



IPRP Video Plugin

Quick Start Guide

Contents

Chapter 1 Overview 1

 1.1 Introduction 1

 1.2 Running Environment 1

Chapter 2 Step 1: Install IPRP Video Plugin 2

Chapter 3 Step 2: Launch Plugin 3

Chapter 4 Step 3: Use Plugin 8

Appendix A. Legal Information 17

Chapter 1 Overview

1.1 Introduction

IPRP VideoPlugin is a plugin which could be integrated with an ARC for alarm-related video verification **without Development**.

With the IPRP VideoPlugin, you can view real-time and history videos of alarms and events triggered by encoding device, security control device, and third-party device for verification. You can also back up the videos to a Server for second video verification.

This manual guides you to use the IPRP VideoPlugin. To ensure a proper usage and stability of the IPRP VideoPlugin, refer to the contents below and read the manual carefully before installation and operation.

1.2 Running Environment

The following is the recommended system requirement for running the plugin.

Operating System: Microsoft Windows 10/8/7, Windows Server 2019

Chapter 2 Step 1: Install IPRP Video Plugin

Before using the IPRP Video Plugin, you should properly install the IPRP Video Plugin to ensure its proper usage and stability.

Before You Start

Make sure the IPRP Video Plugin is compatible with the running environment. See **Running Environment** for details about required running environment.

Steps

1. Double-click the IPRP Video Plugin program file to enter the welcome panel of the InstallShield Wizard.
2. Click **Next** to continue.
3. Click **Browse...** and select a directory as required to install the IPRP Video Plugin, or click **Install** to use the default installation path and start the installation.

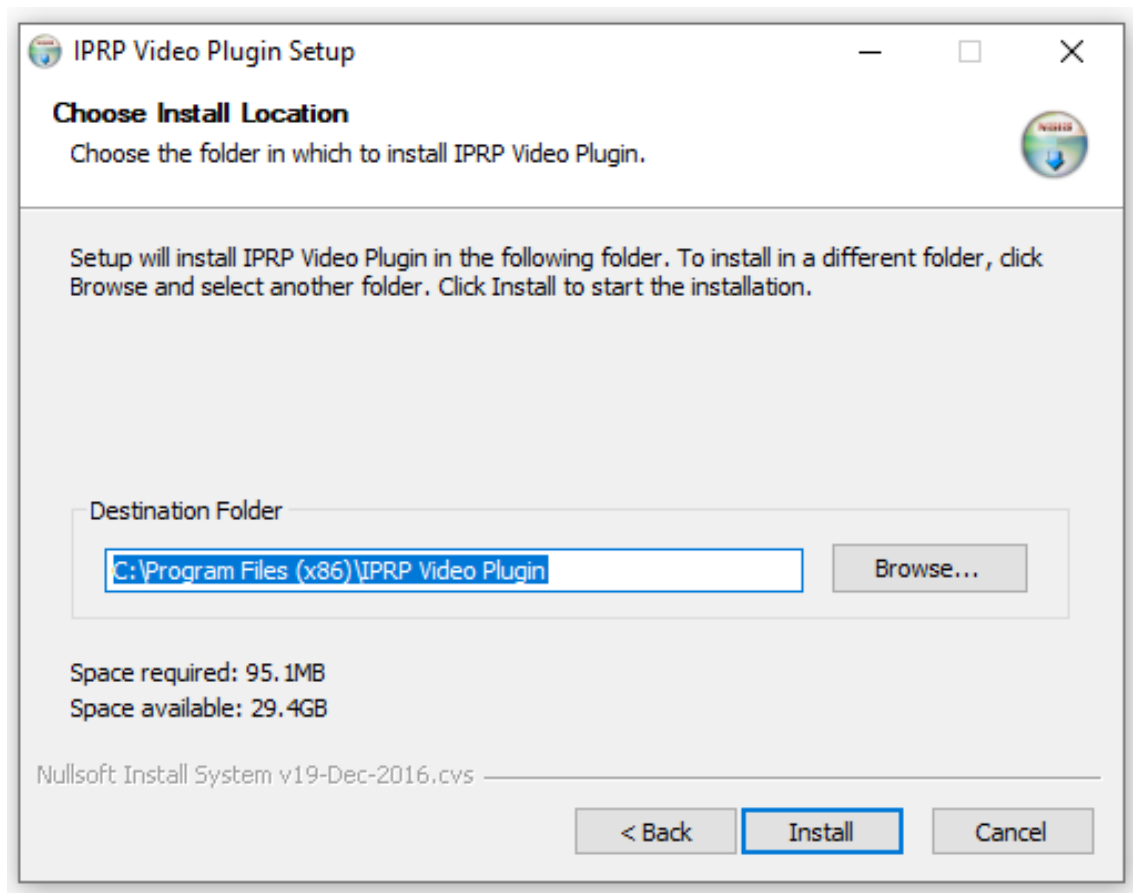


Figure 2-1 Select Directory

4. Click **Finish** to complete the installation.

Chapter 3 Step 2: Launch Plugin

Before verifying alarms, launch the IPRP Video Plugin in one of the following ways as an administrator.

Start Command Prompt

Start Command Prompt, switch to the plugin directory, and enter the alarm-related information sent by IP Receiver Pro. The following table displays the command lines for different types of devices.

