4.3.7 System Settings

Authority Management

Set the authority options.

Click **System → System Options** to enter the System Option Management page.

Wireless Device Poll Check

If the option is enabled, the system will detect all radio peripherals heartbeat. If no peripherals heartbeat is detected, the system will upload an event.

Note

For EN, do not switch to OFF.

Control Panel Arming with Fault

If the option is enabled and there are active faults in a zone, the zone will be bypassed automatically when arming.

Note

You should disable the arming function in the Advanced Settings page. Or the control panel arming with fault function cannot be valid.

Control Panel Status Notification

If the option is enabled, the device will upload report automatically when the control panel status is changed.

Disable Function Key

If the option is enabled, all function keys will be disabled.

Voice Prompt

If the option is enabled, the control panel will enable the text voice prompt.

Voice Prompt of Disarming and Alarm Clearing

If the option is enabled, the control panel will broadcast all system faults before disarming and alarm clearing. Before enable this function, you need to enable **Voice Prompt**.

System Volume

The available system volume range is from 0 to 10.

Authority Advanced Settings

Set advanced authority parameters.

Click **System → System Options → Advanced Settings** to enter the Advanced Settings page.

You can set the following parameters:

Enable Arming

When you enable the function, during the device arming procedure, the system will check the configured fault checklist. When there is fault occurred during the arming procedure, the procedure will be stopped.

Note

PKG keypad and the keyfob do not support this function. If this function is enabled, the arming will fail if there is a fault. It is necessary to eliminate the fault or close the Enable Arming.

Fault Checklist

The system will check if the device has the faults in the checklist during the arming procedure.

Enable Arming with Fault

Check the faults in the Enable Arming with Fault list, and the device will not stop the arming procedure when faults occurred.

Arming Indicator Keeps Light

If the device applies EN standard, by default, the function is disabled. In this case, if the device is armed, the indicator will be solid blue for 5 s. And if the device is disarmed, the indicator will flash 5 times.

When the function is enabled, if the device is armed, the indicator will be on all the time. And if the device is disarmed, the indicator will be off.

Note

Only -P model supports this function.

Prompt Fault When Arming

If the device applies EN standard, by default, the function is disabled. In this case, the device will not prompt faults during the arming procedure.

Note

Only -P model supports this function.

Enable Early Alarm

If you enable the function, when the zone is armed and the zone is triggered, the alarm will be triggered after the delay time.

Note

The early alarm will be taken effect only after the delayed zone is triggered.

Fault Check

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

Click **System → System Options → Control Panel Fault Checklist** to enter the page.

Detect Network Camera Disconnection

If the option is enabled, when the linked network camera is disconnected, an alarm will be triggered.

Battery Supervision

If the option is enabled, when battery is disconnected or out of charge, the device will upload events.

Wired Network Fault Check

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

Wi-Fi Fault Check

If the option is enabled, when the Wi-Fi is disconnected or with other faults, the alarm will be triggered.

Cellular Network Fault Check

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

SIM Card Fault Check

If the option is enabled, the alarm will be triggered for faults of the SIM card.

AC Power Down Check Time

The system checks the fault after the configured time duration after AC power down.

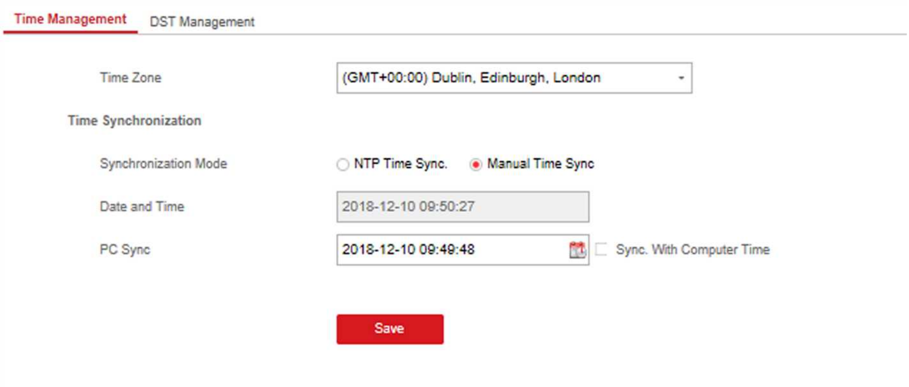
To compliant the EN 50131-3, the check time duration should be 10 s.

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.

Time Management

Click **System → Date and Time** to enter the Time Management page.



Time Management DST Management

Time Zone (GMT+00:00) Dublin, Edinburgh, London

Time Synchronization

Synchronization Mode ○ NTP Time Sync. ● Manual Time Sync

Date and Time 2018-12-10 09:50:27

PC Sync 2018-12-10 09:49:48 □ Sync. With Computer Time

Save

Figure 4-30 Time Management

You can select a time zone from the drop-down list.

You can synchronize the device time manually. Or check **Sync. with Computer Time** to synchronize the device time with the computer time.

Note

While you synchronize the time manually or with the computer time, the system records the log "SDK Synchronization".

DST Management

Click **System → Date and Time → DST Management** to enter the Time Management page.

You can enable the DST and set the DST bias, DST start time, and DST end time.

Security Settings

SSH Settings

Enable or disable SSH (Secure Shell) according to your actual needs.

Click **System → Security → SSH Settings** to enter the SSH Settings page and you can enable or disable the SSH function.

Locking User Settings

Set user locking. You can view the locked user or unlock a user and set the user locked duration.

Steps

1. Click **System → Security → Locking User Settings** to enter the Locking User Settings page.
2. Set the following parameters.

   Max. Failure Attempts

If the user continuously input the incorrect password for more than the configured times, the account will be locked.

Note

The administrator has two more attempts than the configured value.

Locked Duration

Set the locking duration when the account is locked.

Note

The available locking duration is 5s to 1800s.

3. Click 🔓 to unlock the account or click **Unlock All** to unlock all locked users in the list.
4. Click **Save**.

Module Lock Settings

Set the module locking parameters, including the Max Failure Attempts, and locked duration. The module will be locked for the programmed time duration, once the module authentication has failed for the amount of configured times.

Steps

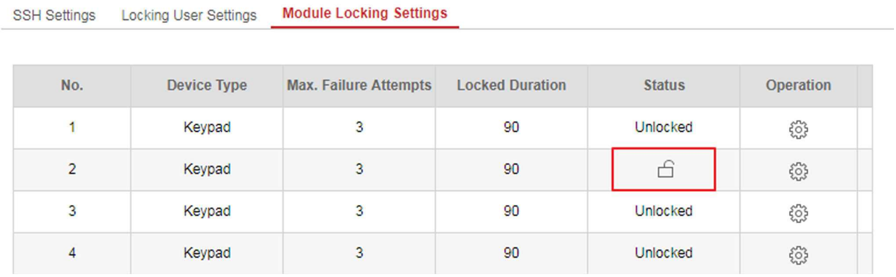
1. Click **System → Security → Module Lock Settings** to enter the Module Lock Settings page.
2. Select a module from the list, and click the ⚙ icon.
3. Set the following parameters of the selected module.

   Max. Failure Attempts

   If a user continuously tries to authentication a password for more than the configured attempts permitted, the keypad will be locked for the programmed duration.

   Locked Duration

   Set the locking duration when the keypad is locked. After the configured duration, the keypad will be unlocked.
4. Click **OK**.
5. **Optional:** Click the **Lock** icon to unlock the locked module.



No.	Device Type	Max. Failure Attempts	Locked Duration	Status	Operation
1	Keypad	3	90	Unlocked	⚙
2	Keypad	3	90	🔓	⚙
3	Keypad	3	90	Unlocked	⚙
4	Keypad	3	90	Unlocked	⚙

Figure 4-31 Module Lock Settings

System Maintenance

You can reboot the device, restore default settings, import/export configuration file, or upgrade the device remotely.

Select the device and click **Remote Configuration** in the client software, or enter the device IP address in the address bar of the web browser. Click **System → System Maintenance** to enter the Upgrade and Maintenance page.

Reboot

Click **Reboot** to reboot the device.

Restore Default Settings

Click **Partly Restore** to restore all parameters except for admin user information, wired network, Wi-Fi network, detector information, and peripheral information to default ones.

Click **Restore All** to restore all parameters to the factory settings.

Import Configuration File

Click **View** to select configuration file from the PC and click **Import Configuration File** to import configuration parameters to the device.

Export Parameters

Click **Export Configuration File** to export the device configuration parameters to the PC.

Upgrade File

Click **View** to select an upgrade file from the PC and click **Upgrade** to upgrade the device remotely.

Note

- Do not power off when the device is upgrading.
- Only manufacturer can use this function.

Certificate Standard

Click **System → System Maintenance → Certificate Standard** to enter the certificate standard settings page.

You can switch between **EN Defaulted** and **General Standard** mode.

The device applies EN Standard by default.

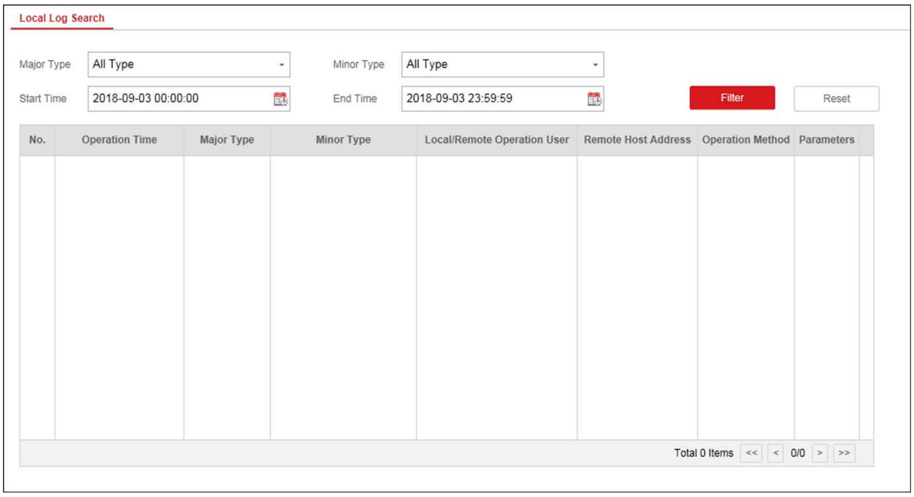
Note

When you select **EN Defaulted**, the user permission and arming parameters will conform to the EN Standard.

Local Log Search

You can search the log on the device.

Click **System → Log** to enter the Local Log Search page.



