Hik-Partner Pro

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.

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.

©2025 Hikvision All rights reserved.

Contents

Chapter 1 Hik-Partner Pro 1
1.1 Entities in Hik-Partner Pro 1
1.2 Running Environment 3
1.2.1 Running Environment for Portal 3
1.2.2 Running Environment for Mobile Client 4
1.3 Function Availability for Different Regions 4
1.3.1 Functions Only Available in Certain Regions 4
1.3.2 Regions Only with Support for Free Functions 5
1.4 Partner Quick Start Guide 7
1.4.1 Step 1: Register Accounts 7
1.4.2 Step 2: Authenticate Company to Use More Features 8
1.4.3 Step 3: Access Products Info & Trends 9
1.4.4 Step 4: Add, Hand Over, and Maintain Devices 14
1.4.5 Step 5: Provide Your Customer with More Value-Added Services 15
Chapter 2 Start Security Business from Presales Stage 19
2.1 How to Compare and Select Products 19
2.1.1 Compare and Select Products Using the Portal 19
2.1.2 Compare and Select Products Using the Mobile Client 21
2.2 HPP Designer: How to Design Your Security and Network Project for Quotation 25
2.2.1 Overview 25
2.2.2 Before You Start 29
2.2.3 Create a Project 31
2.2.4 Part A: Indoor Design 32
2.2.5 Part B: Outdoor Design 56
2.2.6 Device List, Quotation and Export 65
2.2.7 Hikie Designer 71

2.2.8 Global Settings and Templates 73
2.3 How to Create Product Quotations 74
2.3.1 Create Products Quote for Customer Using the Portal 74
2.3.2 Create Products Quote for Customer Using the Mobile Client 76
2.4 How to Create and Manage Project 77
2.4.1 Create a Project 78
2.4.2 Compare Products 79
2.4.3 View Project History 80
2.5 How to Place Orders for Products 83
2.5.1 Create an Order Using the Portal 83
2.5.2 View My Orders Using the Portal 84
2.5.3 Set Availability Alert and Manage My Waiting List Using the Portal 88
2.5.4 Manage Hikvision Quote for Me Using the Portal 89
Chapter 3 Set Up & Deliver Security System and Connect with Your Customers 91
3.1 Quick Initialize Devices on Site and Add to HPP for Remote Maintenance 91
3.1.1 Quick Initialize Network with AC Router and APs 91
3.1.2 Use the SADP Tool to Quick Initialize LAN Devices 93
3.1.3 SADP Tool: Quick Deploy and Professional Modes 101
3.1.4 AI Config Assistant: Scenario-Matched Configuration Recommendation 153
3.1.5 Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance 165
3.1.6 How to Get the Device Serial Number and Verification Code? 169
3.2 Batch Configure Devices on LAN 175
3.2.1 Batch Activate Devices and Assign IP Addresses for Them 177
3.2.2 Batch Link Channels to NVR and DVR 179
3.2.3 Create Template for Setting Parameters 180
3.2.4 Batch Set Parameters for Devices via Template 181
3.3 On-Site Configure Devices Using the SADP Tool / via the Site page 184
3.3.1 Encoding Devices 184

3.3.2 Manage Security Control Panel 190
3.3.3 Manage Network Devices 201
3.3.4 Healthcare Radars 310
3.4 Deliver to Customers & Maintain Customer Relationships 313
3.4.1 Add/Edit Sites to Keep Track of Customer Information 316
3.4.2 How to Hand Over Site & Devices to Your Customer 317
3.4.3 Co-Branding: Maintain Customer Loyalty and Increase Your Brand Visibility 326
3.4.4 Group Sites to Manage Multiple Sites More Efficiently 339
3.4.5 How to Move Devices from One Customer Site to Another? 343
3.4.6 How to Get a Device Management Invitation from Your Customer? 345
3.4.7 How to Apply for Site Authorization & Device Permissions from Customers? 348
3.5 Manage Your Company, Employees, and Service Partners 351
3.5.1 Authenticate Company to Use More Features 352
3.5.2 Add Employees to Your Company and Remove Account Limit with Add-On 353
3.5.3 How to Configure Azure AD Login and Log In to Hik-Partner Pro via Azure AD 362
3.5.4 How to Configure Google Workspace Login and Log In to Hik-Partner Pro via Google Workspace 376
3.5.5 How to Manage Two-Factor Authentication 389
3.5.6 How to Use Biometric Login 406
3.5.7 How to Assign Sites to Installers as Site Managers? 410
3.5.8 Collaborate with an ISP/MSP on Site for Device Installation or Maintenance 414
3.5.9 Transfer Sites and Devices to Another Account 416
3.5.10 Merge Your Company with Another Company 425
Chapter 4 Template Center: How to Use Device Configuration and Handover Templates 434
4.1 What This Is and When to Use It 434
4.1.1 In One Sentence 434
4.1.2 Two Kinds of Templates 434
4.1.3 Typical Scenarios 435

4.1.4 Clients and Permissions at a Glance 436
4.1.5 Scope 436
4.2 Handover Templates: Create One on the Portal 437
4.2.1 Step 1: Set Name and Method 437
4.2.2 Step 2: Set Permissions 438
4.3 Handover Templates: Manage and Use 442
4.3.1 Manage Handover Templates on the Portal 442
4.3.2 Hand Over with a Template on the Mobile Client 444
4.4 Device Configuration Templates: Create One 446
4.4.1 Prerequisites 446
4.4.2 Create a Device Configuration Template Using the Portal 446
4.4.3 Create a Device Configuration Template Using the Mobile Client 448
4.5 Device Configuration Templates: Manage and Use 451
4.5.1 Manage Device Configuration Templates in Template Center 451
4.5.2 Apply Device Configuration Template to Device 454
Chapter 5 Maintain Customers' Devices to Grow Your Aftersales Business 462
5.1 Remote Device Configurations as Powerful as Configurations Over LAN 462
5.2 How to Reset Device Password 463
5.2.1 Reset Password for Nearby Device 464
5.2.2 Reset Password for Devices Added to Hik-Partner Pro 464
5.2.3 Reset Password by Submitting Case 466
5.2.4 Reset Password via Old Password 467
5.2.5 Reset Password via Reserved Email / Security Questions 467
5.2.6 Reset Password by Sending Email to Technical Support 470
5.3 How to Upgrade Devices 472
5.3.1 Batch Upgrade Device on LAN 473
5.3.2 Upgrade Device Automatically 473
5.3.3 Upgrade Device Manually by Uploading Firmware Package 474

5.4 How to Unbind Devices? 476
5.5 How to Set Linkages to Trigger Actions When Events Occur? 477
5.5.1 Add and Enable a Linkage 479
5.5.2 Enable Notification for the Source Device 489
5.5.3 What Are the Six Template Linkages For? 490
5.5.4 Available Triggering Events for Different Source Devices 491
5.5.5 Available Linkage Actions for Different Linked Resources 492
5.6 How to Set Up Exception Rules to Receive Exception Notifications? 494
5.6.1 Add an Exception Rule 495
5.6.2 Enable Notification for the Source Device 497
5.7 How to Configure Device Offline Delay? 498
5.8 How to View Device Health Status in Real Time? 500
5.8.1 View Devices Health Status 500
5.8.2 Supported Device Status and Operations for Different Device Types 506
5.9 Health Monitoring: AI Diagnostics & One-Click Fix Guide 509
5.9.1 Feature Overview 509
5.9.2 Applicable Scenarios 509
5.9.3 Prerequisites 510
5.9.4 Supported Device Types 510
5.9.5 AI Diagnostics Workflow 510
5.10 How to Export Device Health Report and Set Scheduled Report Delivery? 511
5.10.1 Export Reports Manually of a Site 513
5.10.2 Set Scheduled Report Delivery 513
5.11 How to Create Maintenance Quotation? 515
5.12 How to Get Operations Logs of Employees for Troubleshooting? 518
5.13 How to Provide an ARC Service on Hik-Partner Pro to Expand Your Business? 519
5.13.1 Feature Overview 519
5.13.2 Overall Instruction 520

5.13.3 View of Authorizing an ARC Service Provider 521
5.13.4 Authorization Rules for ARC Service 521
5.13.5 Step 1: ARC Company Joins the ARC List of Hik-Partner Pro 523
5.13.6 Step 2: Installer Enables ARC Service for Customer's Devices 525
5.13.7 Step 3: ARC Service Provider Accepts Devices Entrusted by Installers 528
5.13.8 Step 4: ARC Manages Entrusted Devices 530
5.13.9 Step 5: ARC Establishes Communications Between ARC Software and Devices Using IP Receiver Pro 534
5.14 How to Integrate with Hik-Partner Pro? 535
Chapter 6 Provide Value-Added Services: Expand Your Business 538
6.1 Health Monitoring Service: Better Maintenance for Your Customers 538
6.1.1 Step 1: Get Health Monitoring Packages 540
6.1.2 Step 2: Activate Health Monitoring Service for Customers' Devices 542
6.1.3 Step 3: Manage Health Monitoring Packages 543
6.2 Remote Maintenance Pro Service: Better Maintenance for Your Customers 547
6.2.1 Step 1: Get Remote Maintenance Pro Packages 549
6.2.2 Step 2: Activate Remote Maintenance Pro Service for Customers' Devices 551
6.2.3 Step 3: Manage Remote Maintenance Pro Packages 552
6.3 Cloud Storage Service: Secure & Expand Your Customers' Storage 554
6.3.1 Device Compatibility for Cloud Storage Service 555
6.3.2 Step 1: Get Cloud Storage Service Packages 559
6.3.3 (Optional) Step 2: Perform Uplink Bandwidth Test 560
6.3.4 Step 3: Configure Cloud Storage and Activate Service for Devices 561
6.3.5 Step 4: Manage Cloud Storage Service Packages 571
6.4 SIM Data Service: Connect Devices to 4G Network 572
6.4.1 Step 1: Get SIM Card and Set APN on Devices 572
6.4.2 Step 2: Get SIM Data Service Packages 573
6.4.3 Step 3: Activate SIM Data Service for SIM Card 574

6.4.4 Step 4: Manage SIM Cards and SIM Data Service Packages 575
6.5 SIM Data Pool Service: Cards Share Data in a Pool 577
6.5.1 Step 1: Add SIM Cards to Data Pool 578
6.5.2 Step 2: Get SIM Data Pool Service Packages 578
6.5.3 Step 3: Activate SIM Data Pool Service for Pool 579
6.5.4 Step 4: Manage Data Pools and SIM Data Pool Service Packages 579
6.6 Hik-Connect for Teams Services: Provide VSaaS Solution for Enterprise Customers 581
6.6.1 Step 1: Create an HCT System (Team Site) and Select Desired Services 584
6.6.2 Step 2: Add Devices to Team Site 587
6.6.3 Step 3: Get HCT Packages 588
6.6.4 Step 4: Activate/Renew HCT Services 589
6.6.5 Step 5: Hand Over a Team Site 589
6.6.6 Step 6: Manage Devices, Services & Users for a Team Site 593
6.6.7 Step 7: Manage HCT Services for All Team Sites 595
6.7 HikCentral ReGuard Service: Security Management Solution for Customers 596
6.7.1 Step 1: Get HikCentral ReGuard Services 598
6.7.2 Step 2: Generate HikCentral ReGuard Key for HCRG Activation 599
6.7.3 (Optional) Step 3: Receive and Handle Work Orders 599
6.7.4 Step 4: Manage HikCentral ReGuard Services 600
Chapter 7 Get Support & Incentives to Stay Connected with Hikvision 602
7.1 How to Submit Online Support Cases to Get Help from Hikvision 603
7.1.1 Submit and Track Online Support Cases 606
7.2 How to Return Defected Products for Exchange or Repair (RMA) 612
7.2.1 Submit RMA Requests 613
7.2.2 Track RMA Requests 615
7.2.3 Find Repair Stations 616
7.3 How to Join Partner Programs 617
7.3.1 Resellers (DPPs) Submit Program Applications 618

7.3.2 Resellers (DPPs) Manage Certificates 623
7.3.3 Resellers (DPPs) Manage Programs 624
7.3.4 Distributors Manage Agreements 626
7.4 How to Earn Commissions as a Distributor/Reseller 626
7.4.1 The Process of Earning Commissions 627
7.4.2 The Way to Calculate Commission Amount 628
7.4.3 View Commission Details Using the Portal 629
7.5 How to Apply for Compensation and Manage Applications 629
7.5.1 Apply for Compensation Using the Portal 630
7.5.2 Manage Submitted Compensation Applications Using the Portal 632
7.6 How to Earn Reward Points and Redeem for Gifts 633
7.6.1 Earn Reward Points and Redeem for Gifts Using the Portal 633
7.6.2 Earn Reward Points and Redeem for Gifts Using the Mobile Client 634
7.7 How to Claim and Verify eCoupons 635
7.7.1 Step 1: Buyers Claim eCoupons Using the Mobile Client 636
7.7.2 Step 2: Providers Verify eCoupons Using the Mobile Client 638
7.8 How to Join Sell-Out Promotions 639
7.8.1 Step 1: Buyers Submit and Modify Intentions 640
7.8.2 Step 2: Providers Confirm Intentions from Buyers 650

Chapter 1 Hik-Partner Pro

Hik-Partner Pro is a one-stop security service platform where Hikvision partners can get easy access to all Hikvision product information (including HiLook series), promotions, and marketing handouts. You can enjoy efficient customer and device management and extended value-added services with round-the-clock convenience.

Security system setups are much easier with our app

http://enpinfodata.hikvision.com/analysisQR/showQR/57ca4b01.html

Quick Links

Learn	• ***Entities in Hik-Partner Pro*** • ***Typical Applications of Devices*** • ***Typical Scenarios of Handover*** • ***Datasheet***
Quick Start Guide	• ***Use the SADP Tool to Quick Initialize LAN Devices***

1.1 Entities in Hik-Partner Pro

Here we introduce the entities (any physical or conceptual object) involved in Hik-Partner Pro.

Identity Related Entities

Service Provider

Those who provide services such as the design of security solutions, system/device installation, after-sales, and (or) device maintenance. There are several service provider types and the detailed descriptions are as follows.

Installer

Provides device installation and maintenance services for customers.

System Integrator

Integrates multiple systems to provide solutions for customers.

Distributor

Trades with Hikvision and supplies Hikvision devices to other businesses that sell to customers.

Reseller

Bulk purchases Hikvision devices from distributors and then sells the devices to installers.

Alarm Receiving Center (ARC)

Provides the alarm receiving and handling service for customers.

Note

If you are to apply for joining Hik-Partner Pro as ARC, selecting **Alarm Receiving Center** as the type of service provider is recommended when registering.

OEM

OEM partners source products, parts or services from Hikvision and relabeling, rebranding or embedding them as a part to another product or system.

Installation Service Partner (ISP) / Maintenance Service Partner (MSP)

The ISP/MSP is a special type of security service providers. They offer technical support to installers/ARCs who lack technical capabilities and skills. Usually, ISPs collaborate with these ARCs to provide device installation services for end users, and MSPs collaborate with these installers to provide device management/maintenance services for end users. On Hik-Partner Pro, such installers and ARCs can invite ISPs/MSPs to collaborate with them on customer sites. For details, see .

Note

The MSP/ISP can select any of the service provider types when they are registering a Hik-Partner Pro account.

Remote Monitoring Center (RMC)

Provides the alarm receiving and handling services remotely based on the video monitoring via HikCentral ReGuard.

Note

The RMC can select any of the service provider types when they registering an account for logging in to Hik-Partner Pro.

End User

Those who have purchased or rented Hikvision devices (e.g., network cameras, DVRs, alarm devices, video intercom devices, and access control devices) and want to manage the devices via an easy-to-use mobile client. End users are customers of the service provider, and they use Hik-Connect to manage devices.

Site Related Entities

Site

A site represents a physical location where device(s) are installed and through which the Installer / Installer Admin can manage and configure the devices and services for customers.

Personal Site

For individual users and applicable to households and independent stores. It provides services like remote live view, playback, arming/disarming, and alarm receiving on the Hik-Connect Mobile Client. No more than 128 channels can be added to a personal site.

Team Site

For enterprise users and applicable to chain stores, offices, communities, and other scenes where multi-user management is required. It provides services like person and permission management, video security, access contorl, attendance check, and device maintenance on both Hik-Connect for Teams Portal and Mobile Client.

Site Manager

When a site is assigned to an Installer, the Installer becomes the site manager of the site, and can manage and configure the devices and services of the site.

Site Owner

When an installer transfers ownership of a site to an end user, the end user becomes the site owner who is the holder of the site. The installer can also apply for site authorization from the site owner to manage the site.

1.2 Running Environment

The followings are the recommended systems for running the Portal and Mobile Client.

1.2.1 Running Environment for Portal

Operating System

Microsoft Windows® 7/8.1/10 (32-bit and 64-bit).

CPU

Intel® Core™ i5-4460 CPU @3.20GHz 3.20GHz and above.

RAM

8 GB and above (4 GB at least).

Graphics Card

NVIDIA® GeForce GT 730

Web Browser

Versions of Firefox (32-bit and 64-bit), Chrome (32-bit and 64-bit), and Edge (32-bit and 64-bit) released in the latest half year.

1.2.2 Running Environment for Mobile Client

System Requirement

For iOS: iOS 12 or later versions.
For Android: Android 6.0 or later versions.

Memory

For iOS: 1 GB or above.
For Android: 2 GB or above.

1.3 Function Availability for Different Regions

Hik-Partner Pro offers both free functions and value-added functions that cost certain fees. You can purchase certain services in the Service Market of Hik-Partner Pro to get access to the value-added functions. Currently, certain value-added functions are only available in certain countries and regions. And users in some countries and regions can only access the free functions.

Note

This document contains introductions of all Hik-Partner Pro functions, therefore some functions illustrated in this document may Not be supported in your country or region. And contents in some figures in this document may be different from the actual interface, if so, the latter shall prevail.

1.3.1 Functions Only Available in Certain Regions

The following table shows the functions only available in certain countries and regions.

Note

For details about whether your country or region supports the functions contained in the services listed below, refer to the after sales or local distributor.

Service	Function(s) Only Available in Certain Countries and Regions
Health Monitoring Service	Only linkage rule. **Note** Linkage rule is unavailable in the United States and Canada.
Cloud Storage Service	All functions contained in the service.
Cloud Attendance Service	All functions contained in the service.
SIM Data Service	All functions contained in the service.

Service	Function(s) Only Available in Certain Countries and Regions
Alarm Receiving Center (ARC) Service	All functions contained in the service.
Employee Account Add-On	All functions contained in the service.
Hik-Connect for Teams Service	All functions contained in the services.
HikCentral ReGuard Service	All functions contained in the services.

1.3.2 Regions Only with Support for Free Functions

The following two tables shows the free functions and the countries and regions only with support for the free functions.

Table 1-1 Free Functions

Module	Function(s)
Account Management	• Register Installer Admin Account • Manage Company and Account Information
Site Management	• Add Personal and Team Sites • Hand Over Sites • Apply for Site Authorization from Site Owner • Site Collaboration with Installation/Maintenance Partners
Device Management	• Add Device • Apply for and Release Device Permissions • Sync Devices from Hik-Connect Account • Enable Devices to Send Notifications • Upgrade Devices • Configure DDNS for Devices • Manage Security Control Panel • Remote Configuration • Reset Device Password Unbind Device from Its Current Account
Video	• View Live Video • Play Back Video Footage
Log	Search Operation Logs
Tool	Tools for Providing Installation, Maintenance, and Other Services
Solution	View and Search for Solutions, and Add to Favorites

Module	Function(s)
Explore	• View, Search, Like, Share, and Comment on Feeds, and Add to Favorites • View, Search, Like, Share, and Comment on How To, and Add to Favorites • View, Search, Like, Share, and Comment on Videos, and Add to Favorites • Receive and View Notices • Register for and Participate in Events
Project	Create and Manage Projects
Order & Promotion	• View Product Information and Select Products • Place and Manage Product Orders
Incentive	• Rewards Store • Partner Program • Compensation
Support	• Tools • Tutorial Center • Chatbot • Online Support Case • Suggestions • Serial Number Inquiry • Contact Us • Return Products for Exchange or Repair via RMA (Return Materials Authorization)
Distributor Business	Earn Commissions and View Commission Details

Table 1-2 Countries and Regions Only With Support for Free Functions

Continent	Country/Region
Africa	Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo(Brazzaville), Congo(Kinshasa), Cote D'Ivoire, Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Guinea, Guinea-Bissau, Liberia, Madagascar, Malawi, Mali, Mayotte, Mozambique, Namibia, Niger, Nigeria, Rwanda, Senegal, Seychelles, Sierra Leone, Somalia, Tanzania, Togo, Uganda, Zambia, Zimbabwe
Asia	Japan, Taiwan (China)

1.4 Partner Quick Start Guide

This quick start guide helps partners get started with Hik-Partner Pro. The guide helps with:

- Setting up partner accounts (Installer Admin accounts and employee accounts).
- Getting product info & trends.
- Adding and handing over devices.
- Providing value added services.

1.4.1 Step 1: Register Accounts

Your company should first register an Installer Admin account before you can access any features of Hik-Partner Pro. Then, the employees can be invited to register Installer accounts, or they can self-register Installer accounts and apply to join an existing company on registration.

Table 1-3 Account Types

Account Type	Description
Installer Admin	Full access to the features in the system. Usually, the Installer Admin account is owned by the manager of a company.
Installer	"Sub-accounts" to the Installer Admin and controlled via roles and permissions for what they can do. Usually, the Installer accounts are owned by the employees of a company.

Register an Installer Admin Account Using the Portal

Visit ***https://www.hik-partner.com*** , click **Register**, select your company type (installer, system integrator, distributor, reseller, alarm receiving center, or OEM), and enter the required information to register.
You can authenticate your company during the registration, or later. After you successfully register the Installer Admin account, you can start adding employees to your company, refer to ***Add Employees to Your Company and Remove Account Limit with Add-On*** .

Register an Installer Admin Account Using the Mobile Client

Install and launch the Hik-Partner Pro Mobile Client on your mobile device, select your country/region, tap **Register**, select your company type (installer, system integrator, distributor, reseller, alarm receiving center, or OEM), and enter the required information to register.
If you already have a Hik-Connect account, you can also tap **Hik-Connect**to register using the Hik-Connect account.

You can authenticate your company during the registration, or later. After you successfully register the Installer Admin account, you can start adding employees to your company, refer to ***Add Employees to Your Company and Remove Account Limit with Add-On*** .

Figure 1-1 QR Code for App Download

1.4.2 Step 2: Authenticate Company to Use More Features

Authenticate your company to use more features and value-added services on Hik-Partner Pro.

You need to fill in all the required fields and submit the online application to authenticate your company. After your application is approved, you will be notified via push notification and email.

Authenticate Your Company Using the Portal

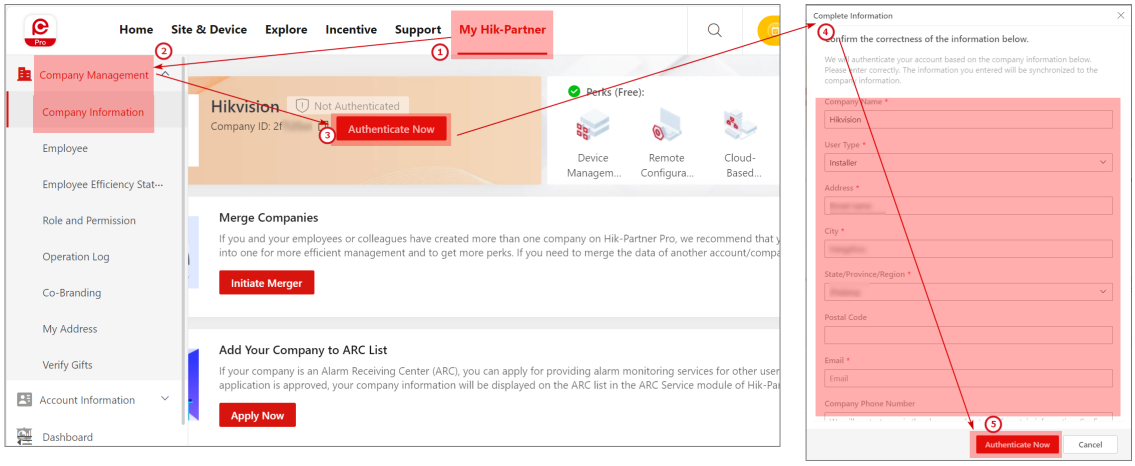


Figure 1-2 Authenticate Your Company Using the Portal

Authenticate Your Company Using the Mobile Client

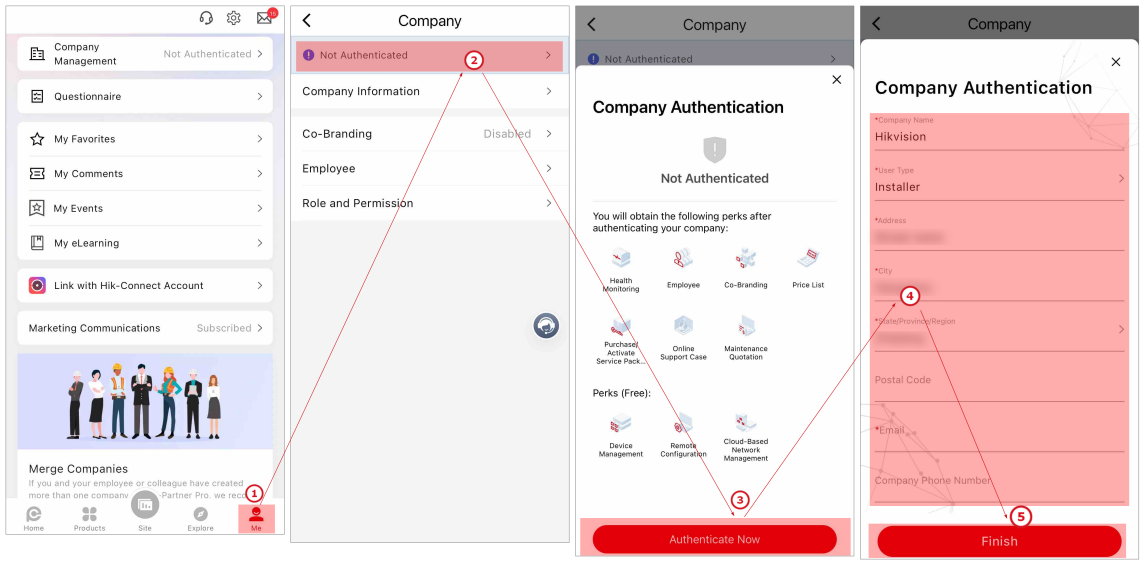


Figure 1-3 Authenticate Your Company Using the Mobile Client

1.4.3 Step 3: Access Products Info & Trends

For partners, Hik-Partner Pro offers full product information and latest product trends.

Access Products Info & Trends Using the Portal

Log in to the Portal and click **Explore**, you can access feeds, events, TechZone, and videos about products. For authenticated channel partners, they can also access the page for orders & promotions using the Portal.

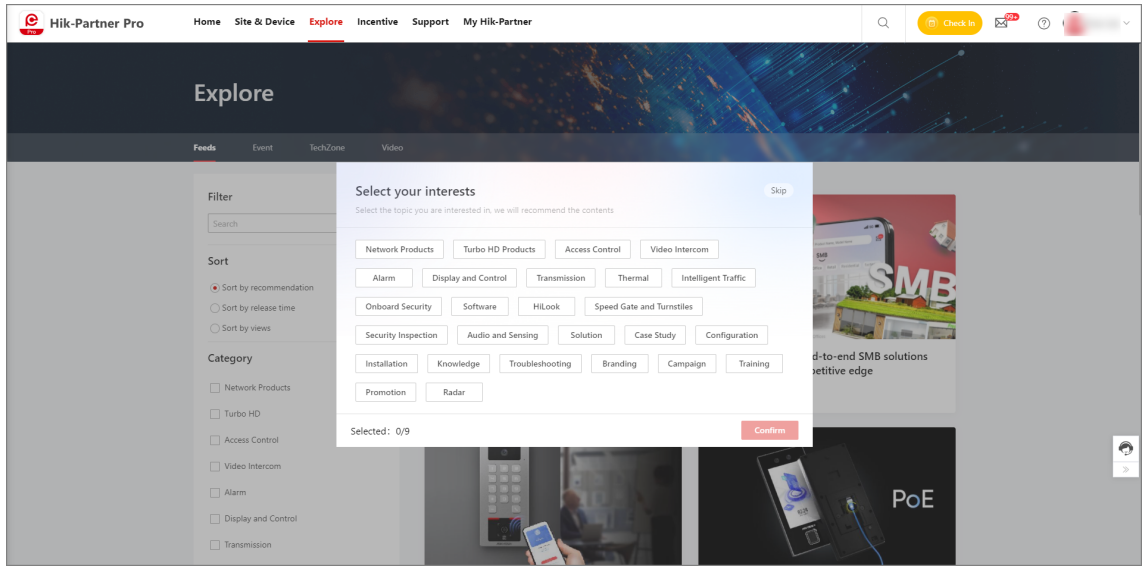
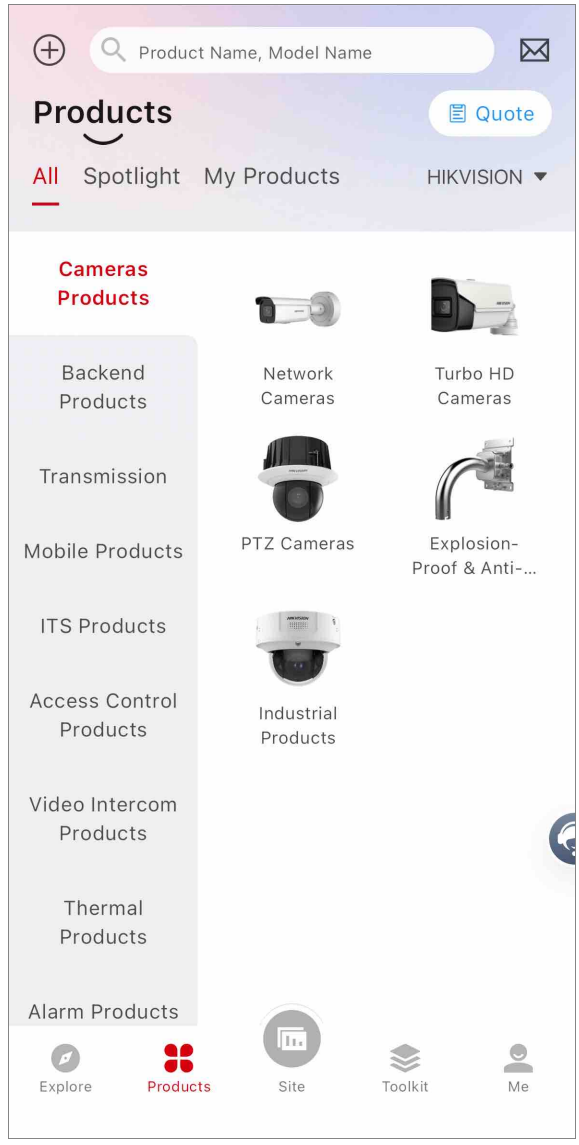
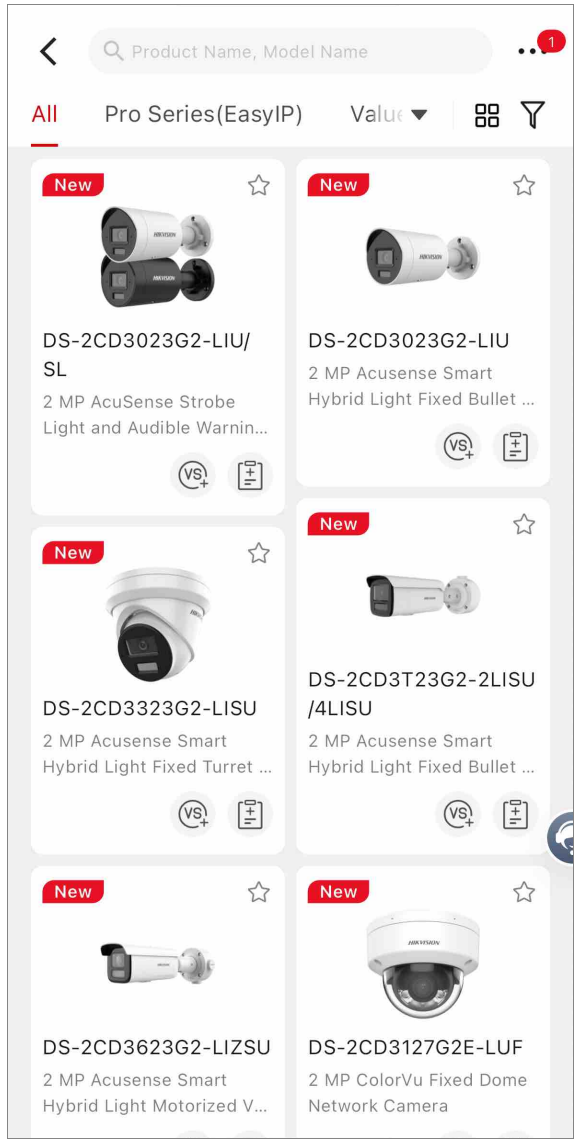


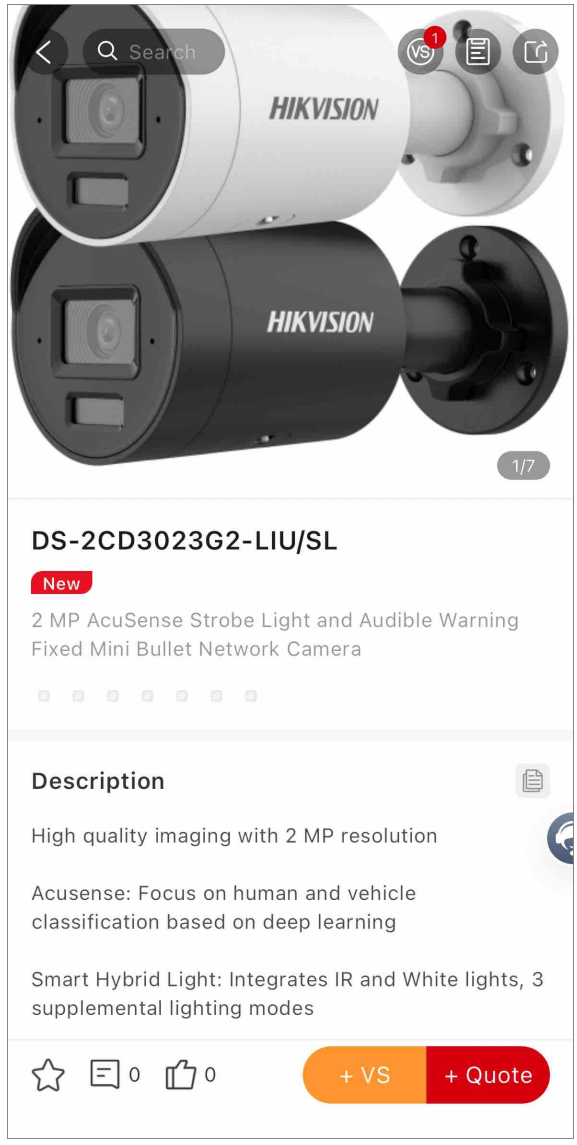
Figure 1-4 Explore on the Portal

Access Products Info & Trends Using the Mobile Client

Log in to the Mobile Client, tap **Explore**, you can access feeds, videos, and TechZone about products. On the Mobile Client, you can find all Hikvision products, and access their parameters and download product documents.


Product Name, Model Name
Products
Quote
All
Spotlight
My Products
HIKVISION
Cameras Products
Backend Products
Transmission
Mobile Products
ITS Products
Access Control Products
Video Intercom Products
Thermal Products
Alarm Products
Network Cameras
Turbo HD Cameras
PTZ Cameras
Explosion-Proof & Anti-...
Industrial Products
Explore
Products
Site
Toolkit
Me


Product Name, Model Name
All
Pro Series(EasyIP)
New
DS-2CD3023G2-LIU/SL
2 MP AcuSense Strobe Light and Audible Warnin...
New
DS-2CD3023G2-LIU
2 MP Acusense Smart Hybrid Light Fixed Bullet ...
New
DS-2CD3323G2-LISU
2 MP Acusense Smart Hybrid Light Fixed Turret ...
New
DS-2CD3T23G2-2LISU/4LISU
2 MP Acusense Smart Hybrid Light Fixed Bullet ...
New
DS-2CD3623G2-LIZSU
2 MP Acusense Smart Hybrid Light Motorized V...
New
DS-2CD3127G2E-LUF
2 MP ColorVu Fixed Dome Network Camera


Search
HIKVISION
HIKVISION
1/7
DS-2CD3023G2-LIU/SL
New
2 MP AcuSense Strobe Light and Audible Warning Fixed Mini Bullet Network Camera
Description
High quality imaging with 2 MP resolution
Acusense: Focus on human and vehicle classification based on deep learning
Smart Hybrid Light: Integrates IR and White lights, 3 supplemental lighting modes
0
0
+ VS
+ Quote

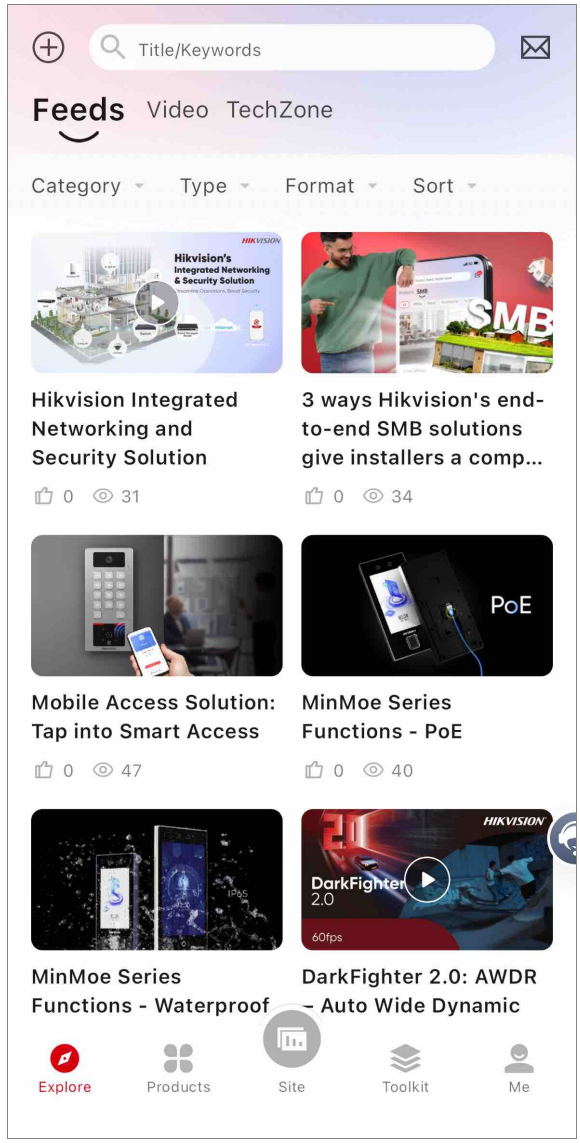


Figure 1-5 Products and Explore on the Mobile Client

1.4.4 Step 4: Add, Hand Over, and Maintain Devices

Hik-Partner Pro offers powerful installation and configuration tool, customer site management tool, and remote maintenance tool.

Access Site & Device Using the Portal

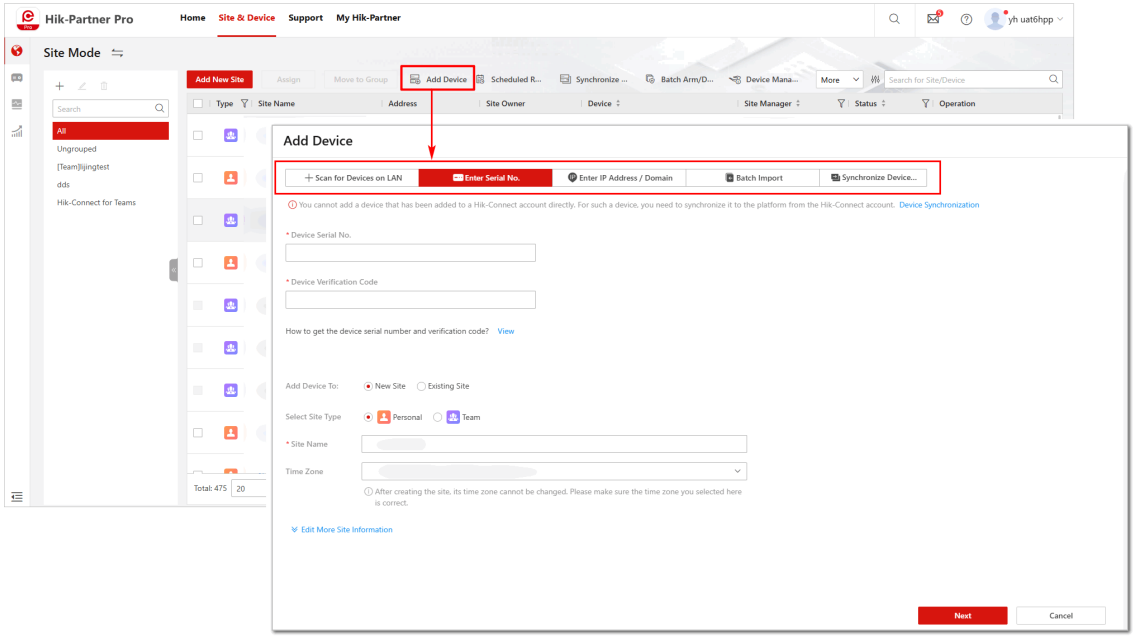


Figure 1-6 Access Site & Device Using the Portal

Access Site & Device Using the Mobile Client

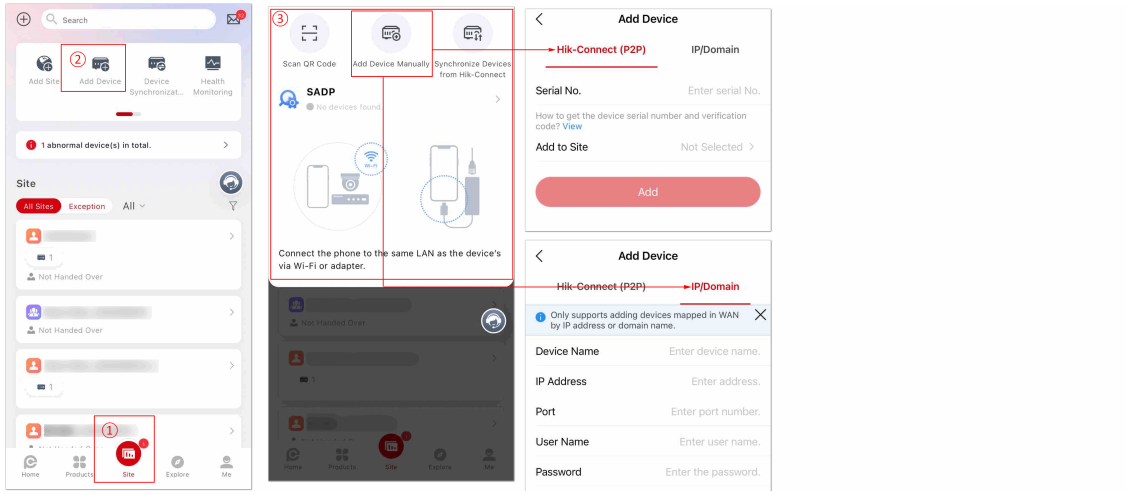


Figure 1-7 Access Site & Device Using the Mobile Client

1.4.5 Step 5: Provide Your Customer with More Value-Added Services

Explore value-added services that you can provide for your customers.

Refer to ***Provide Value-Added Services: Expand Your Business*** to find out more.

Access Service Market Using the Portal

Go to **Site & Device → Service Market** .

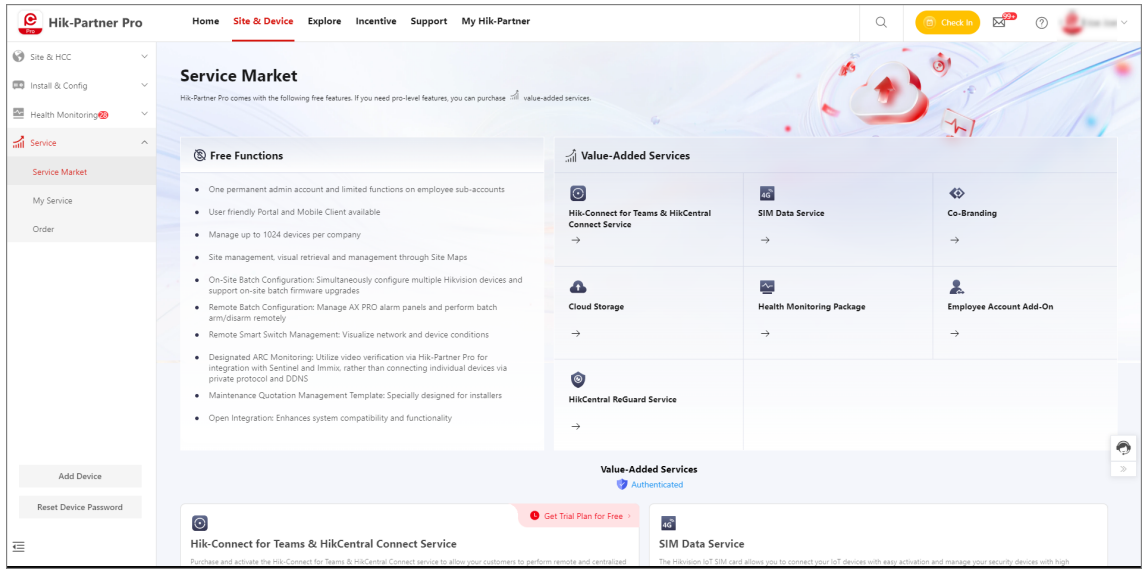
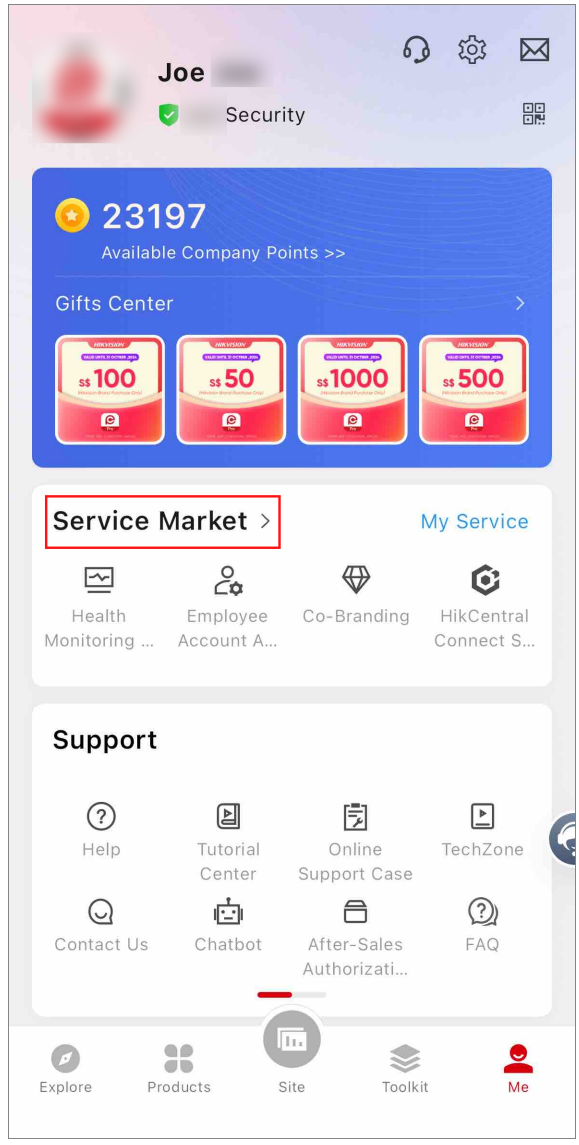


Figure 1-8 Service Market on the Portal

Access Service Market Using the Mobile Client

Go to **Me → Service Market** .


Joe
Security
23197
Available Company Points >>
Gifts Center
Service Market
My Service
Health Monitoring ...
Employee Account A...
Co-Branding
HikCentral Connect S...
Support
Help
Tutorial Center
Online Support Case
TechZone
Contact Us
Chatbot
After-Sales Authorizati...
FAQ
Explore
Products
Site
Toolkit
Me

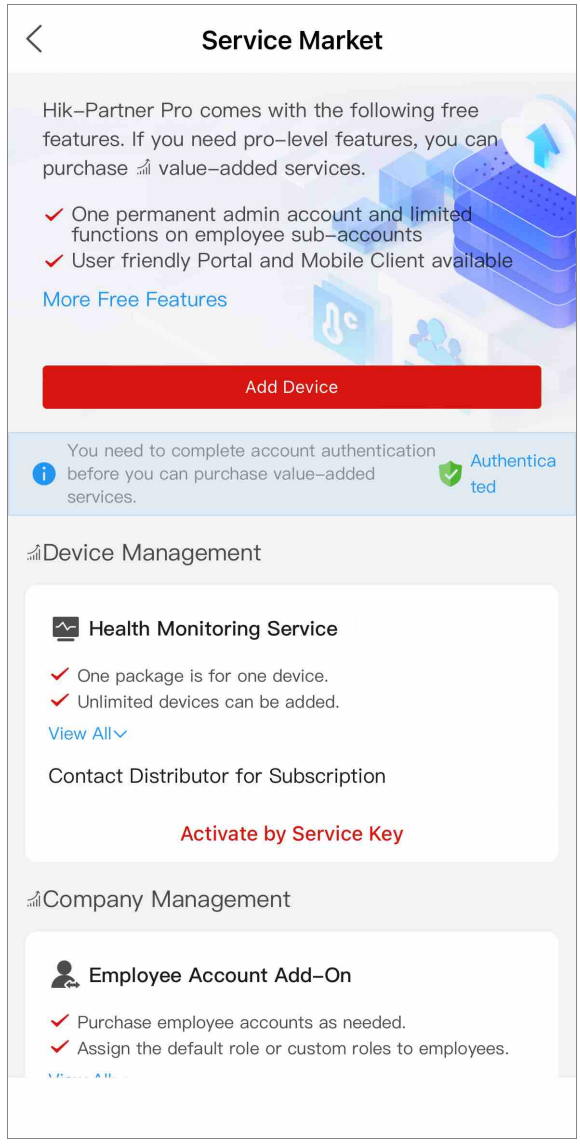


Figure 1-9 Service Market on the Mobile Client

Chapter 2 Start Security Business from Presales Stage

Hik-Partner Pro offers abundant products and presales features to help partners start security businesses.

Steps	Instructions
1. View Product Info and Select Products	***How to Compare and Select Products***
2. Design Project for Quotation	***HPP Designer: How to Design Your Security and Network Project for Quotation***
3. Create Product Quotations Directly Without Design	***How to Create Product Quotations***
4. Create Projects	***How to Create and Manage Project***
5. Place Orders	***How to Place Orders for Products***

2.1 How to Compare and Select Products

2.1.1 Compare and Select Products Using the Portal

The Order & Promotion module supports viewing information of regular products, hot products, and promotional products that are discounted or are put on clearance. You can search for and select products to place an order or submit your product order by uploading a predefined template.

Note

The module is only available to authenticated channel partners.

View and Search for Products Using the Portal

Under the B2B tab of the Order & Promotion module, you can view information of hot products and the products you have recently viewed. You can also view information of the regular products or promotional products (e.g., discount products, clearance products, etc.) by selecting the corresponding tabs under the navigation bar. You can filter the products by product category and search for specific products by product name or model.

Click a product to view its detailed information, including the product picture, description, stock availability, and other related parameters. If needed, you can add a product to Favorites by hovering over it and clicking ★ .

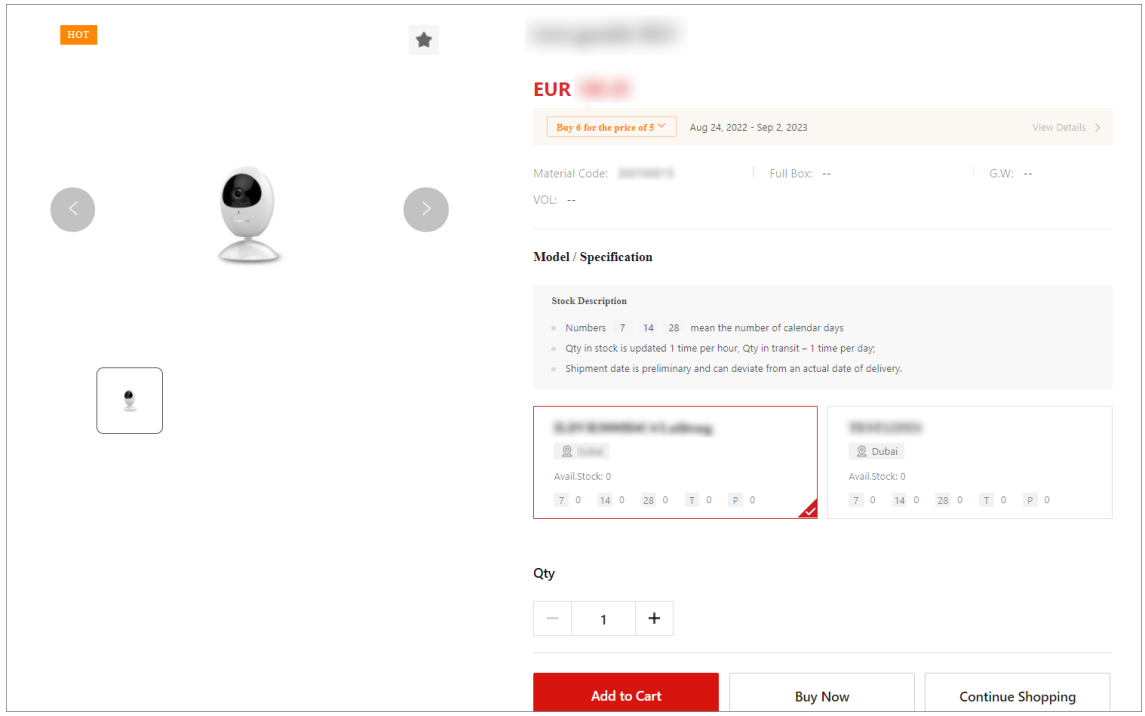


Figure 2-1 Product Information Details

Note

You can find the products you have added to Favorites later in **My Hik-Partner → Account Information → My Favorite → B2B Product** .

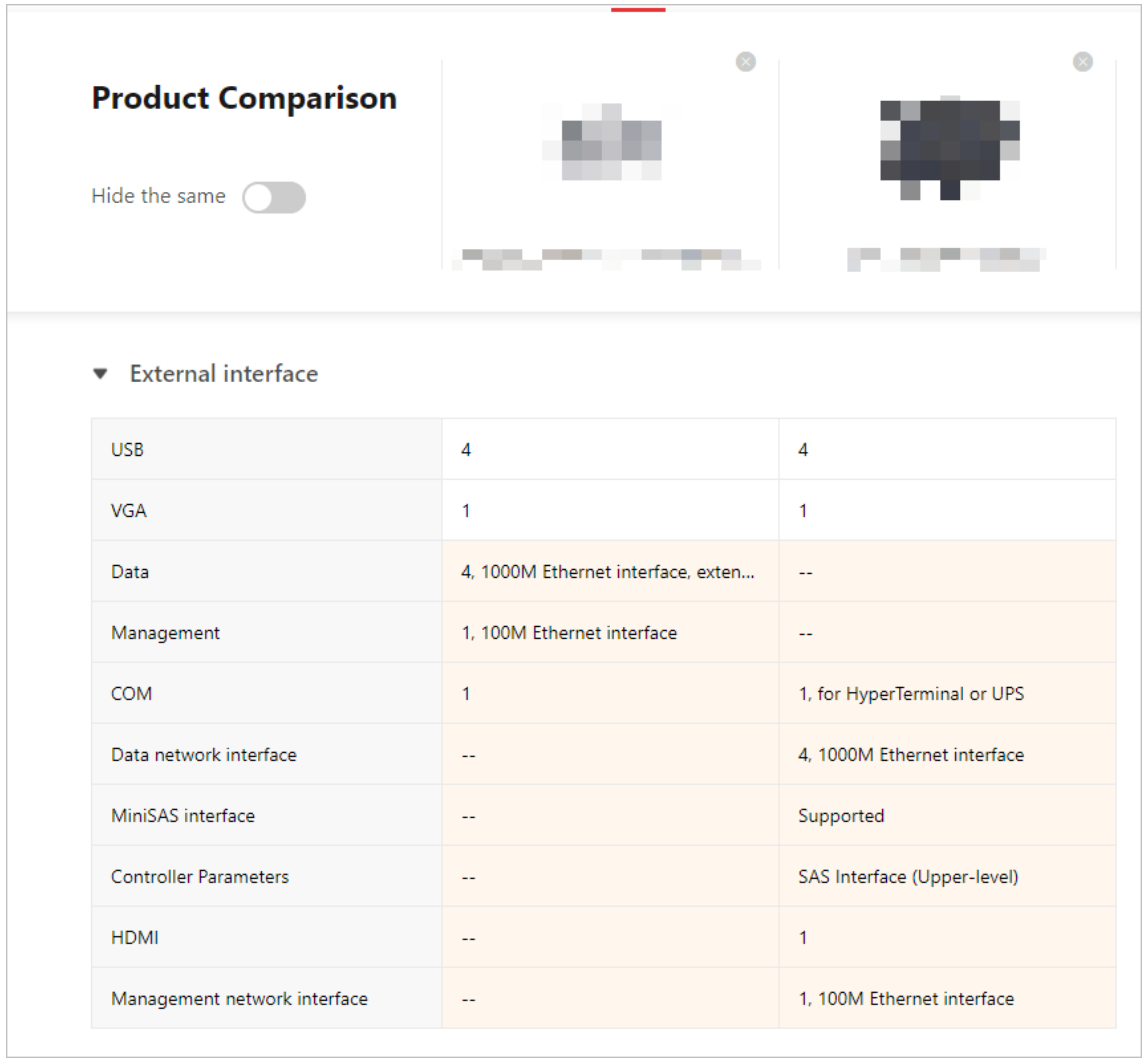
Compare Products Using the Portal

When you select products, you can add multiple products and compare them with their same specifications hidden. In this way, different specifications will be directly displayed and you can choose products as needed.

Note

Only products of the same category and subcategory can be compared.

Click **Project → New Project** , and in the Product Selection part, click VS to start compare products. You can also click VS at the right bottom, and add products to compare them.
To start to compare products, select at least two but no more than four products from the comparison list. On the comparison result page, fields that are different are highlighted with a background color. You can switch on **Hide the Same** on the top left to hide parts that are the same and focus only on the differences.



USB	4	4
VGA	1	1
Data	4, 1000M Ethernet interface, exten...	--
Management	1, 100M Ethernet interface	--
COM	1	1, for HyperTerminal or UPS
Data network interface	--	4, 1000M Ethernet interface
MiniSAS interface	--	Supported
Controller Parameters	--	SAS Interface (Upper-level)
HDMI	--	1
Management network interface	--	1, 100M Ethernet interface

Figure 2-2 Compare Products

2.1.2 Compare and Select Products Using the Mobile Client

The Products module supports viewing information of hot products or a certain type of products. You can search for or filter the products, download the related documents, and share the product information with others. The module also supports comparing the parameters/specifications of products to learn about their similarities and differences.

Note

The Products module is not supported in some countries/regions.

View and Search Products Using the Mobile Client

You can search for products and view detailed product information, including the product picture, description, parameters, and related documents.

You can view a list of hot products on the home page under the tab **Products**, or view the products by product category in the Products module. You can search for a specific product by product name or model, or filter the products by brand, product category, type, series, and the relevant parameters. For a specific type of products, you can switch between gallery view and list view for different product display modes.

Tap on a product to view detailed information about the product, including the product picture, description, parameters, and related documents. On the product details page, you can also leave comments for the product, add it to Favorites, give it a thumbs up, download the related documents, or share the product information with others.

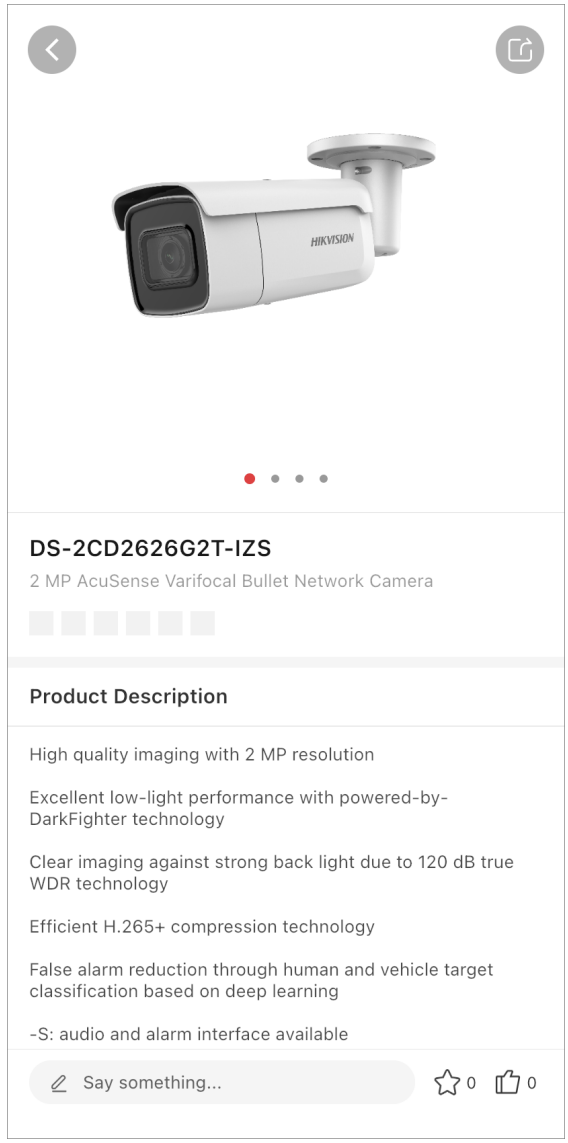


Figure 2-3 Product Details Page

Note

You can find the products you have added to Favorites later in **Me → My Favorites → Products** , and the comments you have left for the products in **Me → My Comments → Products** .

Compare Products Using the Mobile Client

You can compare the parameters/specifications of products to learn about their similarities and differences.

On the product display page, you can add a product to the comparison list by tapping **+VS** next to it. You can check the comparison list by tapping VS on the top right with the total number of added products displayed on top.

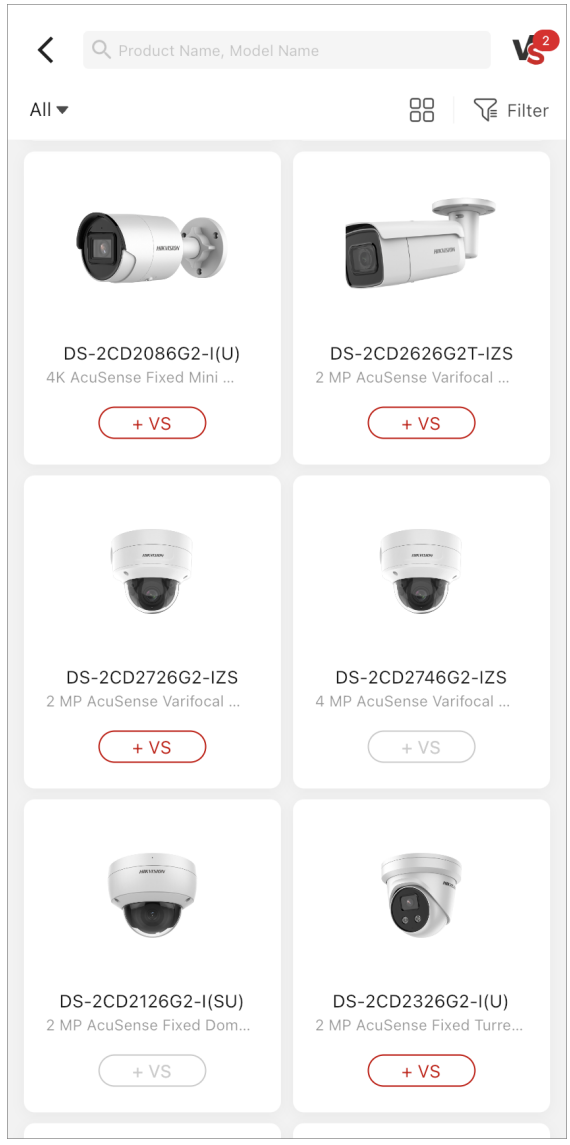


Figure 2-4 Select Products to Compare

To start comparing products, select at least two but no more than four products from the comparison list and tap **Start VS**. On the comparison result page, fields that are different are highlighted with a background color. You can switch on **Hide Same** on the top left to hide parts that are the same and focus only on the differences.

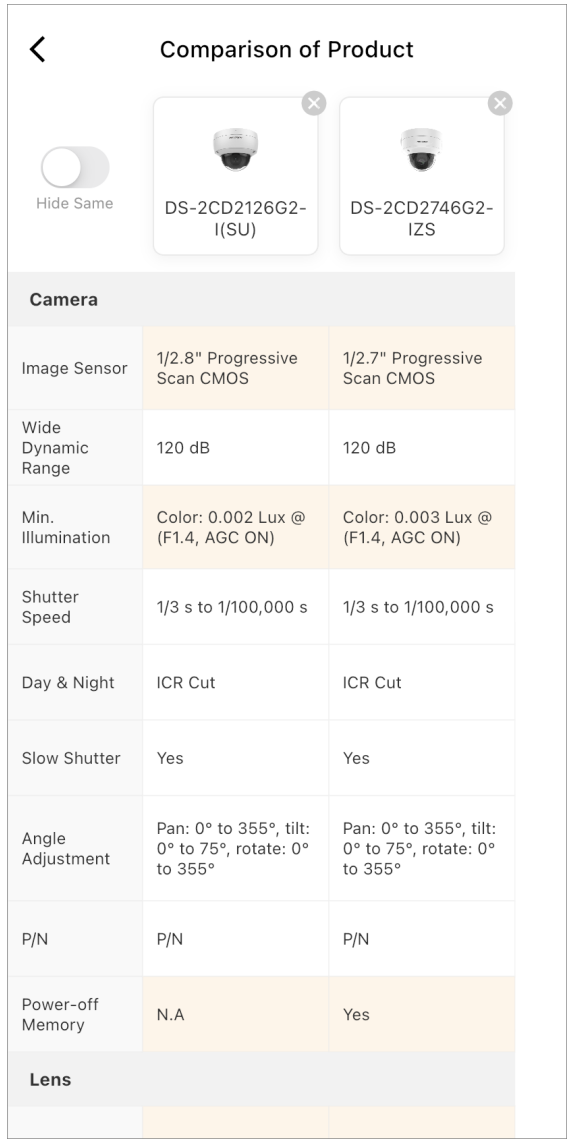


Figure 2-5 Product Comparison

2.2 HPP Designer: How to Design Your Security and Network Project for Quotation

2.2.1 Overview

HPP Designer is the online project design and quotation tool inside Hik-Partner Pro. It lets installers and system integrators lay out a security or network project, simulate how the selected devices will

actually perform on site, and turn the finished design into a priced bill of materials — in one continuous workflow, without leaving the browser.

What You Can Design

Table 2-1 What You Can Design

Scenario	Typical Use
CCTV Video Surveillance	Camera placement, field of view, image quality at distance.
Wireless Network Deployment	Indoor Wi-Fi coverage, outdoor point-to-multipoint bridge links.
Intrusion Alarm Systems	Detector and control panel placement, RF coverage across floors.
Perimeter Protection	Thermal cameras and radar on a satellite map.
Project Quotation	Priced device list, storage sizing, exportable quotation and design report.

How the Workflow Is Organized

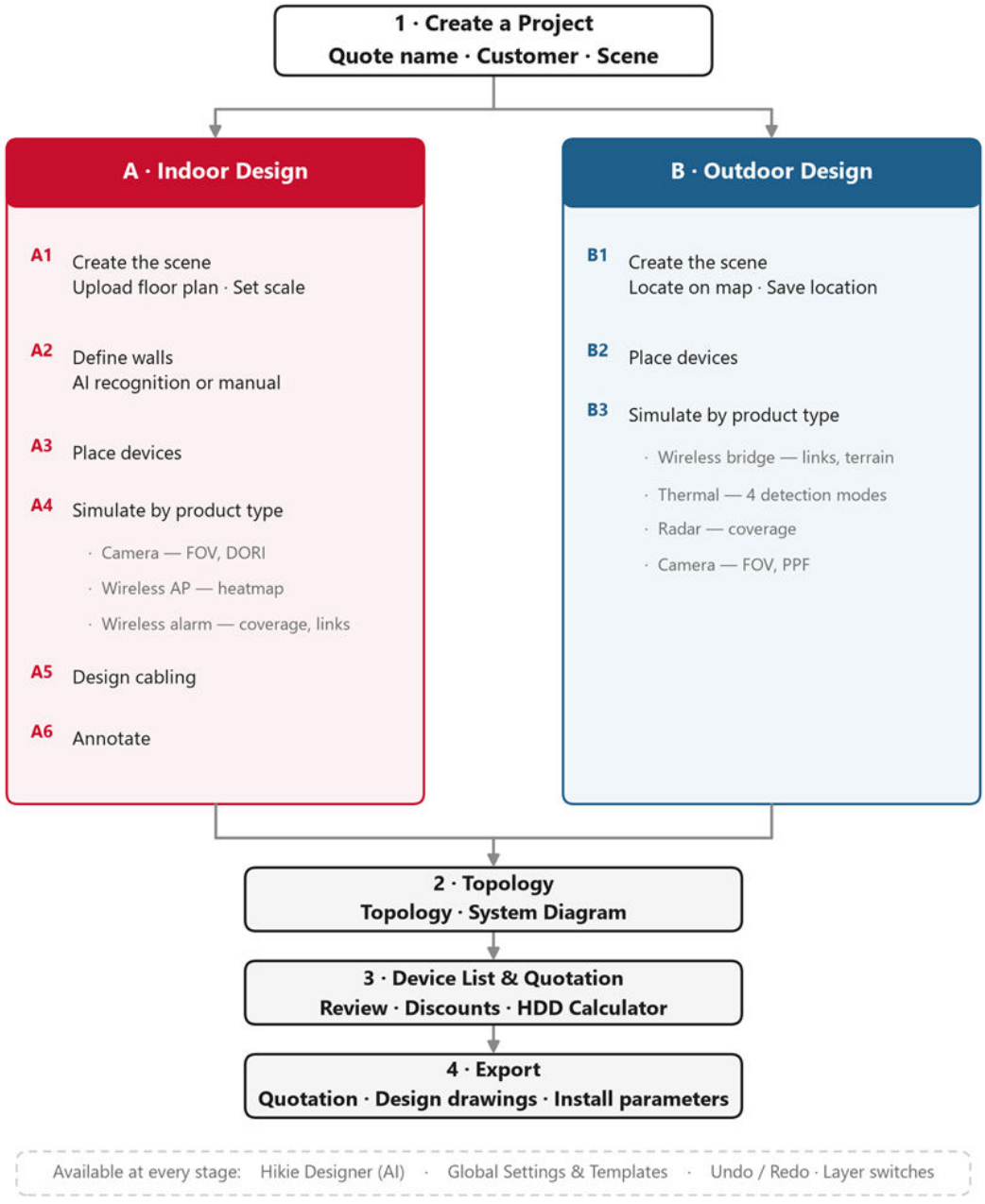


Figure 2-6 HPP Designer Workflow

Stage Reference

Stage	What Happens	See	Key UI entry point
1 · Create a Project	Enter the quote name, customer and scene, then choose the design path.	***Create a Project***	**Create a New Quote**
A1 · Create the scene	Upload a floor plan (or capture a map, or start blank), crop it, set the ceiling height, calibrate the scale.	***Create the Scene***	**Start New Design**
A2 · Define walls	Detect walls with AI or draw them manually; assign a wall class, or a material carrying per-frequency attenuation.	***Define Walls***	**Add Wall**
A3 · Place devices	Drag or continuously place cameras, APs, alarm devices and radar; configure each channel.	***Place Devices***	**Device Deployment**
A4 · Simulate by product type	Camera FOV and DORI, Wi-Fi heatmap, alarm coverage and detector-to-panel links.	***Simulation by Product Type***	Layer switches · **Global Settings**
A5 · Design cabling	Add convergence points and route cables; drawn length × redundancy factor feeds the quotation.	***Design Cabling***	**Cable Routing**
A6 · Annotate	Mark up what the simulation cannot express — equipment room, risers, site constraints.	***Annotate the Design***	**Annotations**
B1 · Create the scene	Search or drag to the site, drop a pin, save it as a scene; add more scenes when sites are spread out.	***Create the Scene***	**Search location** · **Save location**
B2 · Place devices	Place bridges, thermal cameras, radar and cameras on the map.	***Place Devices and Simulation by Product Type***	**Wireless bridge** · **Device Deployment**
B3 · Simulate by product type	Bridge link budget over real terrain, thermal detection modes, radar and camera coverage.	***Place Devices and Simulation by Product Type***	**Auto** / **Manual** · **Add Obstacle**
2 · Topology	Topology and system diagram generated from the design; nodes can be re-arranged and hidden.	***Topology***	**Topology**

Stage	What Happens	See	Key UI entry point
3 · Device List & Quotation	Review by device or by layout, clear the **Undeployed** group, apply discounts, size the storage.	***Device List, Quotation and Export***	**Offer List · HDD Calculator**
4 · Export	Select the content to include, fill in recipient info, download.	***Export Quotation and Design Report***	**Export**

The three capabilities are available at any stage in the workflow: **Hikie Designer** (***Hikie Designer***), **Global Settings and Templates** (***Global Settings and Templates***), and the editing controls.

2.2.2 Before You Start

Open HPP Designer

1. Log in to the Hik-Partner Pro Portal.
2. Enter via one of the following ways:
   - **Select Products Later:** Go to **Products → Quote → Select by Designer** .

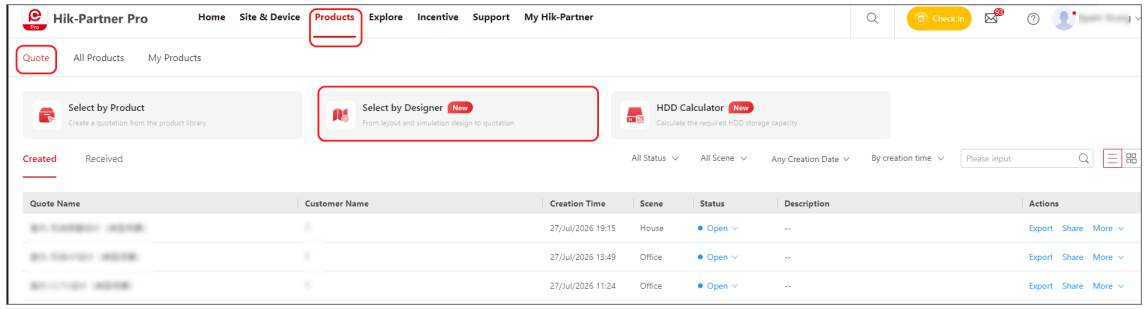


Figure 2-7 Entry 1

   - **Select Products Before Design:** Go to **Products → All Products** , click + to add products to your project, and click **Design to Quote** in the bottom right corner of the page.

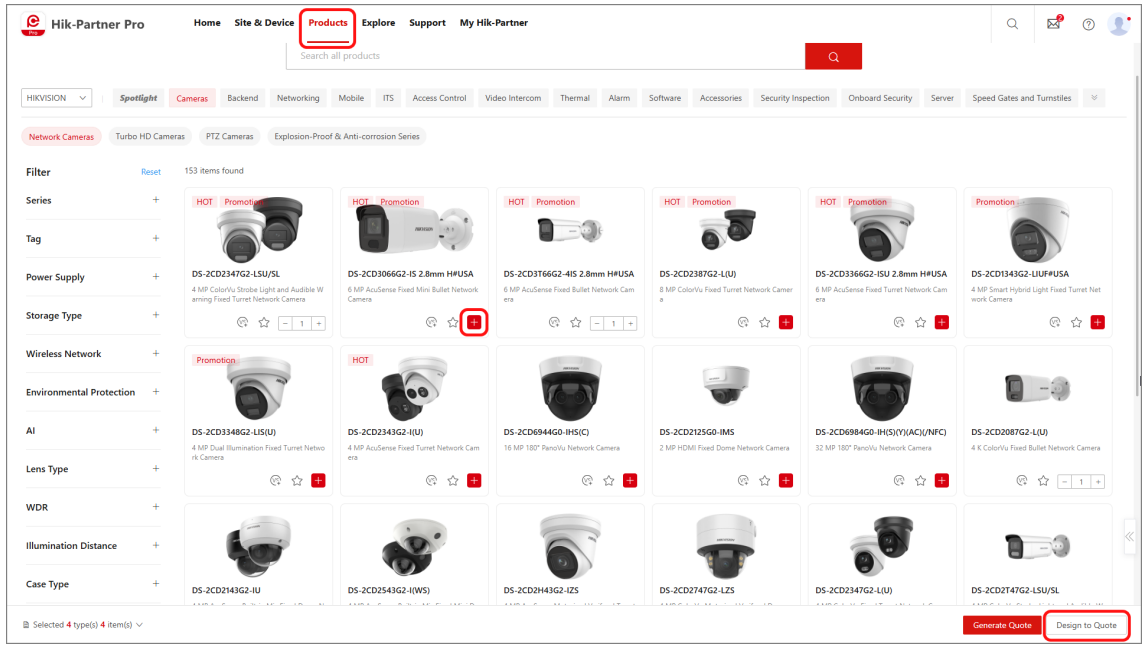


Figure 2-8 Entry 2

- Click **Support → Tools → HPP Designer** . Then, enter the design page via either of the above two ways.

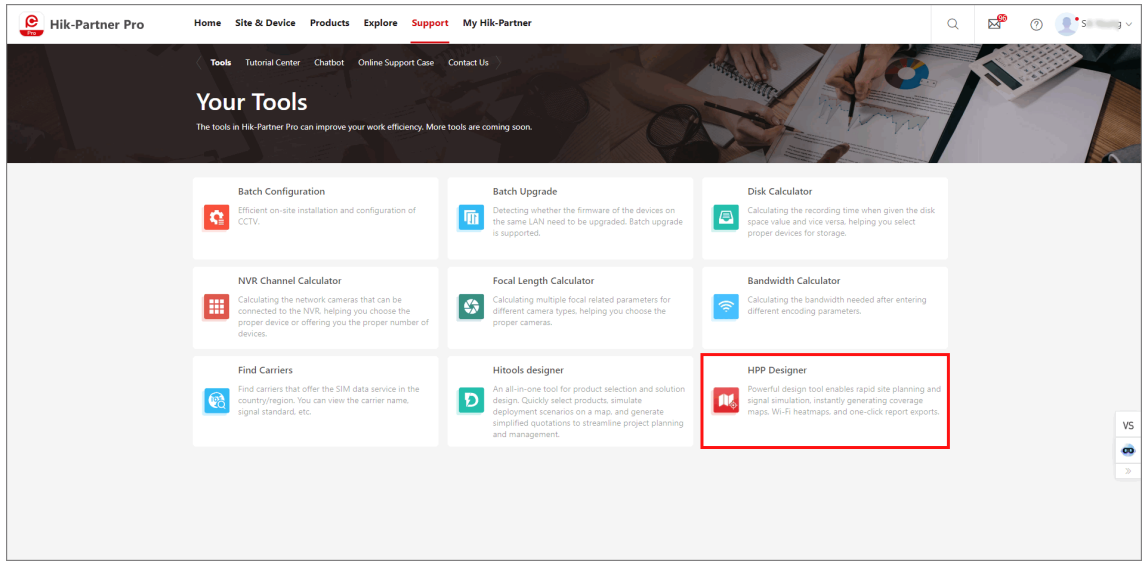


Figure 2-9 HPP Designer

Browser Requirements

- Outdoor Design uses map services and needs an active internet connection.
- When you first open Outdoor Design, the browser asks permission to access your location. Grant it so the map centers on your position. If you deny it, you can still navigate to your site with the search box.
- The map provider and available product catalog vary by region.

2.2.3 Create a Project

1. Click **Select by Designer**.

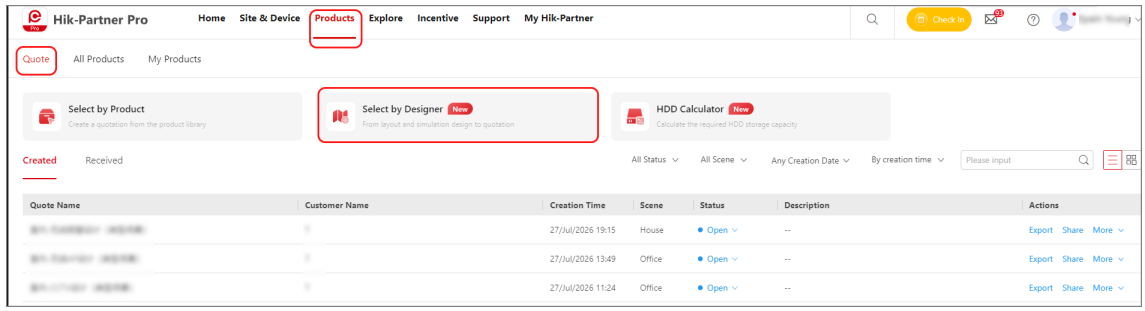


Figure 2-10 Select by Designer

2. Set the quote name, customer name, scene (office, store, house, farm, parking lot, other), and description. Click **Create**.

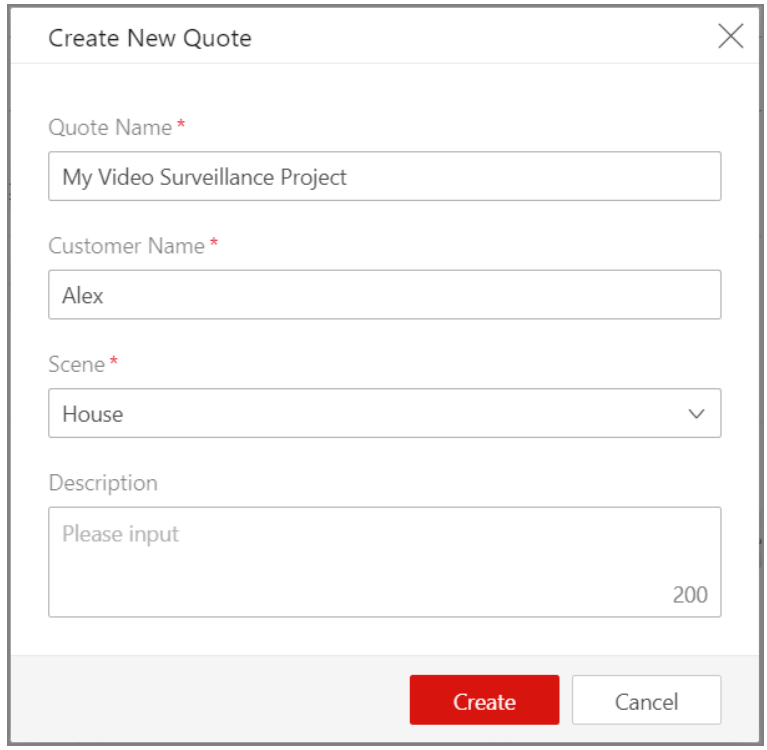


Figure 2-11 Set Quote Info

3. Choose the design path:
   - **Design**: Indoor projects based on a floor plan. Continue with ***Part A: Indoor Design*** .
   - **Outdoor Design**: Outdoor projects based on a satellite or road map. Continue with ***Part B: Outdoor Design*** .

2.2.4 Part A: Indoor Design

Create the Scene

A scene is one floor plan with a known scale. A project can hold as many scenes as the building has floors or zones.

1. On the design page, choose a background source.

Note

Taking **Upload Floor Plan** as the example in this article.

Source	What It Does	Constraints
Upload Floor Plan	Uses your existing drawing.	JPG, PNG, BMP, PDF, CAD (.dwg); **max 15 MB per file**.
Select a Map	Captures an image of the target address from a satellite map.	Requires internet access.
Empty Background	Starts from a blank canvas of a defined size and color.	Use when no drawing exists.

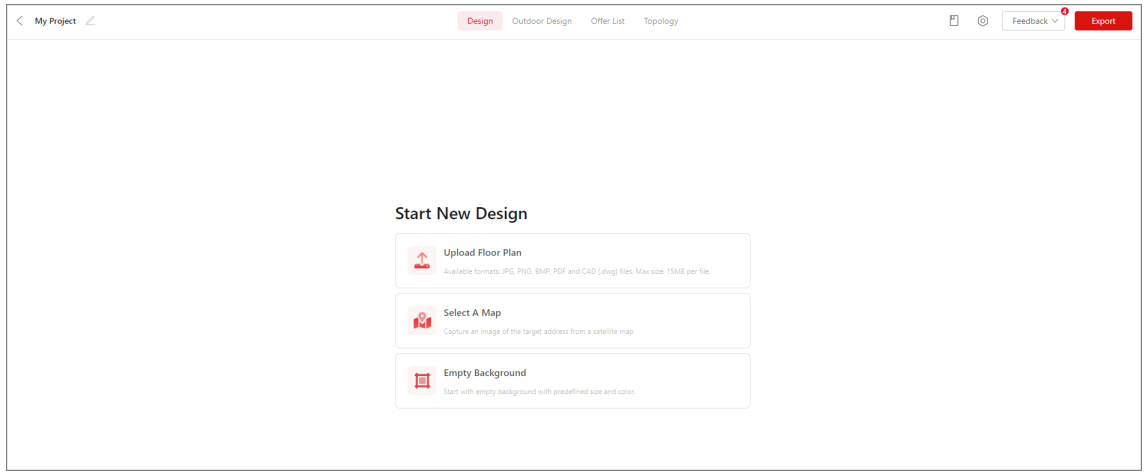


Figure 2-12 Design

2. Drag your file to the upload window or click to upload.

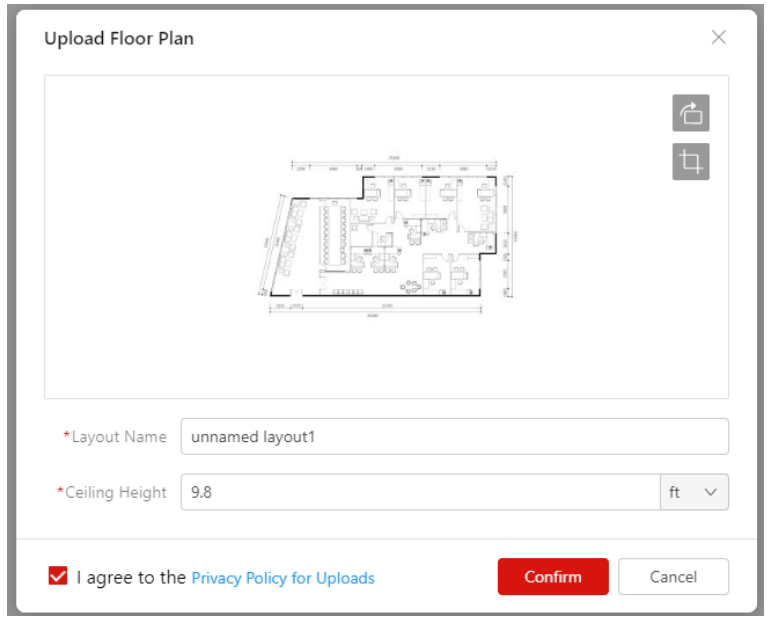


Figure 2-13 Upload Floor Plan

3. Crop and rotate the image using the controls above the preview, then complete the required fields:

Table 2-2 Adjust Image

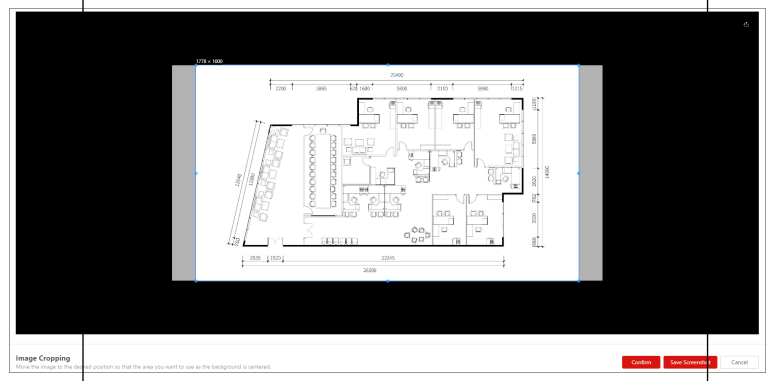
Operation	Description
Crop	Click to crop and adjust the image according to your needs. Then, click **Confirm** or **Save Screenshot**.  **Figure 2-14 Crop Image**
Rotate	Click to rotate the image if needed.

Table 2-3 Required Fields

Parameter	Description
Layout Name	Used throughout the device list and the exported report.
Ceiling Height	Used by the CCTV, wireless and alarm simulations.

4. Accept the **Privacy Policy for Uploads** and click **Confirm**.
5. Set the scale so the tool can convert pixels to real distances: Click twice to draw a blue line to mark a wall on the layout, enter the wall's real length. The active layout thumbnail then shows the resulting scale, for example, 9.8 ft |1 ft : 9.03 px.

Note

You can enable **AI Wall Recognition** to auto detect and mark the walls.

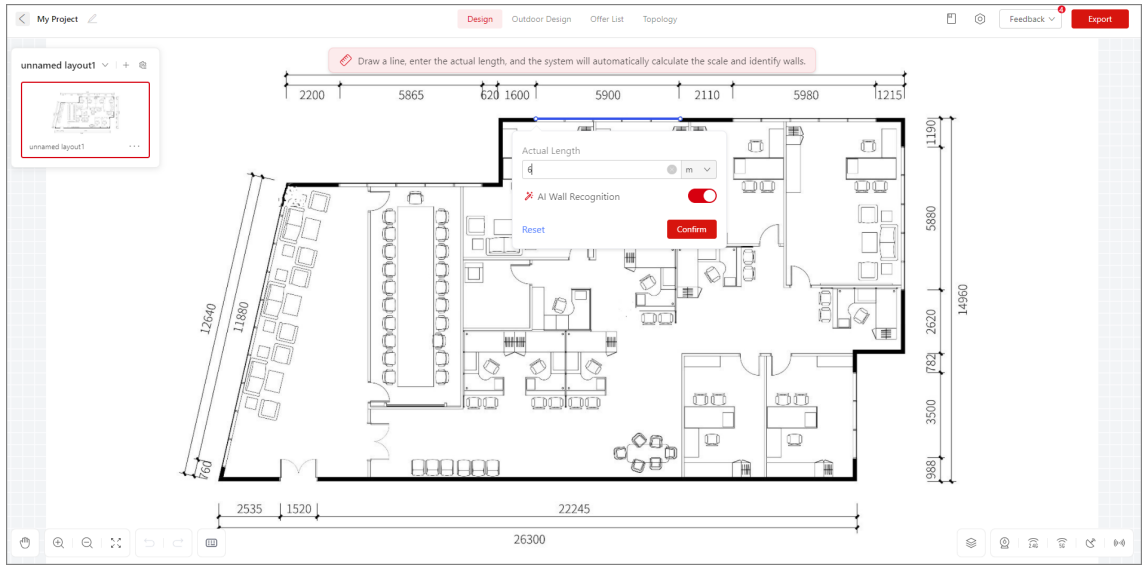


Figure 2-15 Set Scale

6. (Optional) Click on the layout thumbnail card to show the layout settings, you can enable **Scrim** to dim the drawing so the design reads clearly. You can set the color and opacity.

Note

Scrim lays a translucent tint over the floor plan. The drawing stays visible underneath, but it recedes, so everything you place on top of it — walls, devices, cable runs, coverage overlays — separates cleanly from the background.

Control	Effect
Color	The tint laid over the drawing. Pick one that contrasts with your design.
Opacity	How strongly the drawing is pushed back. Raising the opacity pushes the drawing back and leaves the design in the foreground. Lower it again when you need to read the underlying plan: room labels, structural detail.

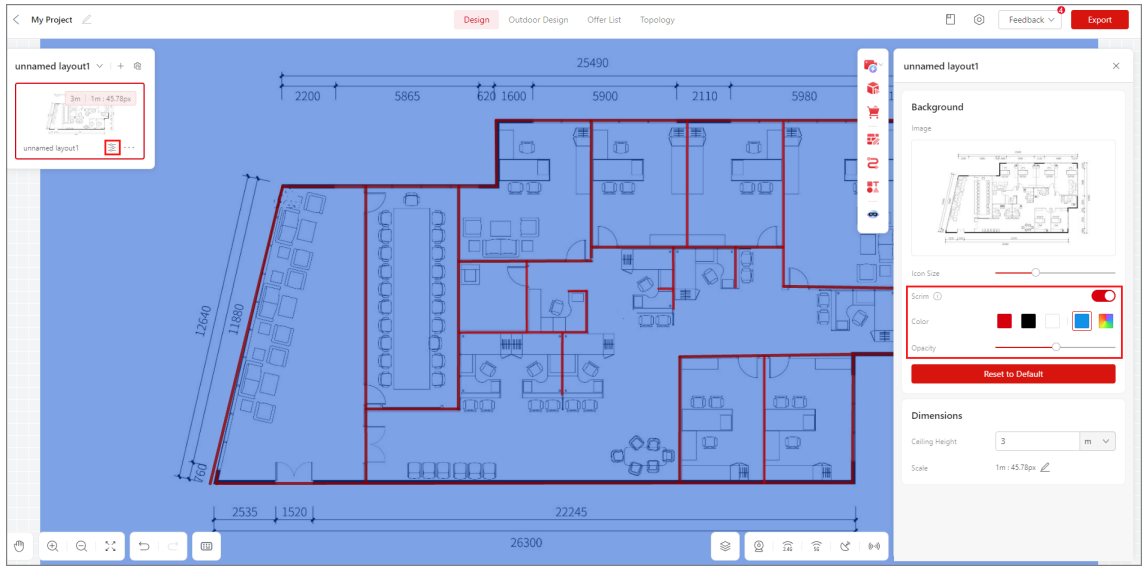


Figure 2-16 Scrim

Multi-Floor Projects

When a project spans several floors, which is a common requirement for intrusion alarm systems, where one security control panel serves detectors on more than one level, HPP designer supports aligning the floors so the simulation can calculate vertical propagation.

1. If you have all floor plans for your project on one image, use **Crop** to separate them when uploading.

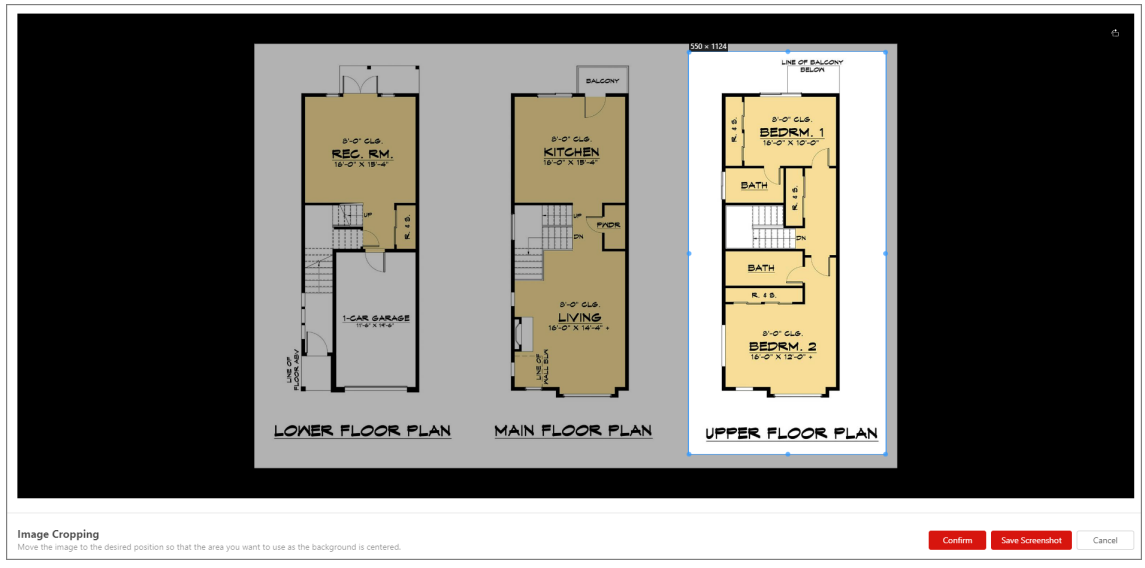


Figure 2-17 Crop

2. Set the layout name and ceiling height, and click **Confirm** to upload all the floor plans at once. Uncheck the original image so it won't be uploaded.

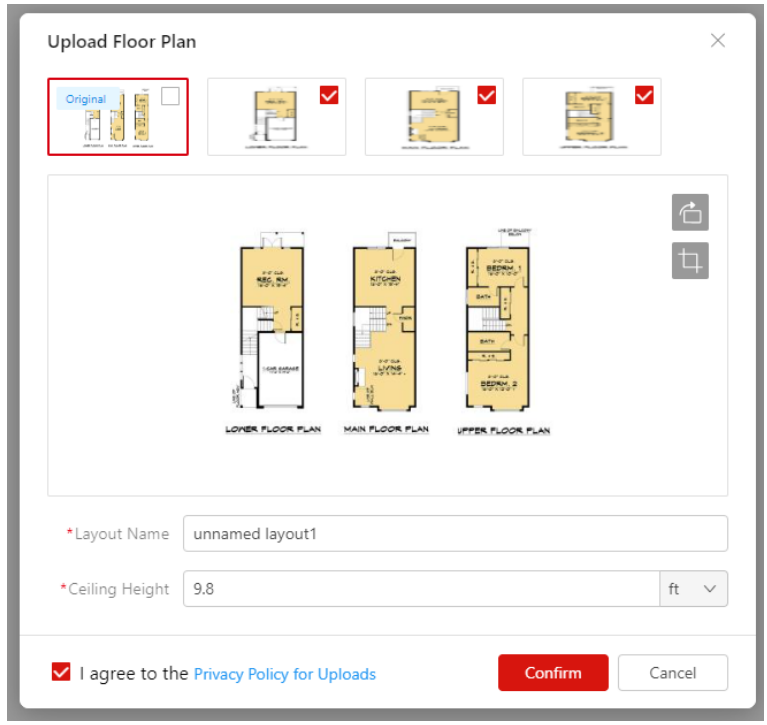


Figure 2-18 Upload Multi-Floor Plans

3. Click ⚙ on the top right of the thumbnail pane to open the **Set Base Floor** page and select the layout that acts as the reference level. Click **Confirm**.

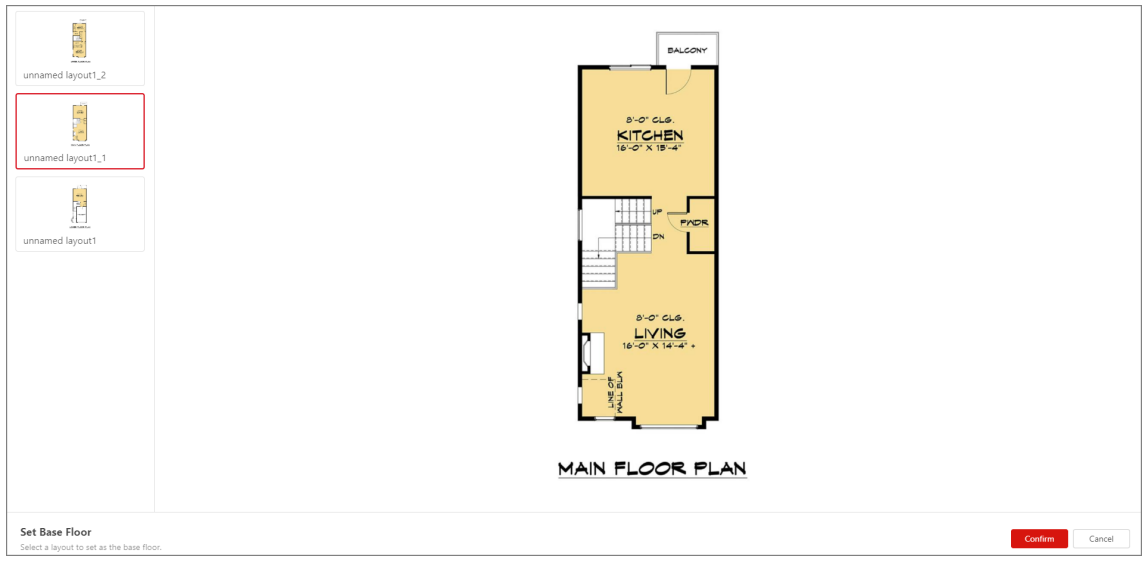


Figure 2-19 Set Base Floor

4. On the **Set Floor Alignment** page, drag and rotate each remaining floor plan until it lines up with the base floor, then click **Next**.

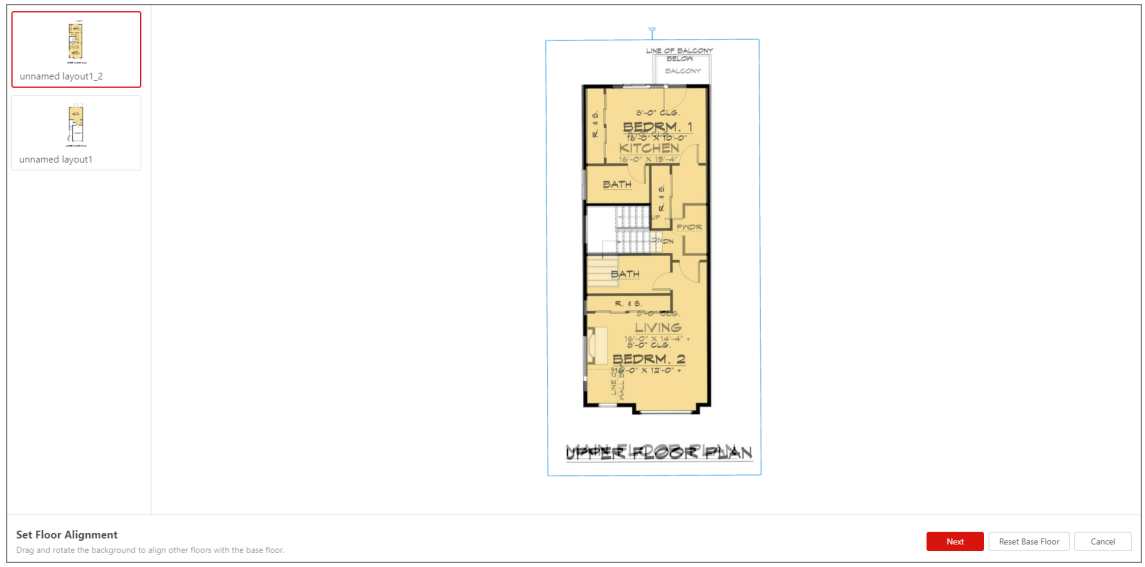


Figure 2-20 Align Floor

5. After you align all floors, click **Submit**.

Define Walls

Use AI to automatically recognize walls, or manually draw, copy, delete, and edit wall properties.

Click **Add Wall** in the right-hand toolbar and perform the operations as needed:

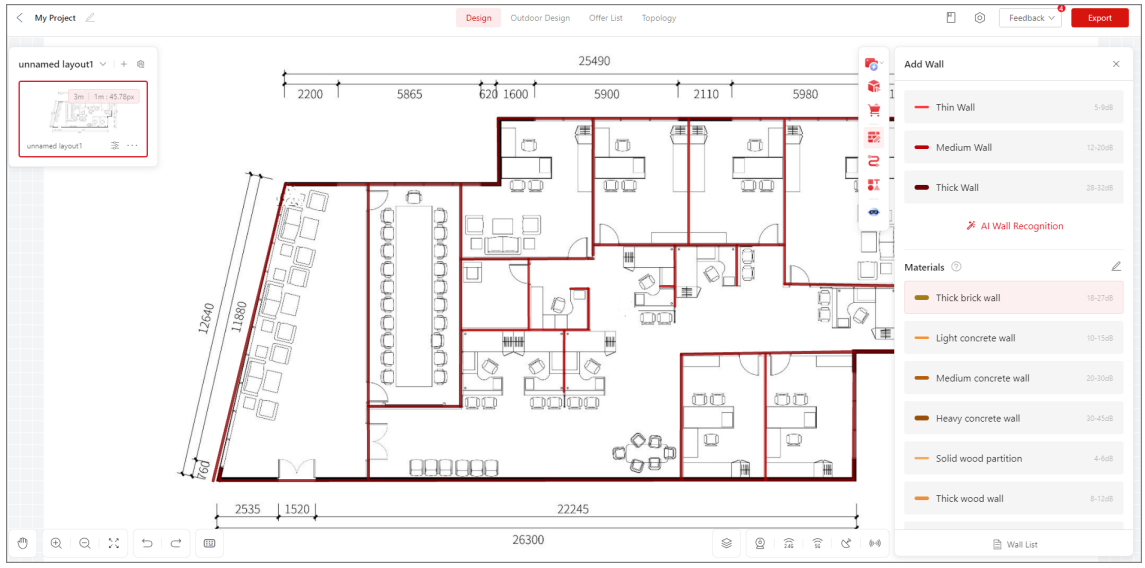
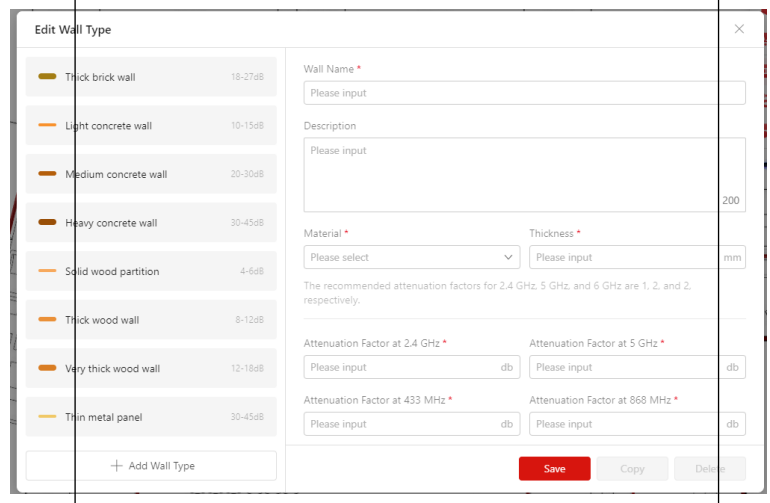


Figure 2-21 Add Wall

Table 2-4 Operations

Operation	Description
AI Wall Recognition	1. Click **Add Wall → AI Wall Recognition** . 2. HPP Designer detects walls automatically from the uploaded drawing. **AI Wall Recognition** is also offered at the scale-calibration step (Step 5 of ***Create the Scene***).
Manual Drawing	1. Click **Add Wall**. 2. Select a wall type (**Thin Wall**, **Medium Wall**, **Thick Wall**, or other types in the **Materials** section), and then draw on the layout. For more instructions, see ***Drawing Instruction*** .
Add/Edit Wall Type	1. Click **Add Wall**. 2. Click above the **Materials** section. 3. Click **Add Wall Type** and set the parameters to add, or select a existing type to edit. For detailed field explanation, see  **Figure 2-22 Add Wall Type**

Drawing Instruction

Table 2-5 Drawing Instruction

Operation	Description
Draw Line / Polyline	Left click to place endpoints to form a line/ polyline. Right click to exit. You can hold **Shift** while drawing to keep the line horizontal or vertical.
Draw Rectangle	Left click and drag to draw a rectangle, release to finish. Right click to exit.
Modify Line	Hover over a line to show its length. Click a line to modify. • **Copy**: Left click to place the copied line. Right click to exit. • **Wall**: Change the wall type. • **Disconnect**: Left click on the line to split it into two or more lines. • **Delete**: Delete a line.

Materials and Custom Wall Types

Walls matter because they attenuate radio signals. Define them before running any wireless or alarm simulation. Wi-Fi, alarm and bridge simulations treat a wall as an attenuator. The signal passes through but is weakened, so the wall's material and per-frequency attenuation determine the result.
Editable wall type fields are shown below:

Field	Notes
Wall Name	Required. Appears in the wall list and the exported report.
Description	Up to 200 characters.
Material	Required. Select from Concrete, Brick, Wood, Metal, Glass, and Other.
Thickness	Required, in mm.
Attenuation Factor at 2.4 GHz	Required. Applies to Wi-Fi and 2.4 GHz bridge links.
Attenuation Factor at 5 GHz	Required. Applies to Wi-Fi and 5 GHz bridge links.
Attenuation Factor at 433 MHz	Required. Applies to wireless intrusion alarm devices.
Attenuation Factor at 868 MHz	Required. Applies to wireless intrusion alarm devices.

Place Devices

1. Select **Device Deployment**.
2. Move your cursor to the device card on the right, click or , move your cursor to the desired position on the scene layout, and click again to drop the product. Right-click to exit. You can select products from **Products**, or **My Products**.

   Each product entry offers two actions: adds it to the quotation without placing it (in the **Device List**), and / places it on the layout.

Table 2-6 List

List	Description
Products	The full Hikvision catalog published for your region. Filter by category (Cameras, Backend, Networking, Access Control and more), then by subcategory, or use the search box and the filter icon.
My Products	Your own shortlist, grouped as **Recent**, **Favorites** and **Custom**.

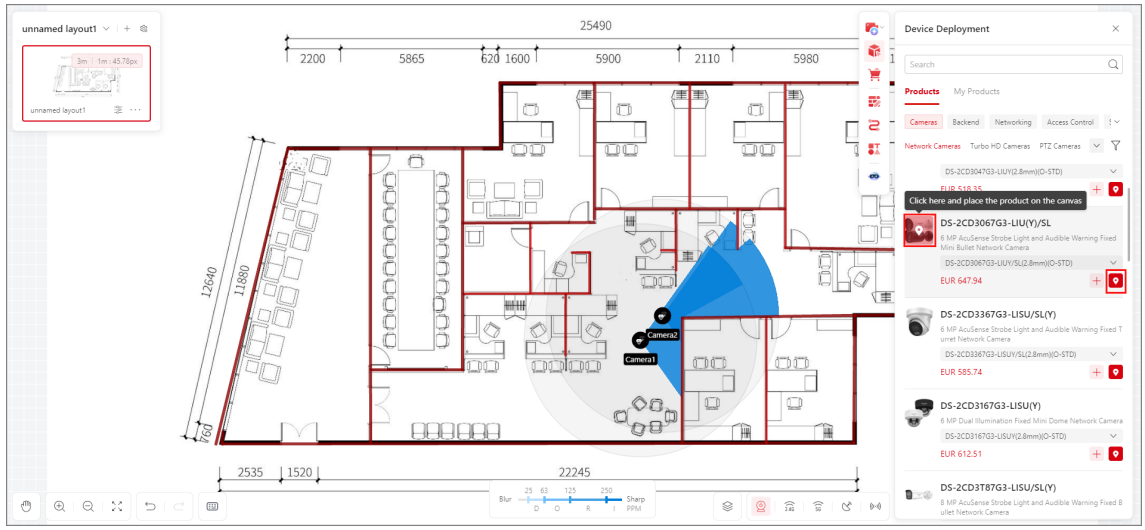


Figure 2-23 Place a Product

3. Repeat until you have placed all products you need onto the scene.

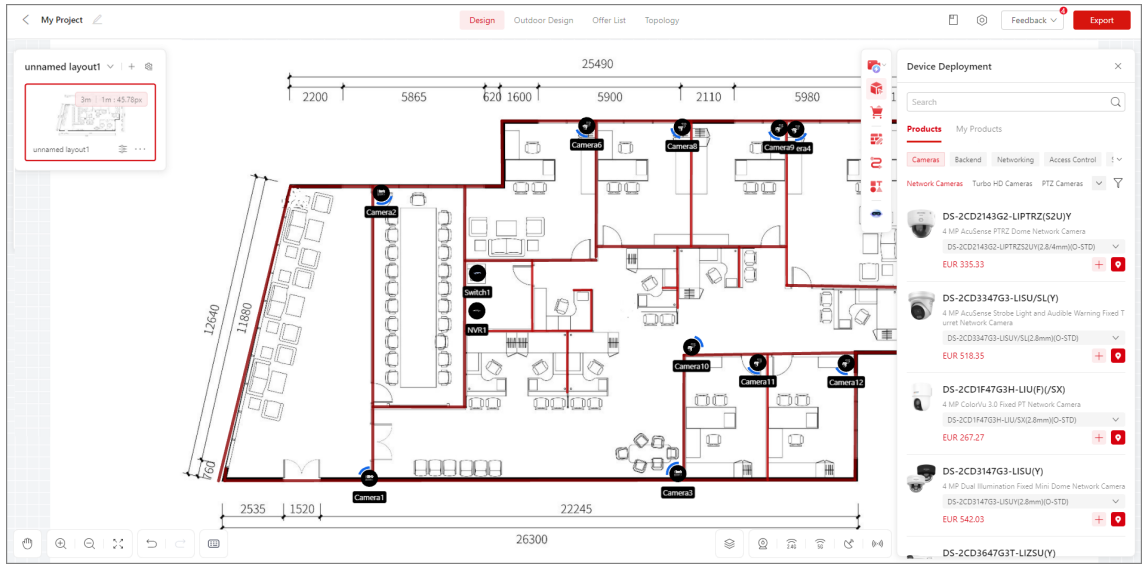


Figure 2-24 All Products Deployed

Quick Device Placement

Use the quick product selector to quick switch the device type and place the product.

1. The button at the top of the right-hand toolbar are for quick device placement. Click the button to quick place a recommended model of the selected device type.
   By default, the button is **Camera**.
   To place other device type, click the arrow ∨ beside the button, and select the device type you are placing: **Camera**, **Alarm**, **AP**, **Radar**. **Alarm** expands into the individual device types.

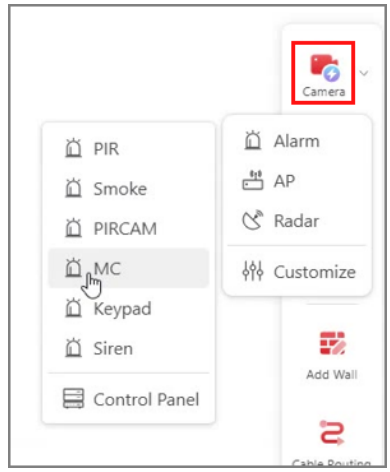


Figure 2-25 Quick Placement Button

2. To change the top device type and the order, click the arrow ∨ beside the button, select **Customize**, and drag to edit the device type order and top device type.

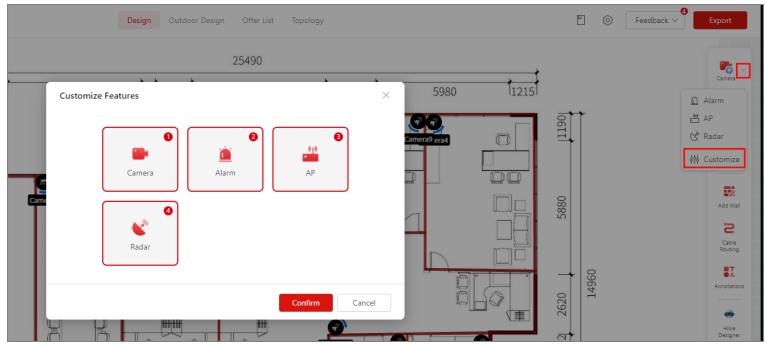


Figure 2-26 Change Order

Custom Products

Products outside the published catalog can still be designed in and quoted.

1. Click **Device Deployment → My Products → Custom** .
2. Click **Add New Product** at the bottom.
3. Set the product properties: category, model, description, brand, unit price, and product image.
4. For the **Cameras** and **AP** categories, click to set more product parameters.

Note

A custom product with these extra parameters is simulated exactly like a catalog product.

Cameras

Simulation parameters. Add one block per channel with **Add Channel**, choose **Fixed Lens** or **Varifocal Lens**, and enter **Resolution**, **Focal Length**, **HFOV** and **VFOV**.

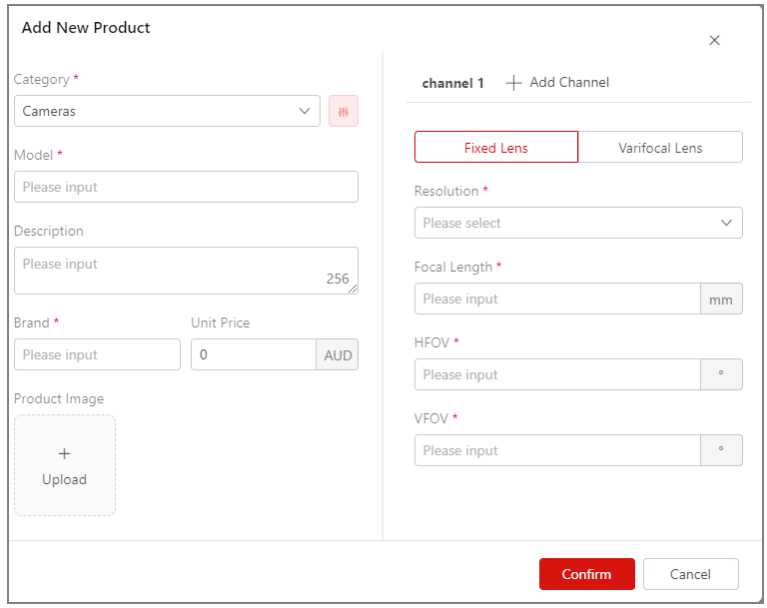


Figure 2-27 Cameras

AP

Simulation parameters. Set the installation type, and transmit power and antenna gain for 2.4G and 5G.

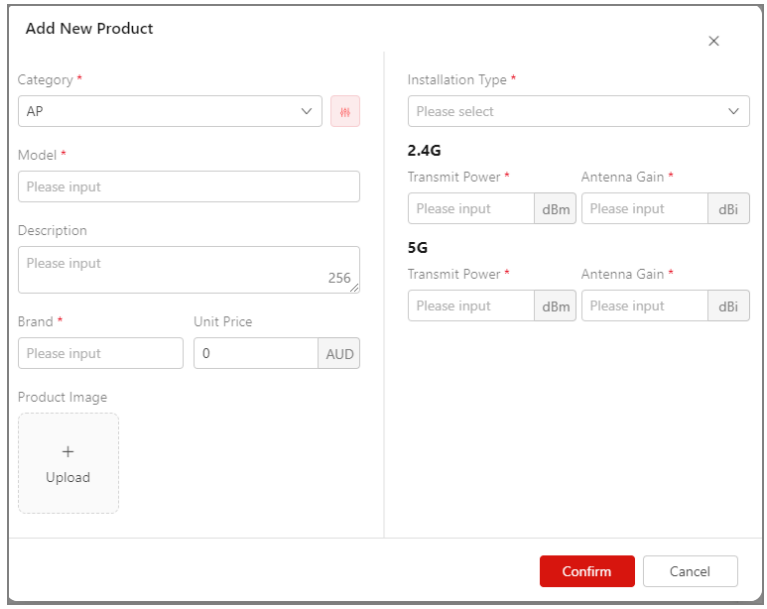


Figure 2-28 AP

5. Click **Confirm**.

Configure a Placed Device

Select a device to open its parameter panel.
For devices other than cameras and APs, only **Device Name** can be edited. **Specifications** may display depending on the device model.

For Cameras

At the top of the panel, you can edit the **Device Name**.

Deployment Parameters always includes **Installation Height**, and a **Reset** button that restores the defaults. It also carries **Resolution**, **Focal Length** and **Tilt angle**, together with a side-view diagram showing the resulting coverage geometry.

Multi-channel cameras expose one tab per channel (CH 1, CH 2...). Configure each channel separately, and each contributes its own coverage cone to the simulation.

In the **PPM/PPF Simulation** section, you can check how the image clarity changes as you adjust the parameters.

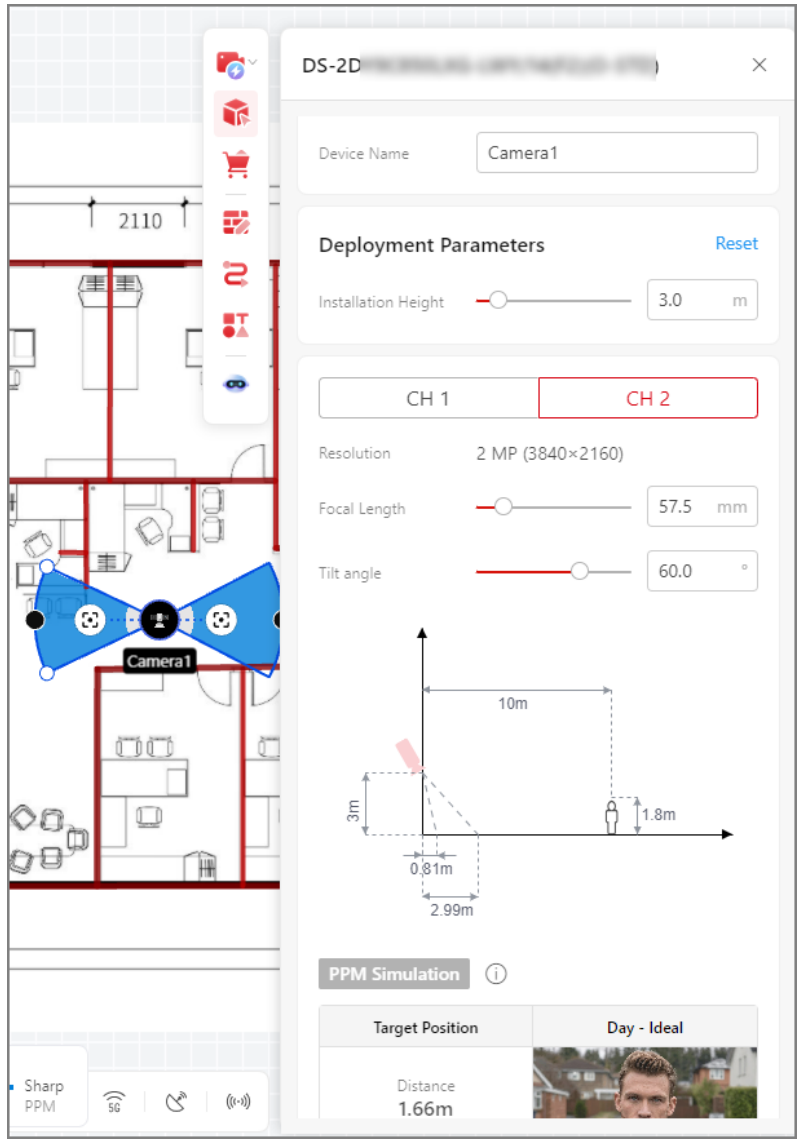


Figure 2-29 Camera Parameters

For APs

At the top of the panel, you can edit the **Device Name**.

Deployment Parameters includes **Installation Type**, **Tilt angle**, **Installation Height**, and **Power level**.

The **Specifications** section is determined by the device model, including **2.4 GHz Max Power** and **5 GHz Max Power**.

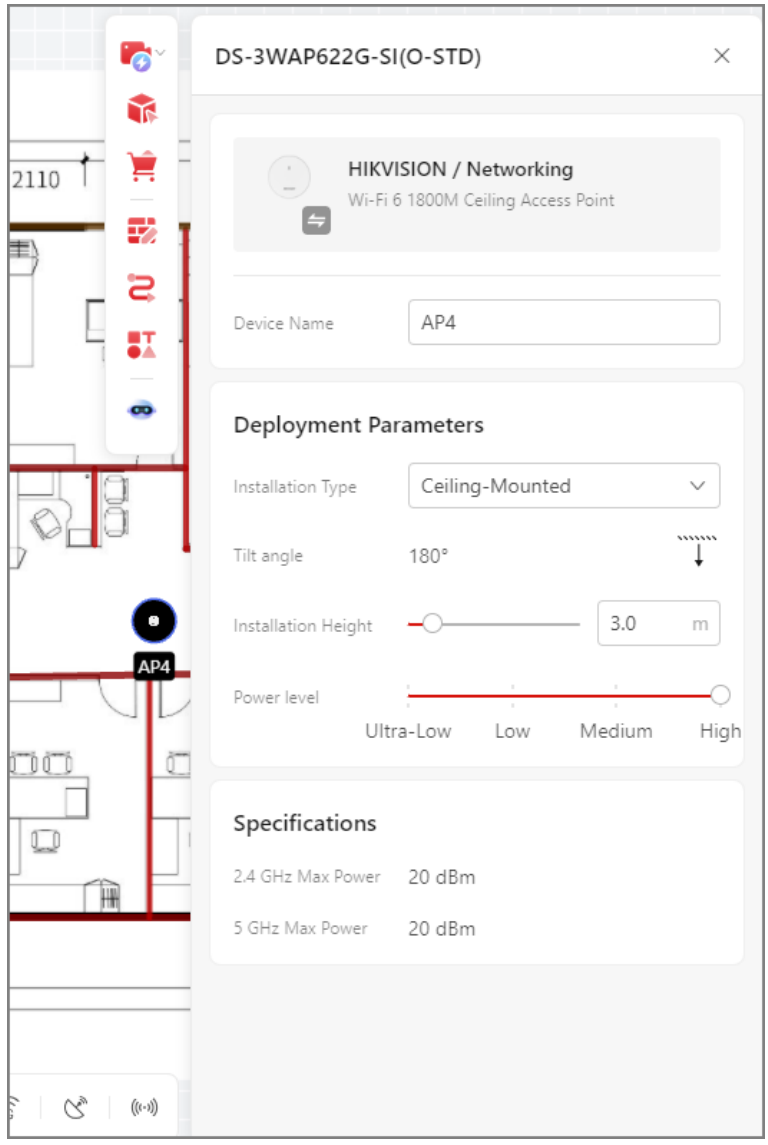


Figure 2-30 AP Parameters

Simulation by Product Type

Simulation results update automatically as you move a device or change a parameter. Use the display switches at the bottom-right of the canvas to show/hide each simulation overlay, and ***Global Settings*** to control what the overlays contain.

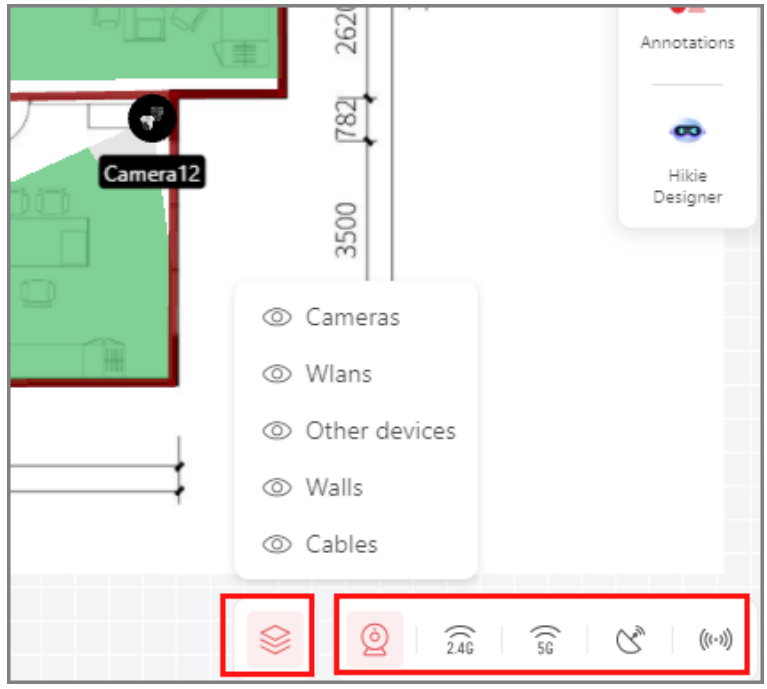


Figure 2-31 Buttons for Viewing Simulation

Camera: Field of View and Image Quality

The camera simulation overlay answers two questions: what the camera sees, and how much detail it captures at each distance.

Click on the bottom right to show the simulation overlay for cameras.

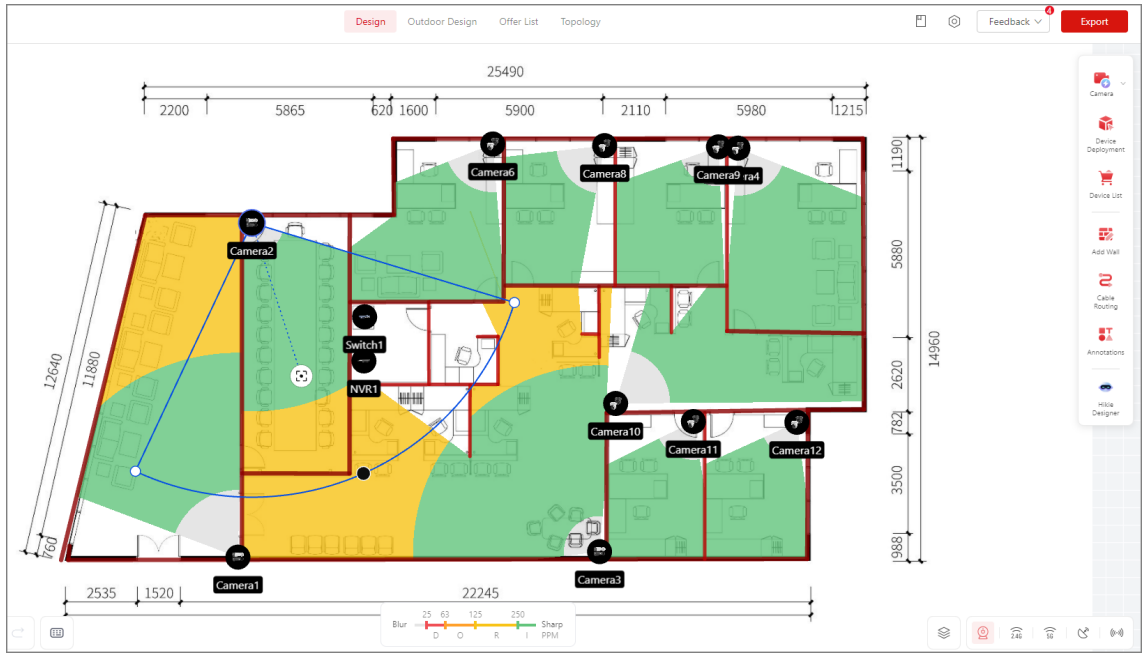
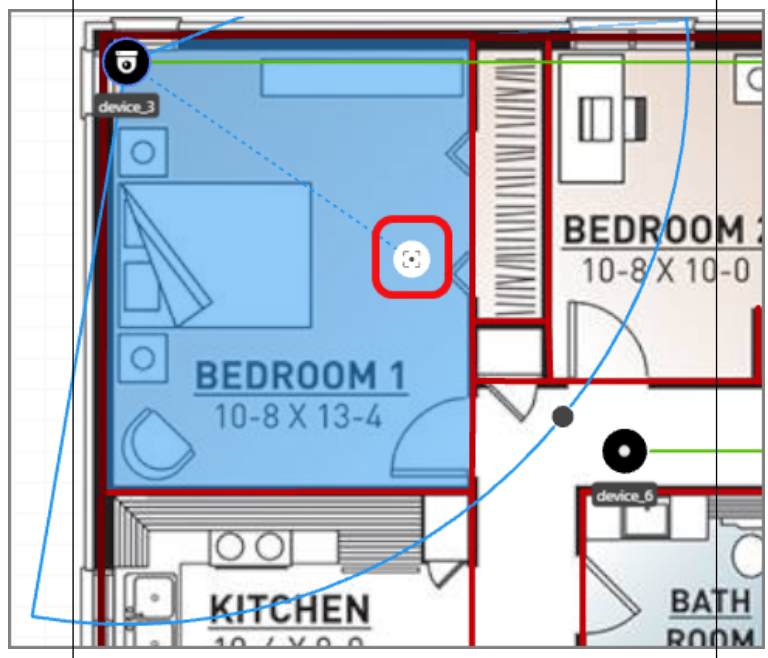
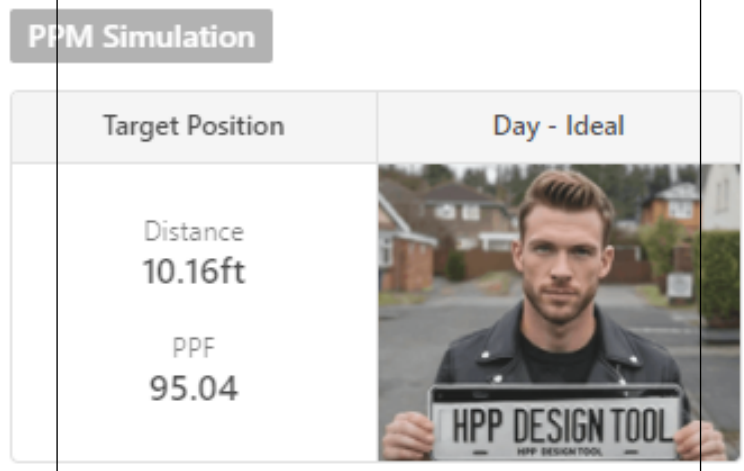


Figure 2-32 Camera Simulation Overlay

Table 2-7 View the Simulation

Item	Description
Field of View	**Field of view** is drawn as a cone from the camera, derived from focal length, resolution, installation height and tilt angle. 1. Drag the gray dot  along the arc to adjust the FOV. 2. As you drag to adjust the FOV, the camera's **tilt angle** and **installation diagram** will update accordingly and dynamically in real time.
DORI Zones	**DORI zones** grade the cone by pixel density: **D**etect, **O**bserve, **R**ecognize, **I**dentify. The legend below the canvas maps the color bands to PPF (pixels per foot) or PPM (pixels per meter), from Blur to Sharp.
Blind Spots	**Blind spots** below the camera can be shown or hidden. It is the gray color brand on the cone.

Item	Description
PPF/PPM Simulation	**PPF/PPM** indicates how many pixels in the image correspond to one meter/foot in the real world. The higher the PPM/PPF, the greater the level of detail captured by the camera. 1. The  icon indicates the target, you can drag it to adjust the target position.  **Figure 2-33 Adjust Target Position** 2. As you adjust the target position or camera parameters, you can check the how the image clarity changes in real time.

Item	Description
	 **Figure 2-34 PPM/PPF Simulation**
Walls Cut FOV	Where a wall crosses a camera's field of view, the coverage stops at the wall and a shadow is cast behind it — the same geometry as light through a doorway.

Wireless AP: Signal Heatmap

Click 2.4G on the bottem right to conduct **2.4 GHz Signal Simulation**, or click 5G to conduct **5 GHz Signal Simulation**.

The heatmap runs from red (poor) through yellow to green (good), and the legend shows the dBm thresholds together with the percentage of floor area in each band. For example (as shown below), -85 / -75 / -60 dBm with 77% / 6% / 17%. Separate overlays are available for **2.4G** and **5G**.

Unlike cameras, AP coverage does take walls into account, using the per-frequency attenuation factors defined in ***Define Walls*** . If a heatmap looks unrealistically good, check that the walls have been drawn and classified.

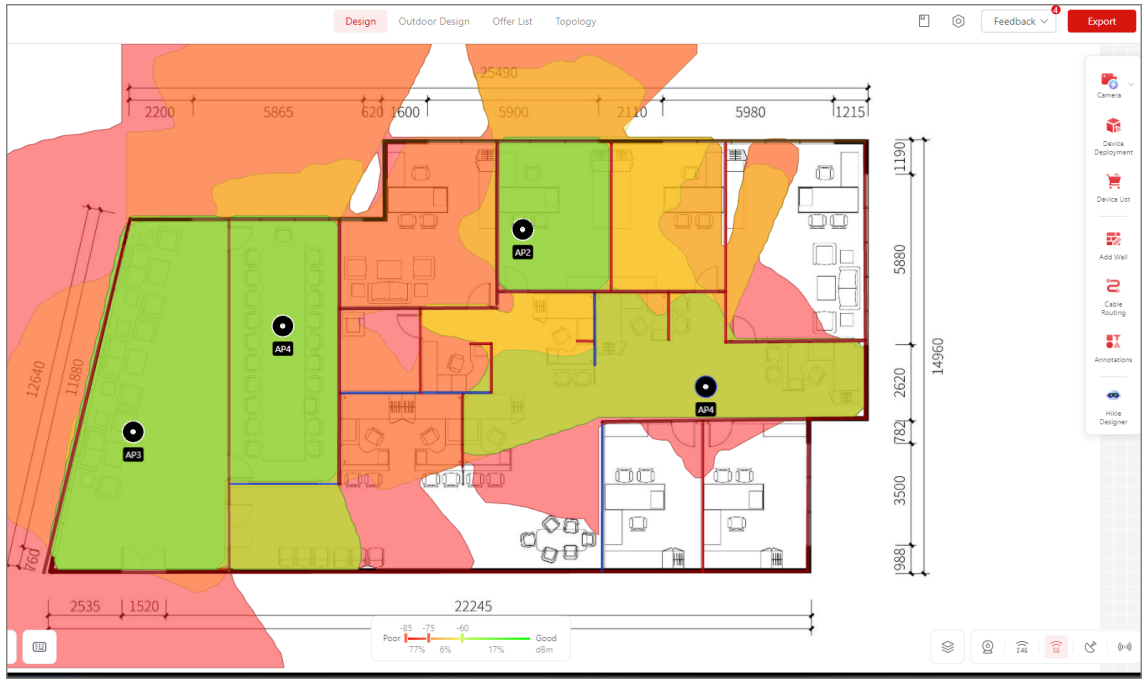


Figure 2-35 AP: Signal Heatmap

Wireless Alarm: Detector Coverage and Links

Place the detectors and the **Control Panel**, and click on the bottom right to show the simulation overlay for alarm devices. The tool draws:

- A **coverage heatmap** showing RF signal strength across the floor, using the per-frequency attenuation factors defined in ***Define Walls*** .
- A **link line** from each detector to the control panel, labeled with the received signal level and the distance, for example -70.50 dBm / 41.93 ft.

Link color tells you whether the design works:

Link	Meaning
Blue dashed	Detector communicates reliably with the control panel
Red dashed	Link fails: the detector is too far away, or too much attenuating structure lies between it and the panel

To fix a red link, move the detector or the control panel, or reduce the number of walls the signal must cross. On multi-floor projects, make sure the floors are aligned (***Multi-Floor Projects***) — otherwise the vertical distance between panel and detector is calculated from the wrong geometry.

The legend readout follows the pointer, so you can hover any point on the plan to read the predicted level at that spot.

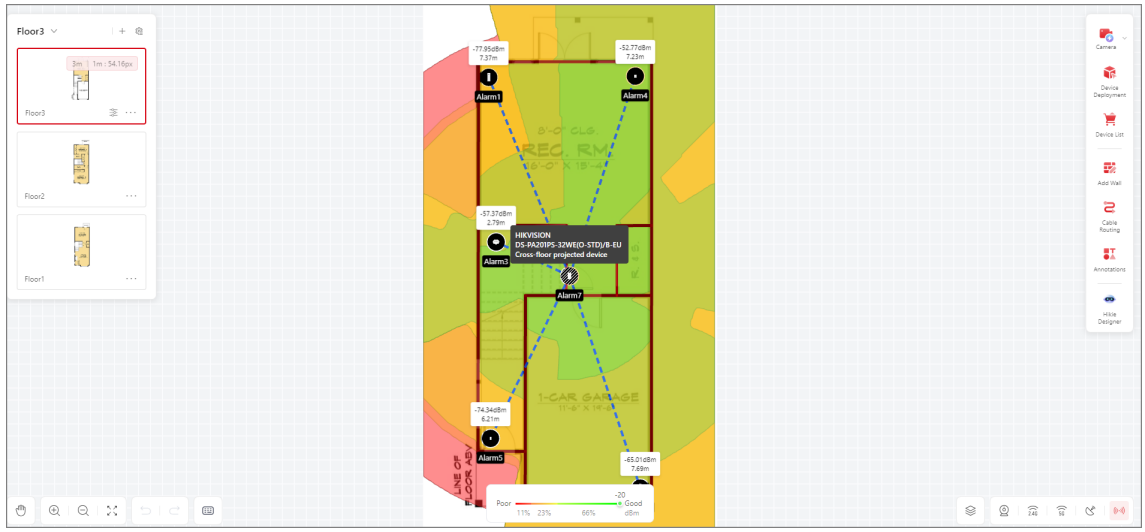


Figure 2-36 Alarm

Design Cabling

Add a convergence point, select cable type (network/fiber/coaxial), and draw connections between devices. The tool automatically calculates total wiring length and adds to the additional fee.