Table 3-1 Command Lines for Encoding Devices Added Directly

Command Line	Description
VideoPlugin.exe VideoPlugin.exe"IP:xx;Port:xx;UserName:xx;Password:xx;ChannelNo.:xx;StreamKey:xx;Time:xx;displaychannelpane:1;isDevice:1;" Example: VideoPlugin.exe "IP:172.7.203.222;Port:83;UserName:admin;Password:sdk123456;ChannelNo.:1;StreamKey:123456;Time:2024-04-27T00:00:00+08:00;displaychannelpane:1;isDevice:1;"	IP; Port; UserName; Password The IP address, port number, user name, and password of the device. ChannelNo. The channel number. Up to 4 channels are supported and they are separated with comma. For example, ChannelNo.:1,2,3,4. StreamKey The stream encryption key. It is only required when the device enables stream encryption. Time The start time of video verification. For example, 2024-04-27T00:00:00+08:00. displaychannelpane Whether to display the camera list. 1 means yes; 0 means no. isDevice Whether to enable video verification for devices added via ISAPI. 1 means yes; 0 means no.

Table 3-2 Command Lines for Devices Added on IP Receiver Pro

Device Type	Command Line	Description
Encoding Devices	<ul style="list-style-type: none"> • VideoPlugin.exe <i>"IP:xx;Port:xx;UserName:xx;Password:xx;AccountID:xx;ZoneNo.:xx;AlarmTime:xx;AlarmInfo:xx;PCAlarmTimerTag:xx;"</i> Example: VideoPlugin.exe "IP:172.7.203.222;Port:83;UserName:admin;Password:sdk123456;AccountID:E58616805;ZoneNo.:1;AlarmInfo:Intrusion;AlarmTime:2024-04-27T00:00:00;PCAlarmTimerTag:1;" • For alarms forwarded via ADM-CID of DC-09 protocol: <ul style="list-style-type: none"> ◦ VideoPlugin.exe <i>"IP:xx;Port:xx;UserName:xx;Password:xx;Alarm:xxx;PCAlarmTimeTag:xxx;"</i> ◦ VideoPlugin.exe <i>"Alarm:xxx;PCAlarmTimeTag:xxx;"</i> Example: VideoPlugin.exe "IP:172.7.203.222;Port:83;UserName:admin;Password:sdk123456;Alarm:D1AA003B"ADM-CID"0006L0#C50405778[#C50405778 1628 00 001]_02:37:41,03-24-2022;PCAlarmTimeTag:0;"	<p>IP; Port; UserName; Password (Optional)</p> <p>The IP Receiver Pro information: IP address, user name, password, and port number.</p> <p> Note</p> <p>If you do not enter the IP Receiver Pro information in the command line, you need to enter the information in the pop-up configuration window after the plugin is launched.</p> <p>Alarm (Required)</p> <p>Alarm messages forwarded by IP Receiver Pro via the DC-09 protocol.</p> <p>Zone Information (Required)</p> <p>Account ID and zone No.</p> <p>Alarm Information</p> <p>Alarm Information: the alarm time (required; For example, 2024-04-27T00:00:00) and alarm information (optional).</p> <p>PCAlarmTimeTag (Optional)</p> <p>If the alarm time is not included in alarm information and there is a time difference between the device and your PC:</p> <ul style="list-style-type: none"> • Enter "1" and the alarm time will be automatically

Device Type	Command Line	Description
		<p>calibrated according to the time difference.</p> <ul style="list-style-type: none"> Enter "0" and the alarm time will be displayed as the local PC time. If you delete the parameter PCAlarmTimeTag, the result will be the same as entering "0".
Video Intercoms	<p>VideoPlugin.exe "IP:xx;Port:xx;UserName:xx;Password:xx;AccountID:xx;ChannelNo.:xx;isTalk:xx;AutoTalkTag:xx;" Example: VideoPlugin.exe "IP:172.7.203.222;Port:83;UserName:admin;Password:sdk123456;AccountID:E58616805;ChannelNo.:1;isTalk:1;AutoTalkTag:0"</p>	<p>IP; Port; UserName; Password (Optional) The IP Receiver Pro Information: IP address, user name, password, and port number.</p> <p>Device Information Account ID and channel No.</p> <p>isTalk Whether to enable intercom verification. 0 means no, and 1 means yes.</p> <p>AutoTalkTag Whether to automatically answer the call. 0 means no, and 1 means yes.</p>
Security Control Panels	<p>"IP:xx;Port:xx;UserName:xx;Password:xx;AccountID:xx;AlarmTime:xx;enableAlarmDevicePlugin:xx;" Example: VideoPlugin.exe "IP:10.67.59.19;Port:81;UserName:admin;Password:Sdk2016+;AccountID:Q02252692;AlarmTime:</p>	<p>IP; Port; UserName; Password (Optional) The IP Receiver Pro Information: IP address, user name, password, and port number.</p> <p>Device Information Account ID and channel No.</p> <p>AlarmTime (Optional)</p>

Device Type	Command Line	Description
	<i>2024-04-27T15:55:45+08:00;enableAlarmDevicePlugin:1;"</i>	<p>The alarm trigger time. For example, 2024-04-27T00:00:00+08:00</p> <p>enableAlarmDevicePlugin</p> <p>Whether to launch the security control panel plugin. 0 means no, and 1 means yes.</p>
IP Speakers	<p><i>VideoPlugin.exe "IP:xx;Port:xx;UserName:xx;Password:xx;AccountID:xx;enableSpeakerPlugin:xx;"</i></p> <p>Example: <i>VideoPlugin.exe "IP:172.7.203.222;Port:83;UserName:admin;Password:sdk123456;AccountID:E58616805;enableSpeakerPlugin:1;"</i></p>	<p>IP; Port; UserName; Password (Optional)</p> <p>The IP Receiver Pro Information: IP address, user name, password, and port number.</p> <p>Device Information</p> <p>Account ID.</p> <p>enableSpeakerPlugin</p> <p>Whether to launch the IP speaker plugin. 0 means no, and 1 means yes.</p>

```


Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>VideoPlugin.exe "IP:172.7.203.222;Port:83;UserName:admin;Password:sdk123456;Alarm:D1AA003B"ADM-CID"0006L0#C50405778[#C50405778|1628 00 001]_02:37:41,03-24-2022;PCAlarmTimeTag:0;"

C:\Windows\system32>_
  
```

Figure 3-1 Command Line for Encoding Devices (Alarms Forwarded via ADM-CID of DC-09 Protocol)

Basic Configuration

If you don't enter the IPRP information in the command line or want to edit IPRP information, select  → **Platform Configuration** in the upper right corner of the plugin page, edit the information, and then restart the plugin.

