



HiTools Delivery

User Manual

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.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



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.

Contents

Chapter 1 Before You Start	1
Chapter 2 Learn HiTools Delivery	3
2.1 Introduction	3
2.2 Software Interface Overview	3
2.3 Documentation Navigation	6
2.4 System Requirements	7
Chapter 3 What's New	8
3.1 V2.1.2.1	8
3.2 V2.1.1.2	10
3.3 V2.1.0.6	12
3.3.1 [New] Picture Validator & Optimizer	12
3.3.2 [New] Password Manager	13
3.3.3 [Updated] Device Search	16
3.3.4 [Updated] Camera Configuration	18
3.3.5 [New] Device Management	18
3.3.6 [Updated] Traffic Camera Configuration Validation	20
3.3.7 [Updated] Device Maintenance	20
3.4 V2.0.2.4	22
3.4.1 [New] Service & Security	22
3.4.2 [Updated] Local Upgrade	23
3.4.3 [Updated] Upgrade Package Lookup Tool	24
3.5 V2.0.1.4	25
3.5.1 Device Upgrade	25
3.5.2 Device Diagnostics	26
3.5.3 System Settings	27
3.5.4 Toolkit	29

3.6 V2.0.0.6	29
3.6.1 Brand New Homepage	29
3.6.2 Device Management	29
3.6.3 Guided Delivery	31
3.6.4 Device Configuration	34
3.6.5 Configuration Verification	34
3.6.6 Maintenance	37
3.6.7 Device Diagnostics	37
3.6.8 Security Hardening	38
3.6.9 System Settings	38
Chapter 4 Project Management	40
Chapter 5 Device Management	41
5.1 How to Add Devices	41
5.1.1 Add Devices on Same LAN	41
5.1.2 Manually Add Devices	41
5.1.3 Follow-Up	42
5.1.4 How-To Video	43
5.2 How to Search for Devices on Other Subnets	43
5.3 How to Activate Devices	44
5.4 How to Reset Passwords	45
5.5 How to Group Devices	49
5.6 How to Preview and Download Channel Snapshots	49
Chapter 6 Guided Delivery	52
6.1 Introduction	52
6.2 How to Create Template	52
6.3 Specifications	52
6.4 Supported Templates	52
6.5 How to Configure Video Intercom Template	53

6.5.1 Scenario	53
6.5.2 Overall Configuration Process	53
6.5.3 Steps	54
6.6 How to Configure Entrance & Exit Template	66
6.6.1 Scenario	66
6.6.2 Overall Configuration Process	66
6.6.3 Steps	67
6.6.4 How-To Video	73
6.7 How to Configure Camera Template	74
6.7.1 Scenario	74
6.7.2 Manual Configuration	74
6.7.3 Online Configuration	75
Chapter 7 Device Configuration	78
7.1 Prerequisites	78
7.2 Function Overview	78
7.3 Supported Devices	78
7.4 Common Configuration	78
7.4.1 Basic Configuration	78
7.4.2 Platform Access	80
7.4.3 Cloud Storage	81
7.4.4 HEOP	82
7.4.5 Maintenance & Security	84
7.4.6 Advanced Configuration	84
7.4.7 Configure More	85
7.5 Camera	87
7.5.1 Function Overview	87
7.5.2 Prerequisites	87
7.5.3 Configuration Items	88

7.5.4 General Configuration	89
7.5.5 Network	96
7.5.6 Picture Overlay	100
7.5.7 Platform Access	101
7.5.8 Storage	102
7.5.9 System	103
7.5.10 Event	104
7.5.11 VCA Resource	108
7.5.12 Maintenance & Security	116
7.6 Recording & Analysis	116
7.6.1 Add Cameras as Channels	116
7.6.2 HDD Management	117
7.6.3 Others	118
7.7 Intelligent Traffic	118
7.7.1 General Configuration	119
7.7.2 Platform Access	120
7.7.3 Application Mode	121
7.7.4 Capture Parameters	136
7.7.5 Captured Images	142
7.7.6 Video	143
7.7.7 System Service	143
7.8 Video Intercom	144
7.8.1 Prerequisites	144
7.8.2 Access Control	144
7.8.3 Audio	148
7.8.4 Event	149
7.8.5 Image	153
7.8.6 Basic Configuration	153

7.8.7 Platform Access	153
7.8.8 HEOP	153
7.8.9 Maintenance & Security	153
7.8.10 Advanced Configuration	154
7.9 Access Control	154
7.9.1 Prerequisites	154
7.9.2 Overall Configuration Process	154
7.9.3 Device Access	154
7.9.4 Access Control	156
7.9.5 Image	159
7.9.6 Basic Configuration	159
7.9.7 Platform Access	159
7.9.8 HEOP	159
7.9.9 Maintenance & Security	160
7.9.10 Advanced Configuration	160
7.10 Speed Gate & Turnstile	160
7.10.1 Entry	160
7.10.2 Prerequisites	160
7.10.3 Basic Parameters	160
7.10.4 Access Control	161
7.10.5 Maintenance & Security	163
7.10.6 Advanced Configuration	163
7.11 LED Screen	163
7.11.1 Prerequisites	163
7.11.2 Entrance & Exit LED Screen	163
7.11.3 Parking Guidance LED Screen	165
7.12 Alarm Device	166
7.13 Audio & Sensing Device	167

7.14 Networking Device	167
7.15 Interactive Flat Panel	167
Chapter 8 Configuration Validation	168
8.1 Validate Video Display	168
8.2 Validate Installation Quality	168
8.2.1 Online Validation	169
8.2.2 Offline Validation	169
8.3 Validate Camera Smart Events	170
8.4 Verify Other Parameters	171
Chapter 9 Maintenance & Security	173
9.1 Common	173
9.1.1 Refresh	173
9.1.2 Set Time for Time Sync	173
9.1.3 Backup & Import	174
9.1.4 SDK Protocol Compatibility Mode	174
9.1.5 Cloud Service	174
9.1.6 Service & Security	176
9.2 Upgrade Devices	179
9.2.1 Prerequisites	179
9.2.2 Entry	179
9.2.3 Constraints	179
9.2.4 Upgrade Settings	180
9.2.5 Upgrade Locally	180
9.2.6 Upgrade Online	184
9.3 Change IP	184
9.3.1 Change IP for Added Devices	184
9.3.2 Edit Network Parameters for Discovered Devices	185
9.4 Edit Device Name	185

9.5 Change Password	185
9.6 Device Diagnostics	187
9.6.1 Introduction	187
9.6.2 Video	188
9.6.3 Steps	188
9.7 Security Hardening	190
9.7.1 Introduction	190
9.7.2 Video	191
9.7.3 Steps	191
Chapter 10 Task Center	193
Chapter 11 Toolkit	194
11.1 Picture Validator & Optimizer	194
11.1.1 Introduction	194
11.1.2 Steps	195
Chapter 12 System Settings	200
12.1 General Settings	200
12.2 Download Extensions	200
12.3 Manage Passwords Across All Projects	203
Chapter 13 How-To Videos	207
13.1 Guided Delivery	207
13.2 Device Management	208
13.2.1 Add Devices	208
13.2.2 Upgrade Devices	208
13.3 Device Configuration	208
13.4 Maintenance & Security	210
13.5 Toolkit	210

Chapter 1 Before You Start

How to Use This Manual?

- New to HiTools Delivery? Start with the [Learn HiTools Delivery](#) to quickly learn main interfaces and basic operations.
- Already familiar with the tool? Check out [What's New](#) to explore key features in the latest version and access related documentation via embedded links.
- For video tutorials, refer to the [How-To Videos](#) . If you need additional videos, submit your needs via the documentation feedback channel. We will promptly review and address them.

Note

To enhance your experience, the product is continuously optimized. Some video content may lag behind the latest version—please refer to the actual application for accuracy. Updates will be released soon; stay tuned via [What's New](#) .

- Customize Table of Contents to Streamline your reading: Use the chapter filter in the top-left corner to select and display only relevant modules.
 1. Click **Customize** → **Select More Chapters** .
 2. Select chapters as needed, and click **Add** → **OK** .
 3. (Optional) Click **Reset** to restore to the original view.

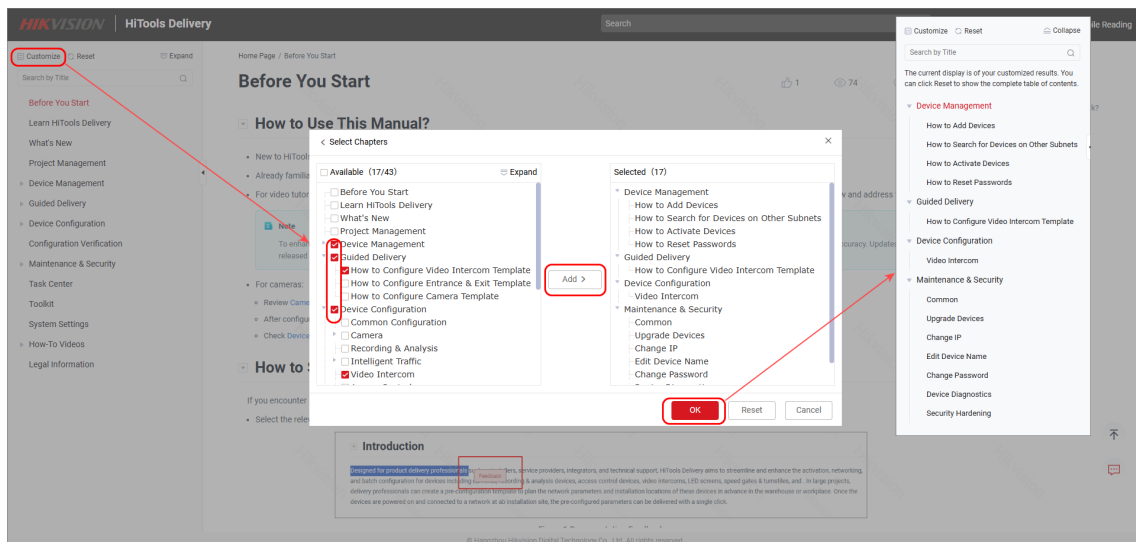


Figure 1-1 Customize Your Table of Contents

- For cameras:

- Review **Camera Configuration** and **General Configuration** for configuration details.
- After configuration, use **Configuration Verification** to verify settings like image quality, PTZ controls, smart events, and platform access.
- Check **Device Diagnostics** and **Security Hardening** to monitor device health and fix vulnerabilities regularly.

How to Submit Your Feedback?

If you encounter issues or have suggestions while reading the documentation, provide feedback through either the following methods. We will follow up promptly.

- Select the relevant text, click **Feedback**, describe the issue, and submit.

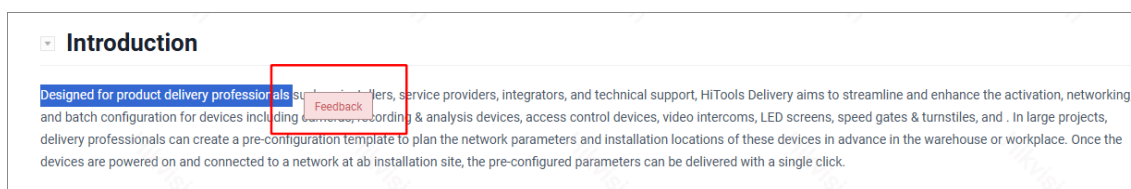


Figure 1-2 Documentation Feedback

- Click the feedback icon  at the bottom-right corner of the document page, describe the issue or suggestion, and submit.

Chapter 2 Learn HiTools Delivery

Documentation Updated on September 3rd, 2026, UTC+8

2.1 Introduction

Designed for product delivery professionals such as installers, service providers, integrators, and technical support, HiTools Delivery aims to streamline and enhance the activation, networking, and batch configuration for devices including cameras, recording & analysis devices, access control devices, video intercoms, LED screens, speed gates & turnstiles, networking devices, and alarm devices.

In large projects, delivery professionals can create a guided delivery template to plan the network parameters and installation locations of these devices in advance in the warehouse or workplace. Once the devices are powered on and connected to a network at an installation site, the pre-configured parameters can be delivered with a single click.

2.2 Software Interface Overview

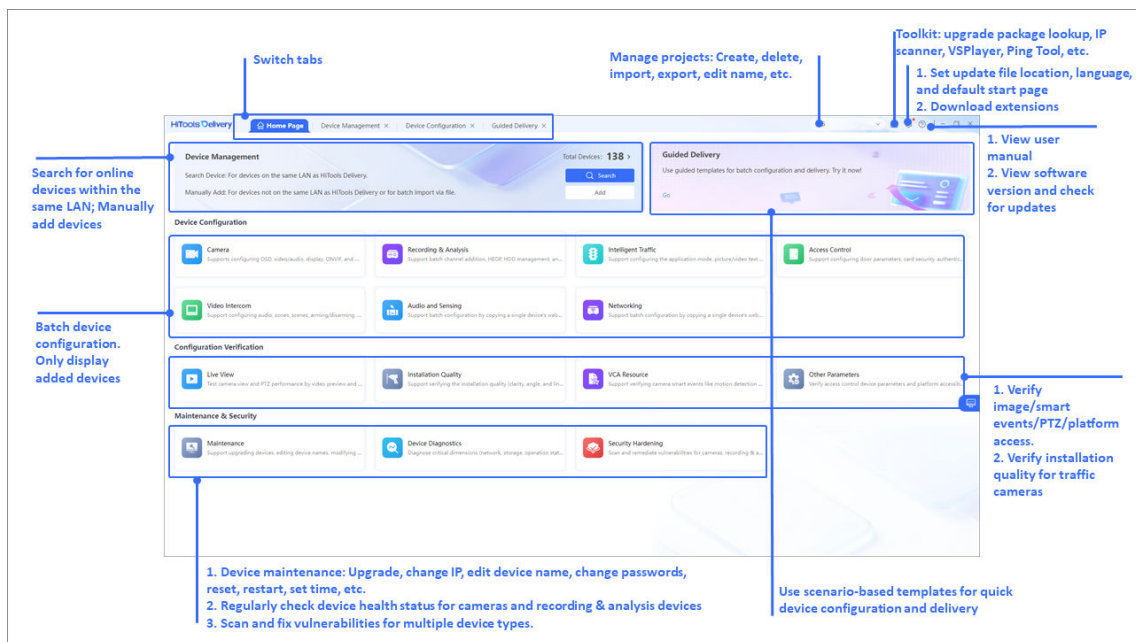


Figure 2-1 Homepage

HiTools Delivery User Manual

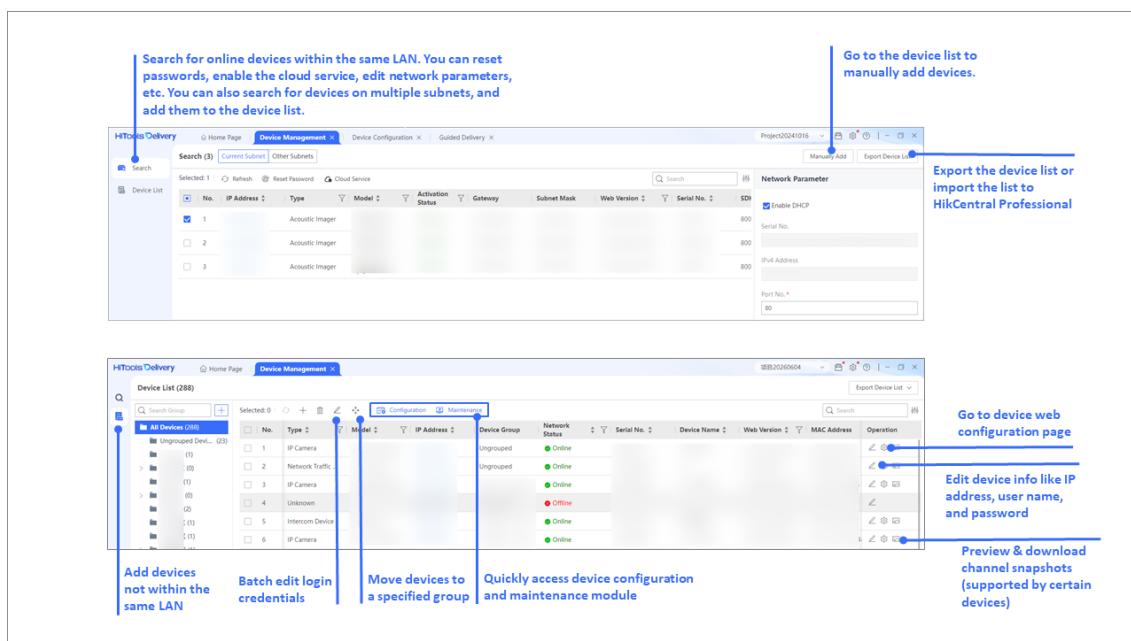


Figure 2-2 Device Management

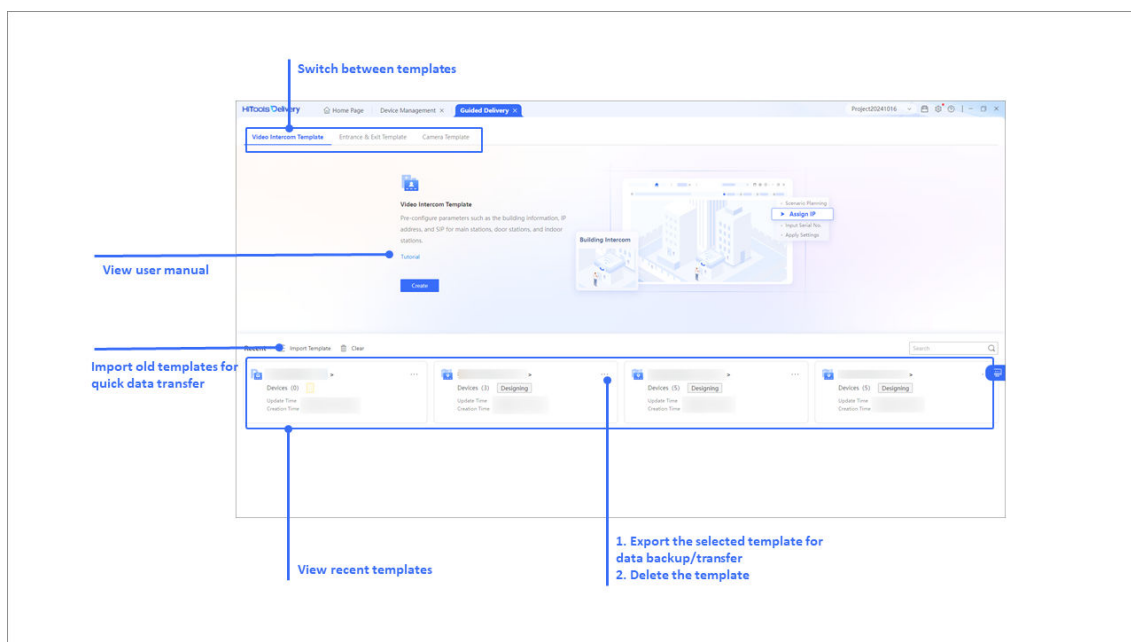


Figure 2-3 Guided Delivery

HiTools Delivery User Manual

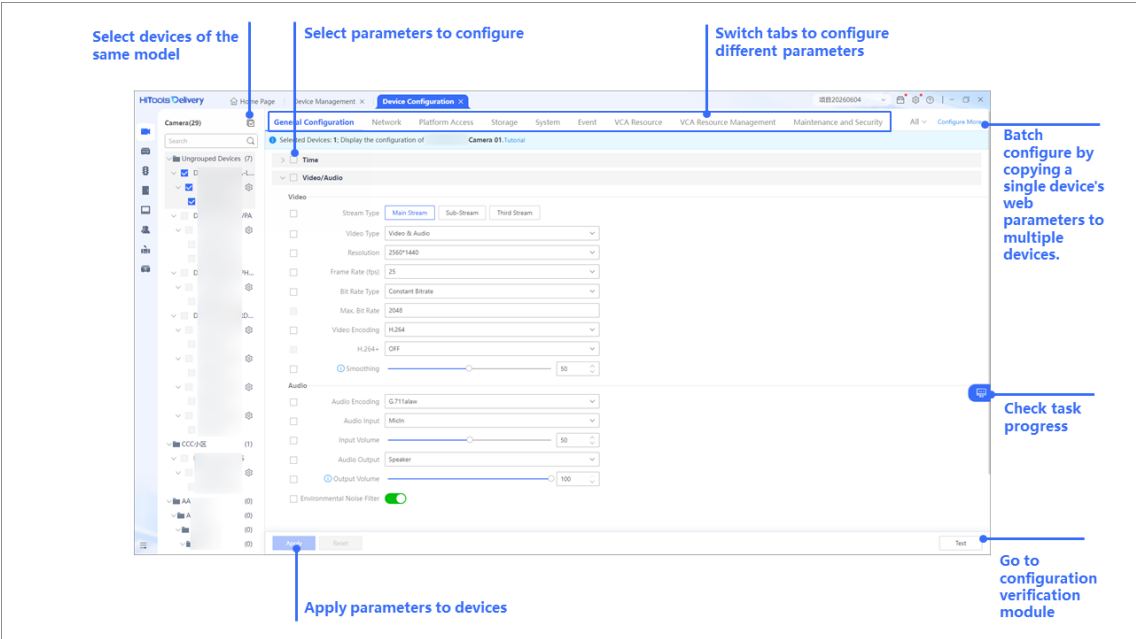


Figure 2-4 Device Configuration

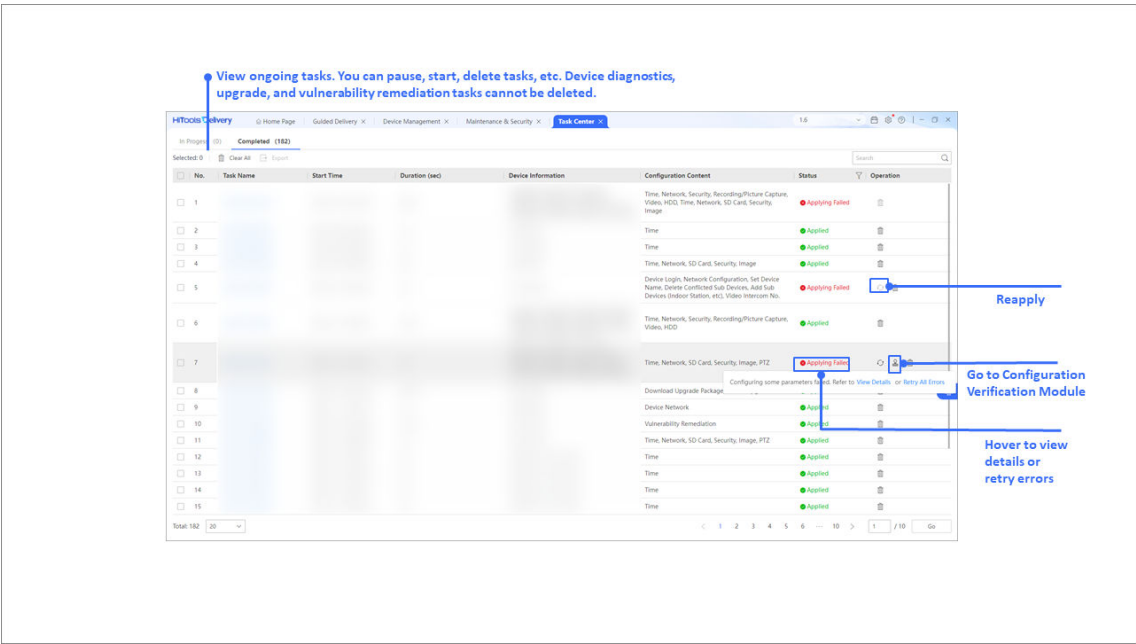


Figure 2-5 Task Center

2.3 Documentation Navigation

Modules	Sub Modules
<u>Project Management</u>	Create/delete/import/export projects.
<u>Guided Delivery</u>	• <u>Video Intercom Template</u> • <u>Entrance & Exit Template</u> • <u>Camera Template</u>
<u>Device Management</u>	• <u>Add Devices</u> • <u>Search for Devices on Other Subnets</u> • <u>Activate Devices</u> • <u>Reset Password</u>
<u>Device Configuration</u>	• <u>Common Parameters</u> • <u>Camera</u> • <u>Recording & Analysis</u> • <u>Access Control</u> • <u>Video Intercom</u> • <u>Speed Gate & Turnstile</u> • <u>LED Screen</u> • <u>Intelligent Traffic</u> • <u>Alarm Device</u> • <u>Audio & Sensing</u> • <u>Networking</u> • <u>Interactive Flat Panel</u>
<u>Configuration Verification</u>	• <u>Live View</u> • <u>Installation Quality</u> • <u>VCA Resource</u> • <u>Other Parameters</u>
<u>Maintenance & Security</u>	• <u>Common Maintenance</u> • <u>Upgrade Devices</u> • <u>Change IP</u> • <u>Edit Device's Name</u> • <u>Change Password</u> • <u>Device Diagnostics</u> • <u>Security Hardening</u>

2.4 System Requirements

Table 2-1 System Requirements

Parameter	Requirement
Operating System	• Recommended: Windows® 10-64 bit / Windows® 11-64bit • Compatible: Windows® 7-64bit / Windows® 8.1- 64 bit / Windows Server 2012 R2 or later (64-bit)
CPU	• Minimum: i3-9100@4.2GHz • Recommended: i5-1135G7@2.40GHz
RAM	• Minimum: 4 GB • Recommended: 16 GB
Graphics Card	• Minimum: GT1030 D5 • Recommended: UHD Graphics 620
HDD	• Minimum: 20 GB • Recommended: 200 GB
Display Resolution	1920*1080 or higher

Chapter 3 What's New

- [V2.1.2.1](#)
- [V2.1.1.2](#)
- [V2.1.0.6](#)
- [V2.0.2.4](#)
- [V2.0.1.4](#)
- [V2.0.0.6](#)

3.1 V2.1.2.1

Updated on September 3rd, 2026, UTC + 8

Service & Security

Related Document: [Network Service](#)

Support the following network services:

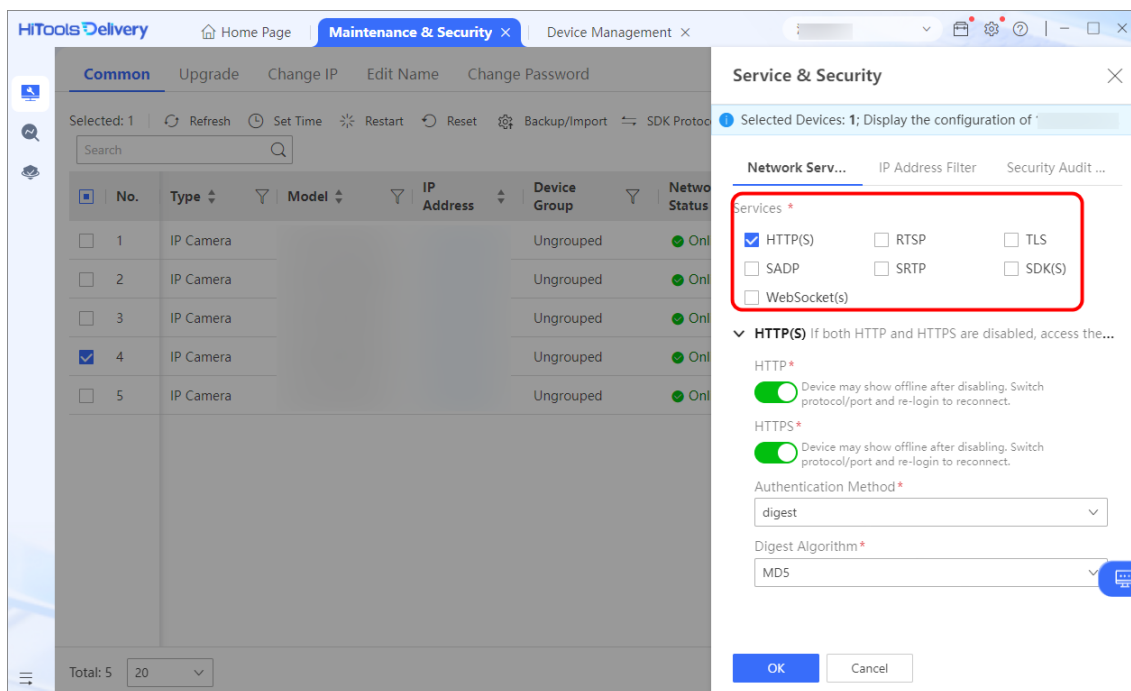


Figure 3-1 More Network Services

Item	Typical Scenarios	
SRTP	Encrypts live audio and video streams transmitted over public networks or untrusted third-party LANs to remote platforms, VMS (Video Management Systems), or the cloud. This service does not affect WebSocket-based web video previews.	
SADP	Search Active Device Protocol: Enables automatic device discovery, activation, password resets, and network parameter configuration within the same VLAN.	
SDK(S)	• SDK: Allows proprietary security platforms and client software within the LAN to actively access Hikvision devices. Supports device configuration, live view, playback, remote O&M (Operations & Maintenance), alarm handling, and PTZ control. • Enhanced SDK: Builds on standard SDK services by adding TLS encryption to guarantee data confidentiality and integrity. Uses port 8443 by default.	
WebSocket(s)	• WebSocket (HTTP-based): Unencrypted stream for plugin-free, real-time video preview directly in web browsers. • WebSockets (HTTPS-based): Encrypted stream for plugin-free, real-time video preview in browsers. Requires simultaneous TLS configuration and certificate creation.	

Reset Single Device's Password

Related Document: [***Reset Single Device's Password via Email***](#)

If you set the SADP mode to **Discovery Only** in the Service & Security module, enter the full registered email address and click **Verify**. Once verified, you can follow the on-screen steps to reset the device password.

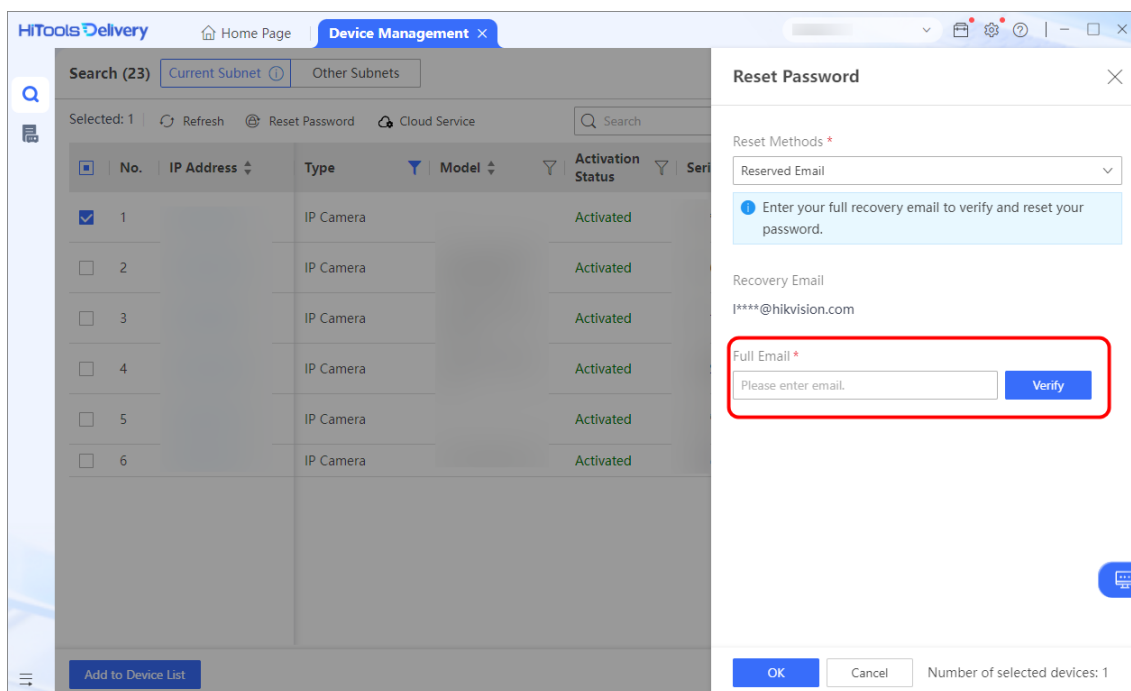


Figure 3-2 Enter Full Email Address to Verify and Reset Password

3.2 V2.1.1.2

Device Management & Search

- Optimized password reset instructions for cameras and recording & analysis devices manufactured before 2015.
- The Device Search interface now supports sorting by Gateway and Subnet Mask.

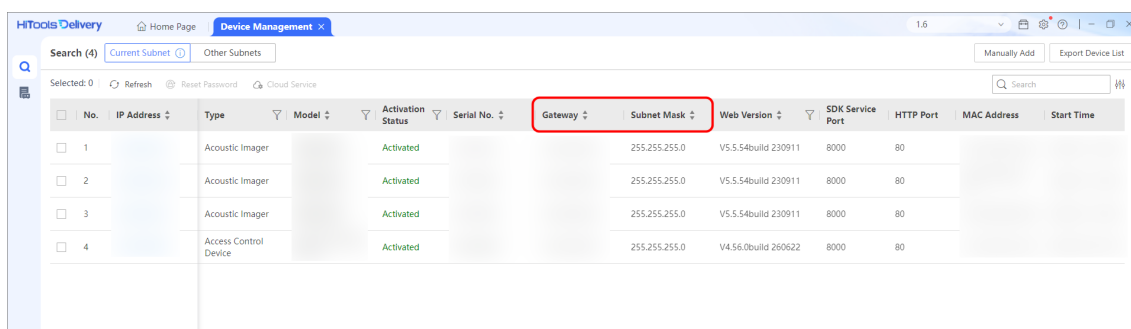


Figure 3-3 Sort by Gateway & Subnet Mask

- After downloading the camera configuration extension, you can redirect to the web configuration page from the device list for certain camera models.

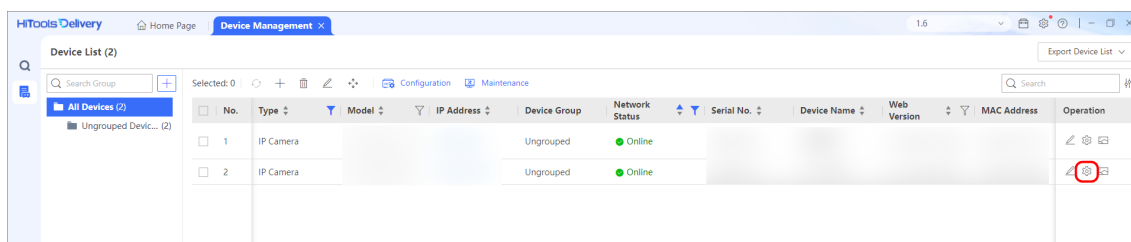


Figure 3-4 Go to Camera's Web Configuration Page

Camera Configuration

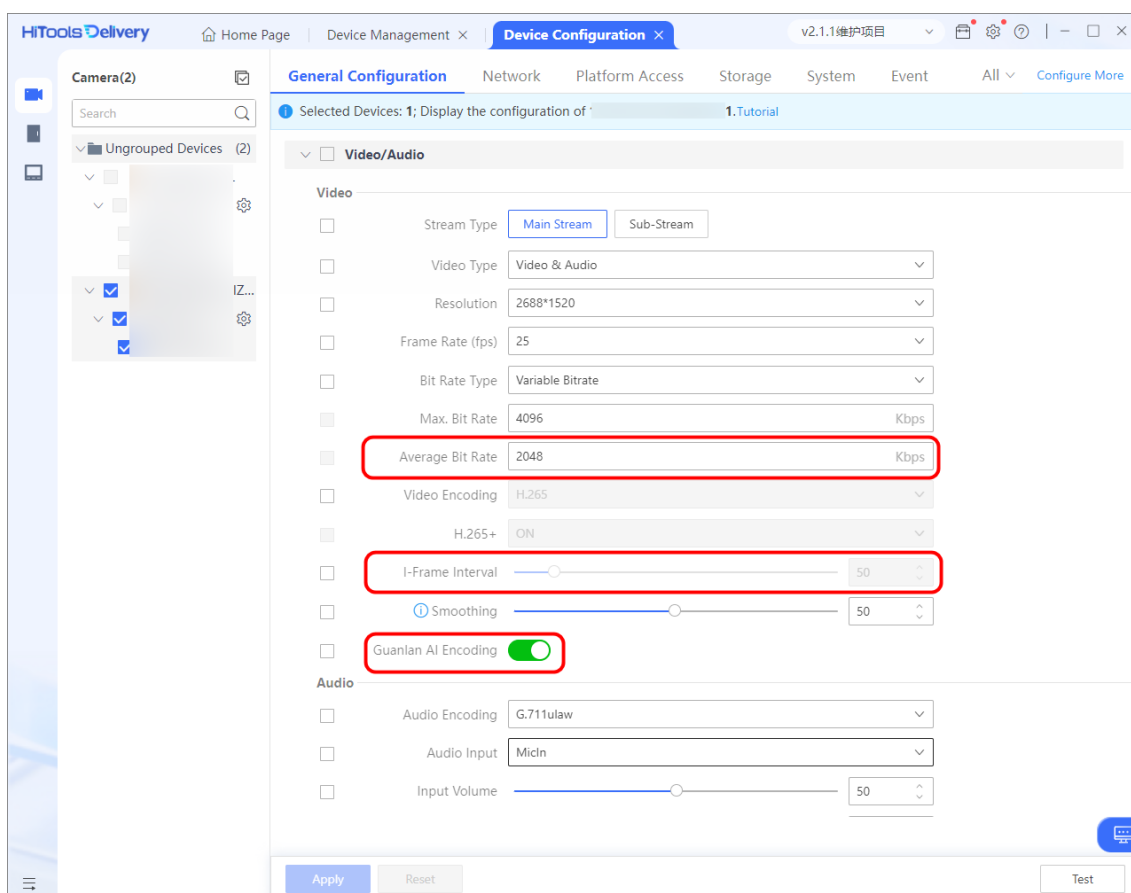


Figure 3-5 New Video/Audio Parameters

Three new parameters are available: **Average Bit Rate**, **I-Frame Interval**, and **Guanlan AI Encoding** (supported by certain cameras). Configuration rules are as follows:

- **Guanlan AI Encoding:** Enabling AI encoding unlocks the Average Bit Rate configuration. It intelligently distinguishes key targets (e.g., people and vehicles) from backgrounds to

dynamically allocate bitrate. Reduces storage consumption by over 50% compared to standard H.265 while preserving critical details.

- **Average Bit Rate:** Defaults to 50% of the maximum bitrate limit.
- **I-Frame Interval:**
 - Editable only when both Smart Encoding and Guanlan AI Encoding are disabled.
 - Higher intervals lower bandwidth and storage usage (e.g., at 25 fps, an I-frame interval of 50 generates one I-frame every 2 seconds).

Change IP

Successfully changing IP addresses automatically generate and export an IP Change Report to your local PC.

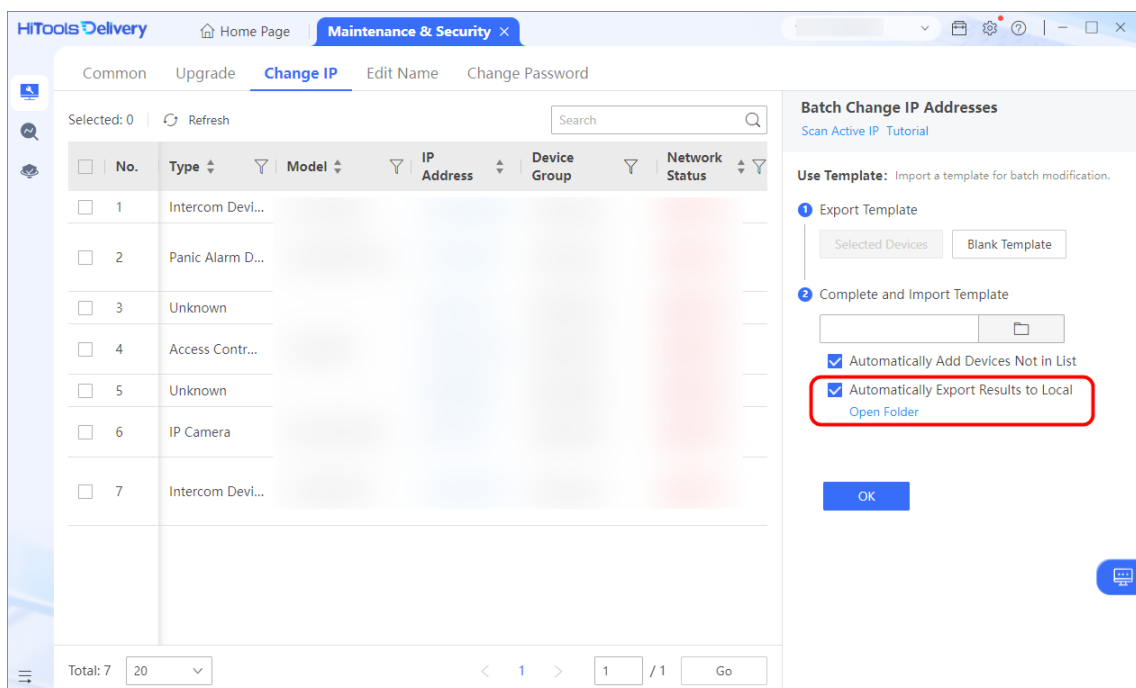


Figure 3-6 Automatically Export IP Change Report to Local

3.3 V2.1.0.6

3.3.1 [New] Picture Validator & Optimizer

This new tool helps prevent batch import failures caused by non-standard photos (occlusions, low clarity, etc.). It provides **pre-screening and batch repair** to ensure high first-time success rates and quickly identify invalid photos requiring re-collection.

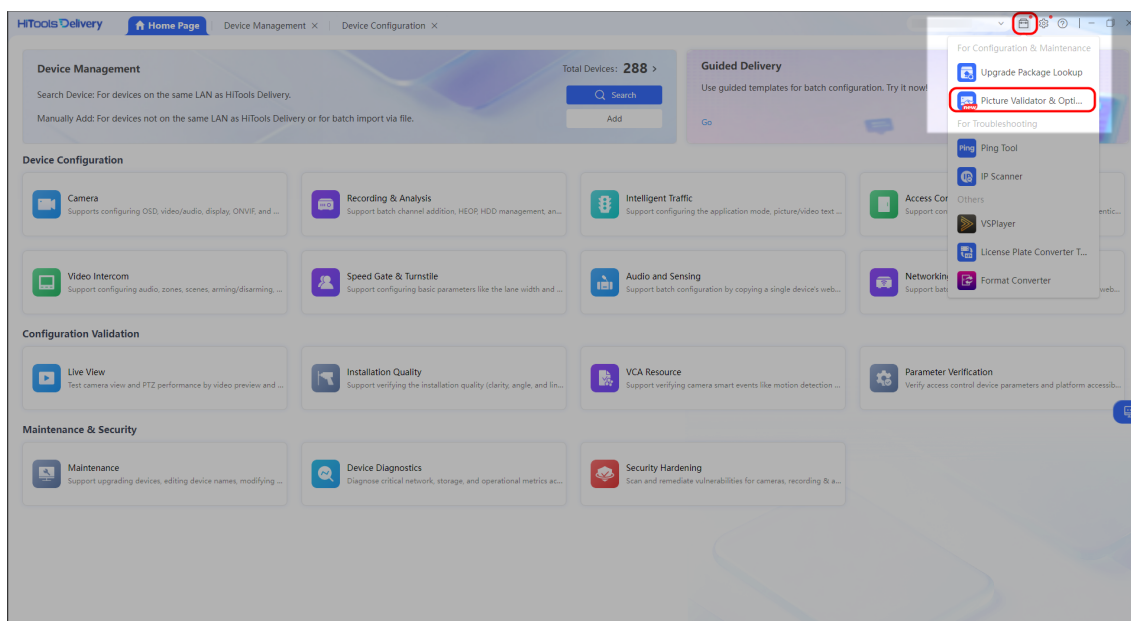


Figure 3-7 Picture Validator & Optimizer

Related Document: [**Picture Validator & Optimizer**](#) .

3.3.2 [New] Password Manager

Saved passwords can be quickly applied in configuration interfaces (such as adding devices, modifying passwords, activating devices, and modifying network parameters) without repeated manual entry. All projects share a single password manager.

- Add Password

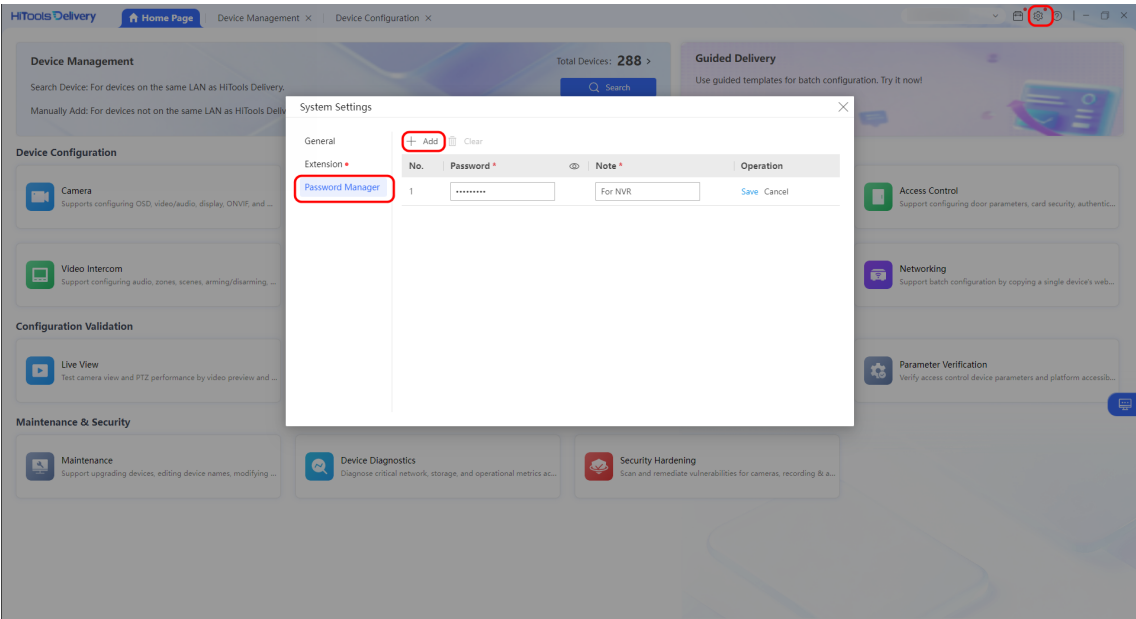


Figure 3-8 Add Password in Password Management Module

Add

Adding Mode

☒ IP

☐ IP Segment

☐ Batch Import

Protocol Type ⓘ

☒ Adaptive

☐ ISAPI

☐ Private

☐ OTAP

Applicable to virtually all products; uses the device's default port for login. If the default port is modified, please use alternate protocols.

IP Address *

User Name *

admin

Password *

.....

New password. [Save to Password Manager](#) for future use? X

Ungrouped Devices

OK

Cancel

Figure 3-9 Add Password to Password Manager via Configuration Interface

- Quickly Apply Passwords

Add

Adding Mode

☒ IP ☐ IP Segment ☐ Batch Import

Protocol Type ⓘ

☒ Adaptive ☐ ISAPI ☐ Private ☐ OTAP

Applicable to virtually all products; uses the device's default port for login. If the default port is modified, please use alternate protocols.

IP Address *

User Name *

admin

Password *

Saved Passwords ⓘ Show Password | ⚙️

For NVR

OK Cancel

Figure 3-10 Quickly Apply Passwords

3.3.3 [Updated] Device Search

Cross-Segment Device Discovery

Support skipping device credential (user name and password) configuration after adding IP segments. Without credentials, **only certain cameras** will display basic information (IP, Model, SN, Gateway, SDK Port, and HTTP Port). Detailed device information will be displayed once correct authentication info is provided.

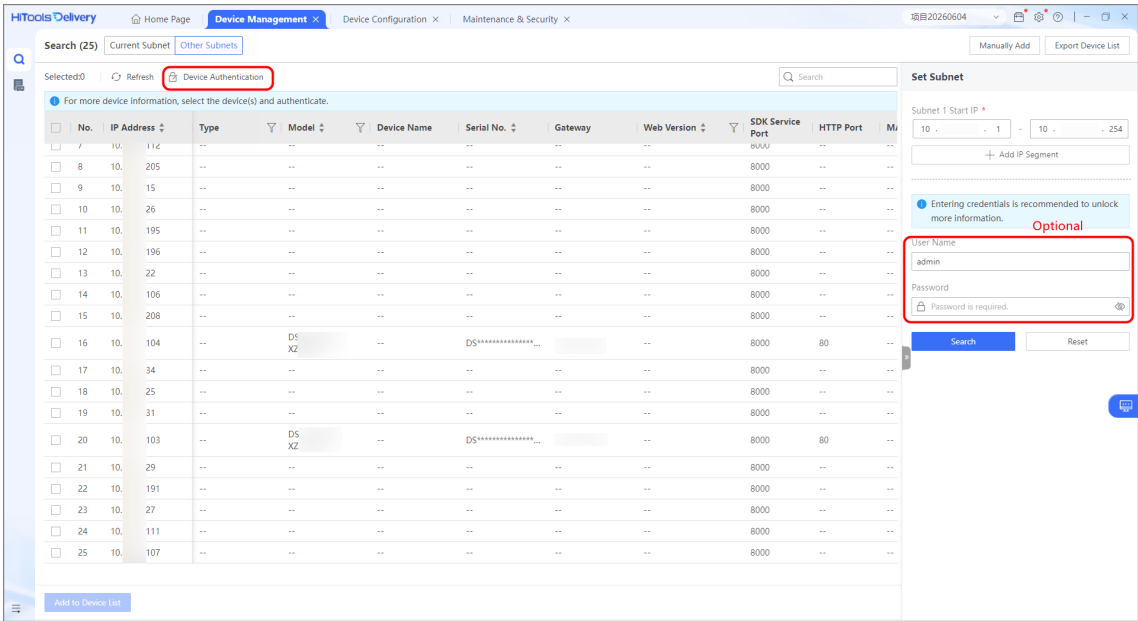


Figure 3-11 Search Devices Across Segments

Batch Password Resetting

Support batch password resetting via Excel (for 30+ devices), XML, or QR code scanning.

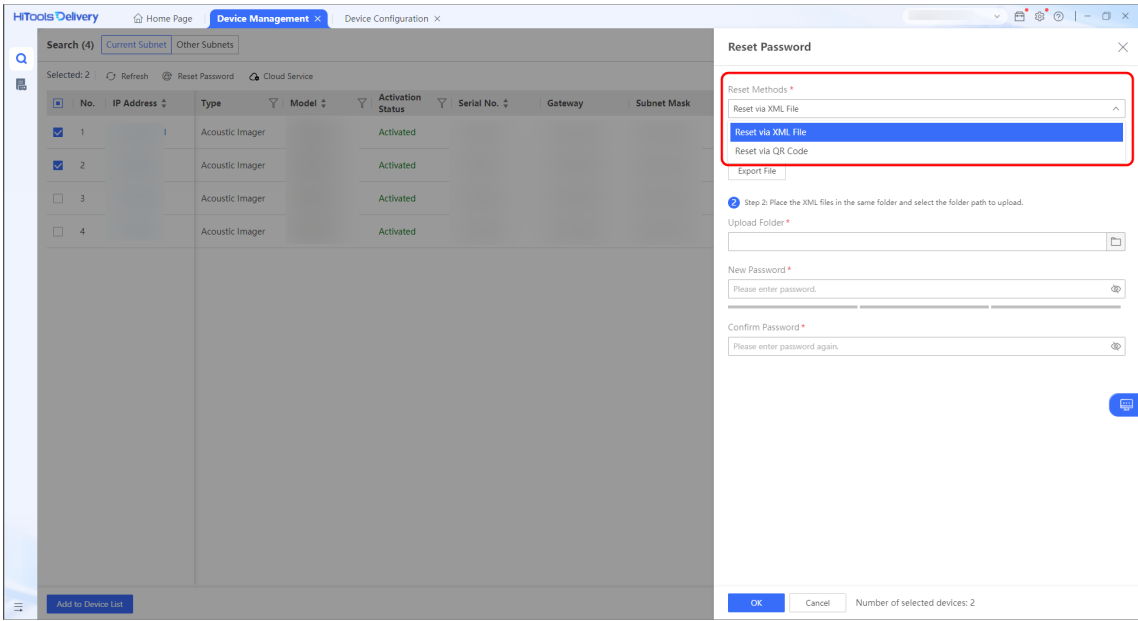


Figure 3-12 Batch Password Resetting

3.3.4 [Updated] Camera Configuration

For multi-channel cameras, support batch parameter configuration based on device model and selected channels.

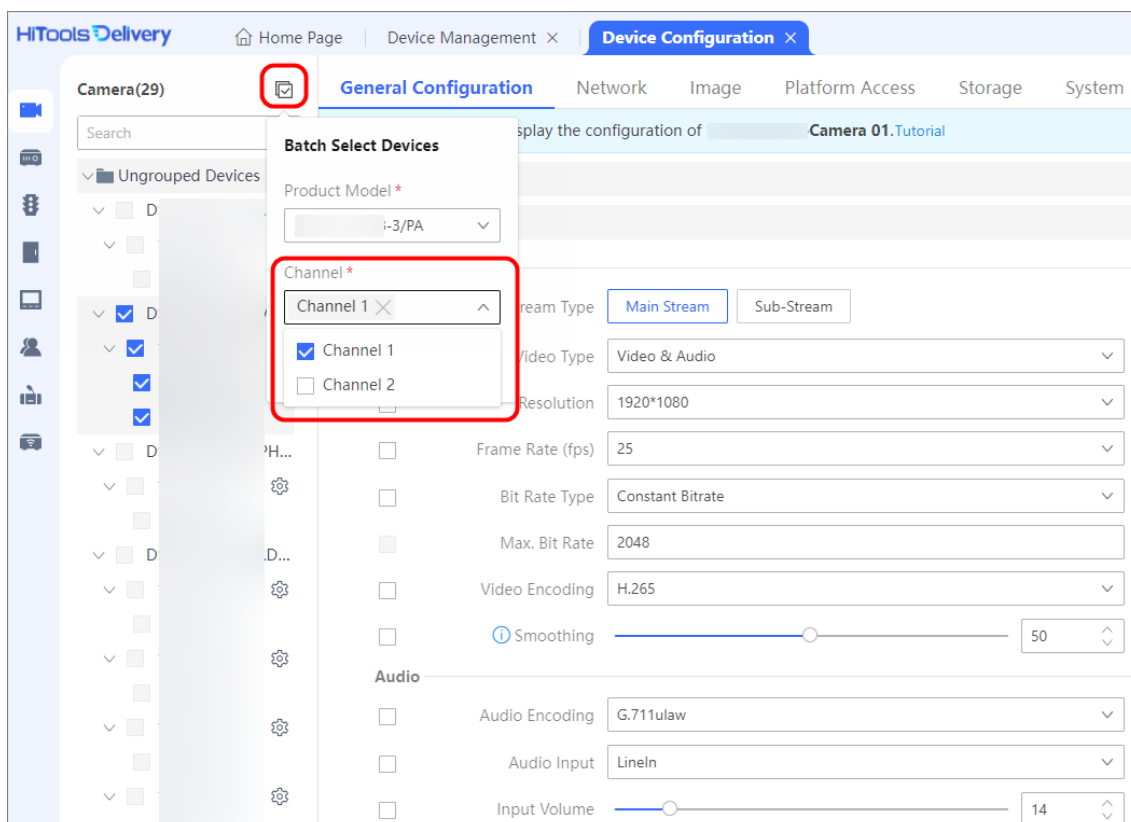


Figure 3-13 Batch Select Channels

3.3.5 [New] Device Management

Device Grouping

Support creating groups by physical space (e.g., buildings, floors, rooms) to facilitate batch management for large campuses or projects. Installers can independently configure deployment policies and upgrade plans for different groups, significantly improving delivery efficiency by eliminating manual device filtering.

