Hik IP Receiver Pro

User Manual

Legal Information and Symbol Conventions

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***)company website.
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.
Trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISIONOUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISIONOUR COMPANY BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISIONOUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISIONOUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISIONOUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW.

ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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

Chapter 1 Overview

1.1 Introduction

As a protocol converter, the Hik IP Receiver Pro connects devices and ARC (alarm receiving center) for data transmission, through LAN or WAN.

There are three methods of adding devices to Hik IP Receiver Pro.

- You can add devices (including AX Pro/AX Hub security control panel, network camera, NVR, and DVR.) managed on the Hik-ProConnect to the Hik IP Receiver Pro to integrate them to the ARC through protocols.
- You can add single or multiple security control panels to the Hik IP Receiver Pro through ISUP5.0 protocol.
- You can add single or multiple third-party devices to the Hik IP Receiver Pro with device name and account ID.

After correct configurations on the Hik IP Receiver Pro and the ARC, the Hik IP Receiver Pro can receive and transmit alarms and alarm-related videos or images from devices on the Hik IP Receiver Pro to the ARC for notification and video or image verification.

This manual guides you to configure the Hik IP Receiver Pro. To ensure a proper usage and stability of the Hik IP Receiver Pro, refer to the contents below and read the manual carefully before installation and operation.

1.2 Running Environment

The following is recommended system requirement for running the Hik IP Receiver Pro.

Operating System

Microsoft Windows 10 (64-bit) / Windows Server 2012 R2 (64-bit) / Windows Server 2016 (64-bit)

Note

For Windows Server 2012 R2 (64-bit), the patch KB2999226 is required to be installed.

CPU

Intel Core i5-7500 @ 3.0 GHz, four-core or above

RAM

8 GB or above

NIC

Gigabit-NIC with latest driver

Note

If the computer with Hik IP Receiver Pro installed goes into sleep mode, an exception will occur to Hik IP Receiver Pro. It is required to disable the sleep mode of your PC to ensure that Hik IP Receiver Pro works properly.

1.3 What's New

The following shows the changes in new versions of Hik IP Receiver Pro.

What's New in Version 1.4.0

1. Added the ***Configure Hot Spare Settings*** describing how to configure a Hik IP Receiver Pro service as a host server or a spare server.
2. Updated the ***Search History Event*** . Supports performing two-way audio. Supports automatic refresh.
3. Updated the ***Enable Alarm Monitor and Check Device's Alarms*** . Supports starting two-way audio on the page where the URL on the Alarm Monitor page is opened.
4. Updated the ***Add Hikvision Device(s) Managed on Hik-ProConnect*** . For devices managed on the Hik-ProConnect, supports viewing details about site.
5. Updated the ***Configure Protocol Parameters*** . On the Protocol page, added the function of viewing the alarm massage example of a selected protocol. Added the function of enabling/disabling device heartbeat and setting device heartbeat interval for Manitou protocol.
6. Updated the ***Event Codes of Encoding Device*** . Added four events for encoding devices.
7. Updated the ***Running Environment*** . It is required to disable the sleep mode of your PC to ensure that Hik IP Receiver Pro works properly.

Chapter 2 Installation

You can install the Hik IP Receiver Pro service to your server or PC, and activate the service. Then you can use the service remotely.

2.1 Port Instruction

Before installing Hik IP Receiver Pro service, ensure the default ports of the Hik IP Receiver Pro are not used by other services, otherwise the Hik IP Receiver Pro service will be unavailable.

Platform Ports

- 80 (TCP) : HTTP port
- 443 (TCP) : HTTPS port

Device Ports

Port Number	Protocol	Port Description
7661	TCP	Used for registering devices to the Hik IP Receiver Pro by ISUP5.0 protocol.
7662	TCP	Used for sending alarms from ISUP5.0 security control devices to the Hik IP Receiver Pro.
7091	TCP	Used for sending picture data from ISUP5.0 security control devices to the Hik IP Receiver Pro.

Note

Scan the QR code below to get more details.

2.2 Install Hik IP Receiver Pro

You can install the Hik IP Receiver Pro service on a computer or server. After that, you can start the service, stop the service or exit the service by watchdog.

Steps

1. Right-click the program file and run as the administrator to enter the welcome panel.
2. Click **Next**.
3. **Optional:** Click **Browse...** to select the path of legacy configuration files and click **Next**.

   Note

   If you have kept the configuration files of an uninstalled Hik IP Receiver Pro, the Hik IP Receiver Pro will reuse the files saved in the selected path when you install a new version.
4. Click **Browse...** and select a proper directory as required to install the service.
5. Click **Next** to continue.
6. **Optional:** Edit the HTTP port if the port number is conflict, otherwise the installation cannot be continued.
7. Click **Install** to begin the installation.
8. Read the post-install information and click **Finish** to complete the installation.

Result

After successful installation, the Watchdog service will get started and hide in the notification area of the desktop. Right-click and select the option to stop the service, start the service, or exist the service.

Note

- If you install Hik IP Receiver Pro remotely, you need to log into the local computer to show the Watchdog service.
- A window will pop up asking whether to keep the configuration file when you re-install the Hik IP Receiver Pro. You can choose to keep it or not.

2.3 Activate Hik IP Receiver Pro

By default, Hik IP Receiver Pro predefined the administrator user named **admin**. When you log in to Hik IP Receiver Pro for the first time, you are required to create a password for the admin user to activate Hik IP Receiver Pro before you can properly configure and operate.

Before You Start

Make sure you have installed the Hik IP Receiver Pro service.

Steps

1. Enter the address of the computer or server running with Hik IP Receiver Pro service and port number in the address bar of the web browser, and press **Enter** key.

Note

The default port is 80. For configuring the port number, see ***Edit Port*** for details.

Example

If the IP address of the computer running Hik IP Receiver Pro service is 172.6.21.96, and the port number is 80, and you should enter ***http://172.6.21.96:80*** in the address bar.

2. Enter the password and confirm password for the admin user in the pop-up Activate Hik IP Receiver Pro window.

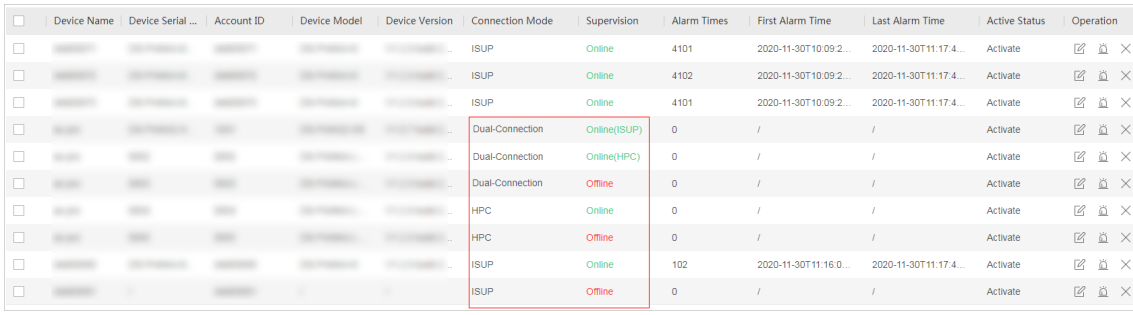
Note

We highly recommend you change the 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.

3. Click **Activate**.

Chapter 3 Device Management

The Hik IP Receiver Pro can manage multiple device types, e.g. network camera, DVR, NVR, and AX Pro security control panel. After adding devices to the Hik IP Receiver Pro and configuring alarm service and zone, the Hik IP Receiver Pro can transmit alarms and images/videos from these devices to ARC.



Device Name	Device Serial ...	Account ID	Device Model	Device Version	Connection Mode	Supervision	Alarm Times	First Alarm Time	Last Alarm Time	Active Status	Operation
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	ISUP	Online	4101	2020-11-30T10:09:2...	2020-11-30T11:17:4...	Activate	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	ISUP	Online	4102	2020-11-30T10:09:2...	2020-11-30T11:17:4...	Activate	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	ISUP	Online	4101	2020-11-30T10:09:2...	2020-11-30T11:17:4...	Activate	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Dual-Connection	Online(ISUP)	0	/	/	Activate	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Dual-Connection	Online(HPC)	0	/	/	Activate	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Dual-Connection	Offline	0	/	/	Activate	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	HPC	Online	0	/	/	Activate	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	HPC	Offline	0	/	/	Activate	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	ISUP	Online	102	2020-11-30T11:16:0...	2020-11-30T11:17:4...	Activate	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	ISUP	Offline	0	/	/	Activate	

Figure 3-1 Device List

Add Device

You can add Hikvision devices managed in the Hik-ProConnect to the Hik IP Receiver Pro, add security control panels by ISUP5.0 protocol, and add third-party devices to the Hik IP Receiver Pro.

Connection Mode

ISUP

If the device only supports direct connection, the connection mode will be displayed as **ISUP**.

Dual-Connection

If the device added by Hik-ProConnect supports direct connection, the connection mode will be displayed as **Dual-Connection**. In this mode, Hik IP Receiver Pro receives alarms by ISUP5.0 protocol in priority, and the **Supervision** of online device will be displayed as **Online(ISUP)**. If an exception occurs when receiving alarm by ISUP5.0 protocol, Hik IP Receiver Pro receives alarms through Hik-ProConnect, and the **Supervision** of online device will be displayed as or **Online(HPC)**.

Online(ISUP)

The device is connected to the Hik IP Receiver Pro by direct connection.

