AX HYBRID PRO

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE

PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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

Contents

Chapter 1 Configuration 1
1.1 Use the Web Client 1
1.1.1 Activate Device via Web Browser 1
1.1.2 Communication Settings 3
1.1.3 Device Management 18
1.1.4 Permission Management 22
1.1.5 Maintenance 26
1.1.6 System Settings 28
1.1.7 Check Status 32
1.2 Using the Mobile Client 33
1.2.1 Download and Login the App 33
1.2.2 Set-up with Hik-Partner Pro 34
1.2.3 Set-up with App 55
Appendix A. Input Types 64
Appendix B. Event Types 67
Appendix C. Access Levels 68
Appendix D. Symbol Conventions 70

Chapter 1 Configuration

Configure the security control panel in the web client or the remote configuration page in client software.

1.1 Use the Web Client

Steps

1. Connect the device to the Ethernet.
2. Search the device IP address via the client software and the SADP software.
3. Enter the searched IP address in the address bar.

Note

- When using mobile browser, the default IP Address is 192.168.8.1. The device must be in the AP mode.
- When connecting the network cable with computer directly, the default IP Address is 192.0.0.64

4. Use the activation user name and password to login.

Note

Refer to *Activation* chapter for the details.

1.1.1 Activate Device via Web Browser

Use web browser to activate the device. Use SADP software or PC client to search the online device to get the IP address of the device, and activate the device on the web page.

Before You Start

Make sure your device and your PC connect to the same LAN.

Steps

1. Open a web browser and input the IP address of the device.

Note

If you connect the device with the PC directly, you need to change the IP address of your PC to the same subnet as the device. The default IP address of the device is 192.0.0.64.

2. Create and confirm the admin/ installer password.

Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

3. Click **OK** to complete activation.
4. Edit IP address of the device.
   1) Enter IP address modification page.
   2) Change IP address.
   3) Save the settings.

Note

- The default user name of admin account is **admin**.
- The Italian user name of admin is **administrator**.

Table 1-1 User Name of Installer

Language	User Name
English	installer
Italian	installatore
Polish	instalator
German	errichter
Turkish	kurulumcu
Russian	монтажник
French	installateur
Spanish	instalador
Portuguese	instalador
Czech	technik

1.1.2 Communication Settings

Connect to Network

Ethernet

You can set the device IP address and other network parameters.

Steps

Note

Functions varied depending on the model of the device.

1. Click **Configuration → Network → Network Settings → Ethernet** to enter the page.

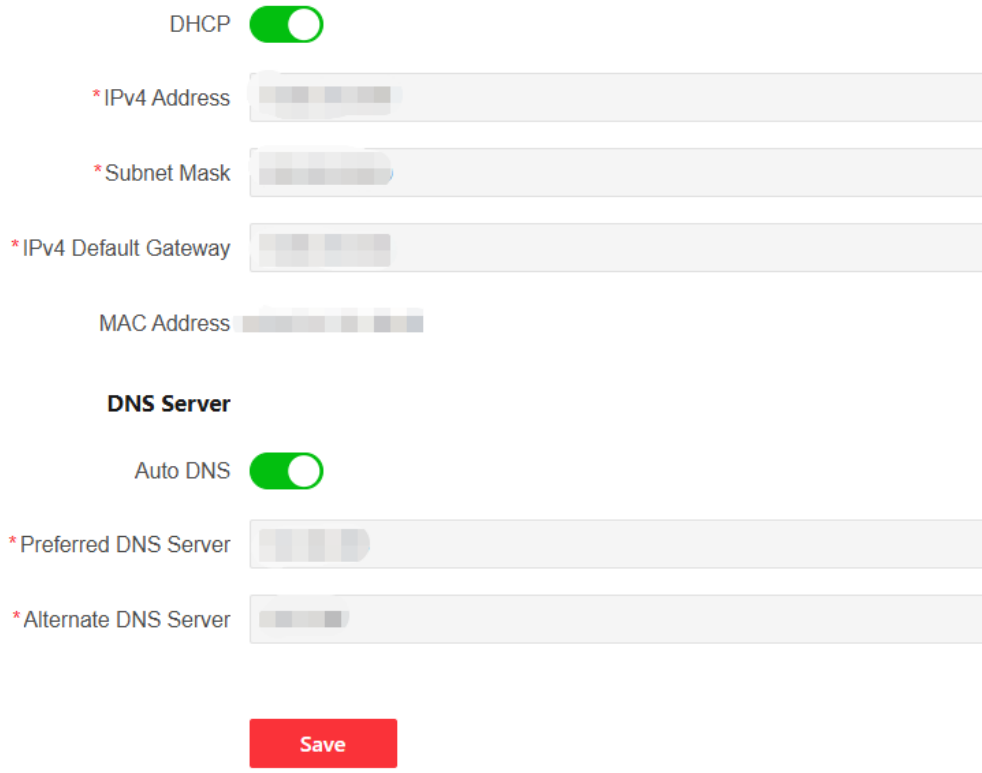


Figure 1-1 Ethernet Settings

2. Set the parameters.
   - Automatic Settings: Enable **DHCP** and **DNS Server**.

- Manual Settings: Disabled **DHCP** and **DNS Server**, set **IPv4 Address**, **Subnet Mask**, **IPv4 Default Gateway**, **Preferred DNS Server**, **Alternate DNS Server**.

3. **Optional:** Set correct DNS server address if the device needs to visit Hik-Connect server via a domain name.
4. Click **Save**.

Wi-Fi

You can connect the device with a Wi-Fi, and set the Wi-Fi's WLAN paramters, so that you can use the WLAN parameters to enter the device web page or use mobile App to add the device.

Steps

1. Click **Configuration → Network → Network Settings → Wi-Fi** to enter the page.

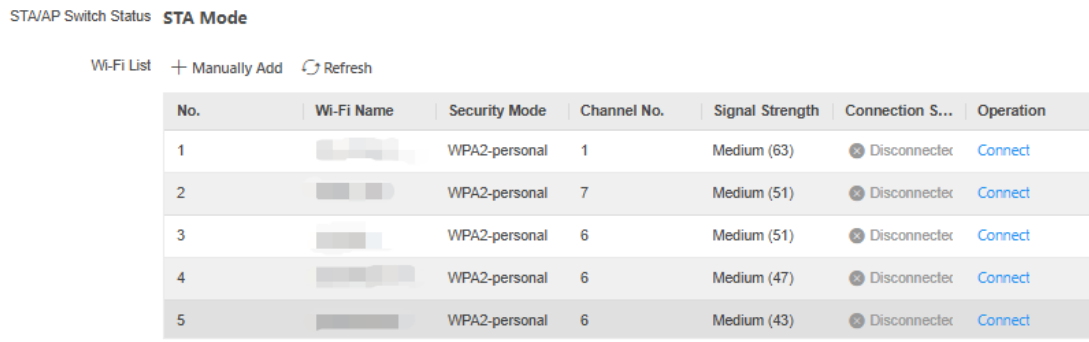


Figure 1-2 Add Wi-Fi

The scanned Wi-Fi will be in the list.

2. Connect to a Wi-Fi.
   - Select a Wi-Fi from the list and click **Connect** and enter the Wi-Fi password to connect to the Wi-Fi.
   - If you cannot find the Wi-Fi in the list, you can manually add a Wi-Fi. Click **Manually Add** , enter the **Wi-Fi Name**, select **Security Mode**, and set **Password**.
3. You can also set the Wi-Fi's WLAN parameters.

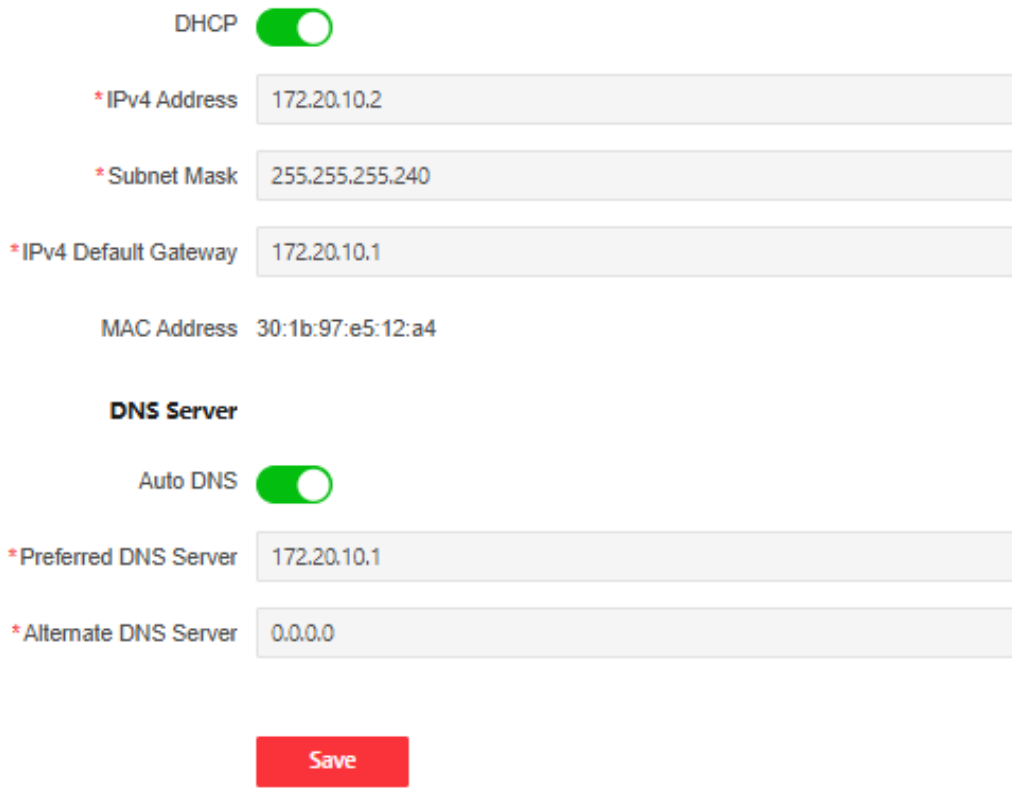


Figure 1-3 WLAN Settings

4. Set **IPv4 Address**, **Subnet Mask**, **IPv4 Default Gateway**, **Preferred DNS Server**and **Alternate DNS Server**.

Note

If enable DHCP, the device will gain the Wi-Fi parameters automatically.

5. Click **Save**.

HTTP(S)

Click **Configuration → Network → Network Service → HTTP(S)** to enter the page.

You can set HTTP port here.

NAT

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to

connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

Steps

1. Click **Configuration → Network → Network Service → NAT** to enter the page.

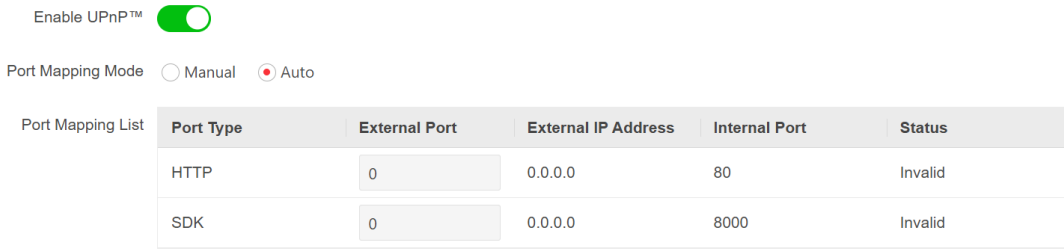


Figure 1-4 Set NAT

2. Drag the slider to **Enable UPnP**.
3. Select the mapping type as **Manual** to set the HTTP port and the SDK port.

Note

If select **Auto**, the device will gain the HTTP port and the SDK port automatically.

4. Tap **Save**.

Connect to Cloud

After enable the cloud service function, the device can be added to the cloud and you can add the device to the App.

Steps

1. Click **Configuration → Network → Cloud Service** to enter the page.

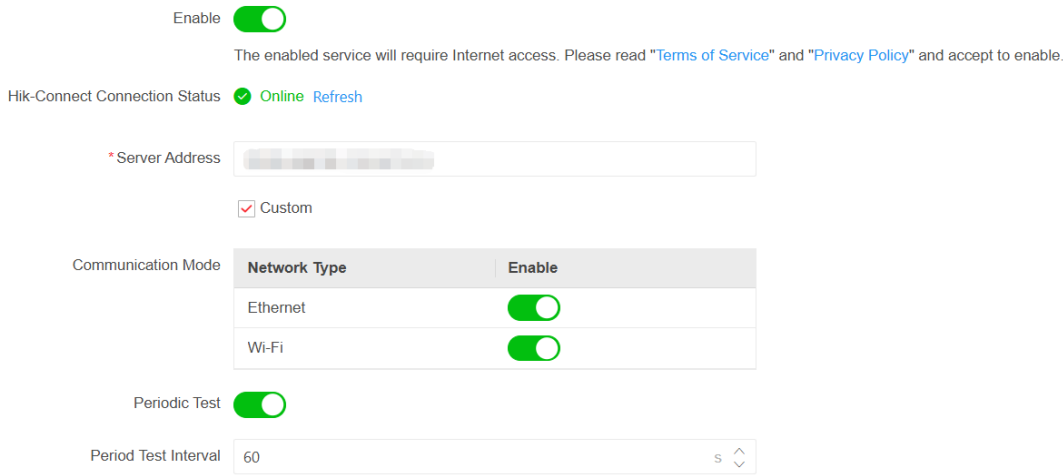


Figure 1-5 Cloud Service

2. Drag the slider to enable the function.

Note

- By default, the device Hik-Connect service is enabled.
- You can view the device status in the Hik-Connect server (www.hik-connect.com).

3. The server address is already displayed in the Server Address box, or you can check **Custom** to edit it.
4. Select **Communication Mode** as **Ethernet**, **Wi-Fi**, **Cellular**or by dragging the slider to enable the function.
5. **Note**

   At least enable one network connection, otherwise the current service will not work.

   Enable **Periodic Test**. Enter the periodic test interval.

   Periodic Test

   After enabling, you can set the time interval, setting how often to send a test event to the ARC to ensure the connection.
6. Click **Save**.

Connect to Alarm Receiving Center (ARC)

Alarm Receiving Center

You can set the alarm receiving center's parameters and all alarms will be sent to the configured alarm receiving center.

Steps

1. Click **Configuration → Alarm Communication → Alarm Receiving Center** to enter the Alarm Receiving Center page.
2. Select the **Alarm Receiver Center** as **1**, **2** , **3**or **4** for configuration , and slide the slider to enable the selected alarm receiver center.
3. Select the **Connection Type** as **Serial Port**, or **IP**.
   - **IP**
4. Select the **Protocol Type** as **SIA-DCS**, ***SIA-DCS**, **ADM-CID**, ***ADM-CID**, **CSV-IP**, **OTAP** or **ISUP**.

Note

Standard DC-09 Protocol
SIA-DCS: The data presenting method of DC-09 is DCS (also called SIA protocol), which is not encrypted and only for uploading alarm report.
*SIA-DCS: The data presenting method of DC-09 is DCS (also called SIA protocol), which is encrypted and only for uploading alarm report.
ADM-CID: The data presenting method of DC-09 is CID, which is not encrypted and only for uploading alarm report.
*ADM-CID: The data presenting method of DC-09 is CID, which is encrypted and only for uploading alarm report.