IPRP Video Plugin Quick Start Guide

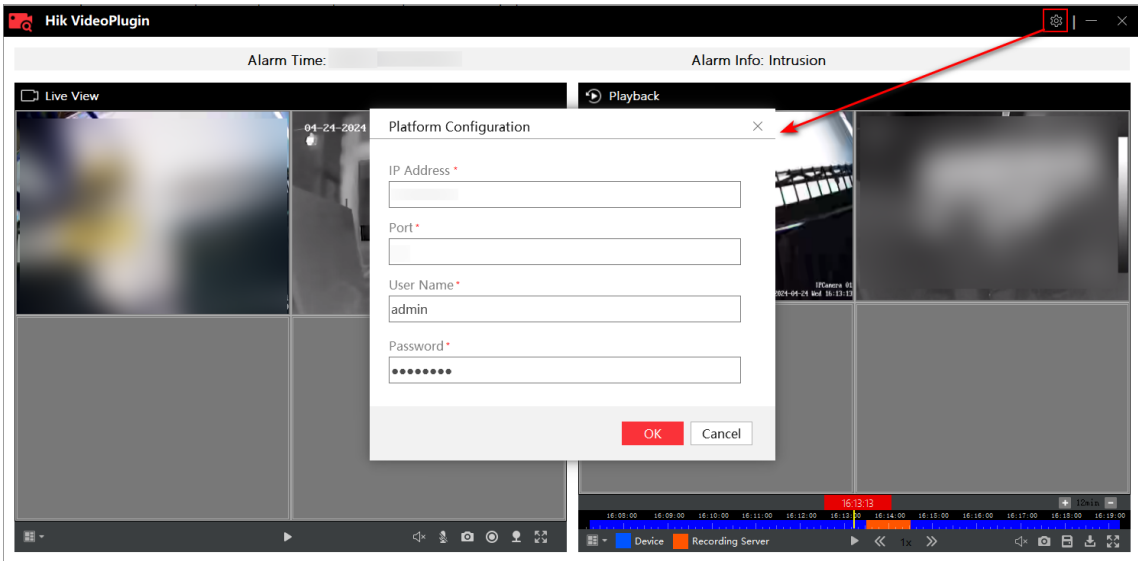



Figure 3-2 Platform Configuration

Captured pictures and recorded videos are saved in the Disk C by default. To change the storage location, select  → **Local Configuration** and select a location.

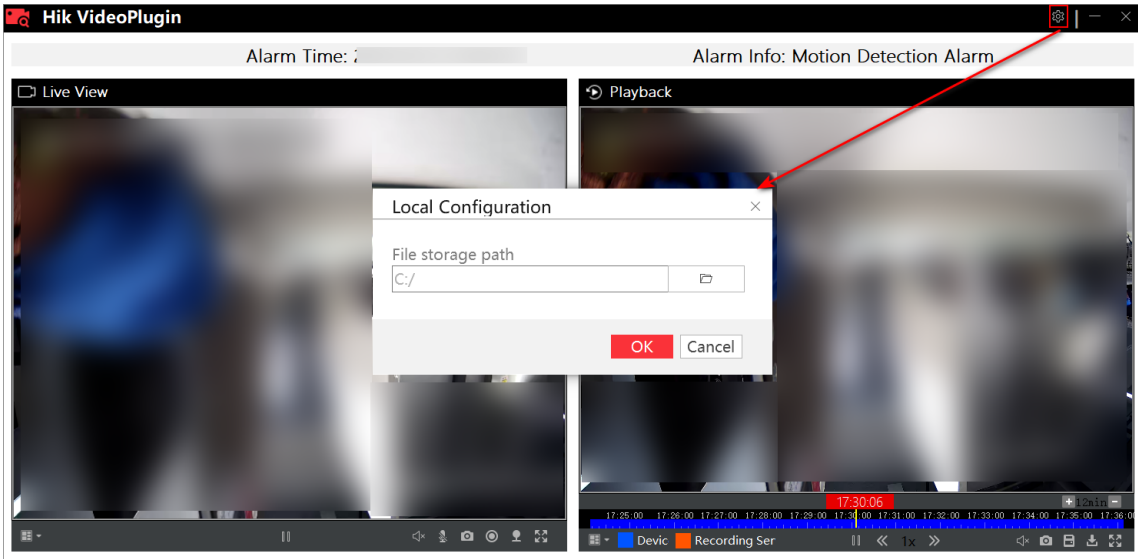


Figure 3-3 Storage Configuration

Chapter 4 Step 3: Use Plugin

You can use the Video Plugin to view real-time and history videos of alarms and events triggered by encoding devices, start intercom verification and remotely open doors for access control devices. You can also use the Security Panel Plugin to start a two-way audio and control security control panels.

