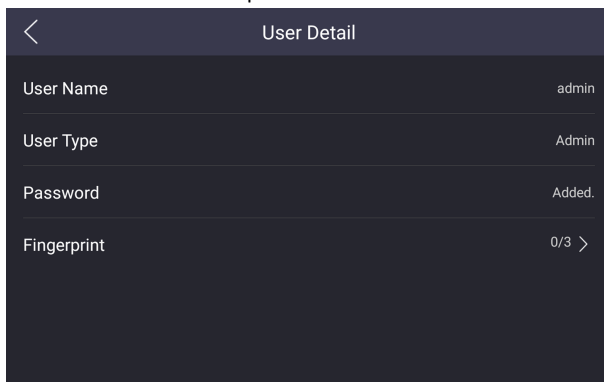


Figure 4-8 Details

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


 **Note**

Up to 3 fingerprints can be added.

4.4 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.

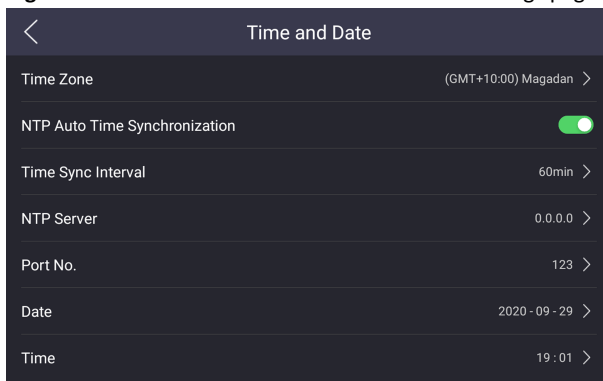


Figure 4-9 Time and Date

2. Select the **Time Zone**.
3. Synchronize time.
 - Configure the **Date** and **Time** manually.
 - Slide the slider to enable the **NTP Auto Time Synchronization** function.
Set the synchronizing interval, enter the IP address of NTP server and port No.

4.5 Call Settings

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

Steps

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

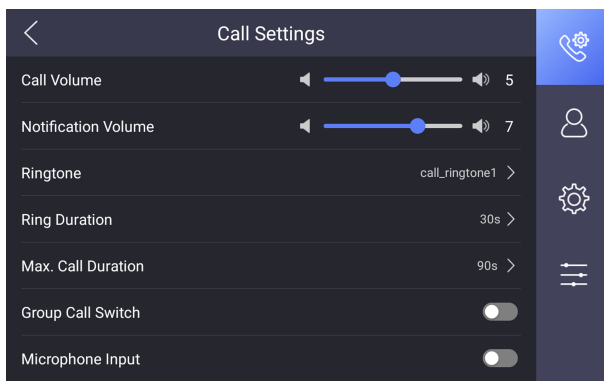


Figure 4-10 Call Settings

2. Set corresponding parameters.

Ringtone

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

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

Volume Settings

Adjust the call volume and notification volume.

Max. Call Duration

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

Group Call Switch


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

Microphone Input

Slide to enable the microphone input. You can use the goose neck microphone to communicate.


4.6 Restore Main Station

Steps

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

 **Note**

Default admin password is the activation password.

2. Tap  to enter the system maintenance page.

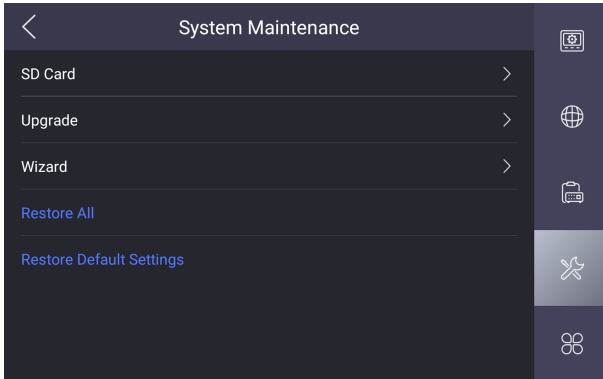


Figure 4-11 Maintenance


3. Tap **Restore Default Settings** to restore the default settings and reboot the system.
4. Tap **Restore All** to restore all parameters and reboot the system.

4.7 Upgrade

Before You Start

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

Steps

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

 **Note**

Default admin password is the activation password.