- **SIA-DCS** or **ADM-CID**.

  Set **Connection Mode** as **TCP** or **UDP**.

  Set **Communication Channel** as **Ethernet**, **Wi-Fi**, or **Cellular** by dragging the slider to enable the function.

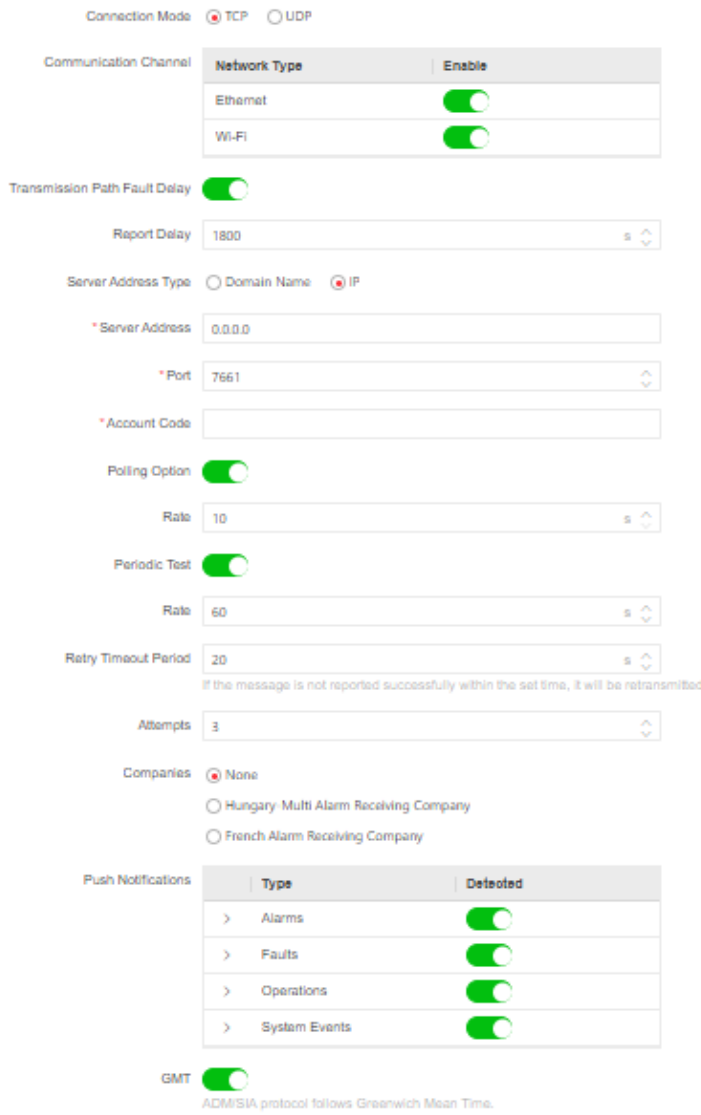


Figure 1-6 SIA-DCS or ADM-CID

Select the **Server Address Type** as **IP** or **Domain Name**, and enter the IP/domain name, server address, port number, account code, retry timeout period, attempts, companies, push notifications.

Transmission Path Fault Delay

After enabling, you can set the delay time, setting how long to send the fault to the ARC to ensure the connection.

Polling Option

After enabling, you can set the rate, setting how often to send the option to the ARC to ensure the connection.

Periodic Test

After setting the monitoring station ping interval, the device will send a test event to the platform at the intervals.

GMT

ADM/SIA protocol follows Greenwich Mean Time.

- ***SIA-DCS** or ***ADM-CID**.

Set **Connection Mode** as **TCP** or **UDP**.

Set **Communication Channel** as **Ethernet**, **Wi-Fi**, or **Cellular** by dragging the slider to enable the function.

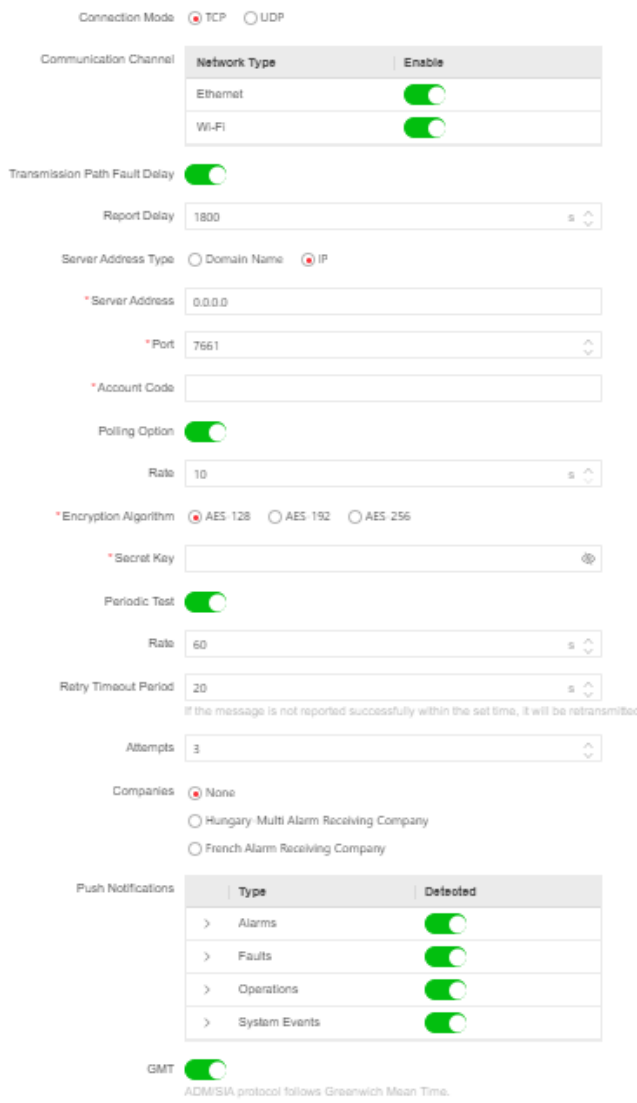


Figure 1-7 *SIA-DCS or *ADM-CID

Select the **Server Address Type** as **IP** or **Domain Name**, and enter the IP/domain name, server address, port number, account code, encryption algorithm, secret key, retry timeout period, attempts, companies, push notifications.

Transmission Path Fault Delay

After enabling, you can set the delay time, setting how long to send the fault to the ARC to ensure the connection.

Polling Option

After enabling, you can set the rate, setting how often to send the option to the ARC to ensure the connection.

Periodic Test

After setting the monitoring station ping interval, the device will send a test event to the platform at the intervals.

GMT

ADM/SIA protocol follows Greenwich Mean Time.

- **CSV-IP**

Select the **Address Type** as **IP** or **Domain Name**, and enter the IP/domain name, server address, port number, account code, retry timeout period , attempts, and authentication information.

Transmission Path Fault Delay

After enabling, you can set the delay time, setting how long to send the fault to the ARC to ensure the connection.

Periodic Test

After setting the monitoring station ping interval, the device will send a test event to the platform at the intervals.

Authentication

After enabling, you can set the user name and password.

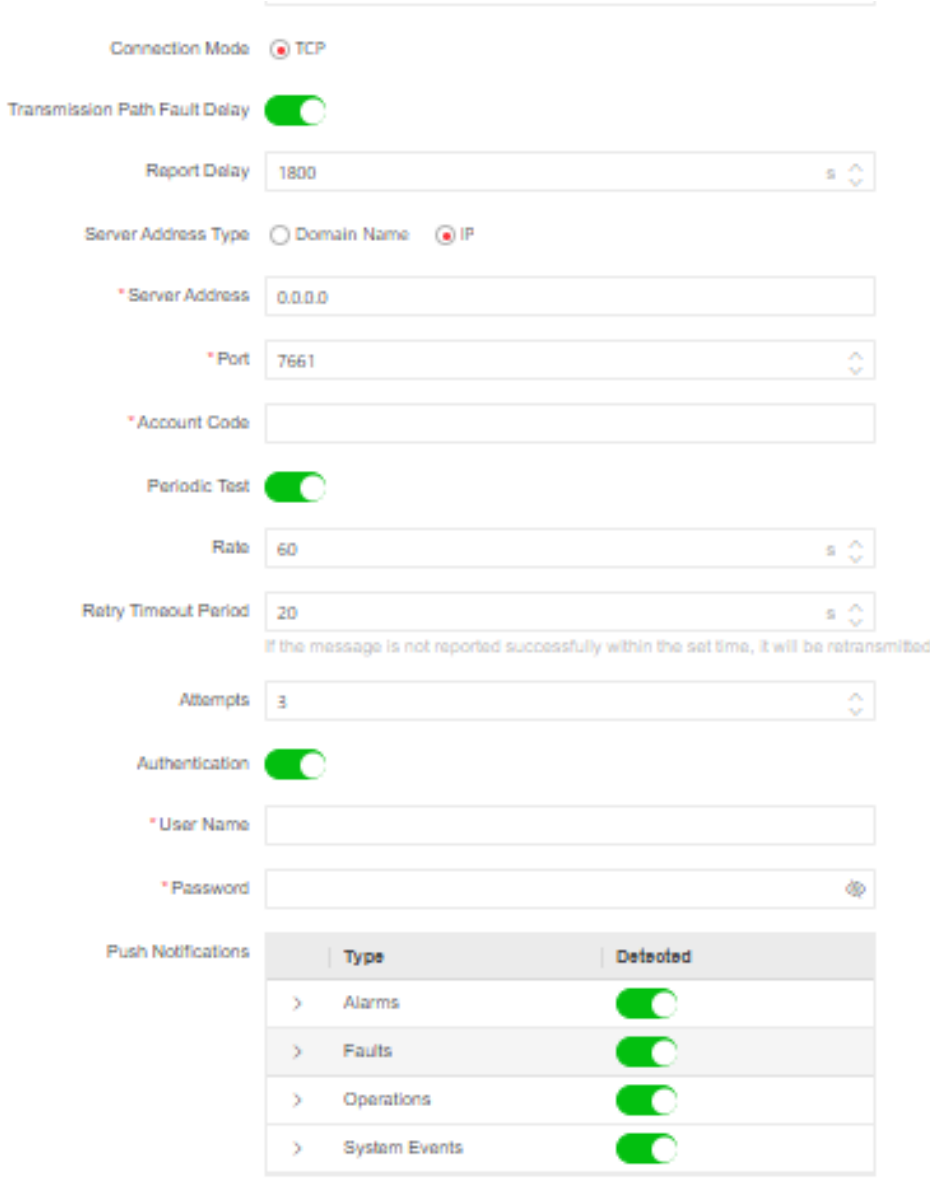


Figure 1-8 CSV-IP

- **OTAP**

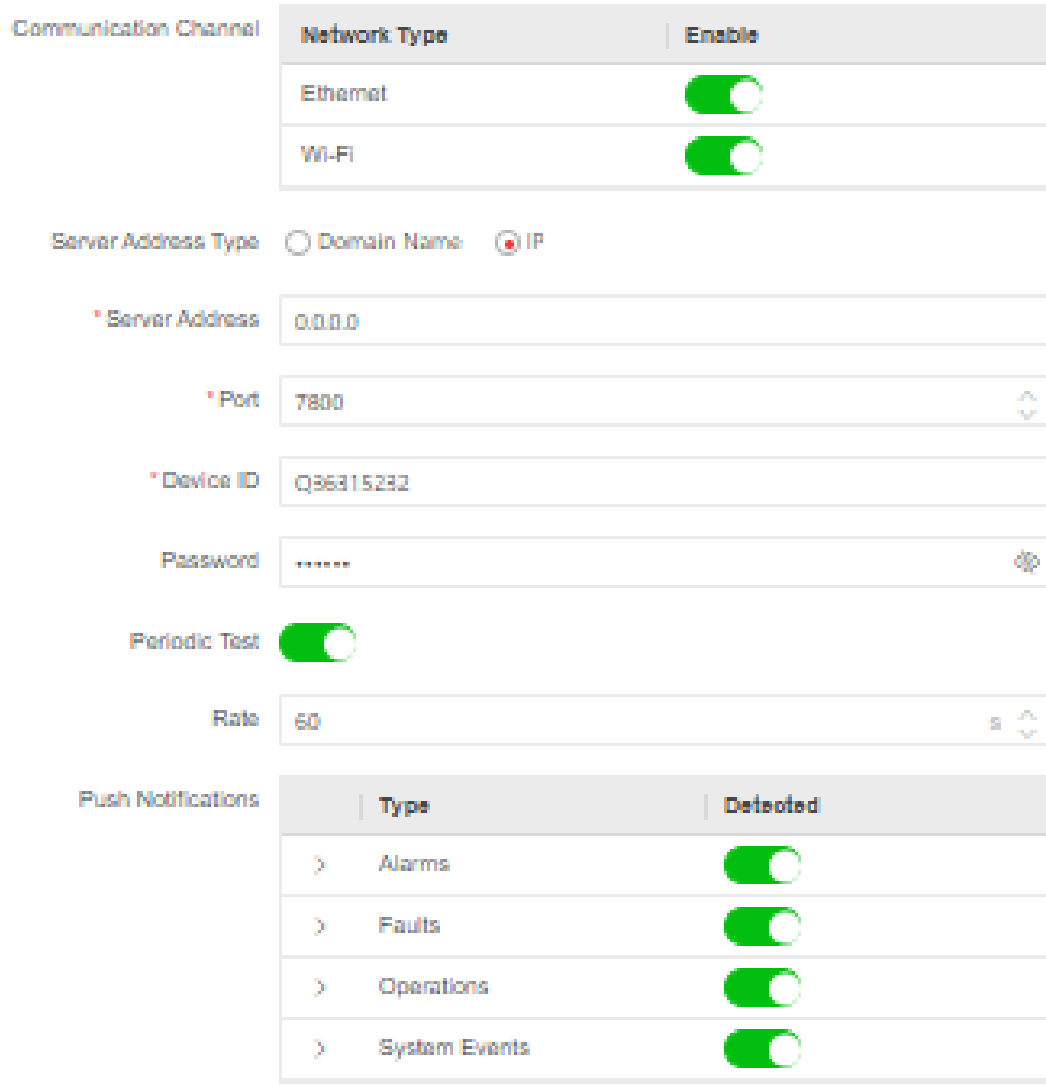


Figure 1-9 OTAP

Set **Communication Channel** as **Ethernet**, **Wi-Fi**, or **Cellular** by dragging the slider to enable the function.

Select the **Address Type** as **IP** or **Domain Name**, and enter the IP/domain name, server address, port number, device ID, password and push notifications.

Periodic Test

After setting the monitoring station ping interval, the device will send a test event to the platform at the intervals.