Video Plugin

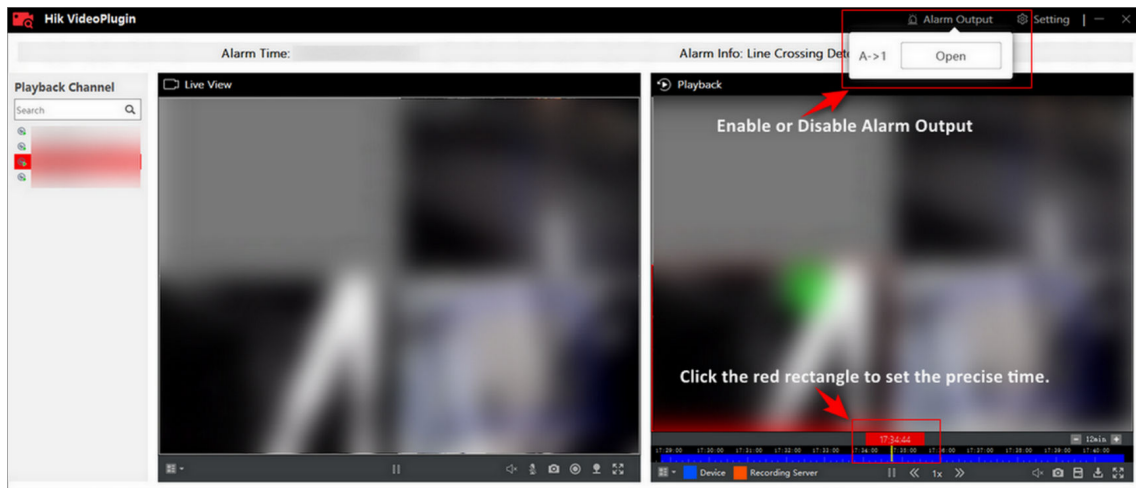


Figure 4-1 Video Verification Page

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.

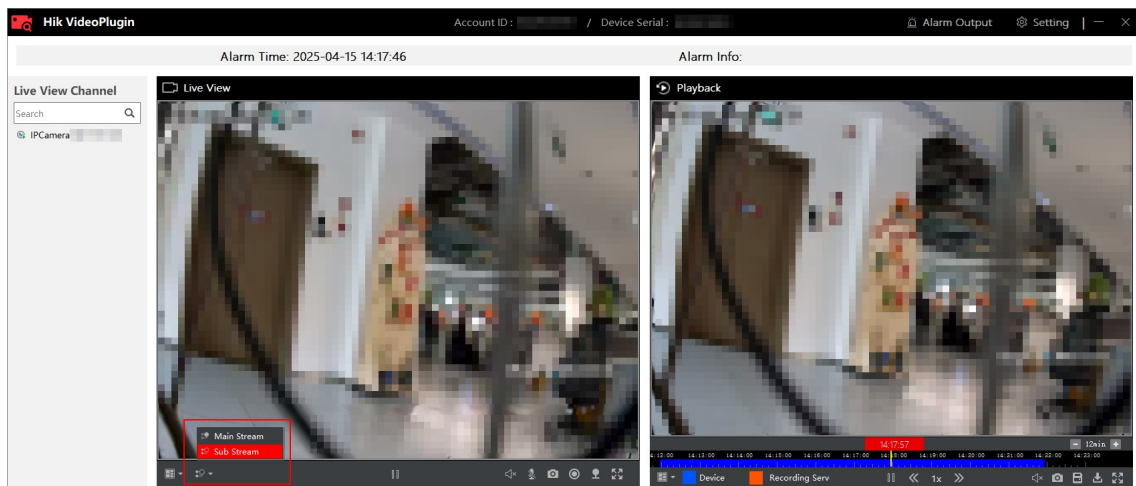


Figure 4-2 Video Verification via Plug-in

Video Intercom Plugin

You can start audio or video intercom verification according to device capabilities.