Online(HPC)

The device is connected to the Hik IP Receiver Pro by Hik-ProConnect.

HPC

If the device added by Hik-ProConnect does not support direct connection, the connection mode will be displayed as **HPC**.

Enable Receiving Alarm and Set Zone

After adding devices to the Hik IP Receiver Pro, you can enable alarm service and add zone for these devices, and then link channels to zones to transmit videos from linked channels to ARC.

3.1 Add Hikvision Device(s) Managed on Hik-ProConnect

You can add Hikvision devices managed on Hik-ProConnect to the Hik IP Receiver Pro. After adding the devices to Hik IP Receiver Pro, the Hik IP Receiver Pro can transmit alarms triggered by these devices to ARC.

Before You Start

Make sure you have accessed the Hik IP Receiver Pro to Hik-ProConnect. See ***Access Hik-ProConnect*** for details.

Steps

Note

This function should be supported by device. Devices including AX Pro security control panel, NVR, DVR, and network camera support this function.

1. On the Device page, click **Add** to enter the Add Device page.
2. Check **Devices on Hik-ProConnect** as the **Device Type**.

   Devices managed on Hik-ProConnect are displayed in the **Choose Device** field.
3. Check devices and click **Next**.
4. Enter account ID.

   Note

   Up to 31 characters are allowed, and it should be the same with the account ID configured on ARC.
5. Check to-be-added devices and click **OK**.

   The added devices are displayed on the **Device** page.

   Note

   - If the device supports direct connection, the device's online status will be displayed as **Online (ISUP)**.
   - To make sure the device supports direct connection, you should configure external IP address and external port beforehand. See ***Set Port Mapping*** for details.

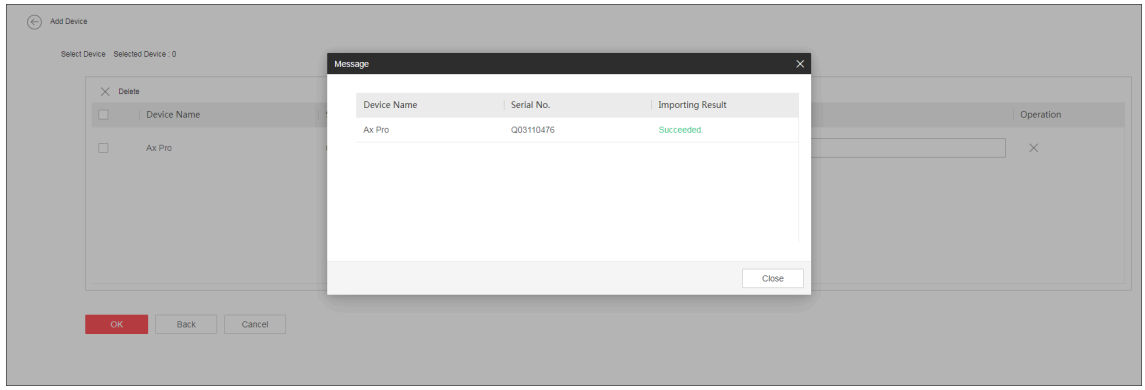


Figure 3-2 Add a Device Managed on Hik-ProConnect

6. **Optional:** Perform the following operations if necessary.

Edit Device	For devices connected in HPC mode, you can click to view the name and edit the account ID of the device. For devices connected in Dual Connection mode, you can edit the account ID and view the device name, device ID and device key.
	Note • Click → **View** to view the site information of the selected device. • You can click to view the device key.
Delete Device	Click × to delete a device; or check multiple devices and click **Delete** to delete the checked devices.
Enable Alarm Service and Set Zone	See ***Set Zone*** for details.
Synchronize Device Information	Select devices, and click **Synchronize Device Information** to Synchronize device information excluding alarm-related information from Hik-ProConnect.

3.2 Add Single ISUP5.0 Security Control Panel

You can add a security control panel to the Hik IP Receiver Pro by ISUP5.0 protocol.

Steps

1. On the Device page, click **Add** to enter the Add Device page.
2. Check **ISUP5.0 Security Control Panel** as the **Device Type**.
3. Select **Single** as the **Adding Mode**.
4. Enter device name, device account ID, and key.

Note

- For account ID, up to 31 characters are allowed, and it should be the same with the device ID.
- For key, up to 32 characters are allowed, and it should be the same with ISUP login password.

5. Click **OK**.

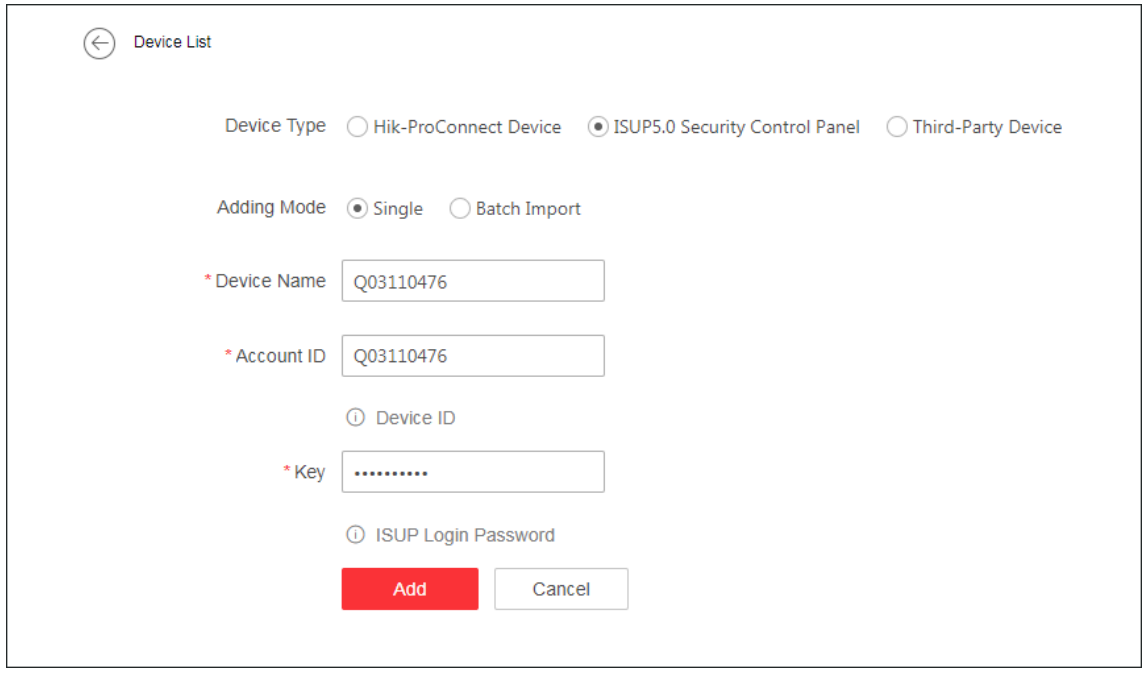


Figure 3-3 Add a Single ISUP 5.0 Security Control Panel

6. **Optional:** Perform the following operations if necessary.

Edit Device	Click to edit device's account ID, device name, and key.
Delete Device	Click × to delete a device; or check multiple devices and click **Delete** to delete the selected devices.
Enable Alarm Service	See ***Set Zone*** for details.
Synchronize Device Information	Select devices, and click **Synchronize Device Information** to synchronize device information excluding alarm information from the devices.

3.3 Add ISUP5.0 Security Control Panels in a Batch

When there are multiple security control panels supporting ISUP5.0 protocol to add, you can enter the device information in a predefined template and then import it to the Hik IP Receiver Pro to add them in a batch.

Steps

1. On the Device page, click **Add** to enter the Add Device page.

2. Check **ISUP5.0 Security Control Panel** as the **Device Type**.
3. Select **Batch Import** as the **Adding Mode**.
4. Click **Export** and save the predefined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added.

   Account ID

   Up to 31 characters are allowed, and it should be the same with the device ID.

   Device Name

   You can custom the device name.

   Key

   Up to 32 characters are allowed, and it should be the same with ISUP login password.
6. Click **Import** and select the edited template.
7. Click **OK** to import the device information to the Hik IP Receiver Pro.

   The devices are added to the Hik IP Receiver Pro and displayed on the device list.
8. **Optional:** Perform the following operations if necessary.

Edit Device	Click to edit device's account ID, device name, and key.
Delete Device	Click × to delete a device; or check multiple devices and click **Delete** to delete the checked devices.
Enable Alarm Service	See ***Set Zone*** for details.
Synchronize Device Information	Select devices, and click **Synchronize Device Information** to synchronize device information excluding alarm information from the devices.

3.4 Add Single Third-Party Device

You can add a third-party device to the Hik IP Receiver Pro by entering device account ID and device name.

Steps

1. On the Device page, click **Add** to enter the Add Device page.
2. Check **Third-Party Device** as the **Device Type**.
3. Select **Single** as the **Adding Mode**.
4. Enter account ID and device name.

   Note

   Up to 31 characters are allowed, and it should be the same with the account ID configured on ARC.
5. Click **OK**.