- **ISUP**

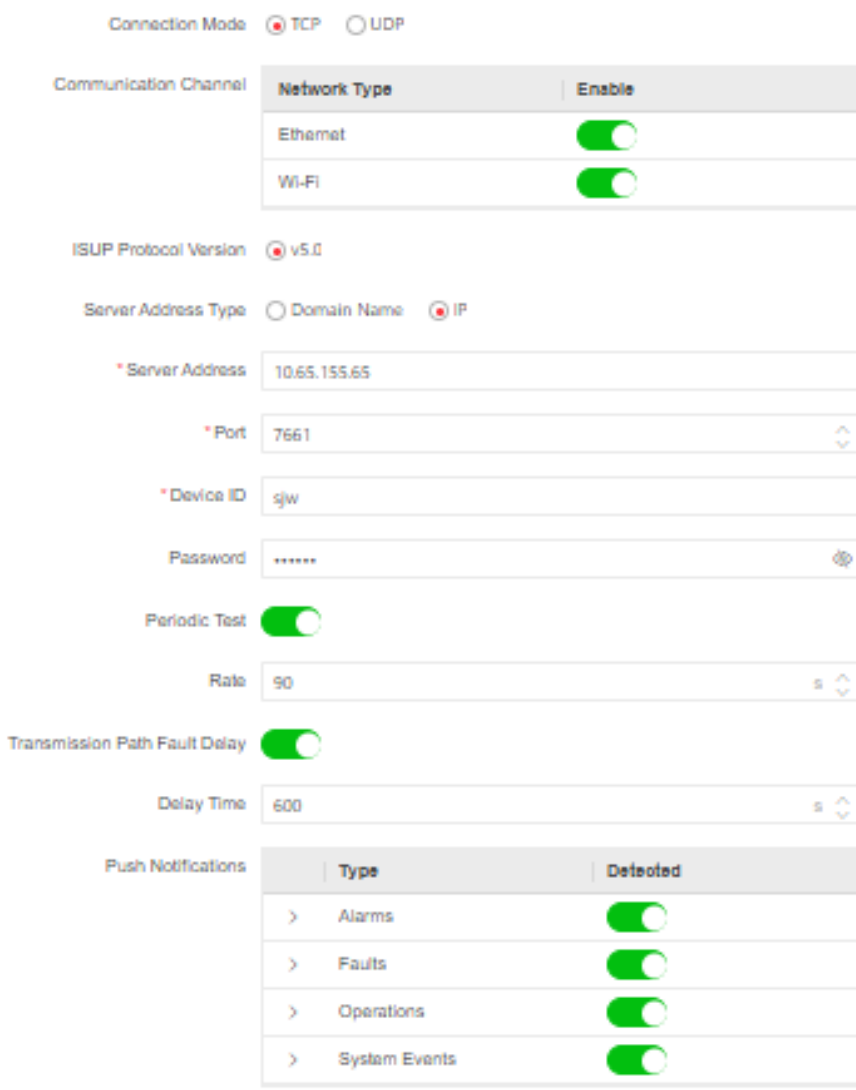


Figure 1-10 ISUP

Set **Communication Channel** as **Ethernet**, **Wi-Fi**, or **Cellular** by dragging the slider to enable the function.

Select the **Address Type** as **IP** or **Domain Name**, and enter the IP/domain name, server address, port number, device ID, password, and push notifications.

Periodic Test

After setting the monitoring station ping interval, the device will send a test event to the platform at the intervals.

Transmission Path Fault Delay

After enabling, you can set the delay time, setting how long to send the fault to the ARC to ensure the connection.

- Set **Connection Type** as **Serial Port**.

  Set **Protocol Type** as **FSK**, **RDS**, and **IDS**.

  Periodic Test

  After setting the monitoring station ping interval, the device will send a test event to the platform at the intervals.

5. Click **Save**.

Phone Call and SMS

Set audio and SMS.

Steps

1. Click **Configuration → Alarm Communication → Phone Call and SMS** to enter the page.

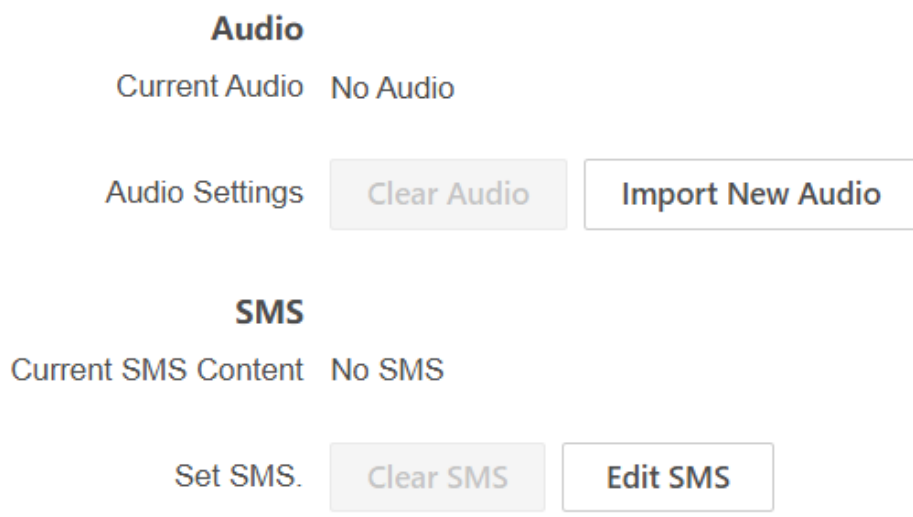


Figure 1-11 Custom Content

2. Click **Import New Audio →** 🗀 to import new audio.

Note

Import WAV audio files with size less than 512 kb and frequency less than 8 kHz. After importing, the original audio will be overwritten, and the push messages consist of custom audio and alarm contents.

3. Click **Edit SMS** to set SMS.

Note

You can set notifications in Message Setting page.

Notification by Email

Steps

1. Click **Configuration → Alarm Communication → Notification by Email** to enter the page.

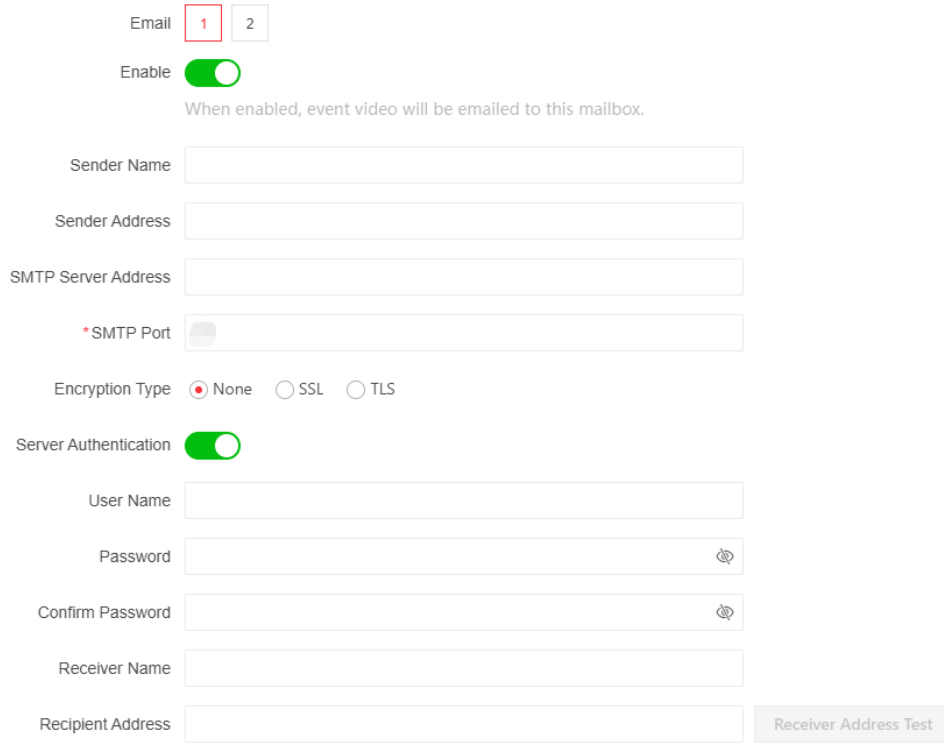


Figure 1-12 Set Email

2. Enable Email 1.
3. Enter the sender name, sender email address, SMTP server address, SMTP port.

Note

It is recommended to use Gmail and Hotmail for sending mails. Only if the zone is linked with a network camera, the alarm email will be attached with alarm video.

4. Select the encryption type as **None**, **SSL** or **TLS**.
5. Enable **Server Authentication**.
6. Enter user name, password, confirm password, receiver name and recipient address. Click **Test Receiver Email Address** to test whether the email address is correct.
7. Tap Save.
8. **Optional:** Configure **Email 2** in the same order. You can choose whether to set email 2 as a backup mailbox.

Note

Video and picture reviews will be sent to both mailboxes. If Email 2 is set as a backup mailbox, the system will push emails to Email 2 only if Email 1 fails to receive.

Set FTP to Save Video

You can configure the FTP server to save alarm video.

Steps

1. Click **Configuration → Alarm Communication → FTP** to enter the page.

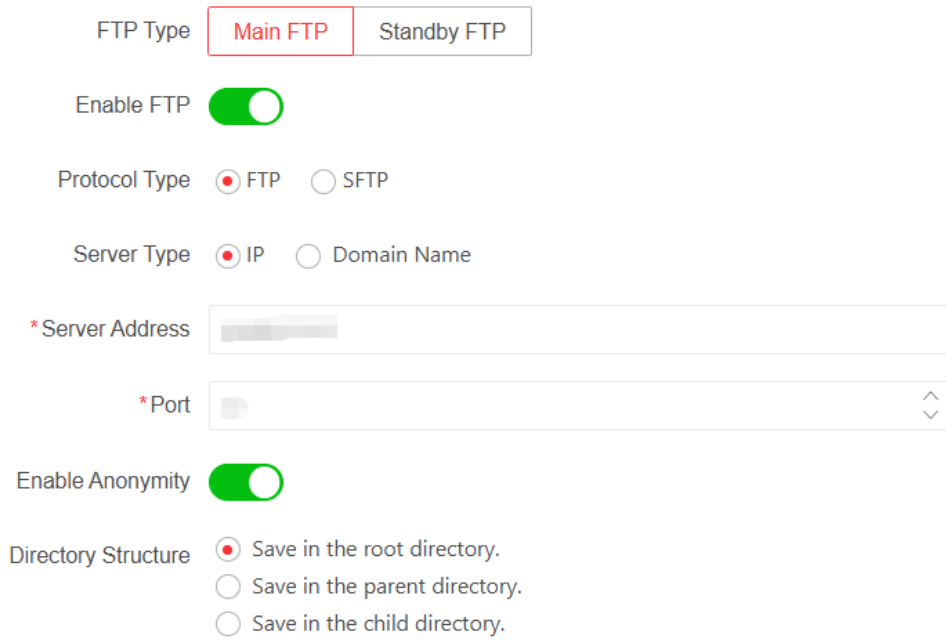


Figure 1-13 FTP Settings

2. Select **FTP Type** as **Main FTP** or **Standby FTP**.
3. Drag the slider to enable FTP.
4. Select protocol type as **FTP** or **SFTP**.
5. Select address type as **IP** or **Domain Name**.
6. Enter the server address or domain name, and port number.
7. Enter user name, password and confirm password.
8. **Optional:** Drag the slider to enable anonymity.

   Anonymity

   The FTP user should have the permission to upload pictures. If the FTP server supports picture uploading by anonymous users, you can enable Anonymity to hide your device information during uploading. Otherwise, you should enter user information.

9. Set **Directory Structure** as the saving path of snapshots in the FTP server.
10. Click **Save**.

1.1.3 Device Management

You can set the area parameters on the page.

Device Management

Steps

1. Click **Area** to enter the page.
2. Click + on the right of the page to enter the Add Area page.
   - **BUS Device**

     Click **Scan to Add** to select bus for scanning registration. Click **OK** to add device.

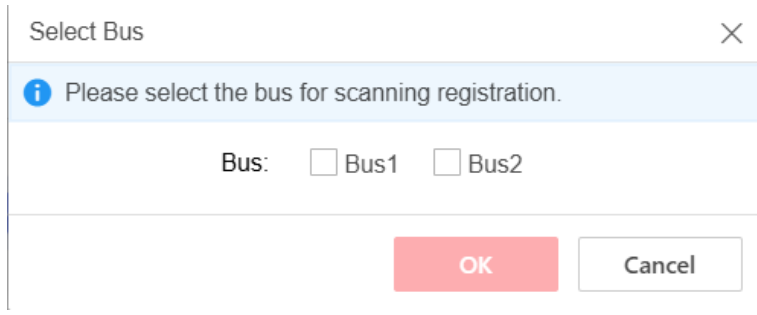


Figure 1-14 Select Bus

   - **Wired Device**

     Click **Manually Add** to select connection method. Set device type, main device type and channel.

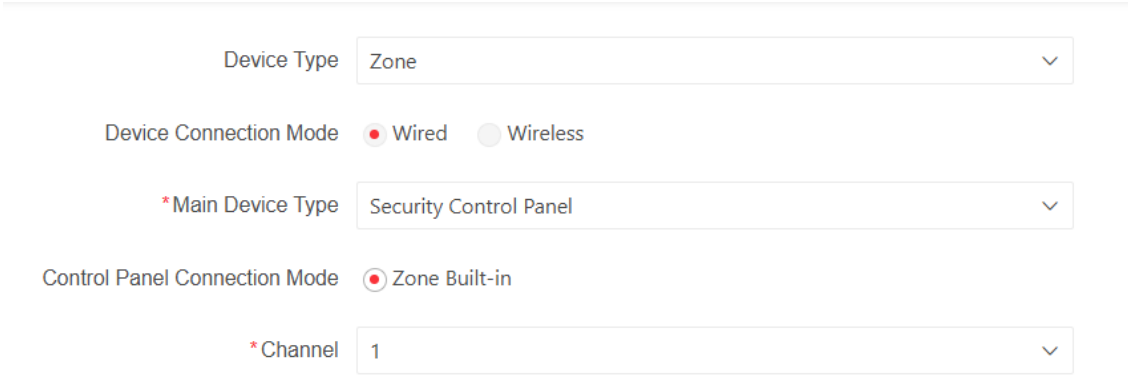


Figure 1-15 Select Connection Method

Click **Next** to set device basic configuration and detector parameters.

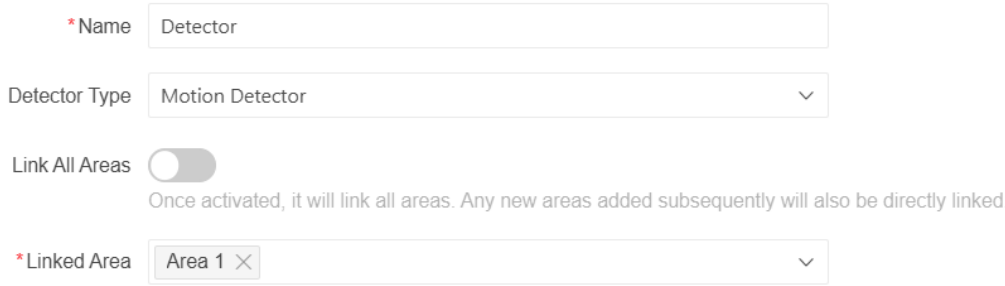


Figure 1-16 Basic Configuration

Link All Areas

Once activated, it will link all areas. Any new areas added subsequently will also be directly linked.

