Hik IP Receiver Pro

User Manual

Contents

Chapter 1 Learn Hik IP Receiver Pro 1
1.1 Introduction 1
1.2 How to Use IPRP 1
1.3 System Requirements 2
Chapter 2 What's New in V2.3.0 3
Chapter 3 Installation & Activation 17
3.1 Installation 17
3.2 Activation 17
3.3 Connect IPRP to CMS 17
Chapter 4 Set Up HPP Account 19
Chapter 5 Configure Hot Spare 21
Chapter 6 Manage Devices 23
6.1 Add Devices 23
6.2 Enable Alarm Service for Event Verification 24
Chapter 7 Configure Protocols 29
Chapter 8 Manage Events and Alarms 33
8.1 Search Events 33
8.2 Verify Events 34
8.2.1 Verify Events via Web Plug-In 34
8.2.2 Verify Events via URL 44
8.3 Add Event Codes 45
8.3.1 Set Sending Interval 45
8.3.2 Restore Event Interval 47
8.4 Event Codes 48
8.4.1 Event Codes for Security Control Panels 48
8.4.2 Event Codes for Encoding Devices 63

8.4.3 Event Codes for Access Control Devices 64
8.4.4 Event Codes for Radars 64
8.4.5 Event Codes for Status 65
Chapter 9 Basic Configuration 66
9.1 Manage Operator 66
9.2 Manage Access 66
9.3 Export Log 68
9.4 Configure Network 69
9.5 Configure Storage 71
Appendix A. Legal Information 73

Chapter 1 Learn Hik IP Receiver Pro

- ***Introduction***
- ***How to Use IPRP***
- ***System Requirements***

1.1 Introduction

Hik IP Receiver Pro (IPRP) is a software to establish communications between different types of devices and a Central Monitoring Station (CMS). IPRP converts the events triggered by devices into supported protocols and transmits events to your CMS. You can use plug-ins for video/image/intercom verification and audio broadcast.

1.2 How to Use IPRP

Step	Description
Install and activate IPRPs	To maintain more than 10,000 devices, install and activate multiple IPRPs.
Access Hik-Partner Pro	Configure your Hik-Partner Pro (HPP) account to add Hikvision devices managed on HPP. IPRP can transmit alarms triggered by these devices to the ARC.
Add Devices	Add multiple types of devices to IPRP(s) and set partitions(areas) and zones so that IPRP(s) can transmit alarms triggered by devices to the ARC.
Configure Protocols	Configure supported protocols for transmitting events to the ARC.
Verify Events	View alarm-related videos or use web plug-ins for event verification.
Set Basic Configuration	Set the system, maintenance, network, and storage parameters.

1.3 System Requirements

Parameter	Minimum	Recommended
CPU	Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz	Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz
RAM	4 GB	8 GB or more
HDD Capacity	30 GB	200 GB or more
Network Card	Million Bits NIC	Gigabit NIC
Operating System	• Microsoft (R) Windows 10 (64-bit) • Windows Server 2012 R2 (64-bit) • Windows Server 2016 (64-bit) • Windows Server 2019 (64-bit) **Note** For Windows Server 2012 R2 (64-bit), the patch KB2999226 is required to be installed.	
Web Browser	• Internet Explorer 9/10/11 • Chrome 31.0 and later versions • Firefox 30 and later • Edge **Note** The event monitor function requires Internet Explorer 11 or later, Google Chrome 57 or later, and Firefox 52 or later.	

Chapter 2 What's New in V2.3.0

Device

1. Supports adding IP speakers managed on Hik-Partner Pro, with IP Speaker added as a new category in the device list.

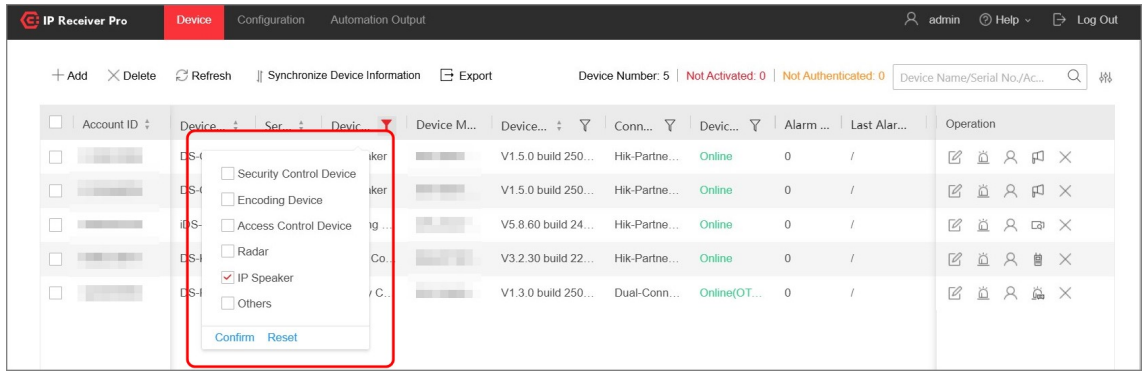


Figure 2-1 Add IP Speaker

2. Supports adding AX HOME V1.2 / Energy-Efficient Panel managed on Hik-Partner Pro (with dual-connection supported) or via OTAP.

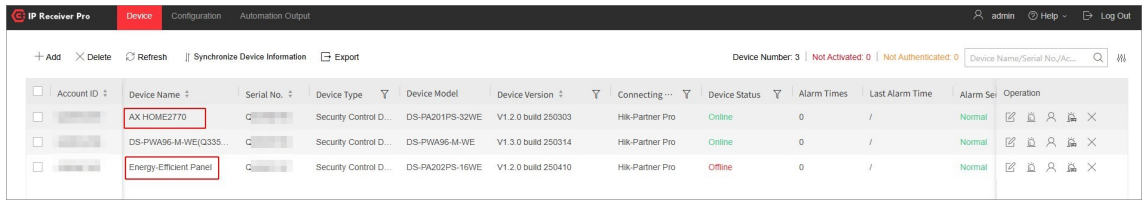


Figure 2-2 AX Home V1.2 / Energy Efficient Panel

3. On the Device page, adds statistics for the total number of devices, devices not activated, and devices not authenticated.

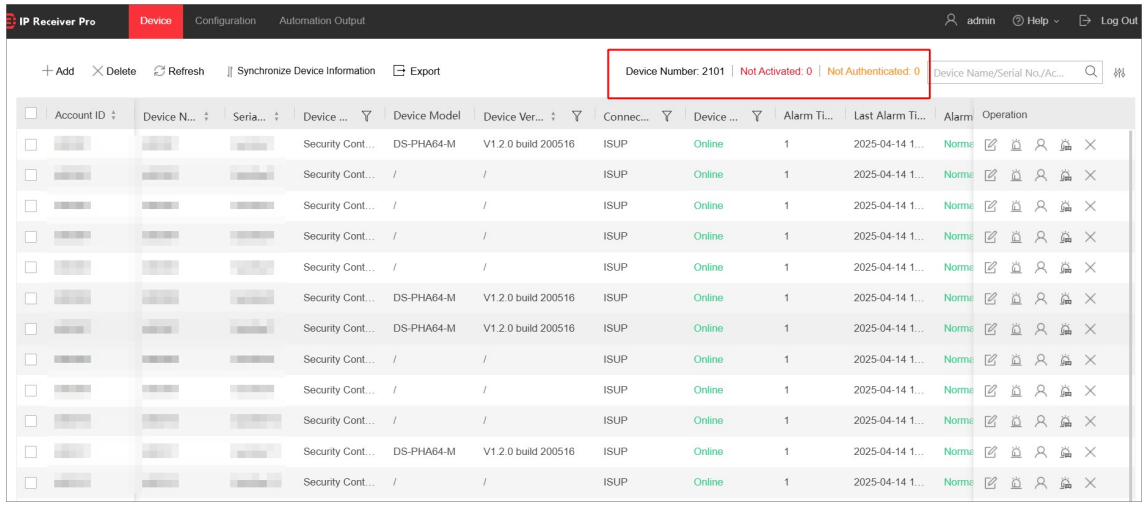


Figure 2-3 Device Statistics

4. For AX HYBRID PRO V2.1.1, the zone list shows Device Number + Zone Name, while its Security Panel Plug-in displays Device + Device Number.

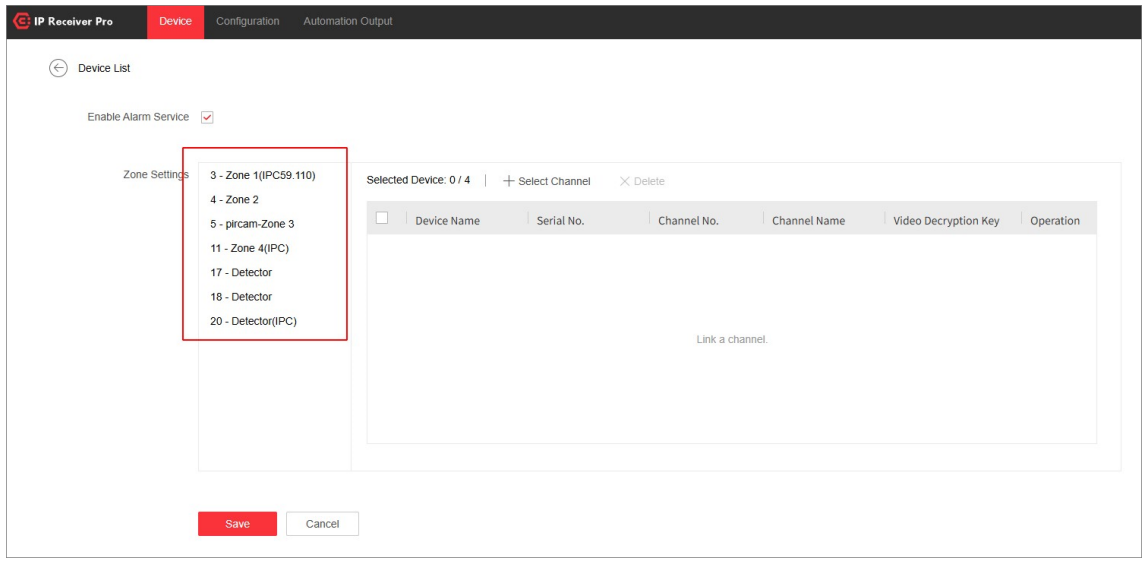


Figure 2-4 Zone List

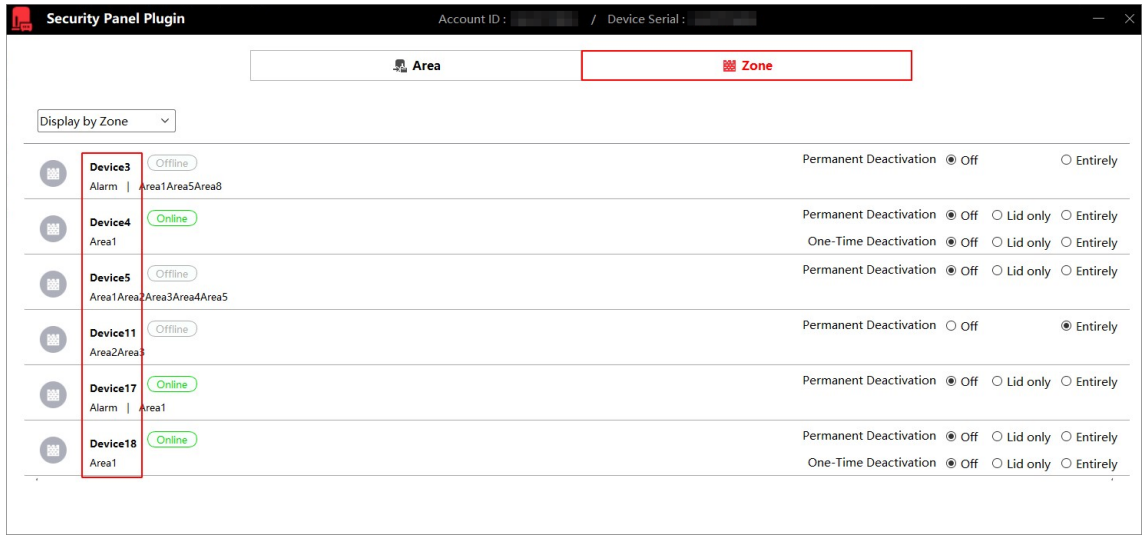


Figure 2-5 Plug-In

Configuration

1. Supports automatic import of HPP devices to IPRP by using HPP devices' account number as the account ID for IPRP devices. You need to set the account number of devices on Hik-Partner Pro (go to **Site & Service → ARC Service → Set Account Number**) before the account number can be used as the devices' account ID. Otherwise, the serial No. will be used as account ID by default.

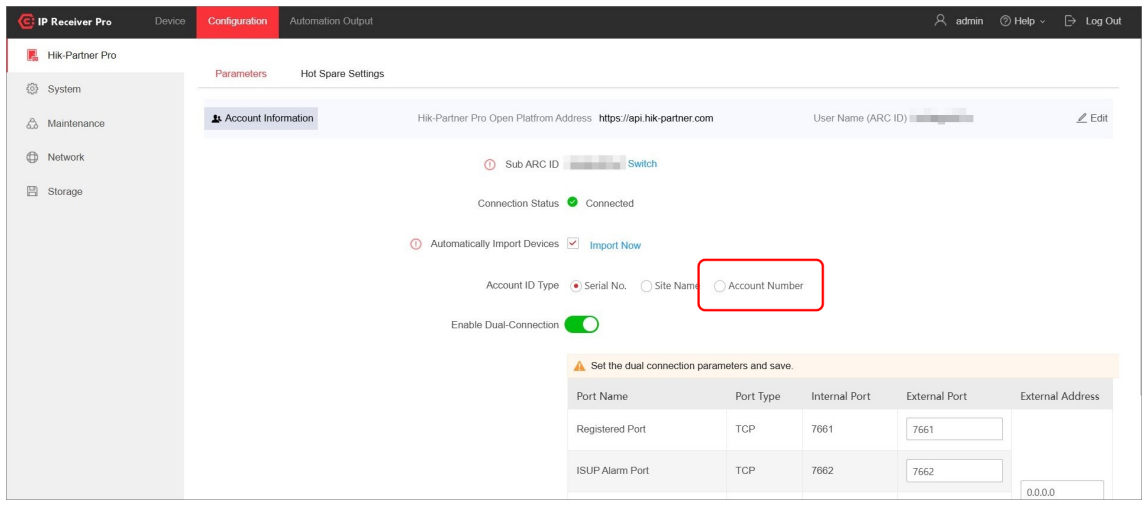


Figure 2-6 Automatic Import Devices

2. On the Alarm Monitor page, you can customize tokens (32-64 alphanumeric characters required). HTTPS requests are required for ensuring secure network transmission of URL requests.

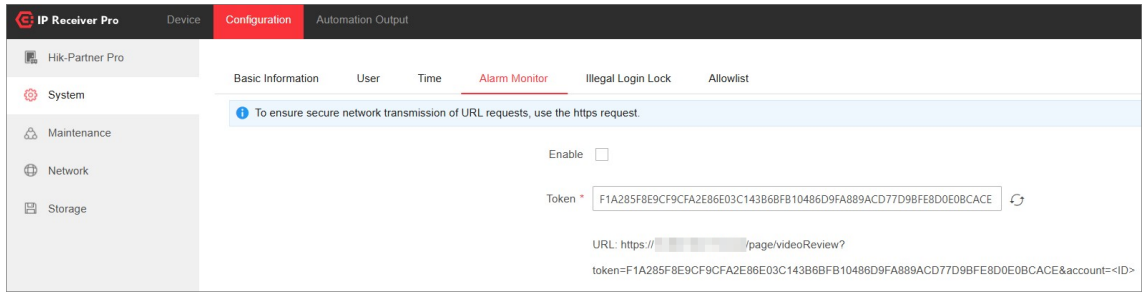


Figure 2-7 Alarm Monitor

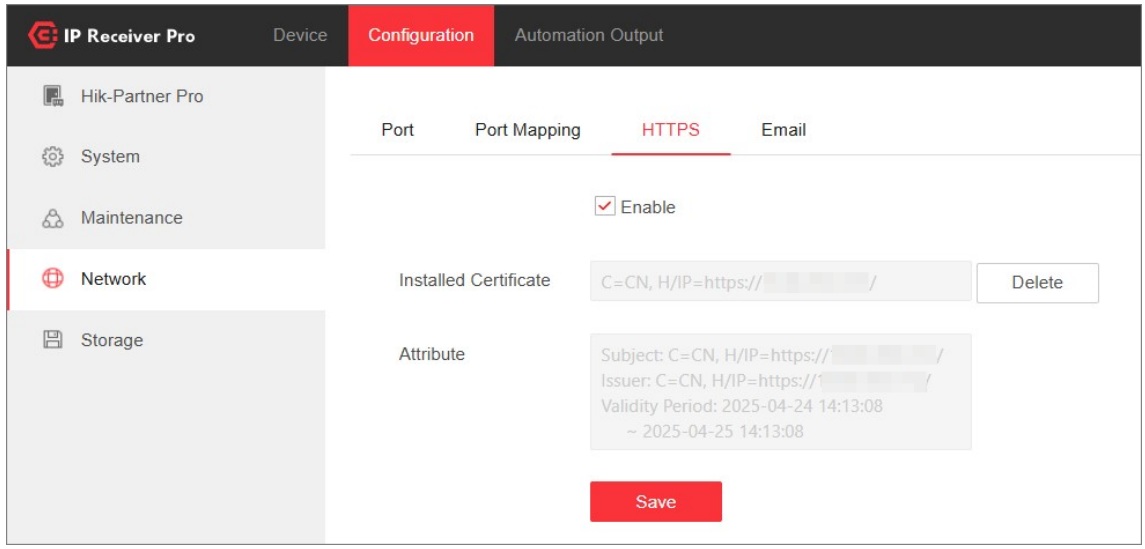


Figure 2-8 HTTPS Configuration

Automation Output

1. On the Event Monitor or the event verification page opened via URL, the system supports displaying the confidence value, indicating the probability of the target being a human, vehicle, or other objects. You can click **View** in the **Video Clips** column to verify the target by reviewing the AI-analyzed videos processed by the perimeter protection server, which are accessible from the security control panels added via Hik-Partner Pro.

Note

Confidence is unchecked by default. You need to check it in the filter column.

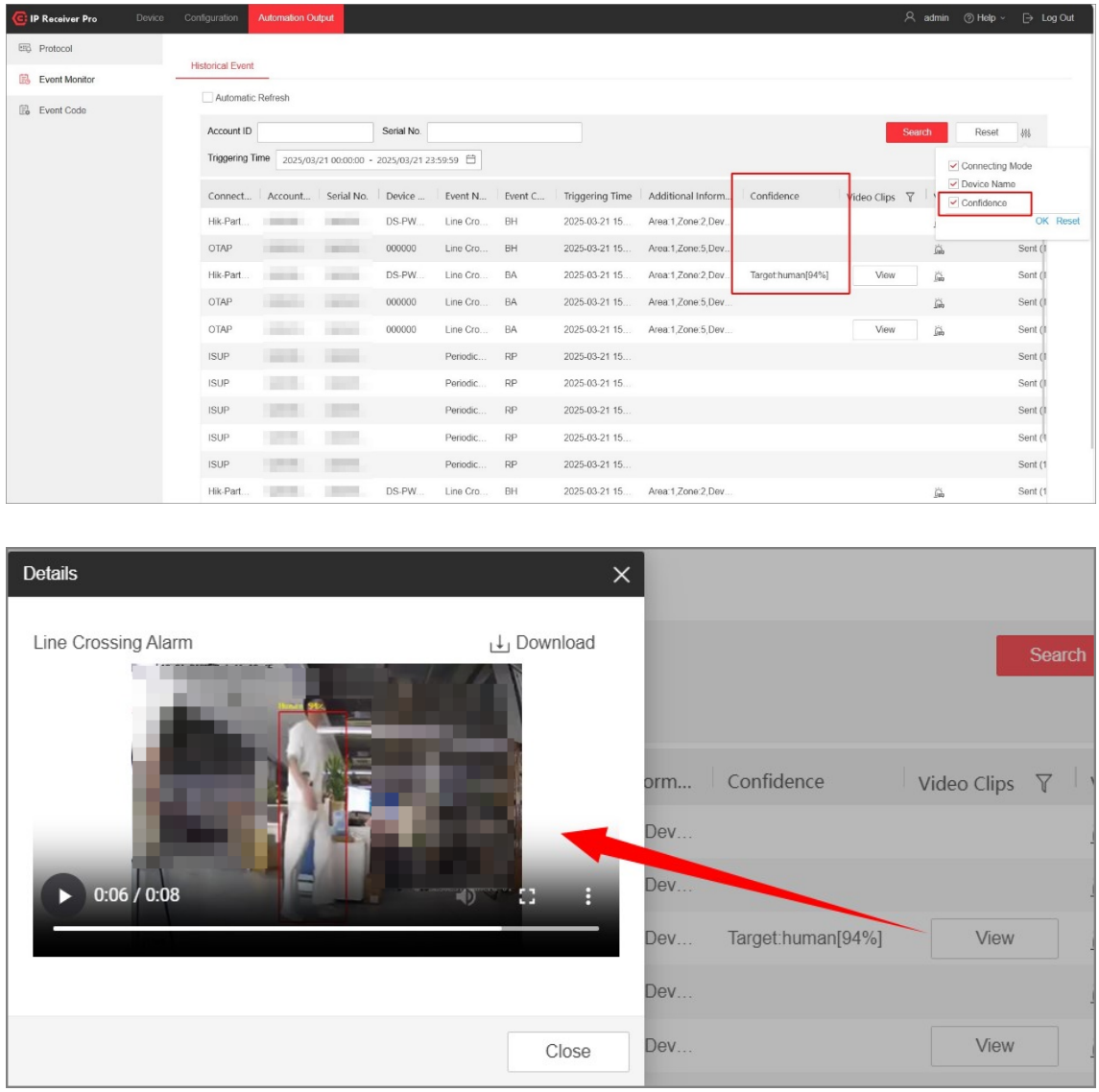


Figure 2-9 Confidence

2. For DC-09 protocol messages forwarded by IPRP, adds confidence information. For example: {"confidence":747,"frameNum":0,"rect":{"height":0.28940199999999999,"width": 0.10546899999999999,"x":0.370313,"y":0.13858699999999999},"targetId": 3,"targetType":"human"}.
3. On the Inspection Event page, adds two event types **deviceHppAbnormal** and **deviceHppNormal** to indicate device network exception on Hik-Partner Pro. **deviceHppAbnormal** is triggered when the HPP link goes offline in a dual-connection mode. You can view the warning in the device list.