1. Click **Cable Routing** in the right-hand toolbar.
2. Click **Add Convergence Point** to place the aggregation points (racks, cabinets, patch panels) that cables run back to.
   The convergence point acts as an **intermediate connection node** where multiple cables from different devices are aggregated before reaching the main communication room.
   You can click the convergence point, and click **Connect to layout** and select another layout to connect the point to it.
3. Select a cable type.

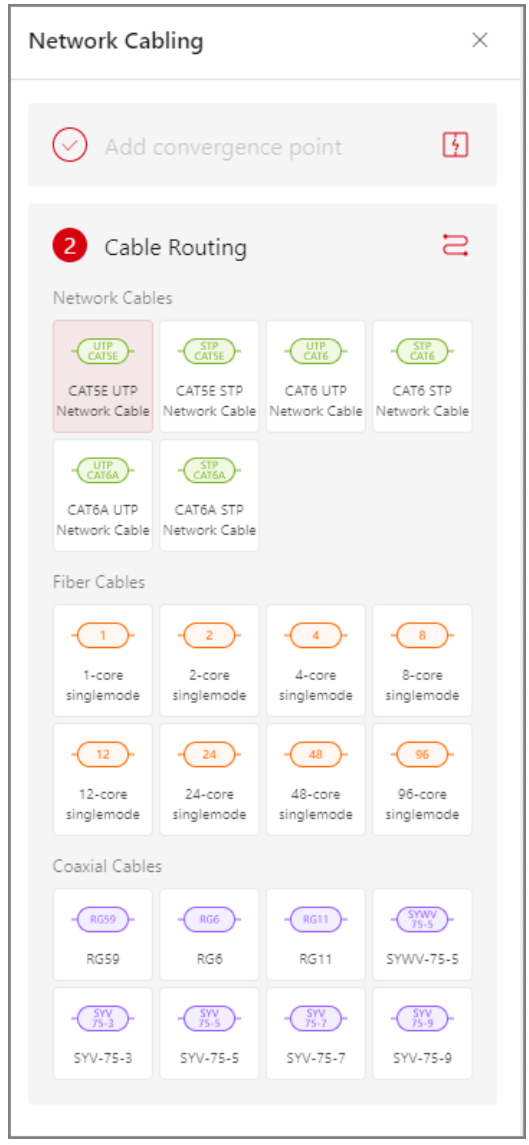


Figure 2-37 Select Cable Type

Table 2-8 Cable Type

Cable Type	Main Use	Distance	Speed	Feature
Network Cable	For LAN or PoE connections.	≤ 100 m	≤ 10 Gbps	Low cost, easy installation.
Fiber Optic Cable	For backbone or long-distance transmission.	Up to several kilometers.	≤ 400 Gbps	High speed, anti-interference.
Coaxial Cable	For analog video or RF signal transmission.	Hundreds of meters.	Low	Stable, reliable.

4. Starting form the convergence point, click any two points you need to connect to draw the cable. Repeat until you finish your cabling design.

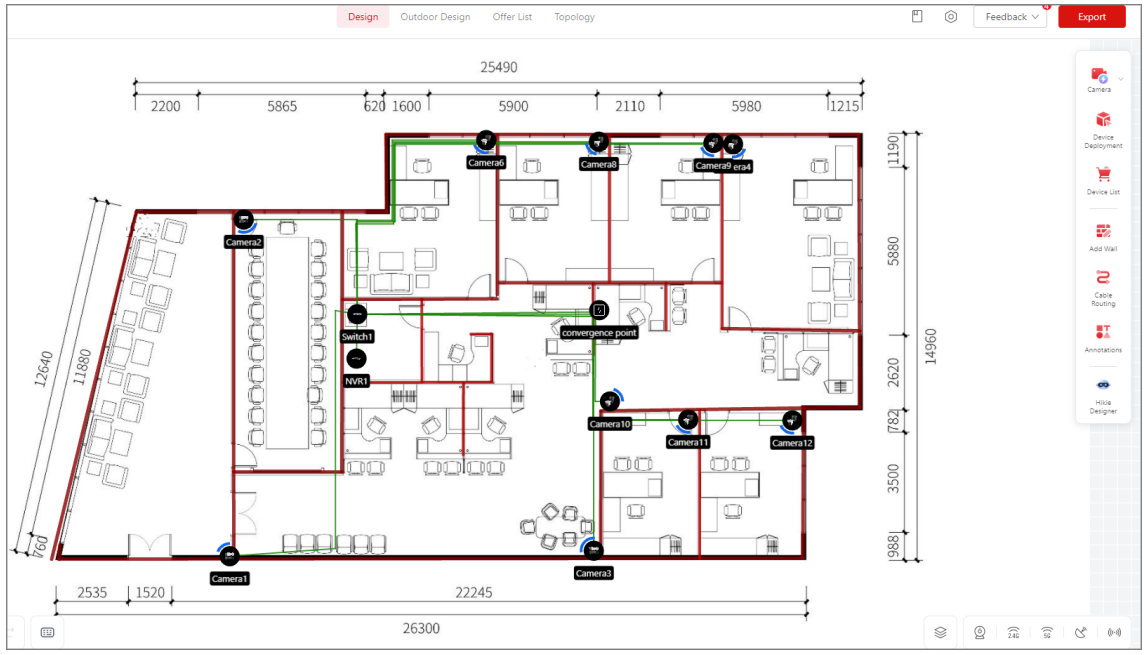


Figure 2-38 Cabling Design

Cable length is calculated from the drawn route and the layout scale, and shown when you hover a run — for example CAT5E UTP Network Cable 106.66 ft. The quantity that reaches the quotation is the drawn length multiplied by the **Redundancy Factor** in Global Settings (default **1.5**), which accounts for slack, vertical drops and terminations that a 2D route cannot represent.

Routes can be re-edited after they are drawn: select a run and drag its vertices.

Annotate the Design

Click **Annotations** in the right-hand toolbar.

Annotations adds explanatory markup that survives into the exported drawings: **Circle**, **Rectangle**, **Polygon**, **Line**, **Text**. Shapes are drawn by holding down the left mouse button; right-click or **Esc** exits the tool.

Use annotations to record what the simulation cannot express — the equipment room, a cable riser, a customer constraint, a site condition noticed during the survey.

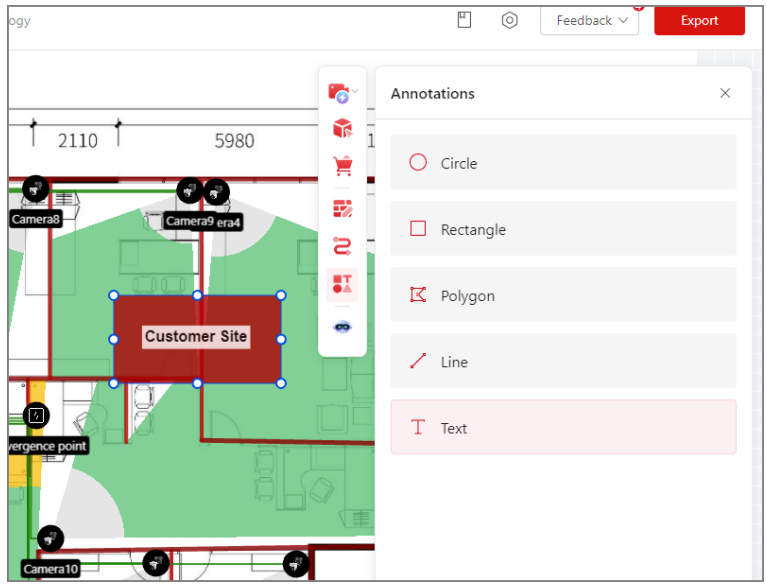


Figure 2-39 Annotation

Generate the Topology

Open **Topology** in the top navigation bar. The system diagram is generated automatically from the device types and the cabling you have drawn. See ***Topology*** for the editing options, which are the same for indoor and outdoor designs.

2.2.5 Part B: Outdoor Design

Create the Scene

1. Click **Outdoor Design** in the top navigation bar. The map opens at your current location.
2. Find the installation site.

- Type the address into **Search location** at the top left.
- Or drag and zoom the map directly.

3. Click **Save location** to turn the pin into a scene.

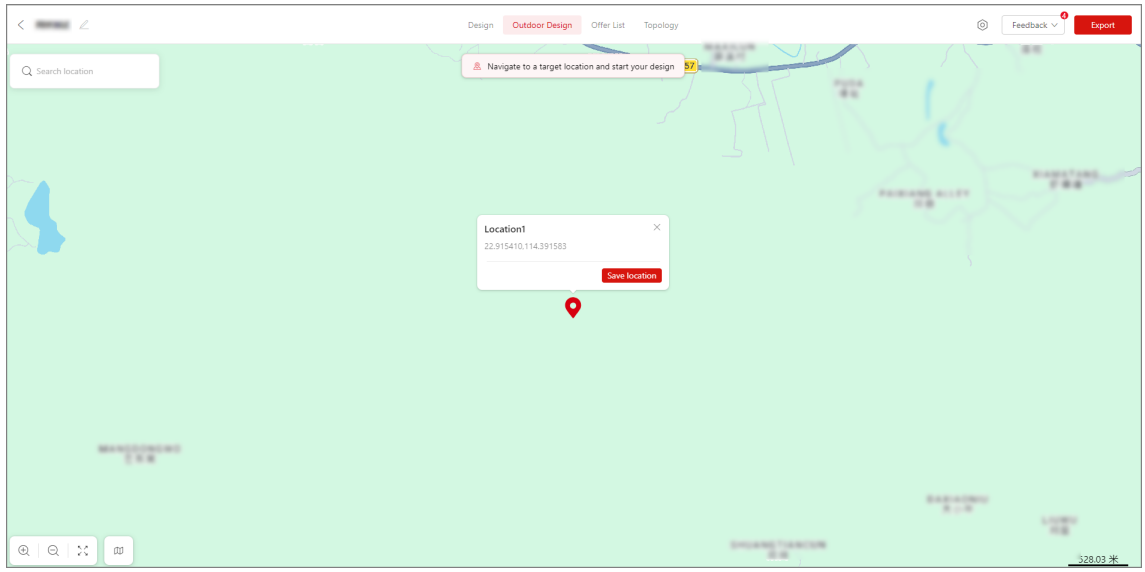


Figure 2-40 Outdoor Location

4. The saved scene appears in the scene list on the left, showing its thumbnail and coordinates.
   - **Use several scenes when the sites are spread out.** A project can hold multiple saved locations, and you switch between them from the scene list. This keeps each map view at a workable zoom level instead of forcing one view to span kilometers of unrelated ground. Click **+** in the scene list to add another location.
   - Map controls sit at the bottom left: zoom in, zoom out, fit to content, and a map style toggle that switches between satellite imagery and the road map. Satellite view is better for identifying mounting structures; road view is better for reading distances and street names.

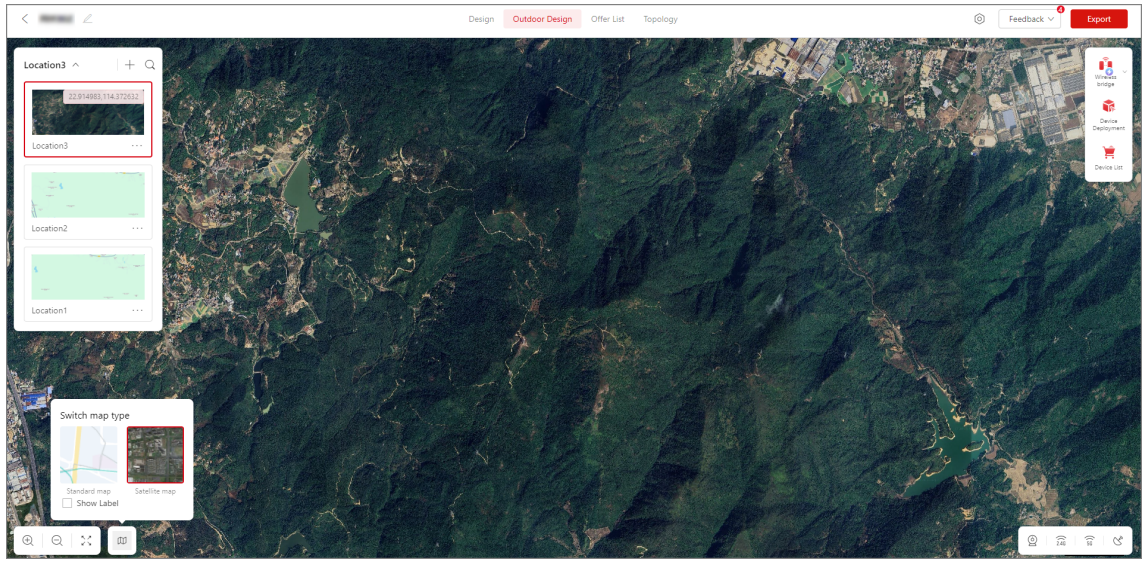


Figure 2-41 Satellite View

Place Devices and Simulation by Product Type

Select products from **Device Deployment** or use the quick product selector exactly as for indoor design, then place them on the map. Selecting a placed device opens its parameter panel on the right.

For details, refer to ***Place Devices*** .

Wireless Bridge

A bridge design links remote camera sites back to a head end. HPP Designer models the radio path over real terrain, so the design accounts for the ground between the two ends, not just the straight-line distance.

For wireless bridges, click **Wireless → Add Bridge** , click once on the map to place the **AP Bridge**, click twice or more to place one or more **CPE Bridges**.

The base station (AP) is the aggregation end; each CPE is a remote end at a camera site. Devices placed together form a **Bridge Group**, which is named automatically and can be renamed with the pencil icon.

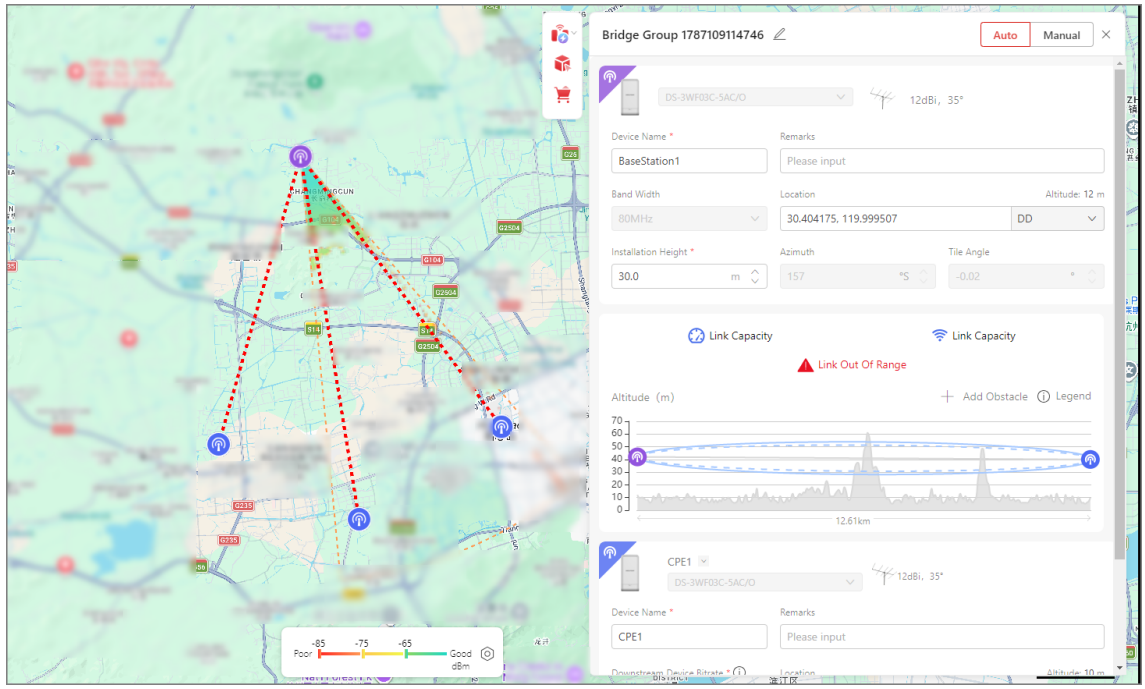


Figure 2-42 Place Wireless Bridges

Setting the required bandwidth

Each CPE carries a **Downstream Device Bitrate** field, in Mbps. Enter the total bandwidth the cameras at that site will produce. This value drives the model recommendation and the link budget — a CPE left at its default may be equipped with a radio that cannot carry the real load.

The **Auto** / **Manual** toggle at the top of the panel controls whether the tool selects the radio models for you or you choose them yourself. **Auto** derives the model from the link distance and the bandwidth you entered.

Reading the device parameters

Field	Meaning
Device Name	Required. Carried into the device list.
Band Width	Channel width of the link, for example 80 MHz.
Location	Coordinates of the device; the format selector switches between decimal degrees and other notations. **Altitude** is read from terrain data automatically.
Installation Height	Height of the antenna above ground. This is the single most effective parameter for clearing an obstruction.
Azimuth	Horizontal bearing the antenna must face.
Tilt Angle	Vertical angle the antenna must be set to.

Azimuth and tilt are calculated by the tool, not entered by you — they are installation outputs. They are reproduced in the export as a compass dial and an antenna elevation diagram for the installer (***Export Quotation and Design Report***).

Reading the link status

Each link reports **Link Capacity** at both ends: uplink and downlink throughput in Mbps, and received signal level in dBm at the base station and at the CPE.

Link on the map	Meaning
Blue dotted	Link is viable at the modeled bandwidth.
Red dotted	**Link Blocked**: the path does not work.

A link is blocked for one of two reasons:

1. **The distance exceeds the maximum range of the selected radios.**
2. **Terrain blocks the path**: A hill or ridge rises into the signal path. Note that **buildings are not part of the terrain model**; only ground elevation is read. On a site where buildings are the real obstruction, add them manually as obstacles.

The terrain profile

The **Altitude (m)** chart below the link capacity figures plots the ground elevation along the path, with the radio path drawn over it. Hover the chart to read, at any point along the link:

- **Distance To Base Station**
- **Height Of Sight**: The height of the line of sight above ground.
- **Fresnel Height**: The clearance the Fresnel zone requires at that point.

A path that looks clear in plan view but shows the terrain rising into the Fresnel zone here will not perform as designed. Raise the installation height at one or both ends, or insert a relay.

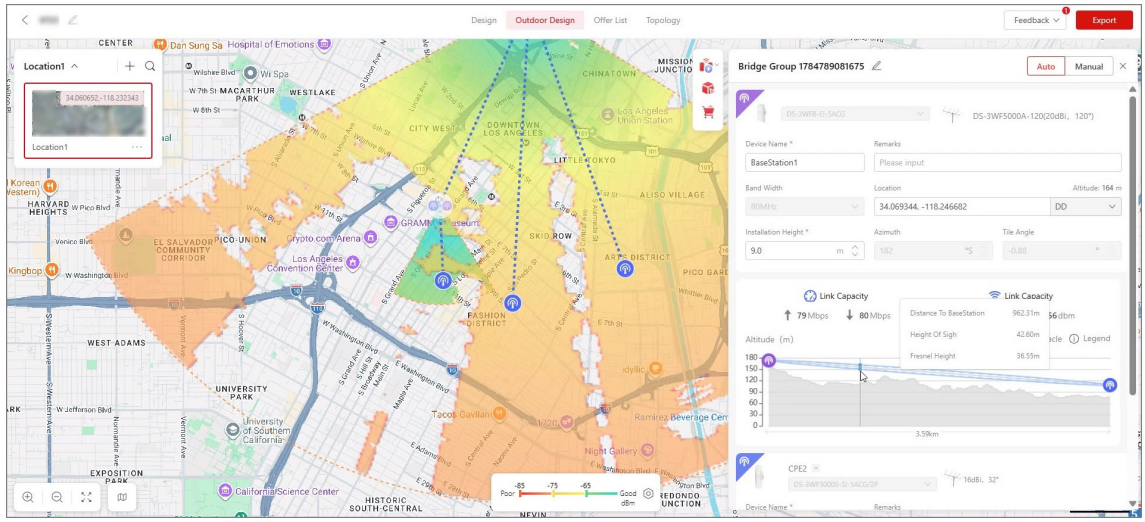


Figure 2-43 Terrain

Adding obstacles

Click **Add Obstacle** to insert an obstruction the terrain model does not know about: a building, a stand of trees, a silo. Once added, the affected links recalculate immediately, and a link that can no longer close turns red.

Fixing a blocked link with a relay

Hover a red link and the tool prompts you to add a relay. There are two ways to insert one:

- **From the link.** Click the red link; the prompt **Click to Add a Bridge Base Station** appears. Clicking it inserts a new pair of bridges at the midpoint of the link.
- **From a CPE.** Select any CPE and click **Add Base Station** at the top of its panel. A new base station is created at that CPE's position, ready to extend the chain onward.

The relay position almost always needs adjusting by hand. Inserting a relay at the geometric midpoint rarely clears the obstruction on both sides at once. After adding it, drag the relay along the route and watch the terrain profile until **both** halves of the path are clear. The full link only returns to normal once neither half is obstructed.

Coverage heatmap

With the bridges in place, the map shows the predicted signal strength as a colored overlay, with the legend running from Poor to Good in dBm. The sector antenna's beam is drawn as a dashed polygon, so you can see which sites fall inside the served sector.

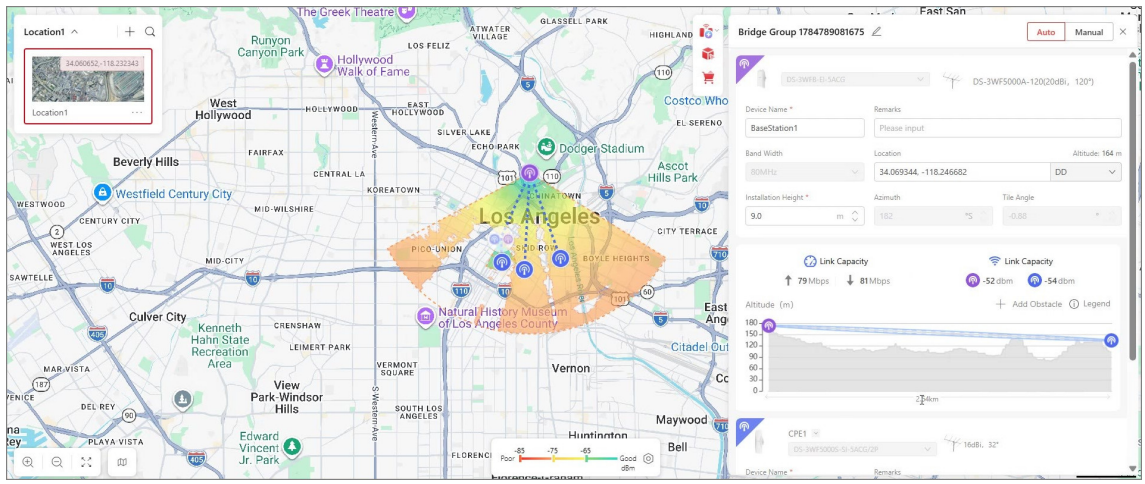


Figure 2-44 Heatmap

Reviewing the group

Open **Device List** to see the bridge groups as a tree: each base station with the CPEs associated to it. Rename or delete a whole group from here.

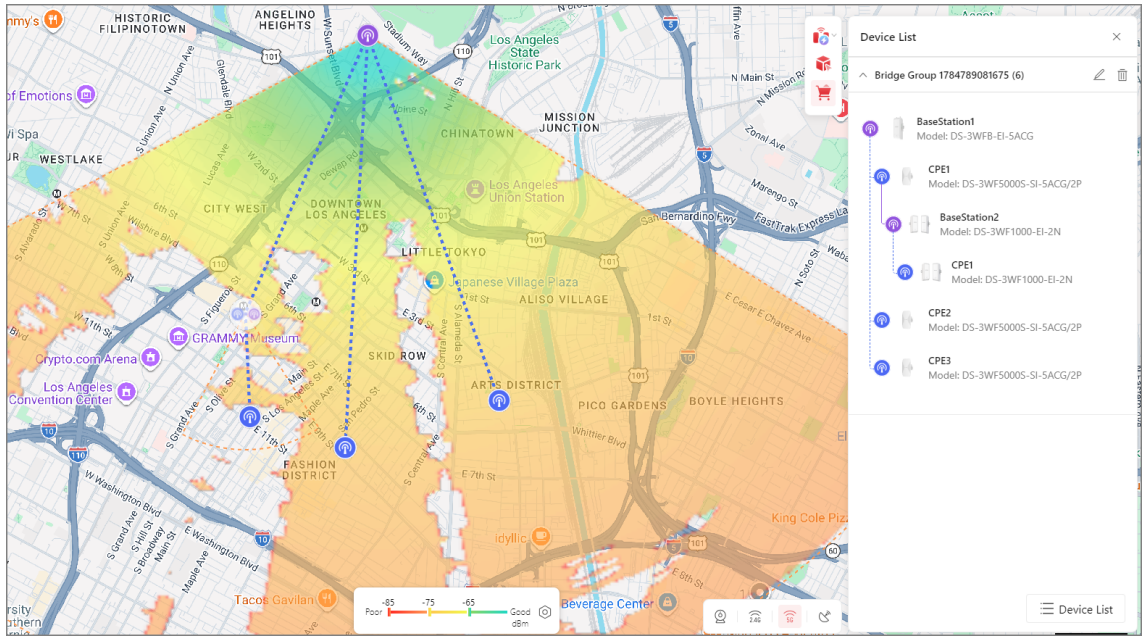


Figure 2-45 Device List

Thermal Cameras

Thermal devices are configured for a specific use, and the parameters change with the use. Select the mode from the tabs in the device panel.

Table 2-9 Thermal Modes

Mode	What it is for	Key parameter
Hik VCA	Video content analytics: intrusion, line crossing, etc.	/
Temp.M & Fire.P	Temperature measurement and fire prevention.	**Target Size (H×V)** in meters: the size of the object that must be resolved.
Fire Detection	Detecting an active fire.	• **Target Size (H×V)** in meters: the size of the object that must be resolved. • Select between **Deep Learning** and **Max. Detection**.
Smoke Detection	Detecting smoke.	**Target Size (H×V)** in meters: the size of the object that must be resolved.

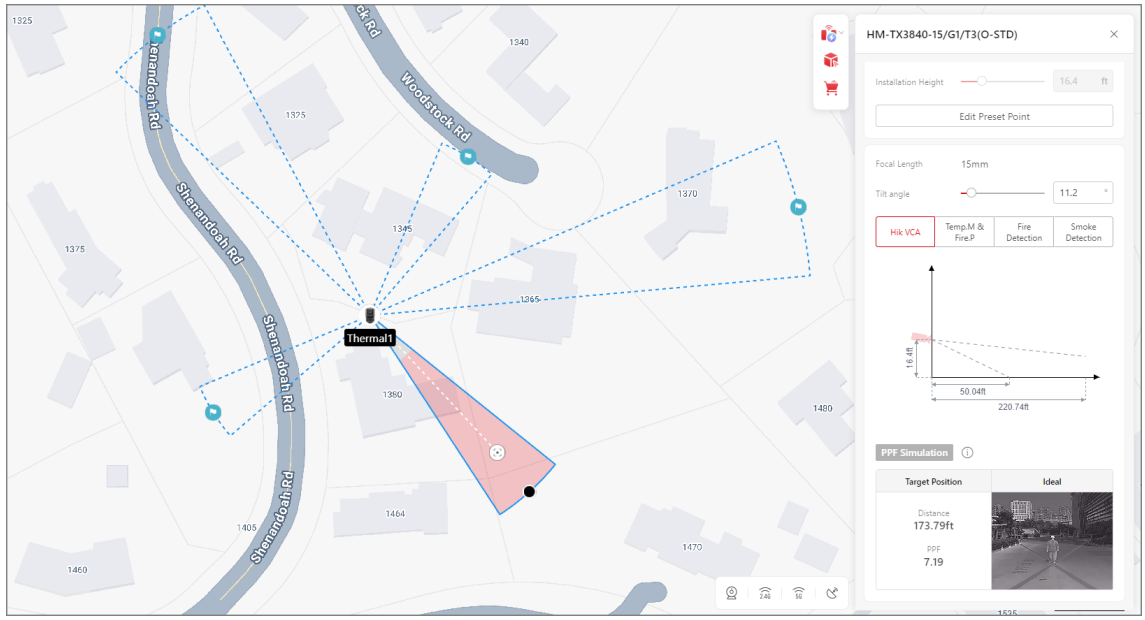


Figure 2-46 Thermal Modes and PPF/PPM Simulation

This distinction matters when specifying a lens. A thermal camera that produces an acceptable *image* at a given distance may still be unable to *measure temperature* on a small target at that same distance, because temperature measurement requires the target to cover a minimum number of pixels. Setting the mode first, then reading the simulation, prevents specifying a lens that satisfies the wrong criterion.

PPF/PPM Simulation renders a preview image at the chosen distance, so the achievable detail can be judged directly rather than inferred from a number.

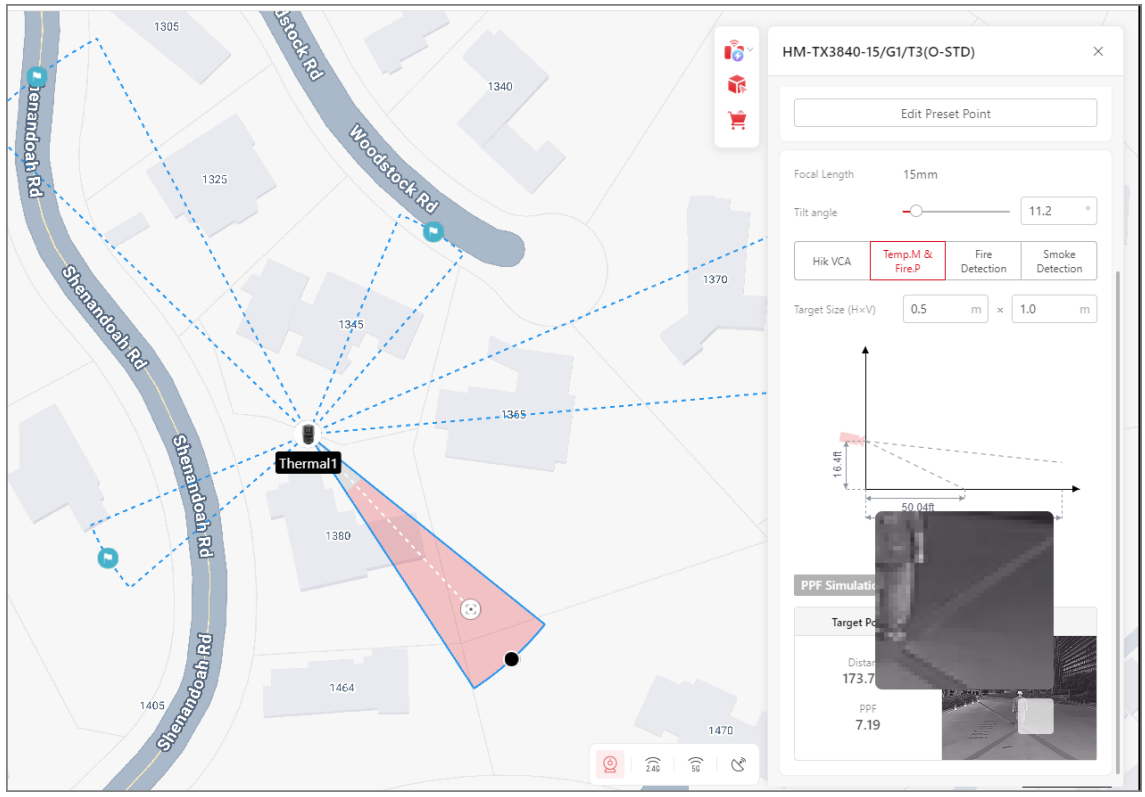


Figure 2-47 PPF/PPM Simulation

Preset points. For scanning and PTZ thermal devices, click **Edit Preset Point** to define the positions the camera patrols. Each preset is drawn on the map with its own line of sight, so the combined coverage of the patrol can be assessed as a whole.

Press **Enter** to save the current preset point and configure the next one.

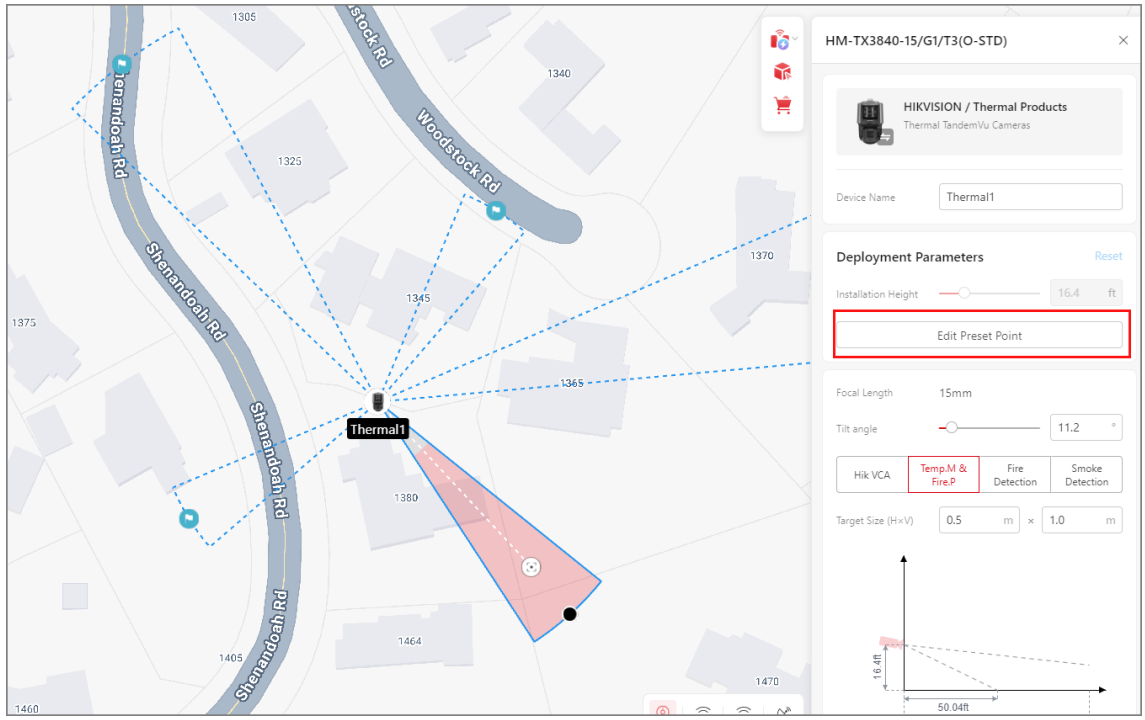


Figure 2-48 Preset Points

2.2.6 Device List, Quotation and Export

Everything placed in any scene, indoor or outdoor, converges here.

Review and Adjust the Device List

Open **Offer List** in the top navigation bar.

The summary strip at the top shows the currency selector and the price breakdown: **Total Price = Products + Additional Fee + VAT/GST**. The tax rate is editable.

Two views are available:

- **View by Device**: One row per model, with **Unit Price**, **Qty**, **Discount** and **Amount**. Expand a row to see the individual placed instances; each instance can be renamed and located.

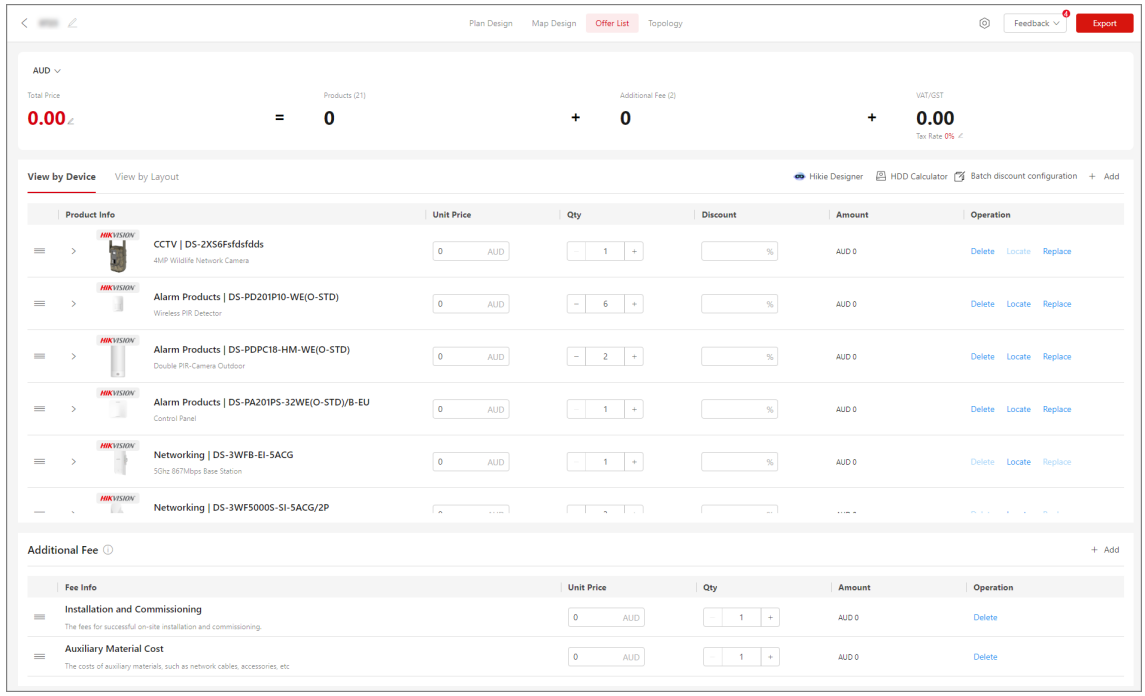


Figure 2-49 View by Device

- **View by Layout**: The same devices grouped by the scene they belong to, with a count per scene. A separate **Undeployed** group collects products that were added to the quotation but never placed on a drawing — check it before exporting, as it is the usual source of a mismatch between the design and the bill of materials.

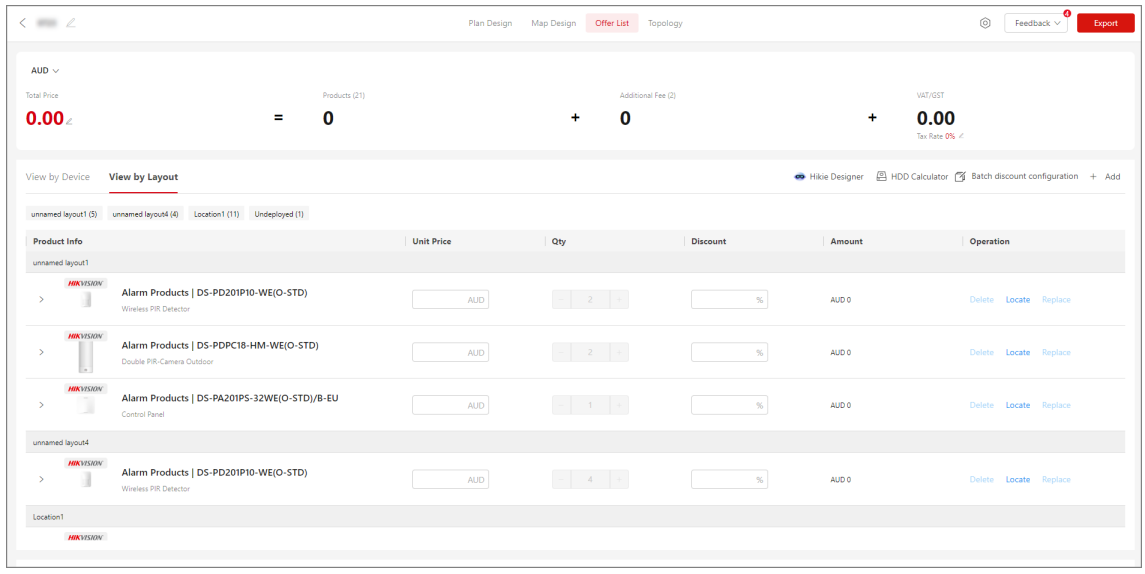


Figure 2-50 View by Layout

Table 2-10 Row Actions

Action	Effect
Delete	Removes the product from the quotation.
Locate	Jumps to the device on its layout or map — use it to find where an unexpected item came from.
Replace	Swaps the model while keeping the position and settings.

Batch discount configuration applies a discount across the list in one operation, rather than row by row.

Click **Add** to add more additional fees.

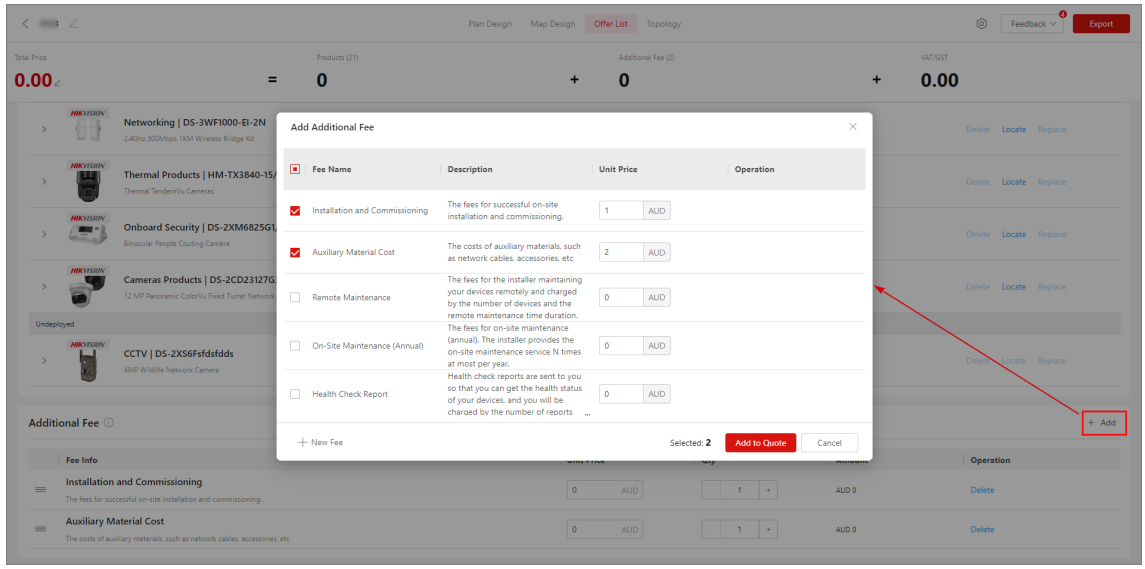


Figure 2-51 Additional Fees

Size the Storage: HDD Calculator

Click **HDD Calculator** in the Offer List toolbar to size recording storage for the project.

1. Build the camera list: **Select from Library** pulls in cameras already in the Hikvision product library, **Custom Camera** adds one by hand.
2. For each row set **Type**, **Count**, **Resolution**, **Codec**, **FPS**, and whether **Guanlan AI Encoding** is enabled.

3. Set **Hours Per Day Recording** with the slider. 24 hours for continuous recording, less for event-driven or scheduled recording.
4. The calculator returns **Total Bandwidth** in Mbps and a **Storage Requirements** table giving the retention achieved by each disk capacity from 0.5 TB to 24 TB, with the most commonly specified size flagged.

Note

The result is an estimate. Actual consumption varies with scene complexity and lighting, because variable-bitrate encoding produces more data from busy, poorly lit scenes than from static, well-lit ones. Size for the retention the customer contracted, not the minimum the table allows.

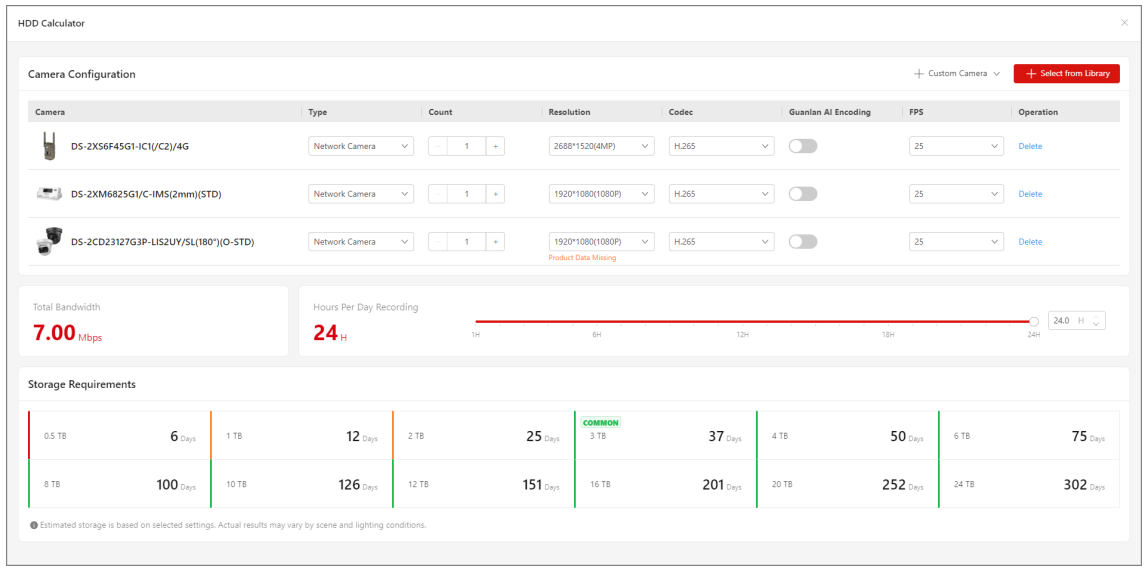


Figure 2-52 HDD Calculator

Topology

Open **Topology** in the top navigation bar. Two diagrams are generated from the design:

- **Topology**: How the devices connect. You can edit the topology and adjust the nodes.
- **System Diagram**: The system architecture view. You cannot edit.

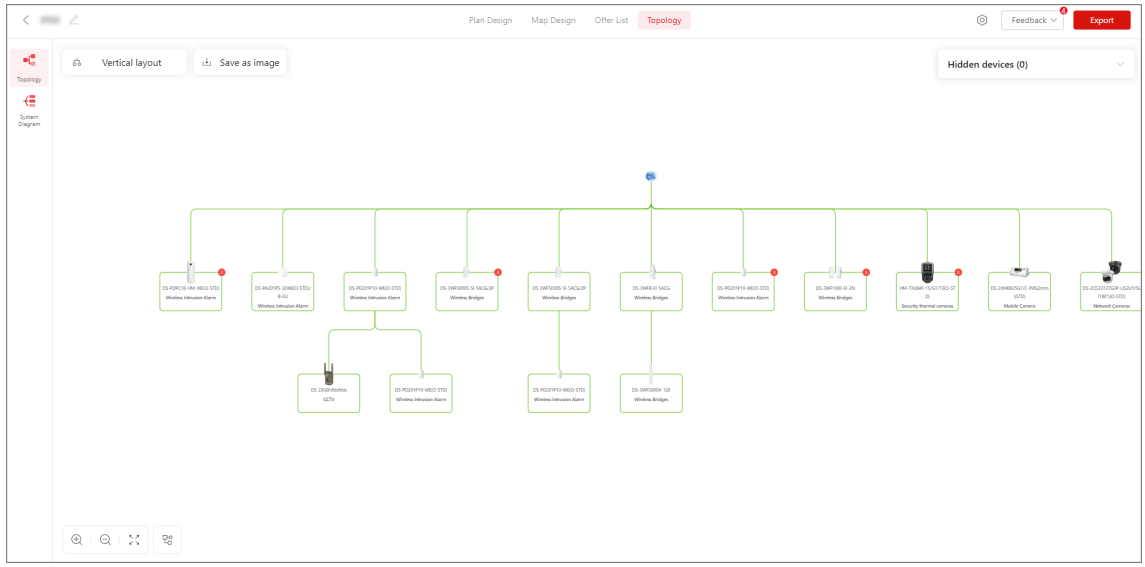


Figure 2-53 Topology

Table 2-11 Available Actions

Control	Purpose
Vertical layout / Horizontal layout	Re-flows the diagram vertically/horizontally.
Drag a node	Repositions it; connections follow.
Hide a node	Right-click a node card, and then click .
Hidden devices	Lists devices excluded from the diagram, and restores them. You can drag a hidden device to the topology to show it again.
Save as image	Exports the diagram.

Export Quotation and Design Report

Preview and export design and quotation reports.

1. Click **Export** to open **Export Preview**, then choose what the document contains. Every item is individually selectable:

Group	Contents
Recipient Info	Customer Name (required), Email, Phone, Address, Delivery Date, Note
Product List	Product List, Additional Fee
Topology	Topology, System Diagram

Group	Contents
Design Drawing	Point Layout, CCTV Coverage Map, Wi-Fi Heatmap (2.4G), Wi-Fi Heatmap (5G), Radar Coverage Map, Alarm Coverage Map, Cable Routing
Outdoor Design	Point Layout, CCTV Coverage Map, Radar Coverage Map, Thermal Coverage Map, Bridge Heatmap (2.4G), Bridge Heatmap (5G), Bridge Installation

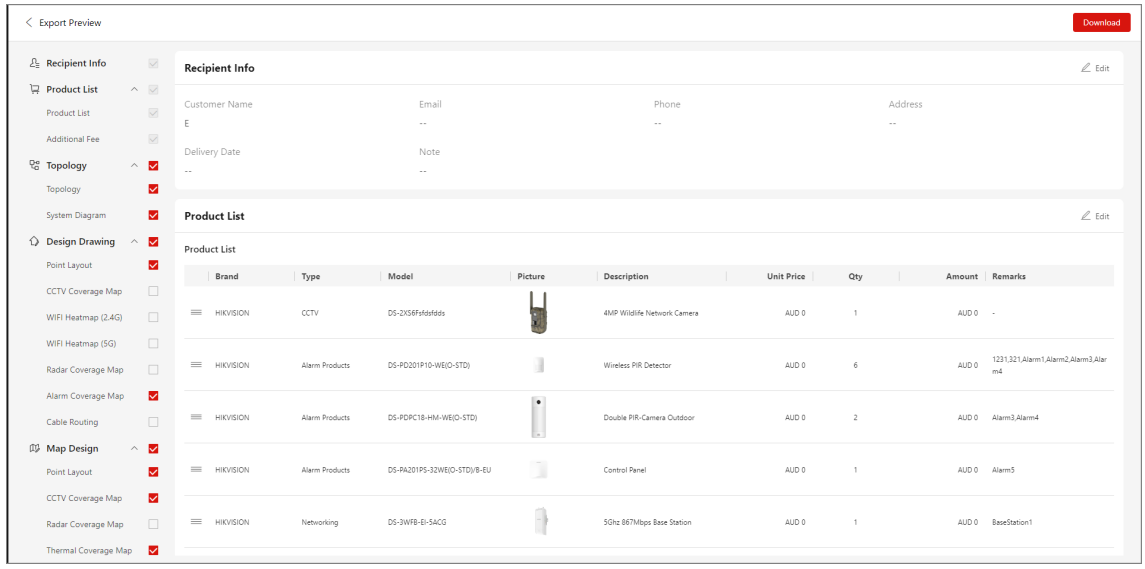


Figure 2-54 Export Preview

2. Click **Download**, and set the export format and custom options (whether to include product pictures, product model name, product parameters, cover and back cover). Click **Download** again.
3. The exported document contains **Full product specifications** for every model in the design: the datasheet content, so the customer does not need separate brochures.

Note

This is exported only if you select **Product Parameters** when downloading.

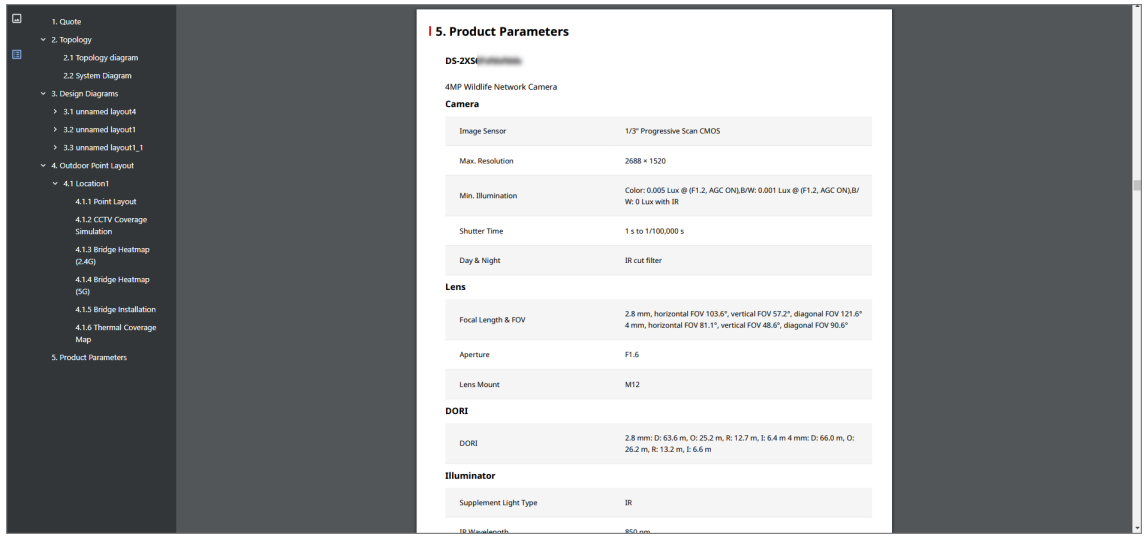


Figure 2-55 Exported

2.2.7 Hikie Designer

Hikie Designer is available from the right-hand toolbar in the indoor design canvas and from the **Offer List** toolbar. It works in natural language: describe what you need rather than navigating the catalog.

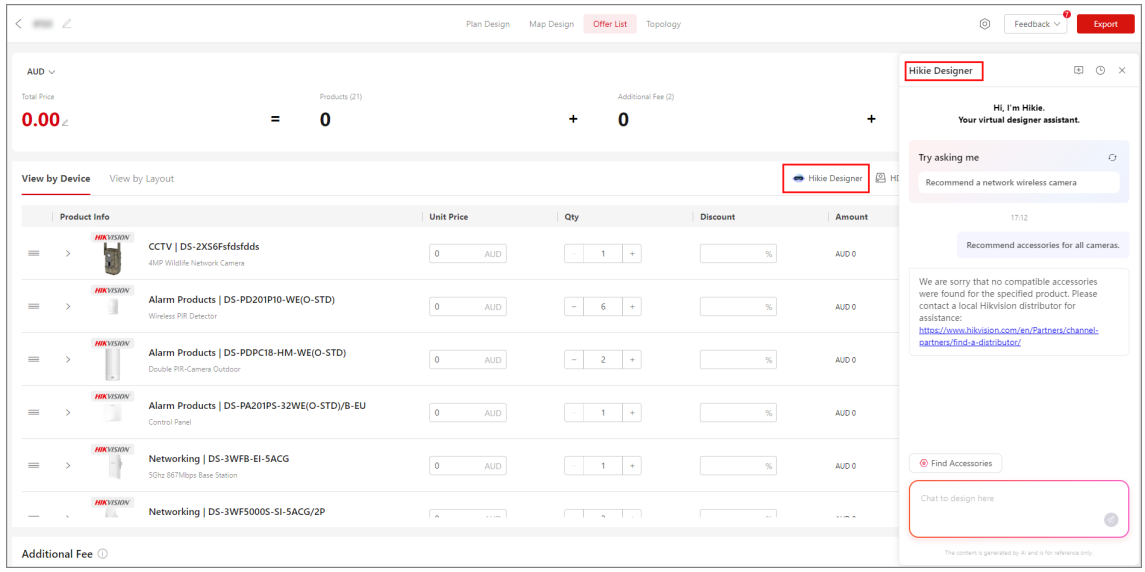


Figure 2-56 Hikie Designer on Offer List

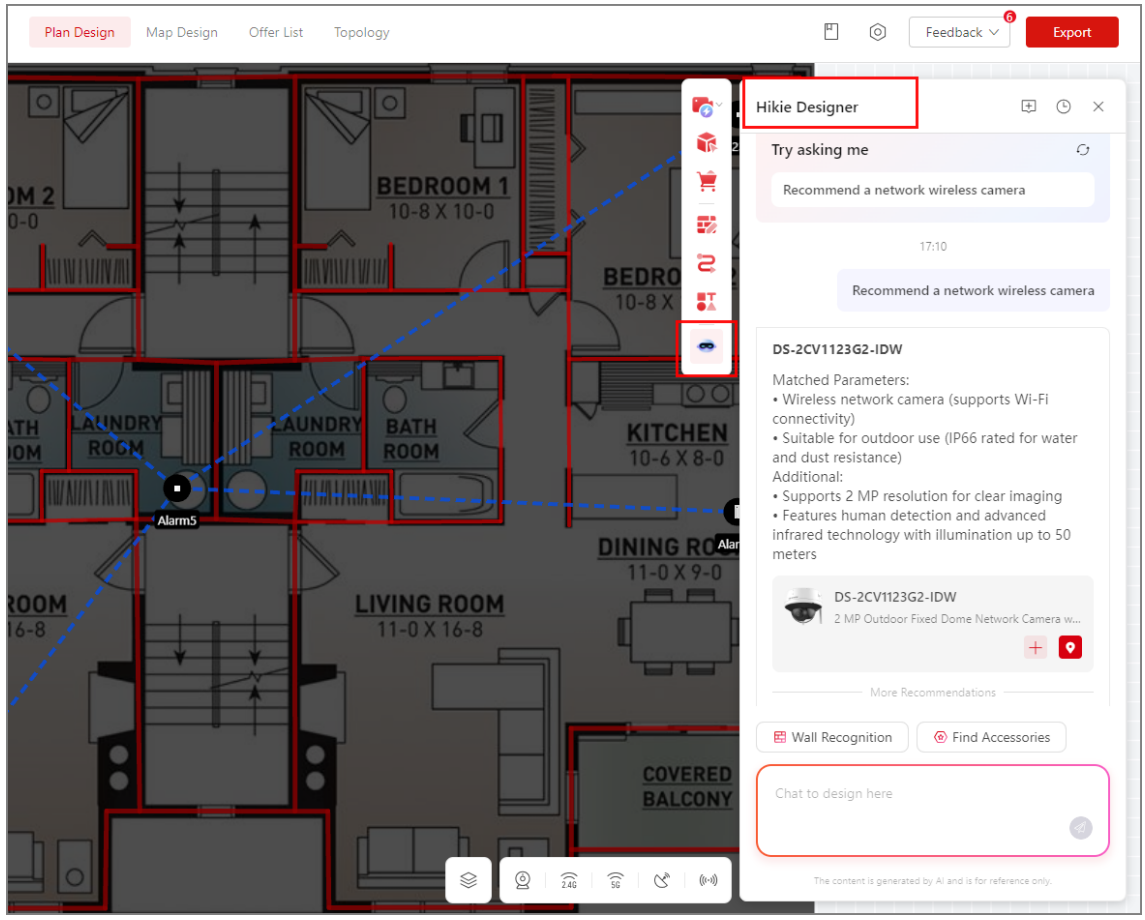


Figure 2-57 Hikie Designer on Indoor Design

Table 2-12 What It Can Do

Task	Example
Recommend products	Enter *"Recommend a network wireless camera"*.
Recommend accessories	Click **Find Accessories**: brackets, mounts and power supplies for the devices already in the design.
Trigger wall recognition	Click **Wall Recognition**.

Each recommendation is returned as a card with the model, its description and the specification points behind the recommendation. Actions are attached to every card:

- **+**: Add the product to the quotation.
- **Location pin**: Place the product directly on the current layout.
- **Add All to Quote** adds every recommendation at once, and **More Recommendations** requests alternatives.

Note

Recommendations are generated by AI and are for reference. Verify the model against the project requirements before quoting it.

2.2.8 Global Settings and Templates

Open **Global Settings** with the gear icon in the top navigation bar. These settings control how the design is displayed and how some quantities are calculated. They apply across the project, not to a single device.

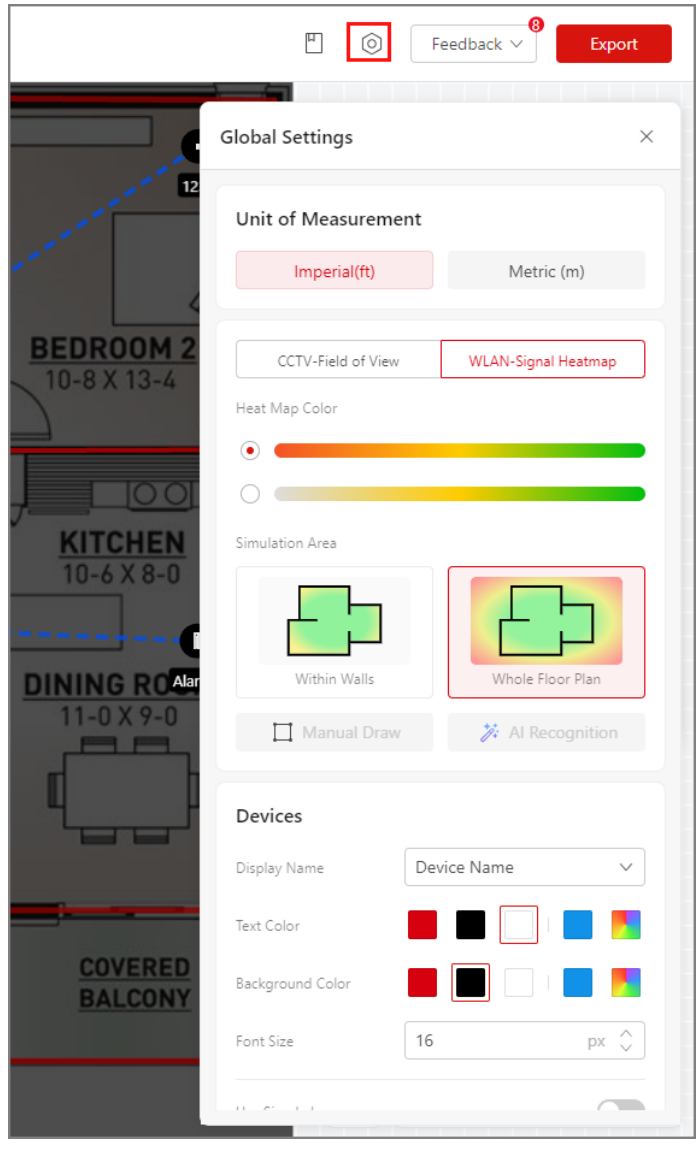


Figure 2-58 Global Settings

Group	Setting	Notes
Unit of Measurement	Imperial (ft) / Metric (m)	Applies to every dimension, including the exported report.
CCTV — Field of View	Show PPM/PPF Zones	The zone for PPM/PPF simulation.
	Show Camera Blind Spots	The dead zone beneath the camera.
	Show DORI	DORI banding, with a choice of two color schemes, and you can customize a color scheme.
WLAN — Signal Heatmap	Heatmap display options	Heatmap color and simulaiton area.
Devices	Display Name, Text Color, Background Color, Font Size	Device labeling on the canvas.
	Use Simple Icons, Background Color, Icon Size	Reduce visual clutter on dense layouts.
Walls	Unify Display Style	Draws all walls in one style regardless of class.
Cables	**Redundancy Factor**	Default **1.5**. Multiplies drawn cable length to give the quoted quantity.
	Customize Cable Color	Per-type cable colors.

Save Settings stores the current configuration as a named template. **Load Settings** applies a saved template: your own, or **Default Settings**.

2.3 How to Create Product Quotations

You can create, send, and manage quotes for your customers. You can add Hikvision products, products of other brands, and additional services to the quotes for your customers, and the created quotes can be sent to your customers in the format of PDF or Excel, which increases your professionalism.

2.3.1 Create Products Quote for Customer Using the Portal

1. Enter the My Quote for Customer page.
   - Go to **My Hik-Partner → Order → My Quote for Customer** .
   - Go to **Support → Tools → My Quote for Customer** .
   - Go to **Home → Tools → My Quote for Customer** .

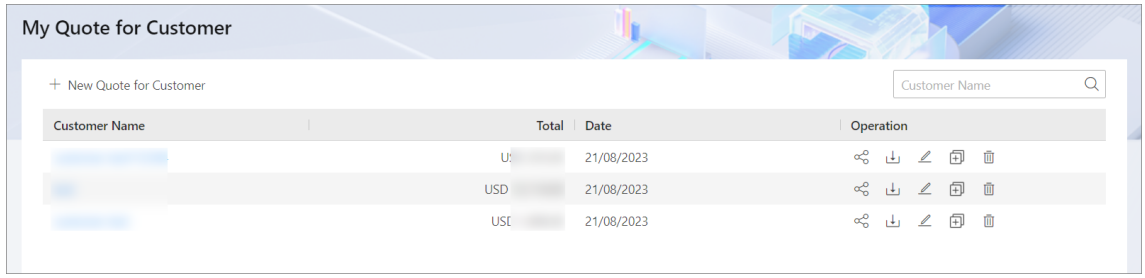


Figure 2-59 My Quote for Customer

2. Click **New Quote for Customer**.
3. In the Product area, select products.
   a. Tap in the upper-right corner to set the currency unit.
   b. Click **My Usual Products**.
   c. Select products in the list.
   d. Click **Add Product** in the upper-left corner, enter the product information such as model and brand to add more products to My Usual Products.
   e. Click **Add to Quote**.
4. In the Additional Fee area, add additional fees.
   a. Click **Add Additional Fee** to select the additional fees.
   b. Click **Add** in the upper-left corner to add other additional fee types.
   c. Click **Add to Quote**.
   d. The selected additional fees and their sub total are displayed in the list.
5. In the Recipient area, enter the customer name and other optional information such as email and phone.
6. In the My Info area, set your contact name and other optional information such as email and phone.

Note

You can also click **Bank Info** to set your bank information.

7. Enter the notes, delivery date, etc.
8. Click **Save** to save the above settings or click **Save & Send Quote** to save the settings and send quote to the customer.
9. Perform further operations.

Operation	Instruction
Search for Quotes	Enter keywords of customer name in the search box to search for quotes.
View Quote Details	Click a quote to view its details such as customer name and products.

Operation	Instruction
Edit Quote	Click in the Operation column to edit the quote. On the Quote Details page, click **Edit** in the down-right corner to edit the quote.
Delete Quote	Click in the Operation column to delete the quote. On the Quote Details page, click **Delete** in the down-right corner to delete the quote.
Duplicate Quote	Click in the Operation column to duplicate the quote. On the Quote Details page, click **Duplicate** in the down-right corner to duplicate the quote.
Share Quote	Click in the Operation column, select a template, and click **Send** to share the quote with others or click **Download** to download the quote template. On the Quote Details page, click **Share** in the down-right corner, select a template, and click **Send** to share the quote with others or click **Download** to download the quote template.

2.3.2 Create Products Quote for Customer Using the Mobile Client

1. Enter the My Quote for Customer page.
   - Tap **Home → Quotation → New Quotation for Customer** .
   - Tap **Home → More → Tools → Quotation → New Quotation for Customer** .
2. Tap in the upper-right corner to set the currency unit.
3. Enter the customer name.

   Note

   Tap **More Info** to set more information such as email and phone for the customer.
4. Select products.
   a. Tap **Select Product**.
   b. Select products from my usual products.
   c. Tap **Add Product** in the upper-right corner, enter the product information such as model and brand to add more products to My Usual Products.
   d. Tap **Add to Quote**.
5. Add additional fees.

a. In the Fee Name area, tap **Select** to select the additional fees.
b. Tap + in the upper-right corner to add other additional fee types.
c. Tap **Confirm and Return**.
d. The selected additional fees and their sub total are displayed in the list.

6. Enter the discount, tax, notes, and the delivery date.
7. Set your contact name.

Note

Tap **More Info** to set your email, phone number, etc. Tap **Bank Info** to set your bank information.

8. Tap **Save**.
9. Perform further operations.

Operation	Instruction
Search for Quotes	Enter keywords of customer name in the search box to search for quotes.
View Quote Details	Tap a quote to view its details such as customer name and products.
Edit Quote	Tap ··· → **Edit** to edit the quote. On the Quote Details page, tap ✎ to edit the quote.
Delete Quote	Tap ··· → **Delete** to delete the quote. On the Quote Details page, tap 🗑 to delete the quote.
Duplicate Quote	Tap ··· → **Duplicate** to duplicate the quote.
Share Quote	Tap ⋖ , select a template, and tap **Share** to share the quote with others. On the Quote Details page, tap **Share** to share the quote with others.

2.4 How to Create and Manage Project

After you register your projects on Hik-Partner Pro, you can not only receive special pricing on essential components, but also receive technical support for your projects.

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

2.4.1 Create a Project

Projects can be created by distributors or system integrators/installers. A project contains project information, information about who creates the project, end user information, support information, product information, and project document.

Create a Project Using the Portal

Steps

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

1. Click **Project** on the top of the page after login.
2. Click **New Project**.
3. Fill in the blanks.
   - If you are a distributor, enter project information, system integrator / installer information, end user information, support information, and product selection. Then upload the project document if there is any.
   - If you are a system integrator / installer, enter project information, distributor information, end user information, support type, support information, and product selection. Then upload the project document if there is any.

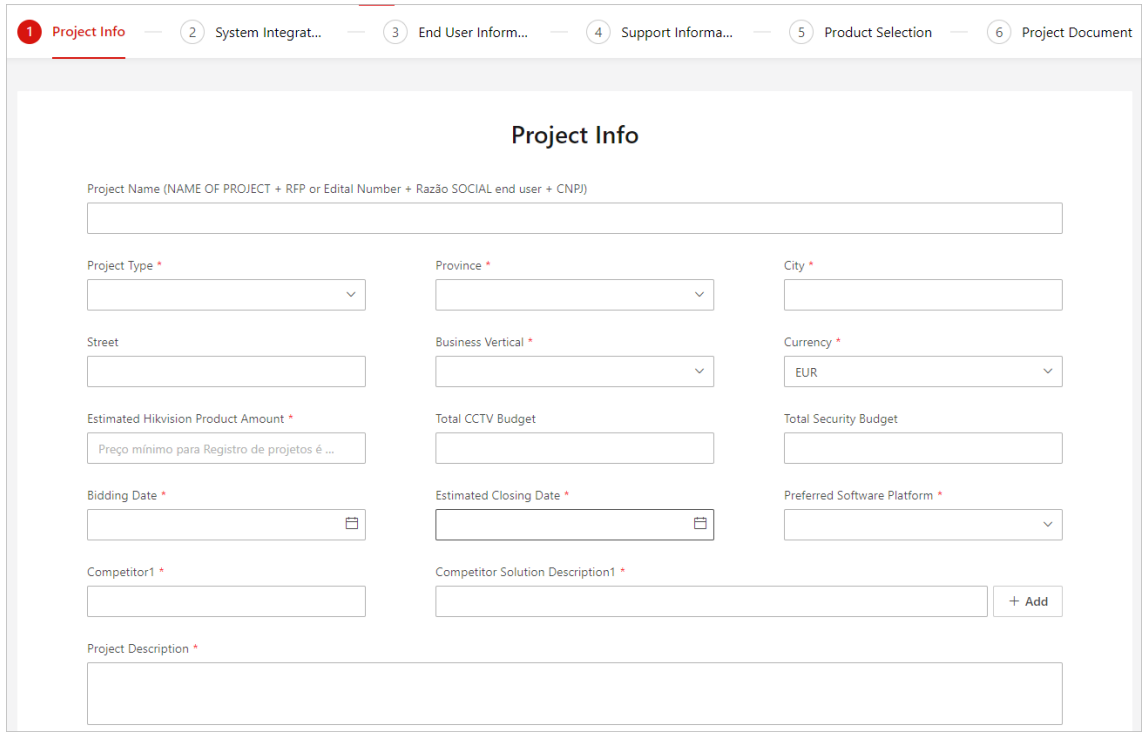


Figure 2-60 Add Project

Note

- For product selection, click **Add** → , select products and click **Confirm**.
- When you select products, you can click to compare products. For details about comparing products, refer to ***Compare Products*** .

4. Click **Save & Submit**.

   The project will be displayed on the Project History page, and the **Status** will be **Waiting for supporter**.

What to do next

For further operations, refer to ***View Project History*** .

2.4.2 Compare Products

When you select products, you can add multiple products and compare them with their same specifications hidden. In this way, different specifications will be directly displayed and you can choose products as needed.

Note

Only products of the same category and subcategory can be compared.

Compare Products Using the Portal

Click **Project → New Project** , and in the Product Selection part, click ⓥS to start compare products. You can also click VS at the right bottom, and add products to compare them.
To start to compare products, select at least two but no more than four products from the comparison list. On the comparison result page, fields that are different are highlighted with a background color. You can switch on **Hide the Same** on the top left to hide parts that are the same and focus only on the differences.

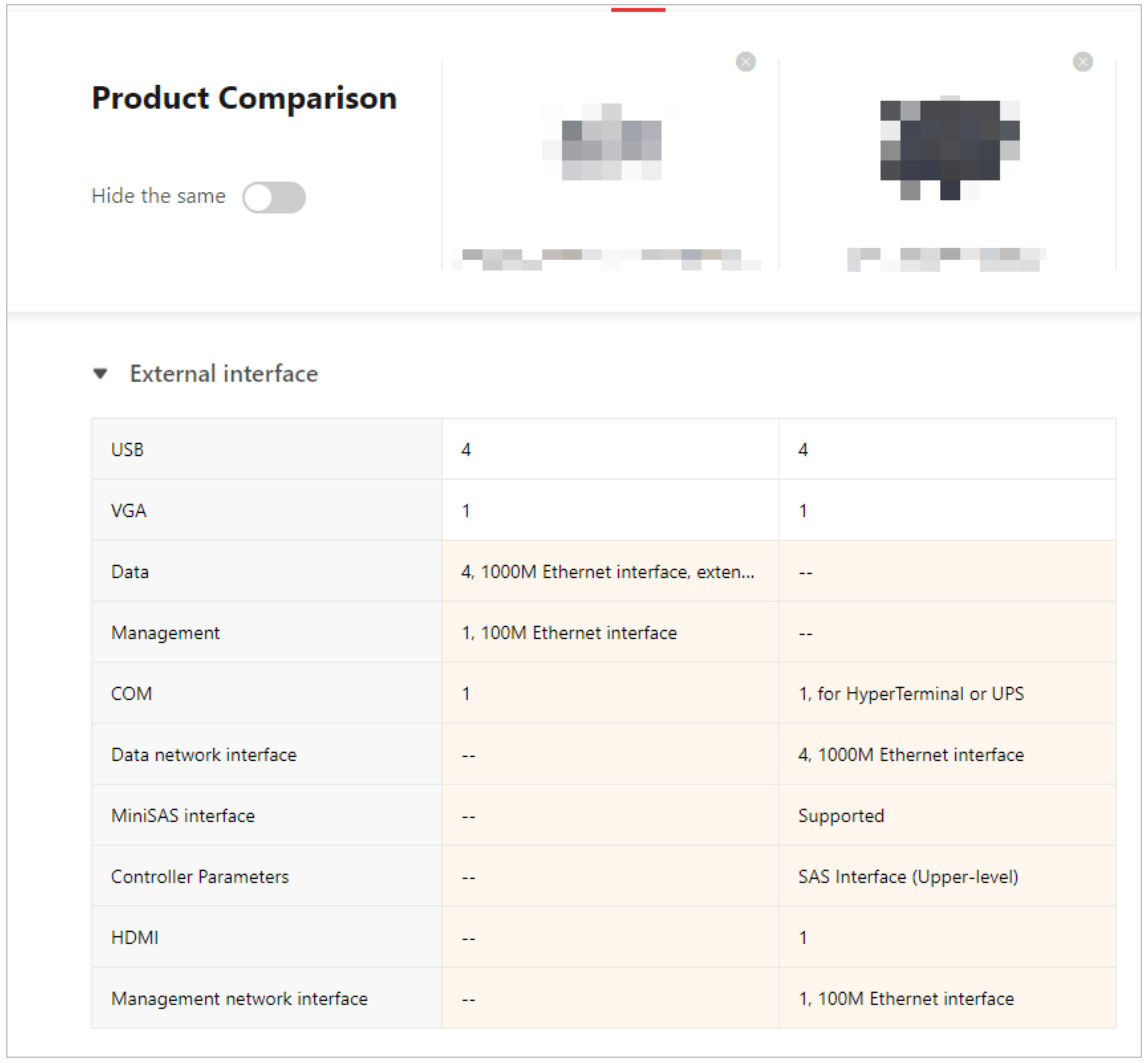


Figure 2-61 Compare Products

2.4.3 View Project History

You can view all projects on the Project History page. You can check the information and perform further operations.

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

View Project History Using the Portal

Click **Project** on the top of the page after login.

For Distributors

There are three tabs **All**, **Project Supported by Hikvision**, and **Project Supported by Me**.

All

All projects will be displayed under this tab. FW means the project is forwarded to you. S means the project is shared to you. For shared projects, you can only check the information but not quote.

Project Supported by Hikvision

It includes projects submitted by you and projects shared to you.

Project Supported by Me

It includes projects forwarded to you. You can click **Go to Quote**, enter distributor prices, and click **Save&Send Quote to Customer** to generate a quote and send it to the customer.

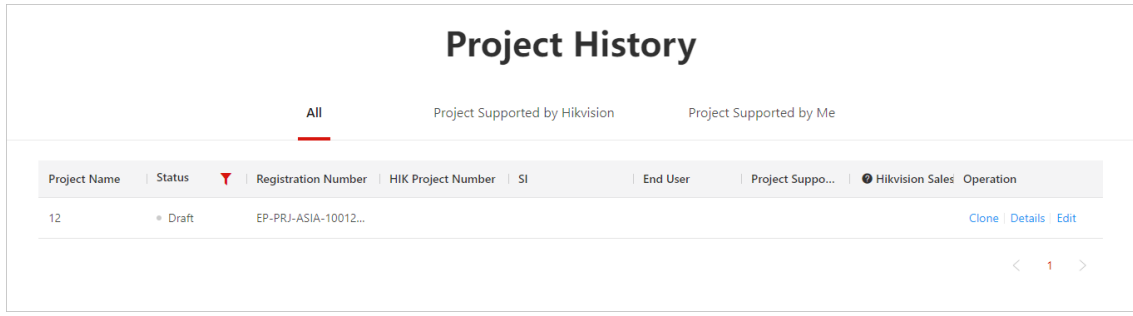


Figure 2-62 Project History for Distributors

For System Integrators / Installers

You can view all projects that you created. In the Operation column, you can click **Quote** and click the document in the Download column of the pop-up window to check the quote list.

Further Operations

Operations	Description
Filter Projects by Status	Click in the Status column to filter projects by their status. Here are some project status types. • Draft: The project is only saved but not submitted. • Waiting for supporter: The project is submitted but not yet processed. • Processing: The project is currently being processed by Hikvision. • Approved: It is only available in some countries and regions. It suggests that the project be approved. • More Info Required: Hikvision needs more information to decide whether to approve the project. • Ineligible: The project is rejected by Hikvision. You can check the comments for why the project is rejected.
Close Project	Click **Close Project** and select among **Close Won**, **Close Lost**, and **Closed Canceled**. • Closed Won: It means the project is closed won, and you can enter Closed Won Amount and upload Purchase Order Document to accept the quote and close the project. • Closed Lost: It means the quote of the project is rejected, and you can select reasons, enter comments and close the project. • Closed Canceled: It means the project is canceled and closed, and you can select reasons, enter comments and close the project.
Copy Project	Click **Copy** to copy the project.
Edit Project	If the status turns to More Info Required or the project is only saved but not submitted, you can click **Edit** to edit the project.
View Details	Click **Details** to view the project details.

2.5 How to Place Orders for Products

The Order & Promotion module supports viewing information of regular products, hot products, and promotional products that are discounted or are put on clearance. You can search for and select products to place an order or submit your product order by uploading a predefined template.

2.5.1 Create an Order Using the Portal

You can place an order by adding products to the shopping cart, selecting the products you need for checkout, and entering the required shipping information.

Note

Besides adding products to the shopping cart, you can also submit an order by uploading information (material code, quantity, etc.) of products with a predefined template via **Order Upload**.

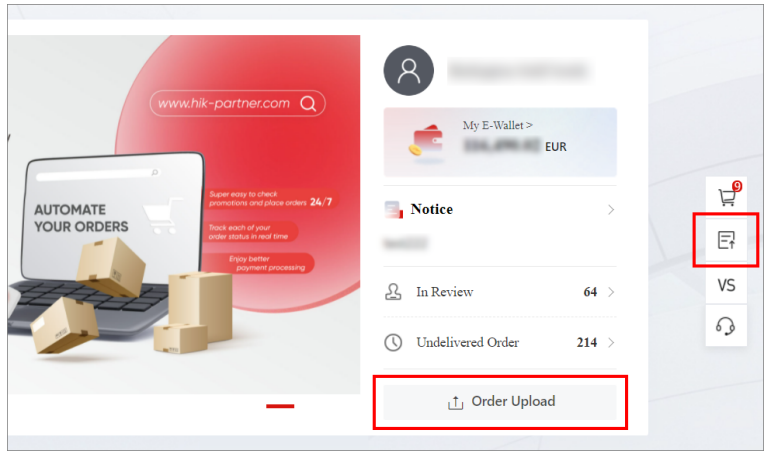


Figure 2-63 Ways for Accessing Order Upload

1. View or search for the products to be ordered.
2. Hover over a product of interest, set the quantity to be ordered, and click **Add to Cart**. Repeat this step to add multiple products to your shopping cart as needed.
3. Click on the right to go to your shopping cart.
4. Select the products to be ordered, adjust the quantity for each product if needed, and click **Next**.
5. On the Check Order Information page, enter your shipping/billing address, select a preferred shipping method, and confirm the order details (quantity to be ordered, total cost, etc.).

Note

- You can also set a preferred future date of delivery and upload a project register form if needed.
- If you have entered a shipping/billing address before, check whether the address information displayed on the page is correct.

6. Click **Submit**.

2.5.2 View My Orders Using the Portal

After submitting an order, you can track the status of your order, perform operations such as canceling or reordering as needed, and view related information such as invoices, transaction records, and logistics.

The following order related information can be accessed via **My Hik-Partner → Order** .

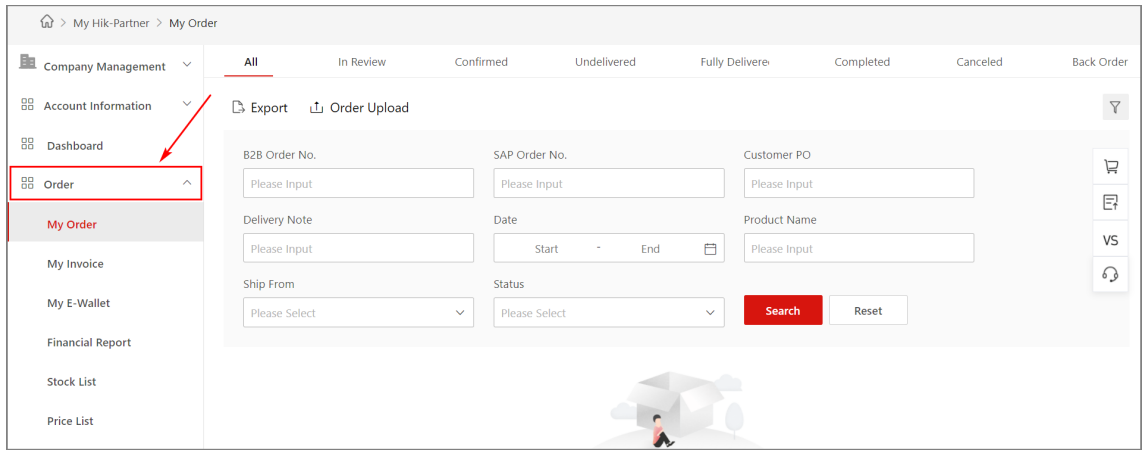


Figure 2-64 Order Related Information of Your Company

My Order Page

On the My Order page, you can view your orders by different status (e.g., In Review, Confirmed, Fully Delivered, etc.) and click an order to view the order details, including the products selected, total cost, and shipping related information.

Note

The My Order page can also be accessed via the In Review and Undelivered Order tabs displayed on the B2B page of the Order & Promotion module.

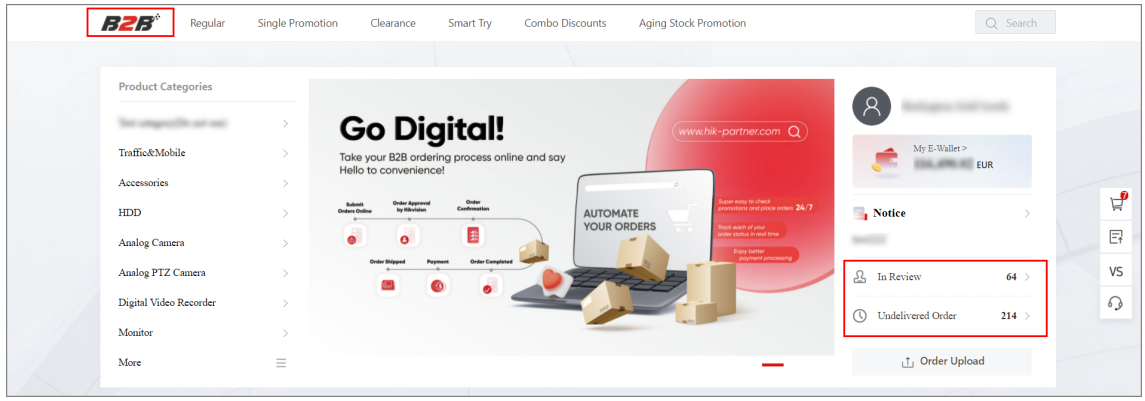


Figure 2-65 Another Way for Accessing the My Order Page

If needed, you can click **Export** to export the list of orders to your local PC, click **Order Upload** to submit an order using a predefined template, click next to an order No. to copy the order No., or click to reorder the same products of an order. To cancel ordering a product, click an order to enter the order details page, and click **Cancel** next to the product.

Note

The ordering of products that are fully delivered or the stock clearance / combo discount products are not allowed to be canceled.

My Logistics

On the My Logistics page, you can search for and view the logistics information (shipping-related) about international trade orders according to actual needs, and save the time of offline consultation and communication.

Note

The logistics information of the recent half a year is displayed.

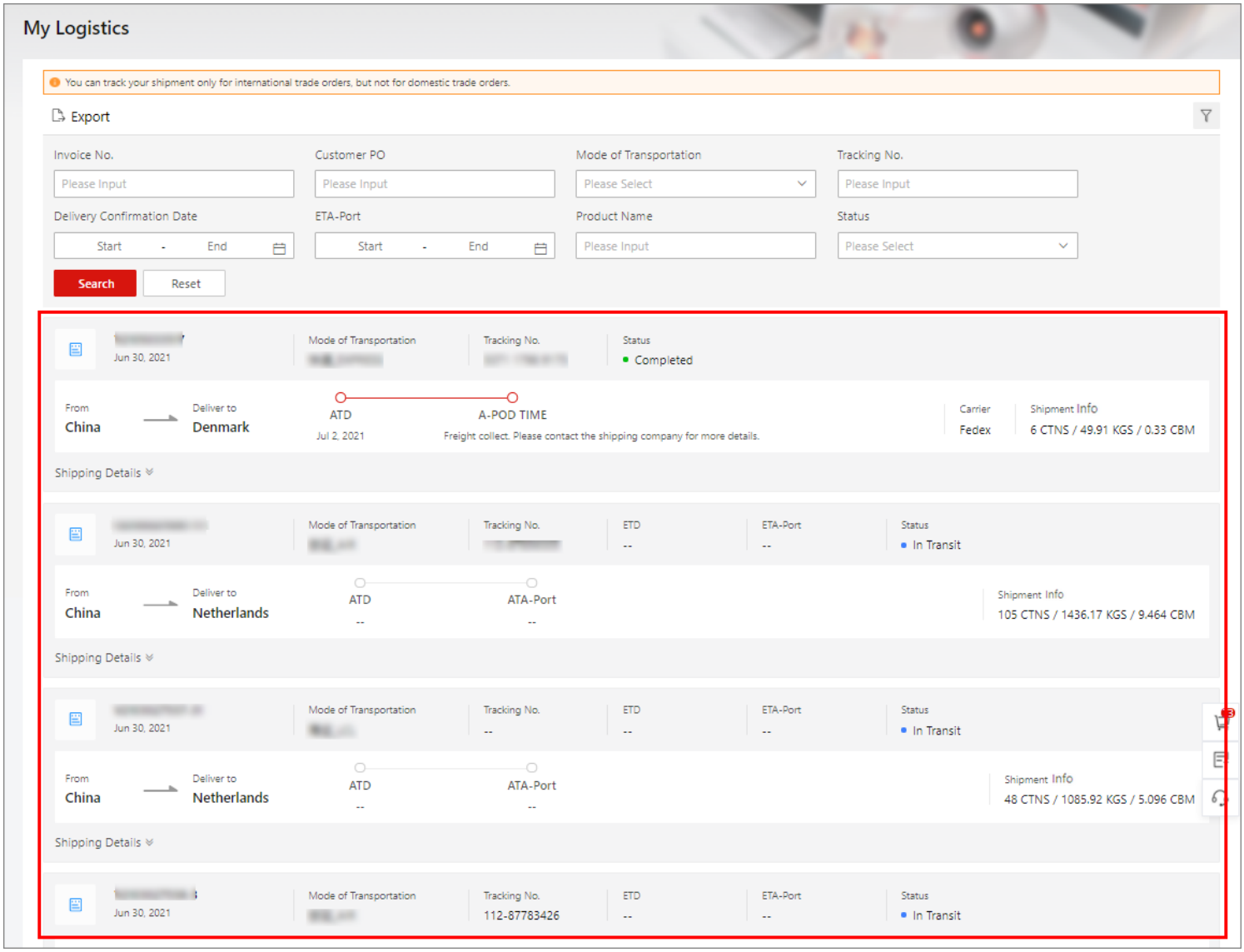


Figure 2-66 My Logistics Page

You can perform the following operations on this page if needed.

- You can set the conditions such as the invoice number and mode of transportation to search for your needed logistics information, including the carrier, places of departure and delivery, ATD (actual time of departure), ATA-Port (actual time of arrival to the port), and A-POD TIME (actual proof of delivery time), etc.
- You can click **Shipping Details** to expand and view the shipping details such as the product name and quantity.

Note

By default, 6 delivery notes are displayed. You can click **More** to view delivery notes of all products.

- You can click **Export** to export all or searched logistics information to the local PC.

My Invoice Page

On the My Invoice page, you can search for and view invoices of your past orders and export the list of invoices if needed.

My E-Wallet Page

On the My E-Wallet page, you can view your E-Wallet balance and transaction records, and search for specific records as needed.

Note

- If the type of a record is "Compensation", the number displayed is the amount you received when the corresponding compensation application is approved.
- You can also click the E-Wallet balance displayed on the B2B page of the Order & Promotion module to access your E-Wallet.

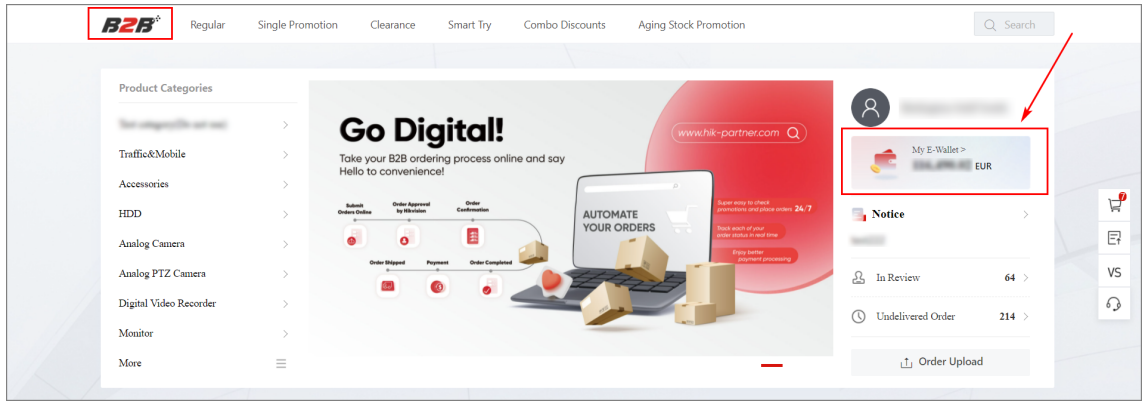


Figure 2-67 Another Way for Accessing the My E-Wallet Page

Financial Report Page

On the Financial Report page, you can view details of your credit status, account payable balance, and basic information of the invoices.

Stock List Page

On the Stock List page, you can view and search for stock related information of your products and export the full stock list or specific search results to the local PC as needed.

Price List Page

On the Price List page, you can view and search for price related information of all products and export the full price list or specific search results to the local PC as needed.

2.5.3 Set Availability Alert and Manage My Waiting List Using the Portal

You can set availability alert for products currently out of stock, follow them on the My Waiting List page, and get notified when they arrive.

Set Availability Alert

On the product list page and product details page, you can set availability alerts for products which are out of stock.
Click **Availability Alert**, set your desired quantity, and click **Confirm**.
After that, the products will be added to My Waiting List, and you will be notified by emails when the products arrive.

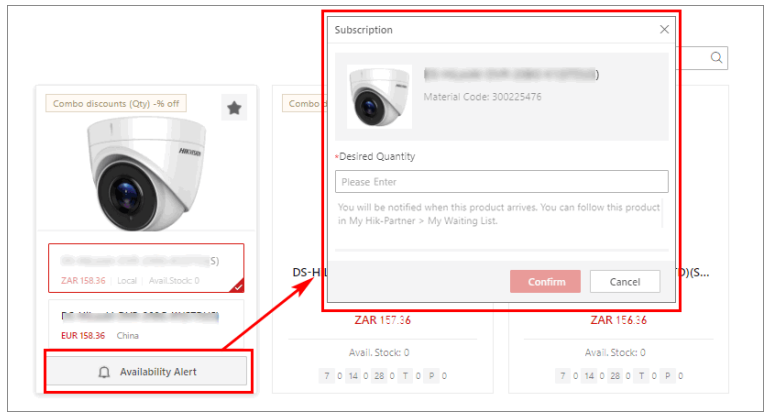


Figure 2-68 Set Availability Alert

Manage My Waiting List

Go to **My Hik-Partner → Account Information → My Waiting List** to enter the My Waiting List page, and you can view the product information in My Waiting List, including the product model, material code, account that added it, desired quantity, modified date, etc.

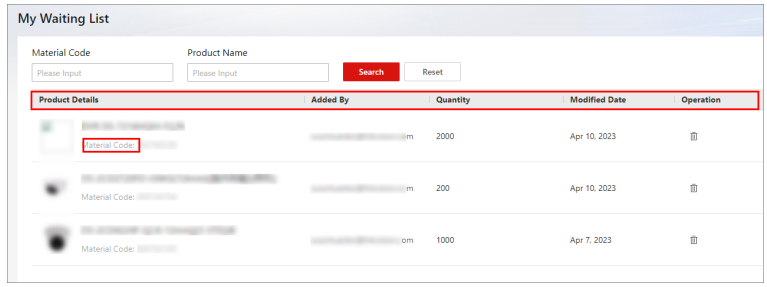


Figure 2-69 My Waiting List

The following operations are supported on this page.

- You can set the conditions including material code and product name to search for the product(s) in My Waiting List.
- Move the mouse cursor to the Quantity column, and you can click to edit the product quantity you demand.
- You can click in the Operation column to delete a product from My Waiting List. It the product is deleted, you will not be notified when the product arrives.

2.5.4 Manage Hikvision Quote for Me Using the Portal

Note

This function is only available to some countries/regions.

Go to **My Hik-Partner → Order → Hikvision Quote for Me** .

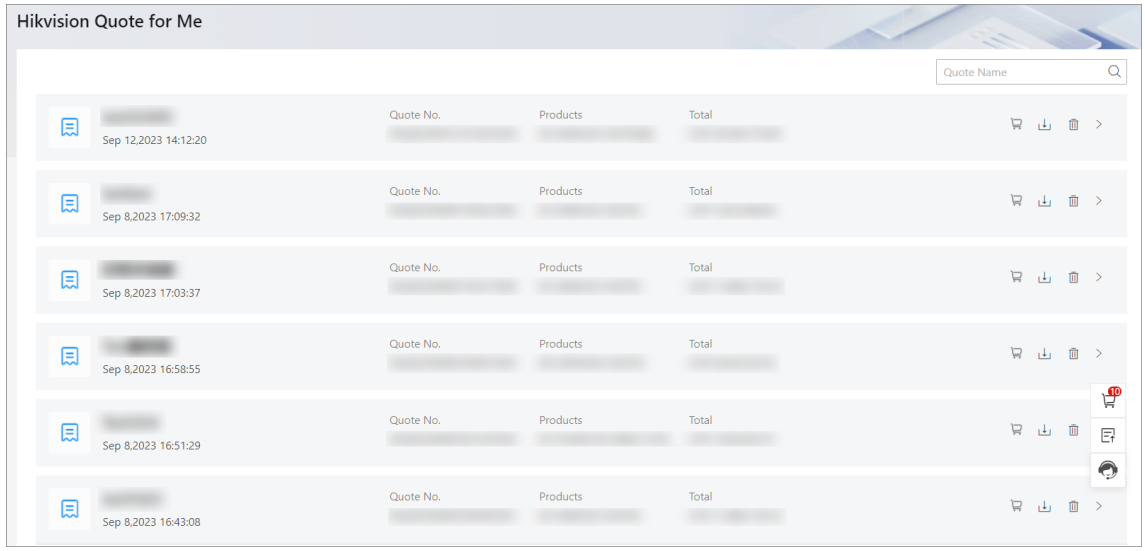


Figure 2-70 Manage Hikvision Quote for Me

Perform the following operations as needed.

Description	Operation
View Quote Details	Click › to view the quote details. In the down-right corner, you can click **Download** to download the quote, and click **Buy Online** to buy the related products listed in the quote.
Buy Products Online	Click to check quote details and click **Buy Online** to buy the related products listed in the quote.
Download Quote	Click to download the quote to local PC.
Delete Quote	Click to delete the quote.
Search for Quote	Enter keywords in the search box in the upper-right corner to search for the quote.

Chapter 3 Set Up & Deliver Security System and Connect with Your Customers

3.1 Quick Initialize Devices on Site and Add to HPP for Remote Maintenance

Table 3-1 Possible Steps for Quick Initialization and Device Adding

Step	Related Topics
1. Initialize the Network	***Quick Initialize Network with AC Router and APs***
2. Quick Initialize the Devices	***Use the SADP Tool to Quick Initialize LAN Devices*** (Except Security Control Panels)
3. (Optional) Add Devices	• ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** • ***Quick Add & Install Securtiy Control Panel (AX HOME) and Peripherals & Detectors***

3.1.1 Quick Initialize Network with AC Router and APs

The AC router can effectively communicate with the APs and easily configure and manage the entire network. With Hik-Partner Pro, you can activate the AC router and network switches on the same LAN together and configure the network settings.

Before You Start

- Connect and power on your AC router, APs, and network switches.
- Only the network switches on the same LAN as the AC router's can be activated together with the AC router (usually connected to the LAN port of the AC router).

Steps

1. Connect to the network devices.
   1) **Optional:** In **Add Device Manually** mode, enter the serial number of the AC router.

   Note

   If the SADP tool detects the unactivated AC, you can also enter the initialization process of the AC router.

   2) Scan the QR code of the AC router, and bring your phone close to an AP.
   3) Tap **Join** to join the Wi-Fi network of the AP so that Hik-Partner Pro can find the AC router and switches.

2. Tap **Activate All** to activate the AC router and network switches by setting the device user name, password, and verification code.

Note

The verification code is set for only the network switches to enable the Hik-Connect service. The AC router does not need one to enable the service.

3. Configure the network by setting the network connection method and WAN mode.

DHCP

The AC router automatically obtains the IP assigned by the superior router to access the Internet.

PPPoE

PPPoE is also known as broadband mode. You enter the broadband account and password to allow the AC router to access the Internet.

Static IP

You manually set the IP to allow the AC to access the Internet. Static IP supports 4 parameters: IP, subnet mask, gateway, and DNS server. The default IP, gateway, and DNS server addresses are auto obtained from the AC router.

Multi WAN

Enable **Multi WAN** to set the network connection methods of multiple WAN ports. Each WAN port can be configured for an independent network connection type.

Note

Multi WAN is enabled by default if two or more WAN ports are connected to the cable. The number of supported WAN ports depends on the AC router capability.

4. Set the Wi-Fi network by setting the Wi-Fi name, password (optional), and frequency band.

Note

In situations where you are far away from the AP or there are many obstacles, the 2.4 GHz band may provide a more reliable connection. However, without these limitations, 5 GHz will likely to be a faster choice.

5. Add devices to a personal site.

Note

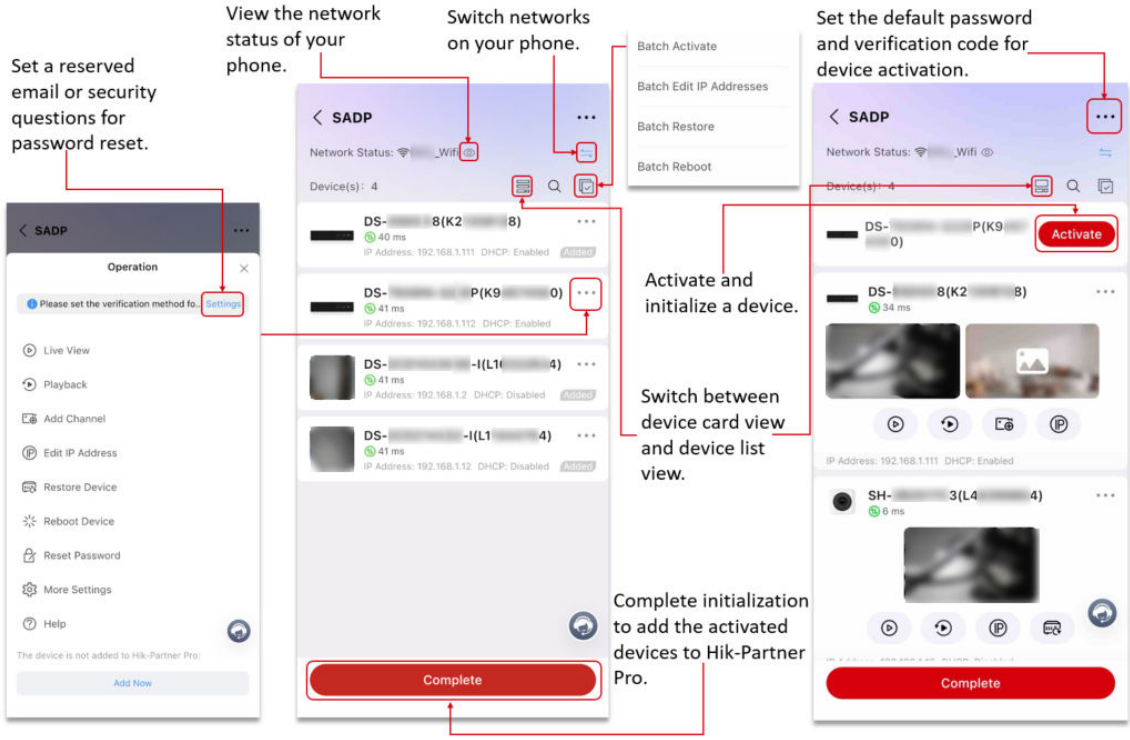
Adding the AC to a team site is not supported.

6. When the AC is added, tap **Auto Connect** to connect your phone to the new Wi-Fi you just configure, or copy the Wi-Fi name and password to manually join the Wi-Fi.

3.1.2 Use the SADP Tool to Quick Initialize LAN Devices

The SADP tool helps installers complete the activation and basic configurations of all LAN (local area network) devices, link network camera channels to the NVR, add devices to Hik-Partner Pro, and hand over the devices to customers. Most of these are done automatically and all are done smoothly, with just the Hik-Partner Pro Mobile Client, and no need for a computer or monitor, which greatly increases the installers' work efficiency.

SADP Tool Overview



Step 1: Prepare the Devices and Connect Your Phone to the LAN

To use the SADP tool on the Mobile Client, make sure the devices are powered on and connected to the LAN, and you should connect your phone to the same LAN as the devices' via Wi-Fi or adapter.

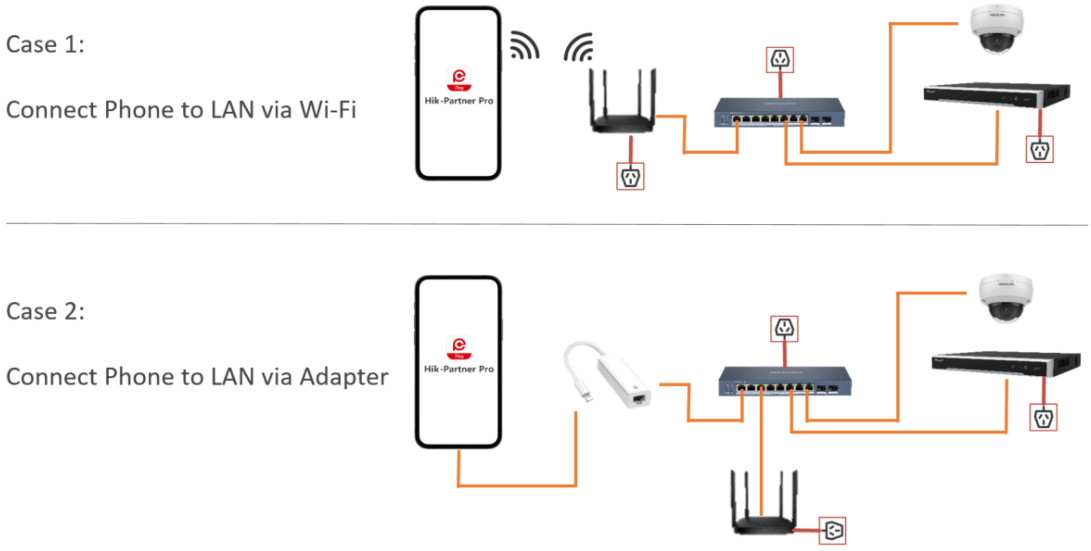


Figure 3-1 Prepare Devices

Step 2: Search for Devices on LAN

After you log in to the Hik-Partner Pro Mobile Client and when your phone is connected to the LAN, the SADP tool will search for LAN devices in the background automatically and constantly.

- The tool tests and displays the ping values and levels in real time. Higher ping means poorer connectivity between the device and your phone. When the ping is high, remote configuration, live view, and playback may fail. Icons of different colors indicate different ping levels:
  - : Less than 50 ms
    You can use the SADP tool to conduct device operations and configurations smoothly.
  - : 50 ms to 200 ms
    Some of your operations or configurations may fail.
  - : More than 200 ms
    The connection between the device and your phone is likely to fail.
- When the SADP tool detects unactivated devices (except for alarm devices) on the LAN, the window of unactivated devices will pop up.

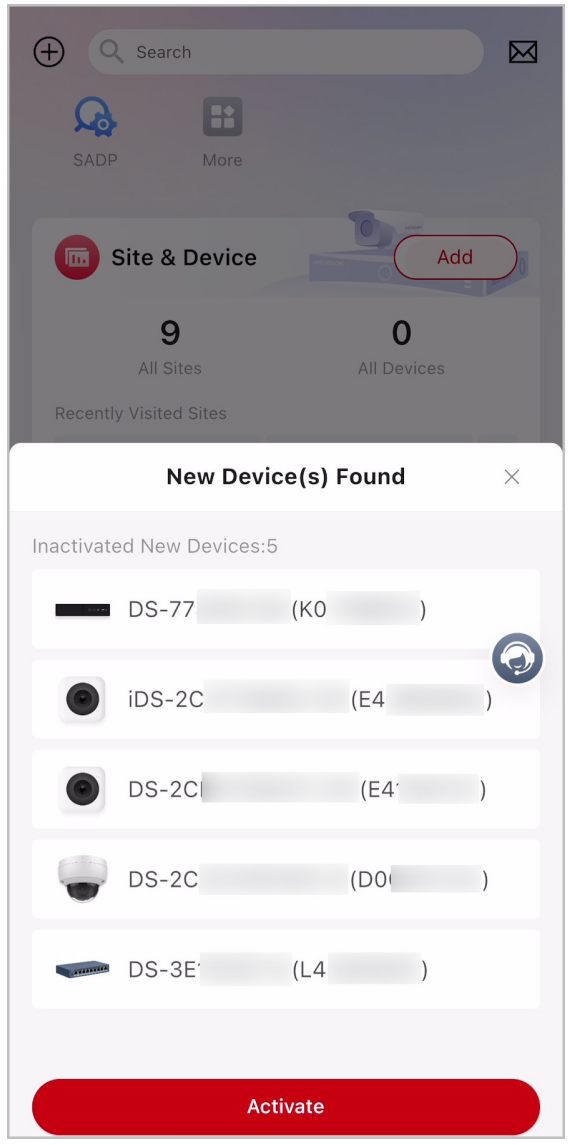


Figure 3-2 Pop-up Window of Unactivated Devices

Step 3: Initialize a Single Device or Batch Initialize Devices

You can use the SADP tool to initialize NVRs, network cameras (including PTZ cameras and thermal cameras), DVRs, access control devices, video intercom devices, Hik-ProConnect boxes, and network switches.

1. - Activate a single device: Tap **Activate** on the SADP page or the pop-up window of an unactivated device.
   - Batch activate devices: Tap → **Batch Activate** on the SADP page, select devices to activate, and tap **Next**. Or tap **Activate** on the pop-up window of the unactivated devices.
2. In the pop-up window, the default password and verification code (if any) will be filled in automatically. Otherwise, set both and you can choose to check **Set as Default Password and Verification Code**.
3. Tap **Next** to enter the Device Initialization page which includes the following automatic configurations:

Table 3-2 Configurations Automatically Done During the Initialization

Configurations	NVR	Network Cameras	Other Devices
Activate Device	√ The SADP tool checks for device batch issues during the activation.		
Configure Network	√ DHCP (dynamic host configuration protocol) is enabled automatically for the NVR so that IP addresses, gateway addresses, subnet masks, and DNS addresses can be assigned automatically to the NVR. Then, it performs ping tests to ensure accurate network settings for stable communication between your phone and the device.	√ For network cameras, DHCP is disabled automatically, in case IP address changes lead to the device going offline.	√ - For network switches (except for EI-series switches) and all DVRs, DHCP is enabled automatically. - For other devices, DHCP status will be synchronized from the default device settings. - After the IP address is set automatically, the tool performs ping tests to ensure accurate network settings for stable communication between your phone and the device
Check Firmware Update	√	√	√

Configurations	NVR	Network Cameras	Other Devices
Sync Device Time With Phone Time	√	√	√
Initialize HDD / SD Cards	√ The HDDs or SD cards will be initialized automatically if any and if they are new and not initialized. If there are data stored on the HDDs and SD cards, they will not be initialized.		
Others	/	Cameras can be auto added to the NVR. - **Motion Detection 2.0** is enabled automatically. All the area is set as the detection area, and **Notify Surveillance Center** is enabled. - The encoding format is set. If the device supports the Smart H.265+ encoding and the current format is the Smart H.264+ encoding, then the Smart H.265+ encoding is enabled automatically.	The Hik-Connect service will be automatically enabled if it is supported by the device.

4. Tap **Complete Initialization**. For NVRs, after the initialization completes, it will enter the channel-adding process, the channel-sorting process, and then the device-adding process. (If the device is a PoE NVR and the PoE channels are enabled by default, it will directly enter the device adding process.)

(Optional) Step 4: Configure and Manage NVR / DVR / Network Camera Channels Using the SADP Tool

The SADP tool allows you to configure and manage channels of NVRs, DVRs, and network cameras during live view. You can set image parameters, video parameters, and other more parameters while checking on the live view image. Moreover, you can edit the channel information (channel name, IP address, management port, user name, and password), sort channels, add channels, and delete channels.

Note

The available parameters and operations vary according to the device capability.

Tap or ··· → **Live View** on the device card of an NVR / DVR / network camera.

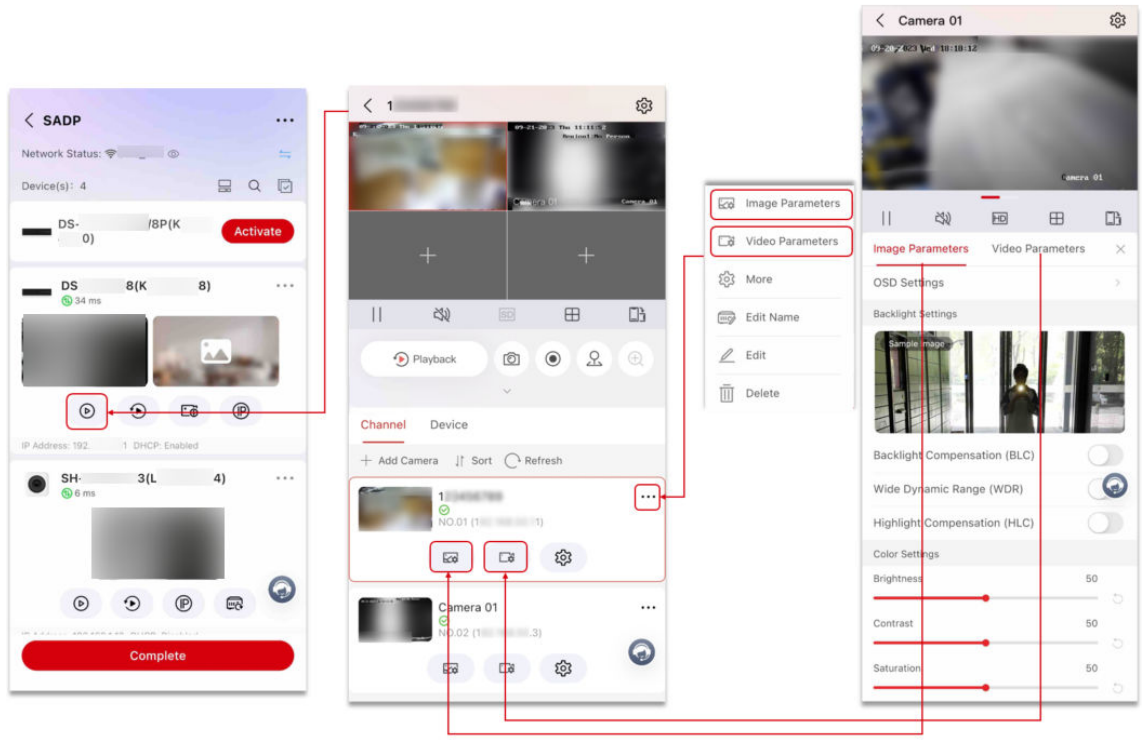


Figure 3-3 Channel Management on the Live View page

Table 3-3 Common Configurations

Parameters	Descriptions
Scene Direction	Select the rotating direction of the camera.
OSD Settings	Set whether to display the camera and time information on the video, and way they are displayed.
Backlight Settings	**Backlight Compensation (BLC)** Select a **BLC Area** where the light is too strong to reduce exposure of this area, thus increasing the exposure of other dark areas. **Wide Dynamic Range (WDR)**

Parameters	Descriptions
	By enabling **Wide Dynamic Range (WDR)**, you can have proper brightness on both the darker and brighter parts of the image. **Highlight Compensation (HLC)** Highlight compensation (HLC) is a setting that allows your camera to compensate for brighter parts of your image by reducing the brightness.
Stream Type	Main stream usually offers the best resolution and frame rate the device can do, but it needs larger storage space and higher bandwidth requirements.
Bitrate Type	The compression speed of constant bitrate is fast with the constant bitrate, but mosaic may occur across the image. The compression speed of variable bitrate is slower than that of the constant bitrate, but it guarantees the image quality of complex scenes.
Frame Rate	A higher frame rate is advantageous when there is movement in the video stream, as it guarantees the image quality throughout. Note that a higher frame rate requires higher bandwidth and larger storage space.

Table 3-4 Other NVR-Related Configurations

Operations	Descriptions
Add Channels to Activated NVR	Tap  → **Auto Add / Manually Select** .
Sort NVR Channels	**Note** Channel sorting is only supported only by some NVR models. 1. - Enter the Sort Channels page.

Operations	Descriptions
	- After you add channels to an NVR, and if the total number of channels of the NVR is more than 1, you will enter the Sort Channels page automatically. - If the total number of channels of an NVR is more than 1, and you have not sorted the channels, you will be prompted to sort channels in the device card view. Tap the prompt to enter the Sort Channels page. 2. Drag and drop the channels to sort them, and tap **Complete** to finish sorting.

(Optional) Step 5: Configure Other Devices Using the SADP Tool

Refer to the ***On-Site Configure Devices Using the SADP Tool / via the Site page*** .

Other Common Operations Using the SADP Tool

Operations	Descriptions
Manage Default Device Password	On the top right of the SADP page, tap ··· → **Manage Default Device Password** to set a default device password and a default verification code.
Edit IP Addresses	Tap ··· → **Edit IP Address** on a device card to edit the IP address of a single device, or tap → **Batch Edit IP Addresses** to batch edit the IP addresses of multiple devices. You can enable **DHCP** to automatically assign the IP address, gateway address, subnet mask, and DNS address, or disable **DHCP** to set them manually. When you set the subnet mask manually, you can select from a list of recommended subnet masks, thus avoiding any invalid values you may enter.
Restore and Reboot Devices	To restore or reboot devices, tap or ··· → **Restore Device** on a device card to restore a single device, or tap → **Batch Restore/Reboot** to batch restore or reboot multiple devices.

3.1.3 SADP Tool: Quick Deploy and Professional Modes

What This Is and When to Use It

Overview

The SADP tool has **Quick Deploy** mode and **Professional** mode (which contains 13 batch tools), so a phone alone is enough on site to discover, activate, configure, re-password, upgrade, and onboard devices.
What used to take 15 minutes per device — two or three days for 100 devices — now takes about 5 minutes per device, with no laptop or cable to carry.

The Two Modes

The SADP tool now has two modes. You pick one when you first enter, and can switch at any time afterwards.

Mode	Suited To	Contents
Quick Deploy	New installs and newcomers: activate, connect, onboard in one flow.	SADP discovery and configuration. Refer to ***Use the SADP Tool to Quick Initialize LAN Devices*** .
Professional	Batch configuration and commissioning on an independent IP network.	The 13 tools described in this guide.

Typical Scenarios

- **Delivering a whole site.** 24 devices in a new store: **IP Scan** to see which addresses are taken, **Batch Activate**, **Edit IP Address** to assign addresses in sequence, **Add to Site** to onboard them, **Edit OSD** to standardize channel names.
- **Cleaning up an older site.** Inconsistent passwords and stale firmware: store the working passwords in **Saved Passwords**, unify them with **Batch Change Passwords**, bring firmware up to date with **Firmware Upgrade**, and reactivate the few devices that need **Batch Restore**.
- **Commissioning checks.** Run the motion detection and recording checks on the video device page to confirm the system will really record and really alarm, and fix any failed item on the spot with one tap.
- **Network troubleshooting.** When a device will not reach the cloud, use **Ping** against the gateway and a public address to see where the packet loss or latency starts.

Before You Start

Three Prerequisites

1. **The phone and the devices share one local network.** Use Wi-Fi, or a wired adapter into the site network. Devices cannot be discovered over mobile data.
2. **Entry permission.** Tool entry points are permission-controlled; if you cannot see them, ask your company administrator.
3. **Site management permission.** Only **Add to Site** needs it; no other tool does.

First Use and Choose a Mode

Tap the **SADP** shortcut on the **Site** page. The first time you enter, the mode selection page appears; your choice is remembered and used from then on.
The upper half **Get Ready** shows the current network. The lower half describes the two modes. Choose one and tap **OK**.

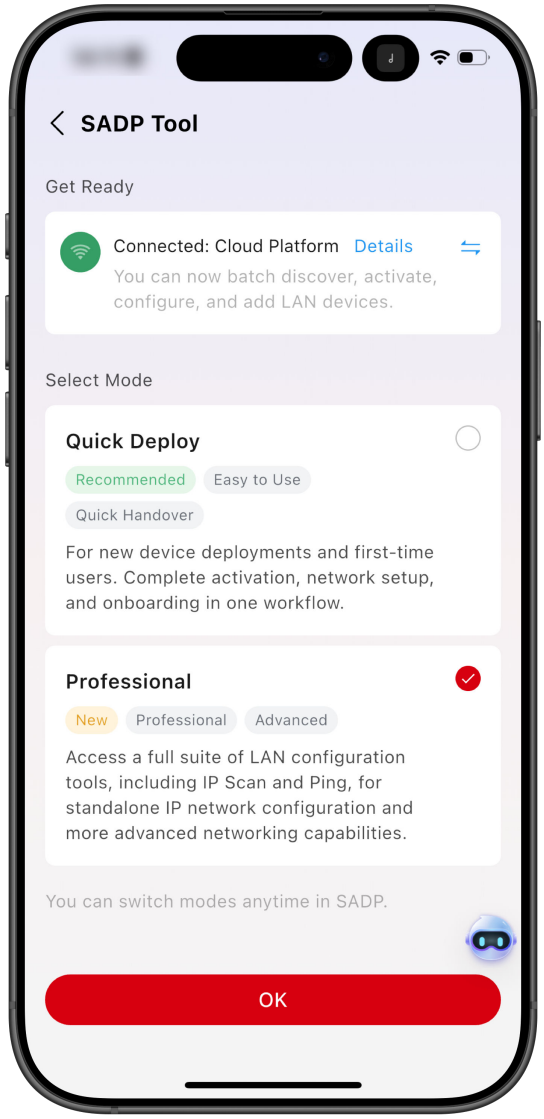


Figure 3-4 Choose a Mode

Switch Modes Later

Tap the mode icon at the top right of the SADP page.

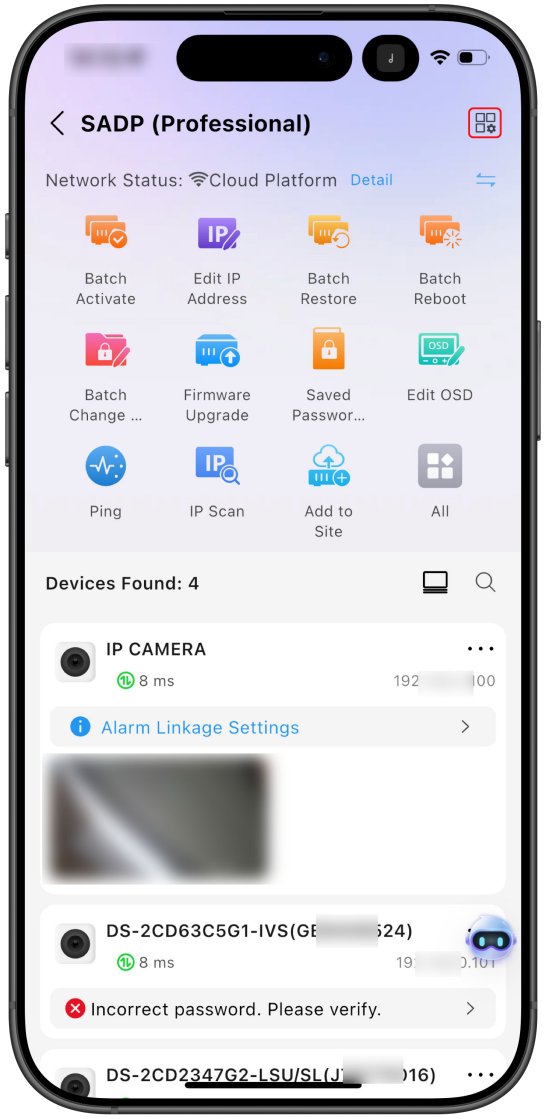


Figure 3-5 Switch Modes

What Professional Mode Looks Like

The page has three blocks, top to bottom:

1. **The network bar**: Current network, **Detail**, and the switch button for switching to another network.
2. **The tool grid**: 11 favorites plus **All**, customizable (***Rearrange Your Favorites***).
3. **The device list**: **Devices found: N**, each showing model, serial number, IP address, and latency. Devices not yet activated are tagged **Not Activated**; devices with problems show **exceptions**; devices running a task show its progress.

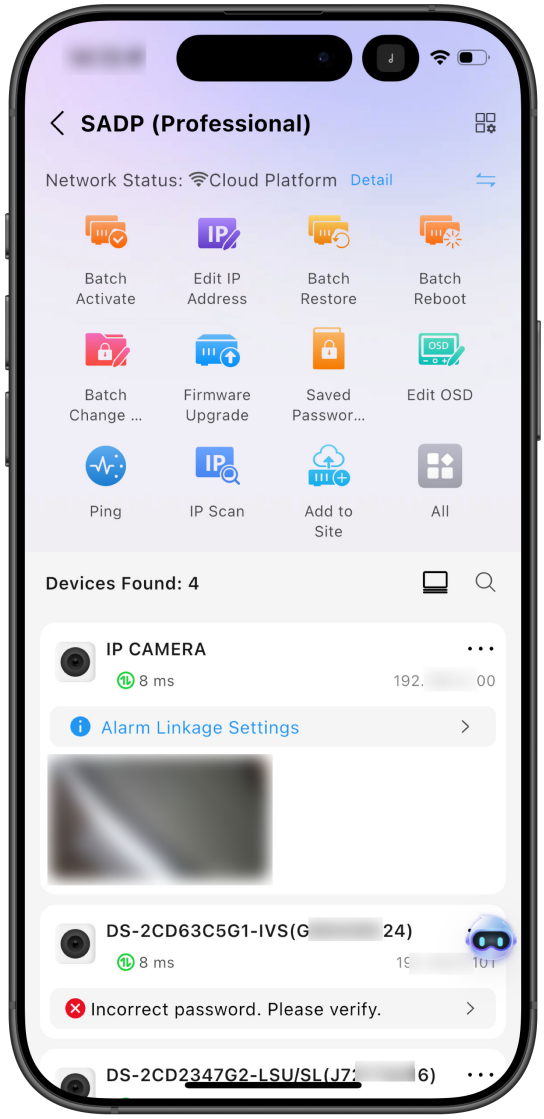


Figure 3-6 What Professional Mode Looks Like

The 13 Tools at a Glance

Quick Reference

This table is the map for the rest of the guide. "Password" means the tool asks you to verify the device administrator password.

Group	Tool	What It Does	Password	Export
Network	**IP Scan**	Scan an IP range for used and free addresses.	No	Yes, as an image.
	Ping	Measure loss and latency to a target.	No	No
Device	**Batch Activate**	Activate new devices with a password.	Sets one.	No
	Edit IP Address	Change IP, mask, gateway, ports in bulk.	Yes	Yes
	Batch Restore	Restore factory defaults.	Yes	No
	Batch Reboot	Reboot devices.	Yes	No
	Edit OSD	Change the channel name and time overlay.	Yes	No
	Exception Notification	Set how faults are reported.	Yes	No
	Batch Change Passwords	Set one administrator password.	Yes	Yes
	Firmware Upgrade	Upgrade online or from a local package.	Yes	No
	Time Sync	Push the phone's time to the devices.	Yes	No
General	**Saved Passwords**	An on-phone password book reused by every tool.	No	No
	Add to Site	Enable the Hik-Connect service and add to a site.	Yes	No

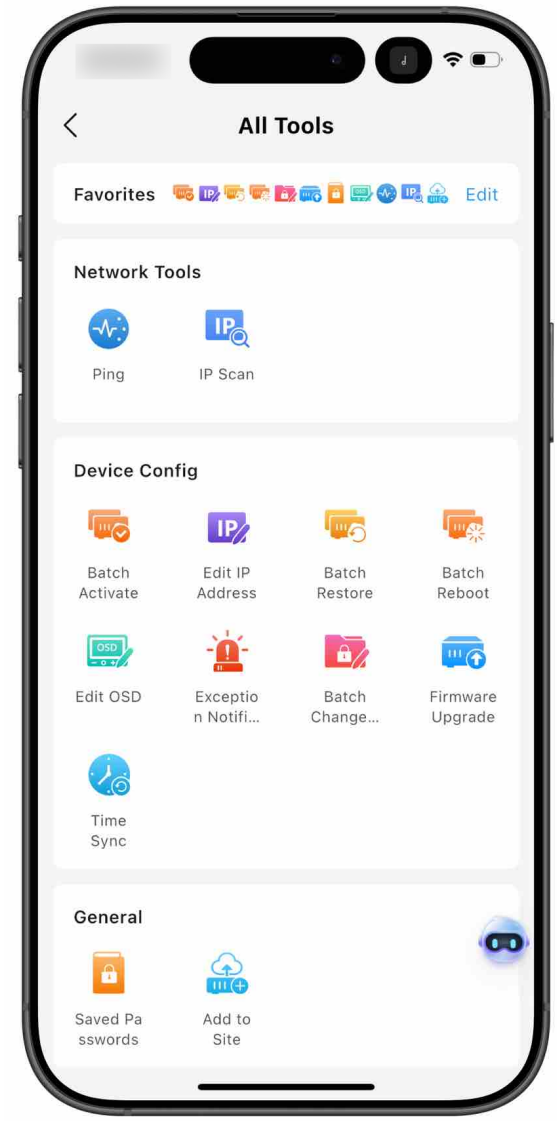


Figure 3-7 All 13 Tools

Rearrange Your Favorites

On the **All Tools** page, tap **Edit** to open **Edit Favourites**. Tools in the favorites area carry a ⊖ to remove them, tools in the other groups a ⊕ to add them, and press and hold to drag one to a new position. Tap **Save** when done.

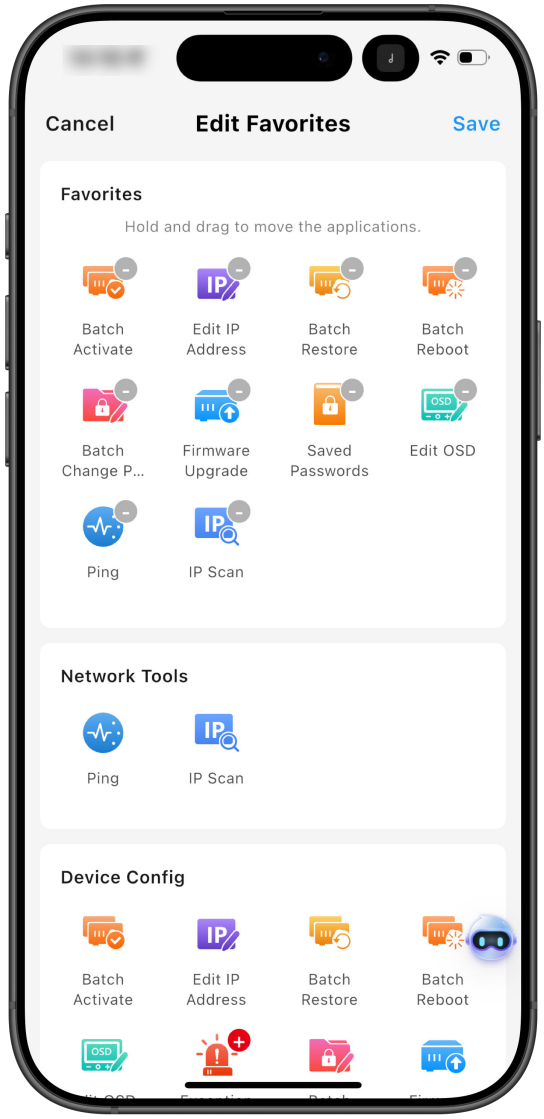


Figure 3-8 Edit Favorites

Tool Reference

IP Scan

What it does: Scans an IP range and marks each address as online, idle, or not scanned. Usually the first thing to run on a site.

Prerequisites: The phone is on the site network. No device password needed.

Steps:

1. Tap **IP Scan**.
2. Enter the **Start IP** and **End IP**.

Note

This tool covers IPv4 on a local network. Both addresses must be valid and the range sensible.

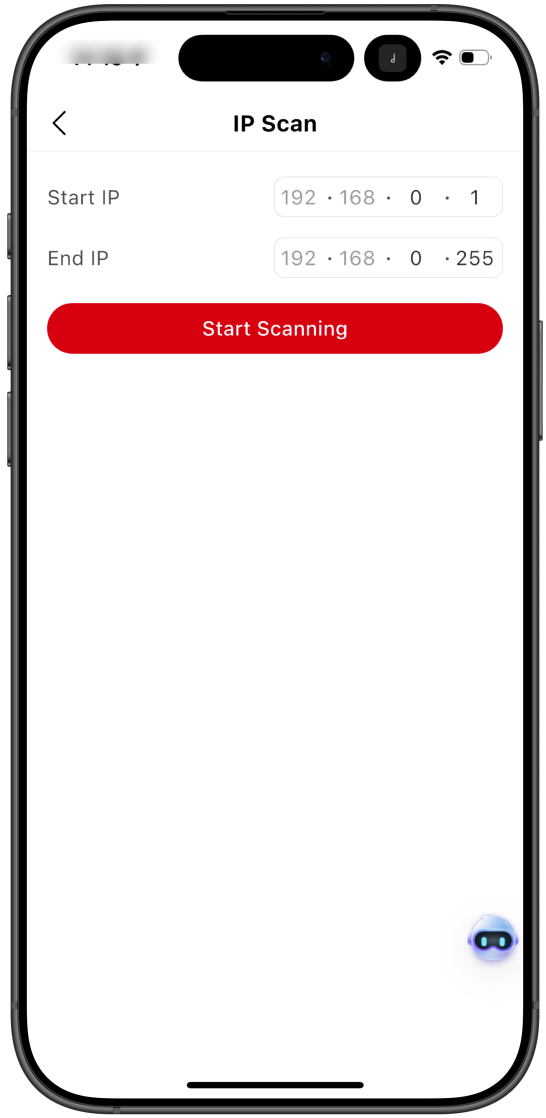


Figure 3-9 Enter IP Range

3. Tap **Start Scanning**; when it finishes the button becomes **Rescan**.
4. Read **Total Online** and the **Grid View**: Green is online, gray is idle, pale is not scanned.

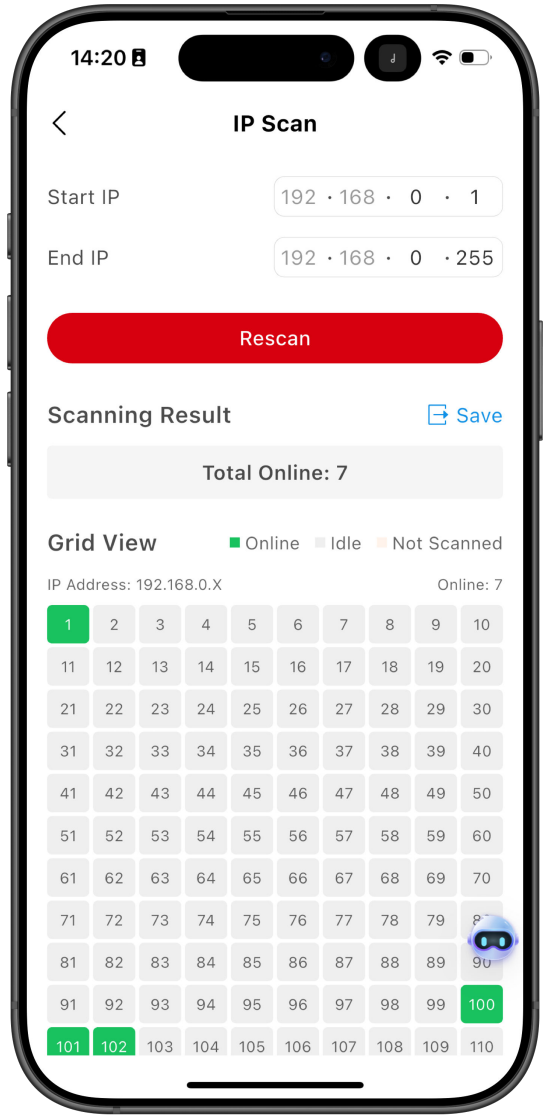


Figure 3-10 IP Scan Result

5. Tap **Save** to produce a Hik-Partner Pro branded result image and tap **Share** to share it through the system sheet.



Figure 3-11 Share Result

Edit IP Address

What it does: Changes network parameters in bulk.

Prerequisites: The devices are activated.

Steps:

1. Tap **Edit IP Address**.
2. Select the devices, tap **Next**, and verify the password in bulk or one by one.

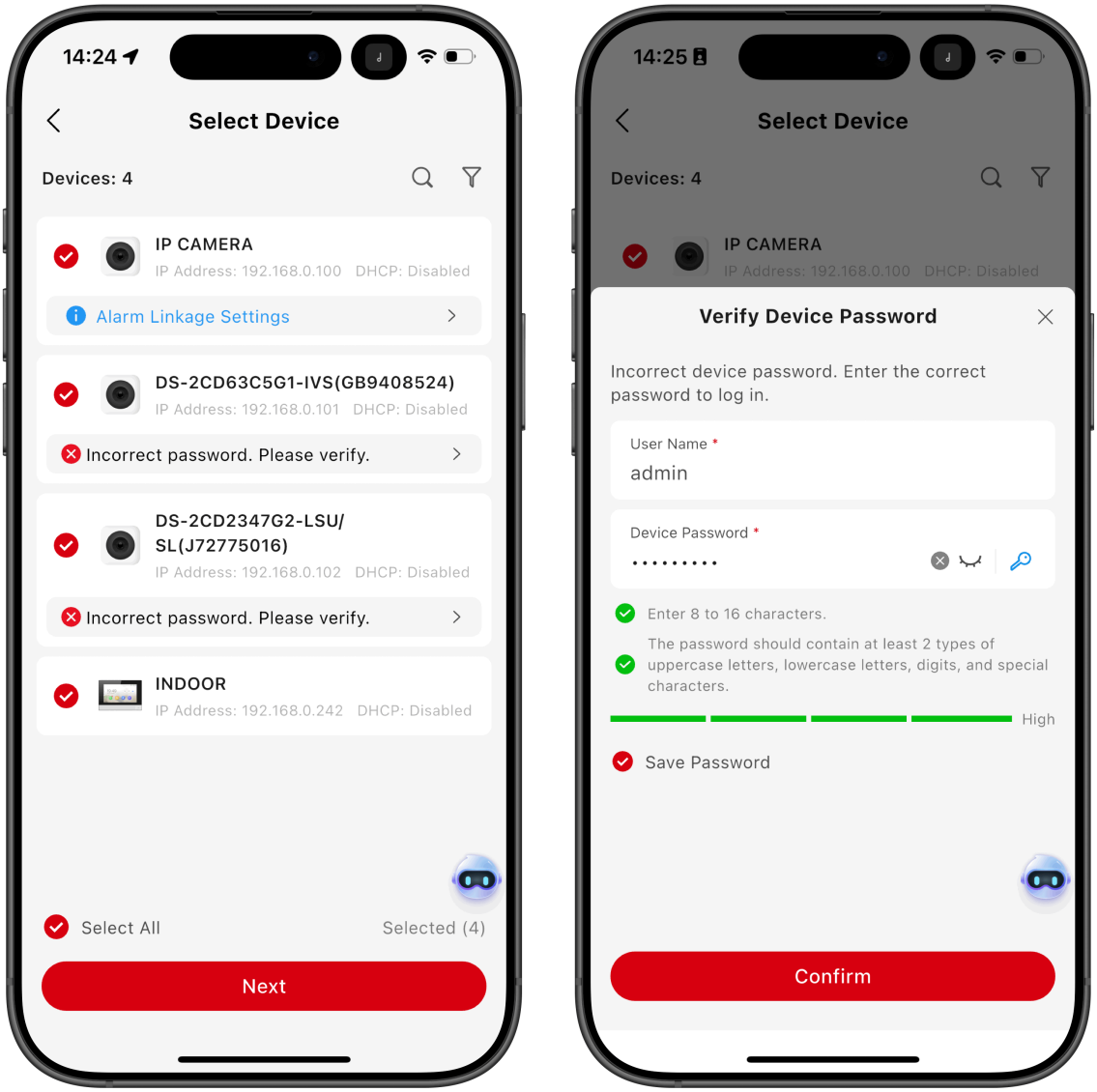


Figure 3-12 Select Devices and Verify Passwords

3. Set **DHCP**:
   a. **DHCP On**: The start IP, gateway, and subnet mask are grayed out and assigned by DHCP. Set **Service Port** (8000 by default), and **HTTP Port** (80 by default).