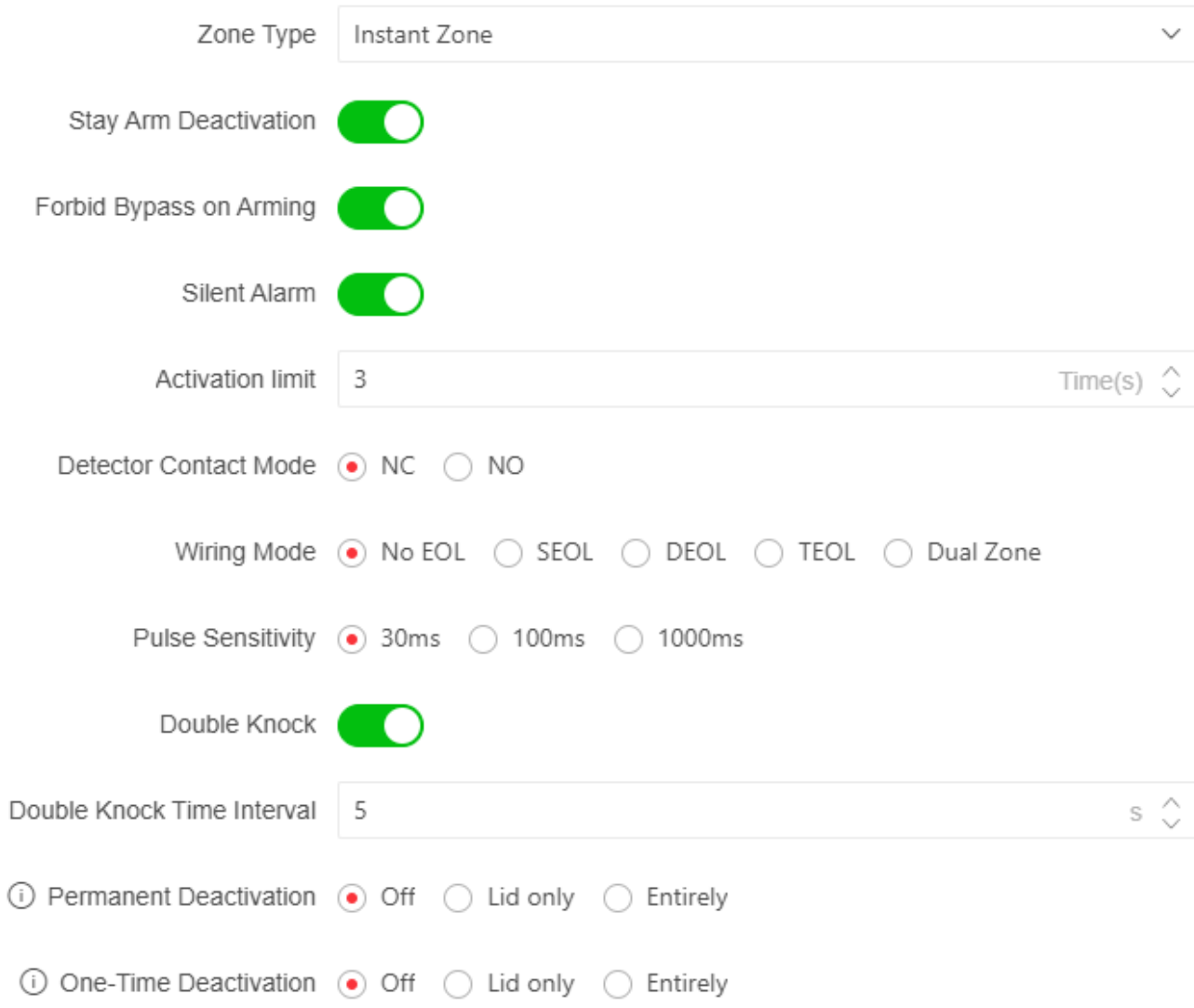


Figure 1-17 Detector Parameters

Stay Arm Deactivation

The zone will be automatically bypassed in stay arming.

Forbid Bypass on Arming

After enabled, you cannot bypass zones when arming.

Silent Alarm

After enabled, when an alarm is triggered, only the report will be uploaded and no sound is emitted.

Double Knock

After enabled, the time interval can be set. If the same detector is triggered twice or continuously in a period of time, the alarm will be triggered.

Click **Save**.

- **Wireless Device**

Enroll in Batch

Click **Enroll in Batch** to select a receiving device to add devices.

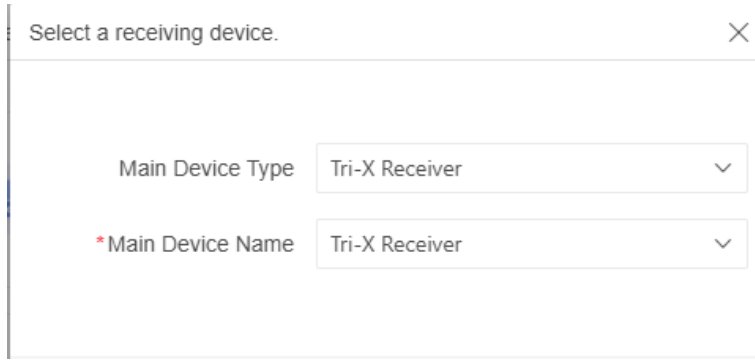


Figure 1-18 Select Receiving Device

Manually Add

Click **Manually Add** to set connection mode and device parameters.

- **Network Camera/IP Device**

SADP Scanning

Click **SADP Scanning** to scan all network cameras in the same LAN. A list will pop up after scanning. You can directly check to add cameras in the list.

Manually Add

Click **Manually Add** to add cameras. And set connection method and device parameters.

3. Click **Save**.
4. Click **Edit Linkage** to edit linkages of the area.
5. After the area is added, you can click , , , , to stay arm, away arm, disarm, delete or refresh the area.

Advanced Settings

Unlock advanced control to seamlessly orchestrate automated routines, schedules, and group actions to realize optimal system management.

Click **Click to Add** to add advanced fuction.

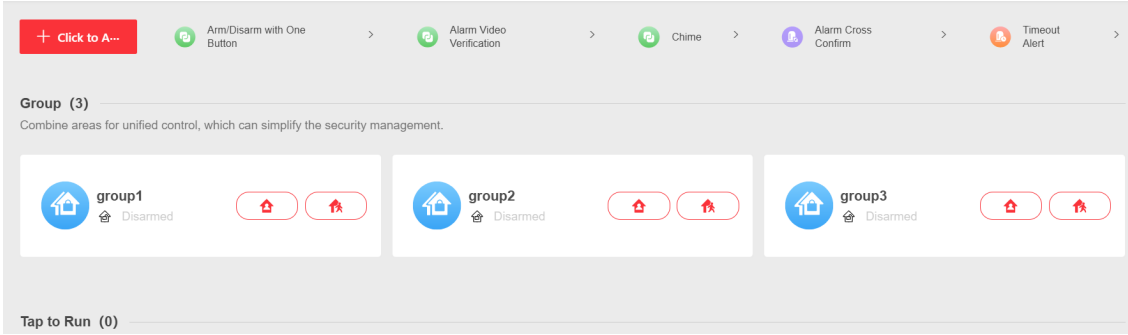


Figure 1-19 Advanced Settings

Group

Set name, linked area to add group arm/disarm function.

Tap to Run

Set name and execute specified actions to add execution scene.

Automation

Set name, trigger spurce and execution devices to add device linkage scene.

Schedule

Set name, time point and execution devices to add scheduled scene.

Note

Enable Holiday Exception function and the zone will not be armed/disarmed in the holiday. You should set the holiday schedule after enabling. Up to 12 holiday groups can be set.

After the function is added, you can click , to set or delete the function.

1.1.4 Permission Management

Add/Edit/Delete User

Administrator can add user to the security control panel, edit the user information, or delete the user from the security control panel. You can also assign different permissions to the new user.

Steps

1. Click **Configuration → User Management** to enter the User Management page.

Note

- The default user name of admin account is **admin**. The password is the activation password.
- The default password of the **installer** is **installer12345**, and the default password of the **maintenance** (for Italian, the user name is **costruttore**) is **hik12345**. These password will have to be changed when first connected.
- The Italian user name of admin is **admin**.

Table 1-2 User Name of Installer

Language	User Name	Language	User Name
English	installer	Russian	монтажник
Italian	installatore	French	installateur
Polish	instalator	Spanish	instalador
German	errichter	Portuguese	instalador
Turkish	kurulumcu	Czech	technik

2. Click **Add**.
3. Set the new user's information in the pop-up window, including the user name, the user property, and the phone number.

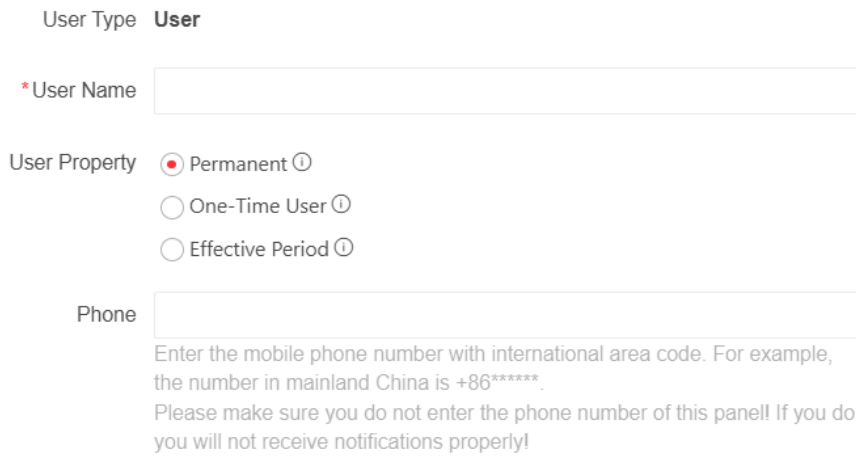


Figure 1-20 Add User Page

4. Set the keypad operation code and duress code (numeric, 8~16 characters).

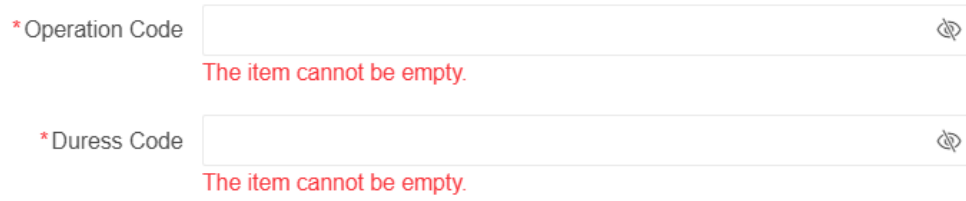


Figure 1-21 Keypad Configuration

5. Check the check boxes to set the user permission.
   The user can only operate the assigned permissions.
6. Click **Next** to enter message settings page.

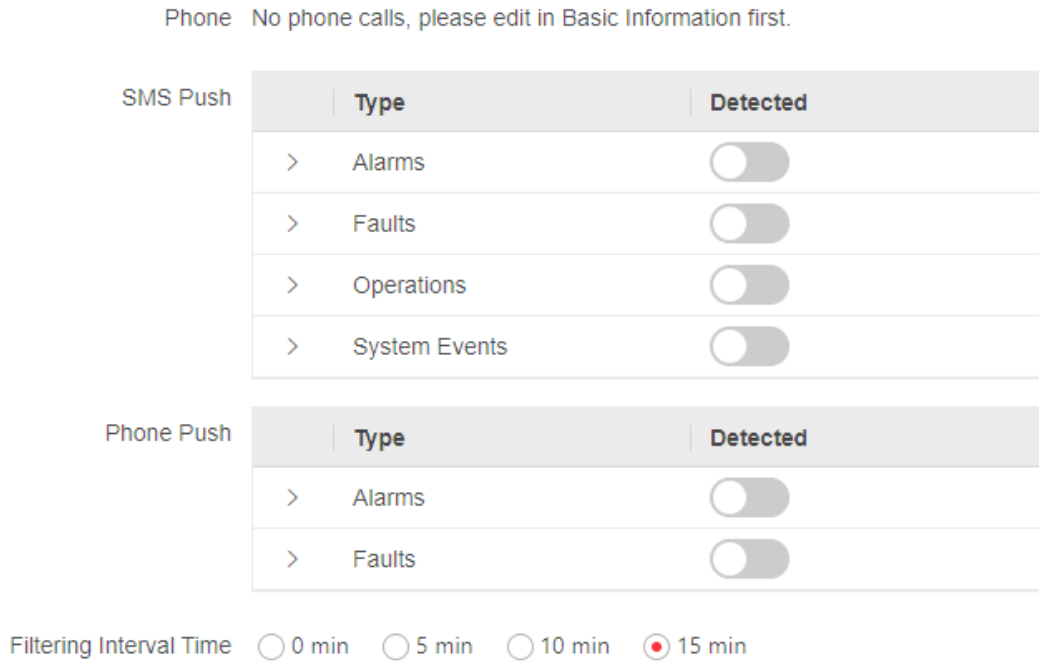


Figure 1-22 Message Settings

7. Set SMS push, phone push, and filtering interval time.
   Filtering Interval Time
   The interval between calls for the same alarm.
8. **Optional:** Select an user and click **Edit** and you can edit the user's information and permission.
9. **Optional:** Delete a single user or check multiple users and click **Delete** to delete users in batch.

Note

The admin, the installer and the maintenance cannot be deleted.

Add/Edit/Delete Keyfob

You can add keyfob to the security control panel and you can control the security control panel via the keyfob. You can also edit the keyfob information or delete the keyfob from the security control panel.

Steps

1. Click **Configuration** → **User Management** → ✎ → **Keyfob&Tag** to enter the Keyfob Management page.

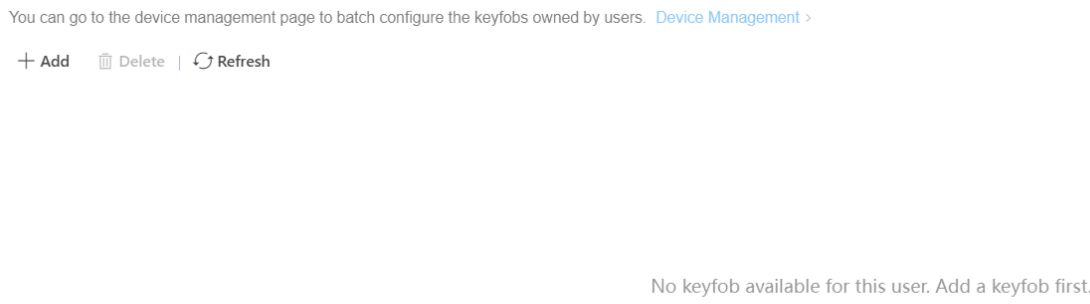


Figure 1-23 Keyfob Management

2. Click **Add** and press any key on the keyfob.
3. Set the keyfob parameters.

   Silence the Panic Alarm

   When enabled, the panic alarm of the wireless keypad will have no linkage prompt.
4. Click **OK**.
5. **Optional:** Click ✎ to edit the keyfob information.
6. **Optional:** Click 🗑 to delete the keyfob.

Add/Edit/Delete Tag (Card)

You can add tag to the security control panel and you can use the tag(card) to arm/disarm the zone. You can also edit the tag information or delete the tag from the security control panel.

