Network Indoor Station

Configuration Guide

Legal Information

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 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 MANUAL AND THE APPLICABLE LAW, THE LATTER 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

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC Conditions

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

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

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

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

Industry Canada ICES-003 Compliance

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

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Contents

1 About this Manual 1

2 Local Operation 2

2.1 Quick Operation 2

2.2 Basic Settings 5

2.2.1 Set Indoor Station Network Parameters 6

2.2.2 Set Linked Device IP 7

2.2.3 Set Indoor Station No. 8

2.2.4 SIP Settings 8

2.2.5 Add Camera 9

2.2.6 Zone and Alarm Settings 9

2.3 Password Settings 12

2.3.1 Modify Admin Password 12

2.3.2 Modify Arm/Disarm Password 13

2.3.3 Modify Unlock/Duress Code 14

2.3.4 Modify SIP Password 14

2.4 Synchronize Time 15

2.5 Sound Settings 15

2.5.1 Call Settings 15

2.5.2 Volume Settings 17

2.6 Link to the Mobile Client 17

2.7 System Settings 17

2.7.1 General Settings 18

2.7.2 Maintenance 19
2.7.3 Preference 20
2.8 Device Information 20
2.9 Output Settings 21
3 Remote Operation via the client software 22
3.1 Activate Device Remotely 22
3.2 Device Management 22
3.2.1 Add Video Intercom Devices 23
3.2.2 Modify Network Information 25
3.3 System Configuration 26
3.4 Remote Configuration 26
3.4.1 System 26
3.4.2 Video Intercom 32
3.4.3 Network 40
3.5 Person Management 43
3.5.1 Organization Management 44
3.5.2 Person Management 45
A. Communication Matrix and Device Command 49

1 About this Manual

Get the manual and related software from or the official website (http://www.hikvision.com).

Product	Model
Network Indoor Station	DS-KH6320-TE1(B)/DS-KH6320-WTE1(B)/DS-KH6320-LE1(B)/DS-KH6350-TE1/DS-KH6350-TE1/DS-KH6360-TE1/DS-KH6360-WTE1

Scan the QR code to get the configuration guide for detailed information.

Scan the QR code to get the operation guide for detailed information.

2 Local Operation

2.1 Quick Operation

You can create a password for the device activation, and configure the device following the wizard.

Steps

1. Activate the device.

1) Power on the device. It will enter the activation page.

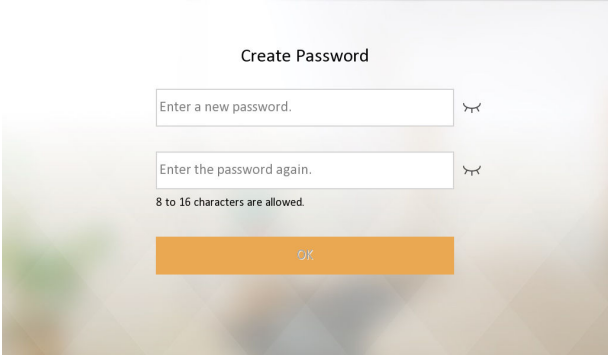

Figure 2-1 Activation Page

2) Create a password and confirm it.

Note

You can click to enable or disable password reveal.

3) Tap **OK** to activate the indoor 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.

After device activation, the wizard page will pop up.

2. Choose Language and tap **Next**. Or tap **Skip** to skip language settings.

Figure 2-2 Language Settings

3. Set password reset method. Or you can tap **Skip** to skip password reset method settings.
- If you need to change password via reserved email, you can enter an email address, and tap **Next**.
- If you need to change password via security questions, you can tap **Change to Security Questions** on the right corner. Select the security questions and enter the answers. Click **Next**.

4. Set network parameters and tap **Next**. Or you can tap **Skip** to skip network settings.
- Edit **Local IP**, **Subnet Mask** and **Gateway** parameters.
- Enable **DHCP**, the device will get network parameters automatically.

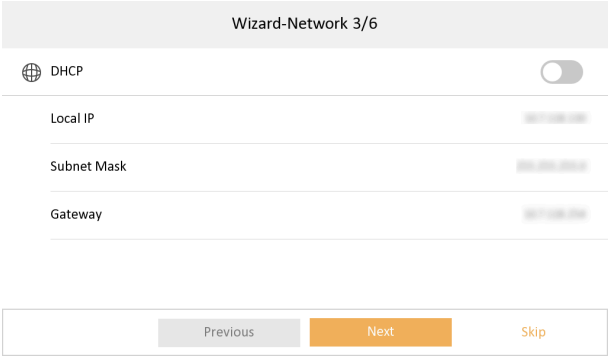

Figure 2-3 Network Parameters

5. Configure the indoor station.

- Select **Device Type** as **Indoor Station**.

  Set **Floor No.**, **Room No.** and **Registration Password**. Configure **Advanced Settings**.

  You can enable **Indoor Extension Settings** to add indoor extensions.
- Select **Device Type** as **Indoor Extension**.

  Set **No.**, **Room Name** and **Registration Password**.

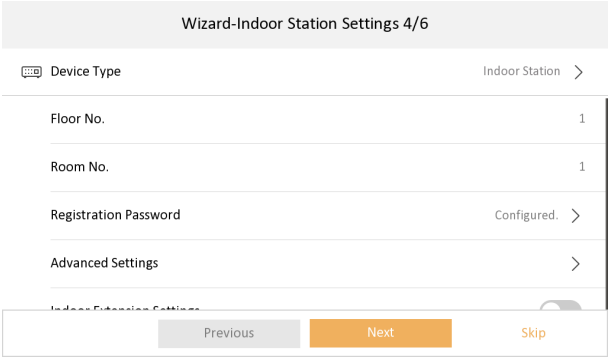

Figure 2-4 Indoor Station Settings

6. Configure the **Hik-Connect** service settings. Or you can tap **Skip** to skip service settings.

1) Enable **Hik-Connect** service.

2) Slide the slider to edit verification code or use the activation password by default.

3) Tap **Next**.

Note

The function of the device varies according to different models. Refers to the actual device for detailed information.

7. Link related devices and tap **Next**. If the device and the indoor station are in the same LAN, the device will be displayed in the list. Tap the device or enter the serial No. to link.

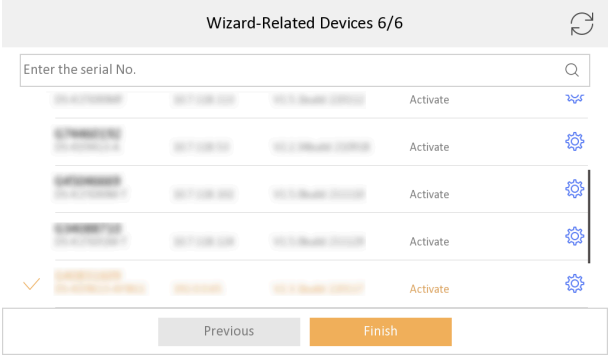

Figure 2-5 Related Device

1) Tap the door station in the list to link.

Note

If the door station is inactive, the system will pop up the dialog to activate the door station.

2) Tap ⚙ to pop up the Network Settings page.

3) Edit the network parameters of the door station manually or enable **DHCP** to get the network parameters automatically.

4) Tap **OK** to save the settings.

8. Tap **Finish** to save the settings.

2.2 Basic Settings

Basic settings is required before starting using the indoor station. It is necessary to set the indoor station network, room No., linked devices, device time display, and so on.

2.2.1 Set Indoor Station Network Parameters

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

Steps

Note

The default IP address of the indoor station is 192.0.0.64.

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

1. Tap **Settings** → → **Configuration** , and enter admin (activation) password.
2. Tap to enter the network settings page.