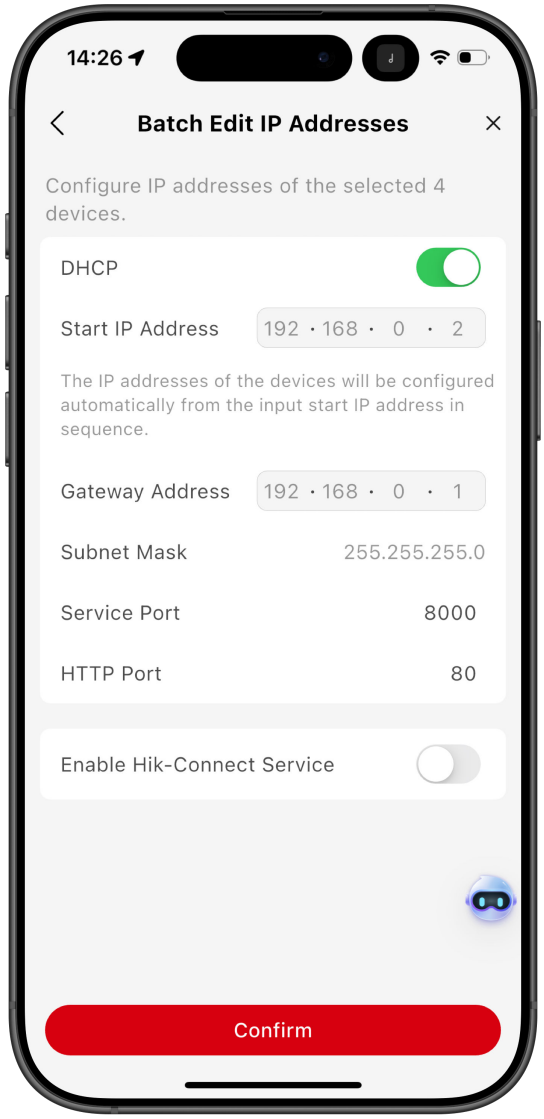


Figure 3-13 DHCP On

b. **DHCP Off**: Enter **Start IP**, **Gateway**, **Subnet Mask**, **Service Port** (8000 by default), and **HTTP Port** (80 by default).

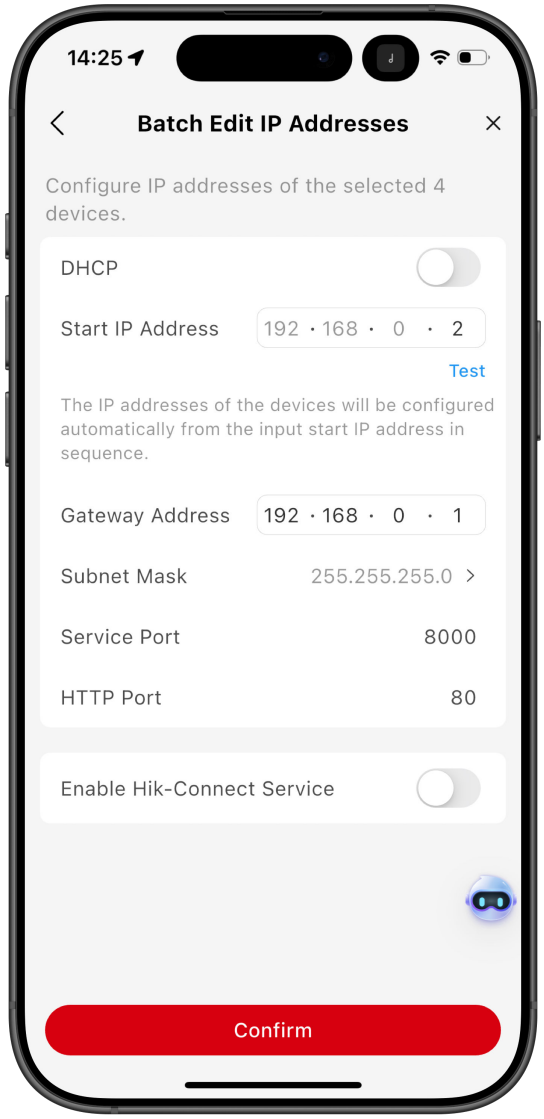


Figure 3-14 DHCP Off

4. Tap **Test** next to the start IP to check whether the range has enough free addresses. If not, a message says the selected range does not have enough, and **Detail** shows what is taken.

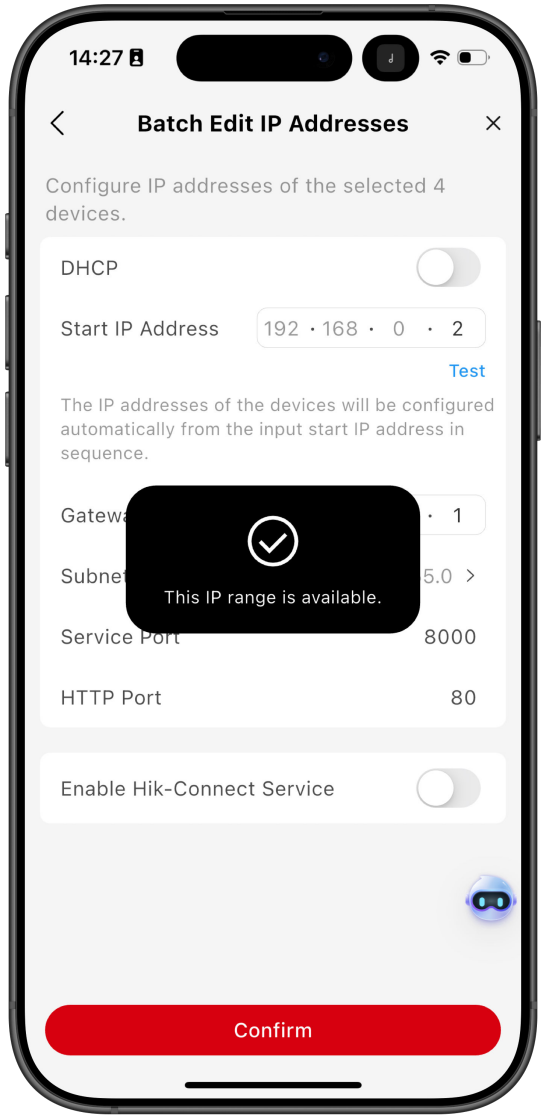


Figure 3-15 Test

5. Set the **Hik-Connect Service** switch as needed and tap **Confirm**.

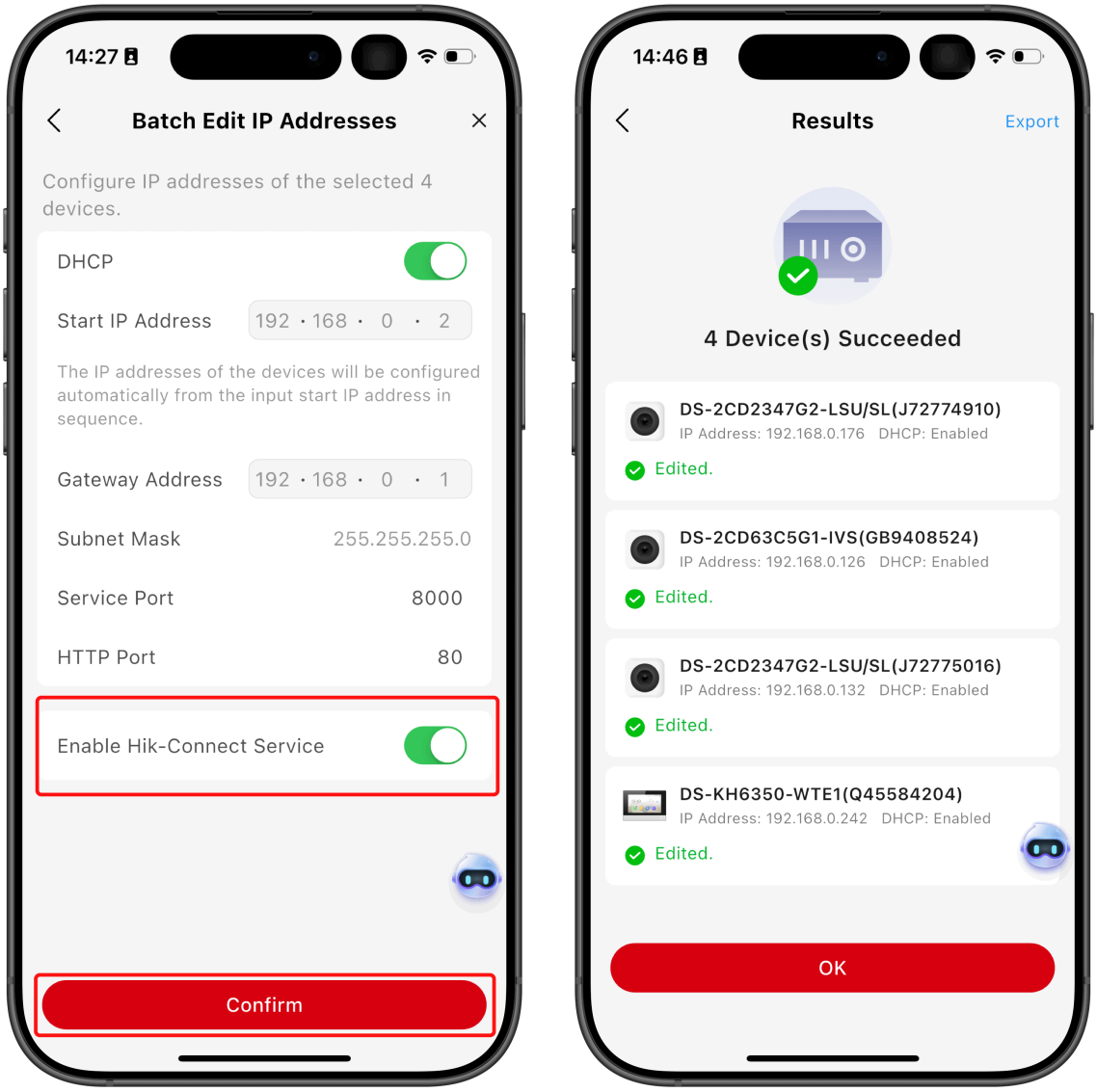


Figure 3-16 Result

Note

Only the first address is entered; the rest increment by one automatically.

Batch Activate

What it does: Sets a password on new devices and activates them. Activation only, and it does not also change the IP, push a time zone, or enable the Hik-Connect service.

Prerequisites: The devices are not yet activated.

Steps:

1. Tap **Batch Activate**.
2. Select the devices to activate and tap **Next**.

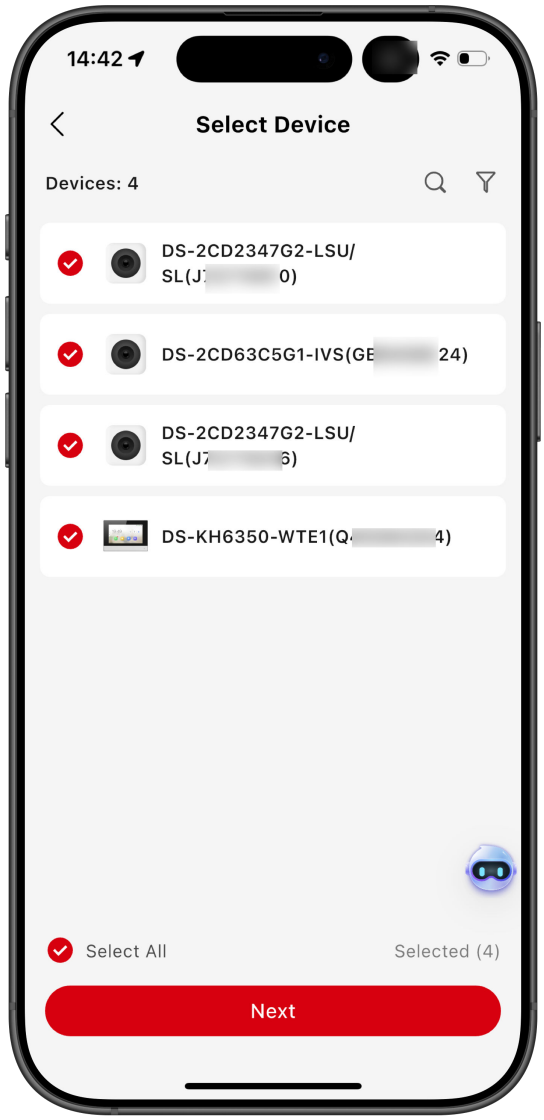


Figure 3-17 Select Device

3. In the **Activate Device** dialog enter the device password and tick **Save Password** if you want.

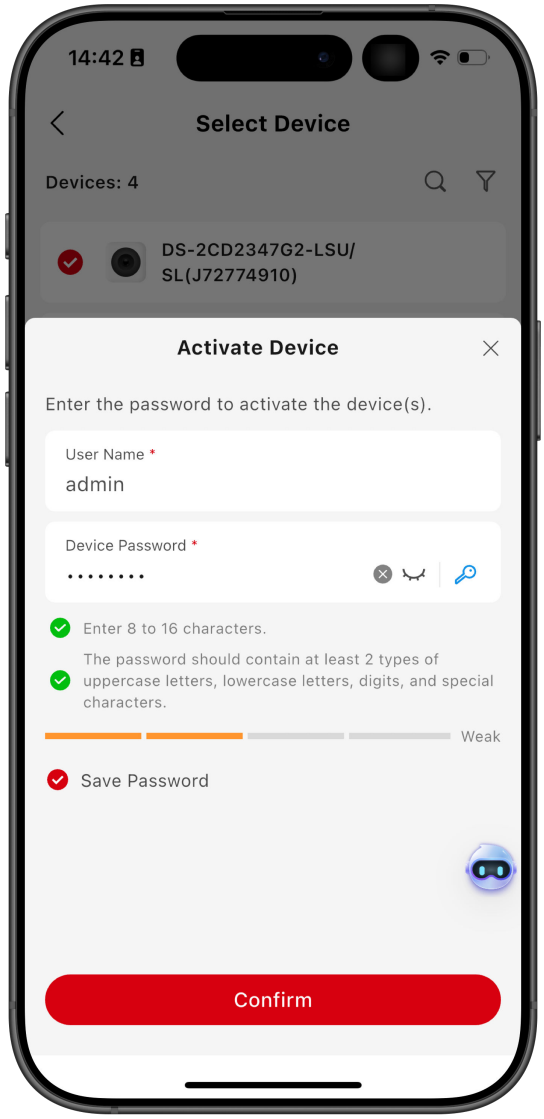


Figure 3-18 Set Password

4. Tap **Confirm** and review the per-device result.

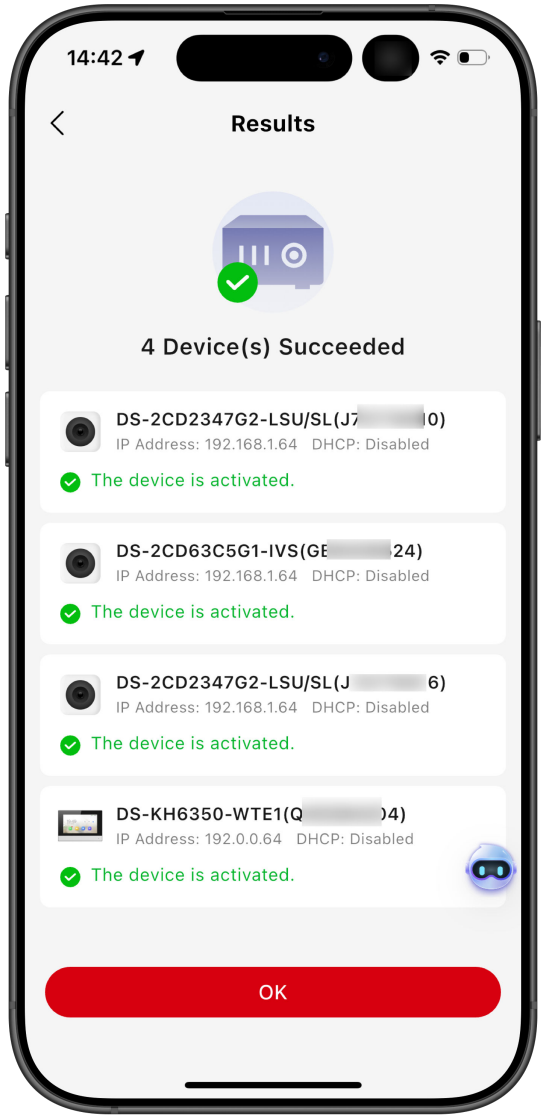


Figure 3-19 Result

Note

Then you can use **Edit IP Address**, **Time Sync**, and **Add to Site** for those jobs.

Exception Notification

What it does: Sets how video devices report their own exceptions, in bulk.

Prerequisites: Video devices, activated and password-verified.

Steps:

1. Tap **Exception Notification**.
2. Select the devices and verify the password if needed. Tap **Next**.

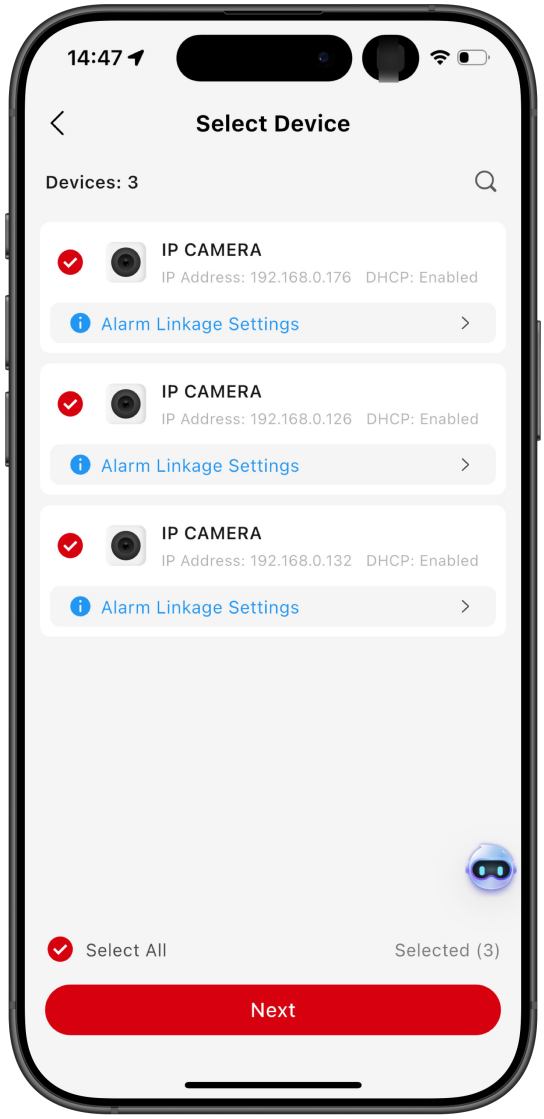


Figure 3-20 Select Device

3. Tap **Exception** to open the list of fault types (HDD full, HDD error, IP address conflict, illegal login, etc.), check the ones to configure, and tap **Confirm**.

Note

The available exception types vary depending on the device model.

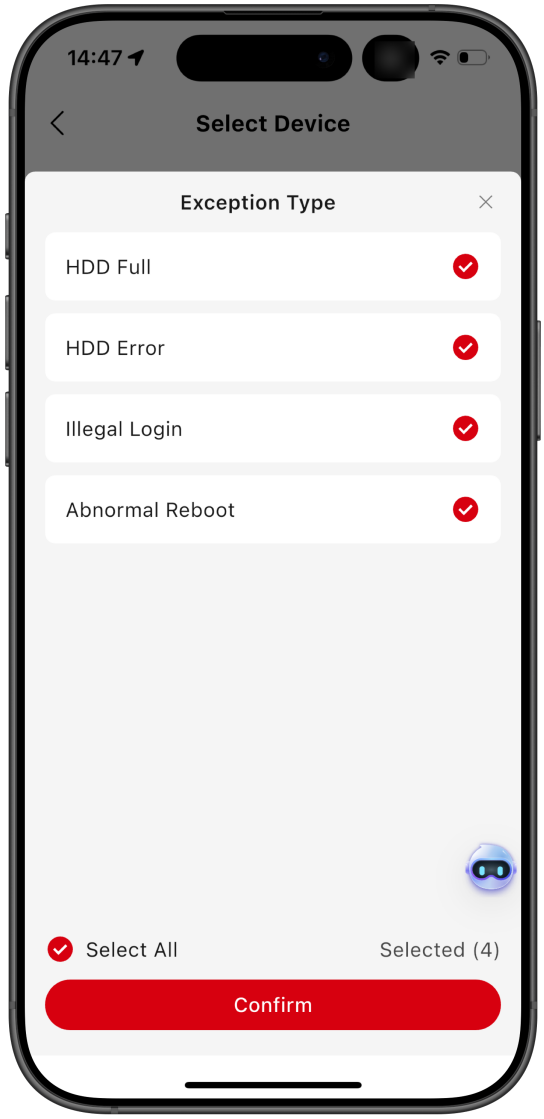


Figure 3-21 Exception Type

4. Set the two notification switches as needed: **Notify Surveillance Center** and/or **Buzzer**.

Note

The available notification methods vary depending on the device model.

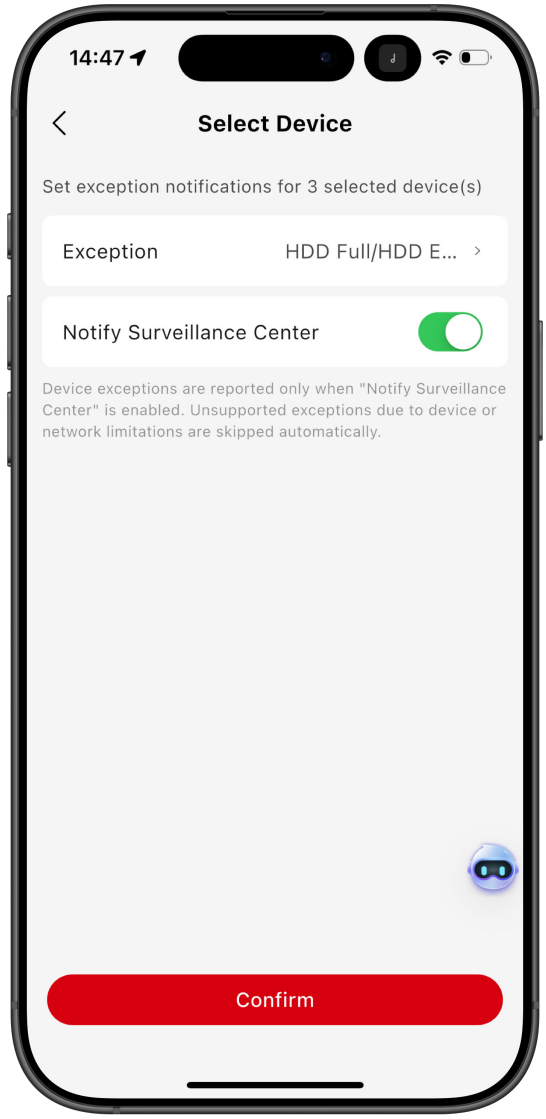


Figure 3-22 Set Notification

5. Tap **Confirm** and review the result.

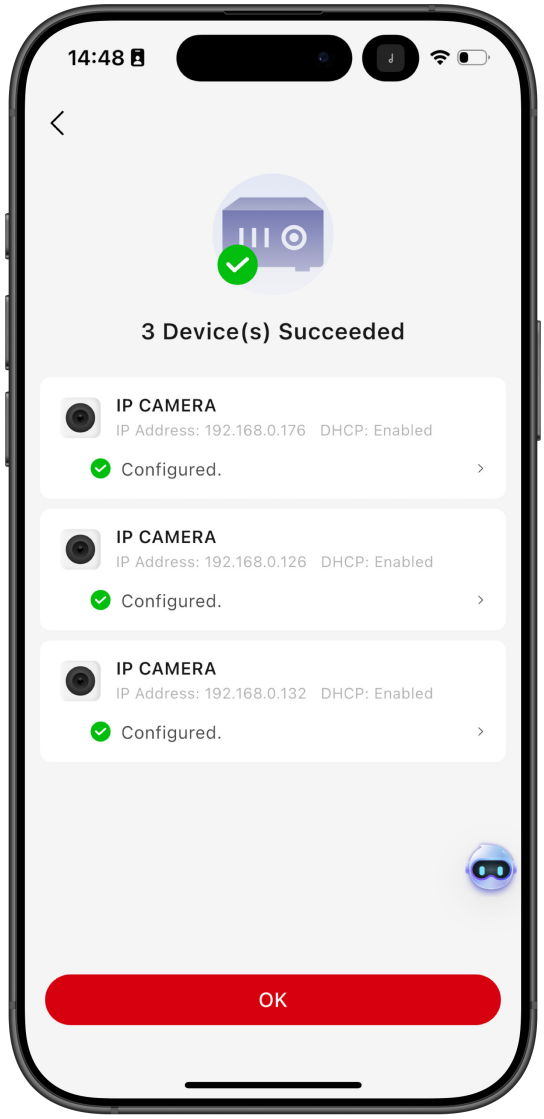


Figure 3-23 Result

Note

- **Notify Surveillance Center** is what sends exceptions to the platform. **Without it the platform receives nothing.** The end user (customer) also has to enable reception in the HC app.
- Some exceptions cannot use **Notify Surveillance Center** because of the device's capability or because the network is down at the time (e.g., network disconnection or IP conflict). Those are skipped automatically.
- Devices with no **buzzer**, such as network cameras, are skipped automatically too.

Batch Change Passwords

What it does: Sets one new device password across a group of devices.

Prerequisites: The devices are activated, and the old password has been verified.

Steps:

1. Tap **Batch Change Passwords**.
2. Select the devices and verify the old password if needed. Tap **Next**.

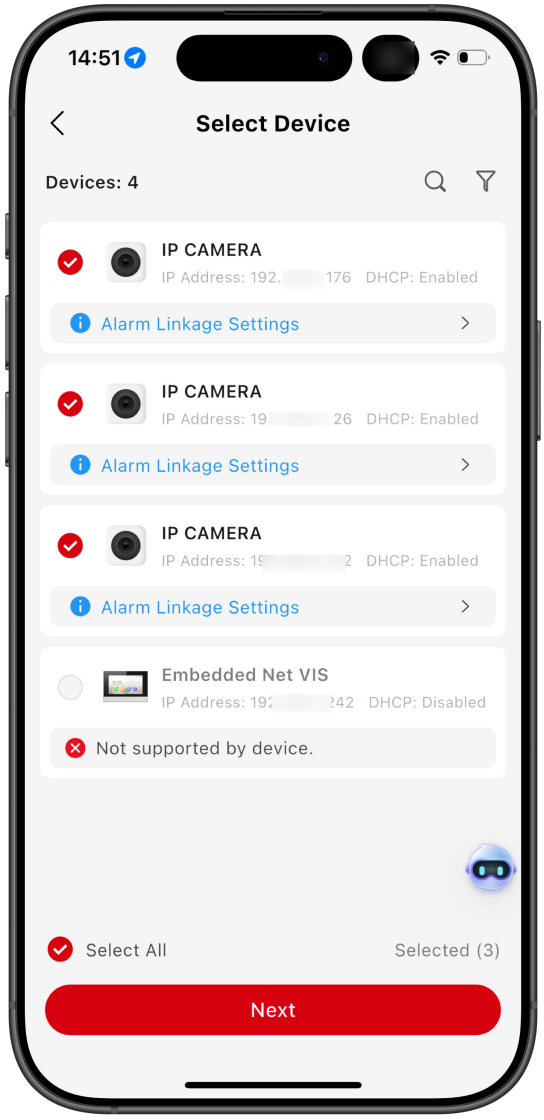


Figure 3-24 Select Device

3. On the **Set New Password** page fill in **Set New Password** and **Confirm Password**. Check **Save to Passwords** if you want.

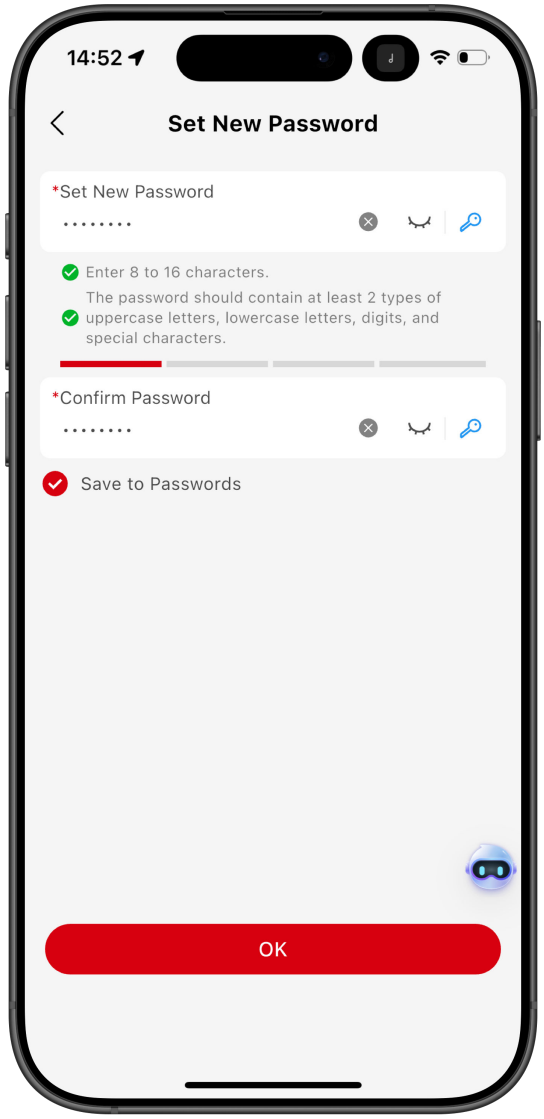


Figure 3-25 Set New Password

4. Tap **OK** and view the result.

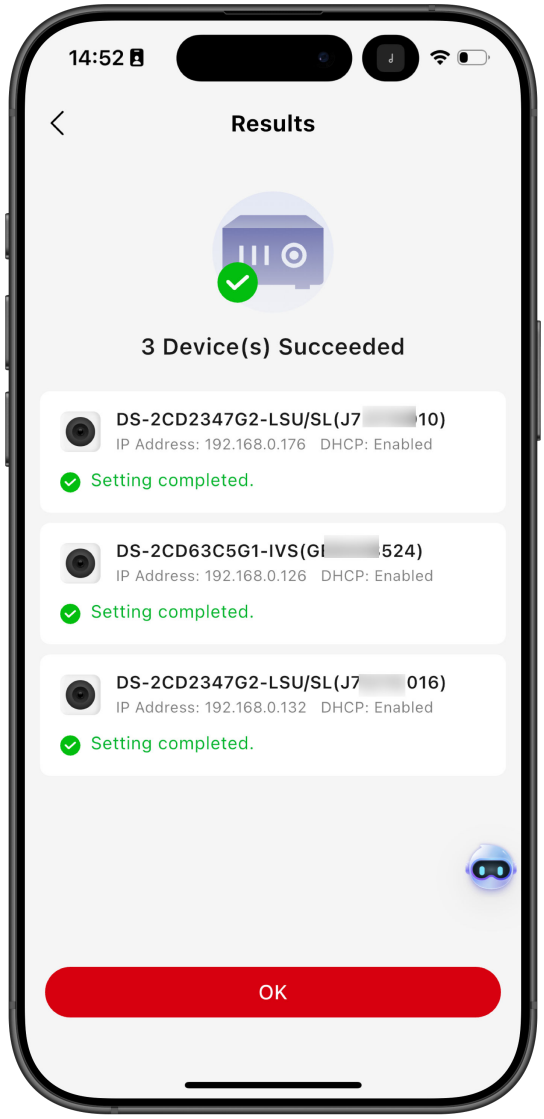


Figure 3-26 Result

Edit OSD

What it does: Standardizes the channel name and time overlaid on the video of encoding devices.

Prerequisites: Encoding devices only.

Steps:

1. Tap **Edit OSD**.
2. Select the cameras, verify the password, and tap **Next**.

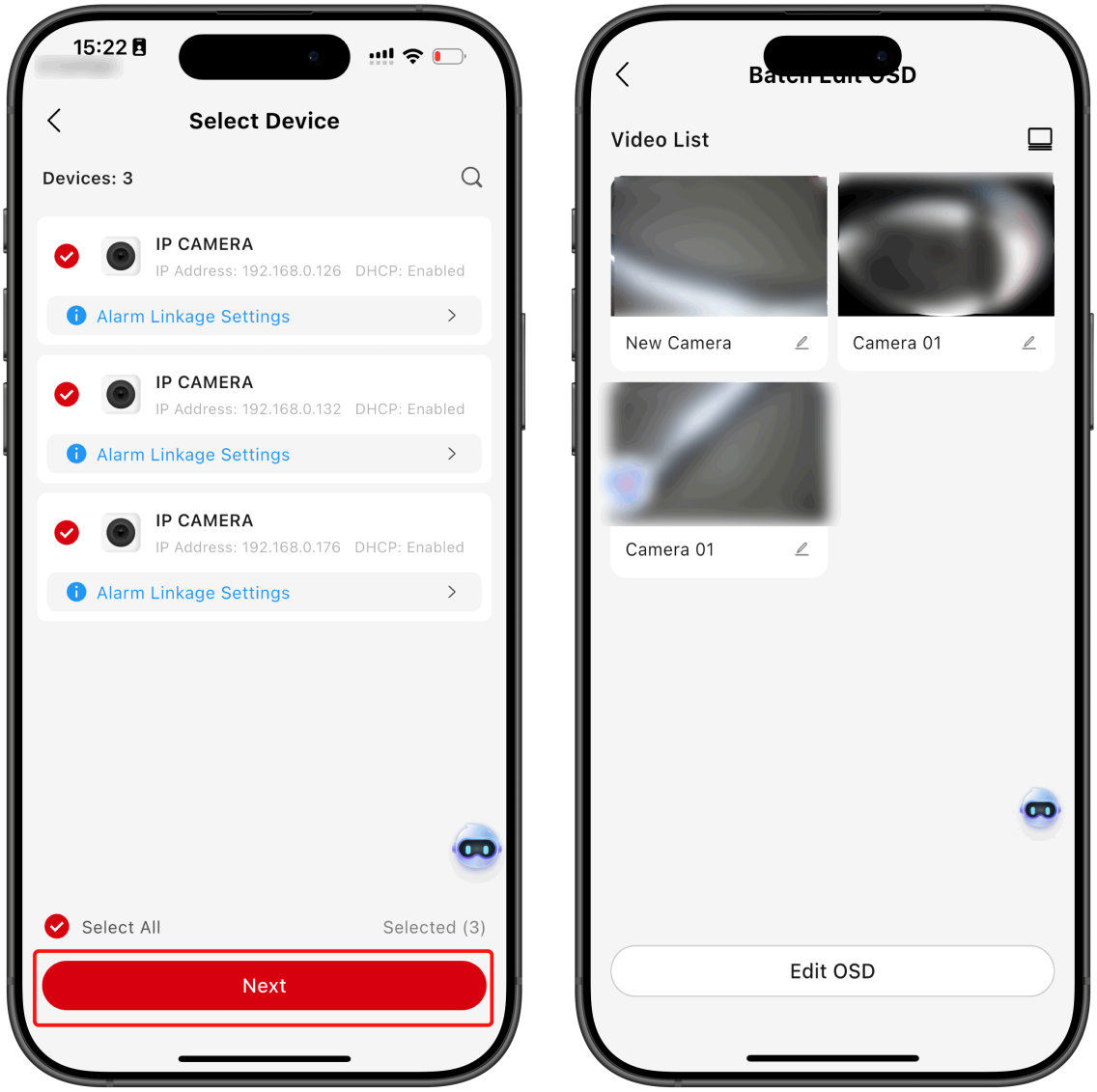


Figure 3-27 Edit OSD

3. Tap the ✎ beside a camera name to rename that one.

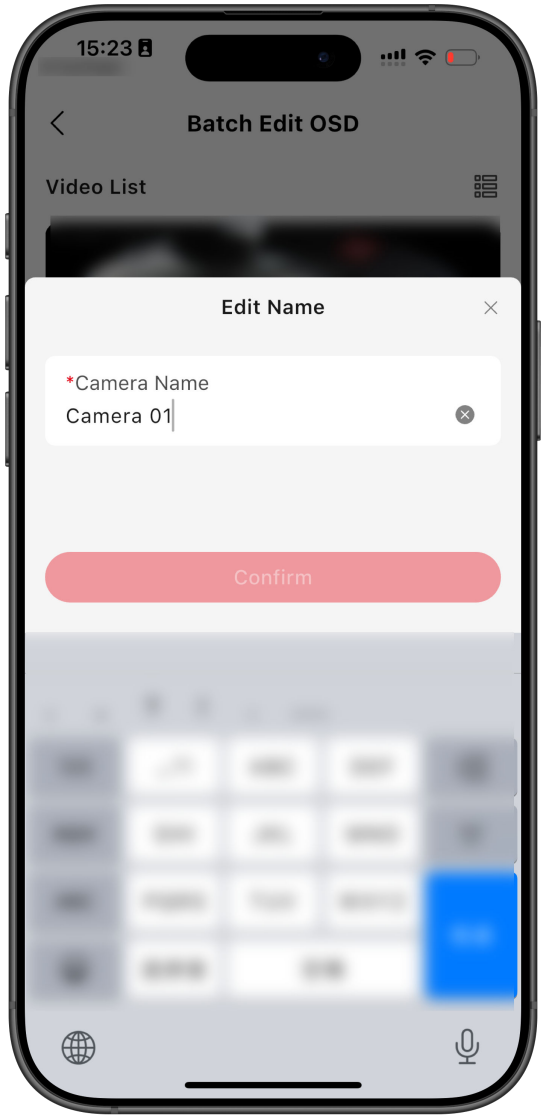


Figure 3-28 Edit Name

4. Tap **Edit OSD** at the bottom to open the settings panel for all selected cameras, in three groups:
   a. **Camera**: **Display Name** switch, and **Position** (lower right, lower left, upper left, upper right, and do not adjust).
   b. **Time**: **Display Time** switch, **Date Format**, **Time Format** (12- or 24-hour), **Position**, **Display Day of Week** switch.
   c. **General**: **OSD Size** (16*16, 32*32, 48*48, 64*64, 96*96, adaptive).

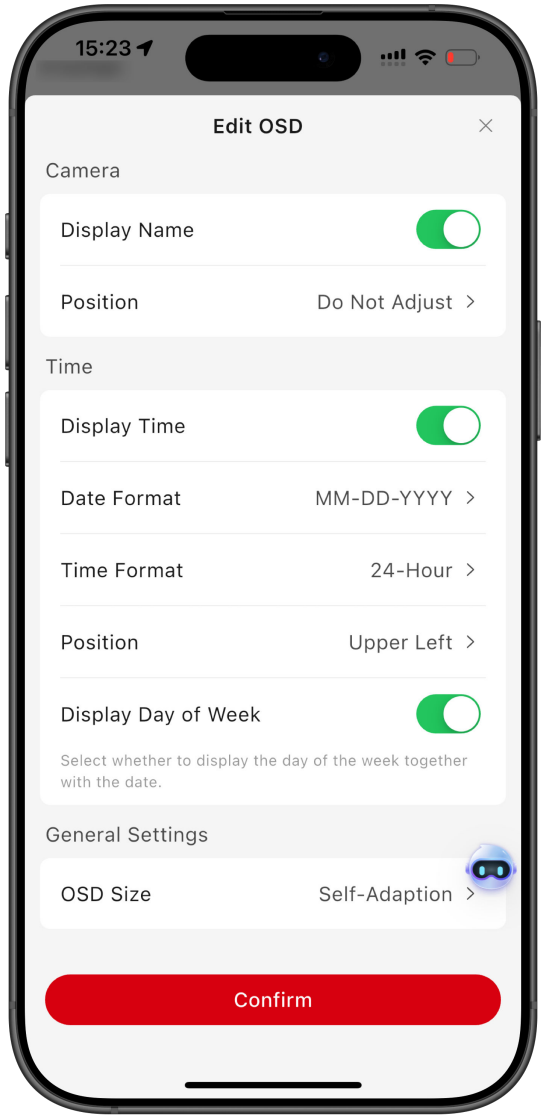


Figure 3-29 Edit OSD

5. Tap **Confirm** to apply.

Note

The day of the week is merged into the date display. Devices or channels that do not support a setting return a failure individually.

Firmware Upgrade

What it does: Upgrades firmware online or from a local package. Once you are inside one route you cannot switch to the other without leaving.

Online Upgrade

1. Tap **Firmware Upgrade**.
2. Tap **Online Upgrade**.

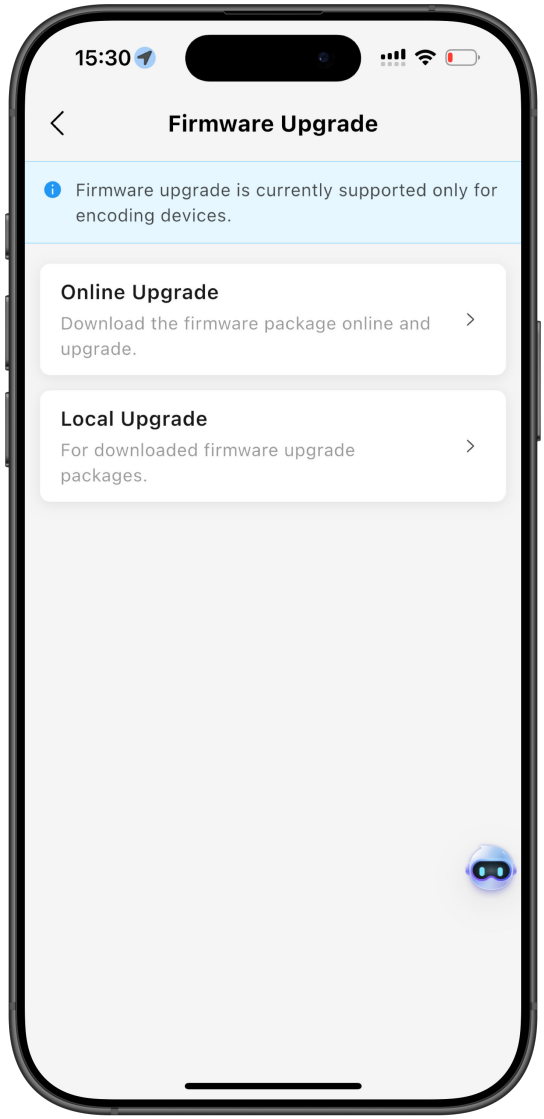


Figure 3-30 Firmware Upgrade

3. Select the devices to upgrade and verify the password if needed. Tap **Next**.

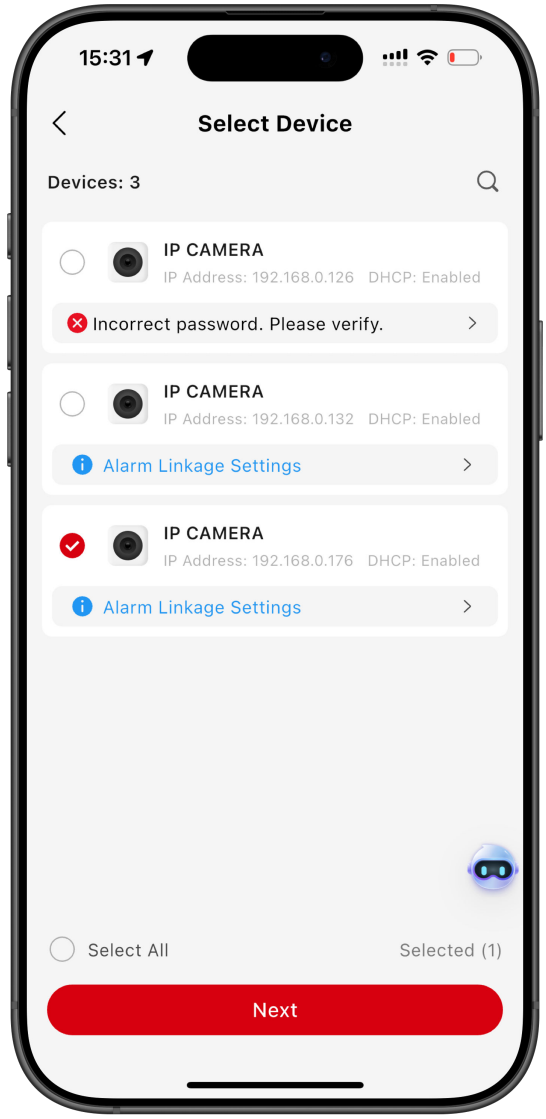


Figure 3-31 Select Device

4. The system queries the available packages; **the phone needs internet access** at this point.
5. Each device shows **new version available** or **latest version already**. Tap the version number to read the release notes.
6. Tap **Upgrade Now** and follow the per-device progress and result.

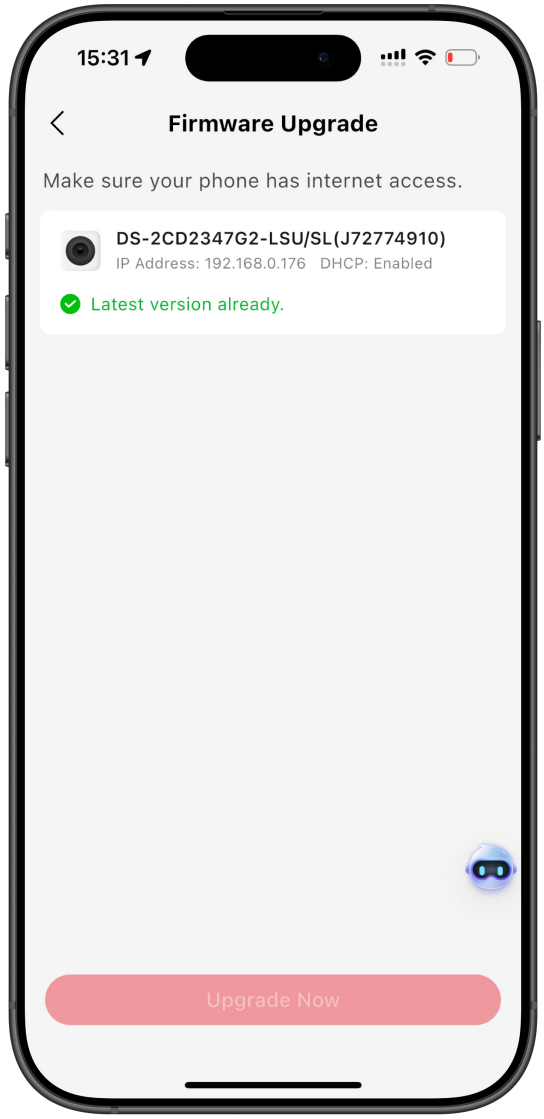


Figure 3-32 Upgrade Now

Local Upgrade

1. Tap **Firmware Upgrade**.
2. Tap **Local Upgrade**.

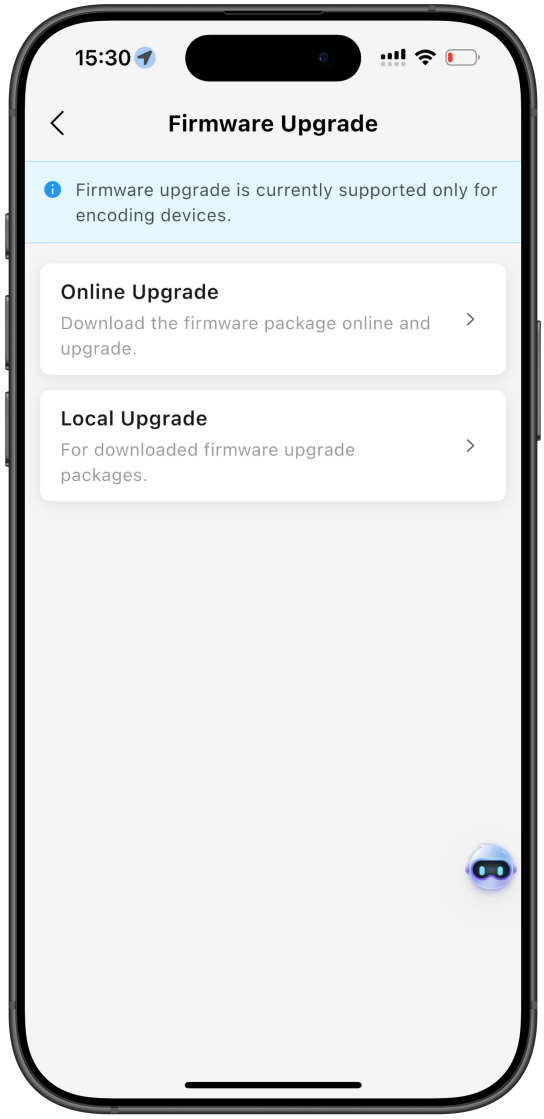


Figure 3-33 Firmware Upgrade

3. Tap **Add Firmware Package** and pick a ZIP file from the phone. The file name must contain the firmware version and date, for example **XXX_V4.26.010_200923.zip**.

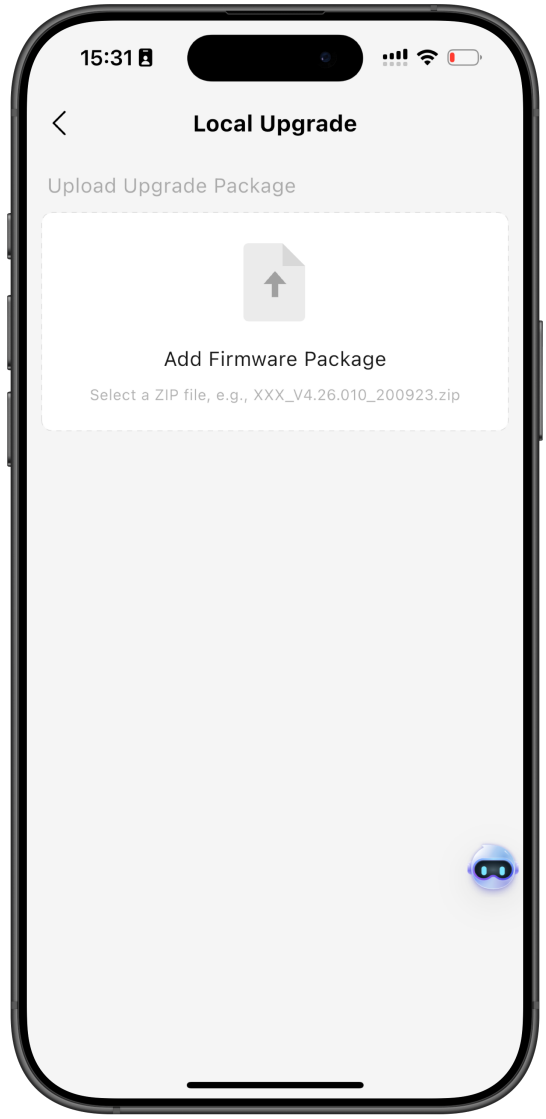


Figure 3-34 Add Firmware Package

4. The selected file is shown. **Reselect** and **Delete** are available. Tap **Confirm**.
5. Select the devices and verify the passwords if needed. Tap **Next**. The system checks them against the package, and incompatible devices cannot be selected or are given a reason.
6. Confirm to run the upgrade.

Note

If you leave during an upgrade, the device card keeps showing **Upgrading firmware**.

Saved Passwords

What it does: A password book on the phone, so you do not retype the same password across a batch of devices.

Tap **Saved Passwords** to enter the page.

What is on the page:

- **Manage Default Device Password**: The **default password and verification code** are filled in automatically when activating or verifying a device. Tap **Manage Default Device Password** to view or change the default device password and verification code.
- **Saved Passwords**: The **device passwords** list, with an eye icon that reveals or hides every entry at once.
- **Add Password**: Tap **Add Password** to manually add a password to the saved list.

How to use it:

Wherever a device password is required, tap the key icon to pick one saved password to auto fill the field. You can also tick **Save Password** during verification / new password setting to add it to the saved passwords automatically.

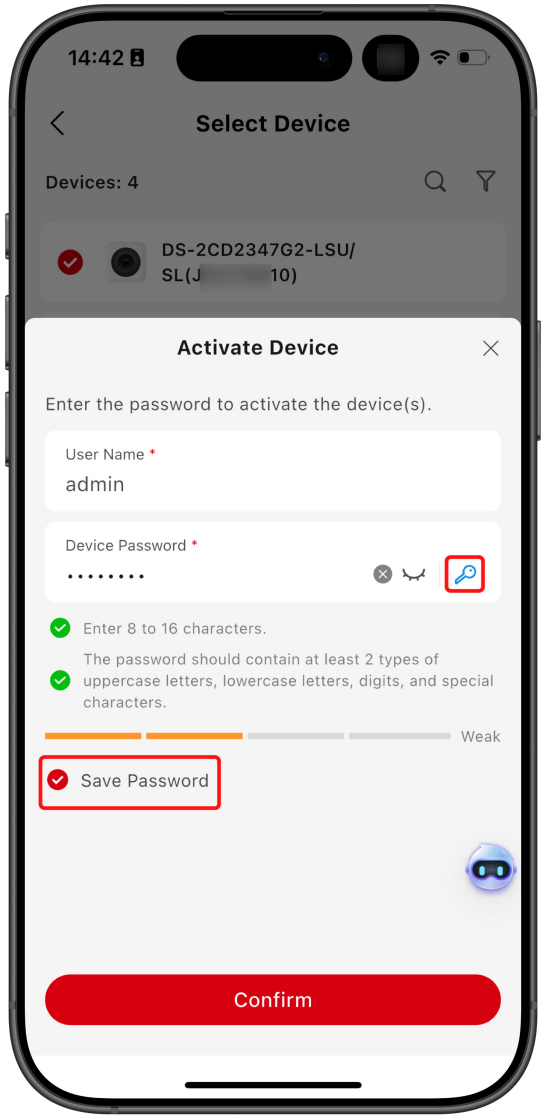


Figure 3-35 Use Saved Passwords

Security:

Passwords live in the operating system's secure store (Keychain on iOS, Keystore on Android) and are never written in plain text. Cloud synchronization is not supported. After sign-out the book is isolated per account, so accounts never see each other's entries. Logs, exports, and analytics never record a plain-text password.

Add to Site

What it does: Enables the Hik-Connect service and adds the devices to a site, in bulk.

Prerequisites: The devices are activated, and **you need site management permission** — without it the tool is not shown.

Steps:

1. Tap **Add to Site**.
2. Choose **Personal** mode or **Team** mode.

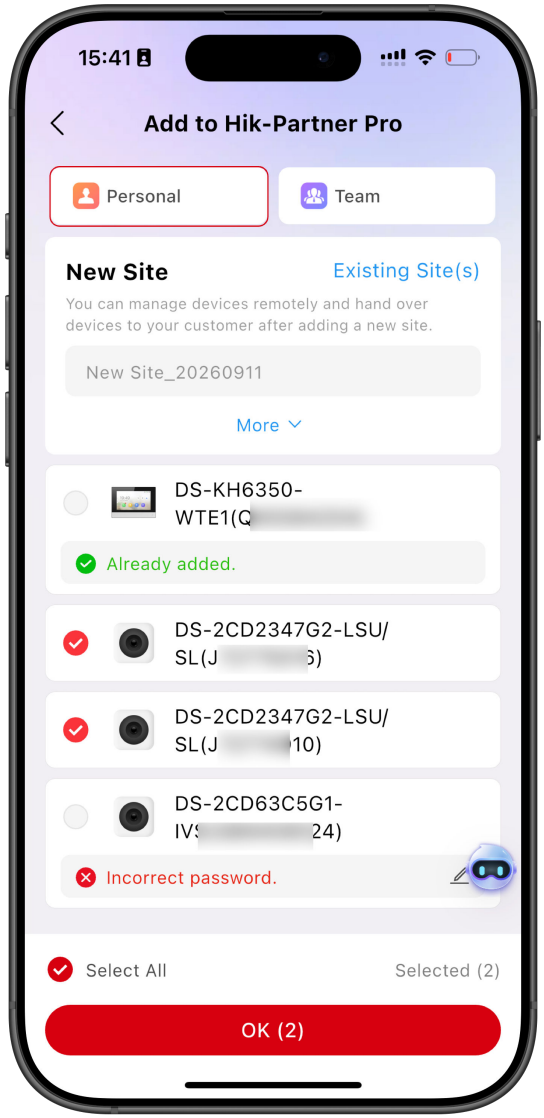


Figure 3-36 Add to Site

3. Create a site (enter a site name; tap **More** to add further site details) or tap **Existing Site(s)** to pick one. A site is what lets you manage devices remotely and hand them over to an end user (your customer).
4. Select the devices to add. Devices such as NVRs show how many sub-devices they carry, which you can expand and check.
5. Tap **OK**.

6. If needed, enter the **Verification Code** in the **Verify Device** dialog. It is used for remote management and for encrypting the video stream.
7. Submit and review the per-device result.

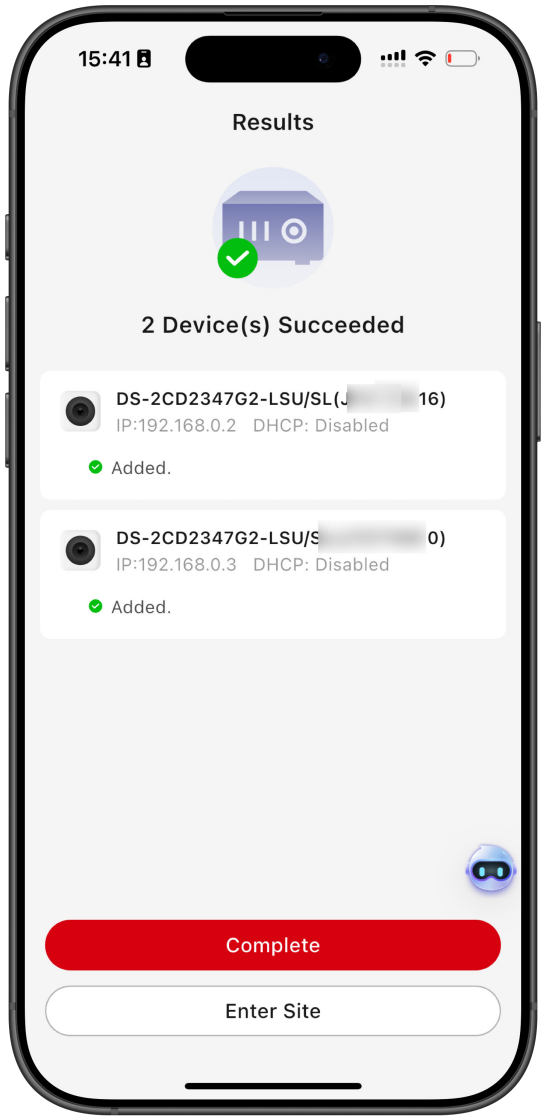


Figure 3-37 Results

Ping

What it does: Measures round-trip time and packet loss to a target, so you can tell where a network problem starts.

Steps:

1. Tap **Ping**.
2. Enter an IP address or domain in **Ping Address**, or pick **Gateway**, **google.com**, or **amazon.com** from **Quick access**.

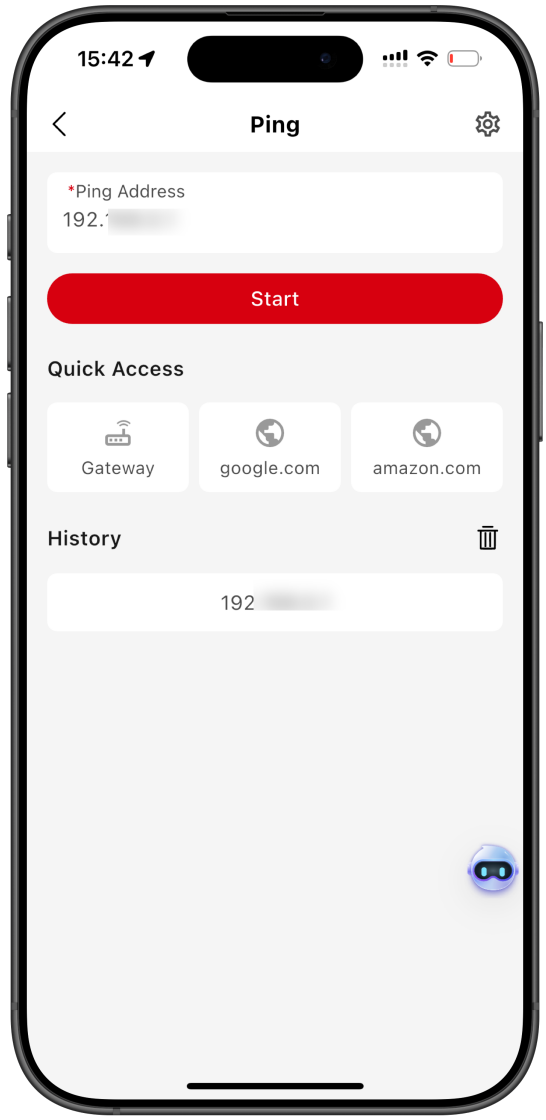


Figure 3-38 Ping

3. If needed, tap the gear at the top right for **Settings**, adjust the three sliders, and tap **OK**.

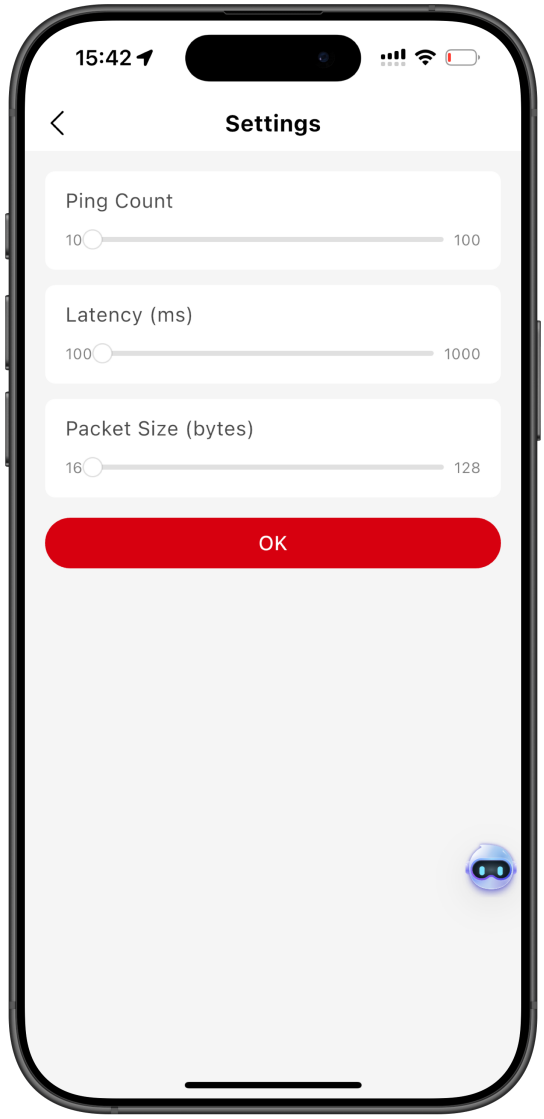


Figure 3-39 Settings

Parameter	Default	Range
Ping Count	10	10 to 100
Latency	500 ms	100 to 1000 ms
Packet Size	32 bytes	16 to 128 bytes

4. Tap **Start**. **Stop Test** is available at any time while it runs.
5. The result page grades the connection at the top, then shows packets sent, packets received, loss rate, and average latency, with a latency chart below.

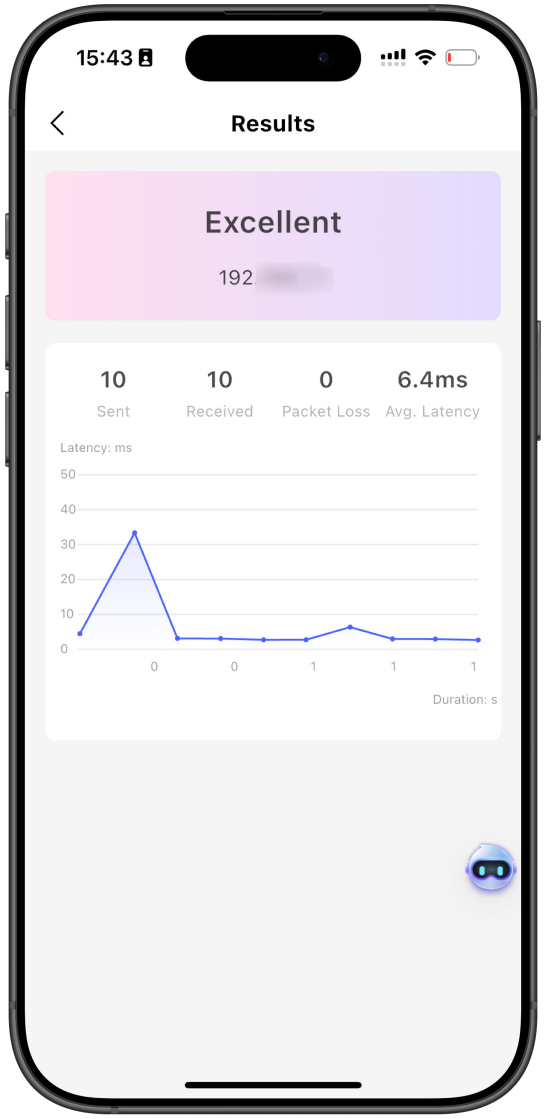


Figure 3-40 Results

Grade	Criteria
Excellent	No loss, under 50 ms
Good	Up to 5% loss, under 100 ms
Fair	Up to 20% loss, under 200 ms
Poor	Over 20% loss, or 200 ms and above
Unreachable	All timed out, DNS failed, or refused

Note

Tests are kept in **History**, where they can be reused one by one or cleared.

Batch Restore

What it does: Restores factory defaults in bulk. **All configuration on the device is erased**, and the device returns to the not-activated state.

Prerequisites: The devices are activated.

Steps:

1. Tap **Batch Restore**.
2. Select the devices and verify the password. Tap **Next**.

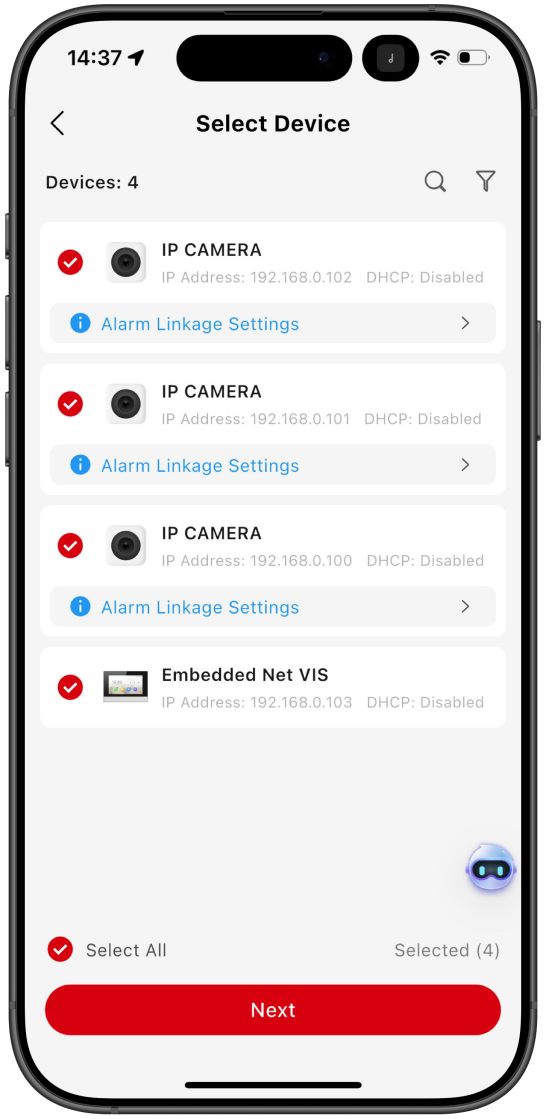


Figure 3-41 Select Devices

3. Read the confirmation dialog, make sure the devices stay powered, and tap **OK**.

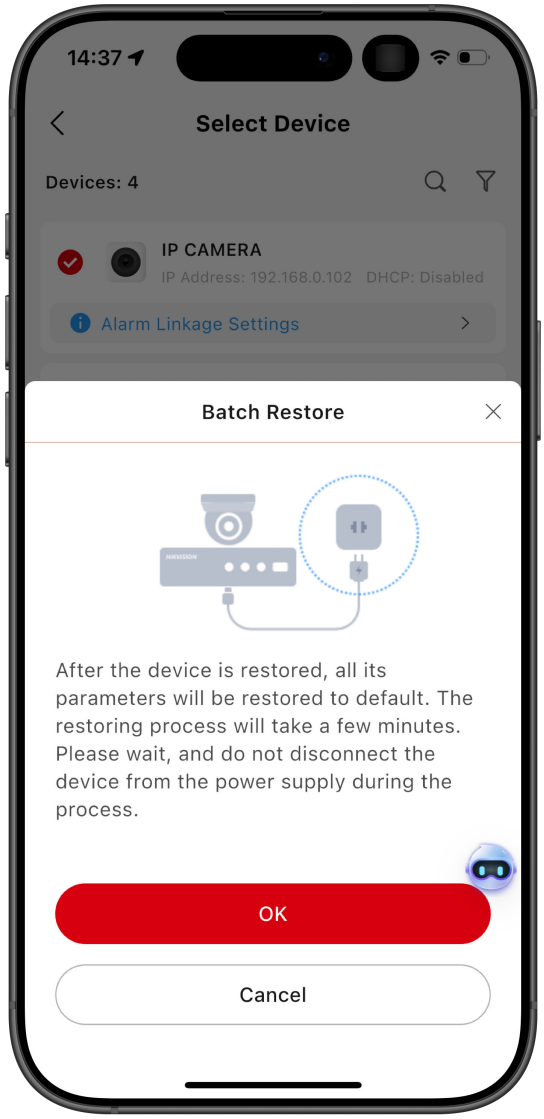


Figure 3-42 Stay Powered

4. While it runs the page warns not to cut the power.
5. On the result page the devices are tagged **Inactivated**.

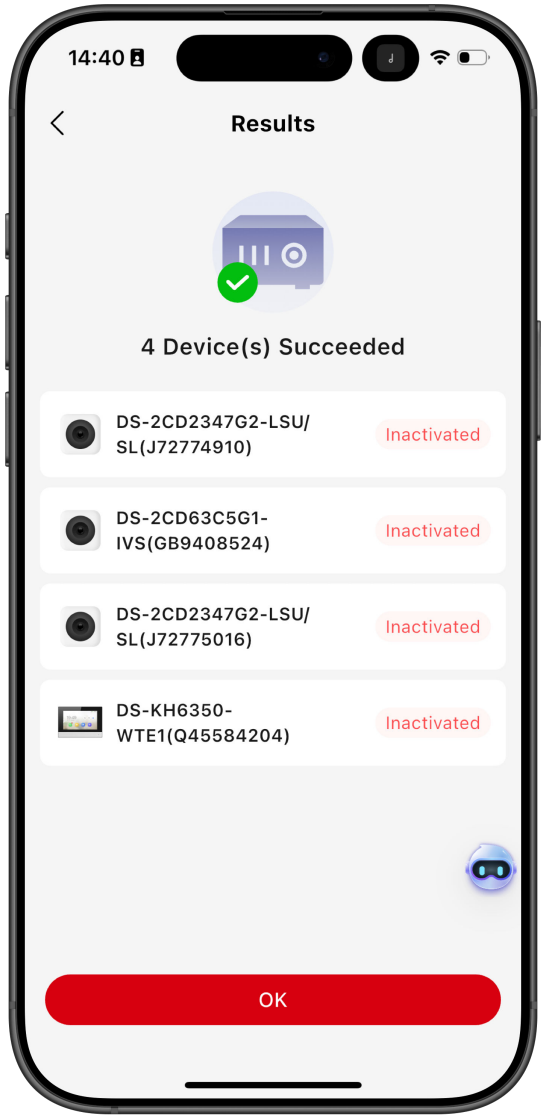


Figure 3-43 Results

Batch Reboot

What it does: Reboots devices in bulk.

Prerequisites: The devices are activated.

Steps:

1. Tap **Batch Reboot**.
2. Select the devices and verify the password. Tap **Next**.
3. Read the confirmation dialog, make sure the devices stay powered, and tap **OK**.

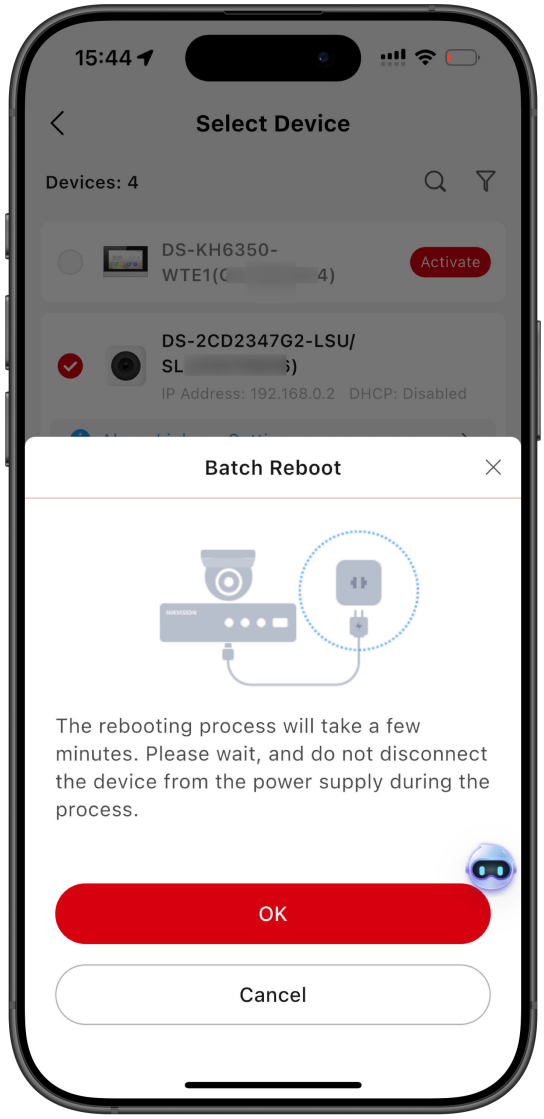


Figure 3-44 Stay Powered

4. While it runs the page warns not to cut the power.
5. On the result page the devices are tagged **Rebooted**.

Note

If you leave, the device card keeps showing the reboot status.

Time Sync

What it does: Pushes **the phone's current time** to the devices.

Prerequisites: The devices are activated.

Steps:

1. Tap **Time Sync**.
2. Select the devices, verify the password, and tap **Next**.
3. On the result page the devices are tagged **device time synced with phone time**.

Note

This syncs the time only; it does not change the device's time zone or daylight saving. Use the device's remote configuration for those.

Video Device Health Checks

Where to Run It

Select a video device in the SADP Tool (either **Professional** or **Quick Deploy** mode), verify its password, and the device page offers three checks: motion detection config check and recording check (including recording config check and storage check). Network cameras and NVR/DVR are both supported.

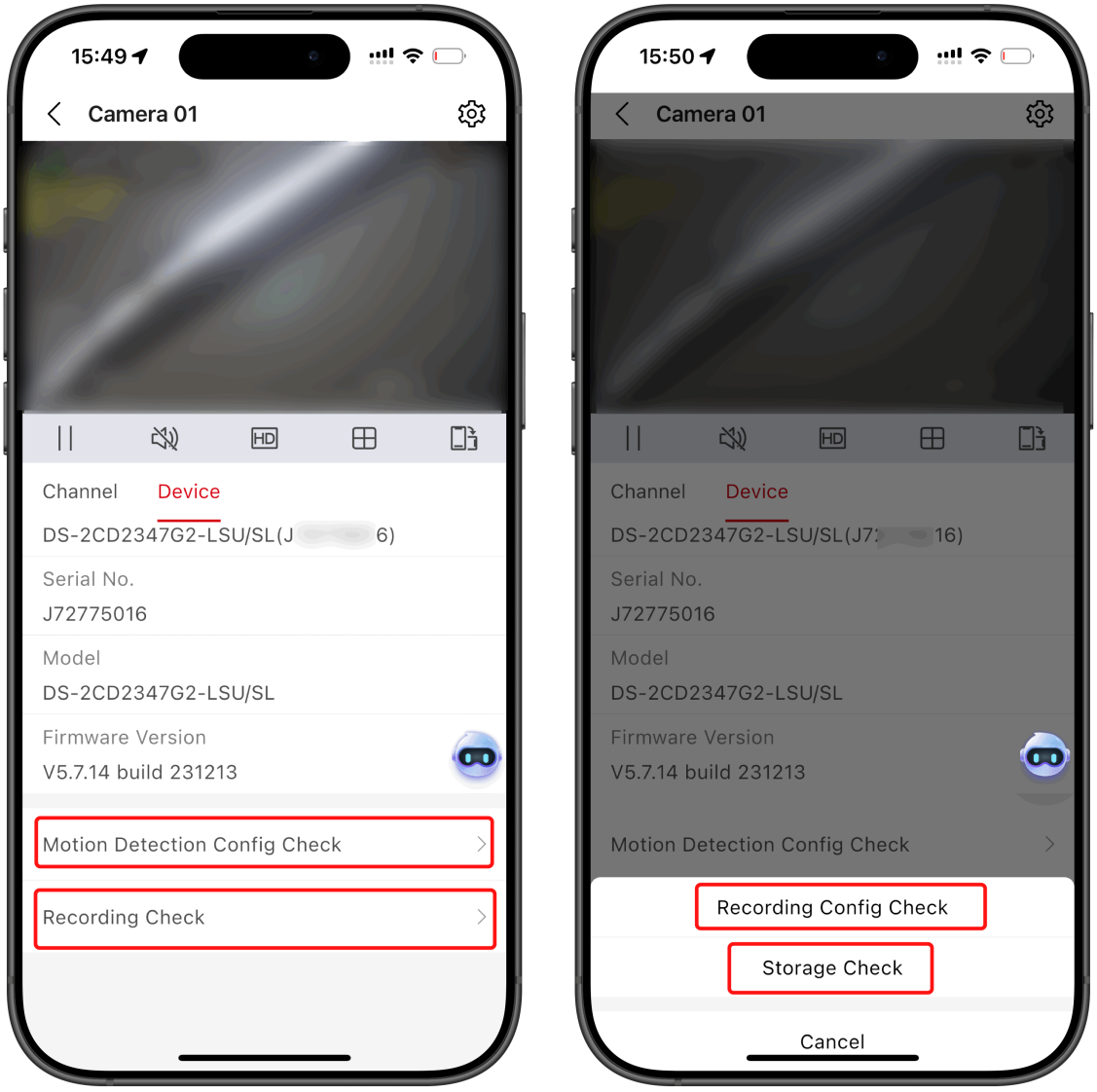


Figure 3-45 Run Check

- On a network camera the check runs at device level.
- On an NVR or DVR it runs per channel: the channel list comes first (channel number, online status, IP address, name), and tapping a channel opens its result.
- Offline channels, and idle channels with no device attached, cannot be checked.

These three checks are the last confirmation before handover: that the system will really record and really alarm.

Motion Detection Check

Four items are checked: **Motion Detection Algorithm Enabled**, **Detection Area Drawn**, **Detection Time Set**, and **Alarm Message Reporting Configured**.

Failed items show **×** and the **Configure All** button appears at the bottom, which fixes the failed items for you.

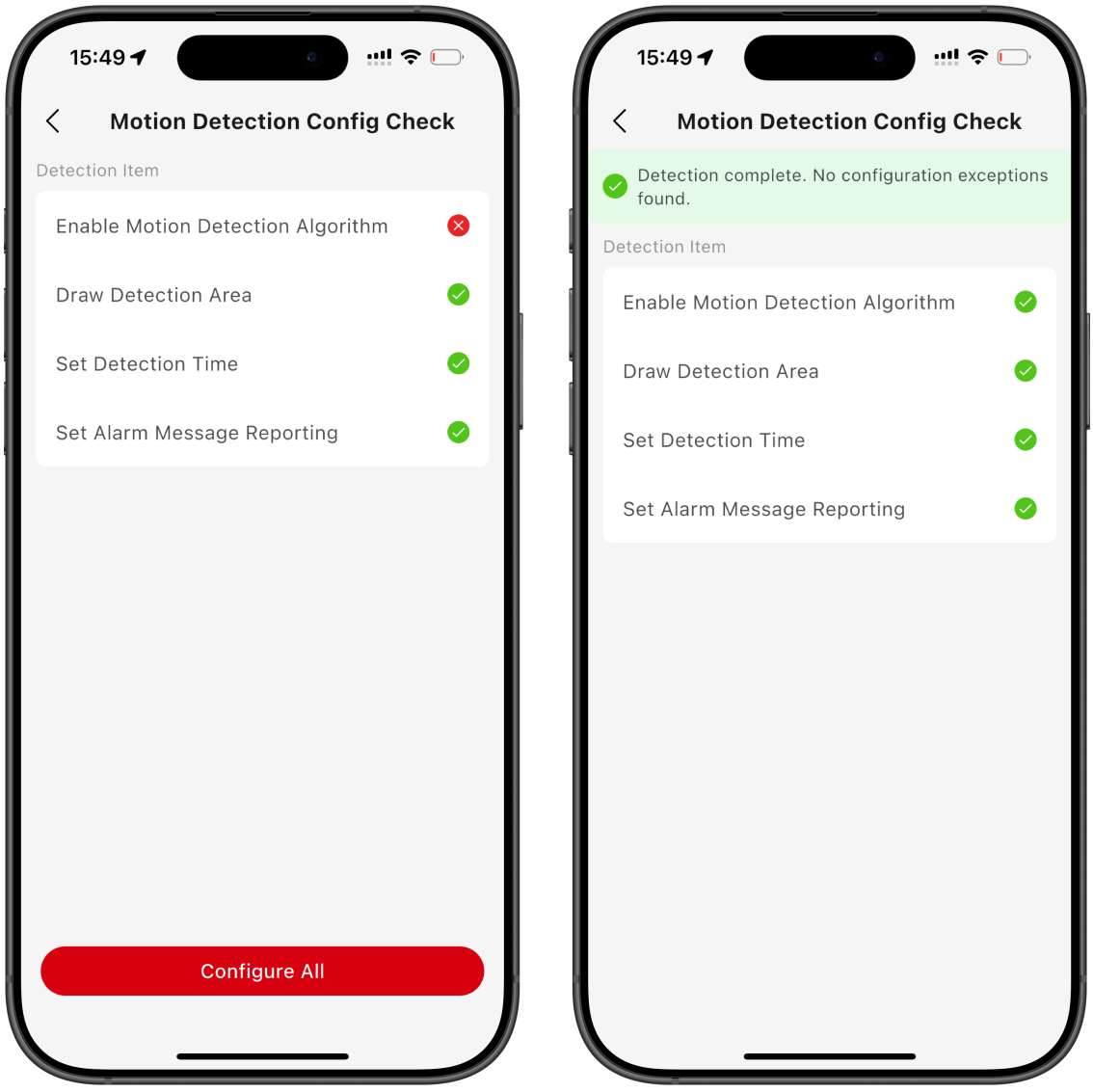


Figure 3-46 Motion Detection Check

Recording Config Check

Six items are checked. Not only recording itself, but the motion detection configuration that triggers it:

Note

For 24/7 recording settings, the motion detection configuration will not be checked here.

1. **Recording Enabled**
2. **Recording Schedule Set**
3. **Motion Detection Algorithm Enabled**
4. **Motion Detection Area Drawn**
5. **Motion Detection Schedule Set**
6. **Recording Linkage Enabled for Motion Detection**

Failed items show **×** and the **Configure All** button appears at the bottom, which fixes the failed items for you.

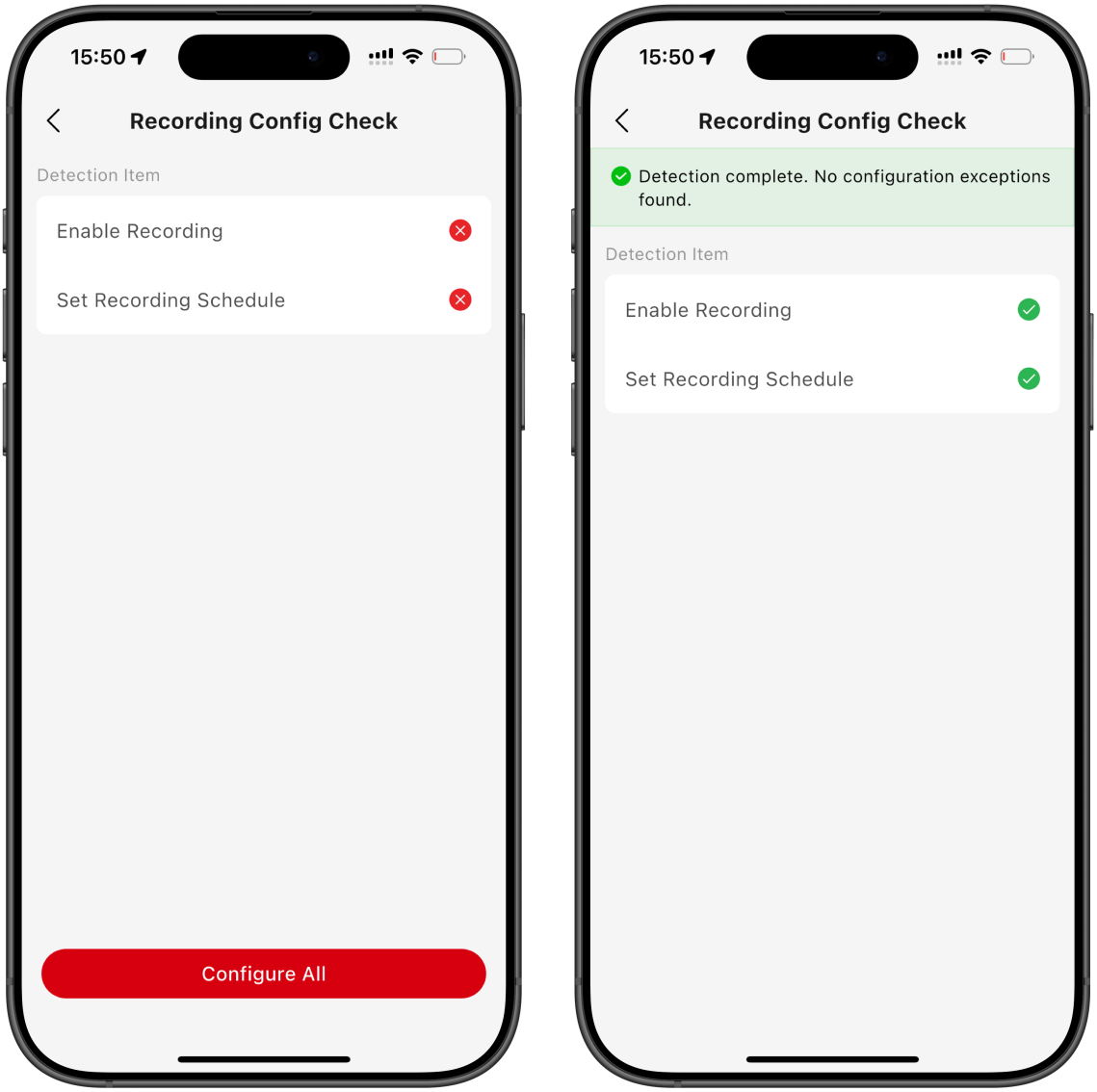


Figure 3-47 Recording Config Check

Storage Check

The storage check reports one medium at a time. On a network camera it checks the memory card, on an NVR or DVR the hard disks. Where there is more than one, each gets its own card and can be selected individually.



Figure 3-48 Storage Check

The Four States

The table gives what the page says for each state, and what you should do.

State	What to do
Not inserted or detected	Fit the medium or add one first, and check again.
Not initialized, which may stop the device recording.	Tap **Initialize**.

State	What to do
Faulty	Try initializing it, or replace it and check again.
Healthy, with the free capacity	Nothing to do.

Initializing

1. Select the media to handle and tap **Initialize SD card** / **Initialize HDD** at the bottom (**Initialize All** when several are selected).
2. The confirmation explains that the disk or card will be formatted and all data on it deleted; afterwards the medium can be used for recording again, but **the existing data cannot be recovered**. Tick the acknowledgement and tap **Confirm**.
3. The page shows the progress percentage.
4. On success the state becomes healthy. On failure the page shows the reason with a **Retry** button.

Note

Initializing formats the medium and deletes every recording on it. Confirm that anything important has been backed up first.

Loop Recording

Even when the medium is healthy, the check flags **Loop recording is off** separately: once the card is full, new recordings cannot be saved. You can tap **Enable** to turn it on, after which the oldest files are overwritten automatically when the space runs out.

This is the item most often missed: the medium is fine and recording is on, but once it fills up the device quietly stops recording.

3.1.4 AI Config Assistant: Scenario-Matched Configuration Recommendation

What This Is and When to Use It

In One Sentence

A chat assistant called **AI Config Assistant** can propose how to configure an AX PRO panel. It reads the peripherals already paired with the panel, works out what kind of premises this is, asks a few questions, and then offers a **configuration template** that you can preview and adjust, or apply in one action.

The Problem It Solves

Hik-Partner Pro already has configuration templates (***Template Center: How to Use Device Configuration and Handover Templates***), but they assume **you already have a good template**. For an installer new to alarm work, producing that first one is itself the obstacle. The hard part is translating what a customer wants day to day into the professional logic underneath: which zones should be 24-hour zones, how long the entry and exit delays should be, whether the system needs several areas.

The **AI Config Assistant** provides the industry know-how.

When to Choose AI Config Assistant Instead of Templates

/	AI Config Assistant
Situation	You have no usable template, or are unsure how this site should be configured.
How	Describe the premises and let **AI Config Assistant** propose one.
Result	A recommended template you can preview, adjust, and apply.
The other route	If you already have a tuned template, you can simply reuse it via the configuration template feature.

Scope

Item	Description
Devices	AX PRO 1.3.x wireless panels and their wireless peripherals.
Clients	Both the Portal and the Mobile Client, with the same capability.
Charging	The basic recommendation is free for all registered users.

Before You Start

Three Prerequisites

1. **The panel is online.**
2. **Every peripheral has been added.** The recommendation infers the scenario from the paired peripheral list, and one missing detector can push it to a different scenario.
3. **The panel is disarmed.** Deploying a configuration while armed may fail.

Entry Points in the Mobile Client

1. The **Mobile Client** offers it at two moments: automatically after the add-device flow finishes, or go to the **Site** page, enter the target site, find the device, and tap the device's **…** → **Configure Control Panel** .

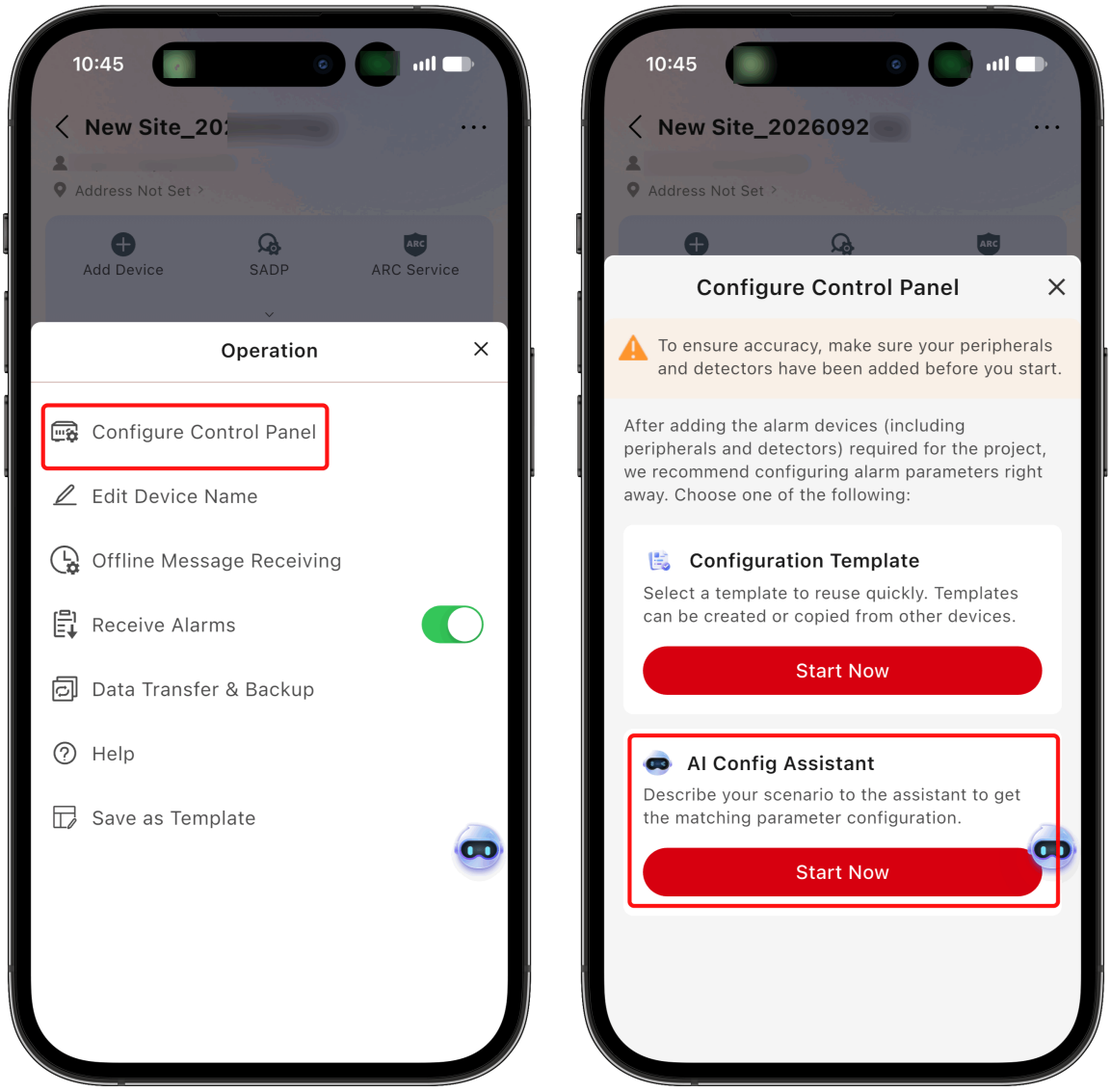


Figure 3-49 Entry (Mobile Client)

2. Tap **Start Now** in the **AI Config Assistant** section.

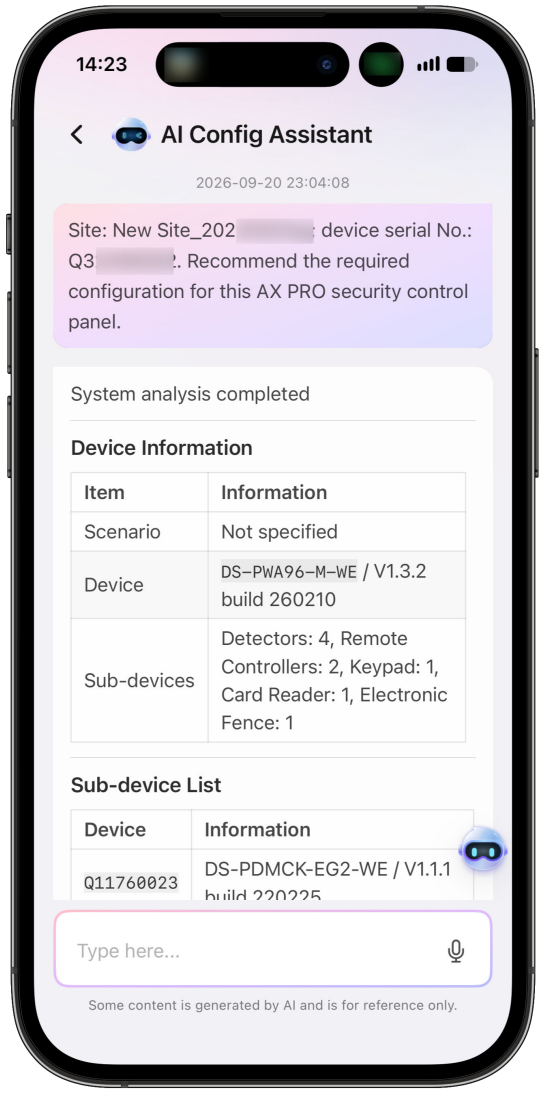


Figure 3-50 AI Config Assistant

Entry Points on the Portal

1. The **Portal** offers it at two moments: automatically after the add-device flow finishes, or go to **Site & Device → Customer Site** . Find the deice, click the **Configure Control Panel** icon on an AX PRO card or list row.

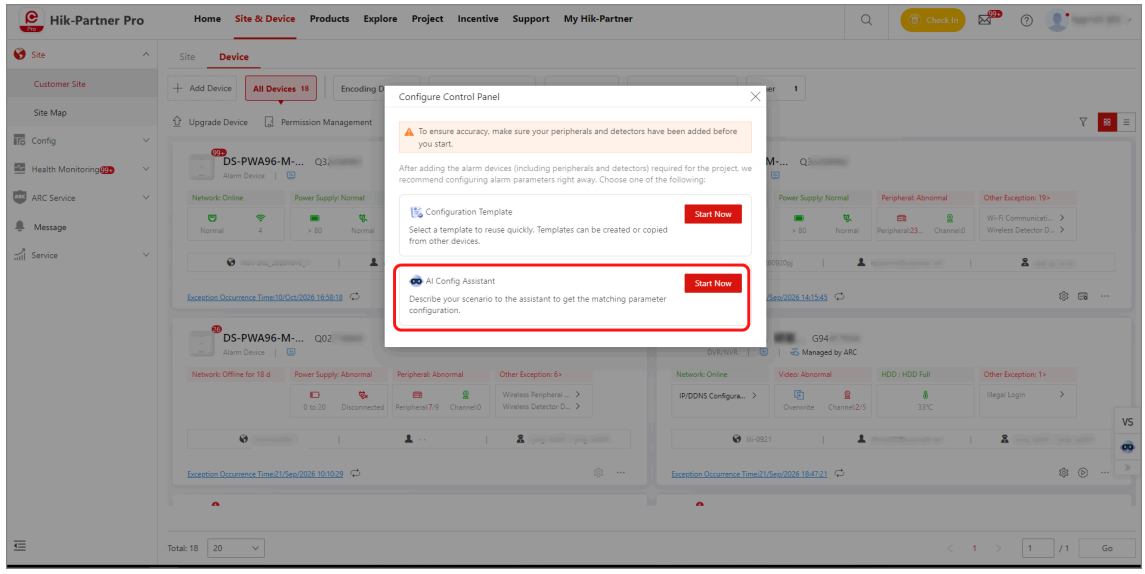


Figure 3-51 Entry (Portal)

2. Click **Start Now** in the **AI Config Assistant** section.

Example: One Complete Conversation

Six steps, from opening the assistant to a deployed configuration. The Portal and Mobile Client show the same content; only the layout differs.

1. Check What the Assistant Read

The assistant opens with **System analysis completed** and lists the panel's model and firmware, the peripheral counts, and every peripheral by serial number.

One thing to do here: check the peripheral list. If a device is missing, go back and add it first. The whole recommendation is built from this list, and one missing detector can point it at the wrong kind of premises.

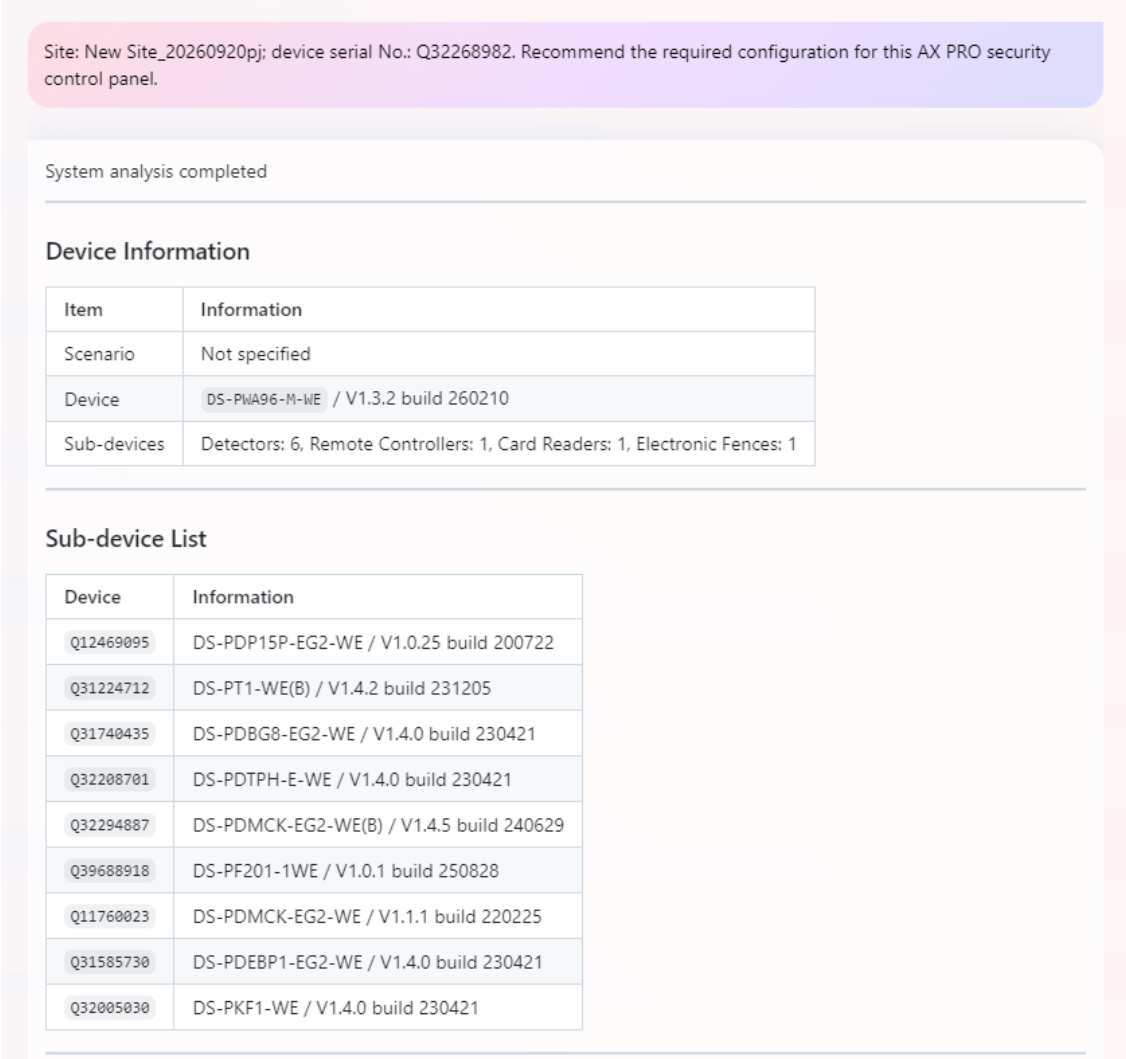


Figure 3-52 Device Info and Peripheral List

2. Read the Candidate Plans

Candidate plans follow, each with a **Match level** of **High**, **Medium** or **Low**.

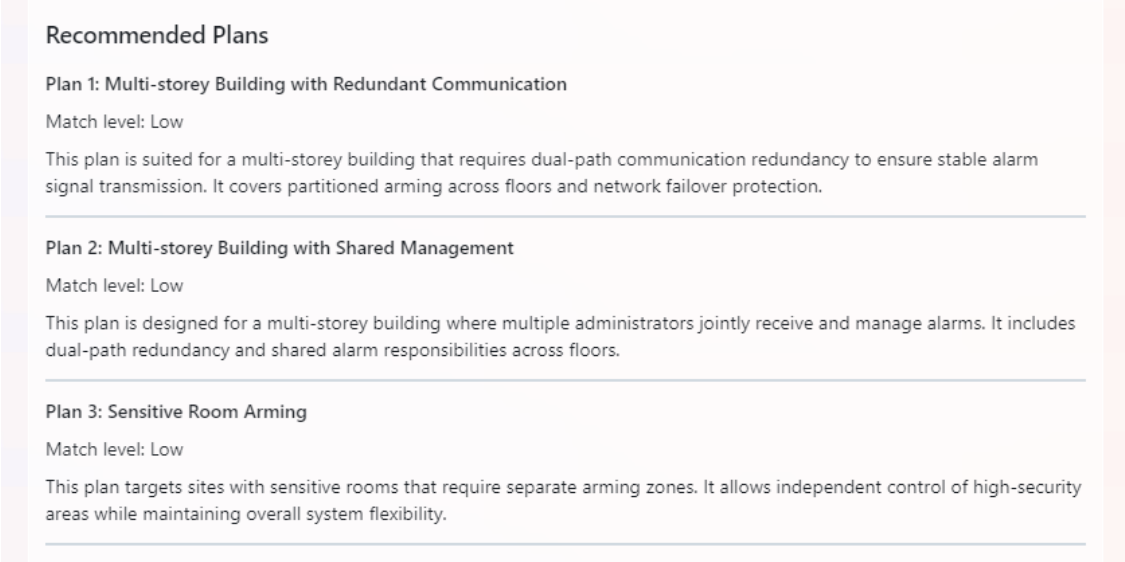


Figure 3-53 Candidate Plans

3. Answer the Questions, or Just Describe the Site

The assistant presents a numbered **Confirmation Checklist**: building structure, dual-path communication, multiple people receiving alarms, rooms that need separate arming, and the like. Three ways to answer, all accepted:

1. **By number. Yes to 1 and 2, No to 3 and 4**. When one question is left, a bare **No** or **Yes** is enough.
2. **Ignore the questions and describe the site.** For example, "we need professional ARC monitoring at home", or "burglary at night is the worry, and the house is empty from eight to five on weekdays". The assistant takes the facts out of what you wrote and carries on. **This way is quicker whenever a question has no clear answer, or it asks about something that is not your concern.**
3. **Mix the two.** Answer a question or two, then add a sentence of your own.

Several facts in one message cuts the number of rounds noticeably. To drop everything and begin again, reply **restart recommendation**.

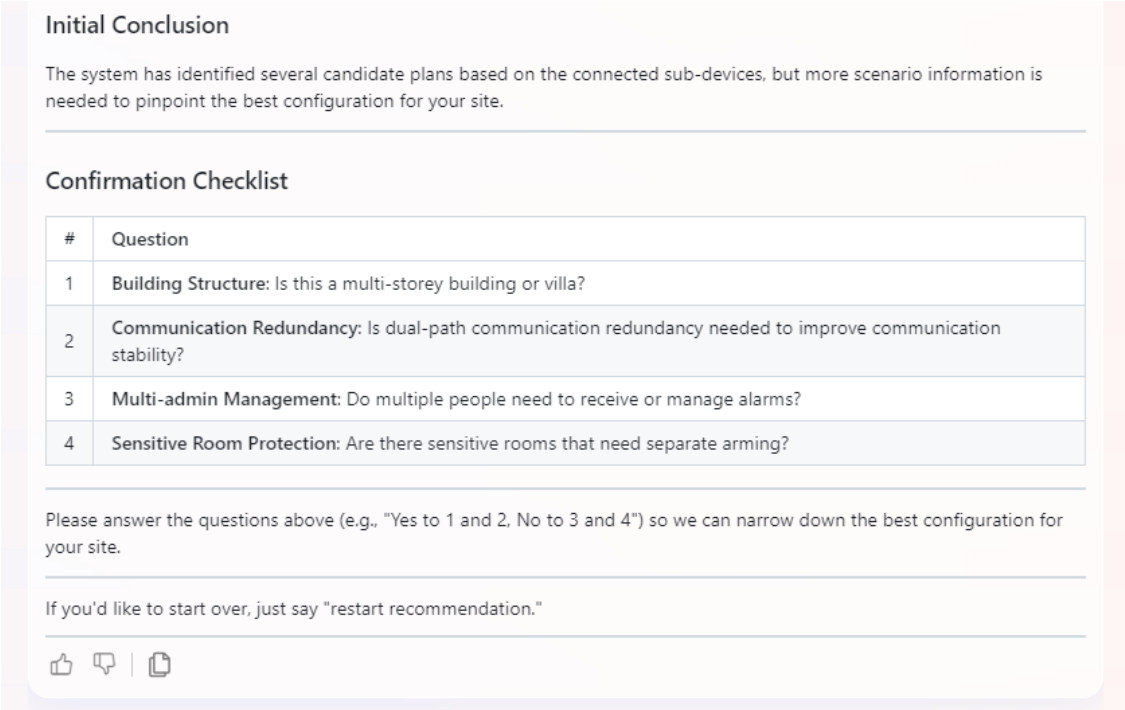


Figure 3-54 Answer Questions

4. Keep Answering Until It Settles

Each answer brings one reply: what it ruled out, the re-ranked candidates, and whatever is still open. Answer specifically and two or three rounds are usually enough.

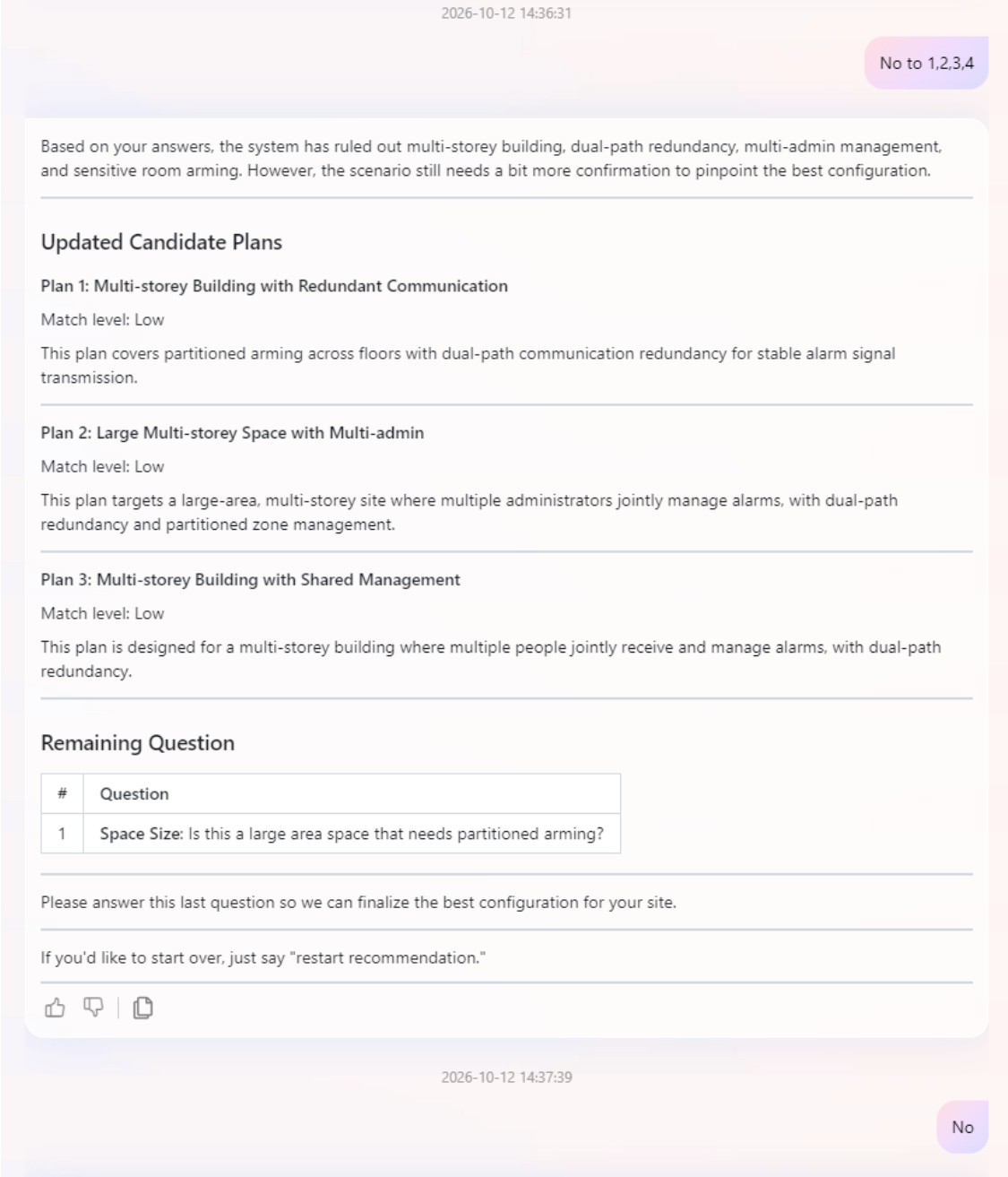


Figure 3-55 Keep Answering

5. Confirm the Final Plan

Once it has enough, the assistant returns **Recommendation Complete**: the plan name, the **Recognized scenario** it settled on, a template card with **Preview/Edit** and **Apply Now**, and a short list of what the configuration is tuned for.

Read the "Recognized scenario" line first: It carries the assistant's whole understanding of the site. If it is wrong, add more detail or reply **restart recommendation** rather than applying.

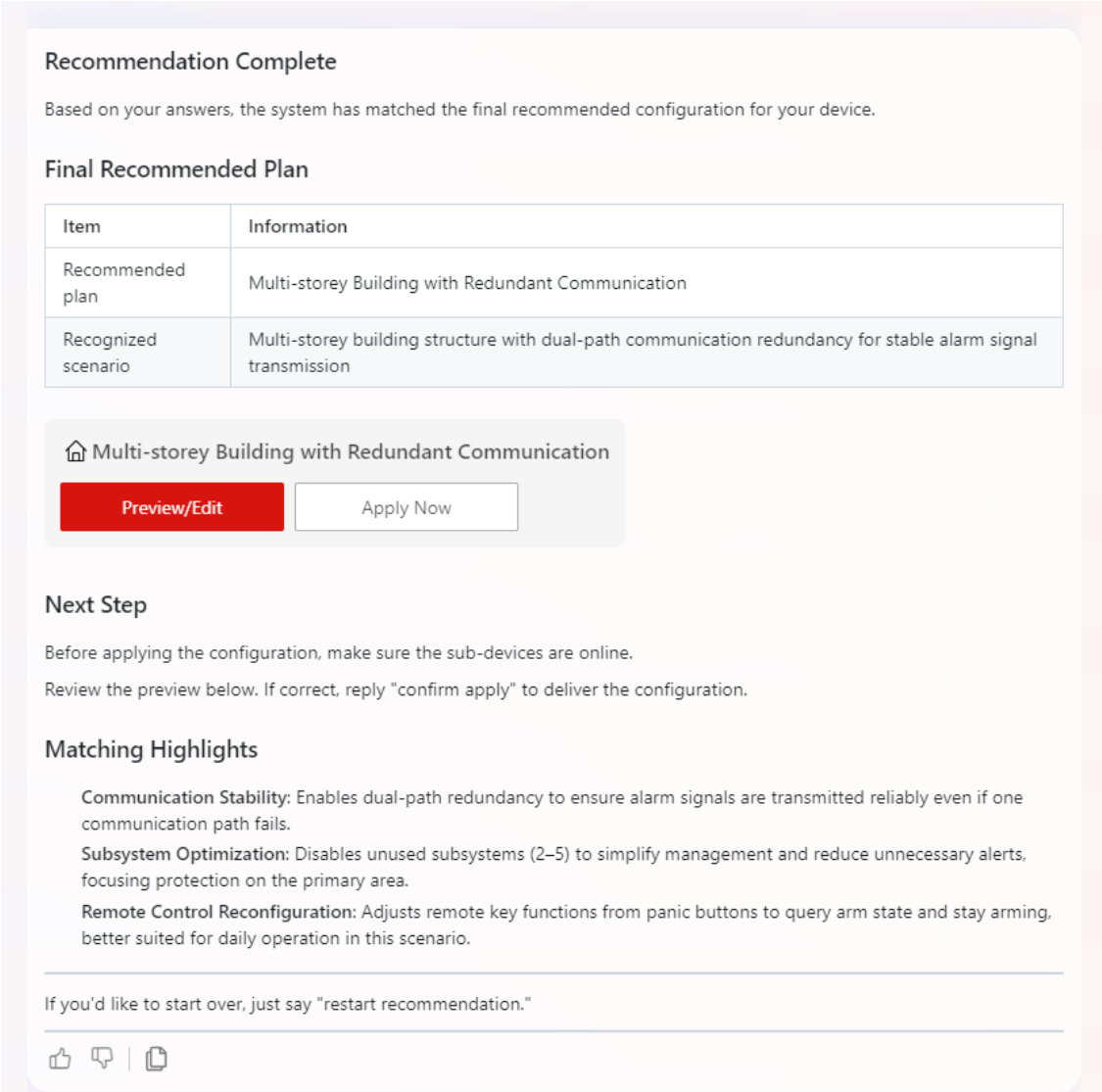


Figure 3-56 Final Plan

To go through the settings one by one, tap **Preview/Edit**: it opens the panel's remote configuration page (**Basic Information**, **Time Settings**, **Control Panel Options**, and so on). Edit if needed, save and go back, and the proposal carries your edits. If nothing needs changing, skip it.

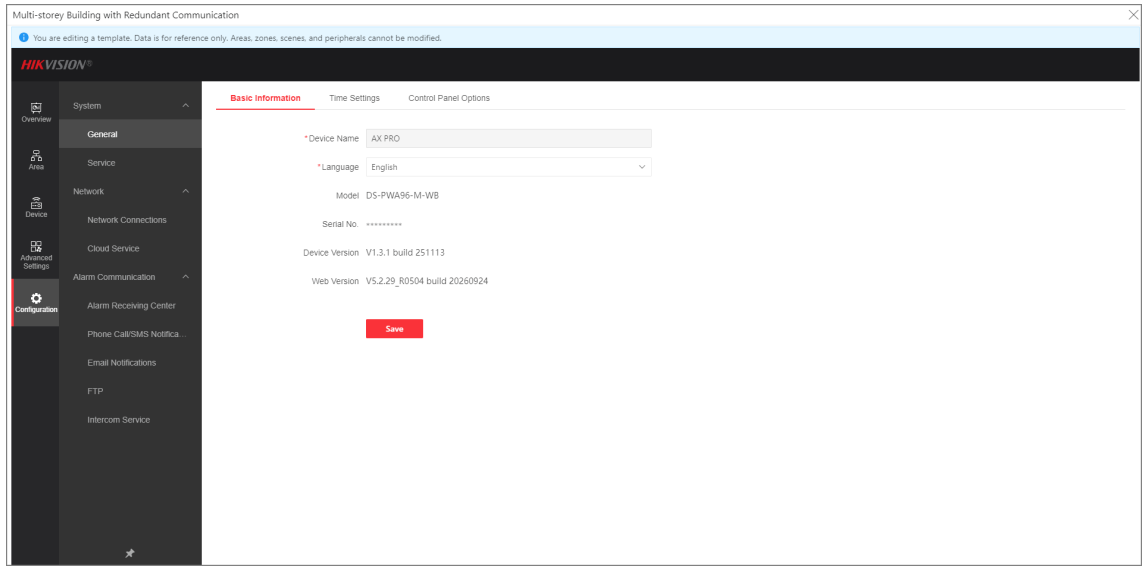


Figure 3-57 Edit in Remote Configuration Page

6. Apply and Check the Result

Make sure the peripherals are online first. Click/tap **Apply Now**, or reply **Apply Now** in the input box.

The assistant answers with a receipt showing **Configuration Application Submitted**. **That means deployment has started, not that it has finished.**

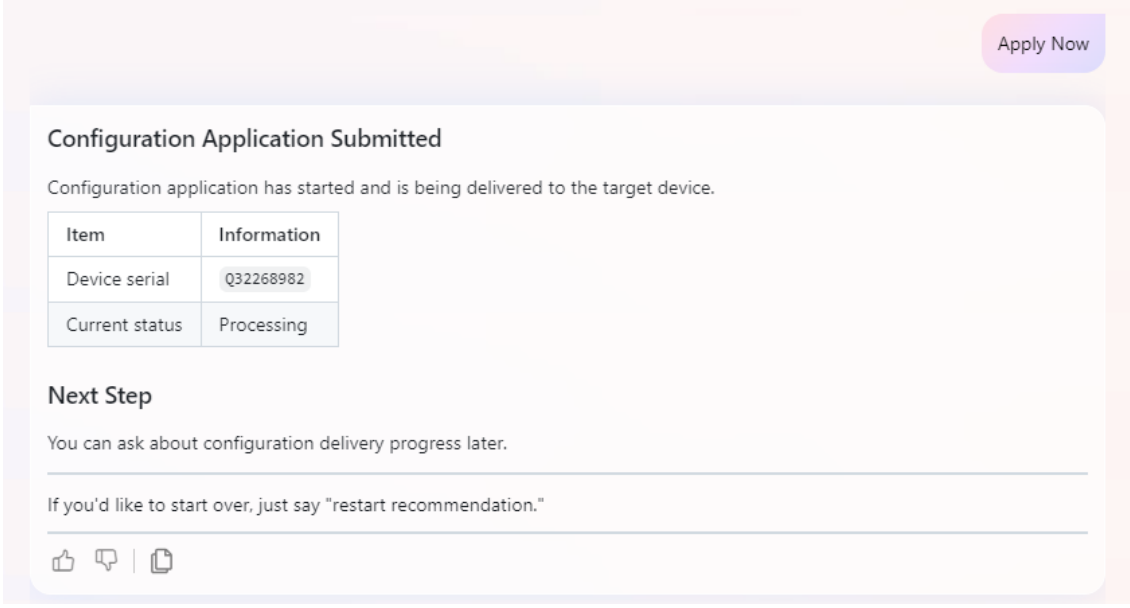


Figure 3-58 Apply Now

A moment later, you can type **Delivery progress** to see the outcome:

- **All successful**: Each change is listed, with the reason for it.

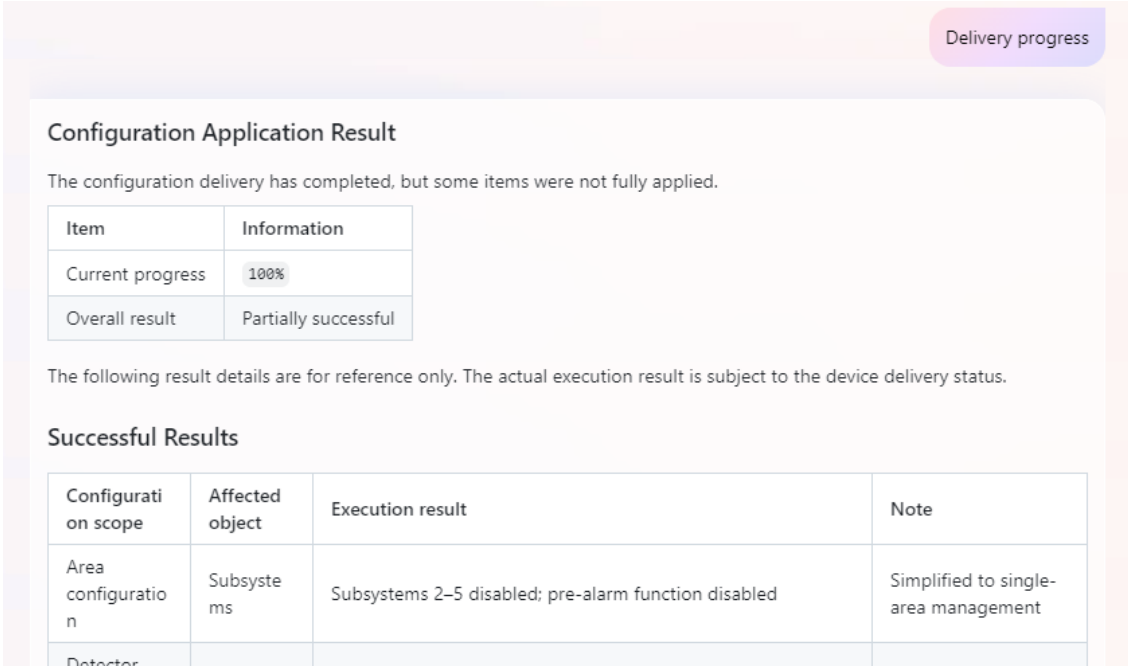


Figure 3-59 Successful Results

- **Partially successful or failed**: The **Failed Results** table gives the reason and a **Suggestion**.

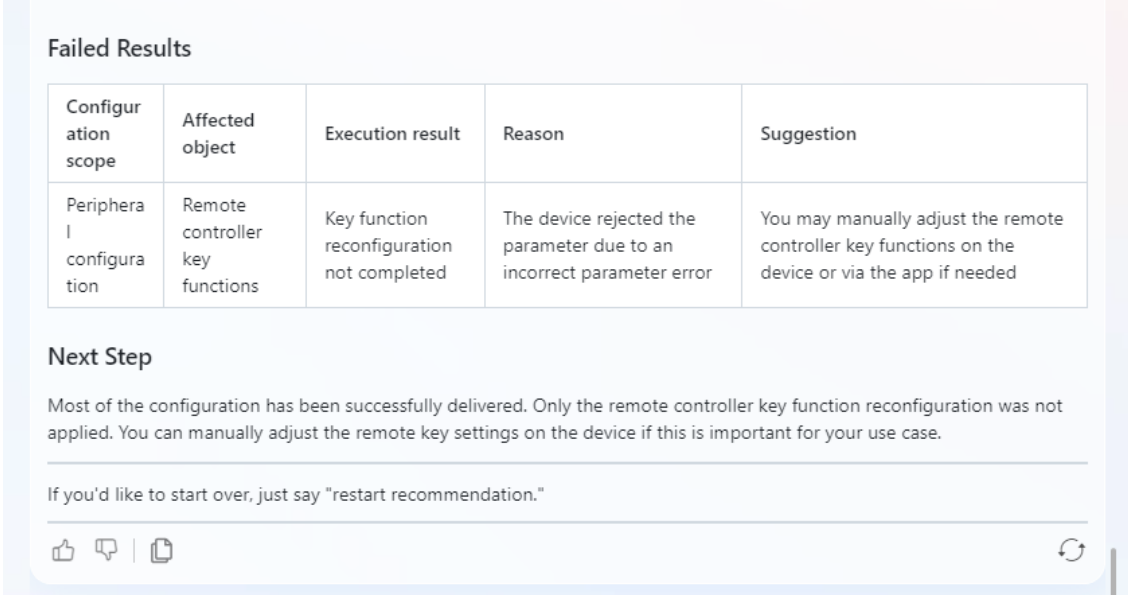


Figure 3-60 Failed Results

How to Get Better Recommendations

- **Finish installing before you start the conversation.** The first step reads the peripheral list, and one missing detector can push the result to a different scenario.
- **Pack several facts into one sentence.** "There is a pet, it reports to an ARC, nobody is home on weekday afternoons" gets a sharper answer than three separate messages.
- **Check the "scenario recognized" block.** That is the assistant's understanding of your project; correct it before applying rather than after.
- **When unsure, use "Preview/Edit".** Reviewing each setting first is cheaper than fixing it afterwards.

3.1.5 Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance

You can select an adding method according to your needs and the device types. Hik-Partner Pro accesses devices by two modes: Hik-Connect (P2P) and Device IP Address / Domain Name, providing different capabilities.

Device Access Mode

Table 3-5 Device Access Mode

Device Access Mode	Device Adding Method	Description of Access Mode
Hik-Connect (P2P)	Scan for Devices on LAN Scan for	• Full access to features based on the Hik-Connect service, such as remote configuration, health monitoring, etc. • Securer data communication (between the platform and devices).
	Enter Serial Number	
	Scan Device QR Code	
	Synchronize Devices from Hik-Connect	
IP Address / Domain Name	Add a Single Device: Enter IP Address / Domain	• Faster data communications. • No access to the features based on the Hik-Connect service.
	Add Devices in a Batch: Import IP Addresses / Domains	

Device Adding Methods Supported by Different Device Types

Table 3-6 Device Adding Methods

Adding Method / Device Type	Encoding Devices	Security Control Panels	Access Control Devices	Video Intercom Devices	Network Devices	Radars	Audio	Doorbells
Add by IP Address or Domain Name	√	×	×	×	×	×	×	×
Add by Scanning QR Code	√	√	√	√	√	√	√	√
Add by Entering Serial No.	√	√	√	√	√	√	√	√
Add Devices on LAN (via SADP Tool)	√	×	√	√	√	√	√	×
Add Devices After Batch Configuring Them on LAN (via On-Site Config)	√	×	×	×	×	×	×	×
Synchronize Devices with Hik-Connect Account	√	√	√	√	√	√	√	√

Detailed Instructions for Device Adding

Select one of the following ways to enter the Add Device page.

- For Portal:
  Click **Site & Device → Customer Site** to enter the Customer Site page.

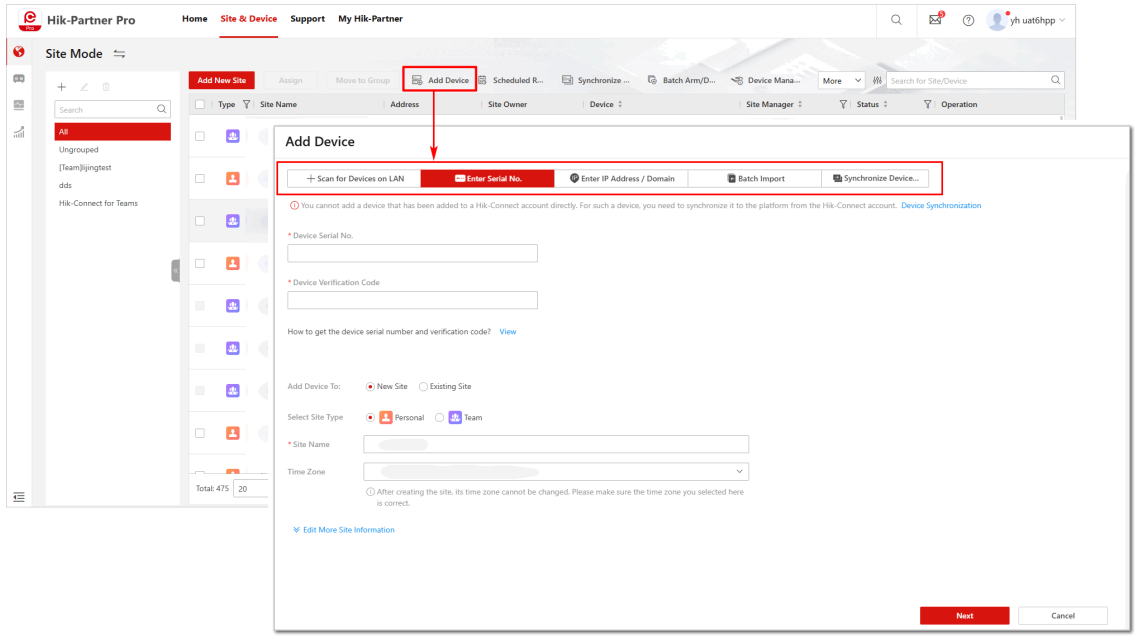


Figure 3-61 Add Devices on Portal

- For the Mobile Client:

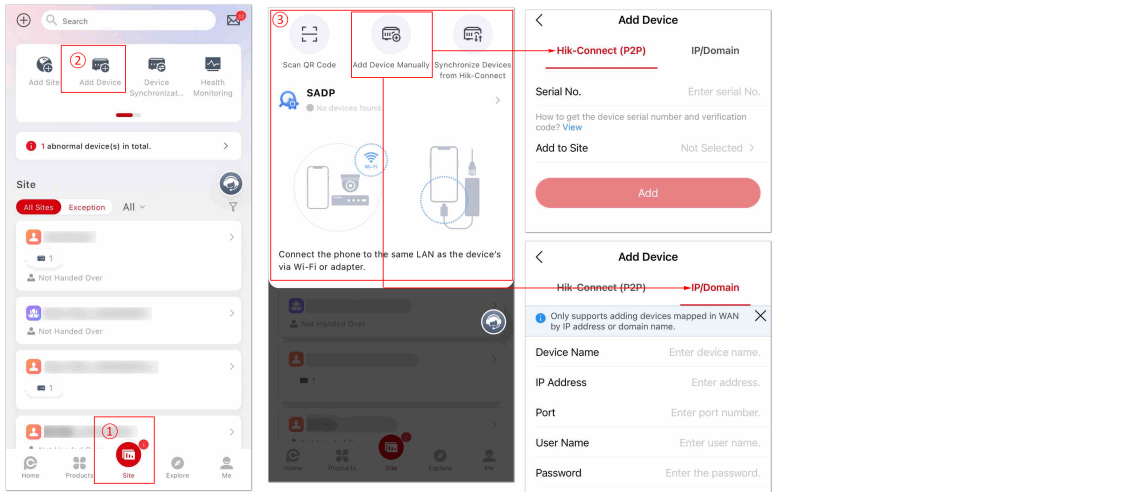


Figure 3-62 Add Devices on Mobile Client

Before you begin:

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.
- Make sure the device has been activated and connected to Hik-Connect service.

Table 3-7 Methods of Adding Devices

Adding Methods	Application Scenario
Add by IP Address or Domain Name	• You can use the method if you know the IP address or domain name of a device. • Only encoding devices mapped in WAN support this function. • When you need to share devices via QR code. Ask your customers to download or update the Hik-Connect Mobile Client (V 4.15.0 or later), so you can share the device by sending the QR code generated after the device setup or the download link shown in the banner on the Home page to them. • Devices added in this mode do NOT support the device handover process. If you need to hand over a device, please add detected LAN devices or add devices by entering serial No.
Add by Scanning QR Code (Only Mobile Client)	You can add a device to a site by scanning the QR code on the device, or add multiple devices to a site by scanning the QR code generated by iVMS-4200 or iVMS-4500.
Add by Entering Serial No.	If a device is connected to Hik-Connect service, you can manually add it to a site by entering the device serial number and device verification code. Enter the device serial number and device verification code. **Note** The device serial number and the default device verification code are usually on the device label. If no device verification code found, enter the verification code you created when enabling Hik-Connect service. Upgrade the device firmware version, or some functions (including health monitoring, linkage, and remote configuration) cannot be used if the device is not compatible with the Hik-Partner Pro.
Add Devices After Batch Configuring Them on LAN (via On-Site Config)	After the devices on LAN are batch configured, select the device(s) to be added, and add the device(s) to an existing or a new site.
Synchronize Devices with Hik-Connect Account	In the following two cases, you need to synchronize devices in the Hik-Connect account with devices in the Hik-Partner Pro account. • Before using Hik-Partner Pro, you managed the devices for the customer by the Hik-Connect Mobile Client after the customer shares her/his devices to your Hik-Connect account. • Before using Hik-Partner Pro, you already have a Hik-Connect account and have added device(s) to it.

Adding Methods	Application Scenario
	1. Log in to **Hik-Connect** by entering your account or by scanning QR code. 2. Select the devices for synchronization. 3. Set the site information in Hik-Partner Pro for your devices to be synchronized. 4. Set the site information in Hik-Partner Pro and set the device permission for the devices shared to you. 5. (Optional) Set the time zone of the devices if needed. 6. Start device synchronization.
Add Devices to Hik-Partner Pro or Hik-Connect Using the SADP Tool	1. Tap **Add** in the Site & Device area on the Home page. 2. Tap **SADP**. Tap **Activate** to activate and initialize the devices to be added if they are not activated. 3. Tap **Complete** to enter the Add to Hik-Partner Pro page. If you do not select a site in Step 1, you can tap **Existing Site** to select an existing site to add the devices to, otherwise, the devices will be added to an automatically-created new site. 4. Tap **Add to Hik-Connect** to switch to the page for adding devices to Hik-Connect. 5. Select the devices to be added and tap **OK**. 6. Scan the device QR codes with your Hik-Connect Mobile Client to finish the device adding.

3.1.6 How to Get the Device Serial Number and Verification Code?

Network Camera

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	×	√ **Configuration → System → System Settings → Basic Information**
Verification Code	×	×	√ **Configuration → Network → Advanced Settings → Platform Access**

PTZ Camera

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	×	√ **Configuration → System → System Settings → Basic Information**
Verification Code	×	×	√ **Configuration → Network → Advanced Settings → Platform Access**

Thermal Camera

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	×	√
Verification Code	×	×	√

DVR/NVR

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	√ **Maintenance → System Info → Device Information**	√ **Configuration → System → System Settings → Basic Information**
Verification Code	×	√ **System → Network → Advanced → Platform Access**	√ **Configuration → Network → Advanced Settings → Platform Access**

NVS

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	×	×
Verification Code	√ Scan QR Code	×	×

Access Control Device (Fingerprint Access Control Terminal)

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	√ **Info. → Device**	×
Verification Code	×	√ **Comm. → Mobile-App**	×

Security Control Device

Note

For AX HOME

- The AX HOME device does not have a verification code. To add AX HOME to Hik-Partner Pro, you only need the device serial number.
- You can add AX HOME to Hik-Partner Pro successfully only using the Hik-Partner Pro Mobile Client, because the Portal requires a verification code, which AX HOME does not have.

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	×	√ **Engineer Maintenance → Device Information**
Verification Code	√ Scan QR Code	×	√ **Communication → Cloud Service**

Video Intercom Device

How to Get		On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Door Station	Serial Number	×	×	√ **System → Device Information**
	Verification Code	√	×	×
Indoor Station	Serial Number	√	√ **Settings → More → Device Information**	×
	Verification Code	√	√ **Settings → Configuration → Hik-Connect**	×

Doorbell

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	×	×
Verification Code	√	×	×

AC Router

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	×	√
Verification Code **Note** The AC router does not have a verification code and does not need one to enable the Hik-Connect service.	×	×	×

Healthcare Radar

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	×	√
Verification Code **Note** The verification code of the healthcare radar is dynamic and keeps updating.	×	×	√

Network Speaker

How to Get	On Device Label	On Device Local Configuration Page	On Device Web Configuration Page
Serial Number	√	×	√
Verification Code	√ Scan QR Code	×	√

On Device Label

In most cases, you can find the verification code or serial number on the device label (if any), which is stuck on the device or device package.

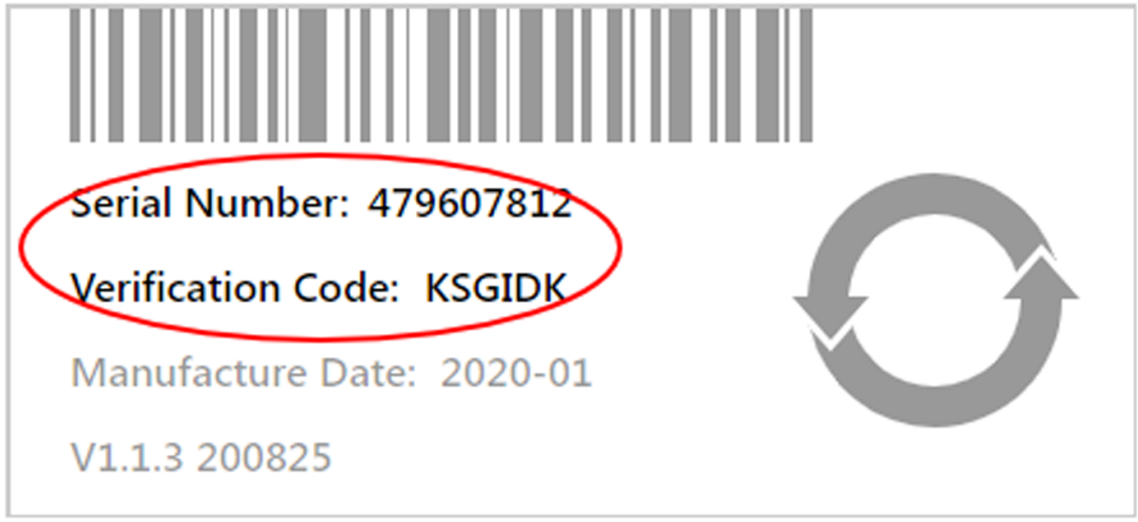


Figure 3-63 Device Label

On Device Local Configuration Page

For DVR and NVR, you can connect it to a monitor to view the device local GUI interface.
For indoor station and access control device, you can log into the device and enter its home page.

Note

On the device local configuration page, if the serial number you find is long and complete (more than 9 characters), then the one you need is a 9-character string, the last character of which is the first digit from the end of the long serial number.
The following two examples show how to get the short serial number from the long one.

- DS-1ABCD2EFGH3IJKLMNOPQRSTUVWXY **Z123T45R6**
- DS-2ABCD2EFGHIJKLMNOPQRS **T123T45R6** UVWXYZ

On Device Web Configuration Page

Log into the device via a web browser by entering the device IP address in the address bar. You will enter the device Web Configuration page.

Note

On the device web configuration page, if the serial number you find is long and complete (more than 9 characters), then the one you need is a 9-character string, the last character of which is the first digit from the end of the long serial number.
The following two examples show how to get the short serial number from the long one.

- DS-1ABCD2EFGH3IJKLMNOPQRSTUVWXY **Z123T45R6**
- DS-2ABCD2EFGHIJKLMNOPQRS **T123T45R6** UVWXYZ

3.2 Batch Configure Devices on LAN

You can batch configure online devices on the same Local Area Network (LAN) with the PC on which the Hik-Partner Pro Portal runs. The available configurations include batch device activation and device IP address assignment, batch linking channels to NVR/DVR, and batch setting parameters for devices via templates. These functions allow you to complete basic configurations for multiple devices with much less effort compared with configuring devices one by one.