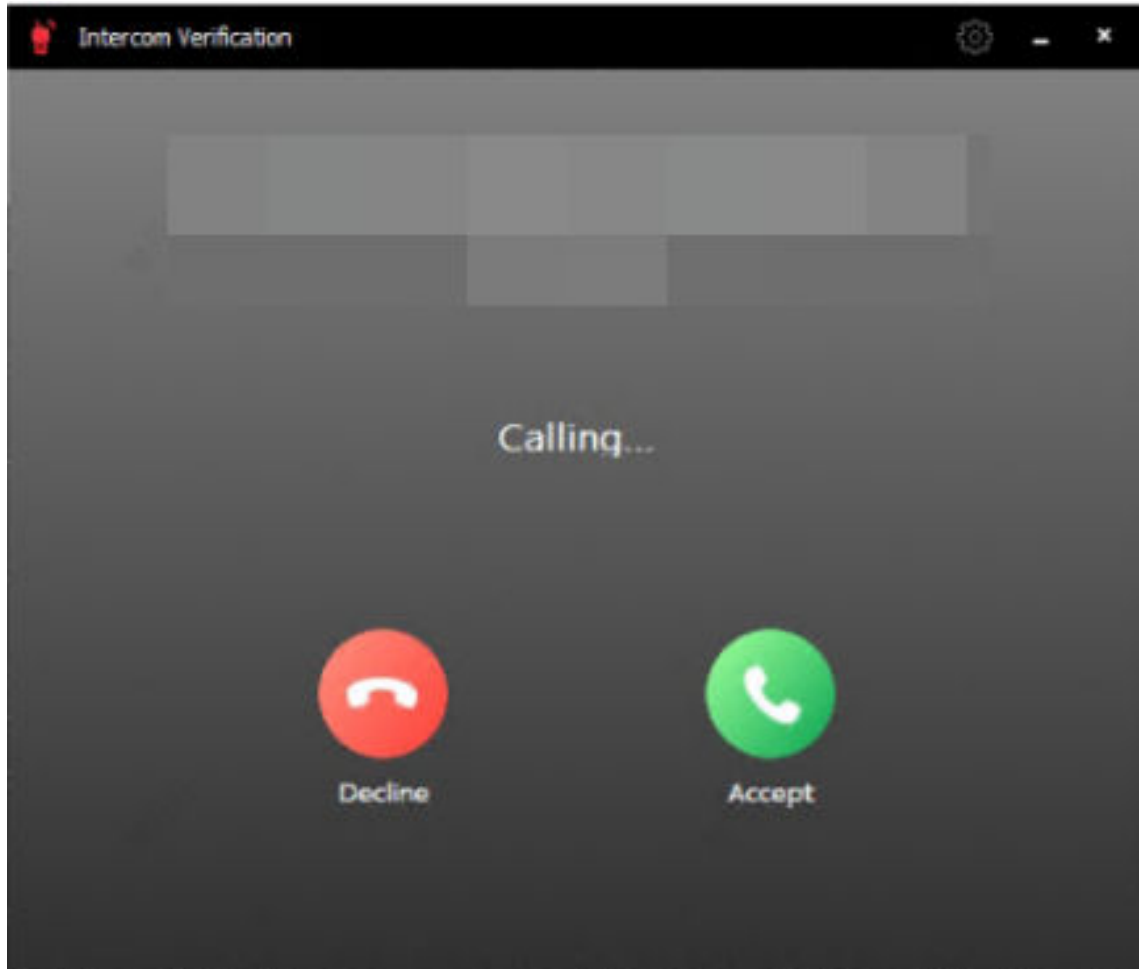


Figure 4-3 Intercom Verification

You can select **Open Door** to open the door remotely.