Local Log Search

Major Type: All Type

Minor Type: All Type

Start Time: 2018-09-03 00:00:00

End Time: 2018-09-03 23:59:59

No.	Operation Time	Major Type	Minor Type	Local/Remote Operation User	Remote Host Address	Operation Method	Parameters

Total 0 Items

Figure 4-33 Local Log Search Page

Select a major type and a minor type from the drop-down list, set the log start time and end time and click **Filter**. All filtered log information will be displayed in the list.

You can also click **Reset** to reset all search conditions.

4.3.8 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.

4.4 Use Mobile Client

4.4.1 Download and Login the Mobile Client

Download the Hik-Connect mobile client from Google Play (for Android) or App store (for iOS) and login the client before operating the security control panel.

Steps

1. Search and download Hik-Connect mobile client from Google Play (for Android) or App Store (for iOS).
2. **Optional:** Register a new account if it is the first time you use the Hik-Connect mobile client.

   Note

   For details, see *User Manual of Hik-Connect Mobile Client*.

3. Run and login the client.

4.4.2 Activate Control Panel via Hik-Connect

Steps

1. Power on the control panel.
2. Select adding type.
   - 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 ⊞ → **Manual Adding** to enter the Add Device page. Enter the device serial No. with the Hik-Connect Domain adding type.
3. Tap 💾 to search the device.
4. Tap **Next**.
5. Enter the device verification code if required and tap **OK**.

   Note

   By default, the verification code is printed on the device label.

6. Tap **Wireless Connection** on the Select Connection Type page.
7. Follow the instructions on the Turn on Hotspot page and change the control panel to the AP mode. Tap **Next**.

Note

You need to remove the rear panel of the device and the AP/STA switch is on the back of the device.

8. Select a stable Wi-Fi for the device to connect and tap **Next**.

   Note

   Make sure the device and the mobile phone are connect to the same Wi-Fi.

9. Follow the instructions. Create the device password and tap **Active**.

   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 reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

10. Follow the instructions on the Turn on Hotspot page and change the control panel to the STA mode. Tap **Confirm**.

    Note

    You need to remove the rear panel of the device and the AP/STA switch is on the back of the device.

11. After the connection is finished, enter the device alias and tap **Save**.
12. **Optional:** You can delete the device.
    1)On the device list page, tap the security control panel and then log in to the device (if required) to enter the partition page.
    2)Tap ⚙ → **Delete Device** to delete the device.

4.4.3 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.
- The control panel has registered to Hik-Connect. For details, see ***Mobile Client Registration*** .

Steps

1. Power on the control panel.
2. Select adding type.
   - 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 ⊞ → **Manual Adding** to enter the Add Device page. Enter the device serial No. with the Hik-Connect Domain adding type.

3. Tap 🖫 to search the device.

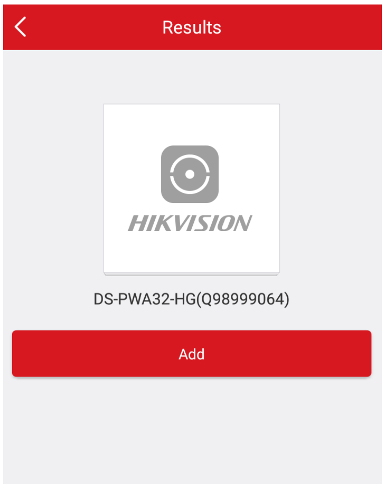


Figure 4-34 Results Page

4. Tap **Add** on the Results page.
5. Enter the verification code and tap **OK**.
6. After adding completed, enter the device alias and tap **Save**.

4.4.4 Add Peripheral to the Control Panel

It is required to enter the activation name and the password login the control panel after it being added. The tampering alarm will not be detected within 5 minutes after you login the device as a setter and does not operate the device.

Before You Start

Make sure the control panel is disarmed.

Steps

Note

Some control panel models do not support add zones or wireless devices remotely. You should add them to the control panel directly. For details, see the user manual of the wireless device.

1. On the device list, tap the security control panel and then log in to the device (if required) to enter the Partition page.
2. Tap ⊞ to enter the Scan QR Code page.
3. Scan the QR code of the peripheral.

Note

The QR code is usually on the back cover of the device.

4. **Optional:** If the QR code fails to be recognized, tap ✎ and enter the serial number of the device, and then select the device type.

Note

The serial number is usually on the back cover of the device.

5. Tap **Add**.

Note

- When the adding peripheral is a detector, the detector will be linked to the zone. You can view the detector information in the Zone tab.
- Up to 32 detectors can be linked to the zone.

The added peripheral will be listed in the Zone tab or the Peripheral Device tab.

Note

One of the most important factors for a reliable wireless installation is the signal strength between a wireless device and the panel. If a device is out of range it will not be able to send events to the control panel therefore it is recommended that a signal strength test is performed before fixing devices into place. The control panel has advanced signal strength mechanism that operates by monitoring all inputs/bells on the web browser. The page will need to be re-freshed every time for a new test. See also Appearance-Function Button.
When performing a signal strength test it is recommended that the system is tested in the 'worst case scenario'. For example with all doors and windows closed.

4.4.5 Add Card

You can add card to the control panel. Use the card to arm, disarm, or clear alarm.

Steps

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

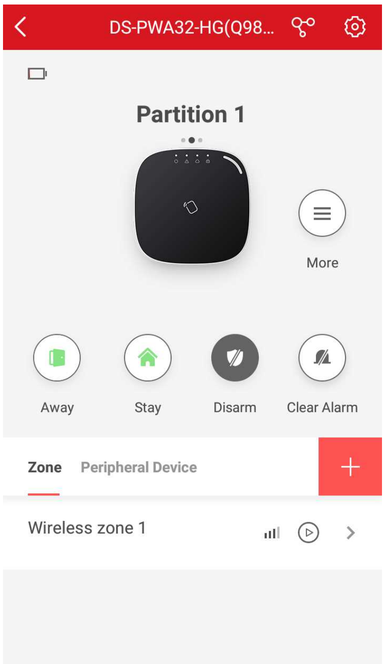


Figure 4-35 Partition Page

2. Tap ⚙ → **User Management** → **Card/Tag Management** to enter the Card/Tag Management page.
3. Tap **+**.
4. When hearing the voice prompt "Swipe Card", you should present the card on the control panel card presenting area.

   When hearing a beep sound, the card is recognized.
5. Create a card name and tap **Finish**.

   Note

   The name should contain 1 to 32 characters.

   The card is displayed in the Card/Tag Management page.

4.4.6 Add Keyfob

You can add keyfobs to the control panel and control partition arming/disarming status. You can also clear alarm when an alarm is triggered.

Steps

Note

Make sure the keyfob's frequency is the same as the control panel's.

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

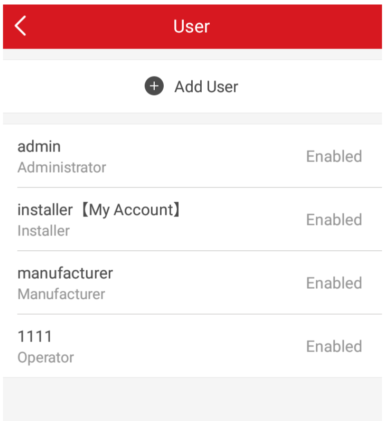
2. Tap ✚ to enter the Scan QR Code page.
3. Tap **Add Keyfob**.
4. Follow the instruction on the page and press any key on the keyfob to add.
5. Create a name for the keyfob and tap **Finish**.

   The keyfob is listed in the Wireless Device page.
6. **Optional:** You can view the keyfob's serial No. and you can also delete it.

4.4.7 User Management

Steps

1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.
2. Tap ⚙ → **User Management → User** .



User

Add User

admin
Administrator
Enabled

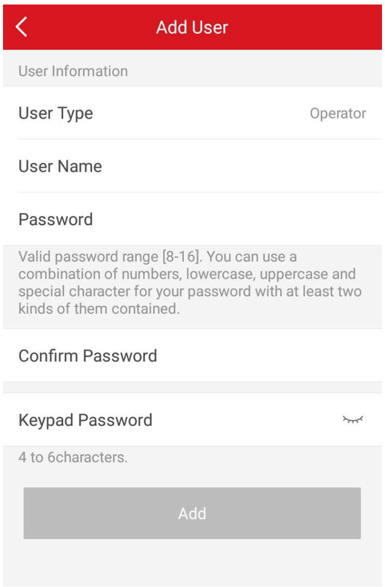
installer【My Account】
Installer
Enabled

manufacturer
Manufacturer
Enabled

1111
Operator
Enabled

Figure 4-36 User Managment

3. Tap **Add User**.



Add User

User Information

User Type Operator

User Name

Password

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm Password

Keypad Password

4 to 6characters.

Figure 4-37 Add User

4. Select **User Type**. Enter **User Name** and **Password**.
5. Enter **Keypad Password**.

Note

The keypad password +1 or -1 is the duress code. Use the duress code can operate the keyboard to arm and disarm normally and upload a duress alarm. For example, if the keypad password is 123456, the duress code is 123455 or 123457.

6. Tap **Add** to add the user.
7. **Optional:** Tap a user to edit the parameters. You can choose to enable the user or not. Select the linked partition and the permission.
8. **Optional:** Tap a user and tap **Delete** to delete the user.

Note

Admin, installer and mabufacturer can not be deleted.

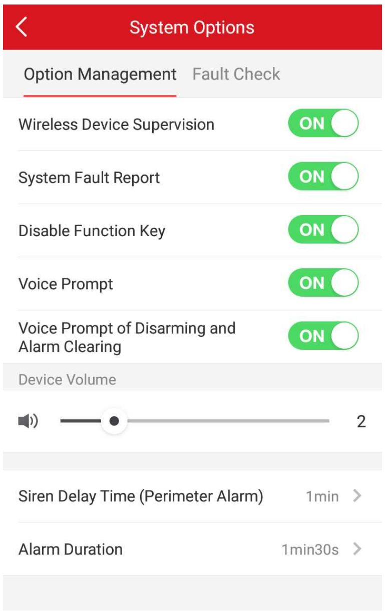
4.4.8 System Settings

System Option

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

Tap ⚙ → **System Option** to set parameters.

For **Option Management**:



System Options

Option Management | Fault Check

Wireless Device Supervision: ON

System Fault Report: ON

Disable Function Key: ON

Voice Prompt: ON

Voice Prompt of Disarming and Alarm Clearing: ON

Device Volume: 2

Siren Delay Time (Perimeter Alarm): 1min

Alarm Duration: 1min30s

Figure 4-38 Option Managment

Wireless Device Supervision

If the option is enabled, the system will detect status of all wireless devices.

