Axiom Security Control Panel

User Manual

Legal Information

About this Manual

Please use this user manual under the guidance of professionals.

Trademarks

Disclaimer

HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Symbol Conventions

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

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

Contents

1 Overview 1

2 Access into iVMS-4200/Web Client 2

2.1 Activation Description 2

2.1.1 Activate Device via iVMS-4200 3

2.1.2 Activate via SADP 4

2.1.3 Activate Device via Web Browser 5

2.2 Network Settings 6

2.2.1 Wired Network 6

2.2.2 Wi-Fi 7

2.2.3 Cellular Network 8

2.2.4 Hik-Connect 9

2.3 Alarm Settings 11

2.3.1 Alarm Center 11

2.3.2 Notification Push 12

2.3.3 Zone 12

2.3.4 Alarm Schedule 15

2.3.5 Output 17

2.3.6 Siren 19

2.3.7 Repeater 20

2.4 Video Management 21

2.4.1 Add Cameras to the Security Control Panel 21

2.4.2 Link a Camera with the Zone 22

2.4.3 Set Email to Receive Alarm Video 23
2.4.4 Set Video Parameters 24
2.5 Permission Management 25
2.5.1 Add/Edit/Delete User 25
2.5.2 Add/Edit/Delete Keyfob 27
2.5.3 Add/Edit/Delete Card 29
2.6 System Settings 29
2.6.1 System Settings 29
2.6.2 Security 31
2.6.3 Security 32
2.6.4 Local Log Search 33
2.7 Query 33
2.7.1 Status 33
2.8 Security Control Panel Operation 34
2.8.1 Operate on the Partition 34
2.8.2 Operate on the Zone 35
3 Security Control Panel Management via Mobile Client 36
3.1 Download and Login the Mobile Client 36
3.2 Add Control Panel to the Mobile Client 36
3.3 Add Peripheral to the Control Panel 39
3.4 Set Zone 40
3.5 Add a Camera to the Zone 42
3.6 Arm/Disarm the Zone 43
3.7 Set Arming/Disarming Schedule 44

3.8 Bypass Zone 45
3.9 Add Card 46
3.10 Add Keyfob 48
3.11 Check Alarm Notification 48
3.12 Check System Status (Zone Status/Communication Status) 50

1 Overview

Axiom wireless security control panel, containing 32 wireless zones, supports Wi-Fi, TCP/IP, and 3G/4G communication methods. It also supports ISAPI, Hik-Connect, Contact ID, and NAL2300, which is applicable to the scenarios of market, store, house, factory, warehouse, office, etc.

- TCP/IP, Wi-Fi, 3G/4G network,
- Connects up to 32 wireless zones, 32 wireless outputs, 8 wireless keyfobs, 4 relays, 2 repeaters, 2 sirens.
- Supports up to 13 network users, including 1 installer, 1 administrator, and 11 normal users.
- Supports doorbell function: The detector rings like a doorbell when it is triggered in disarming status.
- Voice prompt.
- Wi-Fi AP mode.
- Configuration via Web client or mobile client.
- Pushes alarm notification via messages, or phone calls.

  Note

  Only device containing 3G/4G communication method supports this function.

- Views live videos and sends emails of alarm linked videos via mobile client.
- Uploads reports to alarm center.
- Long distance two-way communication with AES-128 encryption.
- Supports LED indicator to indicates system status.
- 4520 mAh lithium backup battery, supports up to 12 h power supply.

2 Access into iVMS-4200/Web Client

You can login the iVMS-4200 Client Software or the web client to configure the device's parameters. You can also configure the security control panel's network parameters, alarm, permission, system, log search via the web client.

Note

You should activate the device the first time you access it to the network for safety reasons. For details, see **Device Activation**.

Access to iVMS-4200 Client Software

Download and install the software. Register to the software and add device in **Control Panel → Device Management → Device for Management**

Note

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

After the device is completely added, click **Remote Configuration** to enter the device configuration page. You can configure the device parameters in this page.

Access to Web Client

After the device is connected to the network, you can search the device IP address via the iVMS-4200 client software and the SADP software. Input the searched IP address in the address bar in the web page and press **Enter**. Use the activation user name and password to login. You can configure the device parameters in the web page.

2.1 Activation Description

In order to protect personal security and privacy and improve the network security level, you should activate the device the first time you connect the device to a network.

You can create an activation password to protect your device from logging in by other persons.

2.1.1 Activate Device via iVMS-4200

iVMS-4200 is a PC client to manage and operate your devices. Security control panel activation is supported by the software.

Before You Start

- Get the client software from the supplied disk or the official website ***http://www.hikvision.com/en/*** . Install the software by following the prompts.
- The device and the PC that runs the software should be in the same subnet.

Steps

1. Run the client software.
2. Enter **Device Management** or **Online Device**.
3. Check the device status from the device list, and select an inactive device.
4. Click **Activate**.
5. Create and confirm the admin password of the device.

   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.

6. Click **OK** to start activation.

   Device status will change to **Active** after successful activation.

7. Modify IP address of the device.
   1) Select a device and click **Modify Netinfo** at **Online Device**.
   2) Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking **DHCP**.
   3) Input the admin password of the device and click **OK** to complete modification.

2.1.2 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

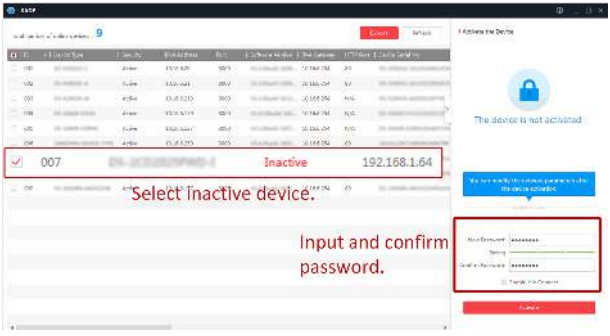
Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the 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.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

2.1.3 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 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 and enter **Live View** page.
4. Modify IP address of the device.
   1) Enter IP address modification page. **Configuration → Network → TCP/IP**
   2) Change IP address.
   3) Save the settings.

2.2 Network Settings

2.2.1 Wired Network

If the device is linked to the wired network, you can set the wired network parameters when you want to change the device IP address and other network parameters.

Steps

Note

The function is not supported by some device models.