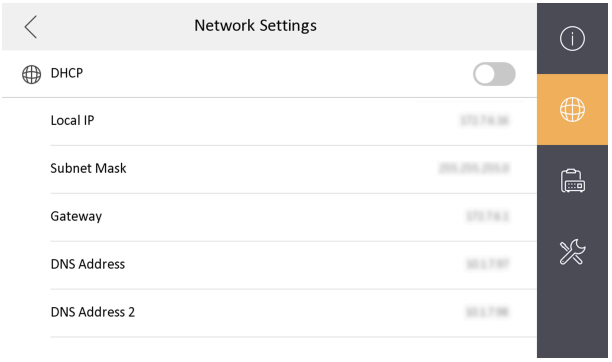

Figure 2-6 Network Settings

3. Set the network parameters.
   - Enable **DHCP**, and the system can assign an IP address of the indoor station automatically.
   - Disable the DHCP function, and set the IP address manually. You should set the device IP address, the gateway, the DNS address.

2.2.2 Set Linked Device IP

Linked network parameters refers to the network parameters of devices (like door station, doorphone, main station, center, etc.), to which the indoor station is linked. Linked devices for the indoor station refers to door station, center, main station, and doorphone.

With the private SIP protocol, intercom can be realized only when all these devices are in the same network segment with the indoor station.

With the standard SIP protocol, intercom can be realized when all these devices support the standard SIP protocol.

Steps

Note

- The doorphone does not support adding with the standard SIP protocol.
- Here take door station network settings as example.

1. Tap **Settings** → → **Configuration** , and enter admin (activation) password.
2. Tap to enter the device management page.
3. Tap **Indoor Extension** and select a connect indoor extension.
4. Tap **Main Door Station** to pop up the device information dialog.

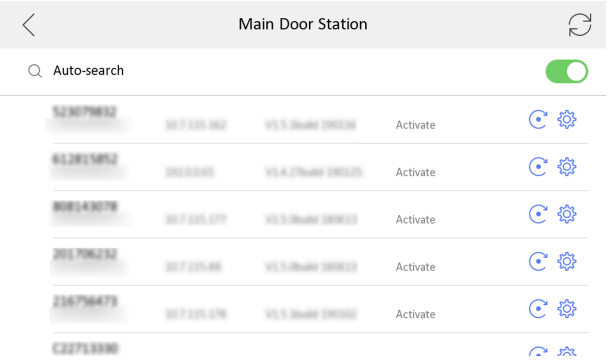

Figure 2-7 Device Information

Restore the door station via indoor station.

Tap to restore the parameters of the door station.

Modify the IP address of the linked door station.

Tap to edit the IP address of door station.

5. Select the device to link. Edit the network parameters.
6. Set the IP address for **SIP Server**, **Platform IP**, **Main Station** and **Main Doorphone**.

2.2.3 Set Indoor Station No.

Indoor station No. and the indoor extension No. are numbers, which can be dialed by other devices to call the indoor station and the indoor extension in an intercom system. The indoor station No., is composed of the floor No. and the room No.

The indoor extension No. Should be a numeric from 1 to 5.

Up to 5 indoor extensions can be set for 1 indoor station.

Steps

1. Tap **Settings** → → **Configuration** , and enter admin (activation) password.
2. Tap to enter the indoor station settings page.
3. Select **Indoor Station Type** from **Indoor Station** or **Indoor Extension** according to your actual needs.
   - Indoor Station: You can set the indoor station's room information, including the room name, community No., building No., Unit No., floor, and room No., the live view duration, the SIP register password, the SIP parameters, password and E-mail address.
   - Indoor Extension: You can set the indoor extension's room information, including the room name and the extension No., live view duration, the SIP register password, password and E-mail address..
4. Tap **Room Information** and set room name, community No., building No., unit No., floor No., and room No. according to your actual needs.

2.2.4 SIP Settings

Devices can communicate with each other via SIP protocol. You create set the SIP register password, enable standard SIP and set VIOP account.

Steps

1. Tap **Settings** → → **Configuration** , and enter admin (activation) password.
2. Tap **SIP Settings** in Local Information Page.
3. Set SIP registration password.

   1) Tap **Registration Password**.

2) Create a new SIP register registration password and confirm the password.

3) Tap **OK**.

4. Select **Stream Transmission Mode** as **Unit Broadcast** or **Group Broadcast**.

5. Optional: Enable standard SIP.

1) Enable **Enable Standard SIP**.

2) Tap **VOIP Account Settings** and configure the account information, including the user name, the phone number, the registered user name, the password, the domain, the port No., and the expiration date.

Note

Up to 32 characters are allowed in the user name.

2.2.5 Add Camera

Steps

1. Tap **Settings →** → **Configuration** , and enter admin (activation) password.

2. Tap to enter the device management page.

3. Tap **+** to pop up the dialog box.

4. Select a protocol to add the camera.

- Select **HIK Protocol** and you can add the camera depended on the **HIK protocol**.

  Enter the device name, IP address, user name and the password of the camera. Edit port No. and channel No.

  Exit the page to save the settings.
- Select **Open Network Video Interface** to add the camera.

  Enter the device name, IP address, user name and the password of the camera.

  Exit the page to save the settings.

2.2.6 Zone and Alarm Settings

Zone Settings

You can set the zone type, alarm type and delay time and other parameters of 8 zones.

Before You Start

Tap **Settings** → → **Shortcut Settings** , and enable **Alarm**.

Steps

Note

Arming status page and zone settings page are hidden by default. You should enable alarm function first.

1. Tap **Settings** → → **Zone Settings** to enter the zone settings page.

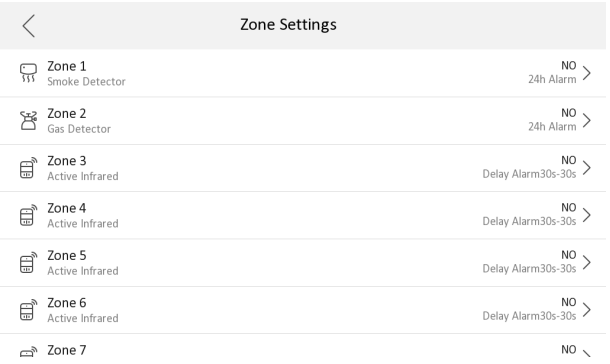

Figure 2-8 Zone Settings

2. Press a zone to pop up the zone editing dialogue box.
3. Set the zone type, alarm type, status of arming status, entering delay, and exiting delay.
4. Tap **OK** to save the settings.

Note

- 7 zone types are selectable: Panic Button, Door Magnetic, Smoke Detector, Active Infrared, Passive Infrared, Gas Detector, and Doorbell.
- 3 alarm types are selectable: 24h Alarm, Instant Alarm, and Delay Alarm.
  Set the alarm type as 24h alarm, and the zone will be armed for 24h.
  Set the alarm type as instant alarm, and the zone will alarm once it's triggered.
  Set the alarm type as delay alarm, and you should set the entering delay duration and exiting delay duration.

- Both the entering delay duration and the exiting delay duration are from 30s to 60s.
- For Gas Detector and Smoke Detector, the alarm type is set as default 24h alarm. The alarm type of them can not be changed.

Arming Mode Settings

4 arming modes can be configured: stay mode, away mode, sleeping mode and custom mode.

Before You Start

Tap **Settings** → → **Shortcut Settings** to enable **Alarm**.

Steps

Note

On the home page, the arming status function and zone settings function are hidden by default. You should enable the alarm function first.

1. Back to the home page, tap **Settings** → → **Scene Settings** to enter the arming mode settings page.
2. Tap **Stay Mode**, **Away Mode**, **Sleeping Mode**, or **Custom** to enter the page.