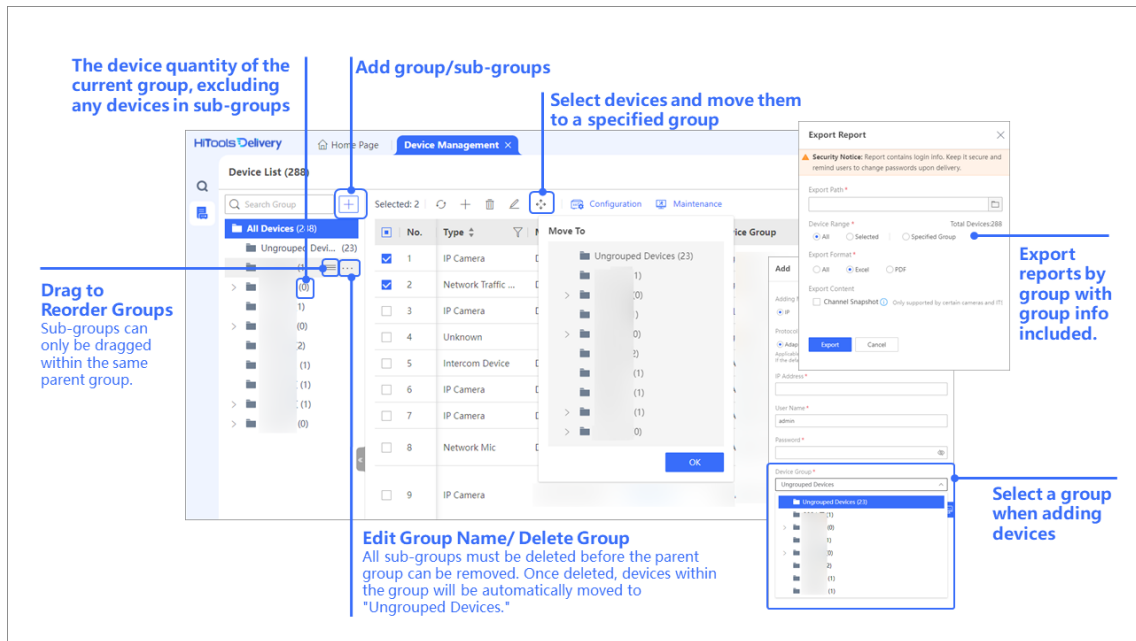


Figure 3-14 Device Grouping Overview

Channel Snapshot Preview

After installing and configuring certain devices (such as cameras, access control, intercoms, and ITS), support previewing and downloading snapshots to ensure they are correctly installed and operating normally. For multi-channel devices, only the preview of the first channel is supported.



Note

This feature is only supported by certain devices.

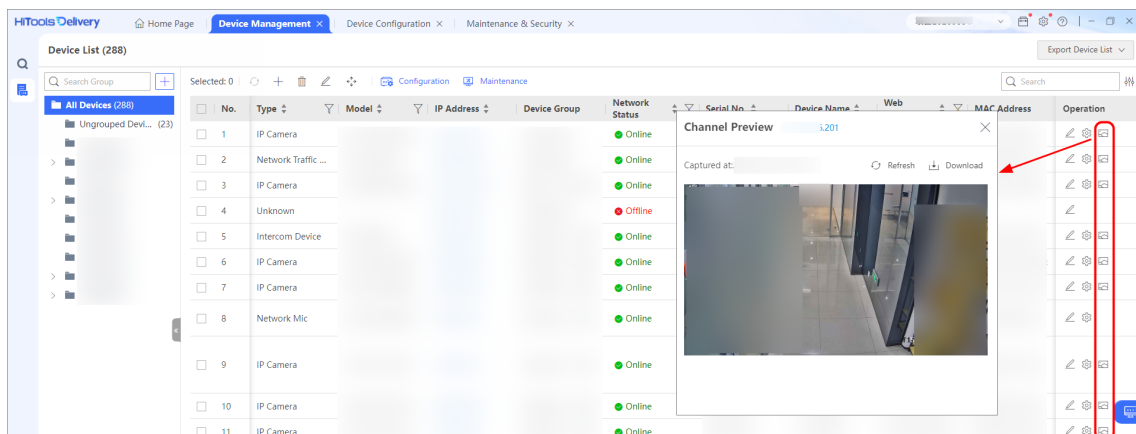


Figure 3-15 Channel Snapshot Preview/Download

3.3.6 [Updated] Traffic Camera Configuration Validation

For offline validation, support automatically detecting the validation mode after picture import. If the mode cannot be identified, you can select it manually.

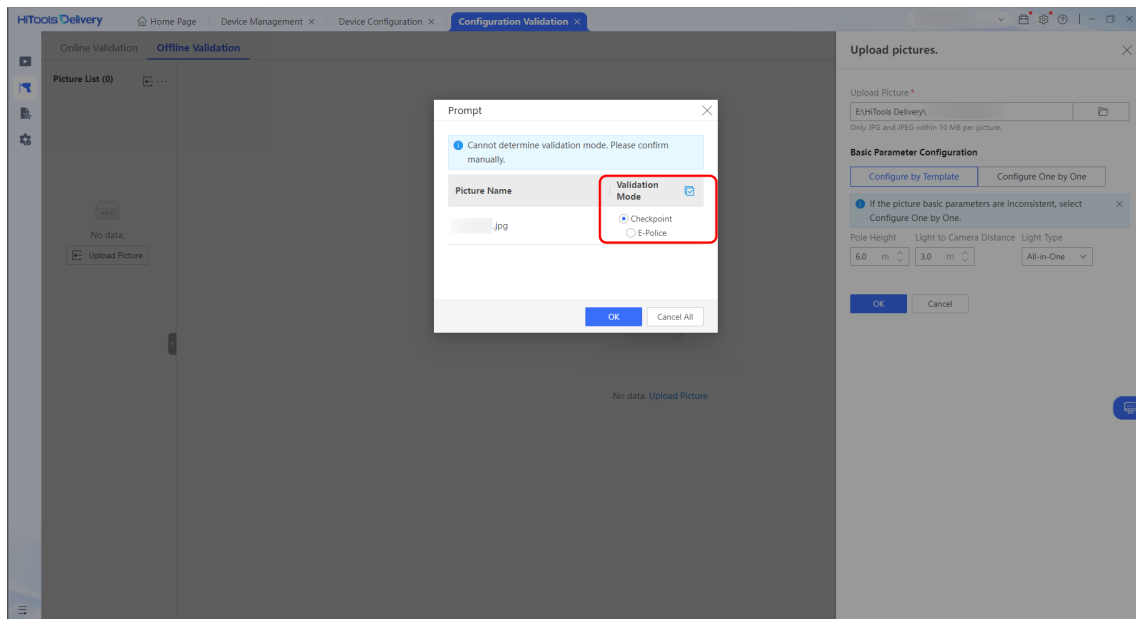


Figure 3-16 Auto Detect Validation Mode

3.3.7 [Updated] Device Maintenance

Device Upgrade

For **VPro Series NVRs with AcuSeek**, the tool performs a pre-check upon importing the upgrade package during local upgrade. If the search algorithm version is incompatible, historical data must be re-indexed (re-modeled), and manual confirmation is required to proceed with the upgrade. If the compatibility test failed, the device cannot be upgraded.

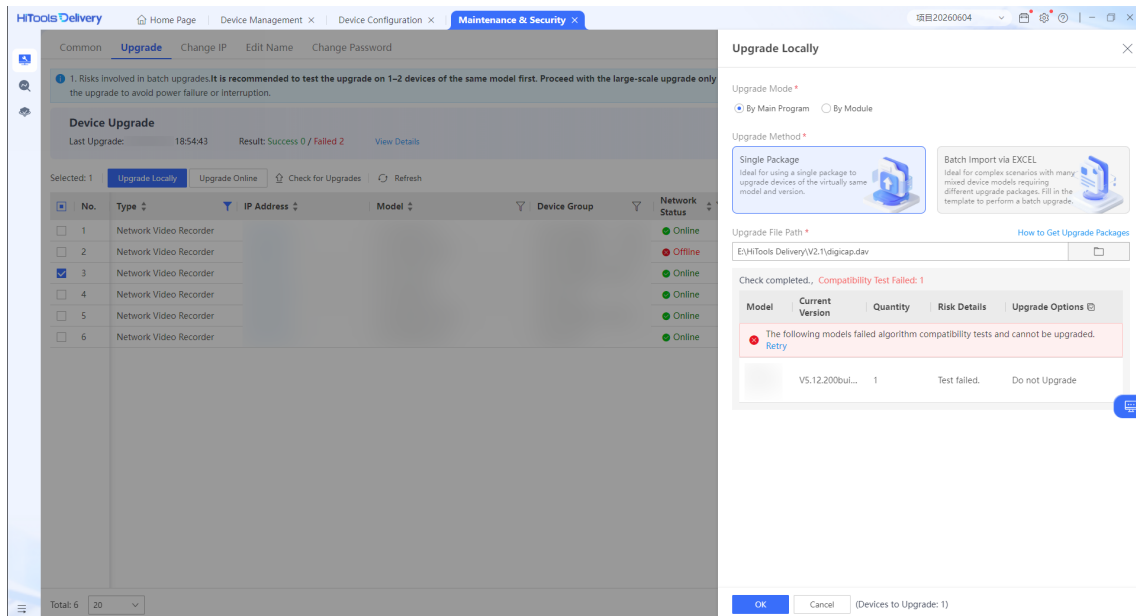


Figure 3-17 Upgrade Pre-check Failed for VPro Series NVRs with AcuSeek

Security Hardening

For **VPro Series NVRs with AcuSeek**, the tool performs a pre-check upon importing the upgrade package during offline remediation. If the search algorithm version is incompatible, historical data must be re-indexed (re-modeled), and manual confirmation is required to proceed with the upgrade. If the compatibility test failed, the device cannot be upgraded.

Device Diagnostics

Device diagnostics supports access control devices and capture cameras. Diagnostics items are listed in the following table:

Table 3-1 Device Diagnostics Items

Device Type	Diagnostics Items
Access Control	- Time Info: Time, Time Zone, and DST. - Network Status: IP Conflicts / Network Disconnection. - Security: Device Locking - Face Recognition: Face Authentication Pass Rate

Device Type	Diagnostics Items
	• Arming Clients • Exception Events: Door Opened by Force; Door Open Timeout
ITS Capture Camera	• Time Info: Time, Time Zone, and DST. • Network Status: Network Latency / Packet Loss • Storage: TF Card Status • Channel Snapshot • Preview & Arming Status: Number of arming clients and streaming channels

3.4 V2.0.2.4

Updated on June 1st, 2026, UTC + 8

3.4.1 [New] Service & Security

Related Document: [**Service & Security**](#)

Streamline device security with bulk configuration for network services, TLS controls, IP filtering, and log uploads.

- Network Service
 - **HTTP(S):** Bulk-disable HTTP/HTTPS ports during critical security incidents and switch to secure private protocols for device access.
 - **RTSP:** Bulk-disable RTSP services during security incidents to block unauthorized video streams and potential attack vectors.
 - **TLS:** Bulk-disable vulnerable legacy TLS versions (e.g., TLS 1.1) and enforce TLS 1.2+ to achieve cryptographic hardening.
- IP Address Filter

P filtering is used not only for incident response but also to enforce allowlists in high-security scenarios.
- Security Audit Log

Security Auditing: Bulk-enable audit logging to meet compliance requirements. Centralize logs on a dedicated server to facilitate global search and rapid incident investigation via the platform.

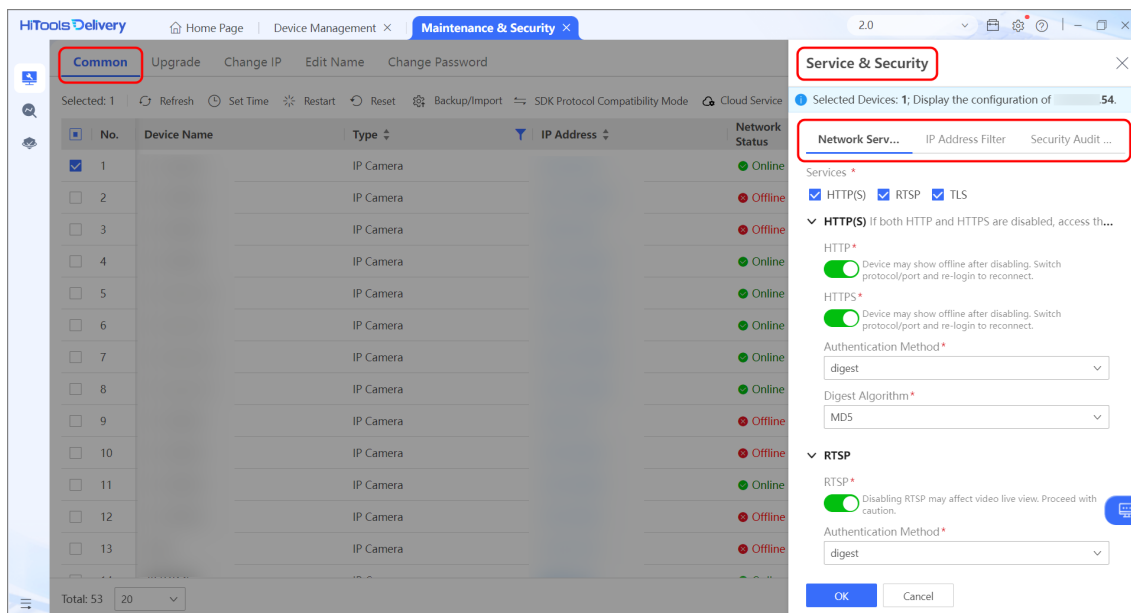


Figure 3-18 Service & Security

3.4.2 [Updated] Local Upgrade

Related Document: [Local Upgrade](#)

Support setting the upgrade method for main program upgrades.

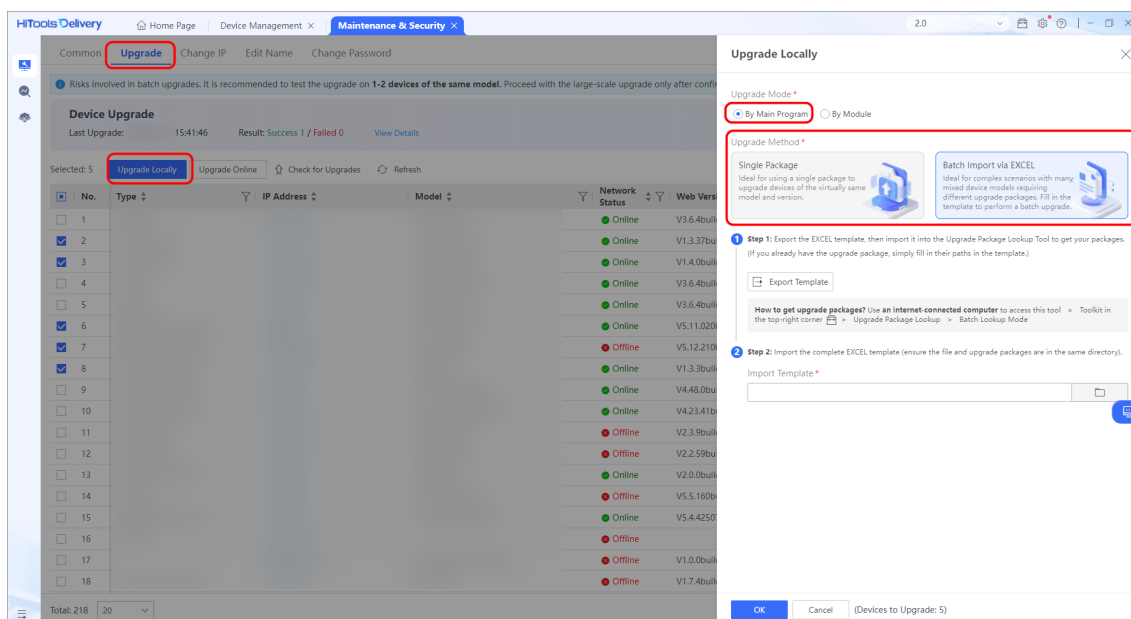


Figure 3-19 Set Upgrade Method

- Single Package
Import a single package to upgrade devices with the virtually same model and version.
- Batch Import via Excel
Ideal for large-scale upgrades involving multiple device models.
 1. Export the template and import it into the **Upgrade Package Lookup Tool**.
 2. Batch download the packages and obtain a template pre-filled with file paths.
 3. Import the completed template to execute the upgrade.

3.4.3 [Updated] Upgrade Package Lookup Tool

Support importing the upgrade package lookup template to search for multiple upgrade packages simultaneously. You can download all required packages in one click. Once unzipped, the resulting template (containing pre-filled package paths) can be imported directly into the local upgrade interface to complete the process.

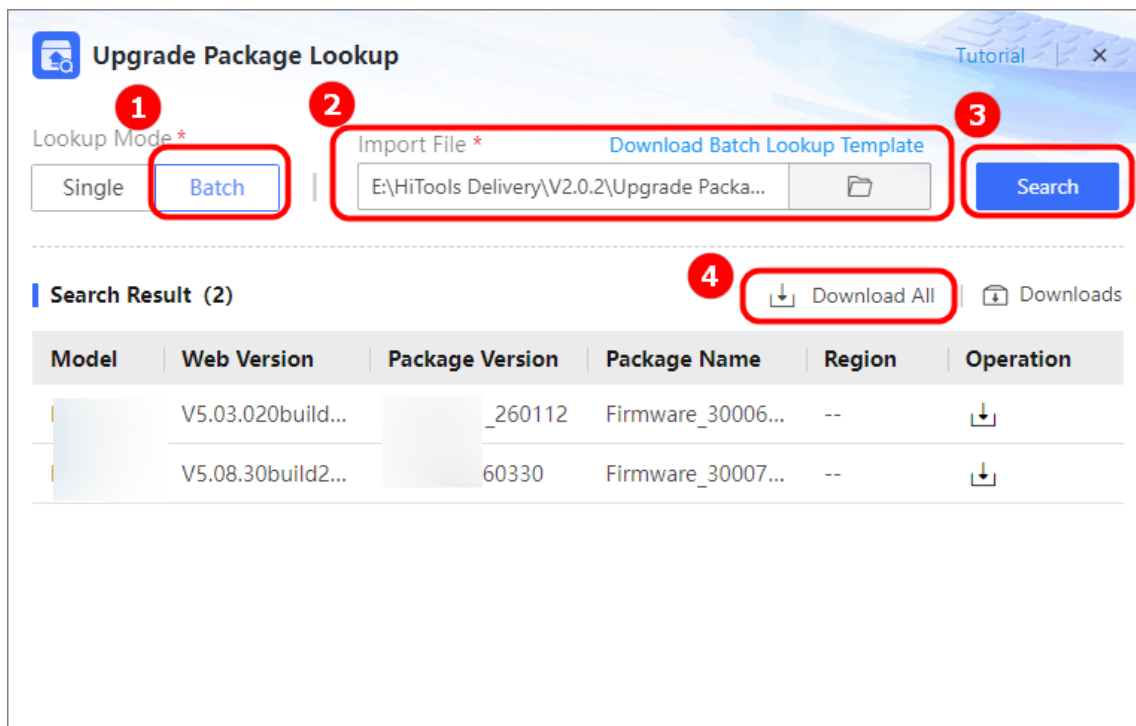


Figure 3-20 Batch Lookup Mode

	A	B	C	D
1	Notes: 1. Upgrade Package Path: The upgrade package must be in the same directory as the Excel template (auto-filled if using the upgrade package lookup tool). 2. If no packages are found, contact technical support.			
2	* Model	* Short Device Serial Number	* Web Version	* Upgrade Package Path (e.g., FolderName/digicap.dav)
3	DS-503-JP1		7build 7	
4	DS-503-W		build 260318	
5	iDS-IXI-P1		020build 3	
6	iDS-IX-P1		210build 3	
7	DS-		build 251219	
8				

Figure 3-21 Upgrade Package Lookup Template

3.5 V2.0.1.4

Updated on February 6th, 2026, UTC+8

3.5.1 Device Upgrade

- When upgrading the card reader module, you can now select the device number.

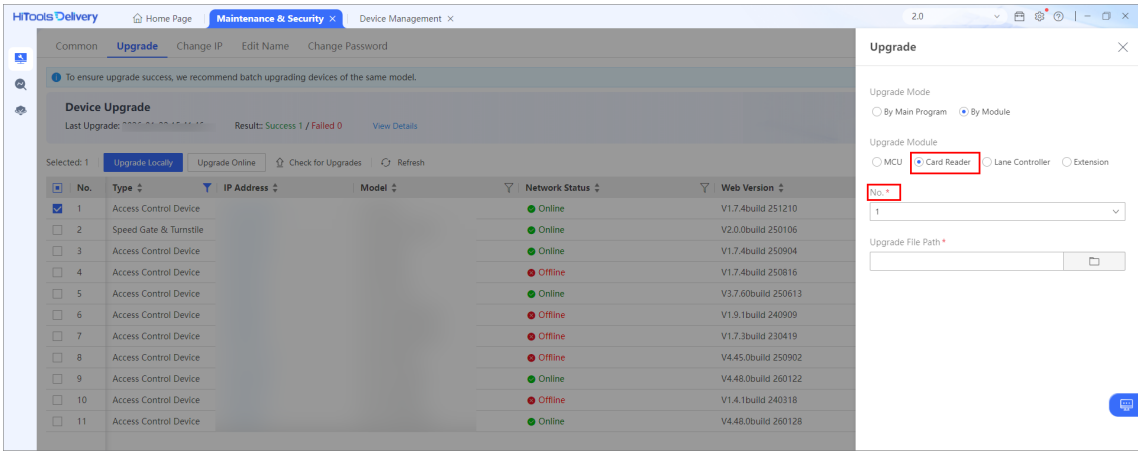


Figure 3-22 Select Card Reader No. to Upgrade

- When upgrading the lane controller, you can select between main and sub lane control boards.

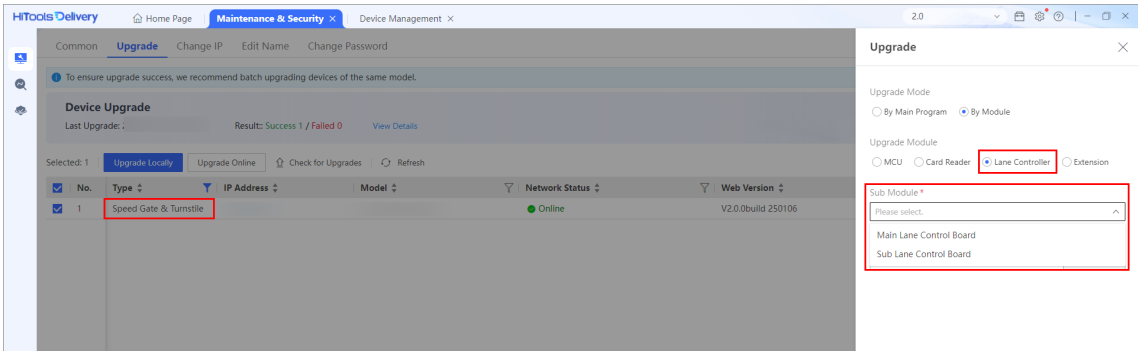


Figure 3-23 Upgrade Sub Module for Lane Controller

3.5.2 Device Diagnostics

The diagnostics report cover now supports summarizing results by device.

 Diagnostic Report	
Basic Information	
Project Name	2.0
Diagnostics Time	2026/2/6 11:11:55
Time Range	2026-02-05 11:11:55 - 2026-02-06 11:11:55
Device Quantity	Cameras: 4
Results by Device	Camera: 4 Abnormal, 0 Failed
Results by Anomaly Count	Camera: 4

Figure 3-24 Diagnostics Results by Device

3.5.3 System Settings

- Support a new software language: Japanese.

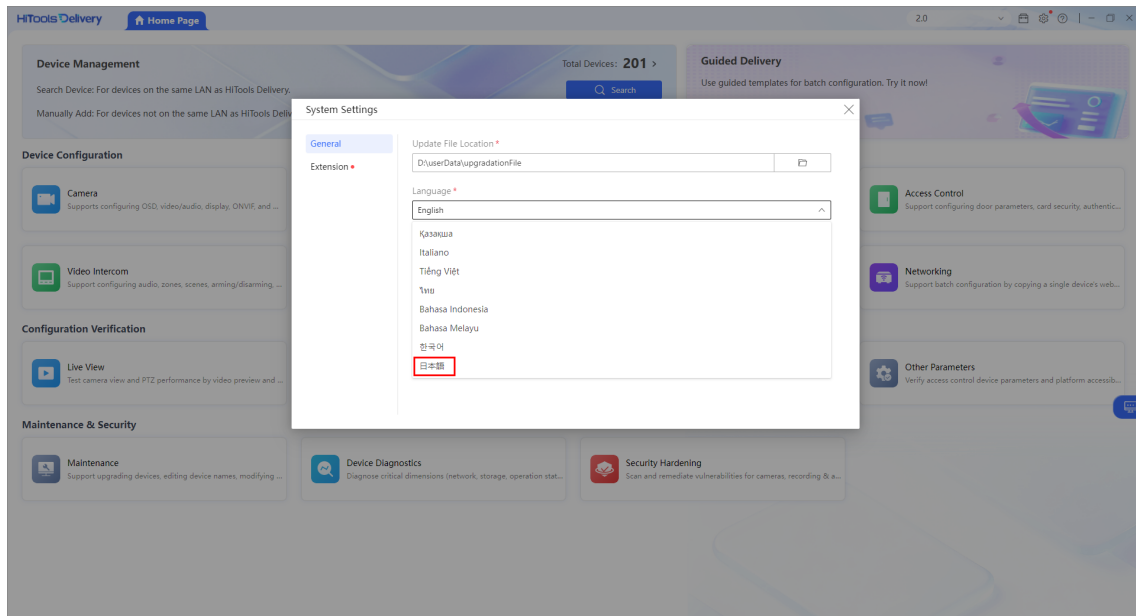


Figure 3-25 Support for Japanese

- Support batch updating, downloading, and importing/exporting extensions. This supports rapid transfer between PCs, boosting delivery efficiency in offline environments.

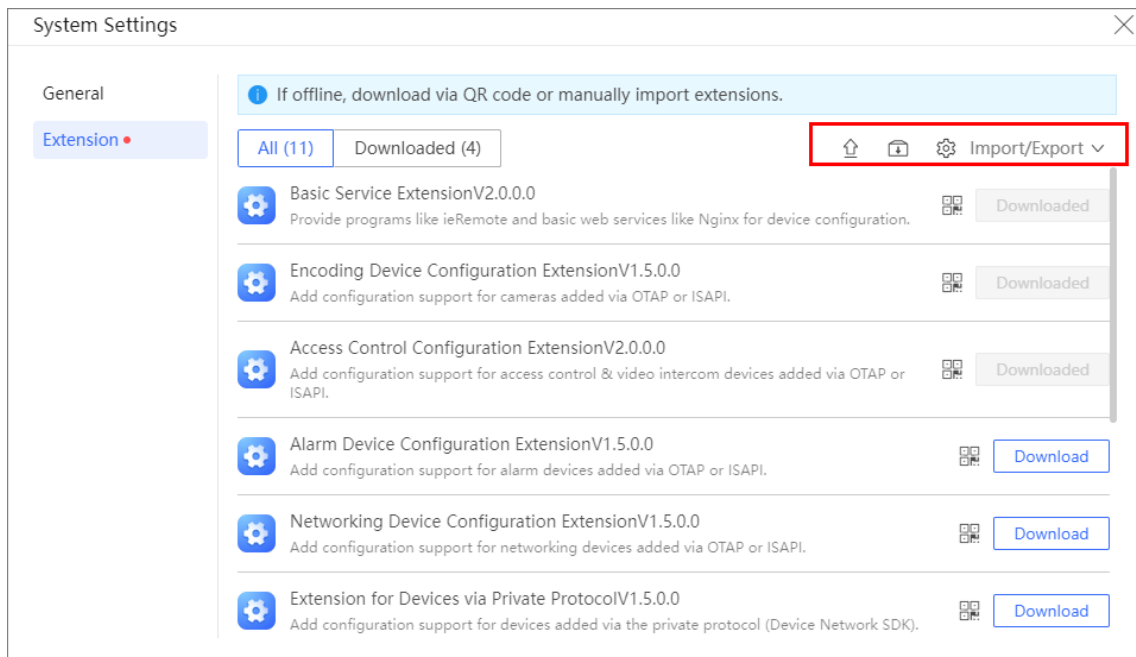


Figure 3-26 Download/Update/Export Extensions

3.5.4 Toolkit

IP Scanner: Starting and ending IPs are automatically filled based on the selected NIC.

3.6 V2.0.0.6

3.6.1 Brand New Homepage

The homepage has been restructured based on user workflows. Five core modules—**Device Management**, **Device Configuration**, **Guided Delivery**, **Configuration Verification**, and **Maintenance & Security**—are clearly segmented. Supporting **multi-tab navigation**, you can quickly switch and efficiently complete various configuration tasks as needed.

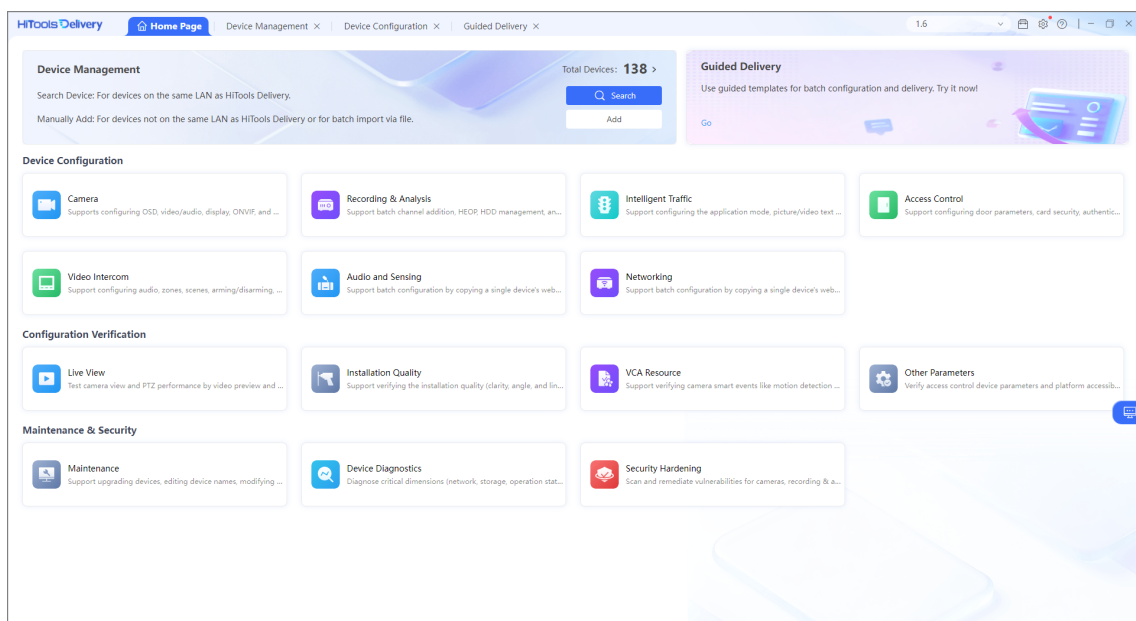


Figure 3-27 Brand New Homepage

3.6.2 Device Management

- The Device Management module focuses on Device Search and Device Addition functions. Other functions such as upgrading, modifying IP addresses, and changing passwords have been moved to the Maintenance module.
- Other functions such as upgrading, modifying IP addresses, and changing passwords have been moved to the Maintenance module.
- Support quick navigation to the **Device Configuration** and **Maintenance & Security** modules on the Device List.

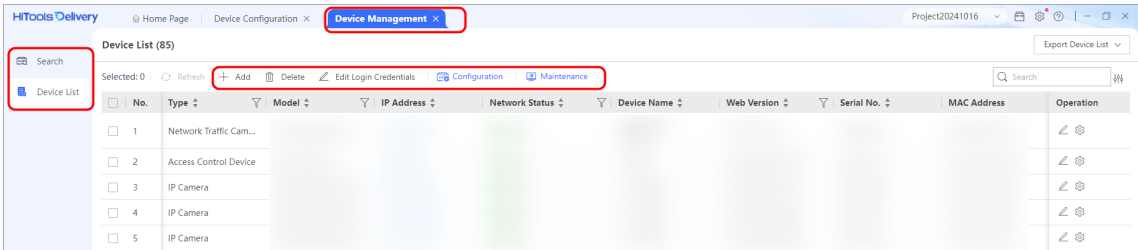


Figure 3-28 New Device List

- Support exporting the device list on the Device Management page.

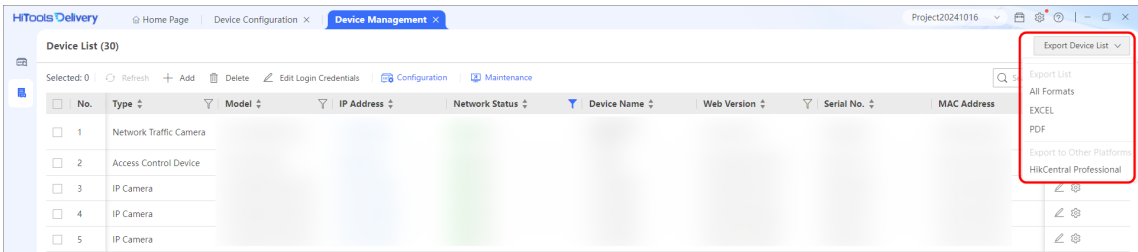


Figure 3-29 Export Device List

- Support batch editing the device login credentials.

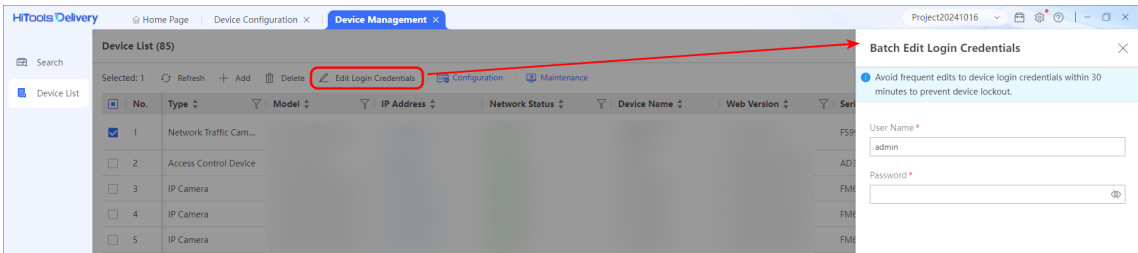


Figure 3-30 Batch Edit Login Credentials

- Support binding an online device to a cloud account via verification code and QR Code. For details, refer to **Cloud Service**.

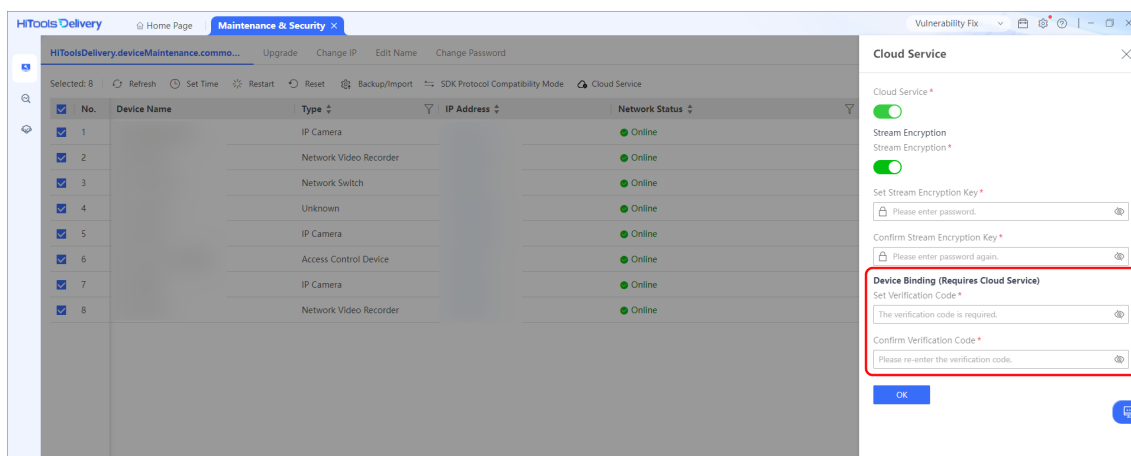


Figure 3-31 Device Binding

- Support setting the default password to add channels when activating NVRs.

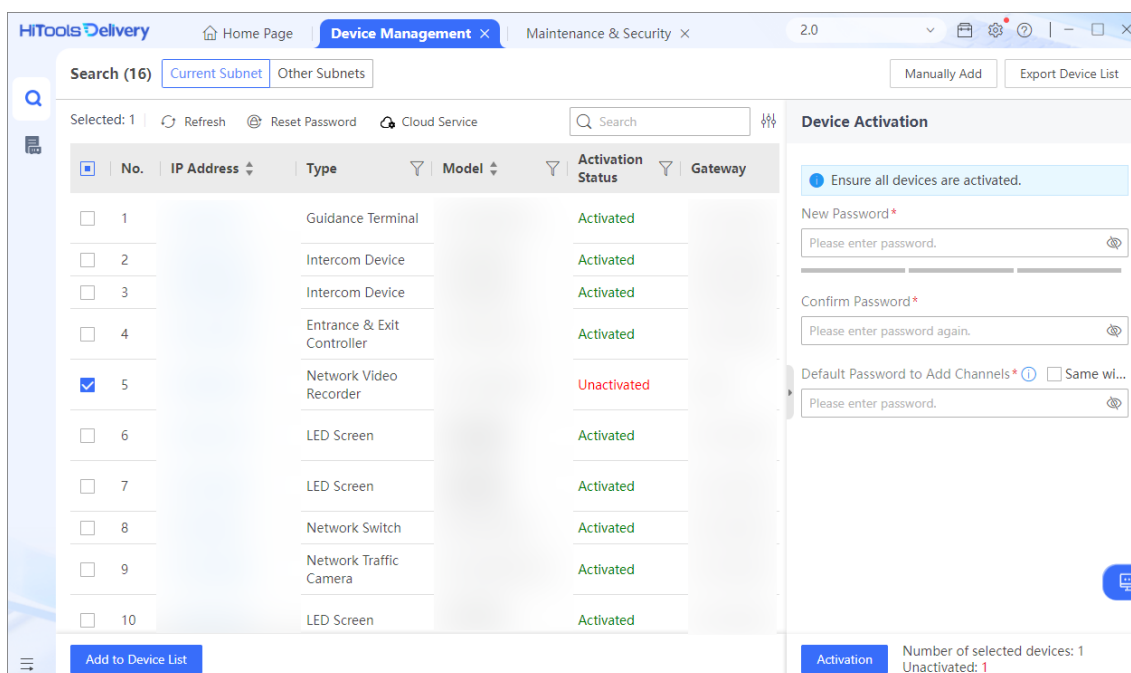


Figure 3-32 Set Default Password to Add Channels

3.6.3 Guided Delivery

Related Document: [*Video Intercom Template*](#)

- The Pre-Configuration module are now renamed to Guided Delivery. User manuals can be accessed by scanning a QR code with your phone, addressing issues with private network restrictions or inconvenience on computers.
- **Basement Scene Configuration:** Support selecting basement levels in Advanced Settings to meet the on-site requirements.

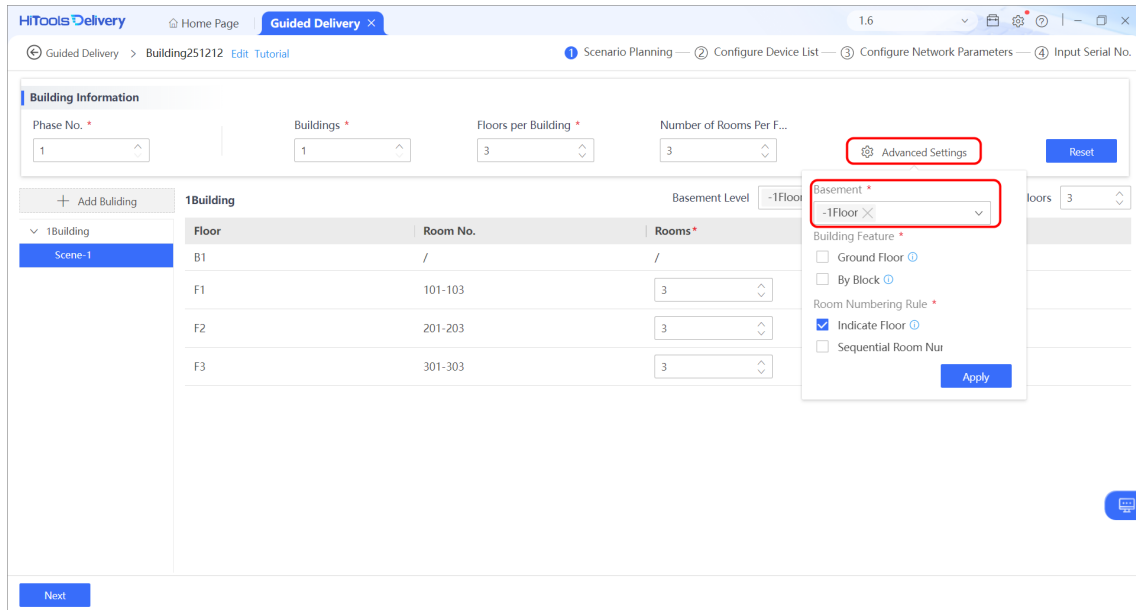


Figure 3-33 Select Basement Levels

- **Elevator Control Configuration:** The **Device Parameter Configuration** page now supports elevator control configuration for a main door station.

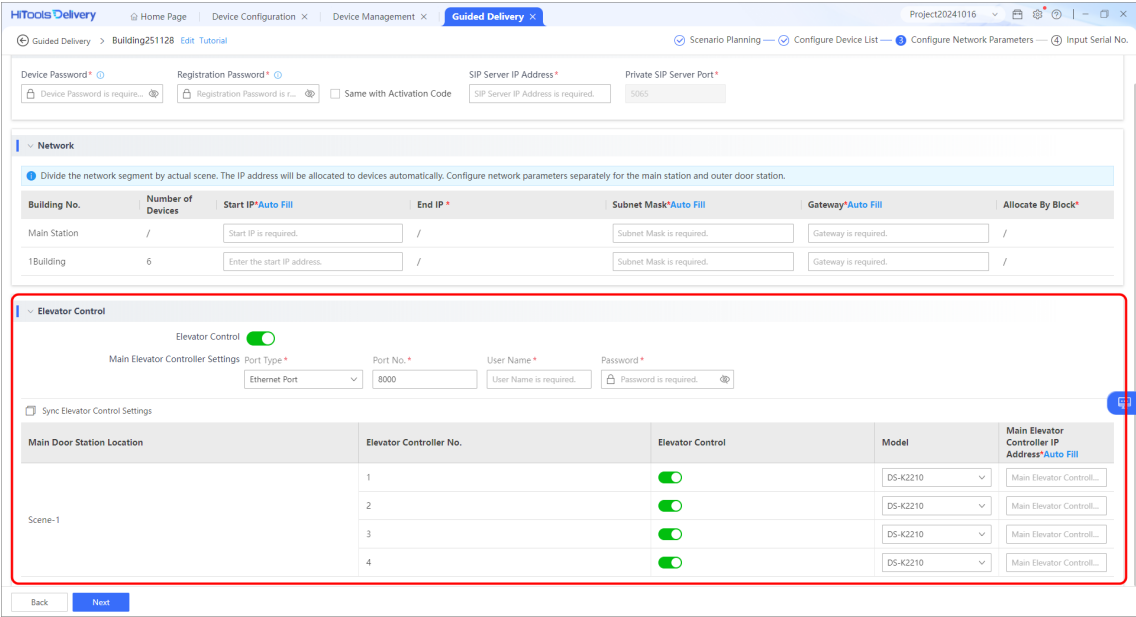


Figure 3-34 Elevator Control Configuration

- **Automatic End IP Calculation:** Introduce an **End IP** column, which automatically calculates the end IP address based on the number of devices in the current scene by default.
- **Auto Serial Number Discovery:** Support automatic matching of serial numbers for devices that have been activated and connected to the network.

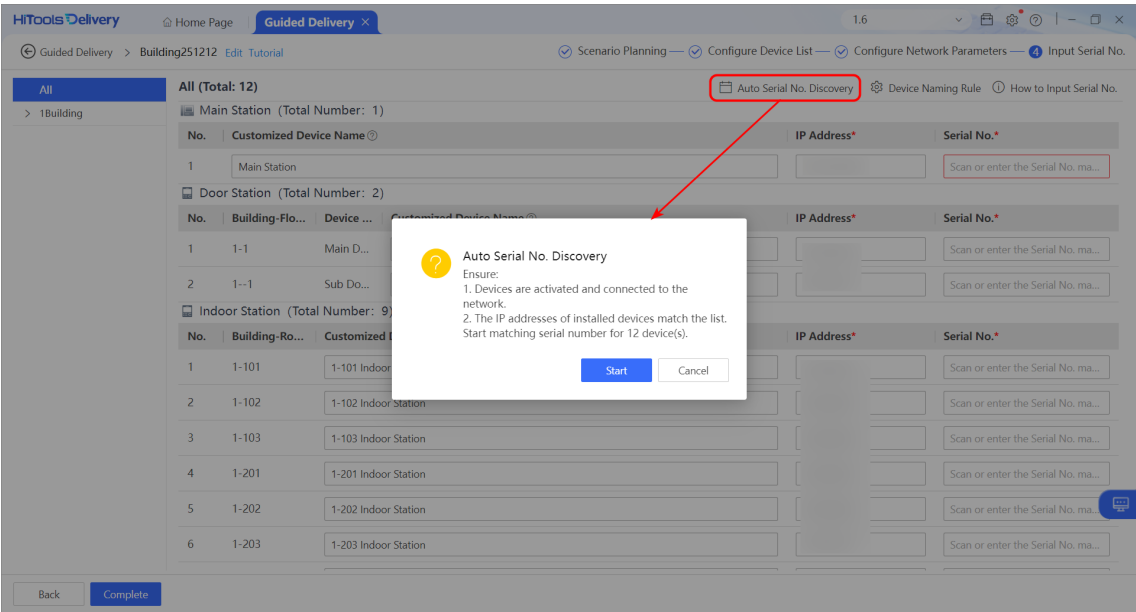


Figure 3-35 Auto Serial Number Discovery

- **Batch Device Naming Rule Modification:** Support for **batch modification** of the prefix of the customized device name.

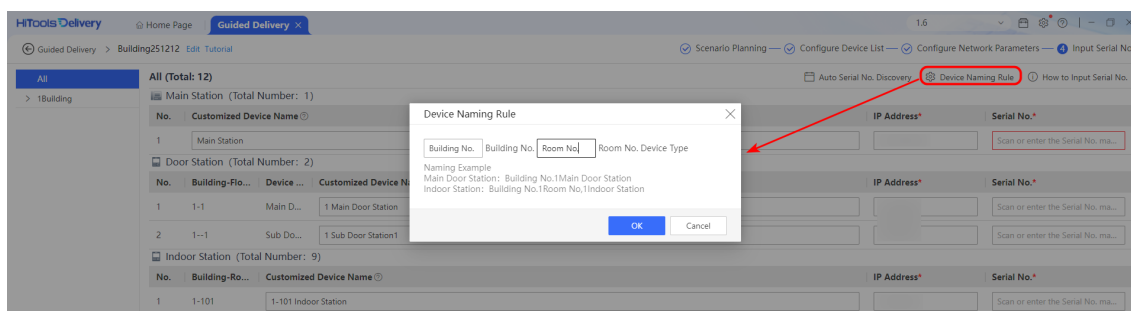


Figure 3-36 Device Naming Rule Setting

- **File Template Import Mode:** Introduce a **File Template Import Mode** that allows batch importing device settings via an Excel template, with the serial numbers to be manually entered in the tool.

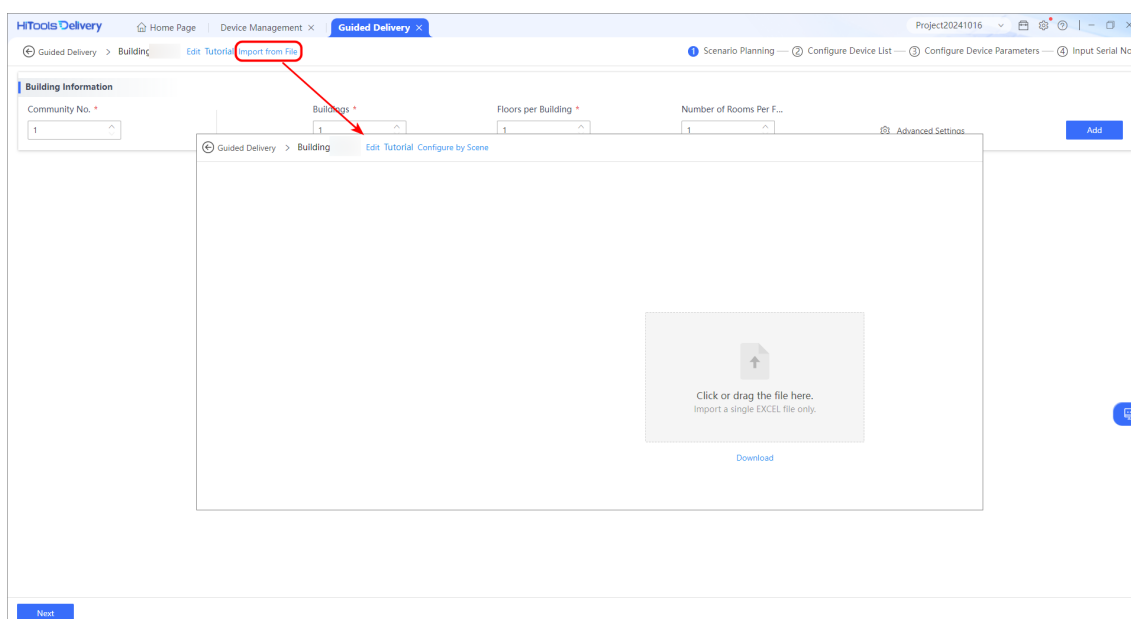


Figure 3-37 Import from File

3.6.4 Device Configuration

For on-street parking cameras, support batch configuration by copying a single device's web parameters to multiple devices.

3.6.5 Configuration Verification

- Support verifying the camera view (OSD/Picture Overlay) and PTZ performance in the Live View module.

Related Document: [Live View Verification](#)

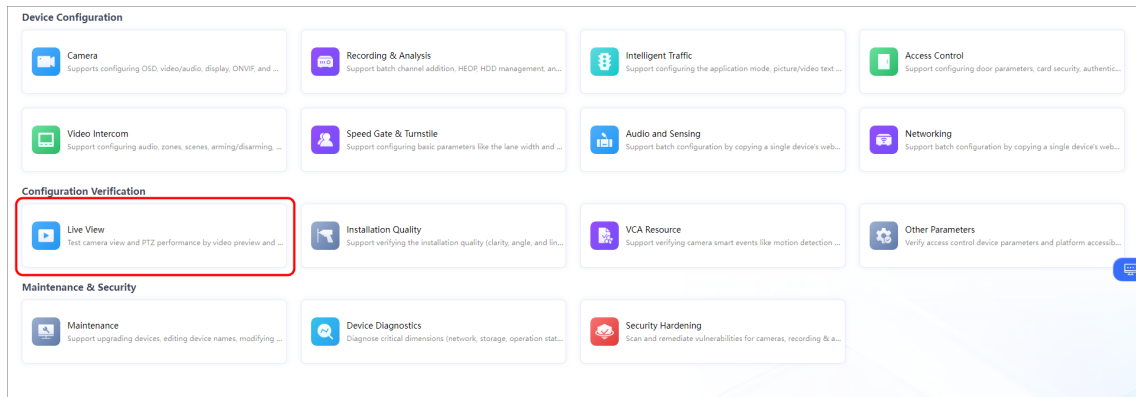


Figure 3-38 Live View Verification

- The **Traffic Camera Configuration Testing** tool have been relocated to the **Installation Quality** verification module.

Related Document: [Installation Quality Verification](#)

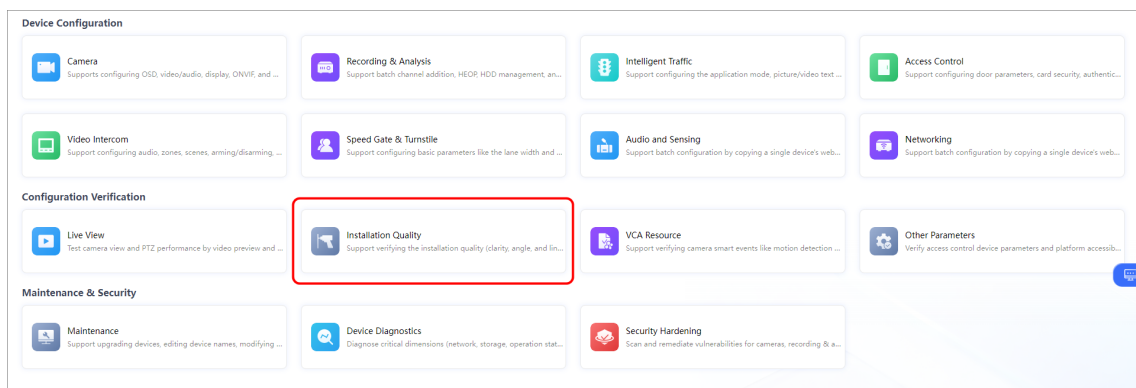


Figure 3-39 Installation Quality Verification

- Support verifying camera smart events like motion detection and intrusion detection, and other VCA resources like face picture capture in the VCA Resource module.