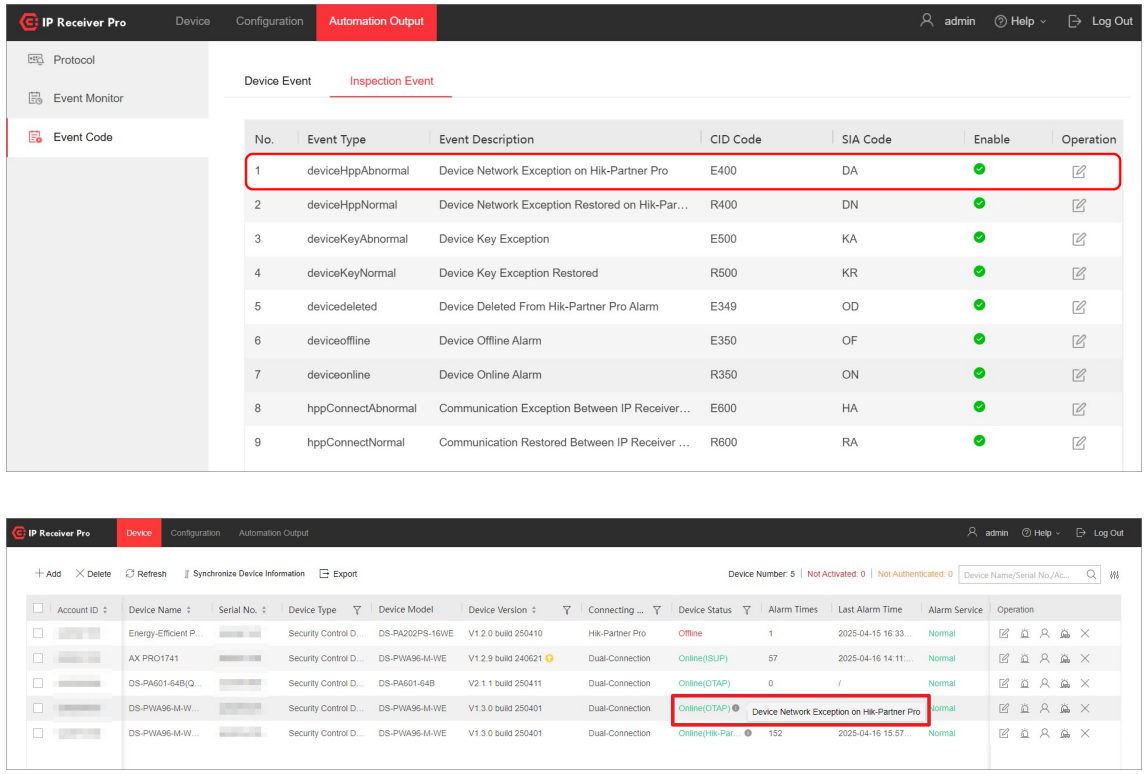


Figure 2-10 Device Network Exception

About Plug-In

1. Adds plug-in icons to the device list, enabling access to device-type-specific plug-ins.

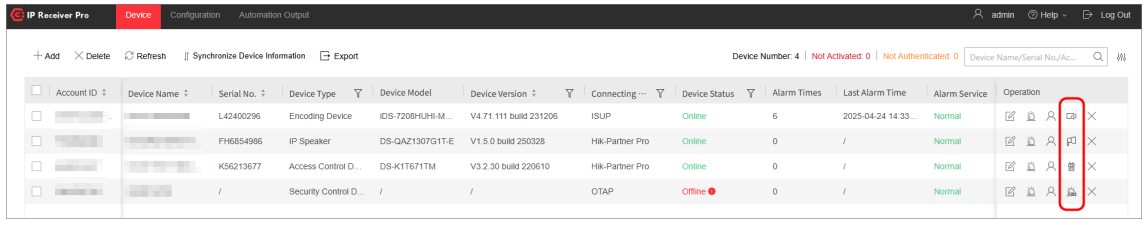


Figure 2-11 Plug-In on the Device Page

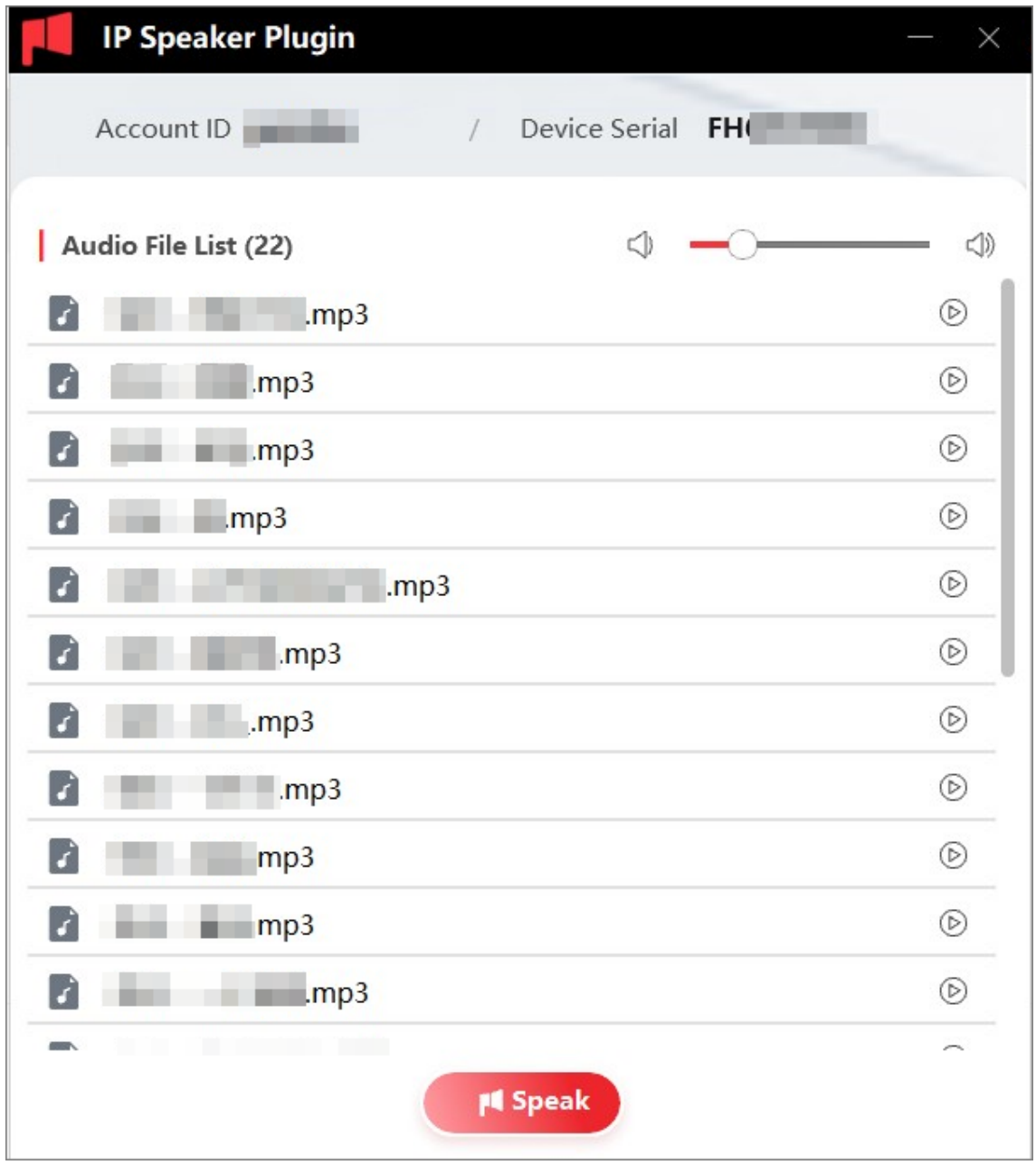


Figure 2-12 IP Speaker Plug-In on the Device Page (Control Single Device)

2. For IP Speakers:
   - Adds a plug-in for managing IP speakers added via Hik-Partner Pro. You can play audio files, control volume (which adjusts both audio file playback and speaking volume simultaneously), and start speaking. With Hik Video Plugin, you can perform these operations for a single device or multiple devices.

Note

- To speak to multiple devices simultaneously, click **Speak** and select devices as needed.
- To play audio files for multiple devices simultaneously, select devices as needed from the drop-down Device Serial No. menu.

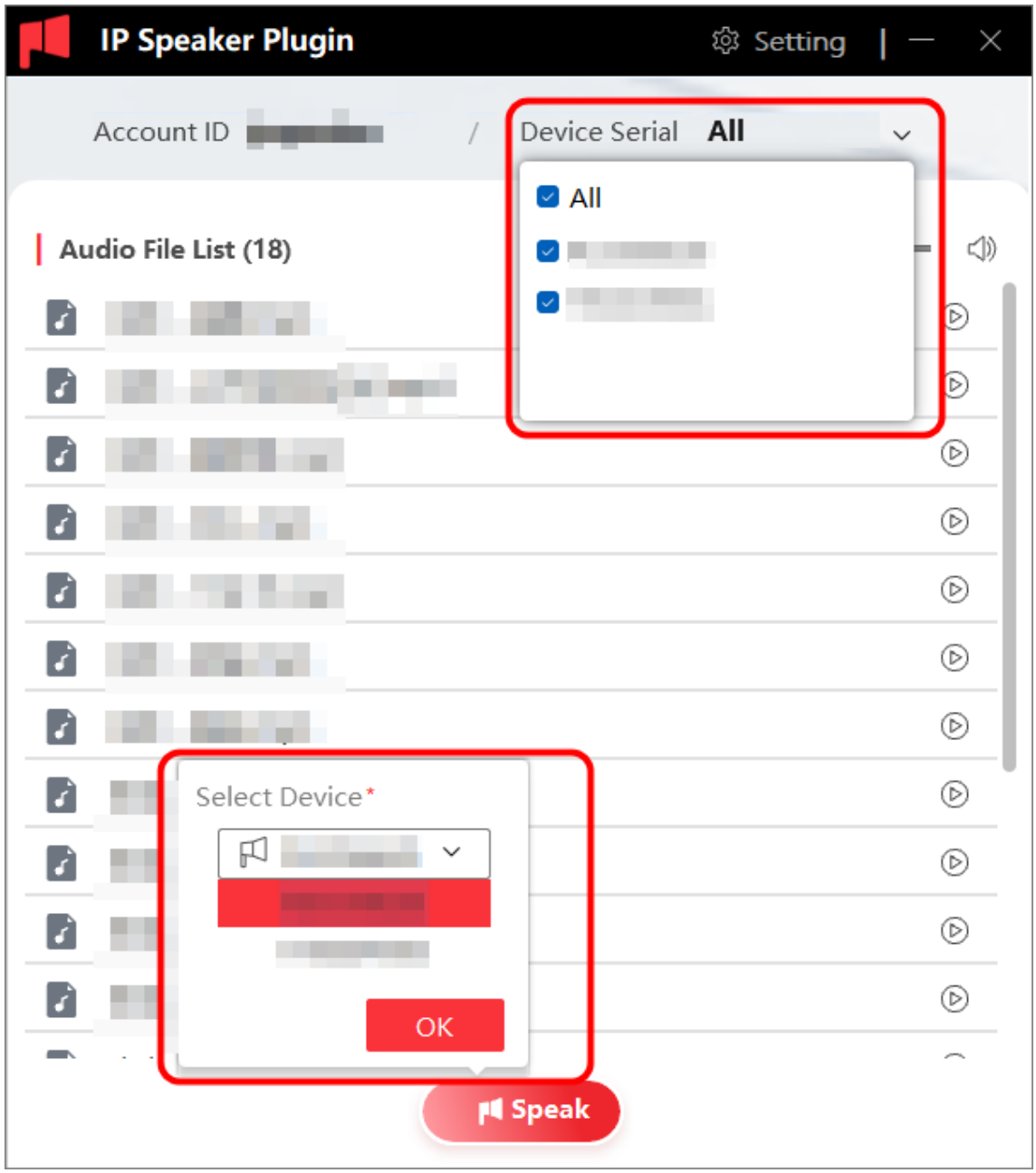


Figure 2-13 Batch Control

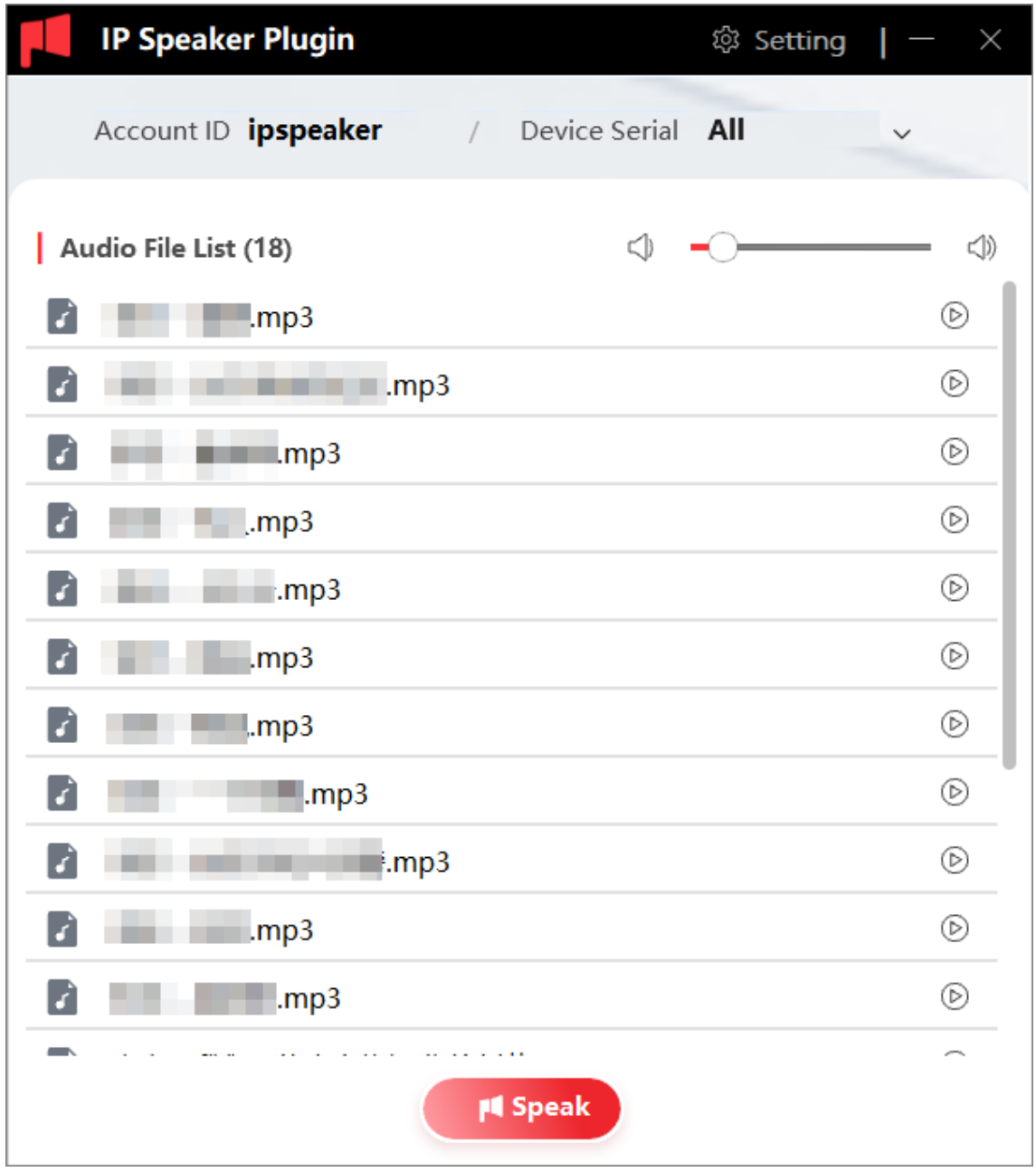


Figure 2-14 IP Speaker Plug-In with Hik Video Plugin (Control Multiple Devices)

- On the **Maintenance → Operation Log** page, adds four operation log types: **Start Playing Audio File**, **Stop Playing Audio File**, **Start Speaking**, and **Stop Speaking**.

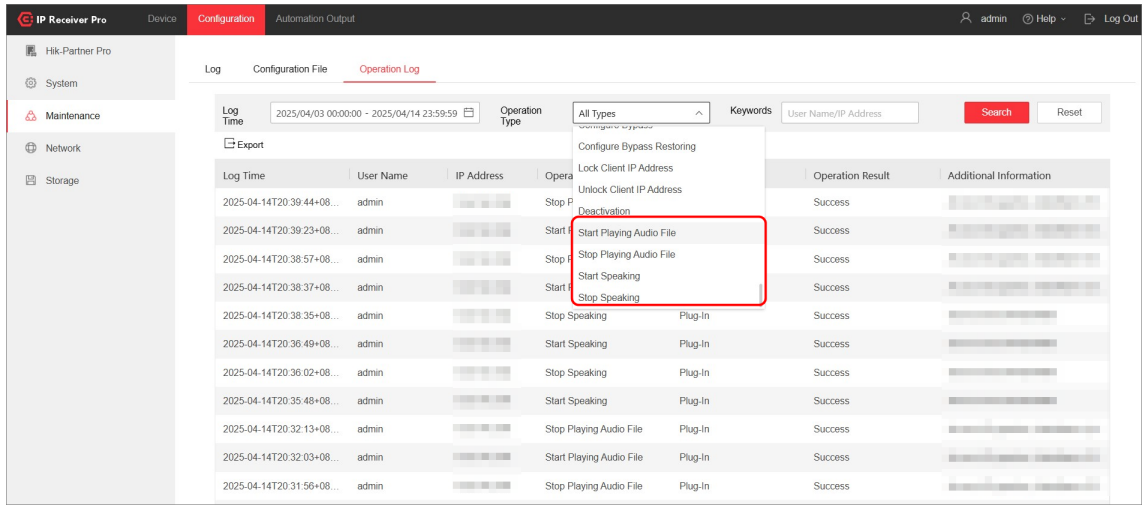


Figure 2-15 Operation Log

3. On the event verification page opened via URL, supports displaying and opening multiple plug-ins simultaneously, with a maximum of one plug-in of each type.

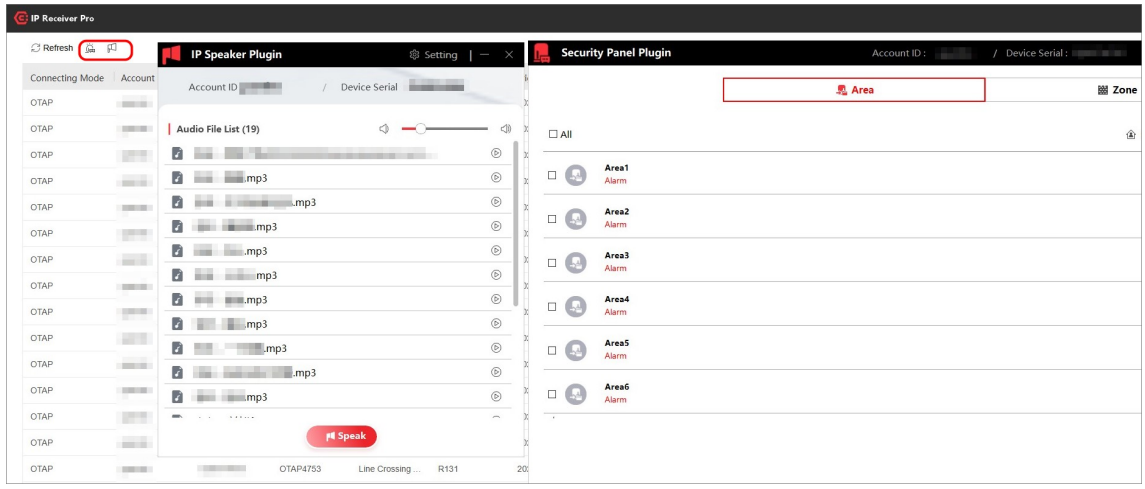


Figure 2-16 Multiple Plug-Ins

4. For the video verification plug-in, supports switching between the main stream and sub stream (by default) from devices managed on HPP in the live view window.