System Fault Report

If the option is enabled, the device will upload report automatically when there is system faults.

Disable Function Key

If the option is enabled, all function keys will be disabled.

Siren Delay Time (Perimeter Alarm)

If you have set the perimeter zone, you can set the delayed time for the zone.

Note

The available time duration range is from 0 s to 600 s.

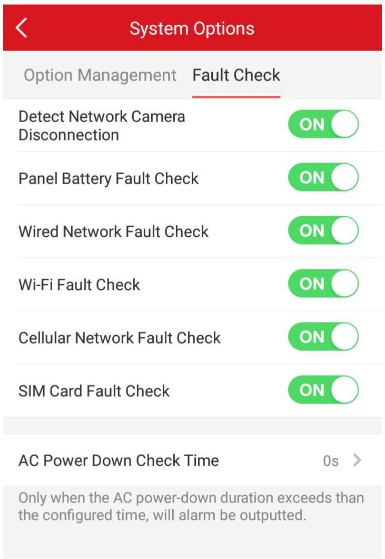
Alarm Duration

If you have set the perimeter zone, you can set the time duration of the alarm.

Note

The available time duration range is from 1 s to 900 s.

For **Fault Check**:



Detect Network Camera Disconnection ON

Panel Battery Fault Check ON

Wired Network Fault Check ON

Wi-Fi Fault Check ON

Cellular Network Fault Check ON

SIM Card Fault Check ON

AC Power Down Check Time 0s

Only when the AC power-down duration exceeds than the configured time, will alarm be outputted.

Figure 4-39 Fault Check

Detect Network Camera Disconnection

If the option is enabled, when the linked network camera is disconnected, an alarm will be triggered.

Panel Battery Fault Check

If the option is enabled, when battery is disconnected or out of charge, the device will upload events.

Wired Network Fault Check

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

Wi-Fi Fault Check

If the option is enabled, when the Wi-Fi is disconnected or with other faults, the alarm will be triggered.

Cellular Network Fault Check

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

SIM Card Fault Check

If the option is enabled, the alarm will be triggered for faults of the SIM card.

AC Power Down Check Time

The system checks the fault after the configured time duration after AC power down.

To compliant the EN 50131-3, the check time duration should be 10 s.

System Maintenance

On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.
Tap ⚙ → **System Maintenance** to set parameters.

Reboot Device

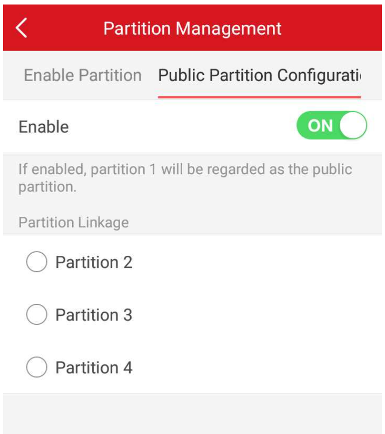
The device will restore all parameters to the default settings.

Partly Restore

The device will restore to its default settings except for admin user information, wired network parameters, Wi-Fi network, detector information, and wireless device parameters.

Public Partition Configuration

On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.
Tap ⚙ → **Partition Management** → **Public Partition Configuration** to set parameters.



Enable ON

If enabled, partition 1 will be regarded as the public partition.

Partition Linkage

○ Partition 2
○ Partition 3
○ Partition 4

Figure 4-40 Public Partition Configuration

After slide **Enable**, the partition 1 will be regarded as the public partition.
You can select linked partition as well.

4.4.9 Arm/Disarm the Zone

Arm or disarm the zone manually as you desired.

Note

Axiom security control panel supports 4 partitions.

On the device list page, tap the security control panel and then log in to the device (if required) to enter the Partition page. You can swipe to the left or right to switch partitions.

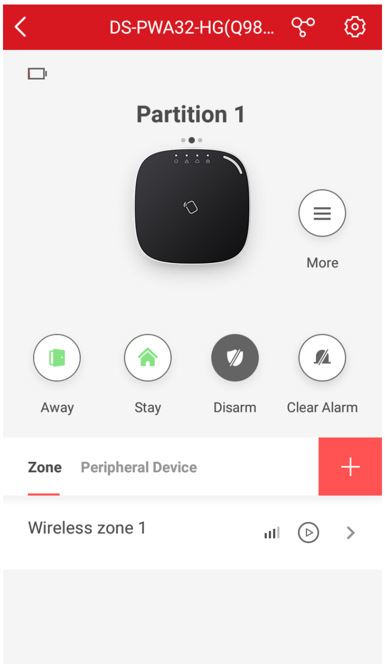


Figure 4-41 Partition Page

Operations for a Single Partition

- **Away**: When all the people in the detection area leave, turn on the Away mode to arm all zones in the partition after the defined dwell time.
- **Stay**: When the people stays inside the detection area, turn on the Stay mode to arm all the perimeter burglary detection (such as perimeter detector, magnetic contacts, curtain detector in the balcony). At the meantime, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarm will not be triggered.
- **Disarm**: In Disarm mode, all the zones in the partition will not trigger alarm, no matter alarm events happen or not.
- **Clear Alarm**: Clear all the alarms triggered by the zones of the partition.

Operations for All Partitions

- **Away**: When all the people in the detection area leave, turn on the Away mode to arm all zones in all partitions after the defined dwell time.
- **Stay**: When the people stays inside the detection area, turn on the Stay mode to arm all the perimeter burglary detection (such as perimeter detector, magnetic contacts, curtain detector in the balcony) set in all the zones of all partitions. At the meantime, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarm will not be triggered.
- **Disarm**: In Disarm mode, all the zones of all partitions will not trigger alarm, no matter alarm events happen or not.
- **Clear Alarm**: Clear all the alarms triggered by the all the zones of all the partitions.

4.4.10 Bypass Zone

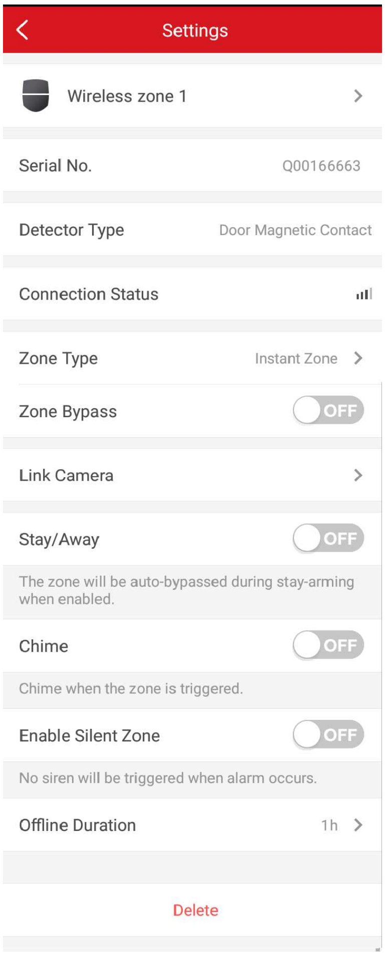
When the partition is armed, you can bypass a particular zone as you desired.

Before You Start

Link a detector to the zone.

Steps

1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the Partition page.
2. Select a zone in the Zone tab to enter the settings page.
3. Select a zone and enter the Settings page.



Settings

Wireless zone 1

Serial No. Q00166663

Detector Type Door Magnetic Contact

Connection Status

Zone Type Instant Zone

Zone Bypass OFF

Link Camera

Stay/Away OFF

The zone will be auto-bypassed during stay-arming when enabled.

Chime OFF

Chime when the zone is triggered.

Enable Silent Zone OFF

No siren will be triggered when alarm occurs.

Offline Duration 1h

Delete

Figure 4-42 Zone Settings Page

4. Enable **Zone Bypass** and the zone will be in the bypass status.

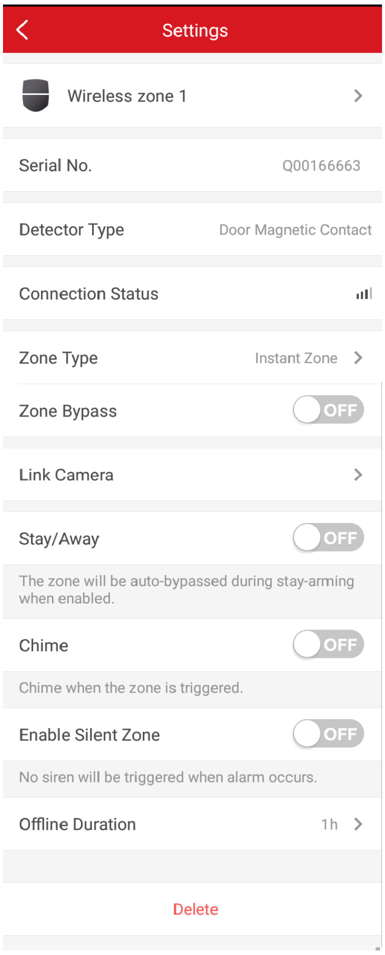
   The detector in the zone does not detect anything and you will not receive any alarm from the zone.

4.4.11 Set Zone

After the detector is added, you can set the zone, including the zone name, the zone type, zone bypass, linked camera, stay/away status, the siren, and the silent zone. You can also view the detector serial No. (only device in 433 HMz) and the detector type of the zone.

Steps

1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.
2. Tap **Zone** and then tap a zone in the Partition page to enter the zone settings page.



Settings

Wireless zone 1

Serial No. Q00166663

Detector Type Door Magnetic Contact

Connection Status

Zone Type Instant Zone

Zone Bypass OFF

Link Camera

Stay/Away OFF

The zone will be auto-bypassed during stay-arming when enabled.

Chime OFF

Chime when the zone is triggered.

Enable Silent Zone OFF

No siren will be triggered when alarm occurs.

Offline Duration 1h

Delete

Figure 4-43 Zone Setting Page

3. Set the following parameters as you desired.

   Zone Type

   Select a zone type from the zone type list.

   If you select **Delayed Zone**, you should select an entry delay (Entry Delay 1 or Entry Delay 2) on the pop-up page.

If you select **Timeout Zone**, you should select a timeout value or tap **Custom** to set a custom value.

Zone Bypass

Enable the function and the zone will be bypassed. No alarm will be received while the zone is bypassed.

Link Camera

You can link the zone to cameras. When an alarm is triggered, you can monitor the zone via the linked cameras.

Stay/Away

If this option is Enabled the zone will be auto bypassed when the alarm system is stay armed. To re-enable the zone deselect the option.

Chime

Enable the function and the zone will be start audible alarm when it is triggered.