Related Document: [VCA Resource Verification](#)

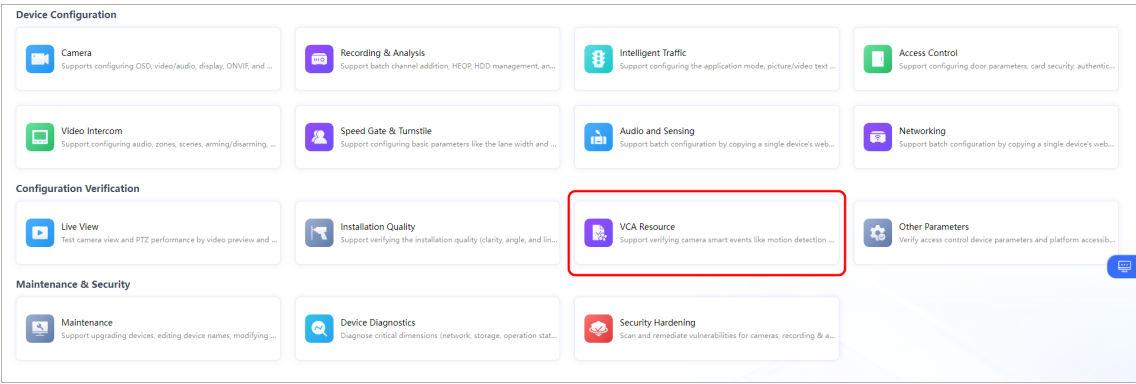


Figure 3-40 VCA Resource Verification

- Support verifying access control device parameters and platform accessibility for cameras and sensing devices like UWB anchors in the Other Parameters module.
- Related Document: **Other Parameter Verification**

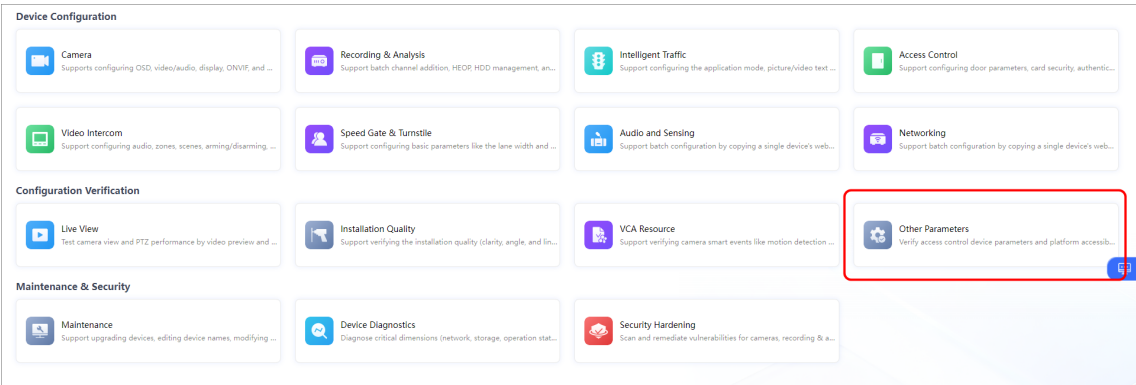


Figure 3-41 Other Parameter Verification

3.6.6 Maintenance

Updates	Related Document
The Refresh, Time Settings, Restart, Reset, Backup and Import , and SDK Protocol Compatibility Mode functions have been moved from the original Device Management interface to the Common module.	<u>Common Maintenance</u>
- Support automatic/manual detection of upgrade packages and display the upgrade detection status. - Optimize local and online upgrade processes. The upgrade execution method and the storage path for online upgrades have been moved to the upgrade settings. - Support displaying the overall and per-device upgrade progress.	<u>Upgrade Devices</u>
The IP Migration tool has been relocated to the Change IP module. From the Change IP interface, you can quickly jump to the IP Scanner to view available IPs. The devices in the template but not yet added to the device list can be automatically added.	<u>Change IP</u>
Support modifying device names in bulk by importing a template. The devices in the template but not yet added to the device list can be automatically added.	<u>Edit Name</u>
- Devices already added to the list and sharing the same password can be modified online. - Devices with inconsistent original passwords can be modified in bulk by importing a template.	<u>Change Password</u>

3.6.7 Device Diagnostics

Add a **Device Diagnostics Module** that allows users to batch check the health status and major parameters (network, storage, operation status, and more) of cameras and recording & analysis devices to identify potential risks.

Related Document: [Device Diagnostics](#)

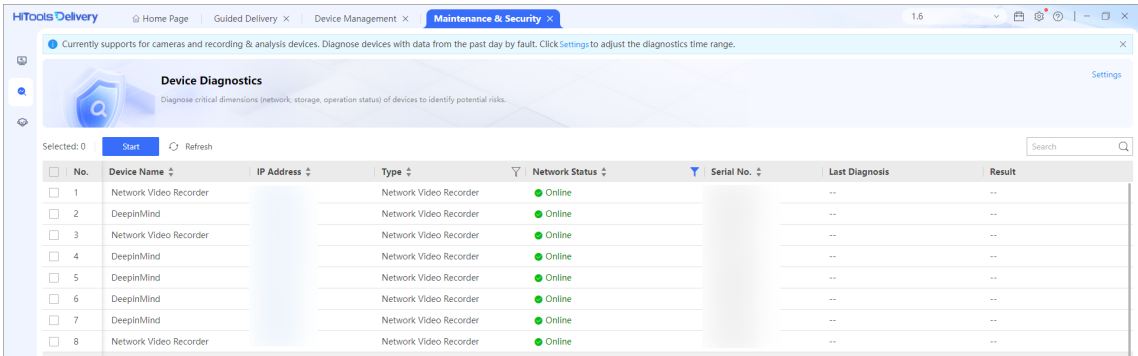


Figure 3-42 Device Diagnostics

3.6.8 Security Hardening

Add a **Security Hardening Module** that supports scanning and fixing vulnerabilities for cameras, recording & analysis devices, access control devices, video intercom devices, and more.

Related Document: [Security Hardening](#)

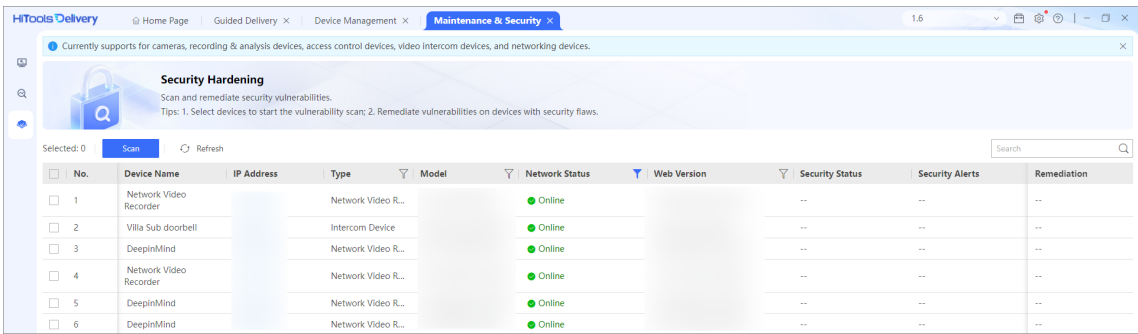


Figure 3-43 Security Hardening

3.6.9 System Settings

- Support setting the default start page and the software language.

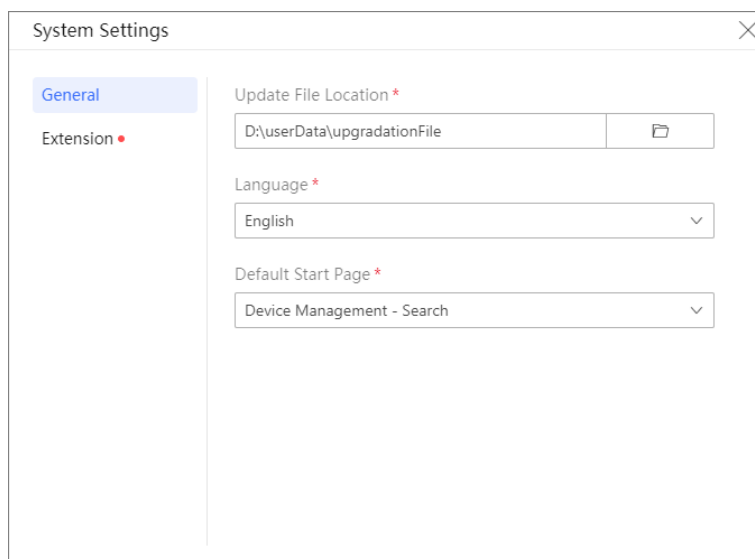


Figure 3-44 General Settings

- Support using your mobile browser to scan the QR code for extensions.

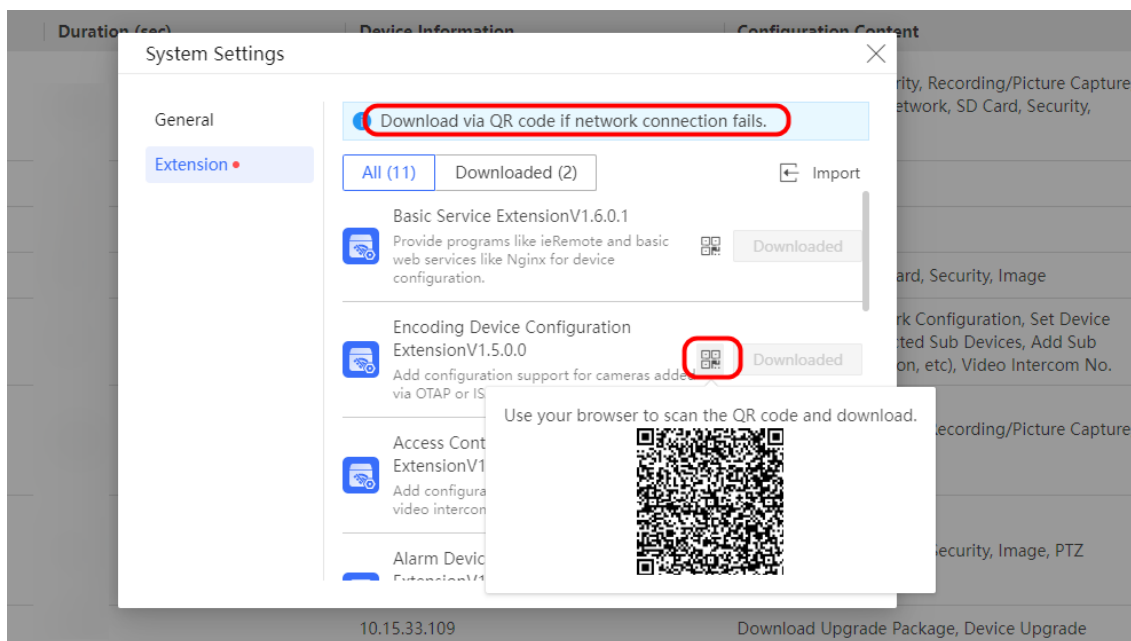


Figure 3-45 Download Extensions via QR Code

Chapter 4 Project Management

Before adding devices or designing your templates, create a project to manage your delivery task.

Note

- Up to 10,000 projects can be added.
- Deleted projects cannot be recovered. Back up your projects by exporting them before deletion.
- Project files from a newer version cannot be imported into an older version.
- Exported deliverables cannot be modified, and fields containing sensitive information are automatically encrypted.

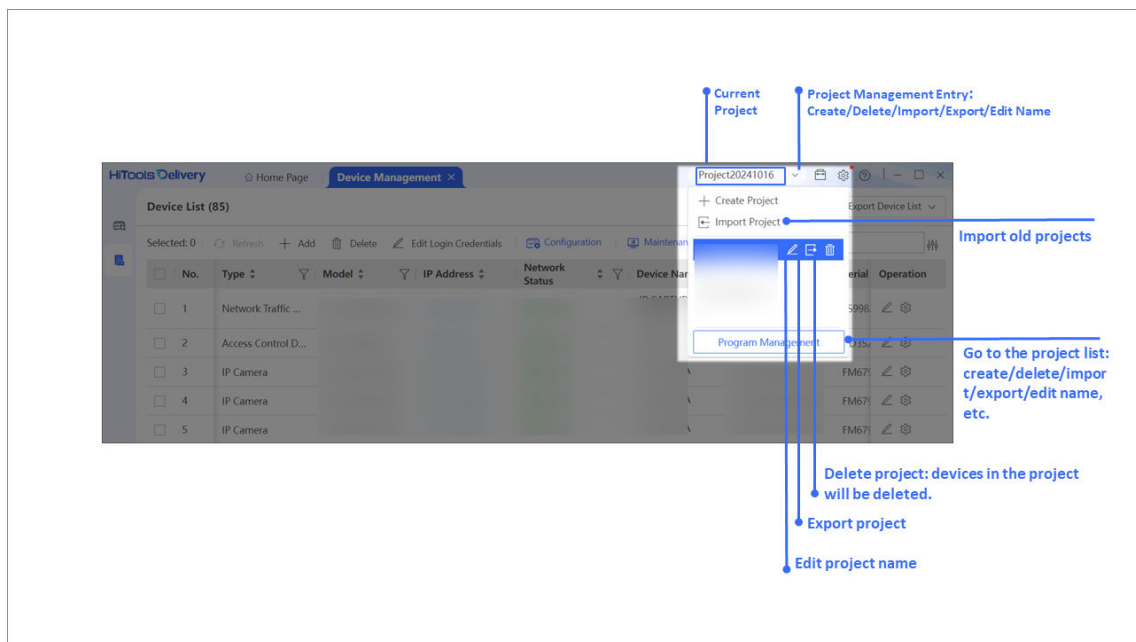


Figure 4-1 Project Management

Chapter 5 Device Management

- Add Devices
- Search for Devices on Other Subnets
- Activate Devices
- Reset Password

5.1 How to Add Devices

You can view online devices and add them to the device list. You can also add devices in various ways.



Caution

You can add up to 5,000 devices.

5.1.1 Add Devices on Same LAN

On the homepage, click **Search** to view devices within the same LAN as HiTools Delivery.



Note

- Up to 400 devices can be detected.
 - The device information will be refreshed automatically every 1 minute. You can also click **Refresh** to refresh the information.
 - If the device goes offline for more than 3 minutes, the information will be removed from the list automatically.
-

1. Select **unactivated devices** and activate them.
2. Select devices to perform the following operations:
 - Configure device network parameters .
 - Reset device passwords.
 - Configure the cloud service (device binding).
3. Check the online activated devices you wish to add, then click **Add to Device List** at the bottom-left.

5.1.2 Manually Add Devices

1. Select **Device Management**.
2. Select a adding method and add devices.

Table 5-1 Adding Methods

Scenario	Adding Methods	Steps
Your devices share the same IP segment and are associated with a single user name and password.	IP Segment	- Select Add → IP Segment. - Enter the start IP address, end IP address, HTTP port, user name, and password. - Select OK.
Have the IP address, password, user name, and port No.	IP	- Select Add → IP. - Enter the IP address, HTTP port, user name, and password. - Select OK.
You have a large number of devices.	Batch Import (CSV/ EXCEL)	- Select Add → Batch Import. - Select Export to export the template. - Import the configured template. - Select OK.

5.1.3 Follow-Up

Table 5-2 Follow-Up Operations

Operation	Description
Filter Devices	In the device list or device search results, click the filter icon next to fields such as device type or model to refine your selection.
Batch Edit Device Login Credentials	On the device list page, click Edit Login Credentials to modify the user name and password for multiple devices at once.
Configure or Maintain Devices	After adding devices, go to the device list page and click Configuration or Maintenance to quickly access batch configuration and maintenance interfaces.
Export Device List for Maintenance or Platform Integration	In the upper-right corner of the device list or device search results, click Export Device List , choose the export format, and download a device inventory for maintenance purposes.

Operation	Description
	Click HikCentral Professional to bulk import the exported devices into the platform.

5.1.4 How-To Video

Video Link	Main Content	Video QR Code
<u>Add Devices</u>	• Introduction to adding methods. • How to batch add devices with an EXCEL template.	

5.2 How to Search for Devices on Other Subnets

In most device installation and maintenance scenarios, devices are often distributed across different network segments. For example, cameras may use 192.168.1.X, access control devices 192.168.2.X, and NVRs 192.168.3.X. Cross-network segment scanning enables quick discovery and centralized management of all powered-on and networked devices, improving maintenance efficiency.

1. On the Device Search page, click **Other Subnets**.
2. Enter the starting IP of the target segment. The ending IP will be auto-filled but can be modified if needed. For example, entering **192.168.1.0** will auto-fill **192.168.1.254**.
3. Click **Add IP Segment** to include additional segments. New segments will auto-increment based on the previous one (e.g., if the prior segment is **192.168.2.0**, the next will show **192.168.3.0** and can be adjusted manually).
4. (Optional) Enter the device user name and password, then click **Search**.

Note

Without a username and password, only certain cameras will display basic information (IP, Model, SN, Gateway, SDK Port, and HTTP Port).

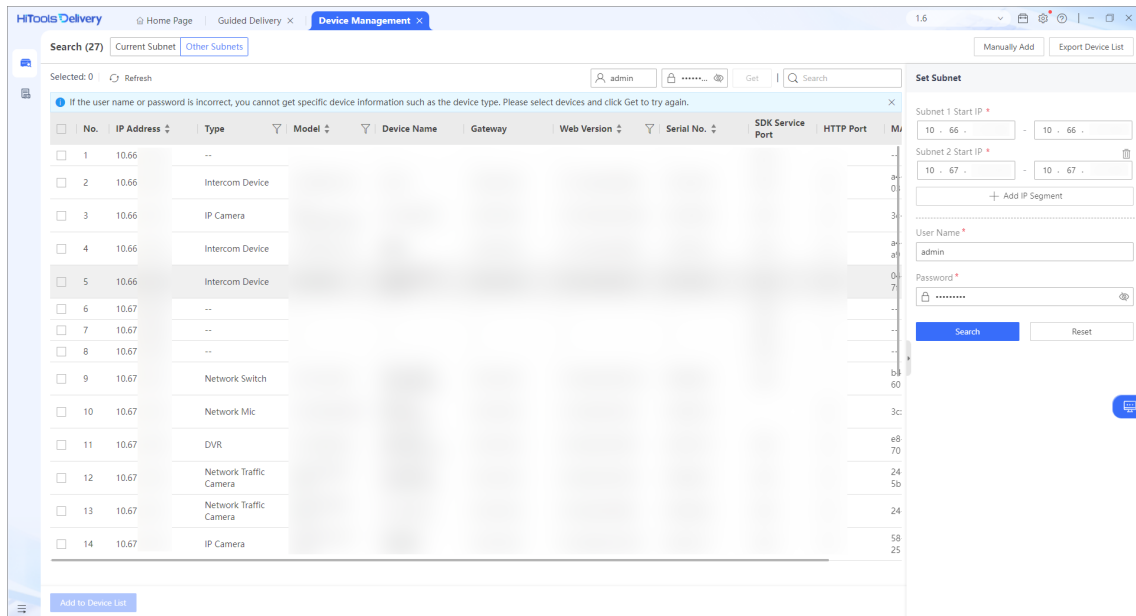


Figure 5-1 Search for Devices on Other Subnets

5. Select the devices to add, click **Device Authentication**, enter the correct username and password, and click **OK**. Detailed device information will be displayed upon successful authentication.
6. Check the desired devices and click **Add to Device List** at the bottom left.

5.3 How to Activate Devices

To enhance the security of data and operations, activate your devices in advance.

1. In the Online Device List, select devices that are not activated.
2. Enter the new password and confirm the password.



Note

For NVRs, you should set the default password to add channels.

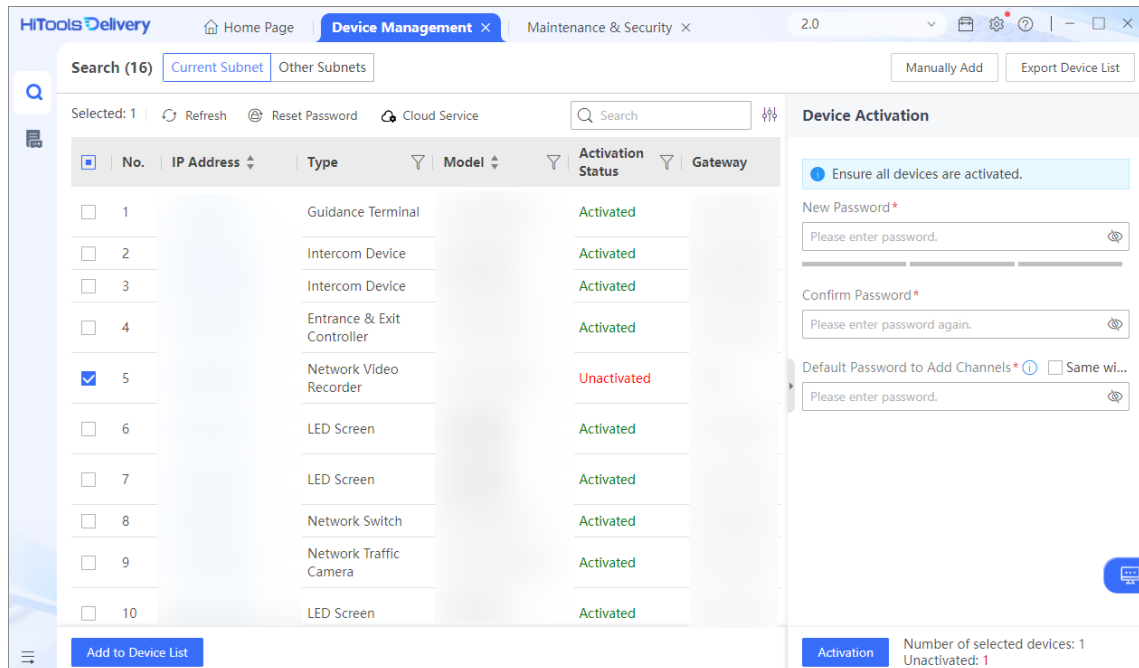


Figure 5-2 Set Default Password to Add Channels

3. Select **Activate**.

Note

You should export the GUID file, set the security questions, or set the email account when you activate your devices.

5.4 How to Reset Passwords

Note

For cameras and recording & analysis devices manufactured before 2015, the password will be reset to 12345.

1. In the Device Search module, select devices and select **Reset Password**.
2. Select a method to reset your password.
 - Batch Reset

Note

- XML and QR Code methods only support batch resetting to the same password. To set unique passwords for multiple devices, use the EXCEL method.
- Resetting via Excel is available only when you selecting more than 30 devices.
- Resetting via QR Code is only supported by certain devices.

- **EXCEL**

Recommended for resetting **more than 30 devices**. Export the EXCEL file and send it to Technical Support. Fill in the returned file (containing security codes) with your new passwords, then upload it.

- **XML**

Export the XML file and send it to Technical Support. Place all decrypted XML files received into a single folder, import the folder, and set the new password.

- **QR Code**

a. Log in to Hik-Partner Pro and scan the QR code to get the reset code.

i. Go to **Toolkit → Online Support Case → Device Password Reset** .

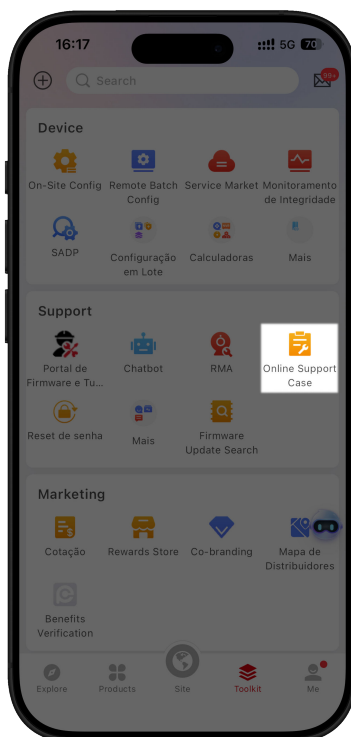


Figure 5-3 Request Online Support Case of Password Resetting

ii. Click  for each device and scan the QR code via Hik-Partner Pro to fill out the device feature code and serial number.

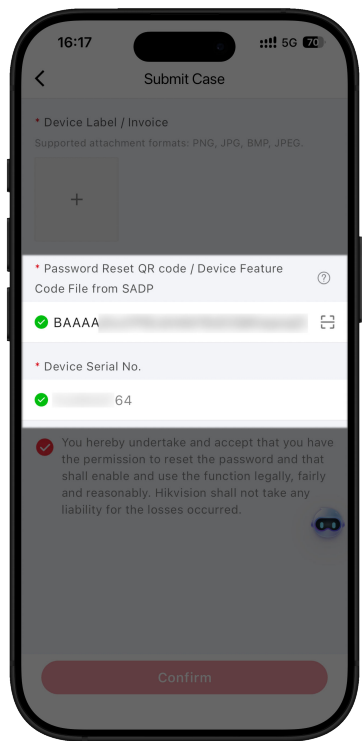


Figure 5-4 Complete Online Case

- iii. Upload a photo of the device label and click **Confirm** to submit the case. Then, wait for the reset code.
- b. Enter the reset code and your new password.
- Reset Single Device's Password

Table 5-3 Password Reset Method

Methods	Description	Steps	Note
Import/ Export Key	Import the key request file and contact our technical support team for the key to reset the password.	XML File a. Click Export File and save the key request file (XML file) to your PC. b. Send the request file to our technical support team. c. Import the key file received from our technical support team to reset the password. d. Enter the reset code and your new password. QR Code	QR code scanning is supported by certain devices.

Methods	Description	Steps	Note
		- Click Generate QR Code. - Log in to Hik-Partner Pro and scan the QR code to get the reset code. - Go to Toolkit → Online Support Case → Device Password Reset. - Click  for each device and scan the QR code via Hik-Partner Pro to fill out the device feature code and serial number. - Upload a photo of the device label and click Confirm to submit the case. Then, wait for the reset code. - Enter the reset code and your new password.	
GUID	For devices supporting GUID such as NVRs and DVRs, import the GUID file to reset the password.	- Click  to select the GUID file you have exported when activating device. - Reset and confirm the new password.	Ensure that you export GUID files when activating your devices.
Security Question	Answer the security questions to reset the password.	- Answer the security questions. - Reset and confirm the new password.	Ensure that you set security questions when activating your devices.
Email	Get an email verification code to reset the password.	(Optional) If you set the SADP mode to Discovery Only in the Service & Security module, enter the full registered email address and click Verify. Once verified, follow the steps below to reset the password. - Click Save or Export XML to download the QR code or XML file to your local PC and then send it to the specified Email address. - Go to the Email for the verification code. - Reset and confirm the new password.	Ensure that you set an Email address when activating your devices.

5.5 How to Group Devices

Group devices by physical hierarchy (e.g., building, floor, or room) to streamline management for large-scale projects. This enables independent configuration of deployment and upgrade plans per group, eliminating manual filtering. A hierarchical spatial view provides an intuitive status overview, replacing disorganized flat lists. Additionally, grouping supports phased delivery and accelerates troubleshooting by pinpointing fault areas quickly.

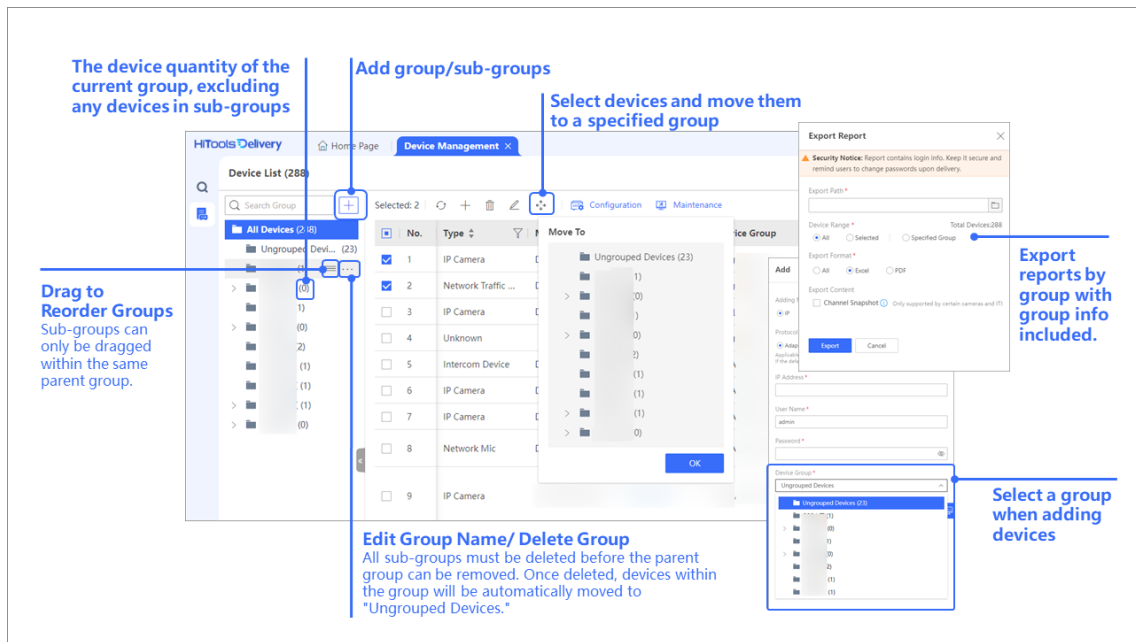


Figure 5-5 Device Grouping Overview

Note

- Add up to 5 levels of sub-groups.
- Add up to 100 sub-groups per group.

5.6 How to Preview and Download Channel Snapshots

After installing and configuring devices (such as cameras, access control, video intercoms, and ITS), preview and download snapshots to ensure they are correctly installed and operating normally.

Note

This feature should be supported by devices.

1. Select devices that support channel snapshot preview and click in the Operation column.

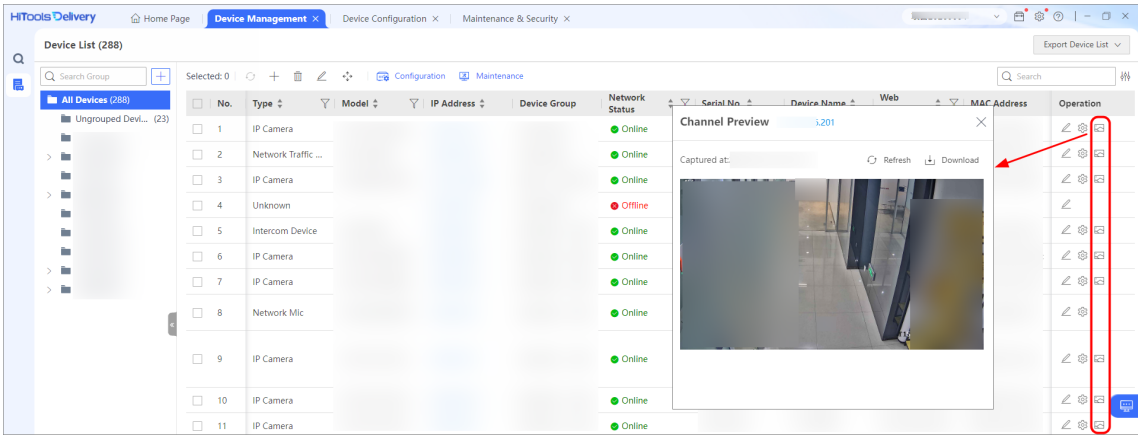


Figure 5-6 Channel Snapshot

2. Preview the snapshot. You can view the timestamp, refresh the image, and download it (PNG format) to your local folder.

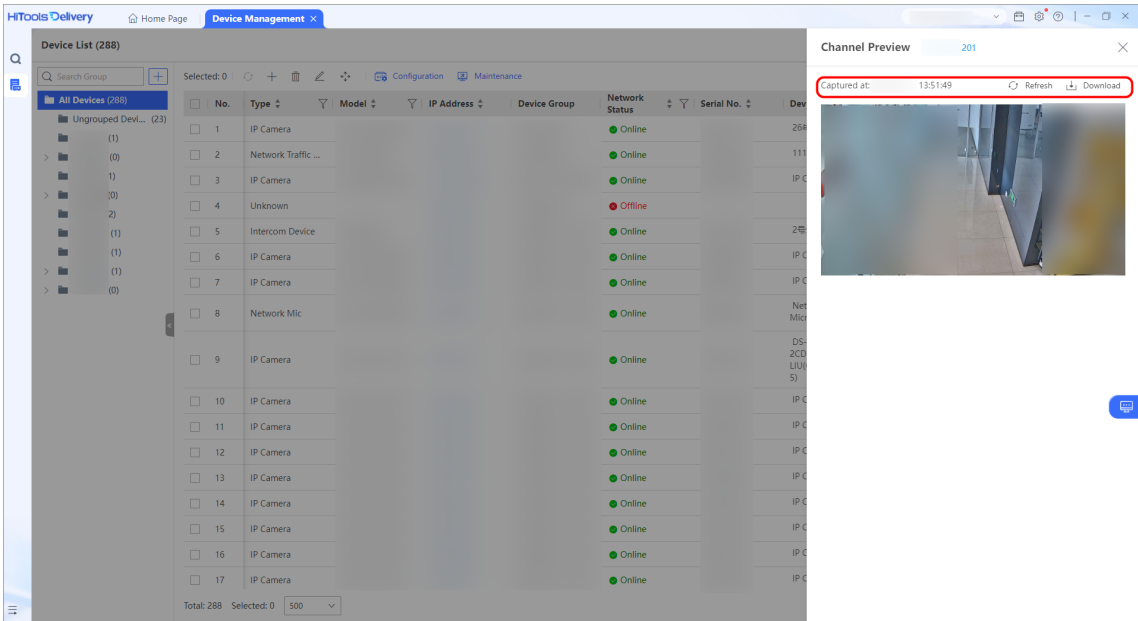


Figure 5-7 Preview/Download Snapshots

Note

For multi-channel devices, only the preview and download of **Channel 1** are supported.

3. (Optional) For certain cameras and ITS devices, click **Export Device List** → **Export Report** in the top-right corner to choose whether to export channel snapshots.

Note

For multi-channel devices, only the snapshot **Channel 1** will be exported.

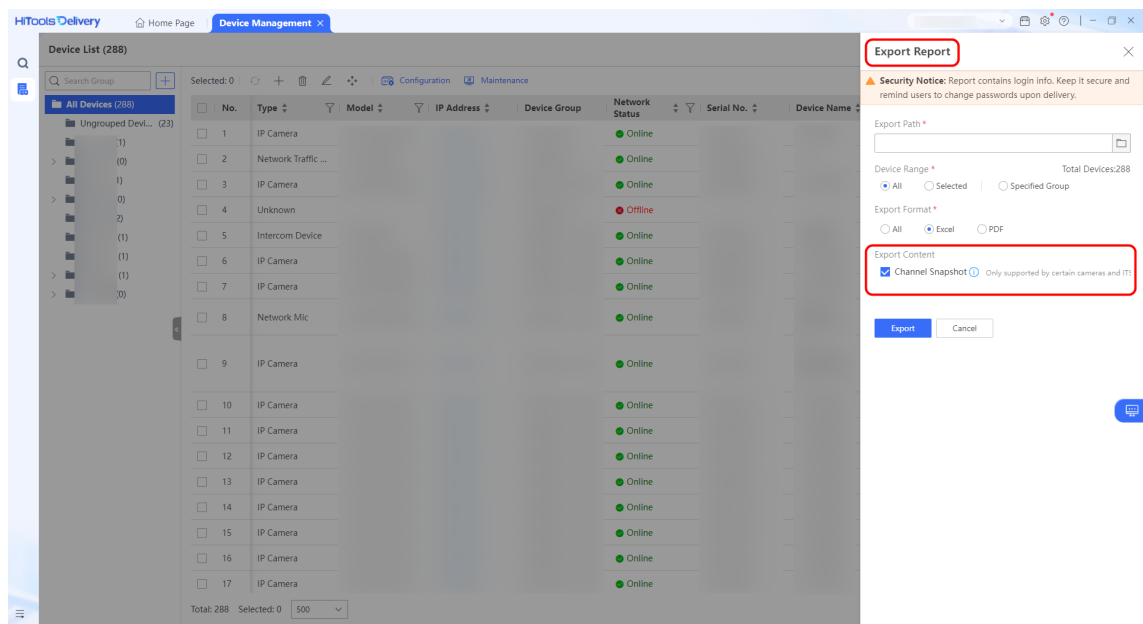


Figure 5-8 Export Channel Snapshots

Chapter 6 Guided Delivery

6.1 Introduction

In large projects, delivery personnel such as installers, service providers, integrators, and technical support can create a pre-configuration template to plan the device parameters in advance based on on-site investigation. Once the devices are powered on and connected to a network at an installation site, the pre-configured parameters can be delivered with a single click.

6.2 How to Create Template

Scenario	Description
Add your first template.	In the Guided Delivery module, select Go to enter the guided delivery page. Select a template and click Create .
You have added templates.	In the Guided Delivery module, select Go to enter the guided delivery page. Select a history template at the bottom of the page.
Delivery Personnel A finished part of the pre-configuration task, and Personnel B will continue the on-site work by importing A's config file into their HiTools Delivery.	In the Guided Delivery module, select Go to enter the guided delivery page. Select a historical template at the bottom of the page. Select Import Template to import a configured template for data transfer.

6.3 Specifications

- Create/Import up to 100 templates.
- Apply parameters to a maximum of 2,000 devices in a camera template and entrance & exit template.
- Apply parameters to a maximum of 5,000 devices in a video intercom template.

6.4 Supported Templates

- **Video Intercom Template**
- **Entrance & Exit Template**
- **Camera Template**

6.5 How to Configure Video Intercom Template

6.5.1 Scenario

When delivering projects in places like residential compounds, you need to manage a large number of main stations, door stations, and indoor stations. To improve efficiency in on-site delivery, you can configure device parameters and building information, and activate devices in advance.

6.5.2 Overall Configuration Process

Configure by Scene

Table 6-1 Overall Process

Step	Description
Step 1: Set the Building Information	Set the building information, including the community number, the number of buildings, units (blocks), basement levels, and floors.  Note If device parameters such as IPs are pre-planned in Excel, you can simply import the file, input the serial number, and apply all parameters.
Step 2: Adjust the Device Quantity	After the building information is configured, a device list will be displayed. You can adjust the device quantity as needed.
Step 3: Configure Device Parameters	Configure parameters such as the activation code, register code, SIP server IP, device IP address, and elevator control.
Step 4: Input the Serial No.	- Check and edit the device's customized name and IP address. - You can automatically match the serial number or manually scan it. If you use the mobile scanning tool, it is recommended to connect your computer to your phone hotspot. If the computer's network changes, refresh the QR code or switch the Ethernet card.
Step 5: Activate Devices and Connect Them to a Network; Apply Parameters to Devices.	- Connect main stations, main door stations, or outer door stations to the same VLAN as your computer, and activate online devices. - Connect your computer to the same LAN as devices and apply parameters to online devices. After parameters are applied, the

Step	Description
	parameters of indoor stations and sub door stations will be applied to the corresponding main door stations, and all video intercom devices' parameters will be applied to the main station.

Import from File

Refer to ***Import from File*** .

Table 6-2 Overall Process

Step	Description
Step 1: Import Device Info File	If you have planned device parameters such as IPs in Excel, you can simply import the file, input the serial number, and apply all parameters.
Step 2: Input the Serial No.	• Check and edit the device's customized name and IP address. • You can automatically match the serial number or manually scan it. If you use the mobile scanning tool, it is recommended to connect your computer to your phone hotspot. If the computer's network changes, refresh the QR code or switch the Ethernet card.
Step 3: Activate Devices and Connect Them to a Network; Apply Parameters to Devices.	• Connect main stations, main door stations, or outer door stations to the same VLAN as your computer, and activate online devices. • Connect your computer to the same LAN as devices and apply parameters to online devices. After parameters are applied, the parameters of indoor stations and sub door stations will be applied to the corresponding main door stations, and all video intercom devices' parameters will be applied to the main station.

6.5.3 Steps

Step 1: Set the Building Information

1. Configure the building information such as the number of buildings.

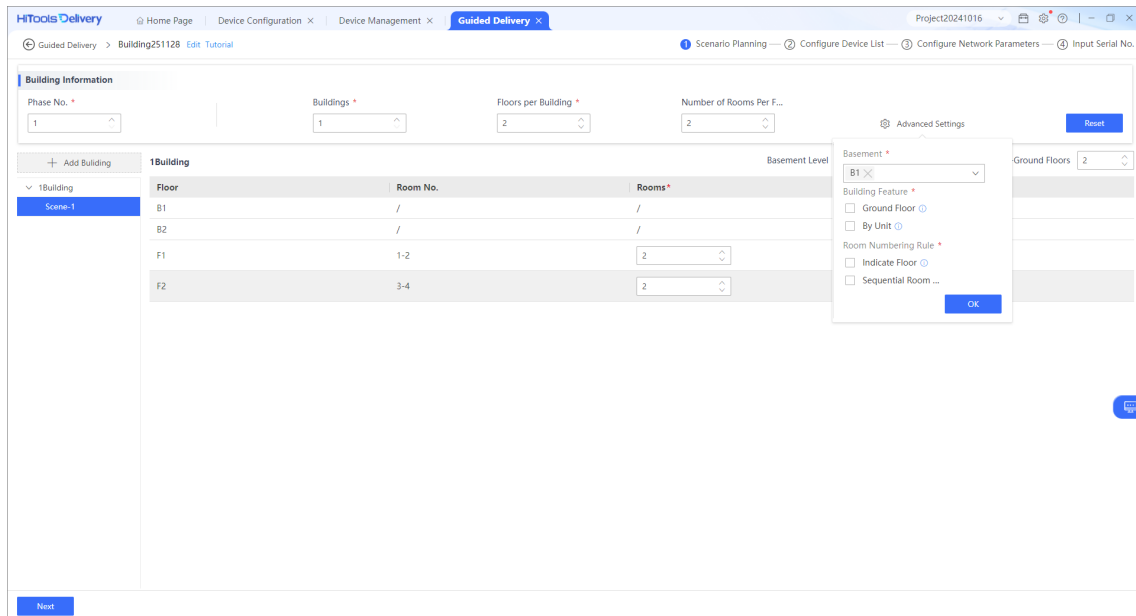


Figure 6-1 Scenario Planning

2. (Optional) Click **Advanced Settings** to adjust basement floors and modify room numbering rules based on actual floor and room arrangements.

Type	Building Information	Room No. Example
Consecutive Number & Indicate Floor	1 Building / 2 Units per Building / 2 Floors per Unit / 2 Rooms per Floor	- Unit 1-1 / 1st Floor: 101-102 - Unit 1-2 / 1st Floor: 103-104
Non-Consecutive Number & Indicate Floor	1 Building / 2 Units per Building / 2 Floors per Unit / 2 Rooms per Floor	- Unit 1-1 / 1st Floor: 101-102 - Unit 1-2 / 1st Floor: 101-102

3. Select **Add**.
4. (Optional) Adjust the number of rooms and units or edit the unit No. as needed. For example, If the first floor is used as commercial areas, you can set the number of rooms to **0**.

Note

The unit No. should be a number from 0 to 20.

5. Select **Next**.

Step 2: Adjust the Device Quantity

Adjust the device quantity as needed and select **Next**.

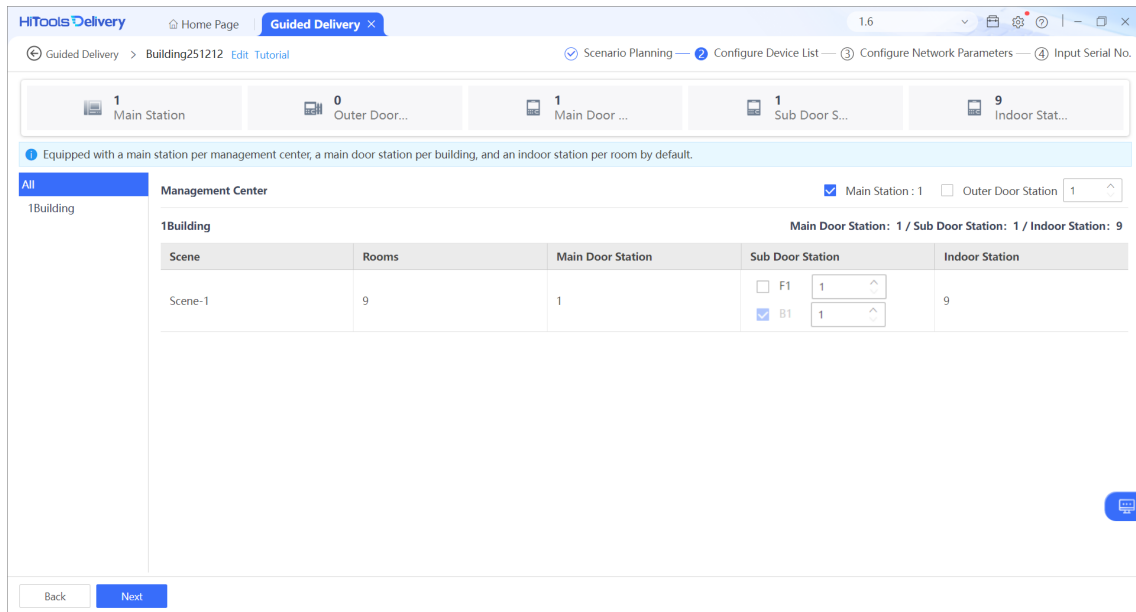


Figure 6-2 Adjust Device Quantity

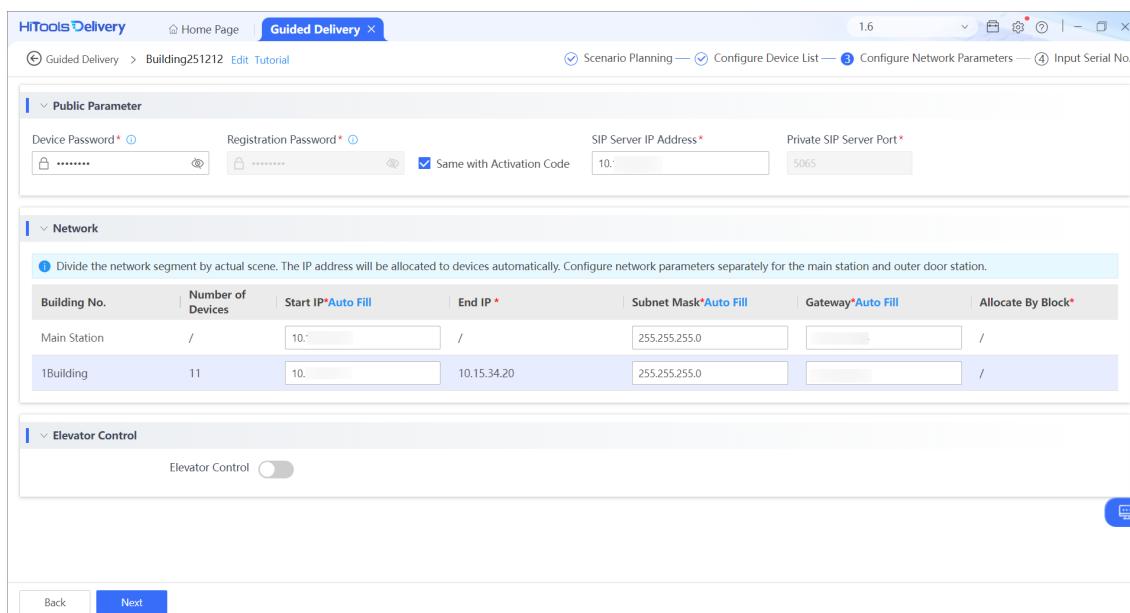
Table 6-3 Device Quantity

Device Type	Quantity
Main Station	1 main station by default. You can uncheck Main Station if no main stations are needed.
Outer Door Station	Up to 10 outer door stations per community. This is unchecked by default. You should select main stations if outer door stations are needed.
Main Door Station	Each unit is equipped with a main door station. This value CANNOT be edited.
Sub Door Station	- If a unit has multiple entrances, you can configure multiple sub door stations. - For underground entrances—such as those from a parking garage—you can independently adjust the number of sub door stations assigned to basement levels.

Device Type	Quantity
	 Note Within a single unit, up to 10 sub door stations can be added for above-ground floors. For underground floors, up to 10 sub door stations can be added per floor.
Indoor Station	Each room is equipped with an indoor station. This value CANNOT be edited.

Step 3: Configure Network Parameters

Configure public parameters, network parameters, and elevator control settings, and select **Next**.



The screenshot shows the 'Configure Network Parameters' step in the HiTools Delivery web interface. The interface is divided into three main sections: Public Parameter, Network, and Elevator Control.

Public Parameter Section:

- Device Password * (password field)
- Registration Password * (password field)
- ☒ Same with Activation Code
- SIP Server IP Address * (text field: 10.)
- Private SIP Server Port * (text field: 5065)

Network Section:

Divide the network segment by actual scene. The IP address will be allocated to devices automatically. Configure network parameters separately for the main station and outer door station.

Building No.	Number of Devices	Start IP*Auto Fill	End IP *	Subnet Mask*Auto Fill	Gateway*Auto Fill	Allocate By Block*
Main Station	/	10.	/	255.255.255.0		/
1Building	11	10.	10.15.34.20	255.255.255.0		/

Elevator Control Section:

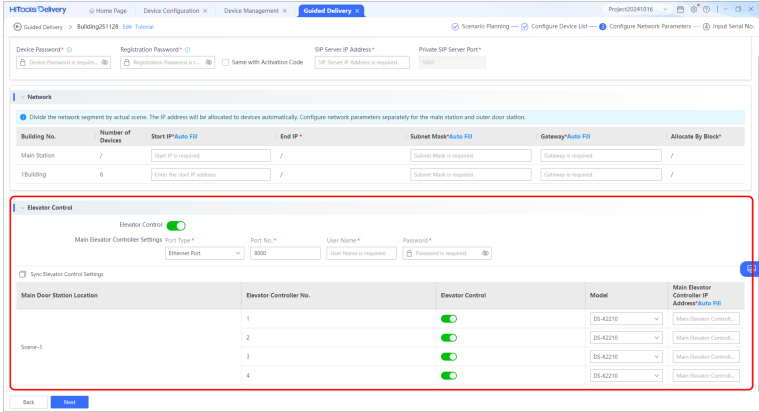
- Elevator Control (toggle switch)

At the bottom of the interface, there are 'Back' and 'Next' buttons.

Figure 6-3 Configure Device Parameters

Table 6-4 Device Parameters

Parameter	Description
General Parameters	- Register Code: The password for indoor stations/sub-door stations to register with the main door stations /main stations and to facilitate mutual communication. You can select Same with Activation Code. - Activation Code: The password for activating all video intercom devices. - SIP Server IP: The SIP server can enable two-way intercom, group calls, and other functions. Generally, the SIP server IP address is the same as the main station's IP address.
Network Parameters	- The start IP address refers to the IP address of the main door station of the building/block. The IP addresses of the sub door stations and indoor stations will be sequentially assigned starting from the start IP address.  Note The end IP address will be automatically calculated based on the number of devices. - For buildings with multiple blocks, floors or rooms per floor, it is recommended to enable Allocate by Block to assign network parameters by block to avoid issues like insufficient IP address resources. - If IP addresses, gateways, and sub masks are consistent or partially consistent, select Auto Fill, select or enter a value, and apply it across rows.  Caution If you select Auto Fill, existing data will be overwritten.
Elevator Control	After enabling, set the port type of the main elevator controller (connection method to the main door station). Based on the number of elevators in the unit, enable elevator control and select the main elevator controller model and IP address (Ethernet port).

Parameter	Description
	 Figure 6-4 Elevator Control Settings  Note You can click Sync Elevator Control Settings to set the elevator control model and enable the number of elevator controls. Parameters will be synchronized to all building units.

Step 4: Input the Serial No. and Mark the Installation Location on the Device Packaging

After successful entering the device serial number, mark the installation location on the device packaging to avoid errors during device assignment and installation.

Use Mobile Scanning Tool

1. Ensure that your phone is in the same LAN as your computer. It is recommended to connect your computer to your phone's hotspot.
2. Use **your phone's camera or the scan function in the browser** to open the scanning tool and scan the serial No.

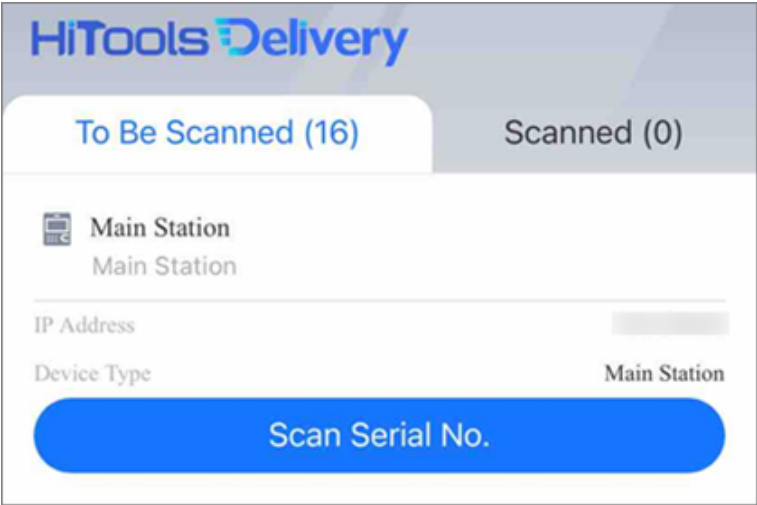
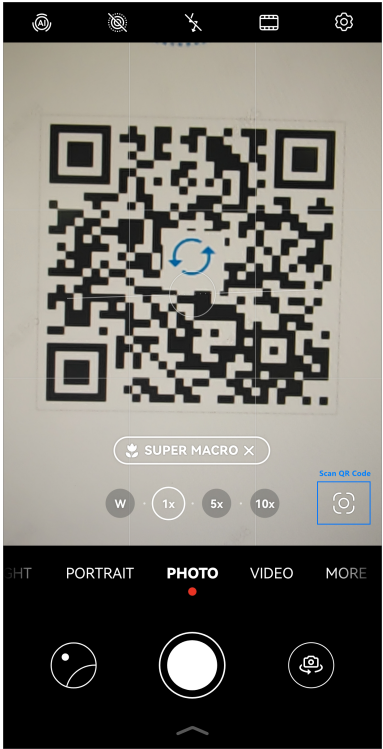


Figure 6-5 Scanning Tool Interface

Phone OS	How to Use Scanning Tool
iOS	Scan the QR code with your phone's camera. After scanning, you will see a notification with a link. Tap that link, and it will open the scanning tool for you.
Android	Use the scan function in your browser or the built-in QR code scanning feature on your phone to scan the QR code.
Harmony	Use the scanning feature of the camera to scan the QR code. After scanning, it will take you straight to the scanning tool.

Phone OS	How to Use Scanning Tool
	The image is a screenshot of a smartphone camera interface. At the top, there is a status bar with various icons. The main view is a camera lens with a QR code scanner overlay. The QR code is in the center, and a blue circular arrow icon is overlaid on it. Below the QR code, there is a 'SUPER MACRO X' button. To the right of this button is a 'Scan QR Code' button with a magnifying glass icon. Below these buttons are zoom options: 'W', '1x', '5x', and '10x'. At the bottom, there is a row of camera modes: 'PHOTO', 'VIDEO', and 'MORE'. The 'PHOTO' mode is selected, indicated by a red dot. Below the modes are three large circular buttons: a shutter button, a flash button, and a gallery button. Figure 6-6 Harmony V4.0.0 Camera Interface

3. Mark the installation location on the device packaging.

Automatic Serial No. Discovery

If the device has been activated, connected to a network, installed, and its IP address matches the list, click **Auto Serial No. Discovery** → **Start** to automatically fill in the device serial number.