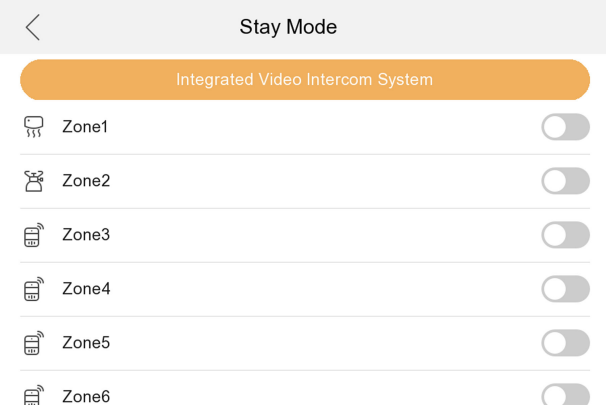

Figure 2-9 Arming Mode Settings

3. Arm the selected zone.

Note

- Zones are configurable on the arming mode page.
- 24H alarm zone including smoke detector zone and gas detector zone will be triggered even if they are disabled.
- Arming mode settings should be configured with the settings of arming status on the user page of the device.

2.3 Password Settings

2.3.1 Modify Admin Password

You can reset admin password via reserved email or security questions.

If you only set the email address or security questions, the admin password can be reset via the method you choose by default.

If you set both the email address and security questions, you can choose either method to reset the admin password.

Change by Email

You can change admin password via email.

Before You Start

- The function of the device varies according to different models. Refers to the actual device for detailed information.
- You need to set a reserved email address at the wizard or tap **Settings** → → **Configuration** → → **Security Settings** → **Email Address** to set or change the reserved email address.

Note

Admin password is required to enter the configuration page.

Steps

1. Tap **Settings** → → **Configuration** .
2. Tap **Forgot Password** at the pop up window.
3. Change your admin password via reserved email address.

Note

Make sure the device has added to the Hik-Connect account.

1) Download Hik-Connect app.

2) Go to **More → Reset Device Password** .

3) Scan the QR code on the device and a verification code will be popped up.

4) Enter the verification code on the device page.

5) Tap **OK**.

4. Create a new password and confirm it.

5. Tap **OK**.

Change by Security Question

You can change admin password via security questions.

Before You Start

You need to security questions at the wizard or tap **Settings →**  **→ Configuration →**  **→ Security Settings → Security Question** to set or change the answers to the questions.

Note

Admin password is required to enter the configuration page.

Steps

1. Tap **Settings →**  **→ Configuration** .

2. Tap **Forgot Password** at the pop up window.

3. Answer the security questions.

4. Tap **OK**.

2.3.2 Modify Arm/Disarm Password

You can create and edit the arm/disarm password of the indoor station.

Steps

1. Tap **Settings →**  **→ Password** to enter the settings page.

2. Tap **Arm/Disarm Password**. Create the indoor station's arm/disarm password. You should enter the arm/disarm password to enable or disable the function.

3. When you slide to disable **Scene Password**, there is no needs to enter password during scene mode switching.

2.3.3 Modify Unlock/Duress Code

You can create and edit the duress code and unlock password of the indoor station.

Steps

1. Tap **Settings** → → **Configuration** , and enter admin (activation) password.
2. Tap → **Password** to enter the password settings page.
3. Tap **Unlock Password** or **Duress Code** to pop up the password settings dialog box.
   Unlock Password

   Create the indoor station's unlock password. If the device has connected to a lock, enter the password to unlock.

   Duress Code

   When you are hijacked and forced to open the door, you can enter the duress code. An alarm will be triggered to notify the management center secretly.

Note

The duress code and the unlock password cannot be the same.

4. Create a new password and confirm it.
5. Tap **OK** to save the settings.

2.3.4 Modify SIP Password

You can change the SIP password.

Steps

1. Tap **Settings** → → **Configuration** , and enter admin (activation) password.
2. Tap → **SIP Settings** to enter the page.
3. Tap **Registration Password** to pop up the SIP registration password settings dialog box.
4. Create a new password and confirm it.
5. Tap **OK** to save the settings.

2.4 Synchronize Time

Steps

1. Tap **Settings** → → **Time and Date** to enter the time synchronization page.
2. Tap **Date Format** and **Time Format** to set the time format.
3. **Optional:** Tap **Time** to set time manually.
4. Tap **Sync Time**.

Figure 2-10 Time Synchronization

1) Select the **Time Zone**.
2) Enable **Enable NTP**.
3) Set the synchronizing interval, enter the IP address/domain of NTP server and port No.

Note

- The default unit of synchronizing interval is minute.
- The time zone can be configured as well if the NTP is not enabled.

2.5 Sound Settings

Set the ringtone sound, the volume, and the auto answer.

2.5.1 Call Settings

You can set the ringtone, ring duration, call forwarding time on call settings page.

Steps

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

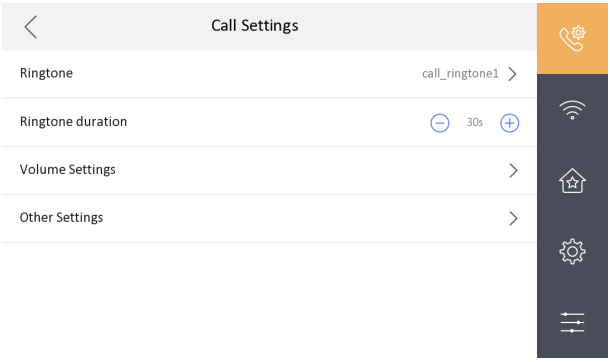

Figure 2-11 Call Settings

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 indoor station when it is called without being accepted. Ringtone duration ranges from 10 s to 30 s.

Other Settings

You can set the Do Not Disturb and Auto-answer functions.

Do Not Disturb Device

Select **All** and all devices will not disturb this device. Select **Indoor Station** and all indoor station will not disturb this device.

Do Not Disturb

Set the do not disturb schedule. Select **Close** and the do not disturb function will not be enabled. Select **All Day** and this device will not be disturbed all day. Select **Schedule** and you can set the do not disturb time duration. Within the configured time, this device will not be disturbed.

Note

Indoor extension does not support the ring duration settings, call forwarding settings, or auto-answer function.

2.5.2 Volume Settings

Set the microphone volume, prompt sound volume, call volume, and enable touch sound.

Steps

1. Tap **Settings** → → **Volume Settings** to enter the volume settings page.
2. Set the microphone volume, prompt sound volume, and the call volume. You can also enable **Touch Sound** to turn on the key sound.

2.6 Link to the Mobile Client

Before You Start

Note

The function of the device varies according to different models. Refers to the actual device for detailed information.

Steps

1. Tap **Settings** → → **Configuration** → → **Hik-Connect Service Settings** to enter the settings page.

   Note

   Admin password is required to enter the configuration page.

2. Enable **Enable Hik-Connect Service**.
3. Edit **LBS** server and **Verification Code**.

   Note

   Verification code is used to add the device to mobile client.

4. **Optional:** Scan the QR code on the screen.

   Note

   - Scan the left QR code on the screen to access Hik-Connect.
   - Scan the right QR code on the screen to add the device to the mobile client.

2.7 System Settings

2.7.1 General Settings

You can format or install TF card, clean the screen, set system language and adjust the screen brightness on this page.

Tap **Settings** → to enter the general settings page.