Enable Silent Zone

Enable the function and no siren will be triggered if an event or alarm occurs.

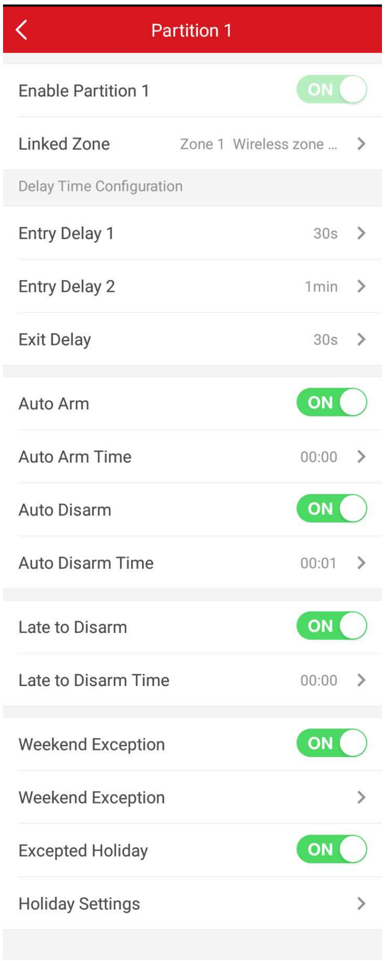
4.4.12 Set Arming/Disarming Schedule

Set the arming/disarming schedule to arm/disarm a particular zone automatically.

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

Tap ⚙ → **Partition Management** and select a partition, or tap ≡ on the Parition page to enter the Settings page.

Enable the auto arm/disarm function and set the auto arm time/auto disarm time. You can also set the late to disarm time, entry delay time, exit delay time, siren delay time, weekend exception and excepted holiday.



Partition 1

Enable Partition 1 ON

Linked Zone — Zone 1 Wireless zone ...

Delay Time Configuration

Entry Delay 1 — 30s

Entry Delay 2 — 1min

Exit Delay — 30s

Auto Arm ON

Auto Arm Time — 00:00

Auto Disarm ON

Auto Disarm Time — 00:01

Late to Disarm ON

Late to Disarm Time — 00:00

Weekend Exception ON

Weekend Exception

Excepted Holiday ON

Holiday Settings

Figure 4-44 Arming or Disarming Schedule Page

Entry Delay 1

Entry Delay 2

Set a value for **Entry Delay 1** and **Entry Delay2**. Entry delay is a time concept. If entry delay is configured for the delayed zone, when you enter an armed delayed zone, the zone alarm will not be triggered until the end of entry delay.

Note

After set value for **Entry Delay 1** and **Entry Delay 2**, you should set the entry delay of a specific zone to the value of **Entry Delay 1** or **Entry Delay 2**.

Exit Delay

Set exit delay for the delayed zone. If exit delay is configured for the delayed zone, after you arm the zone on the indoor unit, you can exit the zone without triggering alarm until the end of exit delay.

Auto Arm

Enable the partition to automatically arm itself in a specific time point.

Auto Arm Time

Set the schedule for the partition to automatically arm itself.

Late to Disarm

Enable the device to push a notification to the phone or tablet to remind the user to disarm the partition when the partition is still armed after a specific time point.

Note

You should enable the Panel Management Notification function on the Web Client of **Communication Parameters → Event Communication** before enabling the Late to Disarm function.

Late to Disarm Time

Set the time point mentioned in **Late to Disarm**.

Weekend Exception

If enabled, **Auto Arm**, **Auto Disarm**, and **Late to Disarm** are disabled on the weekend.

Excepted Holiday

Enable the function and the zone will not be armed/disarmed in the holiday. You should set the holiday schedule after enabling.

Note

Up to 6 holiday groups can be set.

4.4.13 Check System Status (Zone Status/Communication Status)

You can view the zone status and the communication status via the mobile client.

View Zone Status

In the Partition page, tap **Zone** to enter the Zone tab. You can view the each zone's status in the list.

Communication Mode

In the Partition page, tap ⚙ → **Device Information** to enter the page. You can view the device communication status, including the battery, Ethernet network, Wi-Fi, mobile network, data usage and so on.

Enable Arming Process

In the Partition page, tap ⚙ to enter the page. Slide to enable **Enable Arming Process**. After enabled, the device will auto detect its faults during the arming process. You can determine whether to continue arming or not if faults are detected.

EN Mode

the Partition page, tap ⚙ to enter the page. Slide to enable **EN Mode**.

Note

The device will be auto rebooted when you turn on or turn off EN Mode.

4.4.14 Check Alarm Notification

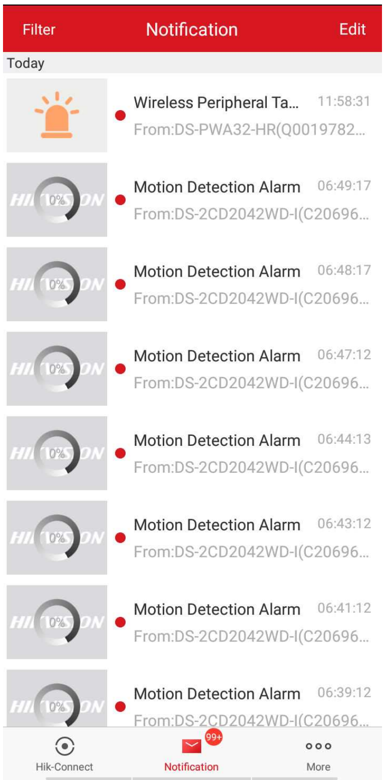
When an alarm is triggered, and you will receive an alarm notification. You can check the alarm information from the mobile client.

Before You Start

- Make sure you have linked a zone with a detector.
- Make sure the zone is not bypassed.
- Make sure you have not enabled the silent zone function.

Steps

1. Tap **Notification** in the mobile client to enter the page.



Today

Wireless Peripheral Ta... 11:58:31
From:DS-PWA32-HR(Q0019782...

Motion Detection Alarm 06:49:17
From:DS-2CD2042WD-I(C20696...

Motion Detection Alarm 06:48:17
From:DS-2CD2042WD-I(C20696...

Motion Detection Alarm 06:47:12
From:DS-2CD2042WD-I(C20696...

Motion Detection Alarm 06:44:13
From:DS-2CD2042WD-I(C20696...

Motion Detection Alarm 06:43:12
From:DS-2CD2042WD-I(C20696...

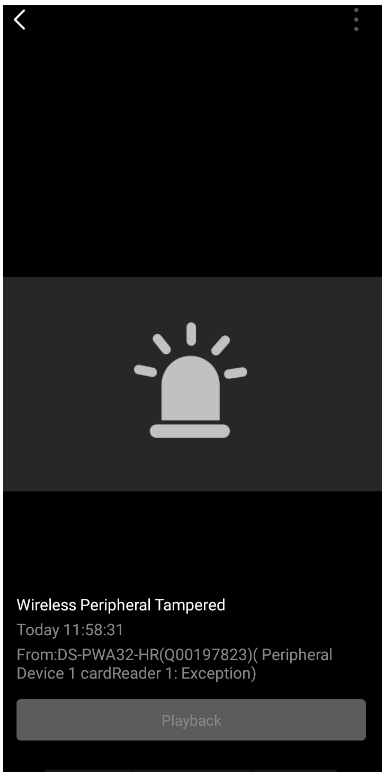
Motion Detection Alarm 06:41:12
From:DS-2CD2042WD-I(C20696...

Motion Detection Alarm 06:39:12
From:DS-2CD2042WD-I(C20696...

Figure 4-45 Notification Page

All alarm notifications are listed in Notification page.

2. Select an alarm and you can view the alarm details.



Wireless Peripheral Tampered

Today 11:58:31

From:DS-PWA32-HR(Q00197823)(Peripheral Device 1 cardReader 1: Exception)

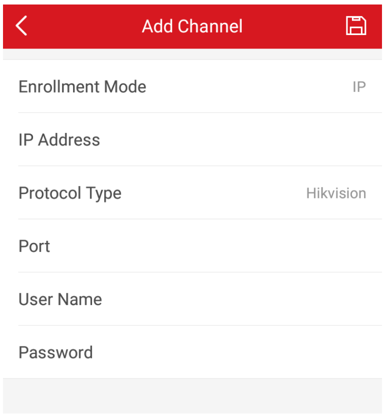
Figure 4-46 Alarm Details

3. **Optional:** If the zone has linked a camera, you can view the playback when the alarm is triggered.

4.4.15 Set Network Camera Channel

Steps

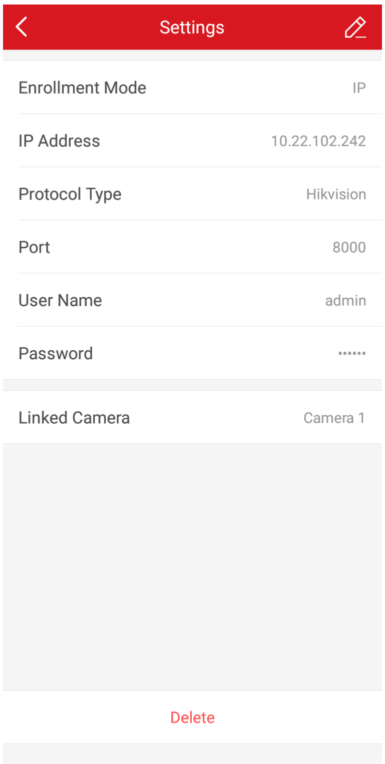
1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.
2. Tap ⚙ → **Network Camera Channel** .
3. Tap **Add Channel**.



Add Channel

Enrollment Mode	IP
IP Address	
Protocol Type	Hikvision
Port	
User Name	
Password	

4. Enter **IP Address**, **Port**, **User Name** and **Password**.
5. Tap 💾 to add channel.
6. **Optional:** Edit a channel.
   1) Select a channel in the list.



Enrollment Mode	IP
IP Address	10.22.102.242
Protocol Type	Hikvision
Port	8000
User Name	admin
Password	······
Linked Camera	Camera 1

Figure 4-48 Network Camera Settings

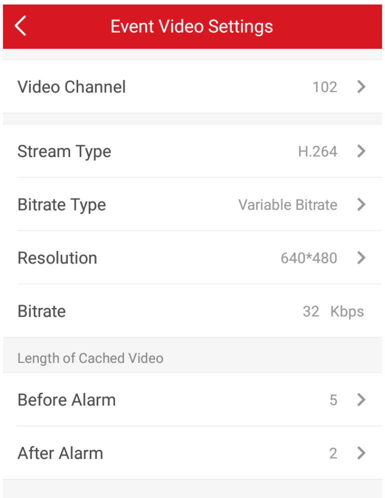
   2) Tap ✎ to enetr the editing mode.
   3) Edit parameters.
   4) Tap 💾 to save.
7. **Optional:** Select a channel and tap **Delete** to delete it.