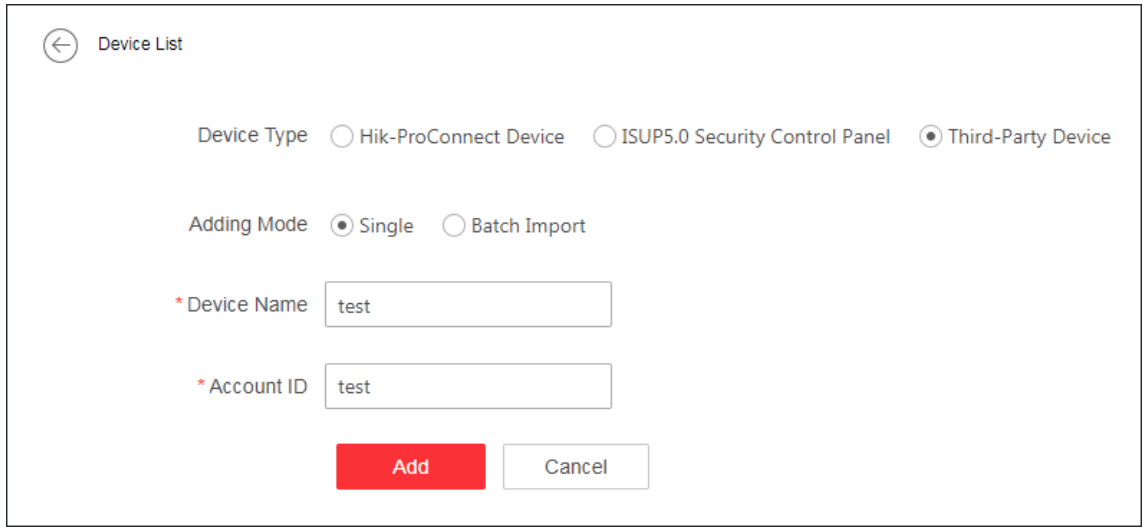


Figure 3-4 Add a Third-Party Device

6. **Optional:** Perform the following operations if necessary.

Edit Device	Click to edit device's account ID and device name.
Delete Device	Click × to delete a device; or check multiple devices and click **Delete** to delete the selected devices.
Enable Alarm Service and Set Zone	See ***Set Zone*** for details.
Synchronize Device Information	Select devices, and click **Synchronize Device Information** to synchronize device information excluding alarm information from the devices.

3.5 Add Third-Party Devices in a Batch

When there are multiple third-party devices to add, you can enter the device information in a predefined template and then import it to the Hik IP Receiver Pro to add them in a batch.

Steps

1. On the Device page, click **Add** to enter the Add Device page.
2. Check **Third-Party Device** as the **Device Type**.
3. Select **Batch Import** as the **Adding Mode**.
4. Click **Export** and save the predefined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added.

Account ID

Up to 31 characters are allowed, and it should be the same with the account ID configured on the ARC.

Device Name

You can custom the device name.

6. Click **Import** and select the edited template.
7. Click **OK** to import the device information to the Hik IP Receiver Pro.

The devices are added to the Hik IP Receiver Pro and displayed on the device list.

8. **Optional:** Perform the following operations if necessary.

Edit Device	Click to edit device's account ID and device name.
Delete Device	Click × to delete a device; or check multiple devices and click **Delete** to delete the checked devices.
Enable Alarm Service and Set Zone	See ***Set Zone*** for details.
Synchronize Device Information	Select devices, and click **Synchronize Device Information** to Synchronize device information excluding alarm-related information from devices.

3.6 Enable Receiving Alarm and Set Partition (Area)

To receive and transmit alarms sent by devices added to Hik IP Receiver Pro, you should enable alarm service first. To manage multiple zones systematically, you can add partitions (areas) where different zones can be added and managed.

Before You Start

Make sure you have added at least one device to the Hik IP Receiver Pro. See ***Device Management*** for details.

Only encoding device and third-party devices support adding a partition (area).

Steps

1. On the **Device** page, select a device and click in the **Operation** column.
2. Check **Enable Alarm Service** to enable alarm service.

Note

By default, it is enabled. If this function is disabled, the Hik IP Receiver Pro will not receive or transmit alarm information from this device.

3. Click **Add Partition(Area)** to open the Add window.
4. Enter the Partition (Area) No. and name.
5. Click **OK** to save the Partition (Area).

Note

By default, the system will add a default partition(area) for the device if there is no partition (area) of the device before. You can edit or delete the partition (area) if you need.

6. **Optional:** Perform the following operation(s).

Edit Partition (Area)	Hover the cursor on the added partition (area) and click to edit the partition (area) name.
Delete Partition (Area)	Hover the cursor on the added partition (area) and click to delete the partition (area).

What to do next

Add zone(s) and link channel(s) to zones for the partition (area). See ***Set Zone*** for details.

3.7 Set Zone

For encoding device and third-party device, only if you have set zones and linked channels to zones can the Hik IP Receiver Pro can transmit alarms and videos from the linked channels to ARC for verification. For AX Pro with zones and linked channels already configured on the device configuration page, the Hik IP Receiver Pro can transmit alarms and videos once the alarm service is enabled.

Before You Start

- Make sure you have added at least one device to the Hik IP Receiver Pro. See ***Device Management*** for details.
- If you are going to link channels to devices managed by the Hik-ProConnect, make sure you have accessed the Hik IP Receiver Pro to Hik-ProConnect. See ***Access Hik-ProConnect*** for details.

Steps

1. On the **Device** page, select a device and click in the **Operation** column.
2. Select a partition (area).

   Note

   Only encoding device and third-party device support adding a partition (area).
3. Add a zone.

   Note

   If you have already added the zone which needs a linkage between channels, skip this step and just select the zone.

   1) Hover the cursor on a partition (area) and click **+** to open the Add window.
   2) Enter the zone No. and zone name.

   Note

   - For encoding devices and third-party devices, you need to add zones for them on the Hik IP Receiver Pro. Make sure the zone information you set are the same with the zone information

set on ARC, or the Hik IP Receiver Pro will fail to transmit videos from the zones-linked channels to ARC.

- For AX Pro, the Hik IP Receiver Pro will automatically get zone information and linked channels configured on the device. So you do not need to add zones for AX Pros on the Hik IP Receiver Pro.

4. Link channel(s) to zone.

1) Select a zone and click **Select Channels** to enter the Link Channel page.

2) Select a device on the left.

Channels of the device are displayed on the right.

Note

- For devices added by Hik-ProConnect, you can only select encoding devices in the same site with the AX Pro on Hik-ProConnect. For security control panels added by ISUP5.0 protocol, you can select encoding devices in any site.
- For encoding devices, you can only link their own channels to their zones.
- For third-party devices, you can link channels of devices in any other sites to their zones, but the third-party devices and the linked channels should share the same ARC.

3) Check channels to be linked and click **Save**.

Note

No more than four channels can be linked to a zone.

The linked channels are displayed on the alarm service and zone settings page.

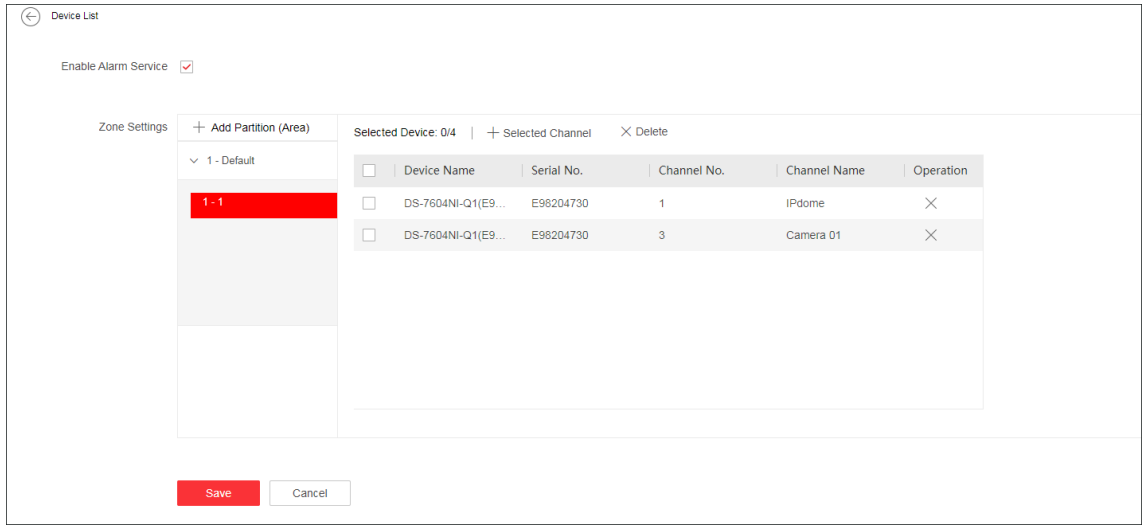


Figure 3-5 Set Zone

5. Optional: Perform the following operation(s).

Edit Zone	Hover the cursor on a zone and click to edit zone name or change the partition (area) of the zone.

Delete Zone	Hover the cursor on a zone and click to delete the zone.
Cancel Linkage Between Channel and Zone	After selecting a zone, check linked channel(s) on the right and click **Delete** to cancel the linkage between channel(s) and the zone.

Chapter 4 Basic Configuration

Configuration module provides basic settings of the Hik IP Receiver Pro such as accessing Hik-ProConnect, system settings, system maintenance, network settings, and storage settings.

4.1 Access Hik-ProConnect

You can access Hik IP Receiver Pro to the Hik-ProConnect so that you can add devices managed on Hik-ProConnect. You can also store the device list, alarms, zones of the Hik IP Receiver Pro in use on Hik-ProConnect, and use another Hik IP Receiver Pro but with the same information. After configuring Hik-ProConnect parameters, you can configure hot spare settings to deploy a maximum of four Hik IP Receiver Pros connected with the same Hik-ProConnect.