1. Click **Communication Parameters → Wired Network Parameters** to enter the Wired Network Parameters page.

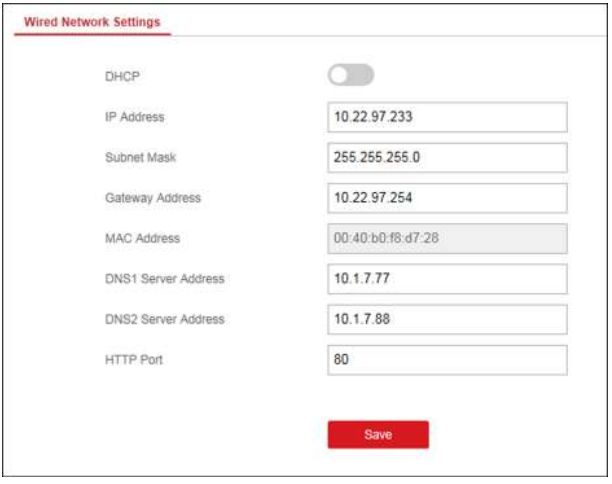


Figure 2-1 Wired Network Settings Page

2. 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**.

   Note

   By default, the HTTP port is 80, which is not editable.

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

2.2.2 Wi-Fi

You can set the Wi-Fi parameters if there are secure and credible Wi-Fi networks nearby.

Steps

1. Click **Communication Parameters → Wi-Fi Parameters** .
2. Click **Wi-Fi** to enter the Wi-Fi page.
3. Connect to a Wi-Fi.
   - Manually Connect: Input the Wi-Fi name and the Wi-Fi password, click **Save**.
   - Select from Network List: Select a target Wi-Fi from the Network list. Click **Connect** and input Wi-Fi password and click **Connect**.
4. Click **WLAN** to enter the WLAN page.

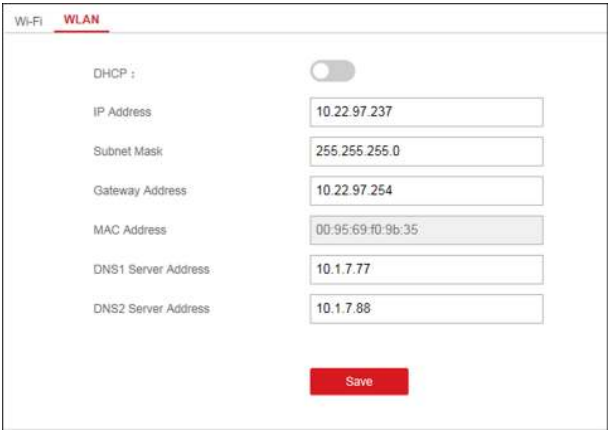


Figure 2-3 WLAN Settings Page

5. Set **IP Address**, **Subnet Mask**, **Gateway Address**, and **DNS Server Address**.

Note

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

6. Click **Save**.

2.2.3 Cellular Network

Set the cellular network parameters if you insert a SIM card inside the device. By using the cellular network, the device can upload alarm notifications to the alarm center.

Before You Start

Insert a SIM card into the device SIM card slot.

Steps

1. Click **Communication Parameters → Cellular Data Network Parameters** to enter the Cellular Data Network Settings page.

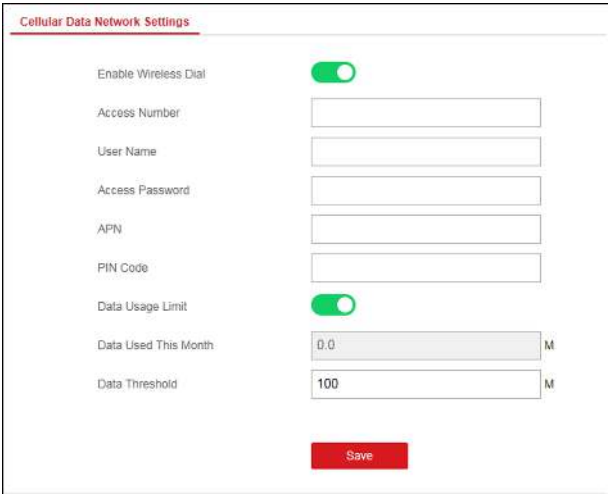


Figure 2-4 Cellular Data Network Settings Page

2. Enable Wireless Dial.
3. Set the cellular data network parameters.

Access Number

Input the operator dialing number.

User Name

Ask the network carrier and input the user name.

Access Password

Ask the network carrier and input the password.

APN

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

Data Usage Limit

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.

Data Used This Month

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

4. Click **Save**.

2.2.4 Hik-Connect

If you want to register the device to the Hik-Connect mobile client for remote configuration, you should set the Hik-Connect registration parameters.

Before You Start

- Connect the device to the network via wired connection, dial-up connection, or Wi-Fi connection.
- Set the device IP address, subnet mask, gateway and DNS server in the LAN.

Steps

1. Click **Communication Parameters → Hik-Connect Registration Parameters** to enter the Hik-Connect Registration Settings page.

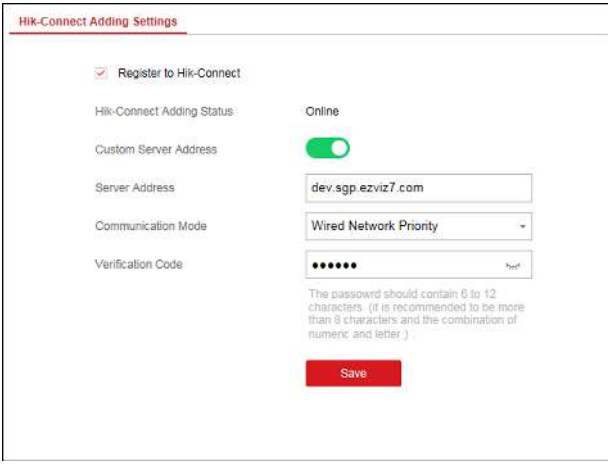


Figure 2-5 Hik-Connect Registration Settings Page

2. Check **Register to Hik-Connect**.

Note

By default, the device Hik-Connect service is enabled.

You can view the device status that in the Hik-Connect server.

3. Enable **Custom Server Address**.

The server address is displayed in the Server Address text box.

4. Select a communication mode from the drop-down list according to the actual device communication method.

Auto

The system will select the communication mode automatically according to the sequence of wired network, Wi-Fi network, and cellular data network.

Wired Network Priority

The system will select wired network only.

Wired &Wi-Fi

The system will select wired network first. If no wired network detected, it will select Wi-Fi network.