4.4.16 Set Event Video Settings

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

Tap ⚙ → **Event Video Settings** to enter the page.

You need to select the video channel and set parameters.



Event Video Settings

Video Channel 102

Stream Type H.264

Bitrate Type Variable Bitrate

Resolution 640*480

Bitrate 32 Kbps

Length of Cached Video

Before Alarm 5

After Alarm 2

Figure 4-49 Event Video Settings

Stream Type

Main Stream: Being used in recording and HD preview, it has a high resolution, code rate and picture quality.

Sub-Stream: It is used to transmit network and preview pictures as a video streaming with features of lower resolution, bit rate and picture quality.

Bitrate Type

Select the Bitrate type as constant or variable.

Resolution

Select the resolution of the video output

Bitrate

The higher value corresponds to the higher video quality, but the better bandwidth is required.

Before Alarm

Length of cached video before alarm.

After Alarm

Length of cached video after alarm.

4.4.17 Add a Camera to the Zone

You can link a camera to the zone to monitor the zone. You can view the alarm videos when an alarm is triggered.

Before You Start

Make sure you have installed the camera in the target zone and the camera has connected the same LAN as the security control panel's.

Steps

1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.
2. Tap **Zone** to enter the zone list page.
3. Select a zone to enter the zone settings page.
4. Tap **Link Camera** to enter the Link Camera page.

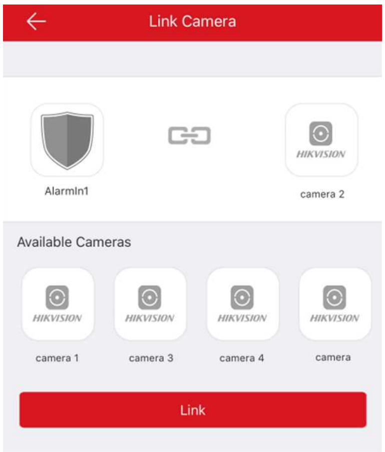


Figure 4-50 Link Camera Page

5. Select a camera in the available cameras, and tap **Link**.

Chapter 5 Operations

You can use the client keyfob, card, client software, or mobile client to do arming, disarming, bypass, and zone disabling.

5.1 Arming

You can use keypad, keyfob, card, client software, mobile client to arm your system.
After the arming command is sending to control panel, the sytem will check the detector status. If the detector is in fault, you will need to choose whether to arm the system with fault.
While the system is armed, the control panel will prompt the result in 5s, and upload the arming report.

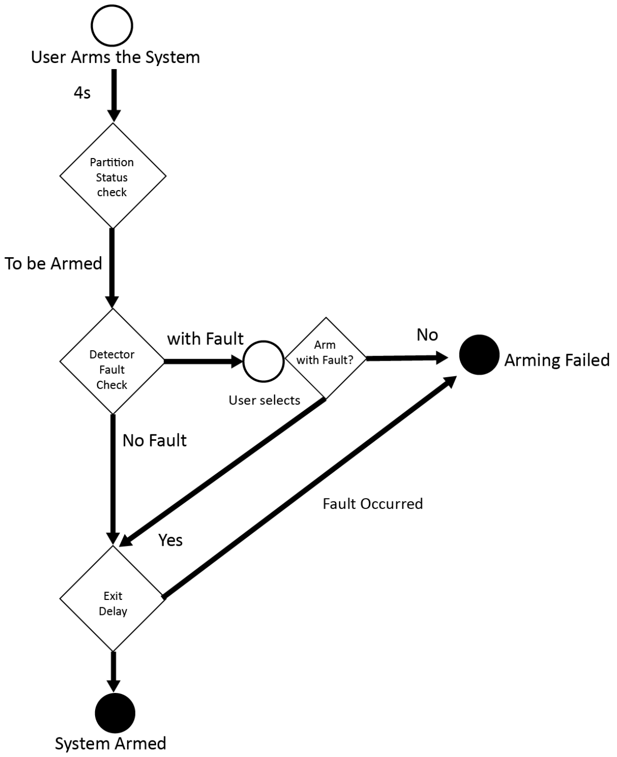


Figure 5-1 Arming Process

Access level of Arming

The user in level 2 or 3 has the permission to arm or partly arm the system.

Arming Indication

The arming/disaring indicator keeps solid blue for 5s.

Reason of Arming Failure

- Intrusion detector triggered (excepts the detector on the exit route).
- Panic alarm device triggered.
- Tampering alarm occurred.
- Communication exception
- Main power supply exception
- Backup battery exception
- Alarm receiving fault
- Siren fault
- Low battery of the keyfob
- Others

Arming with Fault

While the arming is stopped with fault, user in level 2 has the permission to arm the system with fault (forced arming).
Fored arming only taks effect on the current arming operation.
The forced arming operation will be record in the event log.

5.2 Disarming

You can disarm the system with keypad, keyfob, card, client software, or mobile client.

Disarming Indication

The arming/disarming indicator flashes 30s while the user successfully disarm the system through the entry/exit route.
The system will report the disarming result after the operation completed.

Entry Delay Duration

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

Early Alarm

If either the intrusion or tampering alarm occurs on the enter/exit route when the control panel is in the status of entry delay, the control panel then enters the early alarm mode.
The early alarm duration can be set (> 30s).
The control panel will reports the alarm only if the alarm event lasts over the duration of early alarm with the addition of entry delay.

5.3 Use the Keyfob

The keyfod is used for away arming, stay arming, disarming, panic alarm, and clearing alarm.

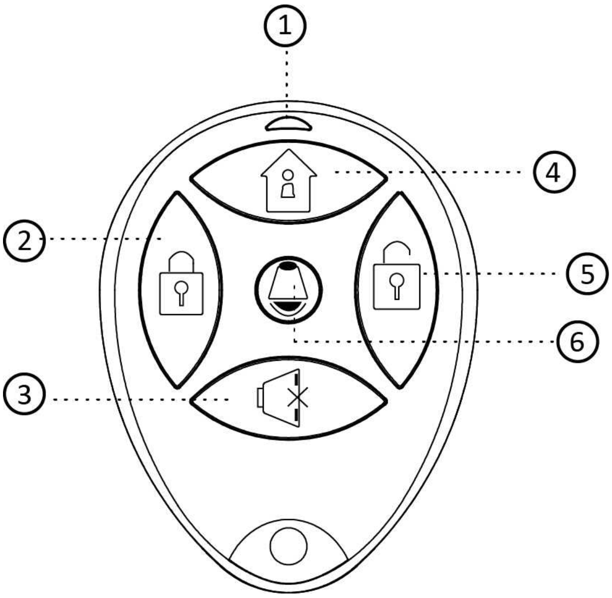


Figure 5-2 Type Ⅰ Keyfob

Table 5-1 Type Ⅰ Keyfob Keys

No.	Description
1	Indicator Green: Successful Operation Red: Press the Key
2	Away Arming
3	Clearing Alarm
4	Stay Arming
5	Disarming
6	Panic Alarm (Duress Alarm) Hold the key for 2 seconds, an alarm report will be send to the alarm center secretly without alerting.

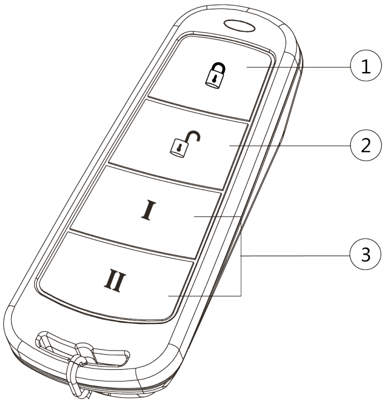


Figure 5-3 Type Ⅱ Keyfob

Table 5-2 Type Ⅱ Keyfob Keys

No.	Description
1	Arming (Lock)
2	Disarming(Unlock)
3	Combo-Function Key

Custom Combination Functions (except Arming + Ⅱ and Disarming + Ⅰ) : Away Arming, Stay Arming, Disarming, Panic Alarm, Clearing Alarm, Fault Inspection, and Arming Status Check.

The following table shows the keyfob operation and responded indications.

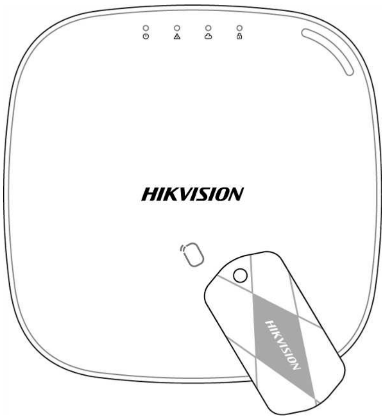
Table 5-3 Type Ⅱ Keyfob Operations and Indications

Keyfob Operation Result	Voice Prompt	Indication
Armed	Away/Stay Arming	Red LED Flashes Once
Arming Failed	Arming failed.	Green LED Flashes Once
Arming	Beep in the first 5 seconds. Fault prompt after the beep for fault occurring	Green LED Flashes 9 Times
No Arming Permission	Operation failed. The keyfob has no arming permission.	Yellow LED Flashes 4 Times
Fault Checking Finished	No Voice Prompt	Yellow LED Flashes 4 Times
Alarm Cleared	Alarm cleared	Green LED Flashes Once
No Permission for Clearing Alarm	Operation failed. The keyfob has no arming permission.	Yellow LED Flashes 4 Times
Disarmed	Disarmed	Green LED Flashes Once

Keyfob Operation Result	Voice Prompt	Indication
No Disarming Permission	Operation failed. The keyfob has no arming permission.	Yellow LED Flashes 4 Times
Panic Alarm Uploaded	Alarm Prompt	Green LED Flashes Once
No Panic Alarm Permission	Operation failed. The keyfob has no arming permission.	Yellow LED Flashes 4 Times

5.4 Use the Card

It is poissible to arm or disarm the system with the card.



While the system is not armed, present a valid card to the control panel to arm the system.

While the system is armed, present a valid card to the control panel to disarm the system.

The card operations and responding voice prompts are shown below.