4.1.1 Configure Hik-ProConnect Parameters

After accessing Hik IP Receiver Pro to the Hik-ProConnect, you can add devices managed on the Hik-ProConnect to Hik IP Receiver Pro, and the Hik IP Receiver Pro can receive and transmit alarms and videos from these devices to ARC.

Note

Make sure you have finished the authorization for ARC.

1. Click **Configuration → Hik-ProConnect → Parameters** to configure Hik-ProConnect parameters.
2. Enter the following parameters and click **Save** to access the Hik IP Receiver Pro to the Hik-ProConnect.

   Hik-ProConnect Address

   Enter the address of the Hik-ProConnect. The addresses of Hik-ProConnect servers locating in different areas vary as the following.

   - Europe: ***https://ieu.hik-proconnect.com***
   - Asia: ***https://isgp.hik-proconnect.com***
   - North America: ***https://ius.hik-proconnect.com***
   - South America: ***https://isa.hik-proconnect.com***

   User Name (ARC ID) and Password (ARC Key)

   After logging in to tpp.hikvision.com, select **Resource → ARC INTEGRATION GROUP** to find *Hik-ProConnect Related Materials for ARC Integration*, where the way for getting ARC ID and ARC key is provided.

   Connect Status

Connected indicates that the Hik IP Receiver Pro is now accessed to the Hik-ProConnect, and if devices managed on the Hik-ProConnect are added to the Hik IP Receiver Pro, the Hik IP Receiver Pro can transmit alarms and videos from these devices to ARC.

Not Connected indicates that the Hik IP Receiver Pro is not accessed to the Hik-ProConnect, and the Hik IP Receiver Pro will fail to transmit alarms and videos from devices managed on the Hik-ProConnect to ARC.

Click **Go** to configure port mapping to enable dual-connection.

Note

For details about port mapping, refer to ***Set Port Mapping*** .

4.1.2 Configure Hot Spare Settings

After configuring Hik-ProConnect parameters, you can configure hot spare settings to deploy a maximum of four Hik IP Receiver Pros connected to the same Hik-ProConnect. In this way, the four Hik IP Receiver Pros can share the same backup information, so that in case any one of the deployed Hik IP Receiver Pros crashes, you can use another one with the same information including devices, events, etc.

Note

Make sure you have configured Hik-ProConnect parameters on Hik IP Receiver Pro, and make sure you have connected all Hik IP Receiver Pros to the same Hik-ProConnect.

Click **Configuration → Hik-ProConnect → Hot Spare Settings** to configure hot spare settings, check **Enable Hot Spare**, and select a hot spare role for the current Hik IP Receiver Pro in use.

Note

- You can select host server, spare server 1, spare server 2, or spare server 3 as the role of the current Hik IP Receiver Pro. Only if you have selected a Hik IP Receiver Pro as the host server, can you configure spare servers.
- The backup priority of the host server, spare server 1, spare server 2, and spare server 3 is in descending order.

After configuration, you will see as follows:

1. After configuration, you can view all hot spare devices connected with the same Hik-ProConnect as the current Hik IP Receiver Pro. The **Hot Spare Details** table also displays the ID, hot spare role, and working status of each Hik IP Receiver Pro.
2. As for the **Backup Information** table, it displays the file name, update time, and update status of the backup file.

4.2 System Settings

You can set the system parameters, such as changing admin user's password, editing product name, etc.

4.2.1 Change Password for Admin User

You can change password for login if you need.

Steps

1. Click **Configuration → System → User** .
2. Click **Change** to enter the Change Password page.
3. Enter the old password, password, and confirm password.
4. Click **Save**.

What to do next

You are required to log in to the Hik IP Receiver Pro service again.

4.2.2 Configure Hik IP Receiver Pro Name

You can view the Hik IP Receiver Pro information and edit the its name according to the actual needs.

Steps

1. Click **Configuration → System → Basic Information** .
2. View the gateway information, including the version, model, and operating system.
3. Enter a name according to the actual needs.
4. Click **Save**.

4.2.3 Configure Time

The Hik IP Receiver Pro supports editing the time zone, date, and time for it.

Steps

1. Click **Configuration → System → Time** .
2. Select a time zone for the computer where the Hik IP Receiver Pro is running. Generally, you select the time zone where this computer locates.
3. Set the date and time for the Hik IP Receiver Pro.
   - Click to select a date and time.
   - Check **Synchronize with Computer Time** to used the current computer's date and time.
4. Click **Save**.

4.2.4 Enable Alarm Monitor and Check Device's Alarms

You can enable alarm monitor function to receive the alarms reported by the devices. The user needs access a special Web page to check the alarms details, including picture and video. If enabled, you can get the URL of the Web page, and send it to the user who wants to check alarms. The user can access the Web page by editing device's account ID in URL to check the alarm information of this device.

Make sure you have added the security control panels and configured protocol parameters. For more details, refer to and ***Configure Protocol Parameters*** .

Click **Configuration → System → Alarm Monitor** to enter alarm monitor setting page. Check **Enable** and click **Save** to enable alarm monitor function.

- **Get URL**: By default, a URL is displayed on this page. You can copy the URL to access the Web page or send it to other users for checking alarms.
- **Change URL**: Click to generate a new URL automatically, so that the previous URL is inactive.
- **Check Alarms**: Edit the device's account ID in URL and enter the edited URL in address bar to enter the Web page. You can check alarms details (e.g., protocol type, event name, event code, time, and account ID), view picture, play video, download picture or video, etc.
- Click **Refresh** to get the latest alarms if you changed the protocol.
- Click in the **Two-Way Audio** column to start two-way audio.

Note

- A plug-in is required for starting two-way audio.
- The two-way audio function is only supported by Chrome, Firefox, and Microsoft Edge.
- You can configure device settings to determine how much time is allowed for starting two-way audio after an alarm is triggered. You can configure it on the Configuration page of that device.
- Make sure that you have installed audio input and output devices on your PC.
- If is not available, you can click **Synchronize Device Information** on the Device page.

Example

If the URL is ***http://10.10.10.1:8080/page/videoReview?token=DXXXXXXXXXXXXXXXXX3C&account=<ID>***, and the device's account ID is 1234, you need to enter ***http://10.10.10.1:8080/page/videoReview?token=DXXXXXXXXXXXXXXXXX3C&account=1234*** in the address bar to enter the Web page for checking alarms.

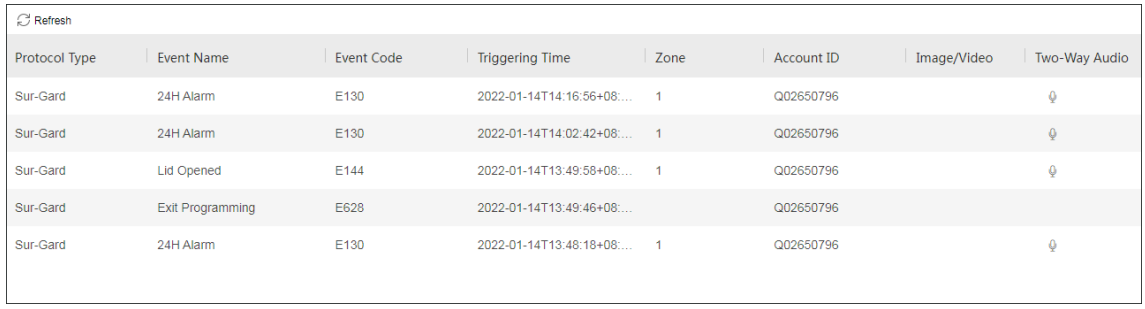


Figure 4-1 Check Alarms

Note

- The page shows the latest 2,000 alarms within two days at most.
- The undefined alarm means the alarms cannot be recognized by the Hik IP Receiver Pro. You can add the event on Event page. For more details, refer to ***Add Event Code of Security Control Device*** .
- If the Hik IP Receiver Pro communicates with the ARC via SIA-DCS protocol, the Event Code will display SIA code, otherwise it will display CID code.

4.3 System Maintenance

In the System Maintenance module, you can manage logs and manage the configuration file.

4.3.1 Manage Logs

You can enable log and export logs to your local PC.

Steps

1. Click **Configuration → Maintenance → Log** to enter the Log Management page.
2. Check **Enable Log**.
3. Select the log level.

   Note

   - Only the logs with the log level higher than the configured level can be recorded.
   - The log level is **Info** by default. We recommend setting **Debug** as the log level to make it easier to find error details. If you select **Debug** as the log level, the Hik IP Receiver Pro performance will be degraded.
4. Click **Save** to save the settings.
5. **Optional:** Click **Export** to download logs to your PC.

4.3.2 Export and Import Configuration File

You can export the configuration file and import it to Hik IP Receiver Pro on another PC in case that you need to quickly start Hik IP Receiver Pro without configuring it on another PC.

Steps

1. Click **Configuration → Maintenance → Configuration File** .
2. Click **Export** and enter your password to save the configuration data to your local PC.
3. When needed, click **Import** and enter the set password to import the configuration file to Hik IP Receiver Pro to start it on another PC.

   Hik IP Receiver Pro will be restarted after importing the configuration file.

4.4 Network Settings

You need to configure network parameters of the Hik IP Receiver Pro correctly to ensure the normal communication.

Various network configuration services are provided, including port editing, port mapping configuration, and HTTPS certification installation.

4.4.1 Edit Port

Some default ports of the Hik IP Receiver Pro can be edited if they are already used by other services.