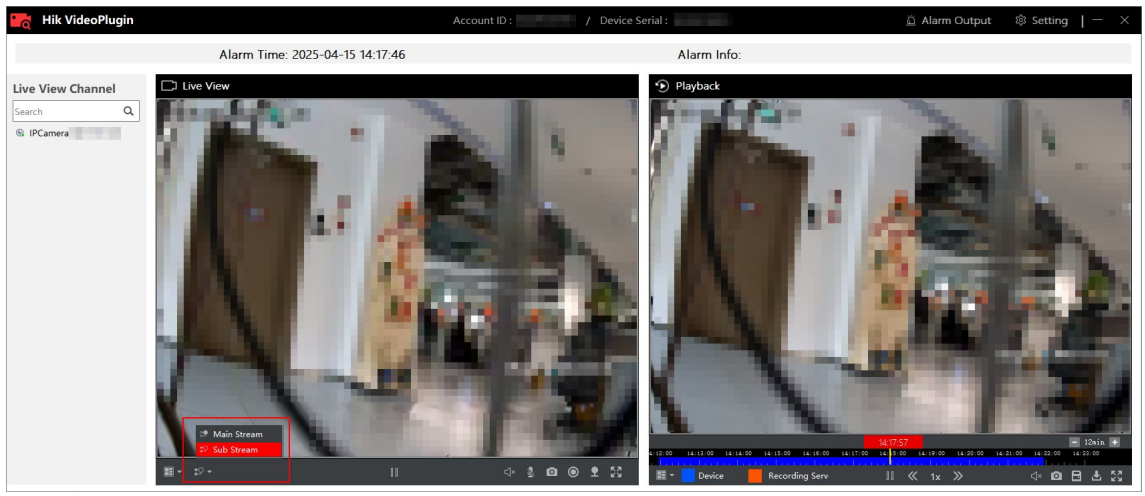


Figure 2-17 Video Verification Plug-in

5. When the intercom verification plug-in is enabled, a window displaying **Call ended on the device** will appear when the call is terminated from the device side.

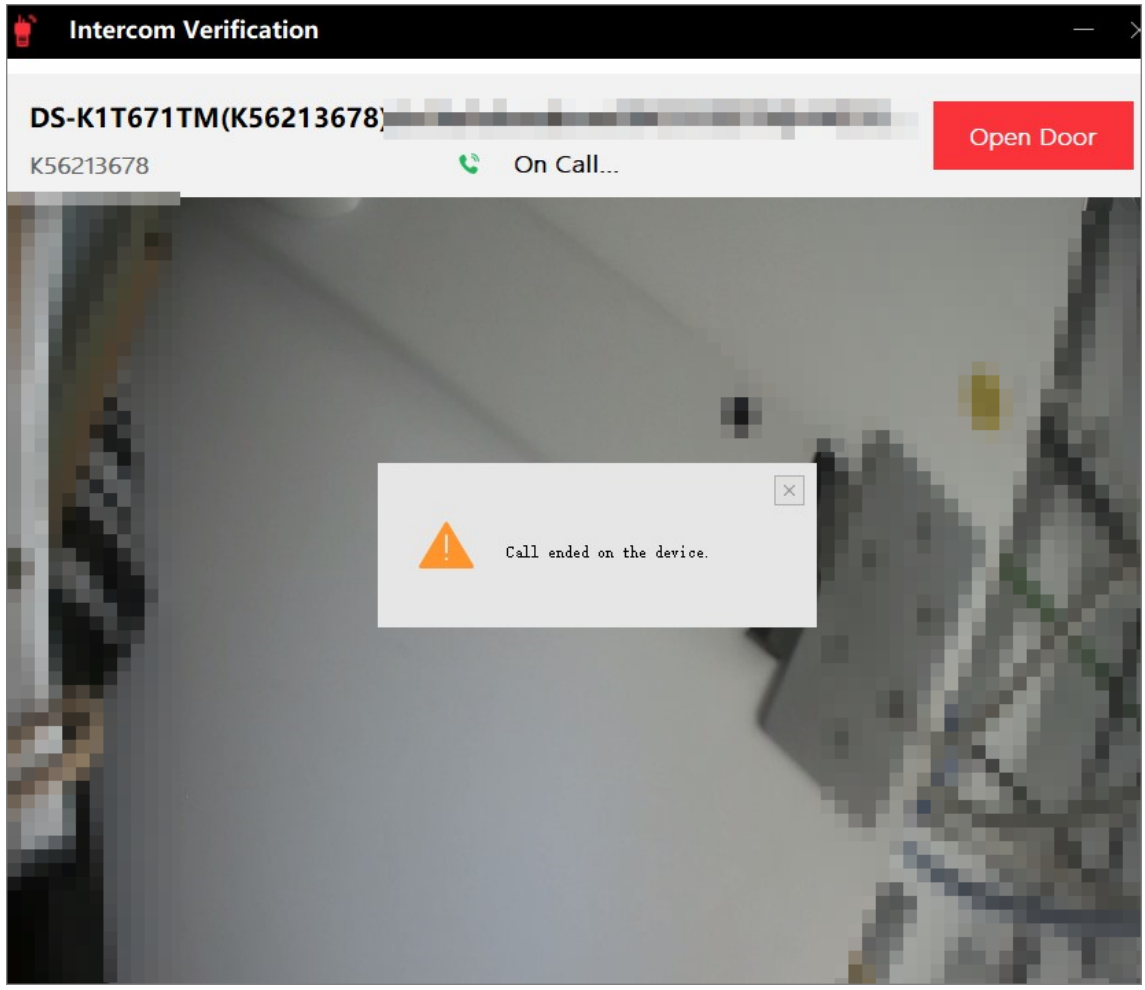


Figure 2-18 Intercom Verification Plug-in

6. For the Security Panel Plug-in:
   - After enabling **Fault Checklist when Arming** on the devices added via OTAP, the arming process will perform area self-checks, including verification of battery status, power supply availability, device connection, etc. This ensures all critical components are in optimal condition before arming completion.

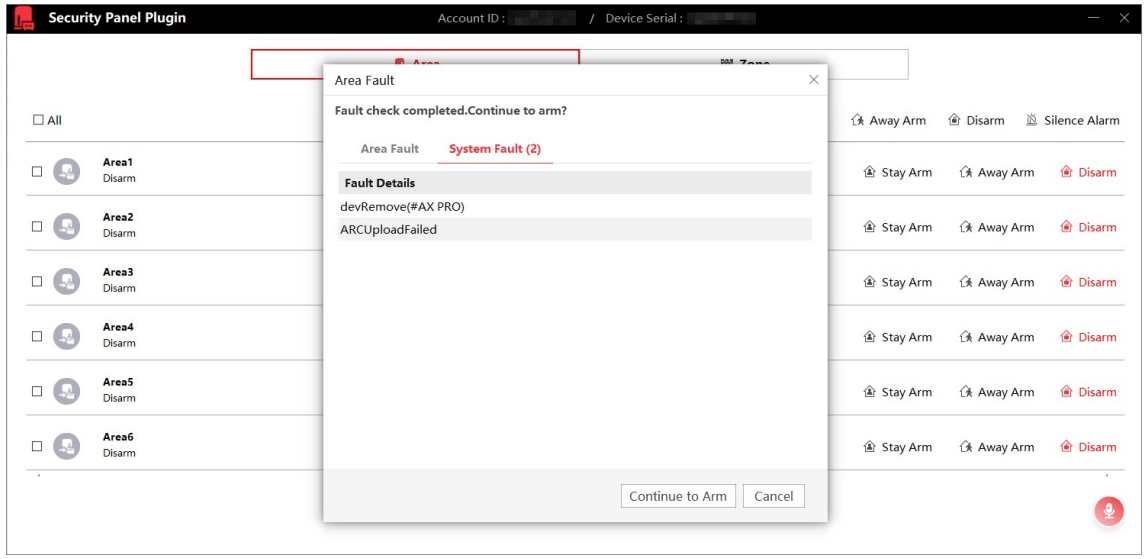


Figure 2-19 Fault Check

- For devices added via OTAP, zone bypass is replaced with permanent deactivation and one-time deactivation. You can select off, lid only, and entirely. See the table below for details.

Table 2-1 Zone Deactivation

Status	Definition	Description
Permanent Deactivation	The system will disable its alarms permanently.	**Off** The device operates in normal mode and transmits all events and alarms. **Lid Only** The system will ignore only tamper alarms. **Entirely** The system will ignore all alarms reported by the device.
One-Time Deactivation	The system will disable its alarms for each time the armed mode is active.	**Off** The device operates in normal mode and transmits all events and alarms. **Lid Only** The system will ignore only tamper alarms. **Entirely** The system will ignore all alarms reported by the device.

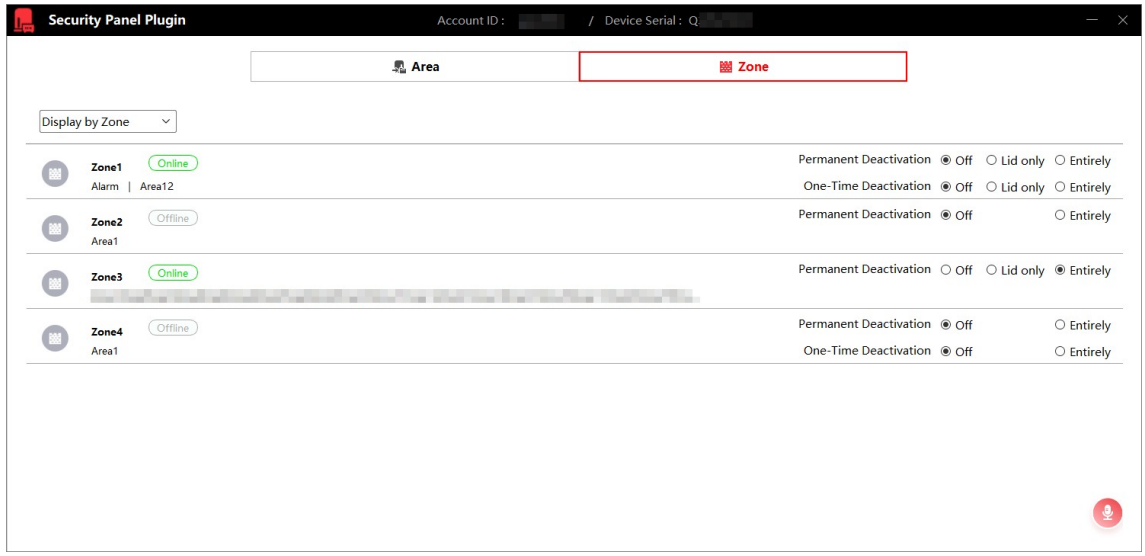


Figure 2-20 Deactivation

- On the **Maintenance → Operation Log** page, adds an operation log type **Deactivation**.

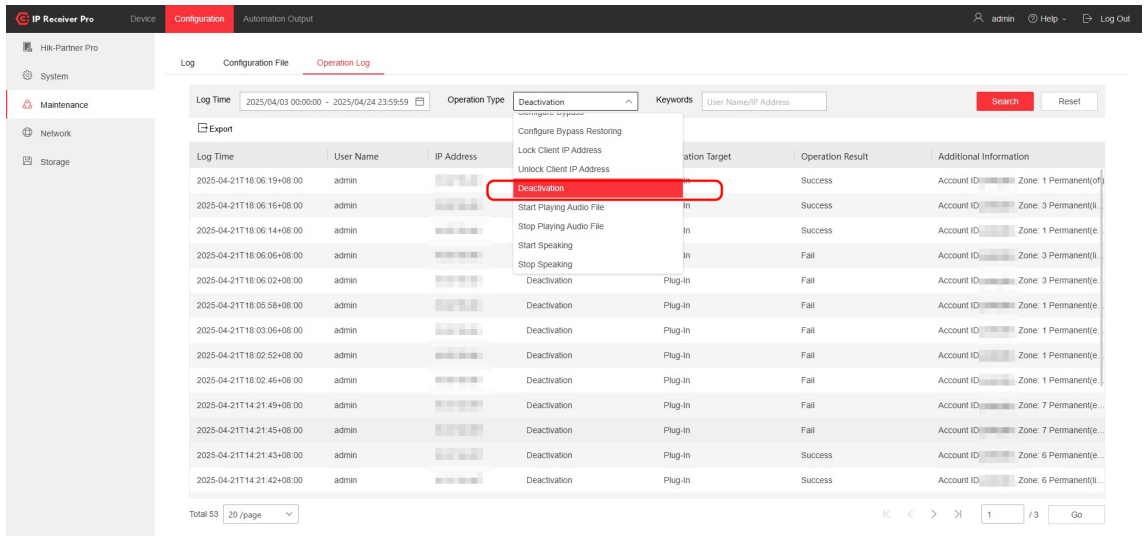


Figure 2-21 Operation Log

Chapter 3 Installation & Activation

3.1 Installation

1. Right-click the program file to run as the administrator and select **Next**.
2. Select **Browse...** to select a proper directory and select **Next**.
3. Edit the HTTP port if the port number is conflicted.
4. Select **Install**, read the post-install information, and then select **Finish**.

Note

- If you install the IPRP remotely, log into your local PC to get the Hik-Gateway Guard service.
- After installation, the Hik-Gateway Guard service will get started and hide in the notification area of the desktop.

3.2 Activation

By default, the IPRP defines the administrator user as admin. When you log into the IPRP for the first time, you are required to create a password for the admin user to activate the IPRP.

1. Enter the address of the computer or server running with the and port number in the address bar of the web browser.
   If the IP address of the computer running the IPRP is 172.6.21.96, and the port number is 80, you should enter http://172.6.21.96:80.
2. Enter the password and confirm password for the admin user.
3. Select **Activate**.

Note

If the IPRP port is occupied, go to **Configuration → Network → Port** to edit the port. Restart the IPRP after editing the port, or the settings will not take effect. You need to add corresponding firewall rules after editing ports for the IPRP, or the IPRP might not start.

3.3 Connect IPRP to CMS

IPRP transmits alarms and events through the event receiver of a Central Monitoring Station (CMS). You can configure communication with the CMS receiver via TCP/IP or COM port.

Connecting via COM Port

- If IPRP and CMS event receiver are installed on the same computer (local server), you can connect them using a COM port virtual emulator such as com0com to create a pair of virtual COM ports.
- You can also use a USD-RS232 adapter to connect separate computers through two physical COM ports. Take the Sur-Guard protocol as an example:

Software	Configuration
IPRP	1. Go to **Automation Output → Protocol** . 2. Set the Protocol Type to **Sur-Guard** and Interface to **RS-232**. 3. Set the Serial Port to **COM1**. 4. Set the following parameters. **Note** Baud Rate / Data Bit / Parity / Stop Bit / Compatibility / Account ID Length / Receiver Number / Line Card Number: Should be consistent with that of CMS.
CMS	1. Set the host IP, port and other parameters of CMS. 2. Set the COM port to **COM2** and set the Baud Rate, which should be consistent with that of IPRP. 3. Keep other parameters consistent with those of IPRP.

If the connection is established, your CMS will start to receive alarms and events from IPRP.

Connecting via Socket (TCP/IP)

1. Go to **Automation Output → Protocol** .
2. Set the Interface to **TCP/IP**.
3. Set the mode and set the address and port.
   - Server means the IPRP works as a server that receives requests from CMS. You need to set the listening port.
   - Client means the IPRP works as a client connecting to CMS. You need to specify the IP address and port of your CMS.

Chapter 4 Set Up HPP Account

Before adding devices managed on the HPP to the IPRP, you should set up an HPP account. To manage more than 10,000 devices on the IPRP, you can use this account to install the IPRP on multiple computers.

1. Select **Configuration → Hik-Partner Pro → Parameters** .
2. Configure the following parameters and select **OK**.

Parameter	Description
Hik-Partner Pro Open Platform Address	- RU: https://api.hik-partnerru.com - Other Countries/Regions: https://api.hik-partner.com
User Name (ARC ID) / Password (ARC Key)	After logging in to tpp.hikvision.com, select **Resource → ARC INTEGRATION GROUP** to get **Hik-Partner Pro Related Materials** for ARC Integration, where you can find how to get the ARC ID and ARC key.

Note

A Super Admin account will be automatically generated if you connect to Hik-Partner Pro successfully for the first time. You can reset the Admin password.

3. Set the account information.
   - If you check **Automatically Import Devices**, devices managed on Hik-Partner Pro will be automatically added to IP Receiver Pro every 5 minutes. You can choose **Account ID Type** as **Serial No.**, **Site Name**, or **Account Number**.

     Note

     For the **Account Number** option, you need to set the account number of devices on Hik-Partner Pro (go to **Site & Service → ARC Service → Set Account Number**) before the account number can be used as the devices' account ID. Otherwise, the serial No. will be used as account ID by default.
   - If you enable dual-connection, you will get more timely alarms and enjoy more stable connections. If an exception occurs when receiving alarms via ISUP5.0 or OTAP, the IPRP will receive alarms via HPP.
   - For security control panels, the dual connection mode is as follows.

Table 4-1 Dual Connection Mode

Device Version	IPRP Version	Dual Connection
AX PRO V1.3.0 / AX HYBRID PRO V2.0 / AX HOME V1.2.0	V2.2 or later	OTAP + HPP (OTAP will be prioritized)
AX PRO V1.3.0 or AX HYBRID PRO V2.0	Earlier than V2.2	ISUP + HPP (ISUP will be prioritized)
AX PRO (versions earlier than V1.3.0) or AX HYBRID PRO (versions earlier than V2.0)	V2.2 or later	- ISUP + HPP - Automatically switched to OTAP + HPP when devices are upgraded to the latest version.

- To ensure that the device supports the direct connection, you can set the port mapping according to your network topology.

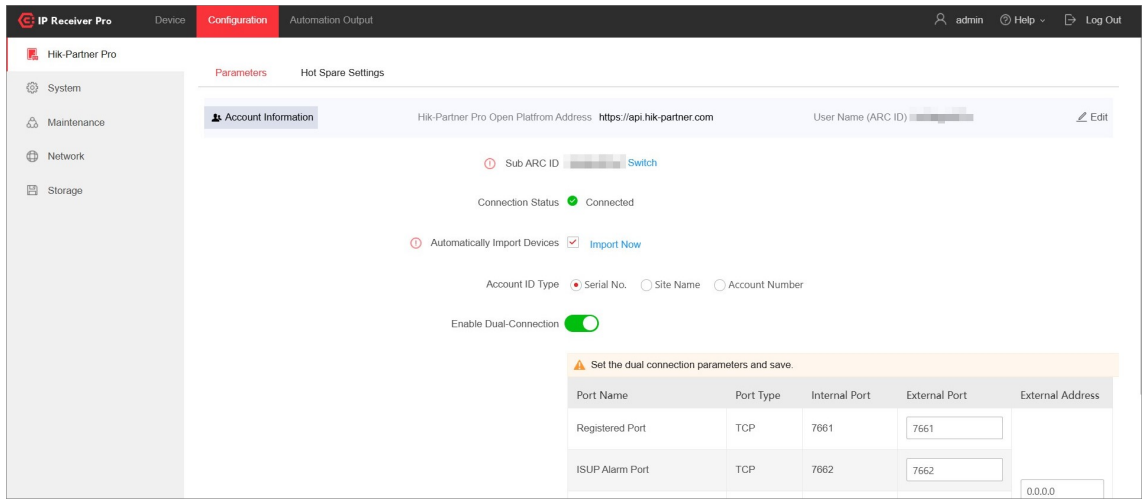


Figure 4-1 Account Information

Related Topics:

- ***Configure Hot Spare***
- ***Add Devices***

Chapter 5 Configure Hot Spare

After configuring HPP parameters, you can set up hot spare settings for a maximum of four IPRPs connected to the same HPP account (the same Hik-Partner Pro Address, ARC ID and ARC Key). This allows the four IPRPs to share backup information, ensuring that if one of them crashes, another one can be used. For detailed introduction and steps, use your phone to scan the following QR code.

Figure 5-1 How to Configure Hot Spare

Steps

For example, the 4 IPRPs' addresses are as follows:

Table 5-1 Server and Address

Server	Address
Host Server	http://10.66.163.157/
Spare Server 1	http://10.66.163.154/
Spare Server 2	http://10.66.163.174/
Spare Server 3	http:// 10.66.163.164/

1. Configure the host server:
   a. Log in http:// 10.66.163.157/, select **Configuration → Hik-Partner Pro → Hot Spare Settings** .
   b. Check **Enable Hot Spare**, and select the hot spare role to **Host Server**.
2. Configure the spare server:
   a. Log in http:// 10.66.163.154/, select **Configuration → Hik-Partner Pro → Hot Spare Settings** .
   b. Check **Enable Hot Spare**, and select the hot spare role to **Spare Server1**.
3. Follow the step 2 to set http://10.66.163.174 to Spare Server2 and http://10.66.163.164 to Spare Server3.