2. Tap  to enter the system maintenance page.

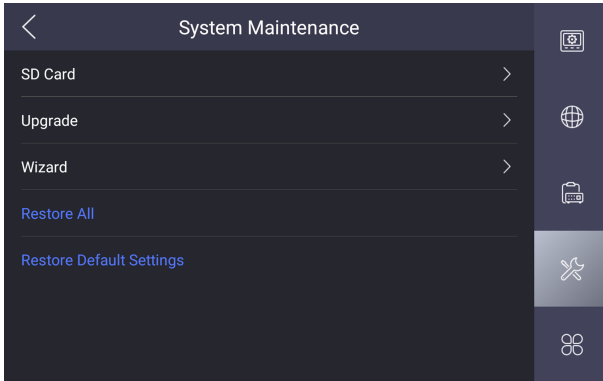



Figure 4-12 Maintenance

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

4.8 Maintenance

SD Card

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

Tap  to enter the maintenance page.

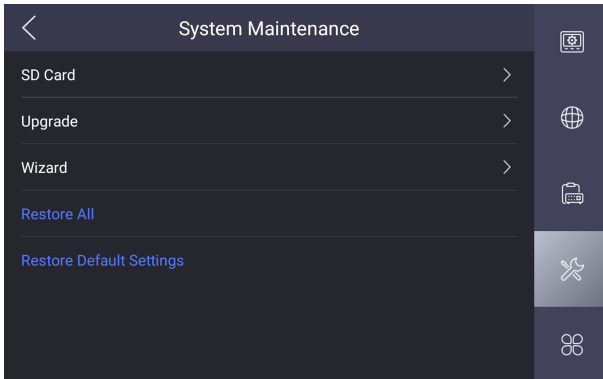




Figure 4-13 Maintenance

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

Wizard

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

Tap  to enter the maintenance page.

Tap **Wizard** to configure the system quickly.

Permission Verification

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

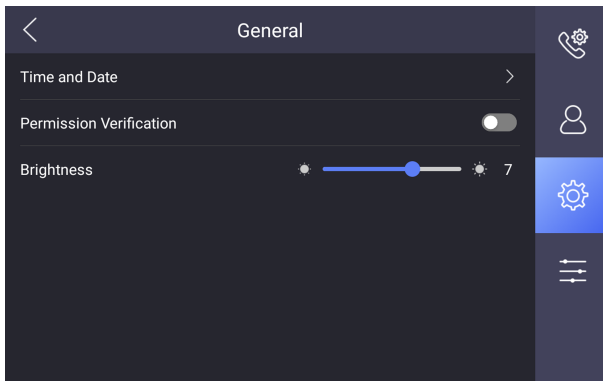



Figure 4-14 General Settings

Slide to enable the permission verification function. You should verify via password or fingerprints to awake the device.

Brightness Adjustment

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

Reboot

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

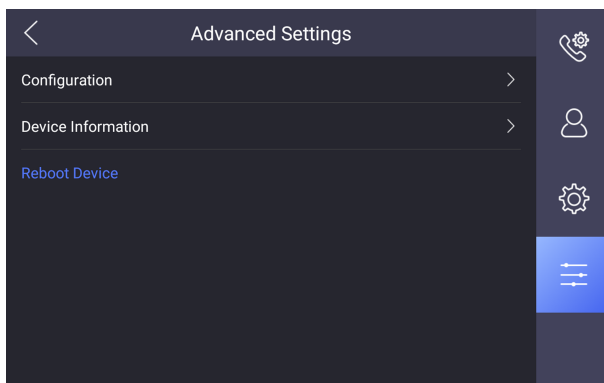


Figure 4-15 Advanced Settings

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


 **Note**

Please do not cut the power during rebooting.

4.9 Device Information

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

Steps

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

5 Remote Configuration via Web

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

This is the start of your concept.

5.1 Activate Device via Web

You are required to activate the device first by setting a strong password for it before you can use the device.

Default parameters of the door station are as follows:

- Default IP Address: 192.0.0.65.
- Default Port No.: 8000.
- Default User Name: admin

Steps

1. Power on the device, and connect the device to the network.
2. Enter the IP address into the address bar of the web browser, and click **Enter** to enter the activation page.

Note

The computer and the device should belong to the same subnet.

3. Create and enter a password into the password field.
4. Confirm the password.
5. Click **OK** to activate the device.

5.2 Device Management

You can manage and view the linked device and camera on the page.