Click **Configuration → Network Settings → Port** , edit the platform port numbers and device port numbers and save the port settings. The port status indicates whether the ports are already occupied.

Normal

The port is used normally.

Abnormal

The port is used abnormally, suggesting that it is already occupied by another program. You need to end the program or enter another port number.

Platform Port

Click **Platform Port** to edit the following ports used for data transmission from devices to the Hik IP Receiver Pro.

HTTP Port

Used for web browser access in HTTP protocol. By default, the HTTP Port is ***80***.

RTSP Port

Used for getting stream from Hik IP Receiver Pro during live view, remote playback, and two-way audio. By default, the RTSP Port is ***554***.

HTTPS Port

By default, the HTTPS Port is ***443***.

Device Port

Click **Device Port** to edit the ports used for data transmission from the Hik IP Receiver Pro to devices.

Note

Restart the Hik IP Receiver Pro after editing the device port, or the settings will not take effect.

4.4.2 Set Port Mapping

If port mapping is required, you need to set the parameters of port mapping on a router beforehand, and then enter the external port number and external IP address on the Port Mapping page.

Click **Configuration → Network Settings → Port Mapping** . Check **Enable** to enable Platform Port Mapping or Device Port Mapping function. Enter the corresponding external ports and external IP addresses of the Hik IP Receiver Pro and save the settings.

Platform Port Mapping

Used for accessing the Hik IP Receiver Pro by Web browser.

Device Port Mapping

Used for receiving data from ISUP devices. Once it's disabled, the function of linking directly or by Hik-ProConnect Server cannot be used.

Note

- By default, the Hik IP Receiver Pro will restart automatically after saving the settings.
- We recommend ***15000 to 17000*** for external port of the ISUP2.0 Stream Port.

4.4.3 Set HTTPS

HTTPS provides authentication of the web site and its associated web server, which protects against attacks. For example, if you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by entering https://192.168.1.64:443 via a web browser. The Hik IP Receiver Pro provides three installing methods of HTTPS certificate.

Steps

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

2. Check one of the installation methods to set HTTPS certificate.

Create self-signed certificate.	Enter the **Country**, **Domain/IP**, **Validity** and other information, and then click **Save**. **Note** If you already had a certificate installed, the "Create self-signed certificate." is grayed out.
Signed certificate is available, start the installation now.	Click **Browse** to select a signed certificate saved in the PC, and then click **Install**.
Create the certificate request first and continue the installation.	a. Click **Create** to create the certificate request. Enter the required information in the pop-up window and click **OK** to save. b. Download the certificate request and submit it to the trusted certificate authority for signature. c. After receiving the signed valid certificate, click **Browse** to select the downloaded certificate saved in the PC, and then click **Install**.

There will be the certificate information after successfully creating and installing the certificate.

3. Check **Enable** to enable the installed certificate.
4. Click **Save** to save the settings.

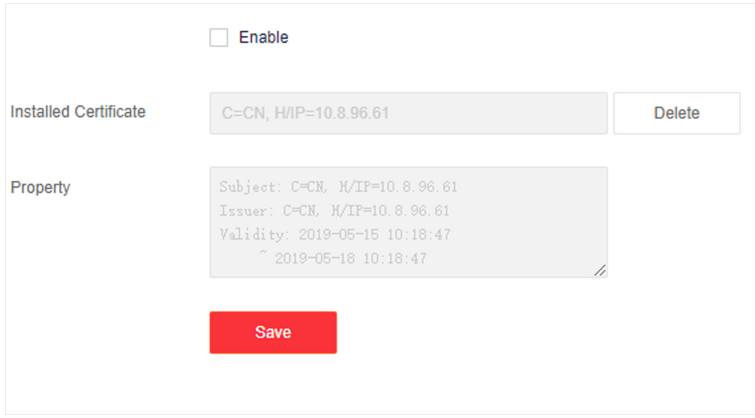


Figure 4-2 Installed Certificate

4.4.4 Set Email

You can set parameters including sender name, sender email, receiver email, sending interval of events, and so on. After these settings, notification emails will be sent to the receiver email(s) automatically and regularly in situations such as when a device added to the Hik IP Receiver Pro is offline. In the email, the receiver(s) can view details about device serial number, event description, and so on.

Notification emails will be sent to the receiver email(s) when Hik IP Receiver Pro detects the following events.

Table 4-1 Event

Event Name	Description
Disk Full	The email will be sent to the receiver(s) immediately when the disk of Hik IP Receiver Pro's cache server is full.
Hik-ProConnect Account Changed	The email will be sent to the receiver(s) immediately when the Hik-ProConnect account is changed.
Disconnected from Recording Server	The emails will be sent to the receiver(s) immediately when Hik IP Receiver Pro is disconnected from the recording server.
Disconnected from ARC	The email will be sent to the receiver(s) immediately when Hik IP Receiver Pro is disconnected from ARC.
Disconnected from Hik-ProConnect	The email will be sent to the receiver(s) immediately when Hik IP Receiver Pro is disconnected from Hik-ProConnect.
Device Offline	This event refers to the situation when the device added to Hik IP Receiver Pro is offline. The email about this event will be sent to the receiver(s) at regular intervals.
Device ARC Service Disabled on Hik-ProConnect	The email about this event will be sent to the receiver(s) at regular intervals.
Direct Connection Failure of Dual-Connection	The email about this event will be sent to the receiver(s) at regular intervals.

Steps

1. On the Configuration page, click **Network → Email** .
2. Enter sender name, sender email, server address, and port No.

Note

- For sender name, up to 32 characters are allowed.
- The sender email should support SMTP service. Only gamil, hotmail, and yahoo are supported.
- The server address and port No. are those of the sender email.

3. Select an encryption type.
4. Enter the sending interval of events.

Note

Sending interval means Hik IP Receiver Pro will send emails at regular intervals. For example, if the interval is 30 minutes, the Hik IP Receiver Pro will send emails every 30 minutes. The sending interval is 3 minutes by default. The sending interval is only used for the events whose notification emails can be sent at regular intervals. If an event of the same device occurs more than once during an interval, the email will only display the information of the event triggered at the first time.

5. **Optional:** Check **Enable Authentication**, and enter user name and authorization code.

Note

- The user name is the same as that of the sender email, and it should contain no more than 32 characters.
- Before authentication, the SMTP service of the sender email should be enabled. The authorization code is used for Hik IP Receiver Pro to send emails via the sender email. It can be the password of the sender email or the authorization code provided by the sender email. The specific authorization code is dependent on the sender email system.
- The email might not be sent to the receiver(s) successfully without authentication.

6. Enter receiver information in the Receiver table.

Note

- For receiver name, up to 32 characters are allowed.
- Up to 5 receivers are allowed.

7. Click **Test** to test whether the receiver email can receive the test email.
8. Click **Save**.

Chapter 5 Storage Settings

Two storage modes are provided: PC disk storage or Recording Server.

- **Storage Disk**: Alarm-related videos will be stored in the selected disk of your PC, and you can set the downloading time for the alarm-related videos.
- **Recording Server**: After connecting the Hik IP Receiver Pro to the Recording Server, you can back up alarm-related videos to the Recording Server by the Hik VideoPlugin. When you need a second video verification for alarm-related details, you can view the video stored in Recording Server by the Hik VideoPlugin.

5.1 Select Storage Disk

The pictures and videos taken by access control devices can be stored in the PC. When there are triggered alarms, the Hik IP Receiver Pro will automatically store the alarm-related pictures and videos in the PC, so that you can view the pictures and videos by the third-party system connected to the Hik IP Receiver Pro. You need to select the storage disk beforehand.

Steps

Note

The videos and pictures could not be stored normally with free space less than 200 MB. Please make enough free space to avoid storage failure. We recommend 50 GB or above.

1. Click **Configuration → Storage Settings** to enter the Storage Settings page.
   The available storage disks of the current PC is displayed.
2. Select a disk to store the files.
3. Click **Save** to save the settings.

   Note

   The videos and pictures will be saved in default folder for 48 hours, after which they will be deleted automatically.

5.2 Set Recording Server for Second Video Verification

A Recording Server is used for backing up alarm-related videos from devices added to the Hik IP Receiver Pro. You can back up an alarm-related video to the Recording Server by the Hik VideoPlugin. When you need a second video verification for alarm-related details, you can view the video stored in Recording Server by the Hik VideoPlugin.

Before You Start

Make sure you have properly installed, activated, and configured Recording Server beforehand.

Steps

1. Click **Configuration → Storage → Recording Server** to enter the Recording Server page.
2. Configure Recording Server parameters.

   Address

   Enter the Recording Server's IP address.

   Port

   Enter the port number of the Recording Server.

   User Name

   Enter the user name of the Recording Server.

   Password

   Enter the password of the Recording Server.

   Enable WAN Access

   If the Recording Server belongs to different network domain from the Hik IP Receiver Pro or the Hik VideoPlugin, enable this function to enable mapping between the Recording Server and the Hik IP Receiver Pro/Hik VideoPlugin.

   WAN IP Address

   Enter the mapped IP Address of the Recording Server.

   WAN Port Number

   Enter the mapped port number of the Recording Server.
3. Click **Save** to connect the Hik IP Receiver Pro to Recording Server.

   Connect Status

   Connected indicates that the Hik IP Receiver Pro is connected to the Recording Server, and you can back up alarm-related videos to the Recording Server by the Hik VideoPlugin.

   Not Connected indicates that the Hik IP Receiver Pro is not connected to the Recording Server, and you will fail to back up alarm-related videos to the Recording Server by the Hik VideoPlugin.