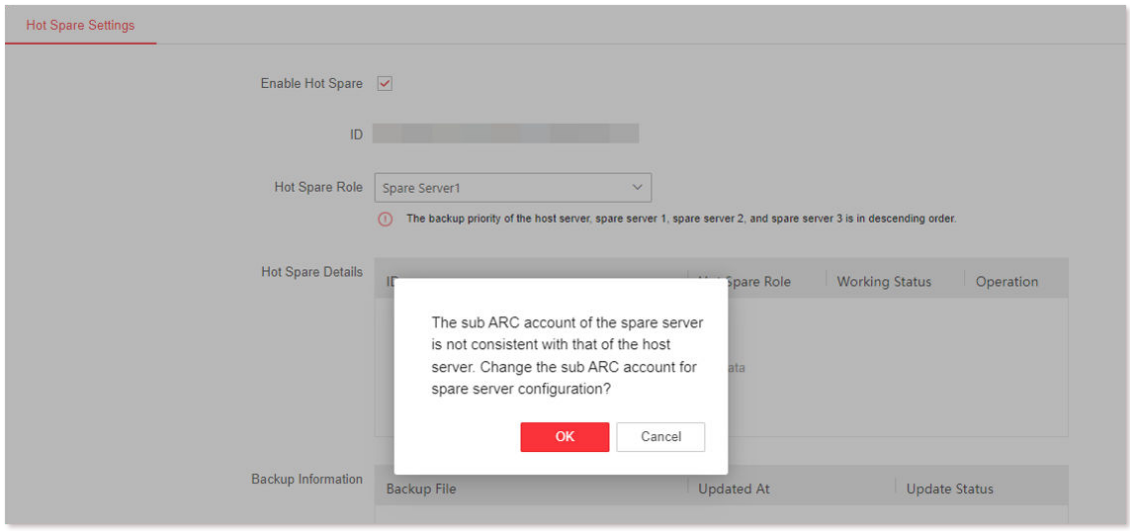


Figure 5-2 Hot Spare Settings

Note

- Only if you have selected a IPRP as the host server, can you configure spare servers.
- Ensure that the dual-connection mode is disabled for spare servers.
- Match the sub ARC accounts of the spare server and host server. If they don't match, switch the sub ARC account of the spare. After switching the sub ARC account of the spare server to match the host server, check **Enable Hot Spare** first. Otherwise, if you switch the sub ARC account of the spare server to a different one, the devices on the host server will be removed.

Chapter 6 Manage Devices

You can add multiple device types like network cameras, fall detection radars, auxiliary care radars, DVRs, NVRs, security control panels, and IP speakers to the IPRP. After devices are added, the IPRP can forward alarms and images/videos triggered by these devices to the ARC.

- ***Add Devices***
- ***Enable Alarm Service for Event Verification***

6.1 Add Devices

1. Configure devices.
   For devices added directly, enable ISUP or OTAP on the device's web configuration page and set the IPRP address and ports.

Table 6-1 Adding Method

Adding Method	How To
Hik-Partner Pro	Enable the ARC service for added devices on Hik-Partner Pro.
Add via ISUP/OTAP	For devices added directly, enable ISUP or OTAP on the device's web configuration page and set the IPRP address and ports.

2. Select **Device → Add** , set the connecting mode and configure the parameters. See the following table for details.

Table 6-2 Connecting Mode

Connecting Mode	Description
Hik-Partner Pro	View the devices that are not added by other IPRPs in the list. To view all added devices in the current IPRP, check **Display All**.
ISUP 5.0	- If the ISUP-enabled devices are added with a public IP address, select **Configuration → Network → Port Mapping** to set the port mapping. - If the ISUP-enabled devices are offline, log into the device's web page to check if the server address and server port are correct.
OTAP	You can add AX PRO V1.3.0 / AX HYBRID PRO V2.0 / AX HOME V1.2.0 to Hik IP Receiver Pro via OTAP. To switch

Connecting Mode	Description
	the connecting mode of devices added via ISUP5.0 to OTAP, you need to add these devices via OTAP.
Third-Party Devices	The alarms triggered by third-party devices will be transmitted to the ARC directly (bypassing the IPRP). You can set zones and channels for third-party devices. After receiving the alarms, you can use our plug-ins for video verification.

3. After adding devices, you can open device-specific plug-ins in the **Operation** column. For more details, see ***Verify Events*** .

6.2 Enable Alarm Service for Event Verification

Introduction

After adding devices, you should enable the alarm service for devices of different types. For details, see the following table.

Device Type	Description
Encoding Devices / Radars / Third-Party Devices	You can add partitions (areas) and zones, and link channels to zones for alarm verification.
Access Control Devices / IP Speakers	You can only enable the alarm service.
Security Control Panels	The partitions (areas) zones and linked channels have been configured on the device's web configuration page. The IPRP will transmit alarms and videos once the alarm service is enabled. You can only link encoding devices to a zone.

How to Enable Alarm Service for Encoding Devices and Radars

1. After adding devices, select on the Operation column to enter the alarm service setting page.
2. Check **Enable Alarm Service**.
3. Select the video verification mode.

Video Verification Mode	Video Verification on DC-09	Alarm URL Format
Plug-in	Plug-in	http://IP:Port/page/videoReview?token=<>&account=<>&event=<>&typ

Video Verification Mode	Video Verification on DC-09	Alarm URL Format
		e=<>&zone=<>&alarmTime=<>&alarmInfo=<>&devSource=<>
Auto Download Video	Plug-in	http://IP:Port/<URI>?token=<>&type=videoReview
Plug-in & Auto Download Video	Plug-in	http://IP:Port/page/videoReview?token=<>&account=<>&event=<>&type=<>&zone=<>&alarmTime=<>&alarmInfo=<>&devSource=<>
Auto Download Video	Alarm Video	http://IP:Port/<URI>?token=<>&type=videoReview

4. Add the partition (area) and zone, and link channels to the zone.

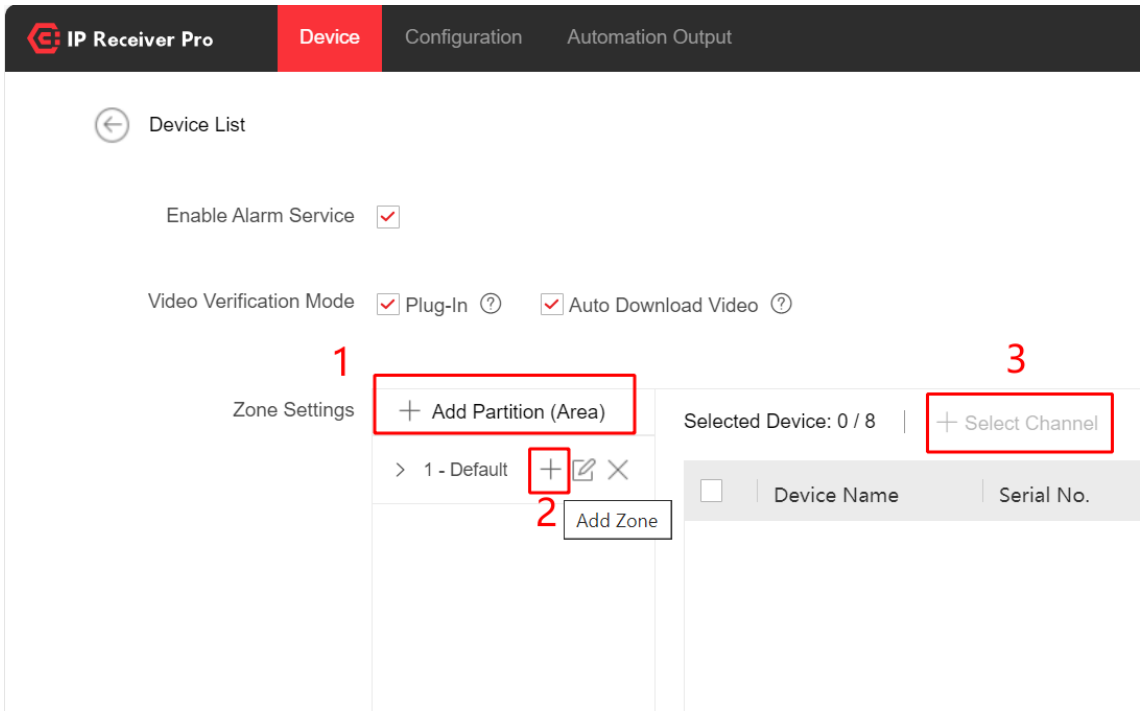


Figure 6-1 Add Partition & Zone

No.	Operation	Note
1	Add Partition (Area)	Only encoding devices, third-party devices, and radars support adding a partition (area).
2	Add Zone	- Ensure that the zone information are consistent on both the IPRP and the ARC. - For fall detection radars and auxiliary care radars, you can add only one partition (area) and one zone.
3	Link Channel to Zone	- For encoding devices, you can only link their own channels to their zones. - For encoding devices, up to 4 video channels and 4 I/O channels can be linked to a zone; For other devices like radars, up to 4 video channels can be linked to a zone. - For third-party devices, you can link their zones with channels of encoding devices added by ISUP5.0 or Hik-Partner Pro (in a single HPP account).

How to Enable Alarm Service for Security Control Panels

1. After adding devices, select on the Operation column to enter the alarm service setting page.
2. Check **Enable Alarm Service**.
3. Link channels to the zone.

Note

- For security control panels added by Hik-Partner Pro, you can only select encoding devices in the same site.
- For security control panels added by ISUP5.0 or OTAP, you can select the encoding devices added by the following methods.

Connecting Method	Description
Hik-Partner Pro	You can select encoding devices authorized to the same ARC in any sites.
ISUP5.0	You can select all ISUP-enabled encoding devices.

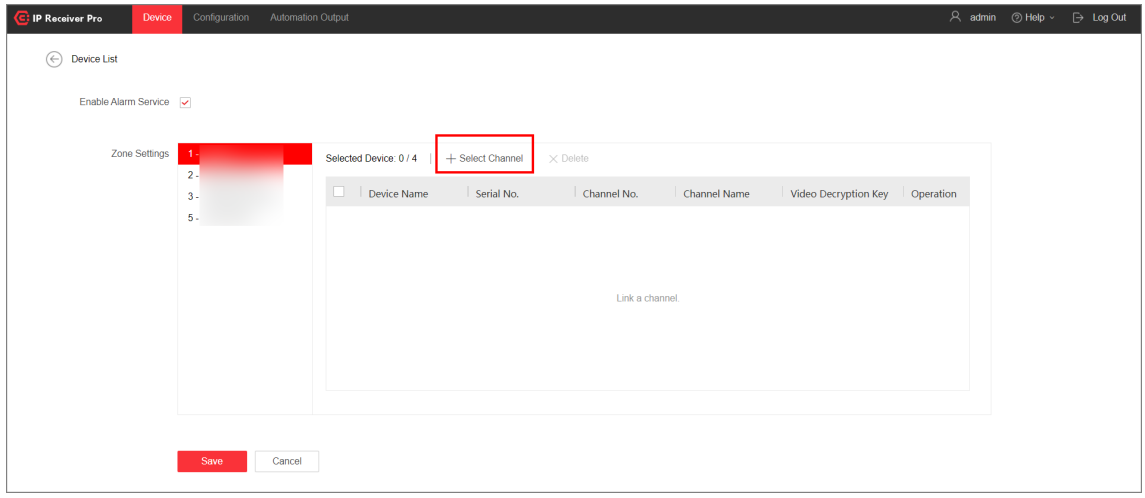


Figure 6-2 Link Channels to Zone

4. Select **Save**.

How to Enable Alarm Service for Access Control Devices / IP Speakers

1. After adding devices, select on the Operation column to enter the alarm service setting page.
2. Check **Enable Alarm Service** and select **Save**.

Note

If you set the protocol type to **DC-09** and the video verification mode to **Plug-In**, the alarm URL format will be http://IP:Port/page/videoReview?token=<>&account=<>&event=<>&type=1&channel=<>&alarmTime=<>&alarmInfo=<>&devSource=<>.

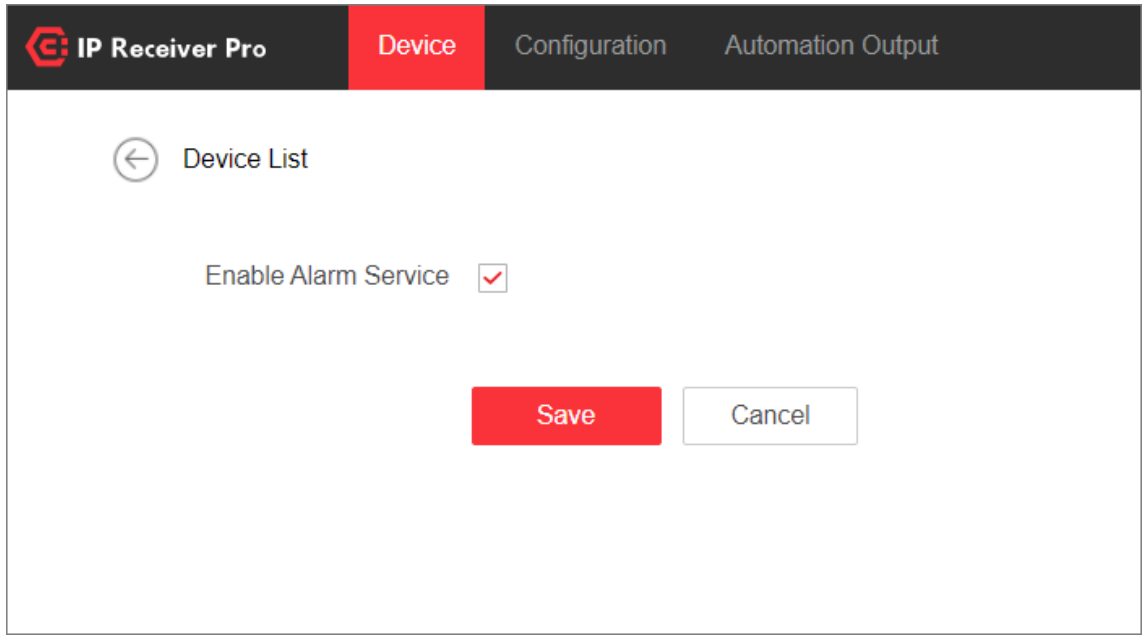


Figure 6-3 Enable Alarm Service for Access Control Devices / IP Speakers

Chapter 7 Configure Protocols

The IPRP receives events triggered by devices, converts them into standardized protocol messages, and transmit them to a CMS software. Configure supported protocols for transmitting events to your CMS. After configuration, you can view the real-time communications between IPRP and CMS.

Steps

1. Select **Automation Output → Protocol → Enable** .
2. Select a protocol from the **Protocol Type** list and configure the parameters.

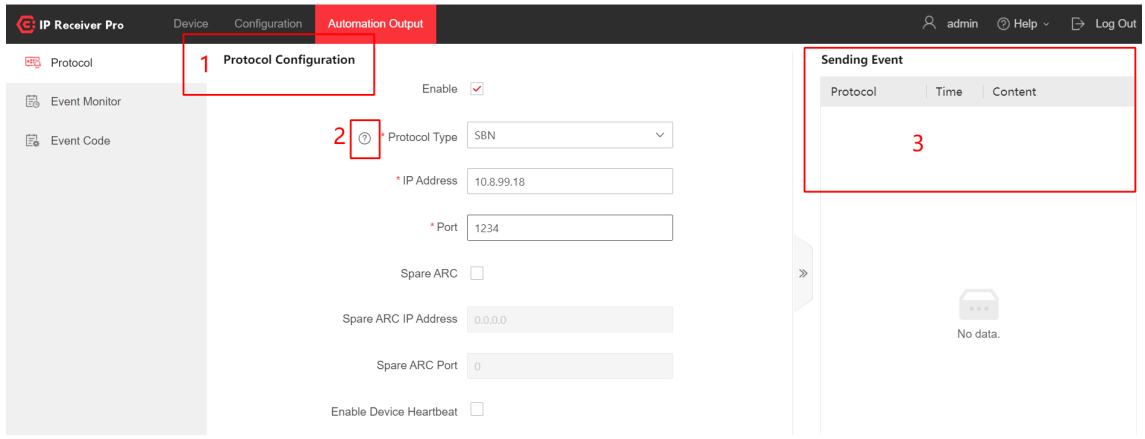


Figure 7-1 Protocol Configuration

NO.	Parameter	Description
1	Protocol Configuration	Configure the protocol parameters as needed.
2	Message Template	Select this tooltip to view the message template.
3	Real-Time Events	Real-Time communications between IPRP and CMS.

Protocol Introduction

The IPRP supports protocols for transmitting events to your CMS software:

Table 7-1 Event Transmission

Protocol	Description
Sur-Gard	• Alarm and event transmission • Alarm verifications by our plug-ins or the URL on Alarm Monitor Page
Ademco 685	• Alarm and event transmission • Alarm verifications by our plug-ins or the URL on Alarm Monitor Page
Manitou	• Alarm and event transmission • Transmission of auto-downloaded video (binary data converted from Base 64) for verifications • Alarm verifications by our plug-ins or the URL on Alarm Monitor Page • Transmission of the coordinates of the panic button pressed in an AX PRO security control panel
SBN	• Alarm and event transmission • Transmission of auto-downloaded video (**<object id="232454994" type="201" ext="mp4" event_id="0">**) for verifications • Transmission of the coordinates of the panic button pressed in an AX PRO security control panel • Alarm verifications by our plug-ins or the URL on Alarm Monitor Page
DC-09	• Alarm and event transmission • Alarm verifications by our plug-ins or the URL on Alarm Monitor Page • Transmission of a video/picture or the URL on Alarm Monitor Page for verifications • Transmission of the panic button pressed in an AX PRO security control panel • Transmission of the device temperature • Transmission of the confidence of the triggered source's probabilities for human, vehicle, or other objects in an AI-analyzed videos from the security control panel added via Hik-Partner Pro

Parameter Description

Event Transmission over Sur-Gard

Parameter	Description
Mode	• Set the Interface to **TCP/IP**. Server means the IPRP works as a server that receives requests from CMS. Client means the IPRP works as a client connecting to CMS. • Set the Interface to **RS-232**. You can use a USD-RS232 adapter to connect separate computers through two physical COM ports.
Compatibility	The Sur-Gard protocol version. To prevent IPRP from being disconnected with your ARC frequently, select the same version on both the CMS and IPRP.
Heartbeat	Hik IP Receiver Pro Heartbeat Interval Range: 10-65535 seconds. Device Heartbeat Interval Range: 10 to 86400 seconds. If you disable Period Test on the Device Configuration page, set the heartbeat interval to allow your CMS to receive Periodic Report Test (HeartBeat Alarm) or other alarms regularly.

Event Transmission over Ademco 685

Parameter	Description
Receiver Number	The number used for marking IPRP as an information receiver. Keep it the same with the number set on your CMS.
Line Card Number	The number of the line used for communications between IPRP and ARC. Keep it the same with the number set on your CMS.

Event Transmission over DC-09

Parameter	Description
Attempts	If the IPRP does not receive the response from the CMS during the response time period, the IPRP will attempt to retransmit the message. It ranges from 1 time to 10 times and 3 times is the default.
Response Timeout Period	If the IPRP does not receive the response from the CMS during this period, it indicates that no response has been sent to the IPRP. It ranges from 5 seconds to 60 seconds, and 20 seconds is the default.
Video Verification Mode	• If you set the mode to **Plug-In**, IPRP will transmit the URL on Alarm Monitor Page to your CMS.

Parameter	Description
	Note If you set this mode to **Plug-In**, you need to set the video verification mode in the Zone Settings page to Plug-in and go to **Configuration → System → Alarm Monitor** to enable Alarm Monitor. • If you set the mode to **Alarm Video**, IPRP will transmit an auto-downloaded video URL or a picture URL to your CMS.

Event Transmission over Manitou

Manitou provides a generic mechanism to allow the IPRP to send a Signal into the CMS by use of an XML signal format.

Test Signal

It refers to periodic signals sent by the IPRP to the CMS to confirm its operational status and communicate in case of an alarm. You can set the test signal interval, ID, event type, and event ID.

Chapter 8 Manage Events and Alarms

You can search for history events by triggering time, start video/image/intercom verifications in various ways, and add undefined events. This chapter contains the following sections:

- ***Search Events***
- ***Verify Events***
- ***Add Event Codes***

8.1 Search Events

You can search the history events to view the event source, event code, triggering time and other detailed information.

Account ID / Serial No.

Fuzzy match search is not supported. You need to enter the full account ID or serial No. for accurate search results.

Triggering Time

The default time range for searching historical events spans from 00:00:00 to 23:59:59 in the PC's time zone. In case the device and the PC have different time zones, you can adjust the time range by setting it one day earlier or later.

Customize Column Items

You can customize column items by clicking in the upper-right corner. **Confidence** is unchecked by default.

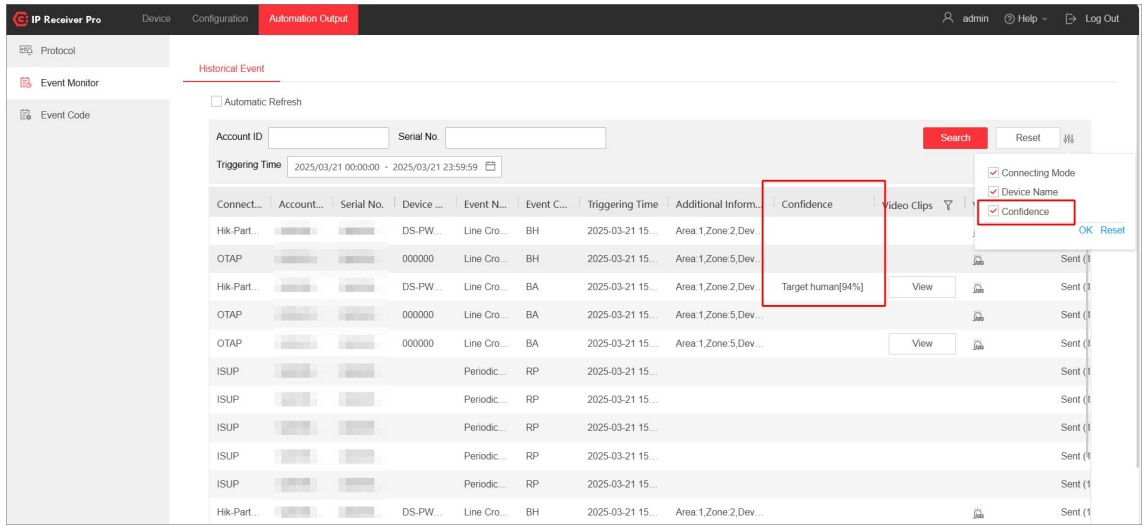


Figure 8-1 Search Events

Note

If you customize columns on the Event Monitor page, the settings will automatically sync to the URL on the Alarm Monitor page.