Note

- For entering the device batch configuration page for the first time, a video tutorial about how to batch configure devices on LAN will pop up and automatically play in the down-left corner.
- The functionality is only available to certain models of cameras, NVRs, and DVRs.
- Before batch configuring devices, make sure you have connected them to the same LAN with the PC on which the Hik-Partner Pro Portal runs.

The flow chart for batch configuration of devices is shown below.

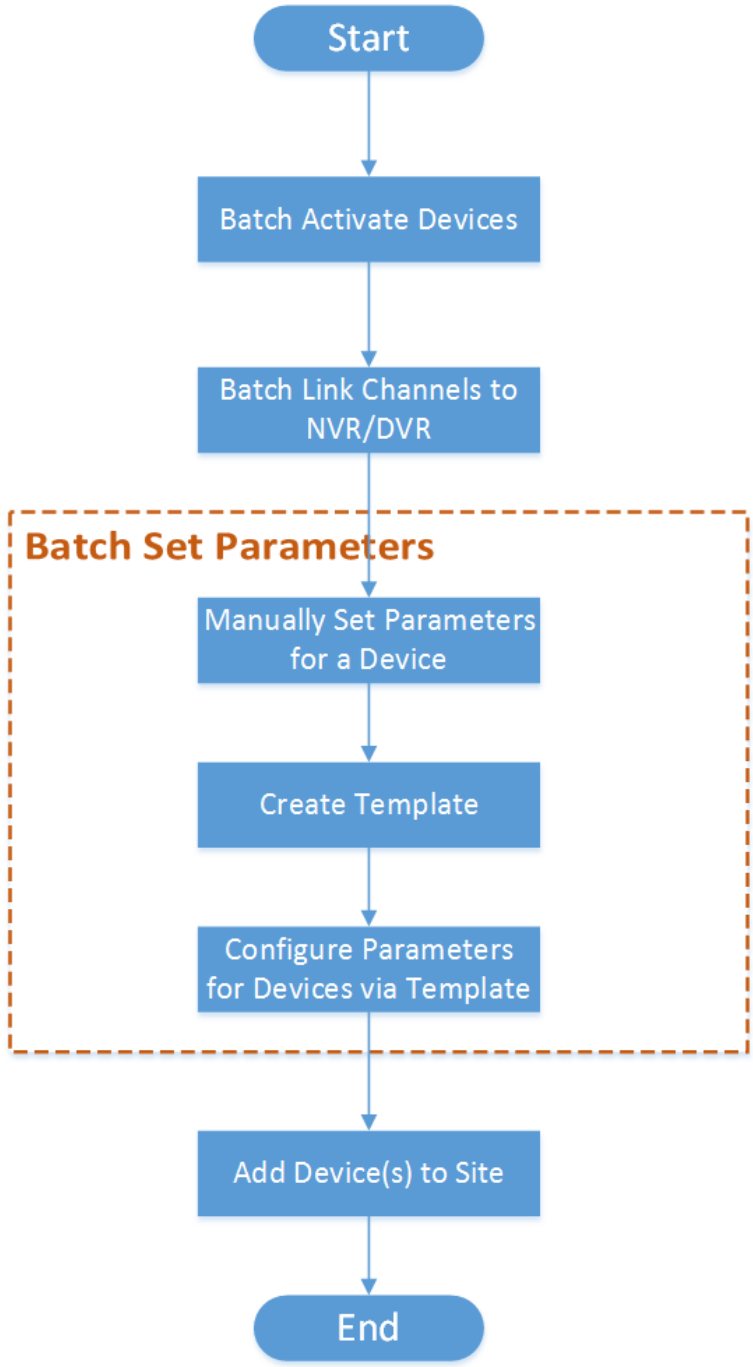


Figure 3-64 Flow Chart

Table 3-8 Flow Chart Description

Step	Sub-step	Description
Batch Activate Devices	N/A	Batch activate online devices on the same Local Area Network (LAN) with the PC on which the Hik-Partner Pro Portal runs, and assign IP addresses for the activated devices. See ***Batch Activate Devices and Assign IP Addresses for Them*** for details.
Batch Link Channels to NVR/DVR	N/A	If the activated devices include NVR or DVR, link channels to NVR or DVR. See ***Batch Link Channels to NVR and DVR*** for details.
Batch Set Device Parameters	Manually Set Parameters for a Device	Select an activated device and set its parameters manually. See ***Create Template for Setting Parameters*** for details.
	Create Template	Created a template based on the manually configured device. See ***Create Template for Setting Parameters*** for details.
	Configure Parameters for Devices via Template	Batch configure parameters for multiple devices via a selected template. See ***Batch Set Parameters for Devices via Template*** for details.
Add Device(s) to Site	N/A	If required, add the activated and configured device(s) to a Site.

3.2.1 Batch Activate Devices and Assign IP Addresses for Them

The Portal can detect available devices connected to the same network with the Portal, and then you can activate devices and assign IP address for them.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.

Steps

1. Move your cursor to the **Site & Device** tab.
2. Click **Install & Config → On-Site Config** to enter the batch device configuration page.

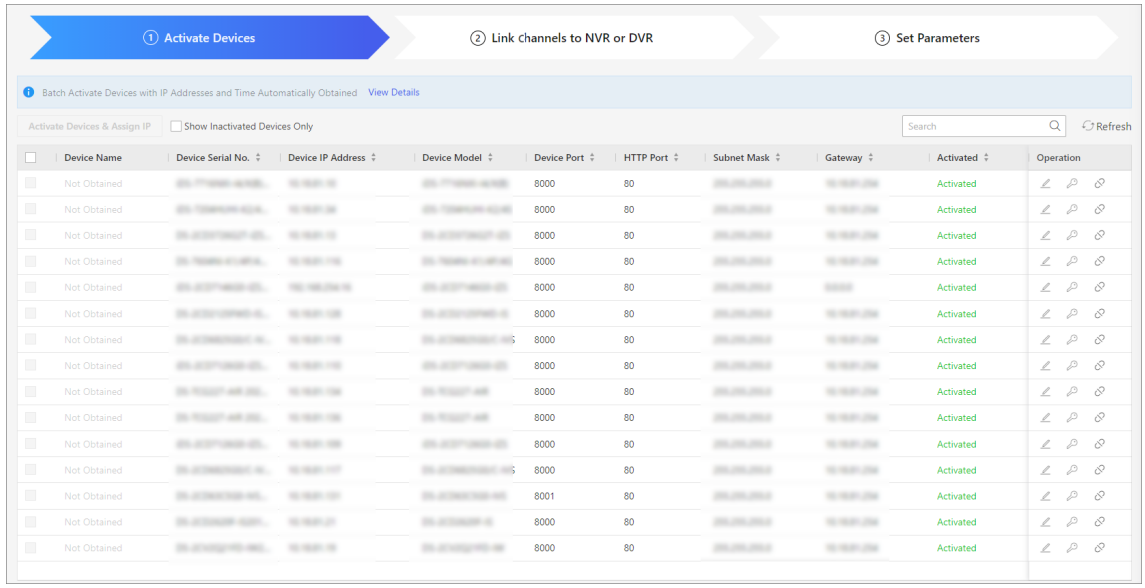


Figure 3-65 Batch Device Configuration

3. Select the detected online devices to be activated.
4. Click **Activate Devices & Assign IP** to open the Activate Devices & Assign IP window.
5. Enter the device admin password and confirm the password.
6. Click **Activate Devices & Assign IP**.

Note

- The unactivated device and the activated device but not be assigned with IP address will be displayed as **Not Obtained** in the **Device Name** column.
- For the activated device and be assigned with IP address, if you hover the mouse on the IP address, **Auto** will be displayed to remind you the IP address is automatically assigned.

The devices are activated, and the device IP address are assigned by the Portal.

The time of the computer will be synchronized to the activated devices.

7. **Optional:** After the devices are activated, you can perform the following operations.

Operation	Description
Edit Device Network Parameters	Click to edit the device network parameters, including IP address, device port, HTTP port, subnet mask, gateway, device admin password and then click **OK**.
Reset Device Admin Password	Click to reset the admin password of the device.
Unbind Device	Click and then enter the device password and verification code to unbind the device from its current account. After unbound, the device can be added to another account.

What to do next

After activating the devices, you should batch add channels to NVR or DVR. For details, refer to ***Batch Link Channels to NVR and DVR*** .

3.2.2 Batch Link Channels to NVR and DVR

If there are online NVR, DVR, and network camera on the same LAN, you can batch link the network camera to the NVR and DVR as channels. After linking, you can manage the linked channels according to your need.

Before You Start

Make sure you have activated the NVR, DVR, and network cameras. See ***Batch Activate Devices and Assign IP Addresses for Them*** for details.

Steps

Note

If there is no online NVR or DVR on the same LAN, skip this task.

1. On the Link Channel page, select an NVR or DVR on the left.

   Note

   If you have not logged in to the device, enter the password to log in.

2. Click **Next**.

   Channels that have been linked will be displayed in the middle.

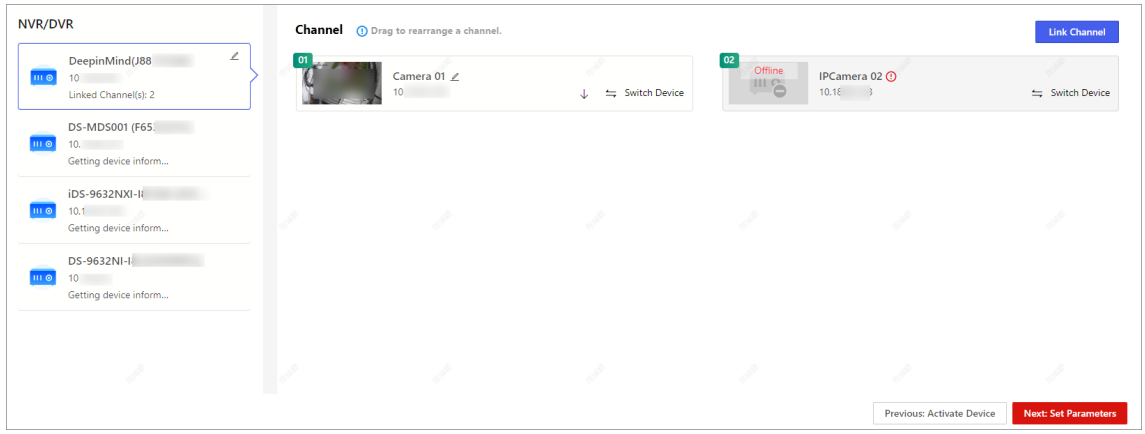


Figure 3-66 Channels on the Same LAN

Note

If a linked channel is offline, ⓘ will be displayed beside the channel name. Hover the cursor on the icon to view the reason for being offline. You can click **Set Parameters** to change channel parameters to try again.

3. Click **Link Channel** to open the Link Channel panel.
4. **Optional:** Select a device and click ⇅ to log in to the device and get device information.
5. Click **+** to link the device.
6. **Optional:** Perform the following operations.

Edit NVR/DVR/Channel Name	Click ✎ to edit the NVR/DVR/channel name.
Sort Channels	Click ↑ or ↓ to sort the channels.
Replace Device	Click **Replace Device** to unlink this channel and link a new device.
Unlink Device	Click 🗑 to unlink channel.

What to do next
Click **Next** to batch set parameters for devices. See ***Batch Set Parameters for Devices via Template*** for details.

3.2.3 Create Template for Setting Parameters

Before batch configuring parameters for devices, you should create a template. After creating a template, you can batch apply it to devices.

Before You Start
Make sure you have activated devices and linked channels to NVR and DVR (if any). See ***Batch Activate Devices and Assign IP Addresses for Them*** and ***Batch Link Channels to NVR and DVR*** for details.

Steps
1. Click a device name or **Set Parameters** to enter the remote configuration page.
2. On the remote configuration page, set parameters for the device.
3. Click **Save as Template** on the top right.
4. Set a template name and check the parameters you want to save in the template.
5. Click **Save** to save the parameters as a template.
6. **Optional:** Add a new template based on device with configured parameters.
   1) Click **Manage Template → +** .
   2) Enter template name.
   3) Select device type.
   4) In the template content field, select a device.
   5) Click **Save**.

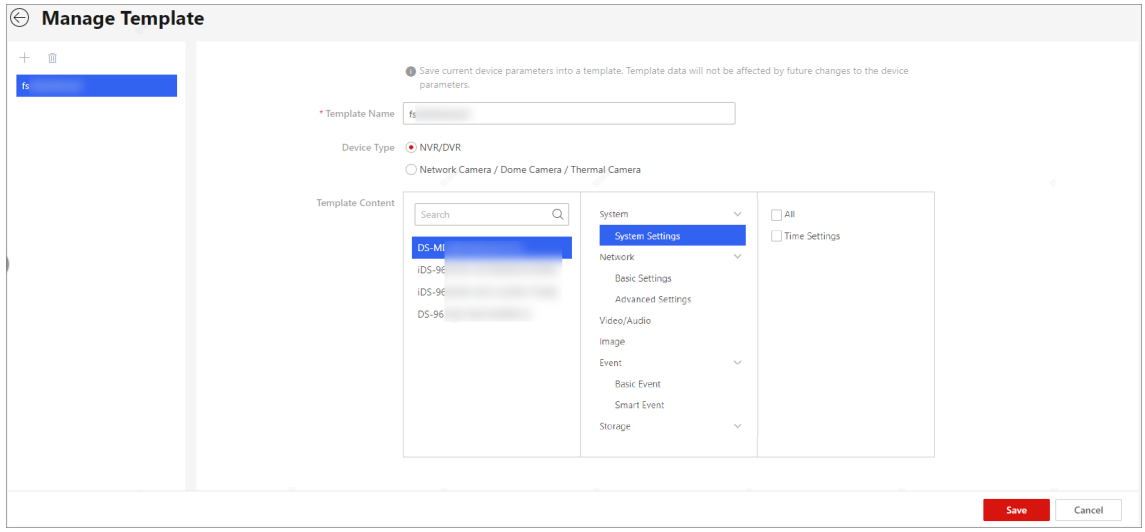


Figure 3-67 Add Template

7. **Optional:** Click to delete a template.

3.2.4 Batch Set Parameters for Devices via Template

To configure devices with high efficiency, you can batch apply parameters in an existing template to devices.

Before You Start

Make sure you have created at least one template for setting parameters. See ***Create Template for Setting Parameters*** for details.

Steps

1. Check device(s) and click **Set Parameters by Template**.

   Note

   Before setting parameters for an NVR or DVR, you can tap **Format** to format the disk of the selected device. Batch formatting is not supported.

2. Select a template.

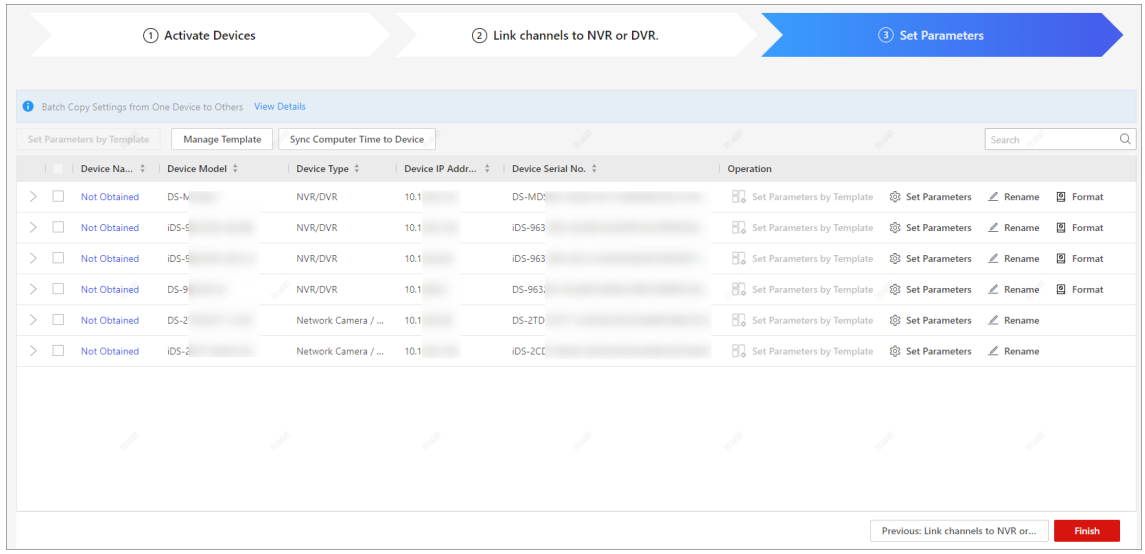


Figure 3-68 Set Parameters

3. Click **Apply Parameters** to apply the configured parameters to devices.

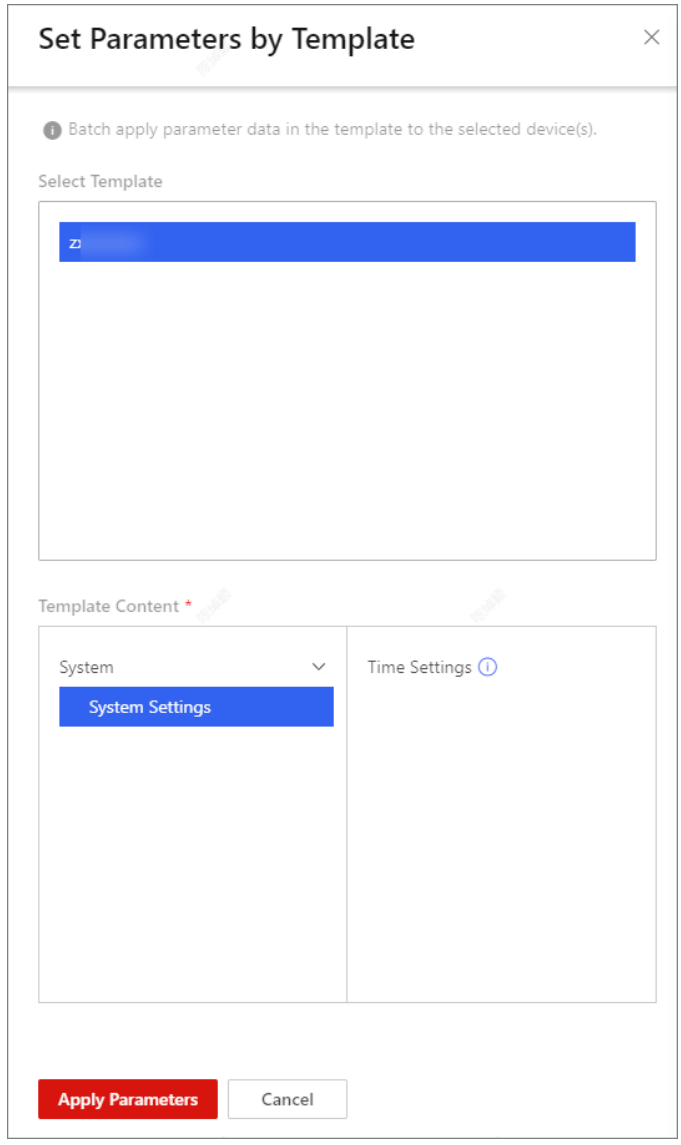


Figure 3-69 Set Parameters by Template

The application process and application results will be displayed.

4. **Optional:** Perform the following operations.

Add Device to Site	Add devices to Sites.
Manage Template	Click **Manage Template** to add new template or delete template. See ***Create Template for Setting Parameters*** for details.
Edit NVR or Channel Name	Click **Rename** to edit name(s) of NVR or channels of NVR.
Synchronize Computer Time to Device	Check device(s) and click **Synchronize Time to Device**. And then check devices and click **OK**.

3.3 On-Site Configure Devices Using the SADP Tool / via the Site page

Introduction

After ***adding various types of devices to your site*** , you can configure these devices on the Portal or Mobile Client for more efficient management.

Configuration for Various Types of Devices

Device Type	Configuration Item	Supported Platform
Encoding Device	***View Live Video and Play Back Recorded Videos***	Portal/Mobile
	Set DDNS to Make Sure Encoding Devices Can Be Managed by Hik-Partner Pro	Portal/Mobile
	Set Cloud Storage for Uploading Recorded Video to the Cloud	Portal/Mobile
Security Control Panel	***Configure an AX HOME, AX PRO, or AX HYBIRD PRO***	Portal/Mobile
	Control Areas/Zones of an AX HOME, AX PRO, or AX HYBIRD PRO	Portal/Mobile
	Batch Configure and Upgrade AX PROs	Portal/Mobile
Network Device	***Configure AC Routers***	Mobile
	Configure Network Switches	Mobile
	View Network Topology with Smart Managed Switches	Portal/Mobile
Healthcare Radar	***Link a Camera to a Radar***	Mobile

3.3.1 Encoding Devices

You can add and manage encoding devices including network cameras, DVRs and NVRs on Hik-Partner Pro. The following chapter introduces functionality supported by these devices such as live view and playback.

View Live Video and Play Back Recorded Videos

View Live Video

You can view live videos of the added online encoding devices. By live view, you can know what happens at this moment.
The following figures show the entries of live view page on the Portal and the Mobile Client.

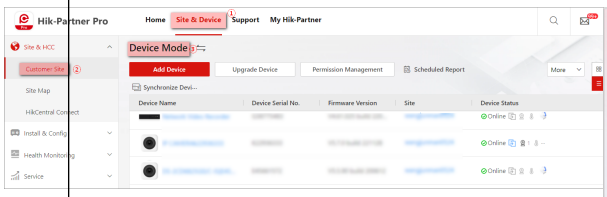


Figure 3-70 The Entry of Live View Page Portal (Device Mode)

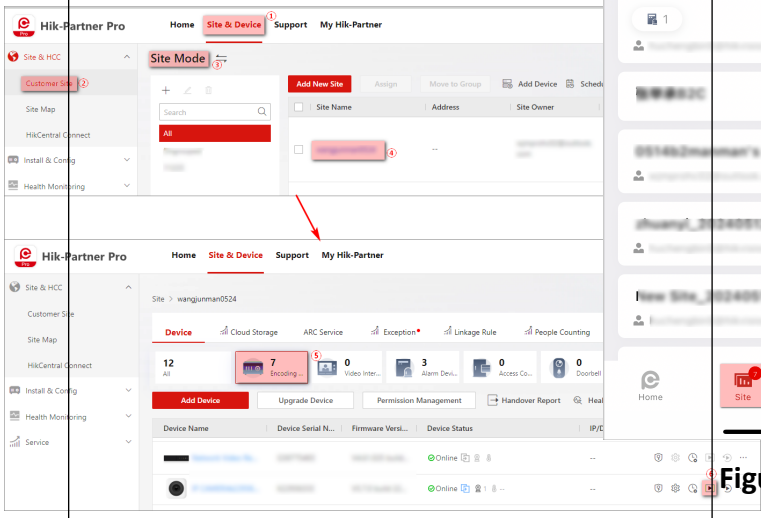


Figure 3-71 The Entry of Live View Page on the Portal (Site Mode)

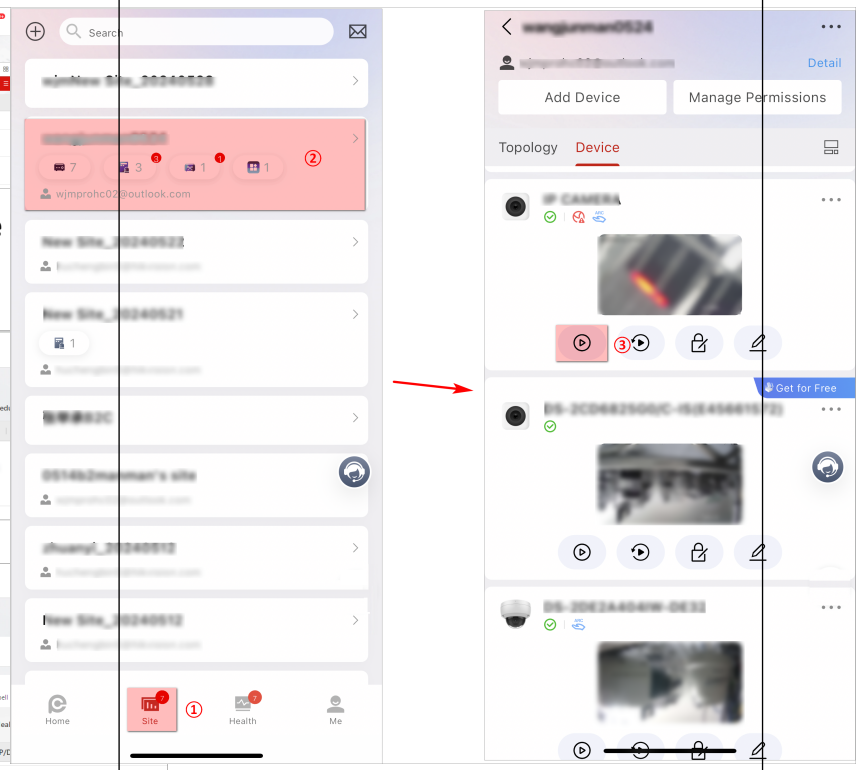


Figure 3-72 The Entry of Live View Page on the Mobile Client

On the Live View page, you can perform operations such as capturing and recording. Refer to the following figures for the explanation of these icons.

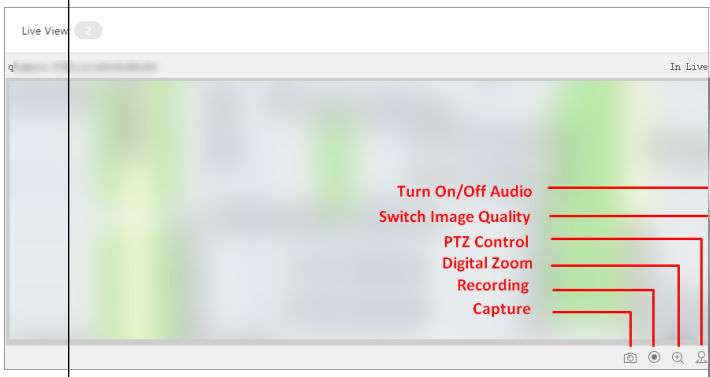


Figure 3-73 Live View Page and Icon Explanations (Portal)

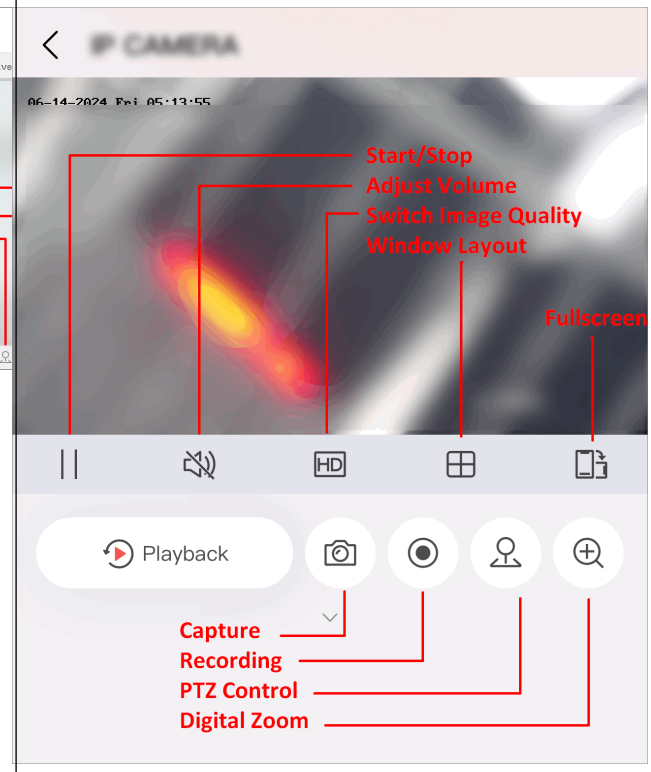


Figure 3-74 Live View Page and Icon Explanations (Mobile Client)

Note

- Up to 16 live view windows are supported.
- If Image and Video Encryption has been enabled for the device on the Hik-Connect mobile client, you are required to enter the device verification code before starting live view. If you don't know the device verification code, ask the end user for it. For details about Image and Video Encryption, see *Hik-Connect Mobile Client User Manual*.
- Please inform your end users to download or update the Hik-Connect Mobile Client (V 4.15.0 or later). You can send the QR code or download link shown in the banner on the Home page to them.

Play Back Video Footage

You can view the recorded video footage of the added online encoding devices. By playback, you can know what happens at the specific time.
The following figures show the entries of playback page on the Portal and the Mobile Client.

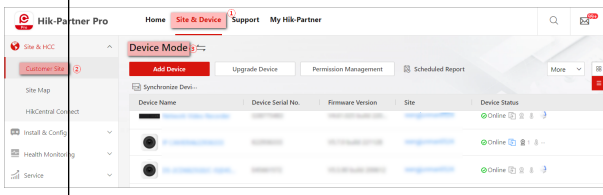


Figure 3-75 The Entry of Playback Page (Portal (Device Mode)

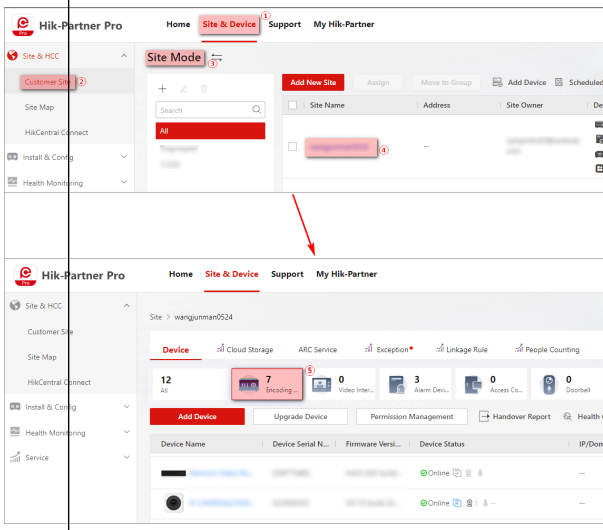


Figure 3-76 The Entry of Playback Page on the Portal (Site Mode)

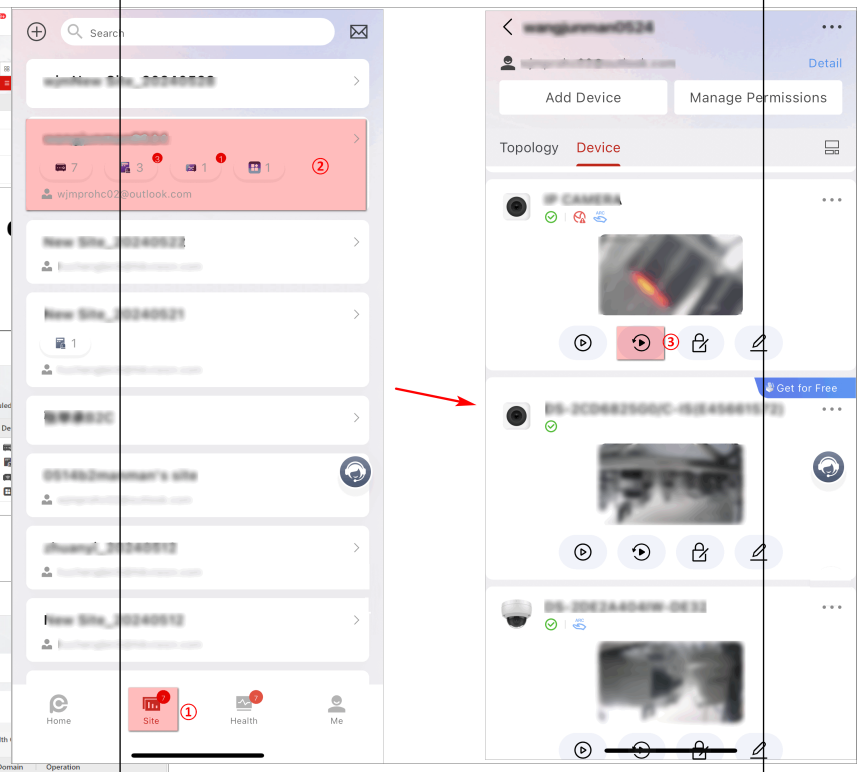


Figure 3-77 The Entry of Playback Page on the Mobile Client

On the Playback page, you can perform operations such as capturing and clipping. Refer to the following figures for the explanation of these icons.

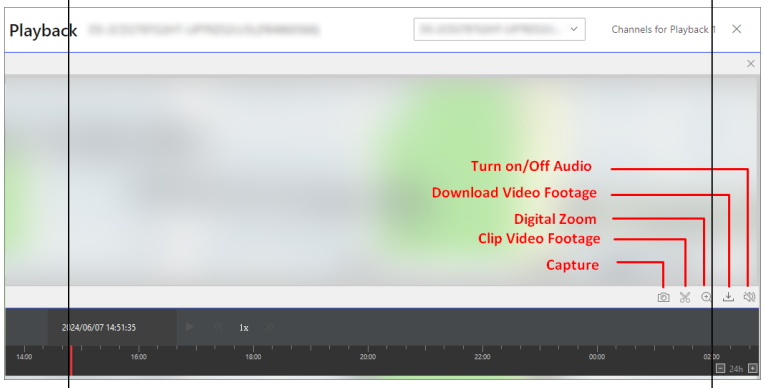


Figure 3-78 Playback Page and Icon Explanations (Portal)

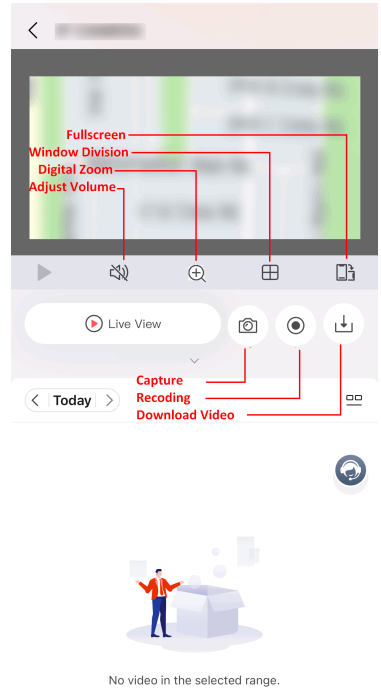


Figure 3-79 Playback Page and Icon Explanations (Mobile Client)

Note

Up to 4 playback windows are supported.

Set DDNS to Make Sure Encoding Devices Can Be Managed by Hik-Partner Pro

For devices with invalid or old firmware version, you can configure DDNS for them to make sure they can be managed by Hik-Partner Pro properly.

Only encoding devices added by Hik-Connect (P2P) support this function.

Steps

1. Enter the DDNS settings page.

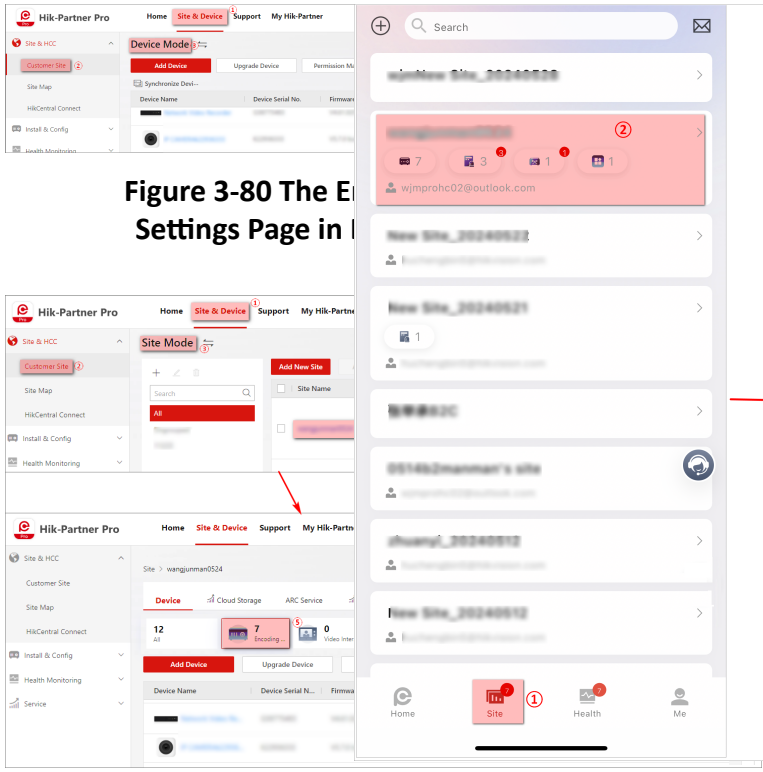


Figure 3-80 The E
Settings Page in

Figure 3-81 The Entry of Entering DDNS Settings Page in Site Mode (Portal)

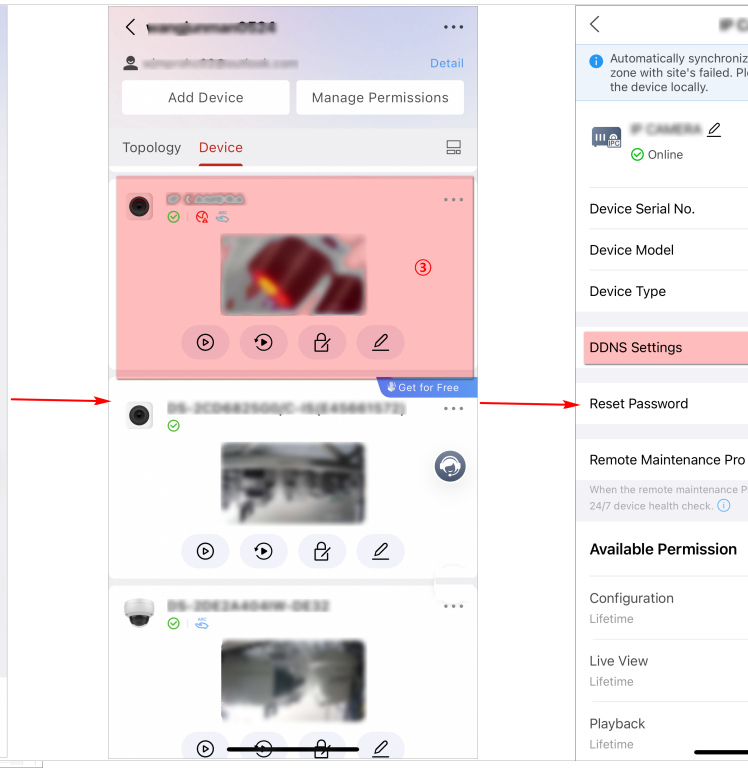


Figure 3-82 The Entry of Entering DDNS Settings Page (Mobile Client)

2. On the DDNS settings page, switch on **Enable DDNS** and set parameters.

Port Mapping Mode

Auto

The service port and HTTP port are obtained automatically, and you cannot edit them after obtaining them.

Manual

Enter the service port and HTTP port manually.

3. Confirm the above settings.

Set Cloud Storage for Uploading Recorded Video to the Cloud

You can enable and set up cloud storage for an encoding device (DVR, NVR, or network camera) when you complete adding a device that supports cloud storage to a site. After that, the device will be able to upload event-related footage of its channel to the cloud.

If your device does not support cloud storage, you can add the channel(s) of the device to Hik-ProConnect box and then enable cloud storage.

Steps

1. Add a device that supports cloud storage to the site by Hik-Connect (P2P).

   The entry for setting cloud storage will be displayed on the adding result page.
2. Enter the cloud storage settings page.
3. **Optional:** Test the network performance if the network bandwidth is limited.
4. Set resolution of the footage to be uploaded to the cloud.
5. Set the events that will trigger video recording action of the channel.

   Note

   - The triggering events include motion detection, intrusion, and line crossing. For the settings of different events are similar, the following takes motion detection as an example.
   - Solar cameras only support setting motion detection.

   Enable Motion Detection

   Turn on the switch to enable motion detection.

   Area Settings

   Draw an area on the image, and then drag the slider to set the sensitivity of motion detection.

   Objects in motion will be detected within the drawn area.

   Arming Schedule

   Define the time period during which motion detection is activated.

   Linkage Method

   Make sure you have selected **Notify Surveillance Center**, otherwise the channel will not record video footage even if the event is detected.
6. Switch on **Cloud Storage** to enable cloud storage functionality for the channel.
7. Activate cloud storage service for the channel.

   The event related video footage of the channel will be uploaded to the cloud.
8. Finish the above settings.

Related Information Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance

3.3.2 Manage Security Control Panel

You can add and manage AX HOME, AX PRO, AX HUB, AX HYBRID, and AX HYBIRD PRO security control panels (hereinafter referred to as "AX HOME / AX PRO / AX HYBIRD PRO device") on Hik-Partner Pro. The following chapter introduces functionality supported by these devices such as batch arming/disarming.

Note

AX HUB or AX HYBRID security control panel does not support the functionality introduced in the following chapter. AX HUB and AX HYBRID support generic device management, such as enabling ARC service, running health monitoring, setting rules for linkage or exception reporting, and configuring parameters remotely. For details, refer to , , , and respectively.

Control Security Control Panels

You can perform operations including adding area, arming/disarming area, and silencing alarm.

Select **Site & Device → Customer Site** to enter the site list page.

- In the site mode, click the name of a site to enter the site details page, and select an AX HOME, AX PRO or AX HYBIRD PRO to open the operation panel.
- Click ⇋ to switch to the device mode, and select an AX HOME, AX PRO or AX HYBIRD PRO to open the operation panel.

You can perform the following operations.

Function	Operation
Arm an Area	• For AX PRO or AX HYBIRD PRO devices, select the **Area** tab, select to arm the area in Arm Stay mode and to arm the area in Arm Away mode. • For AX HOME devices, select the **Area** tab, and then select to arm the area in Away Arm mode. The Arm Stay mode is not supported by AX HOME devices.
Disarm an Area	Select the **Area** tab and then select to disarm the area.
Stay Arm Areas	For AX PRO or AX HYBIRD PRO devices, select the **Area** tab, select areas, and then select to arm all areas in Arm Stay mode.
Away Arm Areas	Select the **Area** tab, select areas, and then select to arm areas in Arm Away mode.
Disarm Areas	Select the **Area** tab, and then select to disarm areas.
Silence Alarms of All/ Multiple Areas	Select the **Area** tab, select areas, and then select . **Note** This function is not supported by the AX HYBIRD PRO device.

Function	Operation
Filter Peripheral Device by Area	Select the **Device** tab. Click ⌄ and select an area to only display the peripheral devices linked to the selected area, or select **All** to display all peripheral devices linked to all the areas. **Note** The AX HYBIRD PRO device only supports adding keyfobs as the peripheral device.An AX HOME device supports adding keyfobs, PIRs, LED keypads, sounders, and magnetic contacts.
Bypass Zone	Select the **Device** tab, and then select a zone and turn on the **Bypass** switch to bypass the zone. **Note** This function is not supported by the AX HOME and AX HYBIRD PRO device.

Configure Security Control Panel

You can remotely configure AX HOME, AX PRO and AX HYBIRD PRO device parameters, apply for PIN (required for upgrading firmware), and switch the language of the device.

Click **Site & Device → Customer Site** to enter the site list page.

- In the site mode, click the name of a site to enter the site details page, and click the name of a device to enter the device details page.
- Click ⇆ to switch to the device mode, and click the name of a device to enter the device details page.

Remotely Configure Security Control Panels

You can click ⚙ **Remote Configuration** to enter the web page of the device to configure its parameters.

Note

For details about remote configuration, see the user manual of the device.

Apply for a PIN

You can click • • • → **Apply for a PIN** to get a PIN code for verification.

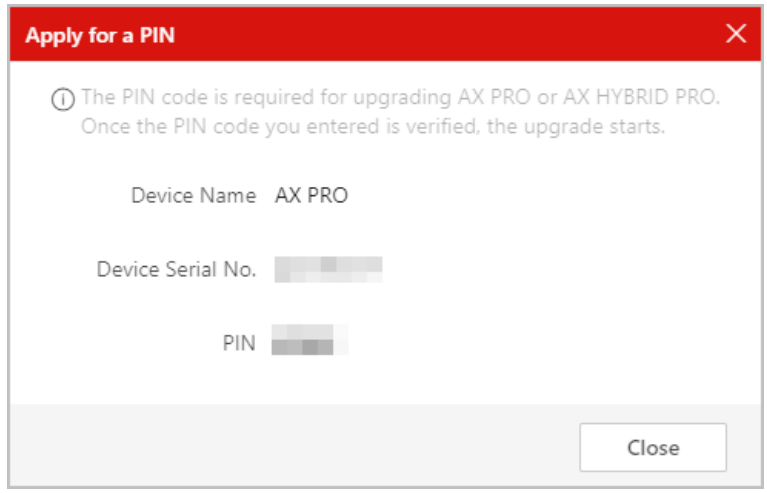


Figure 3-83 Apply for a PIN

Switch Language

You can click • • • → ⇆ **Language** and set the device language. After you click **OK**, a pop-up window will ask you if you need to reset the names of the device and its areas. Click **Reset** to switch the device language and switch the names to the default names in the switched language; click **Cancel** to switch the device language only.

Note

A PIN code is required for switching language.

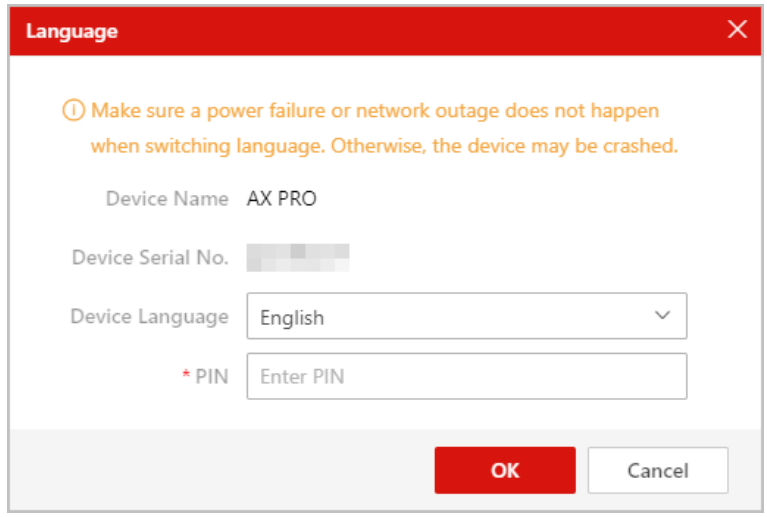


Figure 3-84 Language Window

Batch Configure AX PRO

You can batch configure parameters for the added AX PRO devices by creating templates. You can also batch upgrade the firmware of multiple AX PRO devices.

Note

- Only AX PRO devices (Version 1.1.0 and later) and AX HYBRID PRO devices are supported.
- The function is only supported in certain countries and regions.

Create a Template

You can create a template for batch configuring parameters of AX PRO devices.

1. Go to **Install & Config → Remote Batch Config → Manage Template** to enter Manage Template page.
2. Add a template.
   - Click **Create Template** for adding a template for the first time.
   - If not, click + .
3. Edit the template by configuring parameters as needed, and these configured parameters can be batch applied to AX PRO devices later. See the following for the detailed parameters explanations.

Arming Schedule

Enable auto Arm

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

Enable auto Disarm

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

Note

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

Late to Disarm

Enable the device to push a notification to the phone or tablet to remind the user to disarm the area when the area is still armed after a specific time point.

Weekend Exception

Enable the function and the area will not be armed or disarmed on the weekend.

Holiday Exception

Enable the function and set the holiday schedule. The area will not be armed or disarmed on the holiday.

Note

You can set up to 12 holiday groups.

Auto Arm Sound Prompt

If Auto Arming Sound Prompt is enabled, the AX PRO will sound for a prompt when it is armed automatically.

Note

This setting will take effect on all areas.

Panel Alarm Duration

The time duration of the panel alarm.

Alarm Receiving Center

Protocol Type

Select **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, ***ADM-CID**, **CSV-IP**, **FSK Module**, **RDC Module** and **IDS Module** as the protocol type.

Note

When selecting ***SIA-DCS** or ***ADM-CID**, you should configure the Encryption Arithmetic and Secret Key.

Address Type (Alarm Receiver Server)

Select **IP** or **Domain Name** as the address type, and enter the IP address or domain name of the alarm receiver server accordingly.

Port No. (Alarm Receiver Server)

Enter the port No., of the alarm receiver server.

Account Code

Enter the assigned account provided by the alarm receiving center.

Transmission Mode

Select **TCP** or **UDP** as the transmission mode from.

Impulse Counting Time

Set the timeout period waiting for the receiver to respond. Re-transmission will be arranged if the transceiver of receiving center is timed out.

Attempts

Set the maximum number that re-transmission will be tried.

Polling Rate

Enable the function and set the interval between 2 live polling.

Periodic Test

Enable the function and set the interval between two periodic tests.

Companies

Select a company from the drop-down list.

Note

If you select **French Alarm Receiving Company**, you should configure **PIRCAM Picture Upload Mode**.

Event Types Notification (Alarm Receiving Center)

Select which alarm receiving center to receive event notifications and the corresponding event types, including alarms and tampers, life safety alarms, maintenance and faults, zone alarm/lid opened, etc.

Notification by Email

Enable the function of sending video verification event and configure the related parameters including the sender's name and email address, the SMTP server's IP address and port No., and the receiver's name and email address, etc.

Server Authentication

If enabled, you should enter the sender's user name and password.

FTP Settings

Address Type

Select **IP** or **Domain Name** as the address type, and enter the IP address or domain name of the FTP server accordingly.

Port No.

Enter the port No. of the FTP server.

Protocol Type

Select **FTP** or **SFTP** as the protocol type.

User Name

Enter the user name of the FTP server.

Password

Enter the password of the FTP server.

Enable Anonymity

If enabled, you do not need to enter the user name and password of the FTP server.

Note

This function is only available when selecting FTP as the protocol type.

Directory Structure

The saving path of snapshots in the FTP server.

Batch Configure AX PRO by Template

You can batch configure parameters for AX PRO devices by the predefined template.

Steps

1. Go to **Install & Config → Remote Batch Config** .
2. Select multiple AX PRO devices to be configured.
3. Click **Set Parameters by Template**.

   A window of Set Parameters by Template pops up on the right side.
4. Select a template from the list.

   Note

   - If you have not added a template, you should click **Manage Template** to enter Manage Template page and add a template for AX PRO devices. For details, refer to ***Create a Template*** .
   - You can view the general template content on the lower side.
5. **Optional:** Click **Details** to view the details of the template.
6. Click **Apply** to start applying parameters to the devices.

What to do next

View the applying results. If applying failed, you can view the failure reasons.

Batch Upgrade AX PRO

You can batch upgrade the firmware of multiple AX PRO devices to ensure the proper functioning of these devices. If the firmware version of an AX PRO device is too old, some features might be unavailable.

Steps

1. Go to **Install & Config → Remote Batch Config** to enter the page shown below.

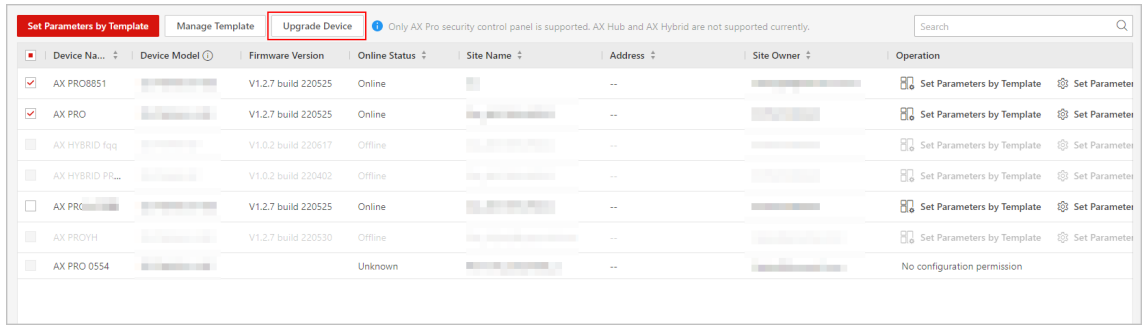


Figure 3-85 Remote Batch Configuration

2. Select AX PRO devices and then click **Upgrade**.

   The **Upgrade Device** window will pop up.
3. Click **Apply for a PIN** to get one.

   The PIN code will be automatically entered.
4. Click **Update**.

Batch Arm/Disarm Security Control Panels

You can batch arm or disarm multiple AX HOME / AX PRO / AX HYBRID PRO devices on multiple sites by grouping the devices. For example, assume that your customer needs to have her office building cleaned in the period from 7:00 a.m. to 8:00 a.m. everyday, you can add all AX HOME / AX PRO / AX HYBRID PRO devices in the building to a group and then disarm the group in the period everyday to avoid the nuisance of false alarms triggered by the cleaning.

Follow the steps to create a group of AX HOME / AX PRO / AX HYBRID PRO devices and then control the group.

Steps

Note

This function is only available in some countries/regions.

1. Go to the Batch Arm/Disarm page.
   - Go to **Install & Config → Batch Arm/Disarm** .
   - Go to **Site & Device → Customer Site → Batch Arm/Disarm** .

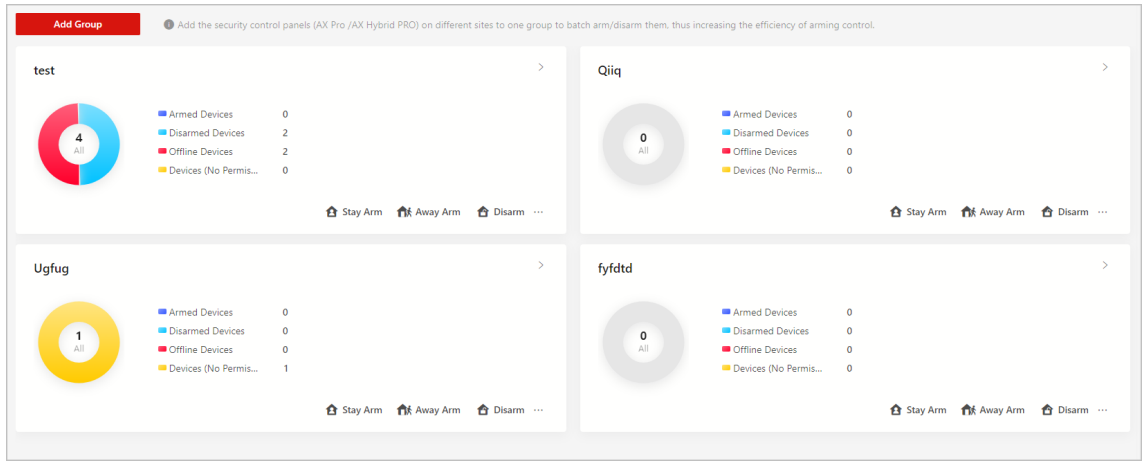


Figure 3-86 Batch Arm/Disarm Page

2. Click **Add Group**.
3. Create a name for the group.
4. Add devices to the group.
   1) Click **Add** and select the devices in different Sites.

   Note

   - Only devices of which you have the **Configuration** permission can be added.
   - Up to 500 devices can be added to one group.

   2) Click **OK**.
   3) **Optional:** Select devices and click **Delete** to remove them from the group.
5. Click **OK**.

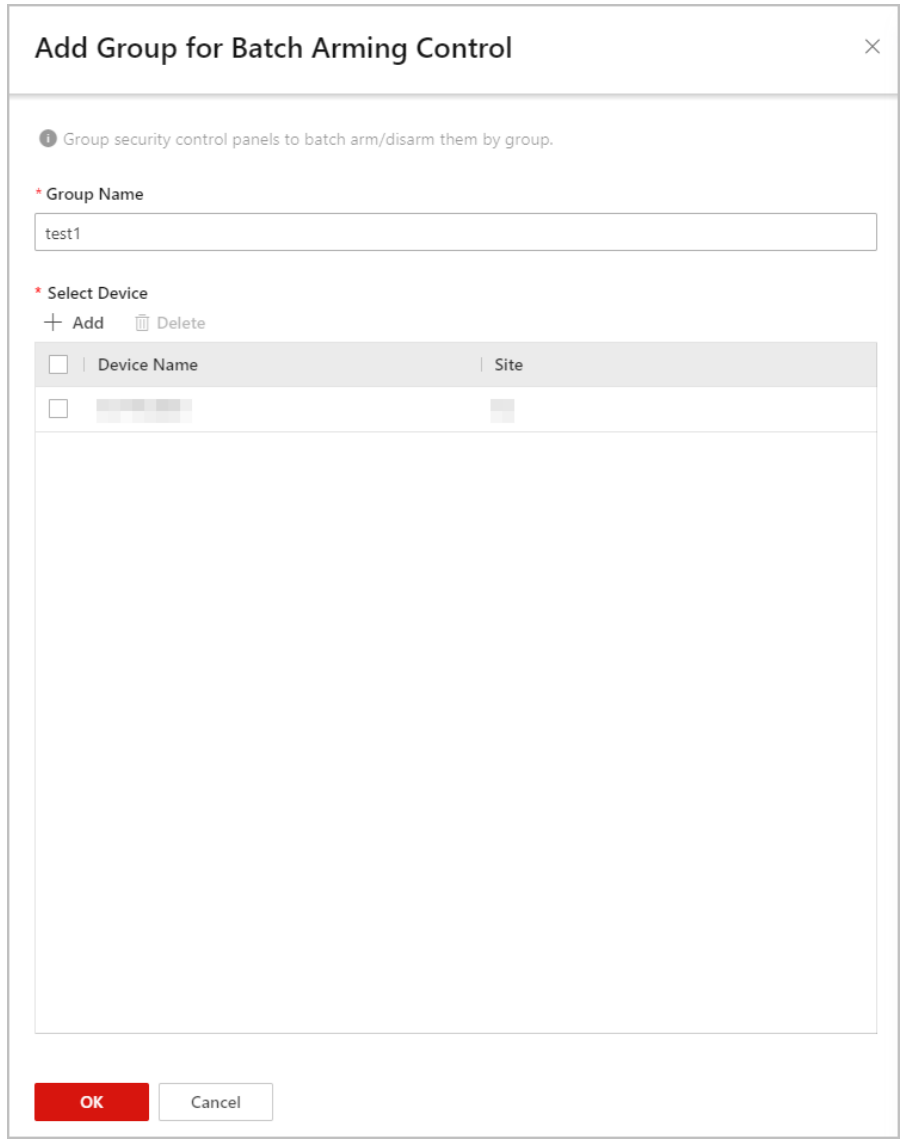


Figure 3-87 Add Group for Batch Arming Control

6. **Optional:** Perform further operations.

View Group Details	Click on the group to view its details, including devices in the group and their arming/disarming status.
Arm/ Disarm Group	Click **Stay Arm** or **Away Arm** to arm all devices in the group. Or click **Disarm** to disarm the group.

Note

- The Arm Stay mode will not be enabled for the AX HOME device.
- If you leave the page after starting arming/disarming, you can click in the upper-right corner to go back. When the arming/disarming process is completed, a notice of result will pop up. Click **Details** to check full result.
- You will also be notified on the Mobile Client when the arming/disarming process is completed.

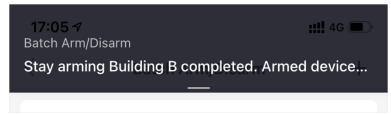


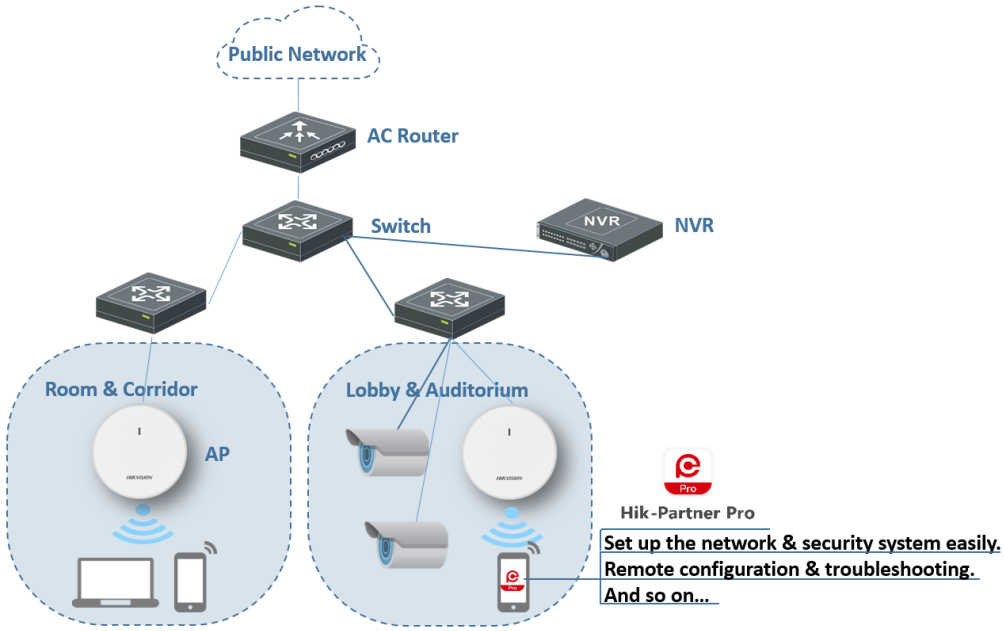
Figure 3-88 Notice on the Mobile Client

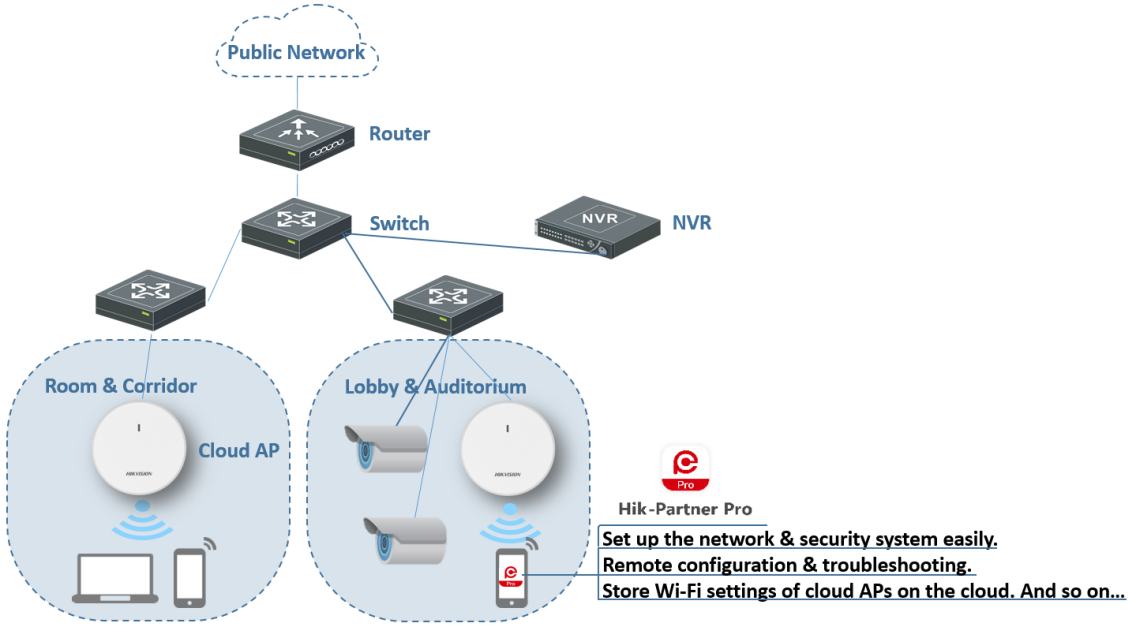
Check Last Result	Click **Last Arming Control Record** to check the last arming/disarming results. If there are devices that failed to be armed/disarmed, you can check the failure reasons and arm/disarm the failed ones again.
Edit Group	Click • • • → **Edit** to edit group name or edit devices in the group.
Delete Group	Click • • • → **Delete** to delete the group.

3.3.3 Manage Network Devices

Setting up network devices like the access control router (AC router), access point (AP), and network switch, and security devices like security control panels and cameras together allows for convenient management. A unified system can provide centralized control and monitoring of both network and security components. After you install and connect the network devices and security devices, you can use the Mobile Client to initialize and configure them together.

Unified Network & Security Architecture





1. Cameras and APs: APs extend the wireless coverage of the network, allowing wireless devices like network cameras to connect to the network. Network cameras and APs are connected to

the network infrastructure through PoE switches, ensuring they have both power and network connectivity.
2. PoE Switch: Provides power and data connectivity to APs and cameras. This simplifies the deployment of APs by eliminating the need for separate power supplies.
3. Aggregation Switch: Collects data traffic from multiple sources, including PoE switches (and thus, from APs and cameras connected to those switches) and directs it towards the network's core or NVRs for storage and analysis. The switch manage large volumes of data and may implement quality of service (QoS) policies to prioritize video traffic, ensuring high-quality video recording and playback. It supports VLAN tagging and can enforce VLAN policies, ensuring that data from different VLANs remains separate as it moves through the network.
4. AC Router (combing AC and router): Offers both routing capabilities to connect the local network with the public internet and include AP management. It also supports VLANs, allowing for different routing rules based on VLAN membership, which might include restricting external access to sensitive VLANs or applying different NAT policies.
5. Connectivity to the Public Network: This connectivity is typically provided through the AC router. It enables remote access to the NVRs or network cameras for video monitoring and system management.

Find Devices on LAN: Device Onboarding and Site Handover

The **Find Devices on LAN** feature helps installers discover, initialize, configure, and add devices to a site. It supports both online and offline deployment scenarios and provides topology verification, local device management, and post-onboarding recommendations to help complete site handover efficiently.

Part One: Before You Start

Supported Deployment Scenarios

Scenario	Description
Online Onboarding	Devices can access the Internet during onboarding.
Offline Onboarding	Devices cannot access the Internet during onboarding.
Site Expansion	Add new devices to an existing site.
Device Replacement	Replace failed or obsolete devices.
Troubleshooting	Manage LAN devices when remote connectivity is unavailable.

Supported Device Types

The onboarding feature supports:

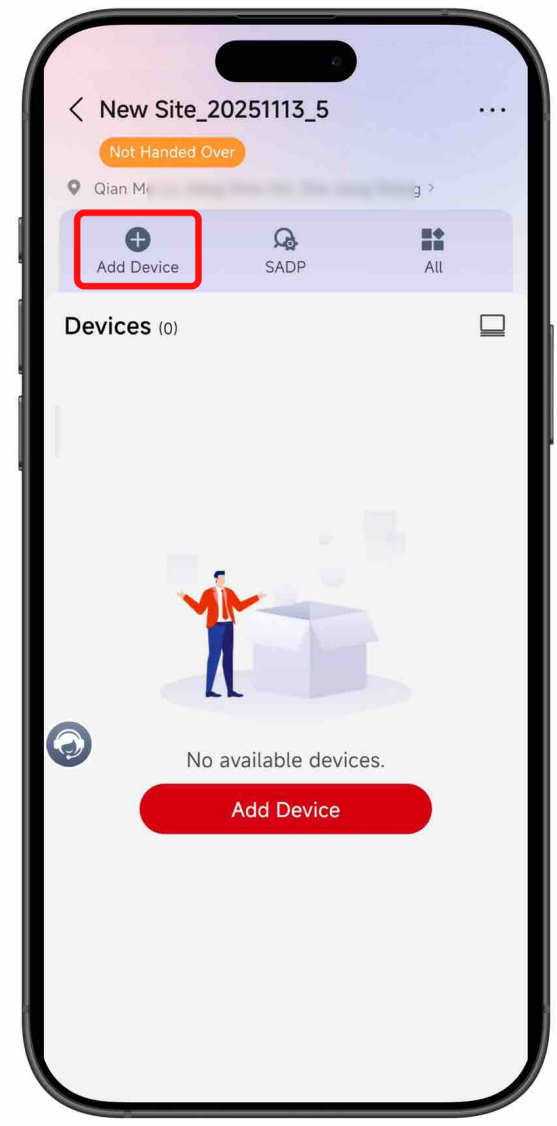
- AC Router
- Cloud AP
- Network Switch
- Wireless Bridge
- Router
- NVR/DVR
- Network Camera
- Access Control Devices
- Video Intercom Devices

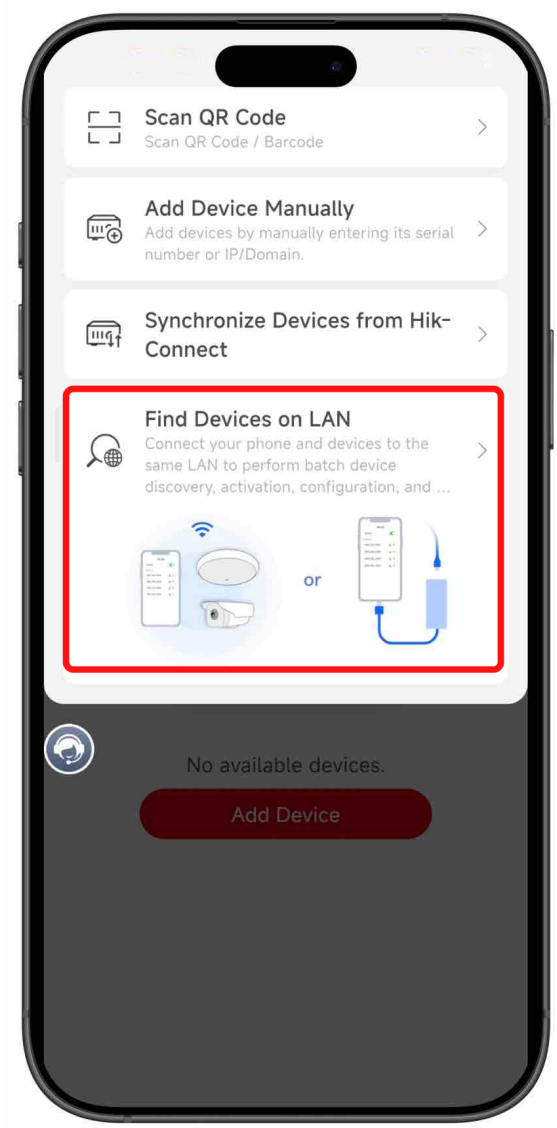
Prerequisites

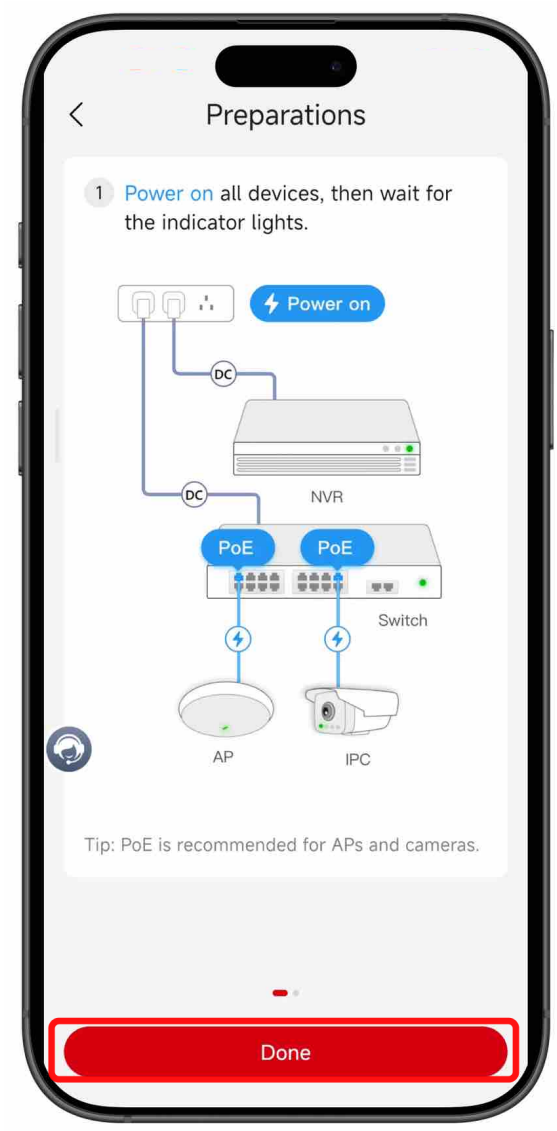
Before onboarding devices:

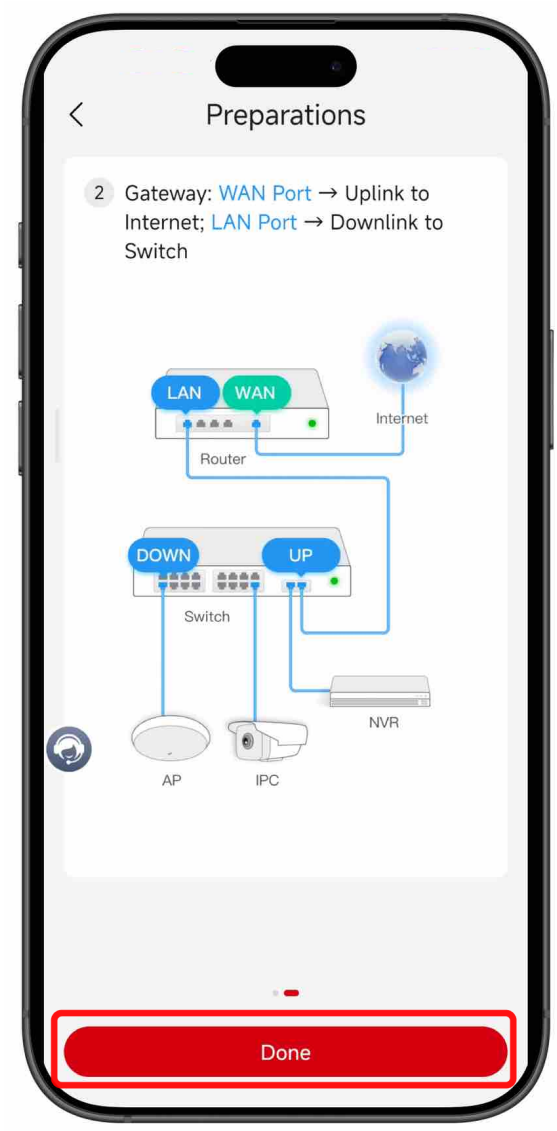
- Connect your mobile phone to the target LAN.
- Enable Location permission.
- Enable Local Network Discovery permission.

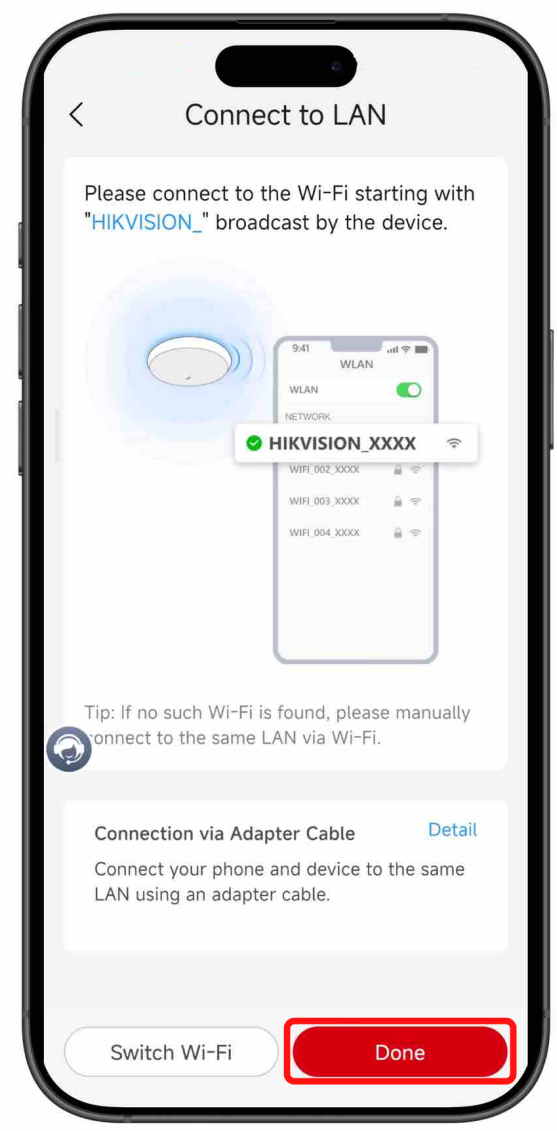
Part Two: Onboard Devices

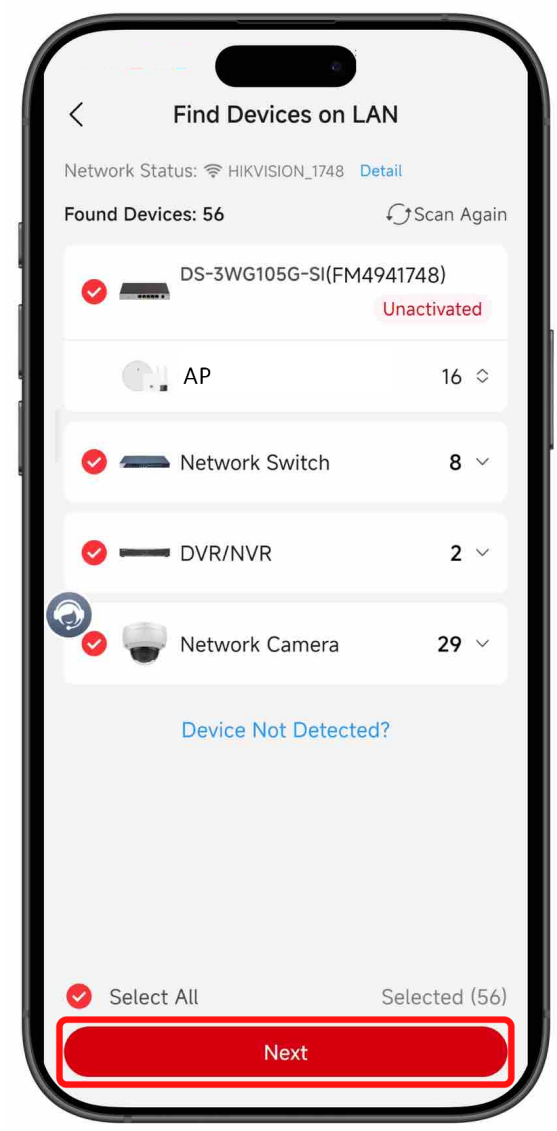


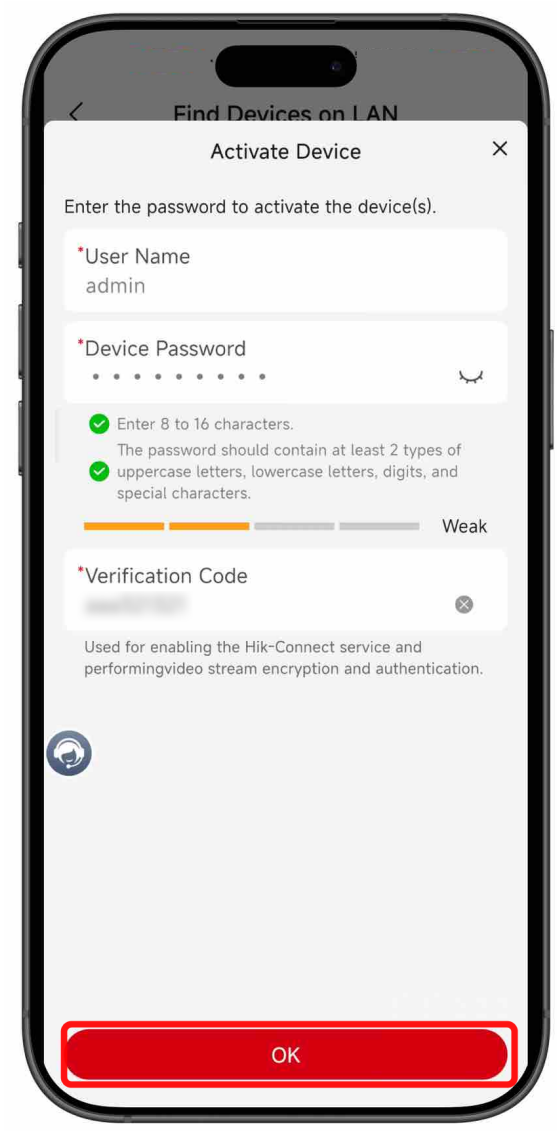

Scan QR Code
Scan QR Code / Barcode
Add Device Manually
Add devices by manually entering its serial number or IP/Domain.
Synchronize Devices from Hik-Connect
Find Devices on LAN
Connect your phone and devices to the same LAN to perform batch device discovery, activation, configuration, and ...
or
No available devices.
Add Device

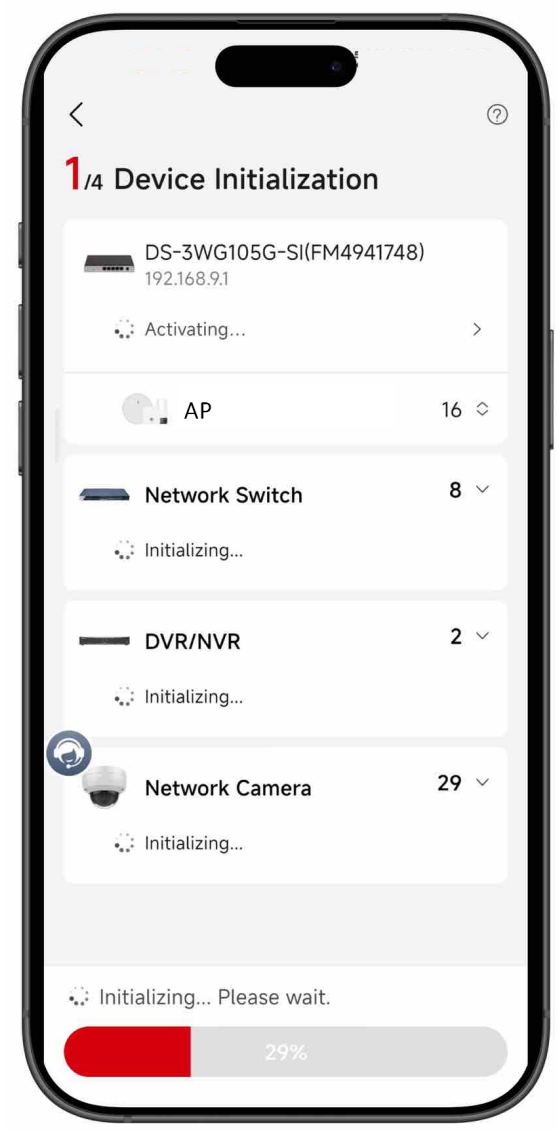

Preparations
1 Power on all devices, then wait for the indicator lights.
Power on
DC
NVR
DC
PoE
PoE
Switch
AP
IPC
Tip: PoE is recommended for APs and cameras.
Done

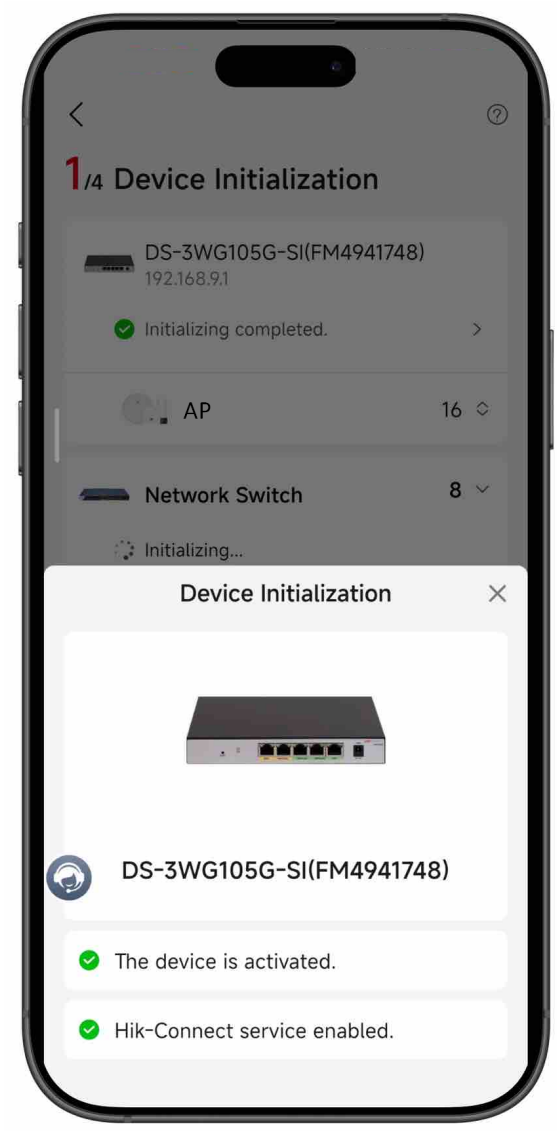

Preparations
2 Gateway: WAN Port → Uplink to Internet; LAN Port → Downlink to Switch
LAN
WAN
Internet
Router
DOWN
UP
Switch
NVR
AP
IPC
Done

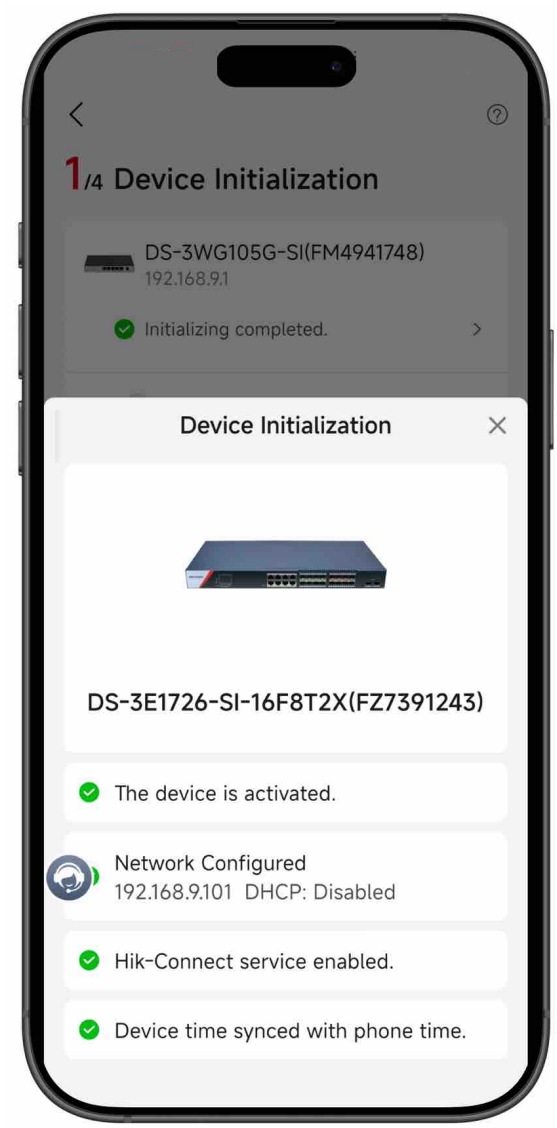

Connect to LAN
Please connect to the Wi-Fi starting with "HIKVISION_" broadcast by the device.
9:41
WLAN
WLAN
NETWORK
HIKVISION_XXXX
WIFI_002_XXXX
WIFI_003_XXXX
WIFI_004_XXXX
Tip: If no such Wi-Fi is found, please manually connect to the same LAN via Wi-Fi.
Connection via Adapter Cable
Detail
Connect your phone and device to the same LAN using an adapter cable.
Switch Wi-Fi
Done

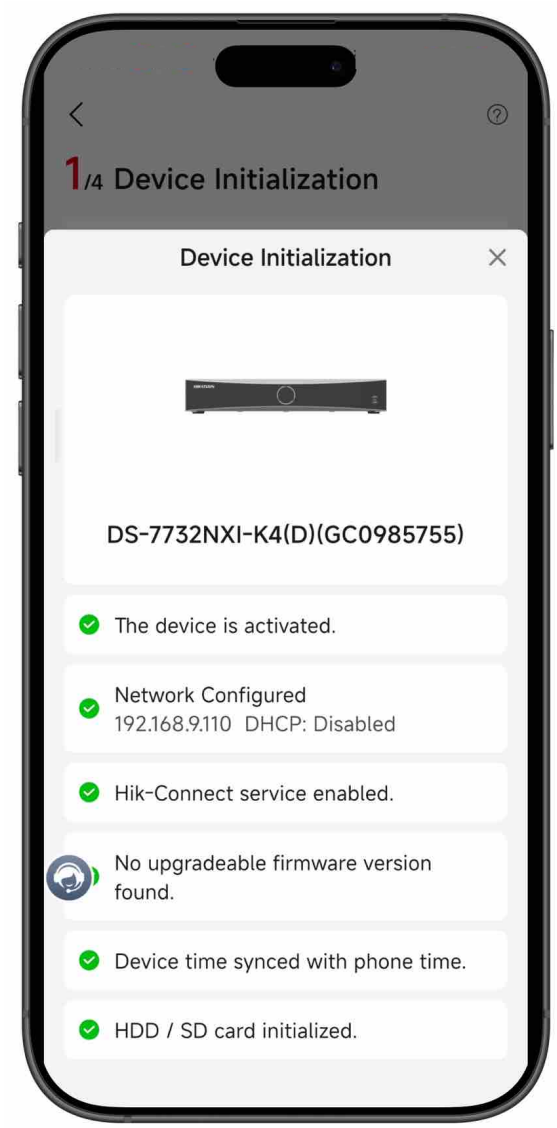

Find Devices on LAN
Network Status: HIKVISION_1748 Detail
Found Devices: 56
Scan Again
DS-3WG105G-SI(FM4941748)
Unactivated
AP
16
Network Switch
8
DVR/NVR
2
Network Camera
29
Device Not Detected?
Select All
Selected (56)
Next

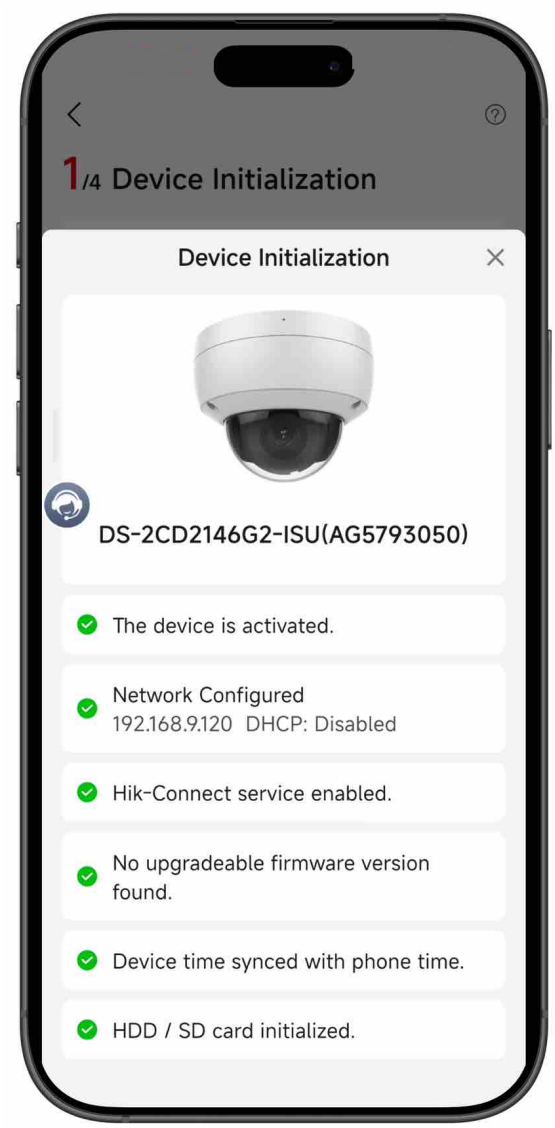

Find Devices on LAN
Activate Device
Enter the password to activate the device(s).
*User Name
admin
*Device Password
Enter 8 to 16 characters.
The password should contain at least 2 types of uppercase letters, lowercase letters, digits, and special characters.
Weak
*Verification Code
Used for enabling the Hik-Connect service and performingvideo stream encryption and authentication.
OK

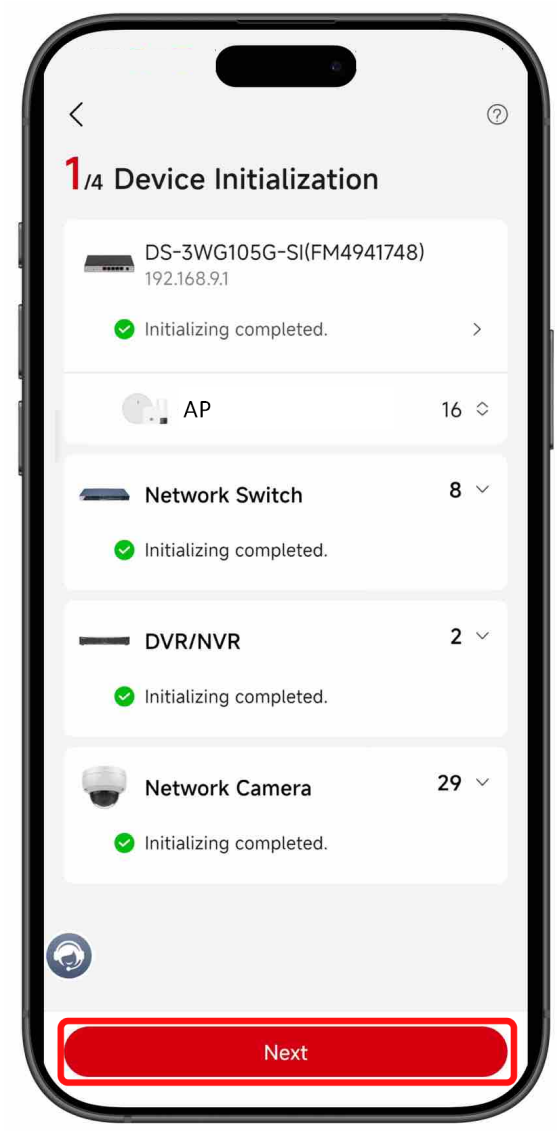

1/4 Device Initialization
DS-3WG105G-SI(FM4941748)
192.168.9.1
Activating...
AP
16
Network Switch
8
Initializing...
DVR/NVR
2
Initializing...
Network Camera
29
Initializing...
Initializing... Please wait.
29%

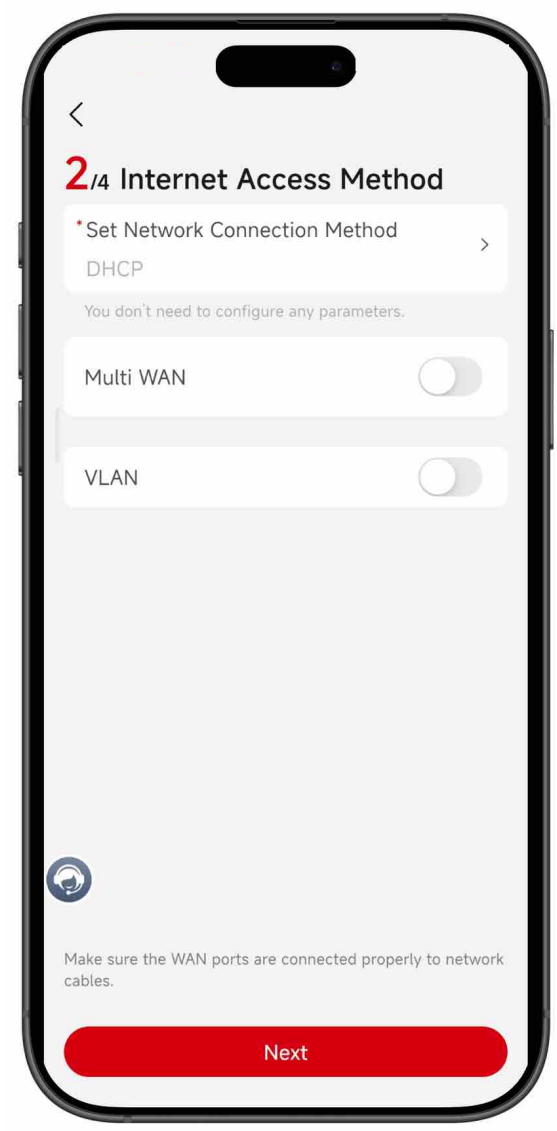

1/4 Device Initialization
DS-3WG105G-SI(FM4941748)
192.168.9.1
Initializing completed.
AP
16
Network Switch
8
Initializing...
Device Initialization
DS-3WG105G-SI(FM4941748)
The device is activated.
Hik-Connect service enabled.

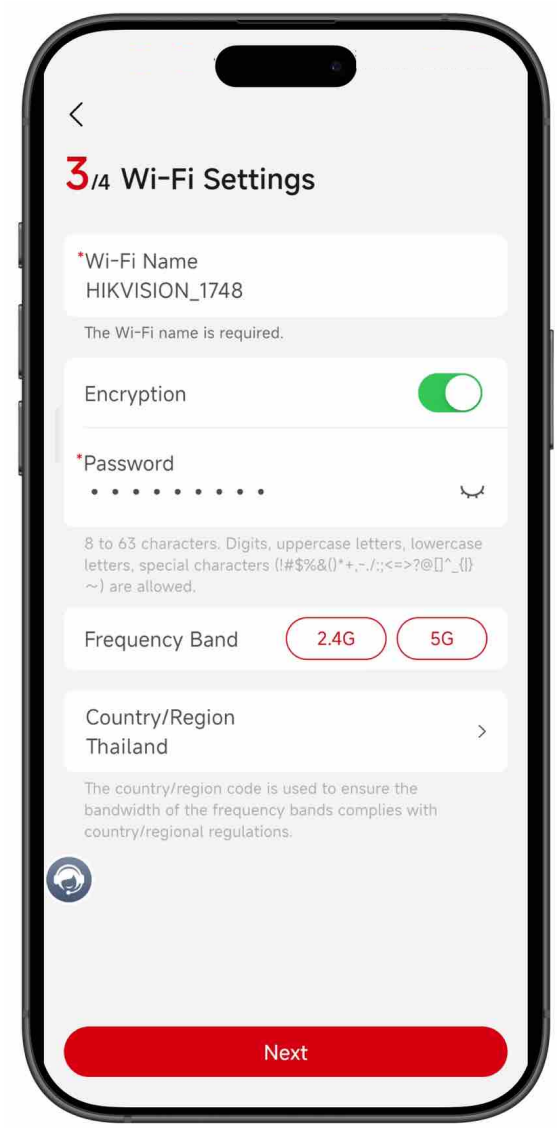

1/4 Device Initialization
DS-3WG105G-SI(FM4941748)
192.168.9.1
Initializing completed.
Device Initialization
DS-3E1726-SI-16F8T2X(FZ7391243)
The device is activated.
Network Configured
192.168.9.101 DHCP: Disabled
Hik-Connect service enabled.
Device time synced with phone time.

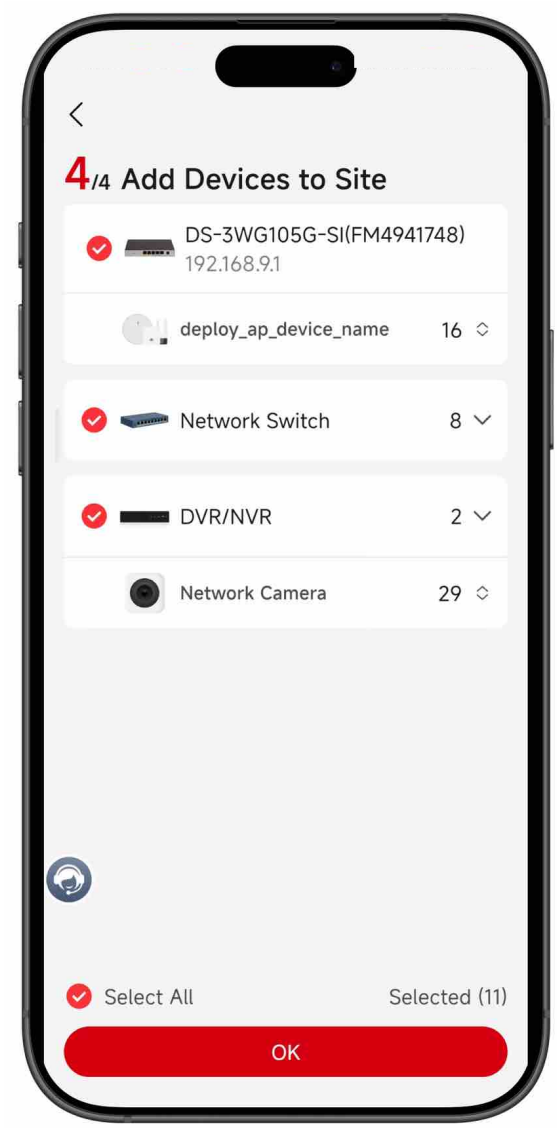

1/4 Device Initialization
Device Initialization
DS-7732NXI-K4(D)(GC0985755)
The device is activated.
Network Configured
192.168.9.110 DHCP: Disabled
Hik-Connect service enabled.
No upgradeable firmware version found.
Device time synced with phone time.
HDD / SD card initialized.

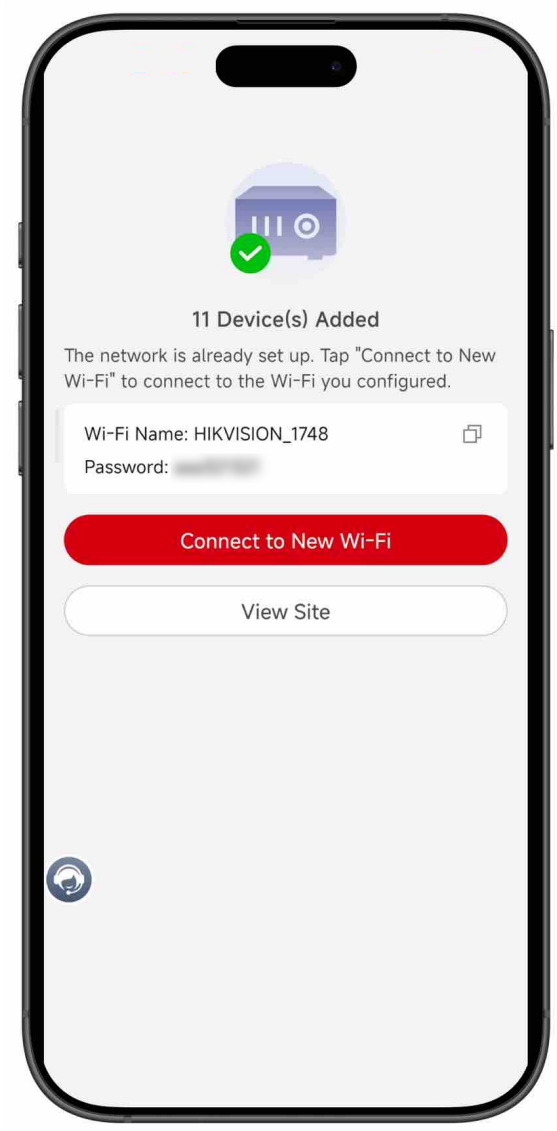

1/4 Device Initialization
Device Initialization
DS-2CD2146G2-ISU(AG5793050)
The device is activated.
Network Configured
192.168.9.120 DHCP: Disabled
Hik-Connect service enabled.
No upgradeable firmware version found.
Device time synced with phone time.
HDD / SD card initialized.

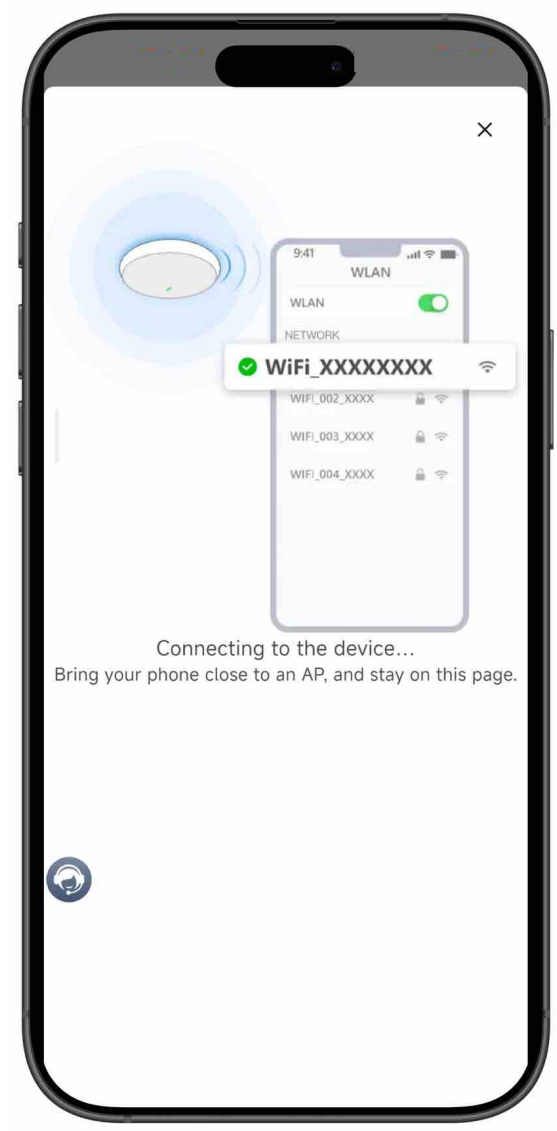

1/4 Device Initialization
DS-3WG105G-SI(FM4941748)
192.168.9.1
Initializing completed.
AP
16
Network Switch
8
Initializing completed.
DVR/NVR
2
Initializing completed.
Network Camera
29
Initializing completed.
Next

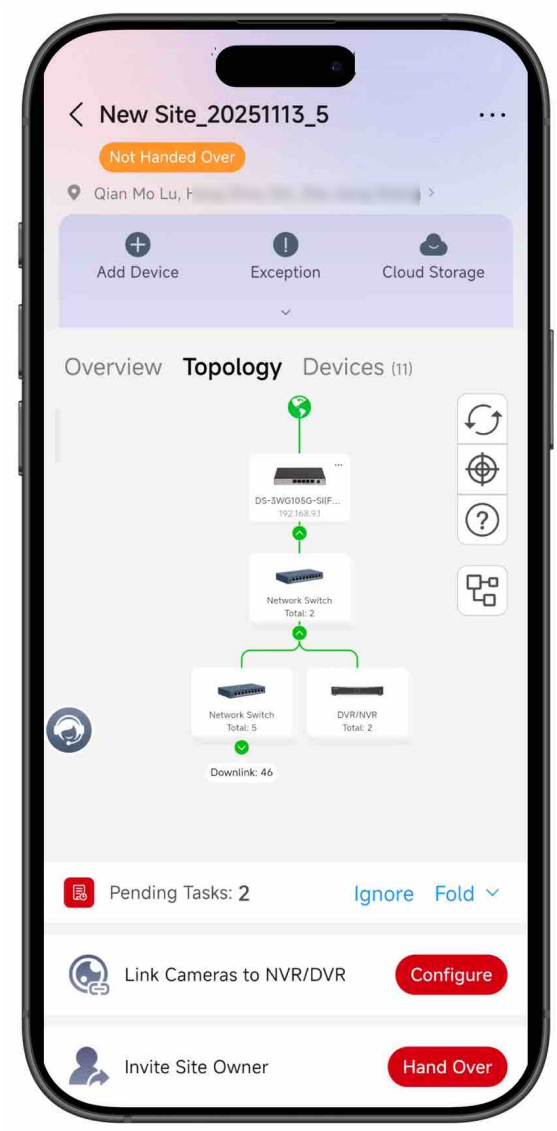

2/4 Internet Access Method
*Set Network Connection Method
DHCP
You don't need to configure any parameters.
Multi WAN
VLAN
Make sure the WAN ports are connected properly to network cables.
Next

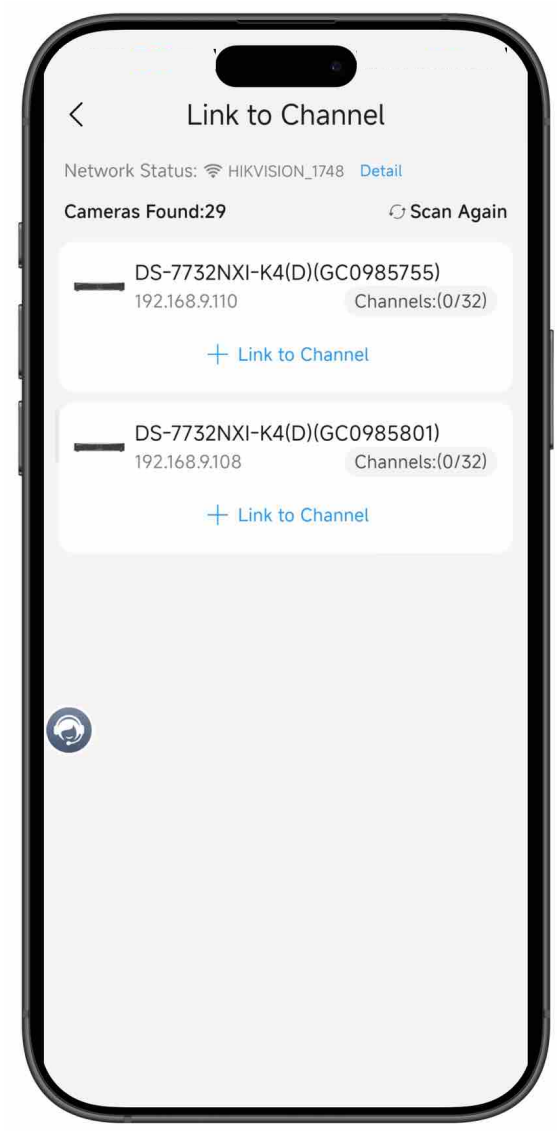

3/4 Wi-Fi Settings
*Wi-Fi Name
HIKVISION_1748
The Wi-Fi name is required.
Encryption
*Password
8 to 63 characters. Digits, uppercase letters, lowercase letters, special characters (!#$%&()*+,-./:;<=>?@[]^_{|}~) are allowed.
Frequency Band
2.4G
5G
Country/Region
Thailand
The country/region code is used to ensure the bandwidth of the frequency bands complies with country/regional regulations.
Next

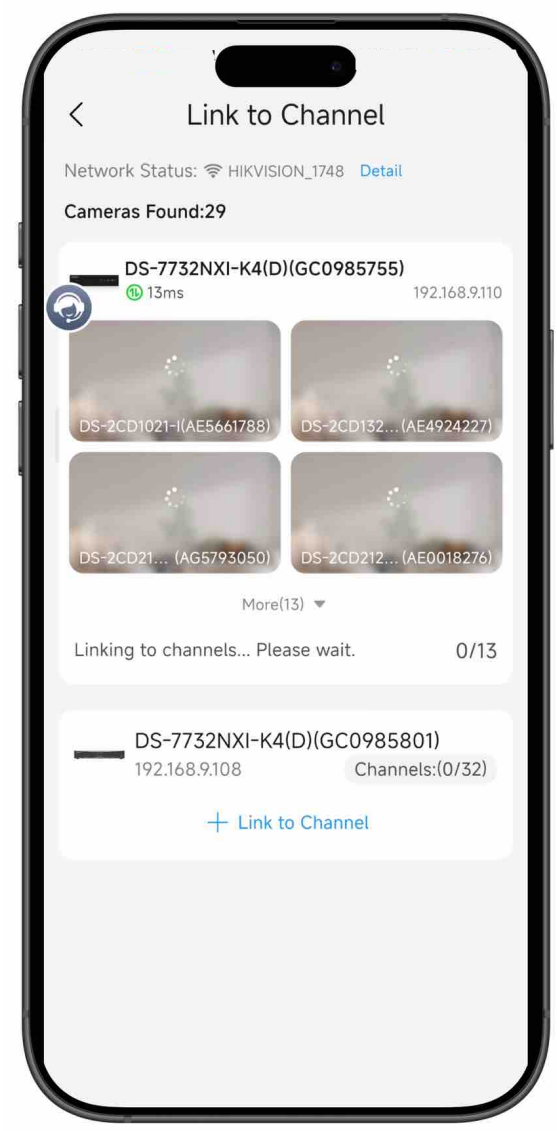

4/4 Add Devices to Site
DS-3WG105G-SI(FM4941748)
192.168.9.1
deploy_ap_device_name
16
Network Switch
8
DVR/NVR
2
Network Camera
29
Select All
Selected (11)
OK

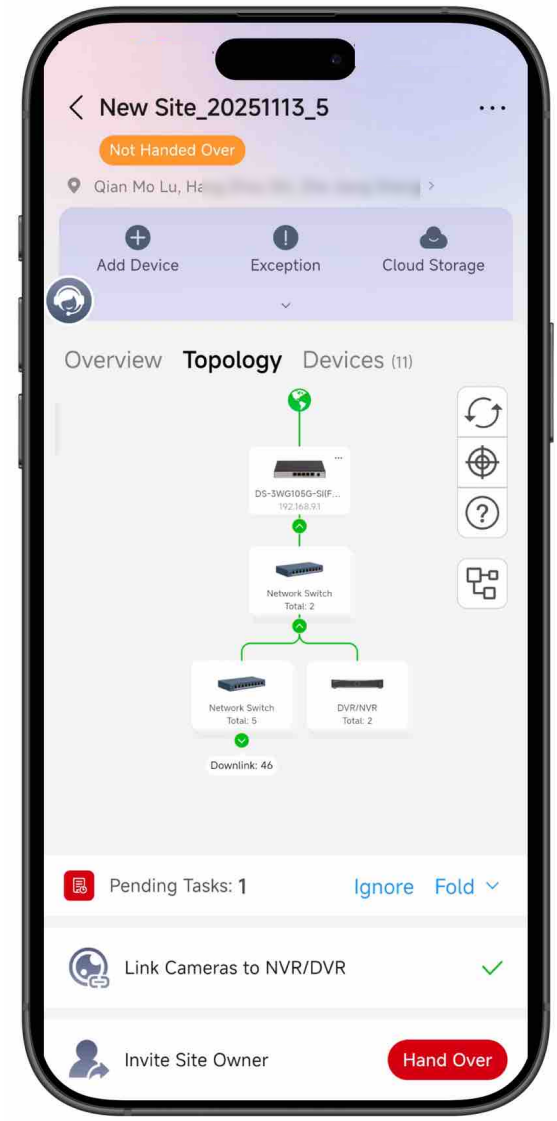

11 Device(s) Added
The network is already set up. Tap "Connect to New Wi-Fi" to connect to the Wi-Fi you configured.
Wi-Fi Name: HIKVISION_1748
Password:
Connect to New Wi-Fi
View Site

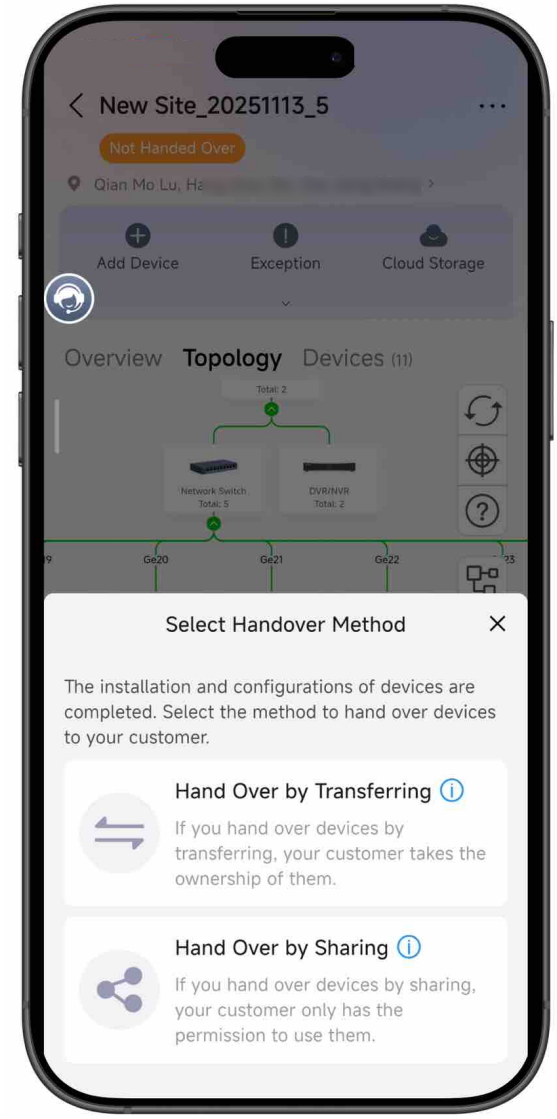

9:41
WLAN
WLAN
NETWORK
WiFi_XXXXXXXX
WIFI_002_XXXX
WIFI_003_XXXX
WIFI_004_XXXX
Connecting to the device...
Bring your phone close to an AP, and stay on this page.

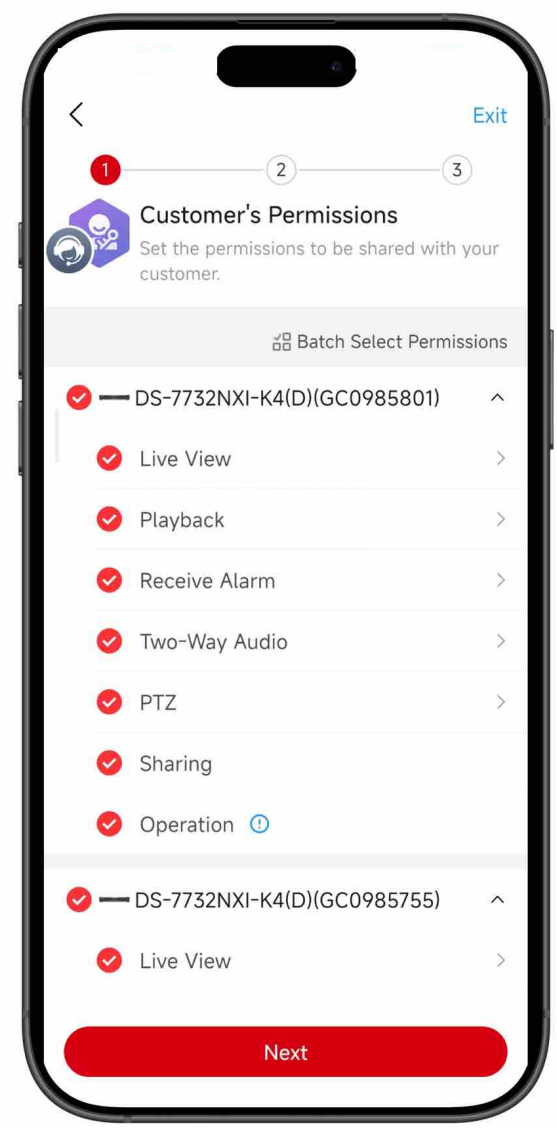

New Site_20251113_5
Not Handed Over
Add Device
Exception
Cloud Storage
Overview
Topology
Devices (11)
Network Switch
Total: 2
Network Switch
Total: 5
DVR/NVR
Total: 2
Downlink: 46
Pending Tasks: 2
Ignore
Fold
Link Cameras to NVR/DVR
Configure
Invite Site Owner
Hand Over

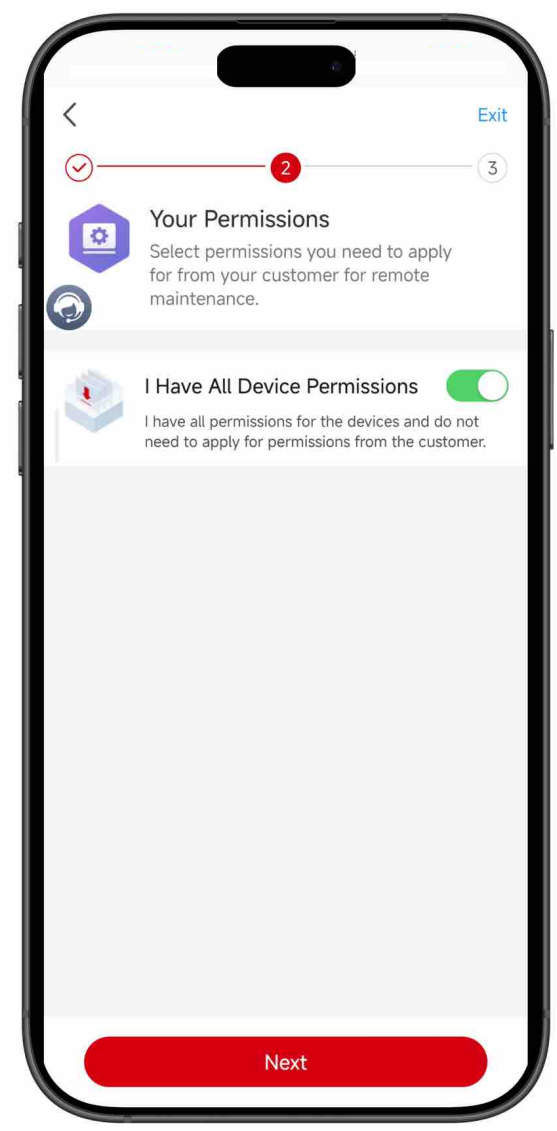

Link to Channel
Network Status: HIKVISION_1748 Detail
Cameras Found:29
Scan Again
DS-7732NXI-K4(D)(GC0985755)
192.168.9.110
Channels:(0/32)
Link to Channel
DS-7732NXI-K4(D)(GC0985801)
192.168.9.108
Channels:(0/32)
Link to Channel


Link to Channel
Network Status: HIKVISION_1748 Detail
Cameras Found:29
DS-7732NXI-K4(D)(GC0985755)
13ms
192.168.9.110
DS-2CD1021-I(AE5661788)
DS-2CD132... (AE4924227)
DS-2CD21... (AG5793050)
DS-2CD212... (AE0018276)
More(13)
Linking to channels... Please wait.
0/13
DS-7732NXI-K4(D)(GC0985801)
192.168.9.108
Channels:(0/32)
Link to Channel


New Site_20251113_5
Not Handed Over
Add Device
Exception
Cloud Storage
Overview
Topology
Devices (11)
Network Switch
Total: 2
Network Switch
Total: 5
DVR/NVR
Total: 2
Downlink: 46
Pending Tasks: 1
Ignore
Fold
Link Cameras to NVR/DVR
Invite Site Owner
Hand Over


New Site_20251113_5
Not Handed Over
Add Device
Exception
Cloud Storage
Overview
Topology
Devices (11)
Select Handover Method
The installation and configurations of devices are completed. Select the method to hand over devices to your customer.
Hand Over by Transferring
If you hand over devices by transferring, your customer takes the ownership of them.
Hand Over by Sharing
If you hand over devices by sharing, your customer only has the permission to use them.


Exit
1
2
3
Customer's Permissions
Set the permissions to be shared with your customer.
Batch Select Permissions
DS-7732NXI-K4(D)(GC0985801)
Live View
Playback
Receive Alarm
Two-Way Audio
PTZ
Sharing
Operation
DS-7732NXI-K4(D)(GC0985755)
Live View
Next


Exit
2
3
Your Permissions
Select permissions you need to apply for from your customer for remote maintenance.
I Have All Device Permissions
I have all permissions for the devices and do not need to apply for permissions from the customer.
Next


Close
3
Hand Over
Hand over devices to your customer.
(Hik-Connect V5.4.0 or later is required.)
Hand Over via QR Code
Scan the QR code with Hik-Connect (V5.4.0 or later) to finish the handover. The QR code can be scanned by multiple customers.
QR Code Valid Until:
16/Nov/2025 19:33
Hand Over via Phone/Email
Enter the account of your customer to hand over the site.



Figure 3-89 Device Onboarding and Site Handover

Table 3-9 What Can Be Done During Onboarding

Stage	Description
1. Discover Devices on the LAN	Tap **Find Devices on LAN** to discover devices connected to the same local network. **Discovery Results** Hik-Partner Pro can discover: • Activated devices • Unactivated devices

Stage	Description
	• Devices already onboarded • Unsupported devices
2. Initialize Devices	Before devices can be added to a site, they may need to be activated. You may be required to enter: • Verification Code • User Name and Device Password
3. Resolve Initialization Issues	Hik-Partner Pro automatically detects common issues. Examples: • IP address conflict • Incorrect gateway • Incorrect subnet mask • Incorrect password • Device already added • Firmware risks
4. Configure Internet Access	For AC devices and Cloud APs, configure the WAN connection before adding devices. Supported modes: • DHCP • PPPoE • Static IP
5. Configure Wi-Fi Settings	When onboarding ACs or Cloud APs, configure wireless settings. Configuration items: • SSID • Wi-Fi Password • Country/Region
6. Add Devices to a Site	After initialization, add devices to the selected site. **Offline Onboarding:** Hik-Partner Pro supports adding devices to sites even when Internet access is unavailable. Devices will be onboarded automatically once the site is connected to Internet.

Part 3: Verify Deployment

View LAN Topology

Hik-Partner Pro automatically generates a LAN topology after the devices are added to the site. The topology helps verify:

- Device connectivity
- Deployment status
- Network structure

View Pending Onboarding Devices in the Topology

Pending onboarding devices are also displayed in the topology.
This allows installers to verify deployment progress before Internet access is available.

Verify Device Status

Verify the following after onboarding:

- Device online status
- Network connectivity
- Camera linkage
- Topology completeness

Part 4: Complete Site Handover

Complete Recommended Pending Tasks

After onboarding, Hik-Partner Pro may recommend pending configuration tasks, including camera linkage and site handover tasks.

Camera Linkage Reminder

Hik-Partner Pro displays camera linkage reminders when:

- The NVR has available channels.
- Unlinked cameras are detected.
- The pending task list has been dismissed.

Site Readiness Check

Before handing over the site, verify:

- All devices are online.
- No pending onboarding devices remain.
- Camera linkage are complete.
- Wi-Fi settings have been applied.
- Network topology is correct.

Part 5: Manage Devices on the LAN

Open the Device Web Page

Open the device web interface for advanced configuration.

Reboot Devices

Reboot devices remotely through the LAN.

Reset Devices

Restore devices to factory settings when necessary.

Part 6: Troubleshooting

Device Cannot Be Added

Possible causes:

- Device already belongs to another account.
- Verification code is incorrect.
- Firmware is incompatible.
- Network connectivity issues.

Device Remains Pending Onboarding

Please check:

- Internet connectivity.
- WAN settings.
- Device power status.

LAN Discovery Cannot Find Devices

Verify:

- The mobile device and target devices are on the same LAN.
- Location permission is enabled.
- Local Network Discovery permission is granted.

Add Network Devices and Initialize Network

Quick Set Up AC Router and APs

The AC router can effectively communicate with and manage the APs, and easily configure and manage the entire network. With Hik-Partner Pro, you can activate the AC router and network switches on the same LAN together and configure the network settings.

Before You Start

- Connect and power on your AC router, APs, and network switches.
- Only the network switches (usually connected to the LAN port of the AC router) on the same LAN as the AC router's can be activated together with the AC router.

Steps

1. Connect to the network devices.
   1) **Optional:** In **Add Device Manually** mode, enter the serial number of the AC router.

   Note

   If the SADP tool detects the unactivated AC, you can also enter the initialization process of the AC router.

   2) Scan the QR code of the AC router, and bring your phone close to an AP.
   3) Tap **Join** to join the Wi-Fi network of the AP so that Hik-Partner Pro can find the AC router and switches.
2. Tap **Activate All** to activate the AC router and network switches by setting the device user name, password, and verification code.

   Note

   The verification code is set for only the network switches to enable the Hik-Connect service. The AC router does not need one to enable the service.
3. Configure the network by setting the network connection method and WAN mode.

   DHCP

   The AC router automatically obtains the IP assigned by the superior router to access the Internet.

   PPPoE

   PPPoE is also known as broadband mode. You enter the broadband account and password to allow the AC router to access the Internet.

   Static IP

   You manually set the IP to allow the AC to access the Internet. Static IP supports 4 parameters: IP, subnet mask, gateway, and DNS server. The default IP, gateway, and DNS server addresses are auto obtained from the AC router.

   Multi WAN

Enable **Multi WAN** to set the network connection methods of multiple WAN ports. Each WAN port can be configured for an independent network connection type.

Note

Multi WAN is enabled by default if two or more WAN ports are connected to the cable. The number of supported WAN ports depends on the AC router capability.

4. Set the Wi-Fi network by setting the Wi-Fi name, password (optional), and frequency band.

Note

In situations where you are far away from the AP or there are many obstacles, the 2.4 GHz band may provide a more reliable connection. However, without these limitations, 5 GHz will likely to be a faster choice.

5. Add devices to a personal site.

Note

Adding the AC to a team site is not supported.

6. When the AC is added, tap **Auto Connect** to connect your phone to the new Wi-Fi you just configure, or copy the Wi-Fi name and password to manually join the Wi-Fi.

Quick Set Up Cloud APs

Cloud APs are managed via the cloud instead of the AC router, and are designed to meet the cost-effective wireless coverage needs of SMBs and stores. You can use Hik-Partner Pro to quickly activate cloud APs and network switches together, set up Wi-Fi, and add the cloud APs and network switches to a site.

Before You Start

- Connect and power on your router, cloud APs, and network switches.
- Only the network switches (usually connected to the LAN port of the router) on the same LAN as the Cloud APs' can be activated together with the cloud APs.

Steps

1. Enter the quick setup process by manually entering the serial number or using the SADP tool.

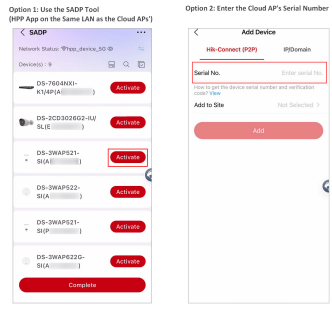


Figure 3-90 Two Options

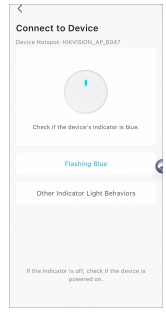
2. Follow the quick setup process.

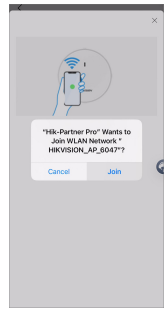
Note

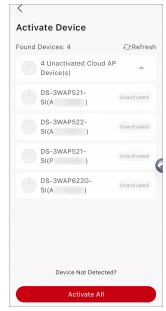
- If your phone is already connected to the same LAN as the AP's, you will start directly from "4. Search for All Unactivated APs on the LAN".
- If you select a site where Wi-Fi is already set up, the existing Wi-Fi networks will be auto applied to the newly added APs.

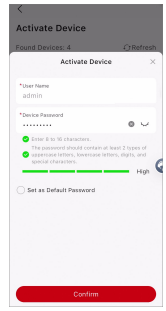


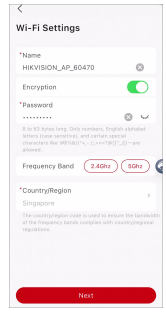
Power on APs and connect them to the network.

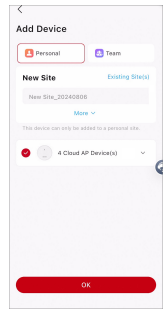


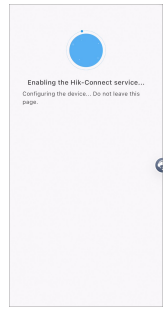


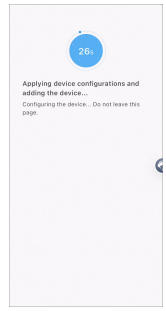

Activate Device
Found Devices: 4
Refresh
4 Unactivated Cloud AP Device(s)
Device Not Detected?
Activate All

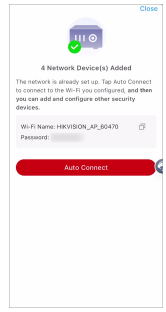

Activate Device
Activate Device
*User Name
admin
*Device Password
High
Set as Default Password
Confirm


Wi-Fi Settings
*Name
HIKVISION_AP_60470
Encryption
*Password
Frequency Band
2.4Ghz
5Ghz
*Country/Region
Singapore
Next


Add Device
Personal
Team
New Site
Existing Site(s)
More
4 Cloud AP Device(s)
OK







Quick Set Up Router

You can use Hik-Partner Pro to quick activate a router, set up the and add it to the Hik-Partner Pro.

Steps

1. Enter the quick setup process.
   - Use the SADP tool to search for the router (on the same LAN as your phone's).
   - Scan the QR code of the router.
   - Enter the serial number of the router.
2. Tap **Activate** and follow the quick setup process.

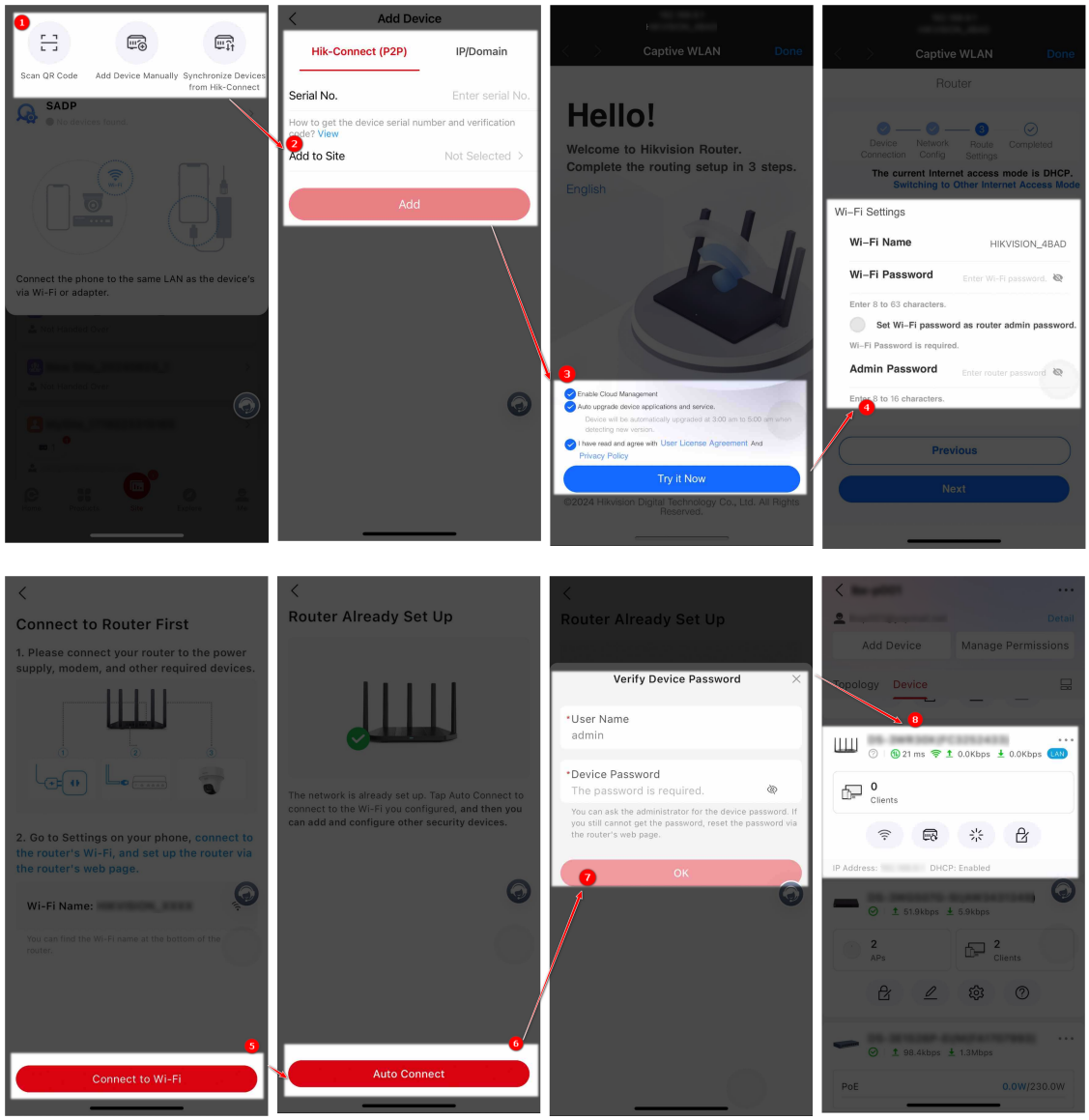


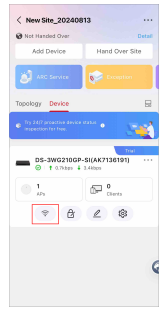
Figure 3-91 Quick Set Up Router

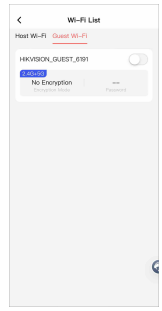
AC Router Operations

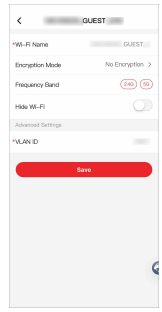
After you add the AC router and initialize the network, you can perform some operations, including rebooting and remotely configuring the device.

On AC Router Device Card

On an AC router device card, you can view the number of APs and clients, uplink & downlink rates, and tap buttons for resetting the password, editing the device name, remotely configuring the device, and setting the Wi-Fi netowrks (host and guest Wi-Fi networks).

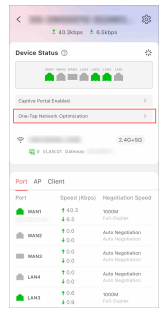


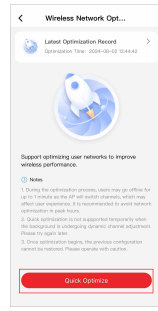


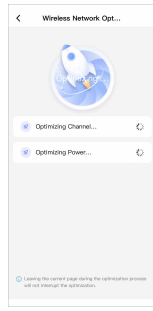


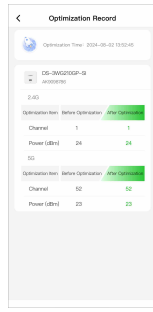
On AC Router Device Details Page

You can tap an AC device card to view its details such as the port status, the uplink & downlink bandwidth utilization rate, and the Wi-Fi list. You can perform the following operations.









Operation	Description
One-Tap Network Optimization	Quick optimize the wireless network performance.
Reboot Device	Tap to reboot the AC.
Configure Wi-Fi	Tap a Wi-Fi to set its name, encryption mode, frequency band, and VLAN ID.
Configure AC	Tap to remotely configure the AC, including setting the LAN, Wi-Fi, password, and health status.
View Diagram Explanation	Tap to know what different types of diagrams mean.

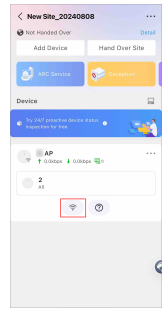
Table 3-10 List of Ports, APs, and Clients

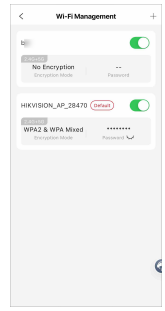
Type	Description
Port	• You can view the port type (WAN/LAN), port name, IP address of WAN port, connection status, uplink & downlink rate, negotiation rate, and peer device. • You can tap a WAN port to go to the WAN settings page.
AP	• You can view the AP name, IP address, online/offline status, connected clients, MAC address, and number of Aps. • Tap an AP to go to the AP details page • Tap ••• → **Find Me** to manually make the AP indicator flash to find the AP. • Tap ••• → **Reboot** to reboot the AP. • Tap 0 to view the client list of an AP. • Tap **AP Indicator Switch**to turn on/off the indicators of all APs.
Client	• You can view the client name, connection mode, connected AP, and uplink & downlink rates. • Tap a client device to jump to its details page.

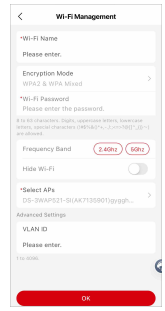
Cloud AP Operations

Unified Wi-Fi Settings for Cloud APs on Site

For cloud APs added to the site, you can set one or more Wi-Fi networks (up to 8) for these cloud APs. For each Wi-Fi network, you can select one or more cloud APs to apply the Wi-Fi settings.

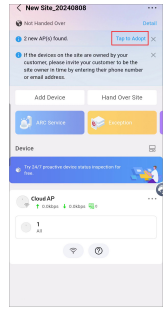


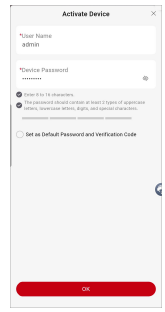


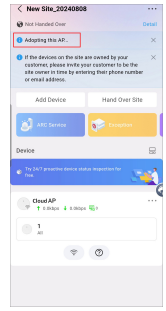


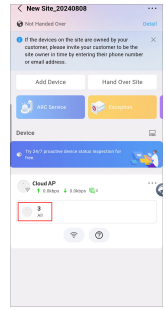
One Tap to Adopt New APs on Site

For new APs found on the same LAN as your phone's, you can tap to adopt these new APs, which is to activate the APs, set the APs to cloud mode, and add the APs to the site.