Steps

1. Click **Configuration** → **User Management** → ✎ → **Keyfob&Tag** to enter the Tag Management page.

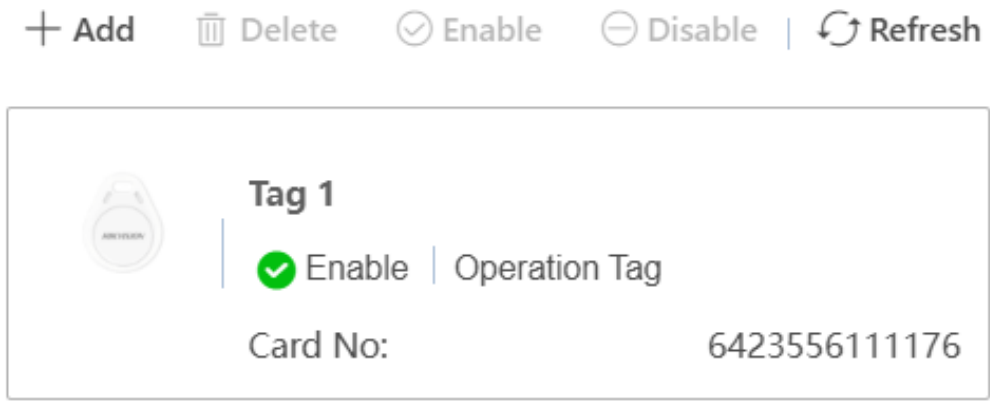


Figure 1-24 Tag Management

2. Click **Add** to enter the adding page.
3. Set tag parameters.
4. Click **OK** and the card(tag) information will be displayed in the list.

Note

The card supports at least 20-thousand serial numbers.

5. **Optional:** Click and you can change the card(tag) settings, including tage(card) type, related net user, linked area, etc.
6. **Optional:** Click to delete the card(tag).

1.1.5 Maintenance

Restart

Click **Maintenance and Security → Maintenance → Restart** to enter the Restart page.

Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security → Maintenance → Control Panel Upgrade →** to upgrade file.

Click **Maintenance and Security → Maintenance → Detector & Peripheral Upgrade** to enter the detector and peripheral upgrade page.

Set upgrade type and peripheral, then click to upgrade file.

Manufacturer PIN

Click **Get Manufacturer PIN** , you can get the pin code.

Backup and Reset

Click **System and Maintenance → Maintenance → Backup and Reset** .

Device Parameters

Click **Export** to export the device parameters.

Note

You can import the exported device parameters to another device.

Default

The device will restore to the default settings, except for the device IP address and the user information.

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Import Config File

Click and select the file to import. Click **Import** to start importing configuration file.

Search Log

Click **System and Maintenance → Maintenance → Event Log** .

Set primary event, secondary event, and time, click **Search**, then the results will be displayed on the below.

Click **System and Maintenance → Maintenance → Security Audit Log** .

Enable log upload server, and set log server IP, log server port. Click to start import CA certificate.

Walk Test

Steps

1. Click **System and Maintenance → Maintenance → Walk Test** to test the whether the device works properly or not. Slide Enable. Trigger the detector in each zone.

   Note

   Only when all the detectors are without fault, you can enter the mode TEST mode.

Device Debugging

You can set device debugging parameters.

Steps

1. Click **System and Maintenance → Maintenance → Device Debugging** .
2. You can set the following parameters.

Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Debug Log

You can click **Start** to collect logs.

Tamper Alarm on HPP Login

If enabled, when logging in to HPP, the system will give an alarm when the device tamper is triggered.

Capture Network Packet

You can set the **Packet Capture Duration**, **Packet Capture API**, **Filter Condition**, and click **Start Capturing Packet** to capture.

Installation Mode

Steps

1. Click **System and Maintenance → Maintenance → Installation Mode** .

Note

- After entering **Installation Mode**, the tampering function is automatically bypassed.
- After enabling, it defaults to stay for 12 hours.

1.1.6 System Settings

Device infomration

You can set device name and view model, serial number, versions of device.

Click **Configuration → System → System Settings** to enter the page.

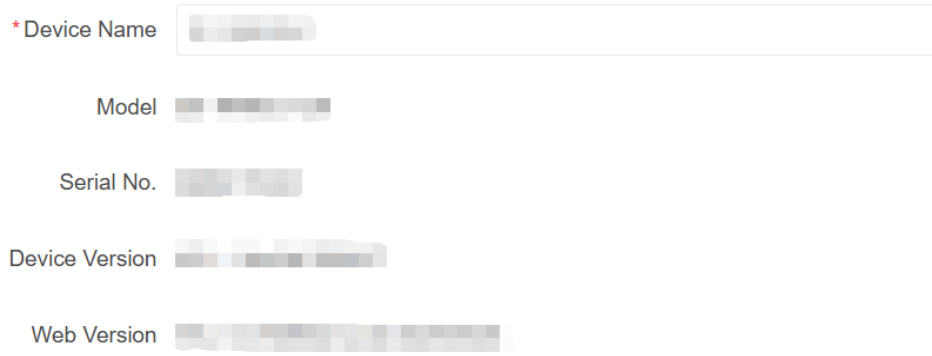


Figure 1-25 Device Information

You can set the device name.

You can view device model, device serial No., device version, web version.

Time Settings

You can set the device time zone, synchronize device time, and set the DST time. The device supports time synchronization via Hik-Connect server.

Click **Configuration → System → System Settings → Time Settings** to enter the page.

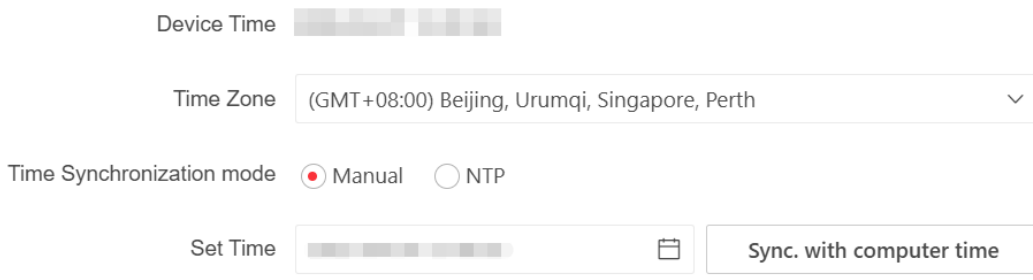


Figure 1-26 Time Settings

Time Zone

Select a time zone from the drop-down list.

Time Synchronization mode

NTP

Set the server address, NTP port and interval. The system will automatically synchronize the time with the server.

Manual

Set the system time manually or click **Sync. with Computer Time** to synchronize the device time with the computer time.

DST

Set the start, end date and bias time for daylight saving time.

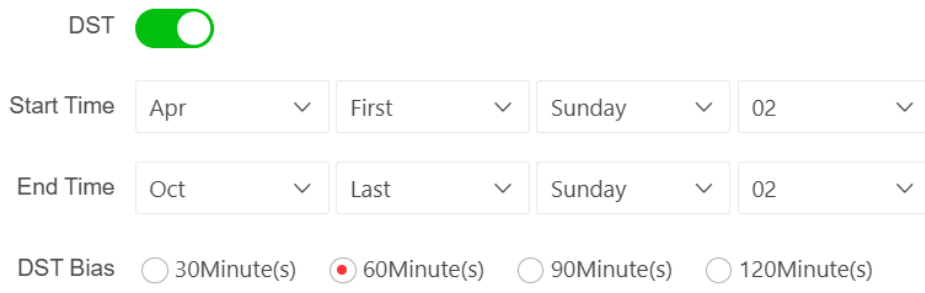


Figure 1-27 DST Settings

Click **Save**.

Panel Options

You can set system alarm duration.

Click **Configuration → System → System Settings → Panel Options** to enter the page.

Enter the alarm duration.

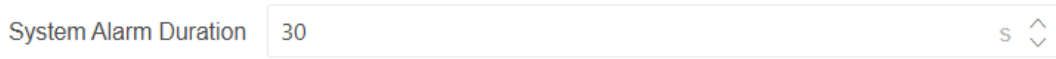


Figure 1-28 Set System Alarm Duration

System Service

Steps

1. Click **Configuration → System → Service** to enter the page.

Figure 1-29 System Service

Re-Arm on Restore

The deactivation zone will back to arm if fault is restored.

Audible Tamper Alarm

While enabled, the system will alert with buzzer for the tamper alarm. Regardless of whether it is enabled or not, the tamper alarm will be normally pushed to Cloud (for APP) and ARC.

Jamming Sensitivity Settings

The device will detect RF interference and push messages when the RF interference interferes with communication. You can adjust the detection sensitivity.

Motion Detector Restore Report

Off: No automatic restore.

Immediate After Alarm: Motion detectors automatically restores immediately after the alarm and reports to Cloud (for APP) and ARC.

After Disarm: Motion detectors automatically restores after disarming and reports to Cloud (for APP) and ARC.

Fault Checklist when Arming

Check the faults in the checklist, and you can manually stop arming if fault occurs.

Panel-Server Polling Interval

Set the time interval of heartbeat sending from control panel to the cloud.

Delay of Server Connection Failure

When exceeding the configured time period of the control panel and the server connection, an offline report will be generated.

Panel Fault Check

The fault check here is only for the control panel in the normal status.

The system determines whether to check the faults listed on the page. The system will only check the fault that is selected.

Power Saving Mode

After the energy save mode is enabled and the main power supply is off, Wi-Fi enters low power consumption mode, 4G is turned off, tag reading is invalid, LED is off, and voice prompt is turned off.

PD6662

PD6662 is applicable to the UK market. If this function is enabled, the arming function and alarm logic of the control panel will change.

Panel Lockup Button

All functions of the device will be frozen after it is enabled. This function can only be enabled by users with installer permission.

INCERT

1.1.7 Check Status

After setting the zone, repeater, and other parameters, you can view their status.

Click **Status**. You can view the status of zone, relay, siren, keypad, card reader, battery, and communication.

- Zone: You can view the zone status, alarm status, detector battery capacity, and signal strength.
- Siren: You can view siren status, battery status, and signal strength.
- Relay: You can view relay status, battery status, and signal strength.
- Keypad: You can view keypad status, battery status, and signal strength.
- Card Reader: You can view card reader status, battery status, and signal strength.

- Battery: You can view the battery charge.
- Communication: You can view the wired network status, Wi-Fi status, Wi-Fi signal strength, GPRS/3G/4G network status, used data, and cloud connection status.

1.2 Using the Mobile Client

1.2.1 Download and Login the App

Download the App and login the client before operating the control panel.

Steps

1. Scan the QR code below to download the App.
   - Download Hik-Connect App.

Figure 1-30 App QR Code

   - Download Hik-Partner Pro App.

Figure 1-31 App QR Code

2. Register a new account if it is the first time you use the App.

Note

- For Hik-Partner Pro App, you should register an account on the portal.
  Hik-Partner Pro Portal Websit: ***https://www.hik-partner.com/***
- For details, see the user manual of the App.

3. Run and login the App.

1.2.2 Set-up with Hik-Partner Pro

Use the Hik-Partner Pro APP

The installer can use the Hik-Partner Pro to configure the device, such as activation, device enrollment, etc.

Add Control Panel to the Mobile Client

Add a control panel to the mobile client before other operations.

Before You Start

- The control panel has been activated.
- Download and login Hik-Partner Pro.

Steps

1. Power on the control panel.
2. Create or search a site.
   - Create a site (Personal): Tap **+**, set site name, time zone, location(optional), address(optional). Slide to enable or disable **Sync Time & Time Zone to Device**. Select **Scene**, **Move to Group** and you can add **Remarks**(optional). Finally, tap **OK** to create a site.
   - Create a site (Team): Tap **+**, set site name, time zone, location(optional), address(optional). Slide to enable or disable **Sync Time & Time Zone to Device**. Select **Scene**, and you can add **Remarks**(optional). Finally, tap **OK** to create a site.
   - Search a site: Enter site name in the search area and tap **Search Icon** to search a site.
3. Tap **Add Device**.
   - Tap **Scan QR Code** to enter the Scan QR code page. Scan the QR code on the control panel.

     Note

     Normally, the QR code is printed on the label stuck on the back cover of the control panel.
   - Tap **Add Device Manually** to enter the Add Device page. Enter the device serial No. and choose a site to add into.
   - Tap **Synchronize Devices from Hik-Connect**. Then you can log into **Hik-Connect**to synchronize devices to **Hik-Partner Pro**.
4. Activate the **Device**.

Add Peripheral to the Control Panel

Before You Start

Make sure the control panel is disarmed.

Steps

1. In the site, tap the security control panel.
2. Tap **Device → Add Device** .
3. Select adding type.
   - Tap **Scan QR Code** to enter the Scan QR code page. Scan the QR code on the control panel.

     Note

     The QR code is usually on the back cover of the device.
   - Tap **Batch Add** to enter the enrollment mode. Powered on peripherals nearby will be enrolled to the control panel automatically. Tap **Finish**.

Main Page

You can view faults, arm and disarm areas, view device status, etc.

Enter a site. On the device list page, tap the control panel and then log in to the device (if required) to enter the device main page.

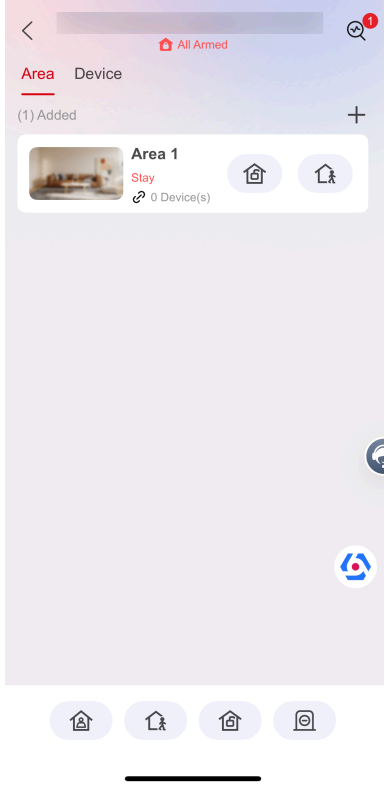


Figure 1-32 Device Main page

View Faults

Tap to view faults.

Area Management

Tap **+** to add an area.

Tap **Area** to enter the area management page. Refer to for details.

Arm/Disarm the Area

Arm or disarm the area manually as you desired.

On the device list page, tap the control panel and then log in to the device (if required) to enter the Area page.

Operations for a Single Area

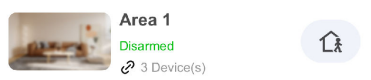


Figure 1-33 Single Area

Arming

Tap to arm a single area when there are people in the detection area. When all the people in the detection area leave, tap to arm all zones in all areas after the defined dwell time.

Operations for Multiple Areas

Figure 1-34 Multiple Area Key

Arming

Tap to arm a single area when there are people in the detection area. When all the people in the detection area leave, tap to arm all zones in all areas after the defined dwell time.

Disarming

Tap to disarm all areas. In Disarm mode, all the zones of all areas will not trigger alarm, no matter alarm events happen or not.

Silent Alarm

Tap to silent alarms for all areas.

Zone Management

Steps

1. Enter a site. On the device list page, tap the control panel and then log in to the device (if required) to enter the device main page.
2. On the main page, Tap **Device** to view linked zones.
3. Tap **Add Device** to add a new zone.