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

Add Linked Device

- Click **Device List** → **Add** to add the indoor station, outdoor station, door station or main station. Enter the parameters and click **OK** to add.
- Click **Device List** → **Import** . Enter the information of the device in the template to import devices in batch.

Export Linked Device Information

Click **Device List**, select the linked device, and click **Export** to export the information to the PC.

Delete Linked Device

Click **Device List**, select the linked device, and click **Delete** to delete the linked device.

Upgrade Linked Device

Click **Device List** → **Upload Updating Package** , click **Browse** to select the upgrade file to upload.

Click **Device List**, select the linked device, click **Timing Upgrade**, slide **Enable Upgrading Device Automatically**, set **Start Time** and **End Time**, and the device will upgrade in the specific period.

Click **Device List**, select the device, click **Upgrade Now**, and the device will upgrade now.




Note

You need to upload updating package before upgrading.

View Linked Device Upgrading Status

Click **Device List** → **Upgrading** , you can view the current linked devices version.

View Linked Device Information

Click **Device List**, select **Status** and **Device Type**, the device information will be displayed the page, including device No., IP Address, Serial No., model, current version, room No., user name, network status information. You can click , ,  to edit, set and delete the linked device.




Add Camera

Click **Camera** → **Add**, enter the corresponding camera parameters, and click **OK** to add the camera.

Delete Camera

Click **Device List**, select the camera, and click **Delete** to delete the camera.

View Camera Information

Click **Camera** to view the camera information, including camera name, No., IP Address, channel No., port No., and protocol information. You can click , , , to edit, set and delete the camera.

5.3 Parameters Settings

Click **Configuration** to set the parameters of the device.

Remote configuration in iVMS-4200 and Batch Configuration Tool is the same as that in Web. Here takes the configuration in web for example.

Note

Run the browser, click  → **Internet Options** → **Security** to disable the Protected Mode.

5.3.1 System Settings

Follow the instructions below to configure the system settings, include System Settings, Maintenance, Security, and User Management, etc.

Click **System** to enter the settings page.

Basic Information

Click **System Settings** → **Basic Information** to enter the settings page. On the page, you can edit **Device Name** and **Device No.**, and select **Language** according to your needs.

Click **Save** to enable the settings.

Time Settings

Click **System Settings** → **Time Settings** to enter the settings page. Select the **Time Zone** of your location from the drop-down list.

- Enable **NTP**, set the **Server Address**, **NTP Port** and **Interval**.
- Enable **Manual Time Sync.**, set the time manually or check the **Sync. with computer time**.

Click **Save** to enable the settings.

View Source Software License

Click **System Settings** → **About** , and click **View License** to view the source software license.

Maintenance

Click **Maintenance** → **Upgrade & Maintenance** to enter the settings page.

- **Reboot**: Click **Reboot** to reboot the device.
- **Restore**
 - Click **Default** to reset the parameters to the default settings, except the IP parameters and user information.

Restore All

Click **Restore All** to restore all parameters to default settings.

- **Export parameters**:
 1. Click **Export** to pop up the dialog box.
 2. Set and confirm the encryption password.
 3. Click **OK** to export parameters.
- **Import Config. File**:

1. Click to select the configuration file.
 2. Click **Import** and enter the encryption password to import.
- Upgrade: Click **Browse** to select the upgrade file.

 **Note**

The upgrading process will last 1 to 10 minutes, do not power off during the upgrading. The device reboots automatically after upgrading.

- Ping Network : You can ping network to check if there is IP conflict. Enter the IP address, and click **Ping Network**.

Search Log Query

Set **Majoy Type**, **Minor Type**, **Start Time**, **End Time**, and click **Search**.

Security Service


Click **Security** to enter the settings page.

- Enable SSH: When the device needs to be debugged in remote, you can slide **Enable SSH**. If the device needn't to be debugged in remote, you should disable it to improve the device security.
- Enable Remote Stop: When the Android system needs to be debugged in remote, you can slide **Enable Remote Stop**. If the Android system needn't to be debugged in remote, you should disable it to improve the device security.

After Settings, click **Save** to enable the settings.

User Management

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

Click  to modify user password, and click **OK** to save the settings.

 **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.

5.3.2 Network Settings

TCP/IP Settings

TCP/IP settings must be properly configured before you operate the device over network. The device supports IPv4.