Cellular Data Network

The system will select cellular data network only.

5. **Optional:** Change the authentication password.

   Note

   - By default, the authentication password is displayed in the text box.
   - The authentication password should contain 6 to 12 letters or digits. For security reasons, an 8-character password is suggested, which containing two or more of the following character types: uppercases, lowercases, and digits.

6. Click **Save**.

2.3 Alarm Settings

2.3.1 Alarm Center

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

Steps

1. Click **Communication Parameters → Alarm Center Parameters** to enter the Alarm Center Settings page.

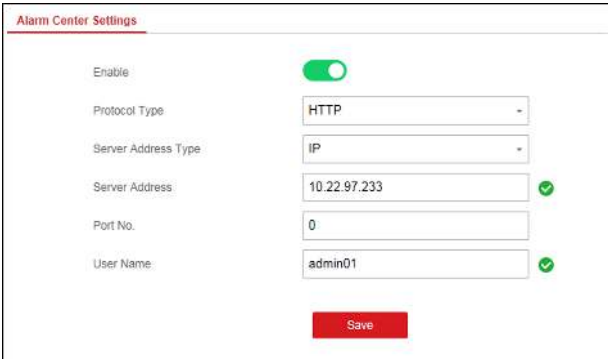


Figure 2-6 Alarm Center Parameters

2. Select a protocol type from the drop-down list, select a server address type from the drop-down list, set the server address, port No., and the user name.

Note

The protocol type HTTP is the Hikvision private protocol.

3. Click **Save**.

2.3.2 Notification Push

When an alarm is triggered, if you want the send the alarm notification to the client, alarm center, cloud or mobile client, you can set the notification push parameters.

Steps

1. Click **Communication Parameters → Message Notification** .
2. Enable the target notification.
   Alarm and Tampering Event Notification

   The device will push notifications when the zone alarm is triggered or the device tamper alarm is triggered or restored.

   Safety Event Notification

   The device will push notifications when fire alarm, gas alarm, or medical alarm is triggered.

   System Status Notification

   The device will push notifications when any status in the system is changed.

   Operation Event Notification

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

   Note

   If you want to send the alarm notifications to the mobile client, you should also set the **Mobile Phone Index**, **SIM Card No.**, and check the **Notification Type**.

3. Click **Save**.

2.3.3 Zone

You can set the zone parameters on the zone page.

Steps

1. Click **Wireless Device → Zone** to enter the Zone page.

Figure 2-7 Zone Page

2. Select a zone and click to enter the Zone Settings page.
3. Edit the zone name.
4. Select a zone type.

Instant Zone

The system will immediately trigger an alarm when it detects triggering event after system armed. Detectors can be set as this type, which can be used in places such as supermarket.

Delayed Zone

Exit Delay: Exit Delay provides you time to leave through the defense area without alarm.

Entry Delay: Entry Delay provides you time to enter the defense area to disarm the system without alarm.

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 keyboard for users.

Note

You can set the delayed time duration in **System → Schedule & Timer** .

Follow Zone

The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise. It is usually set in the living room or hall with perimeter delayed zones at the same time.

Perimeter Zone

The system will immediately alarm when it detects triggering event after system armed. 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 time in case of false alarm. It is usually used in the perimeter area, such as doors and windows.

When the zone is armed, you can set the peripheral alarm delayed time in **System → Schedule & Timer** . You can also mute the siren in the delayed time.

24H Silent Zone

The zone activates all the time without any sound/siren output when alarm occurs. It is usually used in the sites equipped with panic button (e.g., bank, jewelry store).

Panic Zone

The zone activates all the time. It is usually used in the sites equipped with panic button, smoke detector and glass-break detector.

Fire Zone

The zone activates all the time with sound/siren output when alarm occurs. It is usually used in fire hazardous areas equipped with smoke detectors and temperature sensors.

Combustible Gas Zone

The zone activates all the time with sound/siren output when alarm occurs. It is usually used in areas equipped with gas detectors (e.g., the kitchen).

Medical Zone

The zone activates all the time with beep confirmation when alarm occurs. It is usually used in places equipped with medical emergency buttons.

Timeout Zone

The zone activates all the time. It alarms when the event you defined does happen throughout a configurable period. It is usually used in places equipped with magnetic contacts (e.g., fire hydrant box's door).

Shield Zone

Alarms will not be activated when the zone is triggered or tampered. It is usually used to disable faulty detectors .

5. Enable **Stay Arming Bypass**, **Doorbell**, or **Mute** according to your actual needs.

Note

Some zones do not support the function. Refer to the actual zone to set the function.

6. Enable **Link Wireless Detector** , input the serial No., and set the linked camera No.
7. Click **OK**.

Note

After setting the zone, you can enter **Status → Zone** to view the zone status.

2.3.4 Alarm Schedule

You can set the delayed time duration for the delayed zone and the delayed time to exit the zone. You can also set the alarm schedule. The zone will be armed/disarmed according to the configured time schedule.

Steps

1. Click **System → Schedule & Timer** to enter the Schedule & Timer page.

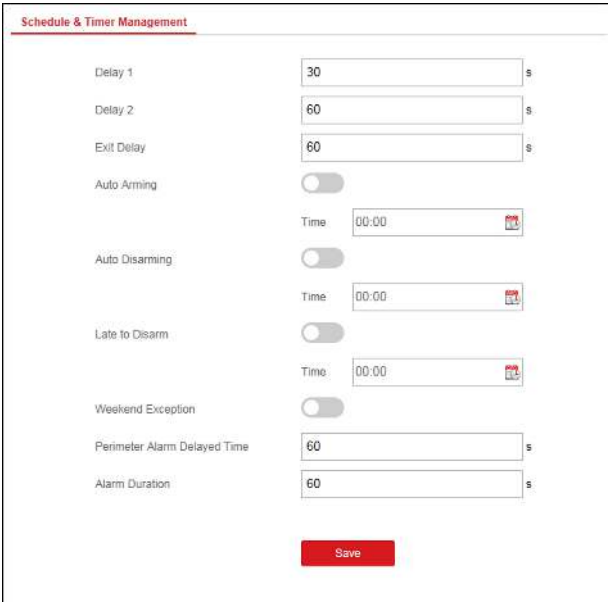


Figure 2-8 Schedule & Timer Page

2. Set time duration of **Delay 1**, **Delay 2**, or **Exit Delay** respectively.
   Delay 1/Delay 2

   If you have set the delayed zone, you can set the delayed time duration here.