4. Tap an added device to enter the management page. You can view device status (e.g. temperature, battery status, single strength, etc.).
5. Tap ⚙ on the upper right corner to enter the device settings page.
6. Select a zone type. You can view the configurable zone types for various detectors through Detector Zone Types.

Instant Zone

This Zone type will immediately trigger an alarm event when armed.

Delay Zone

Exit Delay Time

Exit Delay provides you time to leave through the zone without alarm. You should confirm faults first, and then the zone is in arming process. If the delay zone is triggered within the exit delay time but it restores before the time ends, the alarm will not be triggered and the zone will be armed.

Entry Delay Time

Entry Delay provides you time to enter the zone to disarm the system without alarm.

After triggering, if the zone is not disarmed or silenced before the entry delay time ends, the zone will alarm.

Stay Arm Delay Time

Stay arming uses Stay Arm Delay Time to count down.

The system gives Entry/Exit delay time when it is armed or reentered. It is usually used in entrance/exit route (e.g. front door/main entrance), which is a key route to arm/disarm via operating keypad for users.

Note

Ensure that timer is no longer than 45 seconds in order to comply with EN50131-1.

Panic Zone

24-hour active zone, whether armed or not. Report panic alarm after triggering. It is usually used in the sites equipped with panic button, smoke detector and glass-break detector.

Medical Alarm

24-hour active zone, whether armed or not. Report medical alarm after triggering.

Fire Zone

24-hour active zone, whether armed or not. Report fire alarm after triggering.

Gas Zone

24-hour active zone, whether armed or not. Report gas alarm after triggering.

Disabled

Zone disabled ignoring any alarm event. It is usually used to disable faulty detectors.

24-hour Zone

The zone activates all the time with sound/light output when alarm occurs, whether it is armed or not. It is usually used in fire hazardous areas equipped with smoke detectors and temperature sensors.

Timeout Zone

The zone activates all the time. When this zone has been triggered or restored and exceeds the set time, an alarm will be generated.

It can be used in places equipped with magnetic contacts that require access but for only a short period (e.g., fire hydrant box's door or another external security box door).

Not-Triggered Zone Alarm

If the zone is not triggered for the set time, it will alarm.

Alarm on Zone Activated

If the zone is triggered for the set time, it will alarm.

Retry Time Period

Set the timeout period.

7. Enable other parameters according to your actual needs.

Note

The supported functions vary depending on the zone types. Refer to the actual zone to set the function.

Arm Mode

If the zone is a public zone (the zone belongs to more than one areas), you can set arm mode.

- When all linked areas are armed, the zone will arm. When any of linked areas is disarmed, the zone will disarm.
- When any of the linked areas is armed, the zone will arm. When all linked areas are disarmed, the zone will disarm. When the zone is in alarm, the disarmed areas linked with the zone cannot be armed.

Stay Arm Bypass

The zone will be automatically bypassed in stay arming.

Cross Zone

PD6662 is not enabled

You need to set the combined time interval.

When the first zone is triggered, the system will start timing after the zone is restored. If the second zone is triggered within the set time, both zones will give alarms. Otherwise, no alarm will be triggered.

If the first zone is not be restored, both zones will give alarms when the second zone is triggered, regardless of whether the set time has elapsed.

PD6662 is enabled

You need to set the combined time interval.

The first zone will give an alarm when triggered. If the first zone is not restored and the second zone is triggered, the system will report the alarm confirmation.

If the first zone is restored, the system will start timing. If the second zone is triggered within the set time, the system will report the alarm confirmation.

If the first zone is restored, the system will start timing. If the second zone is not triggered within the set time, no information will be reported.

Forbid Bypass on Arming

After enabled, you cannot bypass zones when arming.

Chime

Enable the doorbell. Usually used for door magnetic detectors.

Silent Alarm

After enabled, when an alarm is triggered, only the report will be uploaded and no sound is emitted.

Double Knock

After enabled, the time interval can be set. If the same detector is triggered twice or continuously in a period of time, the alarm will be triggered.

Sounder Delay Time

The sounder will be triggered immediately (0s) or after the set time.

Final Door Exit

Only magnetic contacts have this option.

After enabling, when the user use keypads or tag readers to arm:

Arm With Faults is enabled

During the arming countdown, if the magnetic contact is triggered and then restored, the arming process will be terminated immediately after restoring, and the arming is completed.

Arm With Faults is disabled

If the magnetic contact is triggered and then restored, the linked area immediately arms the delayed zone.

AM Mode

Alarm Only When ARM

Anti-masking alarm will be triggered only when the zone is armed.

Alarm Only When ARM or DISARM

Anti-masking alarm will be triggered whether the zone is armed or disarmed.

Warning Time Enable

Set the warning time. The warning time countdown will be triggered if the instant zone is triggered during entry delay or the system not be disarmed after entry delay ends. Local alarms are generated during the period, but no messages will be pushed.

Swinger Limit Activations

When the number of times the infrared detector is triggered exceeds the set value, the alarm will no longer be triggered. (Except for anti-masking alarms.).

Dual Zone (Wired Zone)

After enabled, when multi transmitter detects that the entire zone circuit of the local zone and the extended zone is open circuit, both zones trigger lid opened alarms.

8. If required, link a PIRCAM or a camera for the zone.
9. Click **OK**.

Bypass Zone

When the area is armed, you can bypass a particular zone as you desired.

Before You Start

Link a detector to the zone.

Steps

1. On the device list page, tap the control panel and then log in to the device (if required) to enter the Area page.
2. Tap **Device**.
3. Tap a zone in the Device tab.
4. Tap ⚙ to enter the Settings page.
5. Enable **Bypass** and the zone will be in the bypass status.

   The detector in the zone does not detect anything and you will not receive any alarm from the zone.

User Management

The administrator and the installers can manage users. If you are the administrator, you can add, edit, and delete users, and assign different permissions to the newly-added users. If you are a installer, you can only add and delete users.

Steps

Note

There are four types of users for the security control panel, including administrator (or owner), operator, installer (or setter), and manufacturer. Different types of users have different permissions for accessing the functionality of the security control panel.

1. Enter the site, tap the security control panel and then log in to the device (if required) to enter the control panel page.
2. Tap **Next** to invite the user.

Note

The recipient need to accept the invitation.

3. Tap ⚙ → **User Management** → **User** .
4. Tap a user to enter the User Management page.

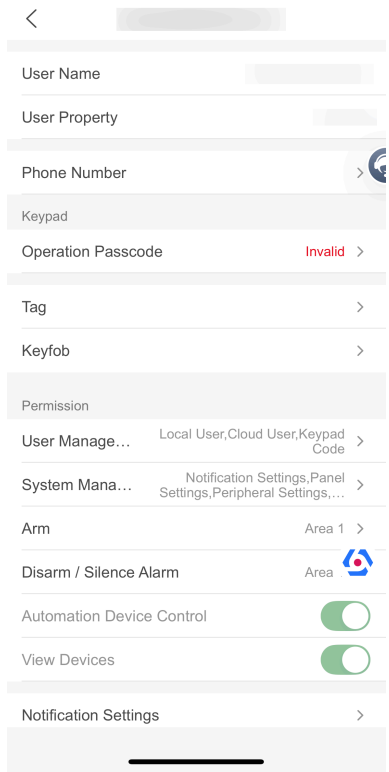


Figure 1-35 Edit User Information

Note

The screenshot here only works as a reference. The real page may vary based on different types of users and devices.

5. **Optional:** Perform the following operations if required.

User Permission	You can tap the target user on the user list and then tap the permission type you want to edit to configure the permissions authorized to the target user. **Note** Only the administrator can do such an operation.

Set Linked Areas	If the target user is a an operator, tap the target user on the user list and then tap **Linked Areas** to set the area linked to the target user. **Note** Only the administrator can do such an operation.
Edit Keypad Password	If the target user is a administrator, an installer, or a manufacturer, you can tap the target user on the user list and then tap **Operation Password** to set the keypad password to the target user.
Notification Settings	If the target user is a administrator, an installer, or a manufacturer, you can tap the target user on the user list and then tap **Notification Settings** to enter the configuration page. Then you can tap on different types of Notifications then slide to enable or disable certain functions.

Note

- Configuration items and user permission will vary according to the user type.
- You can view linked cards/tags and keyfobs of the user and you can tap **Add** at the bottom of the page to add new tags or keyfobs..

Card/Tag Management

After adding cards/tags to the wireless control panel, you can swipe the card/tag to arm or disarm all the detectors added to specific area(s) of the control panel, and silence alarms.

Steps

Note

The tag ID/PIN is a 32 bit long integer, and the variant could be 42949672956.

1. Enter the site, tap the control panel and then log in to the device (if required) to enter the page.
2. Tap **Device** and select a control panel. Tap ⚙ → **User Management** to enter the page.

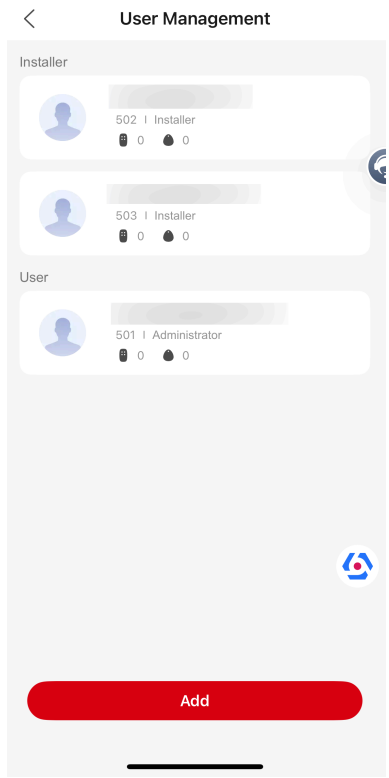


Figure 1-36 User Management

Note

The screenshot here only works as a reference. The real page may vary based on different types of users and devices.

3. Tap a user to enter the configuration page.
4. Tap **+** to add a tag/keyfob.
5. When hearing the voice prompt "Swipe Tag", you should present the tag on the control panel tag presenting area.

   When hearing a beep sound, the tag is recognized.

   The tag will be displayed on the tag list.
6. **Optional:** Tap a tag to enter the configuration page.
7. Tap ✎ to edit the tag name.

Note

- If you log in as an installer, skip this step. Editing tag name is only available to administrator.
- The name should contain 1 to 32 characters.

8. Slide **Enable Tag**.
9. Select a linked user.
10. Select the tag type.

Note

Different linked users have different tag permissions.

Operation Tag

You can swipe the tag to arm or disarm.

Patrol Tag

When you swipe the tag, the system will upload a record.

11. **Optional:** Tap **Delete** to delete the tag.

Device Information

You can change language and select time zone.

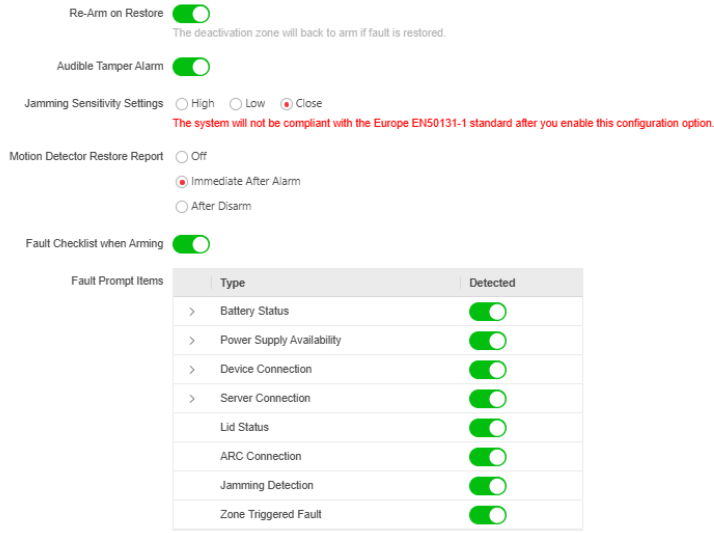
Steps

1. Enter the site. On the device list page, tap the control panel and then log in to the device (if required) to enter the page.
2. Tap **Device** and select a control panel. Tap ⚙ → **System Settings** to enter the page.
3. Select device language and time zone.

System Service

Steps

1. Click **Configuration** → **System** → **Service** to enter the page.



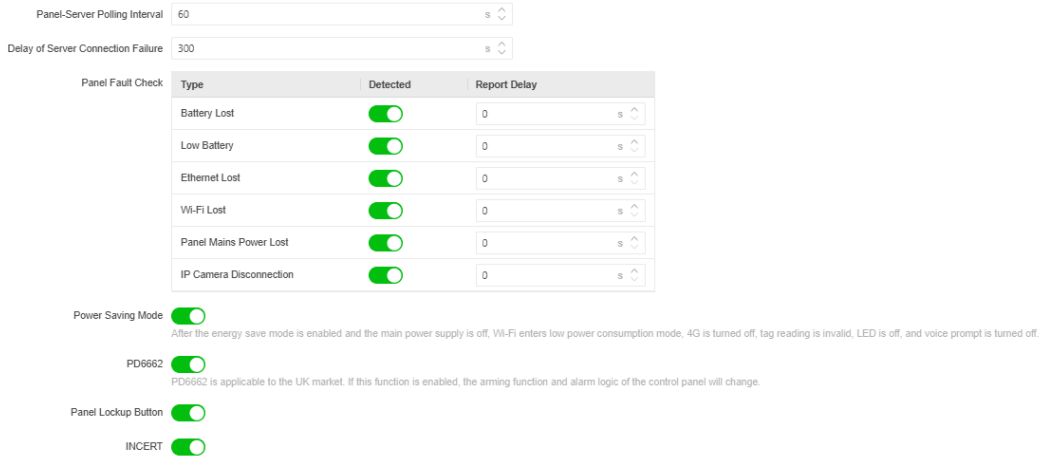


Figure 1-38 System Service

Re-Arm on Restore

The deactivation zone will back to arm if fault is restored.

Audible Tamper Alarm

While enabled, the system will alert with buzzer for the tamper alarm. Regardless of whether it is enabled or not, the tamper alarm will be normally pushed to Cloud (for APP) and ARC.

Jamming Sensitivity Settings

The device will detect RF interference and push messages when the RF interference interferes with communication. You can adjust the detection sensitivity.

Motion Detector Restore Report

Off: No automatic restore.

Immediate After Alarm: Motion detectors automatically restores immediately after the alarm and reports to Cloud (for APP) and ARC.

After Disarm: Motion detectors automatically restores after disarming and reports to Cloud (for APP) and ARC.

Fault Checklist when Arming

Check the faults in the checklist, and you can manually stop arming if fault occurs.

Panel-Server Polling Interval

Set the time interval of heartbeat sending from control panel to the cloud.

Delay of Server Connection Failure

When exceeding the configured time period of the control panel and the server connection, an offline report will be generated.

Panel Fault Check

The fault check here is only for the control panel in the normal status.

The system determines whether to check the faults listed on the page. The system will only check the fault that is selected.

Power Saving Mode

After the energy save mode is enabled and the main power supply is off, Wi-Fi enters low power consumption mode, 4G is turned off, tag reading is invalid, LED is off, and voice prompt is turned off.

PD6662

PD6662 is applicable to the UK market. If this function is enabled, the arming function and alarm logic of the control panel will change.