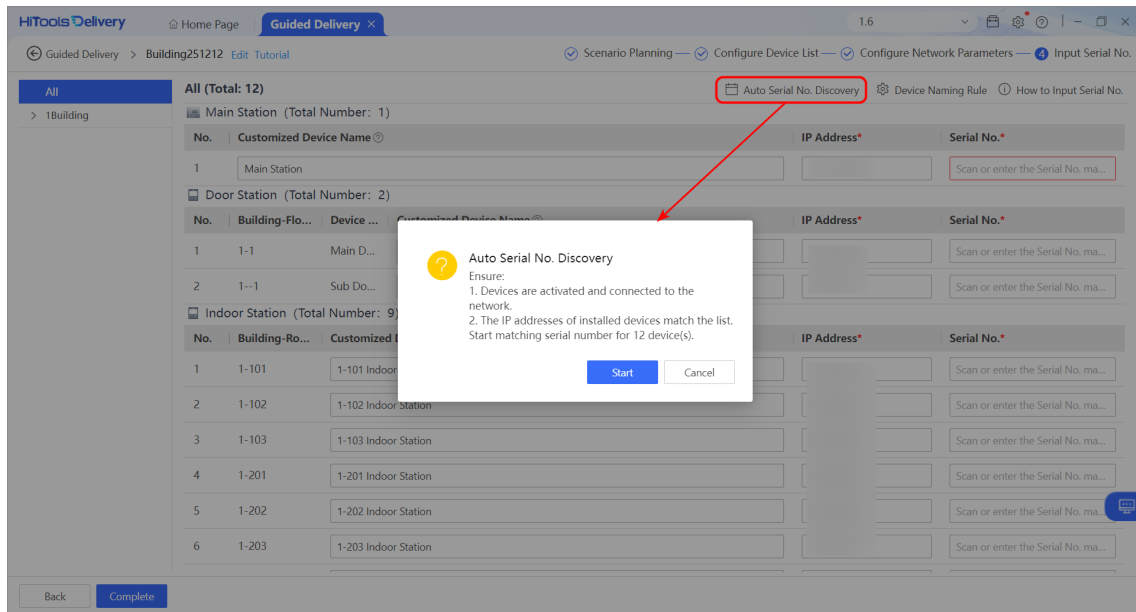


Figure 6-7 Auto Serial Number Discovery

(Optional) Step 5: Activate Devices and Connect Them to a Network

Scenario	Steps
- Devices arrive on-site in batches. - Some devices have been activated, networked, and installed on the corresponding floors, while only a few others need to be activated and networked. - With a large number of devices and a limited number of switch cables available, activate the devices in batches.	To ensure HiTools Delivery can detect devices, connect main stations, main door stations, or outer door stations to the same VLAN as HiTools Delivery, and select Activate & Connect .
Main stations, main door stations, and outer door stations have been activated and networked, and their IP addresses and serial numbers are consistent with the network information configured in the HiTools Delivery in Step 3 . If the information is inconsistent, parameters cannot be applied.	Select Skip .

Step 6: Apply Parameters to Devices

- To ensure your devices remain online with matched network information for seamless communication, login, and configuration, connect main stations, main door stations, outer door stations, and your computer to the same LAN.

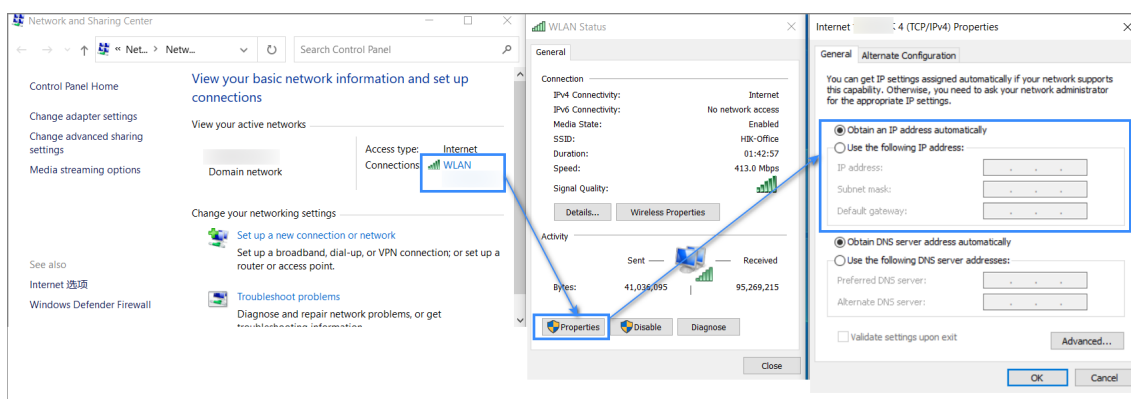


Figure 6-8 How to Edit Computer's IP Properties

2. Select **Apply**. After parameters are applied, the parameters of indoor stations and sub door stations will be applied to the corresponding main door stations, all video intercom devices' parameters will be applied to the main station.



Note

If parameters are not applied after troubleshooting, take the following steps:

- Select **Export** on the upper right corner to export the EXCEL configuration file and copy all the four sheets.

[illegible]

Figure 6-9 Exported Device Info

- b. Go to the main station's web configuration page to download the device template, paste the copied sheets in the template, and import it to the device web configuration page.

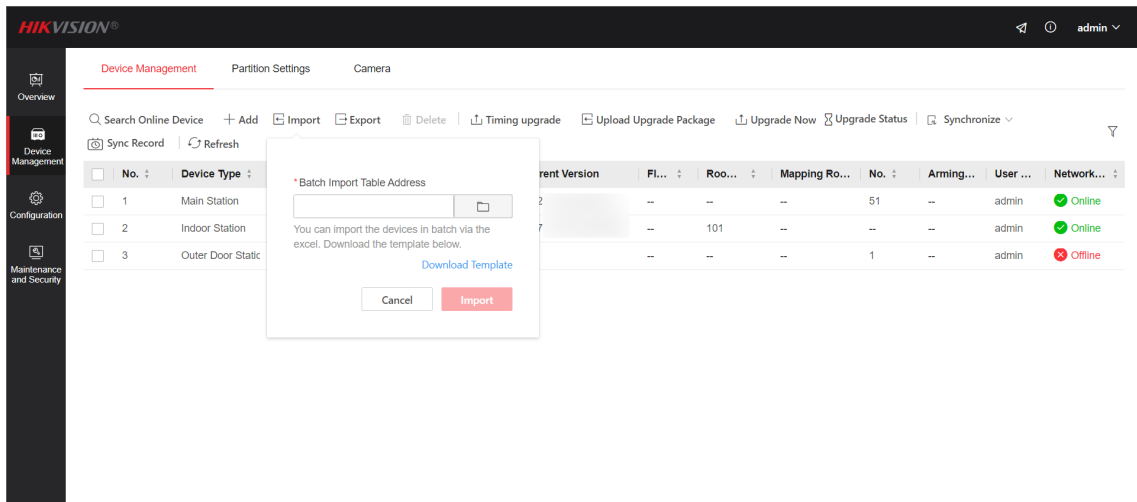


Figure 6-10 Main Station Web Configuration Page

3. Select **Go to List** to check configured devices in the Device List and go to the device's web configuration page for more information.

Import by File

If you have planned device parameters such as IPs in Excel, you can simply import the file, input the serial number, and apply all parameters on HiTools Delivery.

1. **Enable Import Mode:** Navigate to `\HiToolsDelivery\userData\config` and locate the `configDataFile`. Update the setting `isShowBITemplateFileModeSwitch` from `false` to `true` and save the file.

```
1 {
  "globalSetting": {
    "firstOpen": false,
    "isAutoDetection": false,
    "ignoreVersion": "",
    "deviceShowPage": "close",
    "hasFirstSearchOpen": true,
    "firstUpgradeSearch": false,
    "firstPreconfigNetVlan": false,
    "hasUsedToolUpgrade": true,
    "hasUsedToolIpTransfer": true,
    "hasUsedFeedBack": true,
    "currentLanguage": "en_US",
    "isHasShowEzvizCloudSettingFlag": true,
    "preConfigSetting": {
      "gateTipHasVisible": true,
      "commonTemplates": [7, 2],
      "isShowMLTemplate": true,
      "isShowBITemplateFileModeSwitch": true,
      "isHasShowGuidance": true,
      "postAndepoliceValidation": {
        "notSShowSSoWebTip": true,
        "toolboxClick": {
          "PostAndepoliceValidation": true
        }
      },
      "deviceManegeSetting": {
        "filterTipVisible": true,
        "deviceInspect": {
          "downloadPath": "D:\\UserData\\deviceInspect"
        }
      }
    }
  }
}
```

Figure 6-11 Edit Configuration

2. Launch HiTools Delivery. From the Homepage, go to **Guided Delivery → Video Intercom Template → Create**.
3. Select **Import from File** and click **Download**.

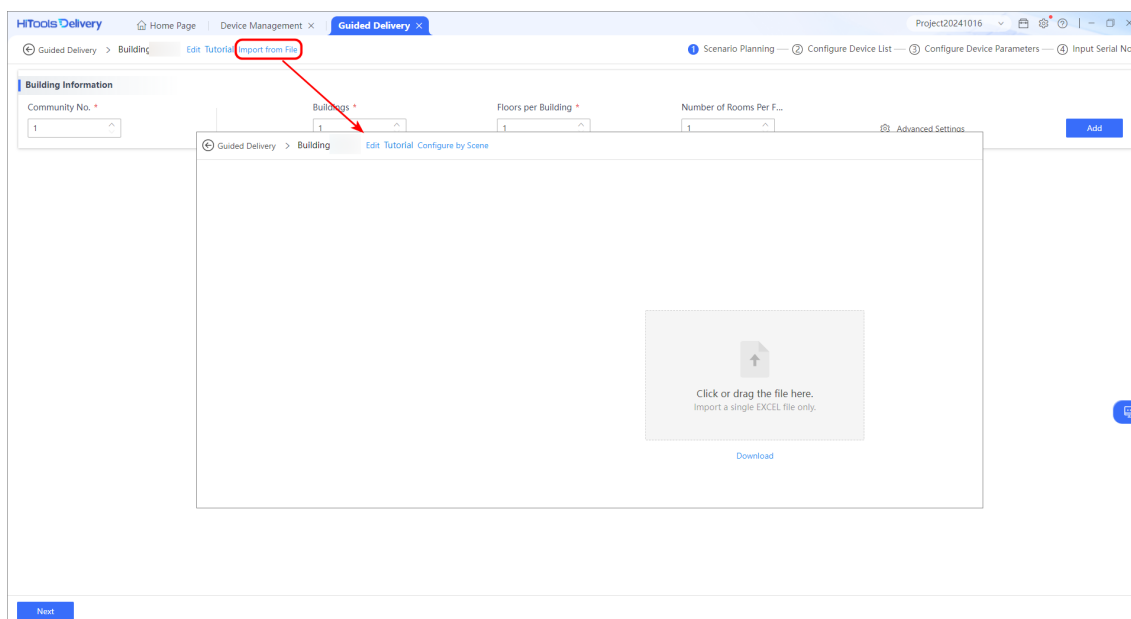


Figure 6-12 Enable Import from File Mode



Note

You can only enable the Import from File mode from Scenario Planning.

4. Fill in the project details according to the template requirements, then import the completed file.

This page is intended for importing main station list. All fields are required, and the gray part is an example.

The following are the rules for each field (column), please fill in the device information according to the rules.

1. Device Name: Length should be 0-32 characters, supports Chinese characters, numbers, letters, and special symbols, except for the following unsupported special symbols: / : * ? ' " < > | % &
2. Serial No.: 9-digit serial No. on the rear panel of the device. (A fixed-length number with 9 digits).
3. Activation Password: The valid password (8 to 16 characters) should contain two or more of the following character types: numeric, lowercase, uppercase, and special character.
4. Registration Password: The registration password registers the device to the private sip server. The valid password (8 to 16 characters) should contain two or more of the following character types: numeric, lowercase, uppercase, and special character.
5. Community No.: Ranges from: 1 to 9
6. No.: Ranges from: 51 to 99
7. IP Address/IP Mask/IP Gateway/SIP IP: Only supports ipv4.

Main Station List									
Device Name	Serial No.*	Activation Password	Registration Password	Community No.*	No.*	IP Address*	IP Mask*	IP Gateway*	SIP IP*
1	2	3	4	5	6	7	8	9	10
1									

1 2 3 4 5

Main Station(Building) Door Station Outer Door Station Indoor Station (+)

Figure 6-13 Complete Template

5. ***Input the serial number .***
6. (Optional) ***Activate devices and connect them to a network .***
7. ***Apply parameters to devices .***

Follow-Up

- After indoor stations are installed, powered on, and connected to a network, they will be automatically activated and configured.
- Due to network unavailability, all devices in the main station's remote configuration page show an Offline status. When the devices are installed in the actual environment, they will automatically register and the status will change to Registered.

6.6 How to Configure Entrance & Exit Template

6.6.1 Scenario

After parking access control devices have been installed, wired, and powered up, you can use HiTools Delivery to select the entrance and exit scene, add and configure devices such as ANRP cameras, all-in-one entrance & exit managers, radars, and coils. After scene design and device configuration, you can apply parameters and adjust the ANRP camera for more accurate recognition. With this feature, you can avoid switching configuration tools to improve the efficiency of configuring parking access control devices.

6.6.2 Overall Configuration Process

Table 6-5 Overall Configuration Process

Procedure	Description
Step 1: Select Scene	When your devices are installed, wired, and powered on, choose from the following scenes: Single In/Out, Mixed Entrance & Exit, Regular Entrance & Exit (Dual Islands), Regular Entrance & Exit, Single In/Out (Dual Barriers), and Mixed Entrance & Exit (Dual Barriers).
Step 2: Configure Devices	Adjust the number of devices, configure device parameters, and toggle the barrier gate up and down according to the actual conditions on-site.
Step 3: Apply Parameters and Adjust Cameras	Ensure your devices and computer are on the same local network. Match each device's serial number or WIFI name with its physical location and apply the parameters. For ANRP cameras or all-in-one entrance & exit manager, adjust the camera angle, adjust the zoom, draw the recognition area, and set the fill light and video parameters to enhance accuracy.
Step 4: Test Configuration	Drive a car from multiple directions to the entrance and exit to trigger events three times or more for each ANRP camera / all-in-one entrance

Procedure	Description
	& exit manager. After testing, you can check the test result or troubleshooting.

6.6.3 Steps

Step 1: Select an entrance & exit scene and configure devices.

1. Select a scene according to the actual condition.
2. (Optional) Hover over a barrier gate, and select **Flip** to toggle the barrier gate up and down.
3. Select devices and configure their parameters. The key device parameters are as follows.



Caution

You cannot add a radar and coil at the same time on the same side of the barrier gate.

Table 6-6 Camera Configuration

Parameter	Description
Device Name	1-32 characters. Before applying parameters, you should link the device name with the device serial No. and device type.
Trigger Type	- Video Trigger: Camera captures only when triggered by video. - IO Coil: Camera captures when triggered by a coil or radar. - Radar Mixed Traffic: Suitable for mixed traffic lanes (entrance and exit on the same lane).
License Plate Recognition	Generally select the bi-direction. If filtering rear plates is required in the video trigger mode of mixed traffic lanes, select the front direction.

Table 6-7 Radar Configuration

Parameter	Description
Device Name	The Wi-Fi name. To prevent multiple Wi-Fi signals from being indistinguishable on the site, modify the device name.
Max. Range	Maximum radar detection distance: The horizontal distance from the radar to the tail of the barrier pole minus 0.2 meters. Not the overall length of the barrier pole minus 0.2 meters. 3 meters by default.
Operating Mode	If the anti-fall radar is installed on the barrier gate, you can face the anti-fall radar to determine whether the barrier pole is on the left or right side of the radar.

Step 2: Apply parameters and adjust cameras.

1. Ensure devices except radars are on the same LAN as the computer, and ensure the radars are connected to the computer via Wi-Fi.
2. Select **Detect Online Device**.
3. After online devices are detected, link the device serial number or WiFi name with the device name set in Step 1, and select **Apply Parameters**.

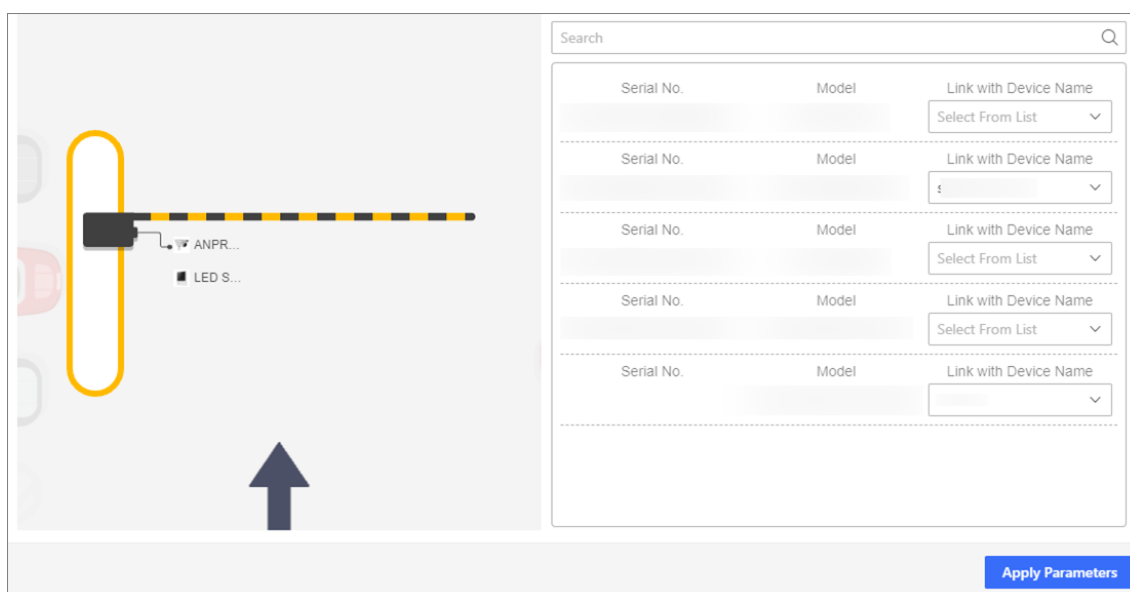


Figure 6-14 Link Device Serial No./ WiFi Name with Device Name

Note

Connect only one radar to your computer at a time. For multiple radars, switch the WIFI connection to the computer one by one.

4. Adjust each camera to improve license plate recognition accuracy.
 - a. Adjust the camera angle.

Note

- Ensure that the license plate is roughly parallel to the bottom edge of the image.
- It is recommended to position the license plate at the bottom 1/3 of the image.



Figure 6-15 Recommended License Plate Position

-
- Adjust the camera's zoom.
 - Park a vehicle 4 meters away from the camera, centered on the road.
 - Manually or automatically zoom. To manually adjust zoom, click , and drag a measurement box in the image to measure the license plate width, ensuring the license plate height is between **25-35 pixels**.
 - Draw the recognition area. Draw the lane lines and trigger lines according to the actual scene, with the midpoint of the lane lines forming the trigger line (shown in the following picture).



Figure 6-16 Example



Caution

- Do not draw irrelevant areas, as this will affect recognition speed.
- The lane line **should not be too short** (shown in the following picture). If the lane line is too short, cameras will capture pictures as soon as the vehicle enters the recognition area, which will make the ANPR algorithm harder to recognize the vehicle accurately.



Figure 6-17 Lane Lines Too Short

- Ensure the license plate is within the recognition area.



Figure 6-18 Not Within Recognition Area

- d. Adjust the supplement light parameters and image parameters.

- For supplement light: Default means the light is not enabled. Environment Brightness means automatically detecting ambient brightness to activate the supplement light.
- To avoid white light pollution and the device supports red light configuration, set the white light brightness to 0 and adjust the appropriate red light brightness.
- If the vehicle's headlights are too bright at night causing overexposure, open wide dynamic, lower the shutter speed, and reduce gain.

Step 3: Test the device configuration.

1. (Optional) Select **Export** at the upper right to export the device information, and import the device information into a control terminal for further configuration.
2. Drive a car from multiple directions to the entrance and exit to trigger events three times or more for each ANPR camera / all-in-one entrance & exit manager. Select **Test**.
3. After events are triggered, select **Stop**.

Table 6-8 Test Result

Test Result	Description
Passed	If all events with license plate character heights are between 25-35 pixels , the test is considered passed.
Failed	If not passed, troubleshoot step by step as follows. After each step of debugging, you can test again to ensure there are no issues. a. Adjust the camera angle to ensure that the license plate is roughly parallel to the bottom edge of the image. b. Adjust the camera focus to ensure that the license plate height is between 25-35 pixels. c. Redraw the recognition area to ensure the license plate is within the recognition area. d. If all the above solutions fail, contact the recognition algorithm development team to troubleshoot algorithm issues.

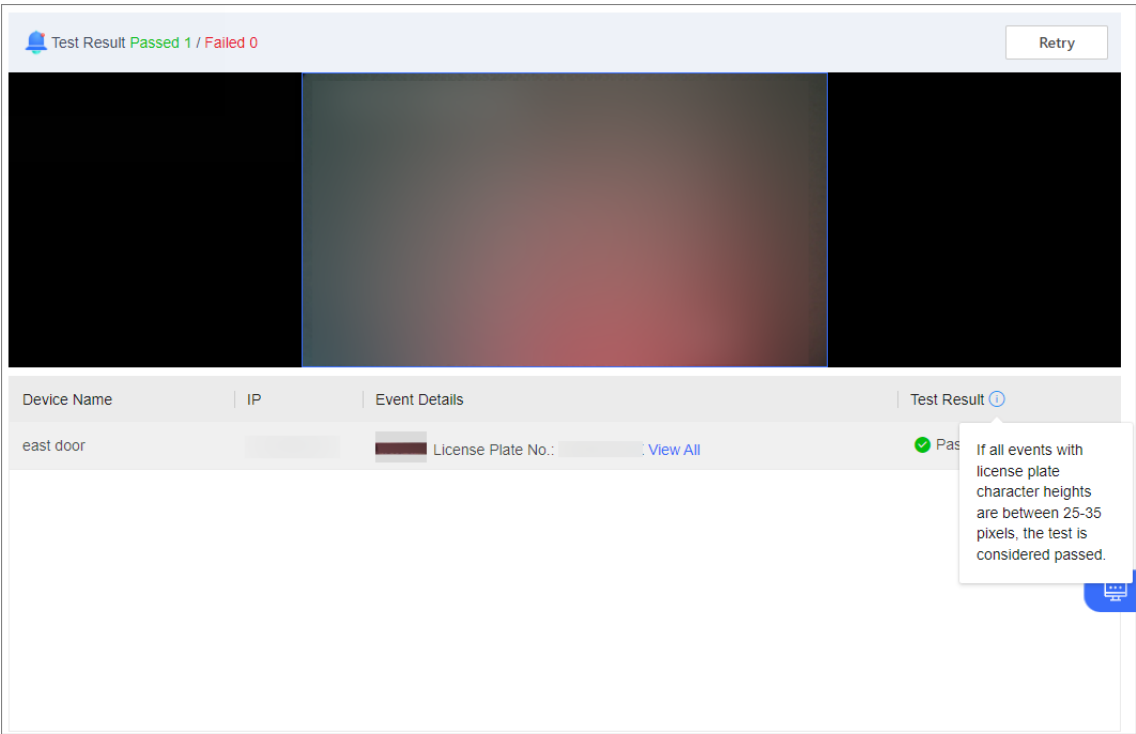


Figure 6-19 Test Result

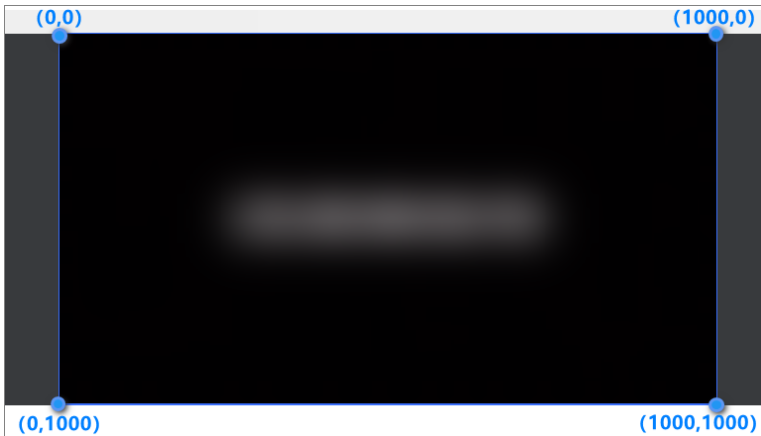
6.6.4 How-To Video



Figure 6-20 How to Configure Entrance& Exit Template

 Note

To enhance your experience, the product is continuously optimized. This video content may lag behind the latest version—please refer to the actual application for accuracy.

Parameters	Requirements
	 Figure 6-22 OSD Coordinates
ISUP Secret Key	8 to 16 characters are allowed.

3. Select **Next → Import Template** to import the configured template.
4. Select **Complete**.
5. Check all parameters. You can select **Edit Parameters** to edit parameters as needed.
6. Make sure all parameters are correct, devices are powered on and on the same LAN as your computer, and select **Quick Apply**. You can go to the task center for the applying results.

6.7.3 Online Configuration

Step 1: Select Configuration Mode

1. Select **Online Configure**.
2. Select the IP configuration mode, configure the parameters, and select **Next**.

Table 6-10 IP Configuration Mode

IP Configuration Mode	Description
Auto Allocate	A local area network (LAN) is available on-site.
Manual Allocate	For sites without a local network, you need to connect through a switch to apply parameters.

Step 2: Input Serial No.

1. Enter the Serial No. according to the scanning guidance. Taking using the mobile scanning tool as an example:

- a. Ensure that your phone is in the same LAN as your computer. It is recommended to connect your computer to your phone hotspot.
- b. Use **your phone's camera or the scan function in the browser** to open the scanning tool and scan the serial No.

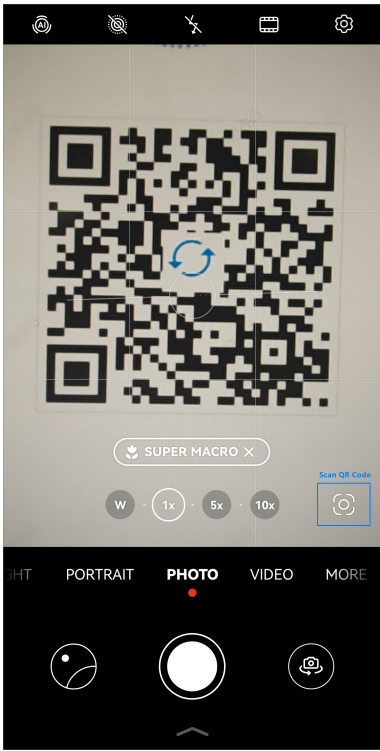
Phone OS	How to Use Scanning Tool
iOS	Scan the QR code with your phone's camera. After scanning, you will see a notification with a link. Tap that link, and it will open the scanning tool for you.
Android	Use the scan function in your browser or the built-in QR code scanning feature on your phone to scan the QR code.
Harmony	Use the scanning feature of the camera to scan the QR code. After scanning, it will take you straight to the scanning tool. 

Figure 6-23 Harmony V4.0.0 Camera Interface

- 2.
3. Check all parameters. You can select **Edit Parameters** to edit parameters as needed.
4. Make sure all parameters are correct, devices are powered on and on the same LAN as your computer, and select **Quick Apply**. You can go to the task center for the applying results.

Step 3: Configure Parameters

1. Select and configure parameters as needed, and select **Next**.

Table 6-11 Camera Configuration

Parameter	Description
Time	- NTP Time Sync: You should set up an NTP time server or get the server information first. Set the server address, NTP port, and interval to automatically sync time with an NTP time server. - Manual Time Sync: You can manually set the time or select Sync with Computer Time. - DST: Set the DST rule by country.
Video / Audio	- Stream Type - The main stream refers to the primary video stream that is transmitted at the highest quality. - The sub stream is a secondary video stream that is usually transmitted at a lower resolution or lower frame rate. - The third stream is often used for specific purposes, such as recording a separate video feed for backup or providing a different resolution or encoding format for specific applications. - Bit Rate Type - Constant bitrate (CBR): The bitrate remains consistent throughout the entire duration of the video or audio file. It can lead to higher file sizes or lower quality in complex scenes that require more data. - Variable bitrate (VBR): VBR, on the other hand, adjusts the bitrate dynamically based on the complexity of the content being encoded. - Video Encoding: Only main streams support H.264+ and H.265+. These encoding technologies can reduce the transmission bandwidth and storage capacity.
ISUP	In scenarios where the device does not have a fixed IP address, you can set the ISUP parameters to allows devices to actively initiate an upstream connection to the ISUP server, ensuring smooth and uninterrupted data communication.

2. Check all parameters. If all parameters are correct, select **Complete**.
3. Make sure all parameters are correct, devices are powered on and on the same LAN as your computer, and select **Quick Apply**. You can go to the task center for the applying results.

Chapter 7 Device Configuration

7.1 Prerequisites

- Add devices to HiTools Delivery.
- The selected devices are of the same model.
- Ensure the selected devices are online, and the network is working well. If the network is bad or blocked, applying parameters may fail.

7.2 Function Overview

In the Device Configuration module, select **Camera** , select parameters, and apply them. Select **Test** to test video parameters.

7.3 Supported Devices

- Common Parameters
- Camera
- Recording & Analysis
- Access Control
- Video Intercom
- Speed Gate & Turnstile
- LED Screen
- Intelligent Traffic
- Alarm Device
- Audio & Sensing
- Networking
- Interactive Flat Panel

7.4 Common Configuration

This section will introduce specific parameters shared by different types of devices, including network cameras, network video recorders, access control devices, and video intercom products. The supported configuration items vary by device capabilities.

7.4.1 Basic Configuration

Time

Scenario

The device's factory time is not synchronized with the current time, which may affect the stream timestamp and recording timestamp. It is recommended to adjust the device time in advance.

Steps

The screenshot shows the 'General Configuration' window with the 'Time' tab selected. The settings are as follows:

- Time Zone:** (GMT+08:00) Beijing, Urumqi, Singapore, Perth
- Time Sync Mode:** NTP Time Sync (selected), Manual Time Sync
- * Server Address:** 1
- * NTP Port:** 123
- * Interval:** 60 min
- Test:** A button to test the configuration.

Figure 7-1 Time Settings

1. Select devices, and then select **Time**.
2. Set the time zone and select a time sync mode.

Table 7-1 Time Sync Mode

Time Sync Mode	Description
NTP Time Sync	a. Set up an NTP time server or get the server information. b. Set the server address, NTP port, and interval to automatically sync time with an NTP time server. c. Select Test to test whether the function works well.
Manual Time Sync	Manually set the time or select Sync with Computer Time .

3. (Optional) Set the DST rule by country.
4. Select **Apply**.

Language

Scenario

When a device's default language doesn't match the regional language, you can change the language. Note that language support varies by device capability.

Steps

1. Select devices, and then select **Language**.
2. Select a language as needed.
3. Select **Apply**.

7.4.2 Platform Access

Cloud Service

Steps

1. In the device list, select devices and select **Cloud Service**.
2. Enable **Cloud Service**.
3. (Optional) Select **Custom** to set the server address according to your device type (Hikvision or Ezviz).
4. Set the verification code. For Ezviz devices, you can find the code on the device packaging.



Note

You can use the code and device serial No. to bind devices to cloud-based Apps like Hik-Connect.

-
5. Select **Apply**.
 6. Select **Test → Other Parameters** to test if cameras are connected to these platforms. You can check the access status in real time (Accessed, Not Accessed, and Not Supported).

ISUP

Scenario

In scenarios where the device does not have a fixed IP address, you can set the ISUP parameters to allow devices to actively initiate an upstream connection to the ISUP server, ensuring smooth and uninterrupted data communication.

Steps

1. Select devices, and then select **ISUP**.
2. Set the ISUP parameters such as the ISUP server address and port.
3. Select **Apply**.
4. Select **Test → Platform Access Test** to test if cameras are connected to these platforms. You can check the access status in real time (Accessed, Not Accessed, and Not Supported).

Batch Configure Test

Picture Test Event Test **Platform Access Test**

Devices: 2

Device Name	IP Address	ISUP	Hik-Connect Service
IP CAMERA			
IP CAMERA			

Figure 7-2 Platform Access Test

7.4.3 Cloud Storage

Scenario

For large-scale projects like public security, cloud storage is chosen as the medium for storing videos and captured images. The images of people, vehicles, and license plates captured are stored in the cloud, and the platform directly requests resources from the cloud.

Steps

Cloud Storage

☒ Enable ☒

☒ Protocol Version Cloud 2.0

☒ * Access Server IP

☒ * Access Server Port

☒ * Access Key Access Key

☒ * Encryption Key Encryption Key

☒ * Picture Storage Pool ID 10002

Test

Figure 7-3 Cloud Storage

1. Select devices, and then select **Platform Access** → **Cloud Storage**.
2. Enable Cloud Storage.
3. Set the storage server parameters.

Parameters	Description
Access Server IP / Port	The IP address and port of the cloud storage server.
Username/ Password	The username and password for logging into the cloud storage server.
Encryption Key	The password used to encrypt data stored on the cloud storage server.
Picture Storage Pool ID	The storage area identifier on the server for uploading images.

4. Select **Test** to check if the image upload is successful.
5. Select **Apply**.

7.4.4 HEOP

Scenario

For network cameras, access control devices, and video intercom devices, you can use Hikvision Embedded Open Platform (HEOP) to import your own applications for more features.

This function can be used in the following scenarios:

- Payment Terminal: In the cafeteria setting, you can import your own applications with features like face-scanning and spending alerts into payment terminals with HEOP capabilities.
- Camera: Import your own applications into cameras with HEOP capabilities.
- Batch Delete: To install new apps on cameras, delete old ones if storage is full.
- Turn Off APP: If a new app won't run due to memory constraints, turn off other apps to start it.
- Enable/Disable Android App: For access control and video intercom devices, use the HiTools Delivery to enable or disable Android apps that can't be directly managed after upload.

Steps

1. Select devices, and then select **HEOP Application..**
2. Perform one of the following operations.

▼ ☒ **HEOP Application**

For an App requires authorization, follow the steps to apply the license and import it. For an App not requires authorization, import the App directly.

- ① Step 1. Click [Export](#) Download the selected device information (such as serial No.) for applying for App license. [Export](#)
- ② Step 2. Upload the template file to the open platform to apply the App permission for the device(s), and then download the App license.
- ③ Step 3. Click [Import App](#) , and import the App and License.

📁 **Import App**

No.	App File Name	App Status	License File	Operation
1		☐		📁 ×
2		☐		📁 ×
3		☐		📁 ×

Maintenance and Security

> ☐ **Import Device Parameters**

Selected Device: 1 Channel: 1

Figure 7-4 HEOP

- Import APP.

Device Type	License	Steps
Camera	For applications with licenses required, use the selected device information to apply the App license.	a. Select Export to get the device information. b. Upload the information to the open platform to get the license file. c. Select Import App to import your application and the license.
Access Control / Video Intercom	- You will get distributed license file. - The application has a built-in license.	Select Import App to import your application and the license.

- You can enable/disable/delete specific Apps.

3. Select **Apply**.

7.4.5 Maintenance & Security

Import Device Parameters

Scenario

For network cameras, access control devices, video intercom devices, and turnstiles, you can import the configuration file of a configured device to devices with the same model for more efficient configuration.

Steps

To take access control devices as an example:

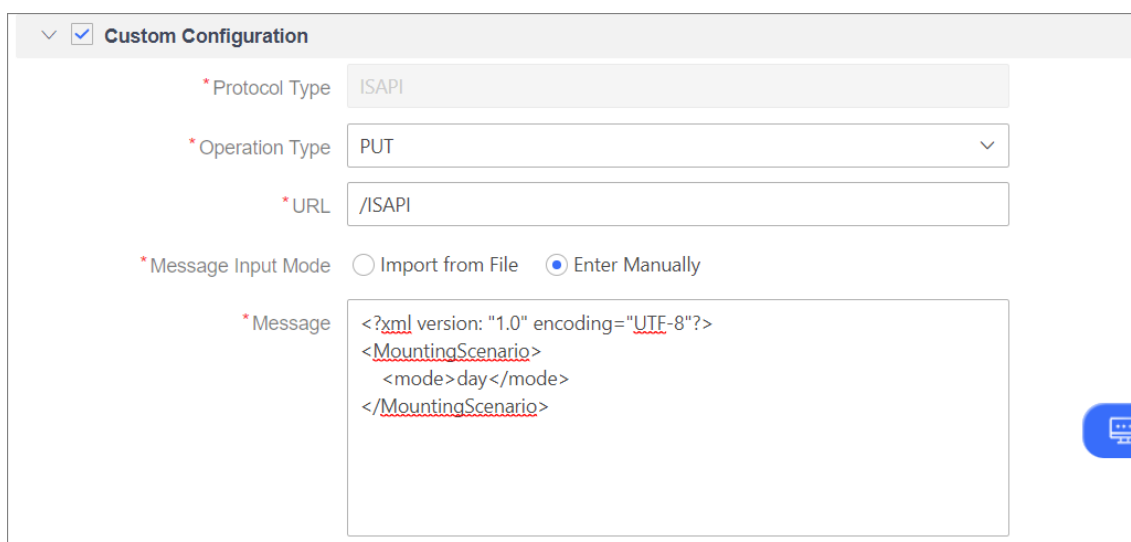
1. In the device list, select  of a configured device to go to the device web configuration page.
2. Select **Maintenance**, and export the device parameter file.
3. Select devices of the same model, select **Import Device Parameters**, and import the file.
4. Select **Apply**.

7.4.6 Advanced Configuration

Scenario

To batch configure parameters that HiTools Delivery does not support, you can call APIs to configure them.

Steps



Custom Configuration

* Protocol Type: ISAPI

* Operation Type: PUT

* URL: /ISAPI

* Message Input Mode: ☐ Import from File ☒ Enter Manually

* Message:

```
<?xml version: "1.0" encoding="UTF-8"?>
<MountingScenario>
  <mode>day</mode>
</MountingScenario>
```

Figure 7-5 Custom Configuration (ISAPI)

1. In the device list, select devices and then select **Custom Configuration**.
2. Set the operation type and URL.
3. Set the message input mode.

Input Mode	Description
Import from File	Select  and import the request message in XML format.
Enter Manually	Enter the request message manually. For example: <pre><?xml version: "1.0" encoding="UTF-8"?><MountingScenario> <mode>day</mode></MountingScenario></pre>

4. Select **Apply**.

7.4.7 Configure More

Support batch configuration by copying a single device's web parameters to multiple devices of the same model.

Supported Devices

Support batch configuring more parameters for the following devices: cameras, recording & analysis (NVR, DVR, DeepMind Intelligence), access control devices, video intercom devices, traffic cameras, audio & sensing (public address devices, speakers), network bridges, alarm devices, on-street parking cameras, control devices (decoders, video wall controllers, MVC, KVM), and interactive flat panels (digital signage series).

Prerequisite

To use this feature, ensure the relevant configuration extension is successfully installed.

Steps

- **Public Network:** Click in the upper-right corner of the software and click **System Settings → Extension** to download or update the extension and check the download progress.
- **Local Network:** Click to scan the QR code and download the extension, or click **Import** to install it manually.
- You can also download extensions from the link. Transfer the downloaded extension to your computer, and then click **Import** to install it manually. The download links are as follows:

Extension Type	Download Link
Basic Service Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/BasePlugin/BasePlugin_Plug_2.1.0.0.zip
Encoding Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/CameraPlguin/CameraPlguin_Plug_2.1.0.0.zip
Access Control & Video Intercom Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/AccessControlPlguin/AccessControlPlguin_Plug_2.1.0.0.zip
Alarm Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/AlarmPlguin/AlarmPlguin_Plug_1.5.0.0.zip
Networking Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/NetworkingPlguin/NetworkingPlguin_Plug_1.6.0.0.zip
Recording & Analysis Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/BackendPlguin/BackendPlguin_Plug_1.6.0.0.zip
Intelligent Traffic Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/ITSPlguin/ITSPlguin_Plug_2.1.0.0.zip
Audio & Sensing Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/AudioSensingPlguin/AudioSensingPlguin_Plug_2.0.0.0.zip
Control Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/ControlPlguin/ControlPlguin_Plug_1.6.0.0.zip
Interactive Flat Panel Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/

Extension Type	Download Link
	HD/FlatPanelDisplayPlguin/ FlatPanelDisplayPlguin_Plug_1.6.0.0.zip
Extension for Devices via Private Protocol	http://hikdownload.hik-connect.com/HiTools/ windows/overSea/ComponentManagement/ HD/RemoteConfugPlugin/ RemoteConfugPlugin_Plug_2.1.0.0.zip

7.5 Camera

7.5.1 Function Overview

Select **Device Configuration** → **Camera** , select devices of the same model, configure parameters, and apply them. Select **Test** to test video parameters.

7.5.2 Prerequisites

- Add cameras to HiTools Delivery.
- The selected devices are of the same model.
- Ensure the selected devices are online, and the network is working well. If the network is bad or blocked, applying parameters may fail.

Note

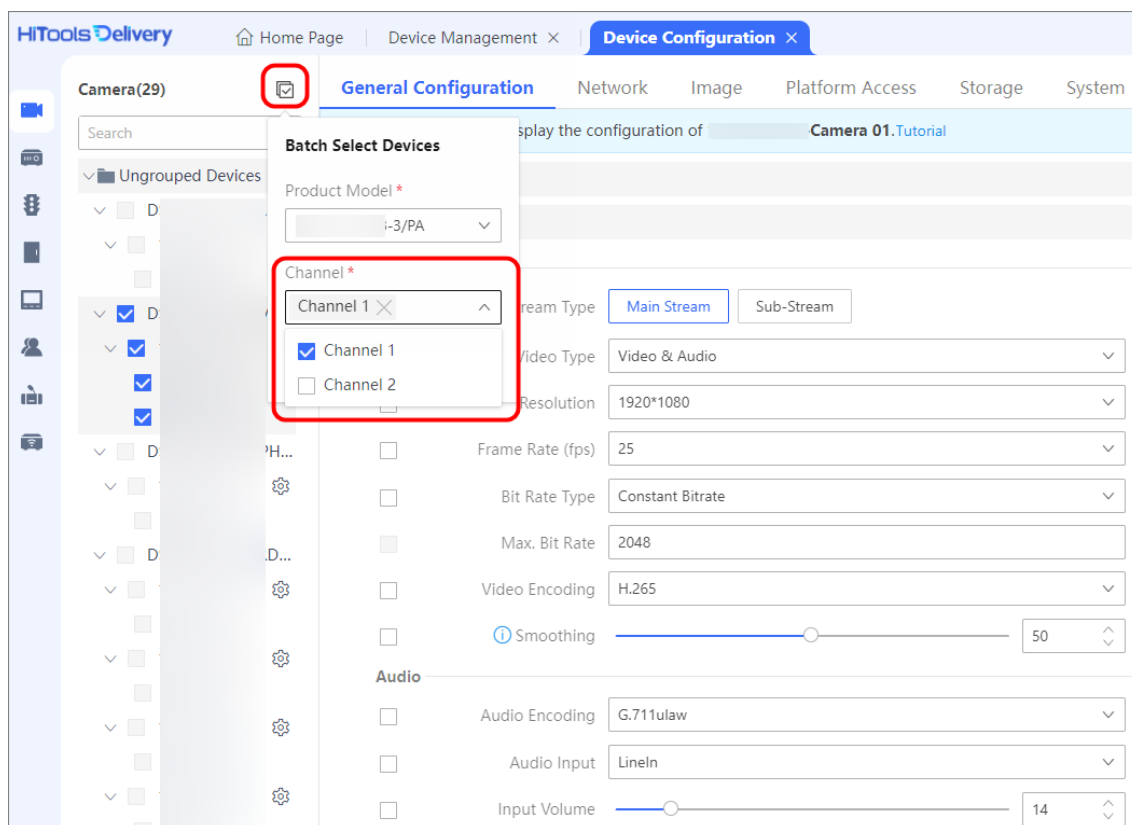


Figure 7-6 Batch Select Channels

For multi-channel cameras, supports batch parameter configuration based on device model and selected channels.

7.5.3 Configuration Items

Table 7-2 Camera Configuration

Configuration	Description
<u>Common Configuration</u>	Time, Language, Cloud Service, Cloud Storage, ISUP, ISAPI, Import Device Parameters, and more.
<u>General Configuration</u>	Video/Audio, OSD, Display, and Preset.
<u>Platform Access</u>	Include ONVIF, ISUP, and Cloud Service.
<u>Event</u>	FTP, Email, and Motion Detection

Configuration	Description
<u>Picture Overlay</u>	Picture Overlay
<u>Network</u>	SNMP, 802.1X, TLS, and Certificate Management.
<u>Storage</u>	HDD Management & Cloud Storage
<u>System</u>	User Management & Account Security
<u>VCA Resource Management</u>	Face Capture, Multi-Target-Type Detection, Line-Crossing Detection, and Intrusion Detection.
<u>Maintenance & Security</u>	Password Reset Methods and Device Parameter Import

7.5.4 General Configuration

This document will mainly introduce how to configure video/audio, OSD, display, and preset.

OSD

Scenario

OSD refers to the additional information displayed on the preview screen such as the channel name, time/date, province/city/county/camera location/camera orientation, and more customized information. You can set and select the OSD information to be displayed and drag the red OSD information on the preview screen to the desired display position.

Overall Configuration Process

1. Configure the OSD information, including channel names, display dates, custom characters, and more. After configuration, verify that the OSD overlay on the first device is correct.
2. Other devices are configured based on the configuration template of the first device.
 - You can configure the OSD characters and channel names for other devices online; the OSD character positions and templates are the same and can be reused or modified.
 - You can also export the configuration template of the first device, configure the OSD information for other devices in an EXCEL file, and import it into HiTools Delivery.
3. Verify that the OSD configuration for all devices is correct.

Steps

1. Select devices and select **OSD**.
2. Set the OSD configuration.
 - a. Set the display configuration such as the channel name and display date.

Note

You just need to set the date/time format without setting the specific time.

- Set the OSD font and alignment.
- Select **Add** to add custom OSD elements.
- Drag red-highlighted OSD elements on the preview screen to adjust their positions.

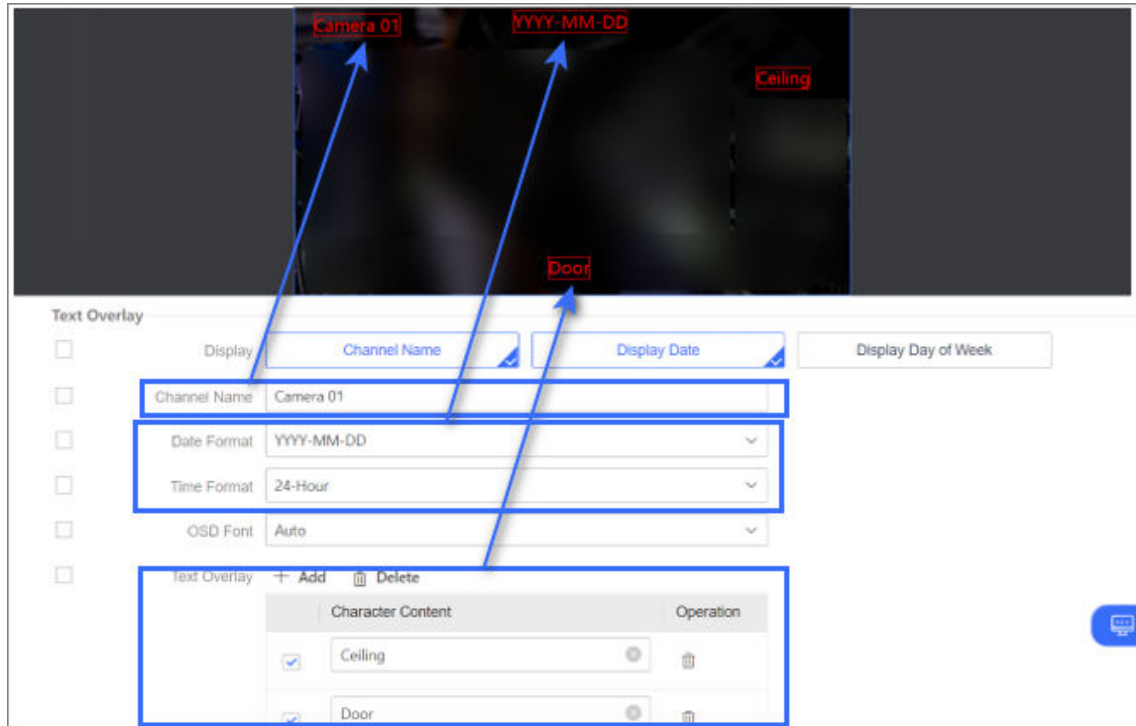
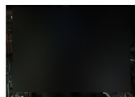
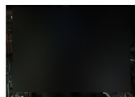
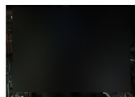
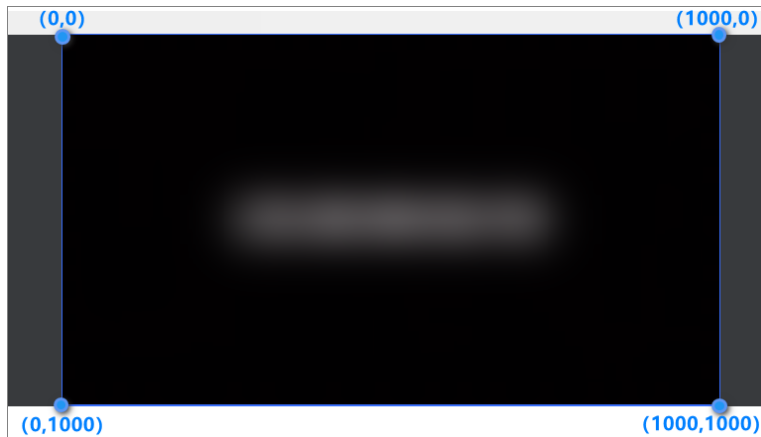


Figure 7-7 Set OSD Elements for First Device

- Select **Preview** to check if the OSD elements are applied.
3. Select other channels and customize OSD elements according to the first channel's configuration.

Table 7-3 Two Configuration Modes

Configuration Mode	Description
Online Configure	- Set the configuration mode to Online Configure. - Select Configure. - Set the text and channel name for other channels, and select OK. - Select Apply.

Configuration Mode	Description																																																																													
	<table><tr><th>IP Address</th><th>Channel No.</th><th>Custom Text 1</th><th>Custom Text 2</th><th>Channel Name</th><th>Capture</th></tr><tr><td></td><td>01</td><td>Ceiling</td><td>Door</td><td>Camera 01</td><td></td></tr><tr><td></td><td>02</td><td>Window</td><td>Table</td><td>Camera 02</td><td></td></tr></table> Figure 7-8 Online Configuration	IP Address	Channel No.	Custom Text 1	Custom Text 2	Channel Name	Capture		01	Ceiling	Door	Camera 01			02	Window	Table	Camera 02																																																												
IP Address	Channel No.	Custom Text 1	Custom Text 2	Channel Name	Capture																																																																									
	01	Ceiling	Door	Camera 01																																																																										
	02	Window	Table	Camera 02																																																																										
Import from File (Recommended)	a. Set the configuration mode to Import from File. b. Select Export Template to export the OSD configuration template in EXCEL format. c. Fill in the template. <table><tr><th colspan="5">Channel Information</th><th colspan="6">Custom Text 1</th></tr><tr><th>Channel No.</th><th>Display Status (0: Not Display, 1: Display)</th><th>Name</th><th>X-Coordinate (0: 1000)</th><th>Y-Coordinate (0: 1000)</th><th>OSD Font Size (0: Auto, 1: 20-16, 2: 12-10, 3: 8-6, 4: 4-2, 5: 8-6-4-2)</th><th>Alignment (1: Custom, 2: Align Character Left, 3: Align Character Right, 4: Align All Left, 5: Align All Right)</th><th>Display Status (0: Not Display, 1: Display)</th><th>Content</th><th>X-Coordinate (0: 1000)</th><th>Y-Coordinate</th></tr><tr><td>1</td><td>1</td><td>Camera 01</td><td>800</td><td>800</td><td>0</td><td>0</td><td>1</td><td>Door 01</td><td>150</td><td>150</td></tr><tr><td>2</td><td>1</td><td>Camera 02</td><td>800</td><td>800</td><td>0</td><td>0</td><td>1</td><td>Door 02</td><td>150</td><td>150</td></tr><tr><td>3</td><td>1</td><td>Camera 03</td><td>800</td><td>800</td><td>0</td><td>0</td><td>1</td><td>Door 03</td><td>150</td><td>150</td></tr><tr><td>4</td><td>1</td><td>Camera 04</td><td>800</td><td>800</td><td>0</td><td>0</td><td>1</td><td>Door 04</td><td>150</td><td>150</td></tr><tr><td>5</td><td>1</td><td>Camera 05</td><td>800</td><td>800</td><td>0</td><td>0</td><td>1</td><td>Door 05</td><td>150</td><td>150</td></tr></table> Figure 7-9 OSD Template  Note - If the OSD elements of the first device are not synchronized in the downloaded template, you need to manually enter the information. - The origin of coordinates at the upper-left corner of the preview screen. As shown in the following image:  Figure 7-10 OSD Coordinates	Channel Information					Custom Text 1						Channel No.	Display Status (0: Not Display, 1: Display)	Name	X-Coordinate (0: 1000)	Y-Coordinate (0: 1000)	OSD Font Size (0: Auto, 1: 20-16, 2: 12-10, 3: 8-6, 4: 4-2, 5: 8-6-4-2)	Alignment (1: Custom, 2: Align Character Left, 3: Align Character Right, 4: Align All Left, 5: Align All Right)	Display Status (0: Not Display, 1: Display)	Content	X-Coordinate (0: 1000)	Y-Coordinate	1	1	Camera 01	800	800	0	0	1	Door 01	150	150	2	1	Camera 02	800	800	0	0	1	Door 02	150	150	3	1	Camera 03	800	800	0	0	1	Door 03	150	150	4	1	Camera 04	800	800	0	0	1	Door 04	150	150	5	1	Camera 05	800	800	0	0	1	Door 05	150	150
Channel Information					Custom Text 1																																																																									
Channel No.	Display Status (0: Not Display, 1: Display)	Name	X-Coordinate (0: 1000)	Y-Coordinate (0: 1000)	OSD Font Size (0: Auto, 1: 20-16, 2: 12-10, 3: 8-6, 4: 4-2, 5: 8-6-4-2)	Alignment (1: Custom, 2: Align Character Left, 3: Align Character Right, 4: Align All Left, 5: Align All Right)	Display Status (0: Not Display, 1: Display)	Content	X-Coordinate (0: 1000)	Y-Coordinate																																																																				
1	1	Camera 01	800	800	0	0	1	Door 01	150	150																																																																				
2	1	Camera 02	800	800	0	0	1	Door 02	150	150																																																																				
3	1	Camera 03	800	800	0	0	1	Door 03	150	150																																																																				
4	1	Camera 04	800	800	0	0	1	Door 04	150	150																																																																				
5	1	Camera 05	800	800	0	0	1	Door 05	150	150																																																																				

Configuration Mode	Description
	d. Import the template and select Apply. e. Select Test → Picture Test to check the result. Picture Test Notes Check if the protective film on the camera is torn away / the picture is clear / the camera is not... PTZ Test Notes Check if the rotation is continuous / the start and end time of rotation is not delayed / the preset l... Camera 01 Setting Door Camera 02 Window Table PTZ Slow Forward Fast Forward Figure 7-11 Verify OSD

Video/Audio

Scenario

The day/night switch, backlight (WDR/HLC), and white balance are all features commonly used in cameras that help to optimize image quality in different lighting conditions. Supported parameters vary by device.