8.2 Verify Events

After enabling the alarm service for devices and the devices report alarms to the IPRP, you can view history events, start event verifications in various ways, and add undefined events.

Make sure you have enabled the alarm service for devices. See ***Enable Alarm Service for Event Verification*** .

8.2.1 Verify Events via Web Plug-In

1. Select **Automation Output → Event Monitor** .
2. In the **Video Clips** column or the **Verification Plug-In** column, select one of the following icons to verify events.

   Note

   For an optimal plug-in experience, it is recommended to set your computer's display scaling to 100%.

Video Verification via Plug-In

If you set the video verification mode to **Plug-In** when enabling the alarm service, you can start video verification via our web plug-in .

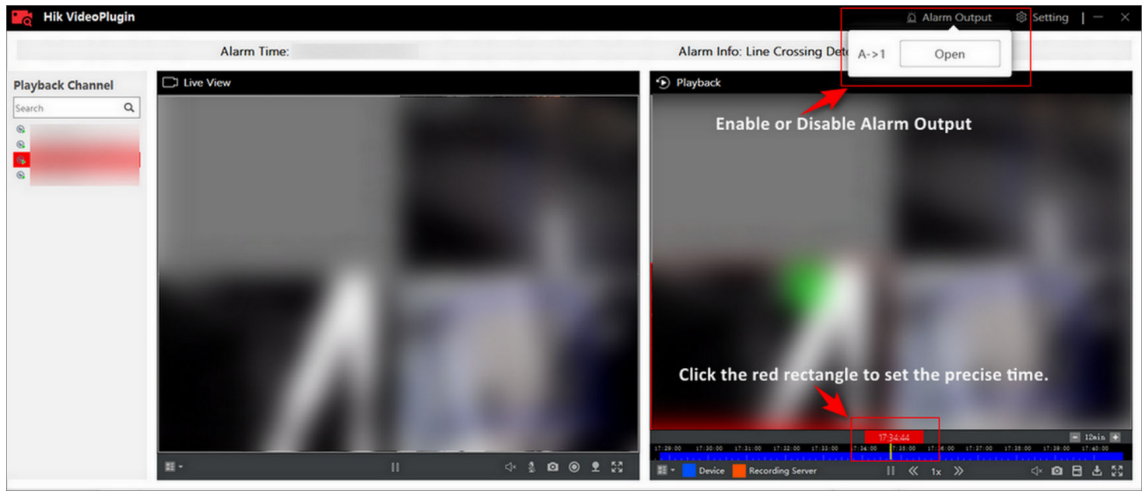


Figure 8-2 Video Verification Page

For devices added via HPP, you can switch between the main stream or the sub stream (by default) based on your actual needs for playback quality, power consumption, etc.

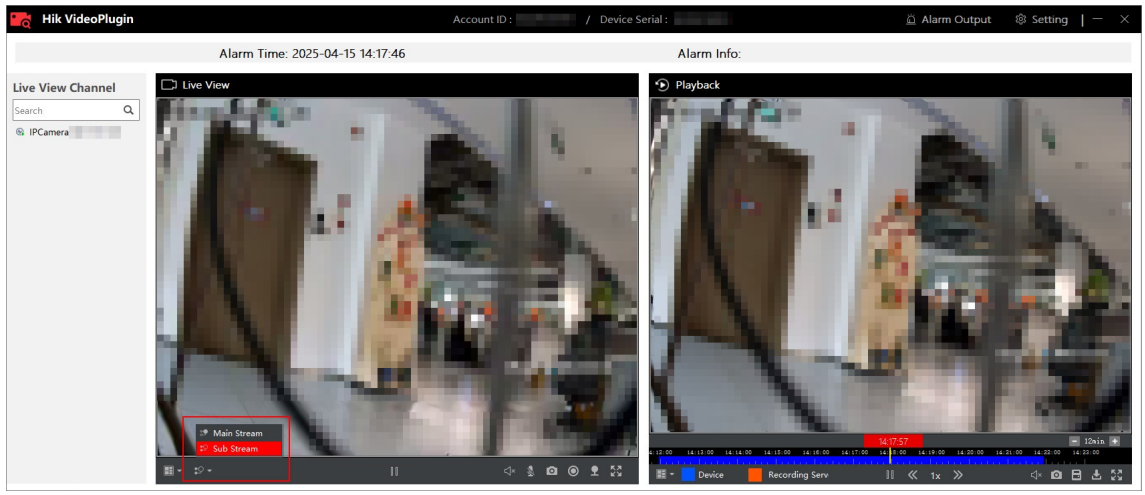


Figure 8-3 Video Verification via Plug-in

Control Security Control Panel via Plug-in

Operate security control panels and start a two-way audio with the sounder of a security control panel via our web plug-in . If this icon shows together with , you can start video verification for linked channels.

Select **Area**, and you can view area information and perform the following operations.

Table 8-1 Area

Operation	Description
Stay Arm	Select a area, and select **Stay Arm** to arm the area in Arm Stay mode when you are at home. Select multiple areas and select **Stay Arm** to arm all the checked areas when you are at home.
Away Arm	Select a area, and select **Away Arm** to arm the system when you are away from home. Select multiple areas and select **Away Arm** to arm all the selected areas when you are away from home.
Disarm	Select a area, and select **Disarm** to disarm the area. Select multiple areas and select **Disarm** to disarm all the selected areas.
Silence Alarm	Select **Silence Alarm** to mute alarms of an area. Select multiple areas and select **Silence Alarm** to mute alarms of the selected areas.

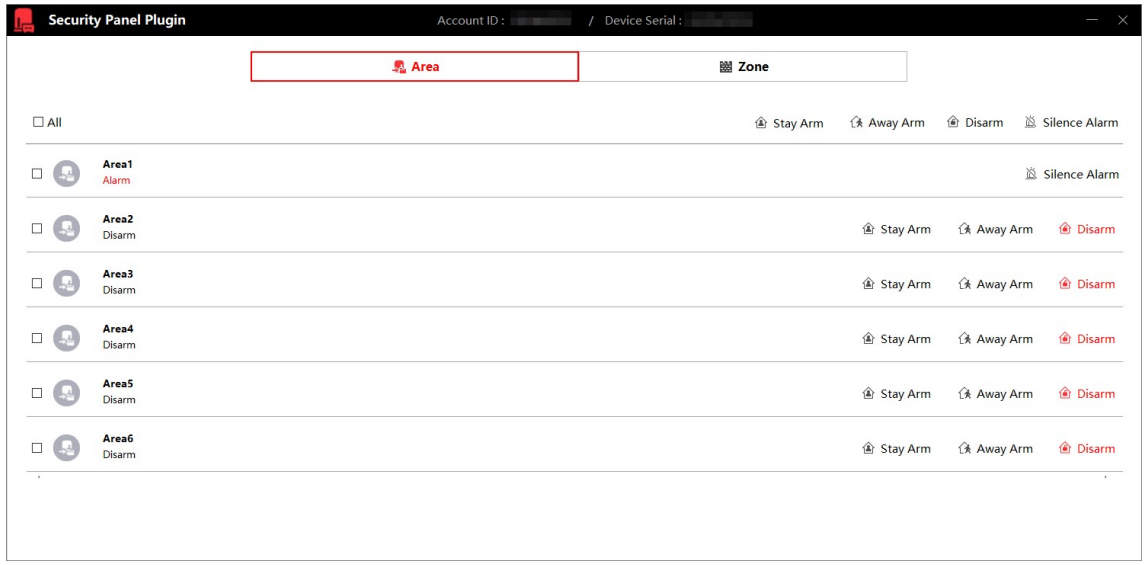


Figure 8-4 Area Settings

After enabling **Fault Checklist when Arming** on the device added via OTAP (go to **Configuration → System → Service**), the arming process will perform zone self-checks, including verification of battery status, power supply availability, device connection, etc. This ensures all critical components are in optimal condition before arming completion.

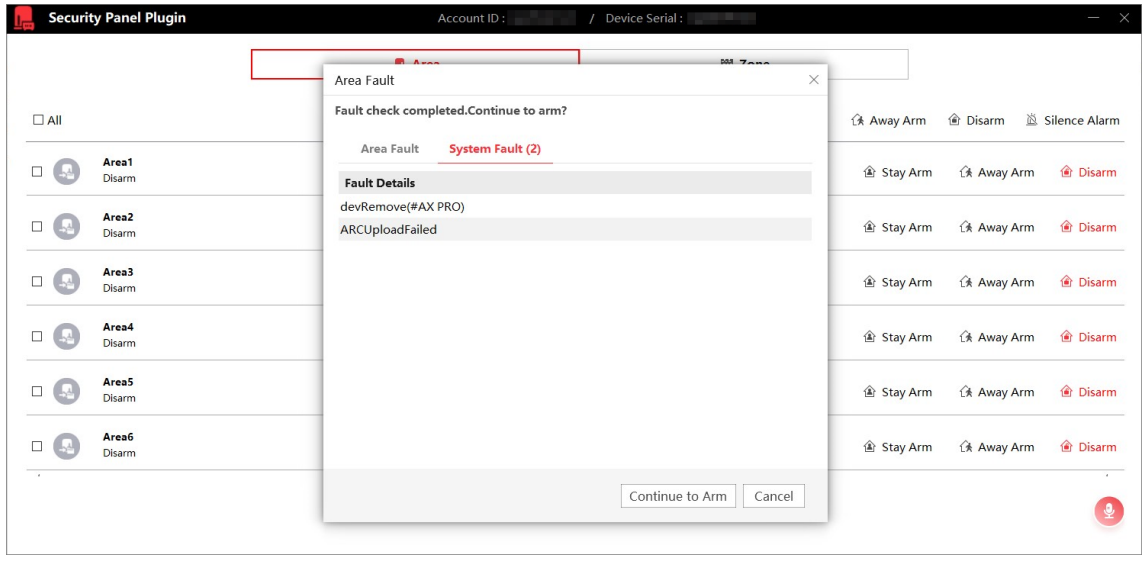


Figure 8-5 Fault Check

Select **Zone**, and you can view the zone information and perform the following operations.

If you want to intentionally arm your area with one or more zones unprotected, select a zone and enable **Zone Bypass**. If you bypass a zone, the zone will NOT be armed (any alarms from the zone will not be triggered), even if other zones in an area is armed.

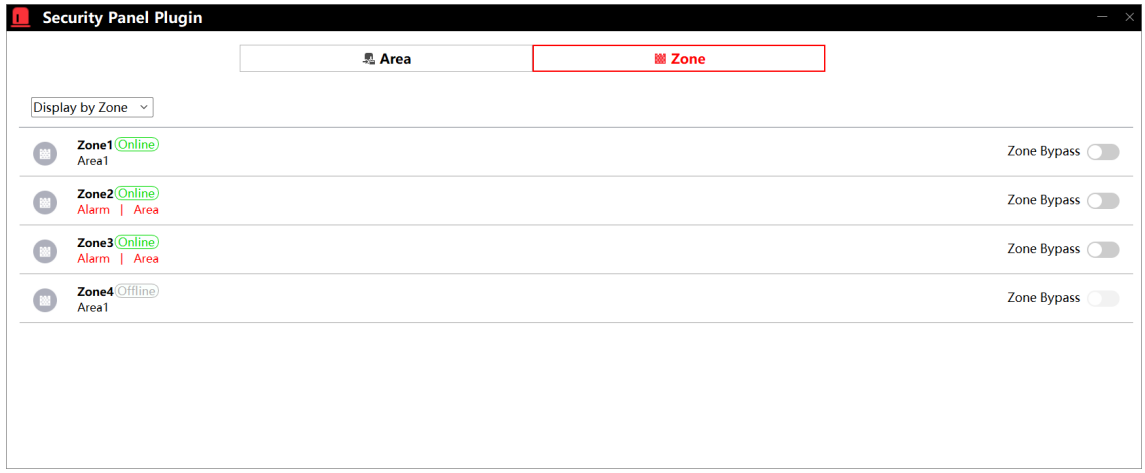


Figure 8-6 Zone Bypass

You can also perform zone deactivation for AX PRO (V1.3.0 or later), AX HYBRID PRO (V2.0 or later) and AX HOME (V1.2.0 or later).

Table 8-2 Zone Deactivation

Status	Definition	Description
Permanent Deactivation	The system will disable its alarms permanently.	**Off** The device operates in normal mode and transmits all events and alarms. **Entirely** The system will ignore all alarms reported by the device. **Lid Only** The system will ignore only tamper alarms.
One-Time Deactivation	The system will disable its alarms for each time the armed mode is active.	**Off** The device operates in normal mode and transmits all events and alarms. **Entirely** The system will ignore all alarms reported by the device. **Lid Only** The system will ignore only tamper alarms.

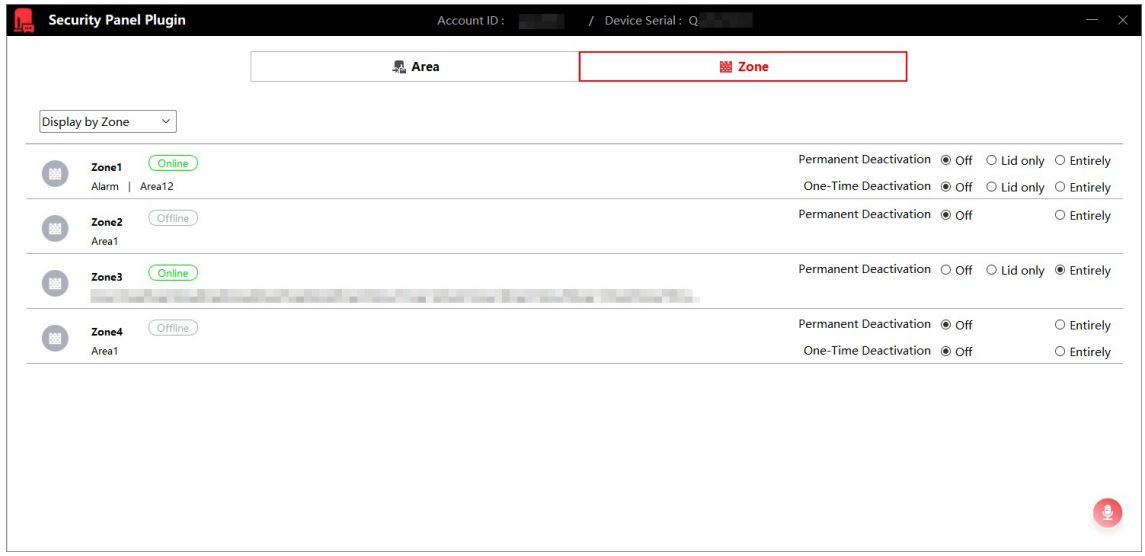


Figure 8-7 Zone Settings

For both half-duplex sounders and full-duplex sounders of an AX PRO device (V1.3 and later), you will automatically be on a call when you launch the plug-in if the two-way audio does not time out.

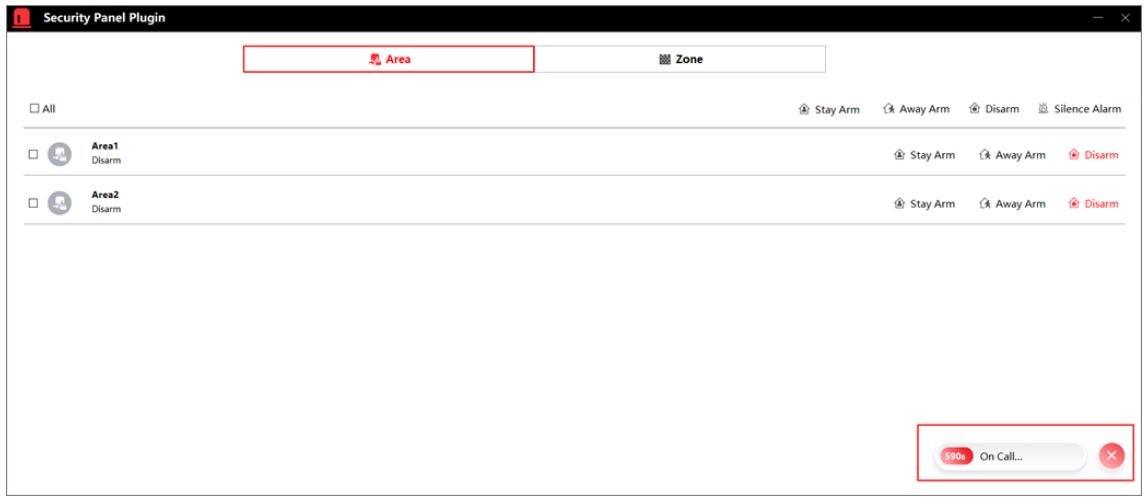


Figure 8-8 Two-Way Audio with Full-Duplex Sounder

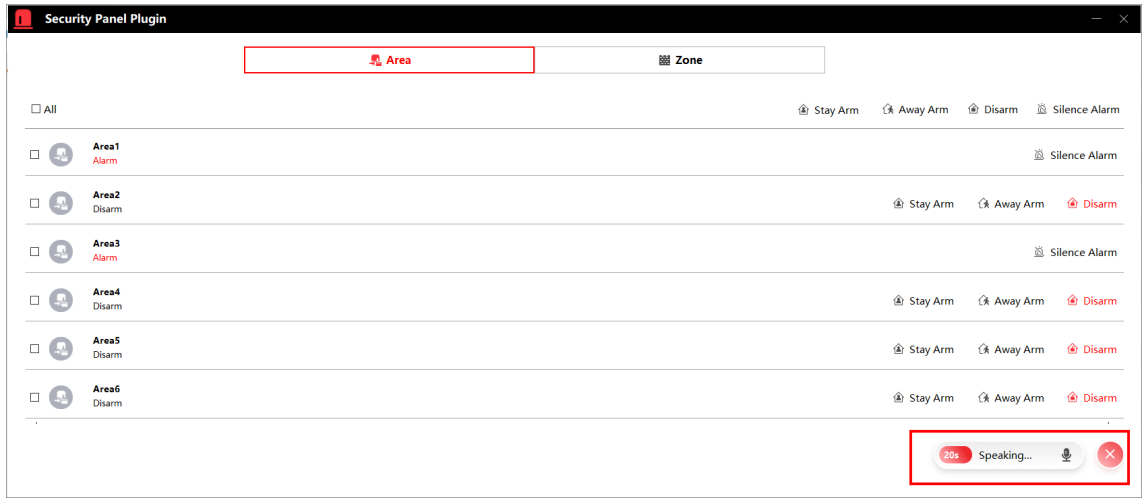


Figure 8-9 Listening with Half-Duplex Sounder

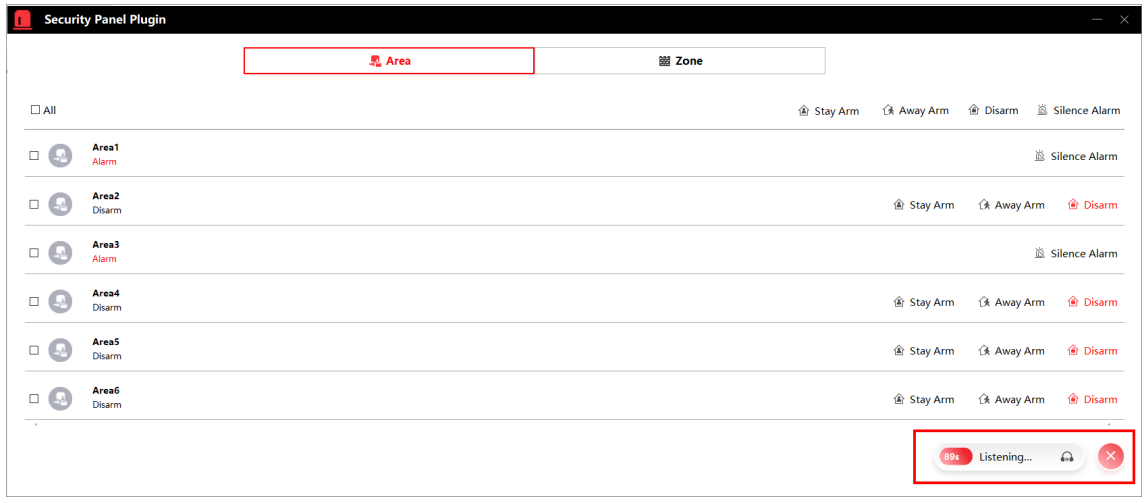


Figure 8-10 Speaking with Half-Duplex Sounder

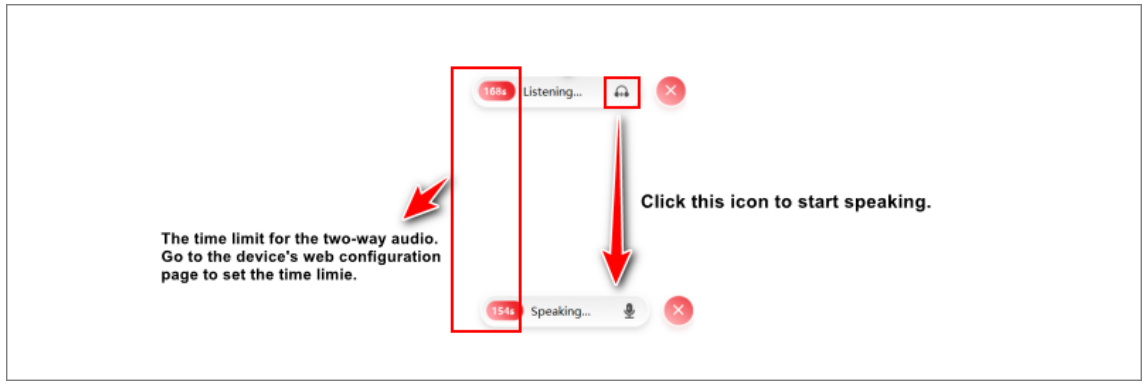


Figure 8-11 Two-Way Audio with Half-Duplex Sounder

Note

The two-way audio function is only available when a security control panel is linked sounder or the two-way audio does not time out.