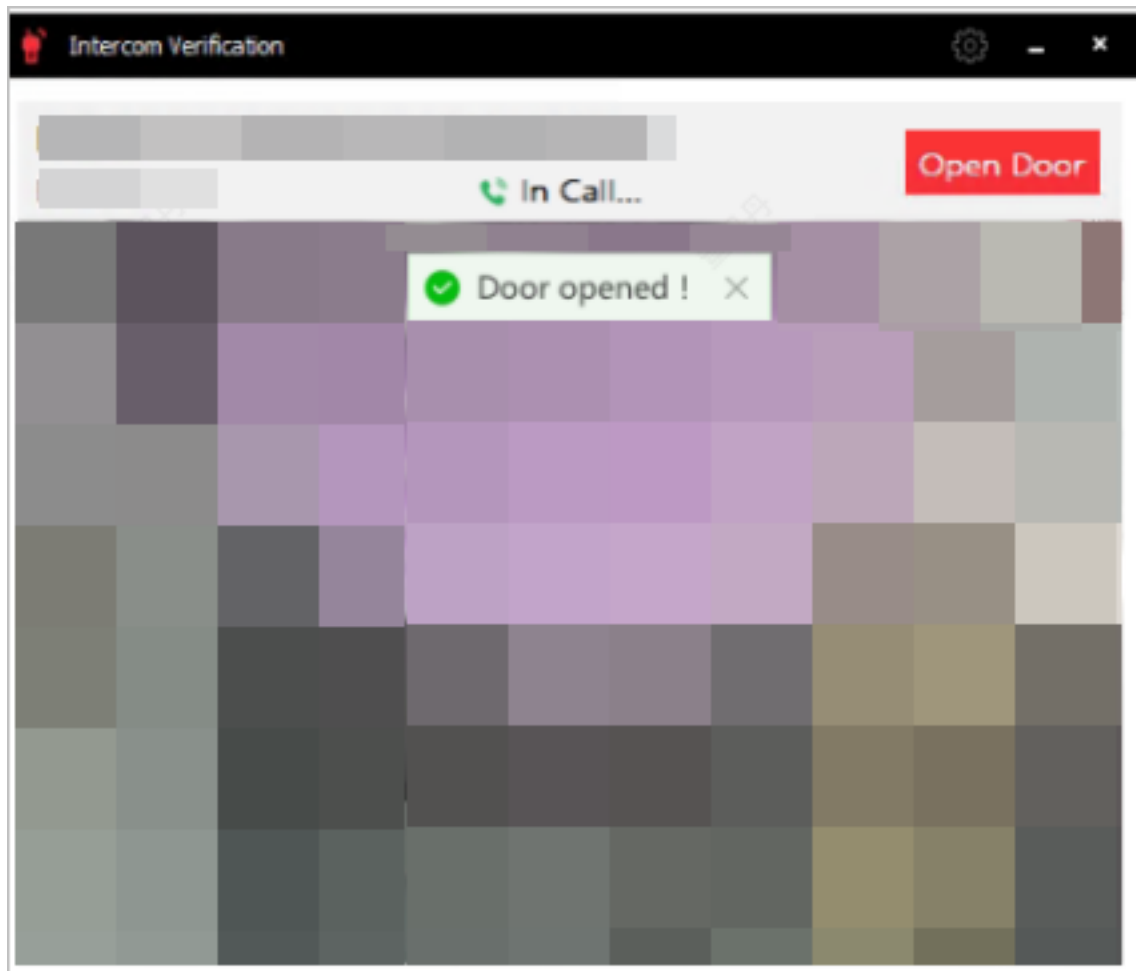


Figure 4-4 Open Door

Security Control Panel Plugin

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

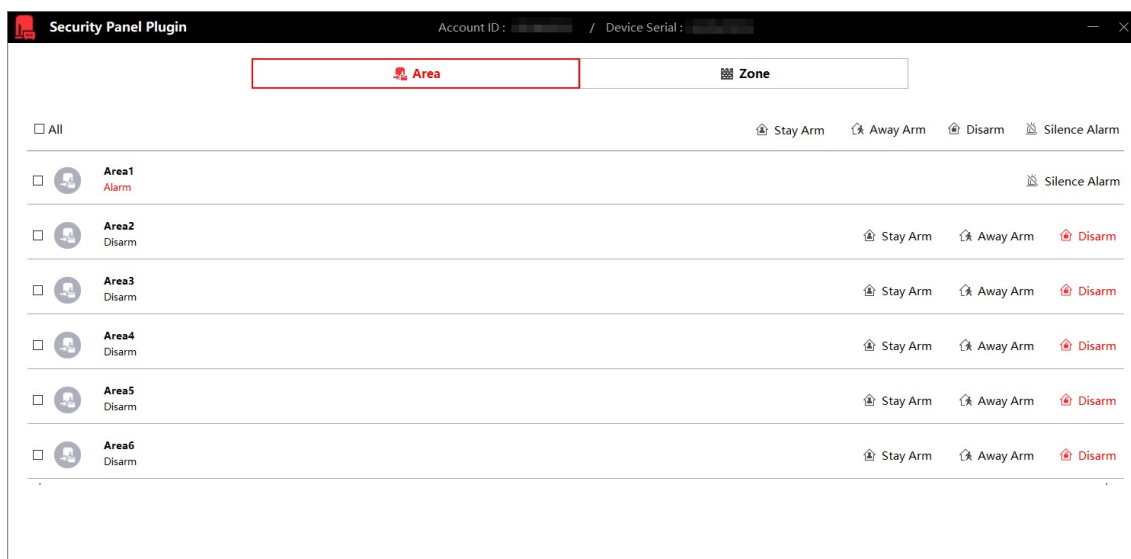


Figure 4-5 Area Settings

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.

After enabling **Fault Checklist when Arming** on the device added via OTAP (go to **Configuration → System → Service**), the arming process will perform subsystem 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.

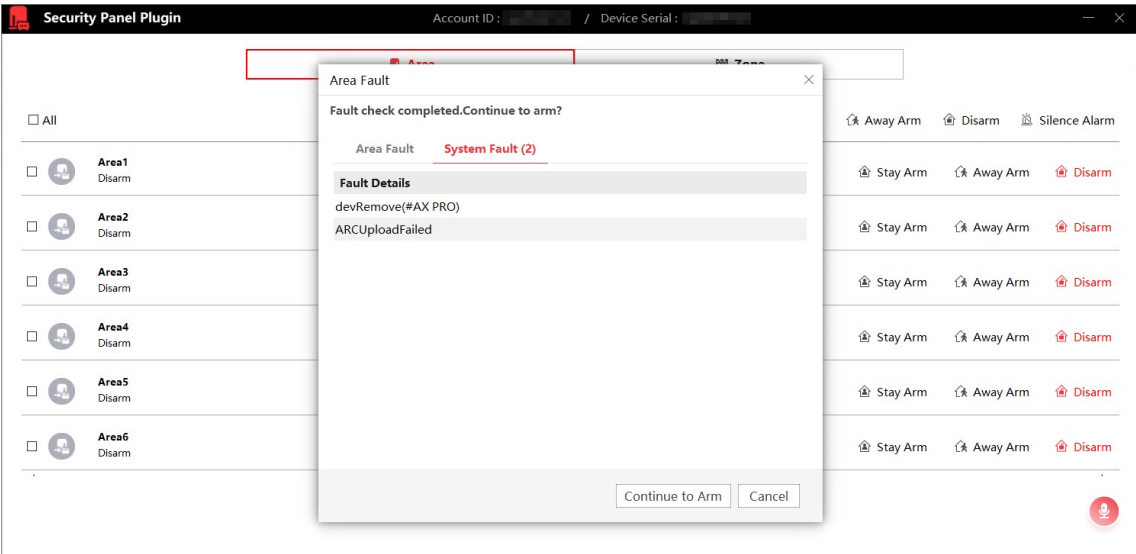


Figure 4-6 Fault Check

Select **Zone**, and you can view the zone information and perform the following operations. For security control panels added via ISUP, you can enable **Zone Bypass** to ignore alarms from zones.

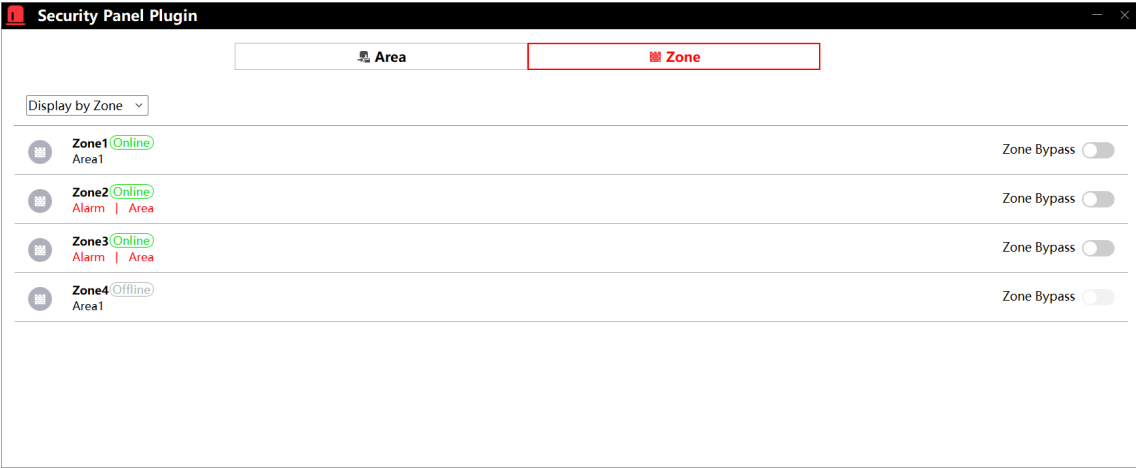


Figure 4-7 Zone Bypass

For security control panels added via OTAP, you can deactivate alarms from zones.