Card Operation Result	Voice Prompt
Armed with Enrolled Card	Away/Stay Arming
Arming Failed with Enrolled Card	Arming Failed
Start Arming with Enrolled Card	Beep in the first 5 seconds. Fault promt after the beep for fault occurring
No Arming Permission for the Enrolled Card	No Voice Prompt
Fault Checking Finished with the Enrolled Card	No Voice Prompt
Disarming with Enrolled Card	Disarmed
No Disarming Permission for the Enrolled Card	No Voice Prompt
Unenrolled Card Operation	Invalid access

5.5 Use the Client Software

Steps

1. Download, install and register to the client software.
2. Add device in **Device Management → Device** .

Note

- Set the device port No. as 80.
- The user name and password when adding device are the activation user name and password.

3. Click ⚙ to enter the Remote Configuration page after the device is completely added,

5.5.1 Add Device to the Client Software

Before You Start

Activate the device and ensure that the device is on the same subnet as the PC.

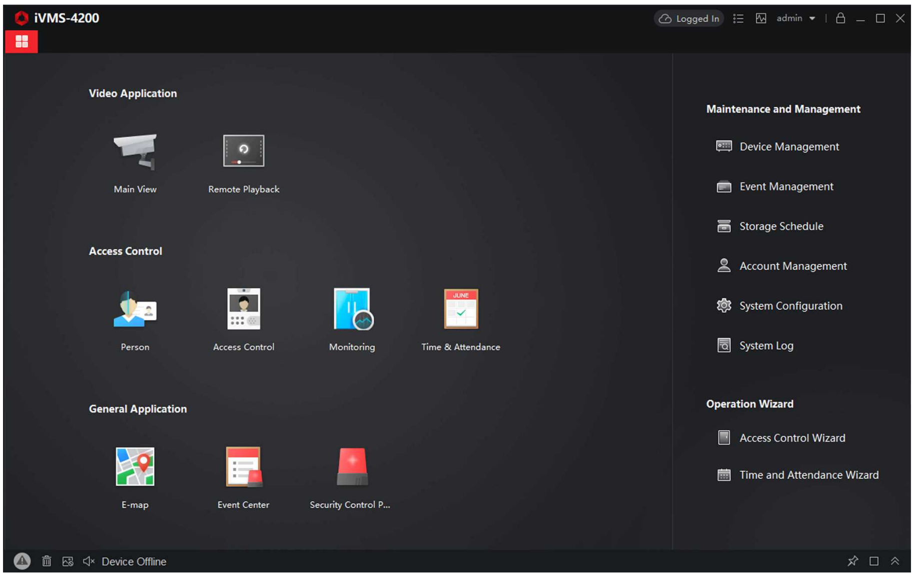


Figure 5-4 Client Software Main Page

In the client software, go to **Device Management → Device** on the **Maintenance and Management** list. You can add devices to client software by several methods on the device management page. The following describes how to add devices through IP/Domain Name. For more information, see *iVMS-4200 Client Software User Manual*.

Steps

1. On the **Device** page, click **Add**.
2. Select **IP/Domain** as the adding mode, edit the device information, including **Name**, **Address**, **Port**, **User Name**, and **Password**.

Note

The port No. is 80.

3. Check **Import to Group**.
4. Click **Add** to add the device.

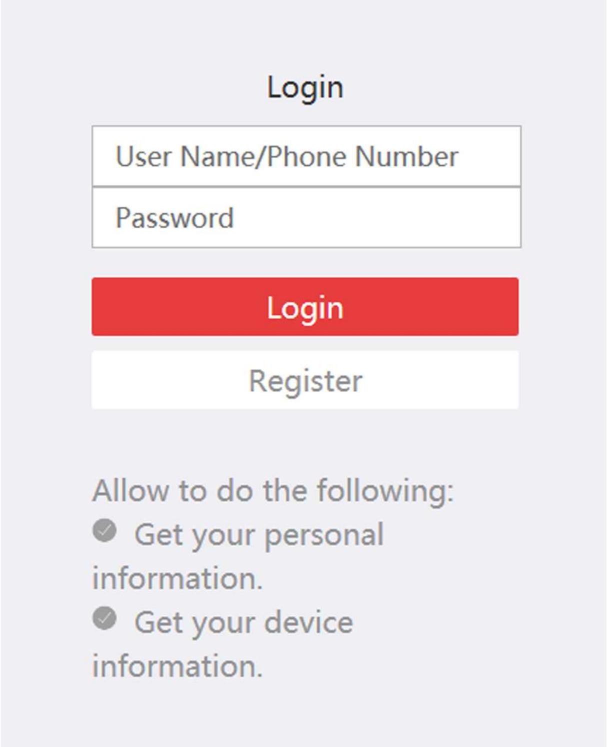
5.5.2 Add Device to the Client Software through Cloud P2P

Before You Start

Enter the prerequisites here (optional).

Steps

1. Click **Device Management → Device** on the **Maintenance and Management** list to enter the page.
2. Log in the Cloud P2P account.
   - Click Not Logged in and select the region. Enter the user name and password on the pop-up window. Click **Login** .
   - Click **Add**, select the region and click **Login** on the pop-up winodow. Enter user name, password and click **Login**.



Allow to do the following:

✓ Get your personal information.

✓ Get your device information.

Figure 5-5 Login Cloud P2P Account

Note

- If you have added a device to your Cloud P2P account, the device will appear in the device list. If not, you need to add a device via cloud P2P or IP.
- After you exit your Cloud P2P account, the device you added to your Cloud P2P account will be remove.

3. Click **Add**, select adding mode as **Cloud P2P**.
4. Enter **Serial No.** and **Verification Code** or click **Online Device** to select a device.

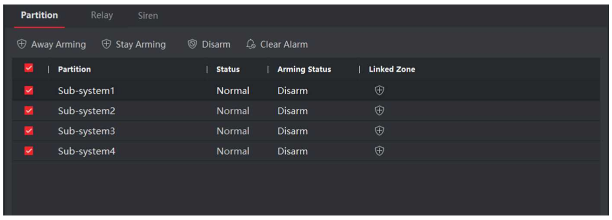
Note

- The device should be on the same network segment as the computer so you can find it in the online device list.
- You can check **DDNS** and enter parameters to enbale it.

5. Check **Import to Group**.
6. Click **Add**.

5.5.3 Partition Operation

In the client software, click **Security Control Panel → Partition** to enter the page. You can control the selected partition, such as **Away Arming**, **Stay Arming**, **Disarm** and **Clear Alarm**.



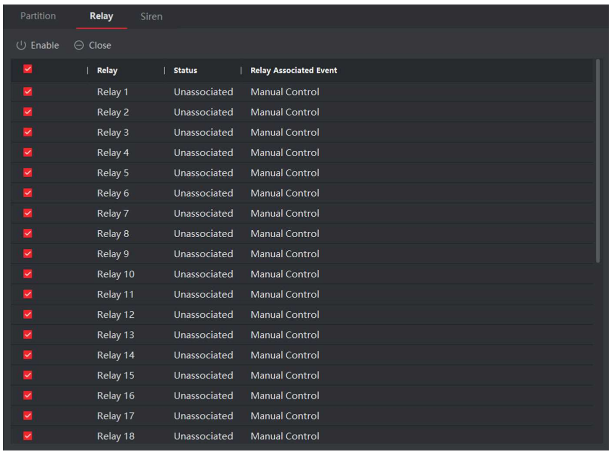
☑	Partition	Status	Arming Status	Linked Zone
☑	Sub-system1	Normal	Disarm	⊕
☑	Sub-system2	Normal	Disarm	⊕
☑	Sub-system3	Normal	Disarm	⊕
☑	Sub-system4	Normal	Disarm	⊕

Figure 5-6 Partition Operation

Click ⊕ to enter the zone operation page. You can **Bypass** and **Bypass Recovered** the selected zones here.

5.5.4 Operate the Relay

In the client software, click **Security Control Panel → Relay** to enter the page. You can **Enable** or **Close** the selected relays.



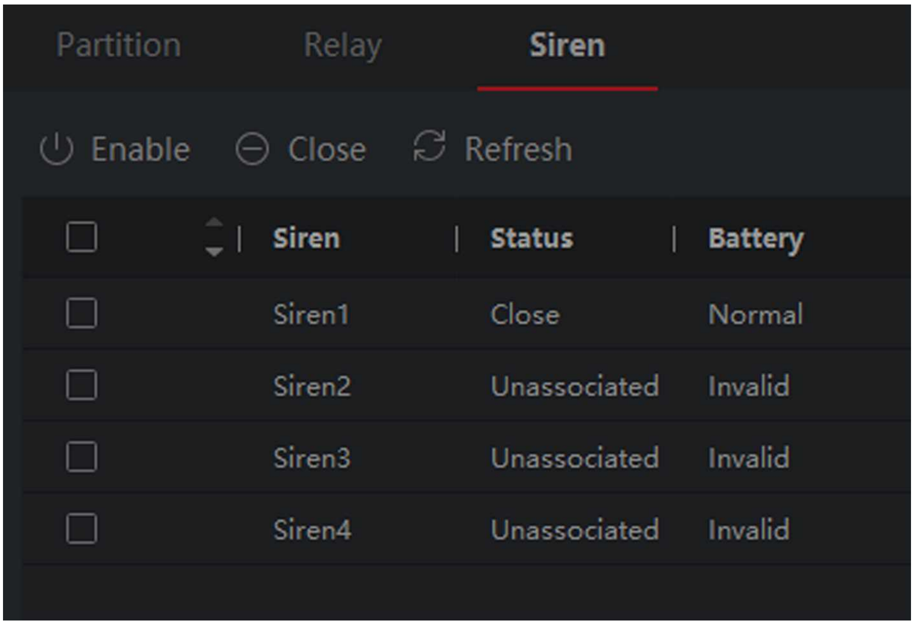
☑	Relay	Status	Relay Associated Event
☑	Relay 1	Unassociated	Manual Control
☑	Relay 2	Unassociated	Manual Control
☑	Relay 3	Unassociated	Manual Control
☑	Relay 4	Unassociated	Manual Control
☑	Relay 5	Unassociated	Manual Control
☑	Relay 6	Unassociated	Manual Control
☑	Relay 7	Unassociated	Manual Control
☑	Relay 8	Unassociated	Manual Control
☑	Relay 9	Unassociated	Manual Control
☑	Relay 10	Unassociated	Manual Control
☑	Relay 11	Unassociated	Manual Control
☑	Relay 12	Unassociated	Manual Control
☑	Relay 13	Unassociated	Manual Control
☑	Relay 14	Unassociated	Manual Control
☑	Relay 15	Unassociated	Manual Control
☑	Relay 16	Unassociated	Manual Control
☑	Relay 17	Unassociated	Manual Control
☑	Relay 18	Unassociated	Manual Control

Figure 5-7 Relay Operation

5.5.5 Operate the Siren

Steps

1. In the client software, click **Security Control Panel → Siren** to enter the page.



□	Siren	Status	Battery
□	Siren1	Close	Normal
□	Siren2	Unassociated	Invalid
□	Siren3	Unassociated	Invalid
□	Siren4	Unassociated	Invalid

Figure 5-8 Siren Operation

2. You can **Enable** or **Close** the selected sirens.

5.6 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.