Panel Lockup Button

All functions of the device will be frozen after it is enabled. This function can only be enabled by users with installer permission.

INCERT

Panel Fault Check

The fault check here is only for the control panel in the normal status. The system determines whether to check the faults listed on the page. The system will only check the fault that is selected.

Steps

1. Enter the site. On the device list page, tap the control panel and then log in to the device (if required) to enter the page.
2. Tap **Device** and select a control panel. Tap ⚙ → **Service** → **Panel Fault Check** to enter the page.

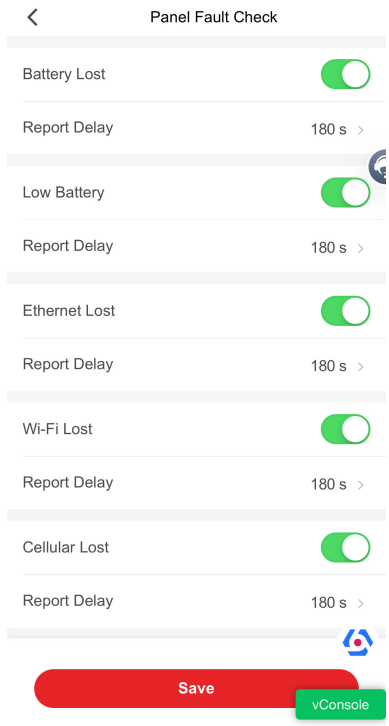


Figure 1-39 Panel Fault Check

Report Delay

If the fault returns to normal within the delay duration, no fault will be reported.

Battery Lost

If the option is enabled, when panel battery is disconnected, the device will upload events.

Wi-Fi Lost

If the option is enabled, when the wireless network is disconnected or with other faults, the alarm will be triggered.

Low Battery

If the option is enabled, when panel battery is in low battery status, the device will upload events.

Ethernet Lost

If the option is enabled, when the wired network is disconnected or with other faults, the alarm will be triggered.

Cellular Lost

If the option is enabled, when the cellular data network is disconnected or with other faults, the alarm will be triggered.

Panel Mains Power Lost

If the option is enabled, an alarm will be triggered when the control panel main supply is disconnected.

Communication

Wired Network

Steps

1. Enter the site. Tap the control panel and then log in to the device (if required).
2. Tap **Device** and select a control panel. Tap ⚙ → **Network Settings** → **Ethernet** to enter the page.
3. Set the parameters.
   - Automatic Settings: Enable **DHCP** and set the HTTP port.
   - Manual Settings: Disabled **DHCP** and set IP Address, Subnet Mask, Gateway Address, DNS Server Address.
4. **Optional:** Set correct DNS server address if the device needs to visit Hik-Connect server via a domain name.
5. Tap **Save**.

Cellular Data Network

Steps

1. Enter the site. Tap the control panel and then log in to the device (if required).
2. Tap **Device** and select a control panel. Tap ⚙ → **Network Setings** → **Cellular** → **SIM1** to enter the page.
3. Slide to enable **Cellular Network**.
4. Set cellular parameters.

   Access Number

   Input the operator dialing number.

   Note

   Only the private network SIM card user needs to enter the access number.

   User Name

   Ask the network carrier and input the user name.

   Password

   Ask the network carrier and input the password.

   APN

   Ask the network carrier to get the APN information and input the APN information.

   MTU

Tap on it to edit. Ask the network carrier to get the MTU information.

PIN

Ask the network carrier to get the PIN.

5. Set data limit parameters. Slide **Enable**.

Traffic Threshold (M)

You can enable the function and set the data threshold every month. If data usage is more than the configured threshold, an alarm will be triggered and uploaded to the alarm center 47 and mobile client.

Used Traffic This Month (M)

The used data will be accumulated and displayed in this text box.

6. Tap **Network Test** to test the cellular network.
7. Tap **Search for USSD** to search for USSD.
8. Tap **Save**.

Alarm Receiving Center (ARC)

You can set the alarm receiving center's parameters and all alarms will be sent to the configured alarm center.

Steps

1. Enter the site. Tap the control panel and then log in to the device (if required).
2. Tap **Device** and select a control panel. Tap ⚙ → **ARC Settings** to enter the page.
3. Slide **Enable**.

Protocol Type

Select the Protocol Type as ADM-CID, ISUP, SIA-DCS, *SIA-DCS, *ADM-CID, CSV-IP, FSK Module or RDC Module to set uploading mode.

Connection Mode

Select a connection mode.

Communication Channel

Set the sending method. You can select to send by Ethernet or Cellular or both.

Server Address Type/Server Address/Port/Account Code

Select the Address Type as IP Address and Domain Name. Enter server address/domain name, port number and account code.

Polling Option

Set the polling rate with the range from 10 to 3888000 seconds. The system will report fault if the time is over the limit. The status of device will be shown as offline.

Periodic Test

After enabling, you can set the time interval, setting how often to send a test event to the ARC to ensure the connection.

Retry Timeout Period

You can set the retry attempts. The device will retry to send for the configured attempts. If the device failed to report for the configured attempts, the device will not continue to report.

Push Notifications

When an alarm is triggered, if you want to send the alarm notification to the mobile phone, you can set the notification push parameters.

Alarm Event Push

The device will push notifications when an alarm is triggered.

Fault Event Push

The device will push notifications when an fault event occurs.

Panel Operation

The device will push notifications when the user operate the control panel.

System Event Push

The device will push notifications when an system event occurs.

GMT

Enable the Greenwich Mean Time.

Device Maintenance

Device Maintenance

You can reboot the device.

Steps

1. Enter the site. Tap the control panel and then log in to the device (if required).
2. Tap **Device** and select a control panel. Tap ⚙ → **Maintenance** to enter the page.

Restart Device

Tap **Restart** and control panel will reboot.

Note

It takes about 3 minutes to reboot the device.

Reset Device

Tap **Reset** to enter the page.

Reset Panel Partly

Restore all data to default settings, except for the device time, user parameters, Ethernet enrolled detector information of zones, and enrolled wireless peripherals information.

Reset Panel to Default

Restore all data to default settings.

Event Log

Select **Primary Event**, **Secondary Event**, **Start Time** and **End Time**. Tap **Search** to view the device logs.

Device Upgrade

Steps

1. Enter the site. Tap the control panel and then log in to the device (if required).
2. Tap **Device** and select a control panel.
3. Upgrade control panel, detector, or peripheral.
   - Upgrade Control Panel: Tap ⚙ → **Maintenance** → **Control Panel Upgrade** . Enter the PIN code and tap **Upgrade** to upgrade the control panel.
   - Upgrade Detector or Peripheral: Tap ⚙ → **Maintenance** → **Detector & Peripheral Upgrade** . Select a detector or peripheral and tap **Upgrade**.

Walk Test

Steps

1. Click **System and Maintenance** → **Maintenance** → **Walk Test** to test the whether the device works properly or not. Slide Enable. Trigger the detector in each zone.

Note

Only when all the detectors are without fault, you can enter the mode TEST mode.

Installation Wizard

You can test the installation environment for devices.

Steps

1. Enter the site. Tap the control panel and then log in to the device (if required).
2. Tap **Device** and select a control panel. Tap ⚙ → **Maintenance** → **Installation Wizard** to enter the page.
3. Tap **+** to enroll more peripherals.
4. Tap 🗑 to delete enrolled peripherals.
5. Tap **Start Installation**, it will test the signal of the control panel.
6. When control panel is ready for installation, tap **Next**. Edit device name and language, and tap **OK**.
7. Tap peripherals in the list, check the installation environment and edit basic information.
8. Tap **Finish** to complete installation test.

View Device User Manual and Video Tutorials

Enter the site. Tap the control panel and then log in to the device (if required).

Tap **Device** and select a control panel. Tap ⚙ → **User Manual** to view the manual.

Use the Hik-Partner Pro Portal

For security control panel, you can perform operations including arming/disarming area, silence alarm, bypassing zone etc., and remotely configure the control panel on the Portal. You can also apply for PIN (required for upgrading the firmware of the control panel) and switch the language of the control panel.

Click **Site** to enter the site list page, and then click the name of a site to enter site details page.

Remotely Operate Control Panel

Click the security control panel to open the operation panel. And you can perform the following operations.

Table 1-3 Operation Description

Operation	Description
Stay Arm a Specific Area	Select the **Area** tab, and then click **Stay Arming** to stay arm the area.
Away Arm a Specific Area	Select the **Area** tab, and then click **Away Arming**.
Disarm a Specific Area	Select the **Area** tab, and then click **Disarm**.
Stay Arm Multiple Areas	Select the **Area** tab, and then select areas and click .
Away Arm Multiple Areas	Select the **Area** tab, and then select areas and click .
Disarm Multiple Areas	Select the **Area** tab, and then select areas and click .
Silence Alarms of Multiple Areas	Select the **Area** tab, and then select areas and click .
Filter Peripheral Device by Area	Select the **Device** tab, and then click and select an area to only display the peripheral devices linked to the selected area, or select **All**

Operation	Description
	to display all the peripheral devices linked to all the areas.
Control Relay	Select the **Device** tab, and then select a wireless output expander to display the sirens linked to it, and then select siren(s) to enable/disable them.
Bypass Zone	Select the **Device** tab, and then select a zone (i.e., detector) and turn on the **Bypass** switch to bypass the zone.

Remotely Configure Control Panel

You can click ⚙ to enter the web page of the security control panel to configure the device.

Note

For details about security control panel configuration, see the user manual of the device.

Apply for a PIN

You can click • • • → 🗎 to open the Apply for a PIN window, and then PIN code will be displayed.

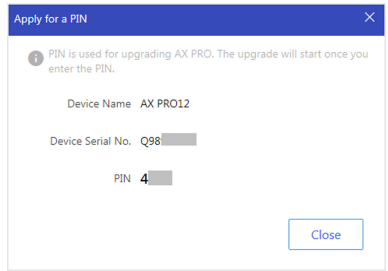


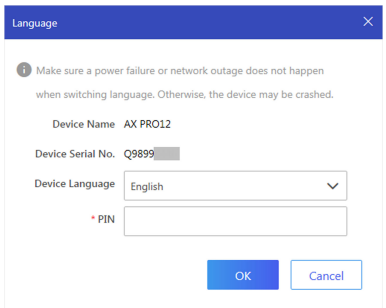
Figure 1-40 Apply for PIN

Switch Language

Note

You should have applied for a PIN.

You can click • • • → ⇆ to open the Language window, and then set the device language and enter the PIN.



Health Monitoring

Steps

1. Enter the Hik-Partner Pro Portal web site, and click **Health Monitoring → Health Status** to enter the page.
2. Select a site.

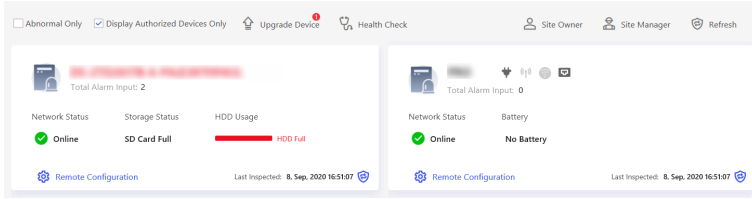


Figure 1-41 Health Monitoring

3. Click **Health Check**, and click **Check Now**.

   When checking is completed, you can view the status and reports of devices. You can also export the report.

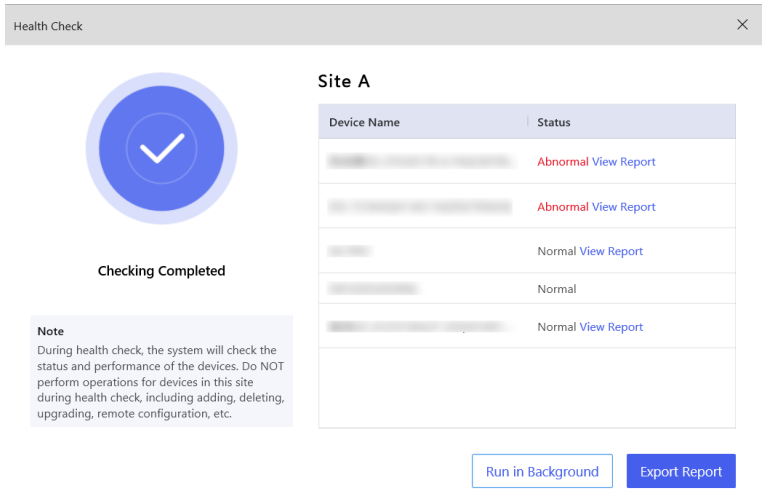


Figure 1-42 Checking Completed

4. Click to get the latest device status.

1.2.3 Set-up with App

The operator can use the App to control the device, such as general arming/disarming operation, and user management etc.

Add Control Panel to the App

Add a control panel to the App before other operations.

Before You Start
The control panel has been activated.

Steps
1. Power on the control panel.
2. If you select adding method as **Scan QR Code**, Scan the QR code on the control panel.

   Note
   Normally, the QR code is printed on the label stuck on the back cover of the control panel.
3. If you select adding method as **Add Device Manually**, enter the device information manually.
   1) Enter the device serial No. with the Hik-Connect Domain adding type.
   2) Tap to search the device.
   3) Tap **Add** on the Results page.
   4) Enter the verification code and tap **OK**.
   5) After adding completed, enter the device alias and tap **Save**.
4. Press POWER RESET according to the image in APP, press the button on the device with 60 sec to add the device to the APP.

Tag Management

Before You Start
Make sure the control panel is disarmed.

Steps
1. On the home page, select the device and tap ··· → **Settings** → **User Management** → **Tag** to enter the page.
2. Tap a user to enter the configuration page.
3. Tap **Add**, and select the tag.
4. Tap **OK**.

Main Page

You can add shortcut, arm or disarm device, view device status, silence alarm, etc.

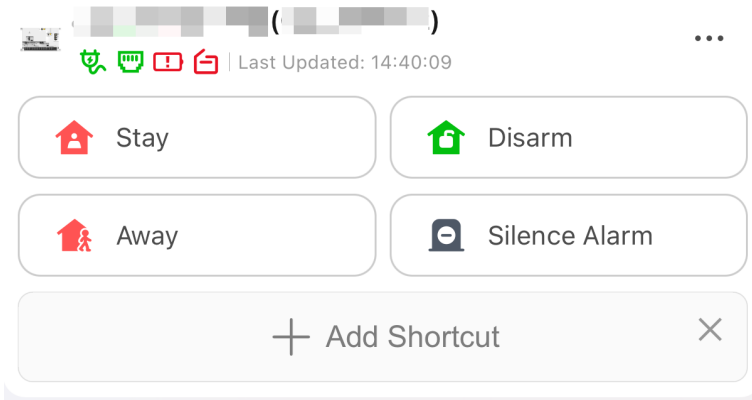


Figure 1-43 Main Page

Status

You can view the device status on the device list page.
Tap control panel, and tap **Device** to enter the device page. Tap control panel or peripherals to view detailed device status.

Shortcut

On the home page, tap **Add Shortcut** or tap ··· → **Manage Shortcut** .
Select area or device, and tap **Add**. The area or device will be shown on the device list page, you can operate the area or device quickly.