IPRP Video Plugin Quick Start Guide

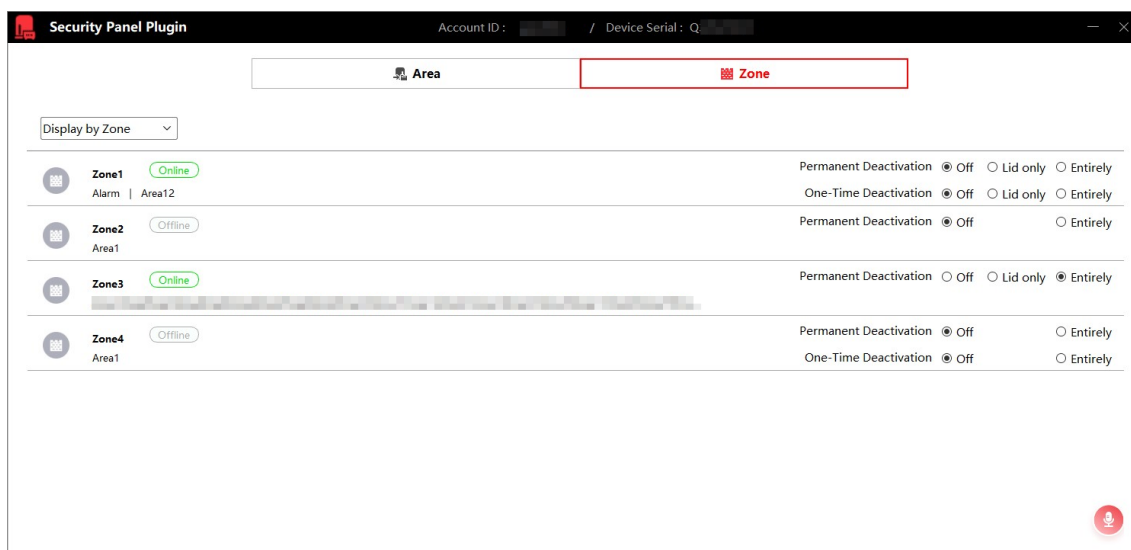


Figure 4-8 Zone Settings

Table 4-1 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. 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.

(Optional) Perform two-way audio with a sounder linked with a security control panel. 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.

Note

- The two-way audio function is only available when a security control has a sounder or the two-way audio does not time out before launching the plugin. For details, see the following pictures.

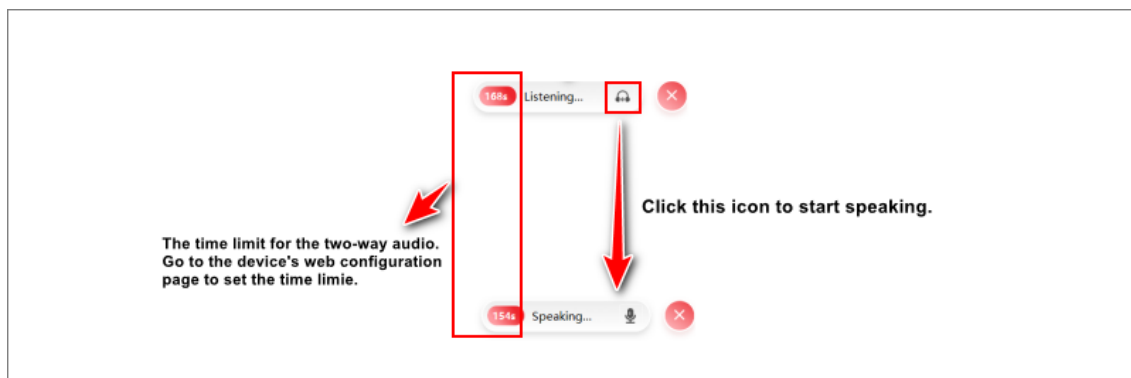


Figure 4-9 Two-Way Audio with Half-Duplex Sounder



Figure 4-10 Listening with Half-Duplex Sounder

IPRP Video Plugin Quick Start Guide

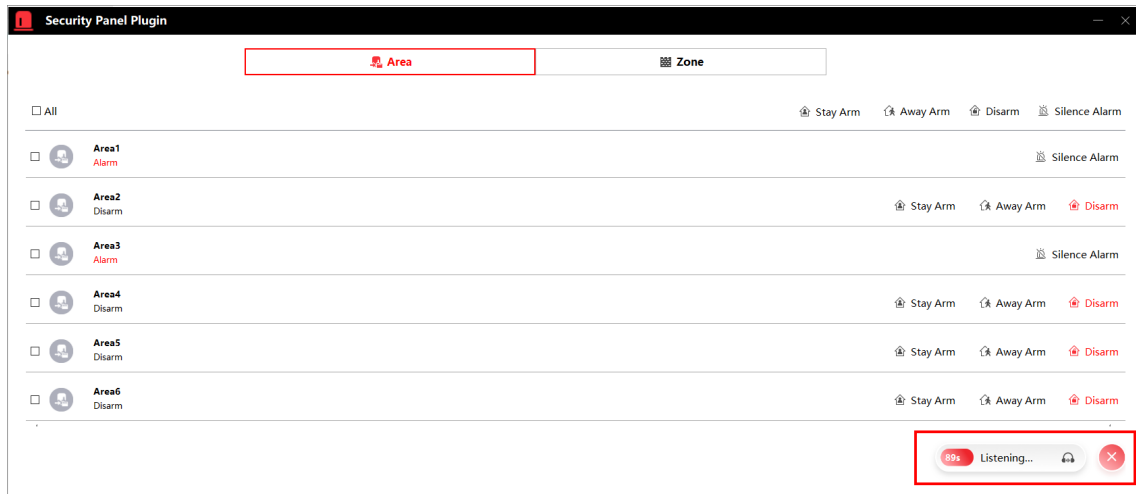


Figure 4-11 Speaking with Half-Duplex Sounder

- You can perform two-way audio with a full-duplex sounder of an AX PRO device (V1.3 and later).