You can click View to view related videos:

- For security control panels linked with a PIR camera, you can view the alarm-related video or image uploaded by the PIR camera.
- For 180° PIRCAM of AX PRO, verify two videos recorded by the top and bottom cameras.
- If you set the video verification mode to Auto Download Video, add a partition/zone, and link channels to the zone for encoding devices, you can view an auto downloaded video.
- You can view AI-analyzed videos from the security control panel added via Hik-Partner Pro. The triggered source, when in motion, are now highlighted with a red detection box and features a confidence level indicator for more effective false alarm filtering. In the **Confidence** column, you can view the source's probabilities for human, vehicle, or other objects.
- If you manually delete these videos/images stored in a disk, you cannot see them when clicking on this button. The default storage period is 2 days.

Intercom Verification via Plug-In

Start the intercom verification via our web plug-in . You can accept or decline calls from the device.

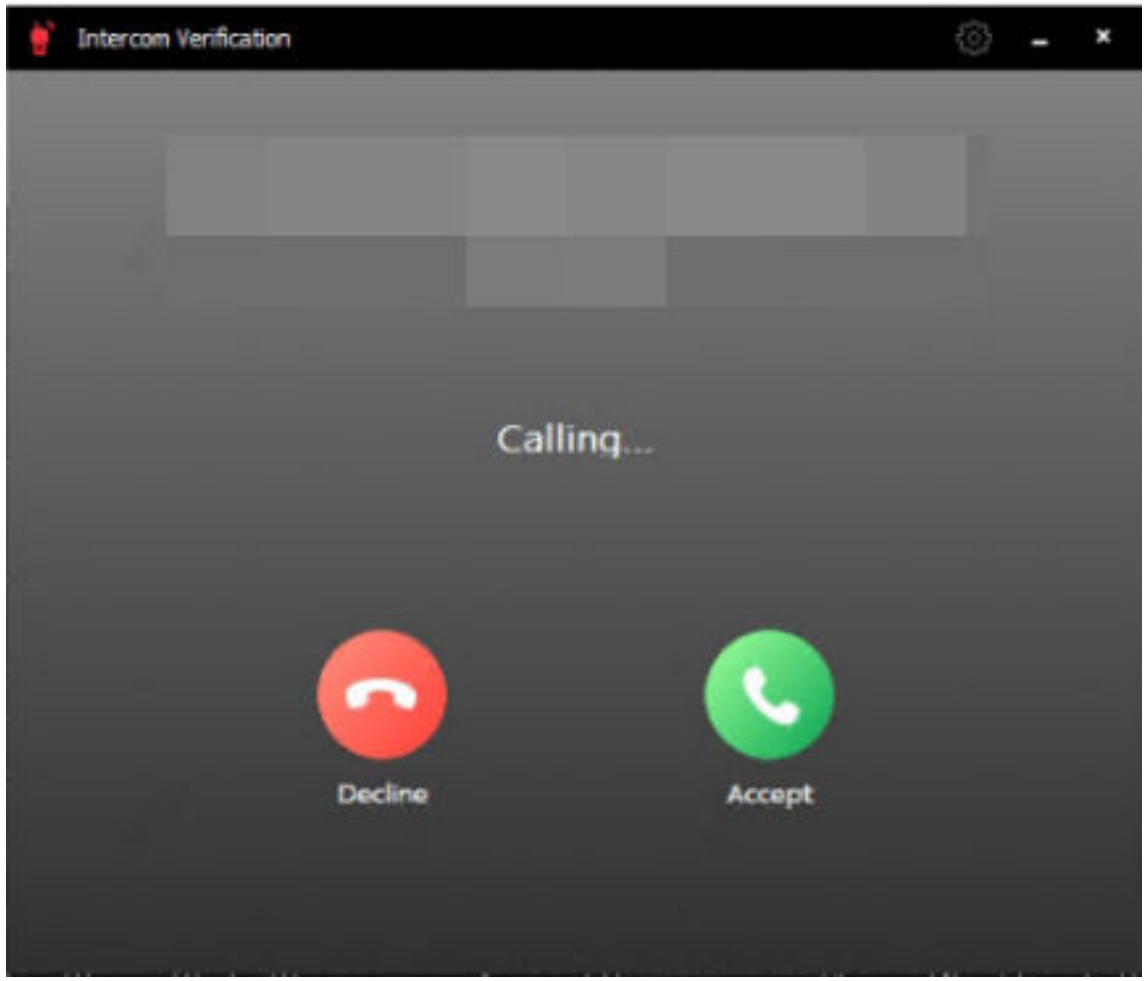


Figure 8-12 Intercom Verification

When accepting calls, you can click **Open Door** to open doors remotely.

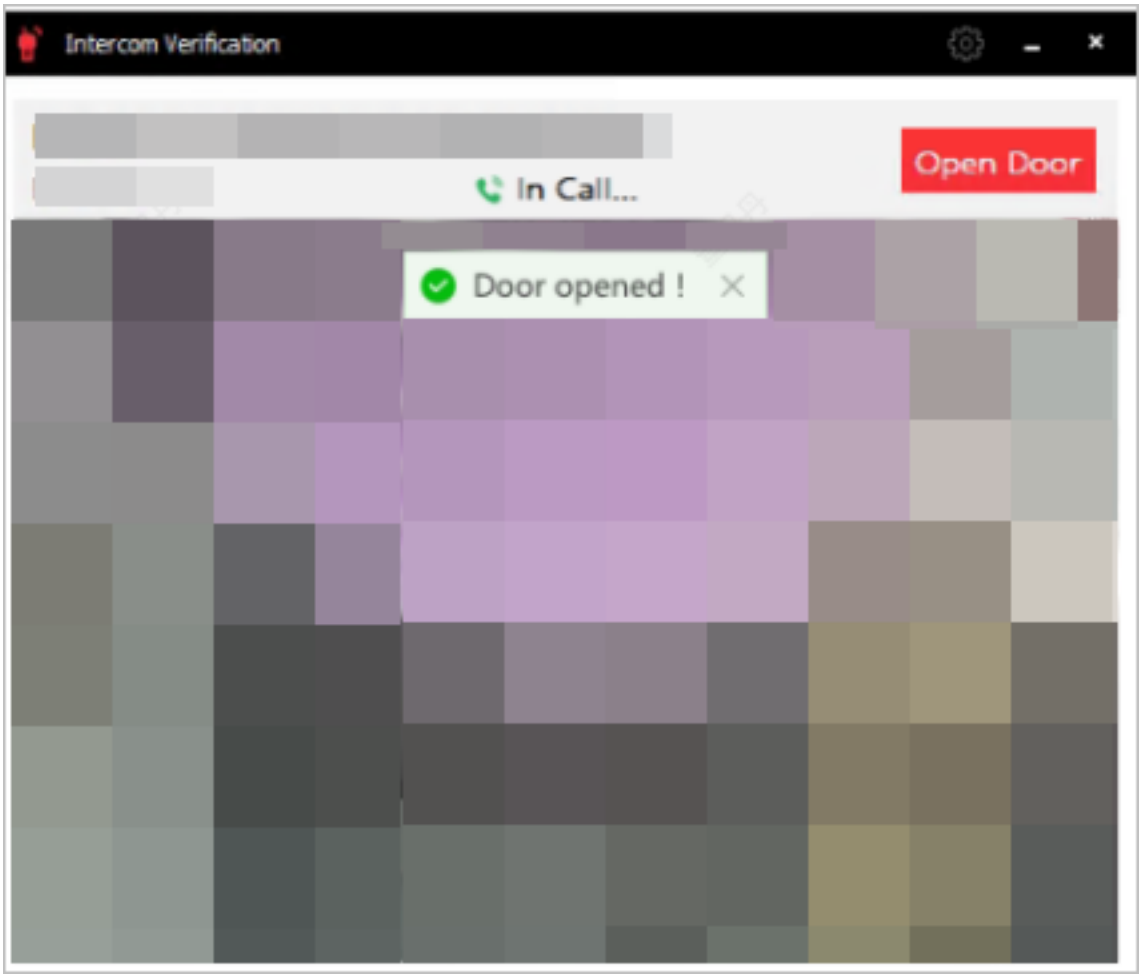


Figure 8-13 Open Door

Note

- A plug-in is required for starting two-way audio. Ensure that you have installed audio input and output devices on your PC.
- You can set the time allowed for starting two-way audio after an alarm is triggered on the device configuration page.
- If the two-way audio is not available, enable this function on the **Device Configuration** page, and then select **Synchronize Device Information** on the **Device List** page.

Control IP Speaker via Plug-in

For IP speakers added managed on HPP, you can play audio files, control volume, and start speaking.

- The volume of audio files and spoken announcements adjusts simultaneously.
- To speak to multiple devices simultaneously, click **Speak** and select devices as needed.
- To play audio files for multiple devices simultaneously, select devices as needed from the drop-down Device Serial No. menu.

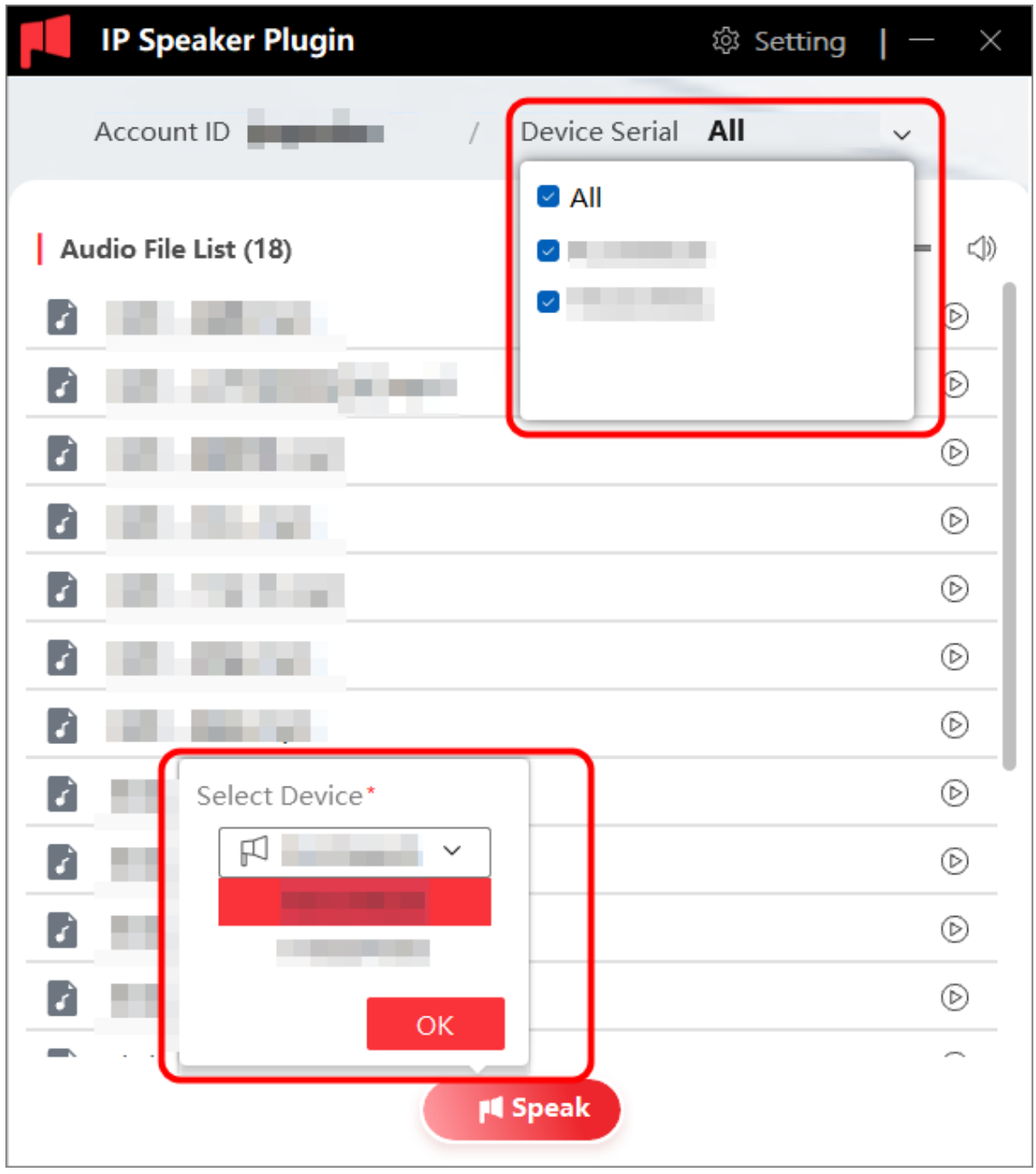


Figure 8-14 Batch Control

8.2.2 Verify Events via URL

1. Select **Configuration → System → Alarm Monitor → Enable** .
   You can customize tokens (32-64 alphanumeric characters required). Note that HTTPS requests are required for ensuring secure network transmission of URL requests. For HTTPS configuration, see ***Configure Network*** .

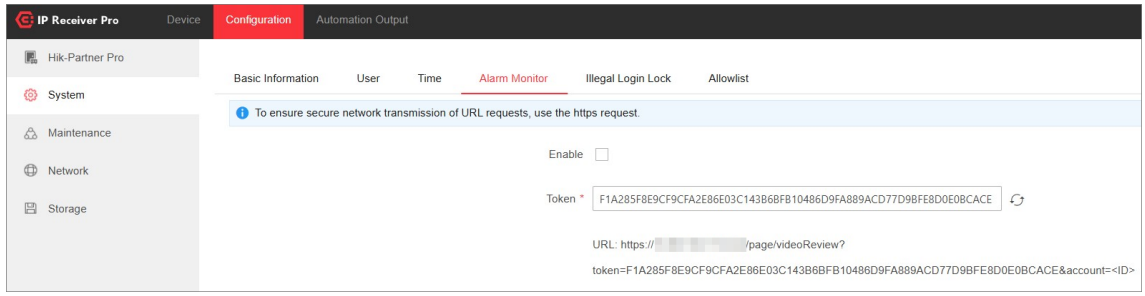


Figure 8-15 Alarm Monitor

2. Copy the URL to access the event verification page.
   For example, if the URL is https://10.10.10.1:80/page/videoReview?token=4XXXXXX&account=<ID>, and the device's account ID is 1234, you need to enter https://10.10.10.1:80/page/videoReview?token=4XXXXXX&account= 1234 to enter the Web page for verifying alarms. You can click the plug-in icon (vary by device type) to open the web plug-in even when no events/alarms are triggered.

Note

You can open multiple plug-ins simultaneously, but only one instance of each type can be active at a time.

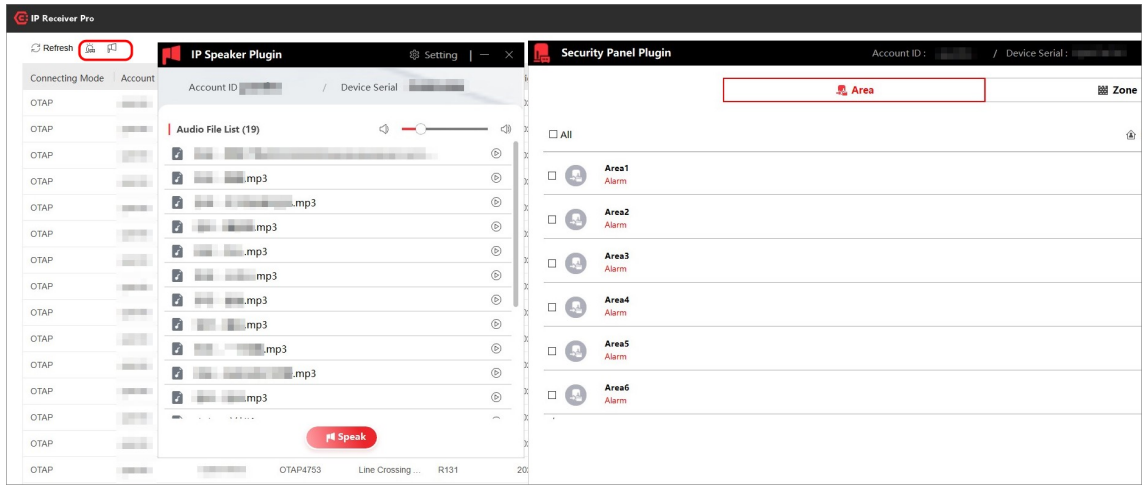


Figure 8-16 Event Verification Page via URL

8.3 Add Event Codes

The ARC identifies events from security control devices using event codes. When a security control device triggers an event, the IPRP receives the original code. It then converts this original code into a target code, such as a CID code or SIA code, which can be understood by the ARC. This allows you to receive event notifications through the ARC. In addition, you can view inspection events including the communications between the IPRP and HPP.

Steps

If the event triggered on the device is not defined, the event name will be Undefined Event. You can add the undefined event and edit events to keep them consistent with those configured on the ARC.

1. Select **Automation Output → Event Code** .
2. Select **Add** to add the event name, original code, CID Code or SIA Code.

Note

- You can delete only the event codes of security control panels.
- Two inspection events: Device Key Exception and Device Key Exception Restored will not be forwarded by fault.
- For event code details, click the following links:
  - ***Event Codes for Security Control Panels***
  - ***Event Codes for Encoding Devices***
  - ***Event Codes for Access Control Devices***
  - ***Event Codes for Radars***
  - ***Event Codes for Status***

8.3.1 Set Sending Interval

For encoding devices, you can configure the alarm sending interval. If multiple alarms are triggered by the same device or channel within (less than) the set interval, the IPRP will only forward the first alarm.

Related Topic: *Restore Event Interval*

Steps

1. Select **Automation Output → Event Code → Device Event** .
2. Select **Encoding Device**, select in the Operation column, and set Sending Interval.

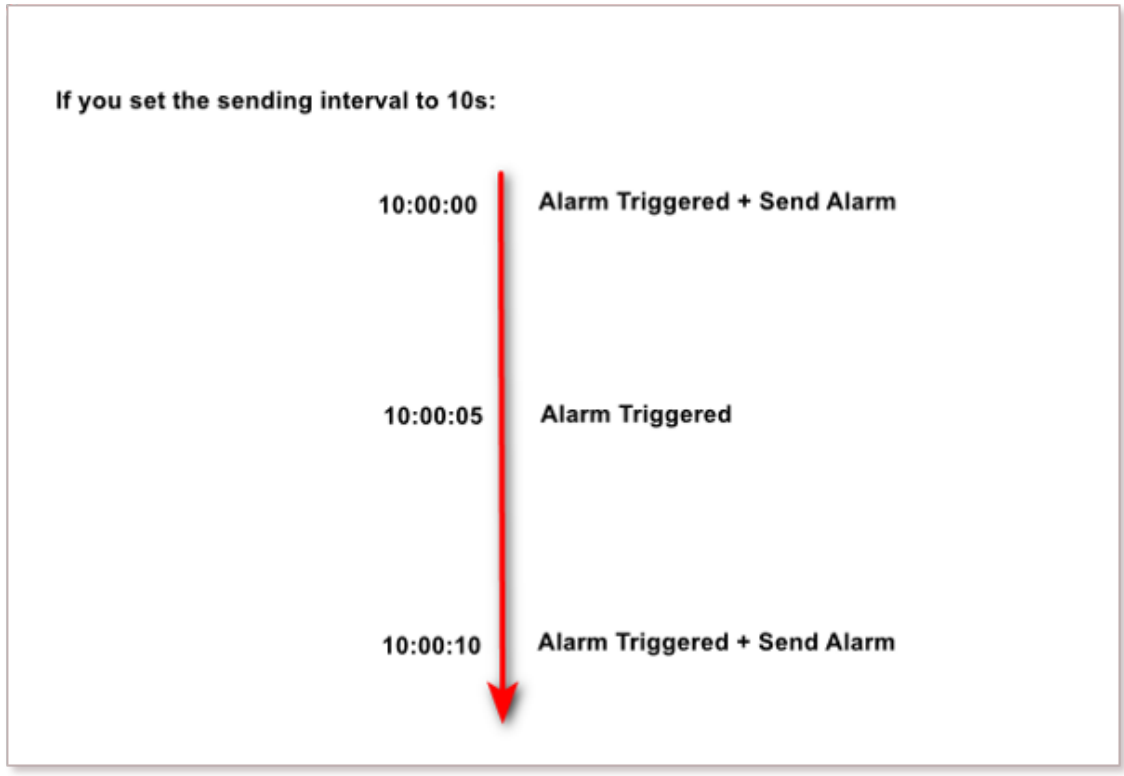


Figure 8-17 What is Sending Interval

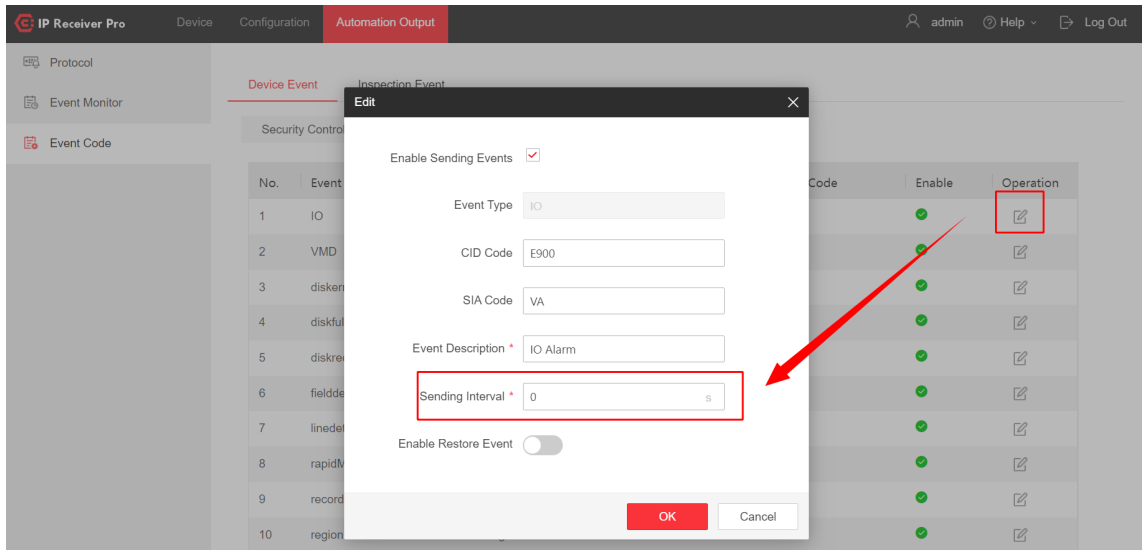


Figure 8-18 Sending Interval

8.3.2 Restore Event Interval

For encoding devices, you can set the restore event interval. If multiple alarms are triggered by the same device or channel within the set interval, the IPRP will send the restore event for the latest alarm.