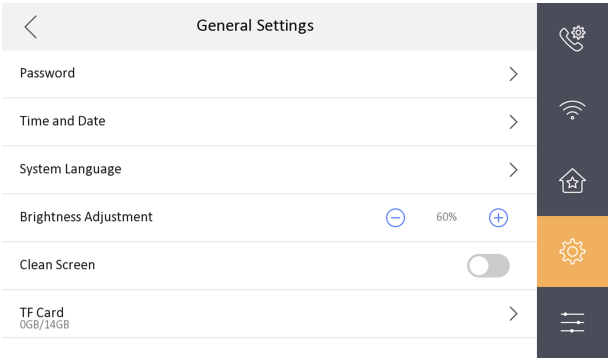

Figure 2-13 General Settings Page

Password

You can manage your arm/disarm password and scene password. For details, see ***Modify Arm/Disarm Password***

Time and Date

You can set the displayed time and date format, current time. You can also tap **Sync Time** and enable NTP to synchronize the device time.

Note

- Make sure your device is connected with the network or the NTP function will not available.
- For details, see ***Synchronize Time***.

System Language

Tap **System Language** to change the system language.

Note

The indoor station supports 11 languages.

Brightness Adjustment

Tap **+** or **-** to adjust the screen brightness.

Clean Screen

Enable **Clear Screen** and the screen will be locked for 30s. And you can clear the screen within the time duration.

Note

- After enabling Clear Screen function, press and hold the Unlock key to exit the clear screen mode.
- The device without unlock key will exit the clear screen mode automatically when the time is out.

TF Card

Tap **TF Card** to view the TF card and you can also format the TF card.

2.7.2 Maintenance

You can restore the device, upgrade system, unlink app account, set wizard, and configure security settings on the system maintenance page.

Tap **Settings** → → **Configuration** → to enter the system maintenance page.

Note

Admin password is required to enter the configuration page.

Restore Default Settings

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

Restore All

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

Upgrade

Tap **Upgrade** to get the upgrade package online.

Unlink APP Account

Tap **Unlink APP Account** to unlink the Hik-Connect account from the platform.

Note

The function of the device varies according to different models. Refers to the actual device for detailed information.

Wizard

Tap **Wizard** and set the language, password reset method, network parameters, indoor station parameters, platform service, and related device. For details, refer to ***Quick Operation***.

Security Settings

Tap **Security Settings** and set the email address or security questions for password reset.

2.7.3 Preference

You can configure zone settings, scene settings and shortcut settings on the preference page.

Tap **Settings** → to enter the preference page.

Zone Settings

Note

Only when enable **Alarm** in the shortcut settings, can the **Zone Settings** displayed on the Preference page.

Set the zone parameters. For details, see ***Zone Settings***.

Scene Settings

Note

Only when enable **Alarm** in the shortcut settings, can the **Scene Settings** displayed on the Preference page.

Set the scene parameters, including the stay mode, the away mode, the sleeping mode, or customize the scene. For details, see ***Arming Mode Settings***.

Shortcut Settings

Enable call elevator, alarm, call management center, leave message or snapshot and the icon will be displayed on the home page.

You can set the leave message time and snapshot time if the two functions are enabled.

2.8 Device Information

View the device information, including the version, model, serial No. and open source disclaimer.

Steps

1. Tap **Settings** → → **Device Information** to enter the Device Information page.
2. View the device version, model, and serial No.

2.9 Output Settings

You can set and control the connected output devices via the output settings page. You can change the relay' name, and open duration. You can also set to display the relay button on the main page or not.

Steps

1. Tap **Settings** → → **Output Settings** .

Note

- Supports up to 2 relays.
- If no relays displayed on the page, the device may not support the function.

2. Select a relay and set the parameters.

Name

You can change the relay's name.

Note

1 to 32 characters are allowed. Supports uppercase letters, lowercase letters, numerics, and special characters.

Remain Open

Enable the function, the relay remains open.

Disabled the function, and you can set the remain open duration.

Note

- By default, the function is disabled.
- 1 to 180 s are available to set.

Hide on Main Page

Enable the function and the relay button will be displayed on the main page. You can control the relay status manually on the main page.

Disabled the function and the relay button will no be displayed on the main page.

3 Remote Operation via the client software

The Video Intercom module provides remote control and configuration on video intercom products via the iVMS-4200 client software.

3.1 Activate Device Remotely

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

Before You Start

Default parameters of indoor station are as follows:

- Default IP Address: 192.0.0.64.
- Default Port No.: 8000.
- Default User Name: admin.

Steps

1. Run the client software, enter **Device Management**, check the **Online Device** area.
2. Select an inactivated device and click the **Activate**.
3. Create a password, and confirm the password.

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

3.2 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.

3.2.1 Add Video Intercom Devices

Steps

Note

- You can add at most 512 indoor stations and main stations in total to the client, and add at most 16 door stations to the client.
- For video intercom devices, you are required to create the password to activate them before they can be added to the software and work properly.
- You can add online video intercom devices, and add them manually. Here take adding online video intercom devices as example.

1. Click **Maintenance and Management → Device Management** to enter the device management page.
2. Click the **Device** tap.
3. Click **Add** to add the device to the client.

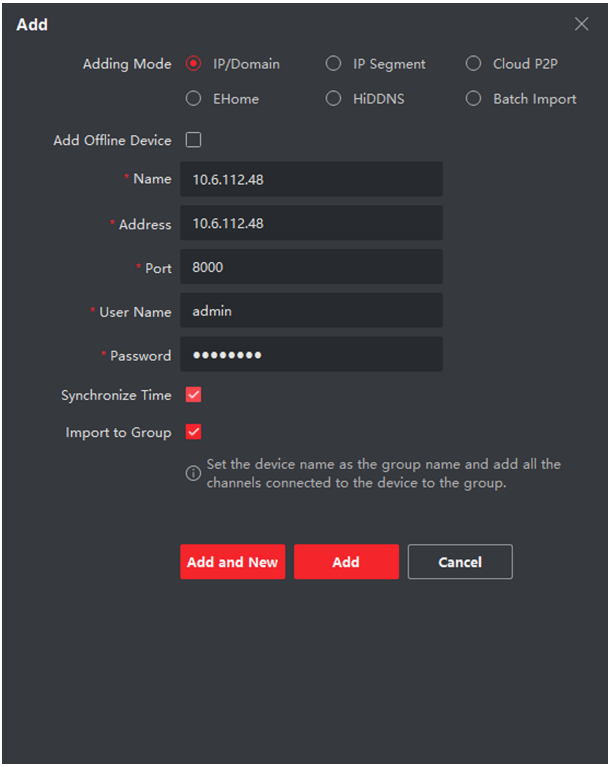

Figure 3-1 Add the Device

4. **Optional:** Click **Online Device**, the active online devices in the same local subnet with the client software will be displayed on the **Online Device** area.

Note

To add online devices to the software, you are required to change the device IP address to the same subnet with your computer first.

1) You can click **Refresh Every 60s** to refresh the information of the online devices.

2) Select the devices to be added from the list.

3) Click **Add to Client** to add the device to the client.

5. Input the required information.
Nickname

Edit a name for the device as you want.

Address

Input the device's IP address. The IP address of the device is obtained automatically in this adding mode.

Port

Input the device port No. The default value is 8000.

User Name

Input the device user name. By default, the user name is admin.

Password

Input the device password. By default, the password is 12345.

6. **Optional:** You can check the checkbox **Export to Group** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default.

   The client also provides a method to add the offline devices. Check the checkbox **Add Offline Device**, input the required information and the device channel number and alarm input number, and then click **Add**. When the offline device comes online, the software will connect it automatically.

Note

- Add Multiple Online Devices: If you want to add multiple online devices to the client software, click and hold **Ctrl** key to select multiple devices, and click **Add to Client** to open the device adding dialog box. In the pop-up message box, enter the user name and password for the devices to be added.
- Add All the Online Devices: If you want to add all the online devices to the client software, click **Add All** and click **OK** in the pop-up message box. Then enter the user name and password for the devices to be added.