Steps

- 1. Select devices and select **Video/Audio**.
- 2. Set the video/audio parameters. The following table will introduce major parameters.

Table 7-4 Video/Audio Parameters

Parameters	Description
Stream Type	- The main stream refers to the primary video stream that is transmitted at the highest quality. - The sub stream is a secondary video stream that is usually transmitted at a lower resolution or lower frame rate. - The third stream is often used for specific purposes, such as recording a separate video feed for backup or providing a different resolution or encoding format for specific applications.
Bit Rate Type	- Constant bitrate (CBR): The bitrate remains consistent throughout the entire duration of the video or audio file. It can lead to higher file sizes or lower quality in complex scenes that require more data. - Variable bitrate (VBR): VBR, on the other hand, adjusts the bitrate dynamically based on the complexity of the content being encoded.
Average Bit Rate	Defaults to 50% of the maximum bitrate limit.
I-Frame Interval	- Editable only when both Smart Encoding and AI Encoding are disabled. - Higher intervals lower bandwidth and storage usage (e.g., at 25 fps, an I-frame interval of 50 generates one I-frame every 2 seconds).
Video Encoding	Only main streams support H.264+ and H.265+. These encoding technologies can reduce the transmission bandwidth and storage capacity. Guanlan AI Encoding: (Only certain cameras are supported.) Enabling Guanlan AI encoding unlocks the Average Bit Rate configuration. It intelligently distinguishes key targets (e.g., people and vehicles) from backgrounds to dynamically allocate bitrate. Reduces storage consumption by over 50% compared to standard H.265 while preserving critical details.
Video Type	For example, in school settings, choose Video & Audio in large-scale exams for comprehensive monitoring. For labs, a video-only stream suffices.
Input Volume	It is the system volume.

3. Select **Apply**.

Display

Scenario

The day/night switch, backlight (WDR/HLC), and white balance are all features commonly used in cameras that help to optimize image quality in different lighting conditions. Supported parameters vary by device.

- Day/Night functionality is designed to switch between color, black-and-white and other modes based on the lighting conditions.
- White balance is a feature that adjusts the camera's sensitivity to ensure that white objects appear as white in various lighting conditions. It ensures accurate color representation by adjusting for the color temperature of the light source.
- Wide Dynamic Range (WDR), High-Light Compensation (HLC), or backlight correction, enhances visibility in both bright and dark areas of a scene. WDR is crucial in environments with strong backlighting or uneven lighting, such as outdoor cameras.

Steps

1. Select devices and select **Display**.
2. Select a scene mode.
3. Set the display parameters.
4. Select **Apply**.

Preset

Scenario

Presets refer to pre-defined settings or positions that the camera can be programmed to move to automatically. Once a preset is saved, you can quickly recall it with a single command. You can also set automated patrols by creating a sequence of presets that the camera will automatically cycle through, providing continuous coverage of multiple areas. In large facilities, presets allow the camera to monitor different areas without manual intervention. In industrial settings, presets can be used to inspect specific equipment or areas at regular intervals.

Steps

1. Select devices and select **Preset**.
2. Set presets.

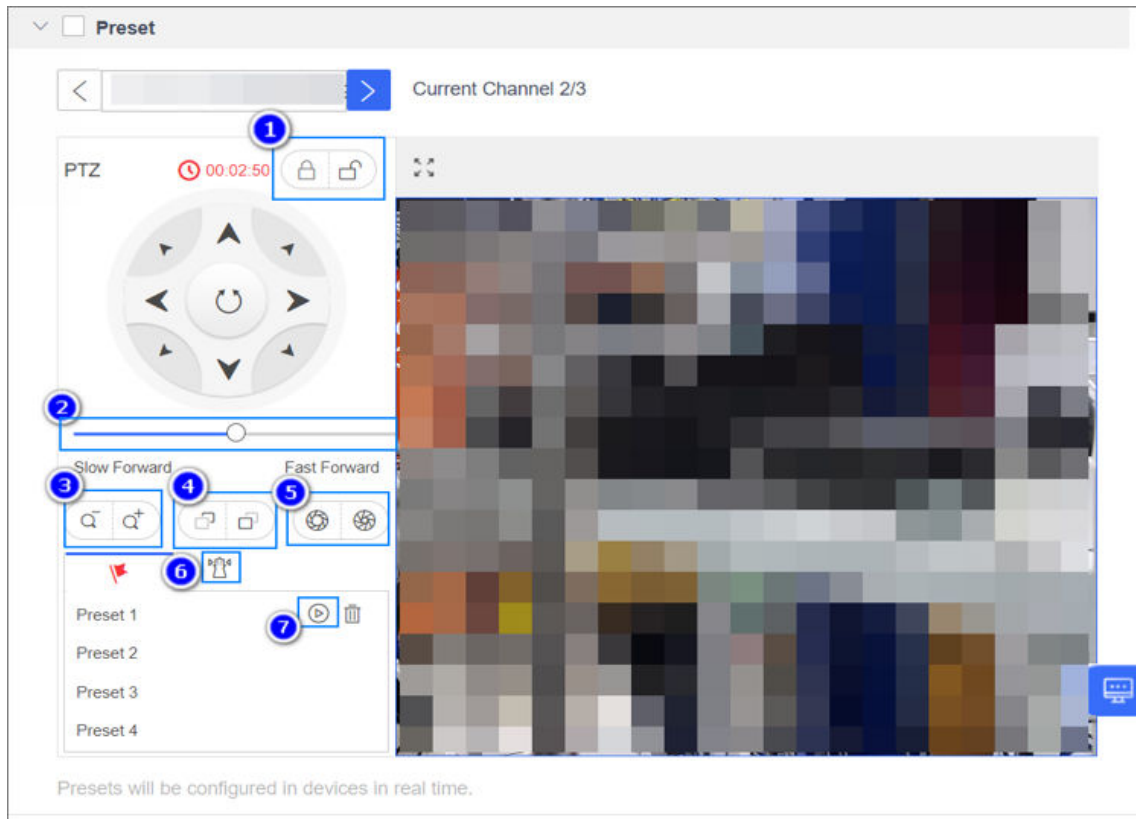


Figure 7-12 Set Presets

No.	Description
1	Lock/unlock the PTZ control.
2	Adjust the speed of PTZ movement.
3	Zoom in/out.
4	Adjust the sharpness and clarity of subjects in an image.
5	Adjust the brightness.
6	Quick park. Within the set time, if the camera does not receive any control commands, it will automatically perform preset actions or return to a preset position. This is suitable for monitoring scenarios that require long periods of unattended operation, such as parking lots, warehouses, or public areas.
7	Call presets.

3. Select **Apply**.

7.5.5 Network

SNMP

Scenario

SNMP (Simple Network Management Protocol) is a widely used network management protocol for monitoring and managing network devices and their functions. It is designed to facilitate the exchange of management information between devices. An SNMP system consists of four major components: network management system (NMS), SNMP agent, managed object, and management information base (MIB).

- SNMPv1: For small networks with simple networking, low requirements for network security or relatively secure network environments, and stable networks, such as campus networks or small enterprise networks.
- SNMPv2c: For large and medium-sized networks with low requirements for network security or relatively secure network environments (such as VPN networks), but with busy operations that may experience network congestion.
- SNMPv3: For networks of all sizes, especially those with high requirements for network security, ensuring that only authorized administrators can manage network devices.

Steps

1. Select devices and select **Network → SNMP**.
2. Enable this function.
3. Select a SNMP version and configure parameters.

Parameters	Description
Read Community String	This is a password that allows an SNMP manager to read (get) information from an SNMP agent (the device being monitored). It is typically used for monitoring purposes.
Write Community String	This is a password that allows an SNMP manager to write (set) information on an SNMP agent. It is used for configuration changes or administrative tasks.
Trap IP Address	The IP address of the SNMP manager or the system that should receive SNMP traps. Traps are unsolicited messages sent by the SNMP agent to notify the manager about specific events or conditions, such as a device failure or a threshold being exceeded.
Trap Port	This is the port number on the SNMP manager where traps are sent. By default, SNMP traps are sent to port 162 .

Parameters	Description
Trap Community String	This is a password that the SNMP agent uses to authenticate the trap messages it sends to the SNMP manager. It ensures that only authorized devices can send traps to the manager.
Security Level	SNMPv3 defines three security levels : noAuthNoPriv (SNMP messages are sent without any security measures), authNoPriv (the message source is authenticated but the message is not encrypted), and authPriv(the message content is encrypted using algorithms like DES, AES).

4. Select **Apply**.

802.1X

Scenario

802.1x is a network access control and authentication protocol. It provides an authentication mechanism to devices connected to a LAN or WLAN. It is primarily used to secure networks by preventing unauthorized access.

Component

- Client: The client device that wishes to gain access to the network.
- Authenticator: Typically a network switch or wireless access point that controls physical access to the network based on authentication status.
- Authentication Server: Typically a RADIUS server that checks the credentials of the client and then informs the authenticator whether access should be granted. 802.1x uses EAP(Extensible Authentication Protocol) over EAPoL for message exchange.

Prerequisites

- The device and switch should support the 802.1X protocol.
- Set up an 802.1X authentication system, including devices, switches, and RADIUS servers.
- Have a trusted Certificate Authority for signing certificates.

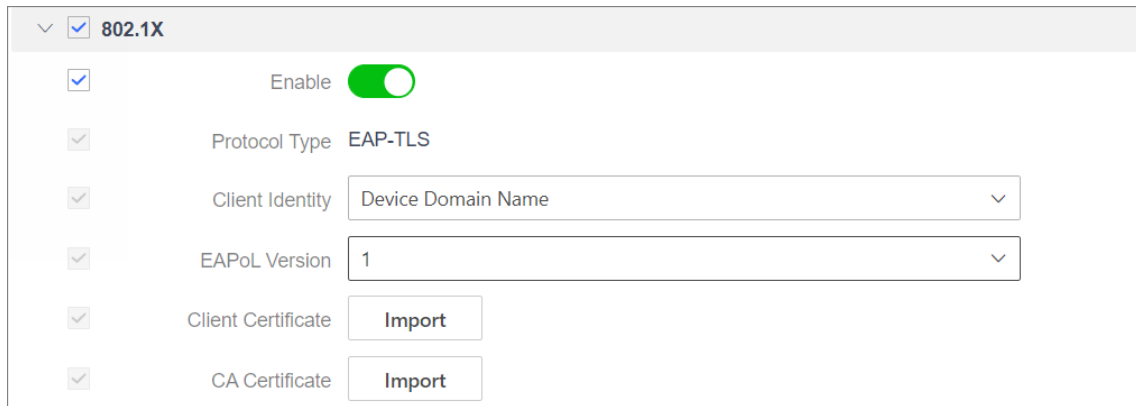
Steps

1. Select cameras, and select **Network → 802.1X**.
2. Enable 802.1X.
3. Set the client identity and EAPoL version.



Note

You can log in to the device's remote configuration page to set the device domain name.



802.1X

Enable ☒

Protocol Type EAP-TLS

Client Identity Device Domain Name

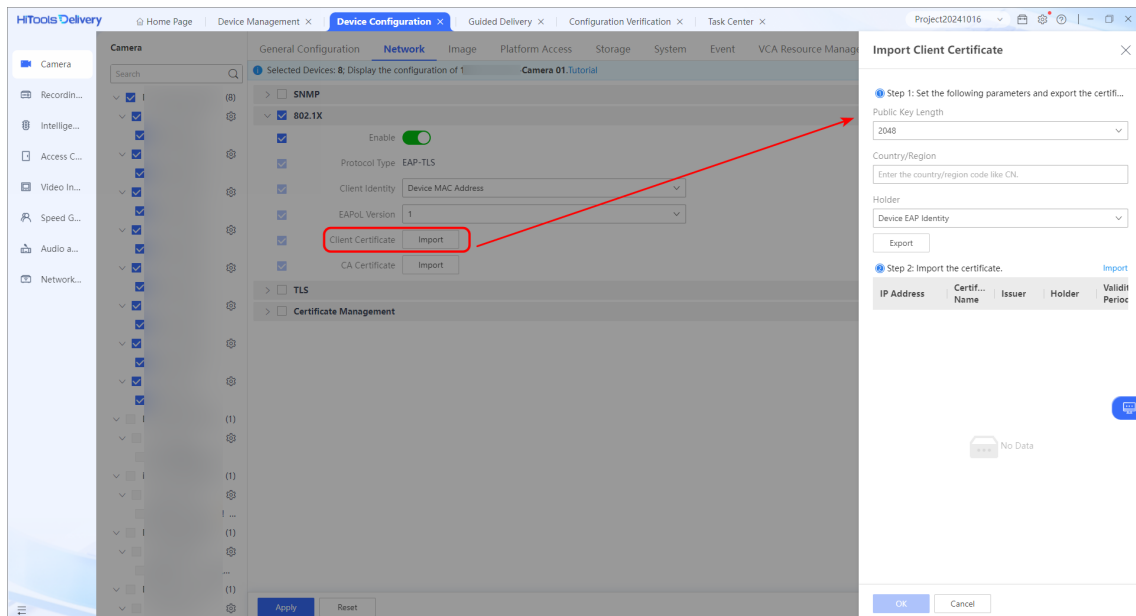
EAPoL Version 1

Client Certificate Import

CA Certificate Import

Figure 7-13 802.1X

4. Import the client certificate.



HiTools Delivery

Device Configuration

Selected Devices: 8. Display the configuration of 1. Camera 01.Tutorial

802.1X

Enable ☒

Protocol Type EAP-TLS

Client Identity Device MAC Address

EAPoL Version 1

Client Certificate Import

CA Certificate Import

Import Client Certificate

Step 1: Set the following parameters and export the certifi...

Public Key Length 2048

Country/Region Enter the country/region code like CN.

Holder Device EAP Identity

Export

Step 2: Import the certificate.

IP Address	Certif... Name	Issuer	Holder	Validit Period
No Data				

OK Cancel

Figure 7-14 Import Client Certificate

- Click **Import**.
 - Enter the public key length, country/region code, and holder information.
 - Click **Export**, and export the certificate request file (including .csr and .key files).
 - Send the certificate request file to the Certificate Authority (CA), and the CA issues the client certificate.
 - Click **Import** to import the client certificate back.
- Select **Import** to import the CA certificate on the CA certificate chain saved on the RADIUS server, used for verifying the validity of certificates between the client and the server.
 - Select **Apply**.

TLS

Scenario

The Transport Layer Security (TLS) is a cryptographic protocol designed to provide secure communication over a computer network. It ensures that data transmitted between the client and server remains private and cannot be tampered with by encrypting the data and using digital certificates to verify the identity of the server and, optionally, the client.

Steps

1. Enable **HTTPS** in Certificate Management.
2. Select cameras, and select **TLS**.
3. Select a TLS version and enable it.



Caution

TLS 1.1 is no longer considered secure due to known vulnerabilities and should be avoided in favor of TLS 1.2 or higher.

-
4. Select **Apply**.

HTTPS Certificate Management

Scenario

Self-signed certificates and self-signed root certificates are used in private networks to ensure secure camera access, data transmission, and device authentication. By generating a self-signed root certificate, issuing self-signed certificates, enabling HTTPS, and regularly updating certificates, you can prevent man-in-the-middle attacks, cracking, and data leakage, ensuring secure network communication.

Parameter Description

A **self-signed root certificate** is the root of the certificate chain, used to issue other self-signed certificates. In a private network, the self-signed root certificate can act as an internal Certificate Authority (CA) for issuing certificates to other devices. The certificate chain issued by the self-signed root certificate ensures device authentication and data encryption.

Steps

1. Select devices and select **Network → Certificate Management**.
2. Import a self-signed root certificate or create a new one by entering your country details, specifying the device domain or IP, and setting the validity period and key length.

Note

- Maintain consistency in the information provided for both self-issued certificates and the self-issued root certificate.
- When entering the country, use the country/region code.

3. Enable **HTTPS**.

4. Select **Apply**.

7.5.6 Picture Overlay

You can upload a 24-bit BMP picture such as a company logo for batch overlay at specified positions. (Device compatibility required.)

1. Select target devices. Select **Image** → **Picture Overlay** , and enable the feature.
2. Click **Upload** to upload a BMP file.
3. Drag a red frame on the live view to adjust the overlay position and picture size.

Note

The picture is positioned based on the top-left corner of the red frame.

4. Click **Apply** to apply the overlay to the selected area.

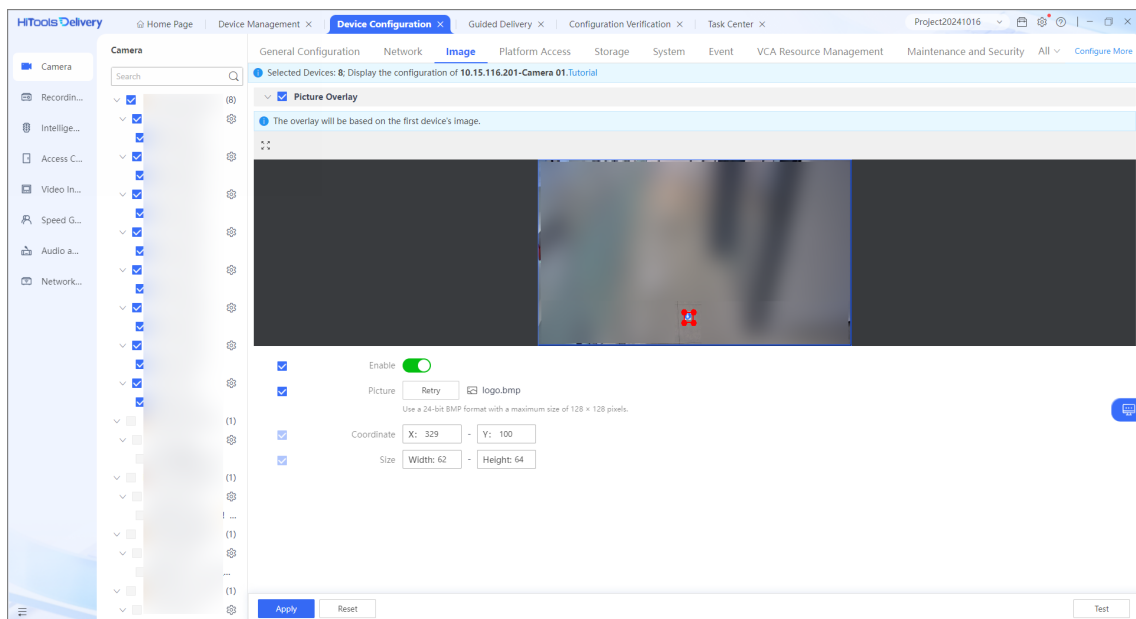


Figure 7-15 Apply Picture Overlay

5. Click **Test** in the bottom-right corner to verify the effect.

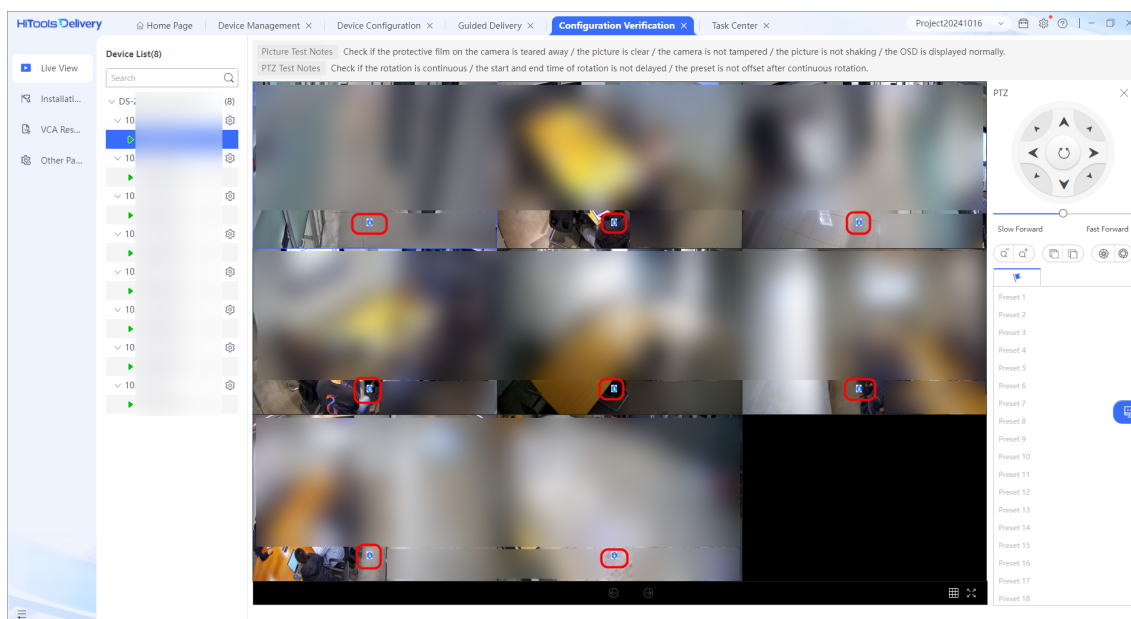


Figure 7-16 Verify Picture Overlay

7.5.7 Platform Access

ONVIF

Scenario

You can add Hikvision cameras to third-party network video recorders or platforms via the ONVIF (Open Network Video Interface Forum) protocol. ONVIF supports two main authentication methods: Digest & ws-username token and Digest. These methods ensure that only authenticated users can access specific device functions. By using usernames and passwords, the ONVIF protocol can verify user identities, preventing unauthorized access.

Steps

ONVIF

Enable ☒

Authentication Mode ☒ Digest&ws-username token ☐ Digest

Compatible to most platforms. Sync device time with platform time first.

User List ☐ + Add ☐ Delete

No.	User Name	User Type	Operation
1		Video User	☐ ☐
2		Operator	☐ ☐
3		Administrator	☐ ☐
4		Operator	☐ ☐
5		Video User	☐ ☐
6		Video User	☐ ☐

Figure 7-17 ONVIF

1. Select devices, and then select **Platform Access** → **ONVIF** .
2. Enable ONVIF.
3. Select an authentication mode.
4. Select **Add** and then set the user name, password, and user type.
5. Select **Apply**.

More Configuration

- Cloud Storage
- ISUP
- Cloud Service

7.5.8 Storage

HDD Management

Before format SD cards, back up your data first.

1. Select the online devices whose SD cards you want to format.
2. Enable **Format SD Card**.
3. Click **Apply**.

Cloud Storage

Refer to Cloud Storage Settings.

7.5.9 System

Support configuring account security and user management.

Account Security Settings

Configure a reserved mobile number for password reset verification. Enter the mobile number, confirm it, provide the administrator password, and then apply the settings.

User Management

In phased delivery projects, users can add new users with the same configuration and permissions as previously delivered batches in subsequent phases. Supports adding, modifying, and deleting users and their permissions. Administrators can create up to 31 users.

Click **Add User** (for the first time) or **Add**.

See the following parameters.

- **User Name:** User names may only contain numbers and letters. Special characters are not supported.
- **User Types**
 - **Administrator:** Has full operational privileges, can add guests and operators, and assign permissions to them.
 - **Guest:** Remotely view logs and statuses, perform remote preview, and remote playback/download.
 - **Operator:** Supported permissions are configured by the administrator. Cannot create users.
- **Password**

To better protect your privacy and enhance product security, it is recommended to change risky passwords to strong ones. The following are considered risky passwords:

 - Less than 8 characters long
 - Contains only one type of character
 - Same as the user name
 - Reverse of the user name
 - Contains the user name
 - Contains the reversed user name

Password Strength Rules

- **Strong Password:** Combines 3 or more character types (e.g., digits, lowercase letters, uppercase letters, special characters).
- **Medium Password:** Combines 2 types among digits & special characters, lowercase & uppercase letters, or letters & special characters.
- **Weak Password:** Combines only digits and lowercase letters, or digits and uppercase letters.

7.5.10 Event

Motion Detection

Scenario

In exclusive residential areas or major facilities, access is restricted to residents and authorized individuals only. You can set the motion detection to capture pictures of movements and report them in real-time to a monitoring center.

Steps

1. Select devices and then select **Motion Detection**.
2. Enable **Motion Detection**.
3. Set the sensitivity. A higher value indicates greater sensitivity, making it easier to detect moving objects but also more prone to false alarms. If the sensitivity is set to 0, this function will not work.
4. (Optional) Enable **Notify Surveillance Center** to set a linkage method such as reporting alarms to the monitoring center when an event occurs.
5. Select **Apply**. You can select **Task Center** to view the progress.

Email

Scenario

You can enable the Email function to send an email to all recipients if an alarm event is detected such as the motion detection event, video loss, and video tampering. It is common to set the same email information for a group of cameras, so that when an alarm is triggered, it gets sent to the same email address.

Steps

☐ **Email**

☐ Enable ☒

☐ Sender Name

☐ Sender Address

☐ SMTP Server

☐ SMTP Port

☐ Email Encryption

☐ STARTTLS ☒

☐ Server Authentication ☒

☐ User Name

☐ Password

☐ Picture Attachment ☐

☐ Recipient + Add 🗑 Delete

☐	No.	Recipient ...	Recipient A...	Operation
☐	1	admin		✎ 🗑

Selected Device: 1 Channel: 1

Figure 7-18 Email

1. Select the devices and select **Email**.
2. Enable **Email**.
3. Set the parameters.

Parameter	Description
Sender Information	This includes the sender's name, sender's address, the SMTP server for the sender's email, and the SMTP port.
Email Encryption	- If you select TLS and do not enable STARTTLS, the email will be sent after TLS encryption, and the SMTP port number should be changed to 465. - If you select TLS and enable STARTTLS, it means the email will be encrypted via STARTTLS, and the corresponding SMTP port number is 25.

Parameter	Description
	 Caution To use the STARTTLS encryption method, ensure that your email server supports this protocol. If you select STARTTLS encryption but your email server does not support it, the encryption method will not be effective.
Server Authentication	The username and password for the sender's email.
Picture Attachment	Include a capture picture with the email. Adjust the capture interval based on your requirements.
Recipient	Click Add and enter the recipient's email details.

4. Select **Apply**.
5. (Optional) Go to the device's remote configuration page, and click **Test** to send a test email, and verify if it was sent successfully.

FTP

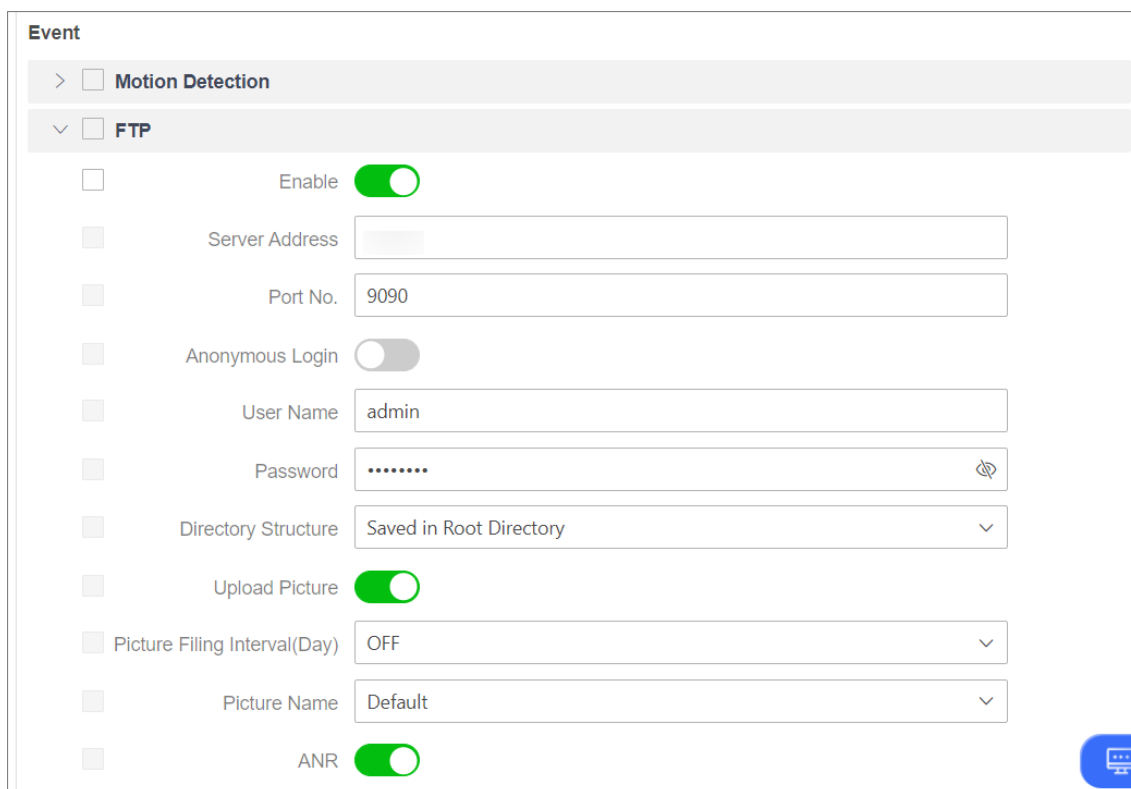
Scenario

Due to limited processing capabilities of the camera or limited network bandwidth, a camera does not perform local analysis but uploads captured images to an FTP server. This saves camera resources and reduces network traffic.

Prerequisites

- Ensure that an FTP server is available.
- The camera is configured with a capture schedule.

Steps



Event

- > ☐ Motion Detection
- ▼ ☒ **FTP**

☐ Enable ☒

☐ Server Address

☐ Port No.

☐ Anonymous Login ☐

☐ User Name

☐ Password 

☐ Directory Structure ▼

☐ Upload Picture ☒

☐ Picture Filing Interval(Day) ▼

☐ Picture Name ▼

☐ ANR ☒



Figure 7-19 FTP

1. Select the devices that require FTP configuration and select **FTP**.
2. Enable **FTP**.
3. Set the following parameters.

Parameters	Description
Server Address and Port	The IP address and port of the cloud storage server.
Username/ Password	Username and password with upload permissions. If anonymous users also have upload permissions, you can enable Anonymous Login , and the device will access the FTP server anonymously.
Directory Structure	The path where files are saved on the FTP server.
Upload Picture (Optional)	When this function is enabled, captured pictures will be uploaded to the FTP server. Set the picture name as needed. When Default is selected, captured pictures will have the device's IP address as a prefix.

Parameters	Description
Picture Filing Interval (Optional)	Automatically create folders on the FTP server to archive captured images by day for easy retrieval later. If the image archiving interval is set to 1 day, the device will create 1 folder per day with the name "Year_Month_Day-Year_Month_Day". Similarly, if the interval is set to 2 days, the device will create 1 folder every 2 days.
ANR (Optional)	In cases of poor network conditions or when the device cannot send information in a timely manner, alarm data is temporarily saved to the device's storage card and uploaded once the network is back to normal.

4. Select **Apply**.
5. (Optional) Go to the device's remote configuration page to check if the FTP feature is available. Events like motion detection, intrusion detection, line crossing detection, face picture capture, and multi-target-type detection can all be linked with FTP.

7.5.11 VCA Resource

The supported VCA resources vary by device model. You need to select devices of the same model for configuration. If you need to configure ten devices, and the first device supports three VCA resources while the others support only two, after the parameters are applied, the VCA resources not supported by the other devices will fail to be applied. However, this is a normal operation and there is no need to reapply.

Smart Event (Intrusion Detection)

Scenario

Intrusion detection refers to the process of identifying and reacting to unauthorized attempts to access, disrupt, or tamper with a protected area. You can set linkage actions when potential security breaches are detected. The function is only supported by certain camera models. Here are some key scenarios:

- In public spaces like airports, train stations, and shopping malls, intrusion detection systems can automatically identify unauthorized entries, loitering, or suspicious activities, triggering alerts for security personnel to take immediate action.
- In residential areas, these systems can monitor for unauthorized access to private properties, such as trespassing in yards or breaking into homes, providing homeowners with real-time notifications and deterring potential intruders. Industrial settings, including warehouses and manufacturing plants, benefit from intrusion detection to safeguard valuable assets and prevent theft or sabotage.
- For Industrial settings, including warehouses and manufacturing plants, benefit from intrusion detection to safeguard valuable assets and prevent theft or sabotage.

Steps

1. Select devices and select **VCA Resource**.
2. Select **Smart Event** → **OK**.
3. Select **Intrusion Detection** and enable this function.
4. (Optional) Enable **Notify Surveillance Center**.
5. Configure detection rules by device.

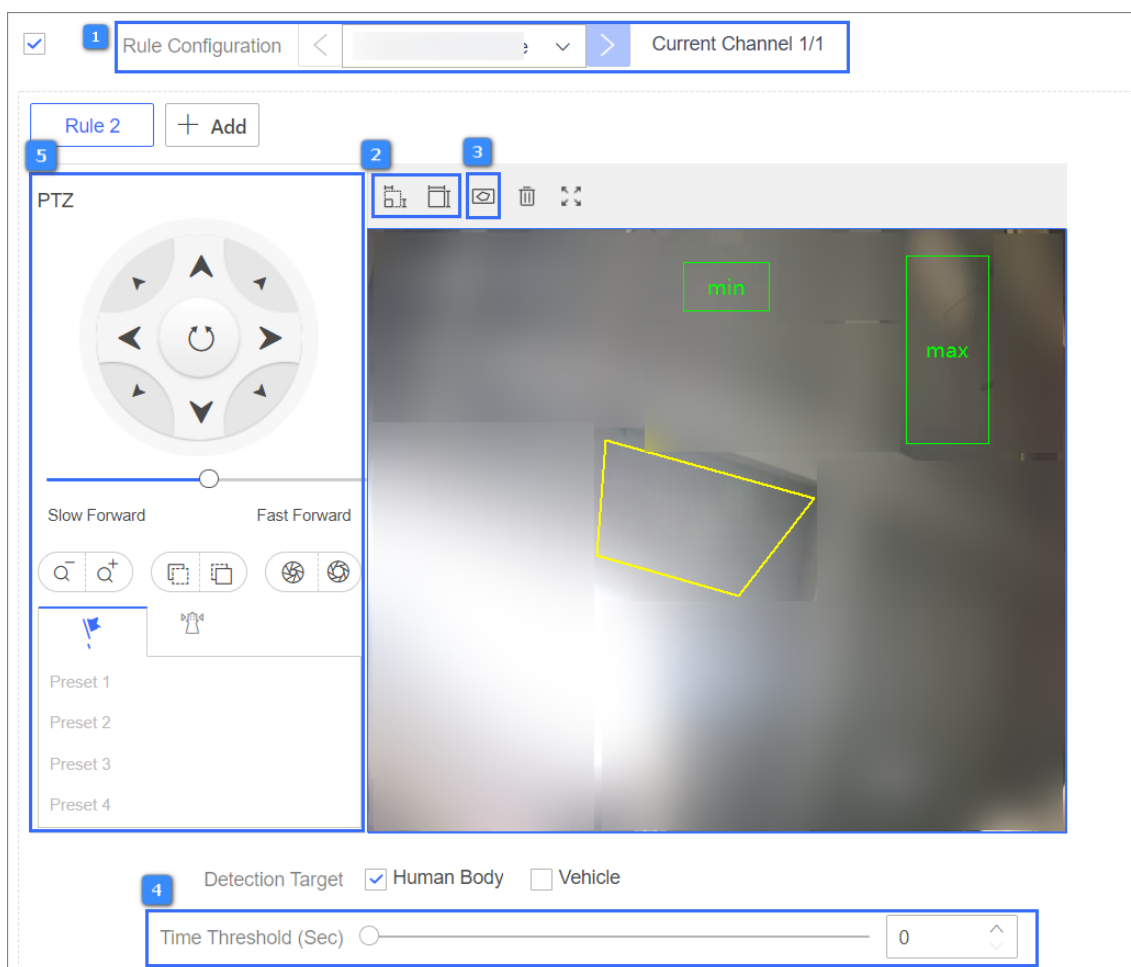


Figure 7-20 Configure Detection Rule

No.	Description
1	Select a channel to configure the detection rule.
2	Set the maximum and minimum target size. Targets smaller or larger than the valid size will not be detected.
3	A pre-defined area (up to 4 vertices) on the live view image. Targets enter and linger in the area will be detected and trigger an alarm.

No.	Description
4	The time threshold refers to the time of a target lingering in the detection area. If you set the value as 0, alarm is triggered immediately after the object enters the area.
5	Remotely control the camera's movement and zoom capabilities.

6. Select **Apply**.
7. **Test** whether the function works well.

Smart Event (Line-Crossing Detection)

Scenario

Here are some key scenarios:

- In traffic management, it helps enforce speed limits and detect violations by monitoring vehicles crossing designated lanes or boundaries, aiding in traffic flow optimization and accident prevention.
- In industrial settings, such as warehouses and manufacturing floors, line-crossing detection ensures that workers and machinery stay within safe zones, reducing the risk of accidents and improving operational efficiency.

Steps

1. Select devices and select **VCA Resource**.
2. Select **Smart Event** → **OK**.
3. Select **Line Crossing Detection** and enable this function.
4. (Optional) Enable **Notify Surveillance Center**.
5. Configure detection rules by device.

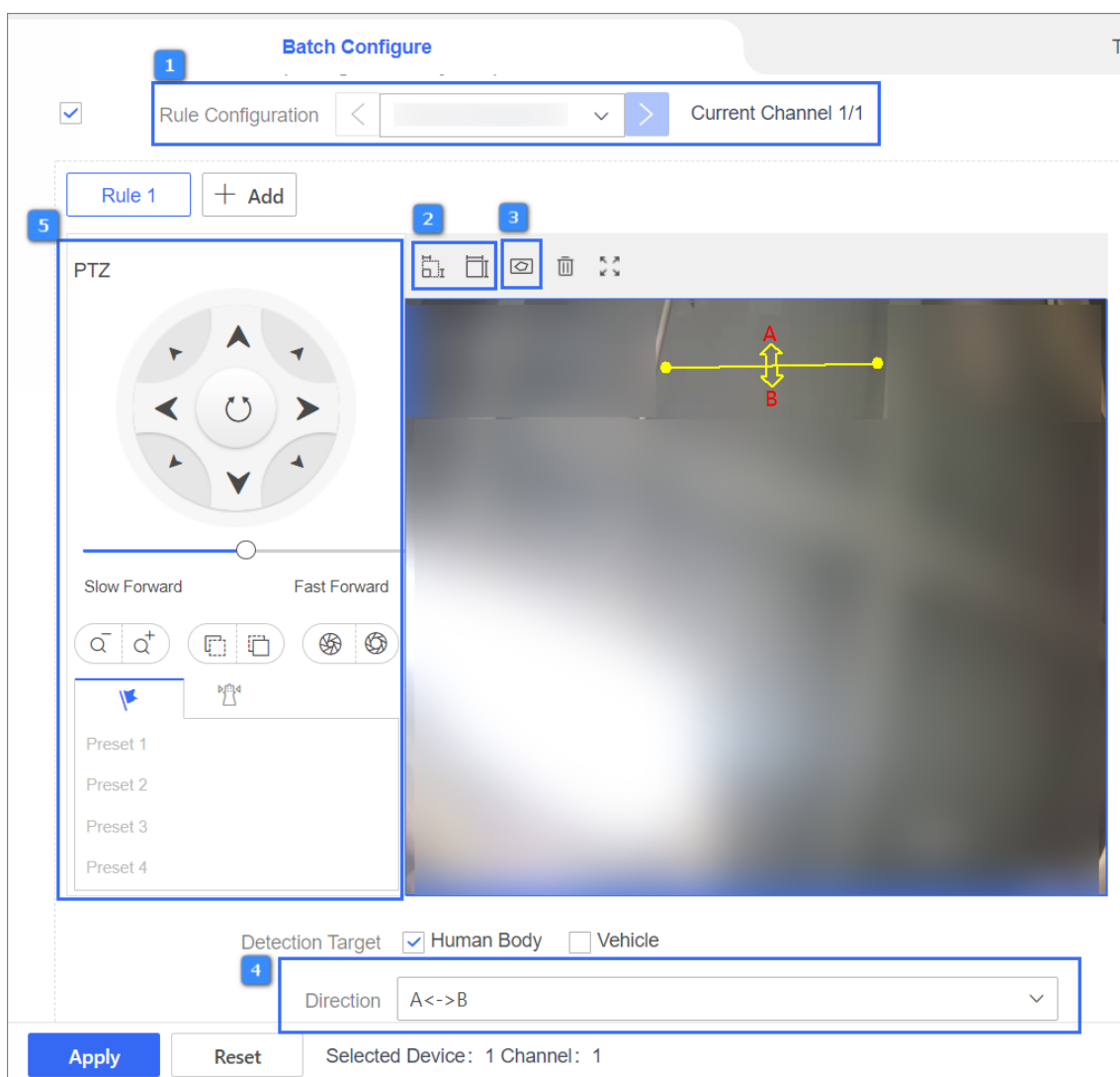


Figure 7-21 Configure Detection Rule

No.	Description
1	Select a channel to configure the detection rule.
2	Set the maximum and minimum target size. Targets smaller or larger than the valid size will not be detected.
3	Drag the end points of the dotted line to adjust the length and direction of the line.
4	A->B means only object crossing the line from A side to B side will be detected.
5	Remotely control the camera's movement and zoom capabilities.

6. Select **Apply**.
7. **Test** whether the function works well.

Face Picture Capture

Scenario

Face picture capture technology in monitoring cameras has a wide range of application scenarios. Here are some major scenarios. For security and monitoring, face picture capture can be used to grant or deny access to secure areas. For example, employees in a corporate office can be granted access to certain floors or rooms based on their facial recognition. It can alert security personnel if an unauthorized person enters a restricted area. For retail and customer experience, retailers can use face picture capture to analyze customer activities, to tailor marketing strategies.

Steps

1. Select devices and select **VCA Resource**.
2. Select **Face Capture** → **OK**.
3. Select **Face Capture** and enable this function.
4. Configure common parameters. The following table will introduce major parameters.

Parameters	Description
Face Capture Mode	- Best Shot: Capture and upload the highest-scoring face pictures as a target moves through a detection area. - Capture Threshold: The quality of face picture that triggers a capture and alarms. - Capture Times: The number of times a face picture is captured within a capture interval. - Quick Shot: Capture and upload face pictures if the score exceeds the quick shot threshold. Otherwise, the highest-scoring picture will be uploaded within the maximum capture interval. - Quick Shot Threshold: The quality of a face picture that triggers a quick shot. - Max. Capture Interval: The longest time to capture a single face picture as a target moves through a detection area.
Upload to FTP / SD Card / NAS	Capture pictures when an alarm is triggered and upload pictures to a FTP server, local memory card, or network attached storage (NAS).
Face Exposure	- Face Exposure: The device will provide supplementary lighting for faces detected in a scene. - You can go to the device's web configuration page to configure the reference brightness and minimum duration.

Parameters	Description
	- Reference Brightness: The device automatically adjusts the brightness of faces based on the reference brightness value. The brighter the face, the brighter the overall picture. - Min. Duration (min): The duration of exposure compensation for the face after it is detected.
Facial Posture Filter	Filter out facial poses based on left, right, forward, and upward angles. You can go to the device's web configuration page to set the angle. When you set both the upward and downward tilt angles to 30 degrees, the device will not capture pictures if the face moves more than 30 degrees away from the lens in either direction.

5. Configure detection rules by device.

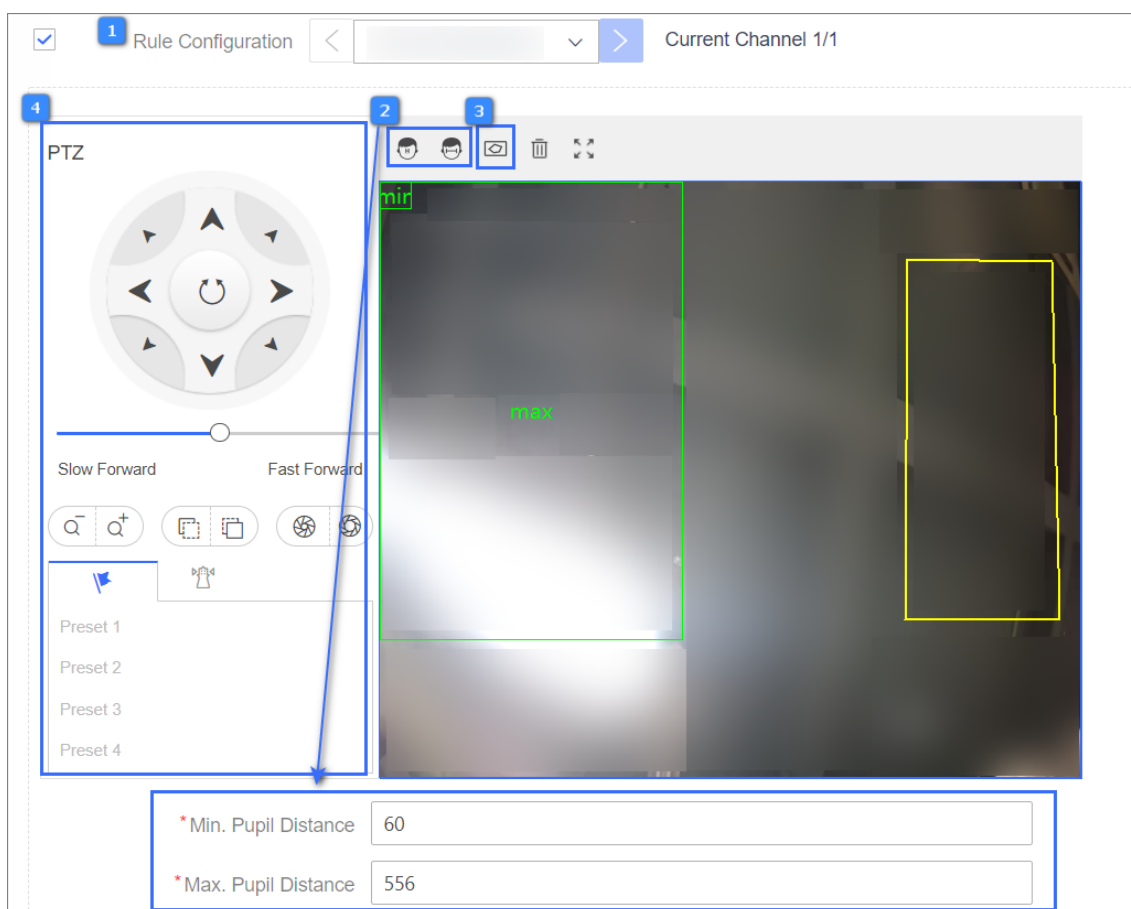


Figure 7-22 Configure Detection Rule

No.	Description
1	Select a channel to configure the detection rule.
2	Set the maximum and minimum pupil distance. If the pupil distance in the picture is larger /smaller than the maximum/minimum distance, the face will not be detected.
3	A pre-defined area (up to 4 vertices) on the live view image. Targets enter and linger in the area will be detected and trigger an alarm.
4	Remotely control the camera's movement and zoom capabilities.

6. Select **Apply**.
7. **Test** whether the function works well.

Multi-Target-Type Detection

Scenario

Multi-Target-Type Detection is designed to detect and differentiate between various types of objects or targets within a scene. This advanced feature can accurately identify and respond to different kinds of objects, such as people and vehicles.

Steps

1. Select devices and select **VCA Resource**.
2. Select **Multi-Target-Type Detection** → **OK** .
3. Select **Multi-Target-Type Detection** and enable this function.
4. Configure common parameters. The following table will introduce major parameters.

Parameters	Description
Face Capture Mode	- Best Shot: Capture and upload the highest-scoring face pictures as a target moves through a detection area. - Capture Threshold: The quality of face picture that triggers a capture and alarms. - Capture Times: The number of times a face picture is captured within a capture interval. - Quick Shot: Capture and upload face pictures if the score exceeds the quick shot threshold. Otherwise, the highest-scoring picture will be uploaded within the maximum capture interval.

Parameters	Description
	- Quick Shot Threshold: The quality of a face picture that triggers a quick shot. - Max. Capture Interval: The longest time to capture a single face picture as a target moves through a detection area.
Upload to FTP / SD Card / NAS	Capture pictures when an alarm is triggered and upload pictures to a FTP server, local memory card, or network attached storage (NAS).
Face Exposure	- Face Exposure: The device will provide supplementary lighting for faces detected in a scene. - You can go to the device's web configuration page to configure the reference brightness and minimum duration. - Reference Brightness: The device automatically adjusts the brightness of faces based on the reference brightness value. The brighter the face, the brighter the overall picture. - Min. Duration (min): The duration of exposure compensation for the face after it is detected.

5. Configure detection rules by device.

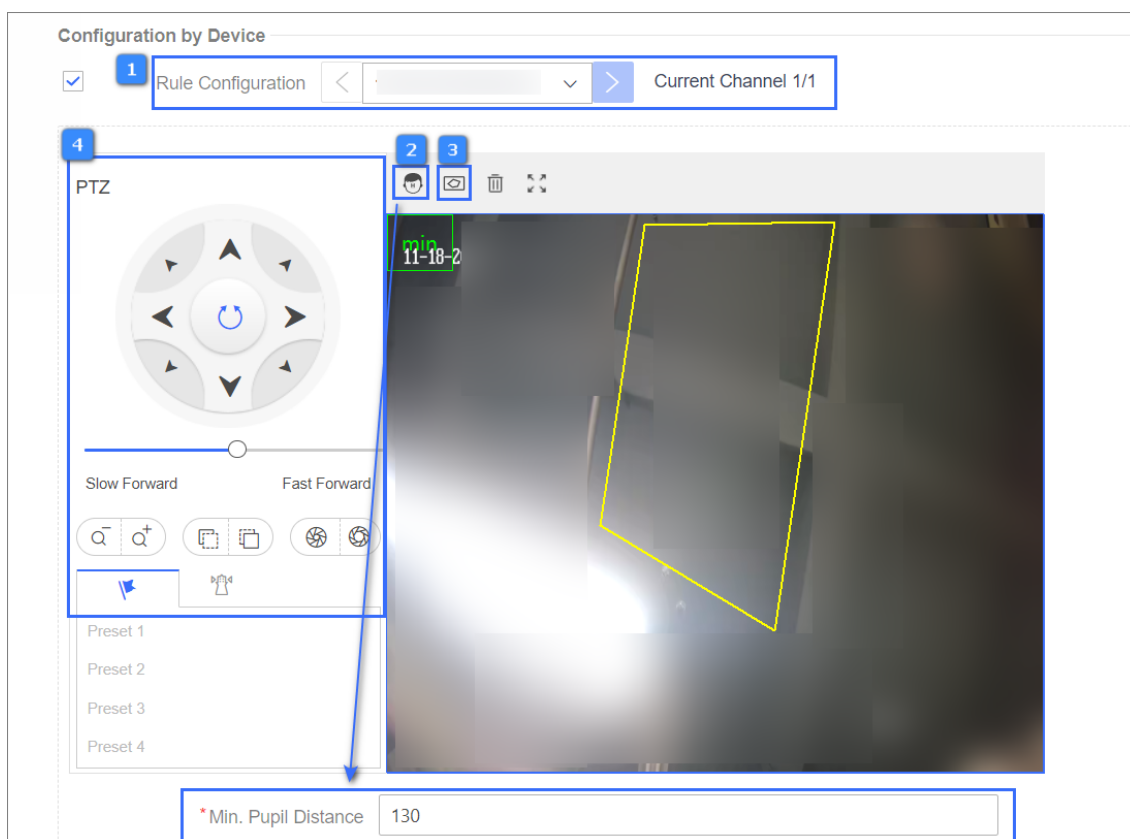


Figure 7-23 Configure Detection Rule

No.	Description
1	Select a channel to configure the detection rule.
2	If the pupil distance in the picture is smaller than the minimum distance, the face will not be detected.
3	A pre-defined area (up to 4 vertices) on the live view image. Targets enter and linger in the area will be detected and trigger an alarm.
4	Remotely control the camera's movement and zoom capabilities.

6. Select **Apply**.

7. **Test** whether the function works well.

7.5.12 Maintenance & Security

Support setting password reset methods and importing device parameters for quick data backup.

Password Reset Methods

- **Import/Export Key:** This method has a lower security level. It is recommended to disable it.
- The following reset methods are enabled by default and cannot be disabled:
 - Security Questions
 - Reserved Email
 - Reserved Mobile Number

Import Device Parameters

Refer to [Import Device Parameters](#)

7.6 Recording & Analysis

After adding cameras and recording & analysis devices like network video recorders, you can batch add cameras to a network video recorder for unified management. Additionally, network video recorders that support hard disk formatting can be batch formatted.

7.6.1 Add Cameras as Channels

Scenario

In scenarios such as a residential compound, if multiple cameras are installed but not powered on and networked during the initial installation, you can power and network the cameras, add them to HiTools Delivery for activation and parameter configuration, and then add all cameras to the compound's network video recorder for unified management.

Prerequisites

- Add cameras and network video recorders.
- The selected devices are of the same model.
- Ensure the selected devices are online, and the network is working well. If the network is bad or blocked, applying parameters may fail.