Chapter 6 Protocol Automation Output Management

You need to configure related protocol parameters to conduct the communication between the Hik IP Receiver Pro and the third-party system.

The Hik IP Receiver Pro communicates with third-party system by Sur-Gard protocol and ISAPI protocol. So that you need to configure the Sur-Gard and ISAPI parameters which are supposed to be the same with those parameters configured in the third-party system. Meanwhile, the Hik IP Receiver Pro supports viewing and managing security control panel's events. You can view event details and add/edit/delete an event.

The Hik IP Receiver Pro communicates with third-party system by ISAPI protocol. So that you need to configure the ISAPI parameters which are supposed to be the same with those parameters configured in the third-party system.

The Hik IP Receiver Pro communicates with third-party system by Sur-Gard protocol, Ademco 685 protocol, Manitou protocol, and SBN protocol. So that you need to configure the parameters which are supposed to be the same with those parameters configured in the protocol. Meanwhile, the Hik IP Receiver Pro supports viewing and managing security control panel's events. You can view event details and add/edit/delete an event.

6.1 Configure Protocol Parameters

To perform communication between the Hik IP Receiver Pro and the ARC, you need to configure protocol parameters first.

Steps

1. Click **Protocol Management → Automation Output → Protocol** .
2. Check **Enable** to enable the protocol you selected below.
3. Select a protocol from the **Protocol Type** list.

Note

You can click ⓘ to view the example of the alarm message of the selected protocol.

4. Configure the parameters of the selected protocol.

Sur-Gard

TCP/IP

Used for communication between the Hik IP Receiver Pro and ARC.

Server

The Hik IP Receiver Pro works as a server for communication.

Client

The Hik IP Receiver Pro works as a client connecting to ARC which works as a server for communication. You need to provide the ARC's IP address if you select this mode.

Port

The port used for communicating with the ARC. By default, the port number is ***1025***.

RS-232

Used for communication between the Hik IP Receiver Pro and ARC.

Serial Port

By default, the serial port is **COM1**.

Baud Rate

Keep it the same with the baud rate set on ARC.

Data Bit

Keep it the same with the data bit set on ARC.

Parity

Keep it the same with the parity set on ARC.

Stop Bit

It cannot be edited and is ***2*** by default.

Compatibility

The versions of Sur-Gard protocol.

Receiver Number

The number used for marking the Hik IP Receiver Pro as an information receiver. You can customize this parameter. Keep it the same with the number set on ARC.

Line Card Number

The number of the line used for communication between the Hik IP Receiver Pro and ARC. You can customize this parameter. Keep it the same with the number set on ARC.

Heartbeat

If you select **Sur-Gard** as the protocol type, check **Enable Hik IP Receiver Pro Heartbeat** to enable heartbeat between the ARC and the Hik IP Receiver Pro.

Hik IP Receiver Pro Heartbeat Interval

It ranges from 10 to 65535 seconds. It is 30 seconds by default.

Device Heartbeat Interval

It ranges from 10 to 65535 seconds. It is 30 seconds by default.

Note

Used for the device which does not support Periodic Test or whose Periodic Test has not been enabled. If the Periodic Test of a device has been enabled, the device heartbeat interval will be the same as that of this device.

Ademco 685

Serial Port

By default, the serial port is **COM1**.

Baud Rate

Keep it the same with the baud rate set on ARC.

Data Bit

Keep it the same with the data bit set on ARC.

Parity

Keep it the same with the parity set on ARC.

Stop Bit

Select **1** or **2** and it is **2** by default.

Receiver Number

The number used for marking the Hik IP Receiver Pro as an information receiver. You can customize this parameter. Keep it the same with the number set on ARC.

Line Card Number

The number of the line used for communication between the Hik IP Receiver Pro and ARC. You can customize this parameter. Keep it the same with the number set on ARC.

Device Heartbeat Interval

It ranges from 10 to 65535 seconds. It is 30 seconds by default.

Note

Used for the device which does not support Periodic Test or whose Periodic Test has not been enabled. If the Periodic Test of a device has been enabled, then the device heartbeat interval will be the same as that of this device.

Manitou

IP Address

Enter the IP address of the ARC which supports Manitou protocol.

Port

The port used for connection with the ARC which supports Manitou protocol. By default, the port number is ***1025***.

Line Card Number

Line number, which ranges from 1 to 999.

Connecting Mode

There are two link modes: dedicated and discontinuous.

Test Signal Interval

It ranges from 60 to 300. Valid when the link mode is discontinuous.

Test Signal ID

Up to 12 characters are allowed. It is ***GATEWAY*** by default. Valid when the link mode is discontinuous.

Test Signal Event Type

Up to 16 characters are allowed. It is ***SYS*** by default. Valid when the link mode is discontinuous.

Test Signal Event ID

Up to 16 characters are allowed. It is ****RP*** by default. Valid when the link mode is discontinuous.

Enable Device Heartbeat

Check the parameter to enable device heartbeat. It is disabled by default.

Device Heartbeat Interval

It ranges from 10 to 65535 seconds. It is 30 seconds by default.

Note

Used for the device which does not support Periodic Test or whose Periodic Test has not been enabled. If the Periodic Test of a device has been enabled, then the device heartbeat interval will be the same as that of this device.

SBN

IP Address

Enter the IP address of the ARC which supports SBN protocol.

Port

The port used for the connection with the ARC which supports SBN protocol. By default, it is ***1025***.

SIA-DCS

IP Address

Enter the IP address of the ARC which supports SIA-DCS protocol.

Port

Enter the port of the ARC. By default, it is ***1025***.

Receiver Number

- The number used for marking the Hik IP Receiver Pro as an information receiver. You can customize this parameter. Keep it the same with the number set on ARC.
- The **Enable** is not checked by default. If it is checked, the receiver number will be displayed in alarm event information.

Line Card Number

By default, the line number is ***0***.

Enable Video Verification

Check **Enable Video Verification** so that you can view alarm-related videos on the ARC.

Response Timeout Period

It ranges from 5 seconds to 60 seconds, and 20 seconds is the default. If the Hik IP Receiver Pro dose not receive the response from the ARC in this period, it indicates that no response has been sent to the Hik IP Receiver Pro.

Attempts

It ranges from one time to 10 times, and 3 times is the default. If the Hik IP Receiver Pro dose not receive the response from the ARC during the response timeout period, the Hik IP Receiver Pro will attempt to retransmit the message.

Hik IP Receiver Pro Heartbeat Interval

If you select **SIA-DCS** as the protocol type, check **Enable Hik IP Receiver Pro Heartbeat** to enable heartbeat between the ARC and the Hik IP Receiver Pro. It ranges from 10 to 65535 seconds. It is 30 seconds by default.

Private

Hik IP Receiver Pro Heartbeat Interval

If you select **Private** as the protocol type, check **Enable Hik IP Receiver Pro Heartbeat** to enable heartbeat between theARC and the Hik IP Receiver Pro. It ranges from 10 to 65535 seconds. It is 30 seconds by default.

5. Click **Save**.

- **Automation Status**: For Sur-Gard protocol, the status means whether the Hik IP Receiver Pro can receive data from the ARC, which supports Sur-Gard protocol.
  - For Server mode of TCP/IP interface, if the data is received normally, the IP address and port number of the ARC and **Connected** will be displayed; For Client mode of TCP/IP interface, if the data is received normally, **Connected** will be displayed.
  - For RS-232 interface, if the data is received normally, the serial port number of Hik IP Receiver Pro and **Connected** will be displayed.
  - If the data cannot be received, it is shown as **Not Connected**.
- **Connect Status**: For Ademco 685 protocol, Manitou protocol, and SBN protocol, the status means whether the Hik IP Receiver Pro can receive data from theARC, which supports Ademco 685 protocol, Manitou protocol, and SBN protocol.
- ◦ For Ademco 685 protocol, if the data is received normally, the serial port number of Hik IP Receiver Pro and **Connected** will be displayed.
  - For Manitou protocol and SBN protocol, if the data is received normally, it is shown as **Connected**.
  - If the data cannot be received, it is shown as **Not Connected**.

6.2 Search History Event

You can search history events which are received by Hik IP Receiver Pro via device account ID and alarm time. After searching, you can view event source, event code, triggering time, etc.

Steps

1. On the Automation Output page, click **Event Monitor** to enter the Historical Event page.
2. **Optional:** Check **Automatic Refresh** to automatically refresh the event list.
3. Enter account ID.
4. Click Triggering Time field to set the start time and end time.

Note

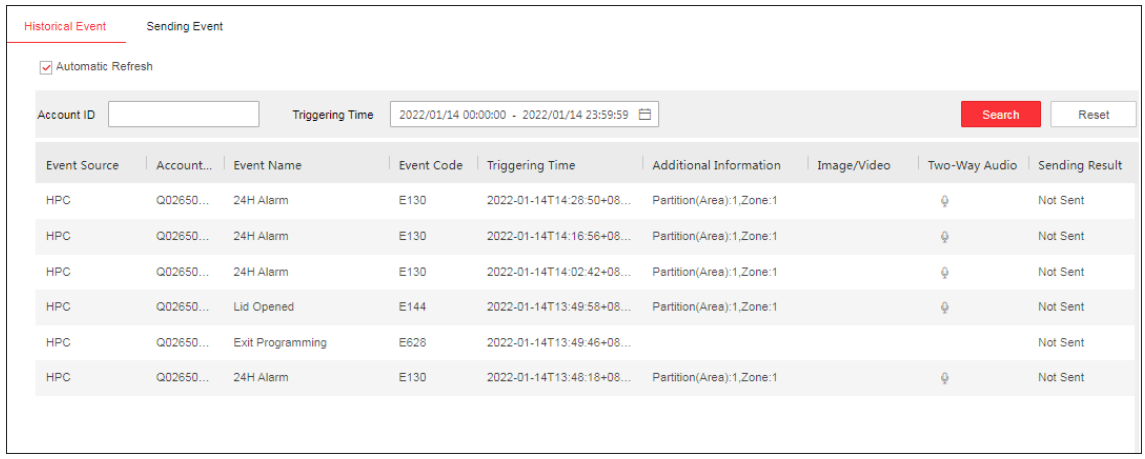
- Only events which are received within two days can be searched.
- The start time should be earlier than the end time.