3.2.2 Modify Network Information

Select the device from the device list, click , and then you can modify the network information of the selected device.

Note

You should enter the admin password of the device in the **Password** field of the pop-up window to modify the parameters.

3.3 System Configuration

You can configure the video intercom parameters accordingly.

Steps

1. Click **Maintenance and Management → System Configuration → ACS & Video Intercom** to enter the system configuration page.
2. Enter the required information.

   Ringtone

   Click **...** and select the audio file from the local path for the ringtone of indoor station. Optionally, you can click for a testing of the audio file.

   Ringtone Duration

   Enter ringtone duration, ranging from 15 seconds to 60 seconds.

   Max. Speaking Duration with Indoor Station

   Enter the maximum duration of speaking with the indoor station, ranging from 120 seconds to 600 seconds.

   Max. Speaking Duration with Door Station

   Enter the maximum duration of speaking with the door station, ranging from 90 seconds to 120 seconds.

   Max. Speaking Duration with Access Control Device

   Enter the maximum duration of speaking with the access control device, ranging from 90 seconds to 120 seconds.
3. Click **Save** to enable the settings.
4. **Optional:** Click **Default** to restore the default parameters.

3.4 Remote Configuration

In the device list area, select a device and click to enter the remote configuration page.

3.4.1 System

Click **System** on the remote configuration page to display the device information: Device Information, General, Time, System Maintenance, User, RS-485, and Security.

Device Information

Click Device Information to enter device basic information page. You can view basic information (the device type, and serial No.), and version information of the device.

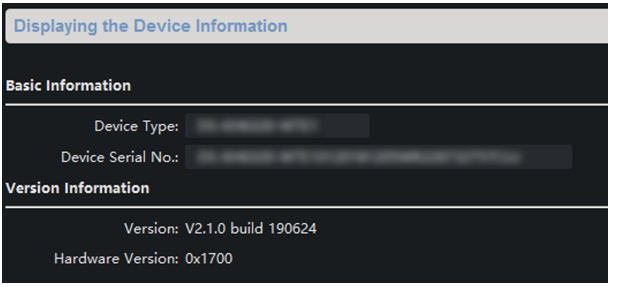

Figure 3-2 Device Information

General

Click **General** to enter device general parameters settings page. You can view and edit the device name and device ID, and select overwrite record file.

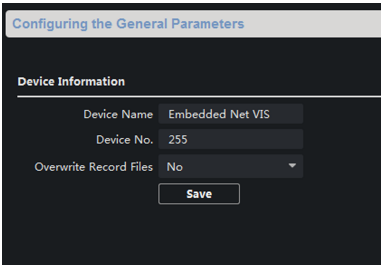

Figure 3-3 General

Time

Click **Time** to enter the device time settings page.

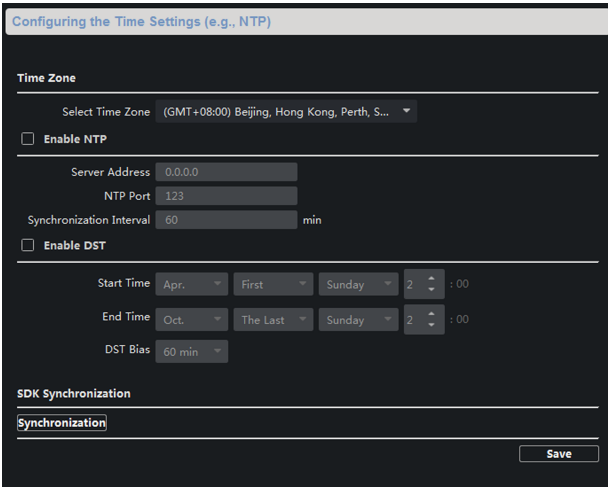

Figure 3-4 Time Settings Page

Select **Time Zone**, **Enable NTP**, **Enable DST**, or **SDK Synchronization**. Click **Save** to save the time settings.

- Time Zone: Select a time zone from the drop-down list menu.
- NTP: Click **Enable NTP**, and enter the server address, NTP port, and synchronization interval.

  Note

  The default port No. is 123.

- DST: Click **Enable DST**, and set the start time, end time, and bias.
- SDK Synchronization: Click **Synchronization**, and the system will synchronize the data to the SDK.

System Maintenance

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

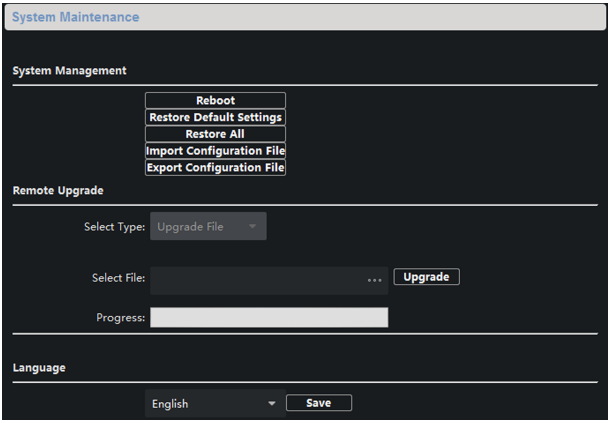

Figure 3-5 System Maintenance

- Reboot: Click **Reboot** and the system reboot dialog box pops up. Click **Yes** to reboot the system.
- Restore Default Settings: Click **Restore Default Settings** to restore the default parameters. All default settings, excluding network parameters, will be restored.
- Restore All: Click **Restore All** to restore all parameters of device and reset the device to inactive status.

Note

all default settings, including network parameters, will be restored. The device will be reset to inactivated status.

- Import Configuration File: Click **Import Configuration File** and the import file window pops up. Select the path of remote configuration files. Click **Open** to import the remote configuration file. The configuration file is imported and the device will reboot automatically.
- Export Configuration File: Click **Export Configuration File** and the export file window pops up. Select the saving path of remote configuration files and click **Save** to export the configuration file.

- Remote Upgrade: Click **...** to select the upgrade file and click **Upgrade** to remote upgrade the device. The process of remote upgrade will be displayed in the process bar.
- Language: Select a language, and click **Save** to change the device system language.

Note

- The device supports 19 languages: English, French, Brazilian Portuguese, Spanish, Russian, German, Italian, Polish, Arabic, Turkish, Vietnamese, Ukrainian, Hungarian, Dutch, Romanian, Czech, Bulgarian, Croatian, Serbian.
- Rebooting the device is required after you change the system language.

User

Click **User** to enter the user information editing page.

Select the user to edit and click **Edit** to enter the user parameter page.

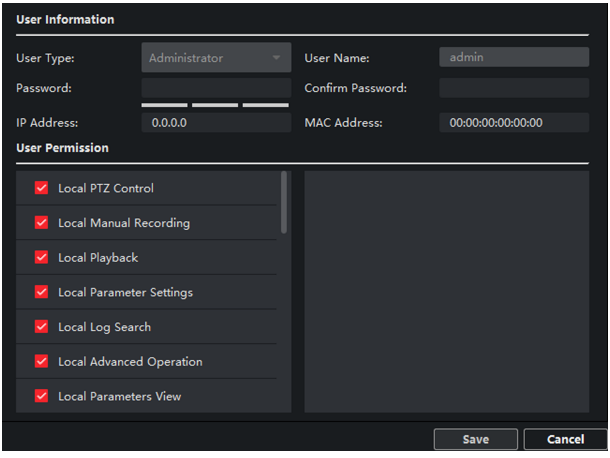

Figure 3-6 User Page

Note

- The new password and confirm password should be identical.
- After editing the password of device, click refresh button from the device list, the added device will not be there. You should add the device again with new password to operate the remote configuration.