Steps

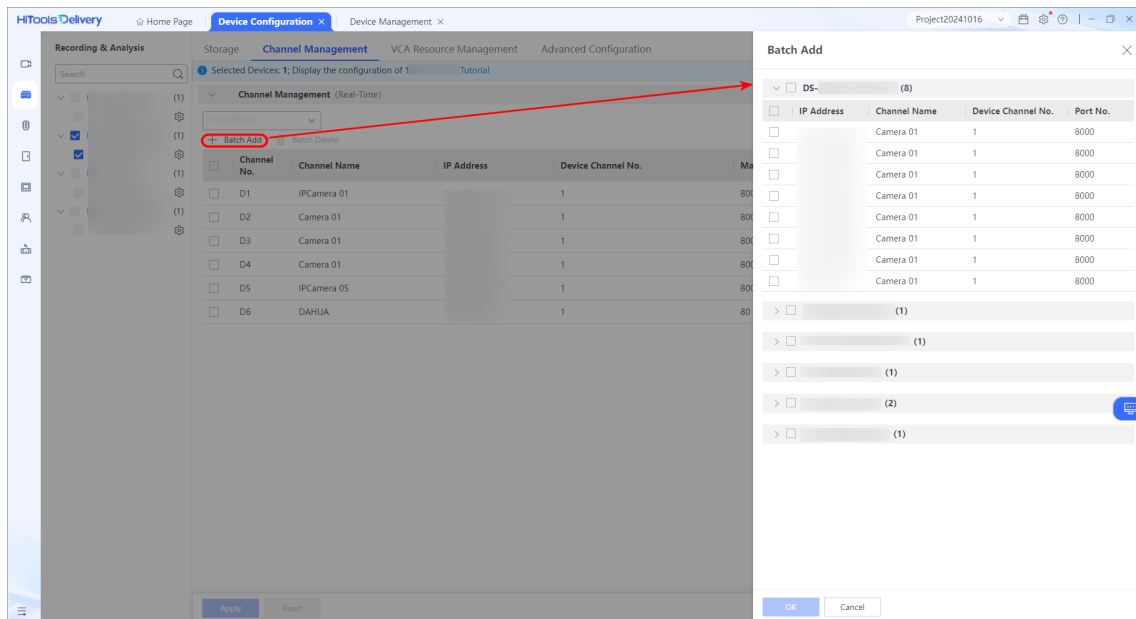


Figure 7-24 Add Cameras as Channels

1. Select a device and select **Channel Management** → **Batch Add** .
2. Select cameras to add as channels.
3. Select **Apply**. You can select **Task Center** to view the progress.

7.6.2 HDD Management

Prerequisite

- Back up your data first before formatting the HDD.
- This function should be supported by devices.

Steps

1. Select a device and select **Storage** → **HDD Management** .
2. Enable **Format Local Drive**.
3. Select **Apply**. You can select **Task Center** to view the progress.

7.6.3 Others

- HEOP
- Custom Configuration
- Configure More (NVR、DVR、DeepinMind Edge)

7.7 Intelligent Traffic

This chapter mainly introduces how to configure the platform access, application mode, capture parameters, and video parameters.

Entry

Select **Intelligent Traffic**, select parameters, and apply them.

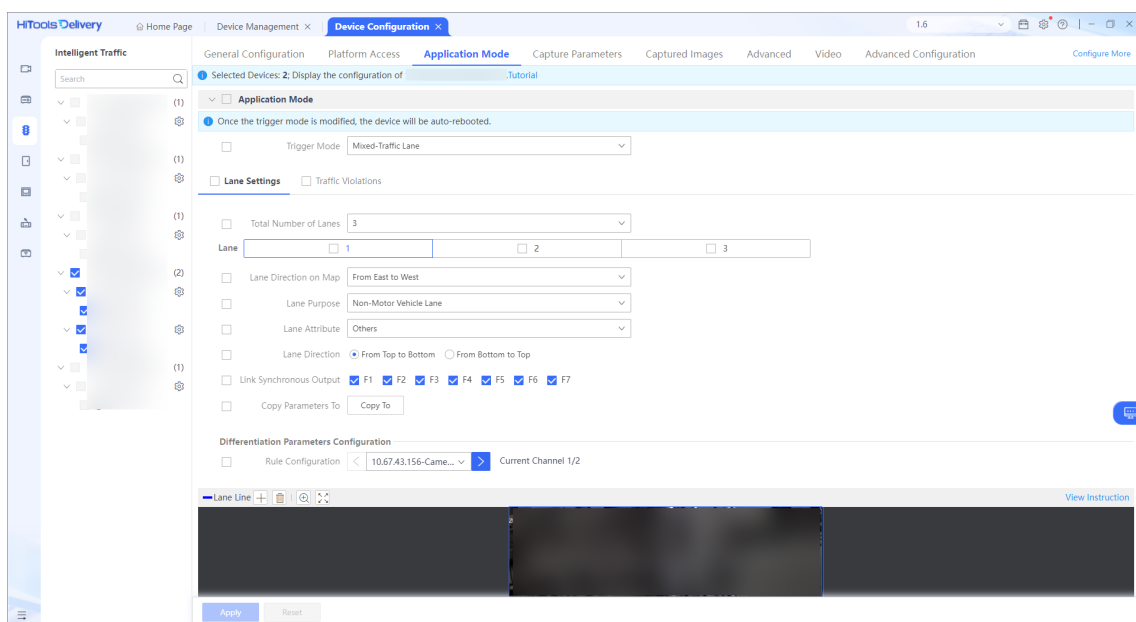


Figure 7-25 Intelligent Traffic Configuration

Prerequisites

- The selected devices are of the same model.
- Ensure the selected devices are online, and the network is working well. If the network is bad or blocked, applying parameters may fail.

Configuration

- General
- Platform Access
- Application Mode

- **Capture Parameters**
- **Captured Images**
- **Video**
- **Advanced**
- **Custom Configuration**

Configuration Verification

After applying the application mode, go to **Configuration Verification → Installation Quality** to test installation quality.

7.7.1 General Configuration

Video Encoding

The major parameters are as follows:

Stream Type

Select the stream type according to your needs. Main stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission. Sub-stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space. Third stream is offered for customized usage.



Note

The supported stream types vary with different models. The actual device prevails.

Frame Rate

It is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Resolution

The higher the resolution is, the clearer the image will be. Meanwhile, the network bandwidth requirement is higher.

Bitrate Type

Select the bitrate type to constant or variable.

Video Encoding

The device supports multiple video encoding types, such as H.264, H.265, and MJPEG. Supported encoding types for different stream types may differ. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate, and image quality.

Time

Refer to ***Time Settings*** .

7.7.2 Platform Access

FTP

To upload and store captured images on an FTP server, you must first deploy the FTP server and ensure that the device has normal network communication with the server. All configured OSD information will be pushed to every deployed FTP server.

The major parameters are as follows:

Table 7-5 Major Parameters

Parameter	Description
Server Address/Port No./User Name/Password	Enter the FTP server login information.
Upload Protocol Type	SFTP provides an encrypted transmission method for file transfer.
Path/Picture Name Encoding Mode	UTF-8: The international universal UNICODE encoding standard, which supports characters from virtually all global languages.
Directory Structure	You can customize the directory structure according to your needs.
Connection Mode	Transitory Connection The device connects to the FTP server for a single transaction. Each file upload requires a new FTP login. Persistent Connection The device maintains a persistent connection with the FTP server until the user manually logs out of the FTP connection.
Upload Content/Name Rule	Set the type of images to be uploaded. You can also customize the image naming rules.  Note Supported functions vary with different models. The actual device prevails.
OSD Information	Click Export Template , fill in information such as the Intersection ID and Device ID , and then Import Template . This will upload the OSD information along with the images to all FTP servers.

Parameter	Description
	 Note If OSD information is configured here, the overlay items added in the Image Overlay section will automatically reuse the OSD information.

Arm Upload

The device uploads captured images and target information in real-time to the (PC) via selected protocol.

You can instantly receive the camera's captured images to verify the device's capture function and debugging results.

Select the target device, click **Arm Upload**, and select a protocol.

Note

Select **License Plate Alarm** by default. For protocol details, refer to the ISAPI Developer Guide.

More Configuration

- [Cloud Storage](#)
- [ISUP](#)

7.7.3 Application Mode

This document introduces the main parameters only. For detailed configuration information, please refer to the device user manual.

After applying the application mode, you can go to **Configuration Verification → Installation Quality** to [test installation quality](#).

Data Collection

Lane Settings

Traffic cameras monitor traffic data such as lane flow, queue length, average speed, and lane status. The trigger modes are Video Analysis E-Police or Incident Detection.

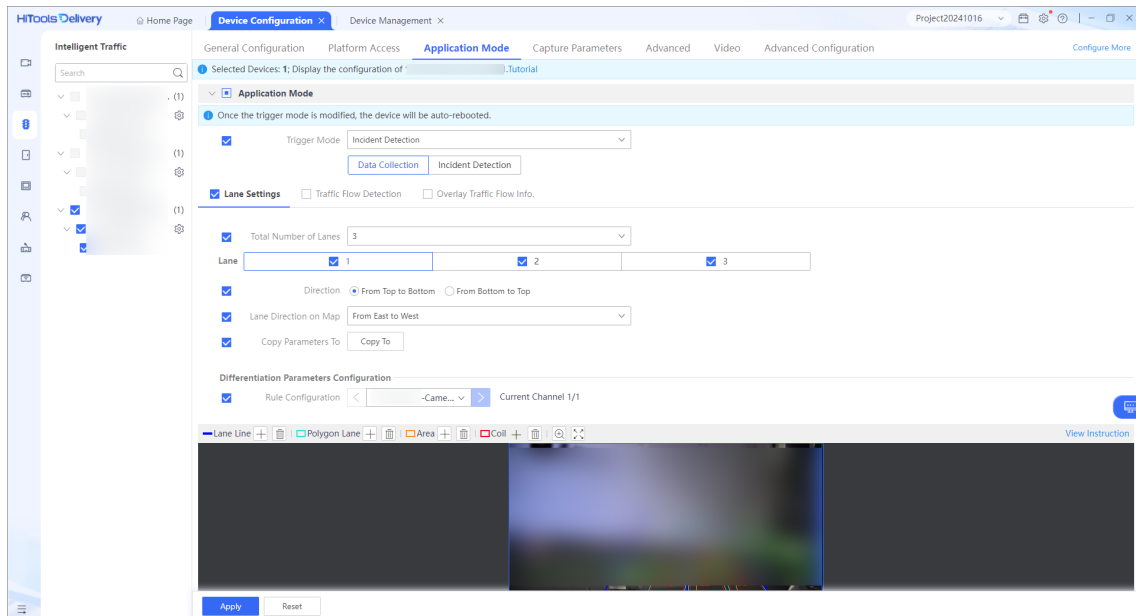


Figure 7-26 Lane Settings

1. Click **Data Collection** and check **Lane Settings**.
2. Set the relevant parameters. The table below covers the **main parameters** only.

Table 7-6 Main Parameters

Parameter	Introduction
Direction	- From Top to Bottom: Vehicles are moving toward the device's mounting location. - From Bottom to Top: Vehicles are moving away from the device's mounting location.  Note Configure each lane based on actual conditions. Incorrect direction settings will prevent traffic flow detection from being triggered.
Lane Direction on Map	Set this according to the actual geographical direction of the lane. For example, From West to East means the device is collecting data for traffic traveling from west to east.

Traffic Flow Detection

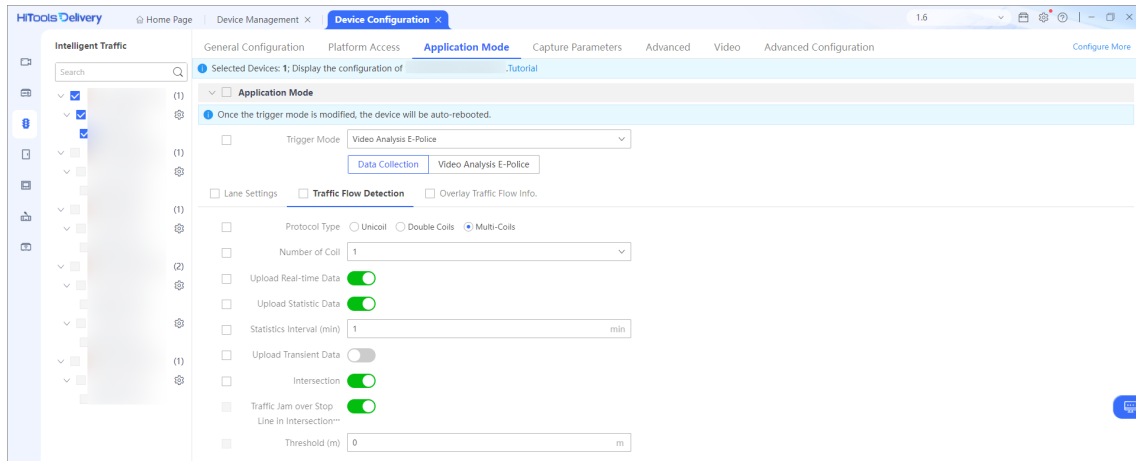
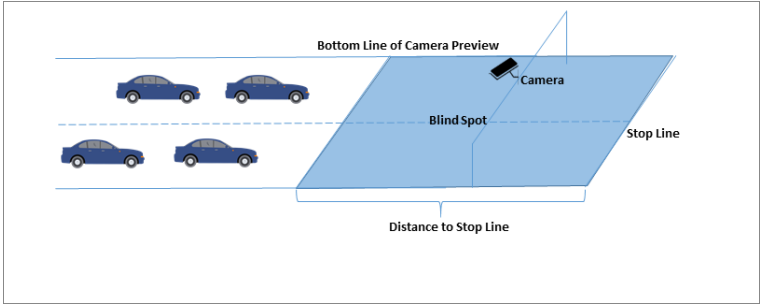
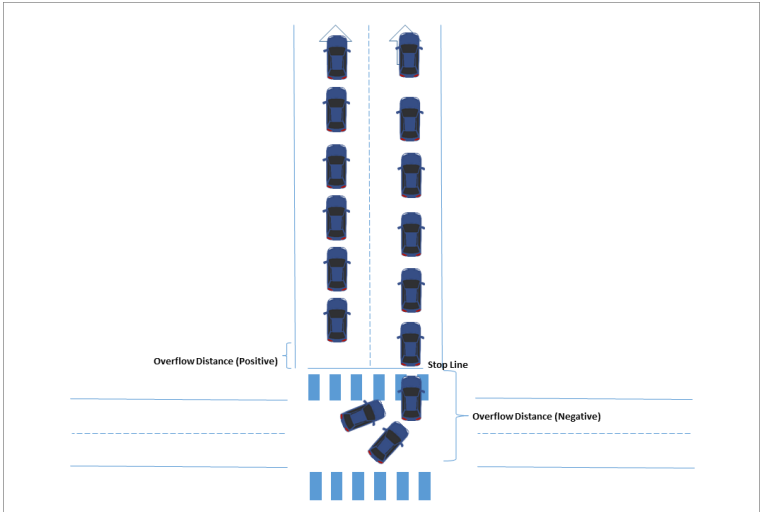


Figure 7-27 Traffic Flow Detection

Table 7-7 Main Parameters

Parameter	Description
Protocol Type	Usually select Multi-Coil . The number of coils should be set according to the actual installation.
Upload Real-time Data	Includes Lane No., Traffic Flow of Left Turn, Traffic Flow of Right Turn, etc. The specific data types are configured in the Overlay Traffic Flow Info settings.
Upload Statistic Data	Includes the average lane space occupancy and average lane time occupancy. The specific data types are configured in the Overlay Traffic Flow Info settings.
Upload Transient Data	Includes the Traffic Jam over Stop Line in Lane (Lane Overflow) and Number of Vehicles in Lane. The specific data types are configured in the Overlay Traffic Flow Info settings.
Distance to Stop Line	If the Intersection function is not enabled , the Stop Line Distance is the distance between the stop line and the device's blind spot. The actual vehicle queue distance is calculated as the Stop Line Distance plus the vehicle queue distance shown on the screen.

Parameter	Description
	 Figure 7-28 Distance to Stop Line
Intersection	This is applicable to traffic collection scenarios that include an intersection. Traffic Jam over Stop Line in Intersection (Intersection Overflow) occurs when a queue of vehicles in an exit lane (downstream) backs up through the intersection and into the approach lane (upstream), often blocking traffic trying to move in adjacent directions. If Intersection Overflow is enabled, set the overflow threshold. If the queue tail distance from the stop line in the backward direction (from bottom to top in the preview screen) is less than the threshold, an intersection overflow is detected.  Note  Figure 7-29 Intersection Overflow Distance

Parameter	Description
	- A positive overflow distance means the queue tail is still within the stop line area. - A negative overflow distance means the queue tail has exceeded the stop line.
Linked Lane No.	Select the lanes for which you want to collect data. If a lane is not associated, no data will be collected for it.
Number of Vehicles in Area	This counts the number of vehicles in a customized area extending 80 meters from the stop line.

Overlay Traffic Flow Info

Table 7-8 Main Parameters

Parameter	Description
POS Information	When enabled , POS information is superimposed onto the video stream and displayed in the preview window, allowing for data observation.
X/Y Position	The coordinates are based on the top-left corner of the preview screen as the origin point (0, 0).
Real-Time Data/ Statistics Data/ Transient Data	Select the desired data types to overlay.
Scheduling Clearing	Periodically clears the selected Real-Time, Statistical, and Transient data. The POS information overlay will remain visible.

Line Drawing

Coil

Coil Drawing Rules:

- Upper Edge:** The upper edge of the coil should be set at a height equivalent to **0.5 times the length of the first vehicle's body**, and must **not be higher than the rear wheel** of the leading vehicle.
- Lower Edge:** The lower edge of the coil is the **stop line**.

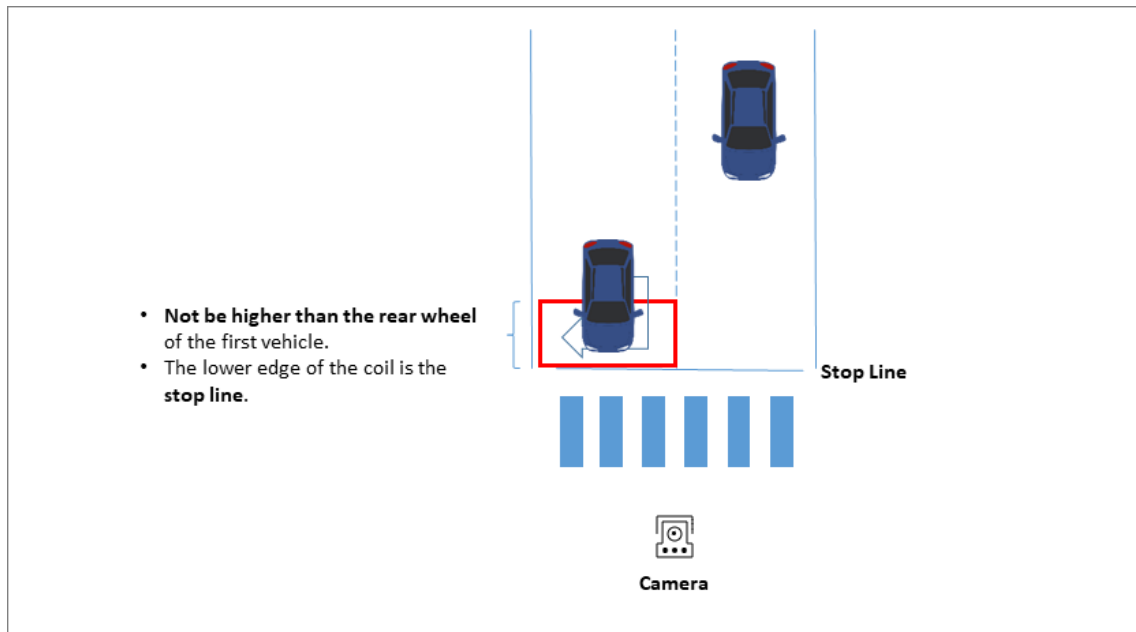


Figure 7-30 Coil Drawing

Stop Line

The stop line must align with the **actual marking on the road surface**. If there is a stepped stop line (staggered stop lines for different lanes), it is recommended to draw a single stop line connecting the leftmost and rightmost lane endpoints.

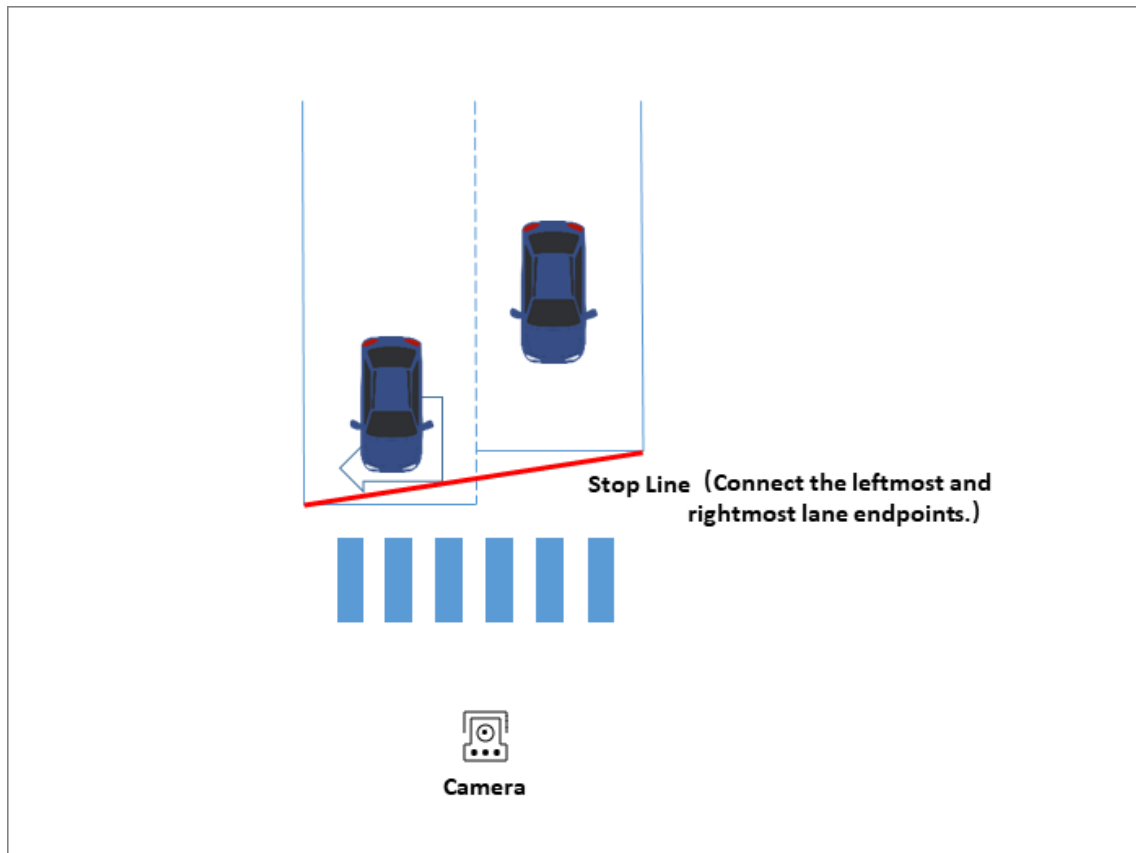


Figure 7-31 Stop Line Drawing

Border Line

The drawing rules are as follows:

- **Left/Right Turn Borderlines:** These lines must be positioned at least **0.5 vehicle body lengths** away from the edge of the preview screen.
- **Standard Mounting:** The left and right border lines should be placed **outside the extension line** of the leftmost/rightmost lane used for calculating traffic flow of left turn and right turn.

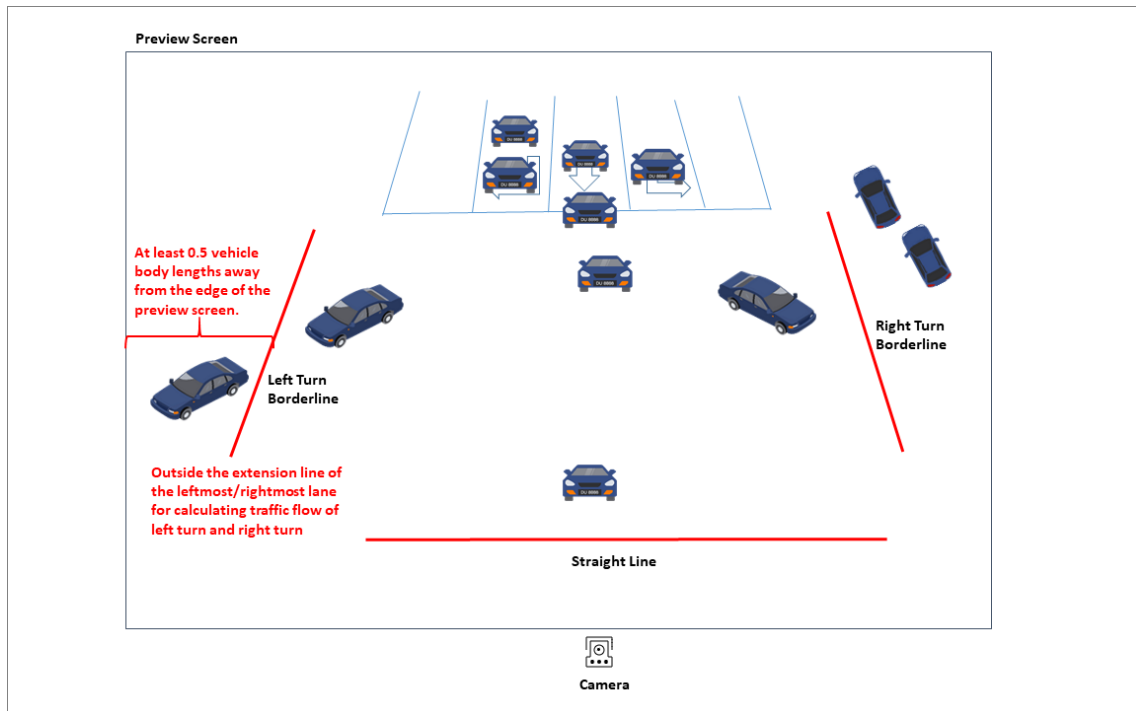


Figure 7-32 Standard Mounting

- **Non-Standard Mounting:** Observe the actual vehicle trajectories. **Ensure that a vehicle only touches one trigger line** during its movement to prevent vehicles from prematurely triggering the straight line while executing a turn.

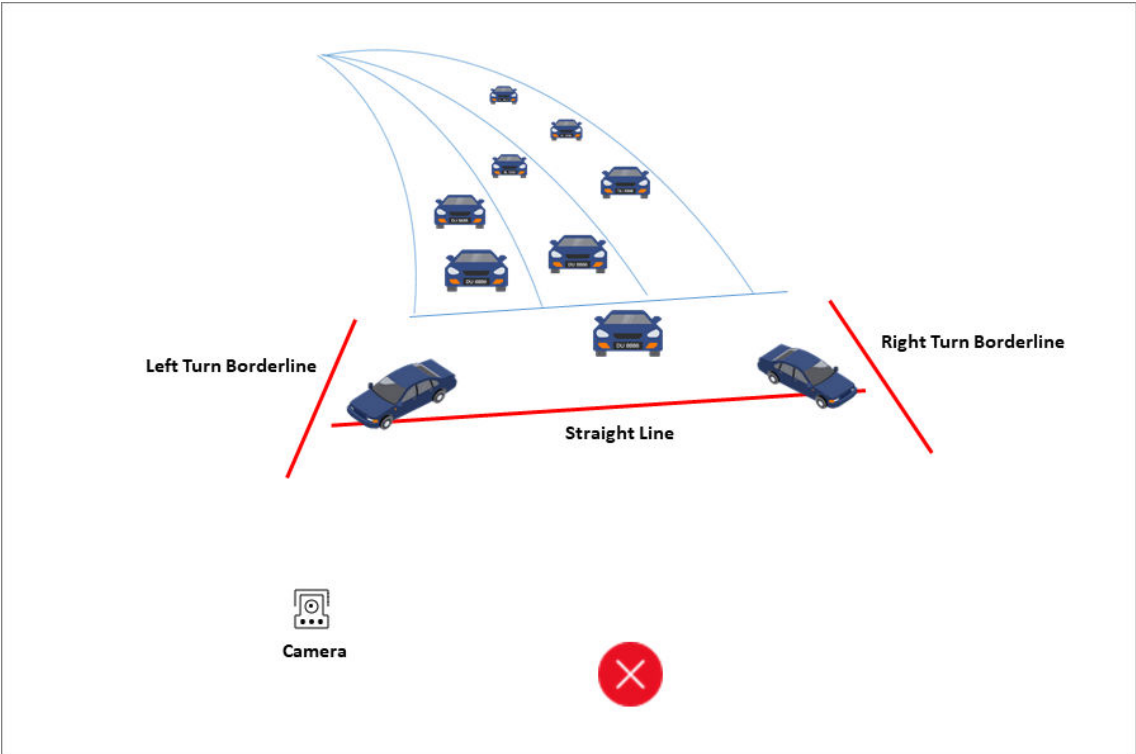


Figure 7-33 Wrong Borderline Drawing for Non-Standard Mounting

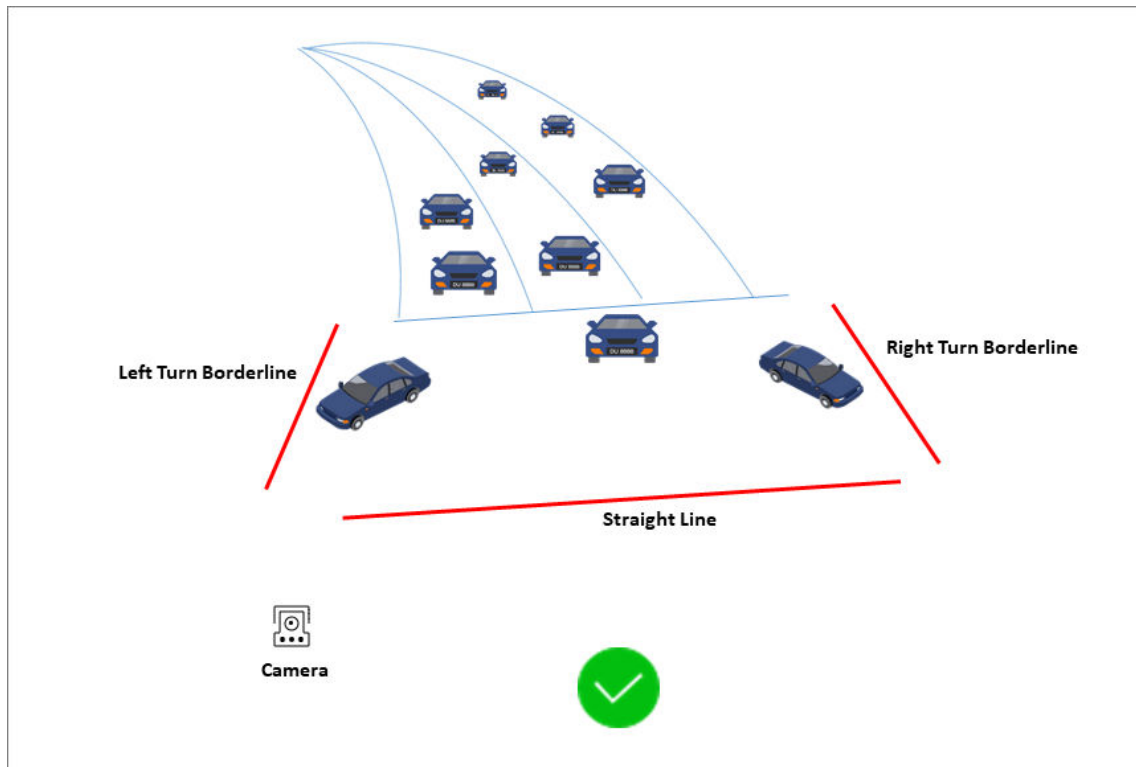


Figure 7-34 Correct Borderline Drawing for Non-Standard Mounting

Lane

- **Straight Lanes:** It is recommended to use **polygonal lanes**.
 - The **upper endpoint** of the straight lane line should be configured approximately **200 meters** away from the stop line.
 - The **lower endpoint** should be drawn at the **stop line position**.
- **Polygonal Lanes:** The **upper endpoint** should also be configured approximately **200 meters** away from the stop line.

Note

- **Visibility Adjustment:** If the 200-meter point is not clearly visible on the screen, adjust the lane line length based on **actual visibility**.
 - **Curved Lane Scenarios:** If the far end of the curve is obscured by trees or heavily blocked by vehicles, the upper endpoint of the polygonal lane line should be placed at a location where the vehicle's lane can be **accurately and visually distinguished** with minimal obstruction.
-

Incident Detection

The trigger modes are Video Analysis E-Police or Incident Detection.

Lane Settings

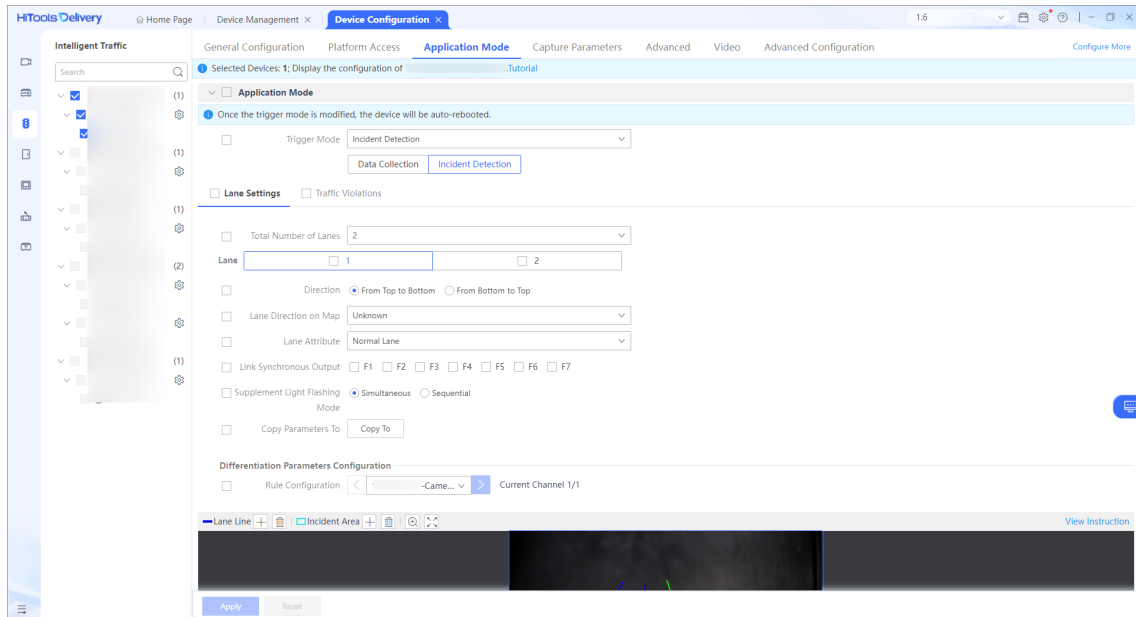


Figure 7-35 Lane Settings

Table 7-9 Main Parameters

Parameter	Description
Lane Attribute	- Trunk Forbidden Lane: If Lane Occupation by Large-Sized Vehicle is selected in the violation events, a heavy vehicle traveling in this lane will trigger an evidence capture. - Emergency Lane: If Emergency Lane Occupation is selected in the violation events, a heavy vehicle traveling in this lane will trigger an evidence capture.
Link Synchronous Output	This setting is optional if there is no associated strobe light connected.
Supplement Light Flashing Mode	If there is no associated strobe light connected, you can use the default setting: Simultaneous .
Speed Settings	If a vehicle's travel speed falls below the Abnormally Low Speed threshold or exceeds the Abnormally High Speed threshold, the speed measurement is considered anomalous. In this case, the device will randomly assign the vehicle a normal speed value between the specified low-speed limit and high-speed limit.

Note

Refer to **Table 7-6** for other parameter configuration.

Traffic Violations

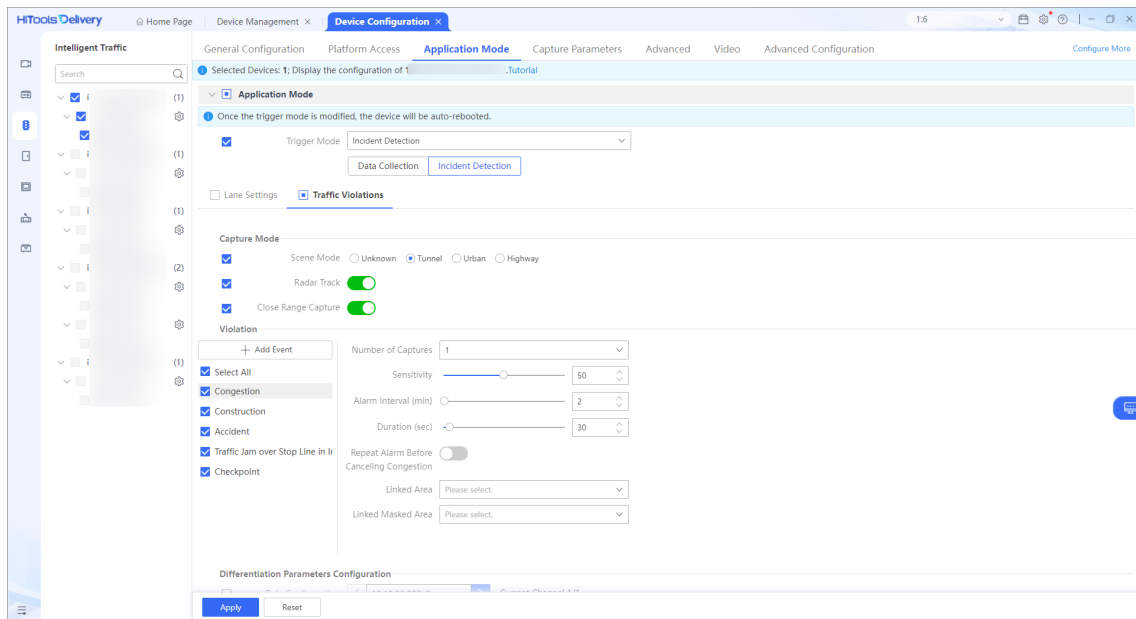


Figure 7-36 Traffic Violation Settings

Capture Mode

Table 7-10 Main Parameters

Parameter	Description
Scene Mode	Select the mode based on the actual traffic scenario. The types of violation events supported will vary depending on the chosen scene mode.
Radar Track	For complex events like Continuous Lane Change or Slalom Driving , the moving trajectory of the target vehicle can be superimposed onto the capture image for clearer evidence.
Close-Range Capture	After capturing and recognizing the license plate from a far distance , the system will automatically perform a second capture to recognize the license plate again as the vehicle drives closer.

Violation

Click **Add Event** and select the required violation events, then configure the associated parameters. The events are described in the table below. For more details, refer to the device user manual.

Event	Capture Settings & Description
Congestion	One capture. The device captures a picture when the detected road congestion time exceeds the configured congestion duration .
Construction	One capture. Requires the presence of road barriers/cones and people in the scene. If Sensitivity is set to 50, at least two barriers must be present. The device captures a picture when the detected construction duration exceeds the configured Duration .
Roadblock	One capture. The device captures a picture when the detection duration of road barriers (such as cones or crash barrels) exceeds the configured Duration .
Pedestrian Detection	Set the number of captures to 1–3 , as required. The device captures a picture when a pedestrian (with a clear outline) is detected for longer than the set Duration .
Fallen Object	One capture. The device captures a picture when a fallen object (tire, rock, bag, etc.) is detected for longer than the configured Duration .
Accident	One capture. Triggered by a rear-end collision or crash between two vehicles, accompanied by people exiting the vehicle to inspect the damage. The device captures a picture when the detected accident duration exceeds the configured Duration .
Single Vehicle Breakdown	Triggered by a single vehicle stopping due to a fault, accompanied by people exiting the vehicle to inspect the fault.
Low Visibility	Determined by the maximum detection range of targets via video and radar. A capture is triggered if this maximum distance remains below a set threshold for a continuous period.
Wrong-Way Driving	Two captures. The device captures pictures when a vehicle's actual driving direction is opposite to the configured lane direction.
Stopped Vehicle	Set the number of captures to 1–3 , as required. Draw the Illegal Parking Area and set the parking duration. The device captures pictures if a vehicle is stopped within the area for longer than the set duration.
Slalom Driving	Three captures. Triggered when a vehicle repeatedly changes lanes between two adjacent lanes over a short distance (less than 50 meters). Sensitivity (default 50) represents the curvature of the snaking path. The

Event	Capture Settings & Description
	event is captured if, after a lane change, the vehicle's center is closer than 1/4 of the lane width to the lane center line.
Low-Speed Driving	Three captures. Supports forward/backward detection. Set the minimum speed limit . If a detected vehicle's speed is below this limit, a capture is triggered.
Street Racing	Three captures. Supports forward detection only. Set the speed threshold and the number of overtakes according to requirements. Captures are triggered if the event occurs.
Speeding	Triggered when the vehicle's speed exceeds the threshold . If detection is configured by triggering line, set the Capture Position Ratio (default 50), meaning the capture is triggered when the vehicle passes 50% of the preview screen's height .
Not Slowing Down at Crosswalk	Three captures. Supports forward/backward detection. Set the maximum and minimum speed limits and draw three crosswalk lines according to requirements. Captures are triggered if the event occurs.
Not Keeping Safe Following Distance	Three captures. Supports backward detection only. Set the Speed Threshold. If the speed is above the threshold, the distance must be less than the High-Speed Minimum Distance. Captures are triggered based on the following: If the speed is below the threshold, the distance to the preceding vehicle (in the same lane) must be less than the Low-Speed Minimum Distance. If the speed is above the threshold, the distance must be less than the High-Speed Minimum Distance. Check Display Vehicle Distance to overlay the vehicle spacing onto the capture image.
Continuous Lane Change	Three captures. Supports forward detection only. Set the Driving Distance . Captures are triggered if the vehicle changes lanes continuously within the set distance.
Driving on the Lane Line	2–3 captures. The lane lines must be correctly drawn and set to the type White Solid Line or Broken-Solid Line . Captures are triggered 2-3 times when a vehicle drives on/across the lane line. If Detection by Area is selected, only events within the associated area will trigger a capture.
Lane Change	Three captures. The lane lines must be correctly drawn and set to the type White Solid Line . Captures are triggered three times when a vehicle crosses the lane line to change lanes. If Detection by Area is selected, only events within the associated area will trigger a capture.

Event	Capture Settings & Description
Overtaking on the Right	Three captures. Supports backward detection only. The event is triggered when a following vehicle changes into the right lane to overtake, and then moves back into its original lane.  Note This event is only applicable when traffic flow is from bottom to top in the preview screen.
Emergency Lane Occupation	Triggered when a vehicle enters a lane designated as an Emergency Lane attribute. If Detection by Area is selected, only events within the associated area will trigger a capture.
Lane Occupation by Large-Sized Vehicle	Three captures. Supports both forward and backward detection. Triggered if a heavy vehicle travels in a lane designated as a Trunk Forbidden Lane .
Queue Jumping	Three captures. Supports forward detection only. Triggered when traffic is congested, and a vehicle cuts in and changes lanes into the space between two vehicles in the adjacent lane. The device captures three pictures to document the cutting-in process.

Mixed-Traffic Lane

Refer to **Table 7-9** in Data Collection and Incident Detection and **Traffic Violation Settings** for details.

Video Analysis E-Police

Refer to **Table 7-9** in Data Collection and Incident Detection and **Traffic Violation Settings** for details. For more violation events, refer to the device user manual.

7.7.4 Capture Parameters

LPR

Table 7-11 Major Parameters

Parameter	Description
Forward	Capture the front of the vehicle (vehicle approaching the device).
Backward	Capture the rear of the vehicle (vehicle moving away from the device).

Supplement Light



Note

- This function is only applicable to the device supporting supplement light.
- The supported parameters vary with different models. The actual device prevails.

Output Mode

Flash Light Mode

The flash light will be triggered by the signals and output high intensity illumination instantaneously. The light can pass through the windshield and help capture the details.

Flash Light Mode

The flash light will be triggered by the signals and output high intensity illumination instantaneously. The light can pass through the windshield and help capture the details.

Housing Fan Mode

You can select this mode to enable the housing fan of the device.

Polarizer Mode

Select it when the image is partially overexposed due to the too strong reflection light.

Constant Light Mode

The constant light supplements light for the scene.

Switch Line Mode

For the environmental protection devices, the supplement light will be controlled by the switch line to flash white light at daytime and IR light at night.

Output in Advance

It is the preact time [0 to 1000 μ s] of the flash light, to ensure that the flash light is on when capture is triggered.

Output Dwell Time

It is the dwell time [0 to 10000 μ s] after the flash light responds. The actual flash light supplement time is the result of the dwell time minus advanced time.

Effective Status

Select the effective status of the supplement light according to the actual condition.

High/Low

When high/low level signal is output to the supplement light, the light will flash.

The effective status should stay different with the default status for I/O to take effect. And the default status changes according to the selection of the effective status. If you set the effective status as high level, the default level goes to low level. Set **Brightness Grade** for the flash light.

Pulse

When pulse signal is output to the supplement light, the light will flash.

If you set the effective status as pulse, you can select **Default Status** as high level or low level, and set other parameters.

Strobe High-light Enhancement

Select the level to enhance strobe light. If you select **Low**, set **Brightness Grade** for the strobe light.

Frequency Coefficient

It is the frequency multiplication of 25 of output pulse by flash light, to keep the flash light as constant. You can set it as default value.

Duty Ratio

It is the time occupation of the high level in a certain period. The higher the duty ratio, the brighter the light. High duty ratio will cut life span of the light.

Light Compensation Mode

Select **Checkpoint** to enable checkpoint capture light supplement. Select **Violation Action** to enable violation capture light supplement.

Activation Mode

Default

Disable the supplement light.

Time Schedule

Enable the supplement light during a fixed time period.

Environment Brightness

The supplemental light should be automatically controlled based on the ambient brightness. A brightness threshold can be set, where a higher threshold makes it more difficult for the supplemental light to turn on.

License Plate Brightness

Enable the supplement light automatically when the light is insufficient for license plate capture.

Sync. with Day/Night Switch Time

Keep the day/night switch of the supplement light consistent with ICR.

Violation Dictionary

The Violation Dictionary contains common illegal and non-compliant behaviors in road traffic. It is used to clearly define the **violation behavior** and the corresponding **violation code**. You can manually input single entries or import a file.

Overspeed Dictionary

The Overspeed Dictionary defines the **violation code** corresponding to each type of speeding behavior, which facilitates the use of codes for identifying speeding incidents. **Using the default parameters is recommended.** You can manually input single entries or import a file.

Face Picture Matting

You can enable driver's, passenger's, or non-motor vehicle user's face picture matting on the capture violation pictures

Enable **Face Picture Matting** and configure parameters. The major parameters are as follows:

Face Picture Matting Object

Driver Face Picture Matting

Check it to mat the driver's face picture.

Passenger Face Picture Matting

Check it to mat the passenger's face picture. Check **Check out Front Passenger Forcedly** to mat the front passenger's face picture no matter there is someone in the seat or not. If not enabled, the front passenger's face picture will only be matted when detected.

Pedestrian's and Non-Motor Vehicle User's Face Picture Matting

Check it to mat the pedestrian's and non-motor vehicle user's face pictures.

Face Picture Matting of Non-Motor Vehicle Rear-seat Passenger

Check it to mat the face picture of the non-motor vehicle rear-seat passenger.

Face Picture Matting of Violation Picture

Check it to mat all the face pictures on the violation capture pictures.



Note

You cannot enable the face picture matting and masking for the same person. For example, if you have enabled driver face picture matting, you cannot enable driver face picture masking at the same time.

Face Picture Overlay Mode

Select the picture type(s) to overlay the matted face pictures. You can select multiple picture types. Please select one scene picture at least.

Overlay Frame on Matting

Check it to overlay frame on the matted picture.

Face Close-up Picture Cutting Ratio

Select the cutting ratio of the face close-up picture to be small, medium, or large.

Face Close-up Picture Ratio

Adjust the zooming ratio of the face close-up picture.

Matting Contrast Enhancement

Check it to enable the function and set the level. The higher the level is, the stronger the contrast between the matting and the overlaid picture will be.

Close-up Picture Output Mode

Not Output

The target close-up pictures will not be output when uploading matted face pictures.

Overlay on Picture

The close-up pictures overlaid with matted face pictures will be output.

Upload Arm

The target close-up pictures will be output simultaneously with matted face pictures.

Overlay and Upload Arm

A close-up picture overlaid with matted face pictures and an independent target close-up picture will be output.

Capture Overlay

Superimpose device detection information or target feature information onto the captured images and composite images.

Select the composite type and enable text overlay. The major parameters are as follows:

Overlay Style

Overlay OSD on Close-up Picture

Check it to overlay the OSD information on the close-up pictures.

Overlay Plate Close-up

Check it to overlay license plate close-up pictures on the captured pictures. Set **Plate Picture Close-Up Zooming Ratio** to adjust the close-up picture size.

Sync. Video Overlay

Enable the function to overlay OSD information on the captured pictures. If you select to overlay on the picture, make sure that the video OSD and picture overlay information does not overlap.

Overlay Content

Click **Add Overlay Item** to select the information to overlay.



Note

The overlay information varies with different models. The actual device prevails.

- **Default Type:** You can view the default overlay information name. If you have edited the name, you can refer to the default name for the definition.
- **Type:** You can edit a custom overlay information name.
- **Space:** Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.
- **Line Break Characters:** Edit the number of characters from 0 to 100 between the current information line and the previous information line. 0 means no line break.
- **Overlay Information:** For some information types, you can edit the detailed information.
- **Overlay Position:** If you check it, the current information will be displayed from a new line.
- **Operation:** You can click  /  to adjust the display sequence of the overlay information, or click  to delete the item.

Picture Encoding and Composition



Note

Functions and parameters vary with different models. The actual device prevails.

Image Encoding

If the captured pictures are not clear, set the resolution, size, and quality of the captured pictures.

The major parameters are as follows:

Capture Resolution

Select the resolution of the captured scene picture. When the picture size keeps the same, the higher the resolution, the more the picture will be compressed, and the slower the picture will be handled.

Close-up Picture Resolution

Select the resolution of the target close-up picture. When the picture size keeps the same, the higher the resolution, the more the picture will be compressed, and the slower the picture will be handled.

Picture Size

The size of the compressed captured picture. The actual size is related to the scene complexity.

Composite Picture Size

The size of the compressed composite picture. The actual size is related to the scene complexity.



Note

Only the device supporting picture composition supports composite picture size settings. The actual device prevails.

Large Picture Quality (Scene/Composite)

Set the quality of the scene pictures and composite pictures. The value ranges from 1 to 100. The higher the value, the better the quality of the captured pictures.

Middle Picture Quality (Close-up)

Set the quality of the target close-up pictures. The value ranges from 1 to 100. The higher the value, the better the quality of the captured pictures.

Small Picture Quality (License Plate/Target/Face)

Set the quality of the license plate, target, or face pictures. The value ranges from 1 to 100. The higher the value, the better the quality of the captured pictures.

Picture Composition

Enable picture composition to merge multiple violation images into a single frame for easier viewing.

Set **Composition Type** for different picture quantities. Click **Configuration**, view the layout displayed on the interface for the composition effect.

The major parameters are as follows:

Close-up Zooming Ratio

The higher the value, the larger the close-up picture.

Non-Motor Vehicle Close-up Zooming Ratio

The higher the value, the larger the non-motor vehicle close-up picture.

Close-up Picture No.

It is the scene picture No. where the close-up comes from.

Close-up Offset

The default value is 0, which is recommended to be adopted. When the captured close-up picture is not complete, you can set the offset to a negative or positive value to adjust the capture area of the close-up picture.

Output Close-up Independently

Enable the function to output a close-up picture before or after the scene picture independently.



Note

Enabling composition and outputting close-up independently functions conflict with each other. You can only enable one.

7.7.5 Captured Images

ICR

The ICR (IR-Cut dual filter switch) setting allows the camera to capture clear images across varying light conditions.

Introduction

- **Daytime Mode (ICR On):** The IR-Cut filter is **engaged** (on). It is used to filter out infrared light, ensuring the camera displays a true, accurate **color image**.
- **Nighttime Mode (ICR Off):** The filter is **disengaged** (off). This **enhances light transmission** to maximize the use of available light, enabling the camera to acquire a clear image (typically in monochrome).

Major Parameters

- **Auto Switch**

The device automatically switches between Day and Night modes based on the **external ambient light level**.

When the external light is sufficient (i.e., **greater than the set threshold**), the ICR status is set to **Daytime**.

When the external light is insufficient (i.e., **less than the set threshold**), the ICR status switches to **Night**.

- **Manual Switch**

Allows the user to manually switch the ICR status to **Daytime** or **Night** according to operational needs.

- **Scheduled Switch:** This mode allows the user to set specific time periods for Daytime and Nighttime operation.

You can set up a switching schedule based on **day of the week or month**, as required.

This feature supports distinguishing between **Daylight Saving Time (Summer Time)** and **Standard Time (Winter Time)** by month. This meets the requirements for having different

Daytime and Nighttime periods, as well as different supplementary lighting periods, across the two different time schedules.

Captured Image Parameters

Set the parameters of captured images to raise the image quality.

Image effects vary by scene mode. Select a mode that matches the actual environment. **Highway** is recommended. Enable correction will reset all image parameters of the selected mode to their default values.

7.7.6 Video

Text Overlay on Video

Scenario

OSD refers to the additional information displayed on the preview screen such as the channel name, time/date, province/city/county/camera location/camera orientation, and more customized information. You can set and select the OSD information to be displayed and drag the red OSD information on the preview screen to the desired display position.

Steps

1. Select a device and set the OSD configuration.
 - a. Set the display configuration such as the channel name and display date.



Note

You just need to set the date/time format without setting the specific time.

- b. Set the OSD font and alignment.
- c. Select **Add** to add custom OSD elements.
- d. Drag red-highlighted OSD elements on the preview screen to adjust their positions.
- e. Select **Preview** to check if the OSD elements are applied.

Camera Parameters

Adjust the image parameters to get clear images.

Refer to **ICR** for configuration.

7.7.7 System Service

Set the enhancement level to control the brightness mode of the strobe light.

7.8 Video Intercom

You can configure parameters of video intercom devices, including the time, language, display, zone and scene.

7.8.1 Prerequisites

- The selected devices are of the same model.
- Ensure the selected devices are online, and the network is working well. If the network is bad or blocked, applying parameters may fail.

7.8.2 Access Control

Zone & Scene

After configuring a zone by setting the detector type, zone type, and alarm type. You can link a scene with a zone and set the arming/disarming for arming/disarming multiple devices. In the following scenarios, you can perform the following operations:

- Batch change the default alarm type of a zone to suit your needs.
- Test whether alarms can be triggered for indoor stations connected with detectors.

Zone Type

Table 7-12 Zone Type

Zone Type	Description
Instant Zone	A security system immediately activates or triggers an alarm upon detecting a breach or intrusion in a specific area.
Delayed Zone	Delays the activation of an alarm for a brief period after a breach is detected, to prevent false positives or to allow for manual overrides. Entry Delay: Provides you time to enter the zone without alarm. Exit Delay: Provides you time to leave through the zone without alarm.
Follow Zone	The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise. It is usually set in the living room or hall.
Perimeter Zone	A security system immediately activates or triggers an alarm upon detecting a breach in the perimeter area such as doors and windows.