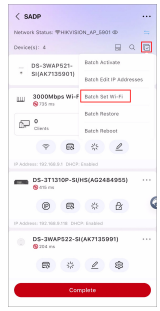


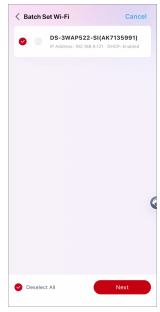


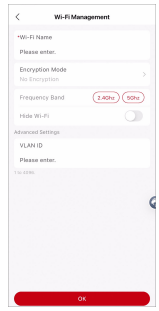


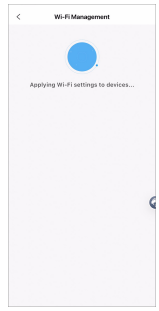
Batch Set Wi-Fi for Multiple APs Using the SADP Tool

You can use the SADP tool to batch set one default Wi-Fi network for multiple cloud APs that are already activated.









Network Switch Operations

On the device list, tap the switch card to enter the device details page.

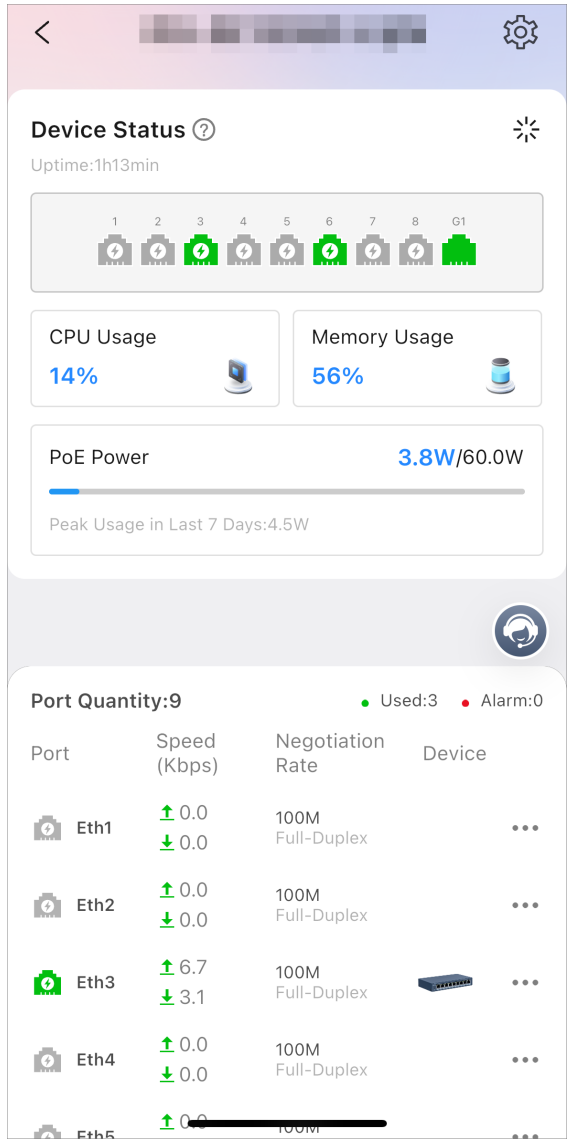


Figure 3-92 Network Switch Detail Page

VLAN Management

Virtual Local Area Networks (VLANs) are used to partition a physical network into smaller, isolated subsections. By isolating devices within a VLAN, network administrators can restrict communication between devices in different VLANs to reduce the risk of unauthorized access or data breaches, and easily troubleshoot issues to reduce downtime.

For example, a company has multiple departments, such as Marketing, Finance, IT, and Human Resources, all located on different floors of the same building. The company has a single physical network infrastructure, and all devices are connected to the same network. The company wants to ensure that each department's network traffic is isolated for better performance, security, and manageability. To achieve this, the network administrator decides to implement VLANs.

This section will guide you through configuring VLANs without going to the device's web configuration page.

1. Tap ⚙ in the upper right corner of the switch detail page, and then tap **VLAN**.
2. Create a VLAN on your switch.
   a. Tap **VLAN ID → Add** .
   b. Select an adding mode.
   c. Set the VLAN ID to identify and differentiate VLANs within a Layer 2 network domain, and tap **Save**.

   Note

   - The maximum number of VLANs that can be added in a batch varies with device models.
   - VLAN ID 1 and 4095 are typically reserved for special purposes. VLAN ID 1 is typically used for the default VLAN. Most switches are assigned to the default VLAN by default if no other VLAN is specified. VLAN ID 4095 is reserved for the use of VLAN trunking protocols. It is not used for regular VLAN traffic.
3. Assign ports to the VLAN to enable logical segmentation of the network.
   a. Tap **Configure**, and select the desired ports.

   Note

   The VLAN configuration is not allowed for ports in an aggregation group. Aggregation groups, also known as link aggregation or port trunking, are used to combine multiple physical ports into a single logical port to increase bandwidth and provide redundancy.

   b. Select a port VLAN type.

   Note

Port Type	Description	Following Operation
ACCESS	Used to connect devices that need to connect devices that need to communicate within a single VLAN. An access port is like a door that leads directly into a specific room (VLAN). When you enter through that door, you can only communicate with the people inside that room. For example, if you have an access port assigned to VLAN 10, any device connected to	None

Port Type	Description	Following Operation
	that port can only communicate with other devices.	
TRUNK	Used to connect devices that need to communicate with multiple VLANs. A trunk port is like an elevator in the building. The elevator can carry people (data) to multiple rooms (VLANs) based on the floor (VLAN tag) they want to go to. For example, if you have a server that needs to communicate with devices in VLANs 10, 20, 30, you would connect the server to a trunk port. The trunk port would carry traffic for all the three VLANs, and the VLAN tags in the data packages would help the switch determine which VLAN the traffic belong to.	Set the accessible VLANs. For example, consider a switch with VLANs 10, 20, and 30. If you have a trunk port connecting to a server, you might only want the server to communicate with devices in VLANs 10 and 20, but not VLAN 30. In this case, you would configure the trunk port to have VLANs 10 and 20 as accessible VLANs, while excluding VLAN 30.

c. Set the PVID (Port VLAN ID) to ensure untagged traffic is routed to the correct VLAN, and tap **Save**.

Note

The PVID is used to used to determine which VLAN an incoming packet belongs to when the packet does not carry any VLAN tag. In simpler terms, the PVID is the default VLAN assigned to a switch port. When a device connected to that port sends a packet without a VLAN tag, the switch will associate the packet with the VLAN specified by the PVID. For example, consider a switch with VLANs 10, 20, and 30. If you have a port connected to a device that doesn't support VLAN tagging, you can assign a PVID to that port. If the PVID is set to VLAN 10, any untagged traffic received on that port will be considered part of VLAN 10 and forwarded accordingly.

Available Operations

Perform the following operations according to your requirements.

Operation	Description
Reboot Switch	Tap ⁜ to reboot the switch.
View Peer Device	Tap **Device** to view the details of the device connected to this port.
Clear Alarm	For port with alarm(s), tap ··· → **Clear Alarm** to clear the alarm(s) of this port.
Restart Port	For the abnormal port, tap ··· → **Restart Port** to restart this port.
Enable/Disable Extend Mode for Port	Tap **Enable Extend Mode/Disable Extend Mode** to extend or not to extend the transmission range of this port. **Note** After enabled, the transmission range of the port will be extended to 200 to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.
Detect Cable Status	Tap → **Cable Detection** , tap a port, and then tap **Detect**. When the detection is finished, you can view the detection result and cable length.

How to Use Switch Port AR Visualization

Feature Overview

The Hik-Partner Pro Mobile Client provides a **Switch Port AR Visualization feature** that allows installers to scan the AR QR code on a switch device and view port and device information using augmented reality.

In the AR view, device information is displayed directly on the corresponding switch ports, including:

- Device name
- Device icon
- IP address
- Upload and download traffic rates

Users can also tap device icons to view device details or perform configuration, improving deployment and maintenance efficiency.

Typical Use Cases

This feature is useful in scenarios such as:

- Network verification before project delivery
- Cable management in equipment rooms
- Quickly identifying devices connected to switch ports during maintenance
- Viewing live snapshots from surveillance devices

The AR view provides an intuitive way to understand port connections and device status.

Prerequisites

Before using the AR feature, ensure that:

- The mobile device runs **Android 8.0 or later** / **iOS 14.0 or later**.
- For **Android**, this feature requires the latest version of **Google Play Services for AR**. Please download and install it first
- The switch model supports AR functionality:
  DS-3E2510-SI-8T2F
  DS-3E2510P-SI-8P2F
  DS-3E2528-SI-24T4F
  DS-3E2528P-SI-24P4F
  DS-3E2728-SI-24T4X
  DS-3E2752-SI-48T4X
  DS-3E2752-SI-48F4X
  DS-3E3728-SI-24T4X
  DS-3E3752-SI-48T4X
  DS-3E3752-SI-48F4X
- You have device management permissions.

Use AR Ports on the Mobile Client

1. Open the **Hik-Partner Pro Mobile Client**.
2. Tap **Site**.
3. Tap the target site to enter the site details page.

   Note

   Make sure the scanned switch device belongs to the selected site.
4. Find and tap **AR Ports** in the site tools, to open the AR scanning interface.

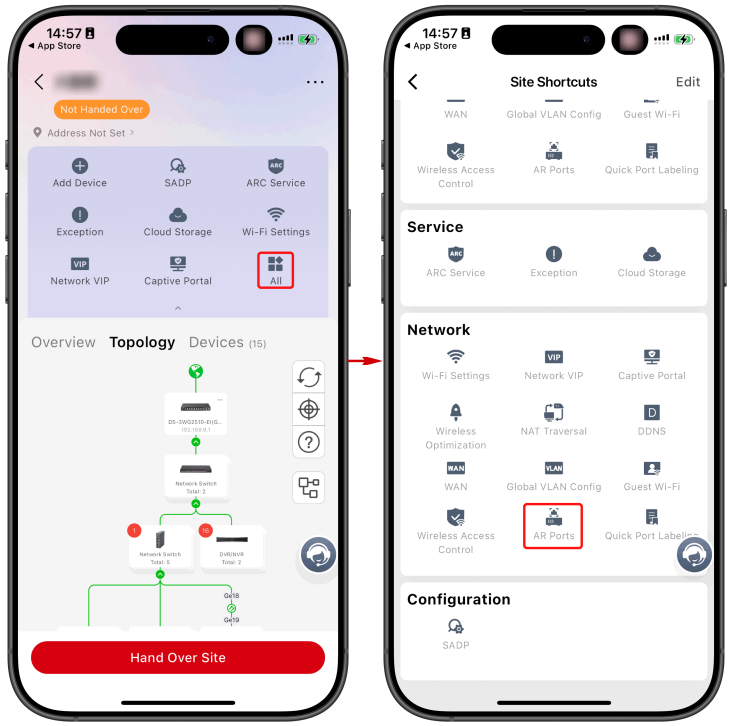


Figure 3-93 AR Ports

5. Move your phone slowly, and scan the switch device and its surrounding environment.

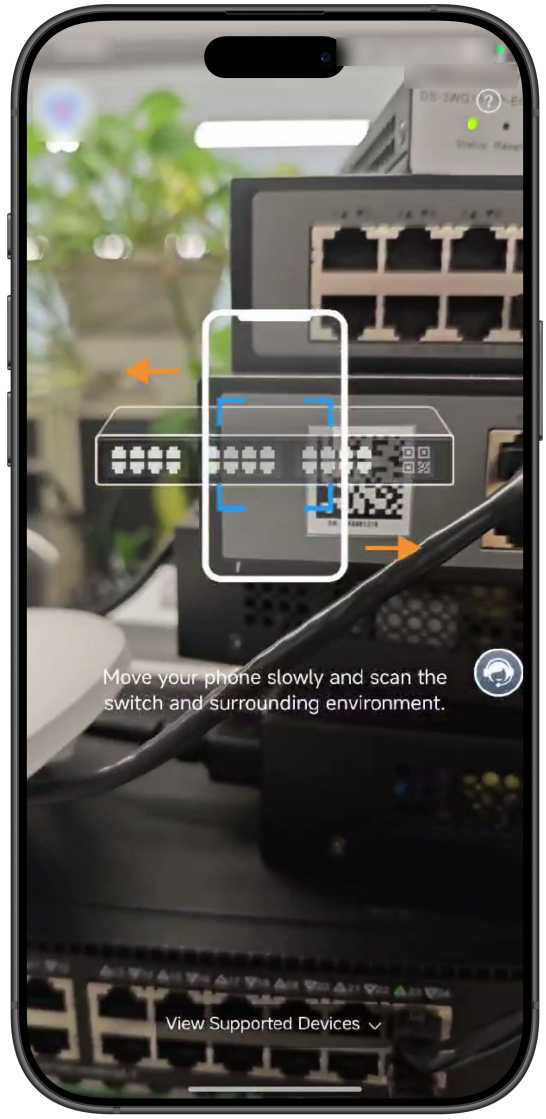


Figure 3-94 Scan Whole Device

6. Scan the AR QR code located on the port panel or at the lower-right corner of the top panel. Make sure it fills the viewfinder.

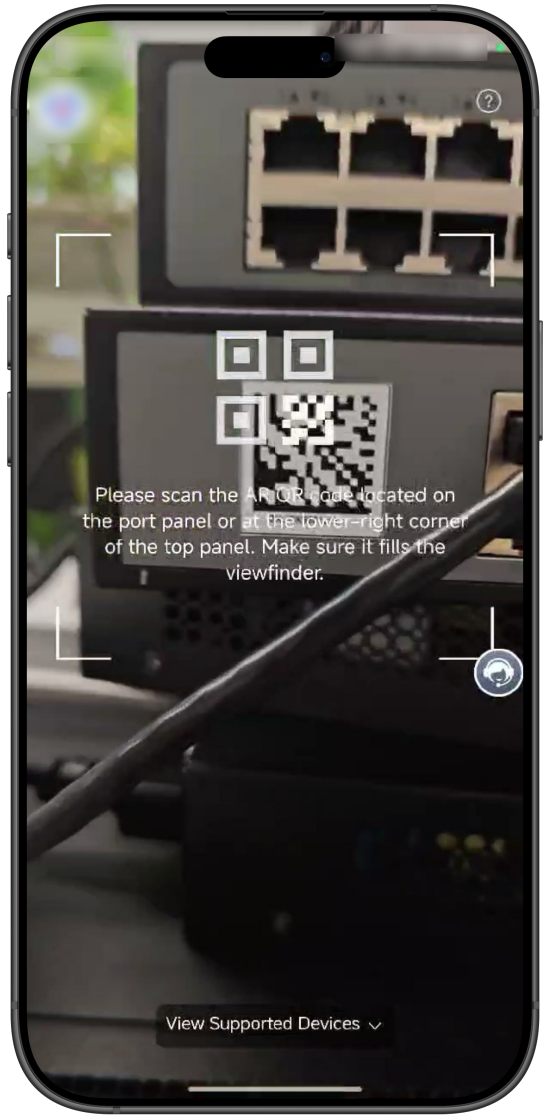


Figure 3-95 Scan AR QR Code

7. Once the device is recognized, it loads switch port information. The screen displays switch ports and connected device information in AR view.



View Port and Device Information

The AR interface displays device information at each port location, including:

- Device name
- Device icon
- IP address
- Upload and download speed

Port status may include:

- Connected
- Disconnected
- Alarm status
- Uplink port

View Port Details

Tap a port area to open the port details panel, which may include:

- Port name
- Port type
- Port status
- Negotiated speed
- VLAN information

Port information can still be viewed even if the port is disabled.

View Device Details

Tap the device icon on a port to view device information:

- **Video devices (network cameras)**
  - Displays the device OSD name
  - Shows the latest snapshot from the camera
  - For multi-channel devices, the first channel is displayed by default
- **Other devices**
  - Tapping the icon opens the device details page

How to Quick Label Ports for Switches

Feature Overview

The Hik-Partner Pro Mobile Client provides a **Quick Port Labeling feature** that allows installers to view devices connected to switch ports and export port label lists.

In large projects or equipment rooms, switches often connect many devices and network cables. With this **Quick Port Labeling feature**, installers can automatically generate port labeling information, reducing manual work and improving deployment and maintenance efficiency.

Typical Use Cases

This feature is useful in scenarios such as:

- Network deployment and port identification before project delivery
- Cable management in equipment rooms
- Quickly identifying devices connected to switch ports during maintenance

The exported label list can be used for physical port labeling and cable organization.

Prerequisites

Before using the quick labeling feature, ensure that:

- The site contains switch devices.
- You have device management permissions.

Access the Quick Port Labeling Tool on the Mobile Client

1. Open the **Hik-Partner Pro Mobile Client**.
2. Tap **Site**.
3. Tap the target site to enter the site details page.

   Note

   Make sure the switch devices to be labeled belong to the selected site.
4. Find and tap **Quick Port Labeling** in the site tools.

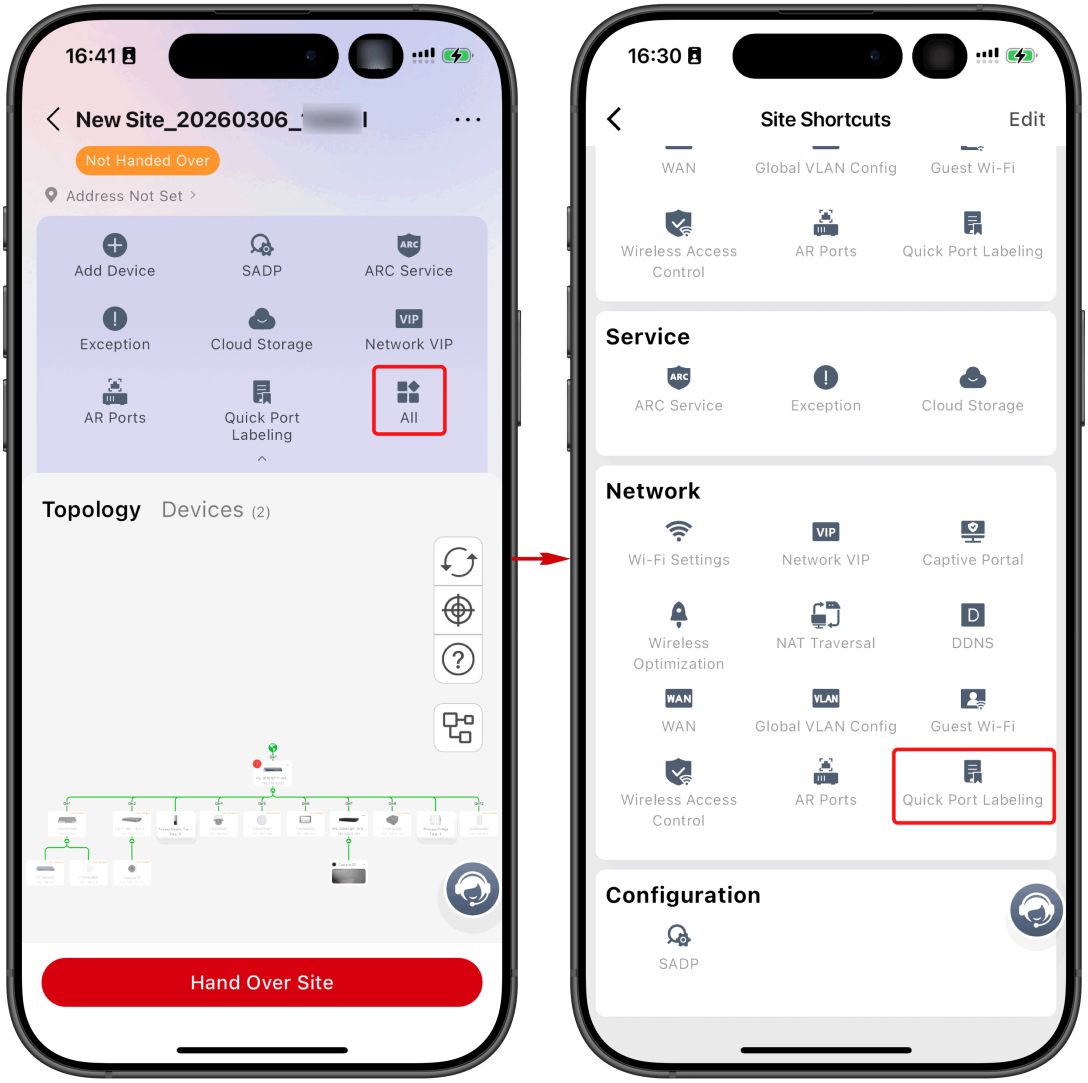
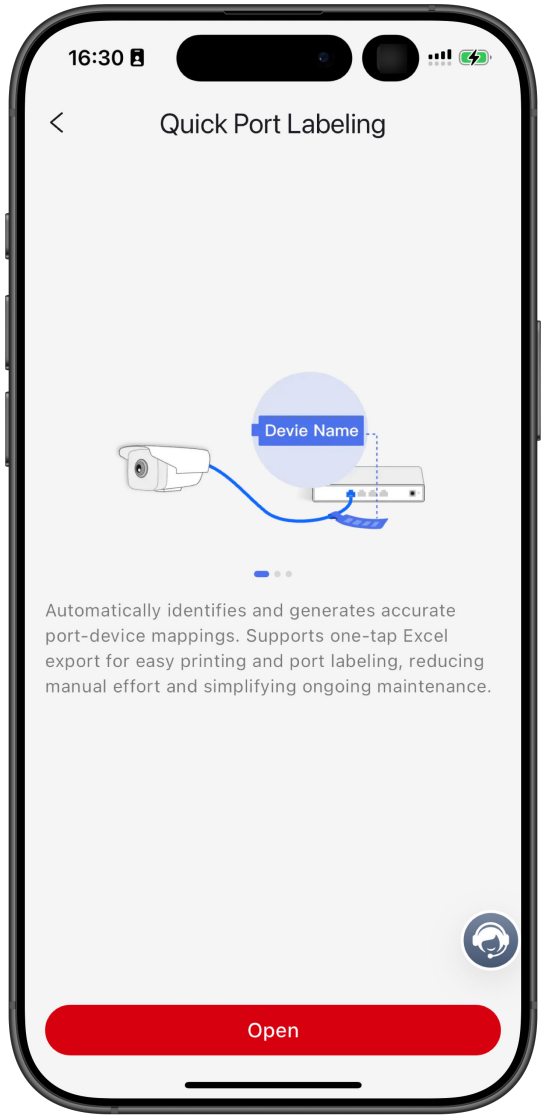
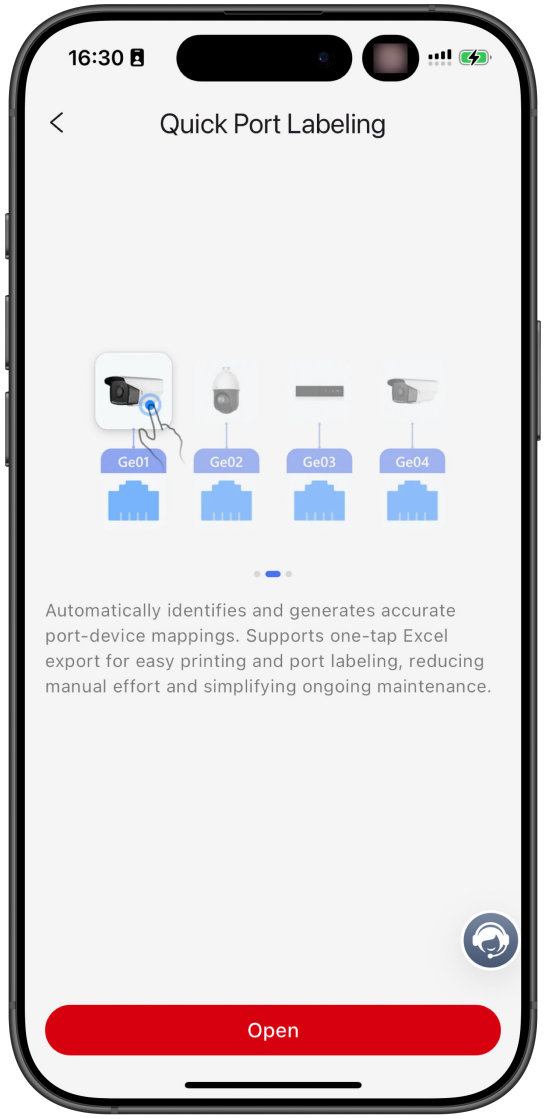


Figure 3-97 Quick Port Labeling Tool

5. If this is your first time accessing this feature, you can view the following feature introduction. Tap **Open** to continue.


16:30
Quick Port Labeling
Devie Name
Automatically identifies and generates accurate port-device mappings. Supports one-tap Excel export for easy printing and port labeling, reducing manual effort and simplifying ongoing maintenance.
Open


16:30
Quick Port Labeling
Ge01
Ge02
Ge03
Ge04
Automatically identifies and generates accurate port-device mappings. Supports one-tap Excel export for easy printing and port labeling, reducing manual effort and simplifying ongoing maintenance.
Open

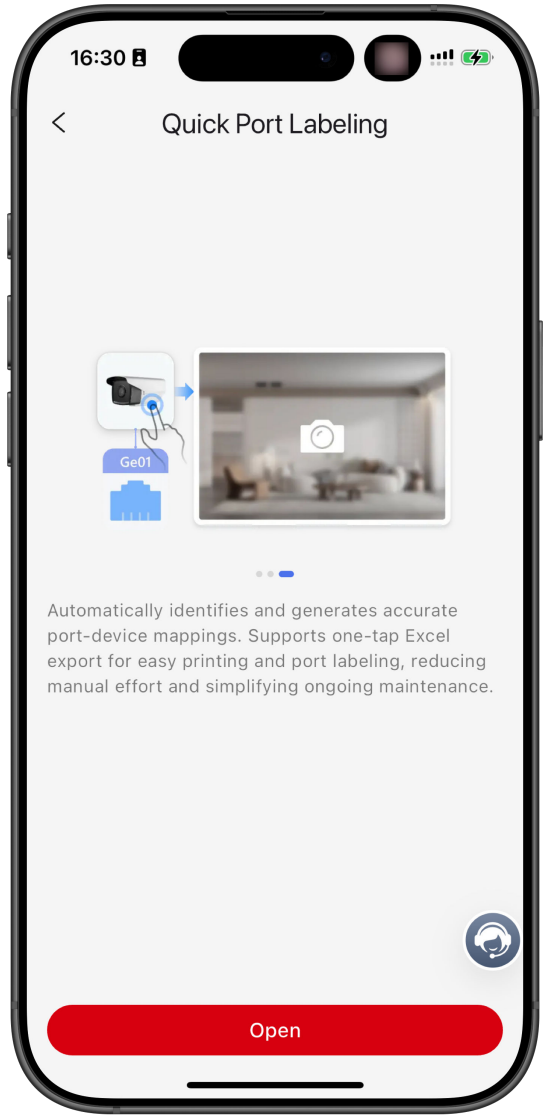


Figure 3-98 Feature Introduction

6. View port info, or tap **Export to Excel** export the port info excel.

Note

To view all the ports, you can drag the red frame on this component left and right.

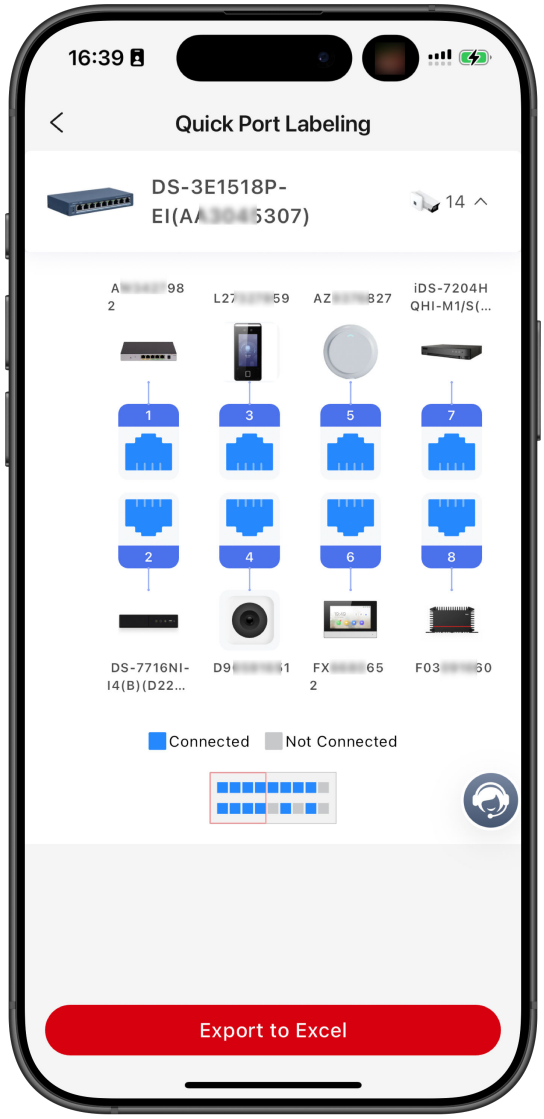

16:39
Quick Port Labeling
DS-3E1518P-
14
iDS-7204H
QHI-M1/S(...
1
2
3
4
5
6
7
8
DS-7716NI-
I4(B)(D22...
Connected
Not Connected
Export to Excel



Figure 3-99 Port Info

View Switch Port Connection Information

After entering the Quick Labeling page, the system displays a list of switches in the site.

For each switch, the following information is displayed:

- Switch name
- Number of connected devices

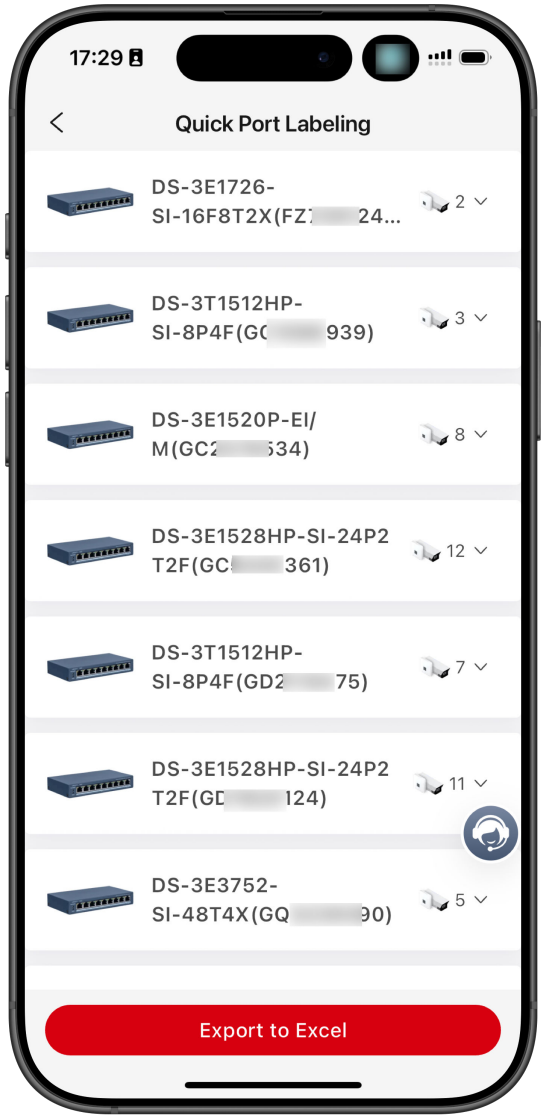
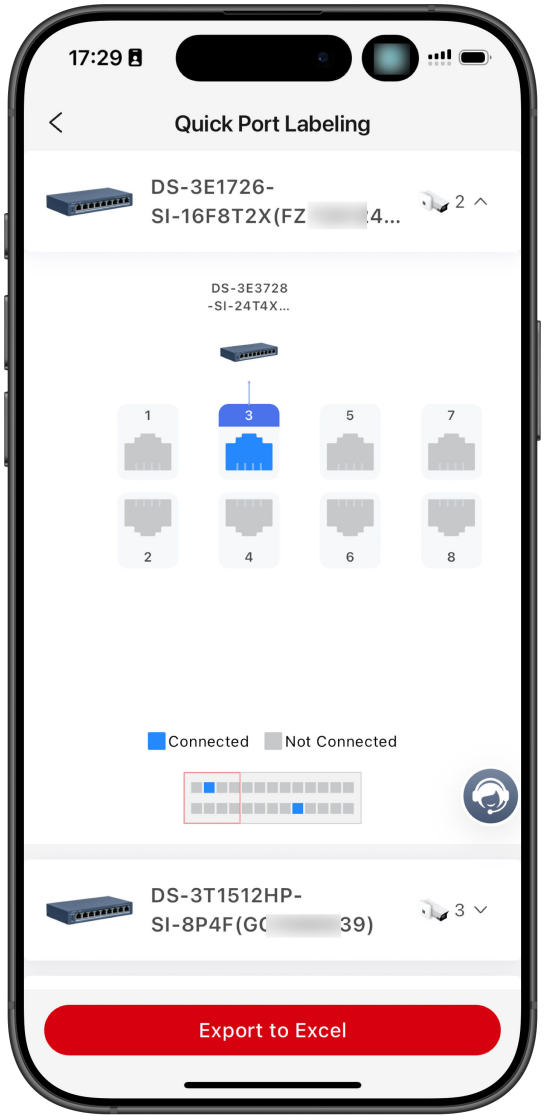


Figure 3-100 Switch List

The first switch is expanded by default to show port connection information.

The port list includes:

- Port number
- Connected device name
- Device type icon
- Port connection status



View Port Details

Tap a port to view detailed information, including:

- Port number
- Device type
- Device model
- Device name (You can edit the device name.)
- Port connection status
- IP address

If the connected device is a network camera, tapping the device icon opens the **Image Capture** window to view the latest image.

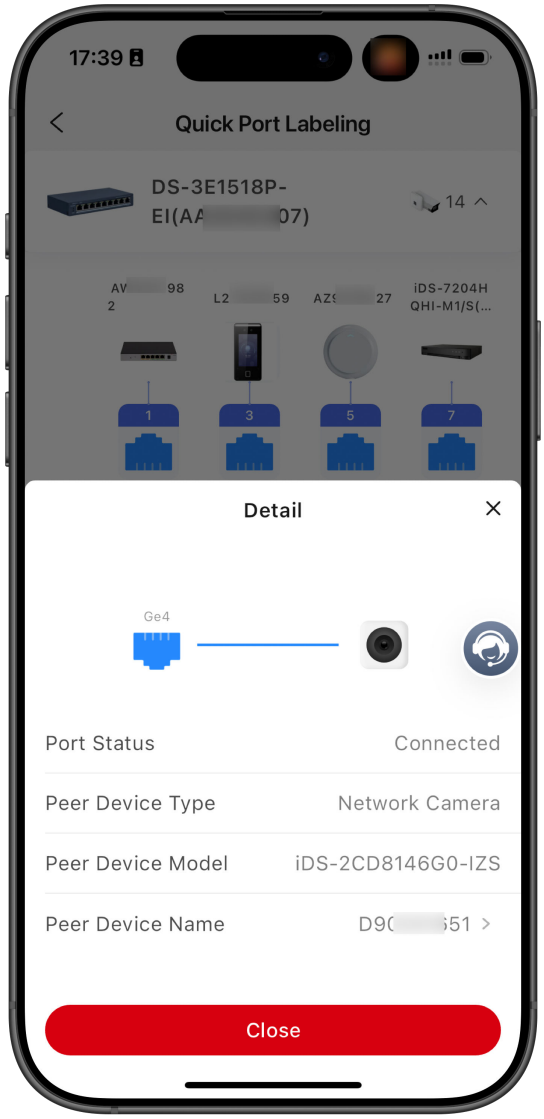


Figure 3-101 Port Details

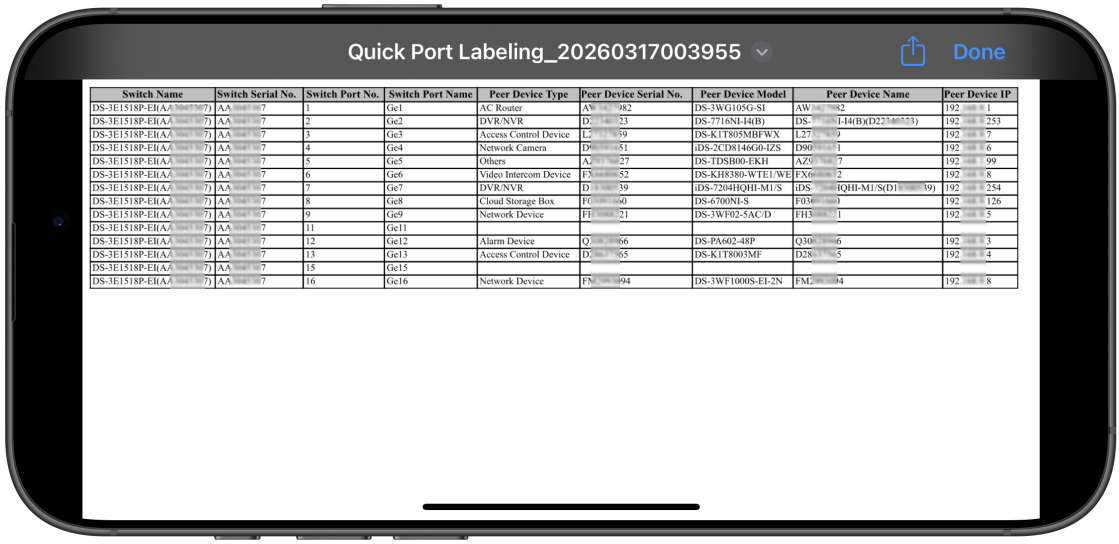
Export the Port Label List

Users can tap **Export to Excel** to export the switch port label list from the Quick Labeling page.

The exported Excel file includes:

- Switch name, serial no., port No., port name
- Peer device type, serial No., model, name, IP

Installers can use this file for port label printing or cable management during deployment.



Switch Name	Switch Serial No.	Switch Port No.	Switch Port Name	Peer Device Type	Peer Device Serial No.	Peer Device Model	Peer Device Name	Peer Device IP
DS-3E1518P-EI(AA 7)	AA 7	1	Ge1	AC Router	A 982	DS-3WG105G-SI	AW 2	192 1
DS-3E1518P-EI(AA 7)	AA 7	2	Ge2	DVR/NVR	D 23	DS-7716NI-I4(B)	DS- I-I4(B)(D22 3)	192 253
DS-3E1518P-EI(AA 7)	AA 7	3	Ge3	Access Control Device	L 39	DS-K1T805MBFWX	L27 9	192 7
DS-3E1518P-EI(AA 7)	AA 7	4	Ge4	Network Camera	D 51	iDS-2CD8146G0-IZS	D90 1	192 6
DS-3E1518P-EI(AA 7)	AA 7	5	Ge5	Others	A 27	DS-TDSB00-EKH	AZ0 7	192 99
DS-3E1518P-EI(AA 7)	AA 7	6	Ge6	Video Intercom Device	F 52	DS-KH8380-WTE1/WE	FX6 2	192 8
DS-3E1518P-EI(AA 7)	AA 7	7	Ge7	DVR/NVR	D 39	iDS-7204HQHI-M1/S	iDS- IQHI-M1/S(D1 39)	192 254
DS-3E1518P-EI(AA 7)	AA 7	8	Ge8	Cloud Storage Box	F 60	DS-6700NI-S	F036 0	192 126
DS-3E1518P-EI(AA 7)	AA 7	9	Ge9	Network Device	FI 21	DS-3WF02-5AC/D	FH3 1	192 5
DS-3E1518P-EI(AA 7)	AA 7	11	Ge11					
DS-3E1518P-EI(AA 7)	AA 7	12	Ge12	Alarm Device	Q 66	DS-PA602-48P	Q30 6	192 3
DS-3E1518P-EI(AA 7)	AA 7	13	Ge13	Access Control Device	D 65	DS-K1T8003MF	D28 5	192 4
DS-3E1518P-EI(AA 7)	AA 7	15	Ge15					
DS-3E1518P-EI(AA 7)	AA 7	16	Ge16	Network Device	FM 94	DS-3WF1000S-EI-2N	FM 4	192 8

Figure 3-102 Exported Excel

Quick Network Device Configuration Guide

Feature Overview

To improve configuration efficiency for installers performing remote maintenance, Hik-Partner Pro Portal offers a **Network Device** quick access entry on the site page.
This feature centralizes frequently used network device configuration options, allowing users to access configuration pages without navigating into each network device individually.
With the **Network Device** module, users can:

- Quickly view supported configuration features.
- Select the target device.
- Open the corresponding device configuration page directly.

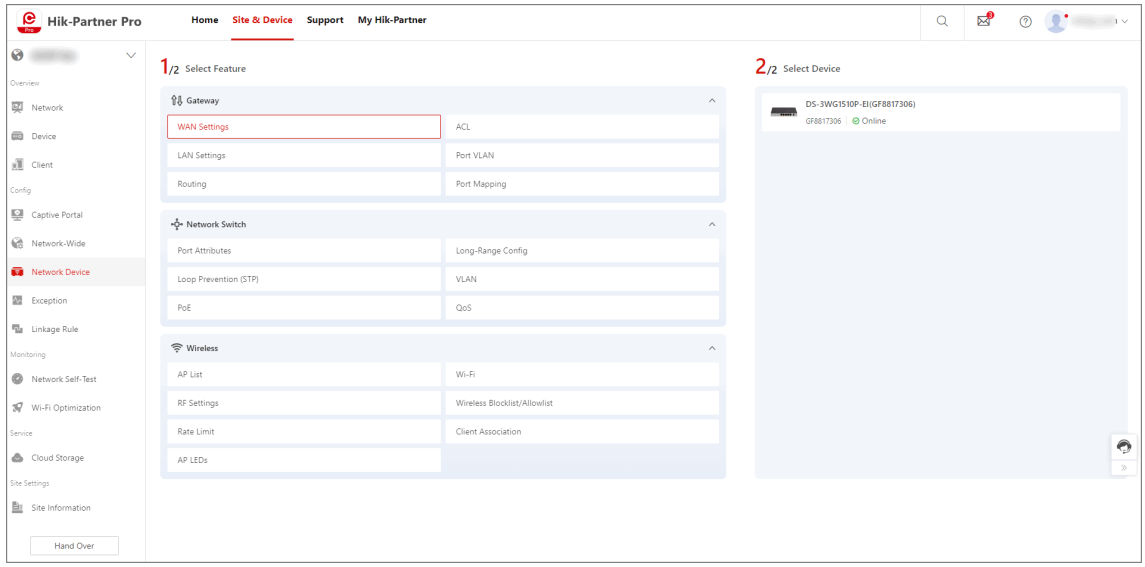


Figure 3-103 Network Device Config

Typical Use Cases

After project deployment, installers often need to perform remote network device configuration or maintenance, such as:

- Adjusting network settings
- Modifying wireless parameters
- Configuring VLAN or port policies
- Managing wireless clients

The **Network Device** quick access entry allows installers to quickly locate and perform these tasks.

Prerequisites

Before using the network device config feature, ensure that:

- Network devices have been added to the site.
- The device supports the selected configuration feature.
- The device is online.
- The user has the site and device management permissions.

Table 3-11 Supported Device Types

Feature Category	Device Type Required
Gateway	AC router.
Network Switch	Network switch.
Wireless	AC router and Cloud AP.

Perform Quick Network Device Config on the Portal

1. Log in to the Hik-Partner Pro Portal.
2. Go to **Site & Device → Customer Site** .
3. Open the target site.
4. Click **Network Device** on the left.

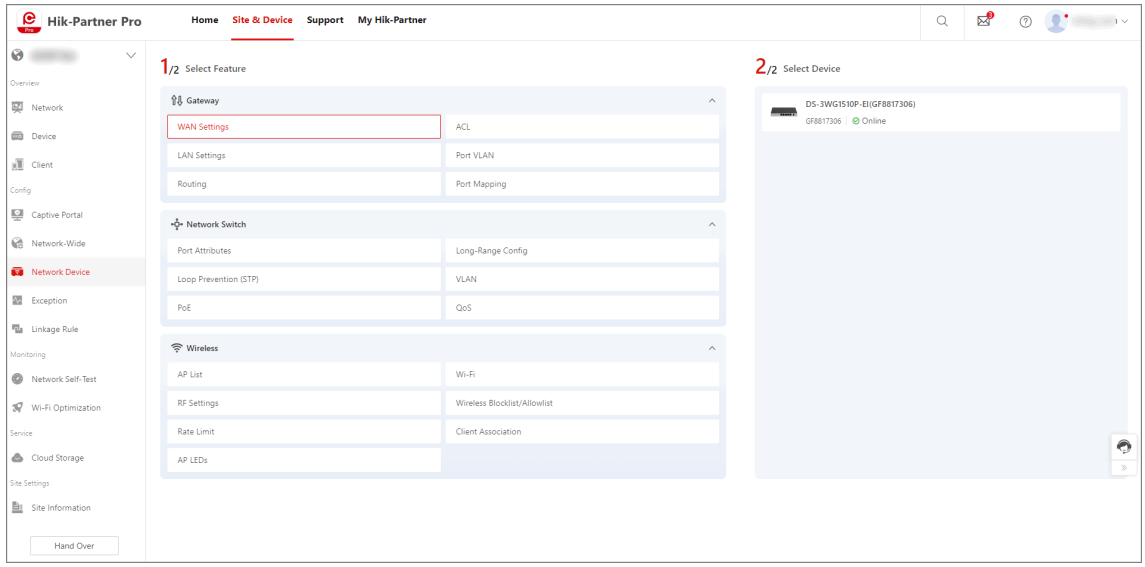


Figure 3-104 Network Device Config

5. Select a configuration feature. After selecting a feature, the system automatically filters devices that support the selected feature.
6. Select a device to configure. The system opens the corresponding device configuration page.
7. After finishing configuration and closing the configuration page, users can return to the previous page and select another device to perform the same configuration.

How to Configure Captive Portal

Overview

Captive Portal allows administrators to require wireless clients to complete authentication before accessing the Internet.
In Hik-Partner Pro, Captive Portal is configured through the following modules:

Module	Purpose
Captive Portal	Create and manage authentication policies.
Portal Template	Selected or created during authentication policy creation; enables authentication methods.

Module	Purpose
Pre-Authorization List	Manage clients that can bypass authentication.
User Management	Create/manage user groups, accounts, and vouchers, and manage registration accounts.
Client	Manage connected clients: block clients, rate limit, disconnect authenticated wireless clients.

A typical configuration flow is:

1. Enter the target site.
2. Go to **Captive Portal**.
3. Create an authentication policy.
4. Select an existing portal template or create a new one.
5. In the portal template, enable one or more authentication methods.
6. Configure method-specific settings.
7. Save the authentication policy.
8. Manage accounts, vouchers, user groups, and clients in related modules.

Applicable Scope

This guide applies to:

Item	Description
Product	Hik-Partner Pro Portal, Hik-Partner Pro Mobile Client
Site type	Personal sites and team sites **Note** For Team sites, Hik-Partner Pro Portal may redirect users to HCT Portal through password-free login when the site contains an AC router that supports Captive Portal.
Device type	AC routers and cloud APs that support Captive Portal
User role	Installer, site administrator, network operator

Prerequisites

Before configuring Captive Portal, make sure that:

1. The site contains an AC router or cloud AP that supports Captive Portal.
2. The device is online.
3. You have the required configuration permission.

Feature Structure

Captive Portal configuration follows this structure:

```
Captive Portal
└── Authentication Policy
    └── Portal Template
        ├── One-click Authentication
        ├── Account Authentication
        ├── Voucher Authentication
        ├── Registration Authentication
        └── Facebook Authentication
└── Pre-Authorization List
```

User and client management is handled separately:

```
User Management
├── User Groups
├── Accounts
├── Vouchers
└── Registration Accounts

Client
├── All Online Clients
│   ├── Block
│   └── Rate Limit
└── Authenticated Wireless Clients
    └── Disconnect
```

Access Captive Portal Configurations

Access Captive Portal

Access Captive Portal Using the Hik-Partner Pro Portal

1. Log in to **Hik-Partner Pro Portal**.
2. Go to **Site & Device → Customer Site** .
3. Select and enter a site.
4. On the left pane, select **Captive Portal**.

The page displays the authentication policy list. If no authentication policy has been created, you can create one.

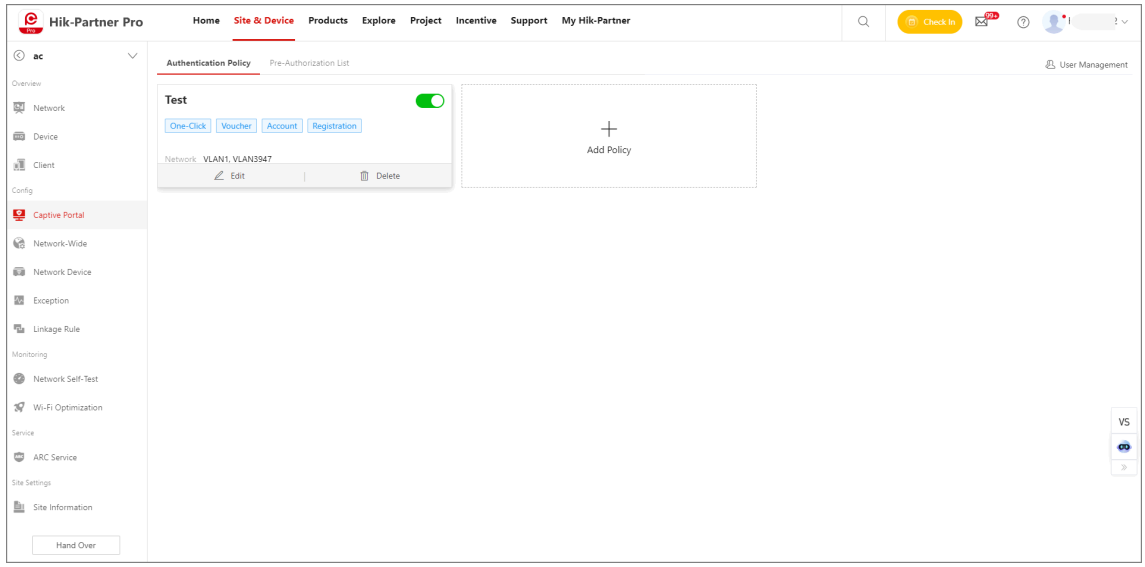
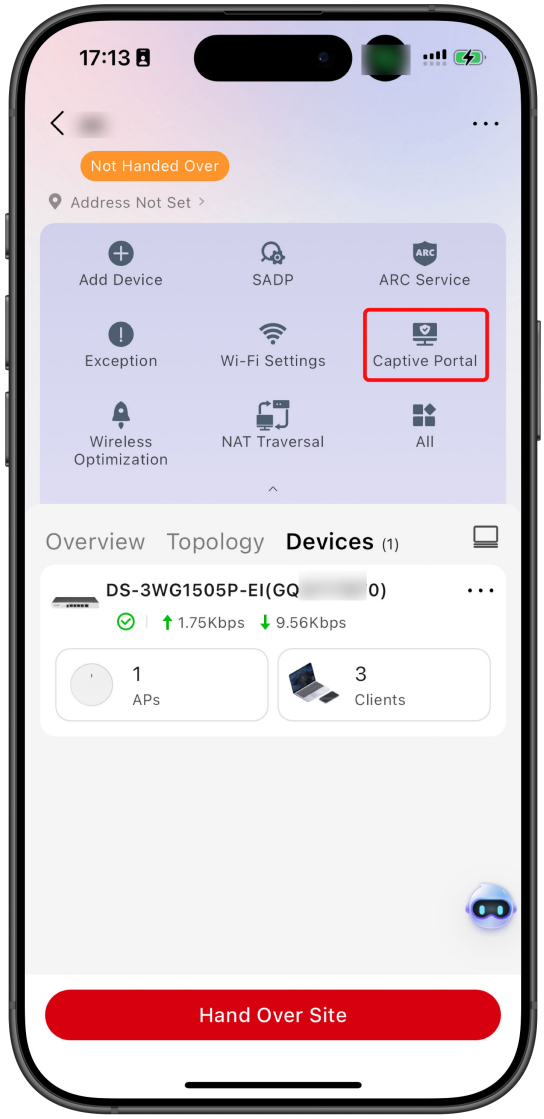


Figure 3-105 Captive Portal

Access Captive Portal Using the Hik-Partner Pro Mobile Client

1. Log in to the **Hik-Partner Pro Mobile Client**.
2. Tap **Site**.
3. Select and enter a site.
4. In the tool section, tap **Captive Portal**.


17:13
Not Handed Over
Address Not Set
Add Device
SADP
ARC Service
Exception
Wi-Fi Settings
Captive Portal
Wireless Optimization
NAT Traversal
All
Overview
Topology
Devices (1)
DS-3WG1505P-EI(GQ 0)
1.75Kbps
9.56Kbps
1
APs
3
Clients
Hand Over Site

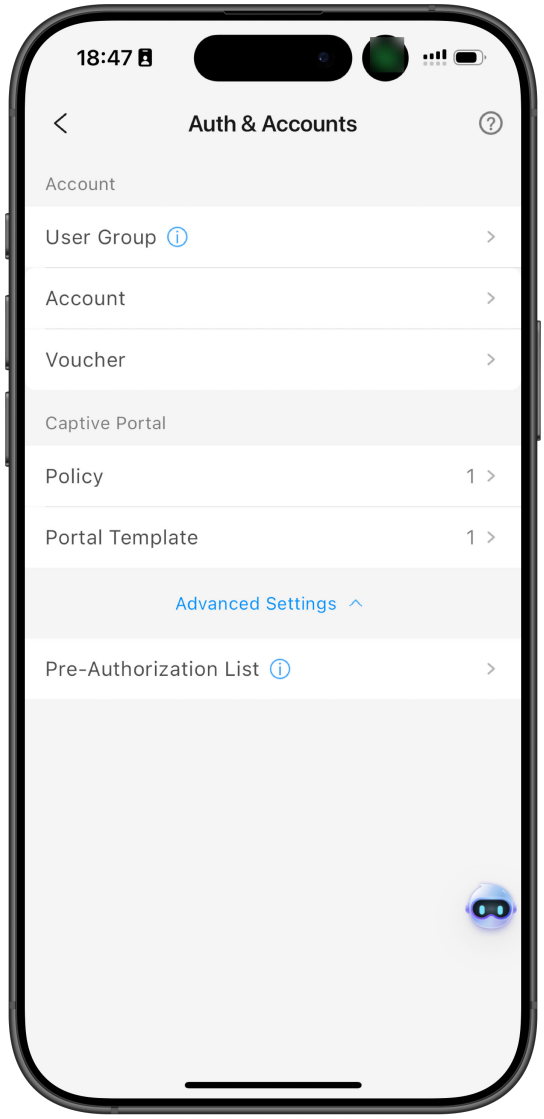


Figure 3-106 Captive Portal

Access User Management

Access User Management Using the Portal

1. Log in to **Hik-Partner Pro Portal**.
2. Go to **Site & Device → Customer Site** .
3. Select and enter a site.
4. On the left pane, select **Captive Portal**.
5. One the top right, select **User Management**.

User Management includes:

- User groups
- Accounts
- Vouchers
- Registration accounts

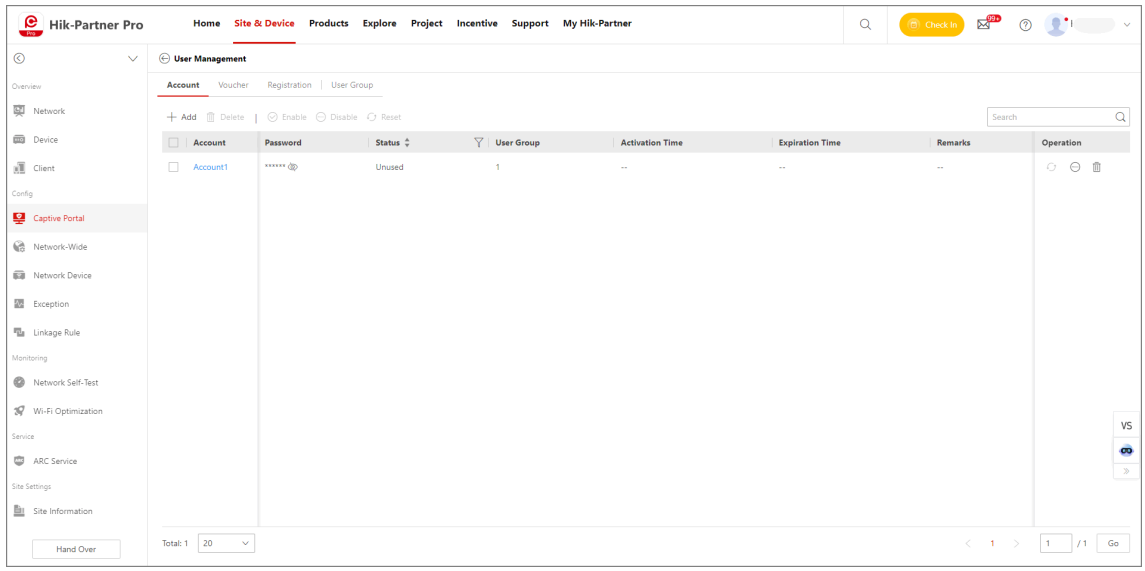
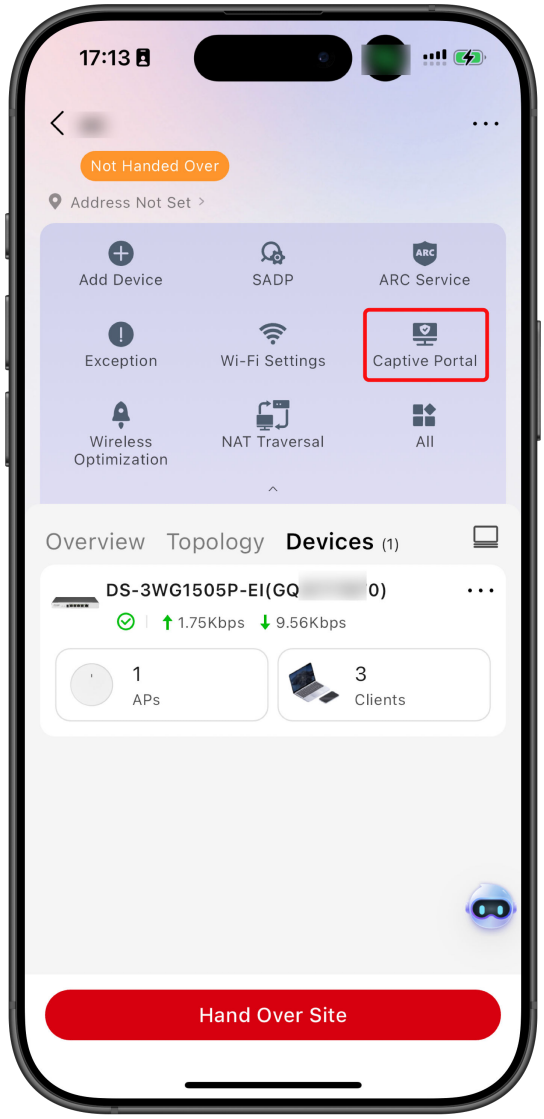


Figure 3-107 User Management

Access User Management Using the Mobile Client

1. Log in to the **Hik-Partner Pro Mobile Client**.
2. Tap **Site**.
3. Select and enter a site.
4. In the tool section, tap **Captive Portal**.


17:13
Not Handed Over
Address Not Set
Add Device
SADP
ARC Service
Exception
Wi-Fi Settings
Captive Portal
Wireless Optimization
NAT Traversal
All
Overview
Topology
Devices (1)
DS-3WG1505P-EI(GQ 0)
1.75Kbps
9.56Kbps
1
APs
3
Clients
Hand Over Site

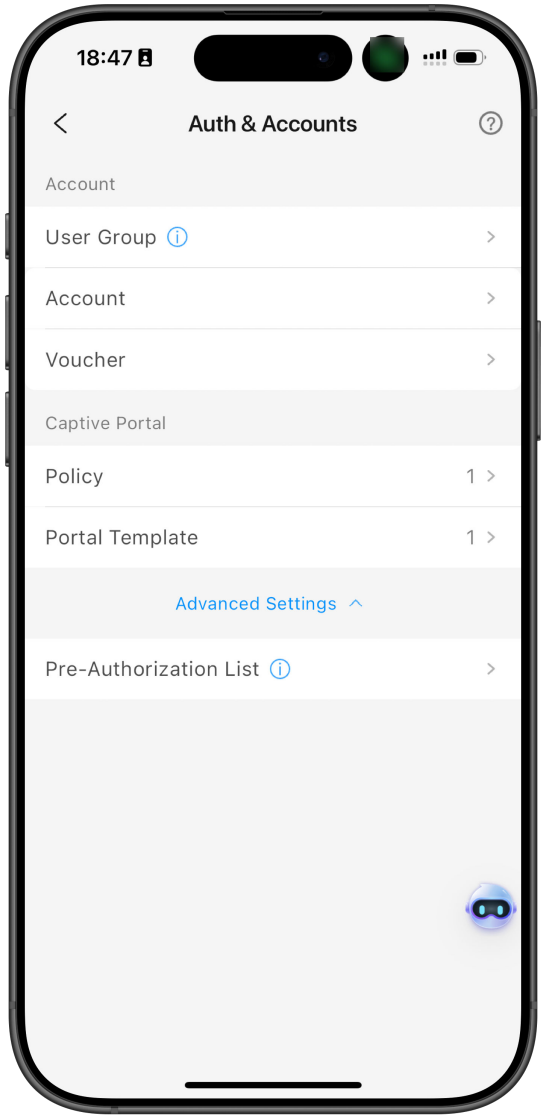


Figure 3-108 Captive Portal

5. You can then tap and access **User Group**, **Account**, or **Voucher**.

Access Client Management

1. Log in to **Hik-Partner Pro Portal**.
2. Go to **Site & Device → Customer Site** .
3. Select and enter a site.
4. On the left pane, select **Client**.

The Client module includes:

- All online clients
- Authenticated wireless clients

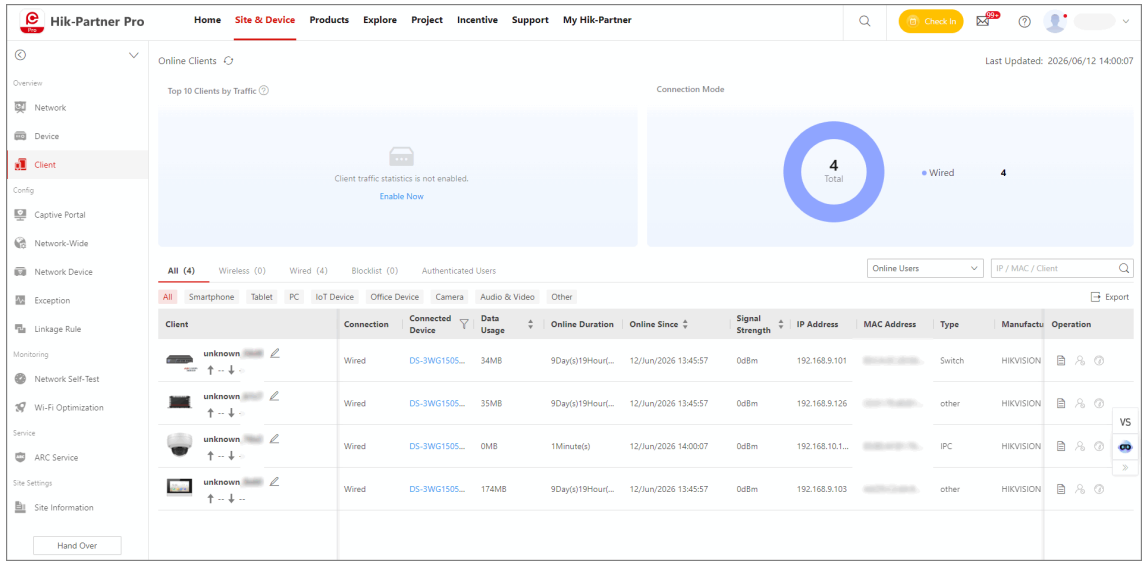


Figure 3-109 Client

Access Pre-Authorization List

1. Log in to **Hik-Partner Pro Portal**.
2. Go to **Site & Device → Customer Site** .
3. Select and enter a site.
4. On the left pane, select **Captive Portal**.
5. Click the **Pre-Authorization List** tab.

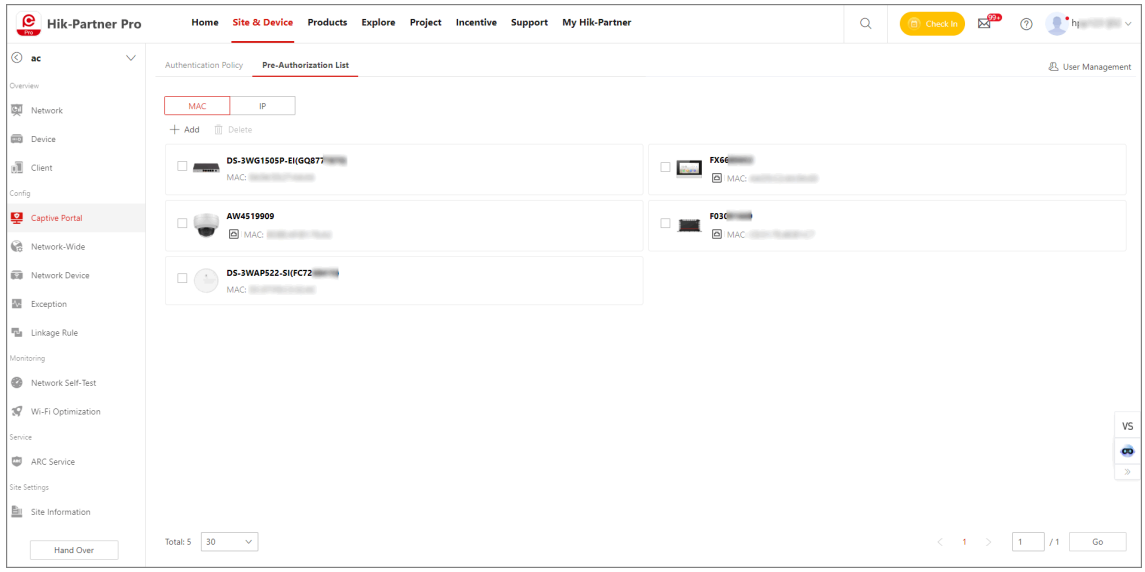


Figure 3-110 Pre-Authorization List

Manage Authentication Policies

Authentication policies define where Captive Portal authentication takes effect and which portal template is used.

Create an Authentication Policy

1. Go to **Captive Portal**.
2. Click **Add Policy**.

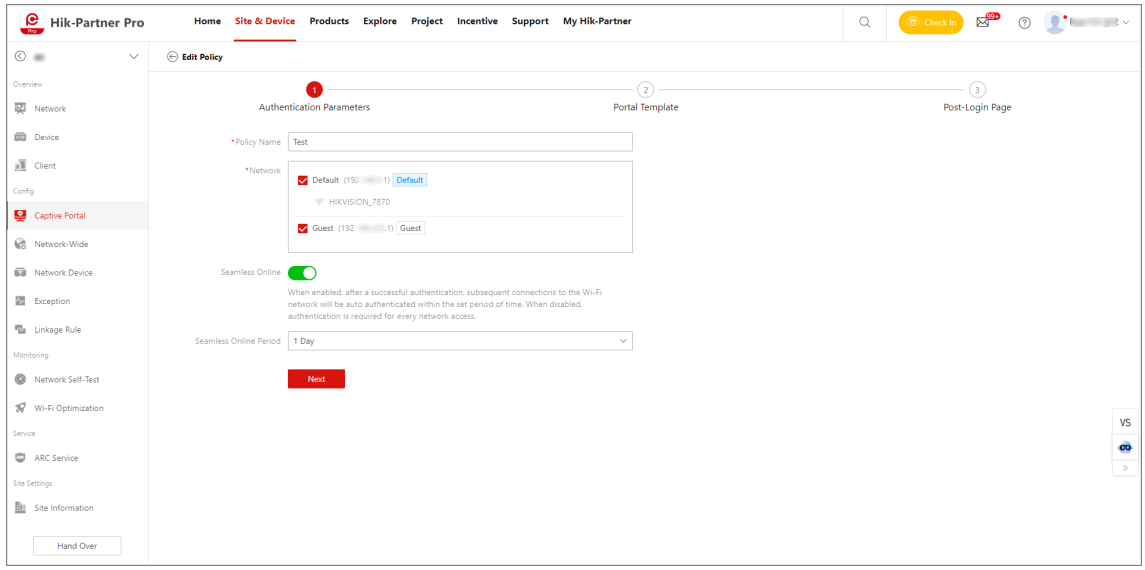


Figure 3-111 Authentication Parameters

3. Set the policy name.
4. Select the target SSID or network.
5. Enable **Seamless Online** and set the **Seamless Online Period**or you can keep it disabled.

Note

When enabled, after a successful authentication, subsequent connections to the Wi-Fi network will be auto authenticated within the set period of time. When disabled, authentication is required for every network access.

6. Click **Next**.
7. Select an existing **Portal Template** or click **Create** to create a template.

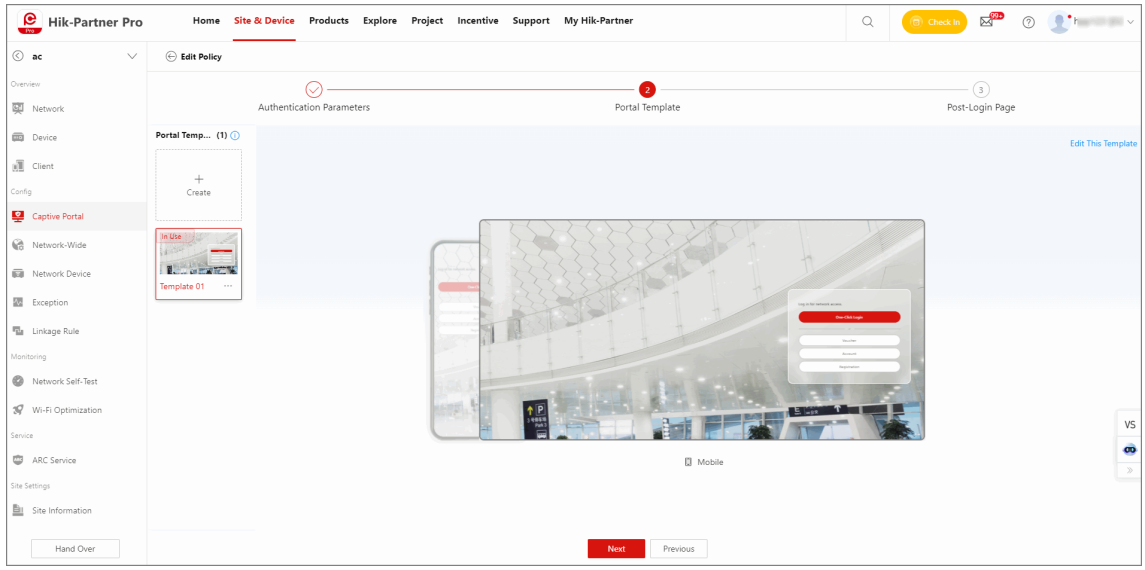


Figure 3-112 Portal Template

8. Confirm the authentication methods enabled in the template.
9. Click **Next**.
10. Set the **Post-Login Page**. Users will be redirected to this page after successful authentication.

Table 3-12 Post-Login Page

Option	Description
Default	A default page prompting successful authentication.
URL	Enter a URL to show to the authenticated users.

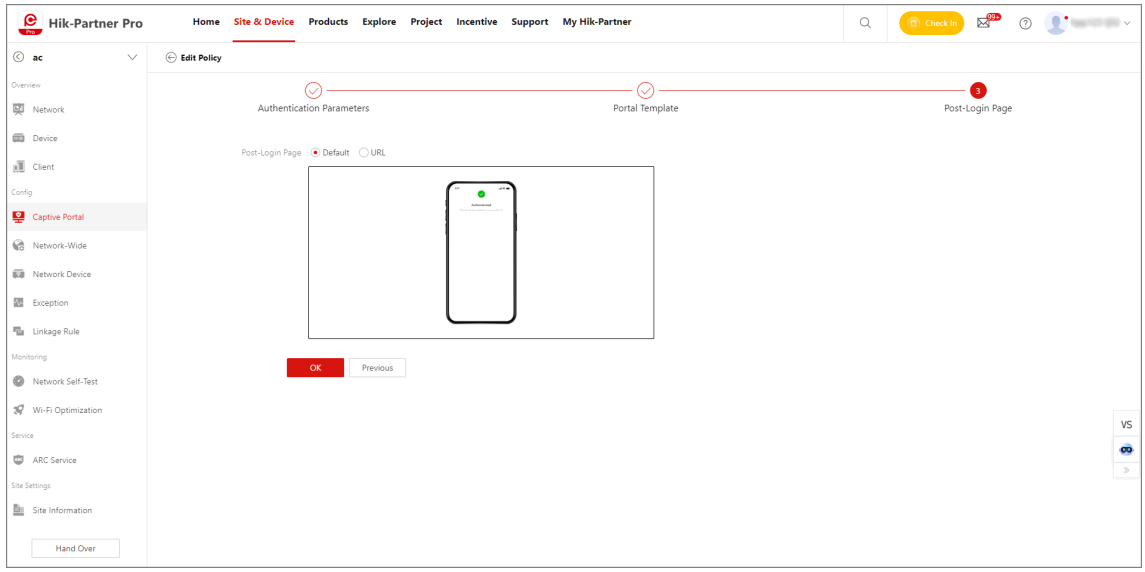


Figure 3-113 Post-Login Page

11. Click **OK** to finish adding the policy.

Note

A maximum of **10 authentication policies** can be created.

Enable or Disable an Authentication Policy

1. Click **Captive Portal** to go to the authentication policy list.
2. Find the target policy.
3. Enable or disable the policy.

Note

When the policy is disabled, clients are no longer authenticated through this policy.

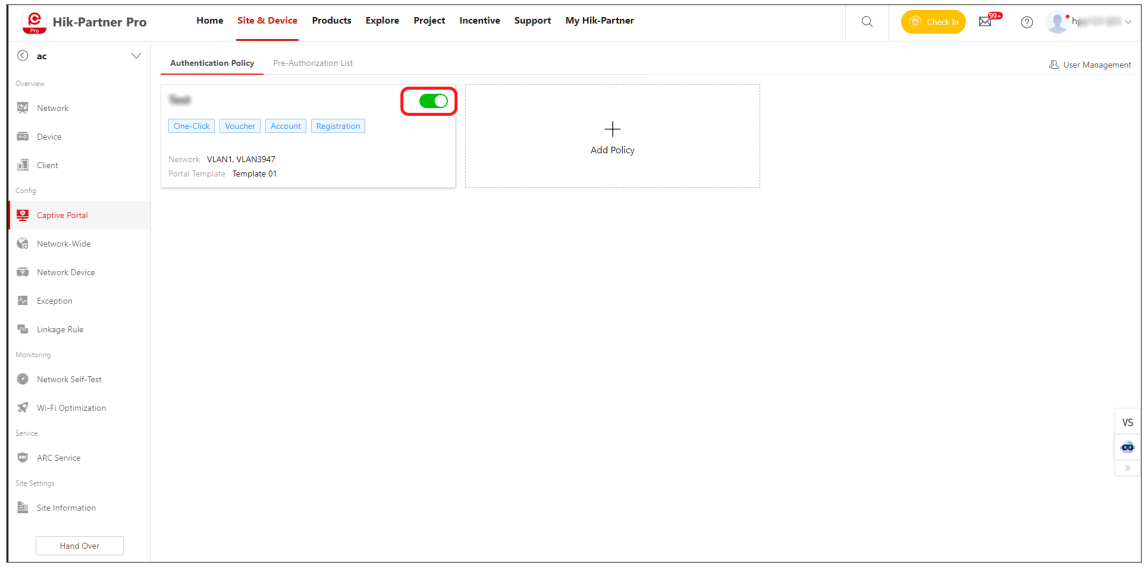


Figure 3-114 Enable/Disable an Authentication Policy

Configure Portal Templates

A portal template is selected or created during authentication policy creation. It defines authentication methods.

The portal template defines:

- Portal page appearance
- Authentication mode settings
- Registration fields, if Registration authentication is enabled
- User group association or user group creation, if required by the selected authentication method

Create a Portal Template During Policy Creation

1. Go to **Captive Portal**.
2. Click **Add Policy**.
3. In the **Portal Template** area, click **Create**.

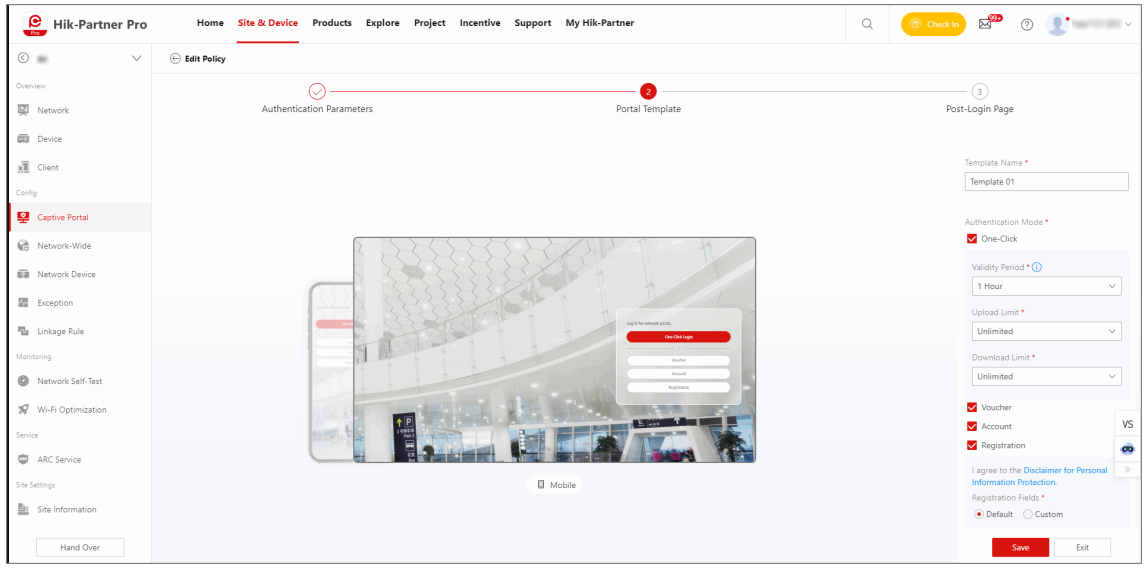
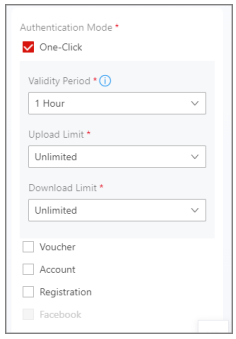
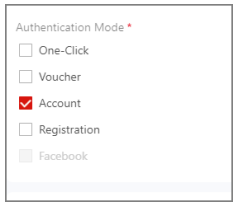
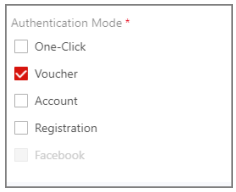
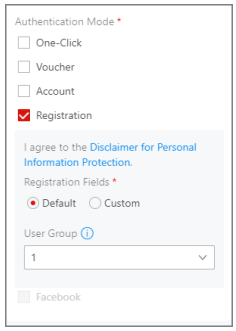


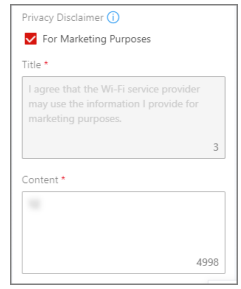
Figure 3-115 Create Portal Template

4. Set the template name.
5. Enable and set one or more authentication modes.

Table 3-13 Supported Authentication Modes and Settings

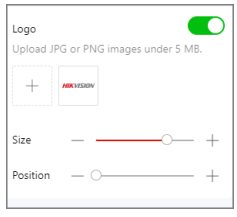
Authentication Mode	Description
One-Click  **Figure 3-116 One Click**	Clients access the Internet by clicking/tapping a login button. **Validity Period** Set the validity period. Time starts after the first successful authentication. Once expired, the user can reconnect to the Wi-Fi to access the Internet again. **Upload Limit & Download Limit** Set specific rate limits. **Unlimited** means no rate limits.
Account	Clients access the Internet with an account and password (which is added in **User Management**).

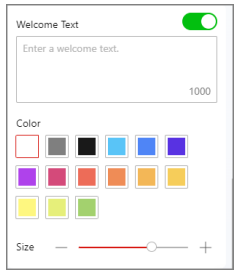
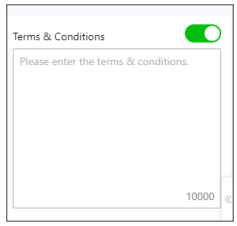
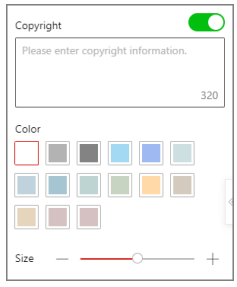
Authentication Mode	Description
 **Figure 3-117 Account**	
Voucher  **Figure 3-118 Voucher**	Clients access the Internet with a voucher code (which is added in **User Management**).
Registration  **Figure 3-119 Registration**	Clients submit registration information before accessing the Internet. a. Upon enabling registration mode, you must read and agree to the**Disclaimer for Personal Information Protection**. b. Configure **Registration Fields**. - Email and phone number can be used as login identifiers (login accounts). - At least one of email or phone number must be provided. - Administrators can configure whether a field is required on the registration and login pages. - Custom fields are supported. c. Select a user group or add a new user group to determine the access duration, rate limits, and other restrictions. d. The Wi-Fi service provider must configure a privacy disclaimer. Select whether collected information will be used for marketing, and set the disclaimer title and content.

Authentication Mode	Description
	 **Figure 3-120 Privacy Disclaimer**
Facebook	Clients log in with a Facebook account. Select a user group or add a new user group to determine the access duration, rate limits, and other restrictions.

6. Configure the portal page appearance.

Table 3-14 Portal Page Appearance

Item	Description
Background  **Figure 3-121 Background**	Upload images (PNG, JPG, GIF) or select from predefined images.
Logo  **Figure 3-122 Logo**	Upload logo (JPG, PNG) or select the predefined logo, and set the size and position.

Item	Description
Welcome Text  **Figure 3-123 Welcome Text**	Enter the welcome text, and set the color and size.
Terms & Conditions  **Figure 3-124 Terms & Conditions**	Enter the terms & conditions.
Copyright  **Figure 3-125 Copyright**	Enter the copyright information and set the text color and size.

7. Click **Save** to finish adding the template.
8. Continue creating the authentication policy.

Manage User Groups

User groups define access rules for accounts, vouchers, registration accounts, and Facebook authentication modes.

User groups can control:

- Total access duration
- Data quota
- Maximum upload rate
- Maximum download rate
- Number of allowed devices

Create a User Group in User Mangement

1. Go to **User Management**.
2. Click **User Group**.
3. Click **Add**.

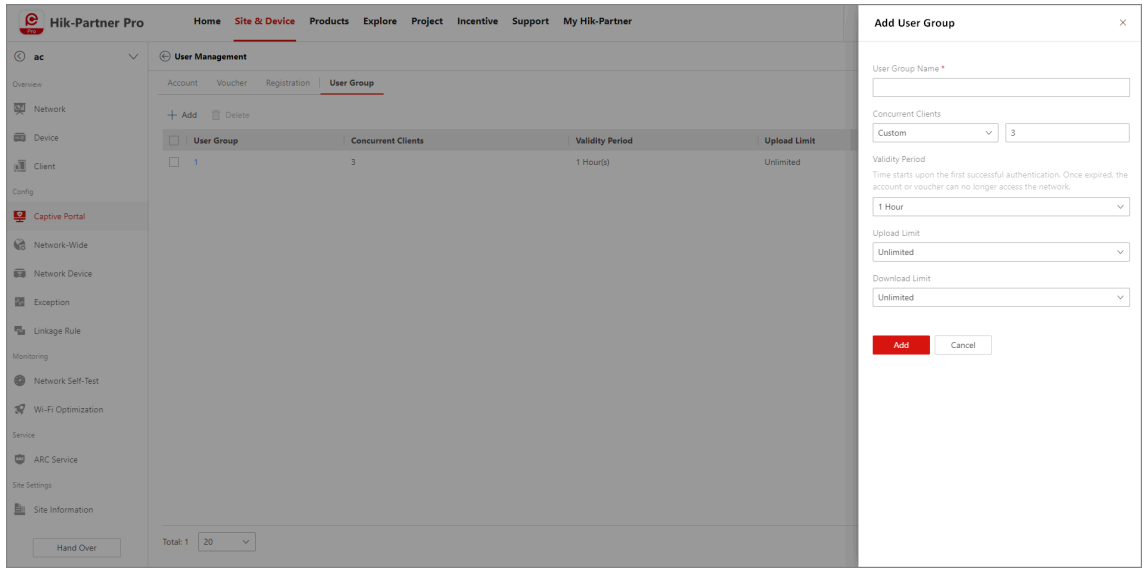


Figure 3-126 Add User Group

4. Enter the user group name.
5. Set the number of allowed concurrent clients.
6. Set the validity period.

Note

Time starts upon the first successful authentication. Once expired, the account or voucher can no longer access the network.

7. Configure upload and download rate limits. Upload and download rate limits support:
   - Unlimited
   - Custom

Table 3-15 Custom Value Range

Item	Range
Maximum upload rate	1–1000 Mbps
Maximum download rate	1–1000 Mbps

Note

Changes to user group duration or rate limits do not affect currently connected clients. Clients must reauthenticate for the new settings to take effect.

8. Click **Add**.

Manage Accounts, Vouchers, and Registration Accounts

Accounts, vouchers, and registration accounts are managed in **User Management**.

Managed Objects

Object	Used By	Created In	User Group Association
Account	Account authentication	User Management	During account creation
Voucher	Voucher authentication	User Management	During voucher creation
Registration account	Registration authentication	Generated after client registration	User group is configured in the portal template

Common Information

The list may display:

- Status
- Associated user group
- Activation time
- Expiration time
- Device count

Status Description

Status	Description
Unused	The account, voucher, or registration account has not been used.
Online	The identity is currently being used by an authenticated client.

Status	Description
Offline	The identity has been used, but no client is currently online.
Expired	The allowed access duration (validity) has expired.
Disabled	The identity is disabled and cannot be used.

Activation and Expiration Logic

Item	Description
Activation time	The time of the first successful authentication.
Expiration time	Activation time plus the access duration configured in the associated user group.
Total access duration (validity period)	Starts from the first successful authentication and continues regardless of whether the client is online or offline.

Note

Once the expiration time is reached, the account, voucher, or registration account can no longer be used for authentication.

Operations on Accounts, Vouchers, and Registration Accounts

The following operations are performed in **User Management**:

- Add
- Enable
- Disable
- Reset
- Delete
- Export

Add Vouchers and Accounts

Add Vouchers

1. Go to **User Management**.
2. Click **Voucher**.
3. Click **Add**.

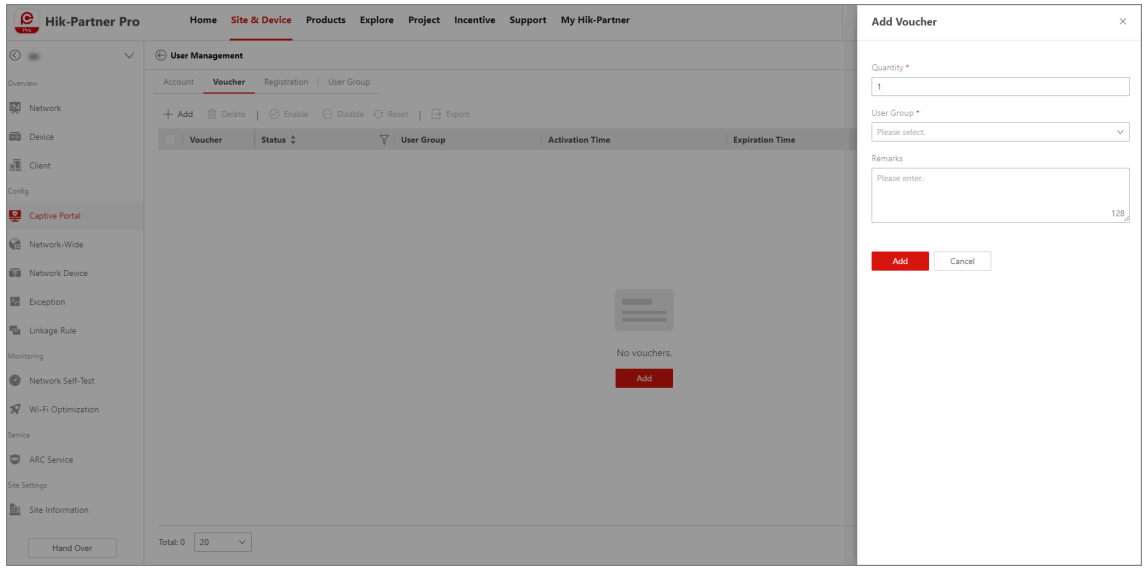


Figure 3-127 Add Voucher

4. Set the quantity of the vouchers to generate. Maximum 500 vouchers can be added.
5. Select a user group or add a new user group to determine the access duration, rate limits, and other restrictions for the vouchers.
6. Set the remarks if needed.
7. Click **Add**. Vouchers will be generated in a batch.

Add Account

1. Go to **User Management**.
2. Click **Account**.
3. Click **Add**.

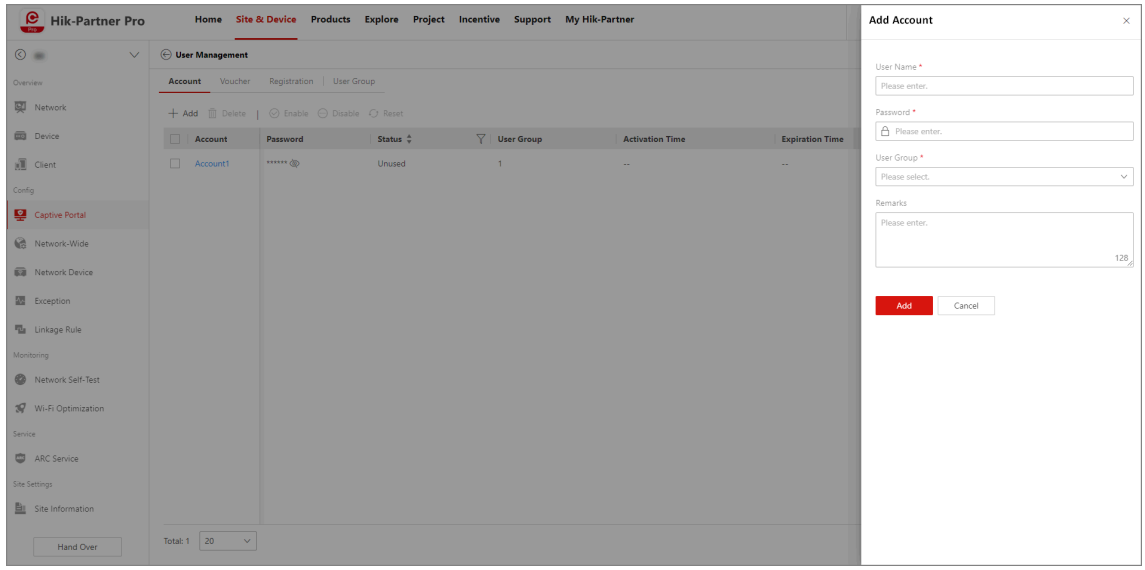


Figure 3-128 Add Account

4. Set the user name and password.
5. Select a user group or add a new user group to determine the access duration, rate limits, and other restrictions for the vouchers.
6. Set the remarks if needed.
7. Click **Add**.

Enable or Disable

1. Go to **User Management**.
2. Open **Account**, **Voucher**, or **Registration**.
3. Select the target items.
4. Click **Enable** or **Disable**.
5. Confirm the operation.

Rules

- Disabled items cannot be used for authentication.
- If an online account, voucher, or registration account is disabled, the corresponding client is disconnected.
- Enabling an item allows it to be used again if it has not expired.

Reset

Resetting restores the access duration (validity period) according to the associated user group.

1. Go to **User Management**.
2. Open **Account**, **Voucher**, or **Registration**.

3. Select the target items.
4. Click **Reset**.
5. Confirm the operation.

Table 3-16 Reset Rules

Status	Reset Supported	Result
Unused	No need to reset	No effect
Online	No	Cannot reset while in use
Offline	Yes	Status returns to Unused
Expired	Yes	Status returns to Unused
Disabled	Yes	Usage data is reset, but the item remains Disabled

After reset:

- Activation time is cleared.
- Expiration time is cleared.
- Usage duration is restored based on the associated user group.

Delete

1. Go to **User Management**.
2. Open **Account**, **Voucher**, or **Registration**.
3. Select the target items.
4. Click **Delete**.
5. Confirm the operation.

Rules

- Deleted items cannot be recovered.
- If an online account, voucher, or registration account is deleted, the corresponding client is disconnected.
- After a registration account is deleted, the visitor can register again if needed.

Export Registration Accounts and Vouchers

Registration account information can be exported for business analysis or marketing purposes, subject to the configured privacy disclaimer. Vouchers can also be exported for business purpose.

1. Go to **User Management**.
2. Open **Voucher** or **Registration**.
3. Click **Export**.
4. Export the voucher or registration account information.

Note

A maximum of **5,000** recent registration account records can be exported.

Manage Clients

Client-related operations are performed in the **Client** module.

Different operations are available in different client lists.

All Clients

The **All** clients list displays all clients detected in the site.

In this list, administrators can perform:

- Block
- Rate limit

Block a Client

Blocking a client prevents it from accessing the network.

1. Go to **Client**.
2. Click the **All** tab.
3. Select the target client.
4. Click in the Operation column.
5. Confirm the operation.

Note

To unblock the clients, please go to the **Block** list.

Configure Rate Limit for a Client

Rate limiting controls the upload or download bandwidth of a client.

1. Go to **Client**.
2. Click the **All** tab.
3. Select the target client.
4. Click .
5. Configure the upload or download rate limit.
6. Save the configuration.

Authenticated Wireless Clients

The **Authenticated Users** list displays wireless clients that have successfully completed Captive Portal authentication.

In this list, administrators can perform:

- Disconnect

Disconnect an Authenticated Wireless Client

Disconnecting a client forces it offline immediately.

1. Go to **Client**.
2. Click the **Authenticated Users** tab.
3. Select one or more online clients.
4. Click **Disconnect**.
5. Click **Confirm**.

After the client is disconnected:

- The client immediately loses Internet access.
- The client is removed from the authenticated wireless client list.
- The client can authenticate again to regain Internet access.

Disconnect Operation Rules

- Disconnecting a client does not block future authentication.
- If seamless authentication is enabled, the client must reauthenticate after being disconnected.

Manage the Pre-Authorization List

The Pre-Authorization List allows specified clients to access the network without completing Captive Portal authentication.

Add a Pre-Authorized Client

1. Go to the **Pre-Authorization List**.
2. Click **Add**.
3. Select between **Select Clients** and **Manually Add**.

   Select Clients

   Select clients in the list, and click **Add**.

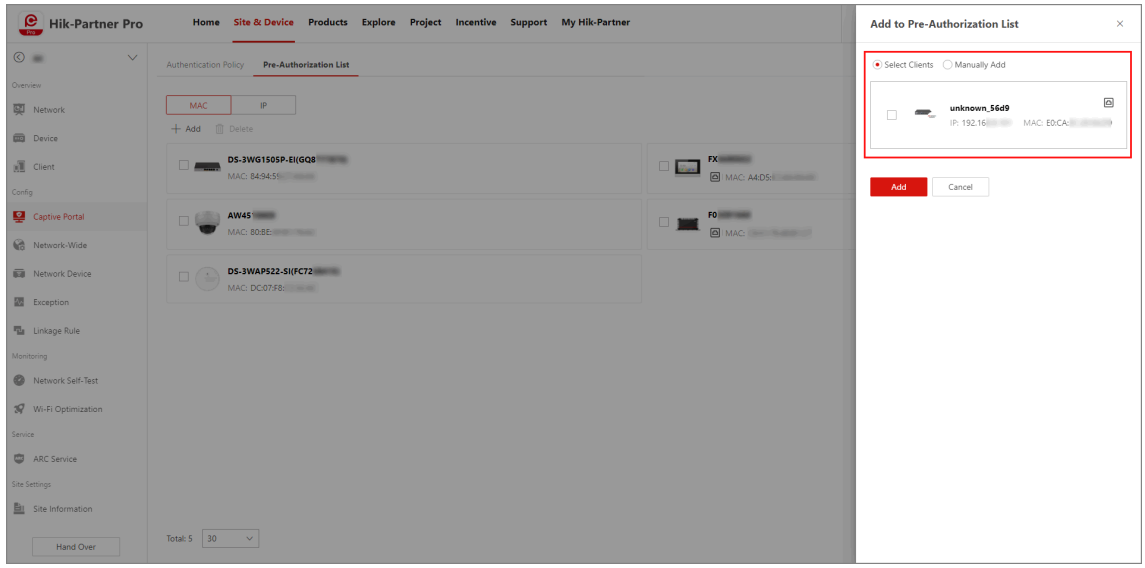


Figure 3-129 Select Clients

Manually Add

Manually enter the IP address, MAC address, or IP range, and click **Add**.

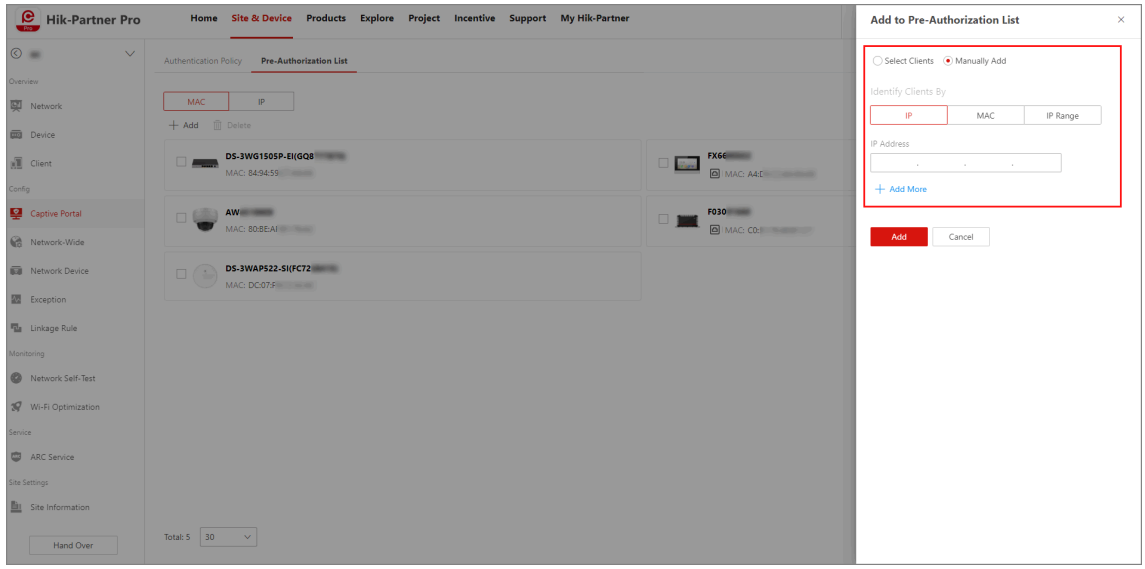


Figure 3-130 Manually Add

The added client can access the network without completing portal authentication.

Remove a Pre-Authorized Client

1. Open the **Pre-Authorization List**.
2. Select the target client.

3. Click **Delete**.
4. Confirm the operation.

After removal, the client must complete Captive Portal authentication to access the network.

Limits and Restrictions

Item	Limit
Authentication policies	Maximum 10
Portal templates	Maximum 10
Voucher generation	Maximum 500
Registration account export	Maximum 5,000 recent records
GIF background size	Maximum 10 MB

Network Overview and Client Management

Feature Overview

Through the **Network** dashboard, users can view the network topology and key metrics such as WAN traffic trends, client connection types, and client traffic rankings. When network issues occur (for example, slow Internet speed or congestion), these insights help users quickly analyze the root cause.

In addition, the **Client** page offers comprehensive client management features, including client lists, client details, traffic statistics, and control actions (such as bandwidth limiting or blocking), enabling fine-grained management of network-connected devices.

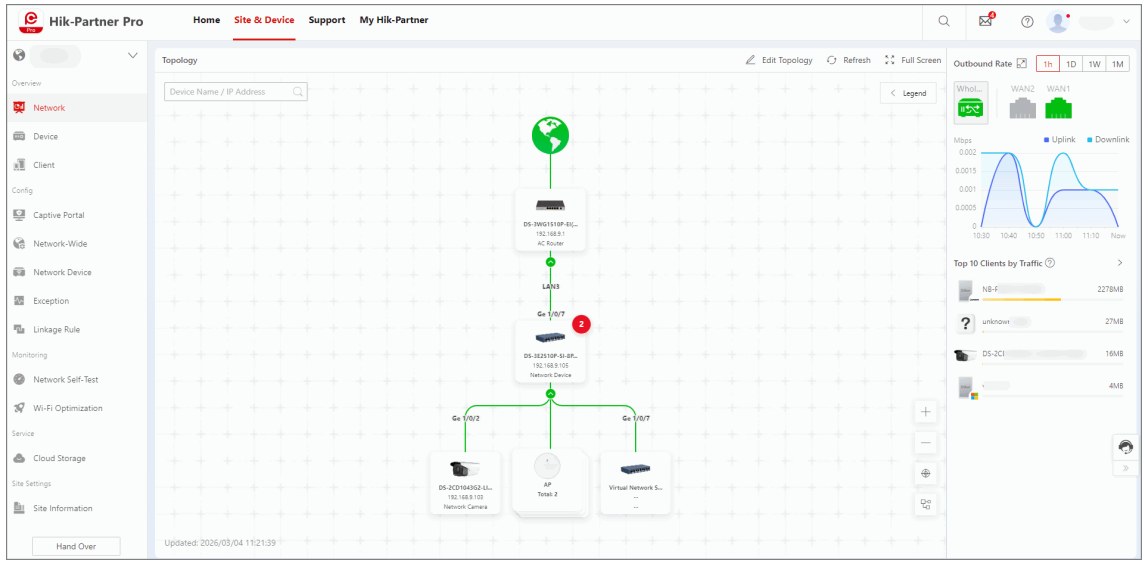


Figure 3-131 Network Overview

Typical Use Cases

When users report slow or unstable network performance, installers can use the **Network** module to troubleshoot:

1. Check WAN traffic trends to determine whether bandwidth is saturated.
2. Identify clients consuming excessive traffic.
3. Analyze client connection types and signal quality.
4. Limit bandwidth or block suspicious clients.

These tools help quickly identify the root cause and take corrective actions.

Prerequisites

Before using this feature, ensure the following conditions are met:

1. The site includes the AC router, cloud APs, routers, or switch devices.

Table 3-17 Supported Device Types

Content	Device Type Required
Topology	Any network device.
Top 10 Clients by Traffic	AC router.
Outbound Rate	AC router.
Client	AC Router

2. The devices support traffic statistics reporting.
3. The user has site and device management permissions.

View WAN Traffic Trends on the Dashboard

WAN traffic trends help monitor the overall bandwidth usage of the site network.

1. Log in to the Hik-Partner Pro Portal.
2. Go to **Site & Device → Customer Site** .
3. Open the target site.
4. Click **Network** on the left.
5. View the WAN traffic trend (**Outbound Rate**) on the top right.

The WAN traffic chart displays:	These metrics help determine:
- Upload Speed (Uplink) - Download Speed (Downlink)	- Whether the network is saturated. - Whether the ISP service may be experiencing issues. - Whether there are high-traffic uploads or downloads.

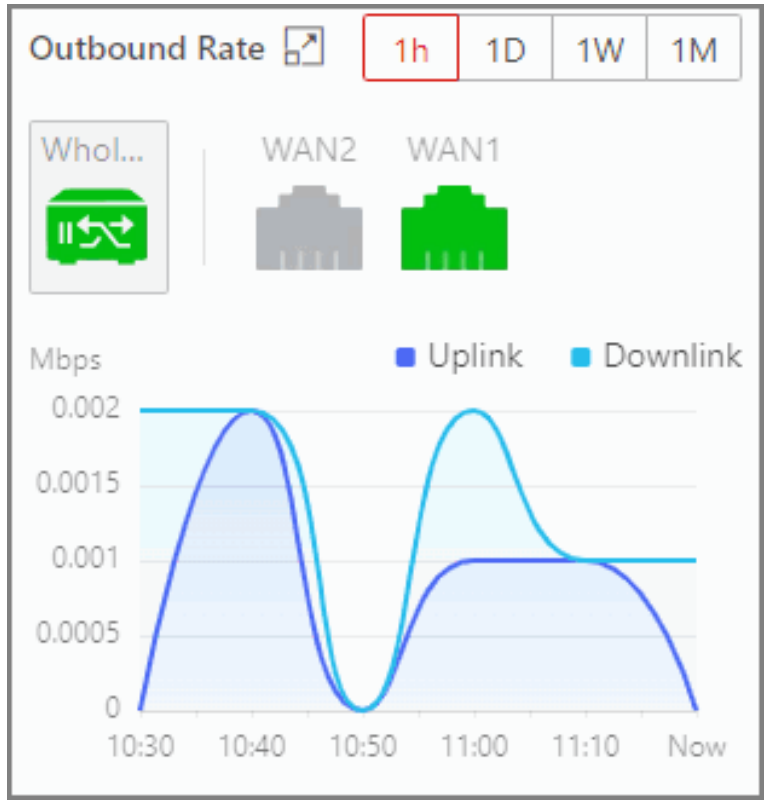


Figure 3-132 WAN Traffic Trend (Outbound Rate)

6. Select different time ranges: **1h**, **1D**, **1W**, or **1M**.
7. If the site has multiple WAN interfaces, you can switch between them or select **Whole Device** to view traffic statistics.

View Client Statistics on the Dashboard

The **Network** dashboard also provides client statistics to analyze device connections and traffic usage.

1. Log in to the Hik-Partner Pro Portal.
2. Go to **Site & Device → Customer Site** .
3. Open the target site.
4. Click **Network** on the left.
5. View the **Top 10 Clients by Traffic** on the top right. The chart displays traffic usages of top 10 clients.

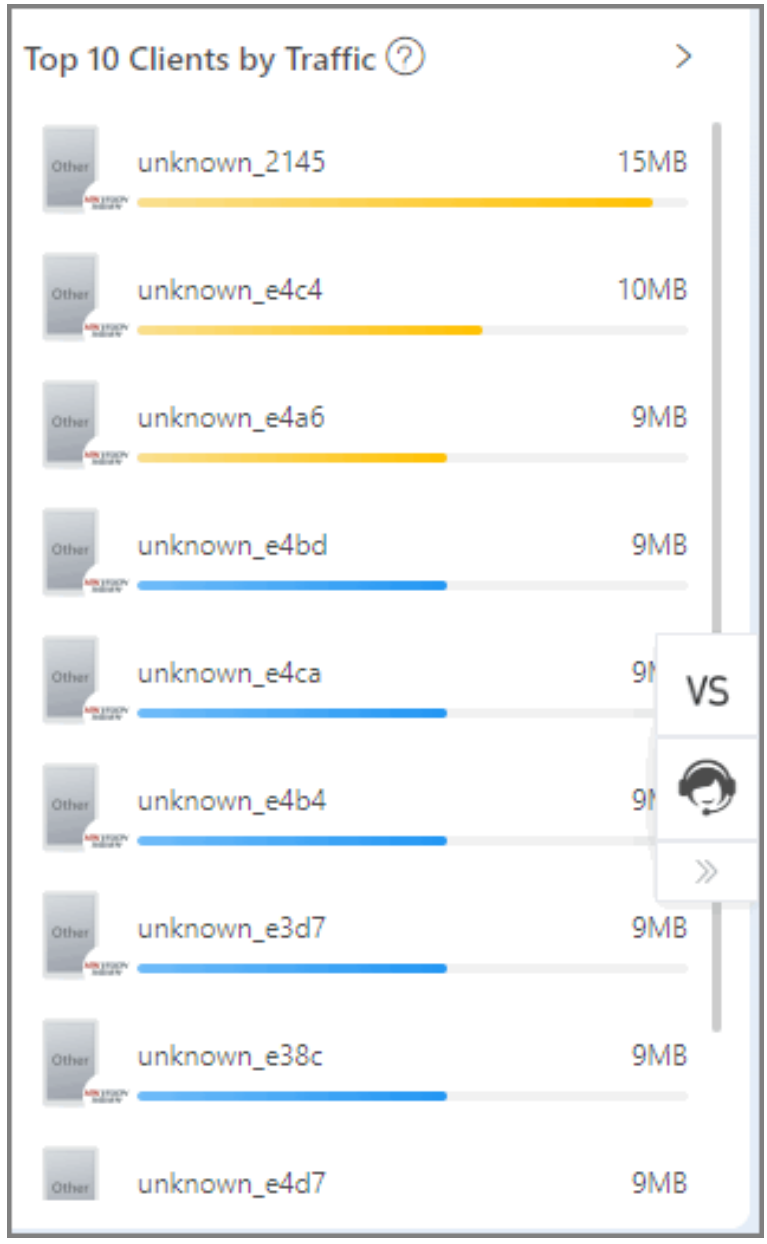


Figure 3-133 Top 10 Clients by Traffic

Client Management

The Portal provides a dedicated client management module for viewing and managing all devices connected to the network.

1. Log in to the Hik-Partner Pro Portal.
2. Go to **Site & Device → Customer Site** .

3. Open the target site.
4. Click **Client** on the left.

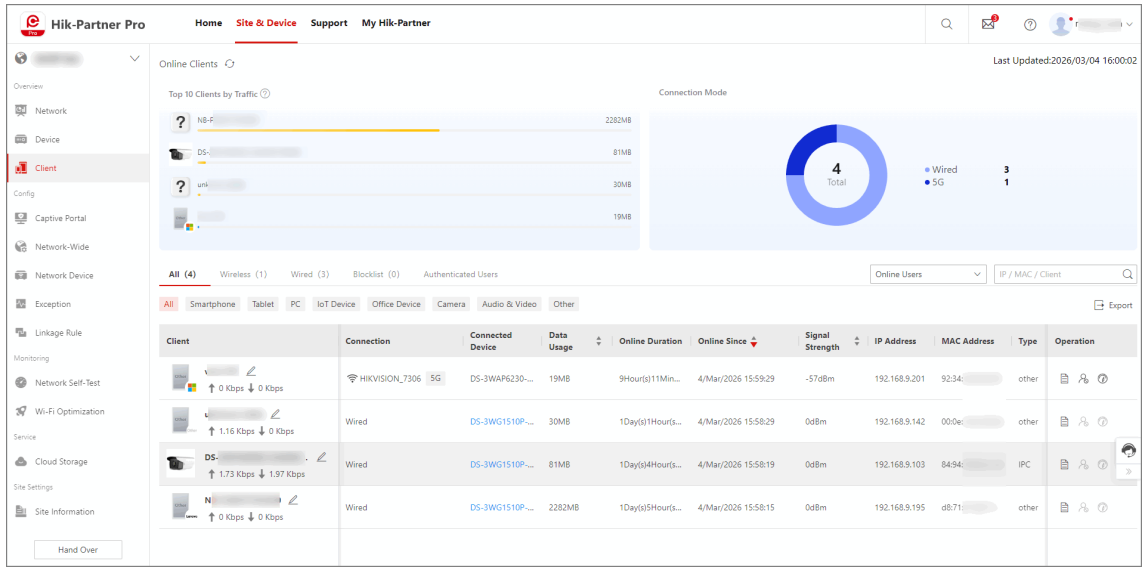
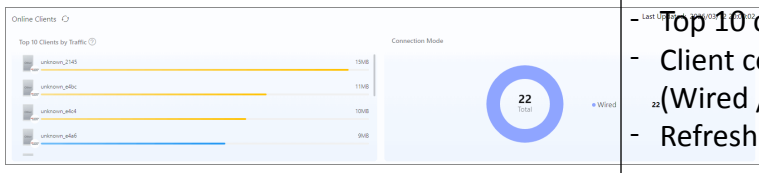
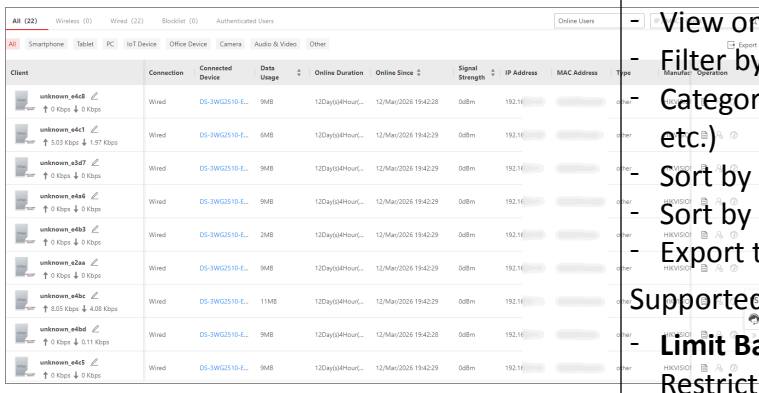
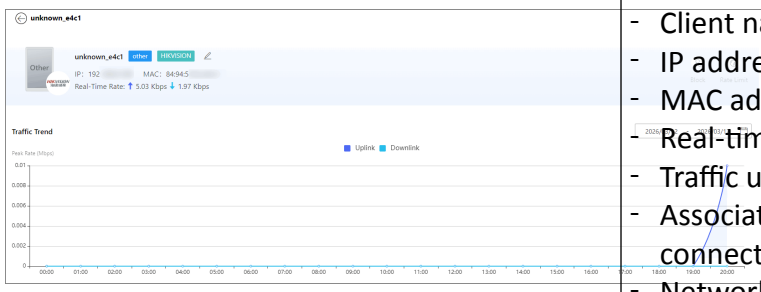


Figure 3-134 Client

Section	Available Data or Features
Charts 	The charts support the following features: - Top 10 clients by traffic usage - Client connection mode distribution (Wired / Wi-Fi 2.4G / Wi-Fi 5G) - Refresh online clients
Client List 	The client list supports the following features: - View online and historical clients - Filter by connection type (wired or wireless) - Categorize by device type (phone, PC, IoT, etc.) - Sort by traffic usage - Sort by signal strength - Export the client list Supported client control actions: - **Limit Bandwidth** Restrict upload or download bandwidth for the client. - **Block Client**

Section	Available Data or Features
	Add the client to the blocklist to prevent network access. - **Edit Client Information** Modify the client name, type, or vendor information. - **Disconnect Authenticated Clients** Under the **Authenticated Users** tab, select the target clients, click **Disconnect**, the disconnected clients will lose Internet access and can authenticate again to regain Internet access.
Client Details  	The client details page displays: - Client name and device type - IP address - MAC address - Real-time upload and download speed - Traffic usage trends - Associated access device (for wireless connection mode) - Network connection path Supported client control actions: - **Limit Bandwidth** Restrict upload or download bandwidth for the client. - **Block Client** Add the client to the blocklist to prevent network access. - **Edit Client Information** Modify the client name, type, or vendor information.

Network Topology

If you have added network devices AC, AP and switches to a site and connected devices to the network switch, you can view these devices' network topology. A network topology displays network links between devices and shows the link exceptions and abnormal devices, allowing you to locate exception source and troubleshoot faults in a visualized way.

Note

Make sure you have configuration permission for the network switch, otherwise network topology is unavailable. For details about applying for the permission, see .

Tap a site on the site list to enter the site page, and then tap **Topology** to view the network topology. You can perform the following operations on the network topology.

There are three display modes of the topology (see the following images). You can tap to switch the mode.

- Mode 1: Devices at the same level are all stacked in a pile.
- Mode 2: (Default Mode) Devices of the same type at the same level are stacked in a pile.
- Mode 3: No devices are stacked.

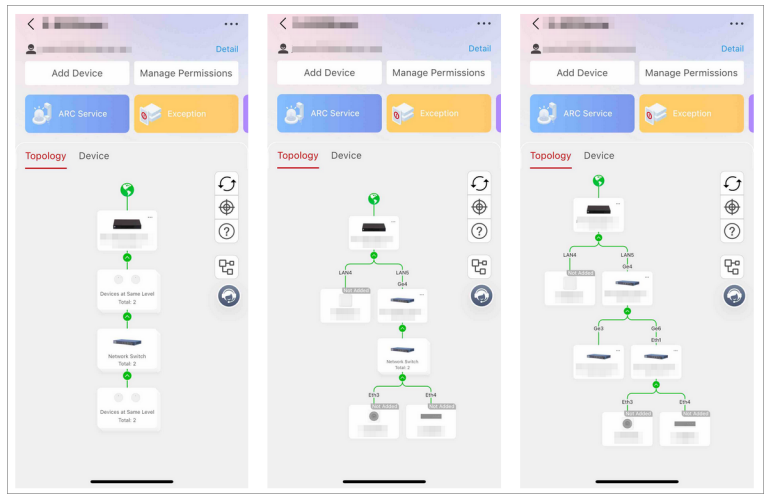


Figure 3-135 Topology Mode 1, 2 and 3

Table 3-18 Available Operations

Operation	Description
Set Root Node	If you want to change the root node, you can select a device and tap ... → **Set Root Node** . **Note** You can set a third-party switch to the root node.
View Network Device Details	You can tap an AC device on the topology to view its details, including the number of AP devices and clients, and the WAN port status.

Operation	Description
View Details of Other Device	Tap a device to view its details, such as device model and network status. **Note** • Make sure you have the configuration permission for the device, otherwise you need to apply for the permission first. • You cannot view details of a virtual network switch. • If the device is not added to the same site with the network switch, you cannot view its details.
View More Information	Tap ⓘ to view the connection type, connection status, and device status.

Network Maintenance Tools

Feature Overview

To help installers perform network maintenance more efficiently, Hik-Partner Pro offers the **Monitoring** module on the site page.
This module centralizes commonly used network maintenance tools, allowing installers to quickly perform diagnostics and wireless optimization after project deployment.
The **Monitoring** module provides the following functions:

- **Network Self-Test**: Identifies network issues.
- **Wi-Fi Optimization**: Improves wireless network performance.

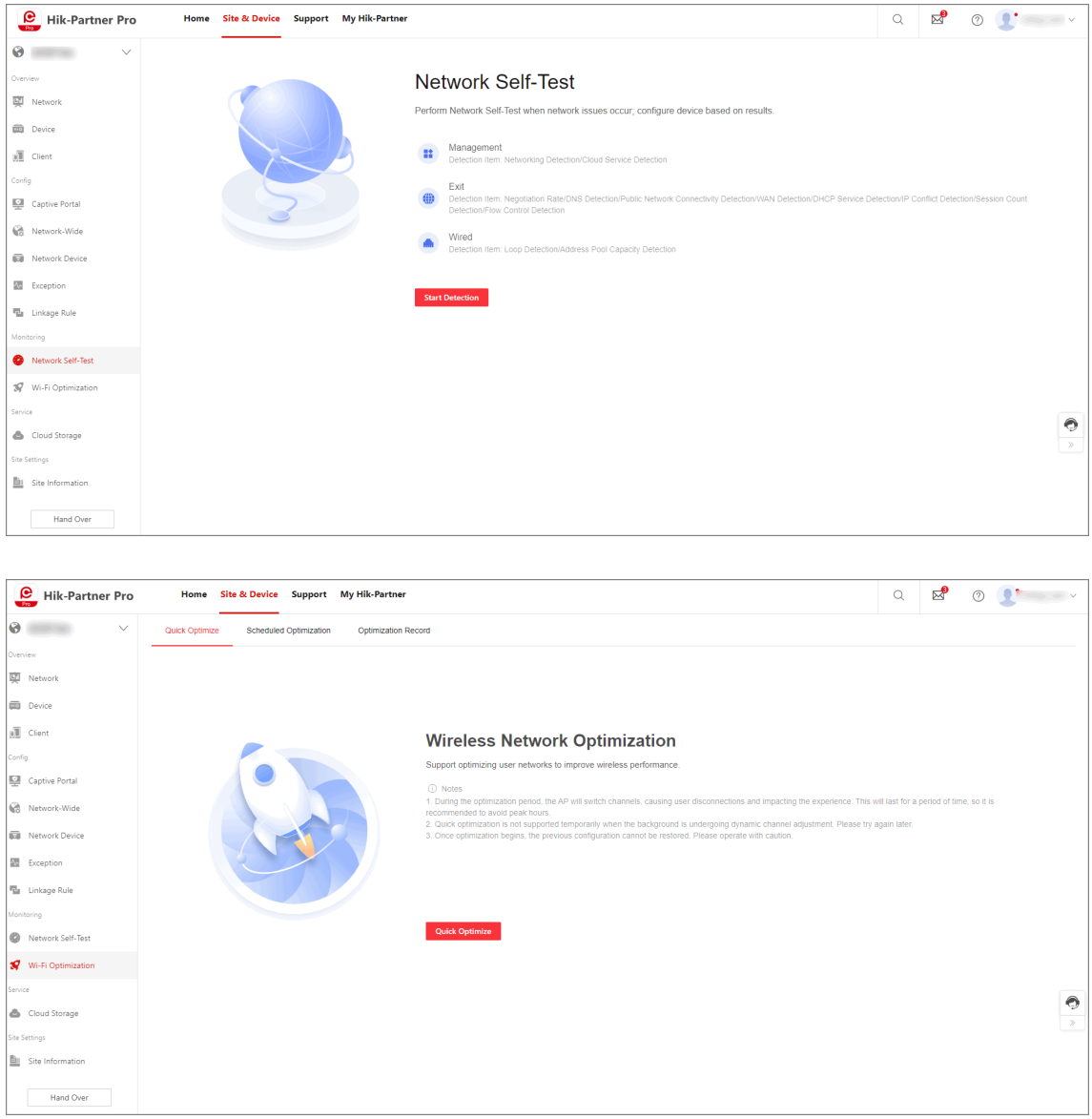


Figure 3-136 Monitoring

Typical Use Cases

After project deployment, installers may need to perform network maintenance or optimization tasks, such as:

- Troubleshooting network connectivity issues
- Diagnosing device status
- Optimizing wireless coverage and roaming performance
- Improving overall network stability

The Operations module provides quick access to the relevant tools for these tasks.

Prerequisites

Before using the **Monitoring** module, ensure the following conditions are met:

- The site includes an **AC router or cloud AP devices**.
- The user has the site and device management permissions.

Perform Network Self-Test

The **Network Self-Test** feature helps check device network status and identify potential network issues.

1. Log in to the Hik-Partner Pro Portal.
2. Go to **Site & Device → Customer Site** .
3. Open the target site.
4. Click **Network Self-Test** on the left.
5. Click **Start Detection** and wait for the test to complete.
   You can perform:
   - Checking network connectivity.
   - Reviewing network configuration.
   - Troubleshooting network issues.

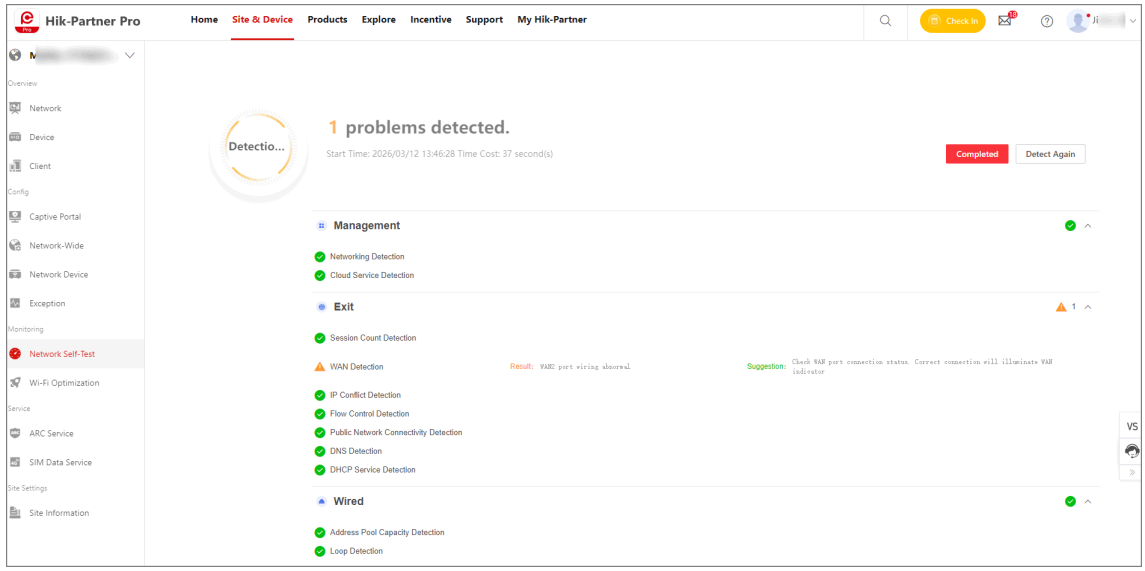


Figure 3-137 Test Result Example

Perform Wi-Fi Optimization

The **Wi-Fi Optimization** feature helps improve wireless network performance.

1. Log in to the Hik-Partner Pro Portal.
2. Go to **Site & Device → Customer Site** .
3. Open the target site.
4. Click **Wi-Fi Optimization** on the left.

Quick Optimize

The device will immediately perform optimization operations.
Under **Quick Optimize**, click **Quick Optimize** to start quick optimization.

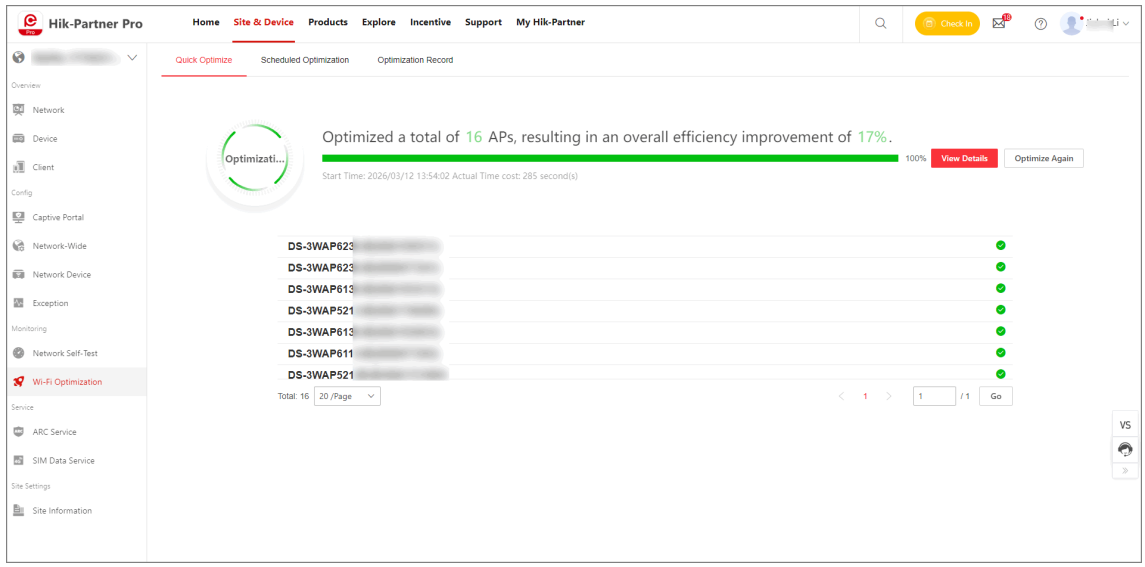


Figure 3-138 Quick Optimization Completed

Scheduled Optimization

The device will perform optimization operations at the specified time and automatically adjust RF parameters.

1. Under **Scheduled Optimization**, turn on **Enable**.
2. Select one day of a week and set the time of a day.
3. Click **Save**.

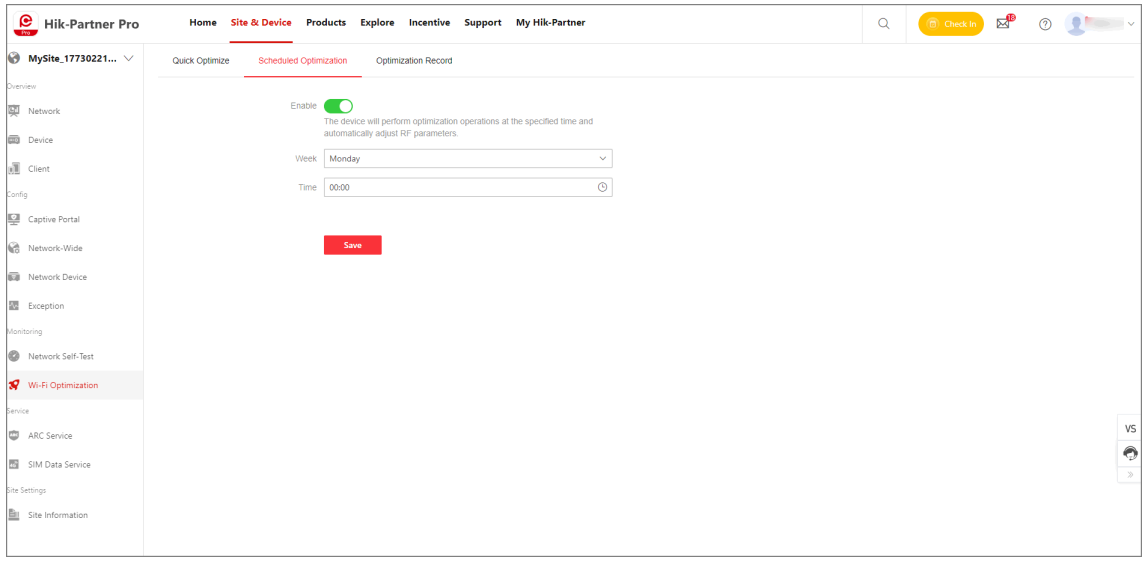
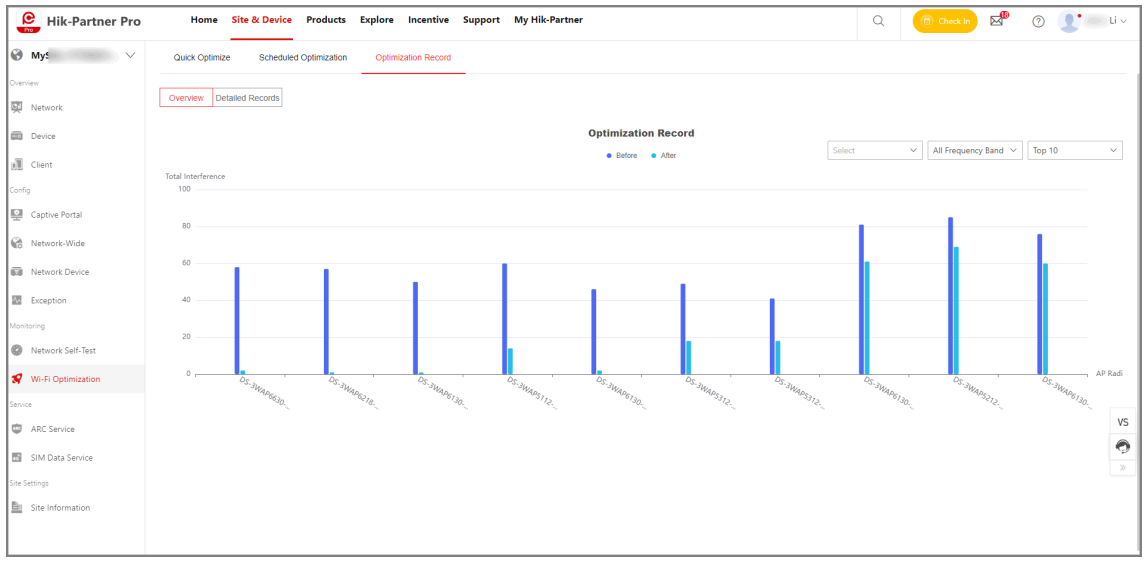


Figure 3-139 Scheduled Optimization

Optimization Record

Under the **Optimization Record**, you can view key metrics before and after the optimization both on the **Overview** and **Detailed Record** page.



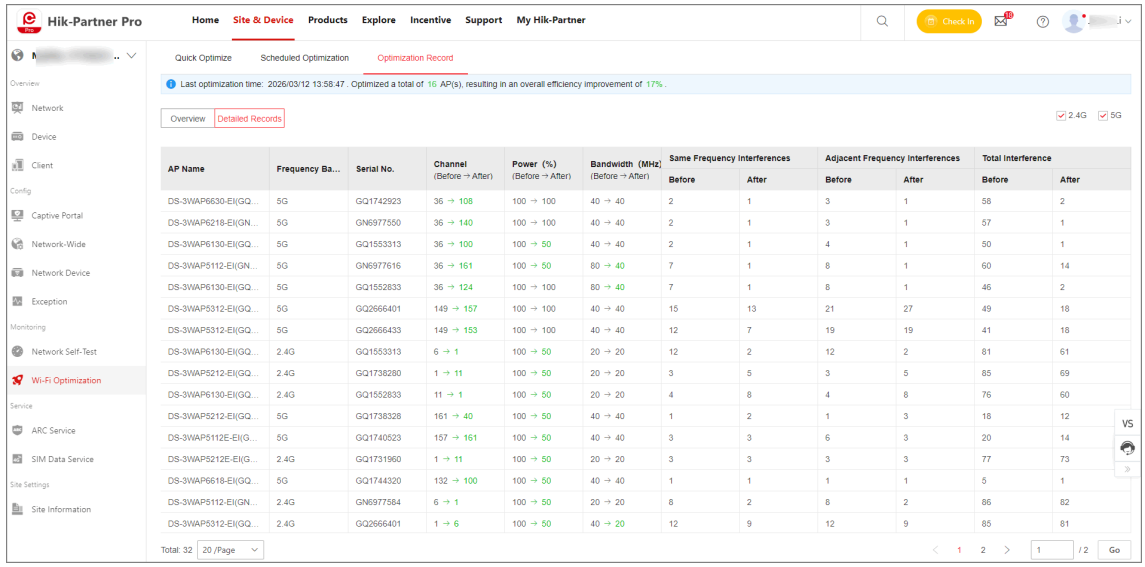


Figure 3-140 Optimization Record

3.3.4 Healthcare Radars

Introduction

After activating and adding radars to a personal site via QR code / serial number / IP / Domain / LAN (SADP Tool), you can remotely configure the radars, check the health status, and link cameras to radars.

Diagram

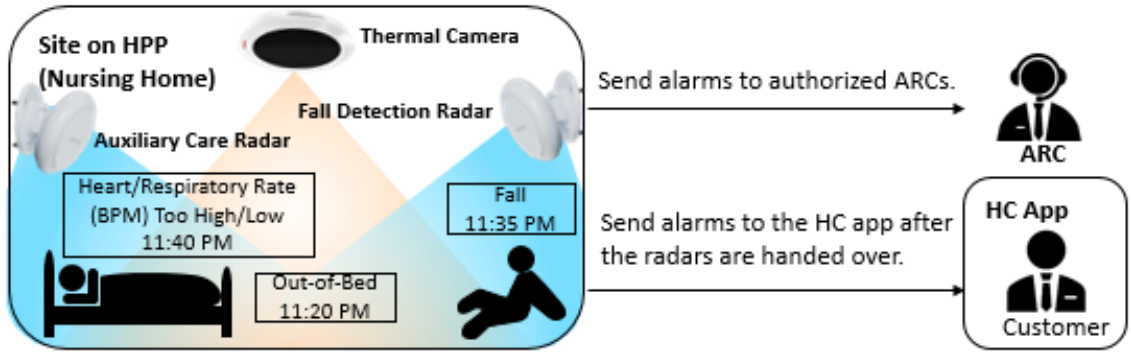


Diagram Details

Table 3-19 Device Operations

Device	Description	Operation
Thermal Camera	Provides presence detection, thermal picture and playback of the incident for double-checking, and thermal live view	-
Auxiliary Care Radar	Provides vital signs monitoring: Out-of-Bed Alarm, Heart Rate (BPM) Too High/Low Alarm, Respiratory Rate (BPM) Too High/Low Alarm.	• Remote Configuration (Wi-Fi, indicator control, alarm parameters, etc.). See the following picture. • ***Link a Camera to a Radar***
Fall Detection Radar	Provides fall detection: Fall Alarm.	• Remote Configuration (Wi-Fi, indicator control, alarm parameters, etc.). See the following picture. • ***Link a Camera to a Radar***

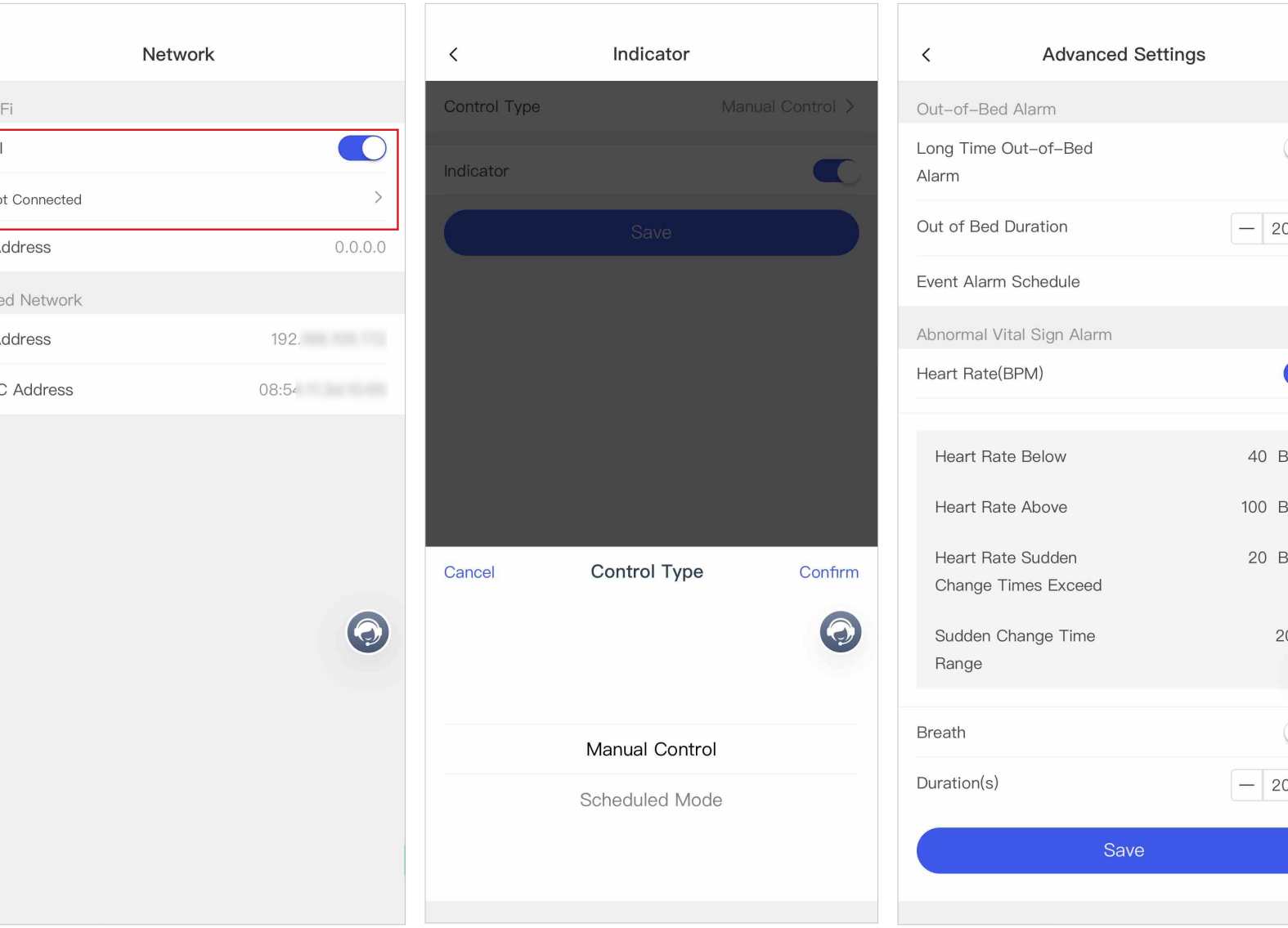


Figure 3-141 Remote Configuration of the Auxiliary Care Radar

Link a Camera to a Radar

To record a video or capture a picture so that your customer and the ARC can double check the incident, or to detect the care receiver's presence, you can link a camera to the radar via the Mobile Client.

Before You Start

Make sure the camera and the radar are added to the same site.

Steps

1. Tap **Site**, and tap the site of the radar.

2. Tap the radar and enter its details page.
3. Tap **Camera Linkage**.
4. Select a camera and tap **Link**.

Note

Only one camera can be linked to a radar.