5. Click **OK**.
6. Click **Search**.

   The matched alarm events are displayed.

   Sending Result

   It displays the result about whether the event notification is sent to the ARC successfully.



Note

If the Hik IP Receiver Pro communicates with the ARC via SIA-DCS protocol, the Event Code will display SIA code, otherwise it will display CID code.

Figure 6-1 History Events

7. **Optional:** Click in **Image/Video** column for verification. The icon means downloading failed, while the icon means the video is being downloaded.
8. **Optional:** Click in the **Two-Way Audio** column to start two-way audio.

Note

- Click **Speak** to start to speak.
- Click **Listen** to start to listen.
- Click **Stop** to stop two-way audio.

Note

- A plug-in is required for starting two-way audio.
- The two-way audio function is only supported by Chrome, Firefox, and Microsoft Edge.
- You can configure device settings to determine how much time is allowed for starting two-way audio after an alarm is triggered. You can configure it on the Configuration page of that device.
- Make sure that you have installed audio input and output devices on your PC.
- If is not available, you can click **Synchronize Device Information** on the Device page.

6.3 Check Event Monitor Logs

The Hik IP Receiver Pro displays the real-time events triggered by the communication between it and the third-party system. On the Event Monitor page, you can view the event details including the access protocol between it and the third-party system, the time at which an event happens, communication bugs, etc. Each event type is marked by different colors for attention. For example, you will be noticed quickly when there are communication bugs between the Hik IP Receiver Pro and the third-party system.

Click **Protocol Management → Automation Output → Event Monitor** .

The real-time events triggered by communications between the Hik IP Receiver Pro and third-party system are displayed.

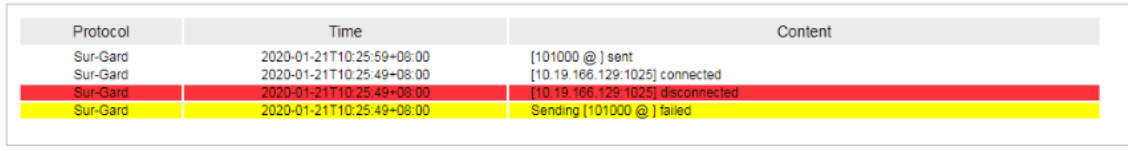


Figure 6-2 Real-Time Events

Different event types are marked by different colors:

Red

Communication failure between the Hik IP Receiver Pro and third-party system. The Hik IP Receiver Pro cannot get communication results.

Yellow

The third-party system responding to the message sent by the Hik IP Receiver Pro timed out.

White

The communication between the Hik IP Receiver Pro and the third-party system goes well.

Note

At most 5,000 events can be printed.

6.4 Add Event Code of Security Control Device

The ARC recognizes security control device's events by event codes. The Hik IP Receiver Pro will receive an original code when a security control device added to the Hik IP Receiver Pro triggers an event. Then, the Hik IP Receiver Pro transfers the original code to a target code (a CID code or a SIA code) which could be recognized by the ARC. After that, the Hik IP Receiver Pro sends the target code to the ARC. In this way, you can receive event notifications by the ARC.

In the top left corner of Home page, click → **All Modules** → **ARC Gateway** → **Event** → **Security Control Device** . Perform the following operations and save the settings.

- Click **Add** to enter the event name, original code, CID code or SIA code, and click **Add**.
- Click to delete an event. You can select multiple events, and click **Delete** to batch delete them.

  Note

  Only the events added by yourself are supported to be deleted.
- Click , and edit **Event Name**, **CID Code** or **SIA Code**.

Note

The Hik IP Receiver Pro will send the original code to the ARC without trans-coding and the ARC will not receive an event notification if you delete an event in this event list.

6.5 Edit Encoding Device Event and Device Status Event

You can edit the information of encoding device event and device status event to keep it the same with the information configured on the ARC.

Note

The CID code and SIA code should be the same with those configured on the ARC.

In the top left corner of Home page, click → **All Modules** → **ARC Gateway** → **Event** .

On the **Encoding Device** page and **Device Status** page, select an event type and click to edit the event's CID code, SIA code, and event name, and click **Save**.

Appendix A. Event Code List

This event code list includes the CID code and SIA code of security control device, encoding device, and device online/offline event.

- For event codes of security control device, see ***Event Codes of Security Control Device*** .
- For event codes of encoding device, see ***Event Codes of Encoding Device*** .
- For event codes of device online/offline event, see ***Event Codes of Device Status*** .

A.1 Event Codes of Security Control Device

The following table displays the event codes of security control device.

HikCode	CIDCode	SIACode	Description
1100	E100	MA	Medical Alarm
1103	E130	BA	Burglary Alarm
1110	E111	FA	Fire Alarm
1121	E121	HA	Duress alarm
1122	E122	HA	Silent Panic Alarm
1123	E123	AA	Audible Panic Alarm
1124	E133	AB	24H Alarm
1125	E133	AC	24H Alarm
1126	E130	BA	Timeout Alarm
1129	E120	PA	Audible Panic Alarm
1130	E130	BA	Burglary Alarm
1131	E131	BA	Perimeter Breached
1132	E132	AD	Interior Burglary Alarm
1133	E130	BA	24H Alarm
1134	E130	BA	Burglary Alarm
1137	E137	TA	Lid Opened
1139	E139	BV	Confirmed Alarm
1141	E141	AE	BUS Open-circuit Alarm
1142	E142	AF	BUS Short-circuit Alarm

HikCode	CIDCode	SIACode	Description
1144	E144	TA	External Probe Disconnected
1148	E148	AG	Device Motion Alarm
1149	E149	AH	Masking Alarm
1151	E162	GA	Gas Leakage Alarm
1207	E207	AI	Zone Early-Warning
1301	E301	AT	Mains Power Lost
1302	E302	YT	Battery Low
1305	E305	ZY	Reset to defaults
1311	E311	YM	Battery Disconnected
1312	E312	YI	Overcurrent Protection Triggered
1318	E311	YM	Power Depletion
1319	E319	YP	Overvoltage Protection Triggered
1333	E333	AJ	Expander Exception
1336	E336	AK	Printer Disconnected
1337	E384	XT	Battery Low
1338	E338	AL	Expander Low Voltage
1339	E301	YP	Mains Power Lost
1340	E311	YM	Battery Disconnected
1341	E144	TA	Lid Opened
1342	E301	YP	Expander AC Power Loss
1343	E144	TA	Lid Opened
1344	E144	TA	Lid Opened
1345	E381	XL	Wireless Siren Disconnected
1346	E144	TA	Lid Opened
1347	E384	XT	Battery Low
1348	E381	XL	Wireless Device Disconnected
1351	E351	LT	Main Signalling Path Fault
1352	E352	LT	Backup Signalling Path Fault

HikCode	CIDCode	SIACode	Description
1354	E354	AM	Telephone Line Disconnected
1359	E354	YC	Uploading Report Failed
1382	E382	AN	BUS Supervision Fault
1383	E144	TA	Lid Opened
1386	E386	AO	Zone Open-circuit Alarm
1387	E387	AP	Zone Short-circuit Alarm
1401	E401	OP	Disarmed
1403	E403	OA	Auto Disarmed
1406	E406	BC	Alarm Silenced
1409	E409	CS	Keyswitch Zone Disarming
1443	E443	AQ	Turn On Output by Schedulet
1452	E452	CT	Late to Disarm
1455	E455	CD	Auto Arming Failed
1460	E460	AR	Turning On Output Failed
1461	E461	AS	Turning Off Output Failed
1462	E462	AT	Auto Disarming Failed
1467	E461	JA	Incorrect Password
1556	E556	AT	Network Change
1570	E570	QB	Bypassed
1574	E574	AU	Group Bypass
1601	E601	AV	Manual Report Test
1602	E602	RP	Periodic Report Test
1607	E607	TS	Walk Test Enabled
1617	E617	AW	Telephone Connection Test
1627	E627	LB	Programming mode
1628	E628	LX	Exit Programming
1759	E131	BA	Intrusion Detection
1773	E131	BA	Cross-Zone Alarm