Related Topic: ***Set Sending Interval***

Steps

1. Select **Automation Output → Event Code → Device Event** .
2. Select **Encoding Device**, select in the Operation column, enable **Restore Event** and set the parameters.

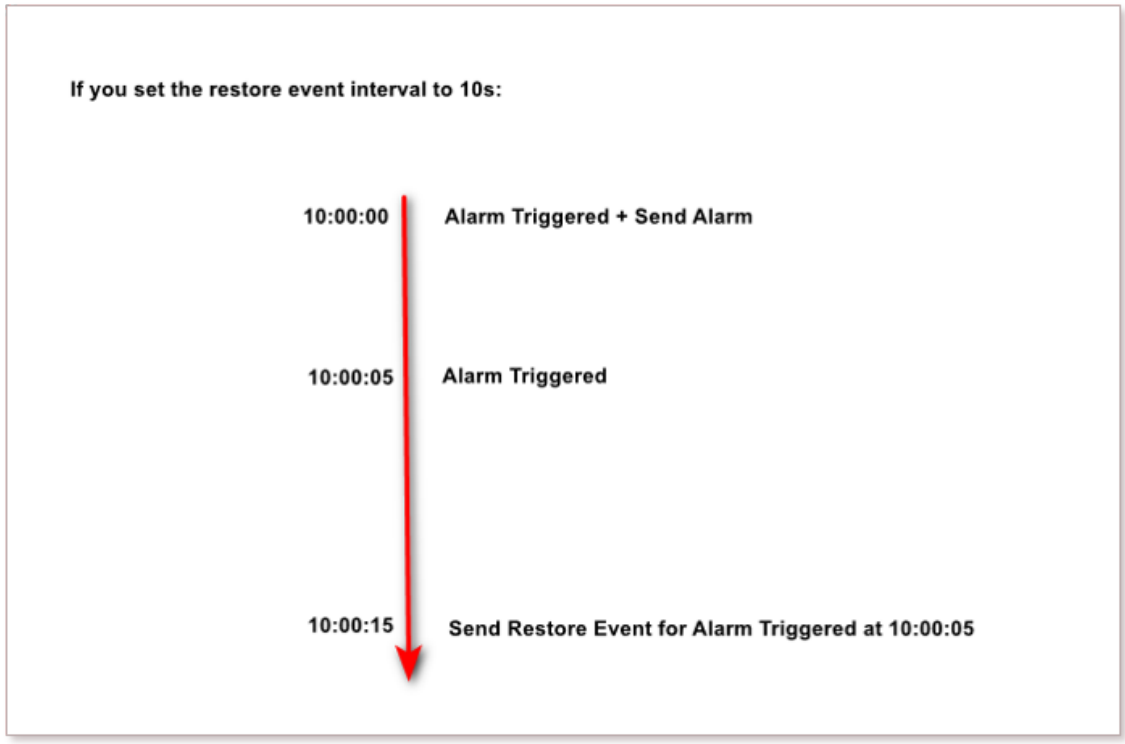


Figure 8-19 What is Event Interval

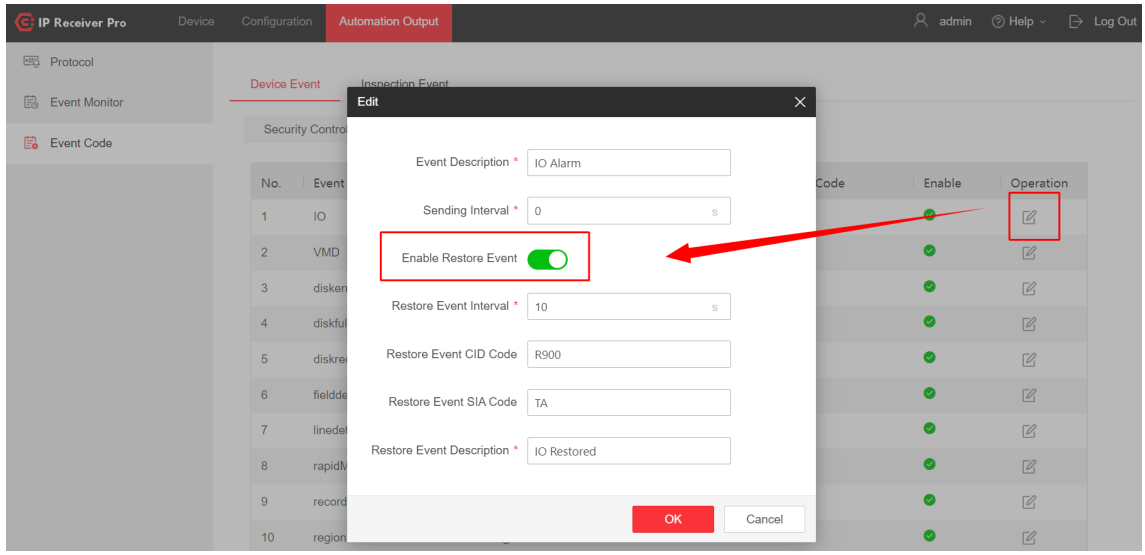


Figure 8-20 Set Event Interval

Note

If you set both the restore event interval and sending interval, the sending interval will prevail.

8.4 Event Codes

- ***Event Codes for Security Control Panels***
- ***Event Codes for Encoding Devices***
- ***Event Codes for Access Control Devices***
- ***Event Codes for Radars***
- ***Event Codes for Status***

8.4.1 Event Codes for Security Control Panels

HikCode	CIDCode	SIACode	Description
1100	E100	MA	Medical Alarm
1103	E130	BA	Burglary Alarm
1110	E111	FA	Fire Alarm
1114	E114	KA	Fire Alarm
1121	E121	HA	Duress
1122	E122	HA	Silent Panic Alarm

HikCode	CIDCode	SIACode	Description
1123	E123	AA	Audible Panic Alarm
1124	E133	AB	24H Alarm
1125	E133	BA	24H Vibration Alarm
1126	E130	BA	Timeout Alarm
1127	E120	BA	Silent Panic Alarm
1129	E120	PA	Panic Alarm
1130	E130	BA	Burglary Alarm
1131	E131	BA	Perimeter Alarm
1132	E132	AD	Interior Burglary Alarm
1133	E130	BA	24H Alarm
1134	E134	BA	Entry/Exit Alarm
1137	E316	TA	Device Tampered
1139	E139	BV	Confirmed Alarm
1141	E141	AE	BUS Open-circuit Alarm
1142	E142	AF	BUS Short-circuit Alarm
1144	E144	TA	External Probe Disconnected
1148	E145	AG	Device Motion Alarm
1149	E137	BA	Masking Alarm
1151	E162	GA	Gas Leakage Alarm
1154	E154	WA	Water Leakage Alarm
1207	E207	AH	Zone Early-Warning
1301	E301	AT	AC Power Loss
1302	E302	YT	Low System Battery
1305	E305	ZY	Control Panel Reset
1310	E311	YT	Battery Fault
1311	E311	YM	Battery Disconnected

HikCode	CIDCode	SIACode	Description
1312	E312	YI	Overcurrent Protection Triggered
1313	E313	YT	Battery Fault
1314	E314	YM	Battery Missing
1318	E311	YM	Power Depletion
1319	E319	YP	Overvoltage Protection Triggered
1328	E328	AI	Power Output Short Circuit
1330	E330	ET	Expander Fault
1333	E333	AI	Expander Exception
1336	E336	AJ	Printer Disconnected
1337	E338	XT	Repeater Battery Low
1338	E338	AL	Expander Low Voltage
1339	E301	YP	Mains Power Lost
1340	E311	YM	Repeater Battery Disconnected
1341	E144	TA	Lid Opened
1342	E301	YP	Expander AC Power Loss
1343	E144	TA	Wireless Repeater Tampered
1344	E144	TA	Wireless Siren Tampered
1345	E381	XL	Wireless Siren Disconnected
1346	E144	TA	Wireless Device Tampered
1347	E384	XT	Low Wireless Device Battery

HikCode	CIDCode	SIACode	Description
1348	E381	XL	Wireless Device Disconnected
1349	E337	YP	External Power Failure
1351	E351	LT	Main Channel ATP Fault
1352	E352	LT	Backup Channel ATP Fault
1354	E354	AM	Telephone Line Disconnected
1359	E354	YC	Uploading Report Failed
1380	E380	FT	Detector Sensor Fault
1382	E382	AN	BUS Supervision Fault
1383	E144	TA	Detector Tampered
1386	E386	AO	Zone Open-circuit Alarm
1387	E387	AP	Zone Short-circuit Alarm
1401	E401	OP	Disarming
1403	E403	OA	Auto Disarming
1406	E406	BC	Alarm Clearing
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

HikCode	CIDCode	SIACode	Description
1462	E462	AT	Auto Disarming Failed
1467	E461	JA	Incorrect Password
1556	E556	AT	Network Change
1570	E570	QB	Zone Bypassed
1571	E570	QB	Deactivated Temporarily
1572	E383	TU	Lid Deactivated / Lid Was Temporarily Disabled
1573	E573	QB	Deactivated
1574	E574	AU	Group Bypass
1601	E601	AV	Manual Report Test
1602	E602	RP	Periodic Report Test
1607	E607	TS	Test Mode Entered
1617	E617	AW	Telephone Connection Test
1627	E627	LB	Enter Programming
1628	E628	LX	Exit Programming
1750	E750	IA	Drilling alarm
1753	E158	KS	High Temperature Alarm
1754	E159	ZA	Low Temperature Alarm
1759	E131	BA	Intrusion Alarm
1773	E131	BA	Cross-Zone Alarm
1774	E774	AX	PIR Alarm
1775	E775	AY	Sudden Increase of Sound Intensity Alarm
1776	E776	AZ	Sudden Decrease of Sound Intensity Alarm

HikCode	CIDCode	SIACode	Description
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
1786	E153	KT	Temperature Alarm
1810	E120	PA	Keypad/Keyfob 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	E421	BD	Unregistered Tag
1910	E910	BE	Keypad Disconnected

HikCode	CIDCode	SIACode	Description
1911	E911	BF	KBUS Relay Disconnected
1912	E912	BG	KBUS GP/K Disconnected
1913	E913	BH	KBUS MN/K Disconnected
1914	E381	XL	Wireless Detector Disconnected
1915	E384	XT	Wireless Detector Low Battery
1916	E381	XL	Expander Disconnected
1917	E381	XL	Wireless Repeater Disconnected
1918	E918	BI	Radar Transmitter Fault
1919	E384	XT	Wireless Siren Low Battery
1920	E920	NT	Cellular Data Network Disconnected
1921	E921	NT	SIM Card Exception
1922	E922	NT	Wi-Fi Communication Fault
1923	E344	XQ	RF Signal Exception
1924	E924	NT	Network Flow Exceeded
1925	E384	XT	Low Keyfob Battery
1926	E926	NT	SIM Card Phone Number Conflicted
1930	E930	NT	IP Address Conflicted
1931	E931	NT	Wired Network Exception

HikCode	CIDCode	SIACode	Description
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	Sending Email 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 Consulting
1970	E970	BX	BUS Query
1971	E971	BY	BUS Registration
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	Wireless Repeater Deleted

HikCode	CIDCode	SIACode	Description
1979	E306	CF	Wireless Siren Deleted
1980	E306	CG	Wireless Device Deleted
1982	E306	XI	Panel Reset to Factory Settings
1983	E983	RB	Upgrading Firmware
1984	E984	RS	Upgrading Firmware Failed
1985	E985	UR	User has been removed
1986	E986	UR	User has been removed
1987	E383	TB	Notifications about the state of the lid are disabled
1988	E570	QB	Device deactivated
1989	E100	MA	Slient Medical Alarm
1991	E991	YI	Bus Overload
3100	R100	MH	Medical Alarm Restored
3103	R130	BH	Burglary Alarm Restored
3110	R111	FH	Fire Alarm Restored
3114	R114	KH	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	BH	24H Vibration Alarm Restored

HikCode	CIDCode	SIACode	Description
3126	R130	BH	Timeout Alarm Restored
3129	R120	PH	Panic Alarm Restored
3130	R130	BH	Burglary Alarm Restored
3131	R131	BH	Perimeter Alarm Restored
3132	R132	CK	Interior Burglary Alarm Restored
3133	R130	BH	24H Alarm Restored
3134	R134	BH	Entry/Exit Alarm Restored
3137	R316	TR	Device Tamper Restored
3139	R139	BW	Confirmed Alarm Restore
3141	R141	CL	BUS Open-circuit Restored
3142	R142	CN	BUS Short-circuit Restored
3144	R144	TR	External Probe Connected
3148	R145	CO	Device Motion Alarm Restored
3149	R137	BH	Masking Alarm Restored
3151	R162	GH	Gas Leakage Alarm Restored
3154	R154	WH	Water Leakage Alarm Restored
3207	R207	CP	Zone Early-Warning Dismissed
3301	R301	AR	AC Power Restored

HikCode	CIDCode	SIACode	Description
3302	R302	YR	Low System Battery Restored
3310	R311	YR	Battery Fault Restored
3311	R311	YR	Battery Reconnected
3312	R312	YJ	Overcurrent Protection Restored
3313	R311	YR	Battery is OK
3314	R311	YR	Battery Reconnected
3319	R319	YQ	Overvoltage Protection Restored
3328	R328	CQ	Power Output Short Circuit Restored
3330	R330	ER	Expander Fault Restored
3333	R333	CQ	Expander Restored
3336	R336	CR	Printer Connected
3337	R338	XR	Repeater Battery Voltage Restored
3338	R338	CS	Normal Expander Voltage
3339	R301	YQ	Mains Power Restored
3340	R311	YR	Repeater Battery Reconnected
3341	R144	TR	Lid Restored
3342	R301	YQ	Expander AC Power Loss Restored
3343	R144	TR	Wireless Repeater Tamper Restored
3344	R144	TR	Wireless Siren Tamper Restored
3345	R381	XC	Wireless Siren Connected

HikCode	CIDCode	SIACode	Description
3346	R144	TR	Wireless Device Tamper Restored
3347	R384	XR	Low Wireless Device Battery Restored
3348	R381	XC	Wireless Device Connected
3349	R337	YQ	External Power Restored
3351	R351	LR	Main Channel ATP Restored
3352	R352	LR	Backup Channel ATP Restored
3354	R354	CU	Telephone Line Connected
3359	R354	YK	Report Uploading Restored
3380	R380	FJ	Detector Sensor Fault Restored
3382	R382	CV	BUS Supervision Restored
3383	R144	TR	Detector Tamper Restored
3400	R400	CL	Arming
3401	R401	CL	Away Arming
3403	R403	CA	Auto Arming
3408	R408	CW	Instant Arming
3409	R409	OS	Keyswitch Zone Arming
3441	R441	NL	Stay Arming
3442	R442	CX	Forced Arming
3443	R443	CX	Turn Off Output by Schedule
3570	R570	QU	Zone Bypass Restored

HikCode	CIDCode	SIACode	Description
3571	R570	QU	Active Again
3572	R383	QU	Active Again
3573	R573	BU	Restored after auto deactivation
3574	R574	CZ	Group Bypass Restored
3607	R607	TE	Test Mode Exited
3750	R750	IR	Drilling Alarm Restored
3753	R158	KA	High Temperature Alarm Restored
3754	R159	ZH	Low Temperature Alarm Restored
3759	R131	BH	Intrusion Detection Restored
3773	R131	BH	Cross-Zone Alarm Restored
3774	R774	CZ	PIR Alarm Restored
3775	R775	DE	Sudden Increase of Sound Intensity Alarm Restored
3776	R776	DF	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

HikCode	CIDCode	SIACode	Description
3783	R158	KH	High Temperature Alarm Restored
3784	R159	ZH	Low Temperature Alarm Restored
3786	R153	KJ	Temperature Alarm Restored
3862	R501	DO	Keypad Unlocked
3864	R501	DO	Tag Reader Unlocked
3900	R400	CF	The area has been armed with faults
3910	R910	DH	Keypad Connected
3911	R911	DI	KBUS Relay Connected
3912	R912	DF	KBUS GP/K Connected
3913	R913	DG	KBUS MN/K Connected
3914	R381	XC	Wireless Detector Connected
3915	R384	XR	Normal Wireless Detector Battery
3916	R381	XC	Expander Connected
3917	R381	XC	Wireless Repeater Connected
3918	R918	DL	Radar Transmitter Restored
3919	R384	XR	Normal Wireless Siren Battery
3920	R920	NR	Cellular Data Network Connected
3921	R921	NR	SIM Card Restored
3922	R922	NR	Wi-Fi Connected
3923	R344	XH	Normal RF Signal

HikCode	CIDCode	SIACode	Description
3925	R384	XR	Low Keyfob Battery Restored
3930	R930	NR	Normal IP address
3931	R931	NR	Normal Wired Network
3940	R131	BH	Motion Detection Alarm Stopped
3941	R941	DM	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	DS	Network Camera Connected
3962	R962	DQ	Fire Alarm Consulting Over
3963	R963	DU	Duress Alarm Consulting Over
3964	R964	DV	Emergency Medical Alarm Consulting Over
3965	R965	DW	Patrol
3973	R973	DX	Single-Zone Arming
3975	R306	DY	Detector Added
3976	R976	DZ	Business Consulting Over
3977	R306	EA	Expander Added
3978	R306	EB	Wireless Repeater Added
3979	R306	EC	Wireless Siren Added

HikCode	CIDCode	SIACode	Description
3980	R306	ED	Wireless Device Added
3984	R984	RS	The firmware has updated
3985	R985	UA	New user has been added
3987	R383	TU	Notifications about the state of the lid are enabled
3988	R570	QU	The device is active again

8.4.2 Event Codes for Encoding Devices

HikCode	CIDCode	SIACode	Description
IO	E900	VA	IO Alarm
VMD	E901	VB	Motion Detection Alarm
diskerror	E902	VC	Disk Error Alarm
diskfull	E903	VD	Disk Full Alarm
diskrecover	E904	VE	Disk Restored Alarm
fielddetection	E905	VF	Intrusion Detection Alarm
linedetection	E906	VG	Line Crossing Detection Alarm
rapidMove	E907	VH	Fast Moving Alarm
recordException	E908	VI	Recording Exception Alarm
regionEntrance	E909	VJ	Region Entrance Detection Alarm
regionExiting	E910	VK	Region Exiting Detection Alarm

HikCode	CIDCode	SIACode	Description
shelteralarm	E911	VL	Video Tampering Alarm
videoloss	E912	VM	Video Loss Alarm
fireDetection	E913	VN	Fire Detection Alarm
TMPA	E914	VO	Temperature Measurement Precautionary Alarm
TMA	E915	VP	Temperature Measurement Alarm
TDA	E916	VQ	Temperature Diff Alarm

8.4.3 Event Codes for Access Control Devices

HikCode	CIDCode	SIACode	Description
requestVoiceTalkEvent	E800	DA	Request Voice Talk Interactive Event
cancelVoiceTalkEvent	R800	NA	Cancel Voice Talk Interactive Event

8.4.4 Event Codes for Radars

HikCode	CIDCode	SIACode	Description
fallingDown	E700	RA	Person Fall Alarm
longTimeLeave	E701	RB	Prolonged Bed Exit Alarm
heartBeatAbnormal	E702	RC	Irregular Heartbeat Alarm
respireAbnormal	E703	RD	Abnormal Respiratory Rate Alarm

8.4.5 Event Codes for Status

HikCode	CIDCode	SIACode	Description
deviceKeyAbnormal	E500	KA	Device Key Exception
deviceKeyNormal	R500	KR	Device Key Exception Restored
devicedeleted	E349	OD	Device Deleted From HPP Alarm
deviceoffline	E350	OF	Device Offline Alarm
deviceonline	R350	ON	Device Online Alarm
hppConnectAbnormal	E600	HA	Communication Exception Between IPRP and HPP
hppConnectNormal	R600	RA	Communication Restored Between IPRP and HPP
deviceHppAbnormal	E400	DA	Device Network Exception on Hik-Partner Pro
deviceHppNormal	R400	DN	Device Network Exception Restored on Hik-Partner Pro

Chapter 9 Basic Configuration

- ***Manage Operator***
- ***Manage Access***
- ***Export Log***
- ***Configure Network***
- ***Configure Storage***

9.1 Manage Operator

There are three user types: Super Admin (ARC Account), Administrator and Operator. A Super Admin can reset the Administrator password and manage operators. An Administrator user can change their password (using the old password), add operators and manage all added operators. Operators verify alarm videos from their managed devices.