   Note

   The available time duration rage is from 5s to 600s.

   Exit Delay

   If the you want to exit the zone without triggering the alarm, you can set the exit delay duration.

   Note

   The available time duration rage is from 5 s to 600 s.

3. **Optional:** Set the following parameters according to actual needs.
   Auto Arming

   Enable the function and set the arming start time. The zone will be armed according to the configured time.

Note

The auto arming time and the auto disarming time cannot be the same.

Auto Disarming

Enable the function and set the disarming start time. The zone will be disarmed according to the configured time.

Note

The auto arming time and the auto disarming time cannot be the same.

Late to Disarm

Enable the function and set the time. If the alarm is triggered after the configured time, the person will be considered as late.

Note

You should enable the Operation Event Notification function in **Communication Parameters → Message Notification** before enabling the Late to Disarm function.

Weekend Exception

Enable the function and the zone will not be armed in the weekend.

Perimeter Alarm Delayed Time

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

Set the time duration of the alarm.

Note

The available time duration range is from 5 s to 600 s.

4. Click **Save**.

2.3.5 Output

If you want to the link the device with a relay output to output the alarm, set the output parameters.

Steps

1. Click **Wireless Device → Output** to enter the Output page.

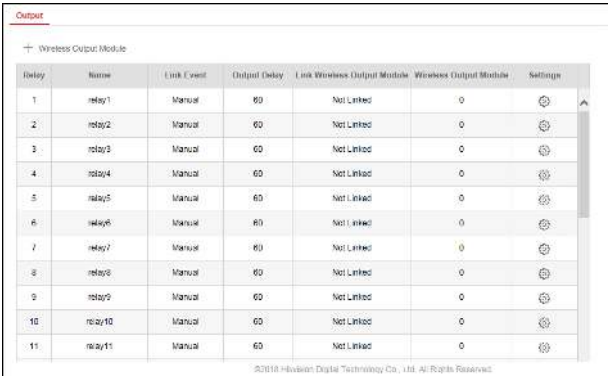


Figure 2-9 Output Page

2. Add a wireless output module.
   1) Click **Wireless Output Module**.

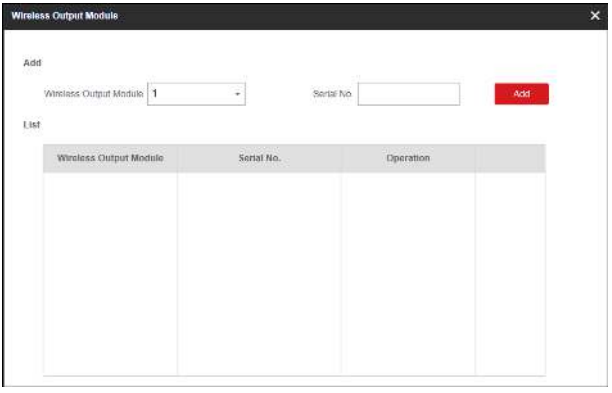


Figure 2-10 Wireless Output Module Settings

   2) Select a wireless output module number from the drop-down list.
   3) Input the serial No. of the wireless output module.
   4) Click **Add**.

3. Click  and the Relay Settings window will pop up.

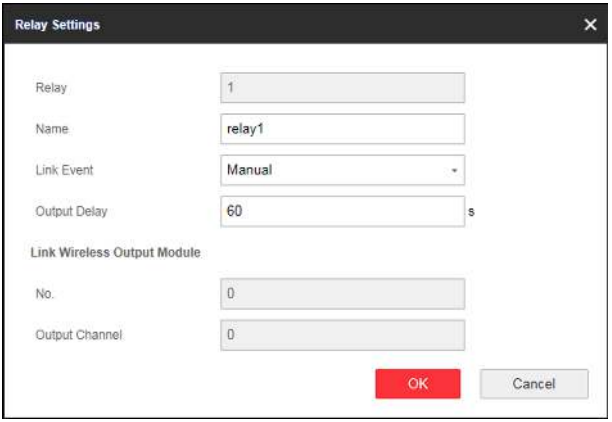


Figure 2-11 Relay Settings Page

4. Edit the relay name, select a link event, and set the output delay time duration.

Note

If the relay has linked to the wireless output module, the wireless output module information will be displayed in the Link Wireless Output Module area.

5. Click **OK**.

Note

After the relay is configured, you can click **Status → Relay** to view the output status.

2.3.6 Siren

If you want to link the security control panel to a siren to report an alarm when the alarm is triggered, you can set the siren parameters.

Steps

1. Click **Wireless Device → Siren** to enter the Siren page.

Figure 2-12 Siren Page

2. Click ⚙ to enter the Siren Settings page.
3. Set the siren name and the volume.

   Note

   The available siren volume range is from 0 to 3.

4. **Optional:** Enable **Link Wireless Siren** and set the siren serial No.

   Note

   Some detectors may not support this function.

5. Click **OK**.

   Note

   After the siren is configured, you can click **Status → Siren** to view the siren status.

2.3.7 Repeater

If the detector is far away from the control panel, set the repeater parameters to enlarge the signal.

Steps

1. Click **Wireless Device → Repeater** to enter the Repeater page.

Figure 2-13 Repeater Page

2. Click to set the repeater parameters.

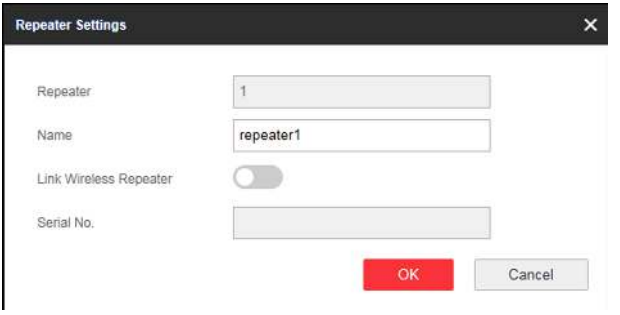


Figure 2-14 Repeater Settings

3. Edit the repeater's name.
4. Enable **Link Wireless Repeater** and input the repeater serial No.
5. Click **OK**.

Note

After setting the repeater, you can enter **Status → Repeater** to view the repeater status.

2.4 Video Management

You can add two network cameras to the wireless security control panel, and link the camera with the selected zone for video monitering. You can also record and view the event video via client and Email.