Steps

1. Click **Network** → **Basic Settings** → **TCP/IP** to enter the settings page.

DHCP

IPv4 Address: 10.7.115.22

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 10.7.115.254

Alarm Center IP: 0.0.0.0

Alarm Host Port: 0

DNS Server

Preferred DNS Server: 10.1.7.97

Alternate DNS Server: 10.1.7.98

Save

Figure 5-1 TCP/IP Settings

2. Configure the network parameters.
 - Check **DHCP**, the device will get the parameters automatically.
 - Set the **IPv4 Address**, **IPv4 Subnet Mask** and **IPv4 Default Gateway** manually.
3. Configure **Alarm Center IP** and **Alarm Host Port**.
4. Configure the DNS server.
5. Click **Save** to enable the settings.

Port Settings

Steps

1. Click **Configuration → Network → Basic Settings → Port** to enter the settings page.

HTTP Port	<input type="text" value="80"/>
RTSP Port	<input type="text" value="554"/>
HTTPS Port	<input type="text" value="443"/>
Server Port	<input type="text" value="8000"/>

Figure 5-2 Port Settings

2. Set the ports of the device.

HTTP Port

The default port number is 80, and it can be changed to any port No. which is not occupied.

RTSP Port

The default port number is 554 and it can be changed to any port No. ranges from 1 to 65535.

HTTPS Port

The HTTPS port is for visiting browser. It needs to be verified the certificate when visiting the browser.

Server Port

The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

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

SIP Setting

Steps

1. Click **Configuration → Network → Basic Settings → SIP** to enter the settings page.
2. Check **Enable VOIP Gateway**.
3. Configure the SIP parameters.

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

5.3.3 Video & Audio Settings

Video Parameters

Steps

1. Click **Configuration** → **Video/Audio** → **Video** to enter the settings page.
2. Select the **Stream Type**.
3. Configure the video parameters.

Video Type

Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.

Resolution

Select the resolution of the video output.

Bitrate Type

Select the bitrate type to constant or variable.

Video Quality

When bitrate type is selected as Variable, 6 levels of video quality are selectable.

Frame Rate

Set the frame rate. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate

Set the max. bitrate from 32 to 16384 Kbps. The higher value corresponds to the higher video quality, but the better bandwidth is required.

Video Encoding

The device supports H.264.

I Frame Interval

Set I Frame Interval from 1 to 400.

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

Audio Parameters

Steps

1. Click **Configuration** → **Video/Audio** → **Audio** to enter the settings page.
2. Select **Stream Type** and **Audio Encoding**.
3. Adjust the **Input Volume**, **Output Volume** and **Speak Volume**.

Note

Available range of volume: 0 to 10.

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

5.3.4 Intercom Settings

Device ID Settings

Set the device ID to manage and communicate with devices.

Steps

1. Click **Configuration** → **Intercom** → **Device ID Settings** to enter the settings page.
2. Select **Device Type**, **Period No.** and **No.**
3. Click **Save** to enable the settings.

Session Settings

You can set session to establish the communication between main station with indoor station, outdoor station, door station or video intercom server.

1. Click **Configuration** → **Intercom** → **Session Settings** .
2. Set **Registration Password**, **Video Intercom Server IP** and **Private SIP Server Port**.
 - **Register Number**: The register number of the main station. It has been set by default.
 - **Registration Password**: The registration password of the communicated indoor station, outdoor station, and door station.
 - **Video Intercom Server IP**: The IP address of video intercom server.
 - **Private SIP Server Port**: The port of private SIP server.
3. Click **Save**.

Time Duration Settings

Set the Max. call duration, ring duration, and live view duration.

Go to **Configuration → Intercom → Time Parameters** .

Drag the block to set the Max. call duration, ring duration, and live view duration. Click **Save**.

Note

The Max. call duration range is 90 s to 120 s.

5.3.5 Grab Bag

When the device is connected to the network, you can grab the data file and export the grab data file.


Click **Configuration → Grab Bag** .

Click **Start Capture**. Wait for the required time duration and click **Stop**. The system will export the grab file.

5.3.6 The Third-Party APP Settings

You can upload the third-party application to the device.