Note

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.

5.6.1 Add/Edit/Delete Card

You can add tag to the security control panel and you can use the 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 **User Management → Card** to enter the management page.
2. Click **Add** and place a card on the card area of the control panel.
3. Customize a name for the card in the pop-up window.
4. Select the card type and card linked partition.
5. Select the permission for the card.

Note

You should allocate at least a permission for the card.

6. Click **OK** and the tag information will be displayed in the list.

Note

The card supports at least 20-thousand serial numbers.

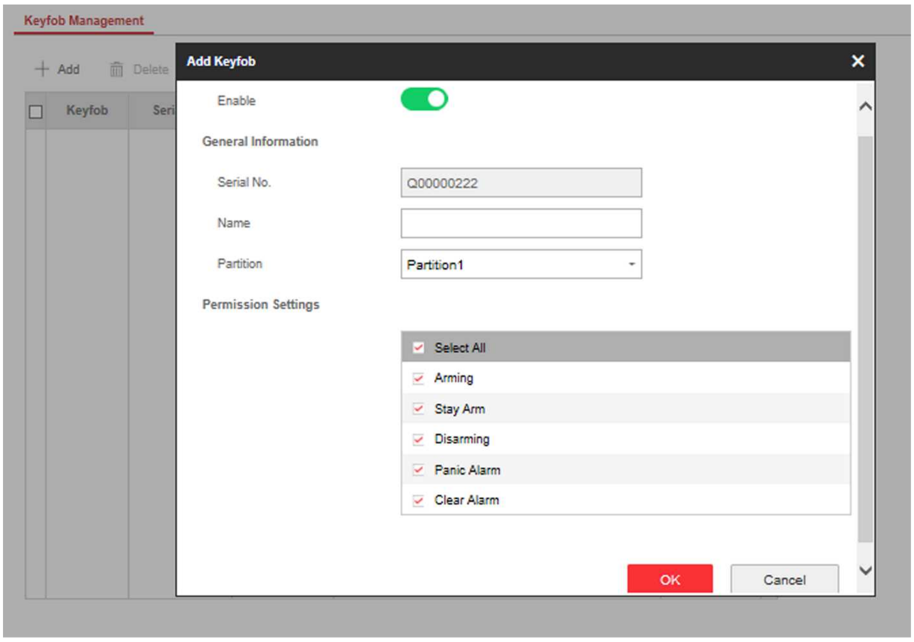
7. **Optional:** Click ✎ and you can change the card name.
8. **Optional:** Delete a single card or check multiple cards and click **Delete** to delete cards in batch.

5.6.2 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 **User Management → Keyfob** to enter the Keyfob Management page.



Keyfob Management

Add Delete

□ Keyfob Seri

Add Keyfob ✕

Enable ●

General Information

Serial No. Q00000222

Name

Partition Partition1

Permission Settings

☑ Select All

☑ Arming

☑ Stay Arm

☑ Disarming

☑ Panic Alarm

☑ Clear Alarm

OK Cancel

Figure 5-9 Keyfob Management

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

   Name

   Customize a name for the keyfob.

   Permission Settings

   Check different items to assign permissions.

   Single Key Settings

   Select from the drop-down list to set I key and II key's functions

   Combination Keys Settings

   Select from the drop-down list to set combination keys' functions.

4. Click **OK**.
5. **Optional:** Click 🖉 to edit the keyfob information.
6. **Optional:** Delete a single keyfob or check multiple keyfobs and click **Delete** to delete the keyfobs in batch.

5.6.3 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 **User Management → User** to enter the User Management page.
2. To compliant the EN requirement, slide the block to enable the installer and manufacturer .

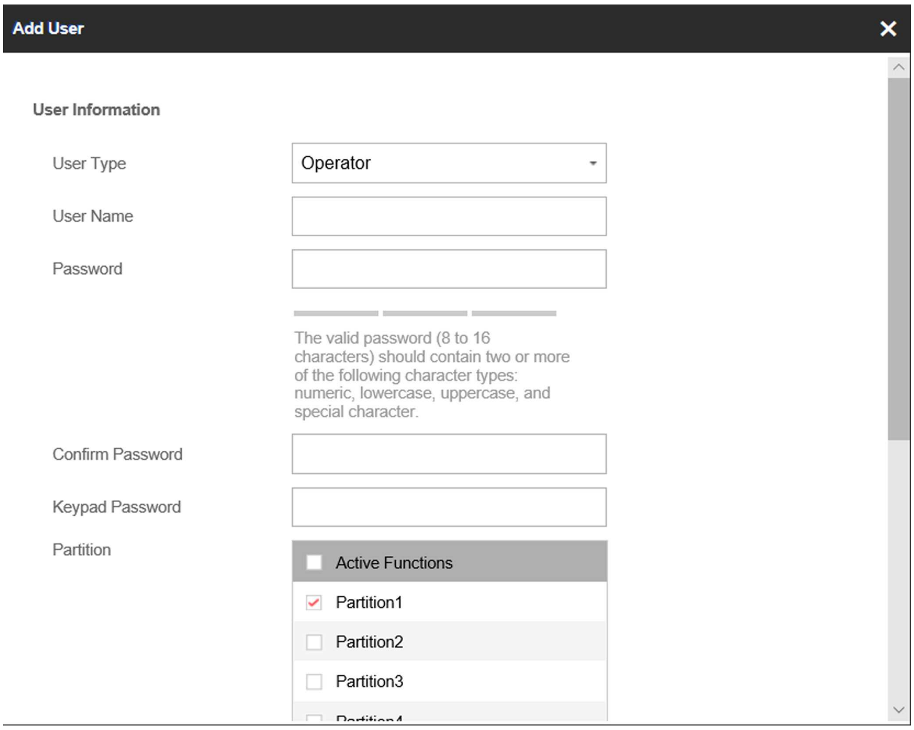
Note

- The default password of the **installer** is **installer12345**, and the default password of the **manufacturer** is **hik12345**. These codes will have to be changed when first connected.
- The Italian user name of admin is **admin**.

Table 5-5 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

3. Click **Add**.
4. Set the new user's information in the pop-up window, including the user type, the user name, and the password.



Add User

User Information

User Type: Operator

User Name

Password

The valid password (8 to 16 characters) should contain two or more of the following character types: numeric, lowercase, uppercase, and special character.

Confirm Password

Keypad Password

Partition

□ Active Functions

☑ Partition1

□ Partition2

□ Partition3

Figure 5-10 Add User Page

5. Set the keypad password (numeric, 8~16 characters).

Note

The keypad password +1 or -1 is the duress code. Use the duress code can operate the keyboard to arm and disarm normally and upload a duress alarm. For example, if the keypad password is 123456, the duress code is 123455 or 123457

6. Check partitions
7. Check the check boxes to set the user permission.

   The user can only operate the assigned permissions.
8. Click **OK**.
9. **Optional:** Enable the user in the Enable User column to allow the enabled user operating the device.
10. **Optional:** Select an user and click **Edit** and you can edit the user's information and permission.
11. **Optional:** Delete a single user or check multiple users and click **Delete** to delete users in batch.

    Note

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

5.6.4 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.

Appendix A. Trouble Shooting

A.1 Communication Fault

A.1.1 IP Conflict

Fault Description:
IP that the panel automatically acquired or set is same as other devices, resulting in IP conflicts.
Solution:
Search the current available IP through ping. Change the IP address and log in again.

A.1.2 Web Page is Not Accessible

Fault Description:
Use browser to access web pages and display Inaccessible.
Solutions:

1. Check whether the network cable is loose and the panel network is abnormal.
2. The panel port has been modified. Please add a port to the web address for further access.

A.1.3 Hik-Connect is Offline

Fault Description:
The web page shows that the Hik-Connect is offline.
Solution:
Network configuration of the panel is error, unable to access extranet.

A.1.4 Network Camera Drops off Frequently

Fault Description:
System reports multiple event logs of IPC disconnection and connection.
Solution:
Check whether the network communication or camera live view is proper.

A.1.5 Failed to Add Device on APP

Fault Description:

When using APP to add devices, it is prompted that the device fails to be added, the device could not be found, etc.

Solution:

Check the web page: whether the Hik-Connect is offline.

A.1.6 Alarm Information is Not Reported to APP/4200/Alarm Center

Fault Description:

After the alarm is triggered, the app/4200/ alarm center does not receive the alarm message.

Solution:

"Message push" - "alarm and tamper-proof notice" is not enabled. You should enable "alarm and tamper-proof notice".

A.2 Mutual Exclusion of Functions

A.2.1 Unable to Enter Registration Mode

Fault Description:

Click the panel function key, and prompt key invalid.

Solution:

The panel is in "AP" mode. Switch the panel to "station" mode, and then try to enter the registration mode again.

A.2.2 Unable to Enter RF Signal Query Mode

Fault Description:

Double-click the control panel function key, and the prompt button invalid.

Solution:

The panel is in "AP" mode. Solution: switch the panel to "station" mode, and then try to enter the RF signal query mode again.

A.3 Zone Fault

A.3.1 Zone is Offline

Fault Description:

View status of zones which displays offline.

Solution:

Check whether the detector reports undervoltage. Replace the detector battery

A.3.2 Zone Tamper-proof

Fault Description:

View status of zones which displays tamper-proof.

Solution:

Make tamper-proof button of the detector holden.

A.3.3 Zone Triggered/Fault

Fault Description:

View status of zones which displays triggered/fault.

Solution:

Reset the detector.

A.4 Problems While Arming

A.4.1 Failure in Arming (When the Arming Process is Not Started)

Fault Description:

When the panel is arming, prompt arming fails.

Solution:

The panel does not enable "forced arming", and when there is a fault in the zone, the arming will fail. Please turn on the "forced arming" enable, or restore the zone to the normal status.

A.5 Operational Failure

A.5.1 Failed to Enter the Test Mode

Fault Description:

Failed to enable test mode, prompting "A fault in the zone".

Solution:

Zone status, alarm status or zone power is abnormal.

A.5.2 The Alarm Clearing Operation on the Panel Does Not Produce the Alarm Clearing Report

Fault Description:

The alarm clearing operation on the panel does not produce the alarm clearing report.