2.4.1 Add Cameras to the Security Control Panel

Steps

1. Click **System → Network Camera** to enter the network camera management page.

Figure 2-15 Network Camera Management

2. Click**Add**, and enter the basic information of the camera, such as camera name, IP address, and port No..
3. Enter the user name and password of the camera.
4. Click **Save**.

Note

You can add two network cameras for a wireless sec control panel.

1. **Optional:** Click**Edit**or**Delete**to edit or delete the selected camera.

2.4.2 Link a Camera with the Zone

Steps

1. Click **Wireless Device → Zone** to enter the configuration page.

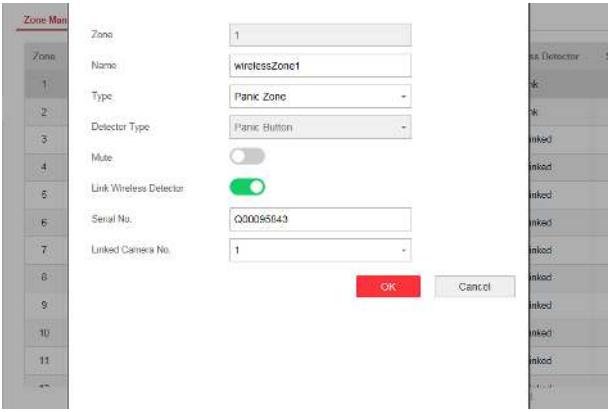


Figure 2-16 Zone Management

2. Select a zone needs video monitoring, and click the **Settings** icon.

Figure 2-17 Zone Configuration

3. Select the **Linked Camera No.**.
4. Click

2.4.3 Set Email to Receive Alarm Video

Steps

1. Click **Communication Parameters → Event Video Transfer via Email** to enter the page.

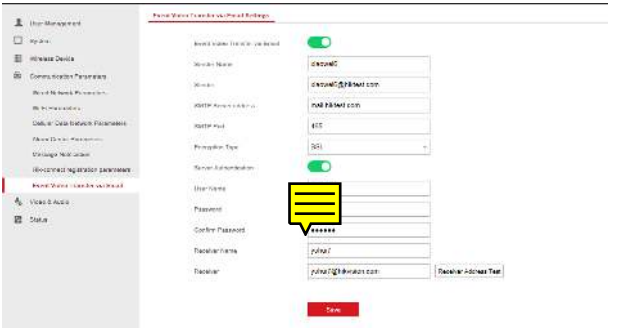


Figure 2-18 Event Video Transfer via Email

2. Click the block to enable the function.
3. Enter the sender's information.
4. Enter the receiver's information.
5. Click **Receiver Address Test** and make sure the address is correct.
6. Click **Sa**

2.4.4 Set Video Parameters

Steps

1. Click **Video&Audio → Event Video Parameters** to enter the page.

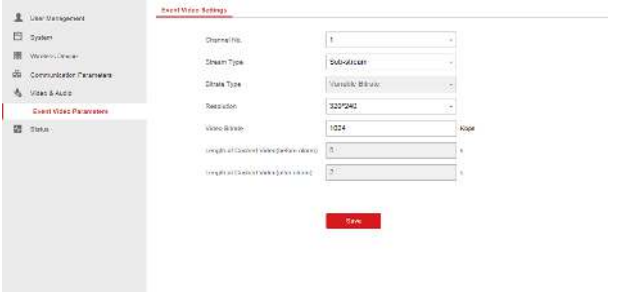


Figure 2-19 Video Settings

2. Select a camera and set the video parameters.
   Stream Ty

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

Video Bitrate

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

2.5 Permission Management

2.5.1 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.

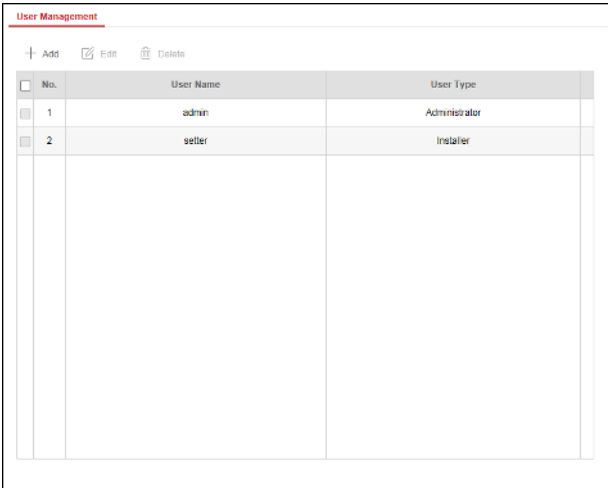


Figure 2-20 User Management Page

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

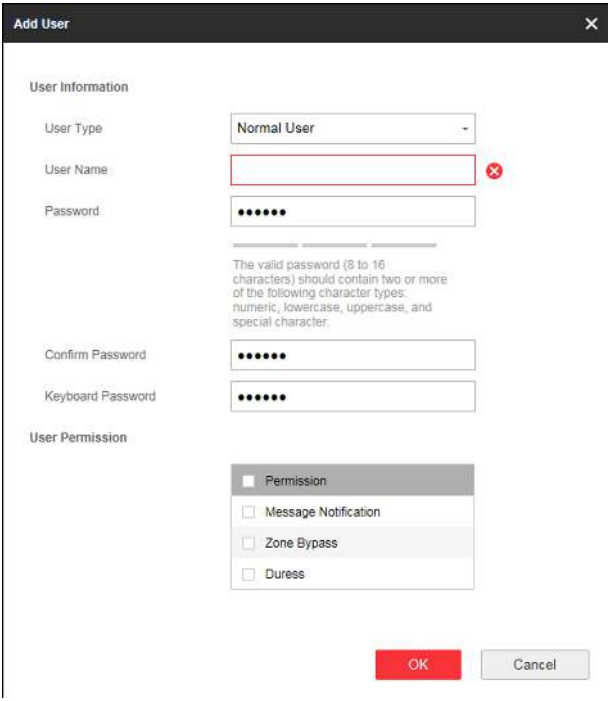


Figure 2-21 Add User Page

4. Check the checkboxes to set the user permission.

   The user can only operate the assigned permissions.

5. Click **OK**.
6. **Optional:** Select an user and click **Edit** and you can edit the user's information and permission.
7. **Optional:** Delete a single user or check multiple users and click **Delete** to delete users in batch.

Note

The admin and the setter cannot be deleted.

2.5.2 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.