Steps

1. Click **Configuration → Open Platform** .
2. If it is the first time to use the function, you should read the Disclaimer and make sure that the application you want to install fit the following conditions.
 - Each application has its own exclusive name.
 - The FLASH memory space that the application takes up is less than the available FLASH memory space of the device.
 - The memory and computing power of the application is less than that available memory and computing power of the device.
3. Click  and select the imported application package from your local computer.
4. Click **Import** to complete the installation.

The installed applications and their related information are displayed in Application List, such as application name, operation, version, memory used, flash used, company, and status.

5. Set other functions.



Enable or disable the application.



Delete the application.

6 Configuration via Client Software

6.1 Edit Network Parameters

To operate and configure the device via LAN (Local Area Network), you need connect the device in the same subnet with your PC. You can edit network parameters via **iVMS-4200** client software.

Steps

1. Select an online activated device and click the **Modify Netinfo**.
2. Edit the device IP address and gateway address to the same subnet with your computer.
3. Enter the password and click **OK** to save the network parameters modification.

Note

- The default port No. is 8000.
 - The default IP address of the door station is 192.0.0.65.
 - After editing the network parameters of device, you should add the devices to the device list again.
-

6.2 Add Device

You should add device to the software so as to configure the device remotely.

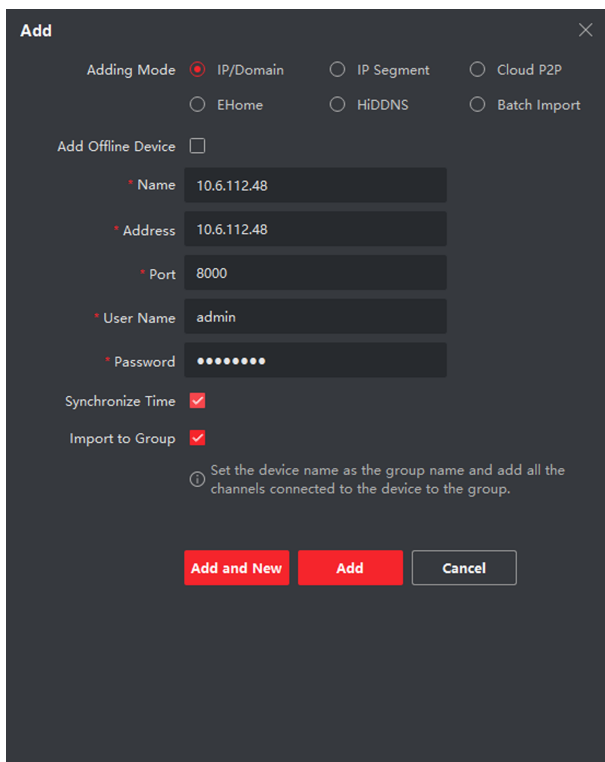
6.2.1 Add Online Device

Before You Start

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

Steps

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



Add ✕

Adding Mode IP/Domain IP Segment Cloud P2P
 EHome HiDDNS Batch Import

Add Offline Device

* Name 10.6.112.48

* Address 10.6.112.48

* Port 8000

* User Name admin

* Password ●●●●●●

Synchronize Time

Import to Group

ⓘ Set the device name as the group name and add all the channels connected to the device to the group.

Add and New **Add** Cancel

Figure 6-1 Add to the Client

6.2.2 Add Device by IP Address

Steps

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

6.2.3 Add Device by IP Segment

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

Steps

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

6.3 Remote Configuration


Select the device, click  to configure the parameters remotely.

6.4 Device Management

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

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

6.5 Organization Management

On the main page of the Client Software, click  **PersonalManagement** to enter the configuration page.

6.5.1 Add Organization


Steps

1. In the organization list on the left, click **+Add**.
2. Enter the **Organization Name** as desired.
3. Click **OK** to save the adding.
4. **Optional:** You can add multiple levels of organizations according to the actual needs.
 - 1) You can add multiple levels of organizations according to the actual needs.
 - 2) Then the added organization will be the sub-organization of the upper-level organization.

 **Note**

Up to 10 levels of organizations can be created.

6.5.2 Modify and Delete Organization

You can select the added organization and click  to modify its name.

You can select an organization, and click **X** button to delete it.

 **Note**

- The lower-level organizations will be deleted as well if you delete an organization.
 - Make sure there is no person added under the organization, or the organization cannot be deleted.
-

6.6 Video Intercom Settings

The Video Intercom Management module provides the function of video intercom, checking call logs and managing notice via the iVMS-4200 Client Software.