Zone Type	Description
24H Silent Alarm	The zone activates all the time without any sound/siren output when alarms occur. It is usually used in the sites equipped with panic buttons such as banks and jewelry stores.
24H Audible Alarm	The zone activates all the time with sound/siren output when alarms occur. It is usually used in the sites equipped with panic buttons.
Medical Zone	The zone activates all the time, panel have beep voice when upload alarm report to center successfully. It is usually used in places equipped with medical emergency buttons.
Timeout Zone	The zone activates all the time. It alarms when the event you defined does happen throughout a configurable period. It is usually used in places like fire hydrant box's doors equipped with magnetic contacts.
Shield Zone	Alarms will not be activated in the zone. It is usually used to disable faulty detectors.
Service Consultation Zone	It is usually used in a specific area set aside within a service-oriented business where customers can receive consultations or advice from experts or professionals such as banks and retail stores equipped with buttons.
Panic Zone	The zone activates all the time. It is usually used in sites equipped with panic buttons, smoke detectors and glass-break detectors.
Fire Zone	The zone activates all the time with sound/siren output when alarm occurs. It is usually used in fire hazardous areas equipped with smoke detectors and temperature sensors.
Combustible Gas Zone	The zone activates all the time with sound/siren output when alarm occurs. It is usually used in areas like kitchens equipped with gas detectors.



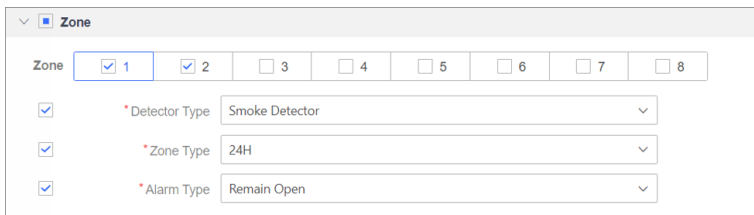
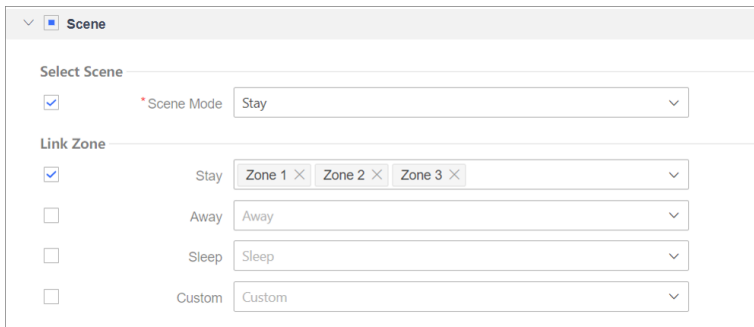
Note

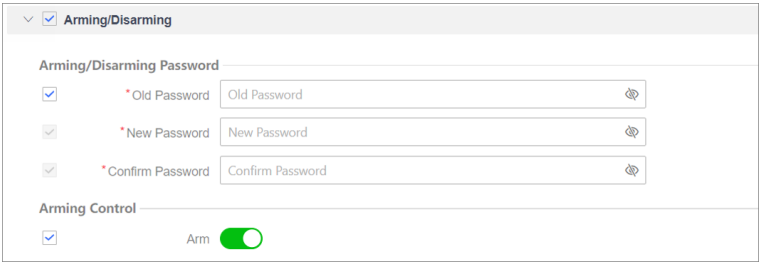
For more zone types and configuration, refer to the device's user manual.

Overall Configuration Process

1. Configure zones.
2. Link scenes with zones.
3. Set the arming/disarming password.
4. Switch the scene.
5. Enable arming/disarming.

Steps

Parameters	Steps
Zone	1. Select indoor stations, and select Zone. 2. Select a zone. The selected zone will be highlighted in blue. 3. Set the detector type, zone type, and alarm type. 4. Select Apply.  Figure 7-37 Zone Settings
Scene	1. Select indoor stations, and select Scene.  Caution Ensure that you have set a password before changing the scene. 2. Select a scene mode and link the scene with a configured zone. 3. Set the detector type, zone type, and alarm type. 4. Select Apply.  Figure 7-38 Scene Settings
Arm	1. Select indoor stations, and select Arming/Disarming. 2. Set the arming/disarming password.  Caution Ensure that you have set a password before changing the scene.

Parameters	Steps
	3. Enable Arm. 4. Select Apply.  Figure 7-39 Arming/Disarming

Button

Scenario

- In office environments, during business hours, the door station's calls are routed to the office's indoor station, and outside these hours, they are rerouted to the security office or a monitoring center.
In low-light conditions, enable the door station's backlight feature; in environments with sufficient lighting, disable this feature.

Steps

Button

Backlight

Backlight Mode

Auto

Button Settings (Set the button to call indoor stations or main stations by Room No. and schedule.)

Link Call Schedule

Call Schedule Settings

Button No.	Module	Button Settings	Link Call Schedule
--	--	1	Link Call Schedule is re

Figure 7-40 Set Button

1. On the left device list, select devices and then select **Button**.
2. Configure parameters.

Parameter	Steps
Backlight	Select Backlight Mode to set the mode.
Button Settings	a. Select Link Call Schedule . b. Select Call Schedule Settings to set the schedule name and time. - For weekly schedules, select Indoor Station or Center and set the time period. - For daily (holiday) schedules, select Add, select Indoor Station or Center and set the time period. c. In the Button Settings column, set the room No. for the call and select a call schedule.

3. Select **Apply**. You can select **Task Center** to view the progress.

Public Password

Scenario

Postal service workers, gardeners, electricians, cleaners, and service personnel can use a common password to open a door.

Steps

1. On the left device list, select devices and then select **Public Password**.
2. Select **Add** to set the password type, enter the password, add remarks (the purpose of passwords), and check the electric lock.
3. Select **Apply**. You can select **Task Center** to view the progress.

7.8.3 Audio

Scenario

Adjust the audio levels of devices in various settings based on specific sound requirements. For example, in library reading sections and hospital rooms, reduce the device volume, whereas in noisy factory environments, increase the volume.

Steps

1. On the device list, select devices and then select **Audio**.
2. Set the audio parameters. The following table introduces only some of the key parameters.

Parameter	Description
Volume	- Speak Volume refers to the volume during two-way calls. - Input/Output Volume is the system volume.

3. Select **Apply**. You can select **Task Center** to view the progress.

7.8.4 Event

Motion Detection

Scenario

In exclusive residential areas or major facilities, access is restricted to residents and authorized individuals only. You can set the motion detection to capture pictures of movements and report them in real-time to a monitoring center.

Steps

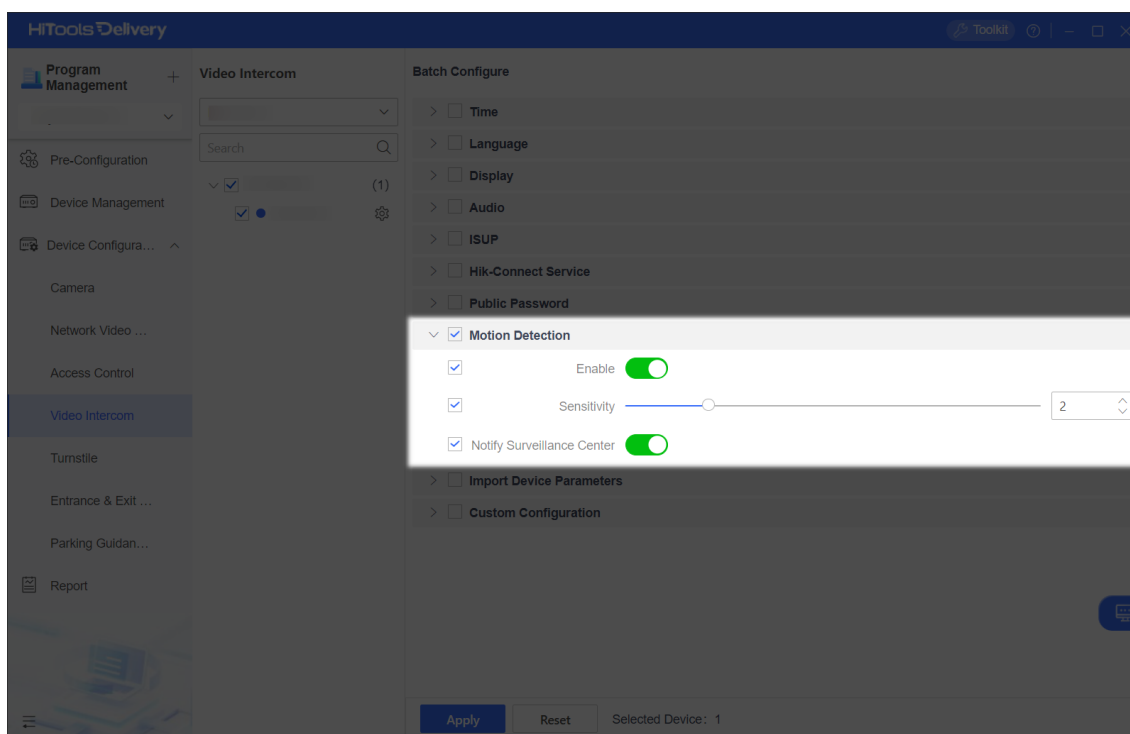


Figure 7-41 Motion Detection

1. Select devices and then select **Motion Detection**.
2. Enable **Motion Detection**.

3. Set the sensitivity. A higher value indicates greater sensitivity, making it easier to detect moving objects but also more prone to false alarms. If the sensitivity is set to 0, this function will not work.
4. (Optional) Enable **Notify Surveillance Center** to set a linkage method such as reporting alarms to the monitoring center when an event occurs.
5. Select **Apply**. You can select **Task Center** to view the progress.

Zone & Scene

After configuring a zone by setting the detector type, zone type, and alarm type. You can link a scene with a zone and set the arming/disarming for arming/disarming multiple devices. In the following scenarios, you can perform the following operations:

- Batch change the default alarm type of a zone to suit your needs.
- Test whether alarms can be triggered for indoor stations connected with detectors.

Zone Type

Table 7-13 Zone Type

Zone Type	Description
Instant Zone	A security system immediately activates or triggers an alarm upon detecting a breach or intrusion in a specific area.
Delayed Zone	Delays the activation of an alarm for a brief period after a breach is detected, to prevent false positives or to allow for manual overrides. Entry Delay: Provides you time to enter the zone without alarm. Exit Delay: Provides you time to leave through the zone without alarm.
Follow Zone	The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise. It is usually set in the living room or hall.
Perimeter Zone	A security system immediately activates or triggers an alarm upon detecting a breach in the perimeter area such as doors and windows.
24H Silent Alarm	The zone activates all the time without any sound/siren output when alarms occur. It is usually used in the sites equipped with panic buttons such as banks and jewelry stores.
24H Audible Alarm	The zone activates all the time with sound/siren output when alarms occur. It is usually used in the sites equipped with panic buttons.
Medical Zone	The zone activates all the time, panel have beep voice when upload alarm report to center successfully. It is usually used in places equipped with medical emergency buttons.

Zone Type	Description
Timeout Zone	The zone activates all the time. It alarms when the event you defined does happen throughout a configurable period. It is usually used in places like fire hydrant box's doors equipped with magnetic contacts.
Shield Zone	Alarms will not be activated in the zone. It is usually used to disable faulty detectors.
Service Consultation Zone	It is usually used in a specific area set aside within a service-oriented business where customers can receive consultations or advice from experts or professionals such as banks and retail stores equipped with buttons.
Panic Zone	The zone activates all the time. It is usually used in sites equipped with panic buttons, smoke detectors and glass-break detectors.
Fire Zone	The zone activates all the time with sound/siren output when alarm occurs. It is usually used in fire hazardous areas equipped with smoke detectors and temperature sensors.
Combustible Gas Zone	The zone activates all the time with sound/siren output when alarm occurs. It is usually used in areas like kitchens equipped with gas detectors.



Note

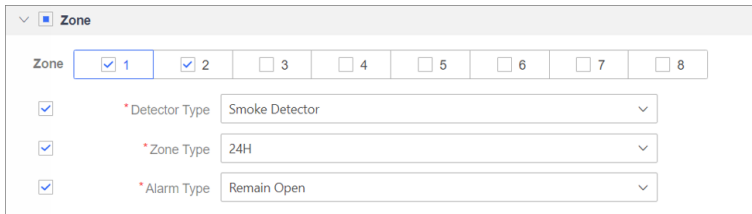
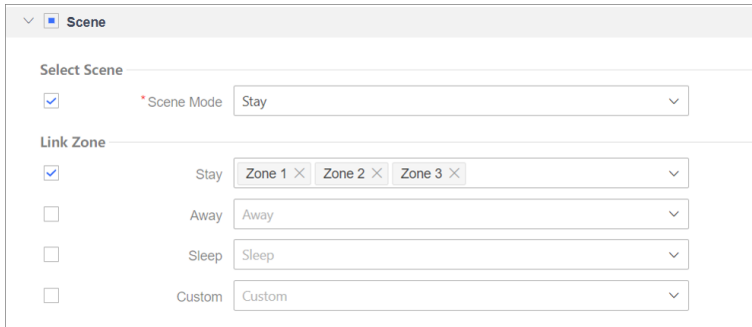
For more zone types and configuration, refer to the device's user manual.

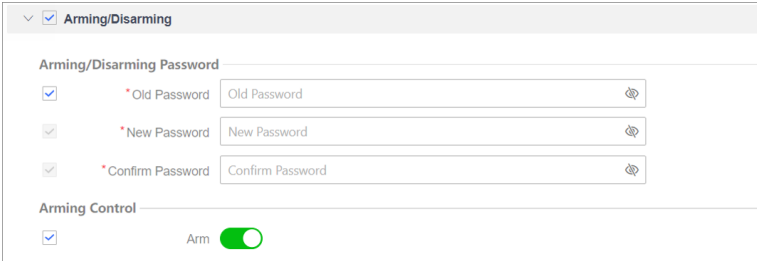
Overall Configuration Process

1. Configure zones.
2. Link scenes with zones.
3. Set the arming/disarming password.
4. Switch the scene.
5. Enable arming/disarming.

Steps

Parameters	Steps
Zone	1. Select indoor stations, and select Zone. 2. Select a zone. The selected zone will be highlighted in blue. 3. Set the detector type, zone type, and alarm type. 4. Select Apply.

Parameters	Steps
	 Figure 7-42 Zone Settings
Scene	1. Select indoor stations, and select Scene.  Caution Ensure that you have set a password before changing the scene. 2. Select a scene mode and link the scene with a configured zone. 3. Set the detector type, zone type, and alarm type. 4. Select Apply.  Figure 7-43 Scene Settings
Arm	1. Select indoor stations, and select Arming/Disarming. 2. Set the arming/disarming password.  Caution Ensure that you have set a password before changing the scene. 3. Enable Arm. 4. Select Apply.

Parameters	Steps
	 Figure 7-44 Arming/Disarming

7.8.5 Image

1. Select the required devices and select **Display**.
2. Enable **WDR**.



Note

Wide Dynamic Range (WDR) enhances visibility in both bright and dark areas of a scene. WDR is crucial in environments with strong backlighting or uneven lighting, such as outdoor cameras.

3. Click **Apply**.

7.8.6 Basic Configuration

- Time
- Language

7.8.7 Platform Access

- ISUP
- Cloud Service

7.8.8 HEOP

HEOP

7.8.9 Maintenance & Security

Import Device Parameters

7.8.10 Advanced Configuration

Custom Configuration

7.9 Access Control

7.9.1 Prerequisites

- The selected devices are of the same model.
- Ensure the selected devices are online, and the network is working well. If the network is bad or blocked, applying parameters may fail.

7.9.2 Overall Configuration Process

1. Select **Access Control** and select devices as needed.
2. Select and configure parameters.
3. Select **Apply**. You can select **Task Center** to view the progress.

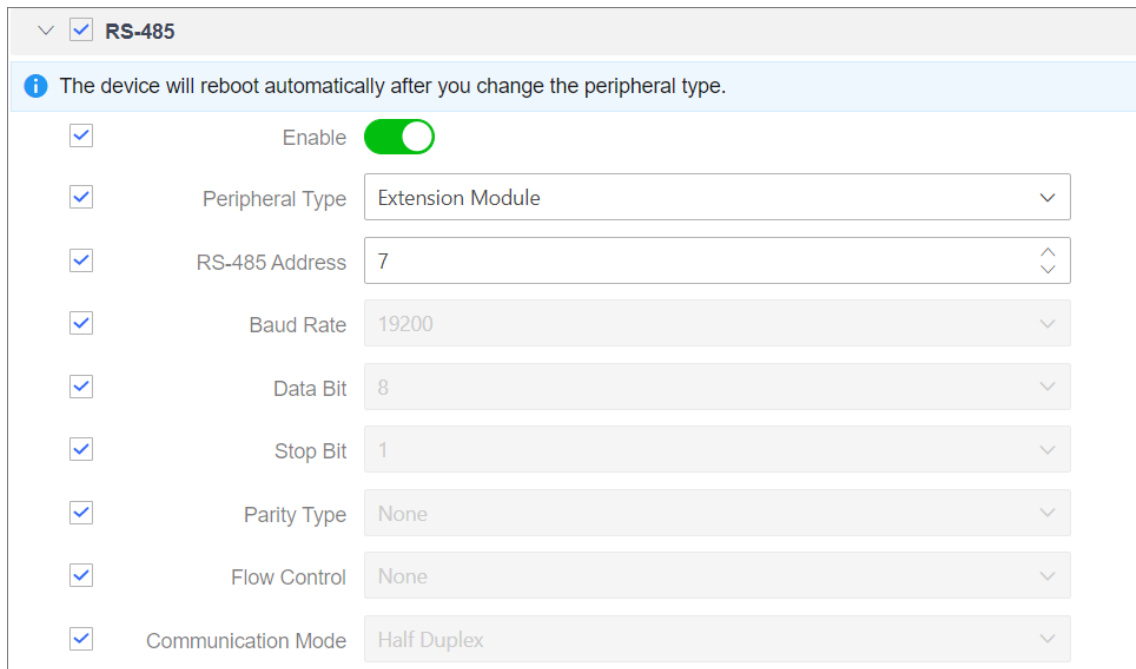
7.9.3 Device Access

RS-485

Scenario

After configuring RS-485 for access control devices, they can communicate with peripherals like card readers, elevator controllers, and access controllers. For example, in an office building with multiple entrance points, devices like card readers and face recognition terminals can be connected to the access controller via RS-485. The controller can then manage all access control devices. This setup is suitable for long-distance and multi-device connection scenarios.

Steps



RS-485

The device will reboot automatically after you change the peripheral type.

Enable ☒ ☒

Peripheral Type ☒ Extension Module

RS-485 Address ☒ 7

Baud Rate ☒ 19200

Data Bit ☒ 8

Stop Bit ☒ 1

Parity Type ☒ None

Flow Control ☒ None

Communication Mode ☒ Half Duplex

Figure 7-45 RS-485

1. On the left device list, select devices and then select **Device Access** → **RS-485**.
2. Enable this function.
3. Configure the following parameters.

Parameters	Description
Peripheral Type	- If you change the peripheral type, the device will reboot automatically. - Extension modules refer to devices such as QR code scanners and infrared thermometer.
RS-485 Address	The RS-385 address (1-255) is a unique identifier assigned to each device, allowing the access controller to communicate with individual devices such as card readers.
Baud Rate / Data Bit / Stop Bit / Parity Type / Flow Control / Communication Mode	Baud Rate/Data Bits/Stop Bits/Parity/Flow Control/Communication Mode are set based on the device capabilities, with defaults already set.
Output Type	The output type is set according to the peripheral device type.

4. Select **Apply**. You can select **Task Center** to view the progress.

Wiegand

Scenario

Access control devices can connect to external devices through the Wiegand interface. For example, a card reader can read the card data and transmit it to the access controller via the Wiegand. Upon receiving the signal, the access controller determines whether the card number is valid and decides whether to unlock the door. This method is not suitable for long-distance transmission or noisy environments.

Steps

1. On the left device list, select devices and then select **Device Access → Wiegand**.
2. Enable this function.
3. Configure the following parameters.

Parameters	Description
Peripheral Type	- If you change the peripheral type, the device will reboot automatically. - Extension modules refer to devices such as QR code scanners and infrared thermometer.
RS-485 Address	The RS-385 address (1-255) is a unique identifier assigned to each device, allowing the access controller to communicate with individual devices such as card readers.
Baud Rate / Data Bit / Stop Bit / Parity Type / Flow Control / Communication Mode	Baud Rate/Data Bits/Stop Bits/Parity/Flow Control/Communication Mode are set based on the device capabilities, with defaults already set.
Output Type	The output type is set according to the peripheral device type.

4. Select **Apply**. You can select **Task Center** to view the progress.

7.9.4 Access Control

Door

Scenario

Once the equipment is installed on-site, you can bulk configure the authentication methods for multiple access control devices that share the same authentication method. For instance, you can switch from Card/PIN to Face/Card, based on your specific requirements.

Steps

The screenshot shows a configuration window titled 'Door'. It contains several parameters, each with a checkbox and a value field:

- ☒ *** Door No.**: A dropdown menu showing the value '1'.
- ☒ *** Open Duration**: A text input field with the value '5' and up/down arrows.
- ☒ *** Door Open Timeout Ala...**: A text input field with the value '30' and up/down arrows.
- ☒ *** Door Contact**: Two radio buttons, 'Remain Closed' (selected) and 'Remain Open'.
- ☒ *** Super Password**: A text input field with a lock icon on the right.

Figure 7-46 Door Parameters

1. On the left device list, select devices and then select **Door**.
2. Select the door No. and configure the following parameters.

Parameter	Description
Open Duration (sec)	Set the door unlocking duration. If the door does not open for the set time, the door will be locked.
Door Open Timeout Alarm (sec)	An alarm will be triggered if the door has not been closed within the configured open duration. When it is set to 0, no alarms will be triggered. This feature can be used to detect if a door is not properly closed or is being deliberately blocked. This feature is used in scenarios where it is essential to ensure doors are closed during non-working hours, such as at night or on holidays. It is also commonly used in areas with high security requirements, like banks and vaults.
Super Password	The specific person can open the door by inputting the super password. In emergencies, such as fires, medical emergencies, or system failures, the super

Parameter	Description
	password can be used to quickly unlock all access points, ensuring the safe evacuation of personnel.
Door Contact	- Remain Open: Used in less secure environments or where rapid evacuation is necessary in emergencies, like in malls, schools, or theaters. - Remain Closed: Used in high-security areas such as office buildings, government agencies, and financial institutions, where doors unlock only after successful verification.

3. Select **Apply**. You can select **Task Center** to view the progress.

Authentication Configuration

Scenario

Postal service workers, gardeners, electricians, cleaners, and service personnel can use a common password to open a door.

Steps

1. On the left device list, select devices and then select **Authentication Configuration**.
2. Select a terminal and configure parameters. Only part of parameters will be introduced in the following table.

The screenshot displays the 'Authentication Configuration' window. At the top, there's a dropdown menu showing 'Authentication Configuration'. Below it, a 'Terminal' selector shows '1' selected. The configuration list includes several items, each with a checkbox and a control (toggle or dropdown):

- ☒ Enable Authentication D...: Toggle switch is turned on (green).
- ☒ Authentication Mode: Dropdown menu shows 'Face/Fingerprint/Card/PIN'.
- ☒ Recognition Interval: Input field shows '3'.
- ☒ Repeated Authenticatio...: Input field shows '0'.
- ☒ Alarm of Failed Authentic...: Toggle switch is turned off (grey).
- ☒ Tampering Detection: Toggle switch is turned on (green).
- ☒ Card No. Reversing: Toggle switch is turned on (green).
- ☒ Bluetooth: Toggle switch is turned on (green).
- ☒ Open Door via Bluetooth: Toggle switch is turned on (green).

Figure 7-47 Authentication Configuration

Parameter	Description
Recognition Interval	The time between 2 consecutive recognitions of a same person. During the interval, a person can be recognized only once.
Repeated Authentication Interval	During the specific interval, repeated authentications (uploaded by different devices) are invalid.
Enable Authentication Device	When this function is enabled, the authentication terminal can be used normally for card swiping.
Tampering Detection	When this function is enabled, if the card reader is removed, the device will automatically trigger an alarm.

3. Select **Apply**. You can select **Task Center** to view the progress.

Card Security

7.9.5 Image

1. Select the required devices and select **Display**.
2. Configure the supplementary light parameters, including the light type and brightness.
3. Click **Apply**.

7.9.6 Basic Configuration

- Time
- Language

7.9.7 Platform Access

- ISUP
- Cloud Service

7.9.8 HEOP

HEOP

7.9.9 Maintenance & Security

Import Device Parameters

7.9.10 Advanced Configuration

Custom Configuration

7.10 Speed Gate & Turnstile

7.10.1 Entry

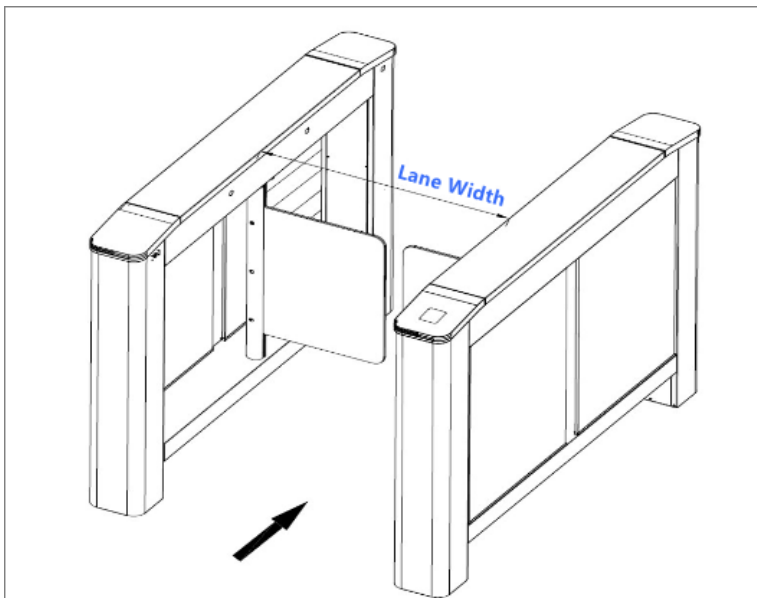
Select **Speed Gate & Turnstile**, select parameters, and apply them. Select **Test** to test video parameters.

7.10.2 Prerequisites

- The selected devices are of the same model.
- Ensure the selected devices are online, and the network is working well. If the network is bad or blocked, applying parameters may fail.

7.10.3 Basic Parameters

1. Select devices and select **Basic Parameters**.
2. Configure the basic configuration and card configuration. The following table will introduce the basic parameters.

Parameters	Description
Lane Width	 Figure 7-48 Lane Width Unit: mm.
Barrier Opening / Closing Speed	You can set it from level 1 to 10. The bigger the number, the quicker the door will open or shut.
Entrance/Exit	If you set the entrance and exit to Inductive , the barrier will remain closed.

3. Select **Apply**. You can select **Task Center** to view the progress.

7.10.4 Access Control

Card Security

1. Select devices, and then select **Card Security**.
2. Enable/disable various types of cards.

Table 7-14 Card Types

Card Type	Description
M1	Enabling M1 card encryption enhances its security, making it more difficult to be copied or forged. You need to set up a sector number. It is recommended to encrypt the 13th sector.
EM	After enabling the EM card feature, the device can recognize EM cards, allowing users to swipe them directly at the reader. If the device supports external EM card readers, after enabling this feature, they can also read EM cards externally.
CPU	CPU cards are commonly used where high security is required, such as identity authentication, financial transactions, public transportation, etc. After enabling the CPU card feature, the device can recognize CPU cards, and users can swipe them directly at the reader.
NFC	Enabling NFC function can protect against unauthorized access to access control devices' data.
ID Card	After enabling the ID card feature, the device can recognize ID cards, and users can swipe them directly at the reader.

3. Select a card authentication mode.

Table 7-15 Card Authentication

Authentication Mode	Description
Full	Reads the entire card number.
3 Bytes	The card number is read through Wiegand26 protocol (only reads three-character card numbers).
4 Bytes	The card number is read through Wiegand34 protocol (only reads four-character card numbers).

4. Select **Apply**.

Cross-Controller Anti-Passback

Scenario

You can configure parameters of turnstiles, including card parameters and anti-passback (APB) parameters. APB is designed to prevent a user from passing back their access to another person to gain unauthorized entry. For example, if you enter through Gate A, you must exit through Gate A before being able to enter through Gate B.

Steps

1. Select devices as needed and select **Cross-Controller Anti-Passback**.
2. Select an anti-passback method.

Method	Description
Entry & Exit Anti-Passback	Set the anti-passback server and turnstile IP.
Route Anti-Passback	Set the entrance & exit information (add up to 32 entrances & exits) and anti-passback route according to the guidance.

3. Select **Apply**. You can select **Task Center** to view the progress.

7.10.5 Maintenance & Security

Import Device Parameters

7.10.6 Advanced Configuration

Custom Configuration

7.11 LED Screen

7.11.1 Prerequisites

- The selected devices are of the same model.
- Ensure the selected devices are online, and the network is working well. If the network is bad or blocked, applying parameters may fail.

7.11.2 Entrance & Exit LED Screen

1. Select **Entrance & Exit LED Screen**.
2. Select **Display Content Configuration** and configure parameters.

Selected devices vary in types and versions, so only parameters supported by responding devices will be applied.
Check application results later.

Display Content Configuration

Content No.1

*Character

hello

*Position

0,0

-

64,16

*Font Color

Red

*Font Size

16

*Scrolling Mode

Static

Content No.2

*Character

12345

*Position

0,16

-

64,32

*Font Color

Red

*Font Size

16

*Scrolling Mode

Static

Figure 7-49 Entrance & Exit LED Screen Configuration

 Note

Position: Enter the starting and ending coordinates (shown in the following picture).



Figure 7-50 Position

-
3. Select **Apply**.

7.11.3 Parking Guidance LED Screen

1. Select **Parking Screen**.
2. Select **Display Configuration** and configure parameters. The following table shows two major parameters.

Selected devices vary in types and versions, so only parameters supported by responding devices will be applied. Check application results later.

Display Configuration

The number of sections varies by your device model.

Section 1 Section 2 Section 3

Section 1

- Brightness: 5
- Content: 1 Icon + 3-Digit Number
- Number: 123
- Font Color: Red
- Icon Color: Red
- Icon: Up

Apply

Figure 7-51 Parking Guidance LED Screen

Parameter	Description
Section	A specific part of your screen. You can configure a maximum of three sections.
Icon	Full On and Completely Off refer to the LED light tubes in the quadrilateral area where the icons are located being fully illuminated or fully turned off.

3. Select **Apply**.

7.12 Alarm Device

For alarm device web configuration, refer to the device user manual.

- Refer to **Configure More** for batch configuration by copying a single device's web parameters to multiple devices of the same model.
- Refer to **Advanced Configuration** : Call APIs to batch configure parameters that HiTools Delivery does not support

7.13 Audio & Sensing Device

Support OTAP and custom configuration.

Entry

Select **Audio & Sensing**, select parameters, and apply them. Select **Test** to test platform access parameters.

Prerequisites

- The selected devices are of the same model.
- Ensure the selected devices are online, and the network is working well. If the network is bad or blocked, applying parameters may fail.

OTAP

Connect devices to the O&M platform via **OTAP** to query device info, upload status and alerts, and perform remote reboots or upgrades. **Device support required.**

Verify the parameters using one of the following methods:

- Click **Test** in the bottom right corner of the configuration interface to go to the configuration verification page.
- Go to **Configuration Verification** → **Other Parameters** → **Sensing** . You can search by device name or IP to confirm access status. For details, refer to [Configuration Verification](#) .

Advanced Configuration

Custom Configuration

7.14 Networking Device

For networking device web configuration, refer to the device user manual.

- Refer to [Configure More](#) for batch configuration by copying a single device's web parameters to multiple devices of the same model.
- Refer to [Advanced Configuration](#) : Call APIs to batch configure parameters that HiTools Delivery does not support

7.15 Interactive Flat Panel

For interactive flat panel web configuration, refer to the device user manual.

- Refer to [Configure More](#) for batch configuration by copying a single device's web parameters to multiple devices of the same model.
- Refer to [Advanced Configuration](#) : Call APIs to batch configure parameters that HiTools Delivery does not support

Chapter 8 Configuration Validation

8.1 Validate Video Display

After configuring parameters such as OSD, image overlay, audio/video settings, and preset points, verify whether the video display is correct or PTZ control functions normally.

1. - In the **Configuration Validation** module, click **Live View**.
 - After successfully applying parameters to cameras, enter the **Task Center** and click  to access the verification interface.
 - In the lower-right corner of the Device Configuration page, click **Test**.
2. Select the required channels to verify:
 - Check for **film removal status, clarity, obstructions, or significant shaking**.
 - Verify if **OSD** are displayed correctly.
 - Operate the PTZ controls or call presets to test functionality.

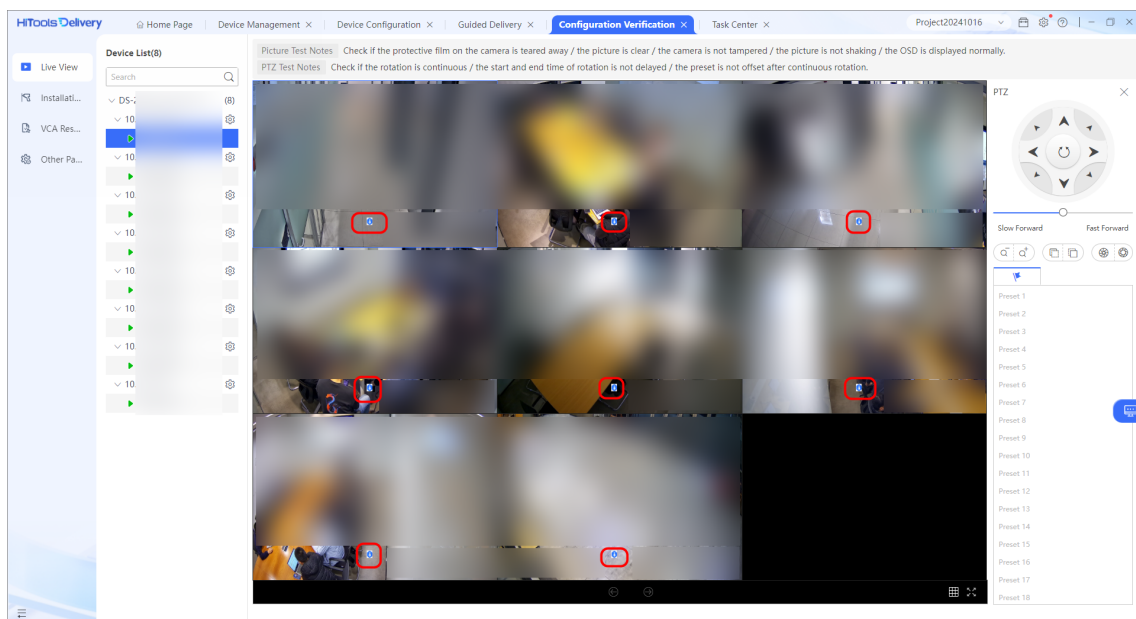


Figure 8-1 Live View Verification

8.2 Validate Installation Quality

After installation and configuration, traffic cameras require validation to ensure image clarity, angle, and line marking to meet on-site requirements.

- In the **Configuration Validation** module, click **Installation Quality**.
- After successfully applying application mode configurations to traffic cameras, enter the **Task Center** and click  to access the Installation Quality Verification interface.

8.2.1 Online Validation

Step 1: Capture Images and Set Basic Parameters

1. Click **Online Validation**.
2. Select a capture mode.



Note

- For **Capture Continuously**, select the current capture lane.
 - For camera versions below V5.5, manual adjustment of the yellow box is required; otherwise, the test result will be compromised.
 - Support multi-level arming for online testing: If the primary arming mode is occupied, the system automatically switches to secondary arming to retrieve capture data.
-
3. After successful capture, the system automatically calculates the license plate's horizontal pixel value. To adjust, drag the vertices of the yellow rectangle to measure the horizontal pixels. Modify basic parameters as needed, then click **Validate**.

Step 2: Review Results and Adjust Configuration

If the result shows **To Be Adjusted**, adjust configuration based on the suggestions and examples provided.

Step 3: Export Verification Results

Click **Export** in the upper-right corner to save results for the current device or all devices.

8.2.2 Offline Validation

Perform offline validation on device installation and configuration by importing captured images, enabling quick adjustments based on validation results.

Step 1: Import Pictures

1. Click **Offline Validation**.
2. Upload a single eligible picture or a folder (up to 1,000 pictures). The tool will automatically detect the validation mode.
3. Choose **Configure by Template** or **Configure One by One**, then input parameters such as the pole height, light-to-camera distance, and light type.

Step 2: Adjust Parameters

After successful import, the system automatically calculates the license plate's horizontal pixel value. To adjust, drag the vertices of the yellow rectangle to measure the horizontal pixels. Modify basic parameters as needed, then click **Validate**.

Step 3: Review Results and Adjust Configuration

If the result shows **To Be Adjusted**, adjust configuration based on the suggestions and examples provided.

Step 3: Export Verification Results

Click **Export** in the upper-right corner to save results for the current device or all devices.

8.3 Validate Camera Smart Events

Verify camera smart events like motion detection and intrusion detection, and other VCA resources like face picture capture.

1. Go to VCA resource validation interface.
 - In the **Configuration Verification** module, click **VCA Resource**.
 - After successfully applying parameters to cameras, enter the **Task Center** and click  to access the verification interface.
 - In the lower-right corner of the Device Configuration page, click **Test**.
2. Select the devices to verify events.
3. Trigger the target event in the real world. When the status changes from **Pending** to **Triggered**, the event configuration is confirmed as successful.

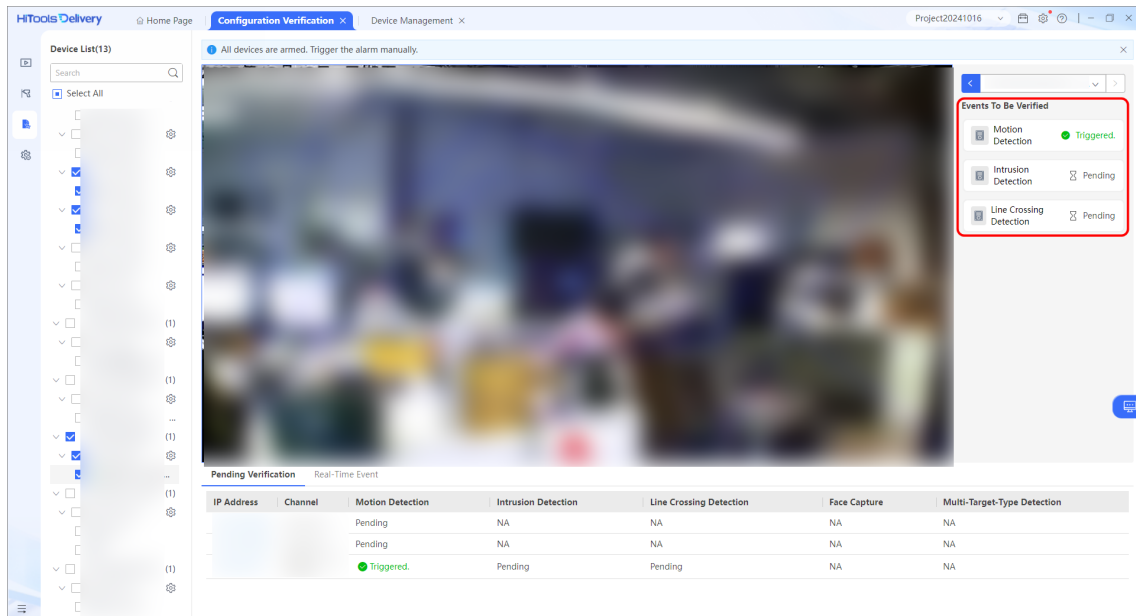


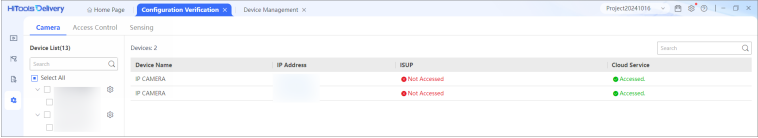
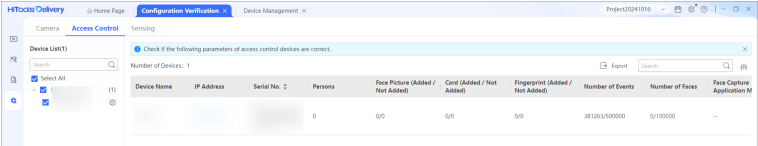
Figure 8-2 Verify Events

8.4 Verify Other Parameters

Verify access control device parameters and platform accessibility for cameras and sensing devices like UWB anchors in the Other Parameters module.

1. Go to the validation interface.
 - In the **Configuration Validation** module, click **Parameter Verification**.
 - After successfully applying parameters to cameras, enter the **Task Center** and click  to access the verification interface.
 - In the lower-right corner of the Device Configuration page, click **Test**.
2. Select devices for parameter verification.

Device Type	Parameter Verification
Camera/Sensing Device	Select the devices to automatically verify platform access results.

Device Type	Parameter Verification
	 The screenshot shows the 'Configuration Verification' page for 'Access Control'. On the left, there's a sidebar with 'Camera' and 'Access Control' tabs. Under 'Access Control', there's a 'Device List(1)' section with a search bar and a 'Select All' button. The main area shows a table with columns: 'Device Name', 'IP Address', 'RDP', and 'Cloud Service'. There are two rows for 'IP CAMERA'. The 'RDP' column shows 'Not Accented' with a red dot, and the 'Cloud Service' column shows 'Accented' with a green dot. Figure 8-3 Platform Access Verification
Access Control	a. Choose the required access control devices to display their parameters in a list. b. Review the configuration parameters for accuracy. c. Click Export to save an Excel file for backup.  The screenshot shows the 'Configuration Verification' page for 'Access Control'. On the left, there's a sidebar with 'Camera' and 'Access Control' tabs. Under 'Access Control', there's a 'Device List(1)' section with a search bar and a 'Select All' button. The main area shows a table with columns: 'Device Name', 'IP Address', 'Serial No.', 'Persons', 'Face Picture (Added / Not Added)', 'Card (Added / Not Added)', 'Fingerprint (Added / Not Added)', 'Number of Events', 'Number of Faces', and 'Face Capture Application M'. There is one row for 'IP CAMERA'. The 'Persons' column shows '0', 'Face Picture' shows '0/0', 'Card' shows '0/0', 'Fingerprint' shows '0/0', 'Number of Events' shows '381261/100000', 'Number of Faces' shows '0/100000', and 'Face Capture Application M' shows '--'. There is an 'Export' button in the top right corner. Figure 8-4 Access Control Parameters Verification

Chapter 9 Maintenance & Security

- [Common Maintenance](#)
- [Upgrade Devices](#)
- [Change IP](#)
- [Edit Device's Name](#)
- [Change Password](#)
- [Device Diagnostics](#)
- [Security Hardening](#)

9.1 Common

This document mainly introduce the following operations: refreshing the device list, setting the time, backing up and importing parameters, configuring the SDK protocol compatibility mode, managing cloud services, and security configuration.

Go to **Maintenance** → **Common** .

9.1.1 Refresh

Refresh the online status and basic information of devices listed on the current page only.

9.1.2 Set Time for Time Sync

The device's factory time is not synchronized with the current time, which may affect the stream timestamp and recording timestamp. It is recommended to adjust the device time in advance.

1. Select online devices, and then select **Set Time**.
2. Set the time zone and select a time sync mode.

Table 9-1 Time Sync Mode

Time Sync Mode	Description
NTP Time Sync	a. Set up an NTP time server or get the server information. b. Set the server address, NTP port, and interval to automatically sync time with an NTP time server. c. Select Test to test whether the function works well.
Manual Time Sync	Manually set the time or select Sync with Computer Time .

3. Select **OK**.

9.1.3 Backup & Import

For cameras, access control devices, video intercom devices, and speed gates & turnstiles, regularly back up device settings. If a device fails or needs replacement, quickly restore settings using the backup file.

1. Select one or multiple devices and click **Backup**.
2. Perform one of the following operations:
 - Click **Back Up Parameters** to back up selected devices.
 - Click **Import Parameters** to import the backup file.

9.1.4 SDK Protocol Compatibility Mode

Early devices (released before March, 2023) store passwords using a reversible method, while new devices store them using an irreversible method. The compatibility mode is designed to ensure that older devices can pass password verification by supporting reversible password authentication. This allows seamless integration with legacy devices while maintaining secure password storage on new devices.

Mode	Description
Enable	Older devices can pass password verification, but password security will be compromised.
Disable	If disabled, password security will be enhanced.

9.1.5 Cloud Service

You can set the verification code or scan the QR code to bind devices to a cloud account. Ensure selected devices are logged in before enabling the cloud service. This function should be supported by devices.

1. Select a target device, enable **Cloud Service**.
 - a. Click **Cloud Service**.
 - b. (Optional) Enable **Stream Encryption** and set the encryption key.



This function should be supported by devices.

2. Bind the device to a cloud account and click **OK**.

Table 9-2 Binding Methods

Scenario	Method	Description
Bind Multiple Devices	Set Verification Code	On your cloud-based app like Hik-Connect, enter the verification code and the device serial No. to bind the device to the cloud account.
Bind a Single Device	Scan QR Code / Dynamic Verification Code	- Use your cloud-based app like Hik-Connect to scan the QR code. - On your cloud-based app like Hik-Connect, enter the dynamic verification code and the device serial No. to bind the device to the cloud account.

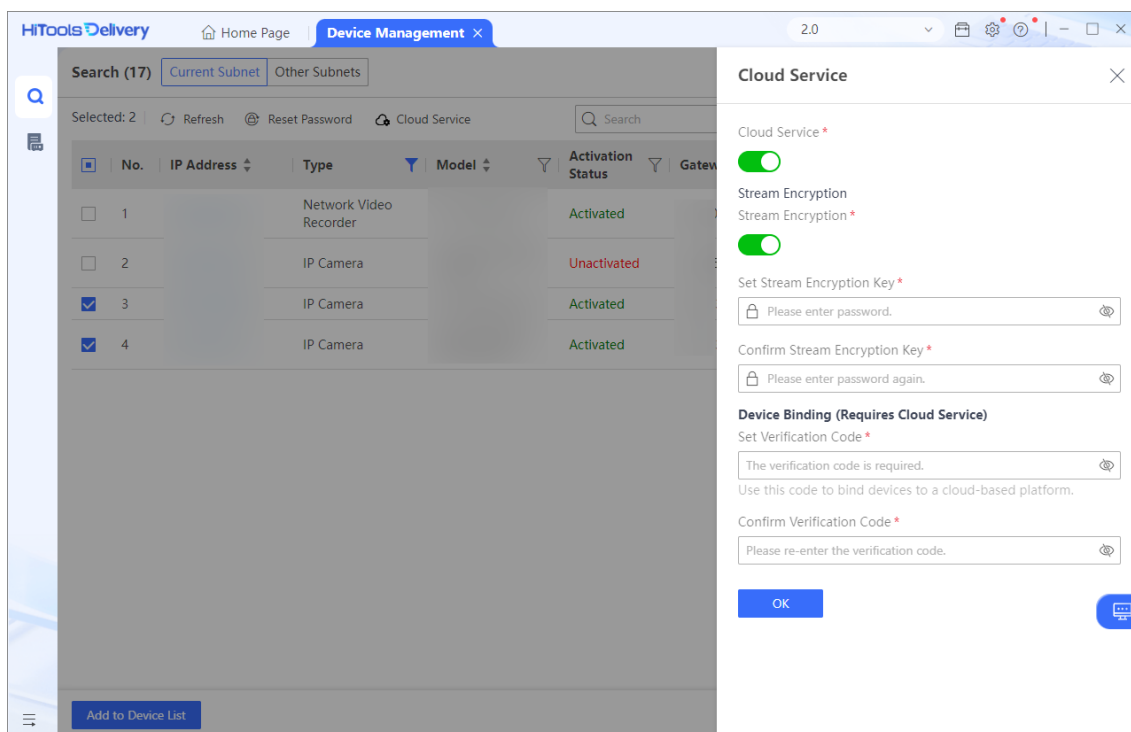


Figure 9-1 Set Verification Code to Bind Devices

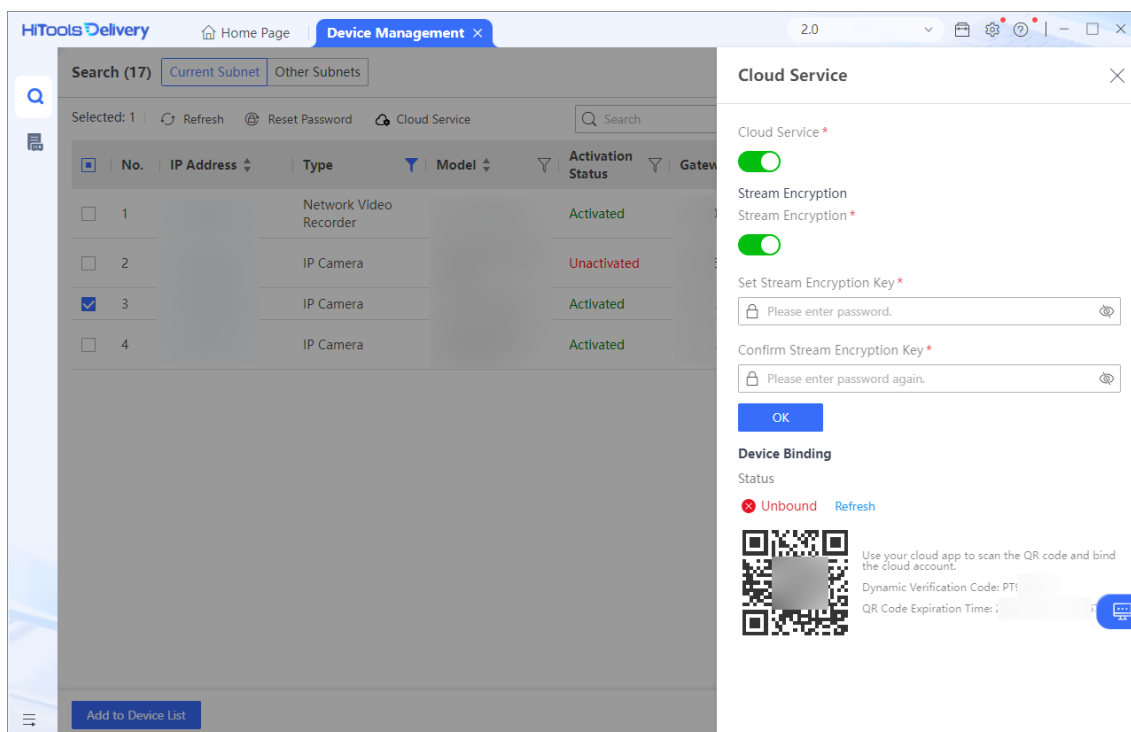


Figure 9-2 Scan QR Code to Bind Devices

3. (Optional) Click  to unbind the device from the cloud account.

9.1.6 Service & Security

1. Select the target devices and click **Service & Security**.
2. Configure the following parameters based on on-site requirements.
 - Network Service

Item	Typical Scenarios	Steps
HTTP(S)	- Emergency Lockdown: In the event of a major security incident, bulk-disable HTTP/HTTPS ports and switch to a more secure private protocol for device access. - Enforced Encryption: Bulk-disable HTTP to enforce encrypted access via HTTPS only.	a. Select HTTP(S). b. Enable/disable HTTP or HTTPS services. - If enabled: Select the authentication mode and digest algorithm.

		 Note Enabling HTTPS requires enabling TLS and creating a certificate. Otherwise, HTTPS will be invalid. - If disabled: The connection between the device and HiTools Delivery will be terminated. To restore access, switch the protocol or port and log in again. c. (Optional) Enable/disable RTSP OVER HTTP(S) . When enabled, video signals (RTSP) are encapsulated into standard web traffic (HTTP/HTTPS) for transmission, solving cross-network transmission issues and bypassing firewall blocks.  Note This function is only supported by certain devices.
RTSP	Attack Mitigation: RTSP protocols are vulnerable to risks like weak default passwords, plain text transmission, and public network exposure. In case of a security breach, bulk-disable to block unauthorized video streams and attack channels.	a. Check RTSP . b. Enable or disable the RTSP service as required.
TLS	Security Hardening: Bulk-disable vulnerable TLS versions (e.g., TLS 1.1) and enforce an upgrade to TLS 1.2 (or higher) to strengthen protocol access control and encryption.	a. Check TLS . b. Enable or disable specific TLS versions as needed.  Note Once TLS is enabled, you must configure a certificate. You can either use a self-signed certificate or import a CA-issued one.
SRTP	Encrypts live audio and video streams transmitted over public networks or untrusted third-	a. Check SRTP . b. Enable or disable SRTP as needed.

	party LANs to remote platforms, VMS (Video Management Systems), or the cloud. This service does not affect WebSocket-based web video previews.	
SADP	Search Active Device Protocol: Enables automatic device discovery, activation, password resets, and network parameter configuration within the same VLAN.	a. Check SADP. b. Enable or disable SADP.  Note If Discovery Only is selected, password reset and network modification will be disabled.
SDK(S)	- SDK: Allows proprietary security platforms and client software within the LAN to actively access Hikvision devices. Supports device configuration, live view, playback, remote O&M (Operations & Maintenance), alarm handling, and PTZ control. - Enhanced SDK: Builds on standard SDK services by adding TLS encryption to guarantee data confidentiality and integrity. Uses port 8443 by default.	a. Check SDK(S). b. Enable or disable the Standard SDK or Enhanced SDK service as needed.  Note Enabling the Enhanced SDK service requires configuring the TLS version and selecting a server certificate for identity verification.
WebSocket(s)	- WebSocket (HTTP-based): Unencrypted stream for plugin-free, real-time video preview directly in web browsers. - WebSockets (HTTPS-based): Encrypted stream for plugin-free, real-time video preview in browsers. Requires simultaneous TLS configuration and certificate creation.	- Check WebSocket(s). - Enable or disable WebSocket or WebSockets as needed.  Note Enabling WebSockets requires enabling the TLS protocol and creating or importing a security certificate.

- IP Address Filter

Typical Scenario:

IP filtering is used not only for incident response but also to enforce allowlists in high-security scenarios.

Operation Steps: Enable **IP Address Filtering**, then choose one of the following methods:

- **Manual Entry:** Click **Add** and enter the allowed IP addresses or IP ranges.
- **Batch Import:** Click **Batch Import → Export**, fill in the required IP addresses, and then upload the completed template.
- Security Audit Log

Typical Scenario:

To satisfy daily **security compliance** requirements, enable **Security Audit Log** in bulk to centralize log storage on a server. In the event of a security incident, the platform allows for **global searches to pinpoint attack sources within seconds**, ensuring end-to-end **traceability** of all device operations and access activities.

Operation Steps: Enable the log upload server, then configure the **Server Address** and **Port**.

3. Click **OK**.

9.2 Upgrade Devices

9.2.1 Prerequisites

- Change to a public network (accessible to the internet) before searching for and download upgrade packages.
- Online upgrade is now available for the following device types: cameras, recording & analysis devices, access control devices, video intercom devices, alarm devices, and networking devices (network switches).