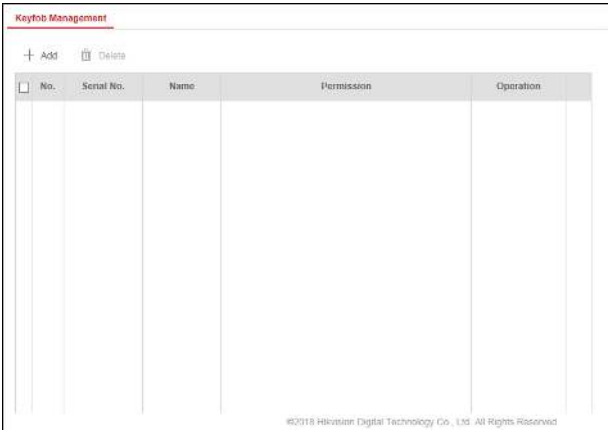


Figure 2-22 Keyfob Management

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.

2.5.3 Add/Edit/Delete Card

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

Steps

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

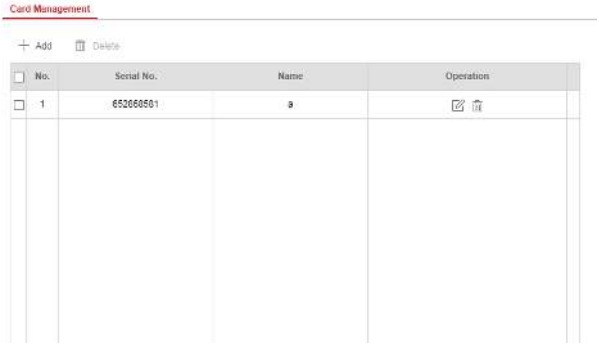


Figure 2-23 Card Management

2. Click **Add** and place a card on the card swiping area.
3. Customize a name for the card in the pop-up window.
4. Click **OK** and the card information will be displayed in the list.
5. **Optional:** Click and you can change the card name.
6. **Optional:** Delete a single card or check multiple cards and click **Delete** to delete cards in batch.

2.6 System Settings

2.6.1 System Settings

You can set the device time zone, synchronize device time, set the DST time, and set option parameters.

Time Management

Click **System → Device Time → Time Management** to enter the Time Management page.

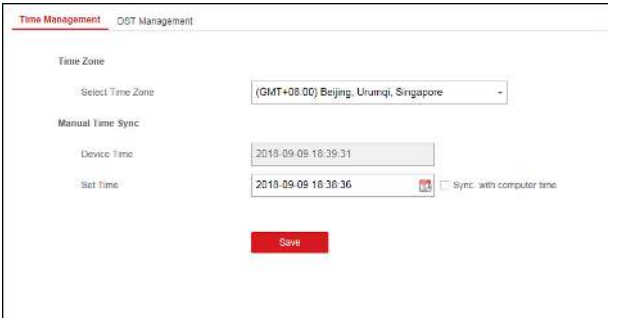


Figure 2-24 Time Management

You can select a time zone form 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.

DST Management

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

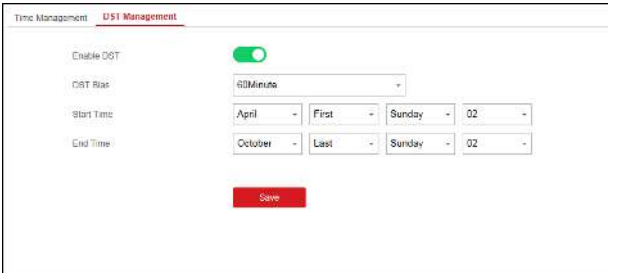


Figure 2-25 DST Management

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

Option Management

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

Set the following parameters as you desired.

Installer Not Allowed

If the option is enabled, the installer cannot login the system and operate the device.

Wireless Peripherals Management

If the option is enabled, the system will detect the peripheral's heartbeat. If no peripheral's heartbeat detected, the system will upload an event.

Disarming Failed: Zone Fault

If the option is enabled and there's fault occurred in the zone, you cannot arm the zone.

System Fault Report

If the option is enabled, the device will upload the system fault report automatically.

Disable Function Key

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

Network Camera Disconnection Detection

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

System Volume

The available system volume range is from 0 to 10.

2.6.2 Security

You can enable or disable SSH (Secure Shell) according to your actual needs. You can also set the user locking parameters and unlock the user.

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

Click **System → Security Settings → Locking User Settings** to enter the target page. You can set the following parameters:

Max. Failure Attempts

If the user continuously input the incorrect password for more than the configured time, 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.

You can also view the locked user information. Click to unlock the account or click **Unlock All** to unlock all locked users in the list.

Click **Save**.

2.6.3 Security

You can enable or disable SSH (Secure Shell) according to your actual needs. You can also set the user locking parameters and unlock the user.

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

Click **System → Security Settings → Locking User Settings** to enter the target page. You can set the following parameters:

Max. Failure Attempts

If the user continuously input the incorrect password for more than the configured time, 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.

You can also view the locked user information. Click to unlock the account or click **Unlock All** to unlock all locked users in the list.

Click **Save**.

2.6.4 Local Log Search

You can search the log on the device.

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

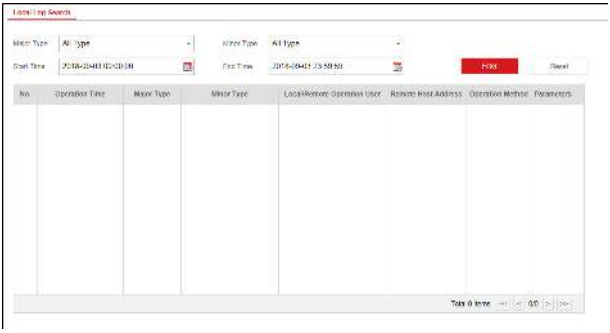


Figure 2-26 Local Log Search Page

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.

2.7 Query

2.7.1 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, battery, communication, and repeater.

2.8 Security Control Panel Operation

You can manage and control partitions and it's related zones in the **Security Control Panel**module.

Note

If there is no **Security Control Panel**dosplayed on the **Control Panel**page, click **Selecting Modules**, and select**Security Control Panel**.

2.8.1 Operate on the Partition

In the **Security Control Panel**module, you can control the selected partition , such as away arming, stay arming, instant arming, disarming, clearing alarm, group bypass, and group bypass restoring.

Note

The wireless security control panel only have one partition.