RS-485

Click **RS485** to enter the RS-485 settings page. You can view and edit the RS-485 parameters of the device.

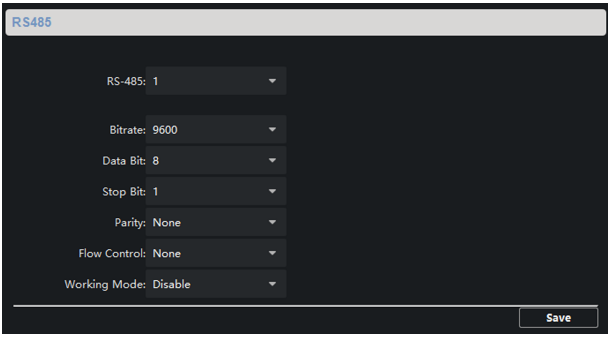

Figure 3-7 RS-485 Settings

Note

For indoor station and main station, there are 3 choices for the working mode: transparent channel, disable, and custom.

Security

Click **Security** to enter the page. You can enable SSH or enable HTTPS on this page.

Click **Save** after configuration.

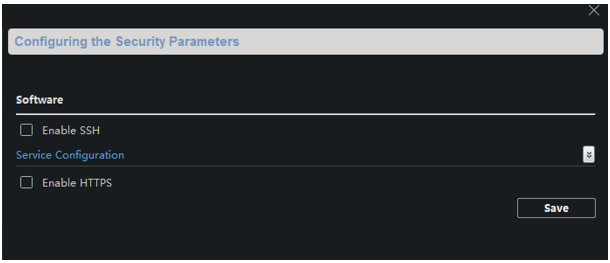

Figure 3-8 Security

3.4.2 Video Intercom

Click **Video Intercom** on the remote configuration page to enter the video intercom parameters settings: Time Parameters, Password, Zone Configuration, IP Camera Information, Volume Input and Output Configuration, Ring, Arming Information, Calling Linkage, Relay, and SIP No.

Time Parameters

Steps

1. Click **Time Parameters** to enter time parameters settings page.

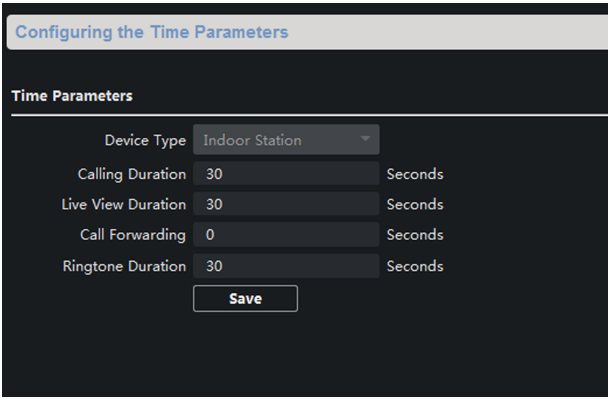

Figure 3-9 Time Parameters

2. Configure the calling duration, live view duration, call forwarding time, and the ringtone duration.
3. Click **Save**.

Note

- Calling duration is the maximum duration of indoor station when it is called without being received. The range of maximum ring duration varies from 30s to 60s.
- Live view duration is the maximum time of playing live view of the indoor station. The range of maximum live view time varies from 10s to 60s.
- Call forwarding refers to the ring duration limit beyond which the call is automatically forwarded to the mobile phone designated by the resident. The range of call forwarding time varies from 0s to 20s.
- For indoor extension, it only requires setting the maximum live view time.

Permission Password

Click **Permission Password** to enter password changing page.

Select password type. Create a new password and confirm it.

Click **Save** to complete the settings.

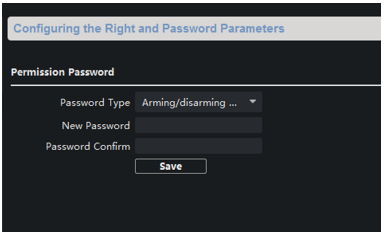

Figure 3-10 Permission Password

Note

For indoor station, you can enter the old password and new password to change the arm/disarm password.

Zone Alarm

Steps

1. Click **Zone Alarm** to enter the zone settings page.

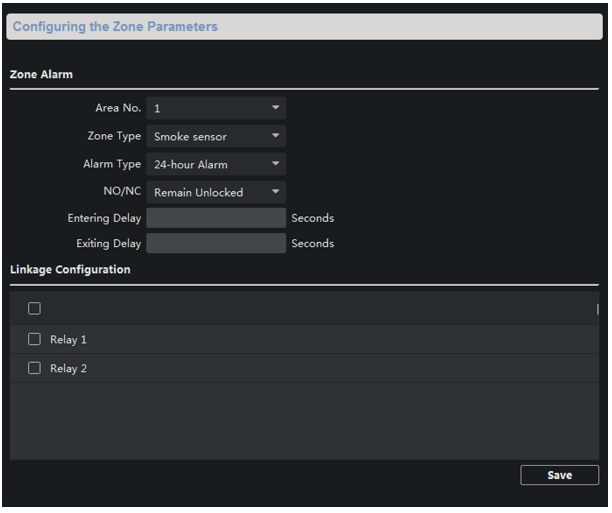

Figure 3-11 Zone Alarm

2. Select **Area No.**

3. Select **Zone Type** from the drop-down list.

4. Select **Alarm Type** from the drop-down list.

5. Set the NO/NC status.

6. Set **Entering Delay** and **Exiting Delay**.

7. Click **Save** to enable zone settings.

Note

- 7 zone types are supported: Emergency Switch, Door Magnetic Switch, Smoke Detector, Active IR Detector, Passive IR Detector, Combustible Gas Detector, and DoorBell Switch.
- 3 types of alarm mode are supported: Instant Alarm, 24H Alarm, and Delay Alarm.
- When the zone type is set to be Instant Alarm, only under arming mode, the indoor station will receive alarm message when the detector is triggered. Under

disarming mode, it will not receive alarm message when the detector is triggered.

- When the zone type is set to be 24H Alarm, the indoor station will receive alarm message when the detector is triggered no matter it is under arming mode or disarming mode.
- When the zone type is set to be Delay Alarm, only under arming mode, the indoor station will receive alarm message when the detector is triggered. Under disarming mode, it will not receive alarm message when the detector is triggered.
- After setting enter delay time, if OK is pressed within the enter delay time after the alarm, the alarm event will not be uploaded to the management center; if OK is not pressed within the enter delay time after the alarm, the alarm event will be uploaded to the management center.
- The exit delay is the time between you enable the arming mode and the arming takes effect.

IP Camera Information

You can add, delete and modify cameras that can be added to the video intercom products, with two ways of getting stream: direct or URL. By exporting and importing the added device information, you can edit added devices parameters in batch.

Add Camera

Steps

1. Click **IP Camera Information** to enter IP camera information page.

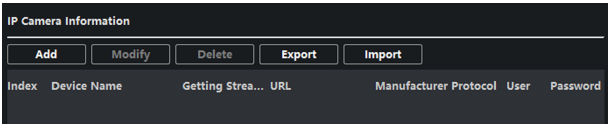

Figure 3-12 IP Camera Information

2. Click **Add** to pop up the device adding dialog box.

3. Enter corresponding information (device name, IP address, port No., user name, password, etc.), and click **OK**.

Note

Indoor extension does not support this function.

Export and Import Added Device Information

Steps

1. Click **Export** to export the added device information file.
2. Edit parameters of added devices in batch in the exported file.
3. Click **Import** to pop up importing box, and open the edited added device information file.