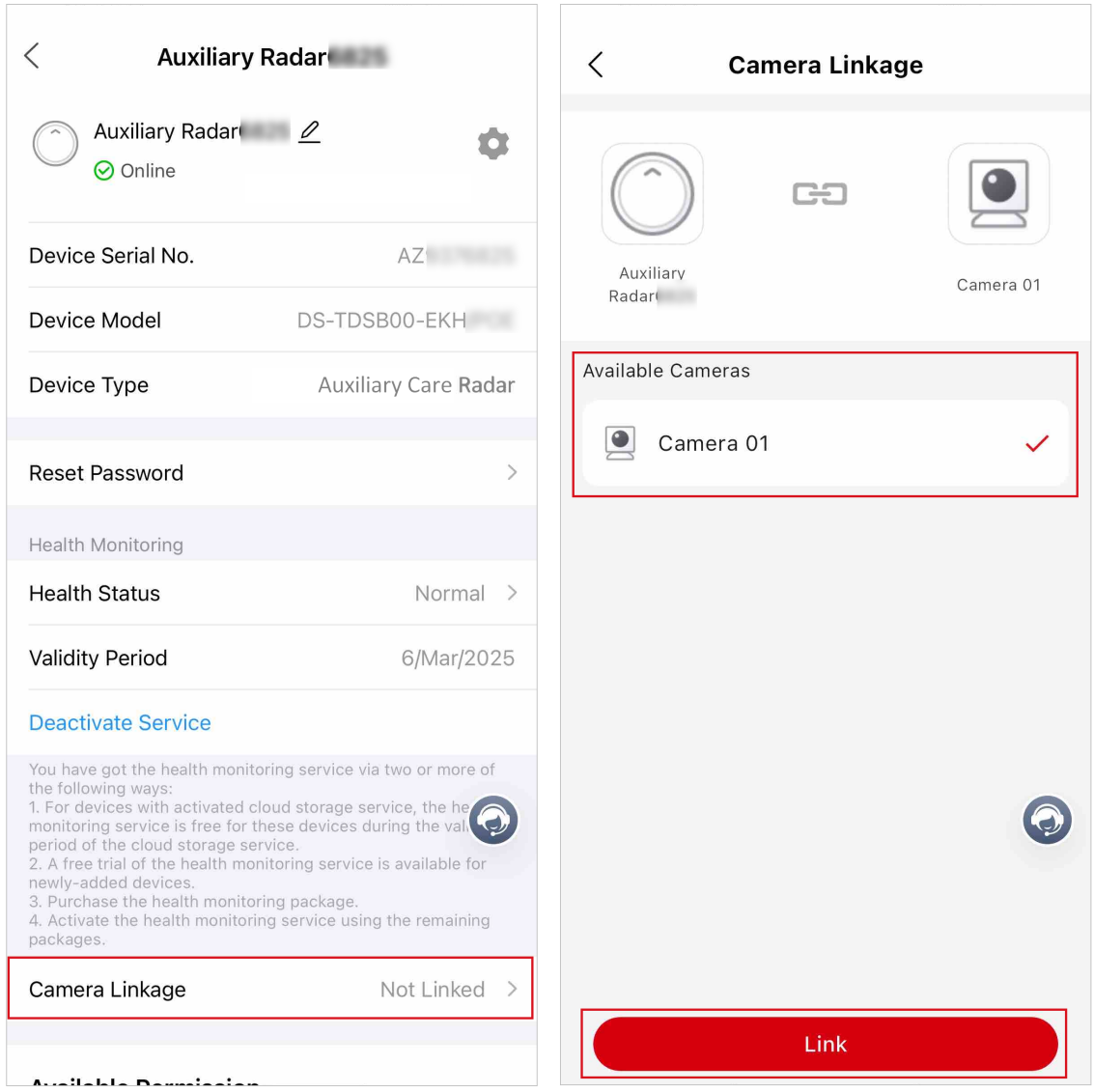


Figure 3-142 Link a Camera to a Radar

3.4 Deliver to Customers & Maintain Customer Relationships

Light CRM Tool: What is A Site?

A site can be regarded as an area or location with an actual time zone and address. There are two types of sites available to different user types and scenarios on Hik-Partner Pro, including personal site and team site. You can add sites to conveniently manage devices for your customers, and after you complete installing and setting up devices on a site, you can hand over the site and devices to your customer.

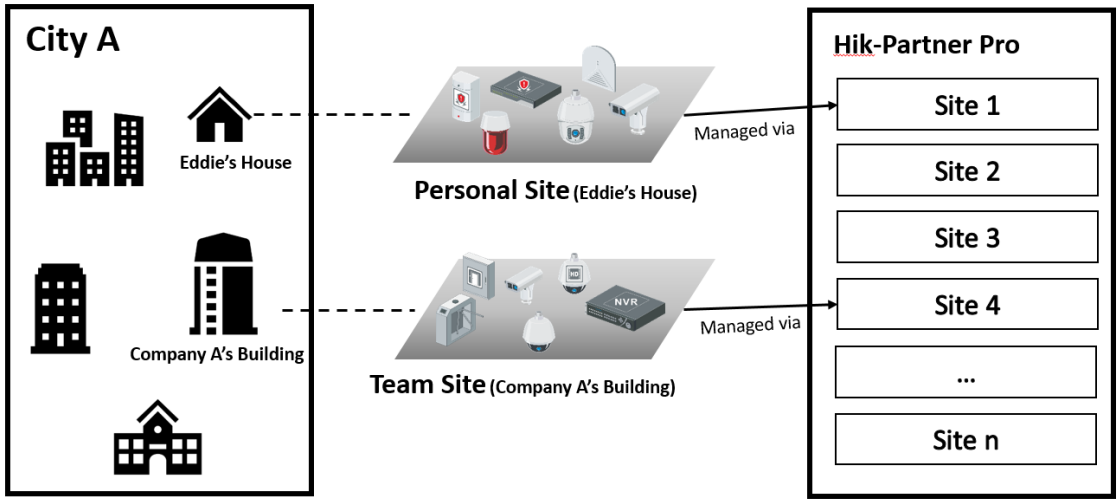


Figure 3-143 Relationship Between "Real Customer Site" and "Site on Hik-Partner Pro"

Light CRM Tool: Sites in Different Status

There are different status for the sites. And according to site status, the Installer Admin and Installers with related permissions can perform different operations.

Not Handed Over

The site is newly added, and you have not handed over the site to the customer.

Not Registered

The handover has been sent to a customer who has not registered a Hik-Connect account.

To Be Accepted

The handover application has been sent but has not been accepted by the customer who has registered a Hik-Connect account.

Handed Over, Not Authorized

The site is handed over to the customer by transferring, but the installer is not authorized to manage the site.

Authorized and Monitoring

The site is handed over by transferring and the Installer gets the site authorization from the customer.

Shared

The site is handed over to customers by sharing.

Disbanded

The site is disbanded by HikCentral Connect.

Table 3-20 Supported Operations for Sites in Different Status

Supported Operations	Status: Not Handed Over	Status: To Be Accepted Not Registered	Status: Handed Over, Not Authorized	Status: Authorized and Monitoring	Status: Shared	Status: Disbanded
Search Site	√	√	√	√	√	√
Assign Site	√	√	√	√	√	×
Hand Over by Transferring	√	×	×	×	×	×
Hand Over by Sharing	√	×	×	×	×	×
Manage Device	√	√	×	√	√	×
Edit Site	√	√	×	√	√	×
Delete Site	√	√	√	√	√	√
Apply for Site Authorization	×	×	√	×	×	×
Apply for Device Permissions	×	×	√	√	√	×
Site Collaboration	√	×	×	√	×	×
Batch Share Devices	×	×	×	×	√	×
Move to Group	√	√	√	√	√	×

Maintain Customer Loyalty: Co-Branding

Refer to ***Co-Branding: Maintain Customer Loyalty and Increase Your Brand Visibility*** .

3.4.1 Add/Edit Sites to Keep Track of Customer Information

Add Personal and Team Sites

Personal site is for individual users and applicable to households and independent stores, while team site is for enterprise users and applicable to scenes where multi-user management is required such as chain stores, offices, and communities.
The following figures show the entries of adding sites on the Portal and the Mobile Client.

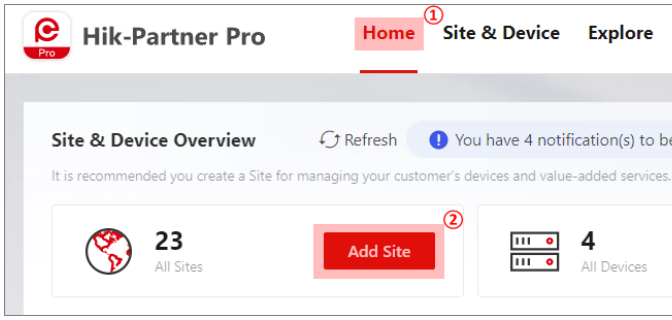


Figure 3-144 The Entry 1 of Adding Sites on th Portal

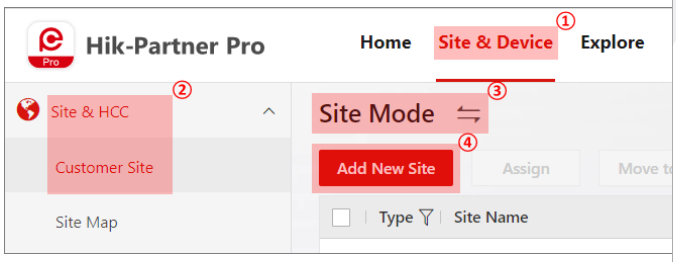


Figure 3-145 The Entry 2 of Adding Sites on th Portal

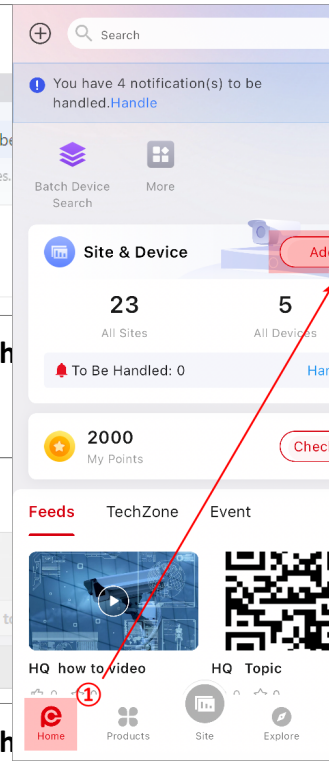


Figure 3-146 The Entry 1 of Adding Sites on the Mobile Client

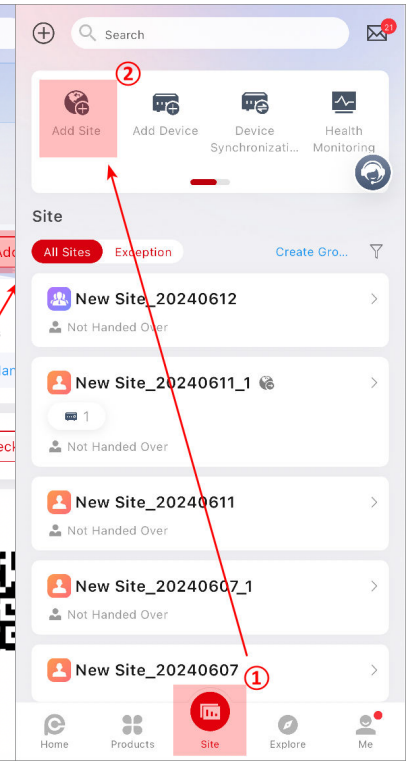


Figure 3-147 The Entry 2 of Adding Sites on the Mobile Client

On the adding site page,

1. Set an unique site name and select the time zone where devices locate.
2. (Optional) Enable **Sync Time & Time Zone to Device** to synchronize the time and time zone of the site to devices installed to the site.

3. (Optional) Set more site information including scene (which helps installers to make appropriate installation plans), site address on the GIS map, city, and state/province/region; move the personal site to a group; or enter the customer information as a remark after you unfold the hidden region.
4. Select **Personal** or **Team** as the site type, (optional) select one or more services to activate for the team site, and then finish adding a site.

Related Topics

- ***Install Devices***
- ***How to Hand Over Site & Devices to Your Customer***
- ***Collaborate with an ISP/MSP on Site for Device Installation or Maintenance***

3.4.2 How to Hand Over Site & Devices to Your Customer

After the installation company completed the device installation on a site, you can hand over the site together with devices to a customer by two methods, that are transferring and sharing. Both the personal site and team site support being handed over by transferring, and after handing over, you can also apply for specified permissions for further device maintenance, but the sharing method is only supported by the personal site.

Typical Transferred and Tenant (Shared) Site Scenarios

Transferred Site Scenario (Where You Hand Over by Transferring)

A typical transferred site scenario is where the devices are owned by customers, and the installer provides the device installation and maintenance service for the customers. The devices will be available to the installer only if the customer grants the installer the corresponding device permissions.

The following diagram shows a typical scenario related to device handover (by transferring) and authorization, as well as the overall process.

In the diagram, HPP represents Hik-Partner Pro and HC represents Hik-Connect.

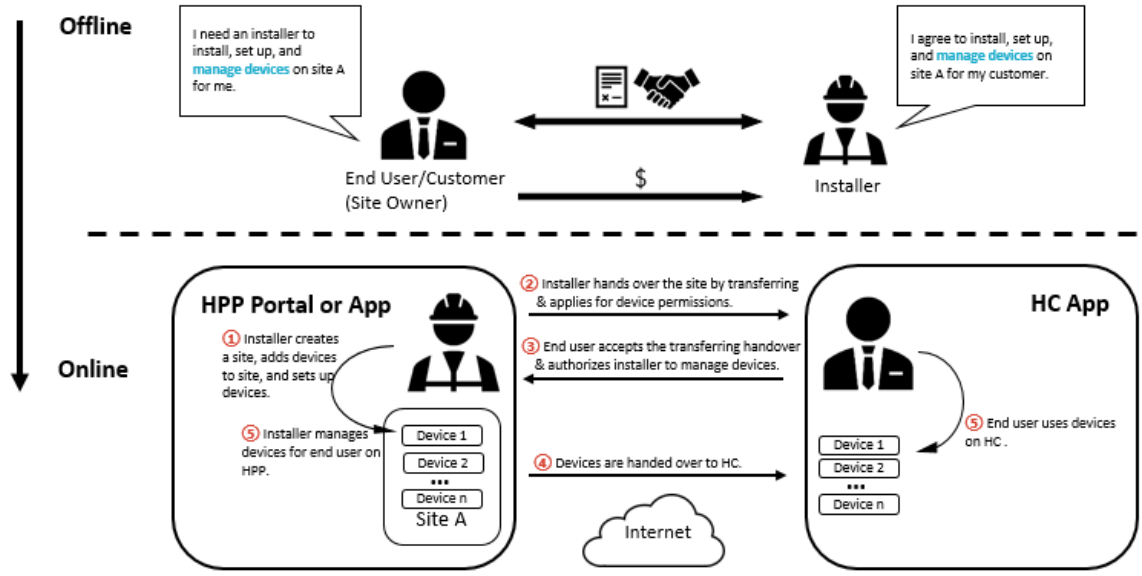


Figure 3-148 Scenario and Process

Tenant Site Scenario (Where You Hand Over by Sharing)

A typical tenant (shared) site scenario is where the devices are owned by the ARC, the installer, or the property management company, and the ARC provides the alarm receiving service for customers with these devices, or the installer helps the property management company provide the device installation and maintenance service for the customers (tenants). The devices will be available to the customers only during the service periods.

The following diagrams show a typical scenario related to device handover (by sharing), as well as the overall process.

Two Agreements Reached

Before you can hand over the devices in the apartment by sharing to the tenant via Hik-Partner Pro, the following two agreements have to be reached.

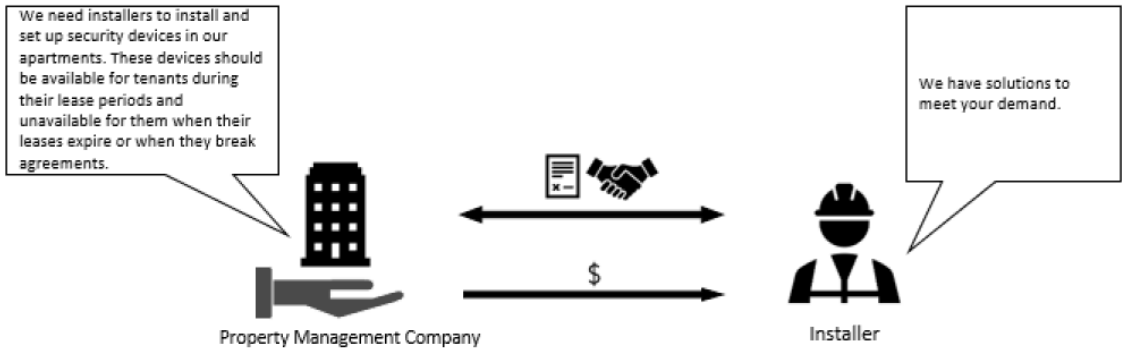


Figure 3-149 Agreement Reached Between the Property Management Company and Installer

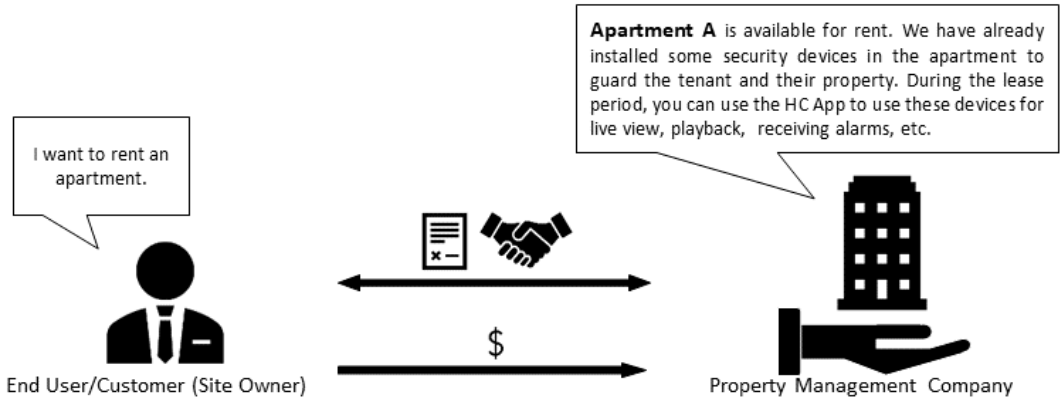


Figure 3-150 Agreement Reached Between the Tenant and Property Management Company

Online Operations

After the two agreements are reached, you will hand over the devices to the tenant by sharing on Hik-Partner Pro, of which the process is shown below:

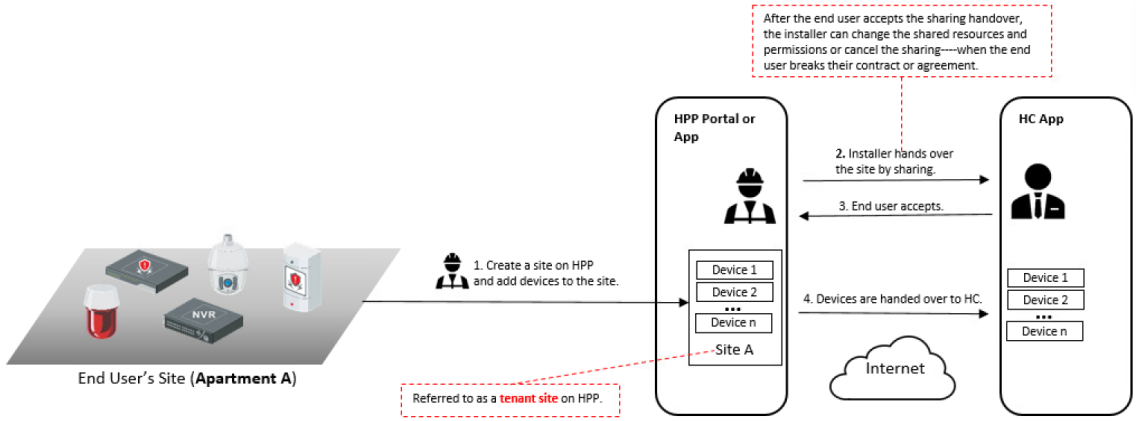


Figure 3-151 Hand Over Devices to the Tenant

Hand Over Site with Devices by Transferring

If the site is handed over by transferring, the customer takes ownership of the devices, and usually the devices are owned by the customers.

Before You Start

- Make sure that the site status is **Not Handed Over** and the services have been activated on the site.
- Make sure you have the permission for site management, such as managing all sites and assigned sites.
- Make sure the devices are added to the site. The supported device types include security control panels, access control devices, encoding devices, video intercom devices, doorbells, Hik-ProConnect boxes, and radars.

Hand Over Personal Sites

Steps

1. Enter the Hand Over Site page.

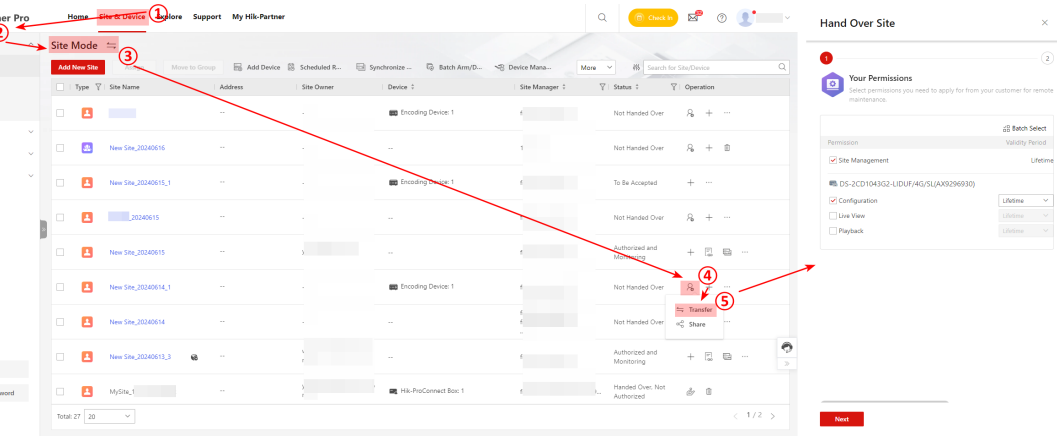


Figure 3-152 Enter the Hand Over Site Page on the Portal

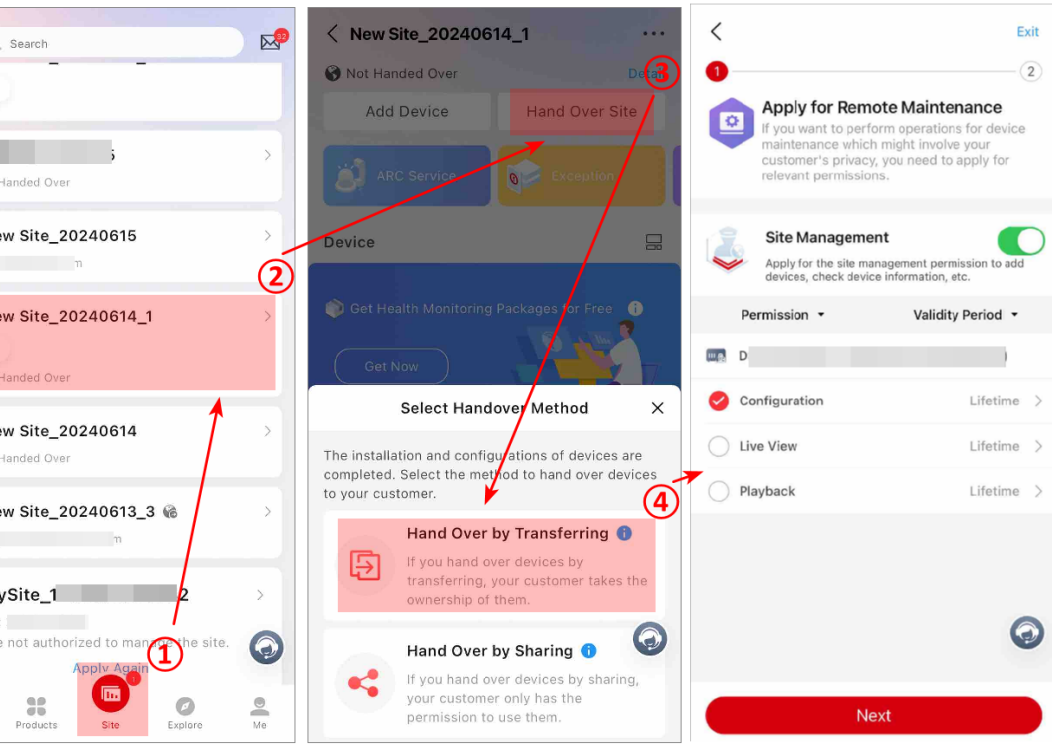


Figure 3-153 Enter the Hand Over Site Page on the Mobile Client

2. Select the permissions, including managing site information, configuring the selected devices on the site, streaming the live video and playing back video from the selected devices on the site, for which you need to apply from your customer in order to maintain the devices, and set the corresponding validity periods.

Note

- If you have no permission to manage devices, you cannot select the permissions of configuration, live view, and playback.
- When your customer accept the handover, the selected permissions will be granted to you without applying for authorization from your customer again.

3. Enter the next page and select a handover method.

Via Email or Phone Number (Both Available on the Portal and Mobile Client)	Enter the email address or phone number of the customer, (optional) enter the remarks (such as the reason for the handover, which your customer can view when they receive the handover via the Hik-Connect Mobile Client), and submit the application. And then your customer will receive the handover application in their email box or via short message with a download link of the Hik-Connect Mobile Client (v5.2.3 or later).
Via QR Code (Only Available on the Mobile Client)	Inform your customers to download or update the Hik-Connect Mobile Client (v5.2.3 or later), and then show the QR code to your customers face to face or share it via a third-party application to ask them to scan the QR code with Hik-Connect.

4. Inform your customer to register a Hik-Connect account first if they do not have one, log in to the Hik-Connect Mobile Client, and accept the handover to become the site owner.

Note

- If the cloud attendance system provided by Hikvision or a third-party manufacturer has been added to the site and activated, after you handed over the site to your customer, your customer will be able to use the cloud attendance system.
- For **Not Registered** or **To Be Accepted** sites, you can submit the handover application again for at most five times in one day and the previous handover will be invalid.

5. **Optional:** ***Apply for handed-over site authorization from site owner*** if your customer wants you to manage and maintain more of their devices after your customer accepts the handover and becomes the site owner.

Hand Over Team Sites

Steps

1. Open the Hand Over Site pane.

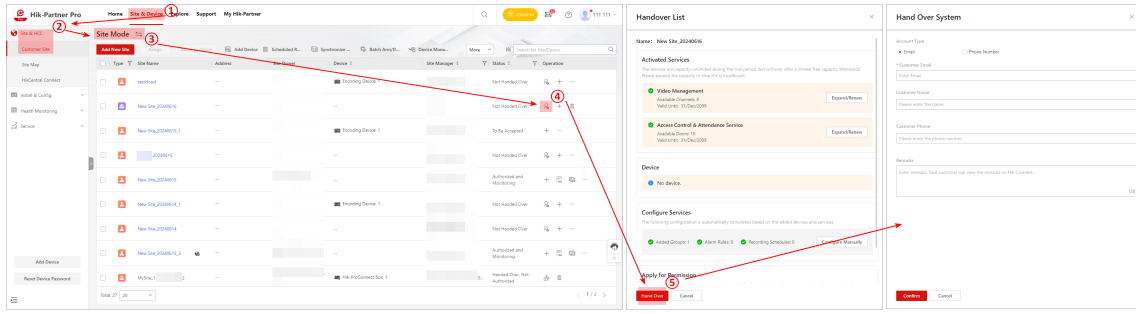


Figure 3-154 Open the Hand Over Site Pane on the Portal

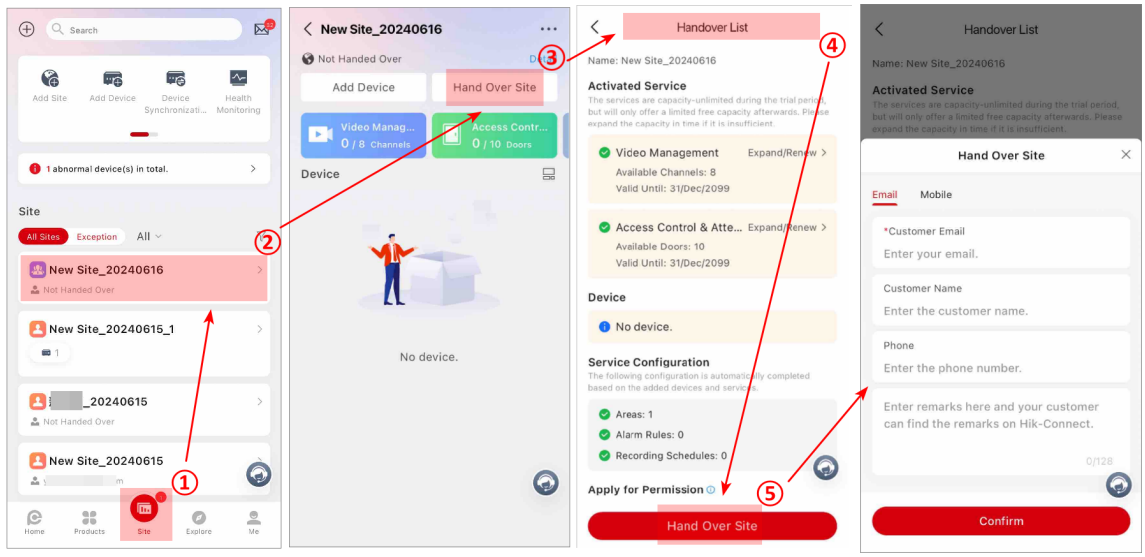


Figure 3-155 Open the Hand Over Site Pane on the Mobile Client

2. Select **Email** or **Phone Number** as the account type and set the corresponding parameters, such as the customer name and remarks.
3. Confirm your settings.

   Your customer will receive the handover application in their email box or via short message with a download link of the Hik-Connect Mobile Client.
4. Inform your customer to download or update the Hik-Connect Mobile Client (V5.2.3 or later), register a Hik-Connect account first if they do not have one, log in to the Hik-Connect Mobile Client, and accept the handover to become the site owner.

Hand Over Site with Devices by Sharing

If devices are owned by your company, for example, if you are an ARC who provides the remote alarm receiving service for customers with your company's devices, you can hand over the devices to multiple customers by sharing without transferring ownership of the devices. To hand over

devices by sharing, you can choose between applying for permissions from your customers (Mode A) and NOT applying for permissions from your customers (Mode B).

Before You Start

- Make sure that the site status is **Not Handed Over**.
- Make sure you have the permission for site management, such as managing all sites and assigned sites.
- Make sure the devices are added to the site. The supported device types include security control panels, access control devices, encoding devices, video intercom devices, doorbells, Hik-ProConnect boxes, and radars.

Steps

1. Enter the handing over by sharing page.

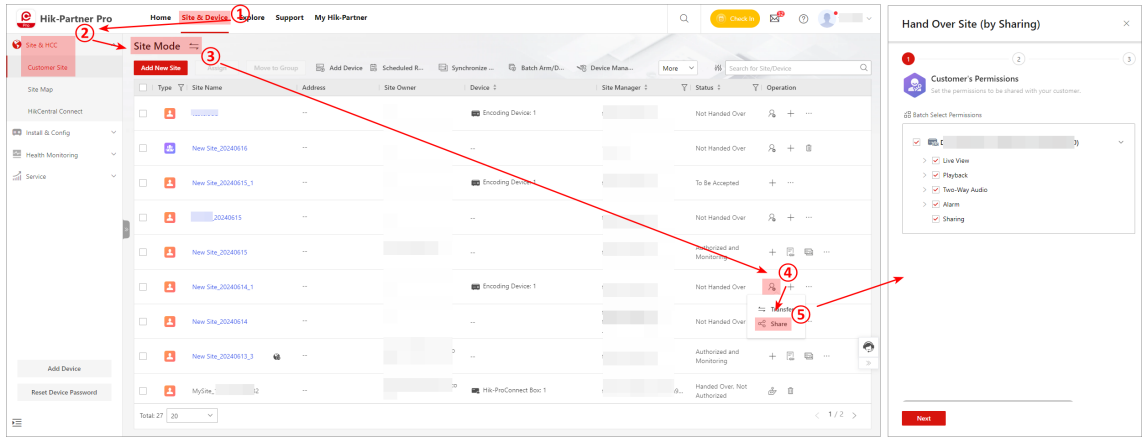


Figure 3-156 Enter the Hand Over by Sharing Page on the Portal

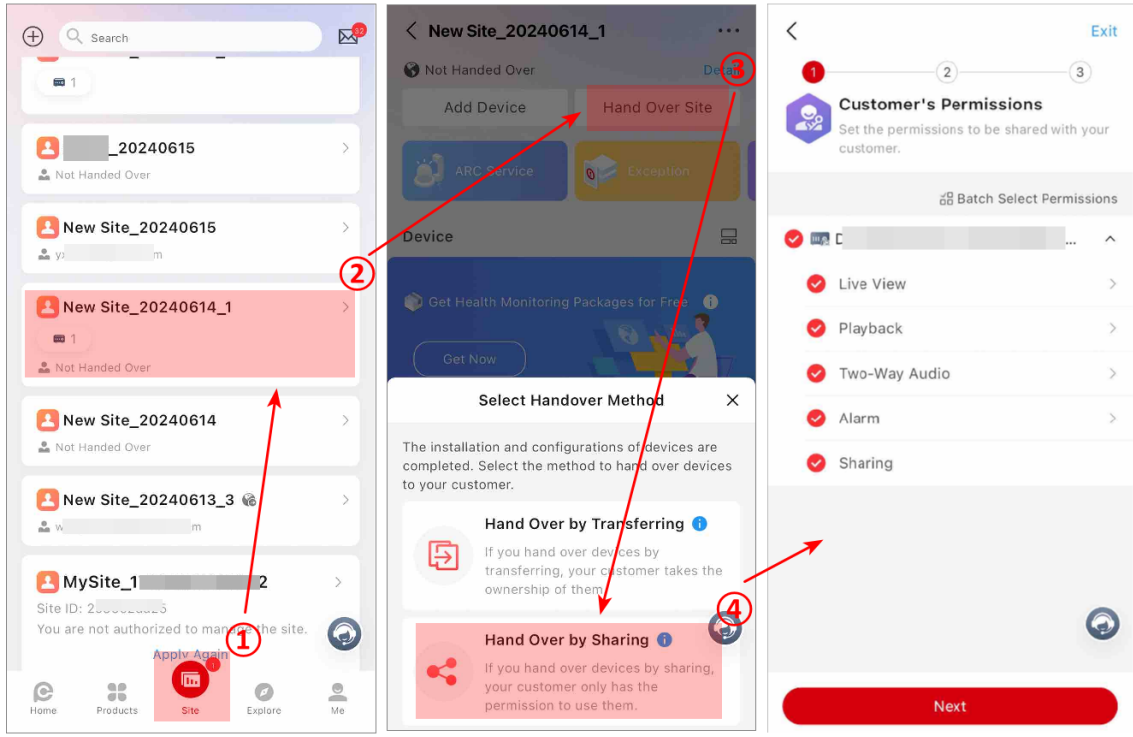


Figure 3-157 Enter the Hand Over by Sharing Page on the Mobile Client

2. Select the resources and permissions to be shared with your customer.

3. Enter the next page and decide whether to enable **I Have All Device Permissions** or not.

- Mode A: If you need to apply for permissions from your customer, do not enable **I Have All Device Permissions**, but you need to apply for sub permissions for alarm devices (PIRCAM GIF and video clips) when the ARC service is enabled and set validity periods of live view or playback permission.

- Mode B: If you have all permissions for the devices and do not need to apply for permissions from your customer for remote maintenance, enable **I Have All Device Permissions**.

4. Enter the next page and select a method for handing over devices to only one customer or multiple customers.

Via Email or Phone Number (Both Available on the Portal and Mobile Client)	Enter the email address(es) or phone number(s) of one or multiple customers, (optional) enter the remarks (such as the reason for the handover, which your customers can view when they receive the handover via the Hik-Connect Mobile Client), and submit the application. And then your customers will receive the handover application in their email box or via short message with a download link of the Hik-Connect Mobile Client (v5.4.0 or later).
Via QR Code (Only Available on the Mobile Client)	Inform your customer(s) to download or update the Hik-Connect Mobile Client (v5.4.0 or later), and then show the QR code to your customer(s) face to face or share it via a third-party application to ask them to scan the QR code with Hik-Connect.

Note

- For Mode A, there should be a customer administrator who reviews your application for permissions. If you hand over devices to only one customer, this customer should be the customer administrator. If you hand over devices to more than one customers, you should select one customer as the customer administrator.
- One device can be shared with no more than 10 customers.

5. Inform your customers to register a Hik-Connect account first if they do not have one, log in to the Hik-Connect Mobile Client, and accept the handover.
6. **Optional:** After sites are shared, the following operations are also supported.
   - For sharings that are rejected and expired, support sharing them again.
   - For sharings that are to be accepted and accepted, support canceling sharing.
   - For sharings that are to not be accepted in Mode A, support editing customers to be shared with.
   - Supports adding new customers and new devices to the existing sharings. By default, these newly added devices will not be shared with any customer, but you can select these devices and their permissions on the customer card to share them with the corresponding customers. The customers do not need to accept the sharing once again.

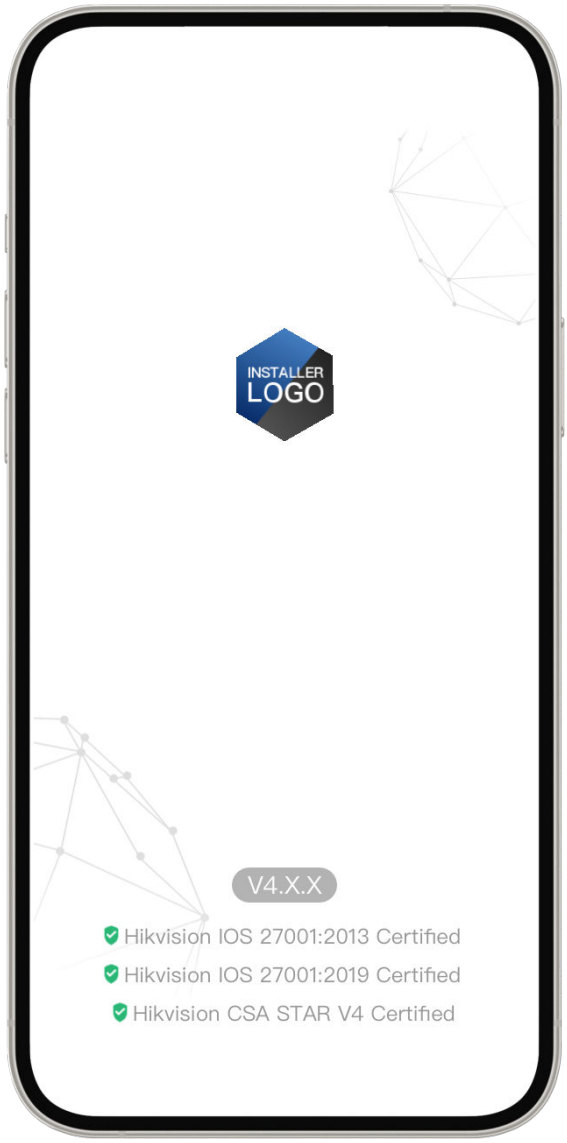
3.4.3 Co-Branding: Maintain Customer Loyalty and Increase Your Brand Visibility

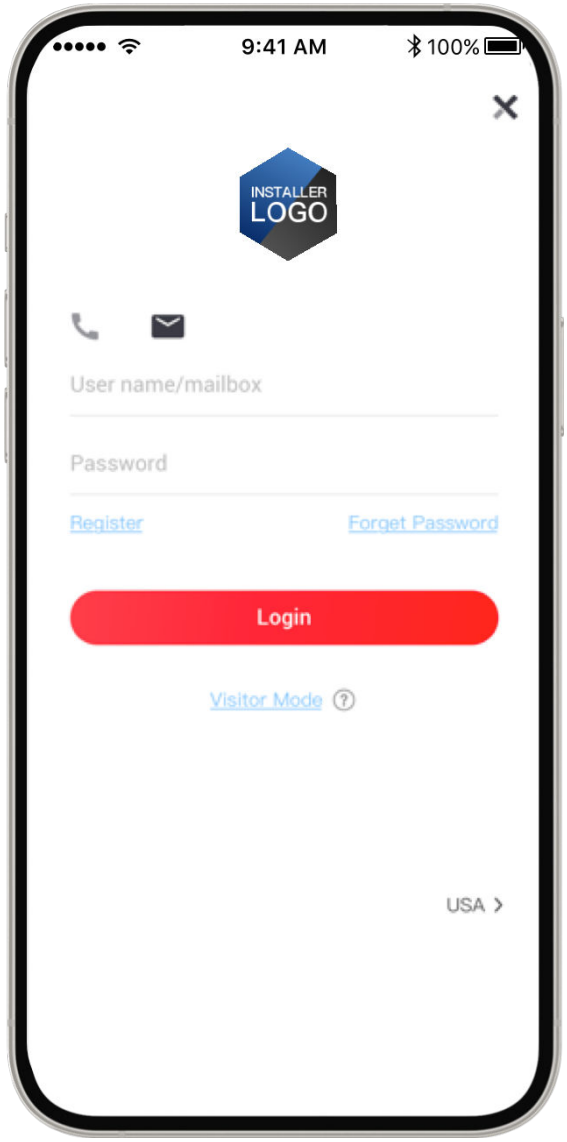
Follow the corresponding instructions to allow your customers to view your company information, such as company logo, email address, and phone number on the Hik-Connect Mobile Client and HikCentral Connect Portal and Mobile Client, which can help you promote awareness of your company brand, products, and services.

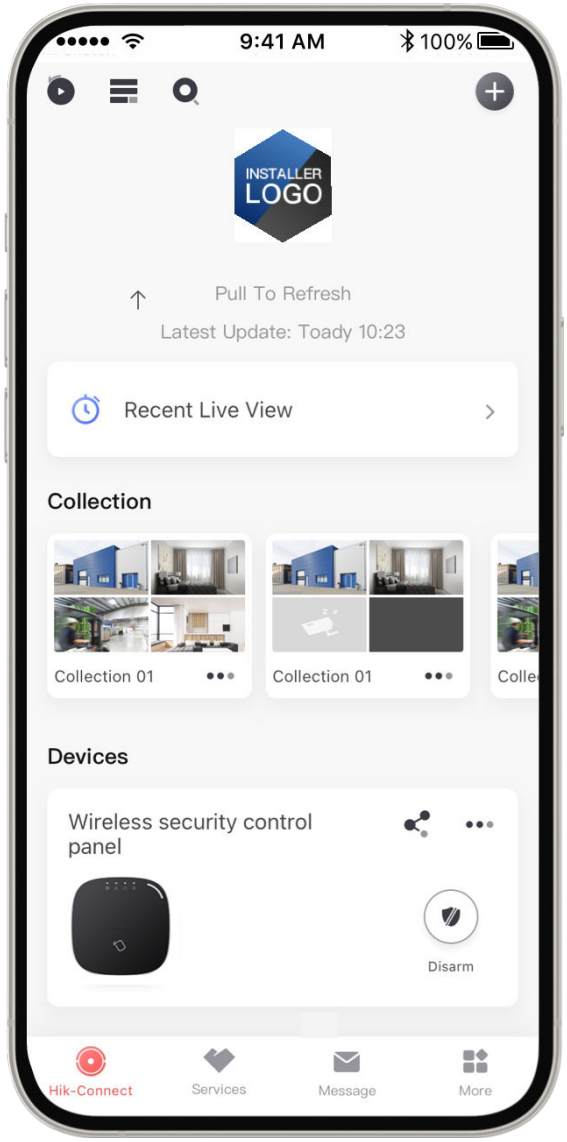
Effects and Benefits of Co-Branding

Effects of Co-Branding: Where Your Customers Can See Your Company Logo

- Hik-Connect: Your customers can see your company logo on the launch page, login page, Home page, About page, and service provider information page (for both personal and team modes).




9:41 AM
100%
INSTALLER LOGO
User name/mailbox
Password
Register
Forget Password
Login
Visitor Mode
USA


9:41 AM
100%
INSTALLER LOGO
Pull To Refresh
Latest Update: Toady 10:23
Recent Live View
Collection
Collection 01
Collection 01
Devices
Wireless security control panel
Disarm
Hik-Connect
Services
Message
More

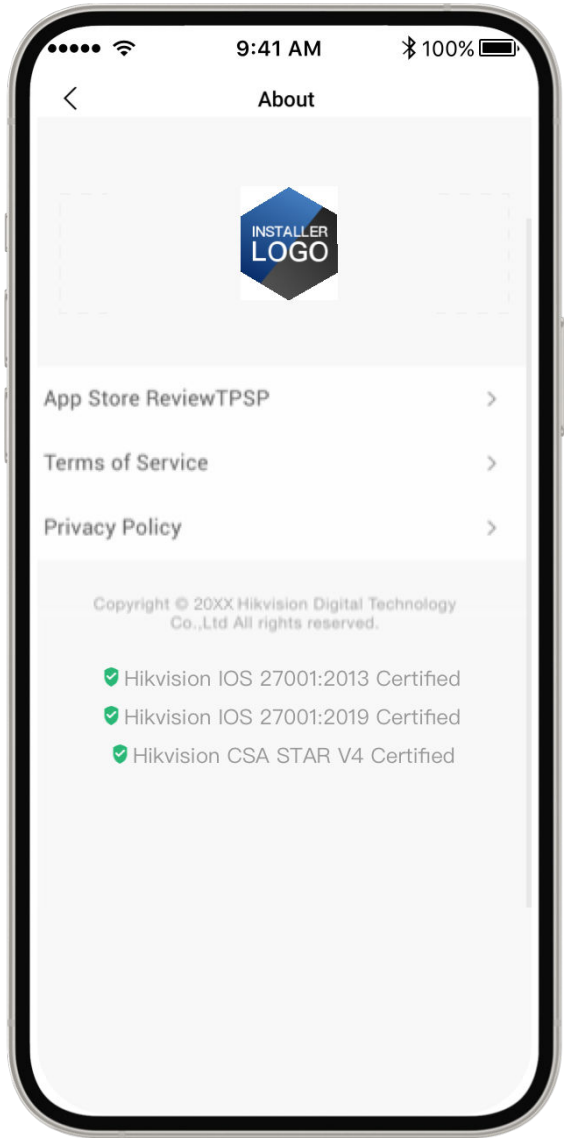


Figure 3-158 Your Company Logo on Hik-Connect

- NVR/DVR: Your customer can view your company logo on the startup and live view pages of NVRs/DVRs. For NVRs/DVRs supporting co-branding, refer to the device compatibility list.

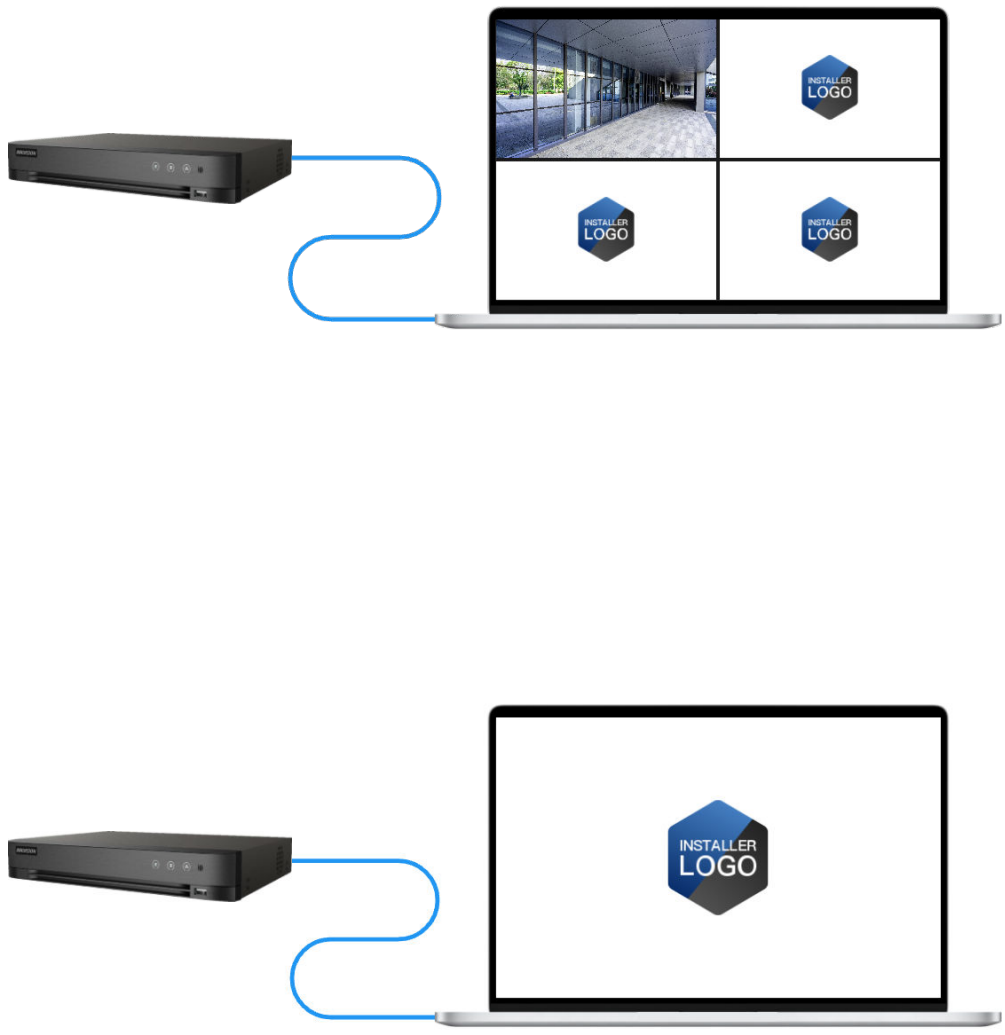


Figure 3-159 Your Company Logo on NVR/DVR

Benefits of Co-Branding

- Maintain customer loyalty
- Increase your brand visibility
- Increase potential business opportunities

Device Compatibility for Co-Branding

Check Device Compatibility for Co-Branding Using the Portal

1. Visit the Portal and scroll down to the bottom of the Portal. Click **Device Compatibility List**.

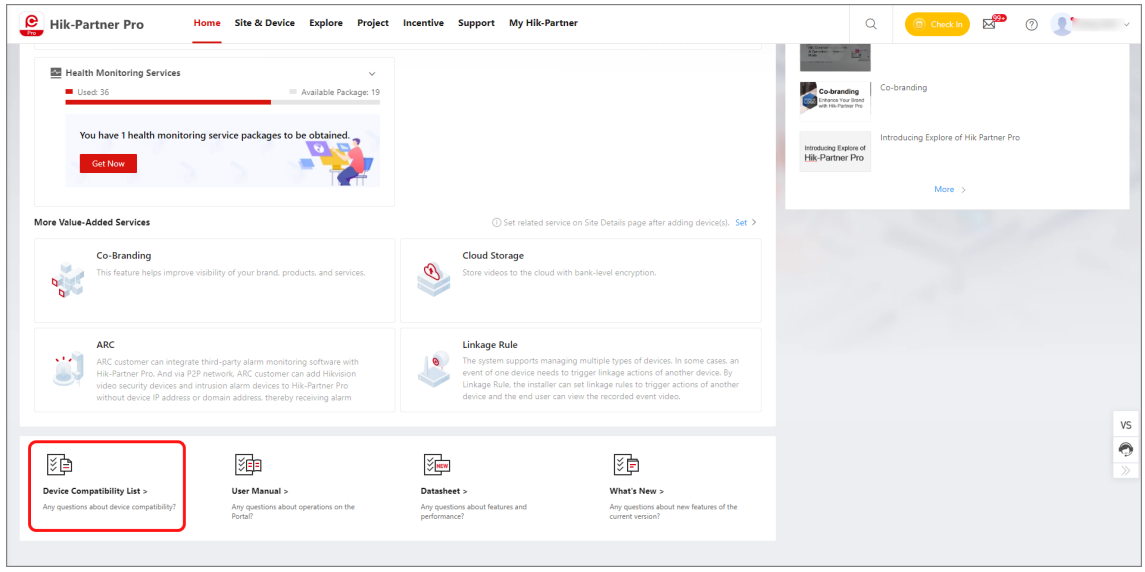


Figure 3-160 Device Compatibility List

2. Click **Compatibility List → Support Co-Branding** , and search for a NVR / DVR model to check whether it supports co-branding.

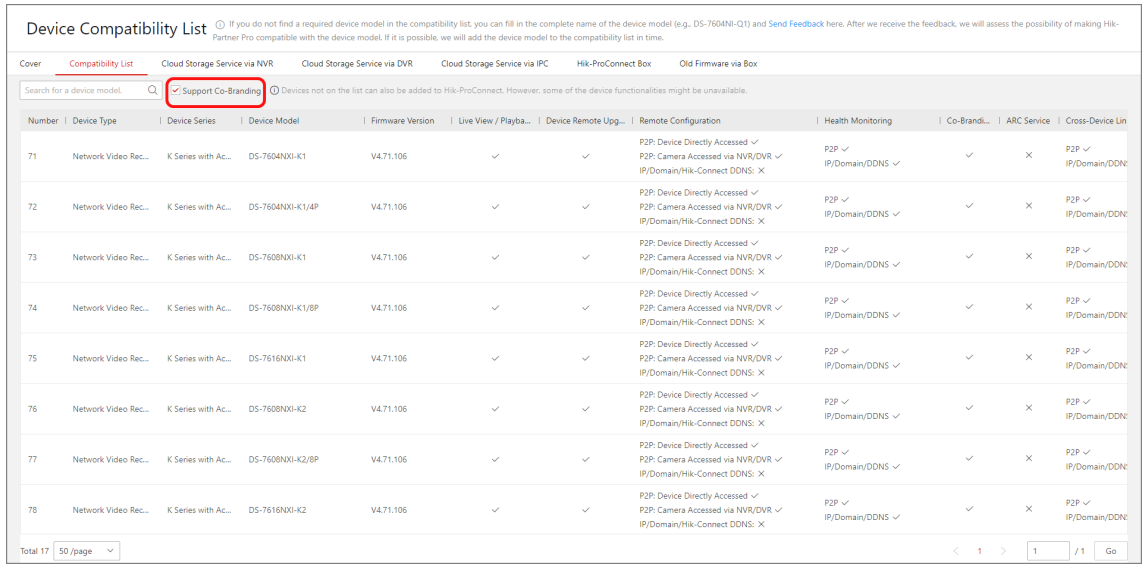


Figure 3-161 Compatibility List

Check Device Compatibility for Cloud Storage Service Using the Mobile Client

1. Log in to the Mobile Client, tap **Me → Tutorial Center** .

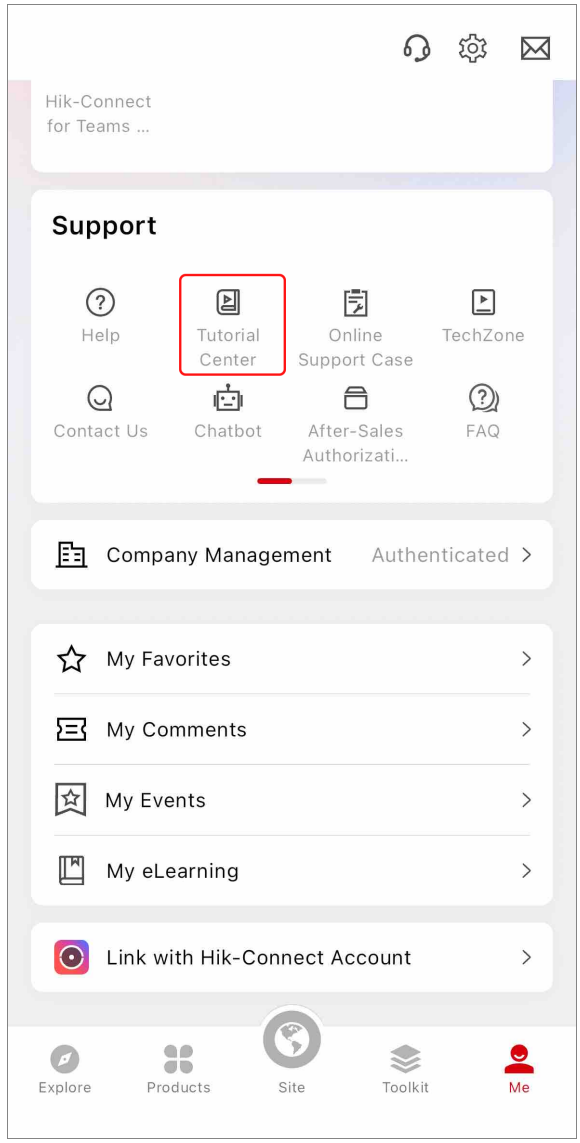


Figure 3-162 Tutorial Center

2. Tap **Technical Guidance → Hik-Partner Pro Device Compatibility List** .

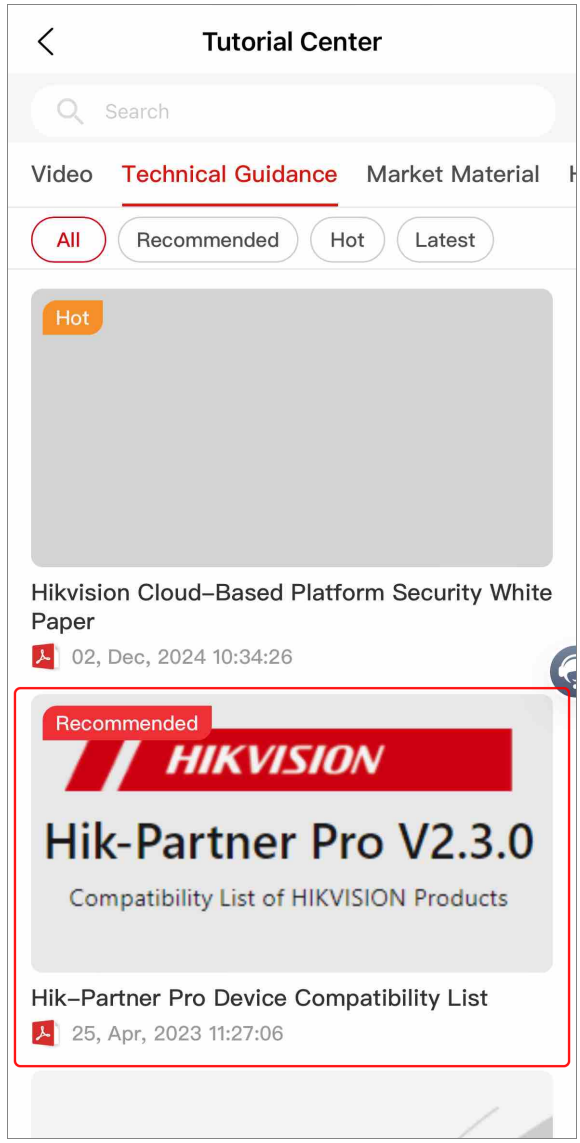


Figure 3-163 Compatibility List

3. Tap **Compatibility List** → , and search for a NVR / DVR model to check whether it supports co-branding.

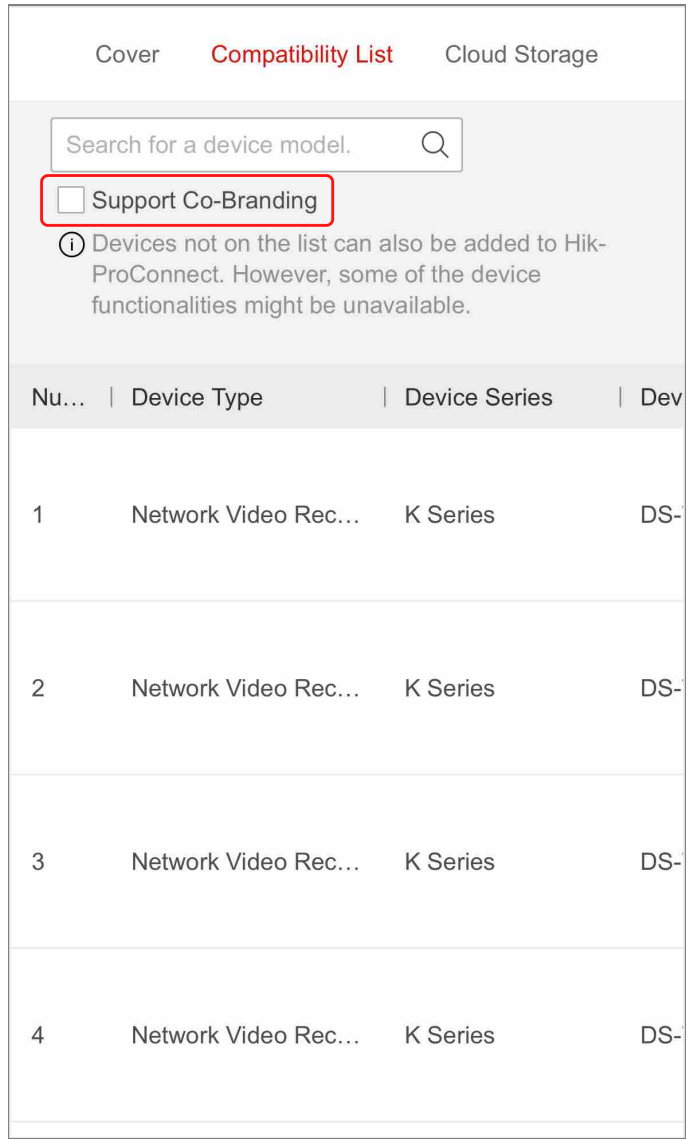


Figure 3-164 Cloud Storage Compatibility

Get Co-Branding

Ways for Getting Co-Branding for Free

Before purchasing and set up co-branding, check the following ways to get free co-branding:

1. You can redeem points for co-branding services in the ***Rewards Store*** . After that, the co-branding service will be available or its validity period will be extended if it is already available.
2. In some countries/regions, you can get the co-branding service for free for one year after ***authenticating your account*** and ***adding 3 devices via P2P*** .

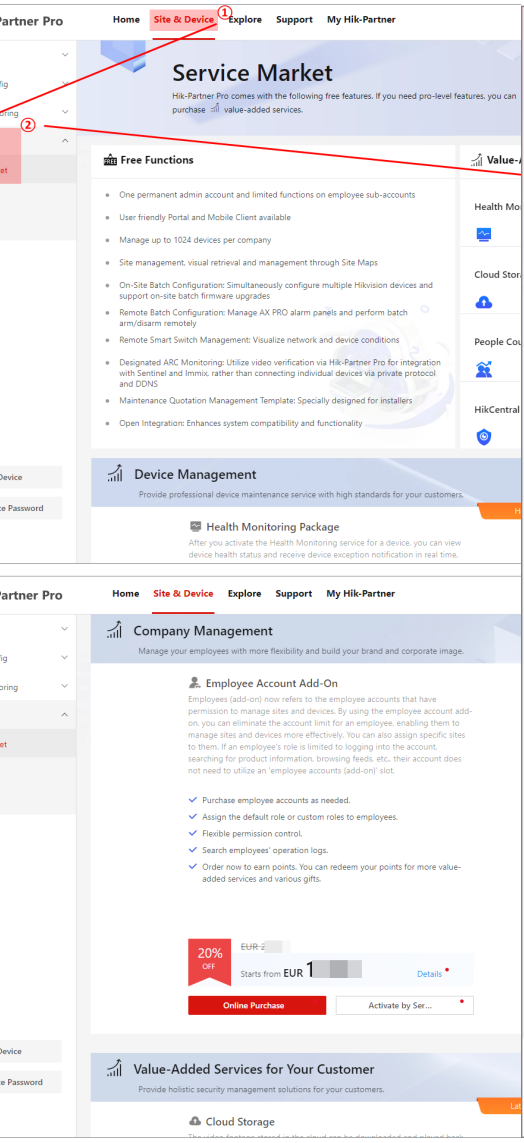
3. A window with notification about getting the co-branding service for free will pop up when your co-branding service expires in 2 months.
4. You can get the co-branding service for free after ***purchasing the annual type of health monitoring packages*** (including All Device Annual Package and Network Camera Annual Package) for the first time.

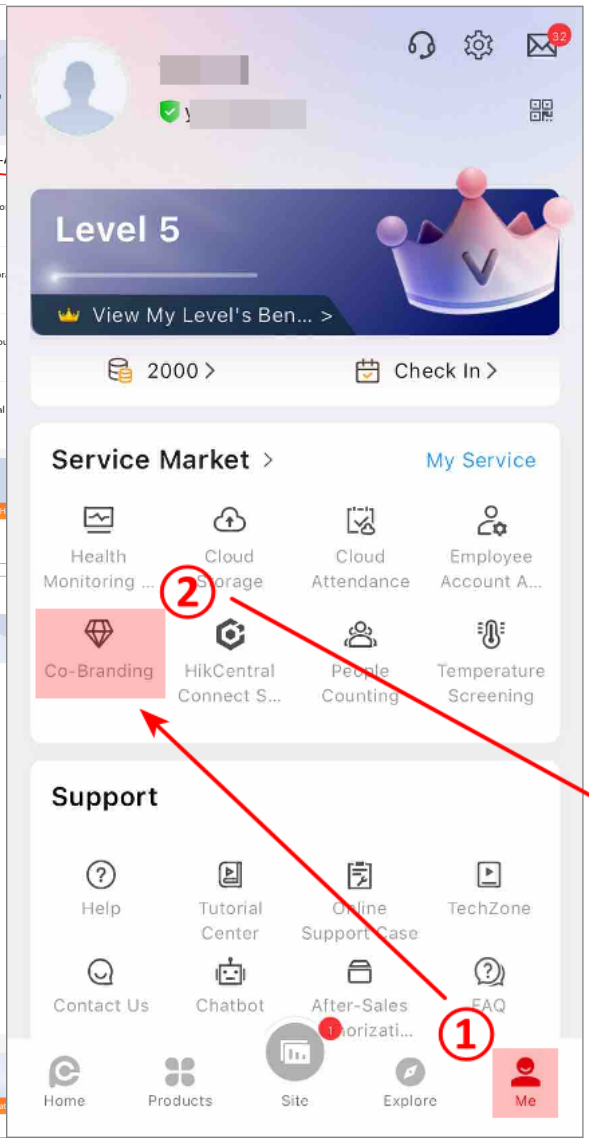
Purchase Co-Branding

Note

- Make sure you get your company authenticated.
- Purchasing co-branding services online is supported only in some countries/areas. Contact a local distributor for details.

1. Get the entry of purchasing co-branding service.





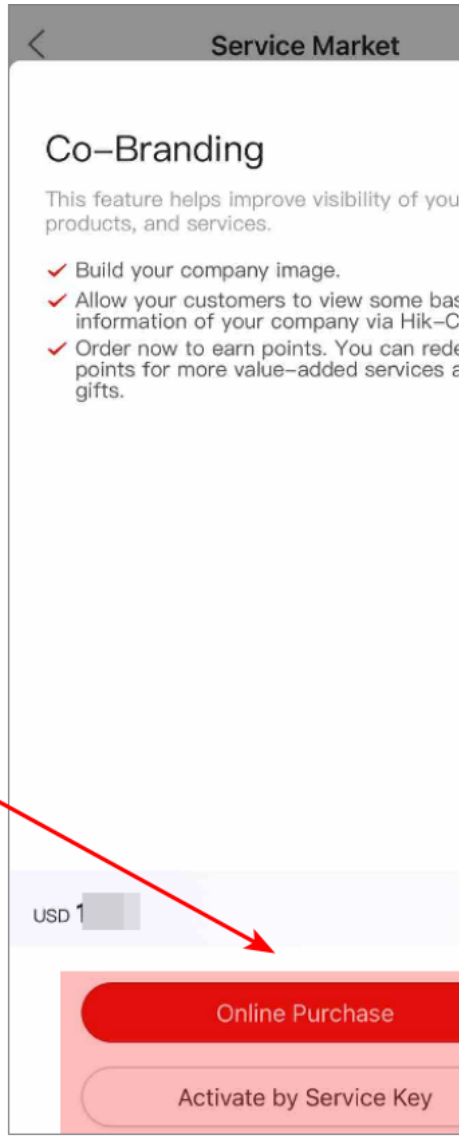


Figure 3-165 The Entry of Purchasing Co-Branding Service on the Portal

Figure 3-166 The Entry of Purchasing Co-Branding Service on the Mobile Client

2. Purchase the service in one of the following ways.

Online Purchase on the Portal	a. Specify the amount which determines the validity period, enter your VAT number, and select the payment method. b. Enter the distributor invitation code and the code from Hikvision sales.

	Note By entering the codes when you purchase services online, you may get some discounts and the distributor/reseller can ***earn some rebates*** . c. Select **Checkout** to enter the payment page and complete your payment.
Online Purchase on the Mobile Client	a. Set the service year and enter the invitation code. b. Select **Checkout** to pay for the service according to the operating system of your phone. - For iOS, sign in with your Apple ID. - For Android, go to the GCPay/PingPong payment page to complete the purchase.
Activate by Service Key on the Portal and Mobile Client	Enter a service key or multiple service keys (separated by commas) that you have purchased from distributors.

3. (Optional) Check your order details on the My Order page.

Note

For iOS, you can view only the orders made on your phone. Go to the Portal for more order details.

Enable Co-Branding

1. Enter the co-branding service page.

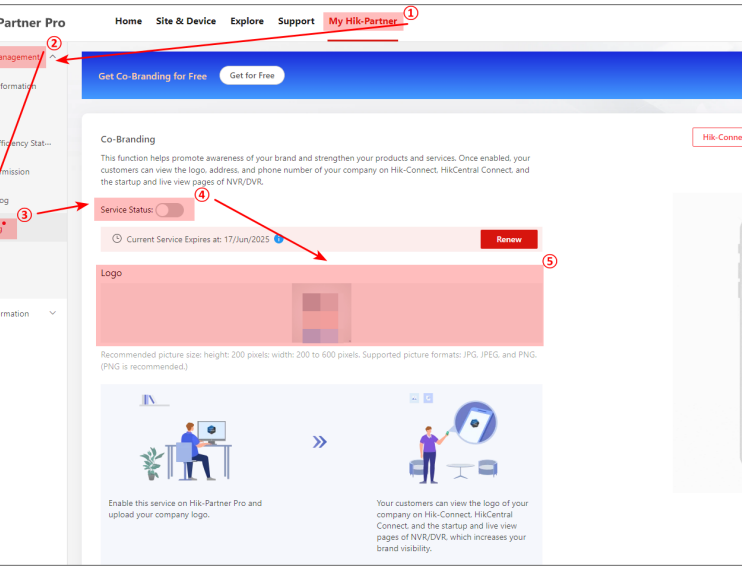


Figure 3-167 Enter the Co-Branding Service Page on the Portal

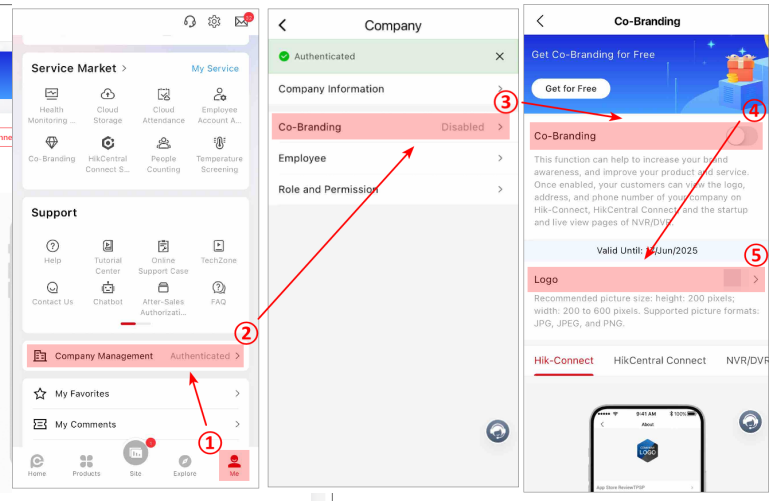


Figure 3-168 Enter the Co-Branding Service Page on the Mobile Client

2. Switch on the button to enable the co-branding service.
3. Upload your company logo in the Logo area for increased brand visibility.

Note

If no company logo is uploaded, your company name, instead of your company logo, will be displayed.

3.4.4 Group Sites to Manage Multiple Sites More Efficiently

If you need to manage individual customers from different cities, or if there is an individual customer who has many sites, such as chain stores, you can group sites by cities or group sites for such a customer who has many sites, thus managing your customers more efficiently.

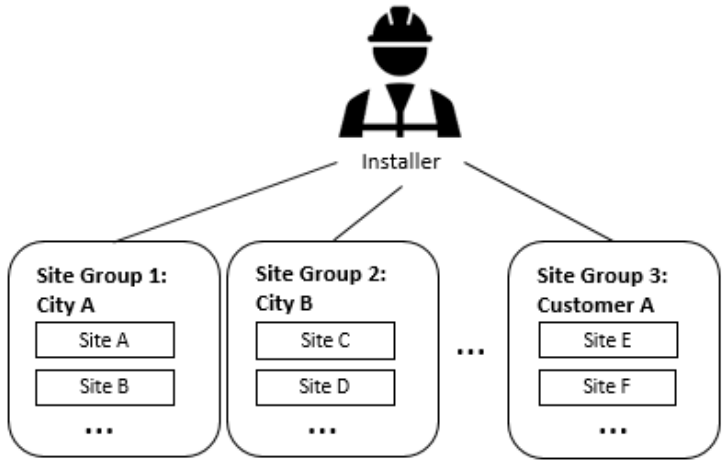


Figure 3-169 Site Grouping Scenario

There are multiple methods for you to group personal sites.

- When adding a personal site, you can create a group or select an existing group to group the new site after you enable **Move to Group**.

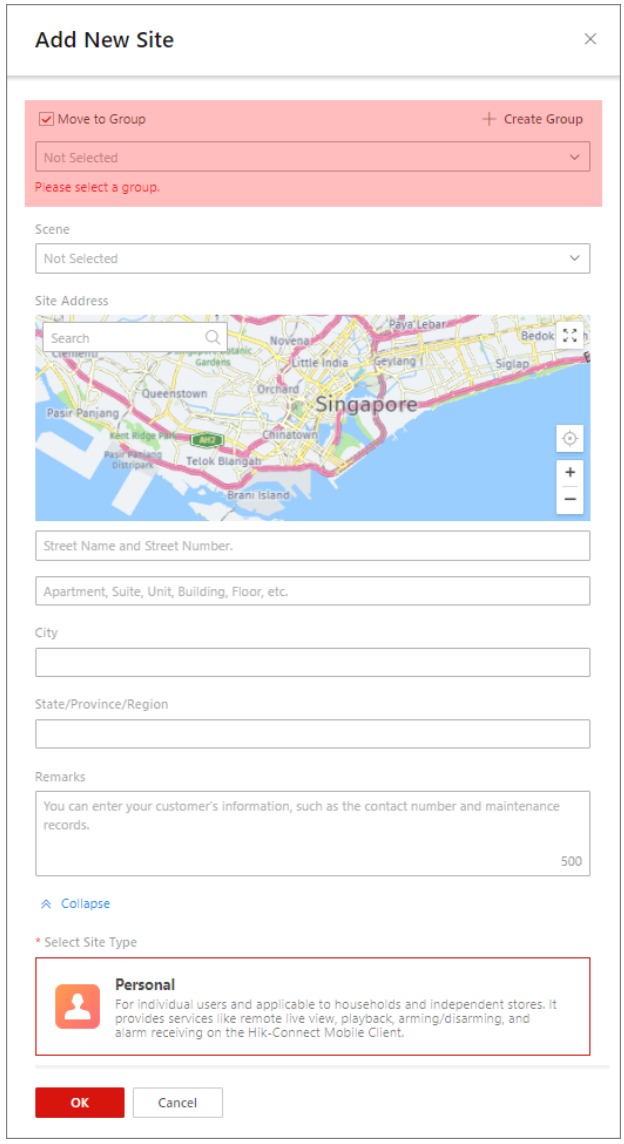


Figure 3-170 Group a Personal Site When Adding It (Portal)

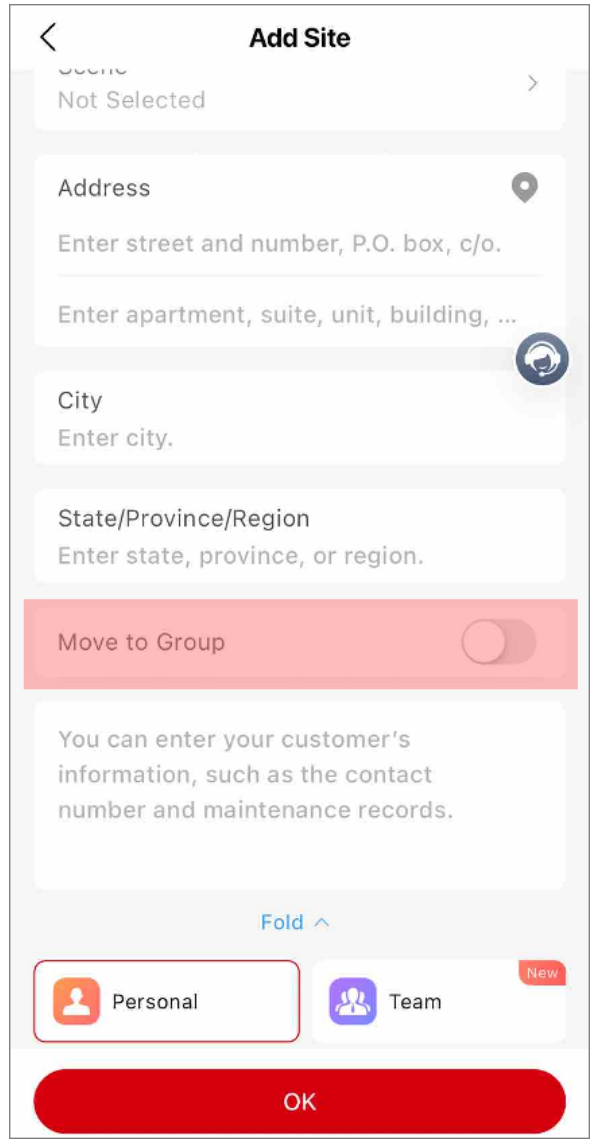


Figure 3-171 Group a Personal Site When Adding It (Mobile Client)

- If you want to group the existing personal sites, you should first create a group if there is no group and then select sites to be added to the new group.

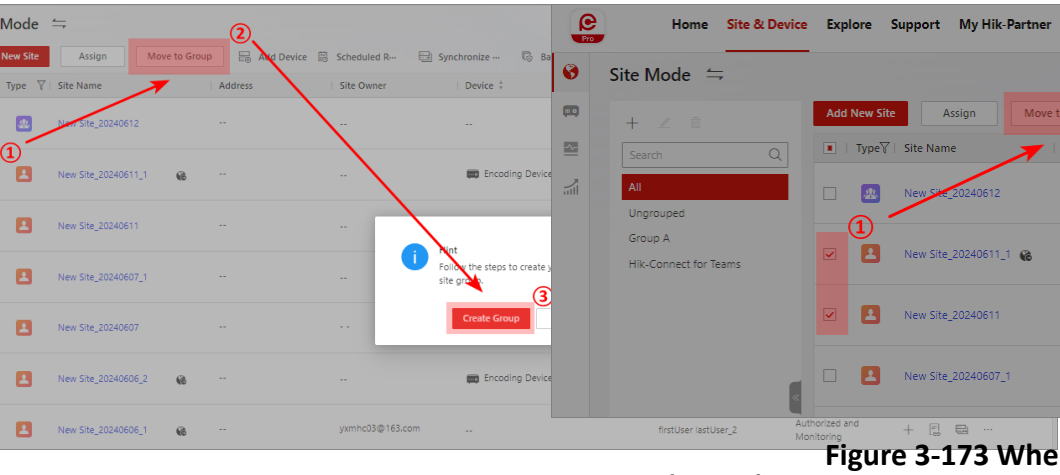


Figure 3-172 When No Site Group (Portal)

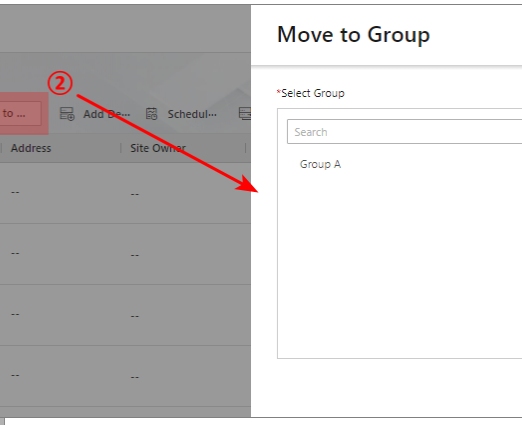


Figure 3-173 When Site Groups Exist (Portal)

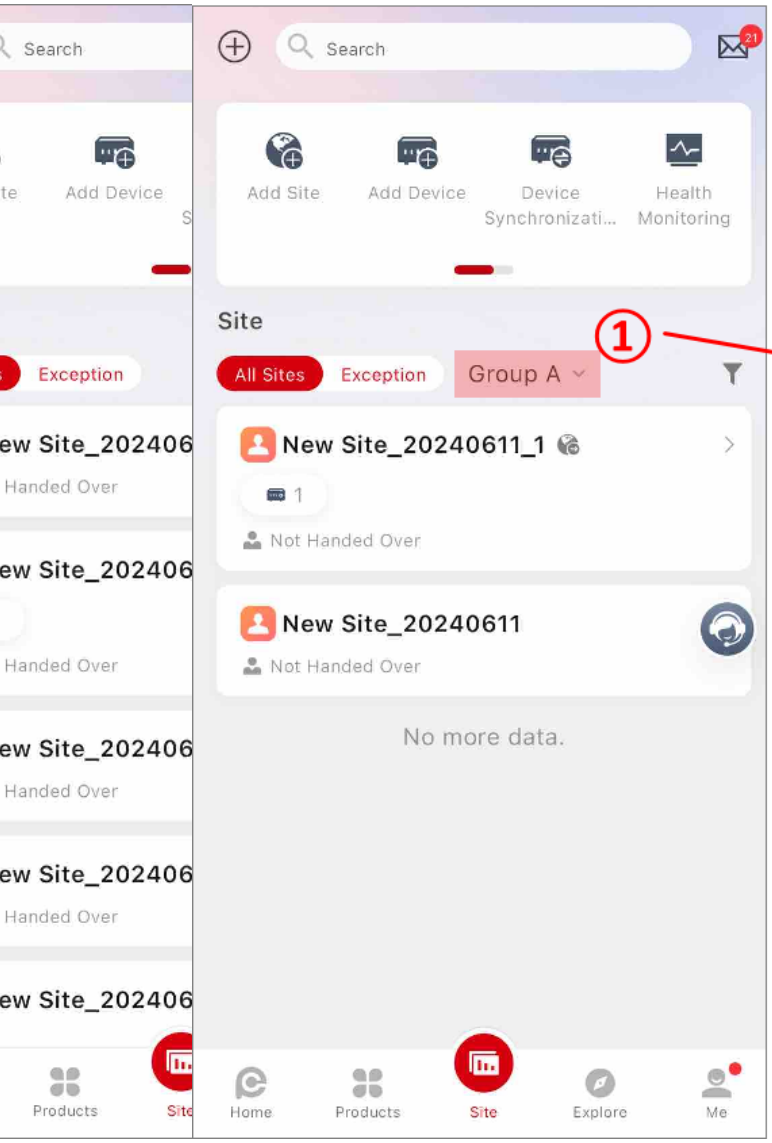


Figure 3-174 When No Site Group (Mobile Client)

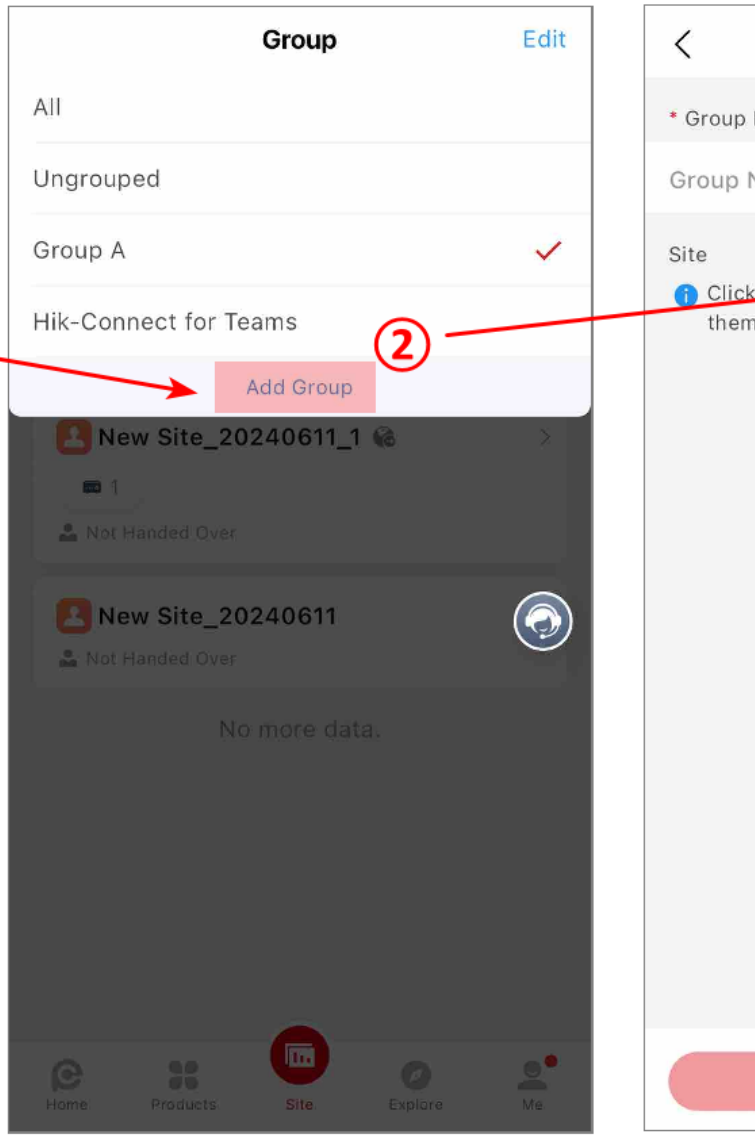


Figure 3-175 When Site Groups Exist (Mobile Client)

Note

One group can contain multiple personal sites, but one personal site can be grouped into only one group.

3.4.5 How to Move Devices from One Customer Site to Another?

You can use the Device Movement feature to move devices from one Site to another. By distributing devices to different Sites, you can manage both the Sites and devices more efficiently.

- The feature is only supported by a device matches the following conditions:
  - The original Site where the device belongs to needs to have been authorized to you.
  - The device needs to be added by Hik-Connect (P2P). The devices added by IP address / domain name are not supported.
  - The original Site and the target Site should belong to the same Site Owner.
- Once a device is moved from its original Site, you need to configure the device again because all the original device configurations will be invalid. In addition, device related configurations including the linkage rules, exception rules, ARC settings, network switch settings, people counting service, temperature screening service, cloud storage service, and cloud attendance service, etc., will be affected. You need to configure these related configurations again also.

Move Devices on Portal

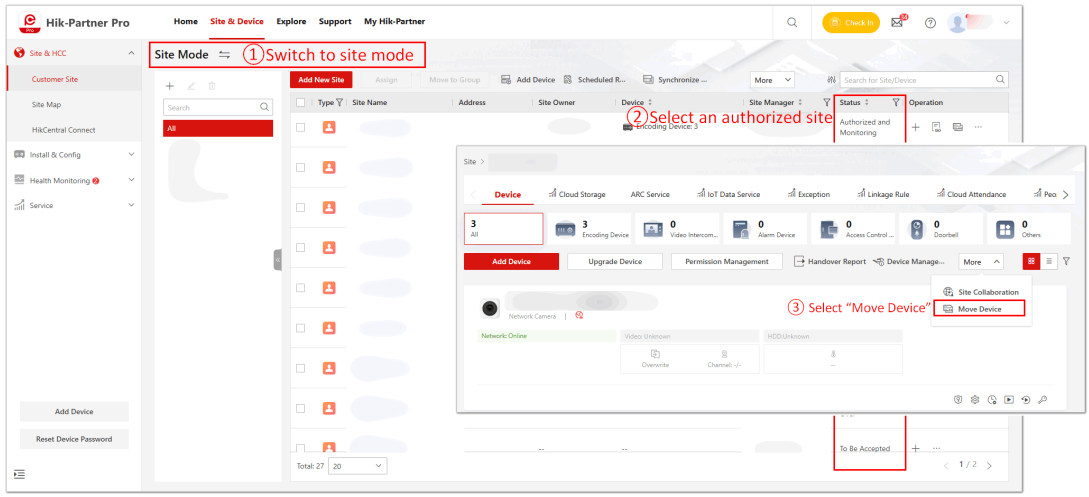


Figure 3-176 Move Device Part 1

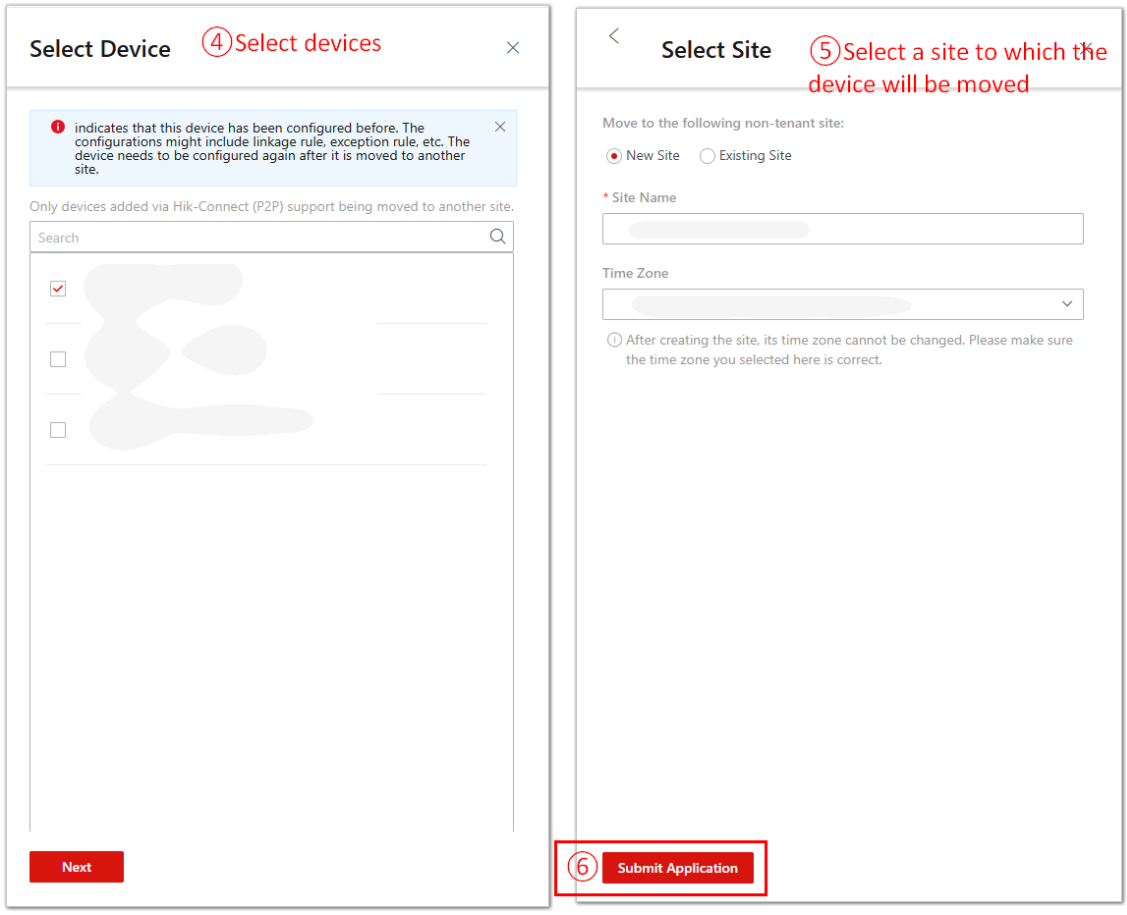


Figure 3-177 Move Device Part 2

Move Devices on Mobile Client

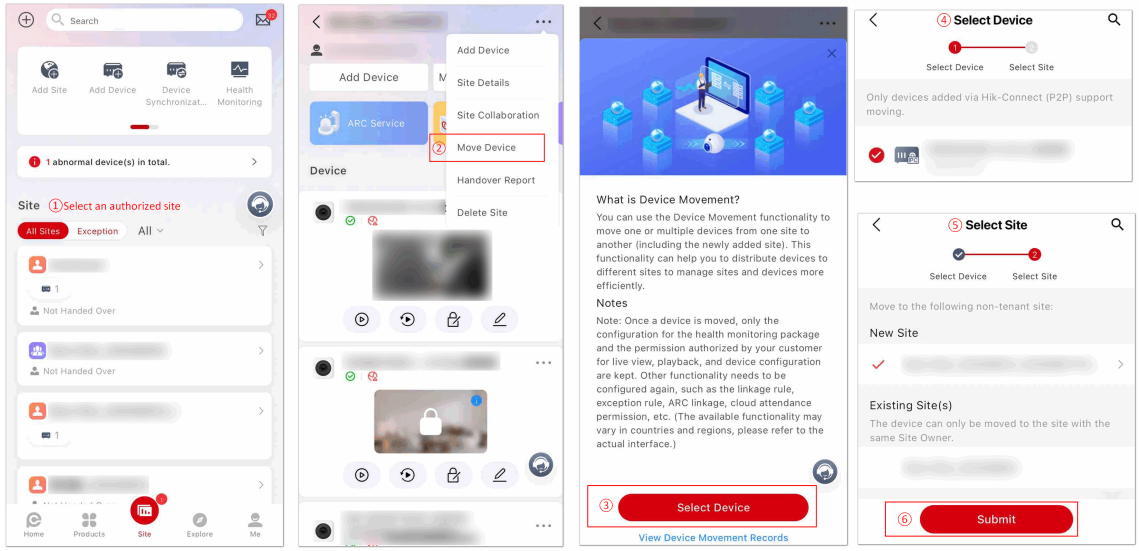


Figure 3-178 Move Devices on Mobile Client

3.4.6 How to Get a Device Management Invitation from Your Customer?

You can accept a device management invitation from your customer to manage a device that has already been added to a Hik-Connect account. In this way, the device, along with its configuration and operation permissions, can be shared with you to allow you to manage it for your customer on Hik-Partner Pro. Compared with migrating the device from Hik-Connect to Hik-Partner Pro, which requires your customer to share their Hik-Connect account name and password with you, this way is much more privacy-friendly and easier to be accepted.

To know more about the device management invitation, read the following sections:

- ***Overall Process***
- ***How Your Customer Invites You to Manage Their Device***
- ***The Email of Device Management Invitation***
- ***The Notification of Device Management Invitation***

Overall Process

If your customer (i.e., the Hik-Connect user) has already added one device to their Hik-Connect account, the customer can use the Hik-Connect Mobile Client to invite you to manage this device. Once the customer completes the invitation, an email containing the invitation information (e.g., the Hik-Connect user name and device name) and the button/link for accepting the invitation will be sent to you, and then you can accept the invitation. Invitations for device management can also be accepted via ✉ → **Business Notification** . Once you accept the invitation, the device will show

on the specified site (namely, the site mentioned in the email or the notification) on Hik-Partner Pro.

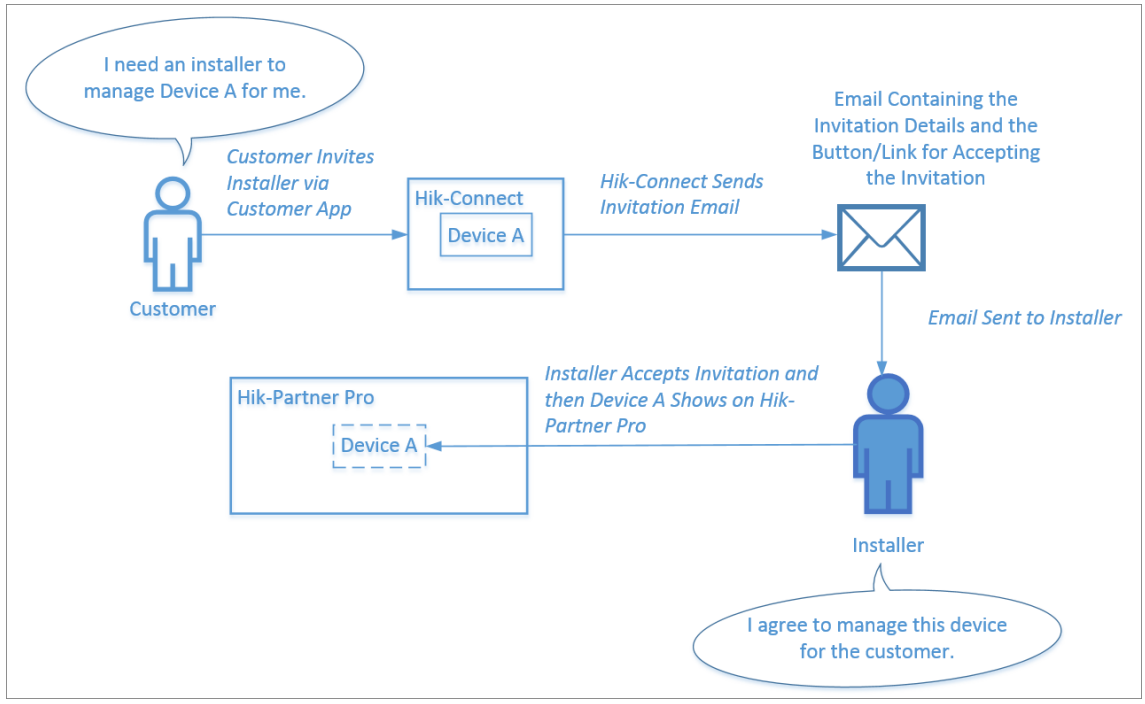


Figure 3-179 Overall Process Diagram

How Your Customer Invites You to Manage Their Device

You can go to the site list page, and then tap **Add Device → Learn More → Authorization Wizard** to open the following page to see how your customer uses the Hik-Connect Mobile Client to invite you to manage their device. It should be noted that you need to provide your Hik-Partner Pro account (email address) to your customer first to let them specify you as the Installer who manages their device.

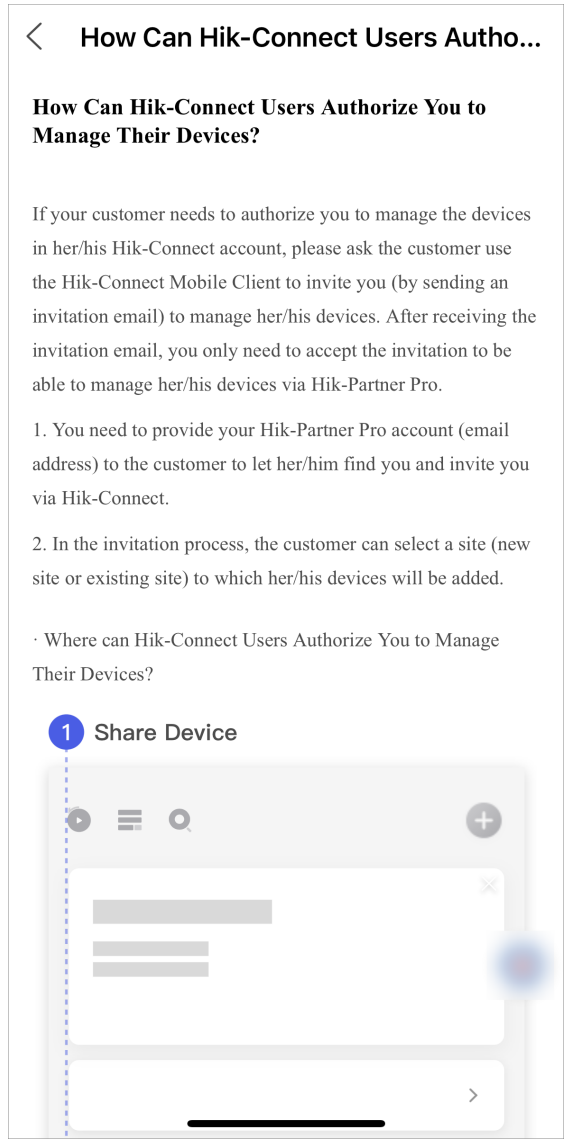


Figure 3-180 How Can Hik-Connect User Authorize You to Manage Their Device

The Email of Device Management Invitation

The email shows the invitation details including the device name, device serial number, name of the site where the device(s) is added, Hik-Connect user account, and the time of invitation. If you agree to manage the device(s) for your customer, you need to accept the invitation in three days, otherwise the invitation will be invalid.

The Notification of Device Management Invitation

The notification shows the invitation details including name of the site where the device(s) is added, device name, device serial No., the Hik-Connect user account, and the time of invitation. If

you agree to manage the device(s) for your customer, you need to accept the invitation in three days, otherwise the invitation will be invalid.

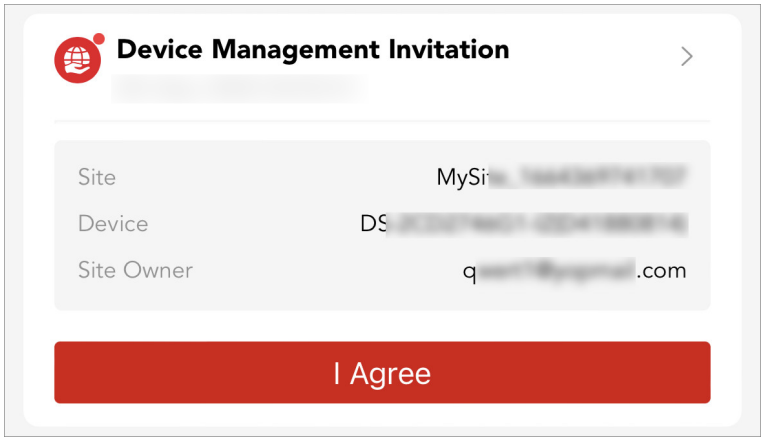


Figure 3-181 Sample Notification

3.4.7 How to Apply for Site Authorization & Device Permissions from Customers?

After handing over a site to your customer, you can apply for the permission from the customer to view the live view or playback of devices added to the site or configure the added devices. If you do not need the permissions of configuration and live view for devices, or you finish the device configuration task earlier than the planned time, you can release the permissions manually

Apply for Permission

Before You Start

Ensure that you hand over a site to your customer.

After you apply for permissions for your devices and your customer approves your application, you will be able to view the live view, playback of the device and configure device.

Steps

1. Tap **Site** to enter the site list page and tap a site.
2. Apply for device permissions.

Your Situation	Solution
Apply for permission for one device.	a. Tap a device to enter the device details page. b. In the Available Permission area, tap beside **Configuration**, **Live View**, or **Playback** to enter the Set Permission page.

Your Situation	Solution
	c. (Optional) Enter a remark. d. Tap **OK** to send the application to the customer.
Apply for permissions for multiple devices.	a. Tap **Manage Permission** on the top. b. Select the needed permissions (Configuration, Live View, and Playback) and set the validity periods ((Permanent, 1 Hour, 2 Hours, 4 Hours, or 8 Hours) respectively for different devices. **Note** You can tap **Permission** and **Validity Period** to batch set permissions and validity periods for all devices. c. (Optional) Enter a remark. d. Tap **OK** to send the application to the customer.

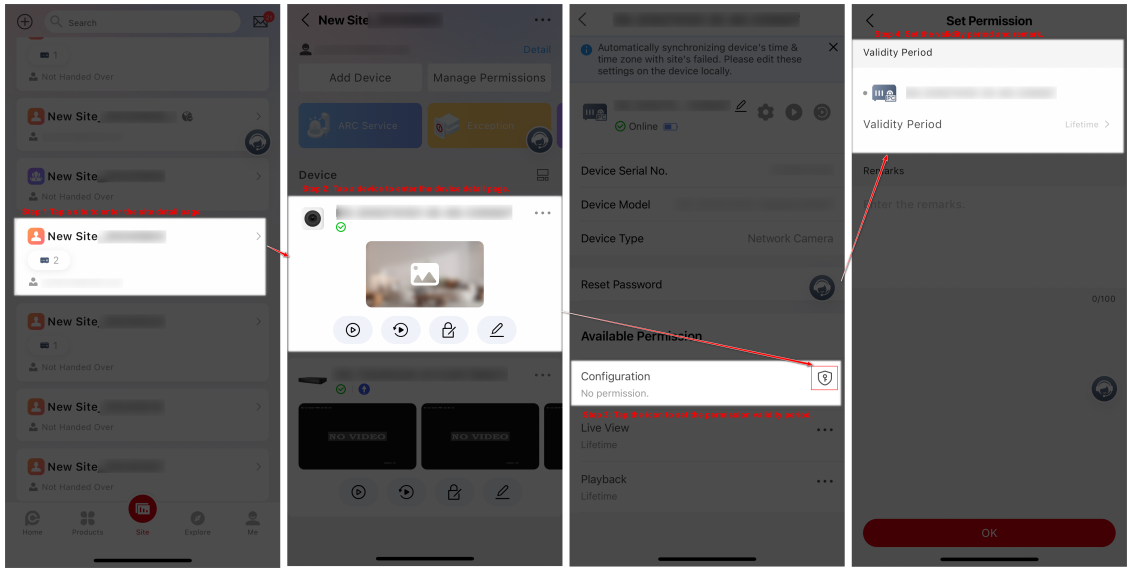


Figure 3-182 Apply for Permission for a Single Device

Release Permission

After being released, the permission will be unavailable for you. You need to apply for it again if needed. You do not have to release permission if the permission validity is **Permanent**.

Steps

1. Tap a site in the site list to enter the site details page.
2. Tap a device on the site details page to enter the device details page.
3. In the Permission area, select a permission, and tap • • • → **Release Permission** → **Release Permission**

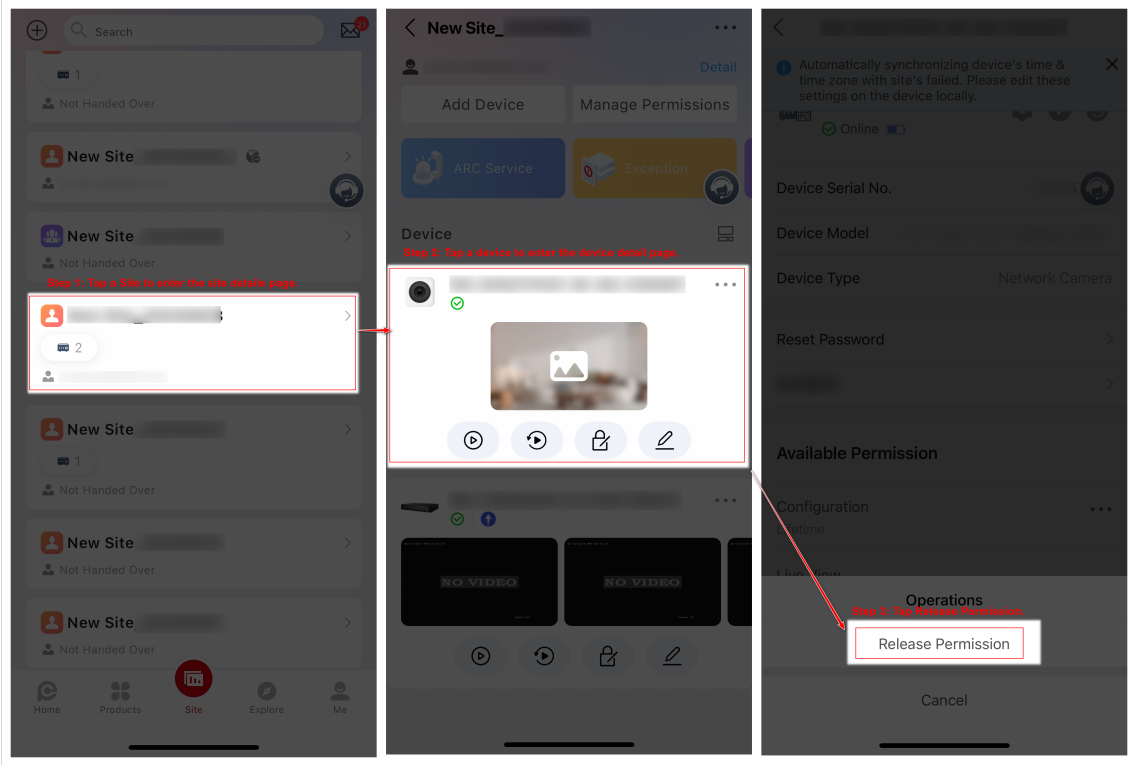


Figure 3-183 Release Permission

3.5 Manage Your Company, Employees, and Service Partners

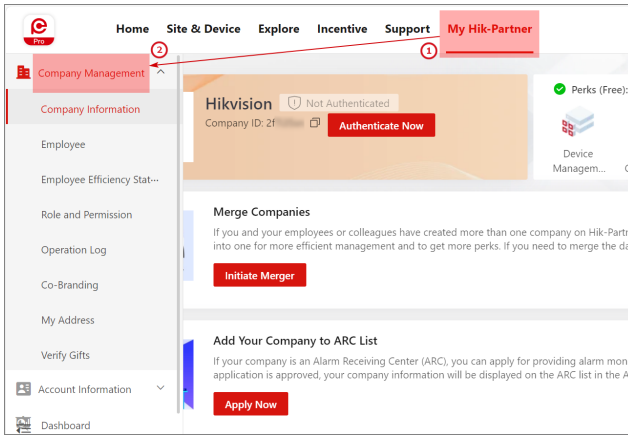


Figure 3-184 Company Management on t Portal

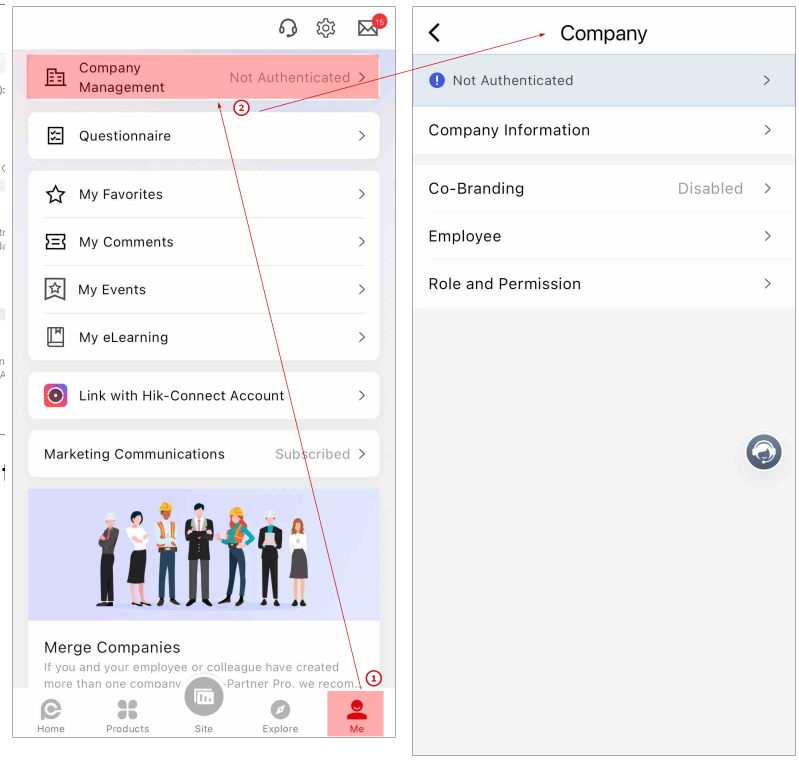


Figure 3-185 Company Management on the Mobile Client

Task	Description
Merge Your Company with Another Company	If you have created more than one Installer Admin account (company) on Hik-Partner Pro, you can merge the companies into one for more efficient management and to carry on your business smoothly (you may have encountered the problem that your second registered account/company cannot be authenticated).
Add Employees to Your Company and Remove Account Limit with Add-On	Add employees to your company, and if you want the employees to be able to manage

Task	Description
	devices, purchase the employee account add-on.
Collaborate with an ISP/MSP on Site for Device Installation or Maintenance	Collaborate with installation and maintenance service partners to add, hand over, and maintain the devices.

3.5.1 Authenticate Company to Use More Features

After Installer Admin registration, you can authenticate your company to purchase value-added services and use more features on Hik-Partner Pro.

You need to fill in all the required fields and submit the online application to authenticate your company. After your application is approved, you will be notified via push notification and email.

Note

The required fields vary depending on your region/country.

Authenticate Your Company Using the Portal

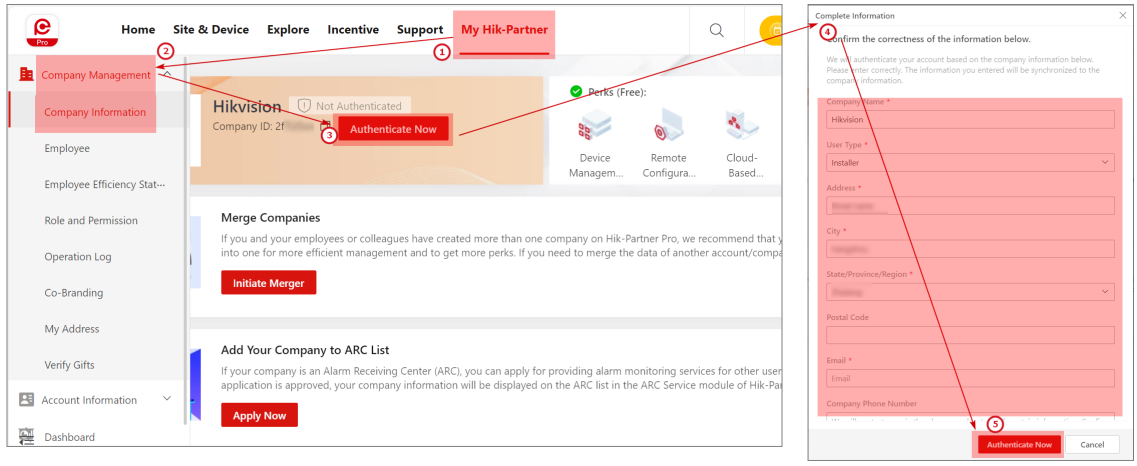


Figure 3-186 Authenticate Your Company Using the Portal

Authenticate Your Company Using the Mobile Client

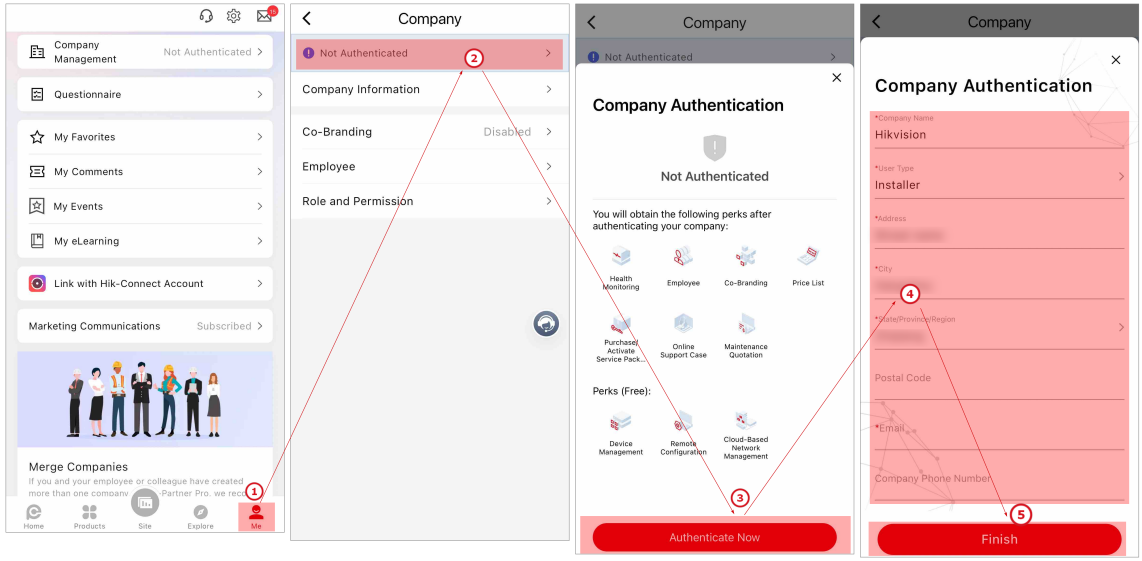


Figure 3-187 Authenticate Your Company Using the Mobile Client

3.5.2 Add Employees to Your Company and Remove Account Limit with Add-On

Step 1: Add Employees: Company Invites Employees or Employees Self-register Accounts

Company Invites Employees Using the Portal

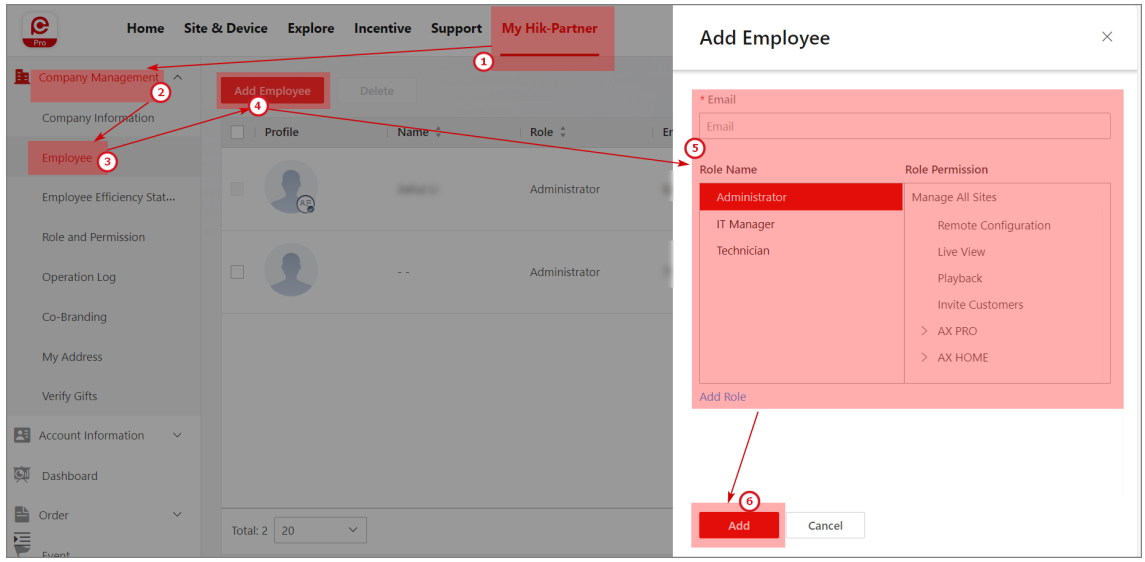


Figure 3-188 Company Invites Employees on the Portal

Company Invites Employees Using the Mobile Client

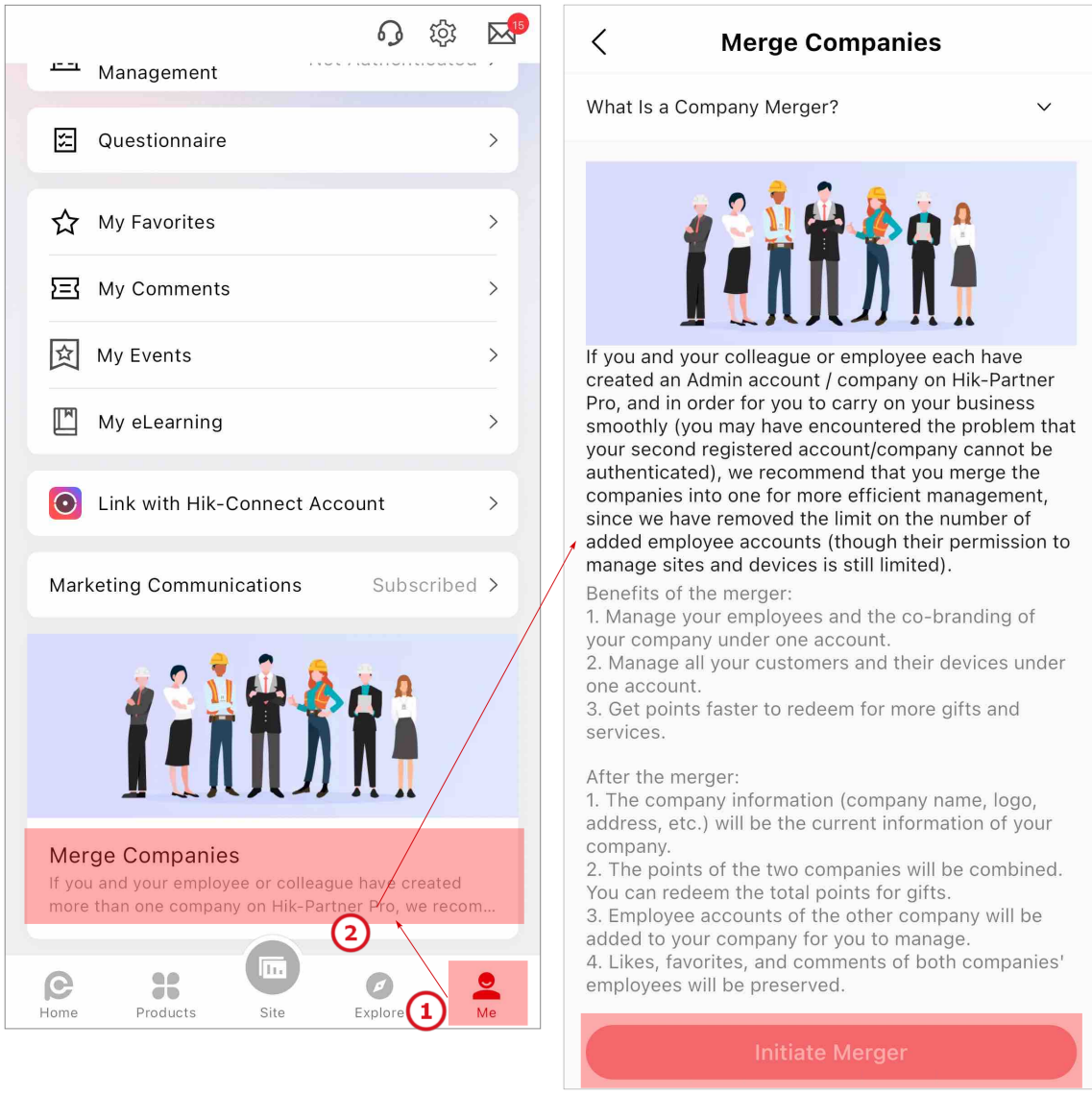


Figure 3-189 Company Invites Employees Using the Mobile Client

Step 2: Employees Accept Registration Invitations or Self-register Accounts

Accept Registration Invitations	After you are invited to register the Installer account, you will receive an email containing the link for registration.
Self-register Accounts Without Invitations	If there are companies with names similar to the company name you enter on the registration page, these companies will be listed, and you can apply to join one of them.

Step 3: (Optional) Add Role and Permissions

Add Role and Permissions Using the Portal

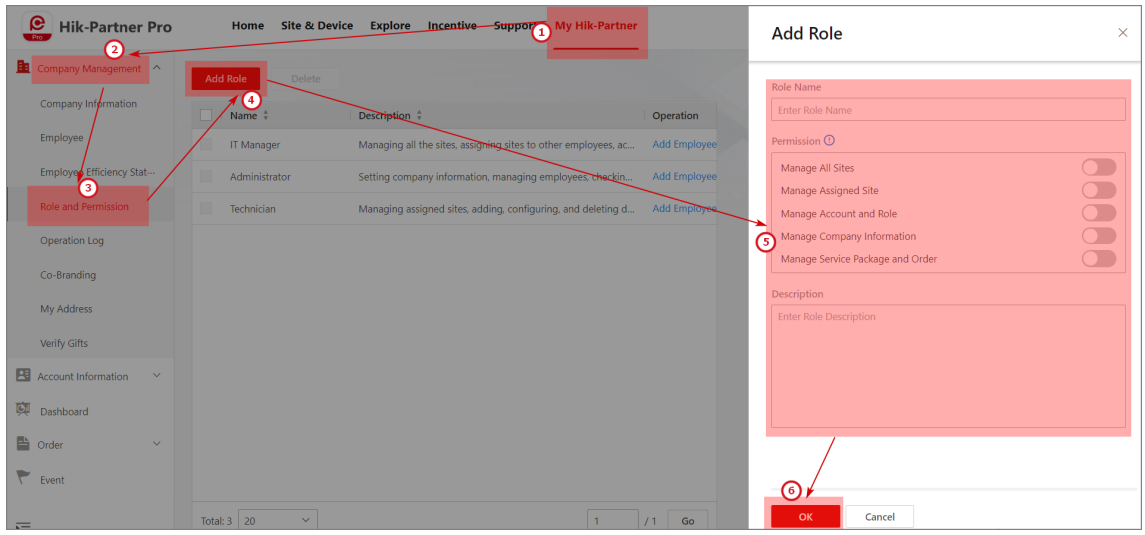


Figure 3-190 Add Role and Permissions Using the Portal

Add Role and Permissions Using the Mobile Client

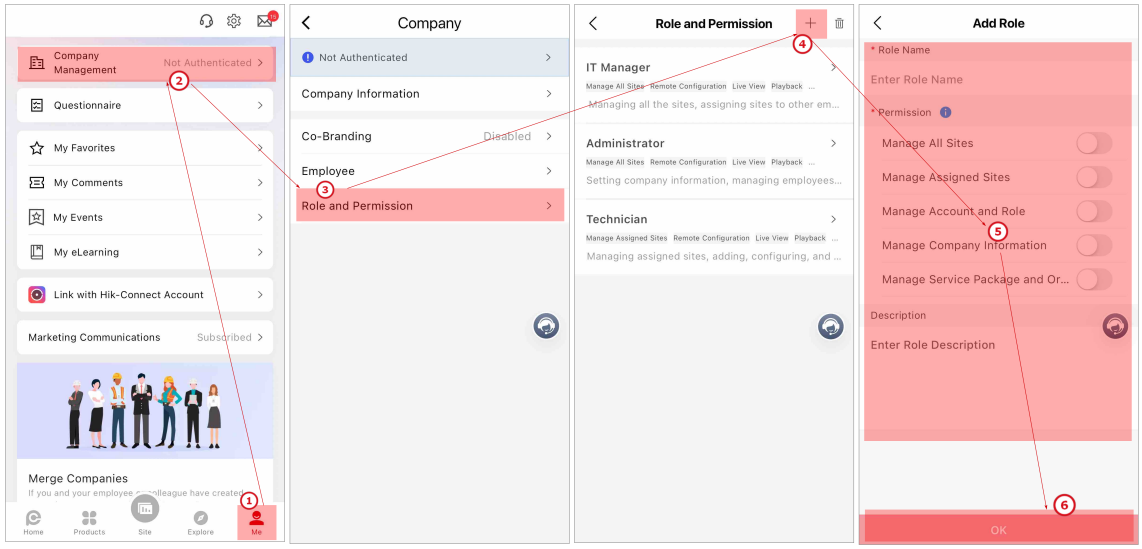


Figure 3-191 Add Role and Permissions Using the Mobile Client

Step 4: (Optional) Purchase Employee Account Add-On

The employee account add-on is for removing the Installer account limit so they can manage sites and devices.

Purchase Method	Description
Purchase Online	Select the item types and quantities, and directly pay for your order online via the Portal or Mobile Client.
Activate by Service Key	Purchase and pay for the items offline at your distributor/dealer, where you get a service key.

Note

Supported purchase methods vary depending on your region/country.

Purchase Employee Account Add-On Using the Portal

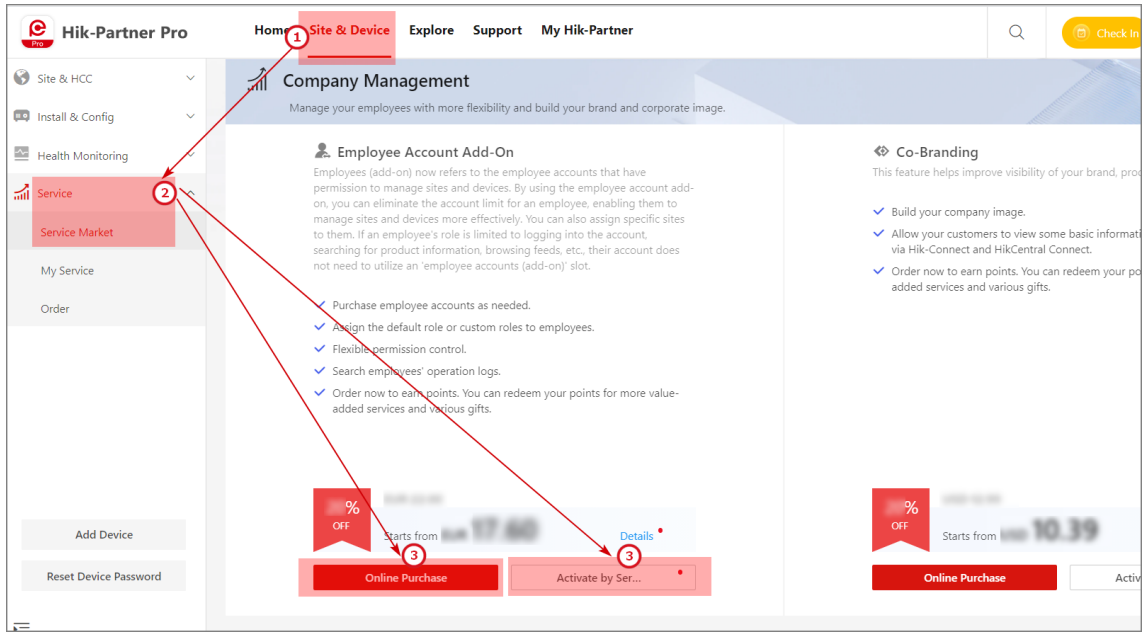


Figure 3-192 Purchase Employee Account Add-On Using the Portal

Purchase Employee Account Add-On Using the Mobile Client

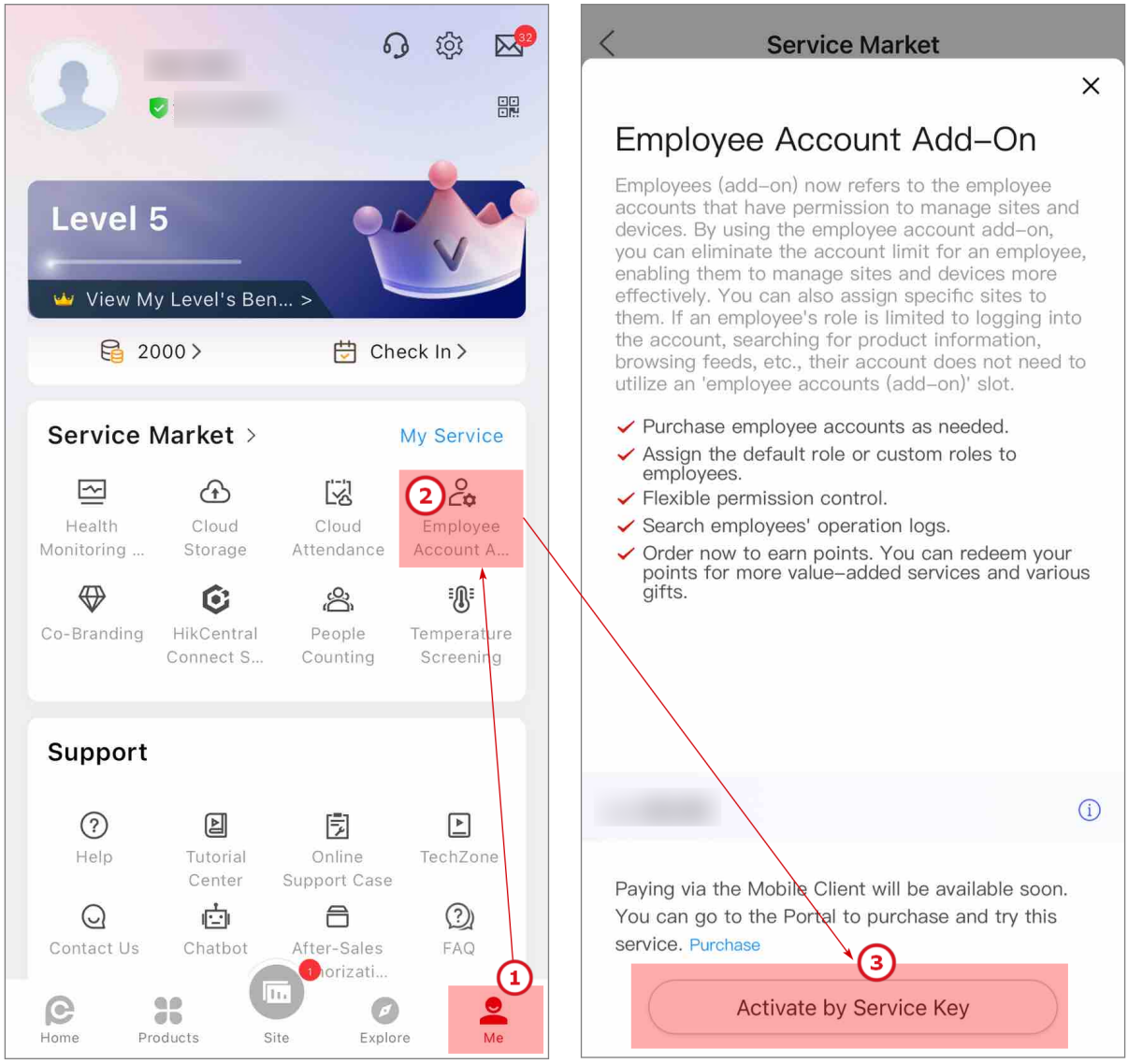


Figure 3-193 Purchase Employee Account Add-On Using the Mobile Client

Step 5: (Optional) Remove Account Limit to Allow Employees to Manage Devices

Note

Remove Account Limit and **Enable Employee Account** are different. The former is to allow the employees to manage the devices, which requires the employee account add-on. The latter is to

allow the employees to log in their accounts, which does not need an 'employee account add-on' slot.

Remove Account Limit Using the Portal

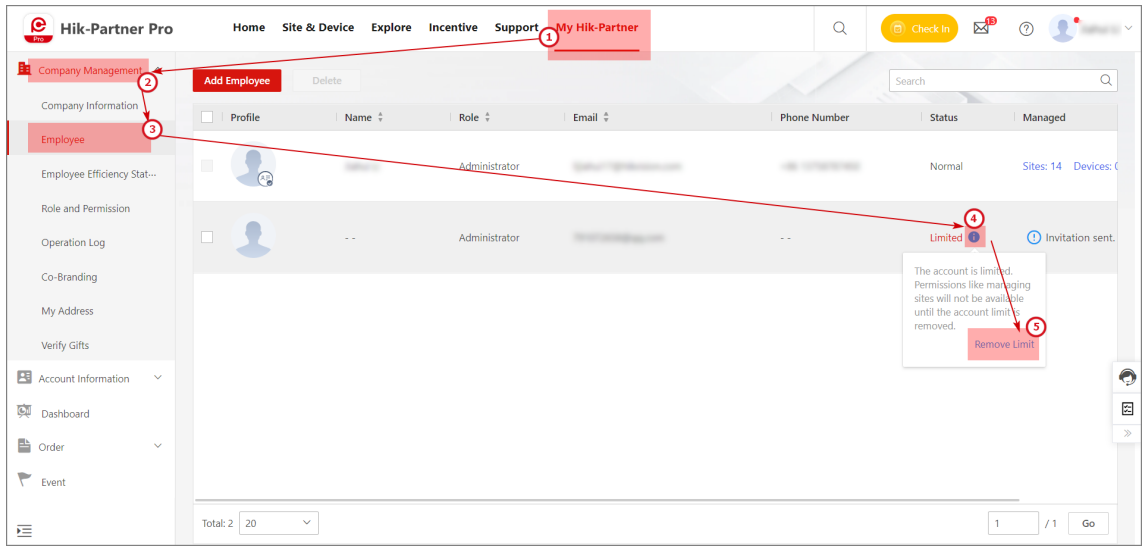


Figure 3-194 Remove Account Limit Using the Portal

Remote Account Limit Using the Mobile Client

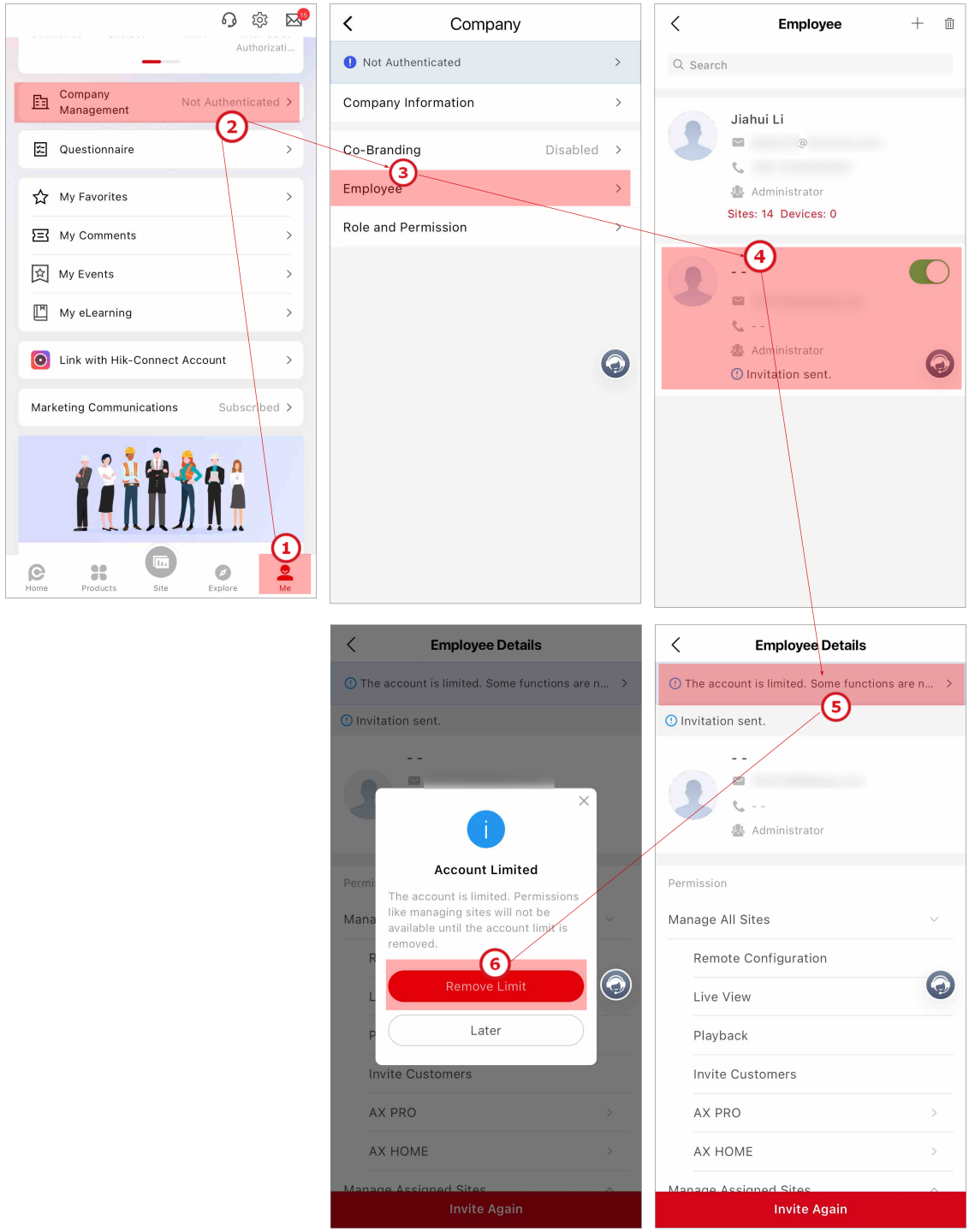


Figure 3-195 Remote Account Limit Using the Mobile Client

3.5.3 How to Configure Azure AD Login and Log In to Hik-Partner Pro via Azure AD

You can configure Azure AD login for auto syncing accounts in your Azure AD, so users can log in to Hik-Partner Pro using the accounts in Azure AD.

Note

- Microsoft has renamed **Azure AD** to **Microsoft Entra ID**.
- This feature is only available in some regions and countries.