9.2.2 Entry

Click **Maintenance → Upgrade**.

9.2.3 Constraints

Each upgrade task supports up to **5,000** devices (recommended: ≤ 100). The maximum concurrent upgrade is 60 (recommended: 30).

9.2.4 Upgrade Settings

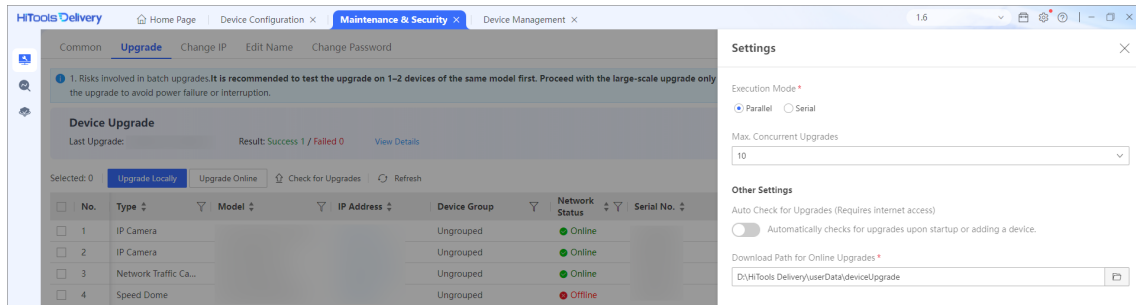


Figure 9-3 Upgrade Settings

Click **Settings** to set the execution mode/maximum concurrent upgrades, enable auto upgrade check, and set the upgrade package download location.

Table 9-3 Execution Mode

Execution Mode	Description
Serial	Multiple programs are upgraded in order.
Parallel	Multiple programs are upgraded simultaneously. You should set the maximum concurrent upgrade according to the device quantity, package size, and network conditions.  Note The maximum concurrent upgrade is 60 (recommended: 30).

9.2.5 Upgrade Locally

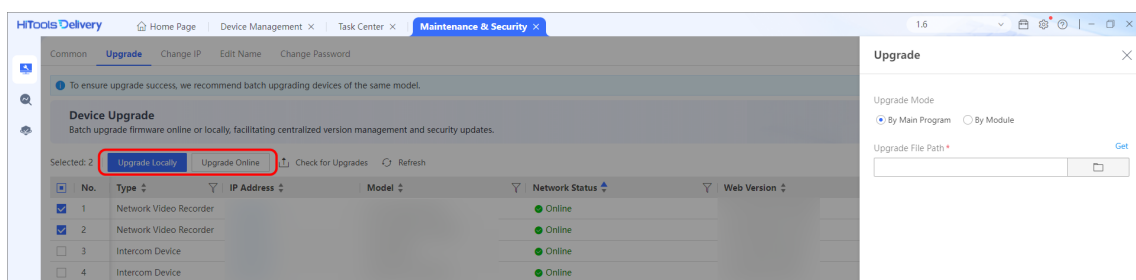


Figure 9-4 Local Upgrade

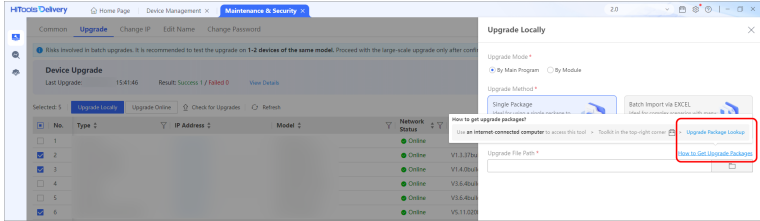
1. In the Device List, select devices and click **Upgrade Locally**.
2. Select an upgrade mode.

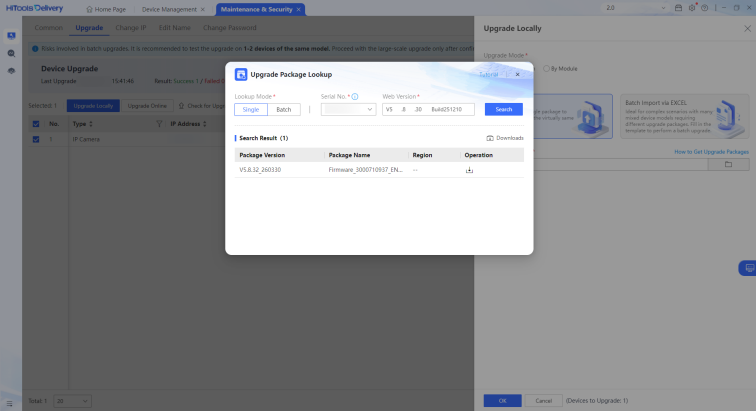
Table 9-4 Upgrade Mode

User Intent	Upgrade Mode
Upgrade speed gates & turnstiles or access control devices linked with peripherals such as MCU and card readers.	Click By Module .
Upgrade parking cameras.	Click By Sub Device .
Upgrade other devices.	Click By Main Program .

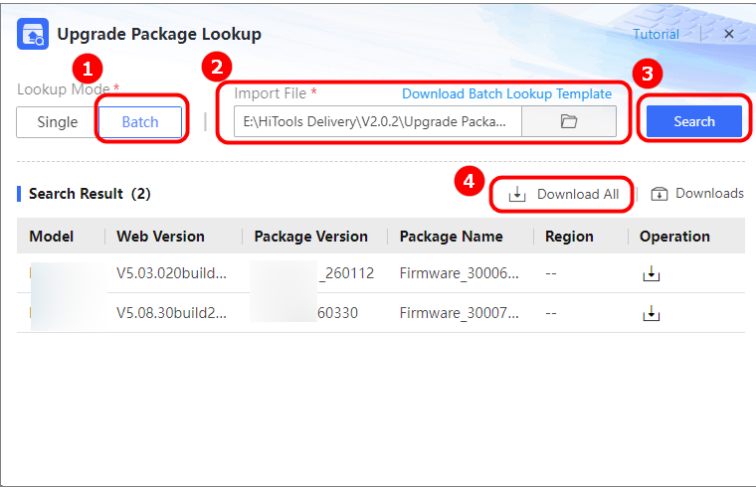
3. Import the upgrade package.

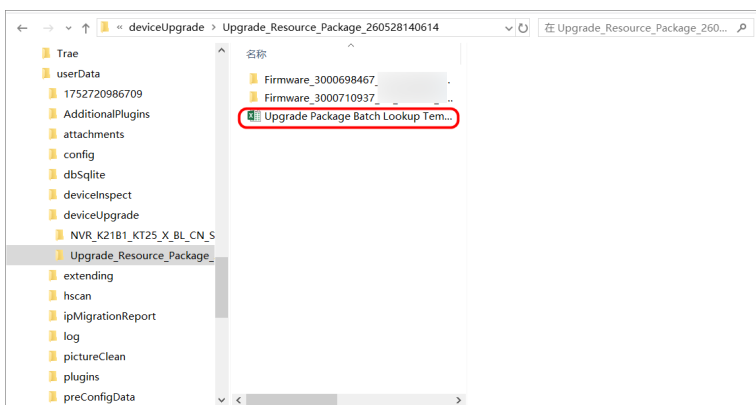
- By Main Program
- **Single Package**

Scenario	Steps
You already have the upgrade packages locally.	Import your package directly.
No upgrade packages.	a. On a public network, click How to Get Upgrade Packages → Upgrade Package Lookup , and wait for the search results.  Figure 9-5 Get Upgrade Package Note If no packages are found, contact technical support. b. Select and download the upgrade package. After the download completes, return to the local upgrade interface—the file path will be auto-populated.

Scenario	Steps
	 Figure 9-6 Download Package

- Batch Import via EXCEL

Scenario	Steps
You already have the upgrade packages locally.	Click Export Template and manually fill in their file paths in the template and import your Excel file directly.  Note The upgrade package must be in the same directory as the Excel template.
No upgrade packages.	 Figure 9-7 Batch Search Upgrade Packages

Scenario	Steps
	a. Click Export Template. b. On a computer with internet access, click  in the top-right corner and select Upgrade Package Lookup. c. Switch to Batch mode and import the completed Excel template. d. Click Search and wait for the search results.  Note If no packages are found, contact technical support. e. Click Download All to download all available upgrade packages. f. Import the Excel file to complete the upgrade.  Figure 9-8 EXCEL Template

 Note

For **VPro Series NVRs with AcuSeek**, the tool performs a pre-check upon importing the upgrade package during local upgrade. If the search algorithm version is incompatible, historical data must be re-indexed (re-modeled), and manual confirmation is required to proceed with the upgrade. If the compatibility test failed, the device cannot be upgraded.

- By Sub Device
Select a sub device and import the package.
- By Module
Select a module, select the module No. for card readers and sub module for lane controllers, and import the upgrade package.

4. Click **OK**.

5. Check the upgrade process. Click **View Details** to check the upgrade result.

9.2.6 Upgrade Online

Upgrade the firmware of devices like network cameras and network video recorders to fix device failures or security issues. Ensure the network can access both your devices and a public network.

1. Click **Check for Upgrades** to view device upgrade status. If automatic upgrade detection is enabled in the upgrade settings, the system will automatically check for upgrades upon reopening the tool or adding new devices.



If no packages are found, contact technical support.

2. Select devices with available upgrade packages and click **Upgrade Online**.
3. Check the upgrade process. Click **View Details** to check the upgrade result.

9.3 Change IP

9.3.1 Change IP for Added Devices

To enhance security (e.g., regular IP updates), you can modify network parameters (IP address, port, subnet mask, gateway) for multiple devices. Cameras support IPv6 addresses.

1. Go to **Maintenance → Change IP**.
2. (Optional) Click **Scan Active IP** to check available IP addresses.
 - a. Set the network card, start IP, and end IP.
 - b. Click **Start** to view available IPs.



- Ensure the new IP, gateway, and subnet mask share the same IP version (IPv4/IPv6).
- IPv6 addresses are static.

3. Select **Export** to export and fill out the IP change template (including the old IP address, old port No., new IP address, and new port No.)
4. Import the template.
5. (Optional) Select **Automatically Add Devices Not in List** to add the devices in the template but not yet added to the device list.
6. (Optional) If you select **Automatically Export Results to Local**, IP change results will be automatically exported to your local PC. You can click **Open Folder** to check the Excel report.
7. Select **OK**.

9.3.2 Edit Network Parameters for Discovered Devices

After devices on the same LAN as HiTools Delivery are activated on the device search page, you can edit network parameters.

1. In the Online Device List, select **activated** devices.
2. Select **Network Parameter** and set the parameters.



Note

If you enable **DHCP**, an IP address and other network configuration parameters will be dynamically assigned to each device.

3. Set the admin password and click **OK**.
4. After editing network parameters, select **Refresh** to check the result.

9.4 Edit Device Name

Export and fill a rename template for batch name modification.

1. Select **Maintenance → Edit Name**.
2. Export and fill out the rename template.
 - **Export selected devices:** Enter the user name, password, and new name for selected devices in the template.
 - **Export blank template:** In the standard template, input device IP, port, username, password, and new name.



Note

Device names must be within 128 characters (subject to device capability; excess characters will be truncated automatically).

3. Import the template and click **OK** to apply changes.

9.5 Change Password

To prevent information leakage, installers can set uniform user names/passwords during deployment and later update them in bulk before handing devices over to end-users or maintenance personnel.

Scenario 1: Change Online

Applicable when devices are already in the device list and share the same current password.

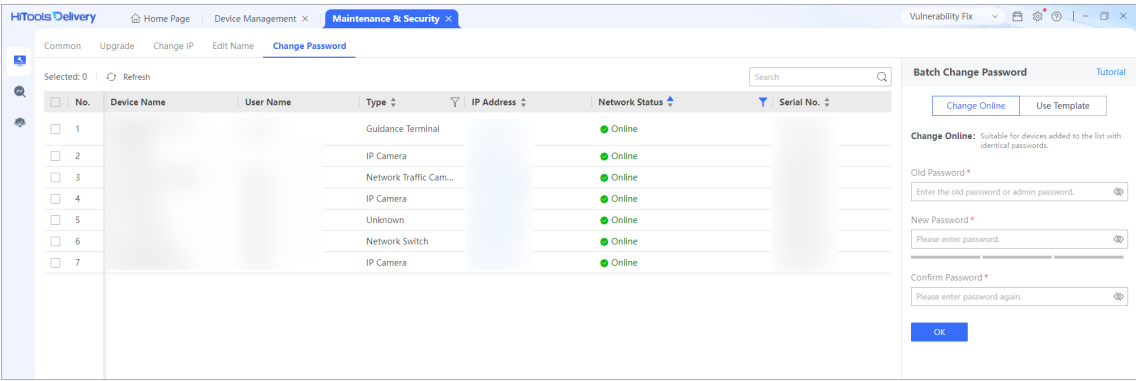


Figure 9-9 Change Online

1. Click **Change Online**.
2. Select target devices, enter the current password, new password, and confirm the new password.
3. Click **OK**.

Scenario 2: Template Modification

Applicable when devices have different current passwords or some devices are not yet in the device list.

1. Click **Use Template**.
2. Export and fill out the password change template.

	A	B	C	D	E
1	Device IP Address	Device Port	User Name	Old Password	New Password
2	10.	80	admin		
3	10.	80	admin		
4	10.	80	admin		
5	10.	80	admin		
6	10.	80	admin		
7	10.	80	admin		
8	10.	80	admin		
9	10.	80	admin		
10					
11					

Figure 9-10 Export Selected Devices

- **Export selected devices:** Enter the current and new passwords for selected devices.
 - **Export blank template:** In the standard template, input device IP, port, user name, current password, and new password.
3. Import the template.

4. (Optional) Select **Automatically Add Devices Not in List** to add the devices in the template but not yet added to the device list.
5. Select **OK**.

9.6 Device Diagnostics

9.6.1 Introduction

Based on the diagnostics schedule, perform bulk checks on the health status and core parameters of cameras, recording & analysis devices, access control devices, and capture cameras. View the Excel inspection report to help installers quickly complete delivery verification and enable maintenance personnel to efficiently troubleshoot device anomalies. **Supported devices and diagnostics items are as follows:**

Table 9-5 Diagnostics Items

Device Type	Items
Camera	• Time Settings: Time Zone, DST, etc. • SD Card • Network Status: IP conflicts, network disconnections, connectivity issues, etc. • Device Security: Unauthorized access attempts, device lock status, 802.1x certificate validity, HTTPS certificate validity, etc. • Picture Capture
Device & Analysis Device	• Time Settings: Time Zone, DST, etc. • HDD Status • Network Status: IP conflicts, network disconnections, connectivity issues, etc. • Device Security: Unauthorized access attempts, device lock status, 802.1x certificate validity, HTTPS certificate validity, etc. • Recording/Picture Capture • Video Parameters: Video signal status, input/output video standards, encoding compatibility, etc.
Access Control	• Time Info: Time, Time Zone, and DST. • Network Status: IP Conflicts / Network Disconnection. • Security: Device Locking • Face Recognition: Face Authentication Pass Rate

Device Type	Items
	- Arming Clients - Exception Events: Door Opened by Force; Door Open Timeout
Capture Cameras	- Time Info: Time, Time Zone, and DST. - Network Status: Network Latency & Packet Loss - Storage: TF Card Status - Channel Snapshot - Preview & Arming Status: Number of arming clients and streaming channels

9.6.2 Video

Video	Supported Software Version	Video QR Code
<u>Device Diagnostics</u>	V2.0 or later	

9.6.3 Steps

1. On the homepage, click **Device Diagnostics**.
2. In the upper-right corner of the diagnostics interface, click **Settings** to set the schedule and report export path.

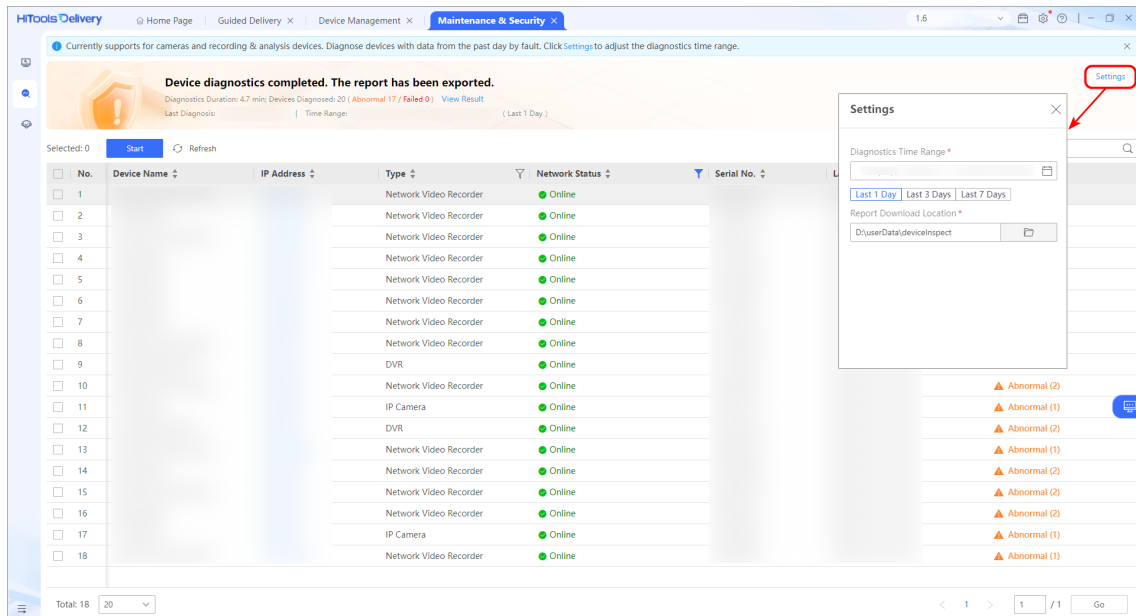


Figure 9-11 Diagnostics Settings

3. Select the online devices to be diagnosed and click **Start**. The diagnostics report will be automatically downloaded to the specified path.

Note

If you click **Stop**, pending diagnostics tasks for unchecked devices will be terminated and marked as failed.

4. View the detailed Excel report and captured images directly from the system popup. You can also Click **View Details** to access the detailed Excel file and captured picture files. If any device anomalies are detected, adjust the device configuration based on the provided recommendations.

Device Name	IP Address	Type	Item	Result	Solution	
IP CAMERA		Time	Time Zone	Normal		
			Time	Abnormal	Keep device time consistent with the PC.	
			DST	Normal		
		Network Status	IP Address Conflict	Normal		
			Network Disconnected	Normal		
			Device Offline	Normal		
			SD Card Faults	Normal		
		SD Card	SD Card Damaged	Normal		
			Security	Illegal Login	Normal	
				Device Locked	Normal	
		802.1x Certificate (Client, CA)		Normal		
		HTTPS Certificate (Server)		Normal		
		SRTP Certificate (Server)		Normal		
		Enhanced SDK Service Certificate (Server)		Normal		
		Image		Capture	Capture	_Camera 01.jpg
				Time Zone	Normal	
				Cover	Camera	Recording & Analysis Device

Figure 9-12 EXCEL Result

9.7 Security Hardening

9.7.1 Introduction

Scan and fix vulnerabilities for cameras, recording & analysis devices, access control devices, video intercom devices, and more. You can perform multiple scans and apply fixes for vulnerabilities.

For security advisories related to device vulnerabilities, visit the Hikvision official website: **Support → Security Advisory** .

9.7.2 Video

Video	Supported Software Version	Video QR Code
<u>Security Hardening</u>	V2.0 or later	

9.7.3 Steps

1. On the homepage, click **Security Hardening**.
2. Select the online devices to be scanned (up to 500 devices supported) and click **Scan**.

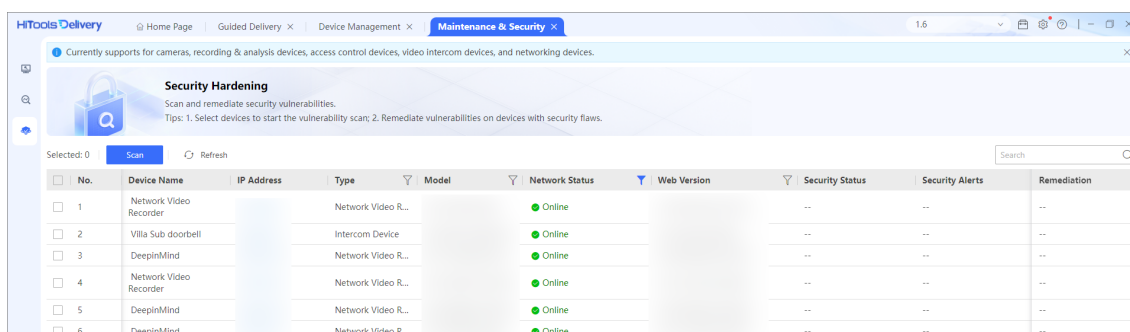
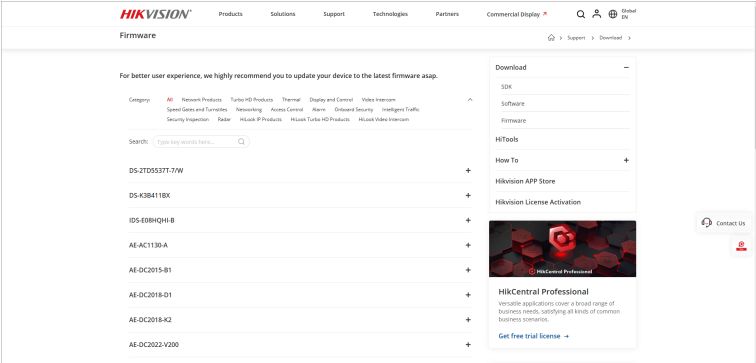


Figure 9-13 Scan Vulnerabilities

3. After scanning, click **View Details** to check results and export the scan report.
4. If vulnerabilities are detected, review security alerts and apply remediation strategies to fix them.

Table 9-6 Remediation Modes

Modes	Description
Offline Remediation	If selected devices require different remediation strategies, use offline remediation: a. Select the target devices and click Offline Remediation. b. Use one of the following methods to get upgrade packages:

Modes	Description
	- In a public network environment, click Get Upgrade Package based on the device type and model, then download the package from the official website.  Figure 9-14 Get Upgrade Package - Click the link in the Security Alerts column to view and download the upgrade package from the official website.  Note The same upgrade package applies to devices of identical models. c. After importing the downloaded upgrade package, click OK.  Note For VPro Series NVRs with AcuSeek, the tool performs a pre-check upon importing the upgrade package. If the search algorithm version is incompatible, historical data must be re-indexed (re-modeled), and manual confirmation is required to proceed with the upgrade. If the compatibility test failed, the device cannot be upgraded.
Online Remediation	In a public network environment, select devices and click Online Remediation.  Note Online remediation is only supported for some network bridges (DS-3WF0AC-2NT / DS-3WF01C-2N/O).

- (Optional) Click **Stop**, only records for devices already remediated and remediating faults will be retained.
- After repair completion, click **View Details** to check and export repair results.

Chapter 10 Task Center

After applying parameters, a task will be automatically created and added to the task center. You can view the progress, status, and results of the task in the task center. If the task fails, you can check the failure details.

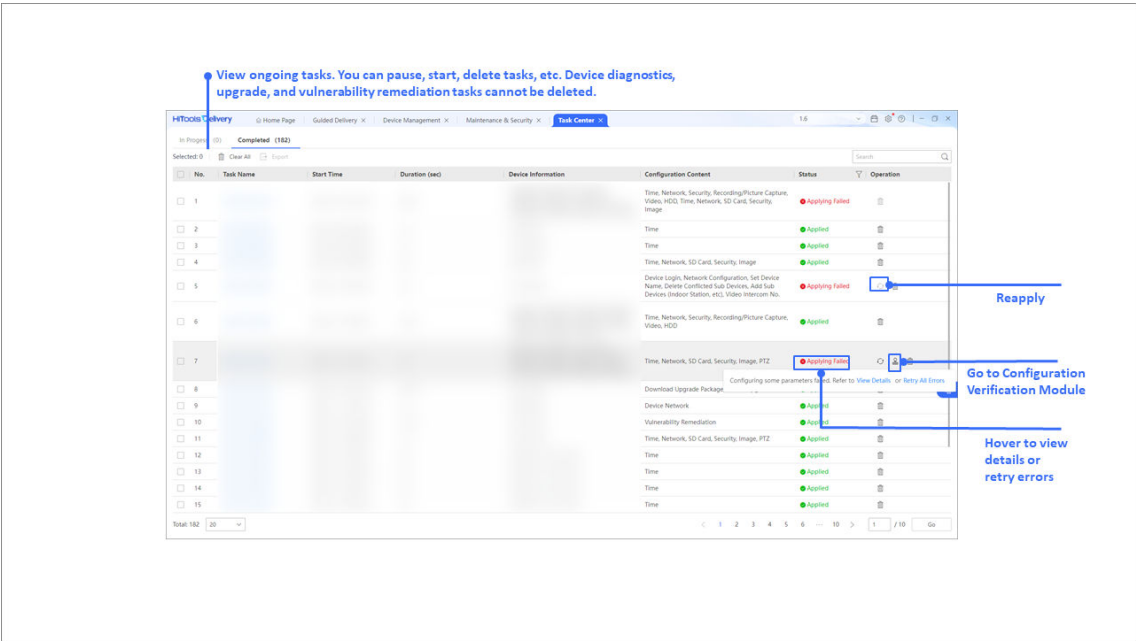


Figure 10-1 Task Center

Chapter 11 Toolkit

In the upper right corner, click  .

Table 11-1 Toolkit Overview

Toolkit	Description
Upgrade Package Lookup	On a public network, select a lookup mode to search for and download the firmware upgrade package. After getting the upgrade package, switch to the private network, then navigate to Maintenance → Upgrade → Upgrade Locally to complete the device upgrade. For details, refer to: <i>Upgrade Devices</i> .
Picture Validator & Optimizer	It is designed for access control, time attendance, and facial recognition. It rapidly filters and optimizes non-compliant images (e.g., incorrect resolution/format/size, missing or multiple faces, and occlusions). By validating processed photos, it ensures high batch-import success rates and prevents authentication failures caused by invalid images. For details, refer to: <i>Picture Validator & Optimizer</i> .
Ping Tool	Test target IPs or domain names, displaying network latency between computers, platforms, or devices.
IP Scanner	Identify active and unused IP addresses on-site. Refer to: <i>Change IP</i> .
VSPlayer	VSPlayer is designed for seamless online streaming and local video playback. It offers advanced features like play control, VCA information overlay, video clipping and merging, and transcoding. It is compatible with various video formats including H.264, Smart264, H.265, SVAC, and MPEG4.
Format Converter	This tool is used for converting the formats of advertisement videos before importing videos to devices such as door stations and MinMoe face recognition terminals in the Linux system.

11.1 Picture Validator & Optimizer

11.1.1 Introduction

Prevent batch import failures caused by non-standard photos (occlusions, low clarity, etc.). This tool provides **pre-screening and batch repair** to ensure high first-time success rates and quickly identify invalid photos requiring re-collection.

11.1.2 Steps

1. Log in to the device for picture validation.

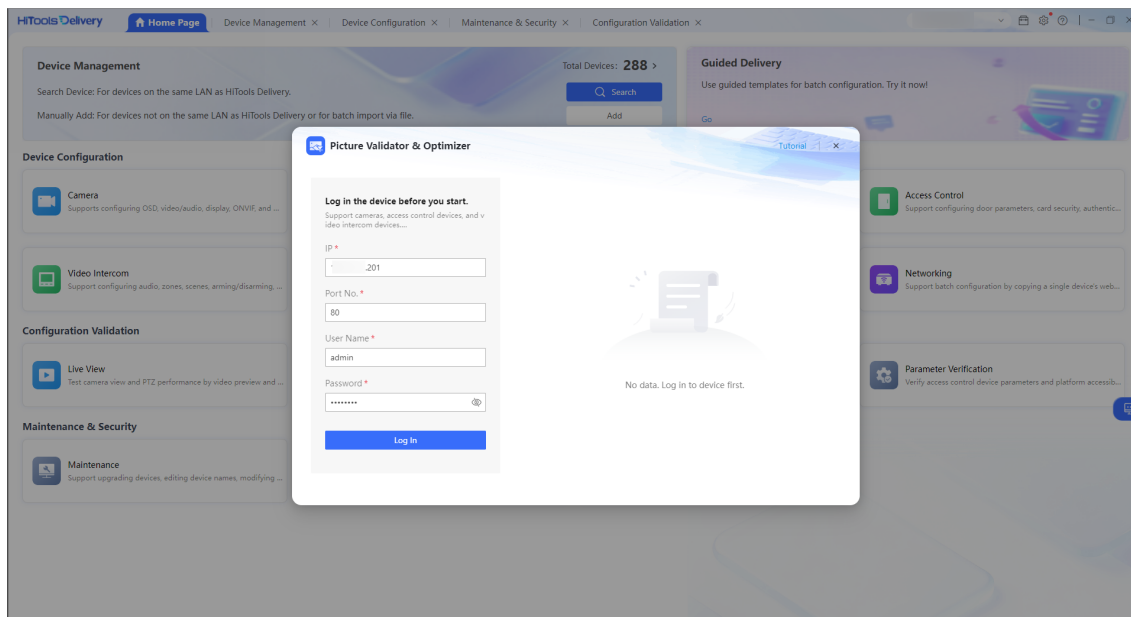


Figure 11-1 Log in to Device

2. Upload pictures or folders, then click **Validate**.

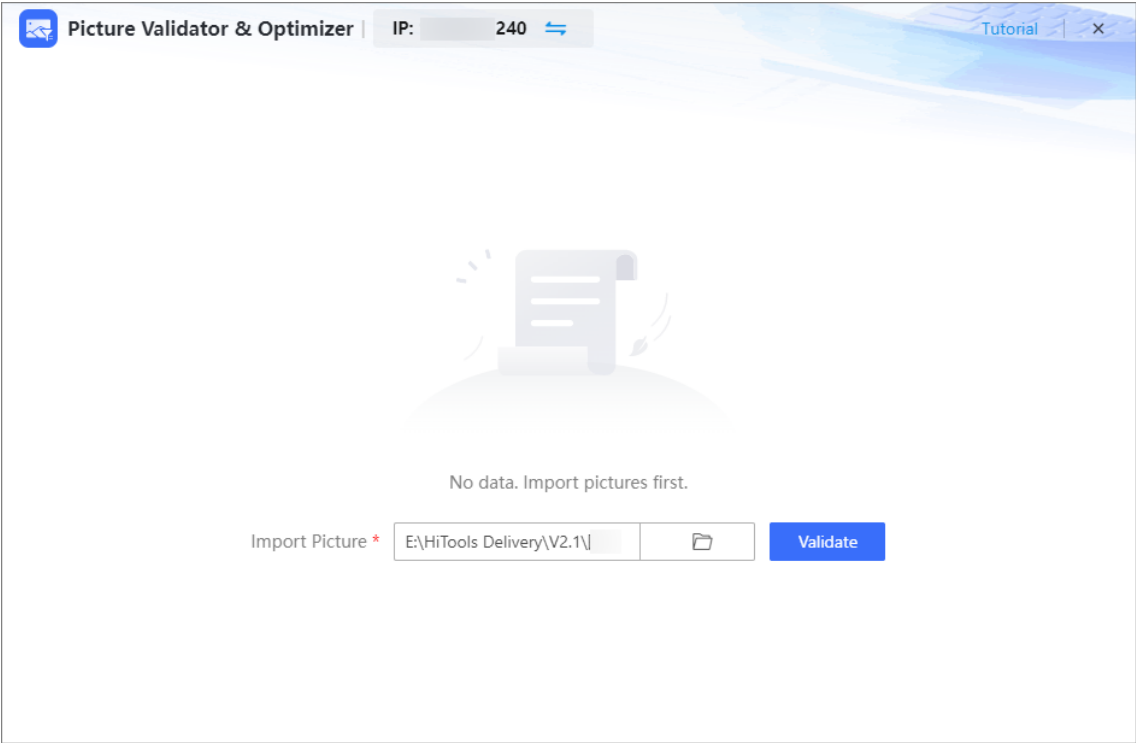


Figure 11-2 Upload Pictures for Validation

3. Review the results. Optimize non-compliant pictures or follow standards to re-collect photos.

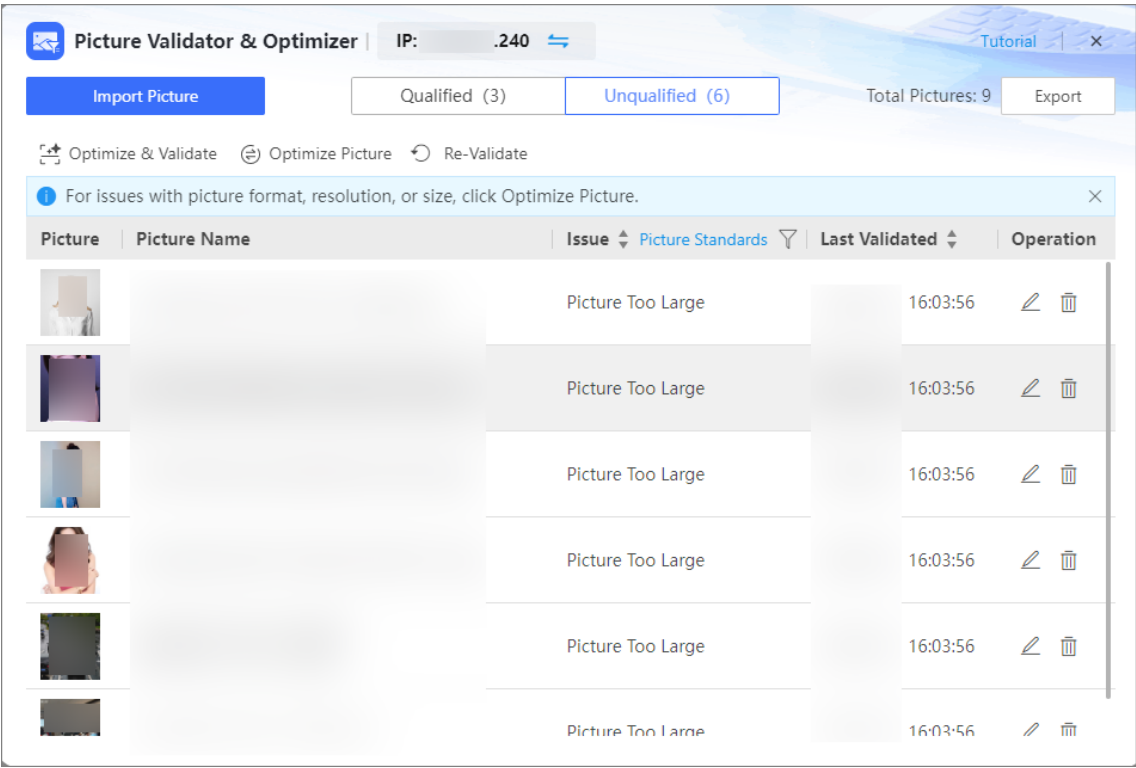


Figure 11-3 Optimize and Validate Non-compliant Pictures

- Optimization & Validation
For issues related to image format, size, or resolution, use the following methods:
 - Click **Optimize & Validate**, set the required size and resolution according to standards, then click **Optimize & Validate** to check the results. If validation fails (e.g., face recognition failure), re-collection is required.

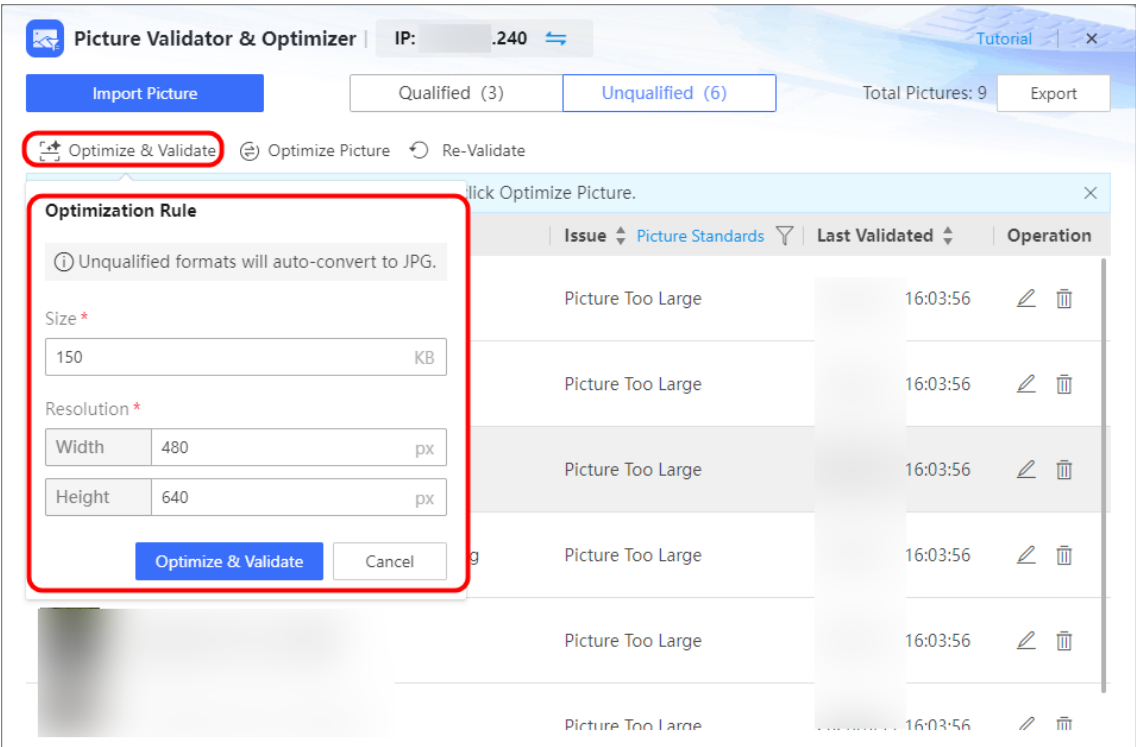


Figure 11-4 Optimize and Validate

- Click **Optimize Picture**, configure the size and resolution, then click **Re-Validate**.
- Click a picture to view the full size. Click **Edit Picture** in the top-right corner to crop or resize, then click **Save** or **Save & Validate**.

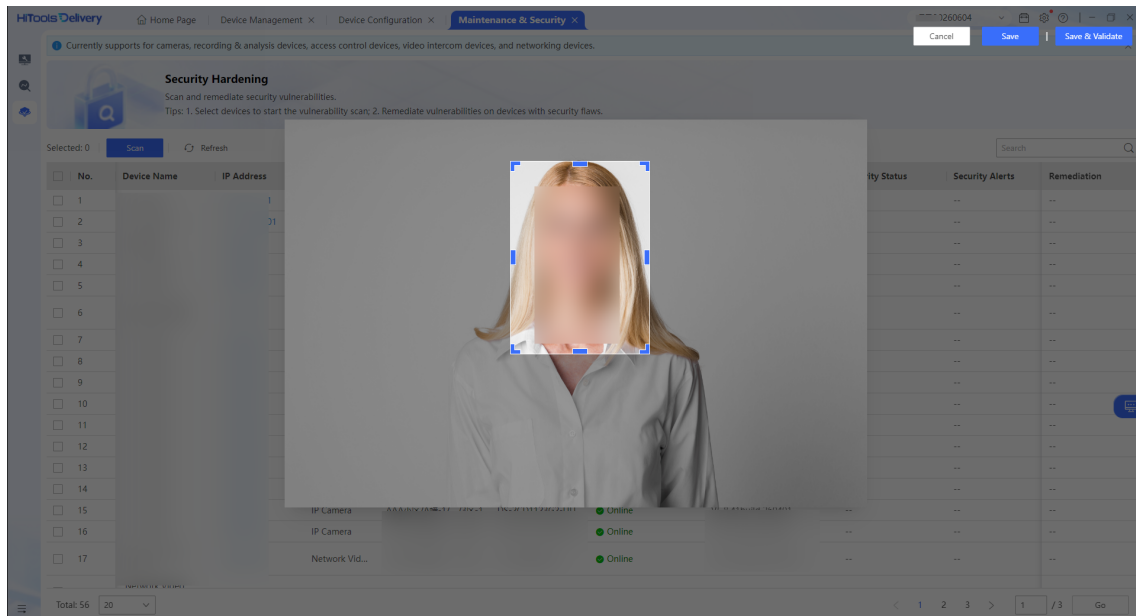


Figure 11-5 Crop Picture

- In the Operation column, click  , adjust the dimensions, and click **Save** or **Save & Validate**.
- Re-collection
For issues that cannot be resolved by resizing (e.g., poor face quality, small interpupillary distance, or occlusions), click **Picture Standards** and follow the guidelines to re-collect the photos.
- 4. (Optional) Click **Import Picture** to add new photos for validation.
- 5. Click **Export** to download the list of non-compliant images and folders (categorized into passed/failed) for further re-collection or device import.

Note

It is recommended to maintain version consistency between the device used for image validation and the destination device for final import.

Chapter 12 System Settings

- **General Settings**
- **Download Extensions**
- **Manage Passwords**

12.1 General Settings

Set the update file location path, default startup page, and the software language.

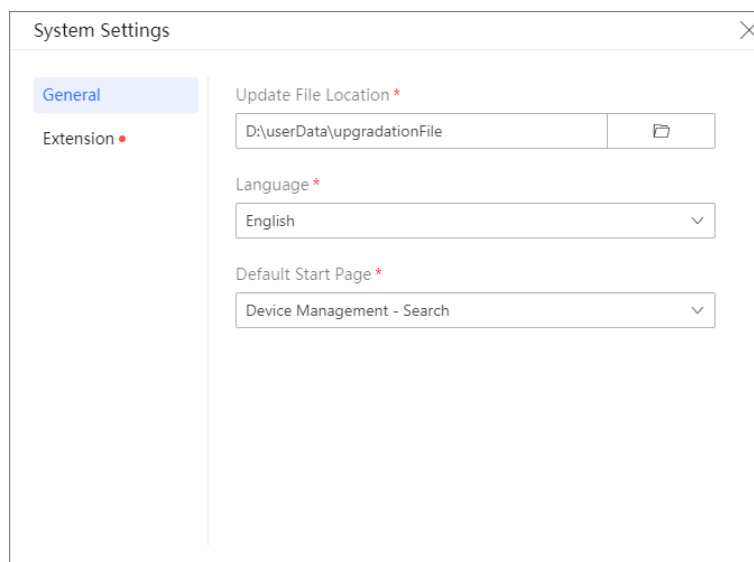


Figure 12-1 General Settings

12.2 Download Extensions

After configuration extensions are downloaded, you can copy a single device's web parameters to multiple devices of the same model.

Supported devices: cameras, recording & analysis (NVR, DVR, DeepMind Intelligence), access control devices, video intercom devices, traffic cameras, audio & sensing (public address devices, speakers), network bridges, alarm devices, on-street parking cameras, control devices (decoders, video wall controllers, MVC, KVM), and interactive flat panels (digital signage series).

1. Download extensions.

Environment	
Public Network	Click  or  to update or download all available extensions.
Private Network	You can download extensions in one of the two ways: - Click , use your mobile browser to scan the QR code and download the extension, transfer the file to your computer, and then click Import/Export → Import to install it manually. - In a public network, click  to download available extensions, and then click Import/Export → Export to export all downloads. In a private network, click Import/Export → Import to import extensions.

You can also download extensions from the links below and import them to the on-site computer.

Extension Type	Download Link
Basic Service Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/BasePlugin/BasePlugin_Plug_2.1.0.0.zip
Encoding Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/CameraPlguin/CameraPlguin_Plug_2.1.0.0.zip
Access Control & Video Intercom Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/AccessControlPlguin/AccessControlPlguin_Plug_2.1.0.0.zip
Alarm Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/AlarmPlguin/AlarmPlguin_Plug_1.5.0.0.zip
Networking Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/NetworkingPlguin/NetworkingPlguin_Plug_1.6.0.0.zip

Extension Type	Download Link
Recording & Analysis Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/BackendPlguin/BackendPlguin_Plug_1.6.0.0.zip
Intelligent Traffic Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/ITSPlguin/ITSPlguin_Plug_2.1.0.0.zip
Audio & Sensing Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/AudioSensingPlguin/AudioSensingPlguin_Plug_2.0.0.0.zip
Control Device Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/ControlPlguin/ControlPlguin_Plug_1.6.0.0.zip
Interactive Flat Panel Configuration Extension	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/FlatPanelDisplayPlguin/FlatPanelDisplayPlguin_Plug_1.6.0.0.zip
Extension for Devices via Private Protocol	http://hikdownload.hik-connect.com/HiTools/windows/overSea/ComponentManagement/HD/RemoteConfugPlugin/RemoteConfugPlugin_Plug_2.1.0.0.zip

- Once downloaded, go to the Device Configuration module and select your devices. In the upper-right corner, click **Configure More** to set the parameters. Close the panel when finished.

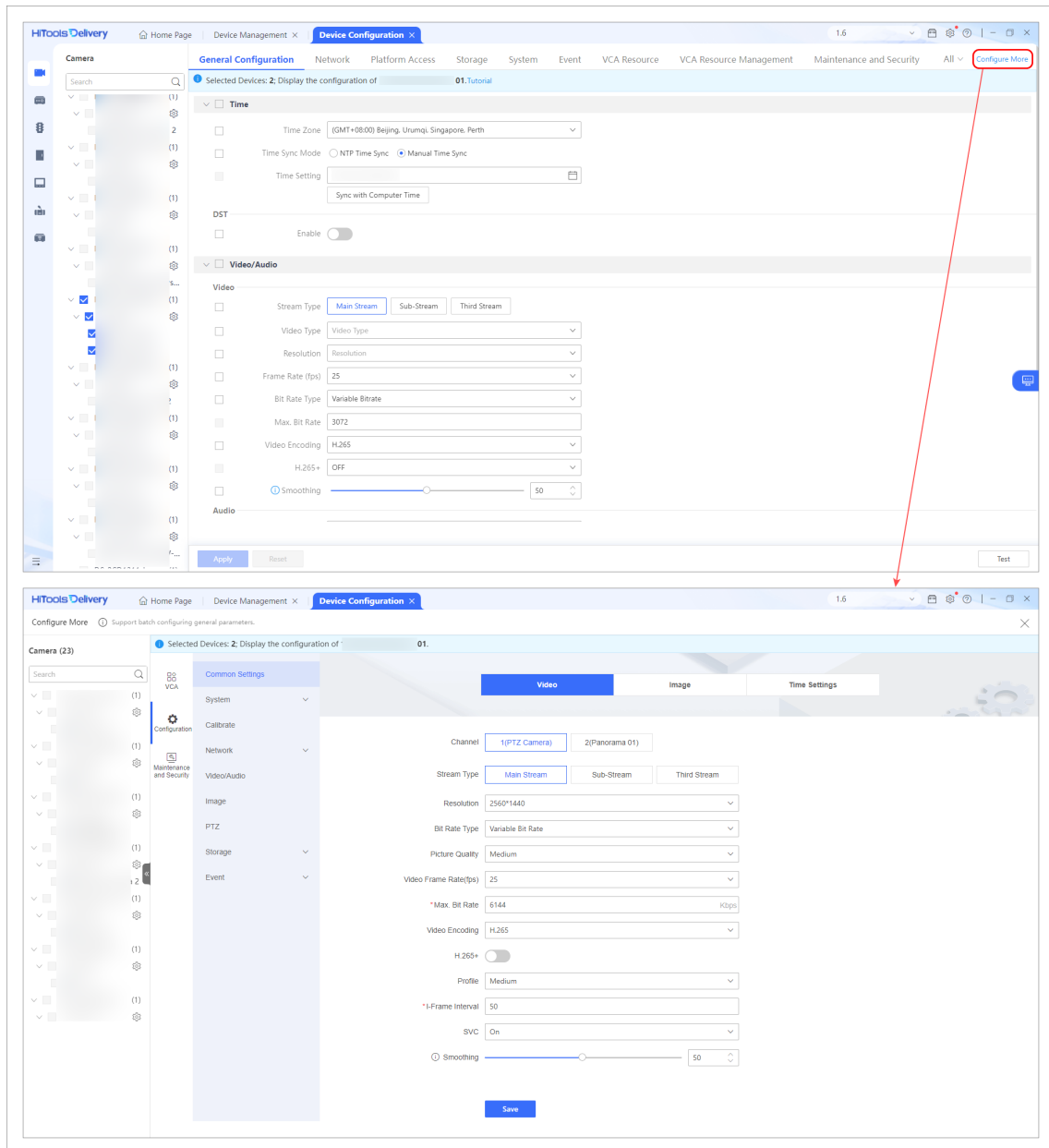


Figure 12-2 Configure More

12.3 Manage Passwords Across All Projects

Passwords saved in the Password Manager can be quickly applied during device addition, activation, or configuration, eliminating the need for repetitive manual input.

Introduction

Passwords saved in the Password Manager can be quickly applied during device addition, activation, guided delivery or configuration, eliminating the need for repetitive manual input.



Note

- Up to 20 passwords can be added.
- Passwords in the Password Manager are shared across all projects.

Two Ways to Create Passwords

- Via Password Manager

In the System Settings interface, go to **Password Manager** → **Add** and enter the password and remarks.

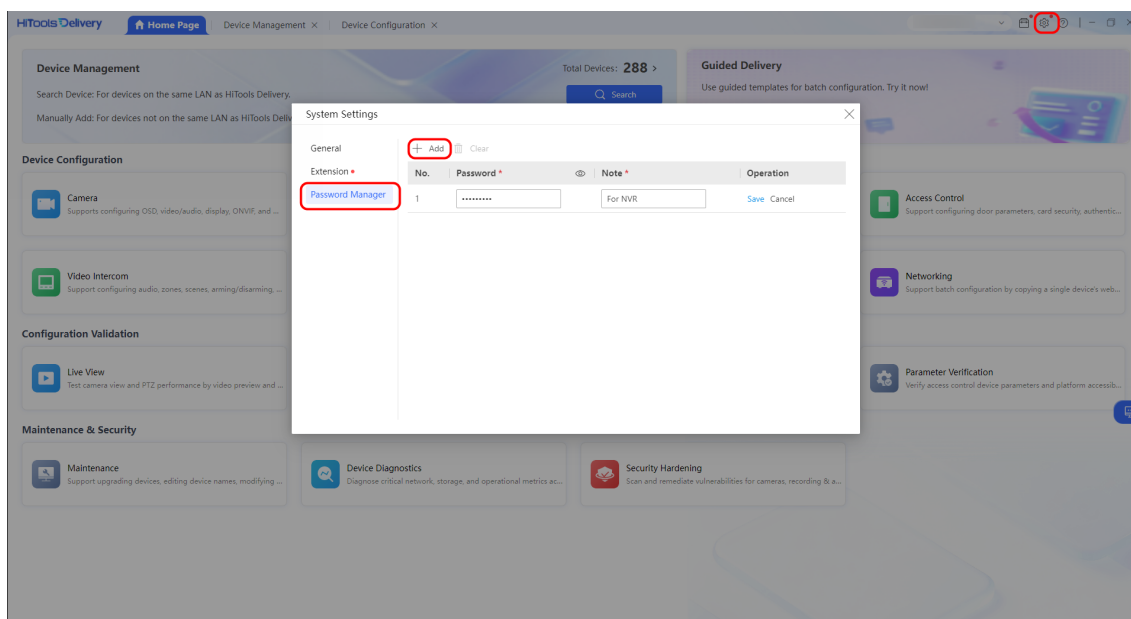


Figure 12-3 Adding Passwords via Password Manager

- Via Configuration Interfaces

When entering a new password in any configuration interface, click **Save to Password Manager**, enter remarks, and click **OK**.

Add [X]

Adding Mode

☒ IP ☐ IP Segment ☐ Batch Import

Protocol Type ⓘ

☒ Adaptive ☐ ISAPI ☐ Private ☐ OTAP

Applicable to virtually all products; uses the device's default port for login. If the default port is modified, please use alternate protocols.

IP Address *

User Name *

admin

Password *

..... [Eye Icon]

New password. [Save to Password Manager](#) for future use? [X]

Ungrouped Devices [v]

[OK] [Cancel]

Figure 12-4 Add Password to Password Manager via Configuration Interface

Quickly Access and Apply Saved Passwords

Once passwords are saved, you can select them from the list during device addition, password modification, activation, or network configuration for quick access.

Add

Adding Mode

☒ IP

☐ IP Segment

☐ Batch Import

Protocol Type ⓘ

☒ Adaptive

☐ ISAPI

☐ Private

☐ OTAP

Applicable to virtually all products; uses the device's default port for login. If the default port is modified, please use alternate protocols.

IP Address *

User Name *

admin

Password *

Saved Passwords

Show Password

For NVR

OK

Cancel

Figure 12-5 Applying Saved Passwords

Chapter 13 How-To Videos

Note

To enhance your experience, the product is continuously optimized. Some video content may lag behind the latest version. Please refer to the actual application for accuracy. Updates will be released soon; stay tuned via **What's New**.

- **Pre-Configuration**
- **Device Management**
- **Device Configuration**
- **Maintenance & Security**
- **Toolkit**

13.1 Guided Delivery

Video	Supported Software Version	Video QR Code
<u>How to Configure Entrance & Exit Template</u>	V1.3.0	
<u>How to Configure Camera Template</u>	V1.1.0	

13.2 Device Management

13.2.1 Add Devices

Video	Supported Software Version	Video QR Code
<u>How to Batch Add Devices with Excel Template</u>	V1.0.0	

13.2.2 Upgrade Devices

Video	Supported Software Version	Video QR Code
<u>Online Device Upgrade</u>	V1.3.0	

13.3 Device Configuration

Supported Version

V1.0.0 and later

Video

Video	Main Content	Video QR Code
<u>How to Configure Cameras and Test Events</u>	• Time Settings (0:00:10) • Video & Audio Settings (0:00:32) • OSD (0:00:51) • Intrusion Detection (0:02:18) • Line-Crossing Detection (0:03:32)	
<u>How to Configure Cameras, Access Control Devices, Video Intercoms, and LED Screens</u>	• 802.1X (0:00:12) • ONVIF (0:01:14) • Multi-Target-Type Detection (0:01:53) • Set Anti-Passback Route for Turnstiles (0:02:42) • Add Cameras to NVR (0:03:43) • Display Configuration of Access Controls & Video Intercoms (0:04:14) • Import App on Video Intercoms via HEOP (0:05:13) • Display Configuration of Entrance & Exit LED Screen (0:05:46) • Upgrade Parking Cameras (0:06:34)	

13.4 Maintenance & Security

Video	Supported Software Version	Video QR Code
<u>Device Diagnostics</u>	V2.0 or later	
<u>Security Hardening</u>	V2.0 or later	

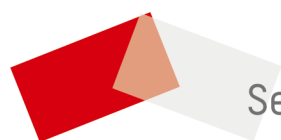
13.5 Toolkit

Supported Version

V1.3 and later

Video

Video URL	Content	Video QR Code
<u><i>Toolkit Introduction</i></u>	• IP Migration • Upgrade Package Lookup	



See Far, Go Further