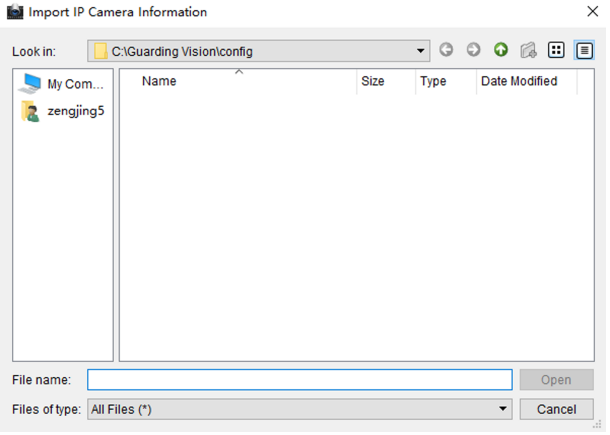

Figure 3-13 Import Added Device Information

Volume Input and Output

Steps

1. Click **Volume Input/Output** to enter the configuring the volume input or output page.

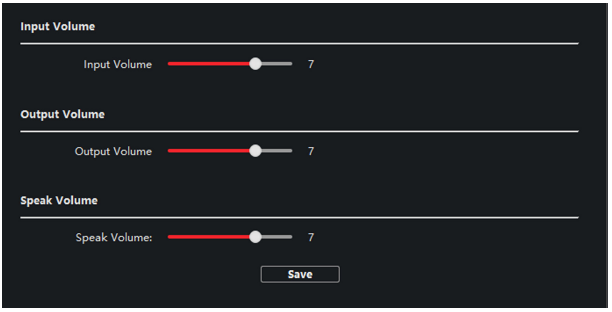

Figure 3-14 Volume Input or Output

2. Slide the slider to adjust the input volume, output volume and speak volume.

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

Ring Import

Steps

1. Click **Ring Import** to enter the ring configuration page.

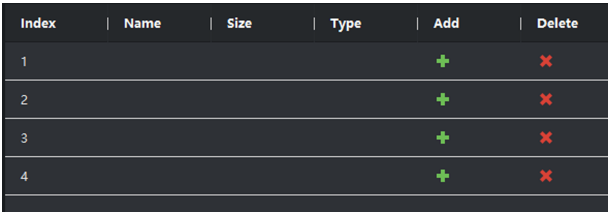

Figure 3-15 Ring Import

2. Click **+** to add the ring, and click **x** to delete the imported ring.

Note

- The ring to be imported should be in the wav format, and the size of the ring cannot be larger than 300k.
- Up to 4 rings can be added.

Arming Information

Click **Arming Information** to enter the configuring arming informaton page and view the arming information.

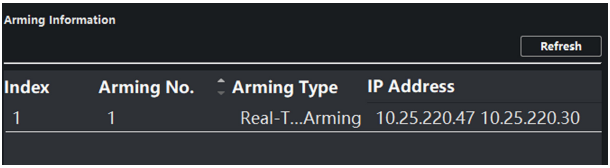

Figure 3-16 Arming Information

Click **Refresh** to refresh the arming information.

Relay

Click **Relay** to enter the set relay parameters page.

Select a relay and click " " and set the relay name and output delay time. Click **Save** to enable the settings.

Click **Copy to...**, and select a relay you want to copy to. Click **Save** to enable the settings.

SIP No. Settings

Steps

1. Click **SIP No. Settings** to enter the settings page.

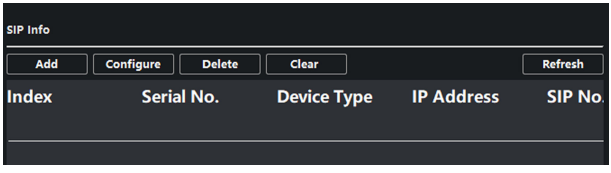

Figure 3-17 Extension Settings

2. Click **Add**.

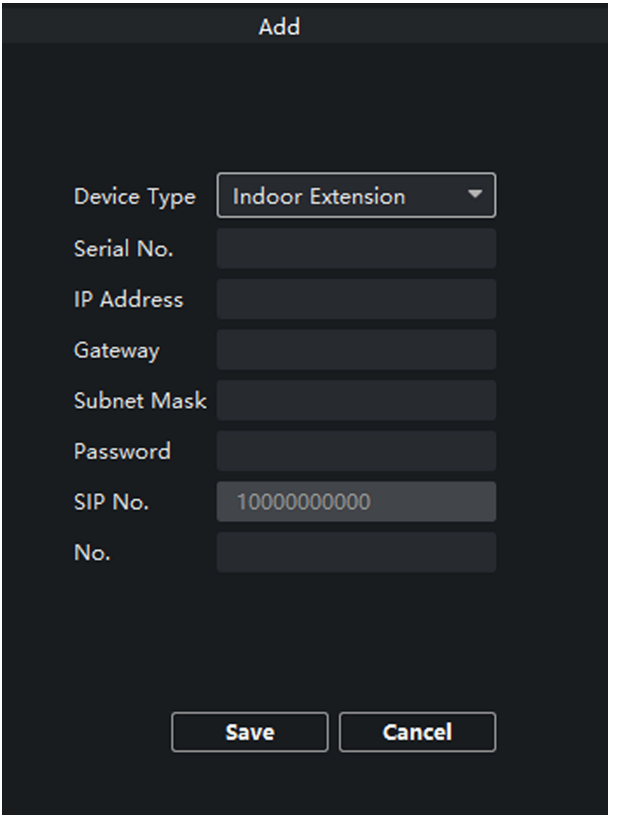

Figure 3-18 Add SIP Info

3. Select **Device Type** as **Indoor Extension**.

4. Enter the required information.

Serial No.

Enter the device's serial No.. The serial No. is on the rear panel of the device (A fixed-length number with 9 digits).

IP Address

Enter the device's IP address.

Gateway

Enter the device's gateway.

Subnet Mask

Enter the device's subnet mask.

Password

Enter the device password, ranging from 8 to 16 characters in length.

No.

Enter the device No., ranging from 1 to 5.

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

6. Set SIP information.

Click Configure	Configure serial No., IP address, gateway, subnet mask, password and No. of the device.
Click Delete	Delete the SIP Number.
Click Clear	Clear all SIP numbers.
Click Refresh	Refresh SIP Information.

3.4.3 Network

Local Network Configuration

Steps

1. Click **Local Network Configuration** to enter the configuring the local network parameters page.

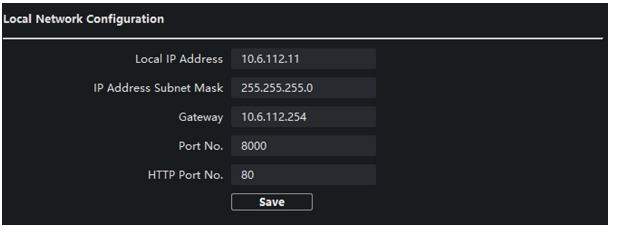

Figure 3-19 Local Network Configuration

2. Enter the **Local IP Address**, **IP Address Subnet Mask**, **Gateway**, **Port No.** and **HTTP Port No.**

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

Note

- The default port No. is 8000.
- After editing the local network parameters of device, you should add the devices to the device list again.