 **Note**

For the user with access control module permissions, the user can enter the Access Control module and manage video intercom and search information.




You should add the device to the software and configure the person to link the device in Access Control module before your configuration remotely.

On the main page, click  **AccessControlInfo** → **Video Intercom** → **Video Intercom** on the left bar to enter the Video Intercom page.

6.6.1 Receive Call from Door Station

Steps

1. Select the client software in the device page to start calling the **iVMS-4200 Client Software** and an incoming call dialog will pop up in the client software.
2. Click **Answer** to answer the call. Or click **Hang Up** to decline the call.
3. After you answer the call, you will enter the In Call window.

- Click  to adjust the volume of the loudspeaker.
- Click  to adjust the volume of the microphone.
- Click **Hang Up** to hang up the dialog.
- Click  to open the door remotely.

Note

- One video intercom device can only connect with one client software.
 - The maximum ring duration can be set from 15s to 60s via the Remote Configuration of the video intercom device.
 - The maximum speaking duration between indoor station and iVMS-4200 can be set from 120s to 600s via the Remote Configuration of indoor station.
 - The maximum speaking duration between door station and iVMS-4200 can be set from 90s to 120s via the Remote Configuration of door station.
-

6.6.2 Live View via Door Station

Steps

1. On the main page of the client software, click **Main View** to enter the Live View page.
2. In the left list of the window, double-click the device IP or click the play icon to live view.
3. **Optional:** On the Live View page, control-click and select **Capture** to get the picture of the live view.

6.6.3 Release Notice

You can create different types of notices and send them to the residents. Four notice types are available, including Advertising, Property, Alarm and Notice Information.

Before You Start

Make sure the person has been added to the client.

Steps

1. On the video intercom settings page, click **Notice** to enter the page.
2. Click **+Add** to pop up the adding dialog box.
3. Select the person according to your needs.

4. Edit the **Subject, Type** and **Information**.
5. Click **View** to select the picture.
6. Click **Send**.

Note

- Up to 63 characters are allowed in the Subject field.
 - Up to 6 pictures in the JPGE format can be added to one notice. And the maximum size of one picture is 512KB.
 - Up to 1023 characters are allowed in the Information field.
-

6.6.4 Search Video Intercom Information

Search Call Logs

Steps

1. On the Video Intercom page, click **Call Log** to enter the page.

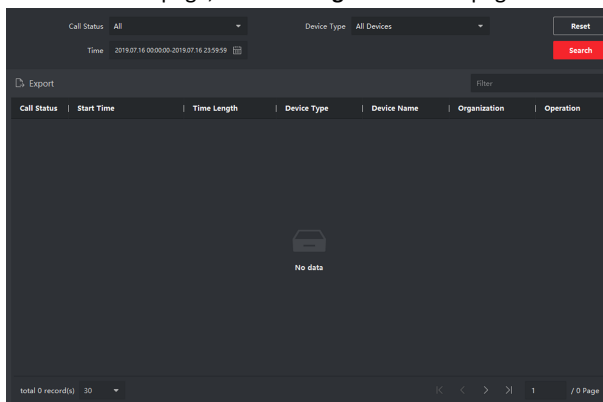


Figure 6-2 Search Call Logs

2. Set the search conditions, including call status, device type, start time and end time.

Call Status

Click **∨** to unfold the drop-down list and select the call status as **Dialed**, **Received** or **Missed**. Or select **All** to search logs with all statuses.

Device Type

Click **▼** to unfold the drop-down list and select the device type as **Indoor Station, Door Station, Outer Door Station** or **Analog Indoor Station**. Or select **All Devices** to search logs with all device types.

Start Time/End Time

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

Reset the Settings Click **Reset** to reset all the configured search conditions.

3. Click **Search** and all the matched call logs will display on this page.
4. **Optional:** Check the detailed information of searched call logs, such as call status, ring/speaking duration, device name, resident organization, etc.
5. **Optional:** Input keywords in the Search field to filter the desired log.
6. **Optional:** Click **Export** to export the call logs to your PC.

Search Notice

Steps

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

Type

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

Start Time/End Time

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

Reset the Settings Click **Reset** to reset all the configured search conditions.

3. Click **Search** and the matched notice will display on this page.
4. **Optional:** Click **Export** to export the notices to your PC.

A. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.

Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.



Figure A-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.

Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.



Figure A-2 Device Command