Stay/Arming /Disarming /Silence Alarm

Stay/Away Arming

Tap / to arm the area as stay status or away status. When someone intrudes into the detection area, the control panel will trigger alarm, and the system will upload alarm information.

Disarming

Tap to disarm the area. When someone intrudes into the detection area, the system will not upload alarm information.

Silence Alarm

Tap to mute alarms but the system will upload alarm information.

Area Management

You can add new area, edit area information, link devices, etc.

Steps

1. On the home page, tap control panel to enter the Area page.

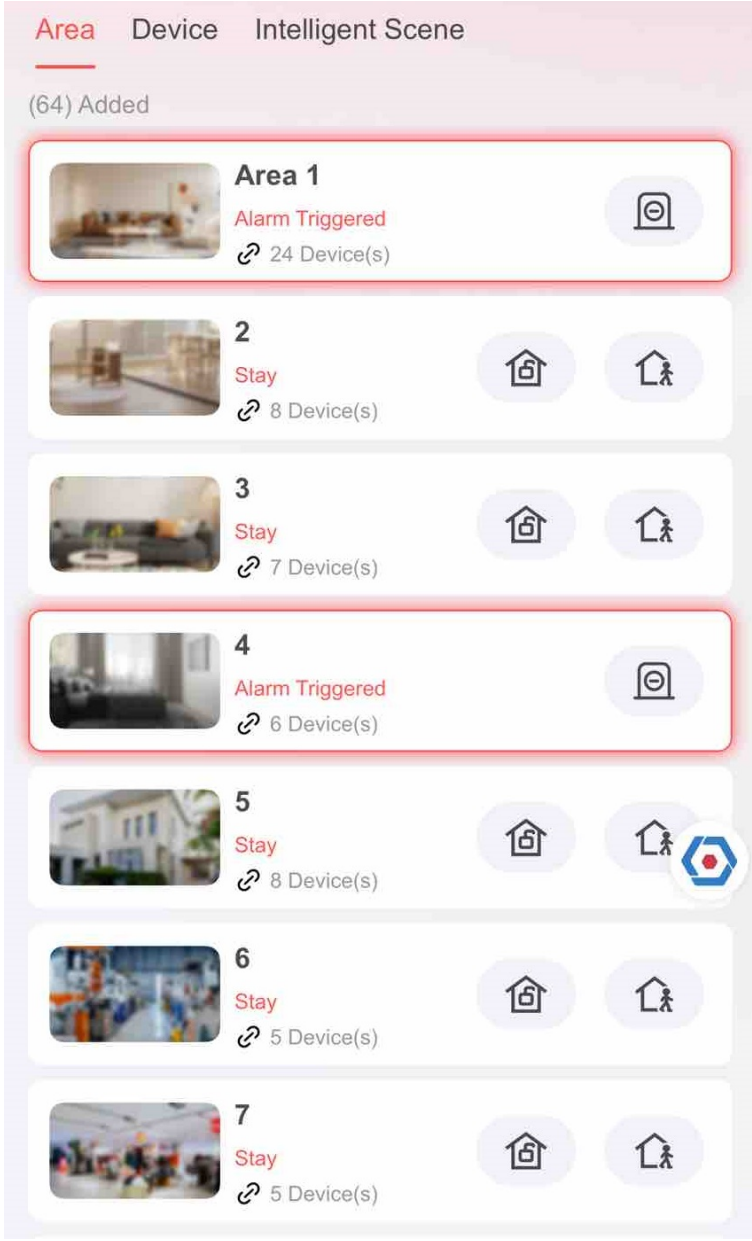


Figure 1-44 Area Management

2. Tap **+**, enter area name, and tap **OK**.
3. Tap to set the area image.
4. Tap **Link to More Devices**, select devices and tap **OK**.
5. Tap **Settings** and slide to enable **Add to Home Shortcut**, the area will be shown on the device list page.
6. Tap to delete the area.

User Management

Add/Edit/Delete Users

The administrator and the installers can manage users. If you are the administrator, you can add, edit, and delete users, and assign different permissions to the newly-added users.

Steps

1. On the home page, select the device and tap ··· → **Settings** → **User Management** to enter the page.
2. Tap **Add**.
3. Enter **User Name**.
4. Select **User Property**.

   Lifetime

   The user is permanently valid.

   Valid Time Period

   You can set the start date, start time, end date and end time. The user is only valid during the configured time period.

   One-time User

   The user's arming and disarming operation is only valid once.
5. Enter **Operation Passcode** and **Duress Passcode**.

   Note

   The Operation Passcode +1 is the Duress Passcode. Use the Duress Passcode can operate the keyboard to arm and disarm normally and upload a duress alarm. For example, if the Operation Passcode is 123456, the Duress Passcode is 123457. If the Operation Passcode is 123459, the Duress Passcode is 123450.
6. Select the linked area for the user.
7. Set permission parameters, and tap **OK** to finish adding.

   Arm/Disarm/Silence Alarm

   Select areas to enable arm, disarm, or silence alarm function.

   Automation Device Control

   After enabling this function, the device will be controlled automatically.
8. Tap **OK**.

Keyfob Management

After adding keyfobs to the control panel, you can press keys to arm or disarm all the detectors added to specific area(s) of the control panel, and silence alarms.

Steps

1. On the home page, select the device and tap ··· → **Settings** → **User Management** to enter the page.
2. Tap a user to enter the configuration page.
3. Tap **Keyfob** → **Add** , scan the QR code of the keyfob or enter the serial No. and select type.
4. Tap a keyfob to edit the parameters.

   Name

   Edit device name.

   User

   Select linked user.

   I/II Key

   Select the function of configurable keys.

   Deactivation

   The selected part will be deactivated.
5. **Optional:** Tap **Delete** to delete the keyfob.

Tag Management

Before You Start

Make sure the control panel is disarmed.

Steps

1. On the home page, select the device and tap ··· → **Settings** → **User Management** → **Tag** to enter the page.
2. Tap a user to enter the configuration page.
3. Tap **Add**, and select the tag.
4. Tap **OK**.

System Settings

System Settings

You can view device basic information, change language, set time and set system alarm duration.

Steps

1. On the home page, select the device and tap ··· → **Settings** → **System Settings** to enter the page.
2. You can view device basic information, change language, set time and set system alarm duration..

Advanced Service

On the device list page, select the device and tap ··· → **Settings** → **Service** to enter the page.

Re-Arm on Restore

While enabled, the deactivation zone will back to arm if fault is restored.

Audible Tamper Alarm

While enabled, the system will alert with buzzer for the tamper alarm. Regardless of whether it is enabled or not, the tamper alarm will be normally pushed to Cloud (for APP) and ARC.

Jamming Sensitivity Settings

The device will detect RF interference and push messages when the RF interference interferes with communication. You can adjust the detection sensitivity.

Note

The System will not be compliant with the Europe EN50131-1 standard after you disable this configuration option.

Motion Detector Restore

Motion detectors include all PIR detectors.

Off

No automatic restore.

Immediate After Alarm

Motion detectors automatically restores immediately after the alarm and reports to Cloud (for APP) and ARC.

After Disarm

Motion detectors automatically restores after disarming and reports to Cloud (for APP) and ARC.

Fault Checklist when Arming

Voice prompt of faults when arming.

Panel-Server Polling Interval

Set the maximum number of times for polling loss of peripherals and detectors. The system will report fault if the time is over the limit. The status of these peripherals and detectors will be shown as offline.

Delay of Server Connection Failure

Set the maximum number of times for delay of server connection failure. The system will report fault if the time is over the limit.

Panel Fault Check

You can enable panel fault events alarm and report delay.

Power Saving Mode

After the energy saving mode is enabled and the main power supply is off, Wi-Fi enters low power consumption mode, 4G is turned off, tag reading is invalid, LED is off, and voice prompt is turned off.

BUS Mode

You can set BUS mode as **Standard Mode** or **Compatible Mode**.

Enable PD6662

Enable PD6662 standard. Functions that do not meet the standard will not take effect.

Panel Lockup Button

All functions of AX HYBRID PRO will be frozen after it is enabled. This function can only be enabled by users with installer permission.

INCRET

You can enable INCRET.

Tap **Save**.

Connect to Network

Wired Network

Steps

1. On the home page, select the device and tap ··· → **Settings** → **Network Settings** → **Ethernet** to enter the page.
2. Set the parameters.
   - Automatic Settings: Enable **DHCP**.
   - Manual Settings: Disabled **DHCP** and set IP address, subnet mask, gateway address, DNS server address.
3. Tap **Save**.

Wi-Fi Configuration

Steps

1. On the home page, select the device and tap ··· → **Settings** → **Network Settings** → **Wi-Fi** to enter the page.
2. Tap a Wi-Fi to connect in the list.

Alarm Receiving Center (ARC)

You can set the alarm receiving center's parameters and all alarms will be sent to the configured alarm center.

Steps

1. On the home page, select the device and tap ··· → **Settings** → **ARC Settings** to enter the page.
2. Slide to enable the ARC and set parameters.

   Protocol Type

   Select as ADM-CID, SIA-DCS, *SIA-DCS, *ADM-CID or OTAP to set uploading mode.

   Connection Mode

   Select as TCP or UDP. UDP is recommended by the SIA DC-09 standard.

   Communication Channel

   Enable communication channels.

   Address Type

   Select as IP or domain name. Enter server address/domain name, port number and account code.

   Periodic Test

   After enabling, you can set the time interval, setting how often to send a test event to the ARC to ensure the connection.

   Transmission Path Fault Delay

   You can set **Transmission Path Fault Delay**.

   Push Notifications

   Enabled events will trigger notifications.
3. Tap **Save**.

Device Maintenance

You can reboot, upgrade, test the device, etc.

Steps

1. On the home page, select the device and tap ··· → **Settings** → **Maintenance** to enter the page.
2. You can perform the following operations.

Operation	Description
Restart	Tap **Restart** to reboot the control panel. **Note** It takes about 3 minutes to reboot the device.
Reset	Tap **Reset** → **Reset Panel Partly** , part of functions and parameters will be restored to factory default settings. Tap **Reset** → **Reset Panel to Default** , all functions and parameters will be restored to factory default settings.

Remote Log Collection	You can enable to collect log remotely.
Control Panel Upgrade	Tap **Control Panel Upgrade** to upgrade the control panel to the latest version.
Detector & Peripheral Upgrade	Tap **Detector & Peripheral Upgrade → Upgrade** to upgrade the peripherals to the latest version.
Walk Test	Tap **Walk Test**, slide to enable the function and view test results of different devices. Tap ⟳ to refresh test results.
Device Debugging	You can enable **Tamper Alarm on HPP Login** and **Event Log for Cellar Service** for device debugging.

Set Push Notifications

You can set notifications pushing voice and message.

Steps

1. On the home page, select the device and tap ··· → **Settings** → **Push Notifications** to enter the page.
2. You can import voice and edit the message.

Other Settings

Click/tap the link to view other settings in HC Mobile Client user manual: ***http://enpinfodata.hikvision.com/analysisQR/showQR/1a7b6537*** .

Appendix A. Input Types

Table A-1 Input Types

Input Types	Operations
Instant Zone	The system will immediately alarm when it detects triggering event after system armed. Audible Response Trigger the system sound and sounder. Voice Prompt: Zone X alarm.
Perimeter Zone	The system will immediately alarm when it detects triggering event after system armed. Audible Response: Trigger the system sound and sounder. There is a configurable interval between alarm and sounder output, which allows you to check the alarm and cancel the sounder output during the interval. Voice Prompt: Zone X perimeter alarm.
Delayed Zone	The system provides you time to leave through or enter the defense area without alarm. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X alarm.
Follow Zone	The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X follow alarm.
24H Silence Zone	The zone activates all the time without any sound or sounder output when alarm occurs. Audible Response: No system sound (voice prompt or sounder).
Panic Zone	The zone activates all the time. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X panic alarm.
Fire Zone	The zone activates all the time with sound or sounder output when alarm occurs. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X fire alarm.

Input Types	Operations
Gas Zone	The zone activates all the time with sound or sounder output when alarm occurs. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X gas alarm.
Medical Zone	The zone activates all the time with beep confirmation when alarm occurs. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X medical alarm.
Timeout Zone	The zone activates all the time. The zone type is used to monitor and report the "ACTIVE" status of a zone, but it will only report and alarm this status after the programmed time has expired (1 to 599) seconds.
Disabled Zone	Alarms will not be activated when the zone is triggered or tampered. Audible Response: No system sound (voice prompt or sounder).
Key Zone	The linked area will arm after being triggered, and disarm after being restored. In the case of the tampering alarm, the arming and disarming operation will not be triggered.
Virtual Zone (Keypad/Keyfob)	The system will immediately alarm when it detects triggering event after system armed. Audible Response: Trigger the system sound and sounder. Voice Prompt: Buzzer beeps.
Tamper Alarm	The system will immediately alarm when it detects triggering event after system armed. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X tampered.
Link	Trigger the linked device when event occurs. e.g. The output expander linked relays will be enabled when the control panel is armed.
Arm	When armed: Voice prompt for fault. You can handle the fault according to the voice prompt.

Input Types	Operations
	• System sound for arming with card or keyfob. • Voice prompt for fault. You can handle the fault according to the voice prompt. • Fault event displays on client. You can handle the fault via client software or mobile client. Voice Prompt: Armed/Arming failed.

Appendix B. Event Types

Table B-1 Event Types

Event Types	Custom	Default 1 (client software notification)	Default 2 (alarm receiving center 1/2)	Default 3 (mobile client)	Default 4 (telephone)
Alarm and Tamper	×/√	√	√	√	√
Life Safety Event	×/√	√	√	√	√
System Status	×/√	√	×	×	×
Panel Management	×/√	√	×	×	×

Appendix C. Access Levels

Level	Description
1	Access by any person; for example the general public.
2	User access by an operator; for example customers (systems users).
3	User access by an engineer; for example an alarm company professional.
4	User access by the maintenance of the equipment.

Table C-1 Permission of the Access Level

Function	Permission			
	1	2	3[a]	4[b]
Arming	No	Yes	Yes	No
Disarming	No	Yes	Yes	No
Restoring/Clearing Alarm	No	Yes	Yes	No
Entering Walk Test Mode	No	Yes	Yes	No
Bypass(zone)/Disabling/Force Arming	No	Yes	Yes	No
Adding/Changing Verification Code	No	Yes[d]	Yes[d]	Yes[d]
Adding/Editing Level 2 User and Verification Code	No	Yes	Yes	No
Adding/Editing Configuration Data	No	No	Yes	No
Replacing software and firmware	No	No	No	Yes

Note

[a] By the condition of being accredited by user in level 2. [b]By the condition of being accredited by user in level 2 and level 3. [d]Users can only edit their own user code.

- The user level 2 can assign the login permission of the controller to the user level 3 or level 4 in the settings page.
- The user level 2 should assign permissions to the user level 3 if the user level 3 wants to login the controller remotely.
- When the controller is bypassed, the user level 3 can login the controller without the permission assignment of the user level 2.

- When the controller is bypassed, the user level 3 can login the controller without the permission assignment of the user level 2.
- The user level 4 can login the controller only when the user level 2 or level 3 has assigned permissions to the user level 4.

Appendix D. 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.

See Far, Go Further

UD42382B