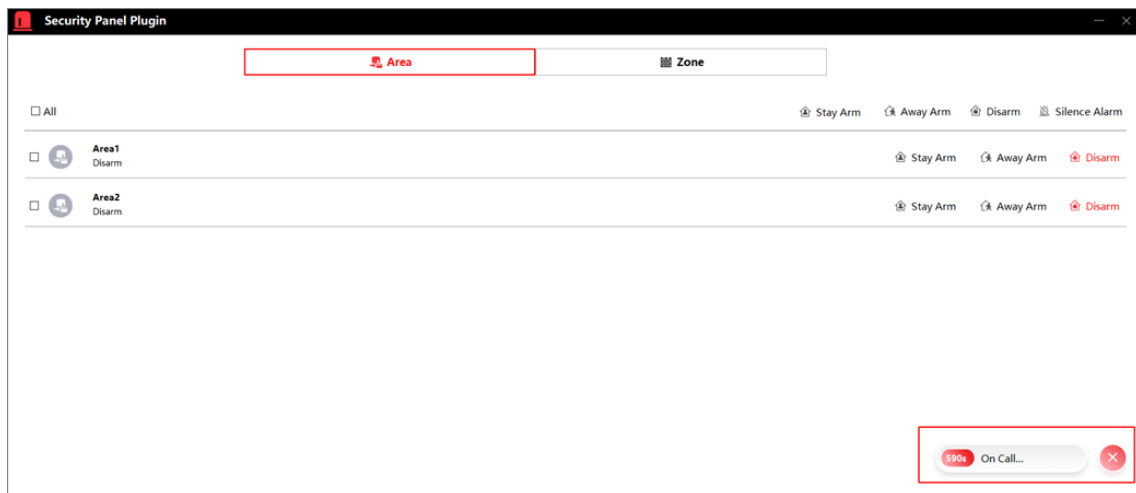


Figure 4-12 Two-Way Audio with Full-Duplex Sounder

IP Speaker Plugin

For IP speakers added via HPP, you can play audio files, control volume, and start speaking—applicable to either a single device or multiple devices sharing the same account ID.

To add audio file materials, go to **Configure → Broadcast Settings → Audio Library** on the device configuration page.

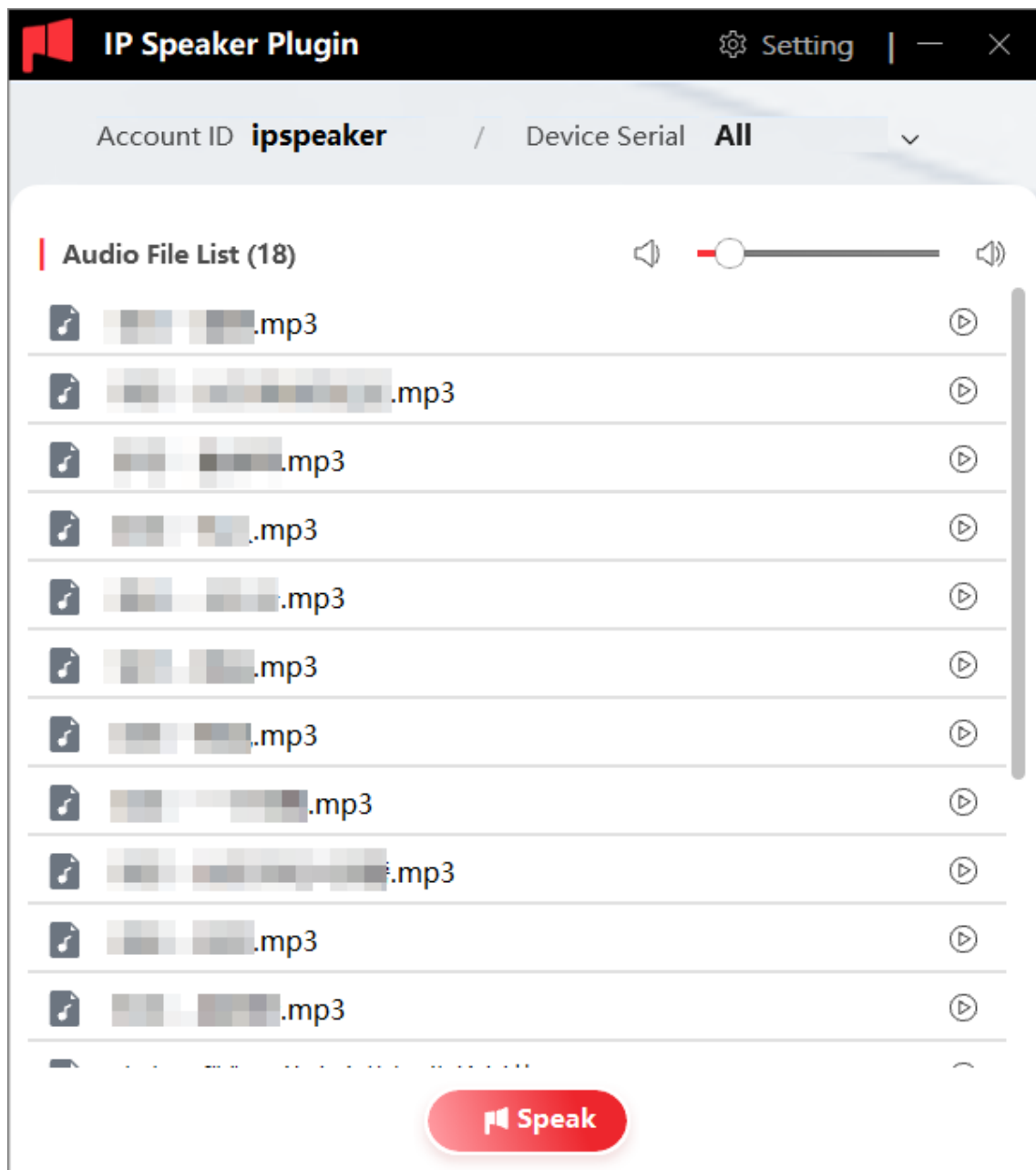


Figure 4-13 Control IP Speaker via Plug-in

Note

- 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.

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