Applicable Scenario

- You are using or about to use the Azure AD (Microsoft Entra ID) system, for managing your company's accounts.
- You need to use Hik-Partner Pro to manage your security business and customers' devices, and log in to Hik-Partner Pro using the accounts in your Azure AD. When changes occur to the accounts in your Azure AD (entry and exit of employees), you need it to be auto synced to Hik-Partner Pro.

If you have the above demands, you can configure the Azure AD login in Hik-Partner Pro according to the steps below.

Note

This feature is supported by SAML/SCIM, which is generally considered more secure than OAuth / OpenID Connect of Azure AD B2C.

Table 3-21 Overall Process of Azure AD Login Configuration

Steps	Instructions
1. Create your enterprise application in Azure AD.	***Step 1: Create an Enterprise Application in Azure AD***
2. Configure SAML SSO.	***Step 2: Configure SAML SSO***
3. Configure Accounts Sync (SCIM)	• ***Step 3: Configure Accounts Sync*** • ***Limitations***
4. Log in to Hik-Partner Pro using the accounts in Azure AD.	***Step 4: Log In to Hik-Partner Pro Using Accounts Synced from Azure AD***

Step 1: Create an Enterprise Application in Azure AD

1. Log in to Azure AD, select **Enterprise applications**
   .

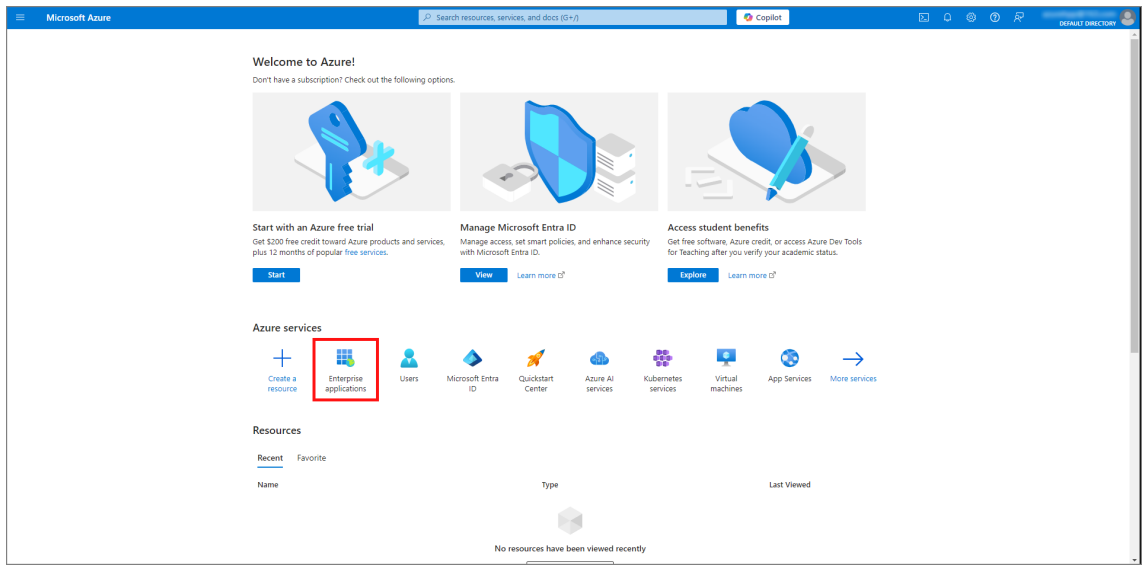


Figure 3-196 Enterprise applications

2. Click **New application**.

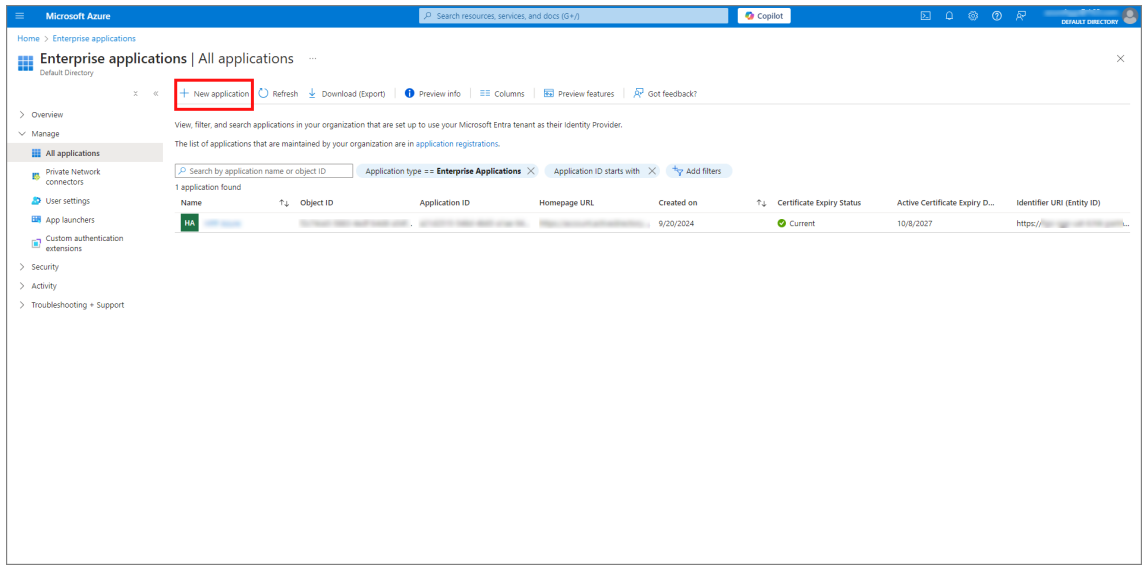


Figure 3-197 New application

3. Click **Create your own application**.
4. Set the name of your app, select **Integrate any other application you don't find in the gallery (Non-gallery)**, and click **Create**.

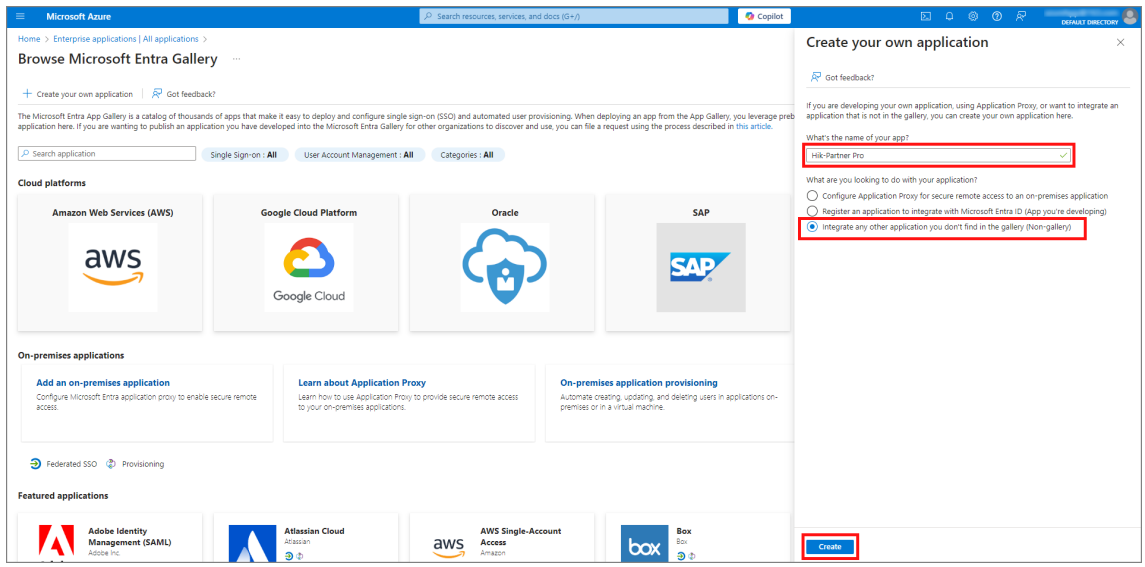


Figure 3-198 Create your own application

Step 2: Configure SAML SSO

1. Enter the enterprise application you create, select **Set up single sign on**.

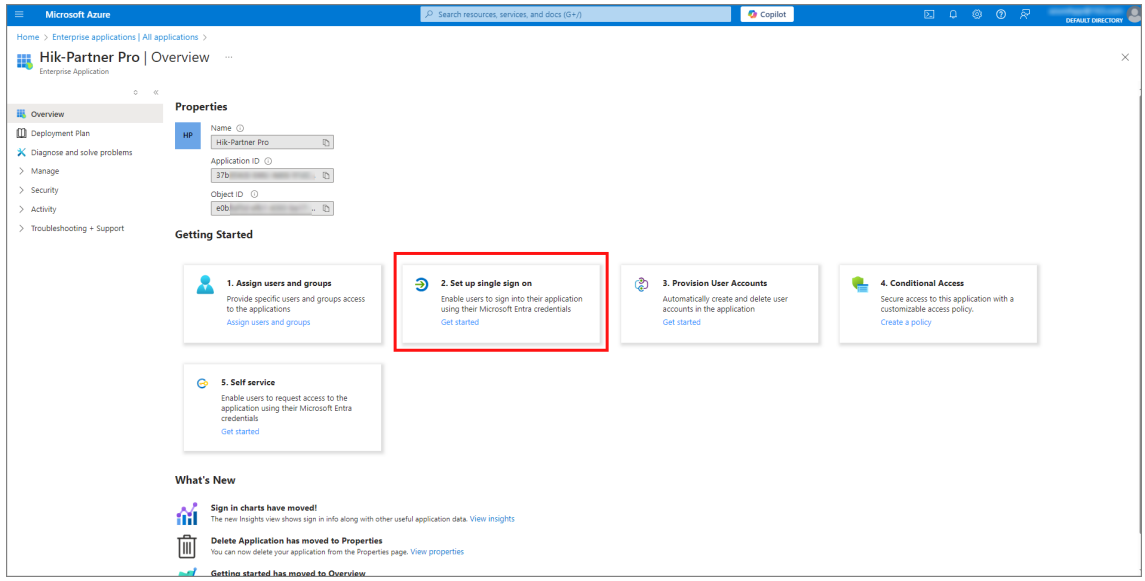


Figure 3-199 Set up single sign on

2. Select **SAML** as the single sign-on method.

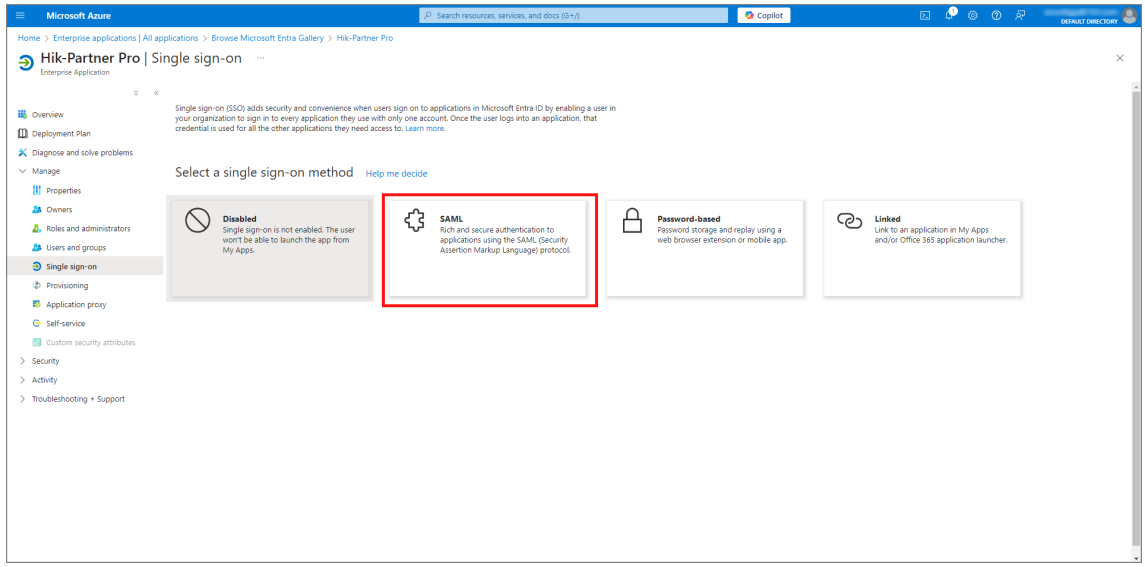


Figure 3-200 SAML Method

3. Set up the single sign on.
   a. Log in to the Hik-Partner Pro Portal, go to **My Hik-Partner → Company Management → Azure AD Login** , and click **Configure**.

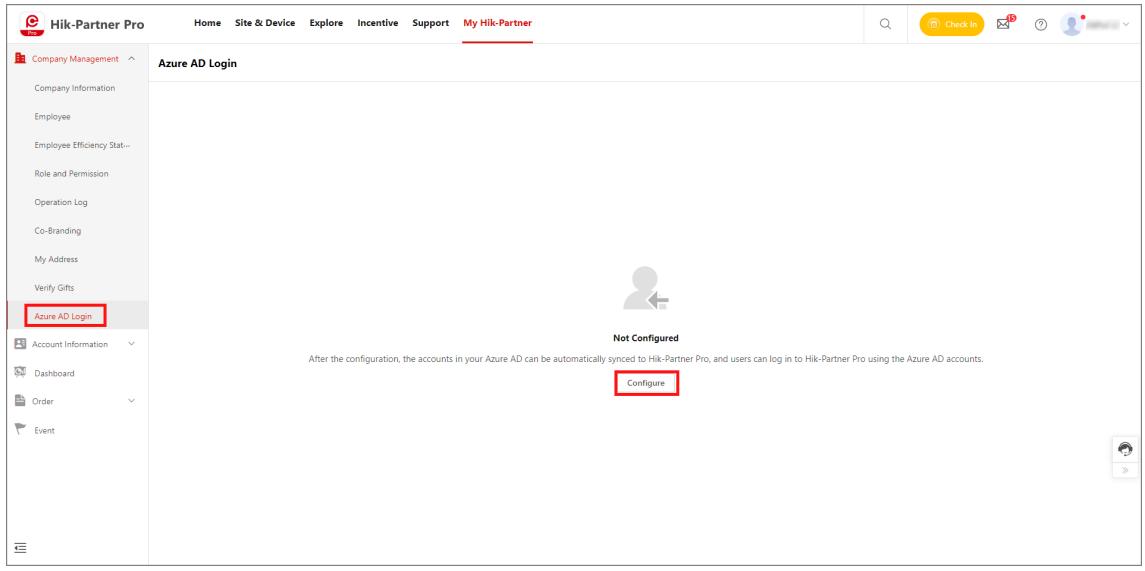


Figure 3-201 Azure AD Login Configuration on Hik-Partner Pro

   b. Click to copy the **Entity ID** and **Reply URL**.

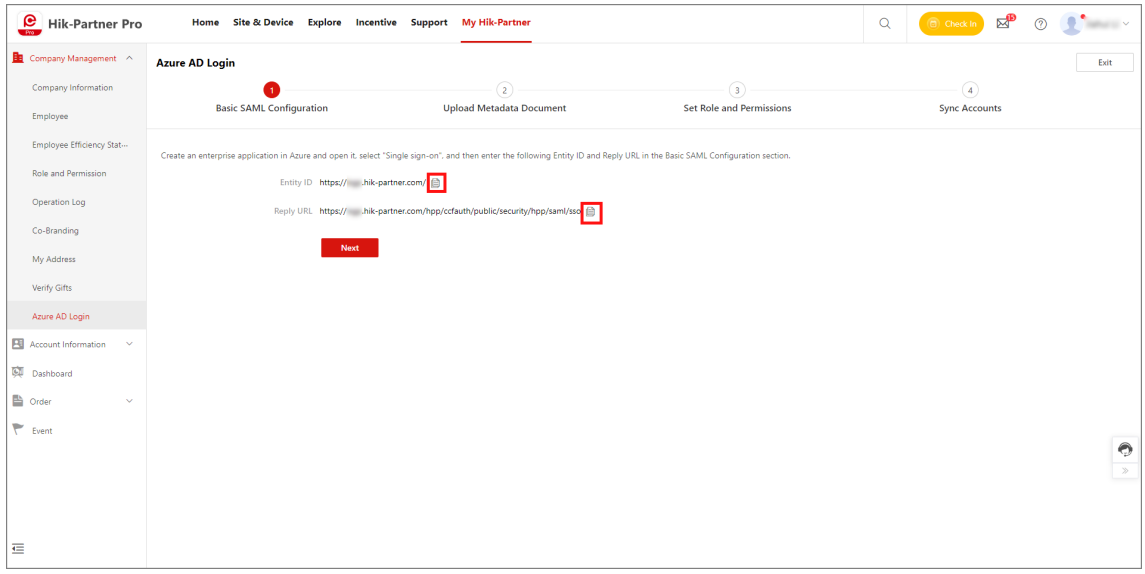


Figure 3-202 Copy Entity ID and Reply URL

c. Enter the **Entity ID** and **Reply URL** to the **Basic SAML Configuration**. Click **Save**.

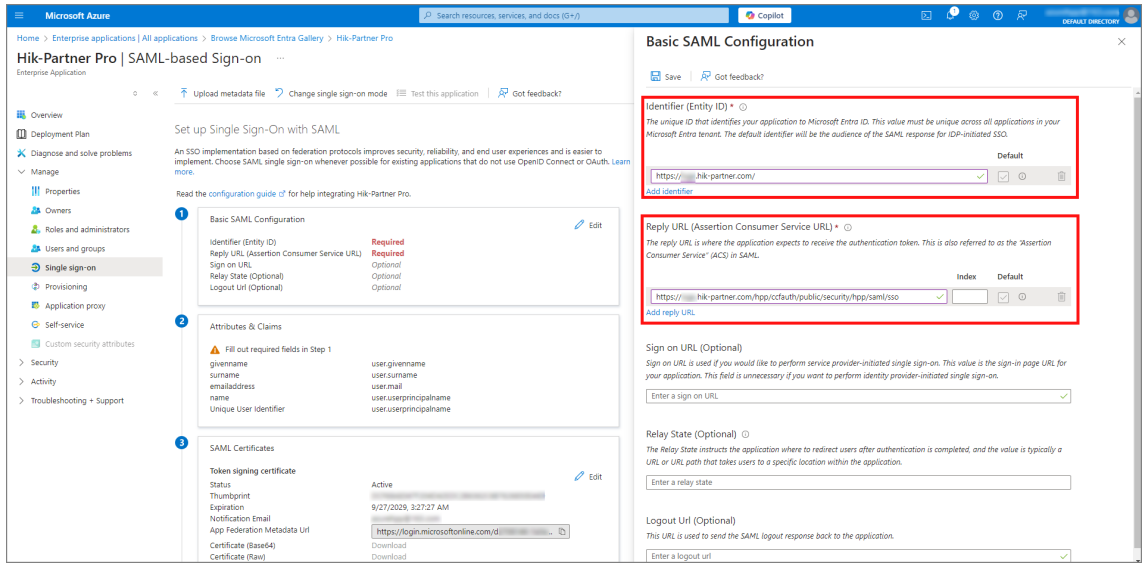


Figure 3-203 Enter Entity ID and Reply URL in Basic SAML Configuration

4. Download the federation metadata XML document from Azure AD, and upload it to Hik-Partner Pro.
   a. Click **Download** to download the federation metadata XML document on the **SAML-based Sign-on** page.

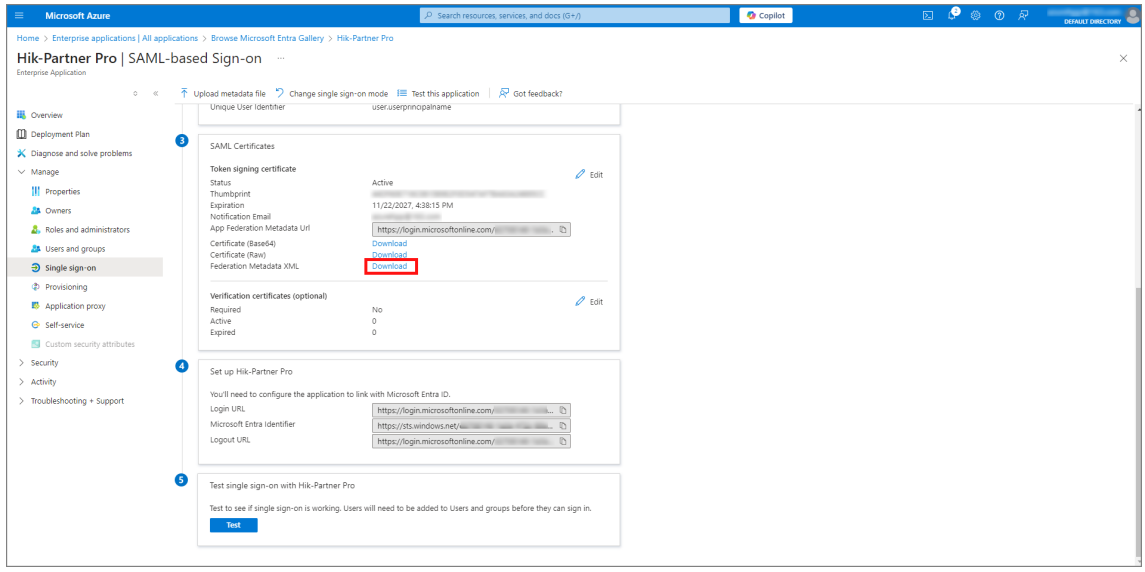


Figure 3-204 Download metadata XML

b. Go back to Hik-Partner Pro, click **Next** to go to the step **Upload Metadata Document**, and click **Upload** to upload the downloaded XML file.

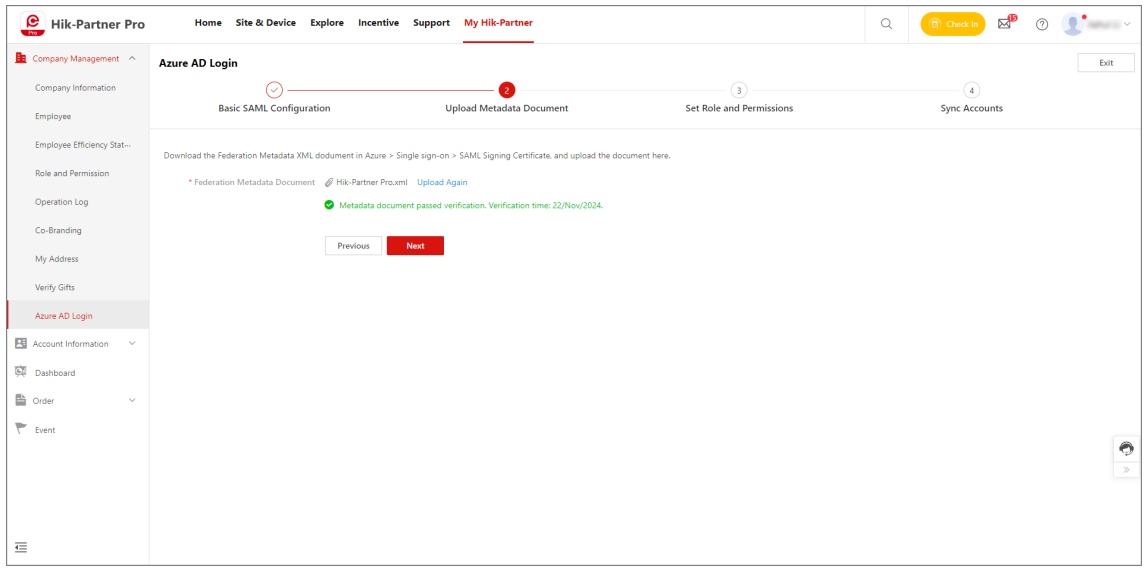


Figure 3-205 Upload

Step 3: Configure Accounts Sync

1. Go back to Hik-Partner Pro, click **Next** to go to the step **Set Role and Permissions**. Select a default role for accounts synced from Azure AD, which you can go back here later to modify.

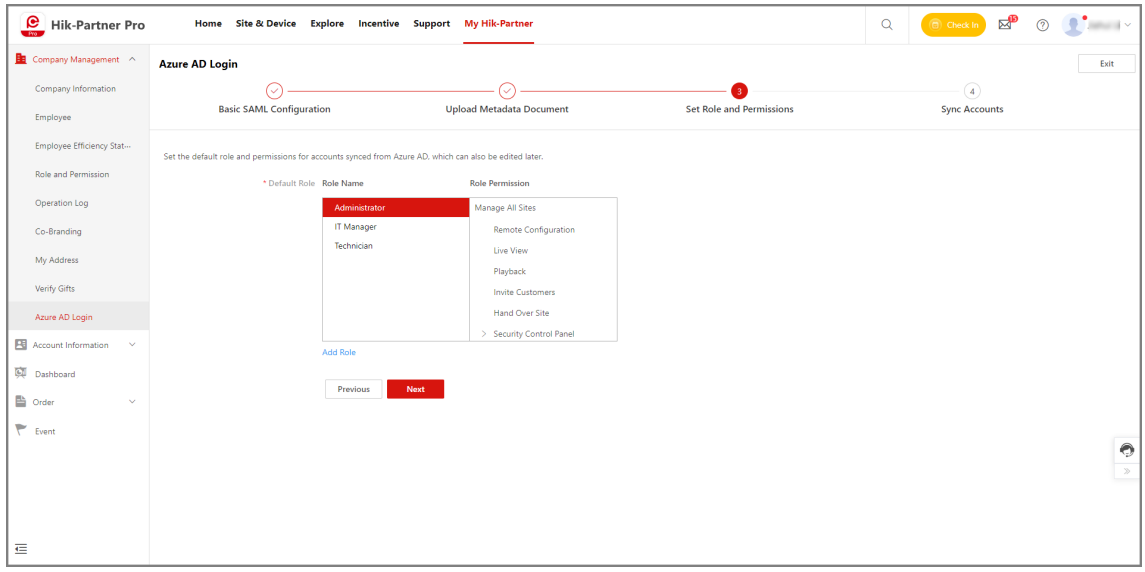


Figure 3-206 Set Role and Permissions

2. Configure accounts sync.
   a. Click **Next** to go to the step **Sync Accounts**, and click to copy the **Secret Token** and **Tenant URL**.

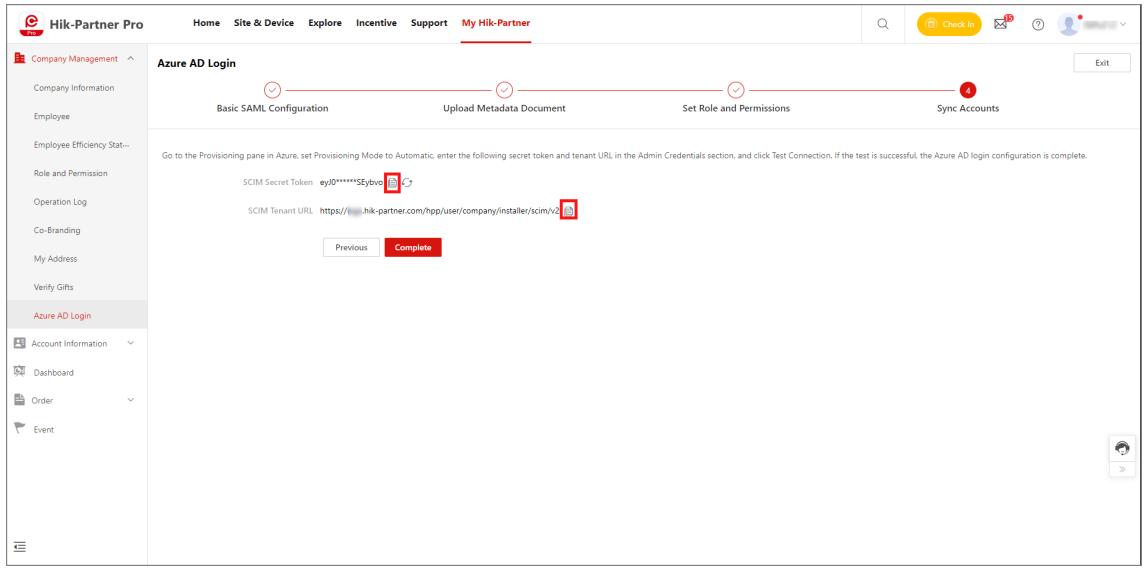


Figure 3-207 Sync Accounts

   b. Go back to Microsoft Azure, select **Provisioning**. Set the **Provisioning Mode** to **Automatic**, and enter the copied **Tenant URL** and **Secret Token** in the **Admin Credentials** section.

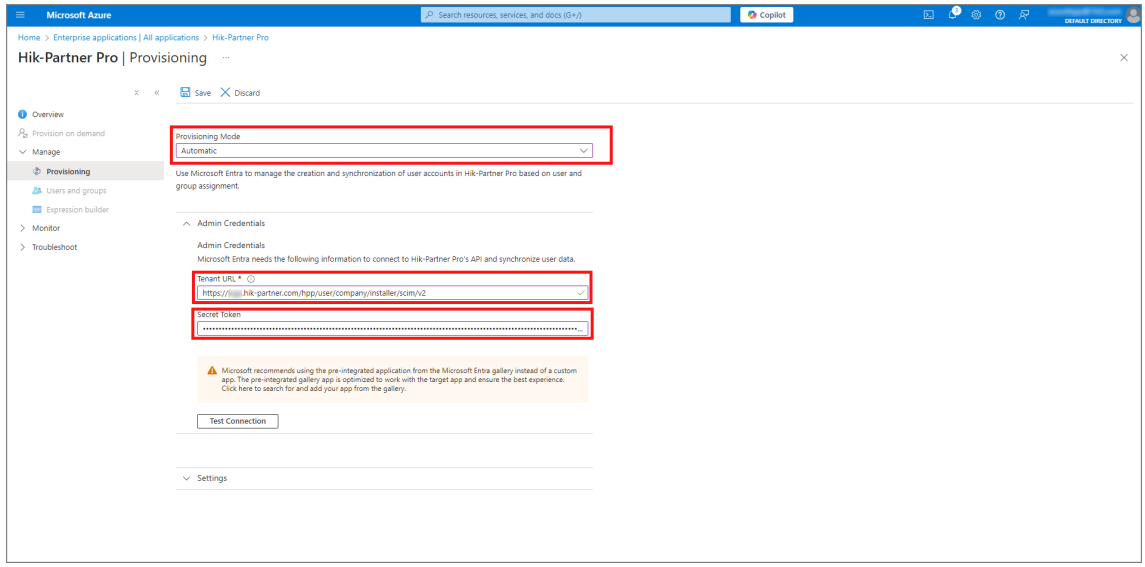


Figure 3-208 Provisioning

c. Click **Test Connection** and wait for the successful prompt.

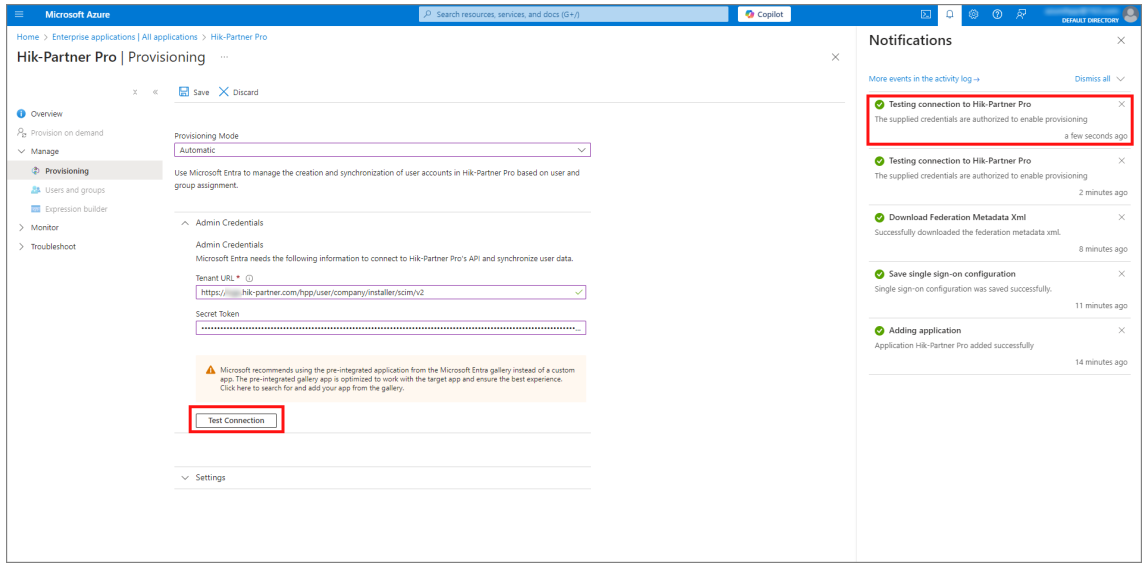


Figure 3-209 Test Connection

d. Click **Save**. Go to the **Overview** page, and click **Start provisioning**.

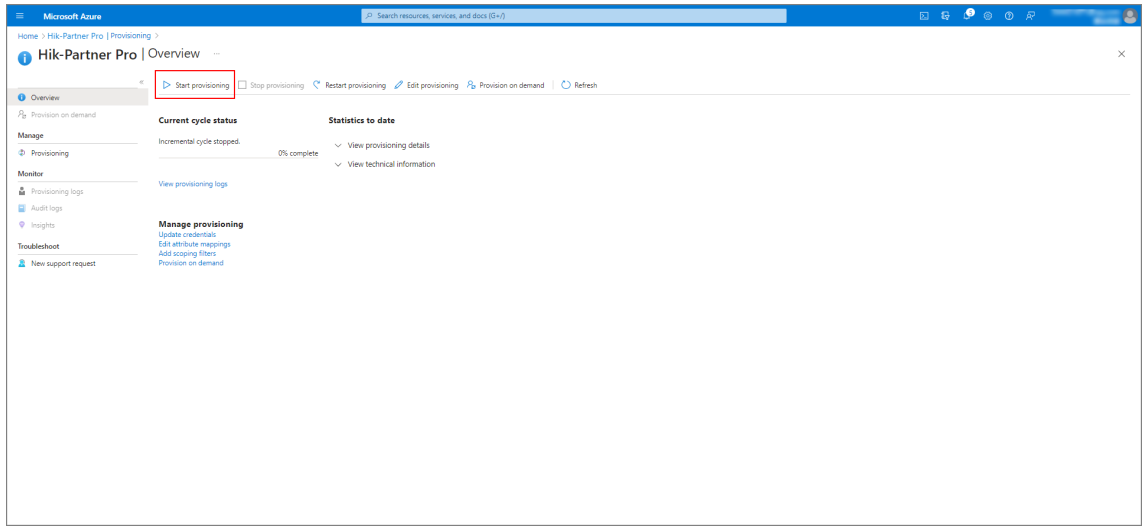


Figure 3-210 Start provisioning

3. Go back to Hik-Partner Pro, click **Complete** to finish the configuration.
4. You can select **Users and Groups → Add user/group** to add the accounts that need to log in to Hik-Partner Pro to the enterprise application in Azure AD according to your needs. These accounts come from your existing Azure AD tenant.

Note

Azure AD will sync the newly added accounts to Hik-Partner Pro in 40 minutes. To check the sync details, go to **Provisioning → View provisioning logs** .

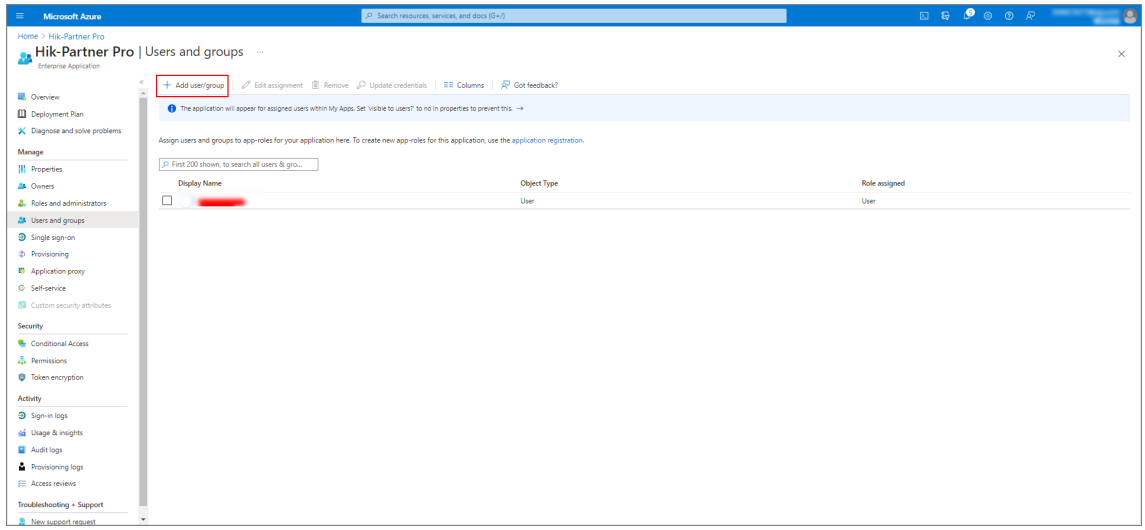


Figure 3-211 Add User

5. If you have added user groups in your Azure, to sync the users successfully:

a. Select **Attribute mapping (Preview)**, and disable **Provision Microsoft Entra ID Groups**. (Make sure the **Enabled** column is **No**.)

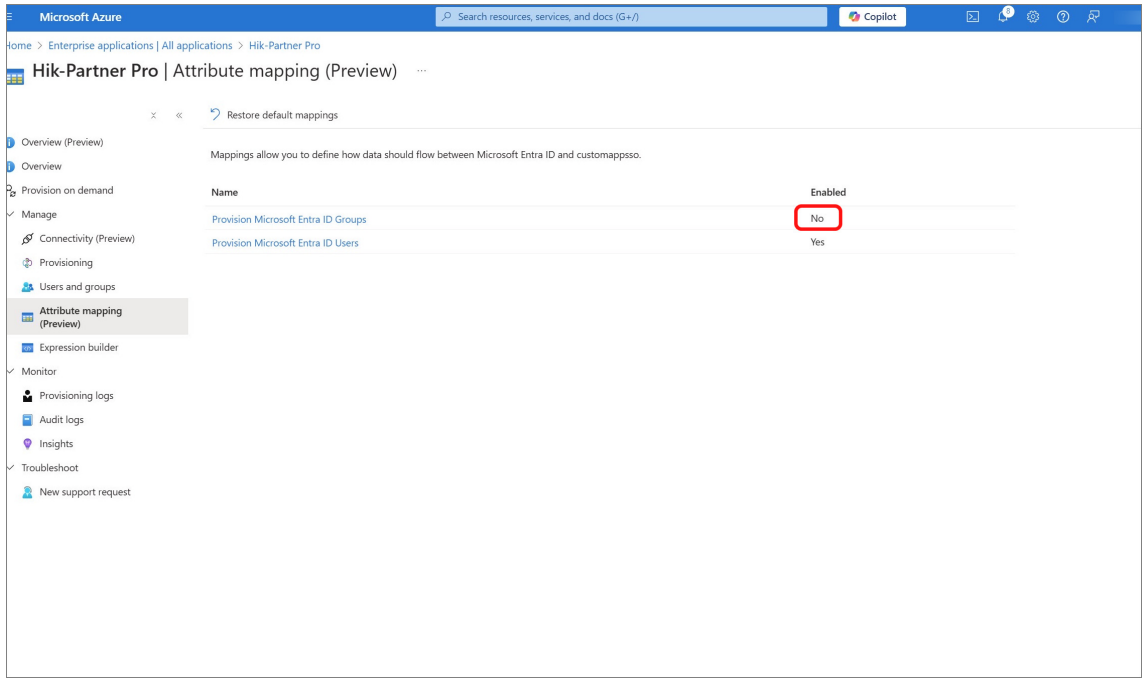


Figure 3-212 Disable Provision Microsoft Entra ID Groups

b. Select **Provisioning**, and click **Restart provisioning**.

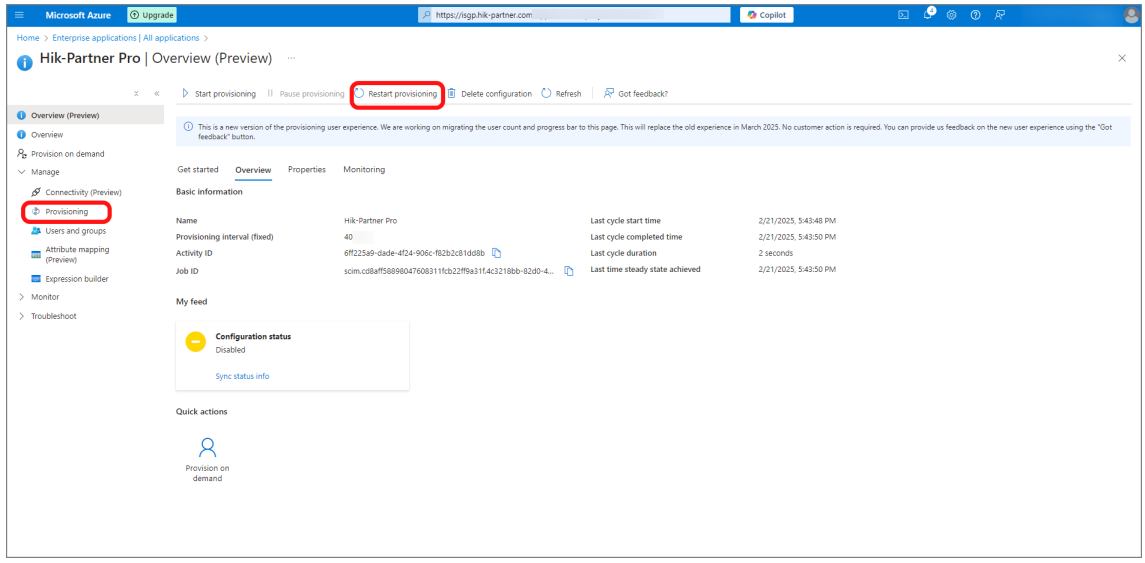


Figure 3-213 Restart Provisioning

6. Go to the **Employee** page of Hik-Partner Pro to check the synced accounts. The synced accounts will be marked with the icon .

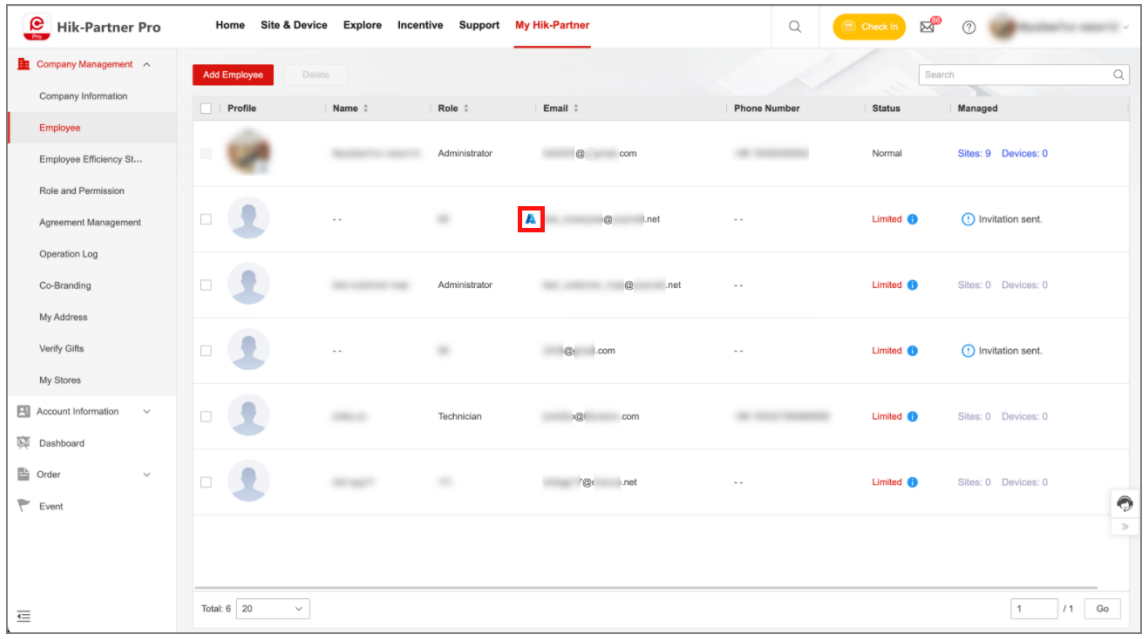


Figure 3-214 Synced Accounts

Step 4: Log In to Hik-Partner Pro Using Accounts Synced from Azure AD

1. Go to the Hik-Partner Pro Portal or Mobile Client, select **Log In via Azure AD**.
2. Enter the account (email) and select **Next**. You will be redirected to the login page of Microsoft Azure.

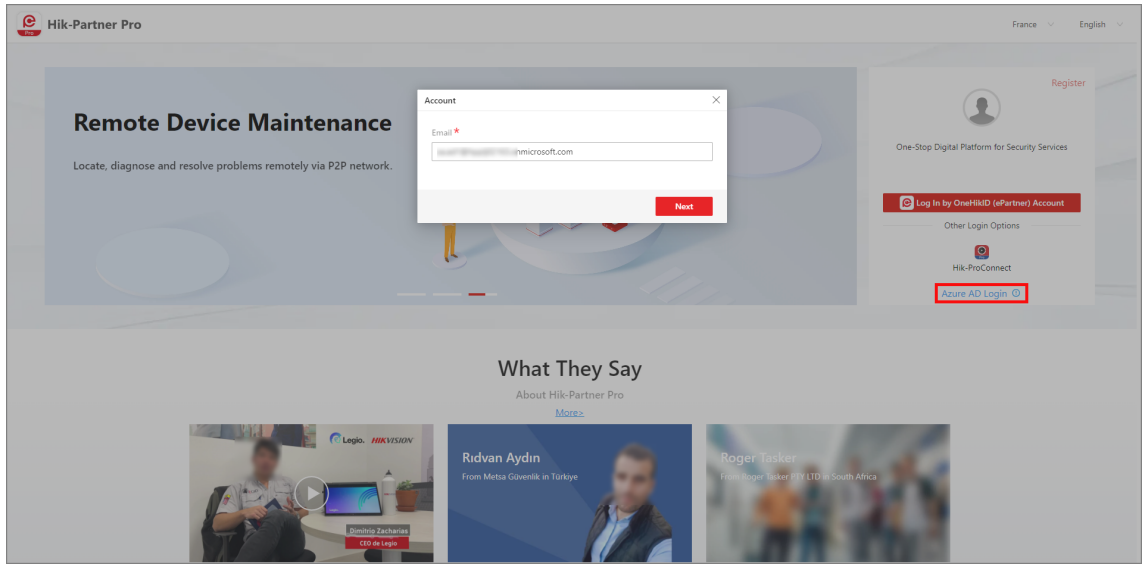


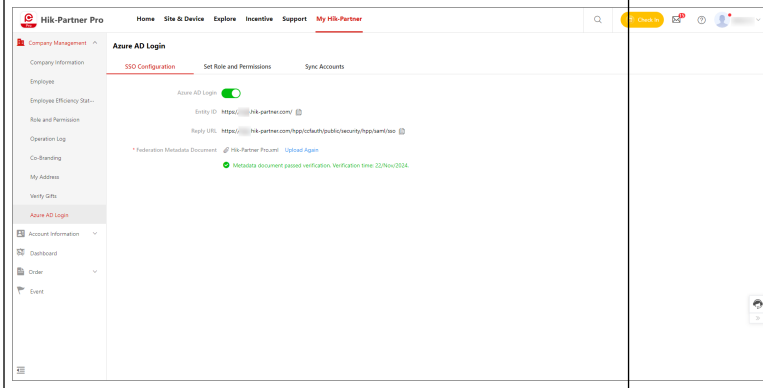
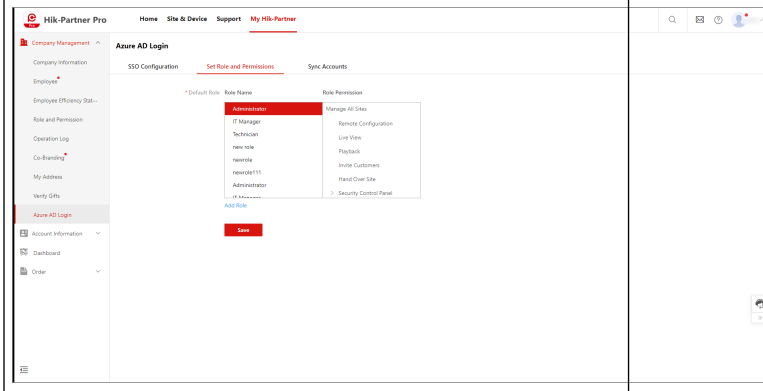
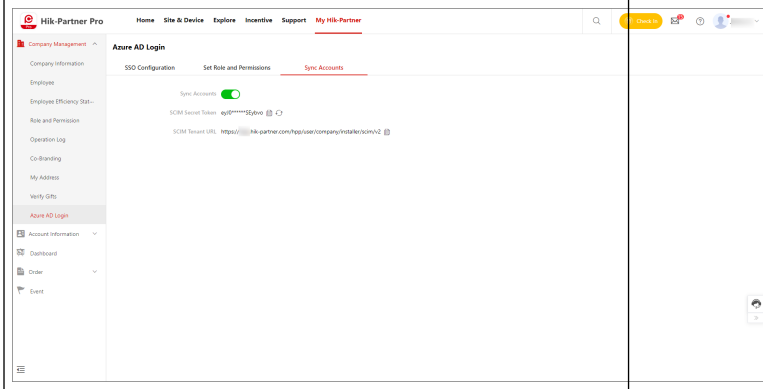
Figure 3-215 Login

3. Enter the password, and select **Sign in**. If verification passed, you will log in to and enter Hik-Partner Pro.

(Optional) Step 5: Modify Azure AD Login Settings

After you complete the Azure AD login configuration, you can also disable Azure AD Login, modify the default role of synced accounts, and disable account login.

1. Go to the Hik-Partner Pro Portal, select **My Hik-Partner → Company Management → Azure AD Login** .
2. The following modifications are available.

Available Operations	Tab
- Turn off **Azure AD Login** to make users unable to log in using the synced accounts. - Upload the metadata XML file again if any changes made.	
Modify the default role for the synced accounts (that are synced from Azure AD after the role modification).	
Turn off **Sync Accounts** to stop syncing any more new accounts from Azure AD.	

Limitations

- A single Azure AD tenant can only be uniquely bound to one Hik-Partner Pro company (i.e., one Installer Admin account).
- Currently, only work/school accounts in Azure AD are supported for synchronization to Hik-Partner Pro. Guest/personal accounts are not supported for logging in to Hik-Partner Pro.

Related FAQ

Q: Why are my Azure AD accounts not synced to Hik-Partner Pro?

A:

Possible Causes:

1. You have added user groups in your Azure, which causes failure when you sync accounts to Hik-Partner Pro.
2. It generally takes about 40 minutes for Azure AD to sync the newly added accounts.

Troubleshooting Steps:

1. If you have added user groups in your Azure, to sync the users successfully:
   a. Select **Attribute mapping (Preview)**, and disable **Provision Microsoft Entra ID Groups**. (Make sure the **Enabled** column is **No**.)

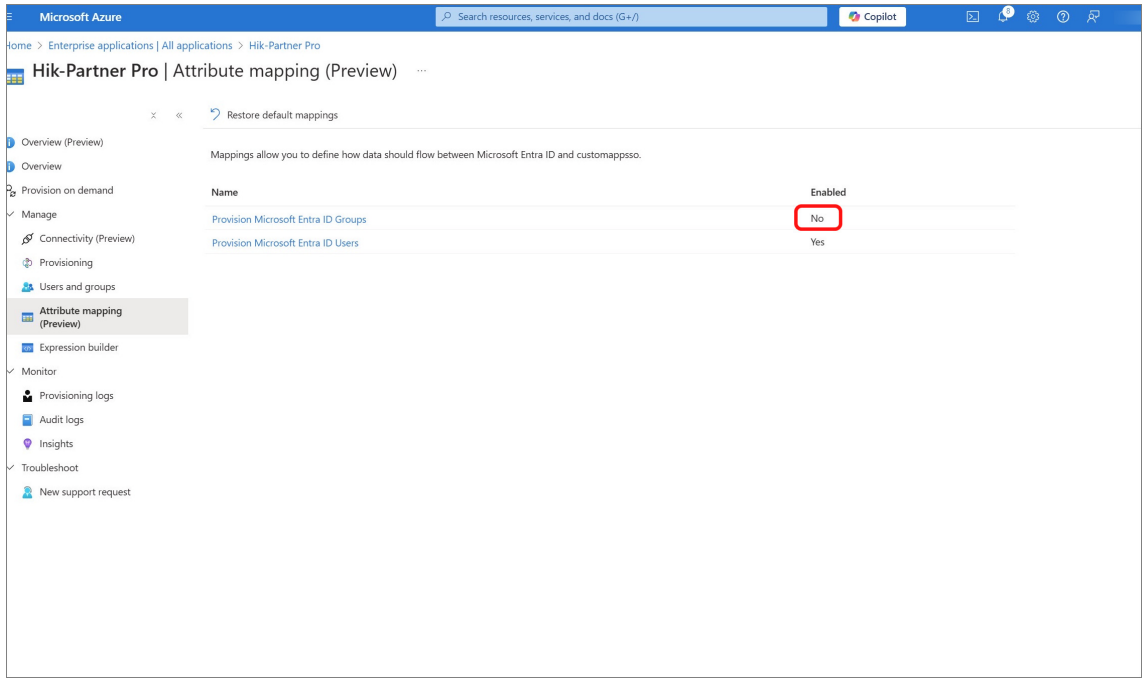


Figure 3-216 Disable Provision Microsoft Entra ID Groups

   b. Select **Provisioning**, and click **Restart provisioning**.

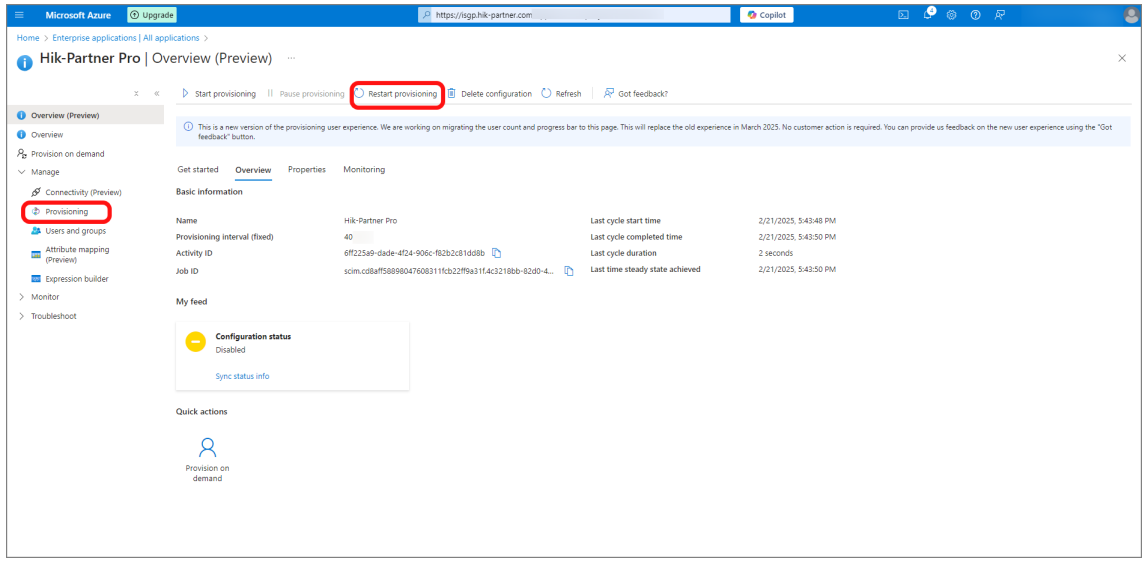


Figure 3-217 Restart Provisioning

2. Azure AD will generally sync the newly added accounts to Hik-Partner Pro in 40 minutes. Wait for 40 minutes, and to check the sync details, go to **Provisioning → View provisioning logs** .

Q: What type of Azure AD accounts can be synced?

A:Currently, only work/school accounts in Azure AD are supported for synchronization to Hik-Partner Pro. Guest/personal accounts are not supported for logging in to Hik-Partner Pro.

3.5.4 How to Configure Google Workspace Login and Log In to Hik-Partner Pro via Google Workspace

You can configure Google Workspace login for auto syncing accounts in your Google Workspace, so users can log in to Hik-Partner Pro using the accounts in Google Workspace.

Applicable Scenario

- You are using or about to use the Google Workspace system, for managing your company's accounts.
- You need to use Hik-Partner Pro to manage your security business and customers' devices, and log in to Hik-Partner Pro using the accounts in your Google Workspace.

If you have the above demands, you can configure the Google Workspace login in Hik-Partner Pro according to the steps below.

Note

This feature is supported by SAML/SCIM, which is generally considered more secure.

Table 3-22 Overall Process of Google Workspace Configuration and Login

Your Role	Related Instructions
Company Administrator Who Needs to Configure Google Workspace Login Account Type: Installer Admin / Google Workspace Admin	• ***Step 1: Add a Custom SAML App in Google Workspace Admin Console*** • ***Step 2: Upload Metadata Document to Hik-Partner Pro*** • ***Step 3: Set Role and Permissions and Complete Configuration*** • ***Step 4: Log In to Hik-Partner Pro Using Accounts Synced from Google Workspace*** • ***(Optional) Step 5: Modify Google Workspace Login Settings*** • ***Limitations***
Employees Account Type: Installer Accounts / Employee Accounts	***Step 4: Log In to Hik-Partner Pro Using Accounts Synced from Google Workspace***

Step 1: Add a Custom SAML App in Google Workspace Admin Console

1. Go to ***admin.google.com*** , log in to the Admin console of your Google Workspace. One the left navigation pane, select **Apps → Web and mobile apps** , and then click **Add app → Add custom SAML app** .
   .

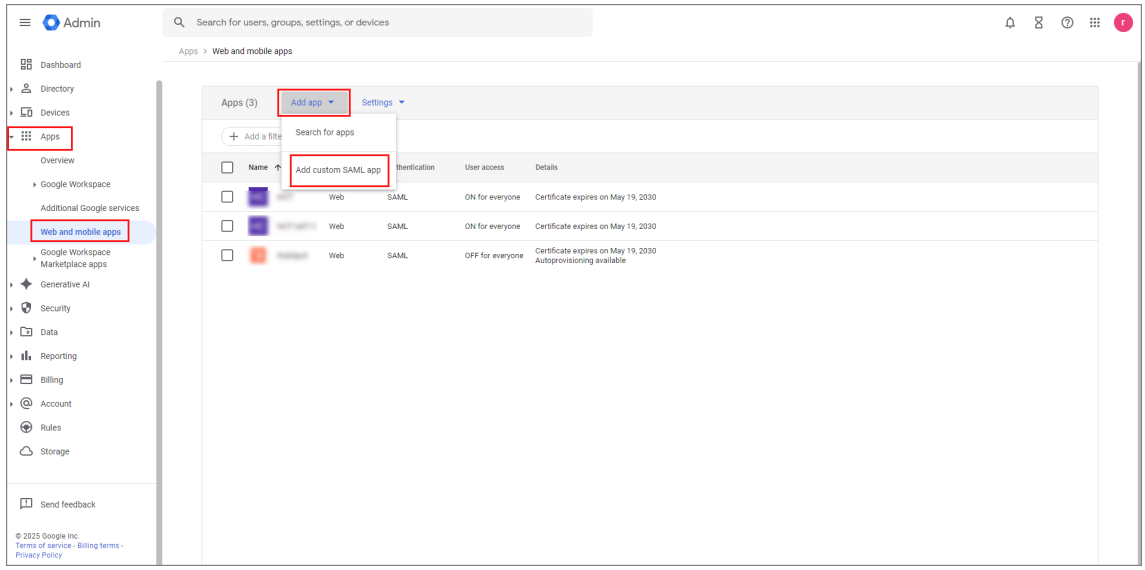


Figure 3-218 Add Custom SAML App

2. Set the name of your app, enter the description, and upload an icon if needed. Click **Continue**.

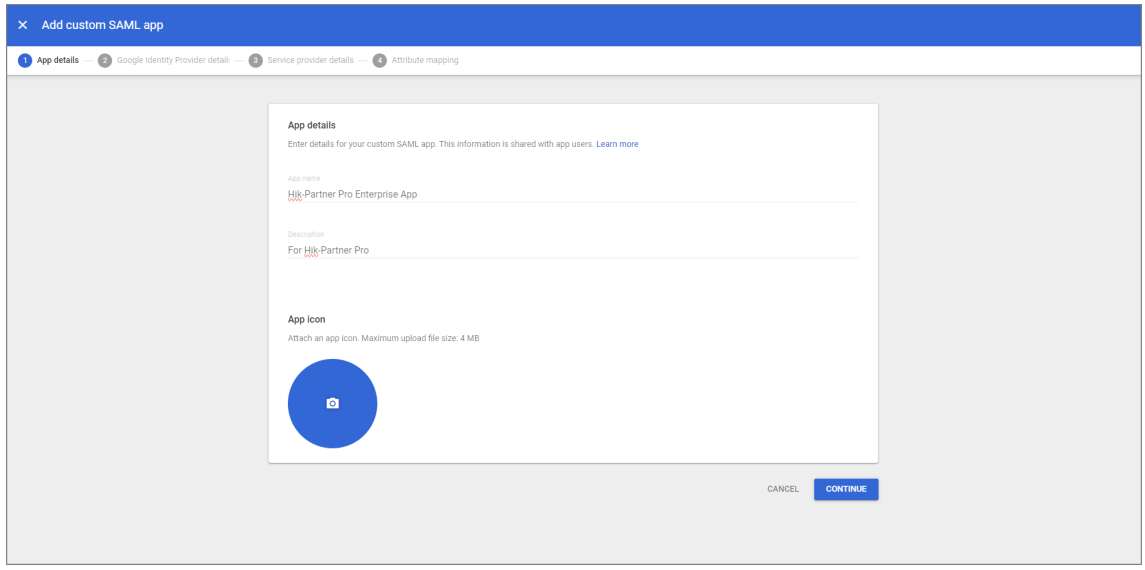


Figure 3-219 Add Custom SAML App (App Details)

3. On the **Google Identity Provider details** page, click **DOWNLOAD METADATA** to download the metadata document to your PC (which should be upload to Hik-Partner Pro later). Click **Continue**.

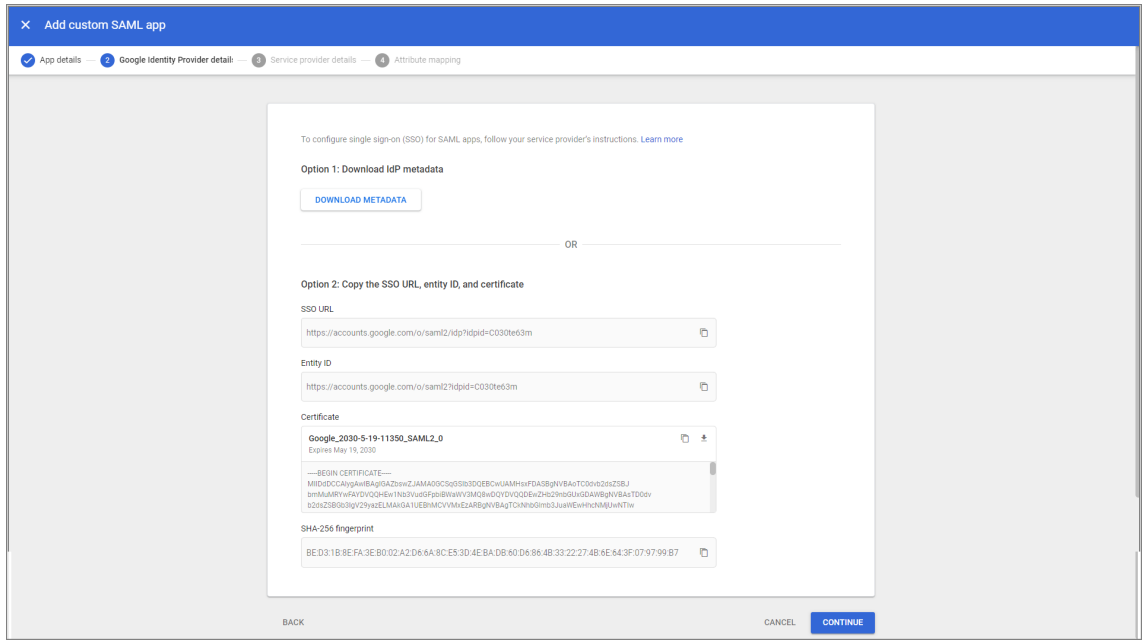


Figure 3-220 Download the Metadata Document

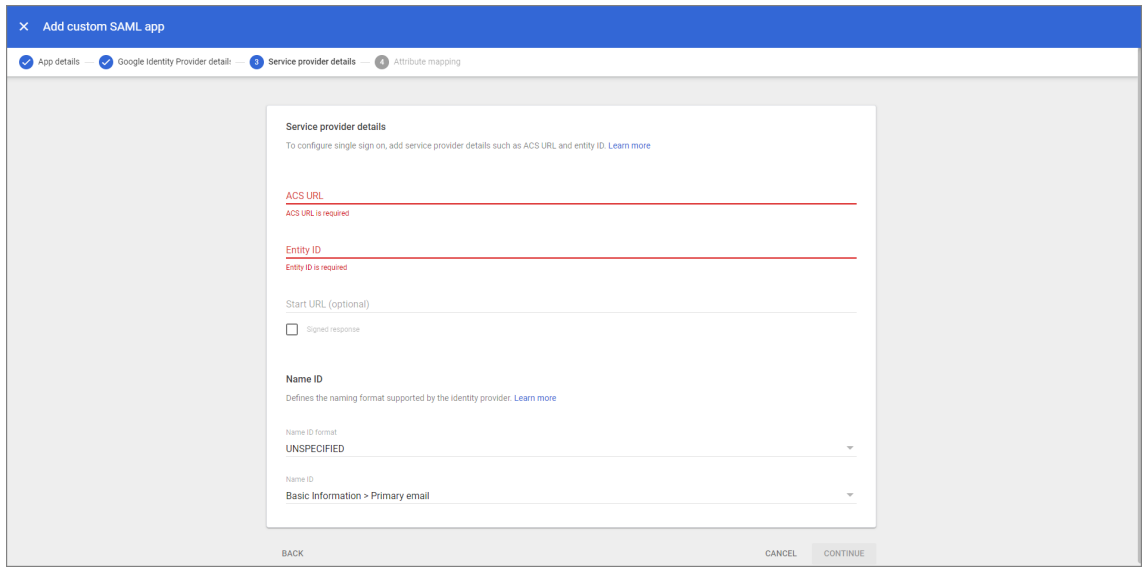


Figure 3-221 Service Provider Details (ACS URL and Entity ID Required)

4. On the **Service provider details** page, to configure single sign on, add ACS URL and entity ID which you should copy from Hik-Partner Pro.
   a. Log in to the Hik-Partner Pro Portal, go to **My Hik-Partner → Company Management → Third-Party Authentication Configuration** , and click **Google Workspace**.

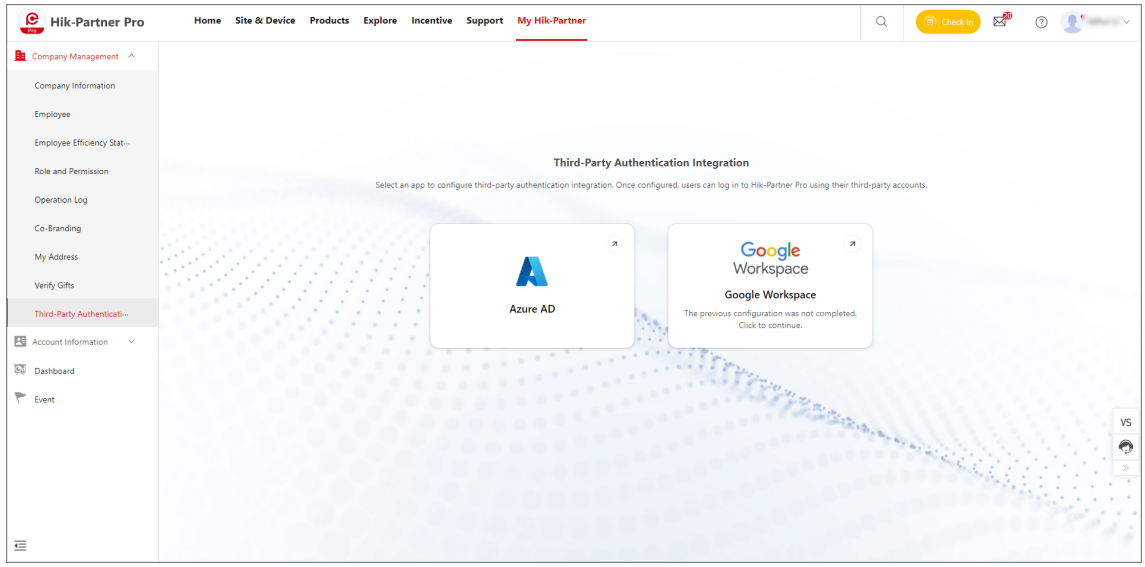


Figure 3-222 Google Workspace Login Config in Hik-Partner Pro

b. Click to copy the **Entity ID** and **Reply URL** (ACS URL) from Hik-Partner Pro, and paste into the **Service provider details** page in Google Workspace Admin Console.

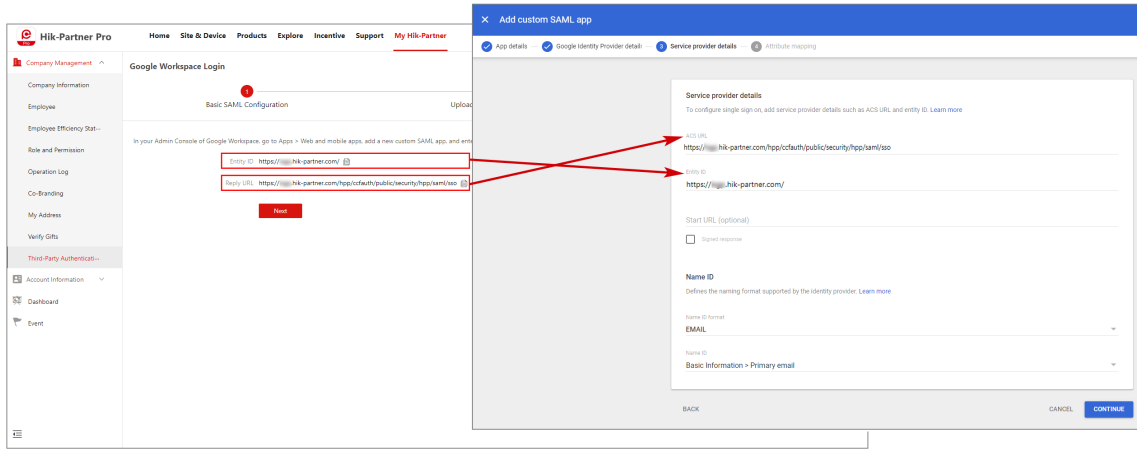


Figure 3-223 Copy from Hik-Partner Pro and Paste into Google Workspace Admin Console

5. On the **Service provider details** page, set the name ID format to **EMAIL**.

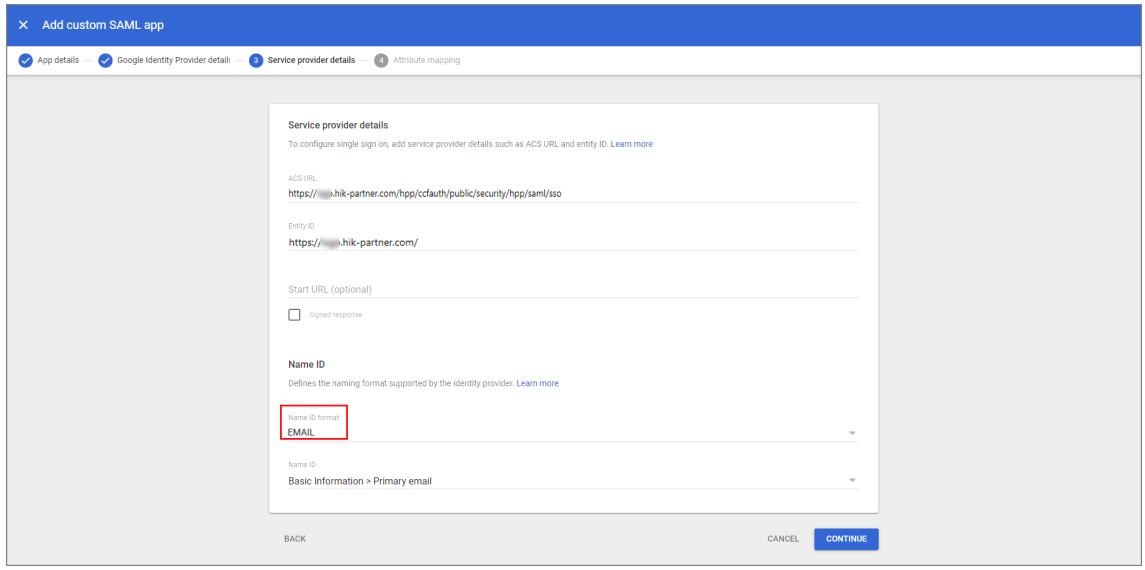


Figure 3-224 Set Name ID Format to Email

6. In Google Workspace Admin Console, click **Continue** to go to the **Attribute mapping** page. Click **ADD MAPPING** to map selected user fields in Google Workspace to those in Hik-Partner Pro.

Note

Please set the mapping strictly according to the table and figure below. The mappings of email address, first name, and last name are required, and the mapping of role name is optional.

Table 3-23 Attribute Mapping

Field (Required/Optional)	Google Directory Attributes	Hik-Partner Pro Attributes
Email Address (Required)	**Basic Information → Primary email**	**emailaddress**
First Name (Required)	**Basic Information → First name**	**firstName**
Last Name (Required)	**Basic Information → Last name**	**lastName**
Role Name (Optional)	Select a user field in Google to map to **roleName**. Do not select the above 3 user fields (which are primary email, first name, and last name). For example, you can map the Google Workspace user	**roleName** The **roleName** field is used by Hik-Partner Pro to identify which Hik-Partner Pro role should be assigned to the Google Workspace user during first login.

Field (Required/Optional)	Google Directory Attributes	Hik-Partner Pro Attributes
	attribute **Department** to **roleName**.	**Note** - The value of the selected Google Works attribute must be the same as an existir Pro role name. The matching is case-ins For example, when the value of the sele attribute is **IT Manager**, it matches an e Partner Pro role name and can be mapp

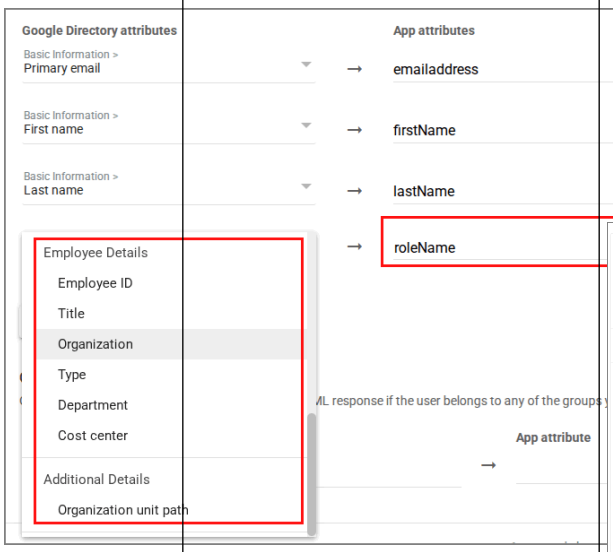


Figure 3-225 Select User Fields in Google

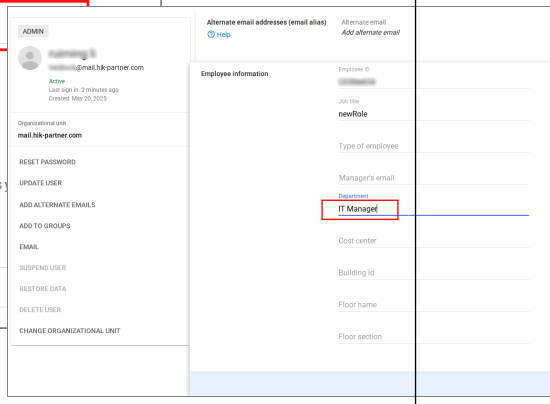


Figure 3-226 Value of Selected Goog

- If no role is matched, the default role co Partner Pro in ***Step 3: Set Role and Perm Complete Configuration*** is used.

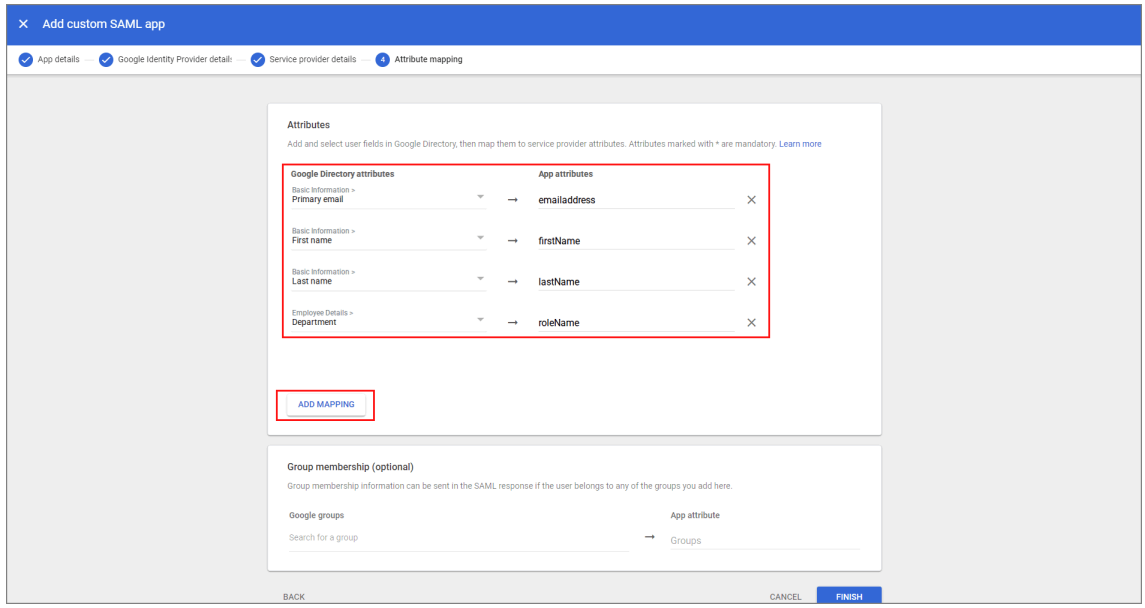


Figure 3-227 Finish Adding

7. Click **FINISH** to finish adding the custom SAML app.
8. To make all users in your Google Workspace able to log in to Hik-Partner Pro, click the **User access** section, select **ON for everyone**, and click **SAVE**.

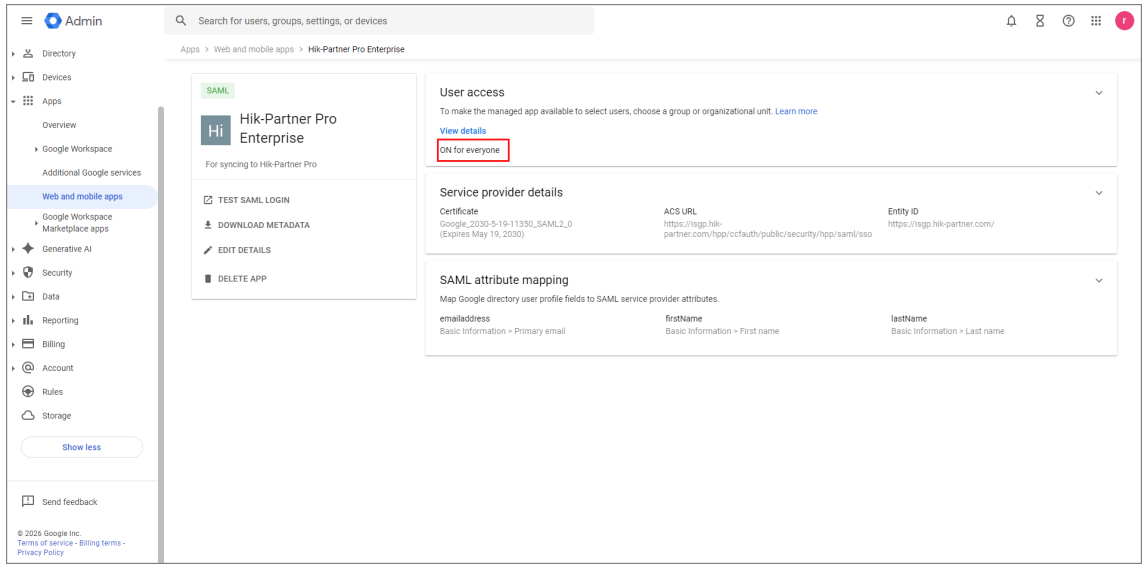
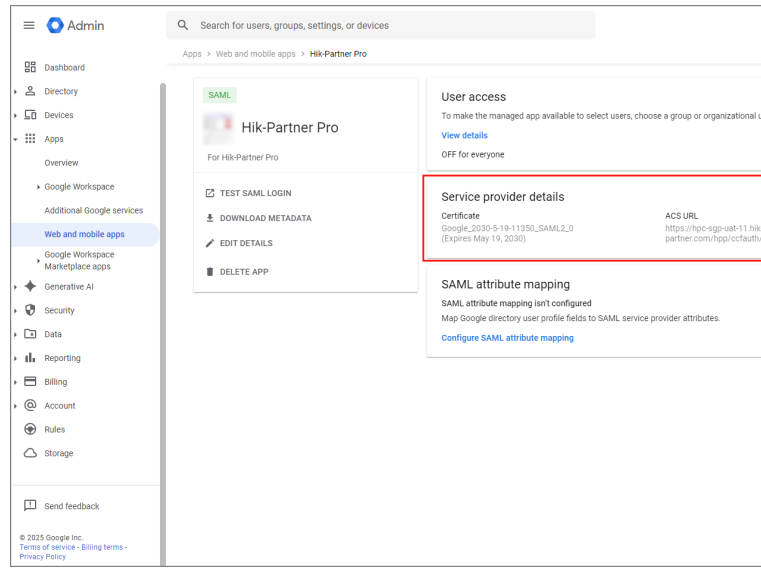


Figure 3-228 The Newly Added SAML App

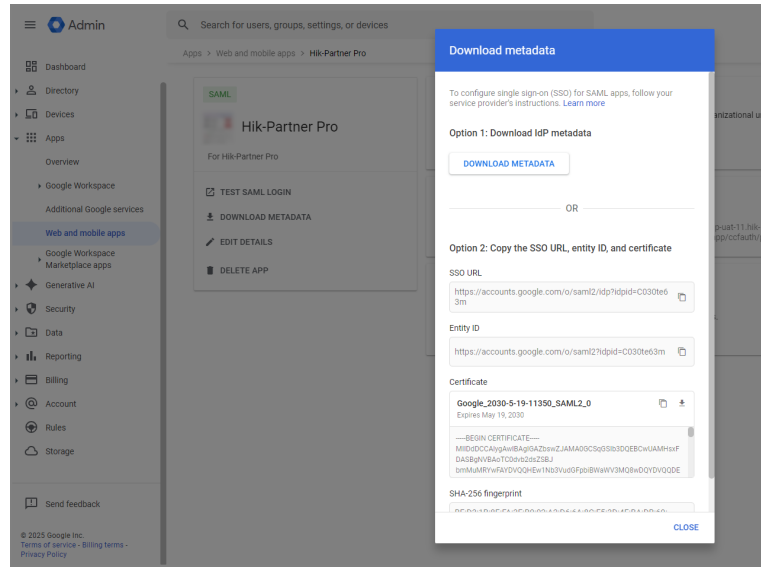
Step 2: Upload Metadata Document to Hik-Partner Pro

1. Find the metadata document (XML file) you has downloaded to your PC when you add the custom SAML app. If you cannot find it, download the metadata document again from the Google Workspace Admin Console

   1. Open the custom SAML app you has added, click **Service provider details**.



   2. Click **DOWNLOAD METADATA** to download the metadata document (XML file) to your PC.



2. Go back to Hik-Partner Pro, click **Next** to go to the step **Upload Metadata Document**, and click **Upload** to upload the downloaded XML file.

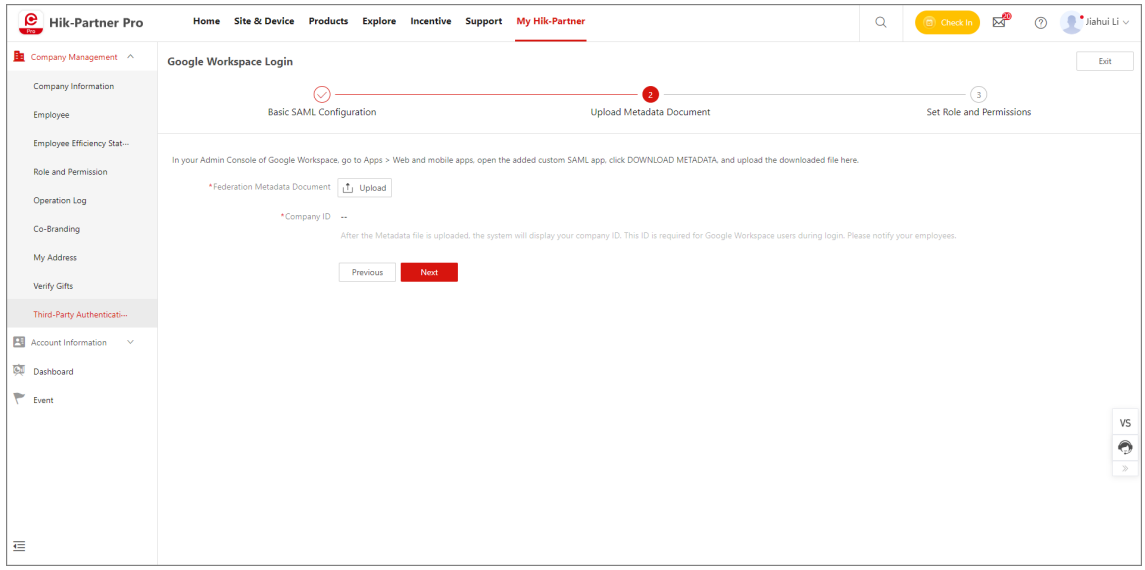


Figure 3-229 Upload Metadata File

3. After the metadata file is uploaded successfully, click to copy your company ID and send it to your employees. The company ID is used for your employee accounts in Google Workspace to log in to Hik-Partner Pro.

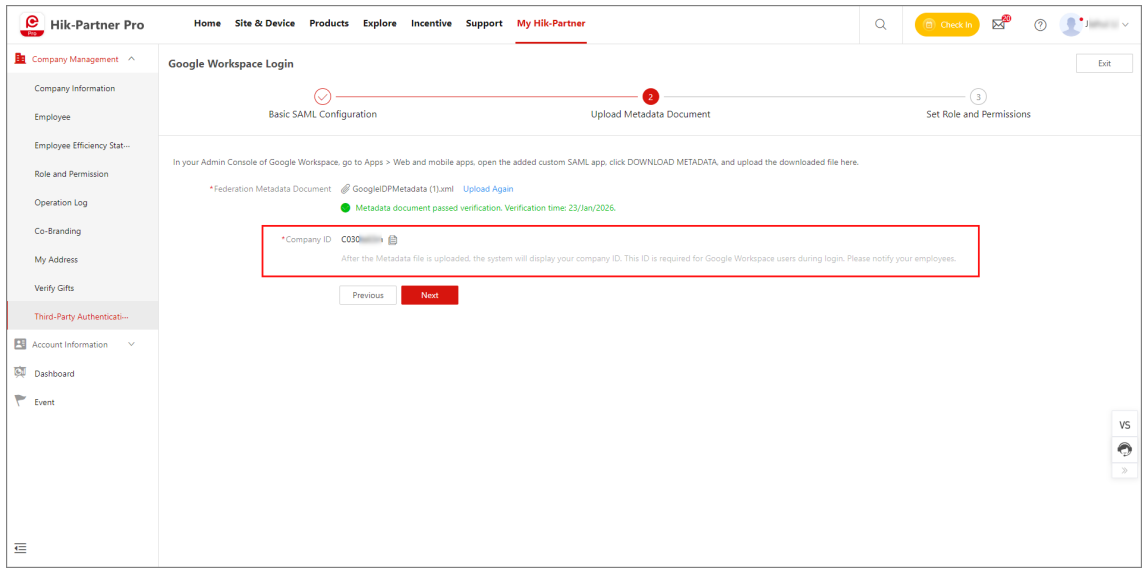


Figure 3-230 Save Your Company ID for Later Login

Step 3: Set Role and Permissions and Complete Configuration

1. Go back to Hik-Partner Pro, click **Next** to go to the step **Set Role and Permissions**. Select a default role for accounts logged in via Google Workspace, which you can go back here later to

modify (default role modifications are only effective for users logged in via Google Workspace for the first time).

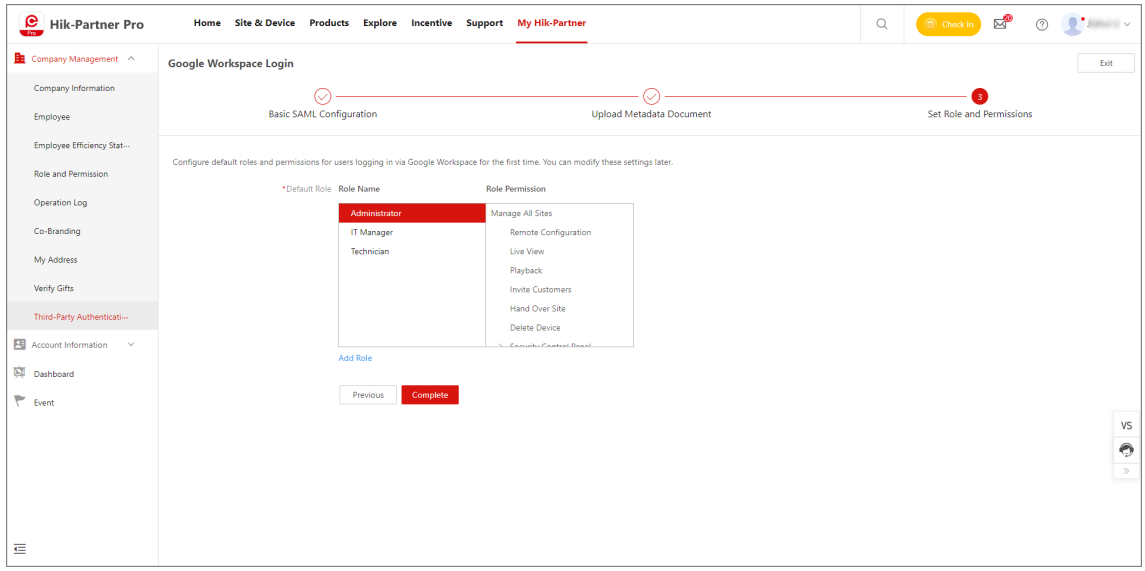


Figure 3-231 Set Role and Permissions

2. Click **Complete** to finish the configuration. Your users can now log in to Hik-Partner Pro with their Google Workspace accounts.

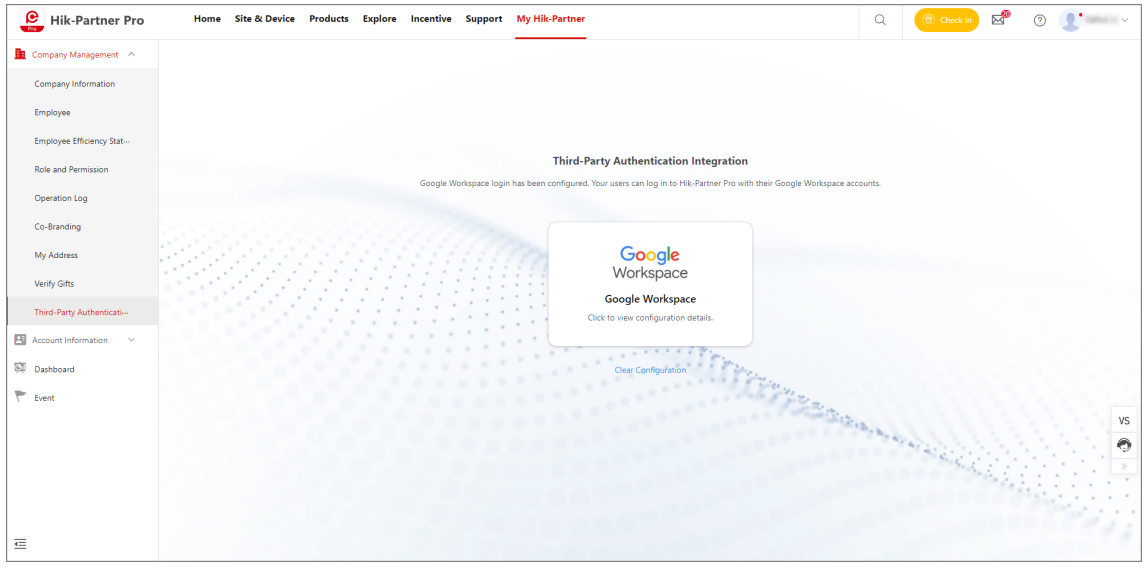


Figure 3-232 Complete Configuration

3. Go to the **Employee** page of Hik-Partner Pro to check the accounts logged in via Google Workspace. The accounts will be marked with the icon .

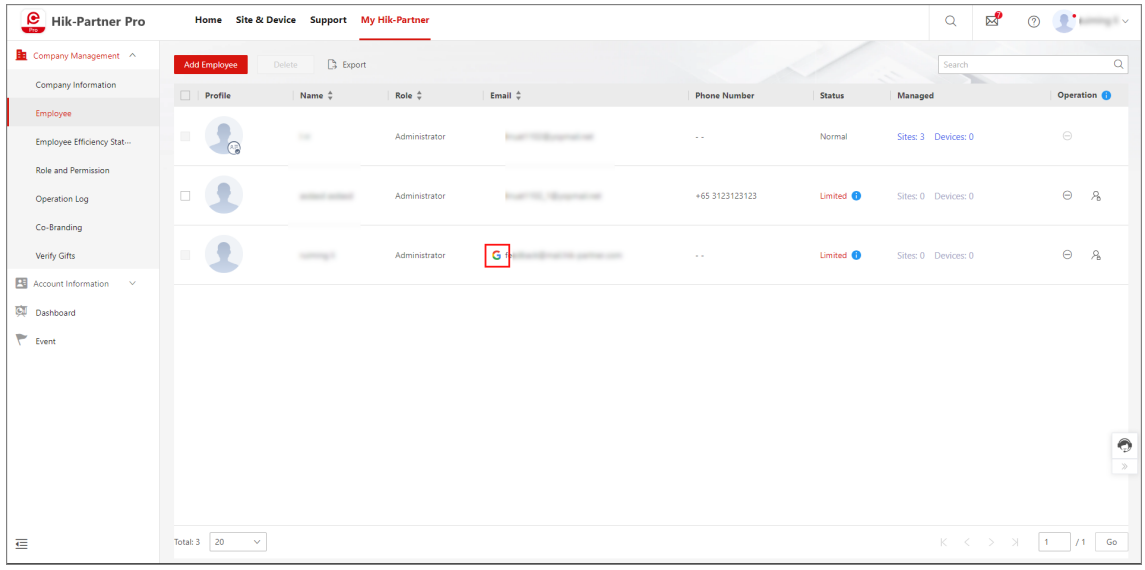


Figure 3-233 Synced Accounts

Step 4: Log In to Hik-Partner Pro Using Accounts Synced from Google Workspace

1. Open the Hik-Partner Pro Portal or Mobile Client, select G (on the Portal) or **Log In via Google Workspace** (on the Mobile Client).

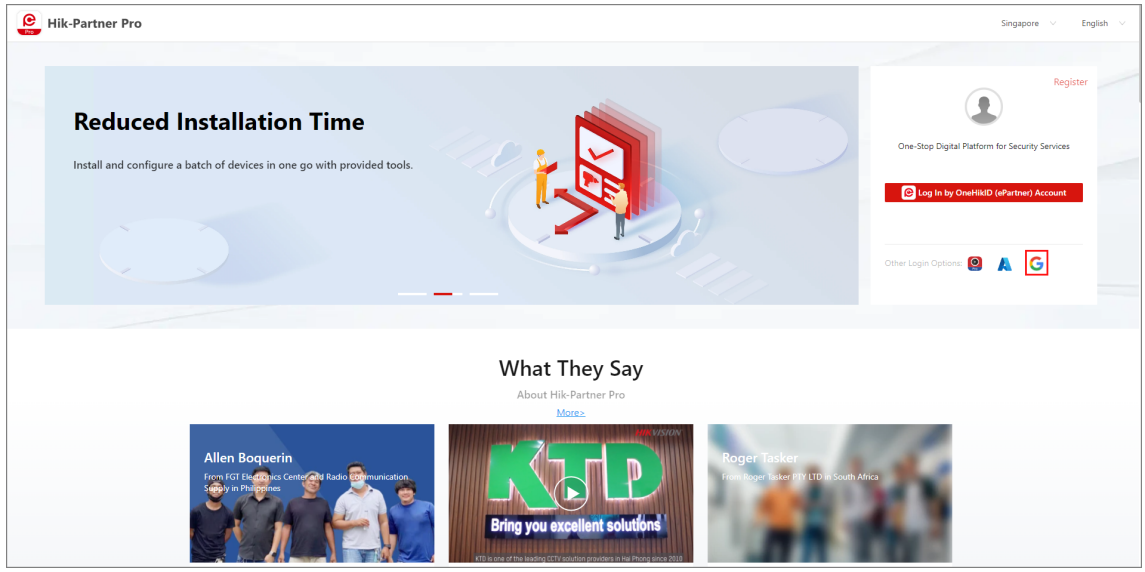


Figure 3-234 Login

2. Enter the company ID, and select **Confirm**. You will be redirected to the login page of Google.

Note

If you are the employee, ask your administrator (whoever sets up the Google Workspcae login) for the company ID.

If you are the administrator (Installer Admin), go to the Hik-Partner Pro Portal, select **My Hik-Partner → Company Management → Third-Party Authentication Integration → Google Workspace → SSO Configuration** to get your company ID.

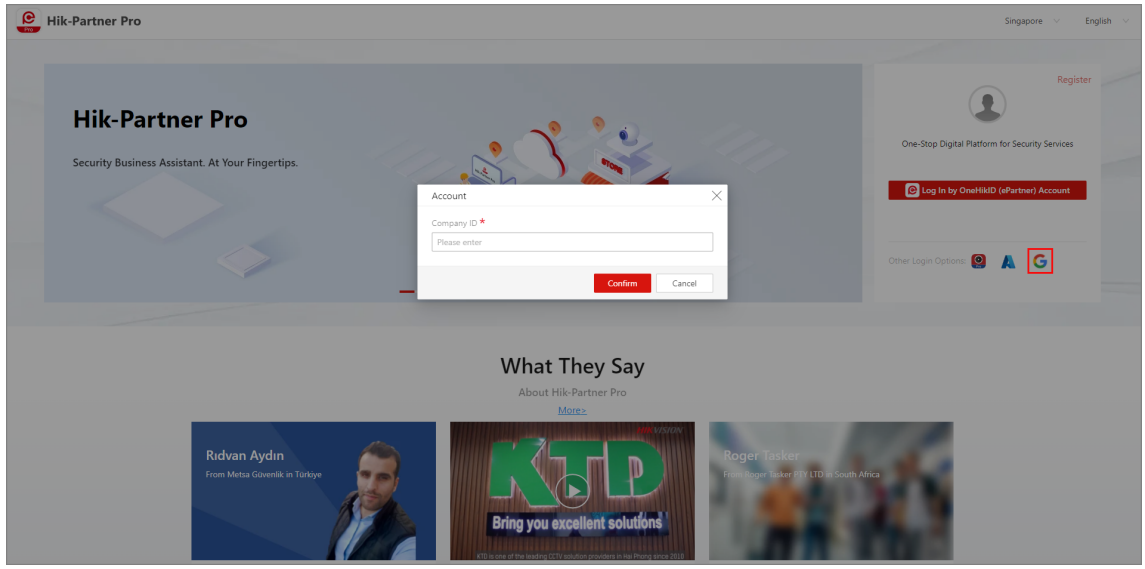


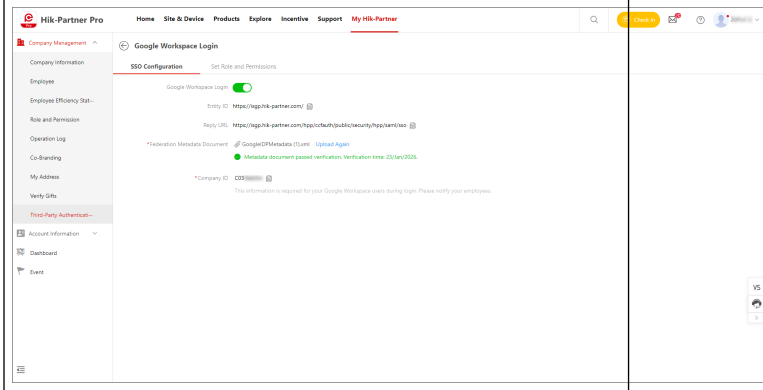
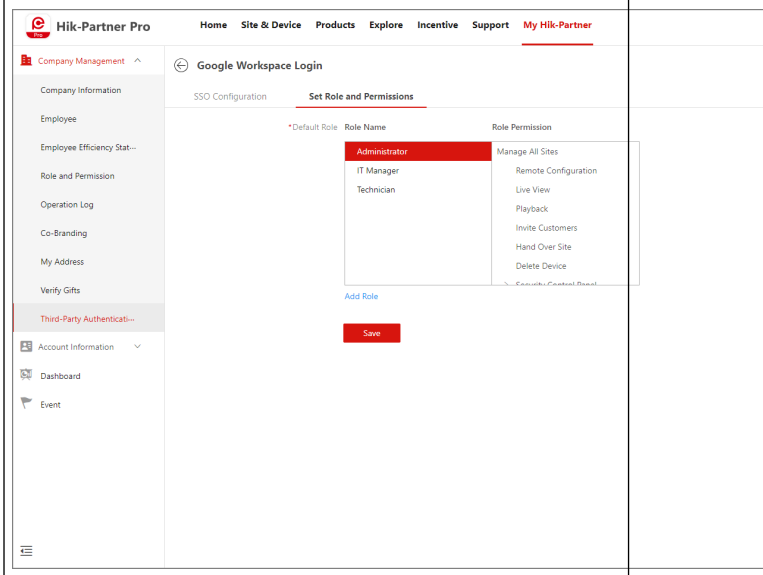
Figure 3-235 Login

3. Log in to your Google account. If verification passed, you will log in to and enter Hik-Partner Pro.

(Optional) Step 5: Modify Google Workspace Login Settings

After you complete the Google Workspace login configuration, you can also view your company ID for login, disable Google Workspace login, and modify the default role of synced accounts.

1. Go to the Hik-Partner Pro Portal, select **My Hik-Partner → Company Management → Third-Party Authentication Integration → Google Workspace** .
2. The following modifications are available.

Available Operations	Tab
- Turn off **Google Workspace Login** to make users unable to log in to Hik-Partner Pro using Google Workspace accounts (including those who have logged in via Google Workspace before). - Upload the metadata XML file again if any changes shall be made. - View and copy your company ID, and give it to your employees who need to log in to Hik-Partner Pro via Google Workspace.	
Modify the default role for the accounts logged in via Google Workspace. (Default role modifications are only effective for users logged in via Google Workspace for the first time).	

Limitations

- A single Google Workspace tenant can only be uniquely bound to one Hik-Partner Pro company (i.e., one Installer Admin account).
- This feature is only available in some regions and countries.

3.5.5 How to Manage Two-Factor Authentication

Feature Overview

Hik-Partner Pro provides Two-Factor Authentication (2FA) to enhance account security.

When 2FA is enabled, users must complete an additional verification step (email verification code) after entering their account and password, helping prevent unauthorized access.

Typical Use Cases

This feature is suitable for:

- Improving overall system security for enterprises.
- Preventing credential leakage or brute-force attacks.
- Protecting sensitive operations (e.g., permission changes).
- Meeting compliance requirements in global markets.

Roles and Permissions

Table 3-24 Roles and Permissions

Dimension	Company Admin	All Users
Can enable/disable 2FA	Yes **Note** The enabling and disabling of 2FA will be applied to all OneHikID accounts (both employees and Admin) under the company.	No
Can manage trusted devices	Can manage own devices	Can manage own devices
Trusted device limit	Up to 10 devices	Up to 10 devices

Company Admin: Enable Two-Factor Authentication

Enable 2FA Using the Portal

1. Log in to the Hik-Partner Pro Portal.
2. Go to **My Hik-Partner → Company Management → Account Security** .

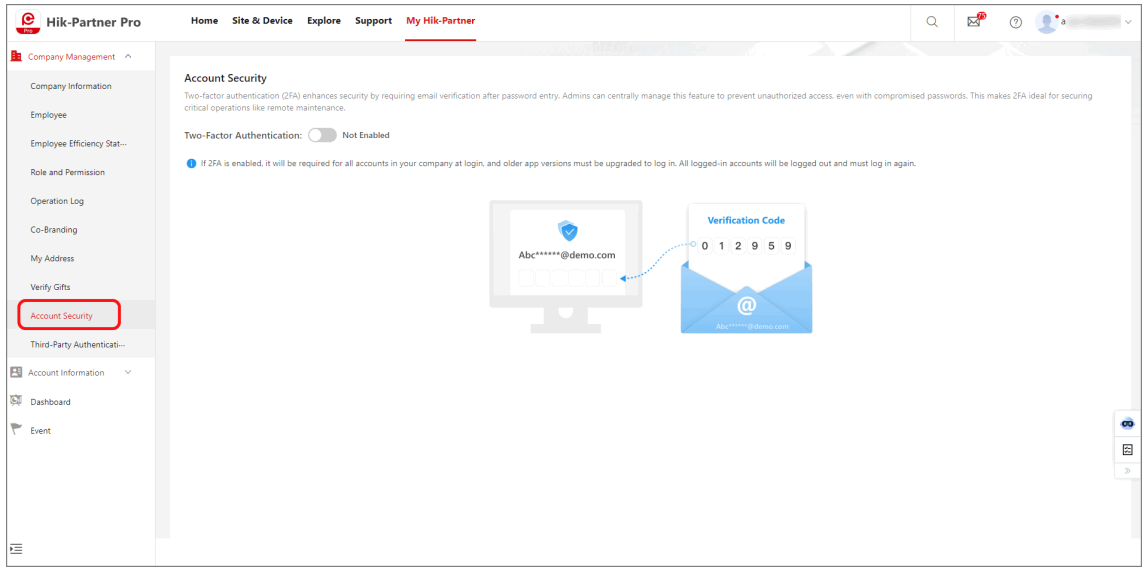


Figure 3-236 Account Security

3. Enable **Two-Factor Authentication**.
4. Enter the email verification code, and click **Confirm**.

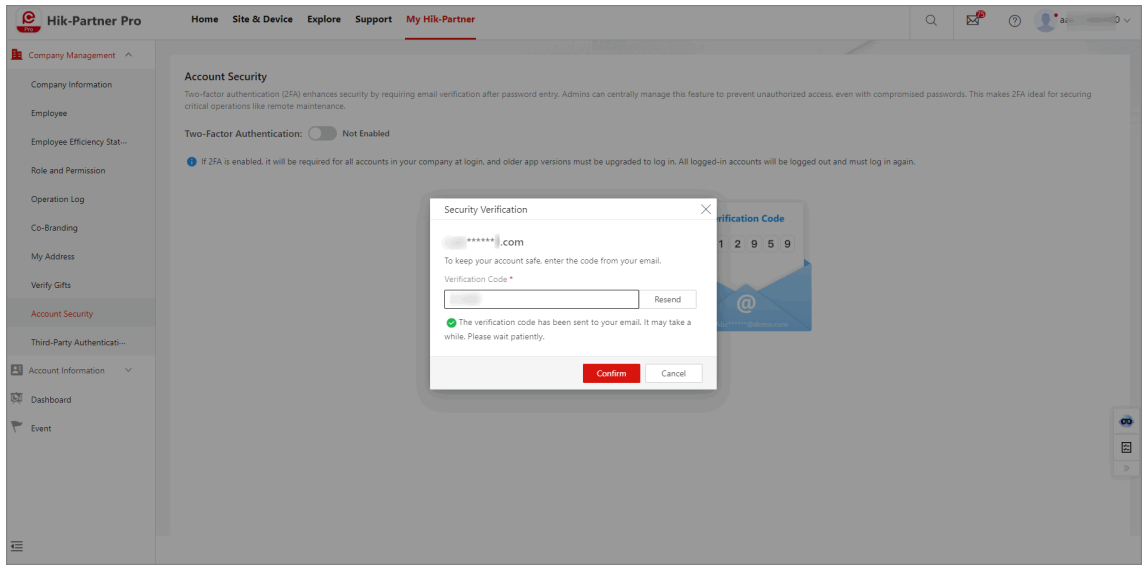


Figure 3-237 Email Verification

5. 2FA status is updated after successful verification.

Note

The enabling and disabling of 2FA will be applied to all OneHikID accounts (both employees and Admin) under the company.

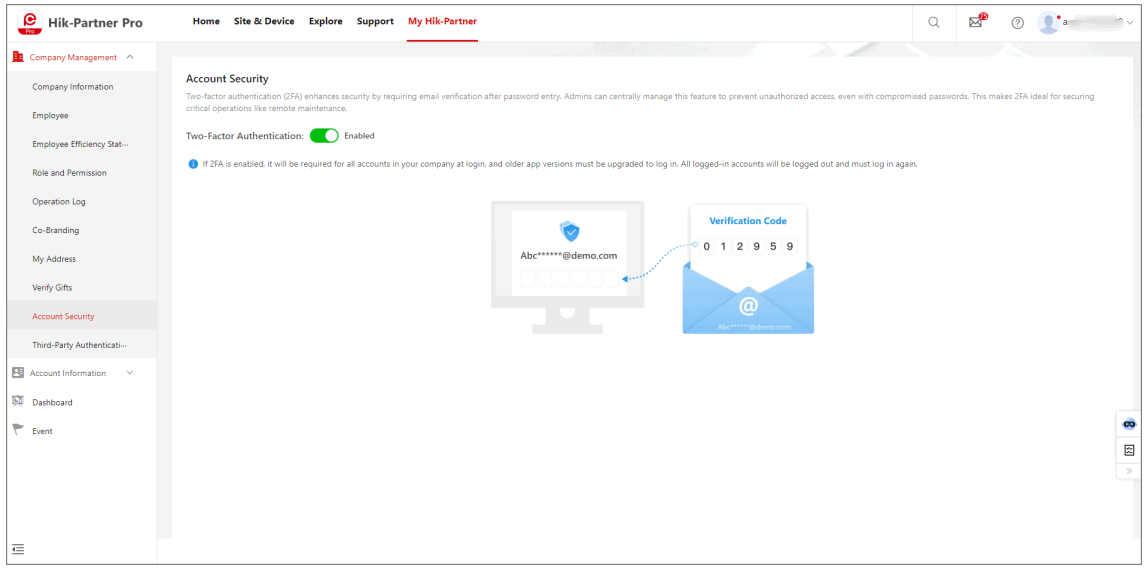


Figure 3-238 Enabled

Enable 2FA Using the Mobile Client

1. Log in to the Hik-Partner Pro Mobile Client.
2. Tap **Me → Company Management** .

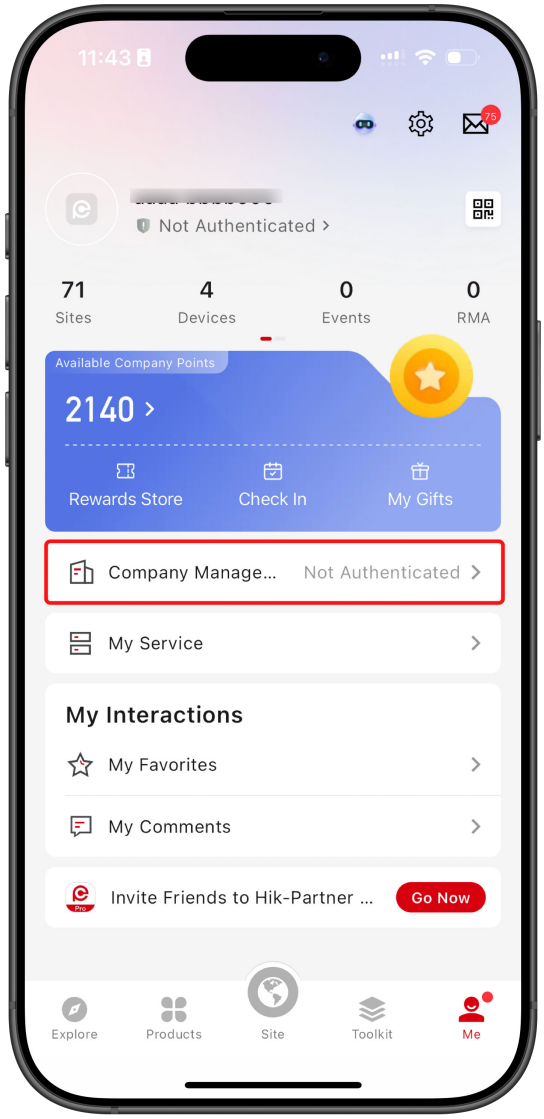


Figure 3-239 Company Management

3. Tap **Account Security**.

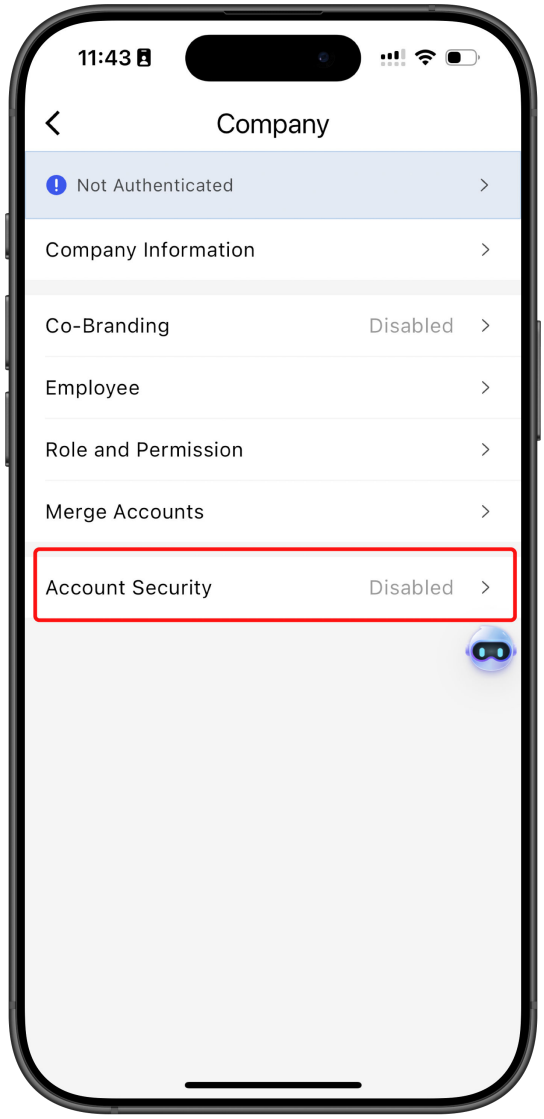


Figure 3-240 Account Security

4. Enable **Two-Factor Authentication**.

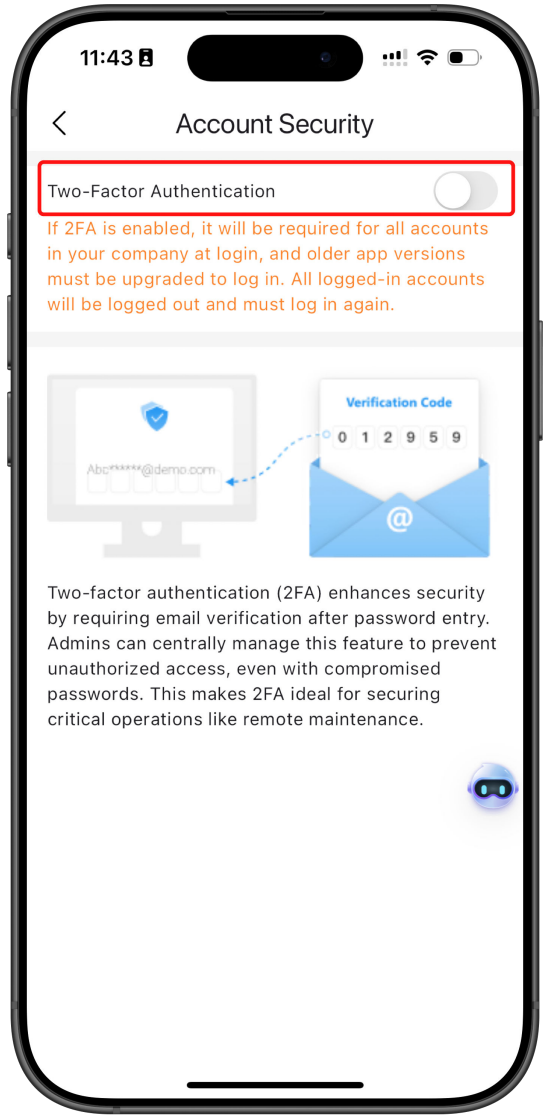


Figure 3-241 Two-Factor Authentication

5. Enter the email verification code, and tap **Confirm**.

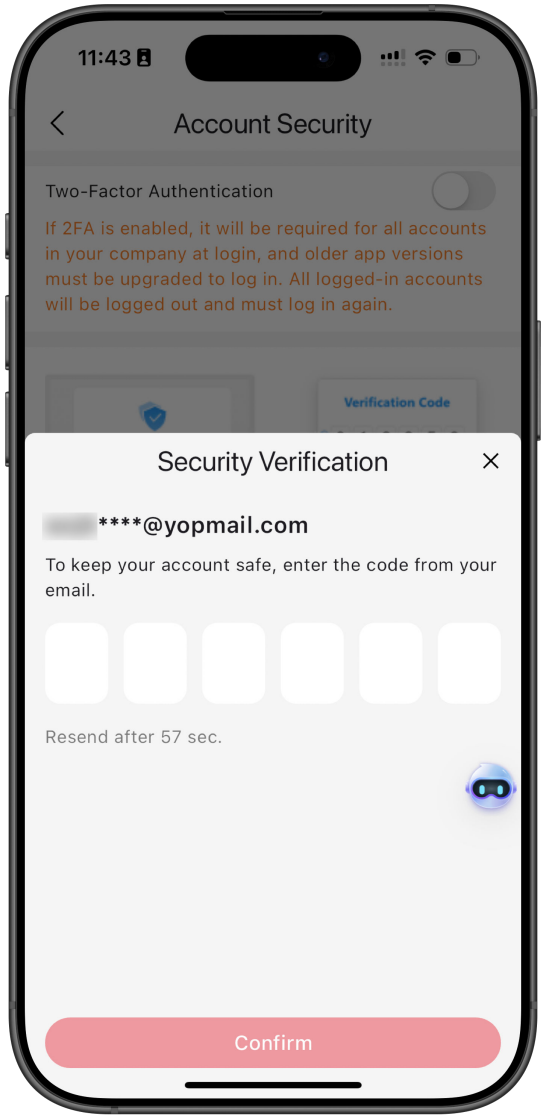


Figure 3-242 Email Verification

6. 2FA status is updated after successful verification.

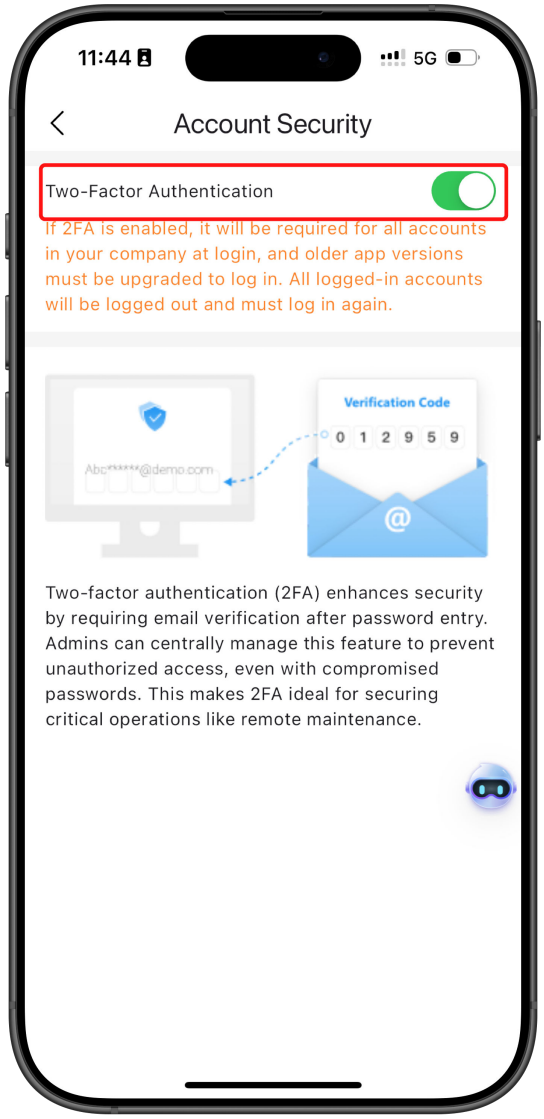


Figure 3-243 Enabled

Important Notes About Enable 2FA

- Once 2FA is enabled, **all users in the company must use 2FA to log in**.
- Users on untrusted devices will be logged out.
- Older app versions may require updates.
- Only OneHikID accounts support 2FA. Other login types (e.g., Google Workspace, Azure AD) do not support this setting.

All Users: 2FA Login Process

2FA Login Process on the Portal

When 2FA is enabled:

1. On the landing page of the Portal, click **Log In by OneHikID (ePartner Account)**.
2. Enter your account and password. Click **Sign In**.
3. The system sends a verification code to your email.
4. Enter the code, and click **Confirm**.

Note

You can check **Trust This Device** so that you can log in without email verification on this same device the next time.

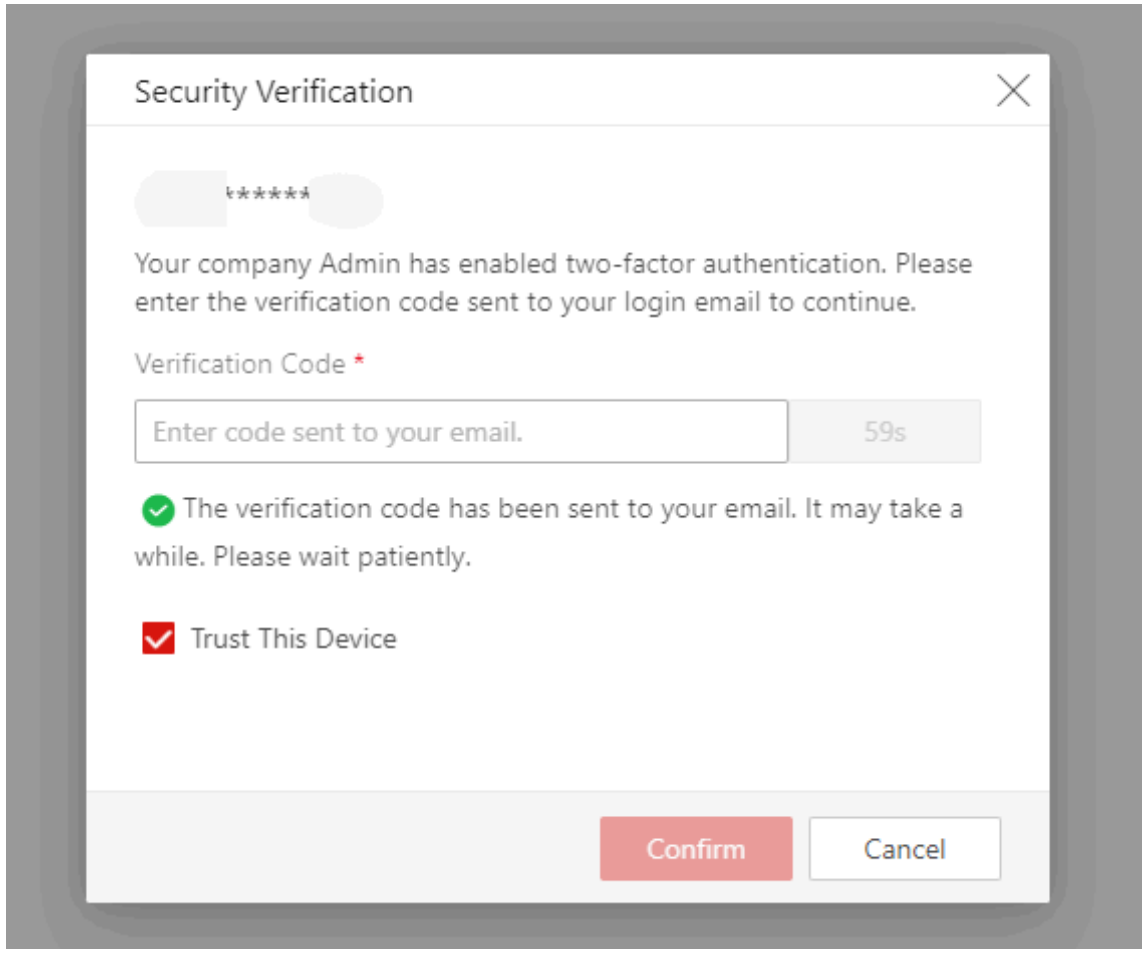


Figure 3-244 Enter Code

5. Login is completed successfully.

2FA Login Process on the Mobile Client

When 2FA is enabled:

1. Open the Mobile Client, tap **Log In → OneHikID (Hik-ePartner) Account** .
2. Enter your account and password. Tap **Sign In**.
3. The system sends a verification code to your email.
4. Enter the code, and tap **Confirm**.

Note

You can check **Trust This Device** so that you can log in without email verification on this same device the next time.

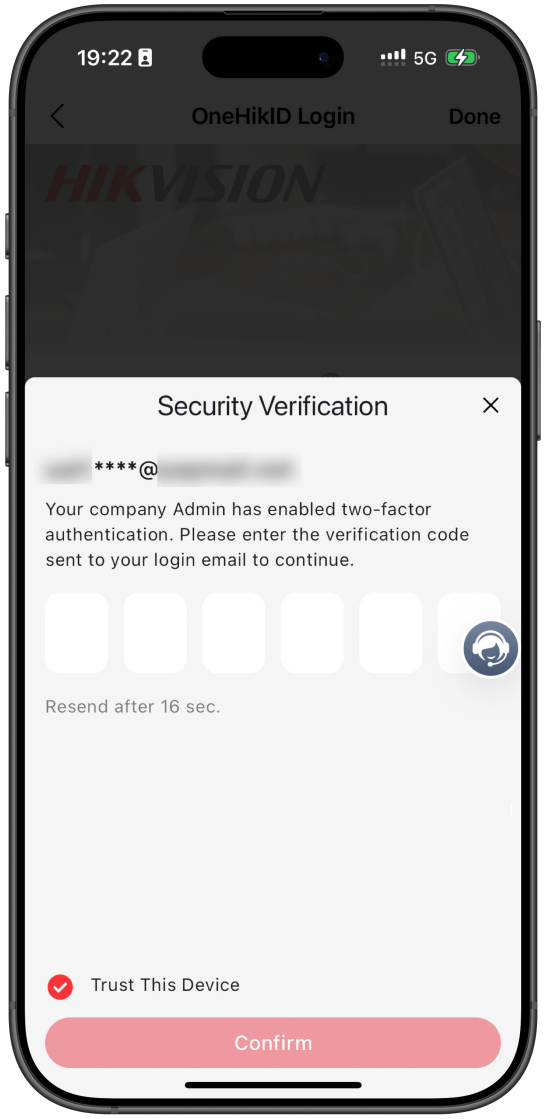


Figure 3-245 Enter Code

5. Login is completed successfully.

All Users: Manage Trusted Devices

View and Remove Trusted Devices Using the Portal

1. Log in to the Portal.
2. Go to **My Hik-Partner → Account Information → My Trusted Devices** . You can check the following device info:

- Device name (phone model / browser)
- Device type (PC / Android / iOS)
- Last login time

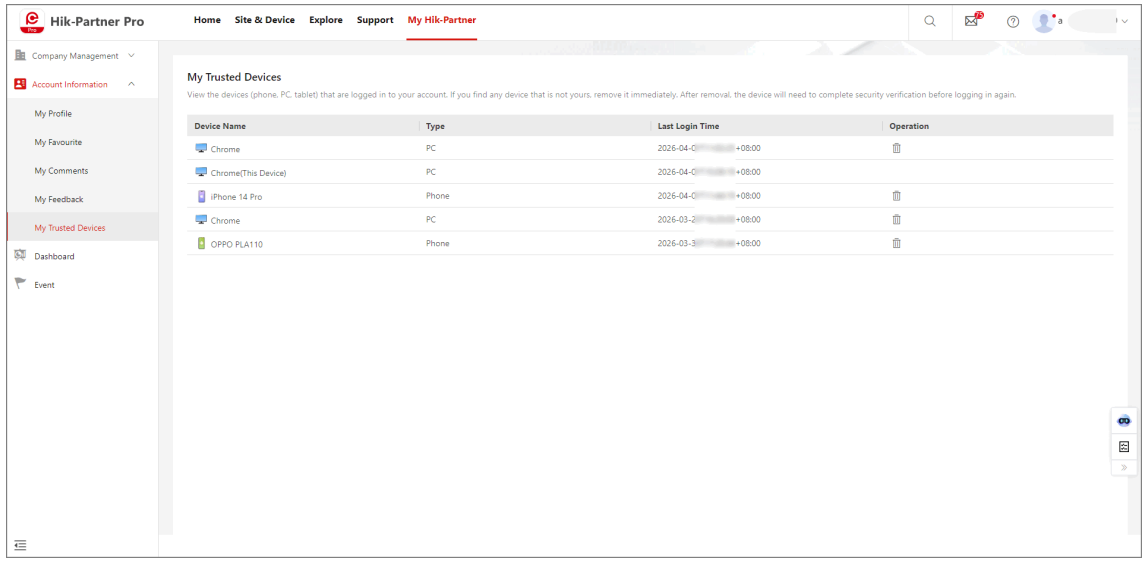


Figure 3-246 My Trusted Devices

3. To remove a trusted device from your account, click in the **Operation** column.
4. Click **Confirm**. Your account logged in on this removed device will be logged out.

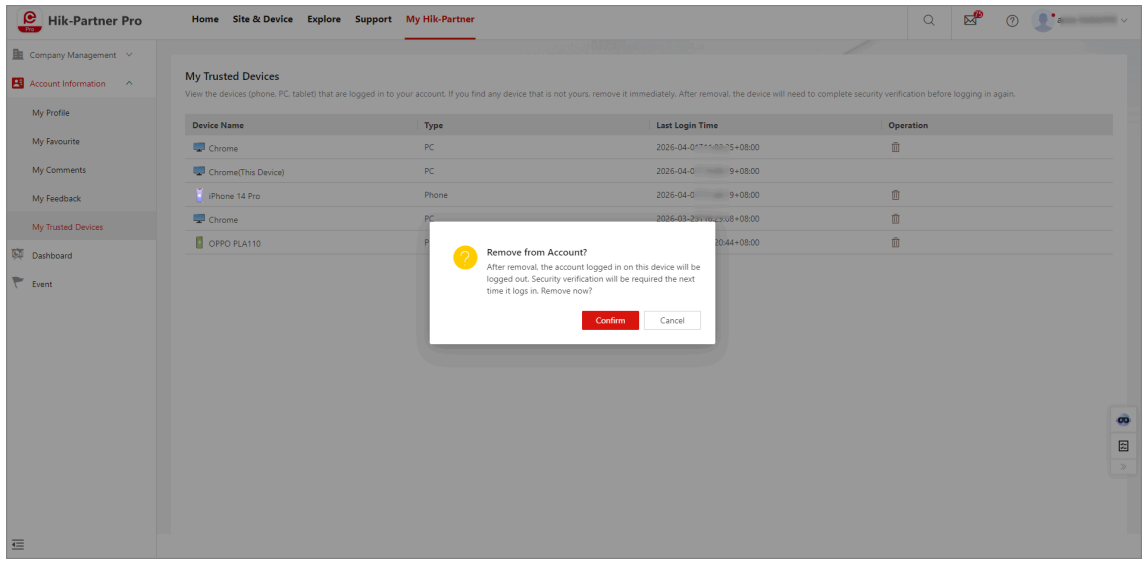


Figure 3-247 Confirm Removal

View and Remove Trusted Devices Using the Mobile Client

1. Log in to the Mobile Client.
2. Tap **Me**, and then tap your profile picture on the left top.

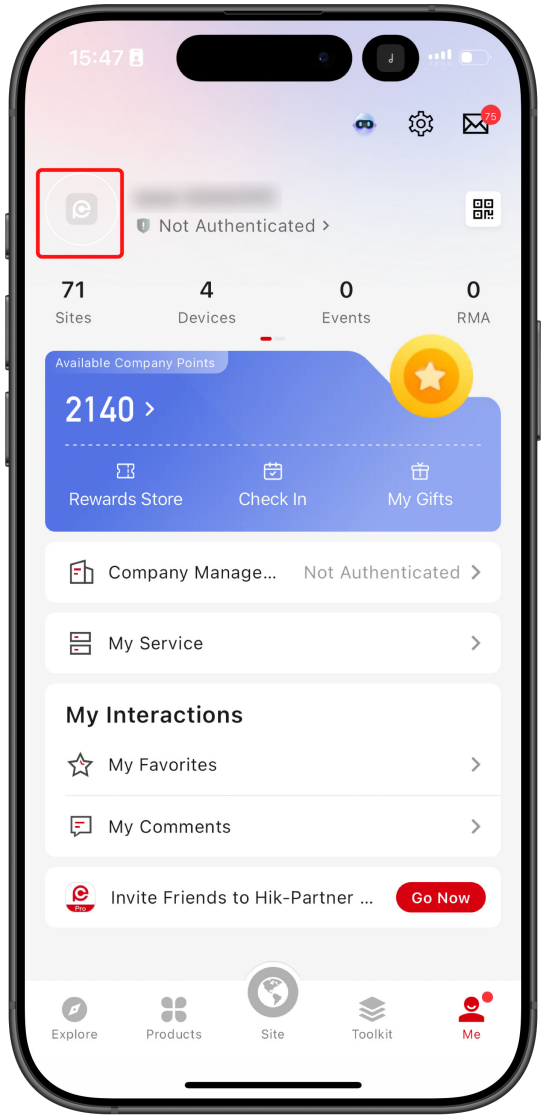


Figure 3-248 Profile Picture

3. Tap **My Trusted Devices**.

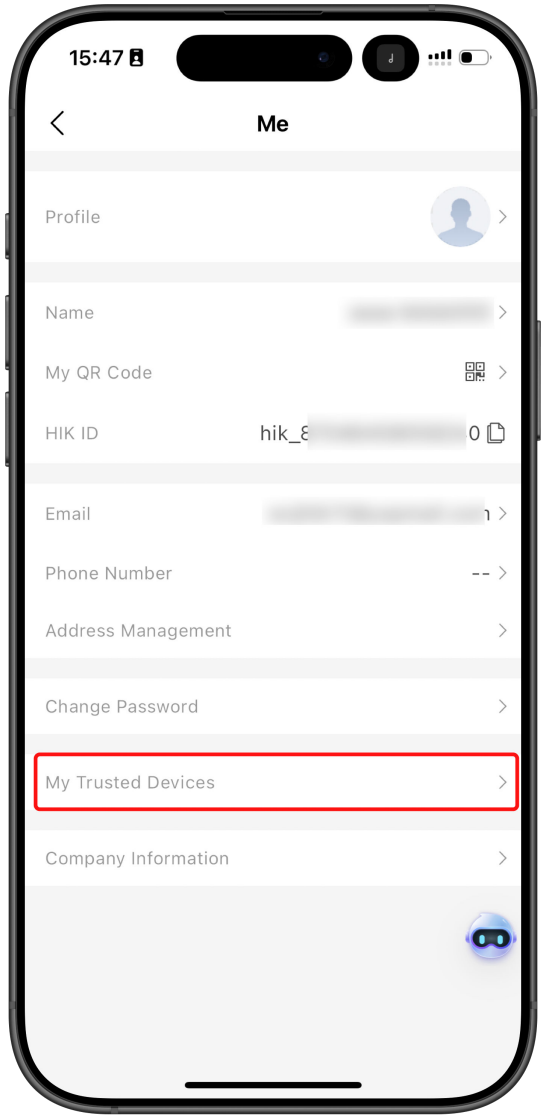


Figure 3-249 My Profile

4. You can check the following device info:
   - Device name (phone model / browser)
   - Device type (PC / Android / iOS)
   - Last login time

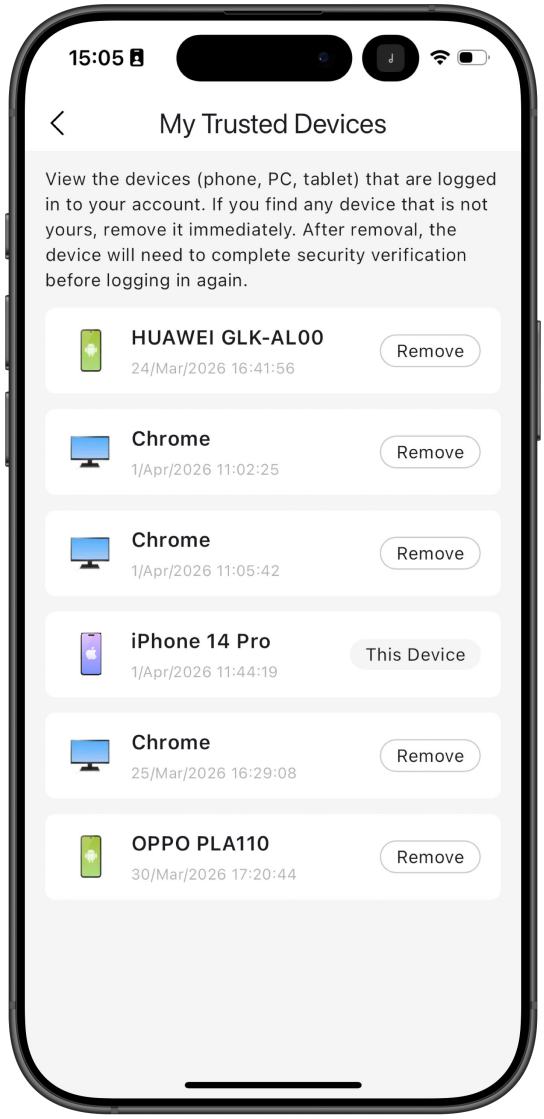


Figure 3-250 My Trusted Devices

5. To remove a trusted device from your account, tap **Remove**.
6. Tap **Confirm**. Your account logged in on this removed device will be logged out.

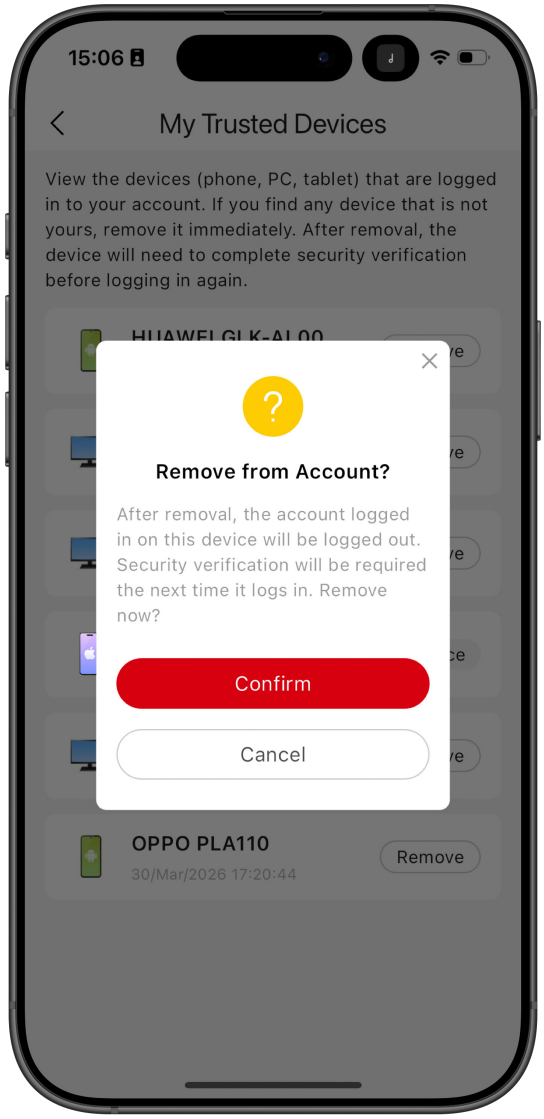


Figure 3-251 Confirm Removal

Related FAQ

Q: What if I haven't linked an email address to my account?