HikCode	CIDCode	SIACode	Description
1774	E774	AX	PIR Alarm
1775	E775	AY	Sudden Increase of Sound Intensity Alarm
1776	E776	AZ	Sudden Decrease of Sound Intensity Alarm
1777	E777	BA	Audio Input Fault
1778	E131	BA	Line Crossing Alarm
1779	E134	BA	Region Entrance Detection
1780	E112	FA	Fire Source Alarm
1781	E158	KS	High Temperature Pre-Alarm
1782	E159	ZS	Low Temperature Pre-Alarm
1783	E158	KA	High Temperature Alarm
1784	E159	ZA	Low Temperature Alarm
1785	E134	EA	Region Exiting Detection
1810	E120	PA	Audible Panic Alarm
1811	E110	FA	Keypad/Keyfob Fire Alarm
1812	E812	BB	Keypad/Keyfob Burglary Alarm
1822	E454	CI	Arming Failed
1847	E100	MA	Keypad/Keyfob Medical Alarm
1862	E501	DK	Keypad Locked
1863	E863	BC	Absence Alarm
1864	E501	DK	Tag Reader Locked
1865	E865	BD	Unregistered Tag
1910	E910	BE	Keypad Disconnected
1911	E911	BF	KBUS Relay Disconnected
1912	E912	BG	KBUS GP/K Disconnected
1913	E913	BH	KBUS MN/K Disconnected
1914	E381	XL	Detector Offline
1915	E384	XT	Detector Battery Low
1916	E381	XL	Expander Offline

HikCode	CIDCode	SIACode	Description
1917	E381	XL	Repeater Offline
1918	E918	BI	Radar Transmitter Fault
1919	E384	XT	Sounder Battery Low
1920	E920	NT	Cellular Data Network Disconnected
1921	E921	NT	SIM Card Exception
1922	E922	NT	Wi-Fi Disconnected
1923	E344	XQ	Jamming Detected
1924	E924	NT	Data limitation Reached
1925	E384	XT	Keyfob Battery Low
1930	E930	NT	IP Address Already Used
1931	E931	NT	Network Fault
1940	E131	BA	Motion Detection Alarm Started
1941	E941	BJ	Device Blocked
1942	E942	BK	Video Signal Loss
1943	E943	BL	Input/Output Format Unmatched
1944	E944	BM	Video Input Exception
1945	E945	BN	Full HDD
1946	E946	BO	HDD Exception
1947	E947	BP	Upload Picture Failed
1948	E948	BQ	Email Sending Failed
1949	E949	BR	Network Camera Disconnected
1960	E960	BS	Duty Checking
1961	E961	BT	Post Response
1962	E962	BU	Fire Alarm Consulting
1963	E963	BV	Duress Alarm Consulting
1964	E964	BW	Emergency Medical Alarm
1970	E970	BX	BUS Query
1971	E971	BY	BUS Registration

HikCode	CIDCode	SIACode	Description
1973	E973	BZ	Single-Zone Disarming
1974	E974	CA	Single-Zone Alarm Cleared
1975	E306	CB	Detector Deleted
1976	E976	CC	Business Consulting
1977	E306	CD	Expander Deleted
1978	E306	CE	Repeater Deleted
1979	E306	CF	Sounder Deleted
1980	E306	CG	Peripheral Deleted
3100	R100	MH	Medical Alarm Restored
3103	R130	BH	Burglary Alarm Restored
3110	R111	FH	Fire Alarm Restored
3122	R122	HH	Silent Panic Alarm Restored
3123	R123	CH	Audible Panic Alarm Restored
3124	R133	CI	24H Alarm Restored
3125	R133	CJ	24H Alarm Restored
3126	R130	BH	Timeout Alarm Restored
3129	R120	PH	Audible Panic Alarm Restored
3130	R130	BH	Burglary Alarm Restored
3131	R131	BH	Perimeter Restored
3132	R132	CK	Interior Burglary Alarm Restored
3133	R130	BH	24H Alarm Restored
3134	R130	BH	Burglary Alarm Restored
3137	R137	TR	Lid Restored
3139	R139	BW	Confrimed Alarm Restore
3141	R141	CL	BUS Open-circuit Restored
3142	R142	CM	BUS Short-circuit Restored
3144	R144	TR	External Probe Connected
3148	R148	CN	Device Motion Alarm Restored

HikCode	CIDCode	SIACode	Description
3149	R149	CO	Masking Alarm Restored
3151	R162	GH	Gas Leakage Alarm Restored
3207	R207	CP	Zone Early-Warning Restored
3301	R301	AR	Mains Power Restored
3302	R302	YR	Battery Voltage Restored
3311	R311	YR	Battery Reconnected
3312	R312	YJ	Overcurrent Protection Restored
3319	R319	YQ	Overvoltage Protection Restored
3333	R333	CQ	Expander Restored
3336	R336	CR	Printer Connected
3337	R384	XR	Battery Voltage Restored
3338	R338	CS	Normal Expander Voltage
3339	R301	YQ	Mains Power Restored
3340	R311	YR	Battery Reconnected
3341	R144	TR	Lid Restored
3342	R301	YQ	Expander AC Power Loss Restored
3343	R144	TR	Lid Restored
3344	R144	TR	Lid Restored
3345	R381	XC	Sounder Online
3346	R144	TR	Lid Restored
3347	R384	XR	Battery Voltage Restored
3348	R381	XC	Wireless Device Connected
3351	R351	LR	Main Signalling Path Restored
3352	R352	LR	Backup Signalling Path Restored
3354	R354	CT	Telephone Line Connected
3359	R354	YK	Report Uploading Restored
3382	R382	CU	BUS Supervision Restored
3383	R144	TR	Lid Restored

HikCode	CIDCode	SIACode	Description
3401	R401	CL	Armed
3403	R403	CA	Auto Disarmed
3408	R408	CV	Instant Arming
3409	R409	OS	Keyswitch Zone Arming
3441	R441	NL	Armed in home mode
3442	R442	CW	Forced Arming
3443	R443	CX	Turn Off Output by Schedule
3570	R570	QU	Bypass Restored
3574	R574	CY	Group Bypass Restored
3607	R607	TE	Walk Test Disabled
3759	R131	BH	Intrusion Detection Restored
3773	R131	BH	Cross-Zone Alarm Restored
3774	R774	CZ	PIR Alarm Restored
3775	R775	DA	Sudden Increase of Sound Intensity Alarm Restored
3776	R776	DB	Sudden Decrease of Sound Intensity Alarm Restored
3777	R777	DC	Audio Input Restored
3778	R131	BH	Line Crossing Alarm Restored
3780	R112	FH	Fire Source Alarm Restored
3781	R158	KR	High Temperature Pre-Alarm Restored
3782	R159	ZR	Low Temperature Pre-Alarm Restored
3783	R158	KH	High Temperature Alarm Restored
3784	R159	ZH	Low Temperature Alarm Restored
3862	R501	DO	Keypad Unlocked
3864	R501	DO	Tag Reader Unlocked
3910	R910	DD	Keypad Connected
3911	R911	DE	KBUS Relay Connected
3912	R912	DF	KBUS GP/K Connected
3913	R913	DG	KBUS MN/K Connected

HikCode	CIDCode	SIACode	Description
3914	R381	XC	Detector Online
3915	R384	XR	Battery Voltage Restored
3916	R381	XC	Expander Online
3917	R381	XC	Repeater Online
3918	R918	DH	Radar Transmitter Restored
3919	R384	XR	Sounder Battery Voltage Restored
3920	R920	NR	Cellular Data Network Connected
3921	R921	NR	SIM Card Restored
3922	R922	NR	Wi-Fi Connected
3923	R344	XH	Jamming Restored
3925	R384	XR	Keyfob Battery Voltage Restored
3930	R930	NR	Normal IP address
3931	R931	NR	Network Restored
3940	R131	BH	Motion Detection Alarm Stopped
3941	R941	DI	Device Blocking Alarm Restored
3942	R942	DK	Video Signal Restored
3943	R943	DL	Input/Output Format Restored
3944	R944	DM	Video Input Restored
3945	R945	DN	Free HDD
3946	R946	DO	HDD Restored
3949	R949	DP	Network Camera Connected
3962	R962	DQ	Fire Alarm Consulting Over
3963	R963	DR	Duress Alarm Consulting Over
3964	R964	DS	Emergency Medical Alarm Consulting Over
3965	R250	DT	Patrol Signing
3973	R973	DU	Single-Zone Arming
3975	R306	DV	Detector Enrolled
3976	R976	DW	Business Consulting Over

HikCode	CIDCode	SIACode	Description
3977	R306	DX	Expander Enrolled
3978	R306	DY	Repeater Enrolled
3979	R306	DZ	Sounder Enrolled
3980	R306	EA	Peripheral Enrolled

A.2 Event Codes of Encoding Device

The following table displays the event codes of encoding device.

Original Code	CID Code	SIA Code	Event Name
IO	E900	VA	IO alarm
VMD	E901	VB	VMD alarm
diskerror	E902	VC	diskerror alarm
diskfull	E903	VD	diskfull alarm
diskrecover	E904	VE	diskrecover alarm
fielddetection	E905	VF	fielddetection alarm
linedetection	E906	VG	linedetection alarm
rapidMove	E907	VH	rapidMove alarm
recordException	E908	VI	recordException alarm
regionEntrance	E909	VJ	regionEntrance alarm
regionExiting	E910	VK	regionExiting alarm
shelteralarm	E911	VL	shelteralarm alarm
videoloss	E912	VM	videoloss alarm
fireDetection	E913	VN	fireDetection alarm
TMPA	E914	VO	Temperature Measurement Precautionary Alarm
TMA	E915	VP	Temperature Measurement Alarm
TDA	E916	VQ	Temperature Diff Alarm

A.3 Event Codes of Device Status

The following is the event codes of Device Status.

Original Code	CID Code	SIA Code	Event Name
deviceoffline	E350	OF	deviceoffline alarm
deviceonline	R350	ON	deviceonline alarm
devicedeleted	E349	OD	devicedeleted from HPC alarm


See Far, Go Further