Select **Configuration → System → User → Add** .

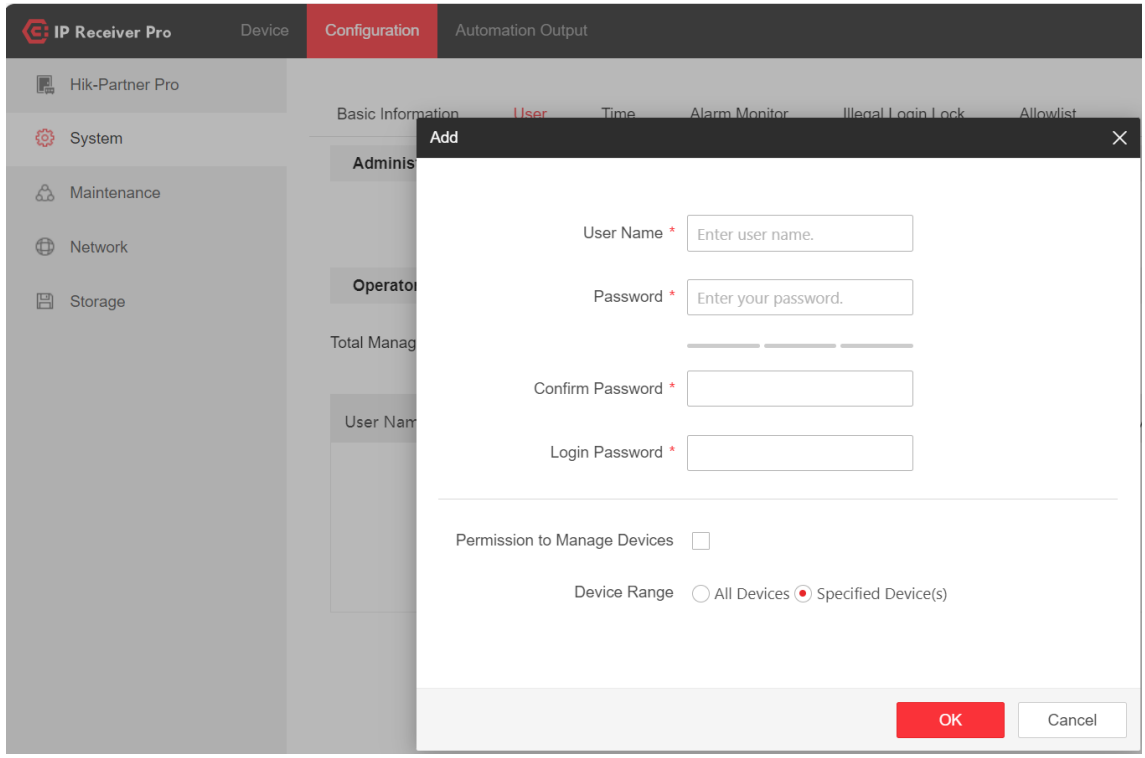


Figure 9-1 Operator Management

9.2 Manage Access

Configure Illegal Login Lock

Specify the maximum failed sign-in attempts that trigger an account lock.
Select **Configuration → System → Illegal Login Lock** .

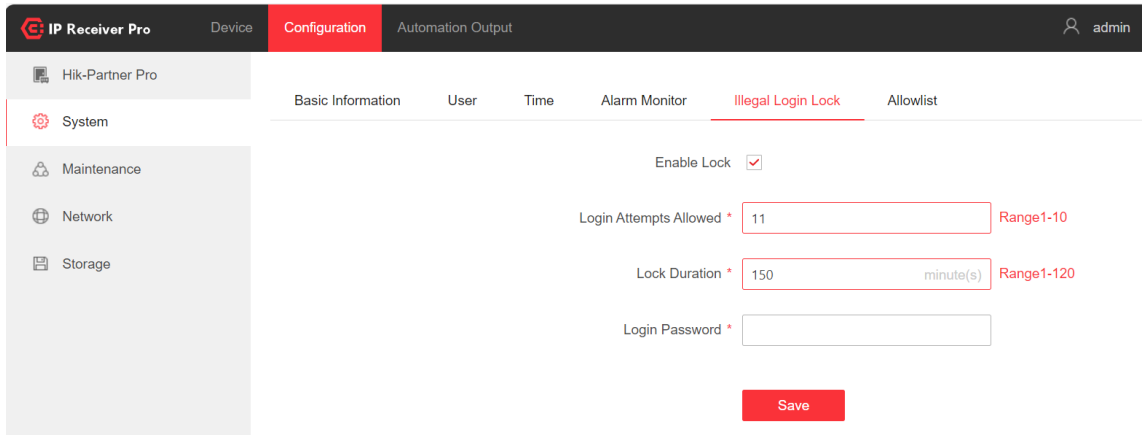


Figure 9-2 Login Lock

Configure Allowlist

As a Super Admin or Admin, you can add IP addresses to the allowlist in the IPRP. This allows those IP addresses to access the IPRP, including the event monitoring URLs and video URLs in the DC-09 protocol.
Select **Configuration → System → Allowlist → Add** .

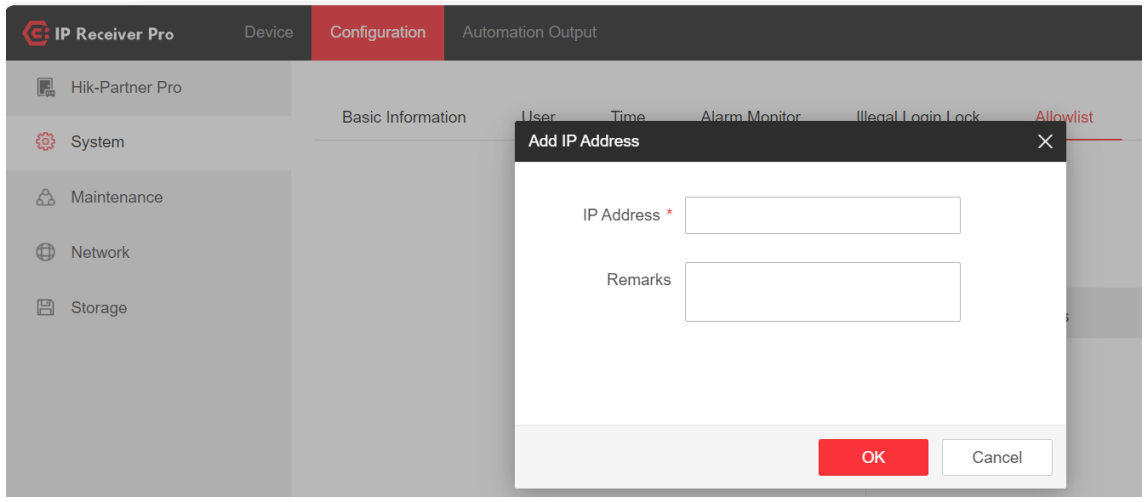


Figure 9-3 Allowlist

9.3 Export Log

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

Select **Configuration → System → Maintenance** .

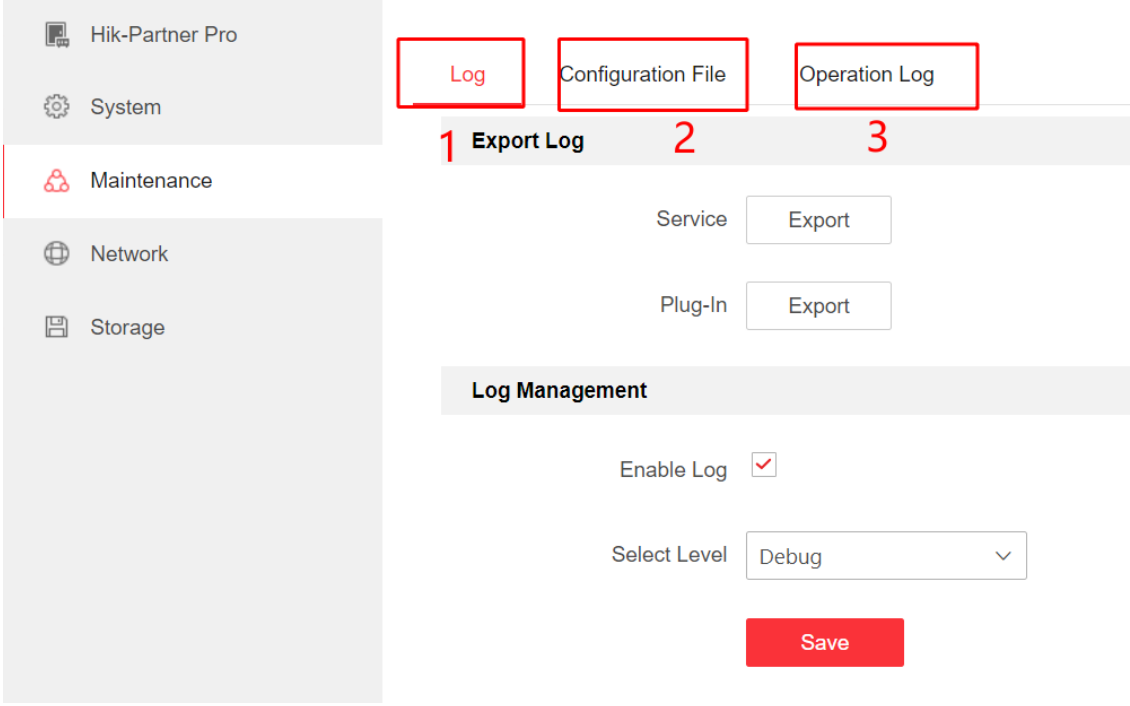


Figure 9-4 Export Log

No.	Parameter	Description
1	System Log	Export the log for debugging. If you select the log level to Debug, logs with a higher log level will also be exported.
2	Configuration File	Export and import the configuration file to another PC for quick configuration of IPRP on another PC. Only the file exported from a lower version of IPRP can be imported to a higher version. The IPRP will

No.	Parameter	Description
		restart after a configuration file is imported.
3	Operation Log	• View and export logs of various operations such as adding devices and configuring zones. • Administrators can also view the operation logs of the Hik Video Plugin. • To record the operation logs of Hik Video Plugin for Manitou, select **Platform Configuration → Log Server** to set the IPRP information first.

9.4 Configure Network

Select **Configuration → System → Network** .

Port

- If the IPRP port is occupied, go to **Configuration → Network → Port → Platform Port** to edit the HTTP port. Restart the IPRP after editing the port, or the settings will not take effect. You need to add corresponding firewall rules after editing ports for the IPRP, or the IPRP might not start.
- For port details, refer to the Communication Matrix document.

Port Mapping

Port mapping allows external traffic from the internet to access the IPRP service and the added devices on a private network. Set up the external port and address on your router first.
Ensure that all settings in **Device Port Mapping** are consistent with those in Dual-Connection.

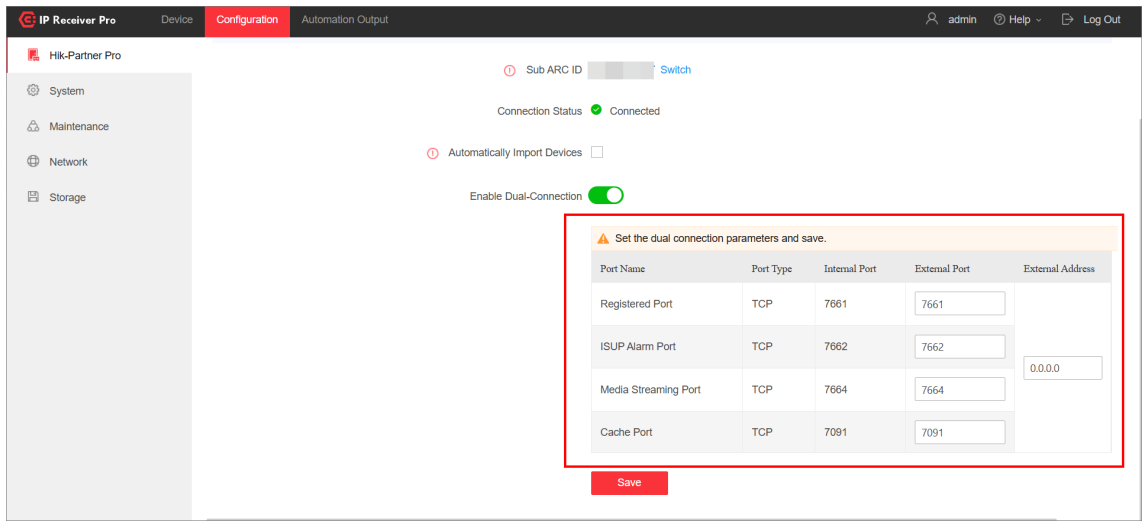


Figure 9-5 Port Mapping for Dual-Connection

HTTPS

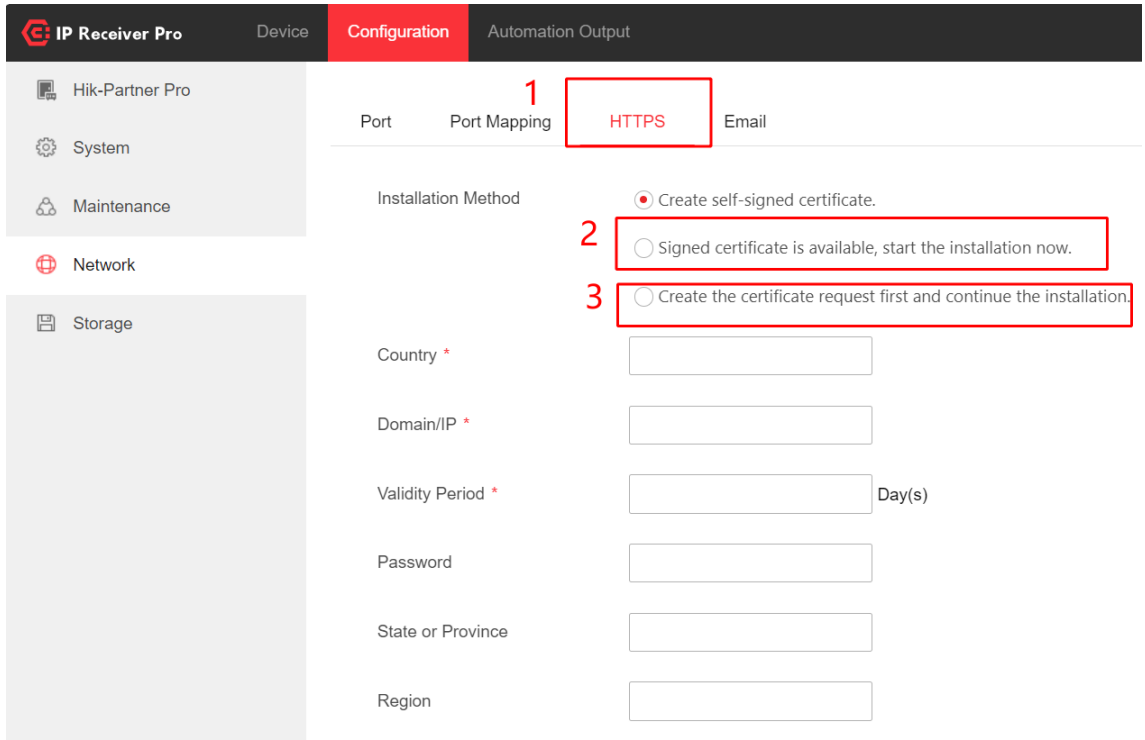
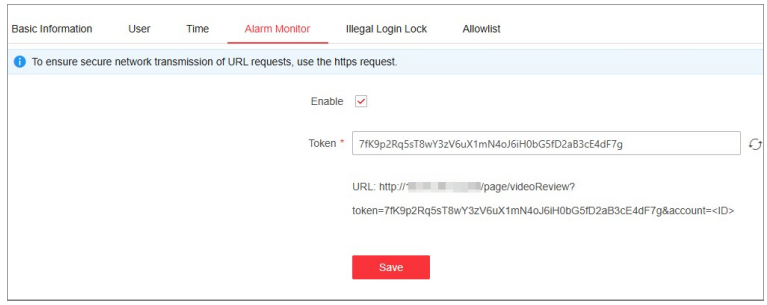


Figure 9-6 HTTPS Configuration

No.	Operation	Description
1	Set HTTPS	HTTPS provides authentication of a web site which protects against attacks. If you set HTTPS, the URL for event verification (go to **Configuration → System → Alarm Monitor**) will start with **https**. For more information, see .  **Figure 9-7 Alarm Monitor**
2	Import Signed Certificate	To disable the notification of the web page is not safe, import a signed certificate to the IPRP.
3	Create Certificate Request	1. Select **Create** to create the certificate request. Enter the required information. 2. Download the certificate request and submit it to the trusted certificate authority for signature. 3. After receiving the signed valid certificate, select **Browse** to select the downloaded certificate saved in the PC, and then select **Install**.

Email

You can set the sender and receiver information so that specified receivers can receive reported alarms.

9.5 Configure Storage

Select **Configuration → Storage** .

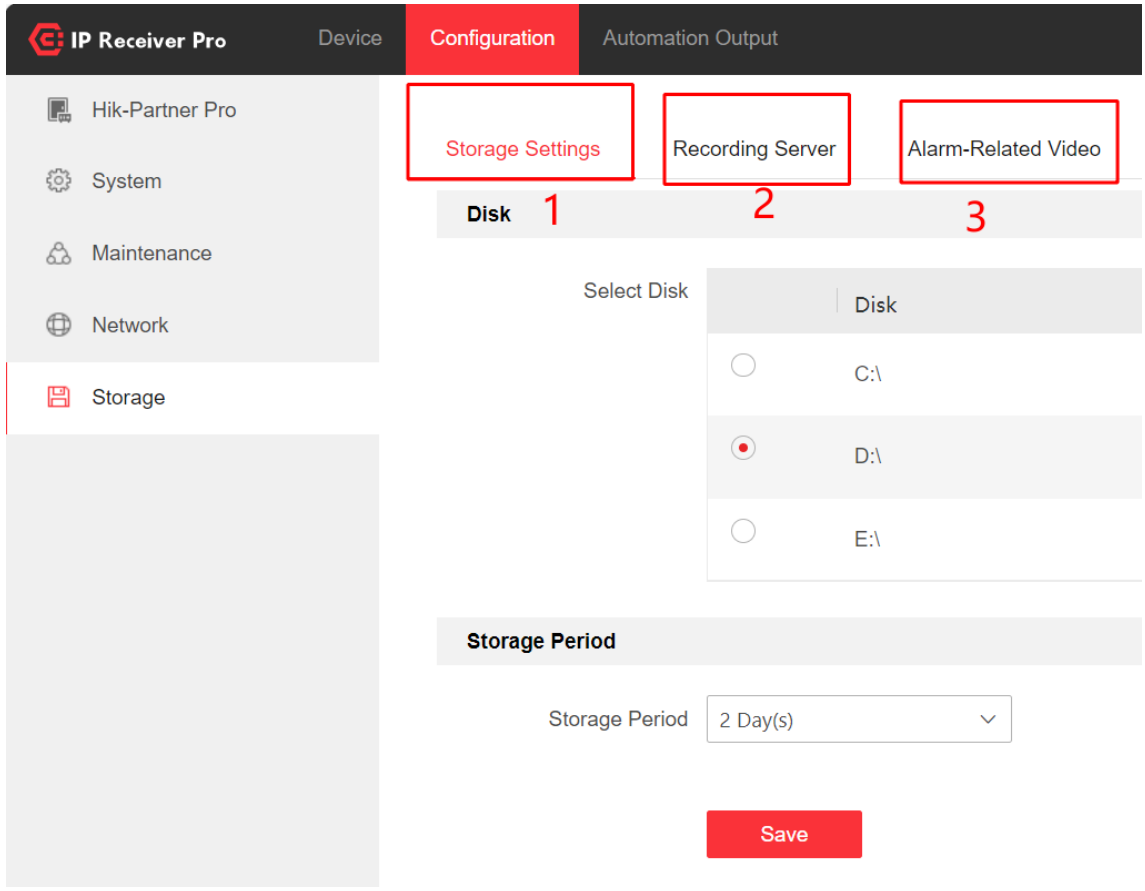


Figure 9-8 Configure Storage

No.	Parameter	Description
1	Storage Disk	The videos will be stored in the selected disk (50 GB or more is recommended) of your PC for a certain period. If you delete videos stored in a disk, you cannot see any videos when clicking on in the Event Monitor page.
2	Recording Server	After connecting the IPRP to the Recording Server, you can store alarm-related videos in the Recording Server by the Hik VideoPlugin.
3	Alarm Video	For example, if you set **Before Alarm** to 10s, the IPRP will download alarm-related videos 10 seconds before an alarm is triggered.

Appendix A. Legal Information

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

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

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

See Far, Go Further