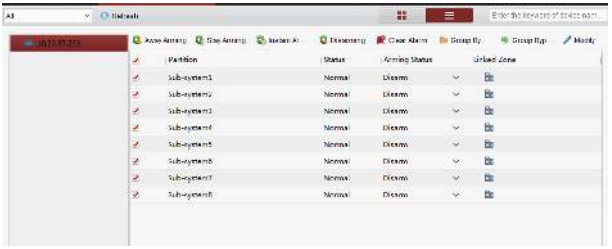


Figure 2-27 Partition Operation

Click**Edit**to edit the partition name and display options.

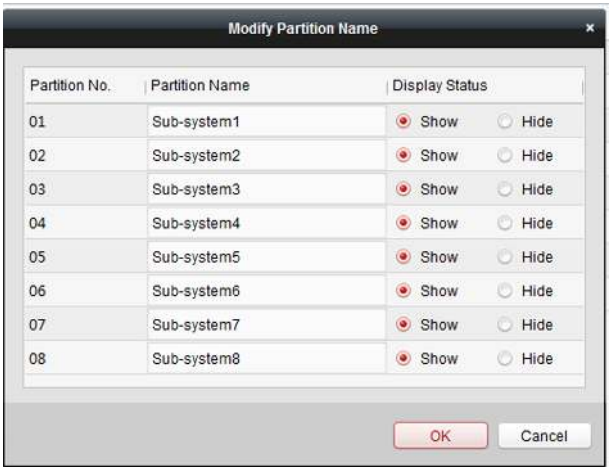


Figure 2-28 Editing Partition Information

2.8.2 Operate on the Zone

Click **Linked Zone**in the partition list of the **Security Control Module**. You can control the selected partition related zones, such as arming, disarming, bypass, or bypass restoring.

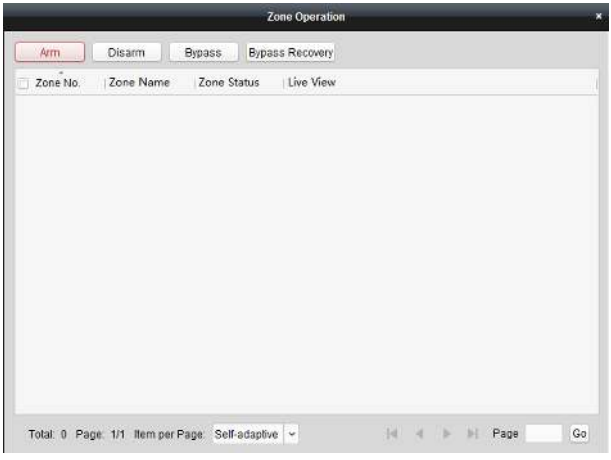


Figure 2-29 Zone Operation

3 Security Control Panel Management via Mobile Client

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

This is the start of your concept.

3.1 Download and Login the Mobile Client

You should download the Hik-Connect mobile client from Google Play (for Android) or App store (for iOS) and login the client before operating the Axiom 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.

3.2 Add Control Panel to the Mobile Client

You should add a control panel to the mobile client before other operations.

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 sticked on the back cover of the control panel.

- Tap → **Manual Adding** to enter the Add Device page. Input the device serial No. with the Hik-Connect Domain adding type.

3. Connect to a network.

1) Tap **Connect to a Network**.

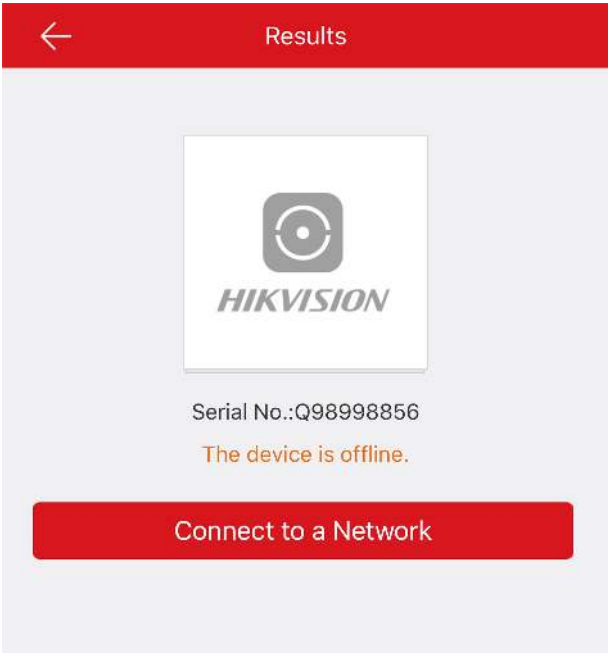


Figure 3-1 Connect to a Network Page

2) Tap **Wireless Connect** on the Adding Type page.

3) Follow the instructions and change the control panel to the AP mode. Tap **Next**.

4) 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.

4. Follow the instructions on the mobile client and connect the mobile phone with the control panel via wireless connection.
5. Create a device password for device activation.

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.

6. Enter the device verification code and tap **OK**.

Note

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

7. Follow the instructions and change the control panel to the Station mode. Tap **Next**.
8. When the control panel is adding completed, tap **Finish**.

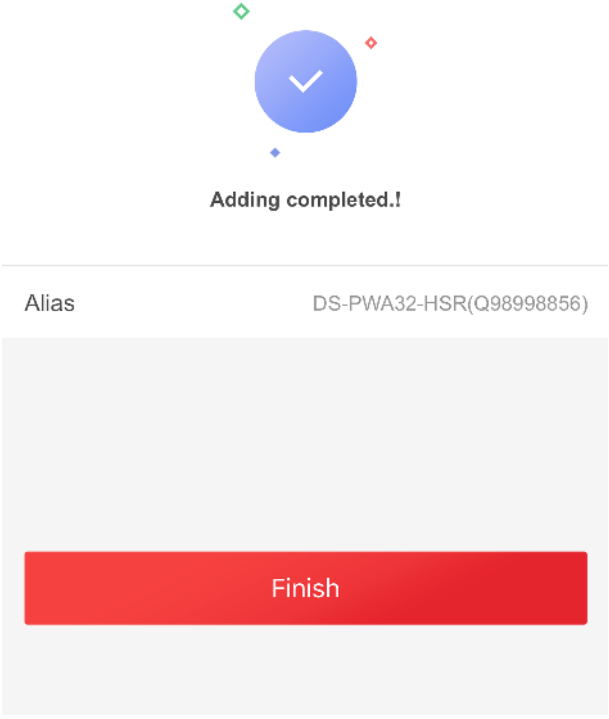


Figure 3-2 Adding Completed Page

The control panel is in the list on the Hik-Connect page.