SIP Server Configuration

Steps

1. Click **SIP Server Configuration** to enter the configuring the SIP parameters page.

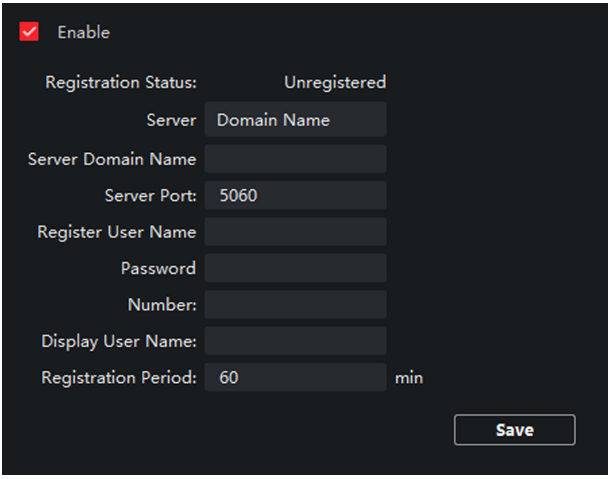

Figure 3-20 SIP Server Configuration

2. Click **Enable**.

3. Set the parameters according to your needs.

Note

- Up to 32 characters are allowed in the Register User Name field.
- Registration password should be 1 to 16 characters in length.
- Up to 32 characters are allowed in the Number field.
- The device location should contain 1 to 32 characters.
- The registration period should be between 15 minutes to 99 minutes.

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

DNS Settings

The indoor station supports 2 DNS address.

Click **Advanced Settings** to enter DNS address settings page.

Edit the IP address and click **Save**.

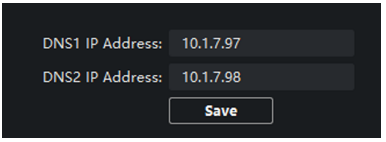

Figure 3-21 DNS Settings

Configure Mobile Client Connection

Configure **Hik-Connect** server parameters before viewing videos via mobile client.

Before You Start

Make sure the indoor station connects to the network.

Steps

1. Click **Hik-Connect** to enter the configuring the settings page.

2. Enable **Enable Hik-Connect**.

Note

- To enable Hik-Connect service, you need to create a verification code or change the verification code.
- The verification code should be 6 to 12 letters or numbers, case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

3. Enter the **Verification Code** and confirm the verification code.

4. Click **OK**.

5. Enable **Custom** and edit **Service Address**.

6. If you forget the verification code, you can enable **View**.

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

8. Optional: Click **Refresh** to refresh the settings.

Group Network Settings

Click **Group Network Settings** to enter the group network settings page.

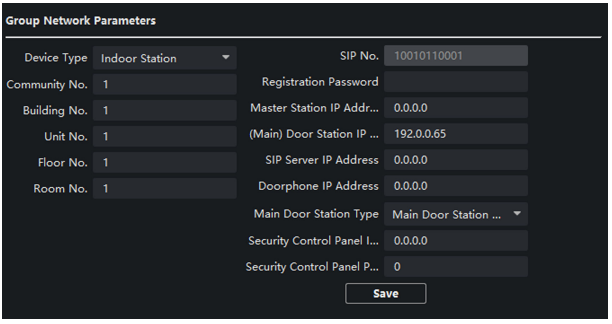

Figure 3-22 Group Network Settings

Device No. Settings

Select the device type from the drop-down list, and set the corresponding information.

Note

- Device type can be set as indoor station or indoor extension.
- When you select indoor extension as device type, the device No. can be set from 1 to 5.

Click **Save** to enable the settings.

Linked Device Network Settings

Enter **Registration Password** and set the corresponding information.

Note

- D series refers to door station, and V series refers to villa door station.
- Registration password is the password of the SIP server.

3.5 Person Management

You can add, edit, and delete the organization and person in Person Management module. Organization and person management is necessary for the video intercom function.

On the main page, click **Person** to enter the page.

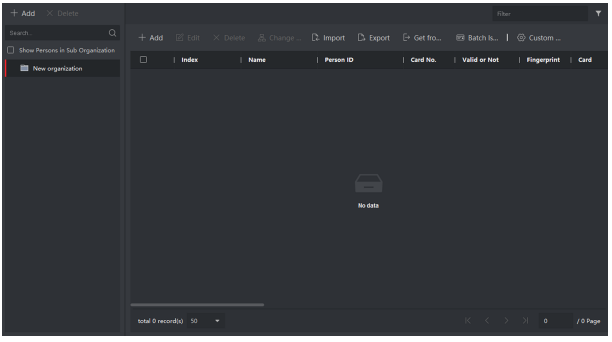

Figure 3-23 Personal Management Application

The page is divided into two parts: Organization Management and Person Management.

Organization Management	You can add, edit, or delete the organization as desired.
Person Management	After adding the organization, you can add the person to the organization and issue card to persons for further management.

3.5.1 Organization Management

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

Add Organization

Steps

1. In the organization list on the left, click **+Add**.

2. Input the organization name as desired.

3. 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.

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.

3.5.2 Person Management

After adding the organization, you can add person to the organization and manage the added person such as issuing cards in batch, importing and exporting person's information in batch, etc.

Note

Up to 10,000 persons or cards can be added.

Add Person

Person information is necessary for the video intercom system. And when you set linked device for the person, the intercom between intercom devices can be realized.

Steps

1. Select an organization in the organization list and click **+Add** on the person panel to pop up the adding person dialog.

Note

The Person ID will be generated automatically and is editable.

2. Set basic person information.

1) Enter basic information: name, gender, tel, birthday details, effective period and email address.

2) **Optional:** Click **Add Face** to upload the photo.

Note

The picture should be in *.jpg format.

Click Upload	Select the person picture from the local PC to upload it to the client.
Click Take Phone	Take the person's photo with the PC camera.
Click Remote Collection	Take the person's photo with the collection device.

3. Issue the card for the person.

1) Click **Credential → Card** .

2) Click **+** to pop up the Add Card dialog.

3) Select **Normal Card** as **Card Type**.

4) Enter the **Card No.**

5) Click **Read** and the card(s) will be issued to the person.

4. Add fingerprints to the person.

1) Click **Credential → Fingerprint** .

2) Click **+** to pop up the Add Fingerprint dialog.

3) Select **Collection Mode**.

4) Select **Fingerprint Recorder** or **Device**.

5) Click **Start** to collect the fingerprint.

6) Click **Add**.

Import and Export Person Information

The person information can be imported and exported in batch.

Steps

1. Exporting Person: You can export the added persons' information in Excel format to the local PC.
   1) After adding the person, you can click **Export Person** to pop up the following dialog.
   2) Click **...** to select the path of saving the exported Excel file.
   3) Check the checkboxes to select the person information to export.
   4) Click **OK** to start exporting.
2. Importing Person: You can import the Excel file with persons information in batch from the local PC.
   1) Click **Import Person**.
   2) You can click **Download Template for Importing Person** to download the template first.
   3) Input the person information to the downloaded template.
   4) Click **...** to select the Excel file with person information.
   5) Click **OK** to start importing.

Get Person Information from Device

If the added device has been configured with person information (including person details, fingerprint, issued card information), you can get the person information from the device and import to the client for further operation.

Steps

Note

This function is only supported by the device the connection mothod of which is TCP/IP when adding the device.

1. In the organization list on the left, select an organization to import the persons.
2. Click **Get from Device** to pop up the dialog box.
3. The added device will be displayed.
4. Click to select the device and then click **Get** to start getting the person information from the device.

Note

- The person information, including person details, person's fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.

Modify and Delete Person

Select the person and click **Edit** to open the editing person dialog.

To delete the person, select a person and click **Delete** to delete it.

Note

If a card is issued to the current person, the linkage will be invalid after the person is deleted.

Change Person to Other Organization

You can move the person to another organization if needed.

Steps

1. Select the person in the list and click **Change Organization**.

2. Select the organization to move the person to.

3. Click **OK** to save the settings.

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


See Far, Go Further