Solution:

In the absence of alarm, no report will be uploaded for arm clearing.

A.6 Mail Delivery Failure

A.6.1 Failed to Send Test Mail

Fault Description:

when configure the mail information, click "test inbox" and prompt test fails.

Solution:

Wrong configuration of mailbox parameters. Please edit the mailbox configuration information, as shown in table 1/1.

A.6.2 Failed to Send Mail during Use

Fault Description:

Check the panel exception log. There is "mail sending failure".

Solution:

The mailbox server has restricted access. Please log in to the mailbox to see if the mailbox is locked.

A.6.3 Failed to Send Mails to Gmail

Fault Description:

The receiver's mailbox is Gmail. Click "Test Inbox" and prompt test fails.

1. Google prevents users from accessing Gmail using apps/devices that do not meet their security standards.

Solution:

Log in to the website (https://www.google.com/settings/security/lesssecureapps), and "start using access of application not safe enough". The device can send mails normally.

2. Gmail does not remove CAPTCHA authentication.

Solution: Click the link below, and then click "continue" (https://accounts.google.com/b/0/displayunlockcaptcha).

A.6.4 Failed to Send Mails to QQ or Foxmail

Fault Description:

The receiver's mailbox is QQ or foxmail. Click "Test Inbox" and prompt test fails.

1. Wrong QQ account or password.

Solution:

the password required for QQ account login is not the password used for normal login. The specific path is: Enter the email account → device → account → to generate the authorization code, and use the authorization code as the login password.

2. SMTP login permission is needed to open.

A.6.5 Failed to Send Mails to Yahoo

Fault Description:

The receiver's mailbox is yahoo. Click "test inbox" and prompt test fails.

1. The security level of mailbox is too high.

Solution:

Go to your mail account and turn on "less secure sign-in".

A.6.6 Mail Configuration

Table A-1 Mail Configuration

Mail Type	Mail Server	SMTP Port	Protocols Supported
Gmail	smtp.gmail.com	587	TLS/STARTTLS (TLS)
Outlook	smtp.office365.com	587	STARTTLS (TLS)
Hotmail	smtp.office365.com	587	STARTTLS (TLS)
QQ	smtp.qq.com	587	STARTTLS (TLSv1.2)
Yahoo	smtp.mail.yahoo.com	587	STARTTLS (TLSv1.2)
126	smtp.126.com	465	SSL/TLS

Mail Type	Mail Server	SMTP Port	Protocols Supported
Sina	smtp.sina.com	25/465/587	SSL/TLS/STARTTLS (SSL/TLS)

Note

About mail configuration:

- SMTP port
  Default to use port 25 without encryption, or using port 465 if SSL/TLS is used. Port 587 is mainly used for STARTTLS protocol mode.
  The STARTTLS protocol mode that is usually used by default when selecting TLS.
- User name
  User name of Outlook and Hotmail require full names, and other email require a prefix before @.

Appendix B. Input Types

Table B-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 siren. 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 siren. There is a configurable interval between alarm and siren output, which allows you to check the alarm and cancel the siren 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 siren. 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 siren. Voice Prompt: Zone X follow alarm.
24H Silence Zone	The zone activates all the time without any sound/siren output when alarm occurs. Audible Response: No system sound (voice prompt or siren).
Panic Zone	The zone activates all the time. Audible Response: Trigger the system sound and siren. Voice Prompt: Zone X panic alarm.
Fire Zone	The zone activates all the time with sound/siren output when alarm occurs. Audible Response: Trigger the system sound and siren. Voice Prompt: Zone X fire alarm.

Input Types	Operations
Gas Zone	The zone activates all the time with sound/siren output when alarm occurs. Audible Response: Trigger the system sound and siren. 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 siren. 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 siren).
Virtual Zone (Keypad/Keyfob)	The system will immediately alarm when it detects triggering event after system armed. Audible Response: Trigger the system sound and siren. 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 siren. 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. • 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 C. Output Types

Table C-1 Output Types

Output Types	Active	Restore
Arming	Arm the control panel	After the configured output delay
Disarming	Disarm the control panel	After the configured output delay
Alarm	When alarm event occurs. The alarm output will be activated after the configured exit/enter delay.	After the configured output delay, disarm the control panel or clear alarm
Zone Linkage	When alarm event occurs, the linked relay will output alarm siganl.	After the configured output duration
Manual Operation	Enable relays manually	Over the triggering time or disable the relays manually

Appendix D. Event Types

Table D-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 E. 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 manufacturer of the equipment.

Table E-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 F. SIA and CID Code

Table F-1 SIA and CID Code

SIA Code	CID Code	Description
BA	E130	Burglary Alarm
BH	R130	Burglary Alarm Restored
HA	E122	Silent Panic Alarm
HH	R122	Silent Panic Alarm Restored
NA	E780	Timeout Alarm
BH	R780	Timeout Alarm Restored
PA	E120	Panic Alarm
PH	R120	Panic Alarm Restored
BA	E131	Perimeter Alarm
BH	R131	Perimeter Alarm Restored
BA	E134	Entry/Exit Alarm
BH	R134	Entry/Exit Alarm Restored
TA	E137	Device Tampered
TR	R137	Device Tamper Restored
TA	E383	Detector Tampered
TR	R383	Detector Tamper Restored
TA	E321	Wireless Siren Tampered
TR	R321	Wireless Siren Tamper Restored
TA	E334	Wireless Repeater Tampered
TR	R334	Wireless Repeater Tamper Restored
ES	E341	Expander or Wireless Device Tampered
EJ	R341	Expander or Wireless Device Tamper Restored

SIA Code	CID Code	Description
PA	E120	Keypad/Keyfob Panic Alarm
MA	E100	Medical Alarm
MH	R100	Medical Alarm Restored
GA	E151	Gas Leakage Alarm
GH	R151	Gas Leakage Alarm Restored
FA	E110	Fire Alarm
FH	R110	Fire Alarm Restored
OP	E401	Disarming
CL	R401	Away Arming
OA	E403	Auto Disarming
CA	R403	Auto Arming
BC	E406	Alarm Clearing
CL	R441	Stay Arming
CD	E455	Auto Arming Failed
BB	E570	Zone Bypassed
BU	R570	Zone Bypass Restored
CT	E452	Late to Disarm
AT	E301	AC Power Loss
AR	R301	AC Power Restored
YT	E302	Low System Battery
YR	R302	Low System Battery Restored
XT	E384	Low Keyfob Battery
XR	R384	Low Keyfob Battery Restored
YM	E311	Battery Fault
YR	R311	Battery Fault Restored
DK	E501	Keypad Locked
DO	R501	Keypad Unlocked
TS	E607	Test Mode Entered
TE	R607	Test Mode Exited

SIA Code	CID Code	Description
RN	E305	Control Panel Reset
UY	E321	Wireless Siren Disconnected
UJ	R321	Wireless Siren Connected
UY	E381	Wireless Detector Disconnected
UJ	R381	Wireless Detector Connected
XT	E384	Wireless Detector Low Voltage
XR	R384	Normal Wireless Detector Voltage
ET	E333	Expander or Wireless Device Disconnected
ER	R333	Expander or Wireless Device Connected
UY	E334	Wireless Repeater Disconnected
UJ	R334	Wireless Repeater Connected
NT	E352	Cellular Data Network Disconnected
NR	R352	Cellular Data Network Connected
NT	E352	SIM Card Exception
NR	R352	SIM Card Restored
NT	E352	Network Flow Exceeded
NT	E351	IP Address Conflicted
NR	R351	Normal IP address
NT	E351	Wired Network Exception
NR	R351	Normal Wired Network
NT	E351	Wi-Fi Communication Fault
NR	R351	Wi-Fi Connected
XQ	E344	RF Signal Exception
XH	R344	Normal RF Signal

SIA Code	CID Code	Description
/	E306	Expander Deleted
/	R306	Expander Added
/	E306	Detector Deleted
/	R306	Detector Added
/	E306	Wireless Repeater Deleted
/	R306	Wireless Repeater Added
/	E306	Wireless Siren Deleted
/	R306	Wireless Siren Added
BA	E130	Burglary Alarm
BH	R130	Burglary Alarm Restored
XT	E338	Low Wireless Device Battery
XR	R338	Low Wireless Device Battery Restored
YC	E354	Uploading Report Failed
YK	R354	Report Uploading Restored
LB	E627	Programming Mode Entered
LX	E628	Programming Mode Exited
CI	E454	Arming Failed
/	R250	Patrol
/	E306	Wireless Device Deleted
/	R306	Wireless Device Added
XT	E384	Low Wireless Siren Battery
XR	R384	Low Wireless Siren Battery Restored
NT	E351	Wired Network/Wi-Fi ATP Failed
NR	R351	Wired Network/Wi-Fi ATP Restored
NT	E352	Cellular Network ATP Failed
NR	R352	Cellular Network ATP Restored

Appendix G. Device in EN Certificate Standard/Basic Standard

Table G-1 User Permission in EN Standard

Function	User Permission in EN Standard				
	Level 1	Level 2		Level 3	Level 4
	Any Body	Basic User	Administrator	Installer	Manufacturer
Arming	x	According to the configured permission	√	√	x
Disarming	x	According to the configured permission	√	√	x
Alarm Clearing	x	According to the configured permission	√	√	x
Walk Test	x	According to the configured permission	√	√	x
Log Query	x	According to the configured permission	√	√	x
Bypass/ Disabling/ Mandatory Arming	x	According to the configured permission	√	√	x
Adding/ Changing Authentication Code	x	According to the configured permission	√	√	√
Adding/ Deleting Level 2 User and Authentication Code	x	According to the configured permission	√	√	x

Adding/ Editing Location	x	x	x	√	x
Exchange Programing/ Firmware	x	x	x	x	√

Table G-2 User Permission in Basic Standard

Function	User Permission in Basic Standard				
	Level 1	Level 2		Level 3	Level 4
	Any Body	Basic User	Administrator	Installer	Manufacturer
Arming	x	According to the configured permission	√	√	x
Disarming	x	According to the configured permission	√	√	x
Alarm Clearing	x	According to the configured permission	√	√	x
Walk Test	x	According to the configured permission	√	√	x
Log Query	x	According to the configured permission	√	√	x
Bypass/ Disabling/ Mandatory Arming	x	According to the configured permission	√		x
Adding/ Changing Authentication Code	x	According to the configured permission	√	√	√
Adding/ Deleting Level 2 User and	x	According to the configured permission	√	√	x

Authentication Code					
Adding/ Editing Location	x	x	√	√	x
Exchange Programing/ Firmware	x	x	√	√	√

See Far, Go Further