9. Tap **Finish**.

3.3 Add Peripheral to the Control Panel

You should add peripheral to the control panel before performing other operations such as arming or disarming.

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. Tap  to enter the Scan QR Code page.
2. Scan the peripheral's QR code to add the peripheral.
3. Select a peripheral type, and create a name for the peripheral.

   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 Wireless Device tab.

3.4 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. and the detector type of the zone.

Steps

1. Tap a zone in the Partition page to enter the zone settings page.

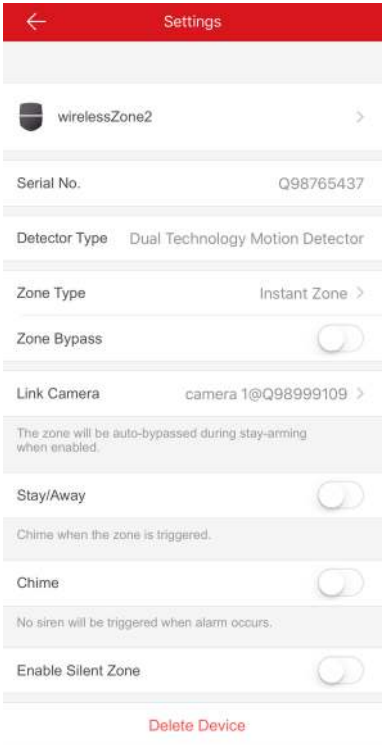


Figure 3-3 Zone Settings Page

2. Set the following parameters as you desired.

Zone Type

Select a zone type from the zone type list. You can tap **?** to view each zones' definition.

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

Enable the function and the zone will be auto bypassed when the zone is in stay or away status.

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.

3.5 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. Tap a security control panel on the Hik-Connect page and tap **Zone** to enter the zone list page.
2. Select a zone to enter the zone settings page.
3. Tap **Link Camera** to enter the Link Camera page.

Figure 3-4 Link Camera Page

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

The selected camera will be linked to the zone. The icon  will be displayed on the right of the zone in the zone list. Tap the icon to view the zone live video.

3.6 Arm/Disarm the Zone

Arm or disarm the zone manually as you desired.

Note

Axiom security control panel supports one partition.

On the Hik-Connect page, tap a security control device to enter the control panel management page. Tap **Away**/**Stay**/**Disarm** to control the partition's status.

You can also tap **Clear Alarm** to clear the alarm when an alarm is triggered.

Figure 3-5 Control Panel Management Page

3.7 Set Arming/Disarming Schedule

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

Tap a security control panel to enter the control page and tap  or  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, and siren delay time.

Figure 3-6 Arming or Disarming Schedule Page

3.8 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. Select a zone in the Zone tab of the Partition page.
2. Select a zone and enter the Settings page.

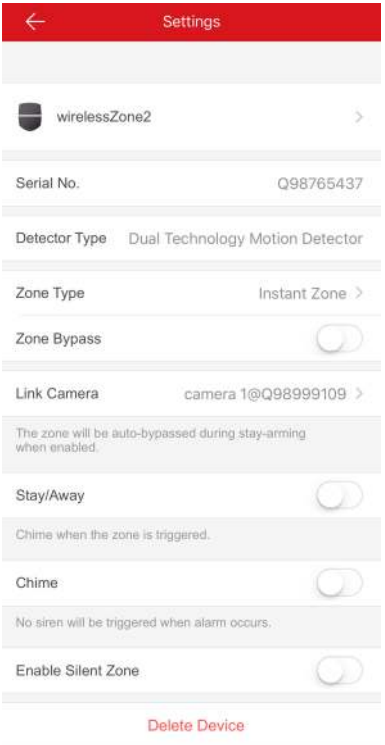


Figure 3-7 Zone Settings Page

3. 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.

3.9 Add Card

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

Steps

1. Select a control panel on the Hik-Connect page to enter the control panel management page.

Figure 3-8 Control Panel Management Page

2. Tap  → **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 alias and tap **Finish**.

   Note

   The alias should contain 1 to 32 characters.

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

3.10 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. Tap  to enter the Scan QR Code page.
2. Scan the keyfobs' QR code to add the keyfob.
3. Create a name for the keyfob and tap **OK**.

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

3.11 Check Alarm Notification

When an alarm is triggered, and the 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 **Message** in the Hik-Connect page to enter the Message page.

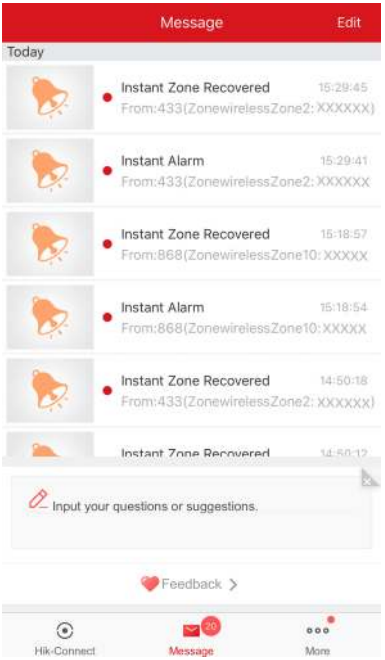


Figure 3-9 Message Page

All alarm notifications are listed in Message page.

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

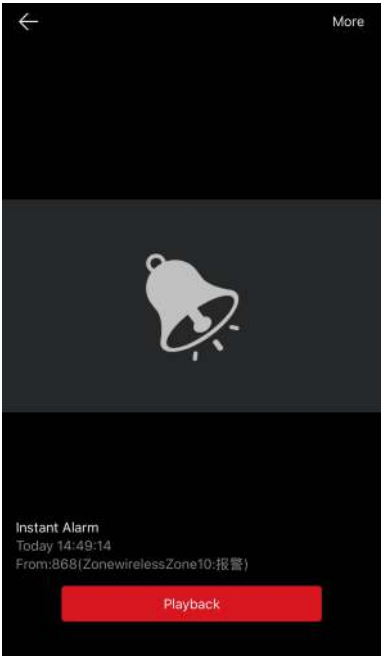


Figure 3-10 Alarm Notification Page

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

3.12 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

Tap  to enter the control panel settings page. You can view the device communication status, including the battery, Ethernet network, Wi-Fi, mobile network, and data usage.


See Far, Go Further