A: If you cannot find your linked email in your profile, please contact the technical support for support.

3.5.6 How to Use Biometric Login

What This Is and When to Use It

In One Sentence

Sign in to the Hik-Partner Pro Mobile Client with your phone's own face or fingerprint check instead of typing your account and password. What took 10 to 15 seconds becomes a single check of one or two seconds.

When It Helps

- **Moving between devices.** Check a site on a tablet, come back to the phone, and the session has been signed out. One check restores it.
- **Occasional use.** Open the app once a week and the session has long expired. You no longer need to look up the password.
- **Signing in in front of a customer.** Typing a password on site can be observed; a face or fingerprint cannot.

Scope

Item	Description
Client	Mobile Client only (iOS and Android). Not on the Portal.
Account	OneHikID only.
iOS	Face ID.
Android	Face and fingerprint.
Phone prerequisite	The phone supports biometrics and has at least one enrolled in system settings.
Not applicable	The next sign-in after an active sign-out or a password change.

Before You Start

1. **A face or fingerprint is already enrolled in the phone's system settings.**
2. **The account has signed in on this phone once with its password.** Biometrics is a shortcut for signing in again.

Enable/Disable Biometric Login

Enable It When the Prompt Appears

1. The prompt asks whether to enable biometric (fingerprint or face) sign-in for one-tap unlocking. The full-screen prompt appears in two situations:
   - The first successful password sign-in after the Mobile Client is updated.
   - After verification failed repeatedly, at a later successful sign-in.

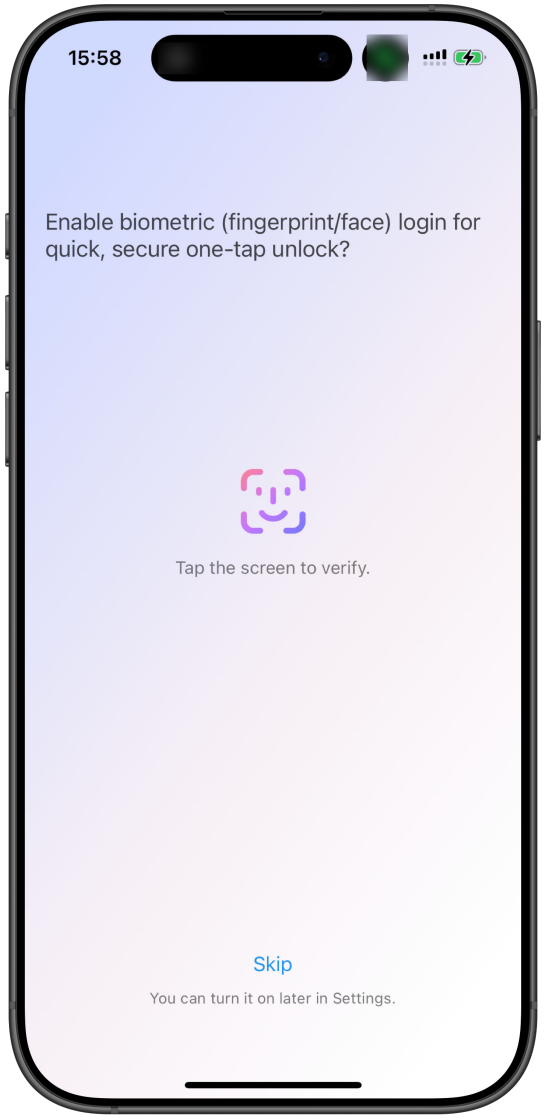


Figure 3-252 Prompt Appears

2. **Tap anywhere on the screen** to raise the check.

Note

If you don't need to enable it now, tap **Skip**.

3. The phone's own face or fingerprint sheet appears. Pass it and the feature is on.

Enable and Disable in Profile

1. Go to **Me**, and tap your profile picture. The switch sits under **Change Password**, and its label follows what the phone supports.

Phone Capability	**Switch Label**
Face	**Face ID**
Generic	**Biometrics**

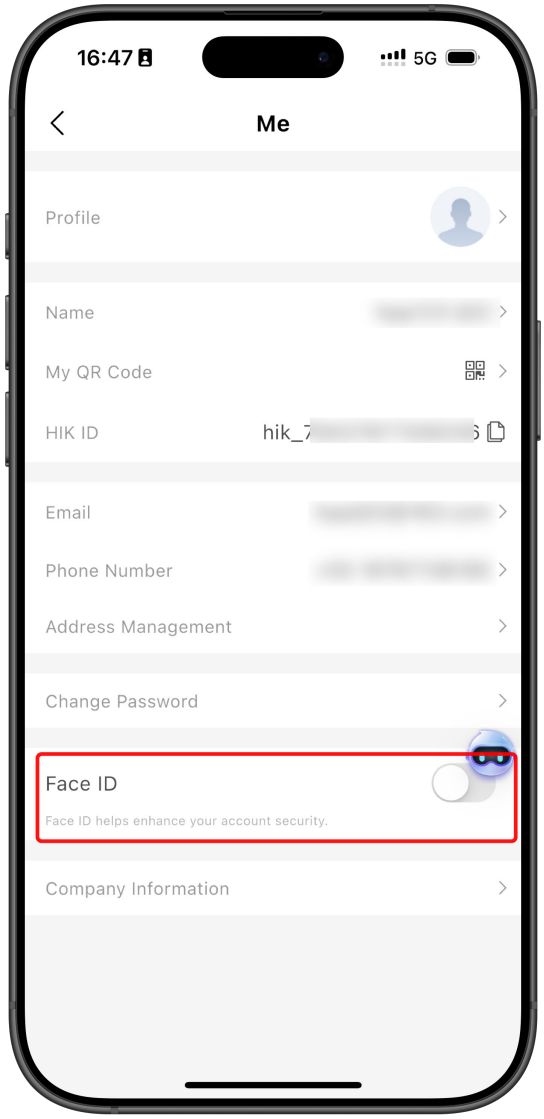


Figure 3-253 Biometric Login Switch

2. Your can turn it on or off to enable/disable biometric login.

Log In with Biometrics

Once enabled, the next time the Mobile Client needs you to sign in you see a verification page rather than a password box. Tap the screen to start verification. Tap **Switch Account** at the bottom to return to the password page and sign in with a different account.

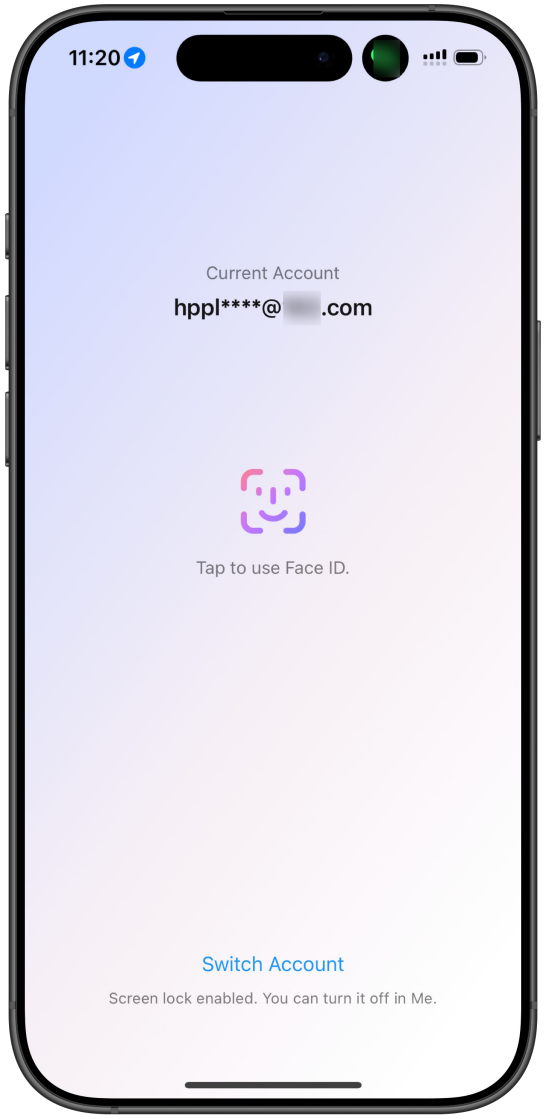


Figure 3-254 Biometric Login

3.5.7 How to Assign Sites to Installers as Site Managers?

Follow the corresponding instructions if you want to assign sites to the specified installers as site managers responsible for configurations of the devices on the site.

Before You Start

Make sure you have been *configured with the Manage All Sites permission*.

Assign Sites on the Portal

Steps

1. Select one or multiple sites for assignment on the Customer Site page and open the Assign Site to Site Manager pane.

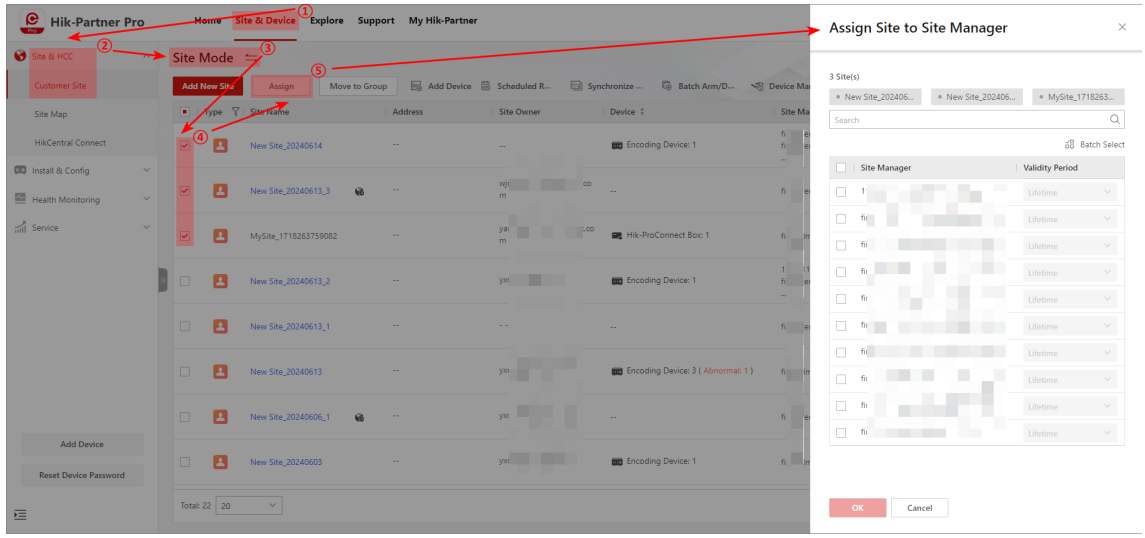


Figure 3-255 Open the Assign Site to Site Manager Page (Portal)

2. Select one or multiple installers as the site manager(s) of the selected site(s).

Note

No more than 100 site managers can be assigned to each site.

3. Set a validity period for each site manager one by one or click **Batch Select** to batch select a validity period for all selected site managers.

Note

- At least one site manager's validity period should be Lifetime.
- By default, the validity period of site managers with the Manage All Sites permission is Lifetime and cannot be edited.

4. Click **OK**.

   The installers assigned with sites will receive a notification on Hik-Partner Pro. In the Site Manager column, the names of site managers and validity period countdown of the permission will be displayed.

5. **Optional:** Click a site name to show the site details on the right, and click or to remove the current or the other account from the site manager list.

Note

- An account without the Manage All Sites permission can only remove its own account from the site manager list, while an account with the Manage All Sites permission can remove all accounts from the site manager list.
- If site managers or validity periods are changed, the corresponding site managers will also receive notifications on Hik-Partner Pro.

Assign Sites on the Mobile Client

Steps

1. Enter the Assign page.

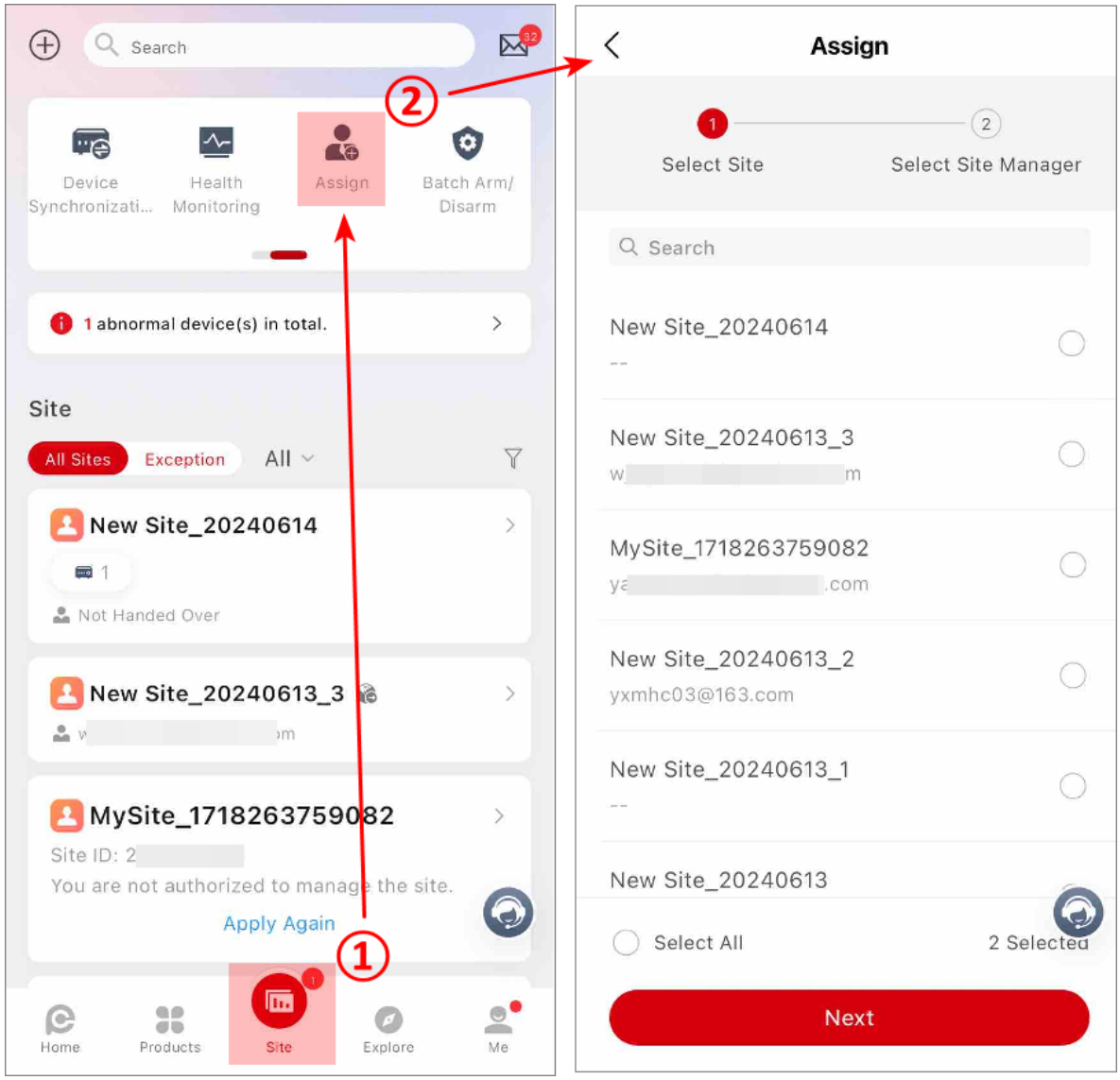


Figure 3-256 Enter the Assign Page (Mobile Client)

2. Select one, multiple, or all sites for assignment, and tap **Next**.
3. Select one, multiple, all Installers as the site manager(s) of the selected site(s).

Note

No more than 100 site managers can be assigned to each site.

4. Tap **OK**.

   The installers assigned with sites will receive a notification on Hik-Partner Pro. And the names of site managers will be displayed on the site details page.
5. **Optional:** Repeat the above steps to change site managers.

Note

If site managers are changed, the corresponding site managers will also receive notifications on Hik-Partner Pro.

3.5.8 Collaborate with an ISP/MSP on Site for Device Installation or Maintenance

You can collaborate with service partners to install and maintain the devices for your customers.

Stage	Service Partner	Description	Related Topics
Before Handover	Installation Service Partner (ISP)	ISP can help you install devices. ISPs have all permissions for the devices.	***Collaborate with ISP to Install and Hand Over Devices Before Handover***
Handover		ISP can help you hand over devices. After the site is handed over or collaboration is canceled, their device permissions are removed. **Note** The handover email/ message your customer receives only contains your company's information.	
After Handover	Maintenance Service Partner (MSP)	After the site is handed over **by transferring**, MSP can help you maintain devices, especially in offering technical support. You and your customer together determine the MSP's permissions for devices.	***Collaborate with MSP to Maintain Devices After Handover***

Collaborate with ISP to Install and Hand Over Devices Before Handover

The diagram below shows the overall process of site collaboration before you hand it over to your customer, and in this scenario, suppose your company is an ARC company.

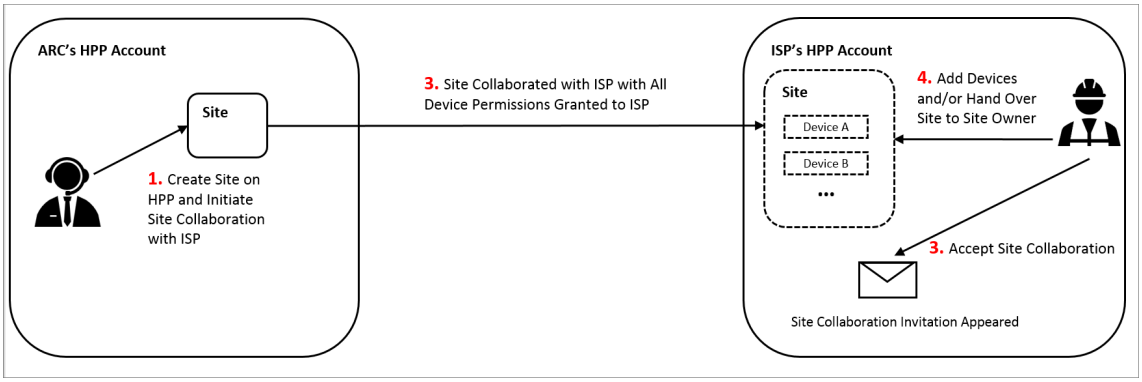


Figure 3-257 Overall Process

Collaborate with MSP to Maintain Devices After Handover

The diagram below shows the overall process of site collaboration after the site is handed over by transferring to your customer, and in this scenario, suppose your company is an installation company.

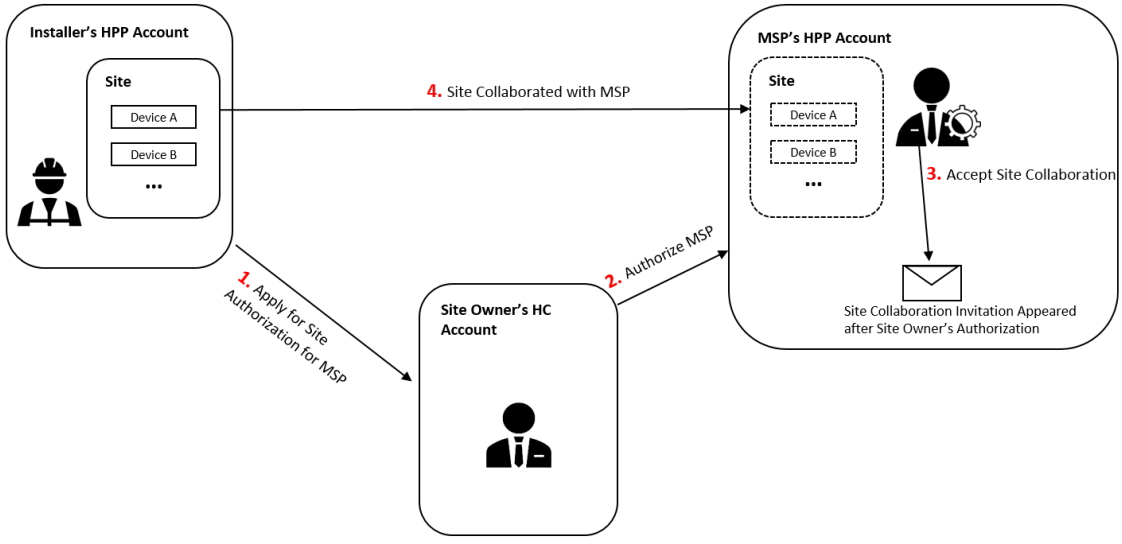


Figure 3-258 Overall Process

Limitations

- Site collaboration is not supported in some countries/regions or by some accounts.
- You can only invite these accounts to collaborate with you on the site: your MSP's Installer Admin account, and your ISP's account with the Manage All Sites or Manage Assigned Sites permission.
- Your account and the account which you invite need to be in the same country/region.
- You cannot invite any Installer account of your company.
- You can initiate site collaboration with your ISP before the site handover only on the Portal. The Mobile Client currently does not support initiating site collaboration with the ISP.

3.5.9 Transfer Sites and Devices to Another Account

What This Is and When to Use It

In One Sentence

Move your sites and devices — together with cloud storage, ARC relationship, and end-user (customer) handover relationships — to another Hik-Partner Pro company. The transferor starts it on the Portal, the recipient accepts, and the platform transfers everything in the background. Customers' devices stay online and need no reconfiguration.

The Problem It Solves

The usual case is an acquisition: company A sells part of its business to company B, and the digital assets have to follow — devices, sites, customers, and their management data.

The hard part is **not disturbing the customers**. Nobody should have to re-add devices, reconfigure alarm reception, or lose sight of their cameras because their provider changed.

That is what this feature is for. Once both companies agree, the platform migrates the assets in one pass and the end user (customer) gets a notification that the provider has changed.

What Moves and What Does Not

This is the most important thing to check first. **Anything outside the scope has to be rebuilt in the recipient company.**

Asset	Transfers or Not	Notes
Hikvision devices	Yes	All associated hardware will be transferred, with results reported for each device.
Customer site information	Yes	The site configuration and address will be copied to a new site under the recipient company.
Customer basic information	Yes	Contact and account details.
Device binding	Yes	The association between customer and device.
Cloud storage	Yes	Activated packages and data where applicable; works normally afterwards.
ARC relationship	Yes	The ARC connection is kept connected throughout.
Customer (end-user) handover	Yes	The handover status and associated Hik-Connect users are unchanged.
Hik-Connect and service partner accounts on the device	Yes	The former installer company's account is deleted.
Health monitoring state	**No**	Historical monitoring data does not transfer.
Exception rules	No	Must be reconfigured in the recipient company.
Linkage rules	No	Must be reconfigured in the recipient company.
Health monitoring service packages	No	Must be reconfigured in the recipient company.
Accounts inside the security control panel.	No	Must be reconfigured in the recipient company.

What Each Party Sees Afterwards

Role	What Changes
Transferor	The transferred devices disappear. Where **every** device in a site is transferred, the site no longer appears in the site list; where only some are transferred, the site remains. The transfer record stays available.
Recipient	New sites and devices appear. The new site manager is the recipient's Primary Admin, and the handover status and Hik-Connect users are unchanged.

Role	What Changes
End User / Customer (Hik-Connect)	Receives a notification naming the new installer. Device use is not interrupted and nothing needs re-adding.
ARC	ARC authorization moves with the devices and stays connected throughout.

Typical Scenarios

- **Acquisition.** Company A sells its business in one region to company B and the sites and devices move as a whole.
- **Merger.** Two installers merge and consolidate the assets under the surviving company.
- **Divesting part of a business.** Only certain sites or devices move and the rest stay. Selecting device by device.

Before You Start

Where to Find It

On the Portal: Go to **My Hik-Partner → Company Management → Device Asset Transfer** .

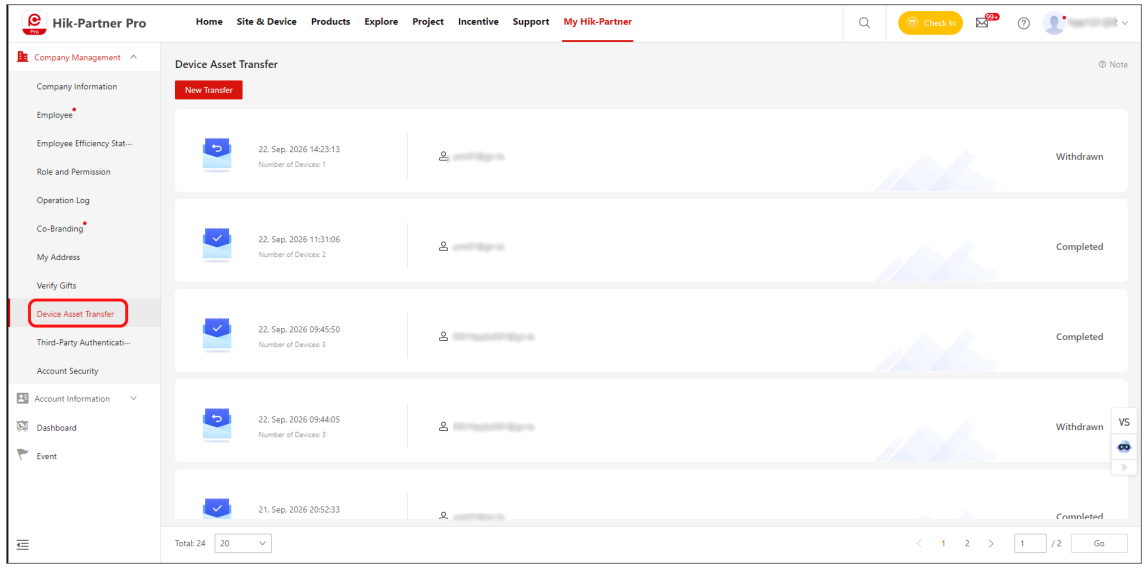


Figure 3-259 Device Asset Transfer

Pre-Transfer Checklist

- **Is the feature open to your company?** It is controlled by country/region and by company. If the entry point is missing, contact our support team first.
- **Does your account have the permission?** Initiating requires the **Manage All Sites** permission.
- **Is the recipient's email address an administrator of their company?** The wrong address means they never see the message.
- **Has the previous transfer finished?** Only one transfer may be open at a time.
- **Does the recipient have room?** Without a value-added subscription the ceiling is 1,024 devices, counting their existing devices plus this transfer.
- **Have you noted what does not transfer?** Exception rules, linkage rules, health monitoring packages, and accounts inside the control panel all need rebuilding.

For Transferor: The Four-Step Guide

Step 1: Select Devices

1. Expand the site tree on the left and tick the devices to transfer. Selecting only some of a site's devices is supported.
2. Click **>** to move them to **Selected**. You can click **<** to move them back.
3. Click **Next**.

Note

If you transfer all devices in a site, the site will no longer be kept in your site list.

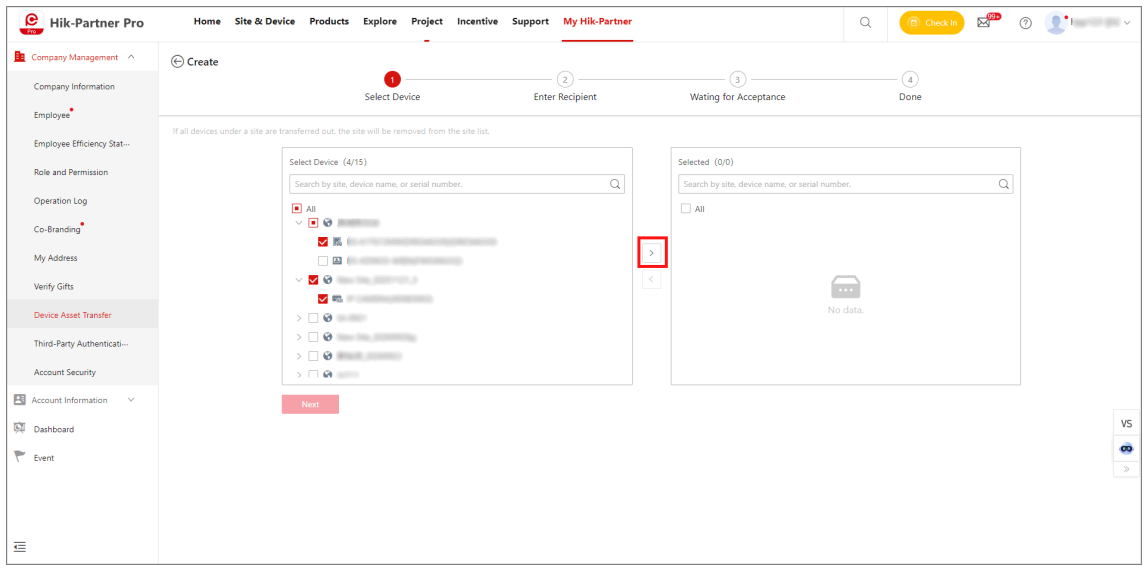


Figure 3-260 Select Devices

Step 2: Enter the Recipient

1. Enter the address of an administrator in the receiving company.
2. Click **Transfer Now**.
3. Click **OK** in the confirmation window.
4. **If that email address belongs to more than one company**, choose one, and click **OK**. When in doubt, ask the recipient which one first.

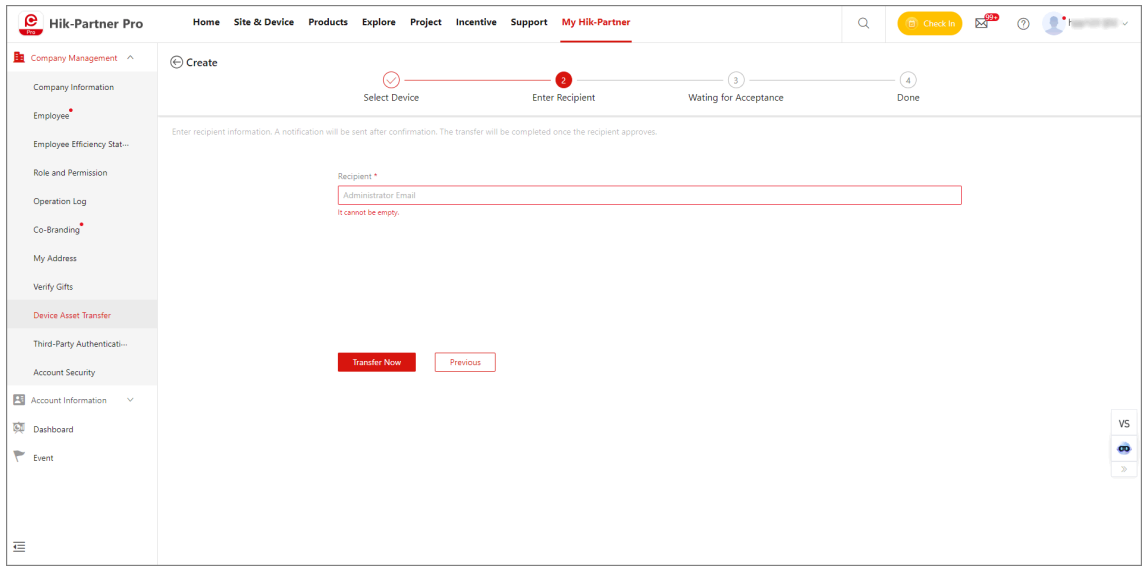


Figure 3-261 Enter Recipient

Step 3: Awaiting Acceptance

The page shows **Sent**: the transfer request has been sent and the recipient should log in to Hik-Partner Pro to accept it. The recipient's email address is shown beneath.

To change your mind, you can click **Withdraw**, so the recipient's message becomes invalid and that a new request can be raised afterwards if needed.

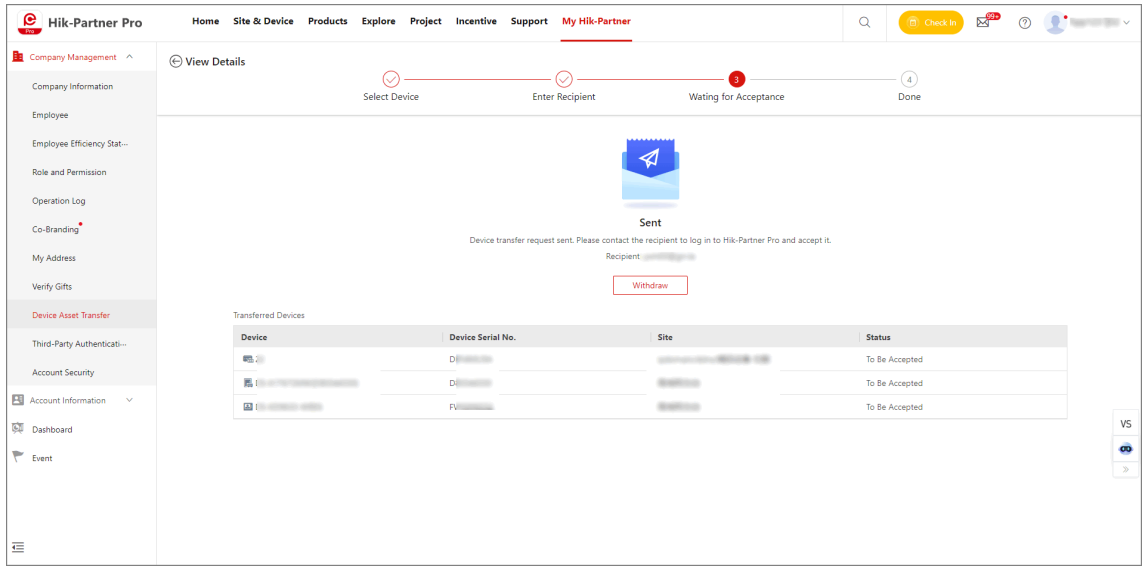


Figure 3-262 Submitted

Step 4: Done

Once the recipient has acted, this step settles into one of three outcomes.

Result	Description
Completed	The device transfer is complete.
Rejected	The request was rejected. Ask the recipient for details.
Withdrawn	The request was withdrawn. Raise a new one if needed.

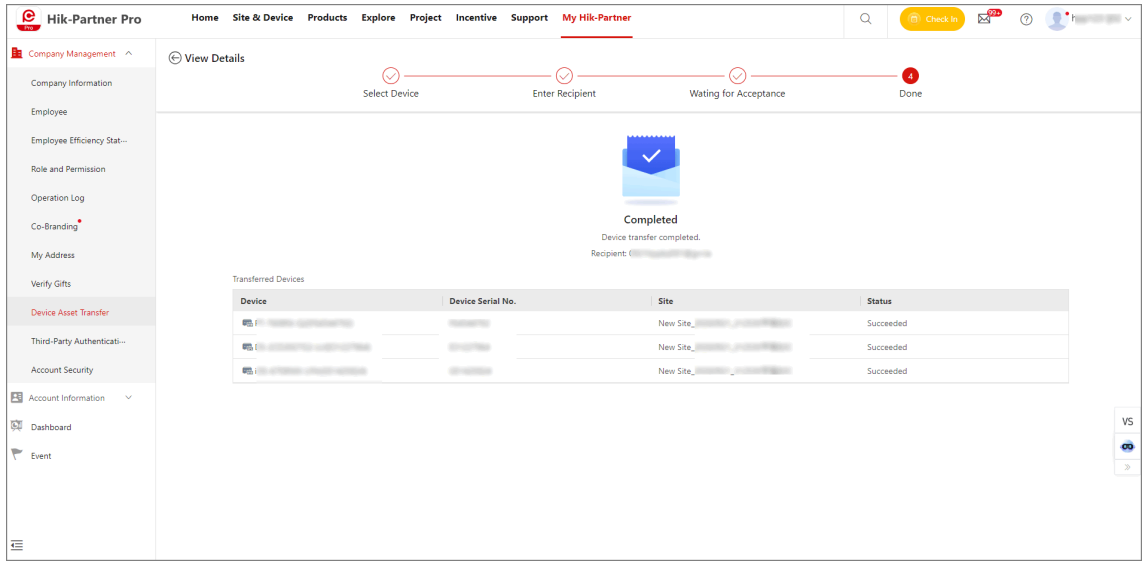


Figure 3-263 Result Page

For Recipient: Accept or Reject

- **Portal**: Go to **Site & Device → Message → Site Message** . Or click on the top right, and then click **Site Message**.

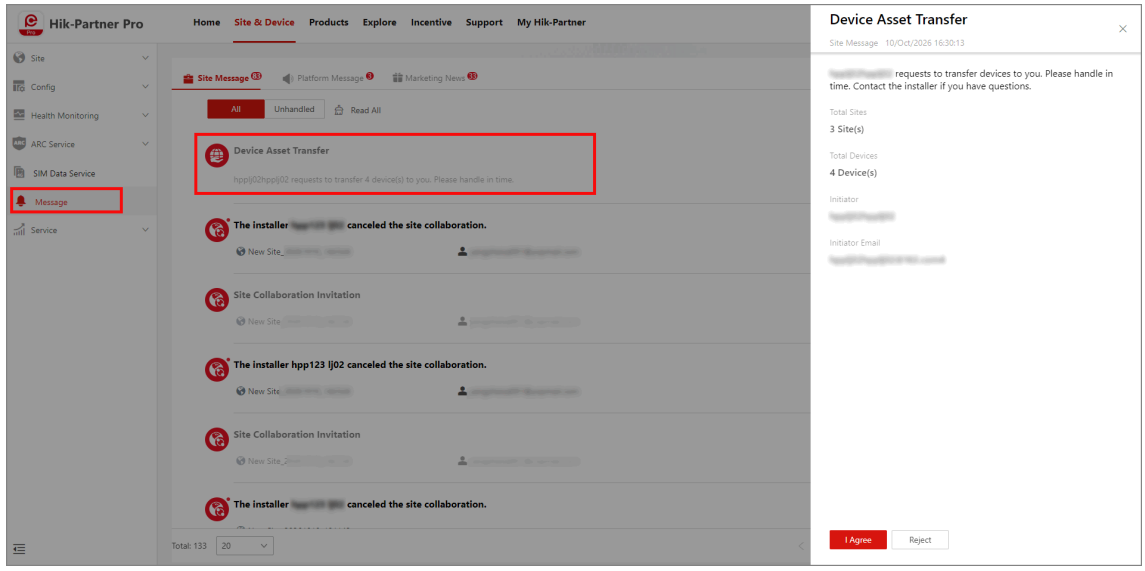


Figure 3-264 Transfer Message (Portal)

- **Mobile Client**: Tap on the top right of the Mobile Client, and then tap **Site Message**.

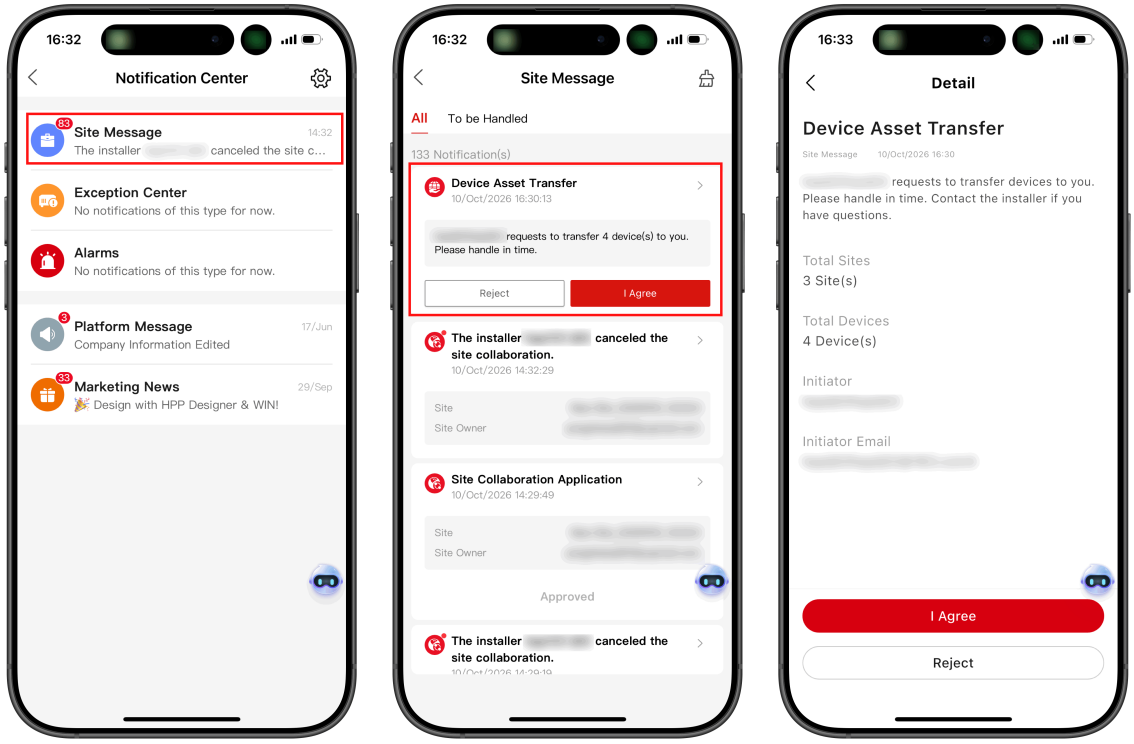


Figure 3-265 Transfer Notification (Mobile Client)

The message shows:

- The company is transferring devices to you and you can contact that installer if with any questions.
- **Total sites** and **total devices**.
- The **initiator** (the transferor's company name) and the **initiator's email**.

You can either accept or reject.

- Select **I Agree**: The platform then starts the transfer in the background.
- Select **Reject**: The transferor's received the rejection and a new request must be raised by the transferor if needed.

Transfer Records

The **Device Asset Transfer** page is the record list. Each row shows the **time it was raised**, the **device count**, the **recipient's email**, and the **status**.

Click any row to open **View Details**. The **Transferred Device** table lists each device with its serial number, site, and status. **Some devices can fail**, and any that still fail can be identified here by serial number for a support case.

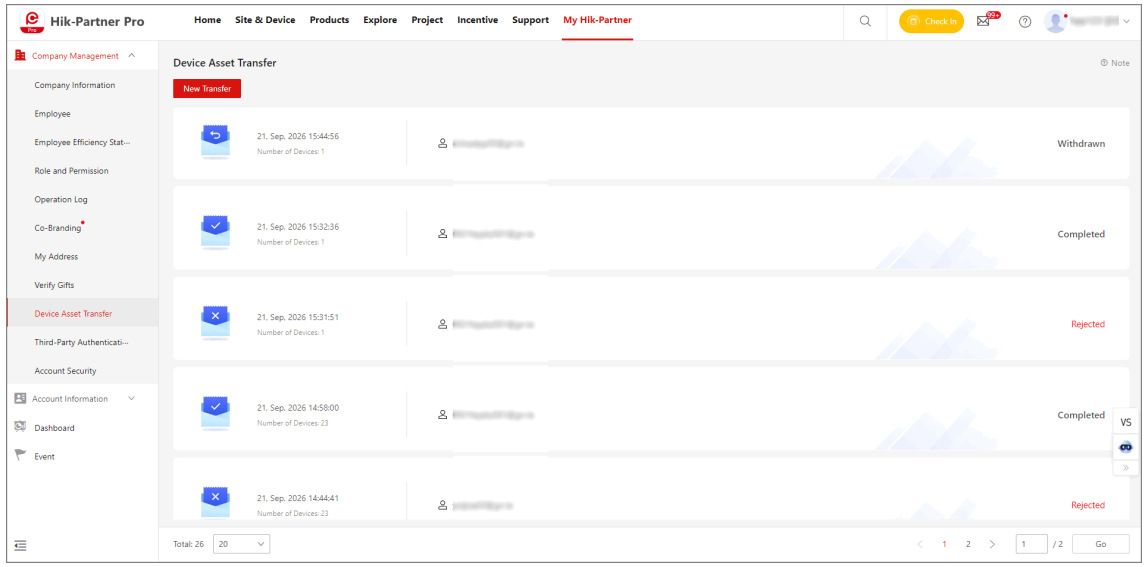


Figure 3-266 Transfer Record

What to Do After Transfer

The recipient:

1. Check the site and device counts against the notification.
2. Rebuild what did not come across: exception rules, linkage rules, health monitoring packages, and the accounts and permissions inside each security control panel.
3. If a site name has a time suffix, this means that a site of that name already existed and the platform added the suffix to avoid a clash. Rename it if you prefer.

The transferor:

1. Confirm the transferred devices have gone from your account.
2. Confirm that sites whose devices all moved have left your site list.
3. Keep the transfer record for reference.

Clients and Permissions at a Glance

Operation	Portal	Mobile Client	Permission
Initiate a transfer	Yes	No	Manage All Sites
Revoke a transfer	Yes	No	Manage All Sites
View records and details	Yes	No	Manage All Sites

Operation	Portal	Mobile Client	Permission
Receive, accept, or reject	Yes	Yes	An administrator with access to the notification center.
Receive the completion notice	Yes	Yes	An administrator with access to the notification center.

3.5.10 Merge Your Company with Another Company

If you and your colleague or employee have created more than one Installer Admin account (company) on Hik-Partner Pro, you can merge the companies into one for more efficient management and to carry on your business smoothly (you may have encountered the problem that your second registered account/company cannot be authenticated).

View of Company Merger

There are two modes of company merger, **Mode A** is to preserve Company B's assets, and **Mode B** does not or does not need to preserve Company B's assets.
Mode A: If you need to keep the assets of Company B after merger, the merger diagram is as follows.

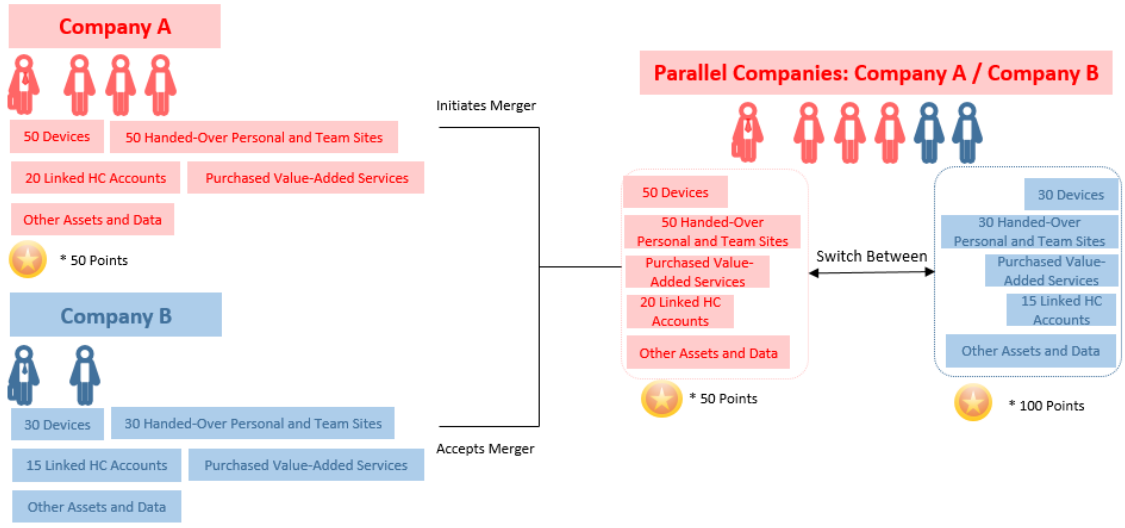


Figure 3-267 Mode A: View of Company Merger (To Keep Company B's Assets)

Mode B: If you do not need to keep Company B's assets or if Company B does not have any assets, the merger diagram is shown below.

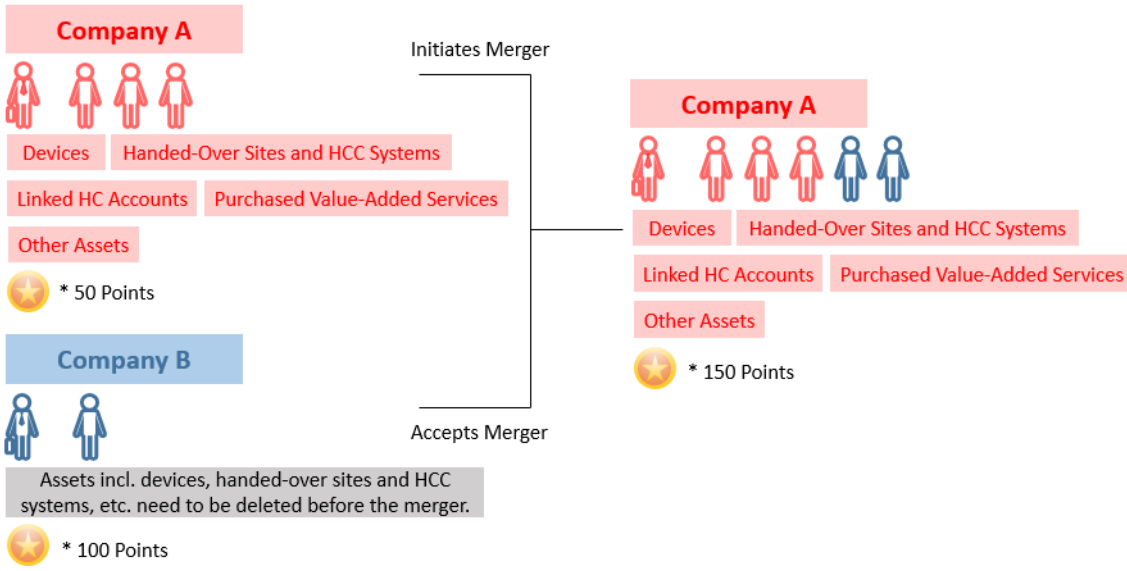


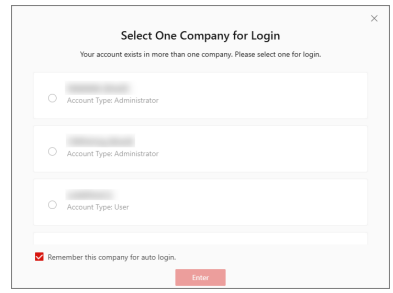
Figure 3-268 Mode B: View of Company Merger (No Need to Keep Company B's Assets)

Benefits of the Company Merger

- Manage your employees and the co-branding of your company via one account.
- Manage all your customers and their devices under one account.
- Get points faster to redeem for more gifts and value-added services.

Effects on the Accounts/Companies After the Merger

Installer Admin and Employee Accounts	• The Installer Admin who initiates the merger is still the Installer Admin. The Installer Admin of the invited company becomes an employee with the role of administrator under the initiating company. • All employee accounts of the invited company are migrated to the initiating company and become employees under the Installer Admin who initiates the merger. The employees that are already disabled will still be disabled after they are migrated. No matter whether the total number of free and purchased employee accounts (add-on) of the initiating company is insufficient or not, all employee accounts of the invited company will become limited accounts after the merger.

	If an employee has not become a Hik-Partner Pro user, they can still be migrated to the initiating company only if their previous Installer Admin has become a Hik-Partner Pro user. • If there is an account (email address) exists in both the initiating and invited companies before the merger, this account will still exist in both companies after the merger (in mode A) and will exist only in company A (in mode B), with its role the same as before.
Reward Points	Points of both companies will be combined and points history of both companies and all employees will be preserved.
Company Information	**Mode A:** Both companies' information will be preserved and you can switch between the two companies. **Mode B:** Only the information (company name, logo, address, authentication status, etc.) about the initiating company will be preserved.
Others	• **Mode A:** The two companies become parallel companies, all employees can switch between the two to manage devices, sites, services, etc.  **Figure 3-269 Switch Between Companies** • **Mode B:** The invited company will be deleted. • **Mode B:** All accounts of the invited company will be logged out after the merger. After they log in again, they will be in the initiating company.

	• If there are invited employees of the invited company who have not registered right before the merger, the links for registration will become invalid after the merger. • Likes, favorites, and comments of all accounts will be preserved.

Limitations

- This feature is not available in some countries/regions.
- Both the account that initiates the company merger and the account that is invited to merge companies need to be Installer Admin accounts, should have been upgraded to OneHikID accounts, and should have upgraded and become Hik-Partner Pro users.
- The invited company cannot be an authenticated channel partner, or be added to the ARC list already.
- The initiator's account and the invited account need to be in the same country/region.

Initiate Company Merger

Note

If the company merger is initiated by Hikvision, you do not need to initiate the merger manually.

1. Initiate a merger and send the company merger invitation by entering the Installer Admin account of the invited company. The invited company will be able to see your company name and your email address.
2. Contact the invited Installer Admin (who will receive an email and a message reminder) to log in to Hik-Partner Pro and accept the company merger request in the Notification Center.

Initiate Company Merger Using the Portal

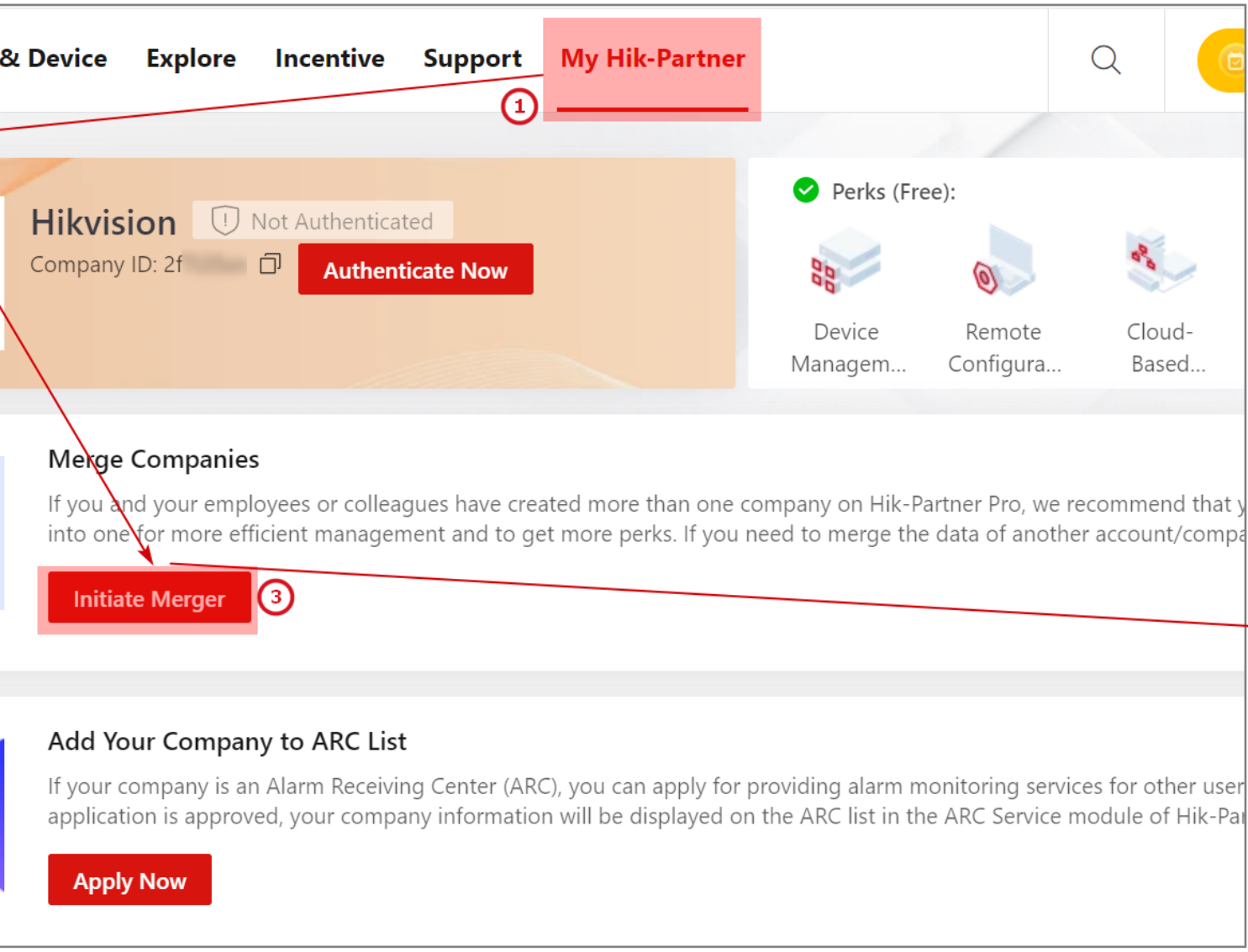


Figure 3-270 Initiate Company Merger Using the Portal

Initiate Company Merger Using the Mobile Client

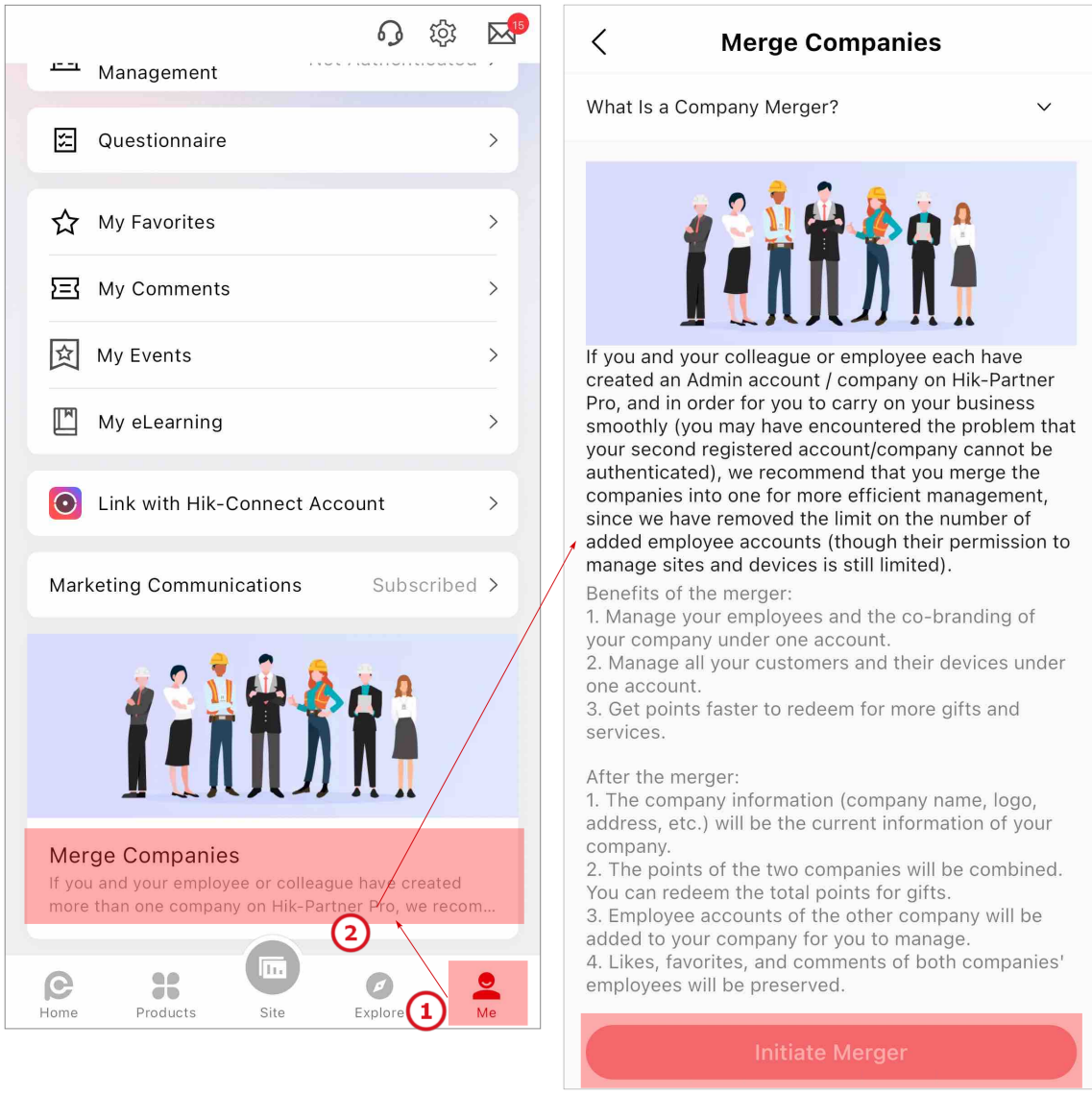


Figure 3-271 Initiate Company Merger Using the Mobile Client

Handle Company Merger Invitations

For the Merger Initiated by Another Company

Go to the notification center, select **Site Message**, and select the company merger notification to handle it.

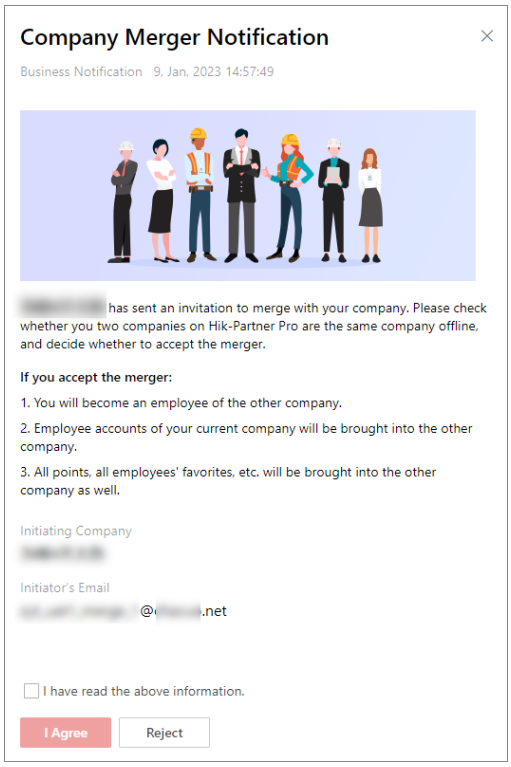


Figure 3-272 Company Merger Notification (Portal)

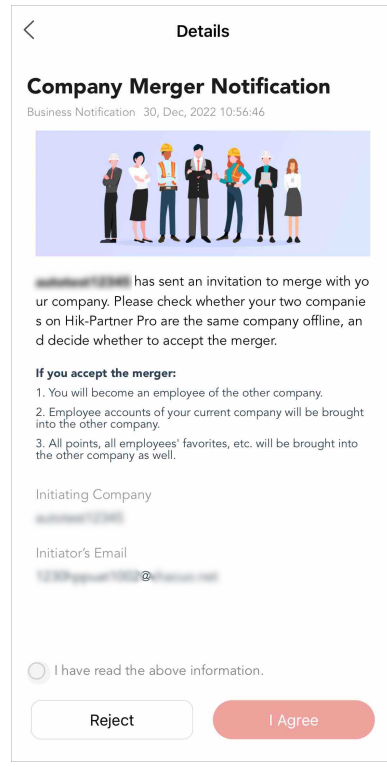


Figure 3-273 Company Merger Notification (Mobile Client)

For the Merger Initiated by Hikvision

If a company merger is initiated by Hikvision, after both companies to be merged agree to the merger, and the company (Company B) to be merged into the other company (Company A) does not have assets under their account, the company merger completes.

1. The Installer Admin of Company B first receives the merger message as a platform message in the Notification Center or upon login.



Figure 3-274 Company B Receives the Message in Notification Center

2. After Company B accepts the merger, the Installer Admin of Company A receives the platform message of the merger.

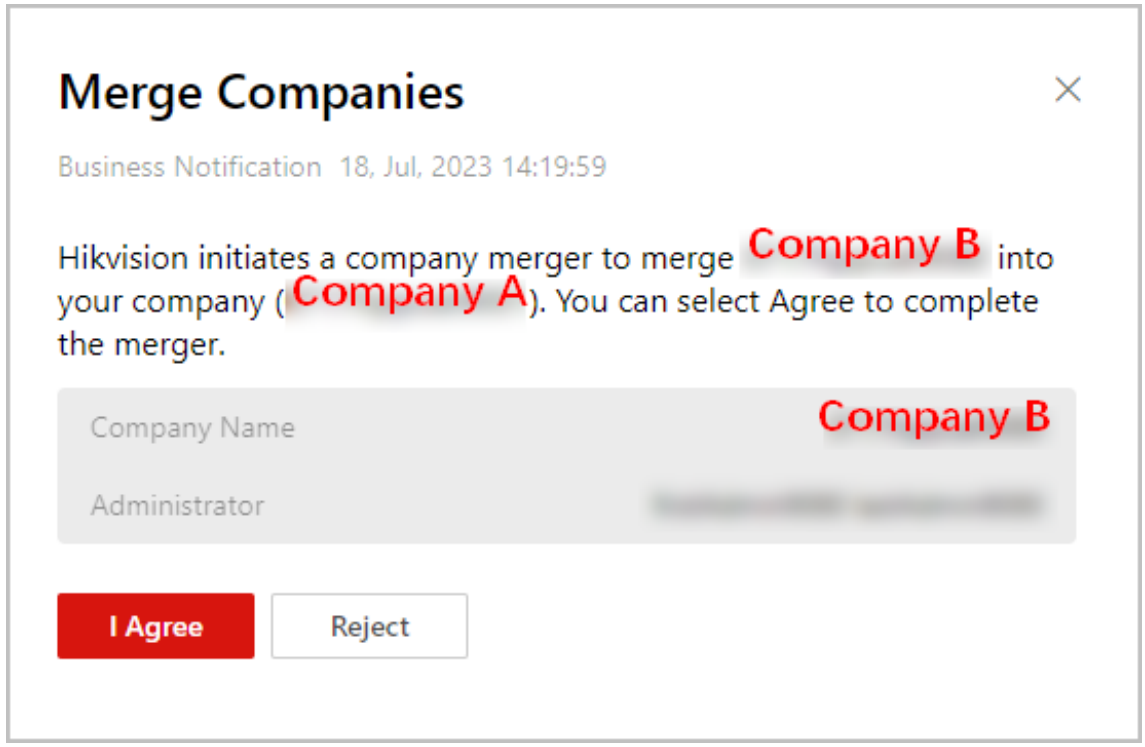


Figure 3-275 Company A Receives the Message in Notification Center

Chapter 4 Template Center: How to Use Device Configuration and Handover Templates

4.1 What This Is and When to Use It

4.1.1 In One Sentence

The **Template Center** lets a company do two repetitive things once and then reuse them: **which permissions you or a customer gets when a site is handed over** (handover templates), and **how an AX PRO panel should be configured** (device configuration templates).

4.1.2 Two Kinds of Templates

Item	Handover Template	Device Configuration Template
What it controls	Which permissions the customer receives at handover, and which you keep for maintenance.	An AX PRO panel's business parameters: zones, areas, arming schedules, communication settings.
What it holds	A method (transfer or share) plus the permissions and validity chosen per device type.	The full configuration read from one source device.
Who configures it	Someone with **Manage All Sites** permission, usually the company administrator.	Someone with **Manage All Sites** permission, usually the company administrator.
Who uses it	Field installers, picking one when handing a site over in the Mobile Client.	Anyone with configuration permission on the target device.
Where to configure and use	Configured on the Portal, used in the Mobile Client.	Either client, for both.
Limit	3 per company.	10 per company.
Devices covered	Every device type supporting transfer or share handover.	AX PRO 1.3.x only.
In this guide	• ***Handover Templates: Create One on the Portal*** • ***Handover Templates: Manage and Use***	• ***Device Configuration Templates: Create One*** • ***Device Configuration Templates: Manage and Use***

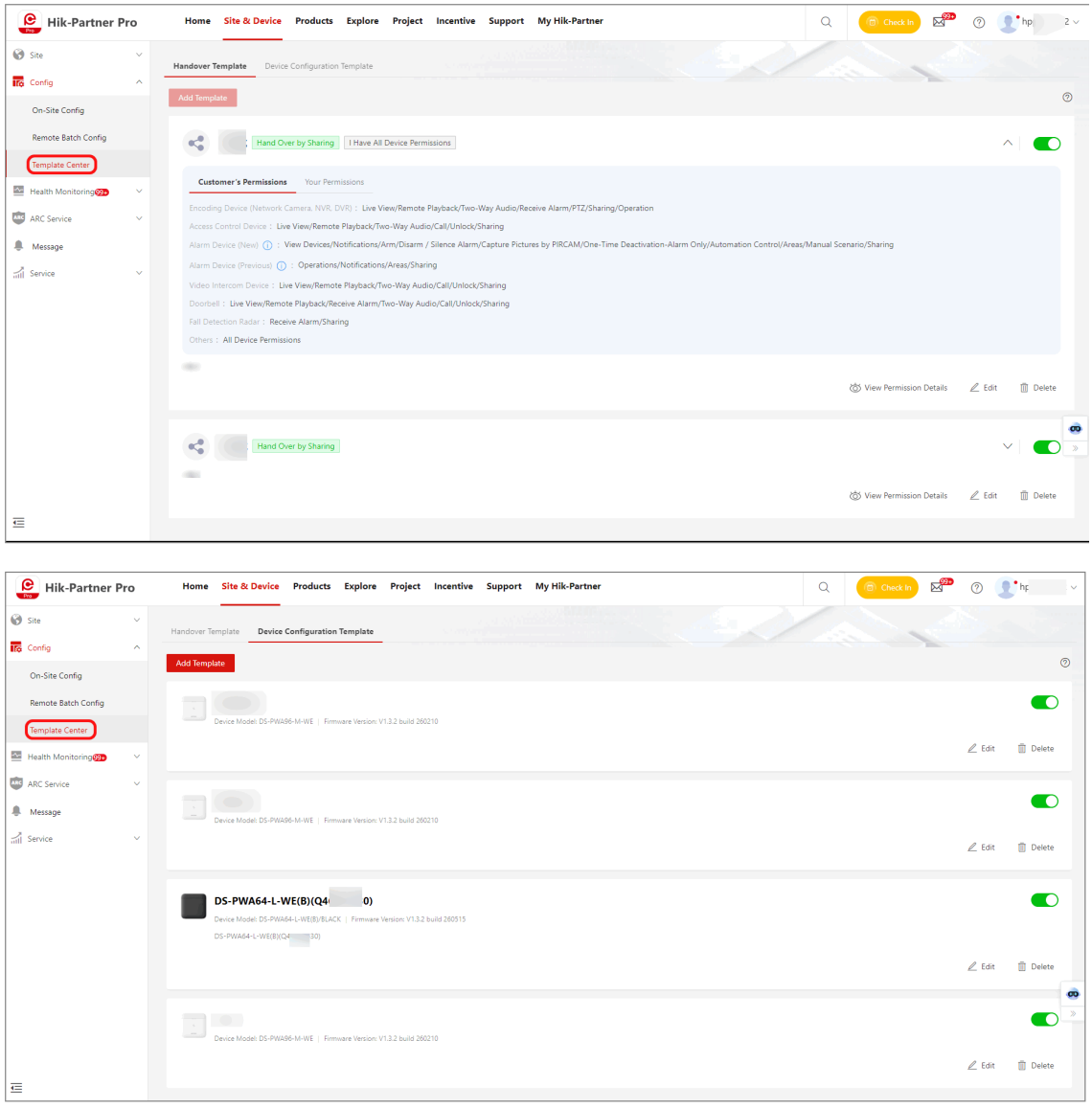


Figure 4-1 Two Tabs of the Portal Template Center

4.1.3 Typical Scenarios

Handover Templates

Bulk Handover at an ARC Company. A monitoring company with a hundred-odd installers always hands alarm devices over by sharing and video devices by transferring. The administrator configures two templates and the installer simply picks one on site.

Device Configuration Templates

- **Standardizing a retail chain.** A pharmacy chain opens 100 stores with identical alarm strategy. Tune the first store, capture it as "pharmacy standard", and at the remaining 99 the installer only has to add the devices, pick the template, and apply.
- **Copying across sites.** A template can be taken from a device in any site and applied to a panel of the same model in any other site. Site boundaries do not restrict it.

4.1.4 Clients and Permissions at a Glance

Operation	Portal	Mobile Client	Permission
Handover template: View the list	Yes	No	Site management permission; without **Manage All Sites** the permission detail is hidden.
Handover template: Create, edit, enable, delete	Yes	No	**Manage All Sites** permission
Handover template: Hand a site over using one template	No	Yes	Site management permission.
Device configuration template: View the list	Yes	Yes	Unrestricted
Device configuration template: Create, edit, enable, delete	Yes	Yes	**Manage All Sites** permission
Device configuration template: Apply to a panel	Yes	Yes	Configuration permission on that target panel.

4.1.5 Scope

Table 4-1 Scope

Item	Handover template	Device configuration template
Hardware	Any device type supporting transfer or share handover.	AX PRO 1.3.x panels and their peripherals.
Site type	Personal sites only.	Personal sites only.
Limit	3 per company across both methods.	10 per company.
Charging	Free	Free

4.2 Handover Templates: Create One on the Portal

4.2.1 Step 1: Set Name and Method

Choose the handover method first, the permission step that follows depends on the handover method you choose.

1. Go to **Site & Device → Config → Template Center → Handover Template** .

   Note

   - **Users without Manage All Sites permission do not see the page**. If you need to configure a template and cannot find the page, ask a colleague who holds that permission.
   - The handover template cannot be configured on the Mobile Client.

2. Click **Add Template**.
3. Set the name (required) and handover method (required).
   - **Transfer**: The devices move to the customer, who owns them.
   - **Share**: The devices are shared with the customer, who may only use them.
4. Set the remarks (optional) if needed.

   Note

   Remarks are shown to field staff and are **the only thing they have to go on when choosing a template**. The Mobile Client does not show the permission detail, so make the remarks explicit, for example "video projects only; customer views but does not configure".

5. Click **Next**.

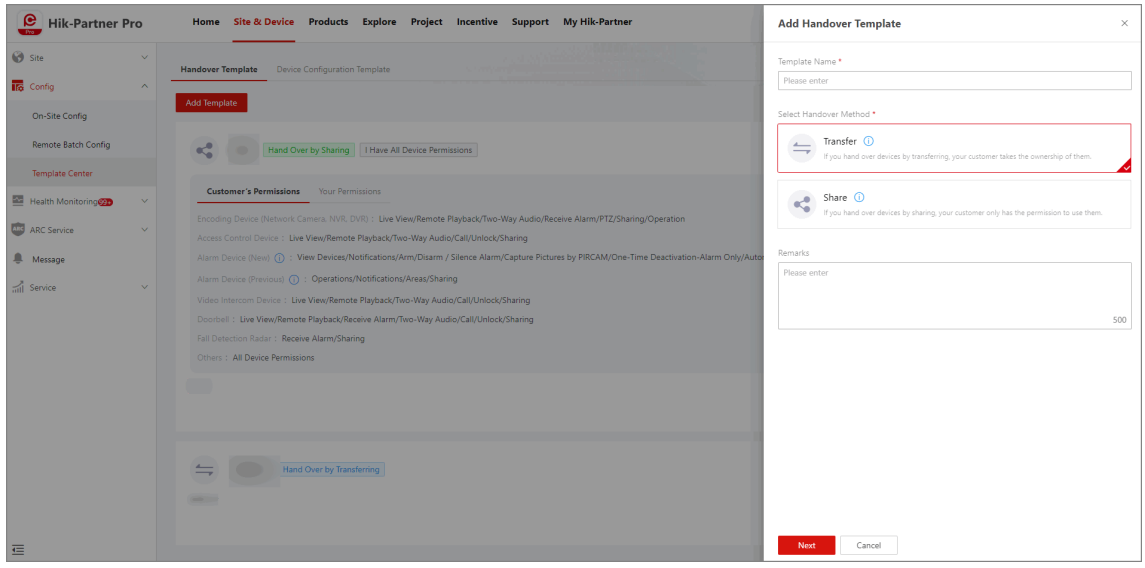


Figure 4-2 Add Handover Template

4.2.2 Step 2: Set Permissions

Transfer: What You Keep for Maintenance

On the **Your Permissions** page, choose what you need to request from the customer in order to maintain the system remotely. Then click **Confirm**.

Note

The devices in this transfer scenario now belong to the customer, so continued maintenance means asking for permission, and this page defines that request.

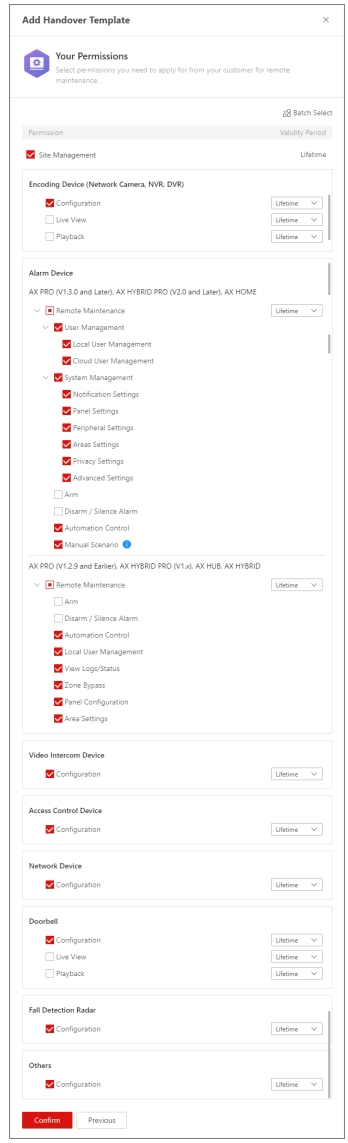


Figure 4-3 Your Permissions

The layout:

- Two columns: **Permission** and **Validity Period**.
- **Site Management** is ticked by default with a fixed validity of **Lifetime**.
- Below it, groups per device type. For example, **Video Devices (Network Camera, NVR, DVR)** holds **Configuration**, **Live view**, and **Playback** permissions. Access control, video intercom, alarm, network, doorbell, fall detection radar and other devices each have their own. **Every permission item has its own validity dropdown.**
- **Batch Select** at the top right sets the first-level permission and validity for a whole device type at once.

Transfer allows you to tick nothing at all: when you will not be maintaining the system after handover.

Share: First the Customer, Then Yourself

Share has **two** pages: first what the customer gets, then what you keep.

On the **Customer's Permissions** page, set what will be shared with the customer, and click **Next**.

Unlike transfer, this page enforces **two rules**:

1. **At least one device sharing permission must be selected.**
2. **Alarm devices must include the Areas permission.**

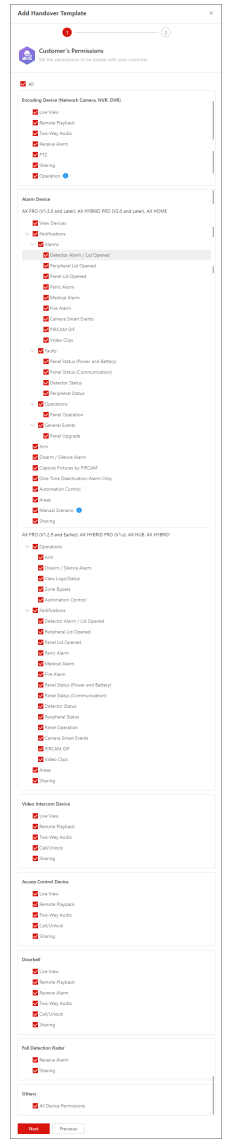


Figure 4-4 Customer's Permissions

On the **Your Permissions** page, set the permissions you request for your own remote maintenance (same as that for the transfer scenario) and click **Confirm**. The difference is a switch at the top:

I Have All Device Permissions: I already have every permission on these devices and need not request any from the customer.

- Turning it on makes this a **peer share**: nothing needs requesting for your remote maintenance, you have all permissions by default.

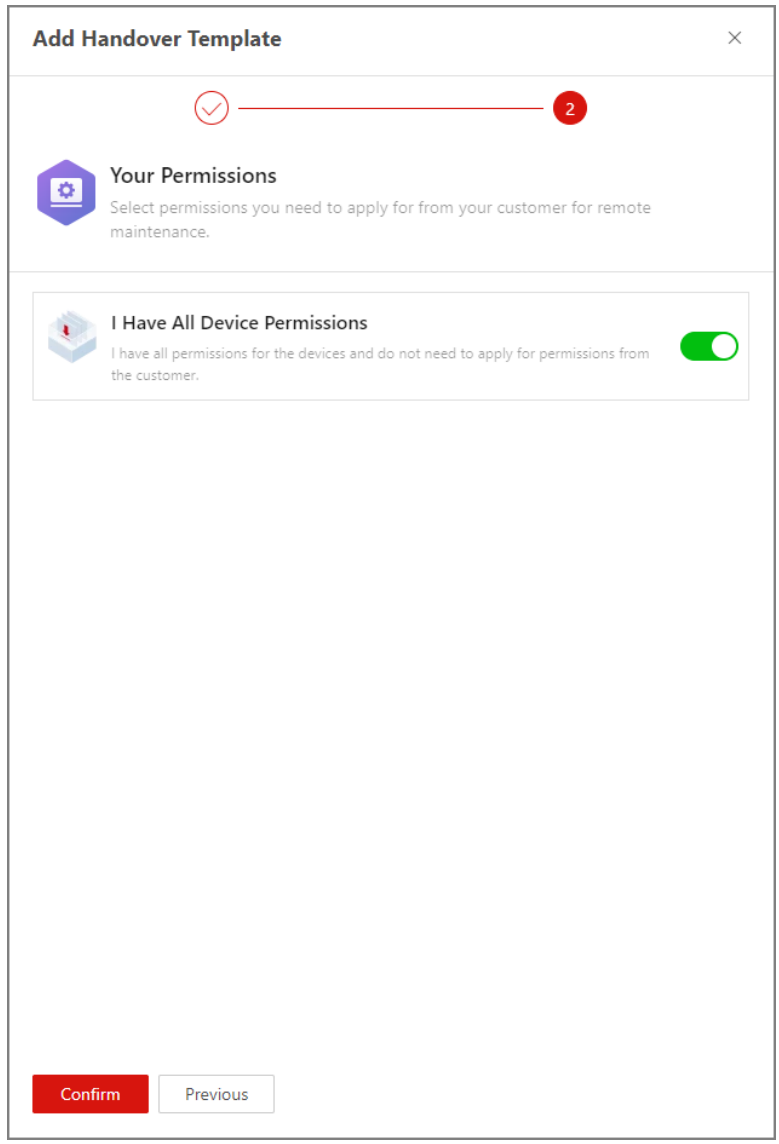


Figure 4-5 Peer Share

- Turning it off, it is a **non-peer share**: you need to request permission item by item, and at handover the customer is additionally asked for privacy permissions.

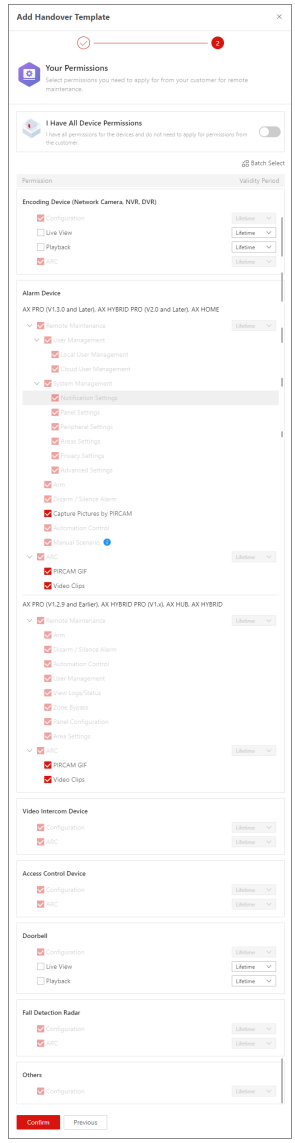


Figure 4-6 Non-peer Share

4.3 Handover Templates: Manage and Use

4.3.1 Manage Handover Templates on the Portal

- View what a template grants.
  Click **View Permission Details** to open the **Permission Details** dialog with two tabs:
  - **Customer's Permissions**: What they receive.

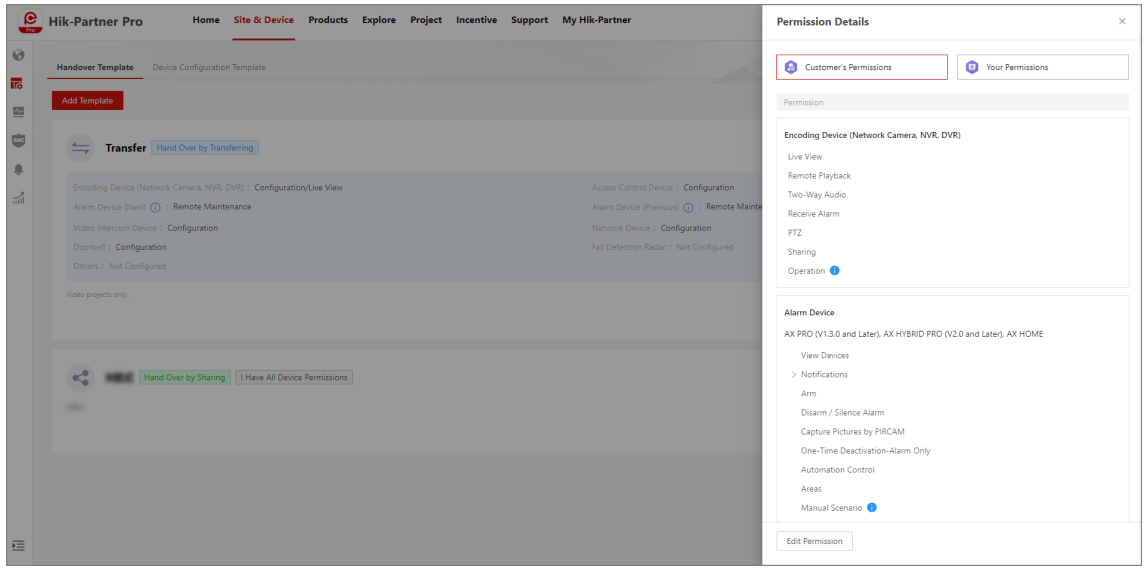


Figure 4-7 Customer's Permissions

- **Your Permissions**: What you keep.

Note

For a transfer template only **Your Permissions** has content.

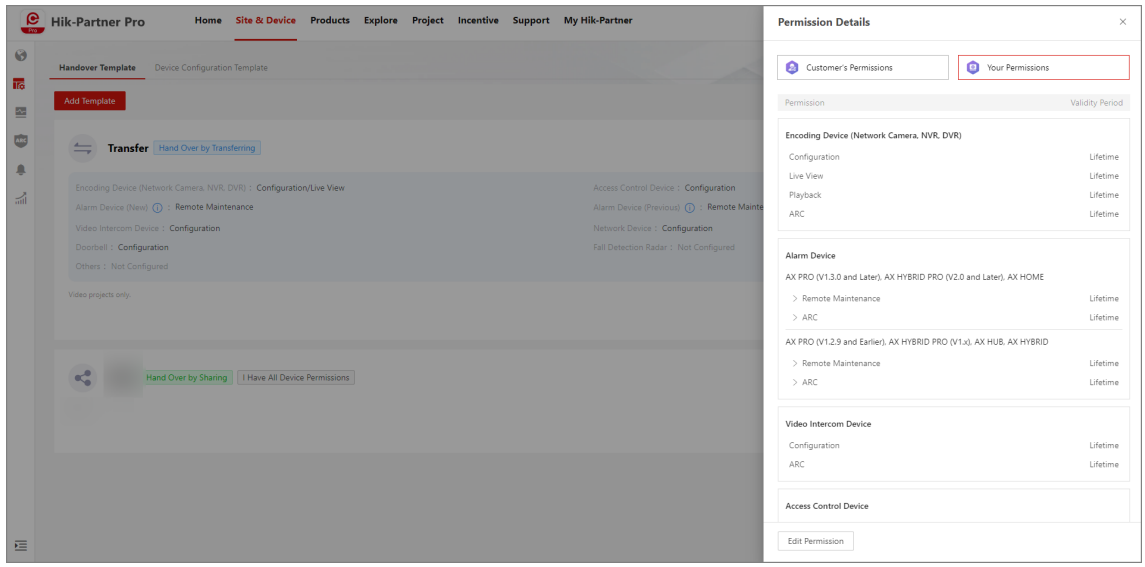


Figure 4-8 Your Permissions

- Click **Edit** to rename a template and edit remarks.
- Click **View Permission Details → Edit Permission** to change device permissions and validity.
- Turn on/off the switch to enable/disable a template.

- Click **Delete** to delete a template.
- The handover method cannot be edited.

Field	Editable
Template name	Yes
Remarks	Yes
Device permissions and validity	Yes
Handover method	**No**
Peer or non-peer sharing	**No**

4.3.2 Hand Over with a Template on the Mobile Client

1. Open a site that has not been handed over and tap **Hand Over Site** at the bottom.

   Note

   When you add devices in bulk with the SADP tool, and **when the company has usable templates,** you can also select a handover template.

2. The **Hand Over Site** panel opens: the administrator has configured handover templates, tap to choose one.

   Note

   You can also tap **Customize Handover** at the bottom to return to the manual flow.

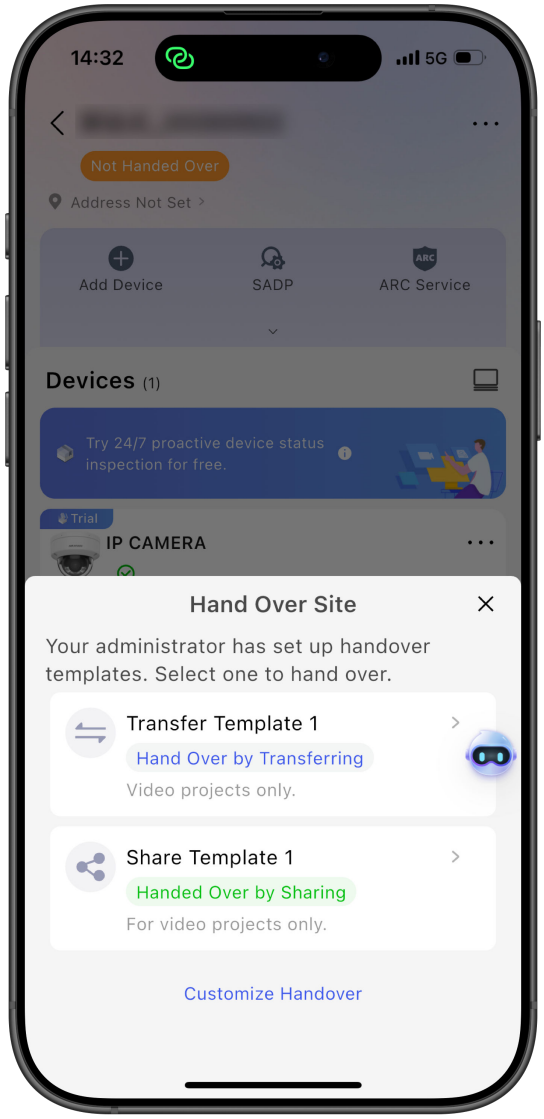


Figure 4-9 Handover Template

3. Once the template is chosen and the end user's details are in, the **Handover** page offers two ways to complete it:
   - **QR Code**: The customer scans it with Hik-Connect. On a share handover the code can be scanned by several customers.
   - **Phone Number / Email**: Enter the end user's account.

   A peer share adds a note that the customer administrator will review the permissions you requested, plus a **Hand Over to More Customers** entry.

4.4 Device Configuration Templates: Create One

4.4.1 Prerequisites

1. You hold the **Administrator permission**.
2. The AX PRO panel (source device) you want to mirror is **online**.
3. Your company has not reached the limit of 10 device configuration templates.

4.4.2 Create a Device Configuration Template Using the Portal

1. Choose either of the following two ways to add a device configuration template:
   - **Go to the Template Center.**
     Go to **Site & Device → Config → Template Center → Device Configuration Template** . Click **Add Template**.

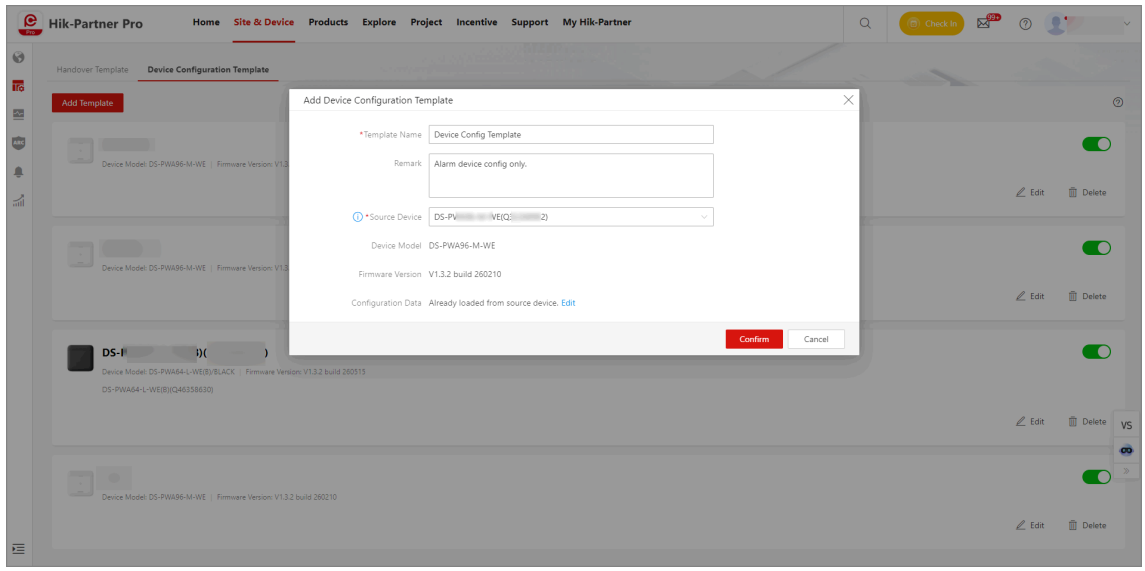


Figure 4-10 Template Center

   - **Go to the site device list.**
     Find the device. Click the device's **…** → **Save as Template** .

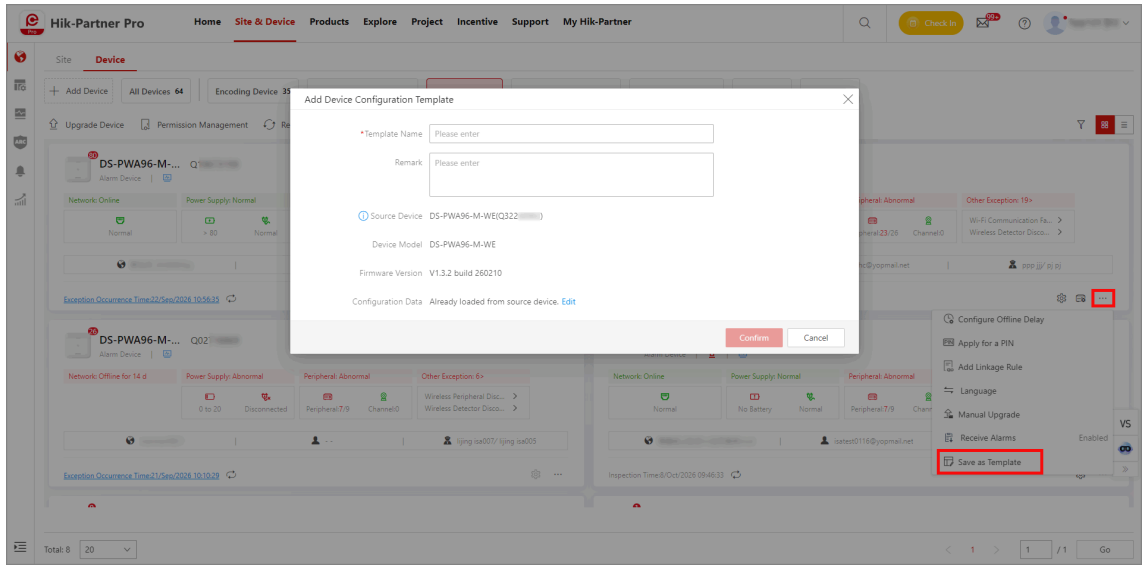


Figure 4-11 Save as Template

2. Set the template name, remark, and source device (if not set yet).
3. Once the mirror device is chosen, **device model**, **firmware version**, and **configuration data** are read and filled in automatically.
4. Adjust the configuration data. Once the configuration data has been read, click **Edit** to open a **virtual remote configuration page** and to adjust the configuration.

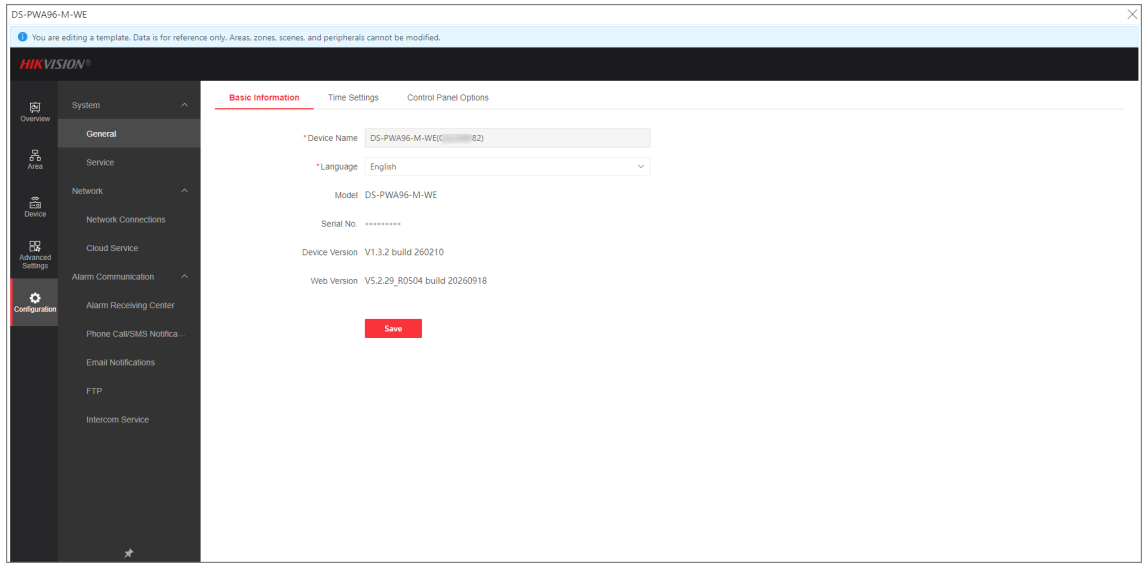


Figure 4-12 Edit Configuration Data

5. Return to the add-template form and click **Confirm**.

4.4.3 Create a Device Configuration Template Using the Mobile Client

1. Choose either of the following two ways to add a device configuration template:
   - **Go to the Template Center.** The Mobile Client has two entry points:
     - **Toolkit → Device → Batch Config → Template Center** . Tap **Add Template**.
     - Tap **Template Center** in the shortcut row at the top of the **Site** page. Tap **Add Template**.

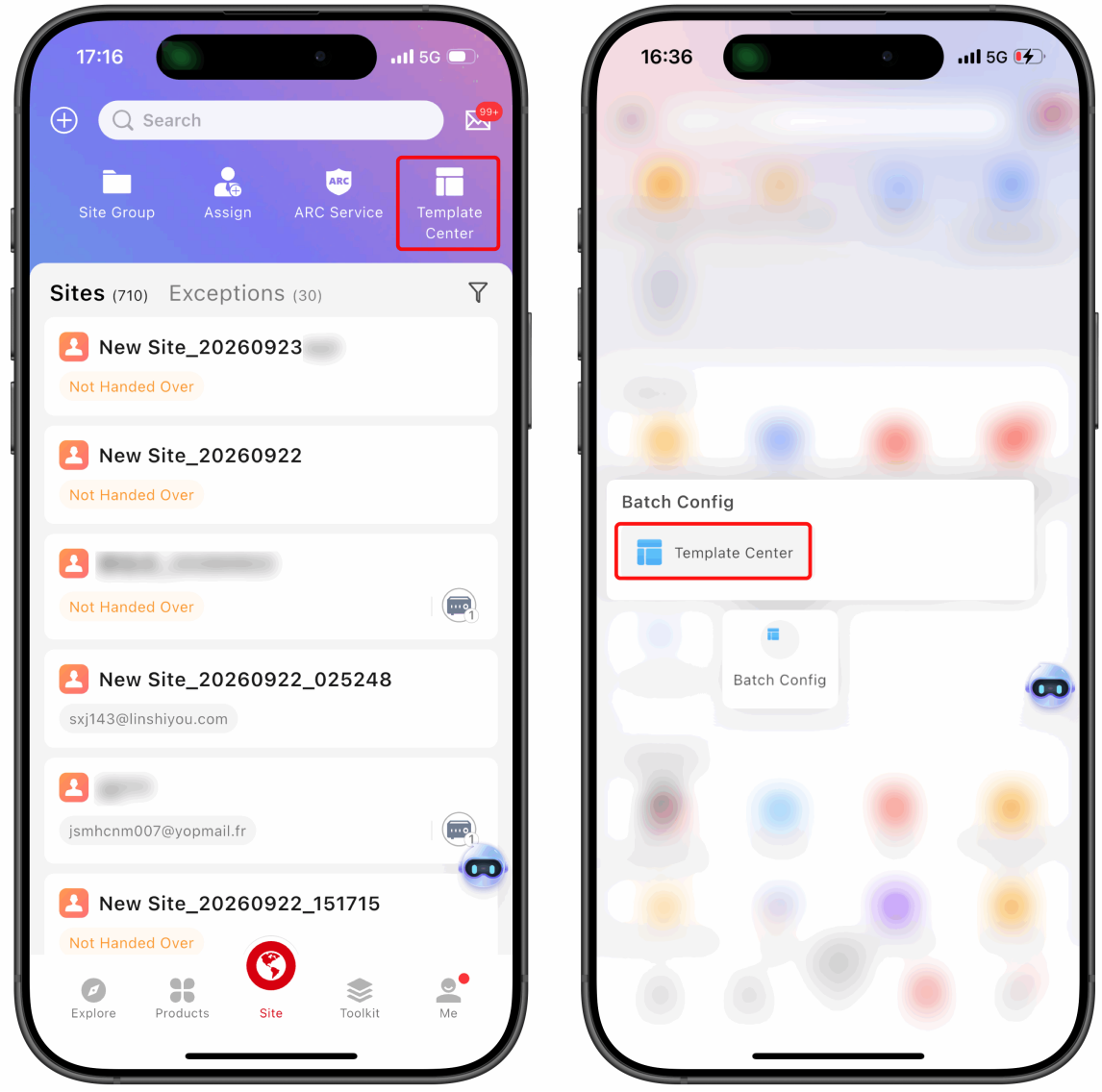


Figure 4-13 Two Entries

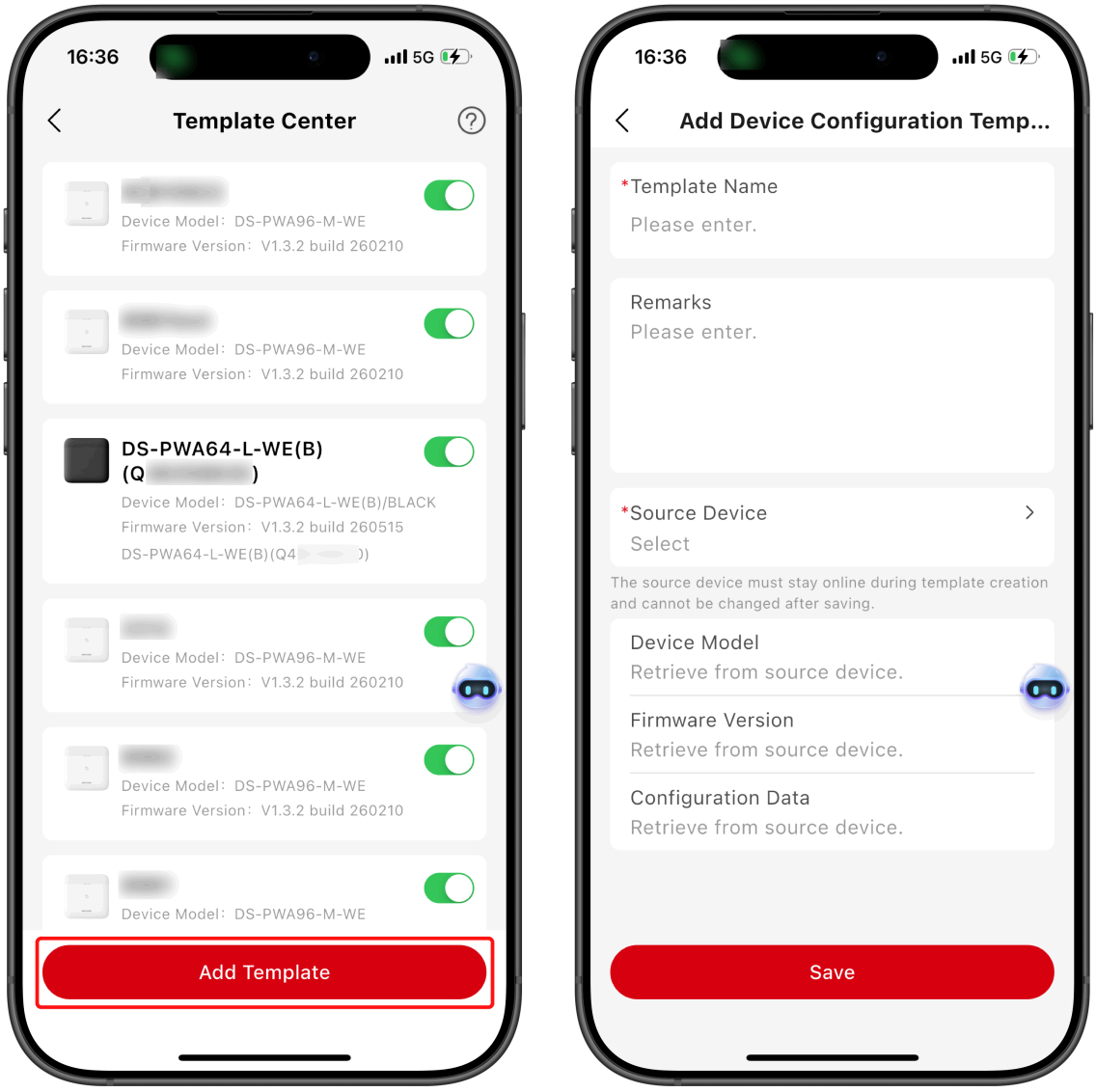


Figure 4-14 Add Template

- **Go to the site device list.**
  Find the device. Tap the device's **…** → **Save as Template** .

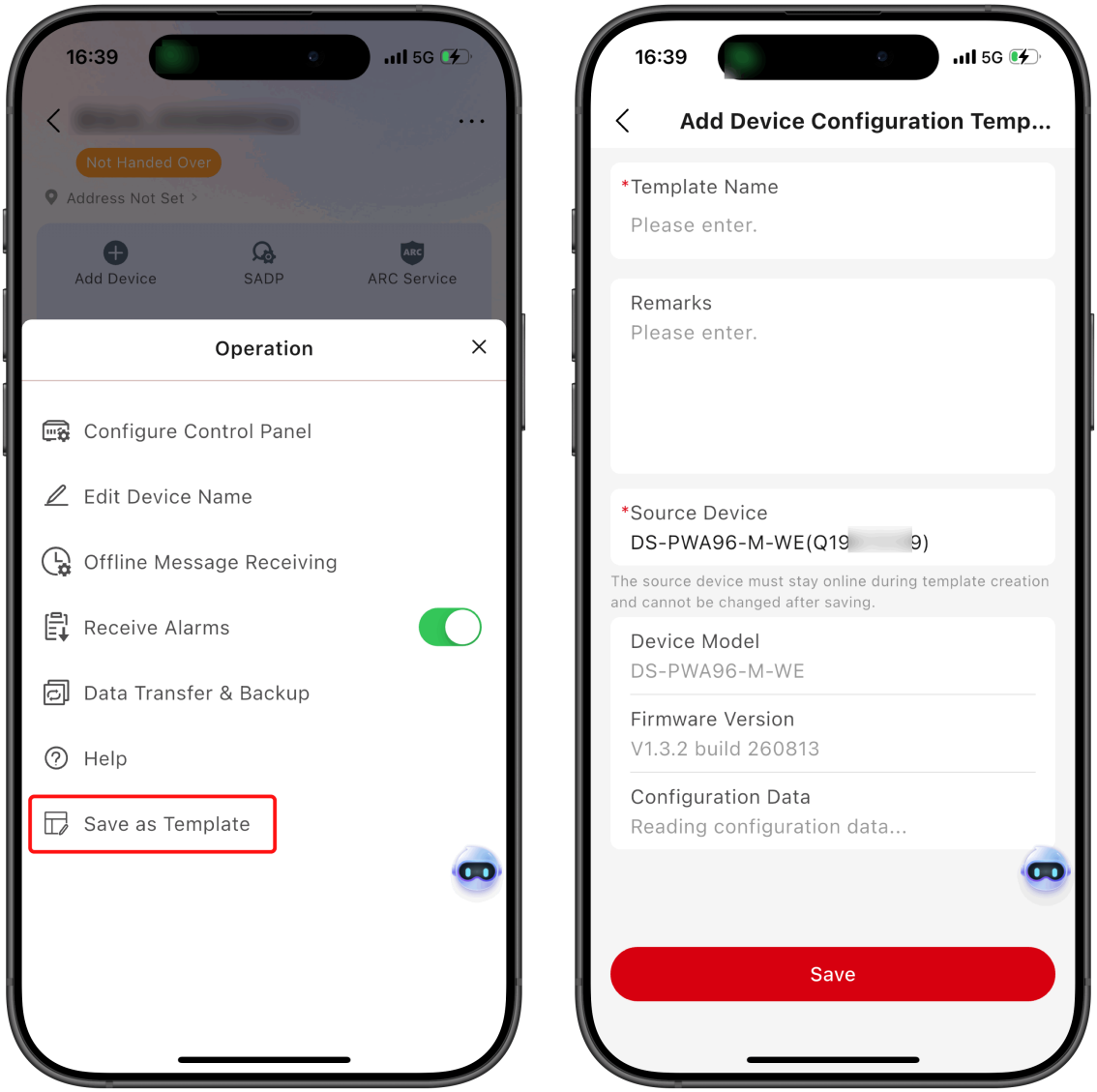


Figure 4-15 Save as Template

2. Set the template name, remark, and source device (if not set yet).
3. Once the mirror device is chosen, **device model**, **firmware version**, and **configuration data** are read and filled in automatically.
4. Adjust the configuration data. Once the configuration data has been read, tap **Configuration Data** to open a **virtual remote configuration page** and to adjust the configuration.

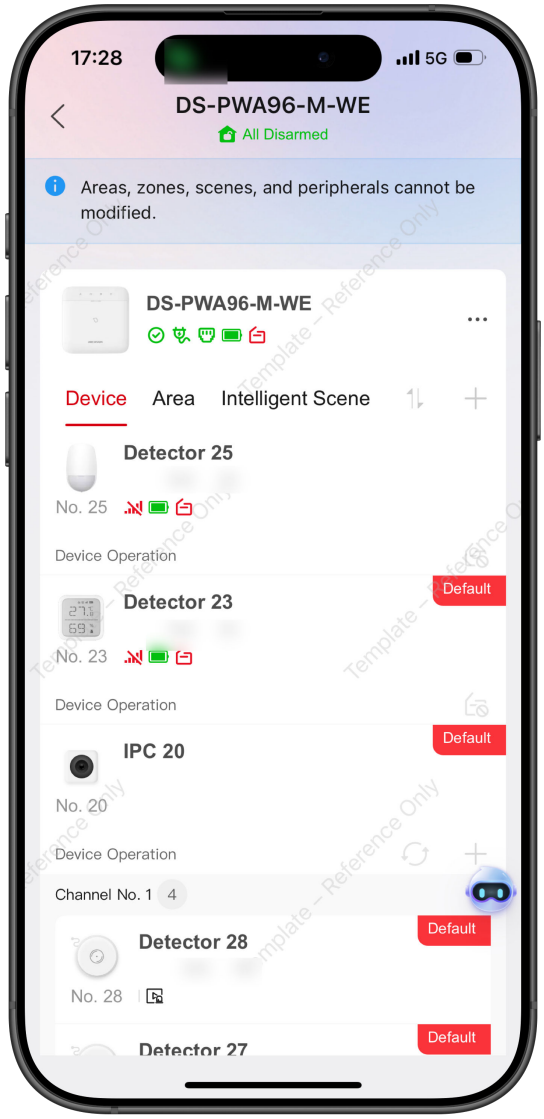


Figure 4-16 Edit Configuration Data

5. Return to the add-template form and tap **Save**.

4.5 Device Configuration Templates: Manage and Use

4.5.1 Manage Device Configuration Templates in Template Center

Portal: Site & Device → Config → Template Center → Device Configuration Template .

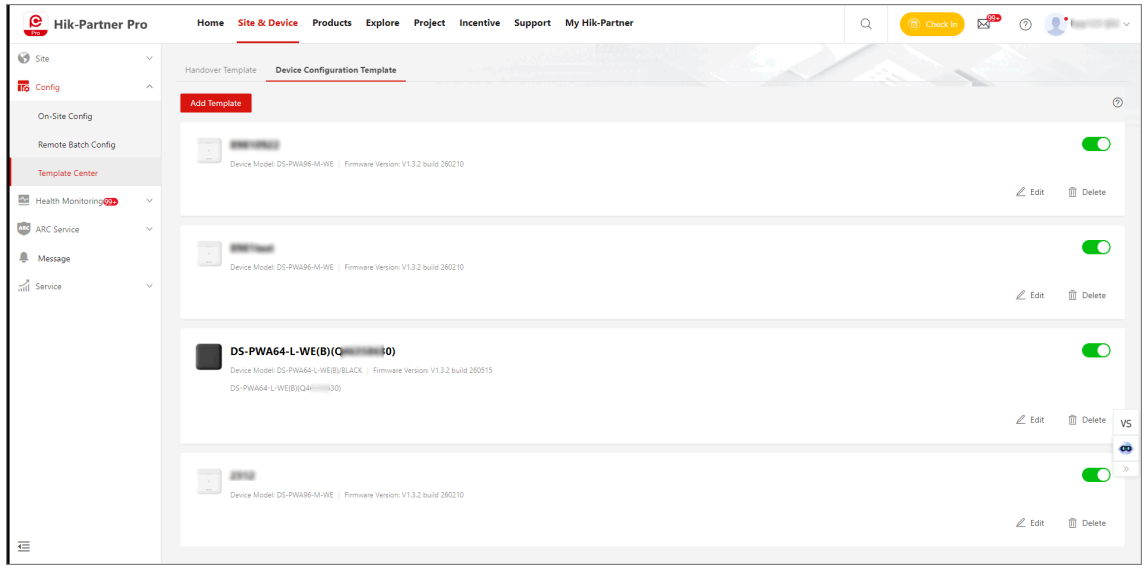


Figure 4-17 Template Center (Portal)

Mobile Client has two entry points:

- **Toolkit → Device → Batch Config → Template Center** .
- **Template Center** in the shortcut row at the top of the **Site** page.

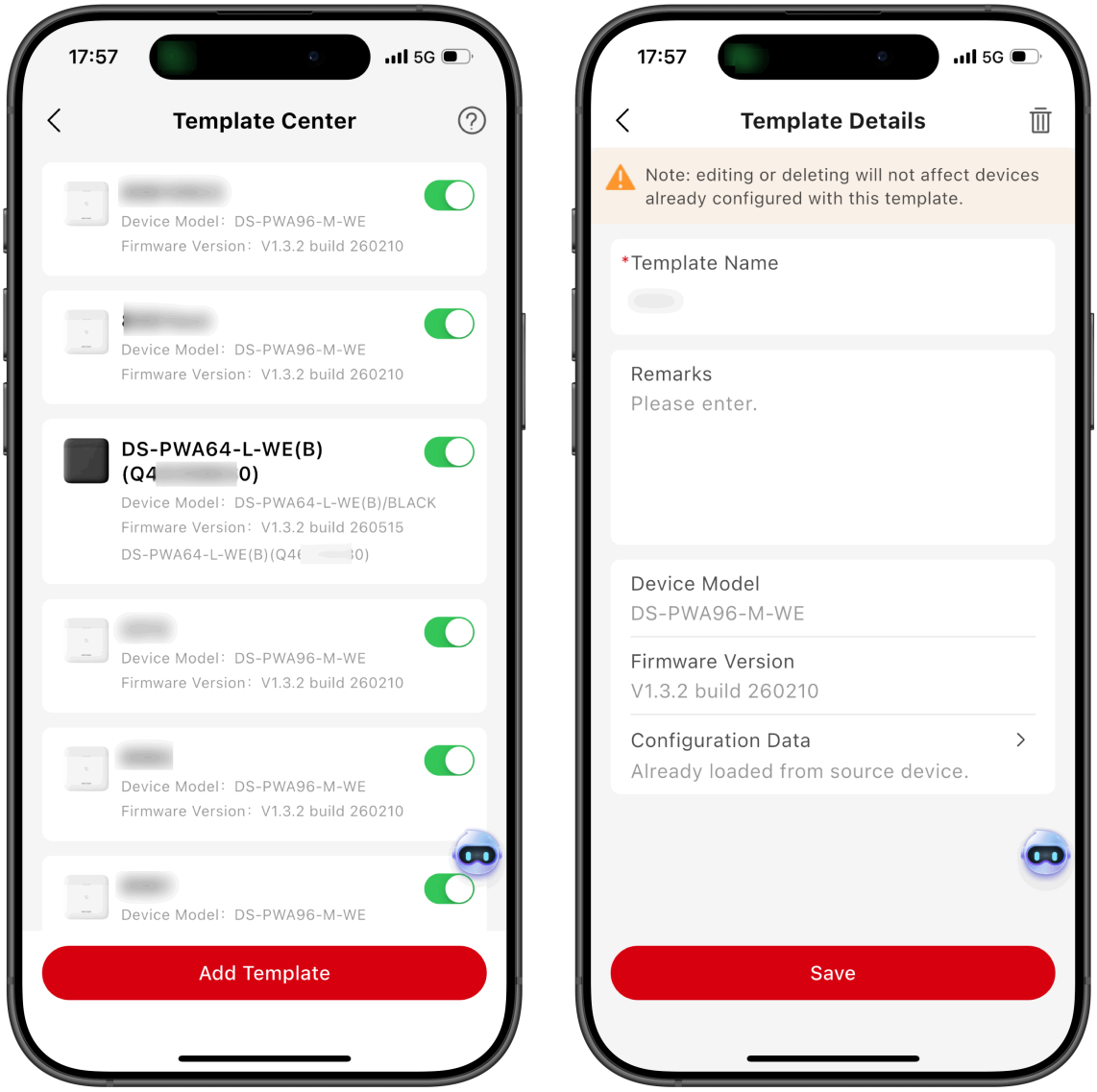


Figure 4-18 Template Center (Mobile Client)

Each card shows the template name, **device model**, **firmware version**, and remarks, with an **enable switch** on the right. You can also **Edit** and **Delete**.

Table 4-2 What Can and Cannot Be Changed

Field	Editable
Template name	Yes
Remarks	Yes
Configuration data	Yes, through the virtual configuration page

Field	Editable
Device model	No, display only
Firmware version	No, display only
Source device	No, fixed once saved

4.5.2 Apply Device Configuration Template to Device

Prerequisites for Applying

1. You have **device configuration permission** on the target device.
2. The target panel is **online** and its model matches the template.
3. At least one template is **enabled**.
4. **All peripherals have been added and the target panel is disarmed.**

Apply Template to Device Using the Portal

1. Go to **Site & Device → Customer Site** . Find the deice, click the **Configure Control Panel** icon on an AX PRO card or list row.

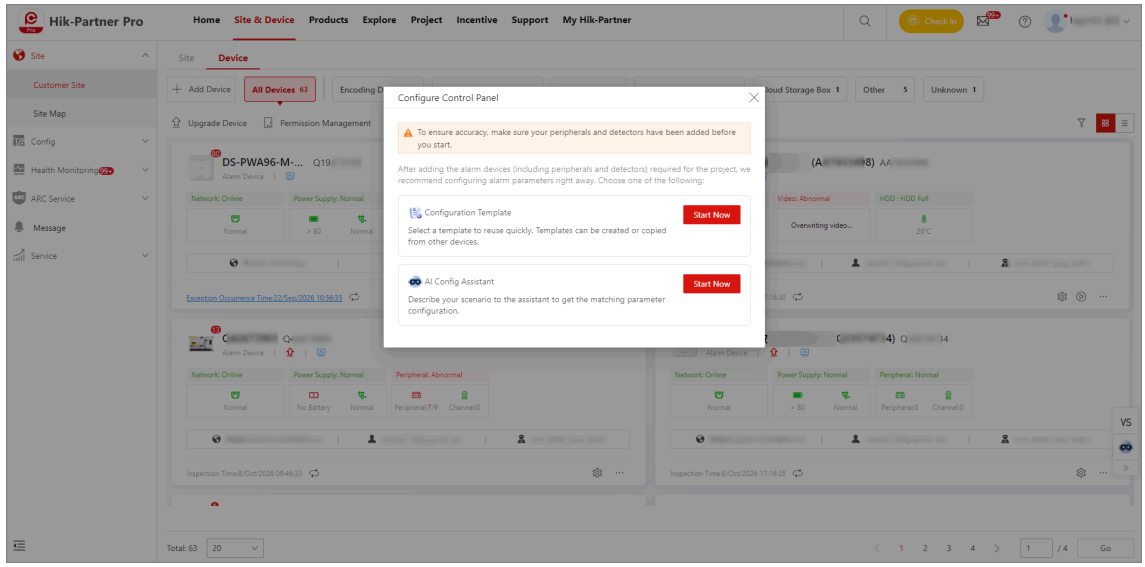


Figure 4-19 Smart Config

2. Click **Start Now** in the **Configuration Template** section. Follow the two steps:
   a. Select a template.

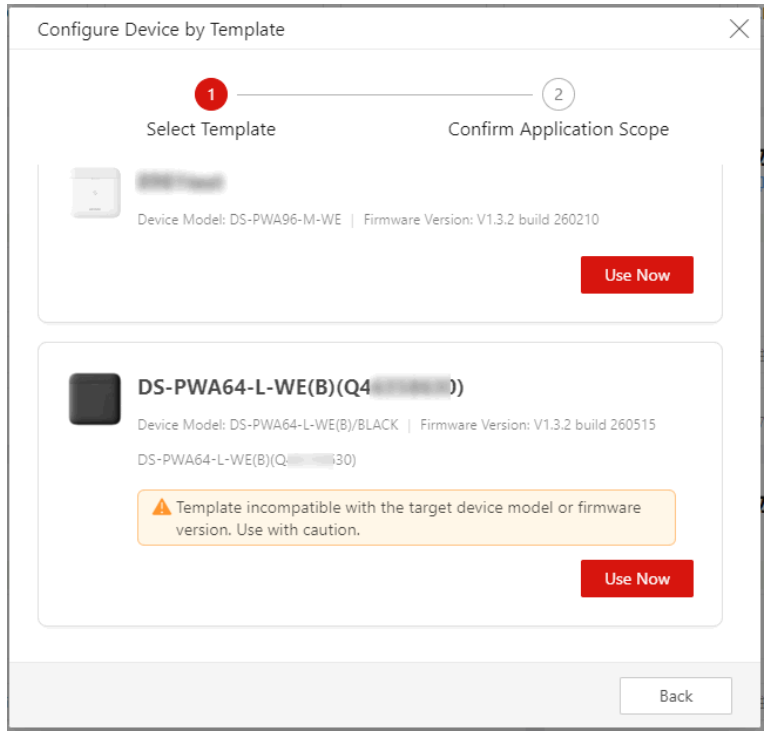


Figure 4-20 Select Template

b. Confirm the scope.

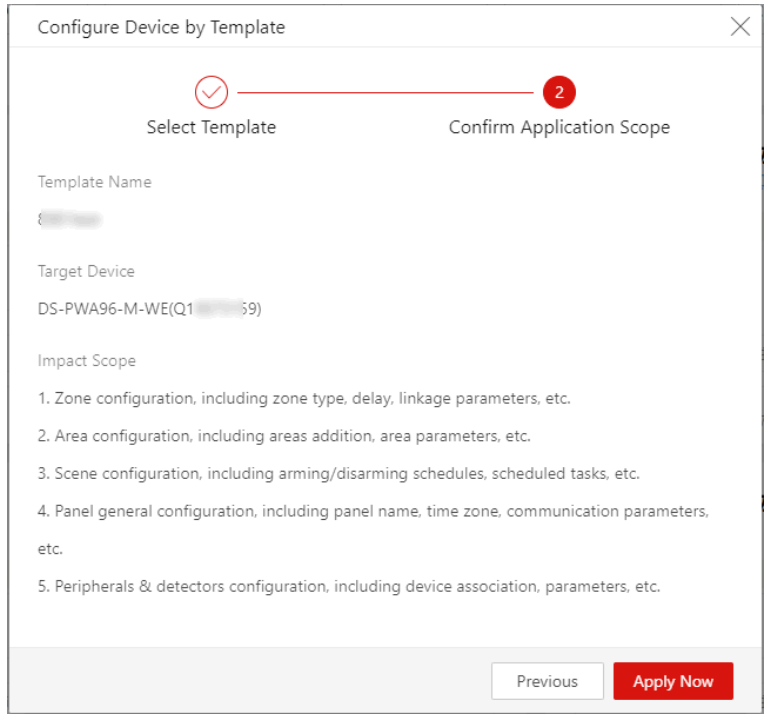


Figure 4-21 Confirm Scope

3. Click **Apply Now**. You can retry failed items.

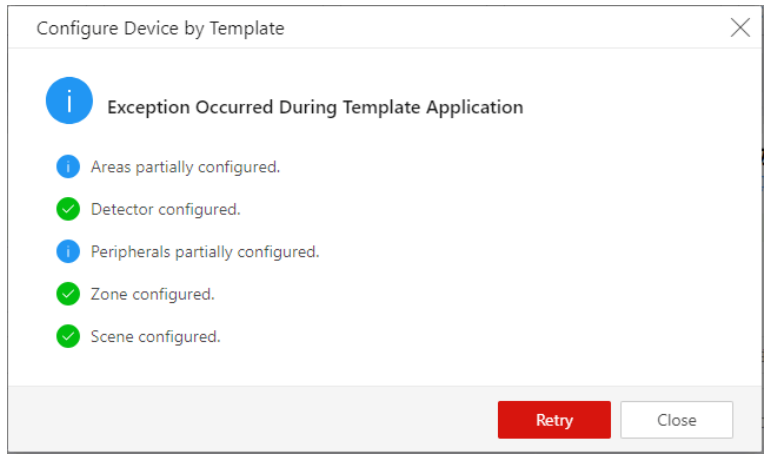


Figure 4-22 Application Result

Apply Template to Device Using the Mobile Client

1. The **Mobile Client** offers it at two moments: automatically after the add-device flow finishes, or go to the **Site** page, enter the target site, find the device, and tap the device's **…** → **Configure Control Panel** .

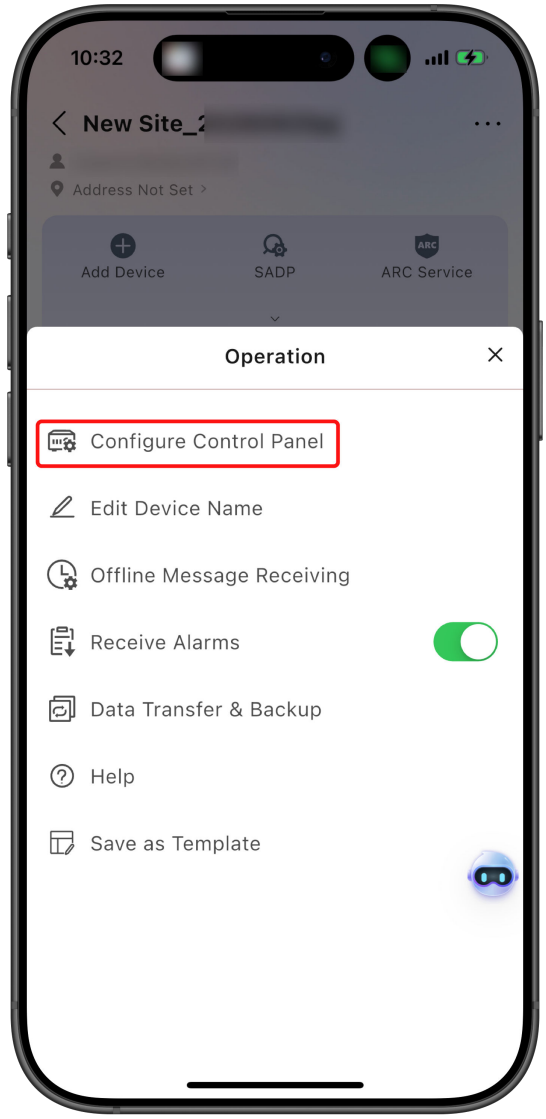


Figure 4-23 Configure Control Panel

2. Tap **Start Now** in the **Configuration Template** section. Follow the two steps:

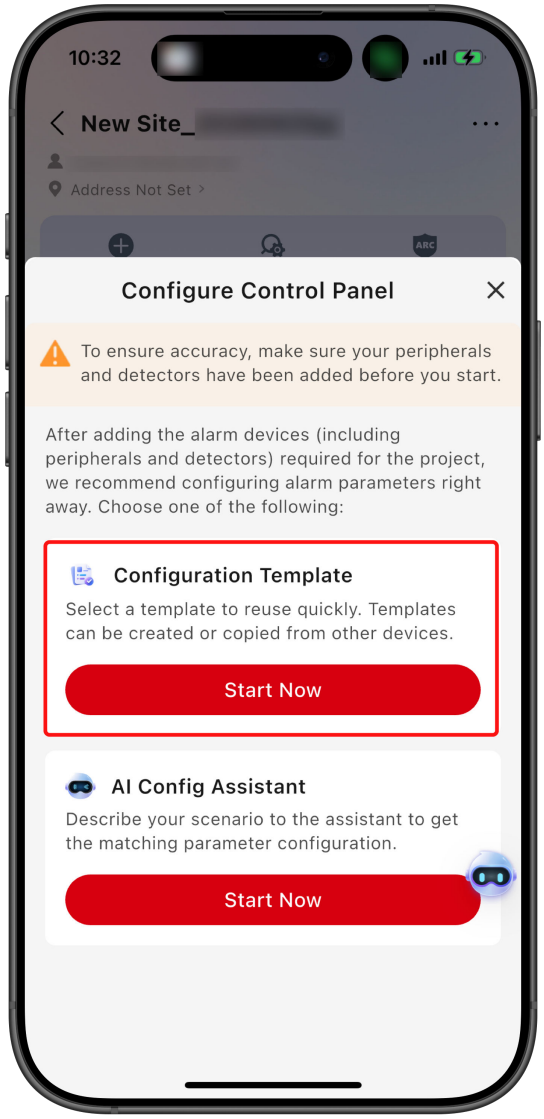


Figure 4-24 Start Now

a. Select a template.

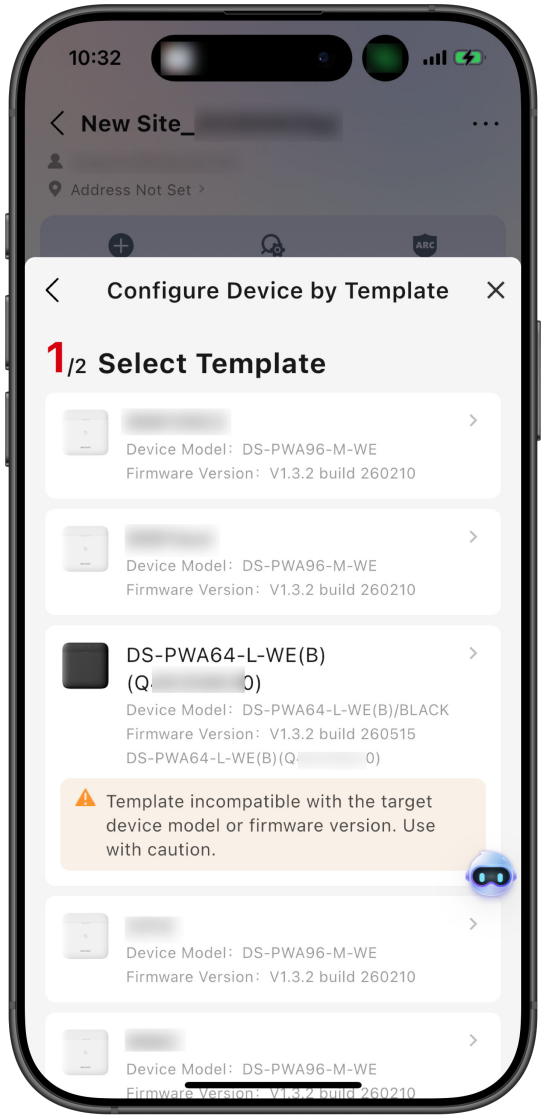


Figure 4-25 Select Template

b. Confirm the scope.



Figure 4-26 Confirm Scope

3. Tap **Apply Now**. You can retry failed items.

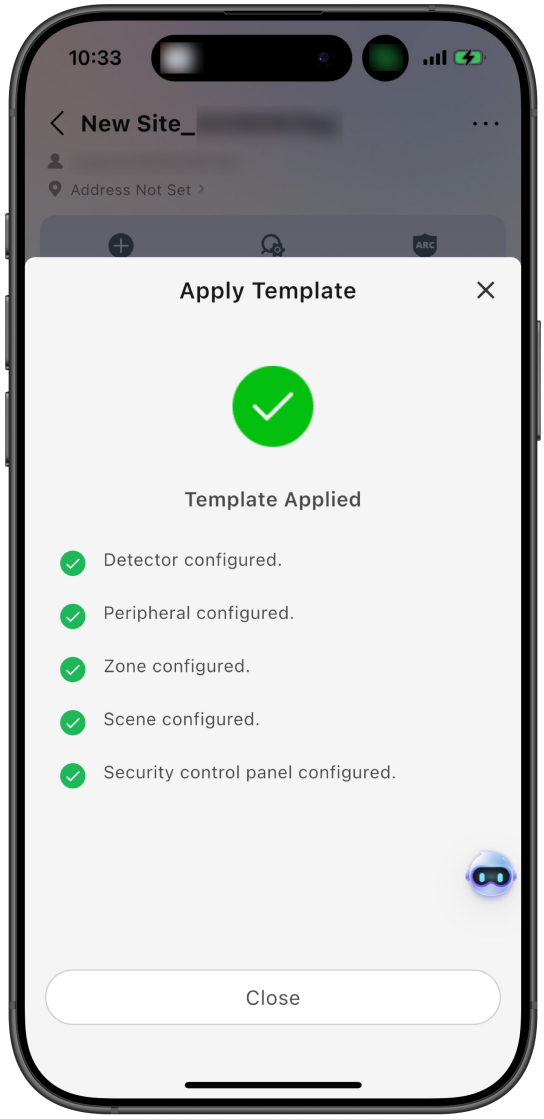


Figure 4-27 Application Result

Chapter 5 Maintain Customers' Devices to Grow Your Aftersales Business

Hik-Partner Pro offers powerful device maintenance and health monitoring features to help partners provide maintenance services for their customers.

Feature	Instructions
Reset Password Remotely / via LAN	***How to Reset Device Password***
Upgrade Device Remotely / via LAN	***How to Upgrade Devices***
Unbind Devices via LAN	***How to Unbind Devices?***
Detect Events and Trigger Linkage Actions	***How to Set Linkages to Trigger Actions When Events Occur?***
Detect Exceptions & Alarms and Send Notifications	• ***How to Set Up Exception Rules to Receive Exception Notifications?*** • ***How to Configure Device Offline Delay?***
Device Health Status Dashboard	***How to View Device Health Status in Real Time?***
Device Health Check Report	***How to Export Device Health Report and Set Scheduled Report Delivery?***
Create Quote for Providing Maintenance Services	***How to Create Maintenance Quotation?***
Access Operation Logs of Your Company	***How to Get Operations Logs of Employees for Troubleshooting?***
Alarm Receiving and Handling Services via Hik-Partner Pro	• ***How to Provide an ARC Service on Hik-Partner Pro to Expand Your Business?*** • ***How to Integrate with Hik-Partner Pro?***

5.1 Remote Device Configurations as Powerful as Configurations Over LAN

When you are not able to access the LAN on your customers' sites, with Hik-Partner Pro and if devices are added to sites you can remotely configure devices.

Encoding Devices

Device Operations/ Configurations	NOT Over the LAN: On the Site Page	Over the LAN: On the Site Page or On the SADP Tool Page
Configure Cameras Added to the NVR	√	√
View Live Video and Play Back Recorded Videos	√	√
Set DDNS to Make Sure Encoding Devices Can Be Managed by Hik-Partner Pro	√	√
Set Cloud Storage for Uploading Recorded Video to the Cloud	√	√

5.2 How to Reset Device Password

Follow the corresponding instructions according to your actual situation.

Situations and Corresponding Solutions

Your Situation		Solution
You cannot access the device LAN.	You can access the device local GUI.	Scan the password reset QR code and get a verification code to reset the password on the device local GUI. See ***Reset Password for Nearby Device*** .
	The device is handed over and you have the site authorization. Also, your customer's Hik-Connect and the device are on the same LAN.	Send password reset applications using either the Portal or Mobile Client to your customer's Hik-Connect. See ***Reset Password for Devices Added to Hik-Partner Pro*** .
	For other situations and if **Support Case** is available in your country/region.	Submit a password reset case using the Mobile Client. See ***Reset Password by Submitting Case*** .
Your phone and the device are on the same LAN.	The device is added to Hik-Partner Pro and not handed over.	Reset the password directly. See ***Reset Password for Devices Added to Hik-Partner Pro*** .

Your Situation		Solution
	The device is handed over and you have the site authorization.	Send password reset applications using either the Portal or Mobile Client to your customer's Hik-Connect. See ***Reset Password for Devices Added to Hik-Partner Pro*** .
	You do not forget the password.	Enter the old password to reset it using the SADP tool on the Mobile Client. See ***Reset Password via Old Password*** .
	You have set a reserved email.	Reset the password via reserved email using the SADP tool on the Mobile Client. See ***Reset Password via Reserved Email / Security Questions*** .
	You have set the security questions.	Answer the pre-defined security questions using the SADP tool on the Mobile Client. See ***Reset Password via Reserved Email / Security Questions*** .
	For other situations and if **Support Case** is not available in your country/region.	Send an email to technical support using the SADP tool on the Mobile Client. See ***Reset Password by Sending Email to Technical Support*** .
	For other situations and if **Support Case** is available in your country/region.	Submit a password reset case using the Mobile Client. See ***Reset Password by Submitting Case*** .

5.2.1 Reset Password for Nearby Device

Scan the Password Reset QR Code Using the Mobile Client

1. On the local GUI of the device, select **Forget Password → Verify by Hik-Connect** to show the password reset QR code.
2. On the Hik-Partner Pro Mobile Client, tap **Me → Support → Reset Password → Nearby Device (Scanning)** , and scan the password reset QR code to get the code for password reset.
3. Enter the code on the local GUI of the device.
4. Set a new password and select **OK** on the local GUI of the device.

5.2.2 Reset Password for Devices Added to Hik-Partner Pro

Reset Password for Devices Added to Hik-Partner Pro Using the Portal

1. Go to **Site & Device → Customer Site** , find the device, and click or → .
2. You may enter automatically or choose one of the following processes of password reset.

Your Situation	Instructions
The device is not handed over and your Hik-Partner Pro Mobile Client and the device are on the same LAN.	Please use the Mobile Client.
The device is handed over and you have the site authorization. Also, your Hik-Partner Pro and the device are on the same LAN.	a. Click **I Am at the Site** to send the application to your customer. b. Wait until your customer reset the password on their Hik-Connect.
The device is handed over and you have the site authorization. Also, your customer's Hik-Connect and the device are on the same LAN.	a. Click **I Am Not at the Site** to send the application to your customer. b. Wait until your customer reset the password on their Hik-Connect.

Reset Password for Devices Added to Hik-Partner Pro Using the Mobile Client

1. Access the Password Reset function via either of the following ways.
   - Tap **Site**, enter a site, select the device, and tap **Reset Password**.
   - On the **Me** page or in the application center, go to **Support → Reset Password → Device on Hik-Partner Pro** .
2. You may enter automatically or choose one of the following three processes of password reset.

Your Situation	Instructions
The device is not handed over and your Hik-Partner Pro Mobile Client and the device are on the same LAN.	a. (Optional) Tap the device. b. Enter and confirm the new password on the Set New Password page. c. Tap **Confirm**.
The device is handed over and you have the site authorization. Also, your Hik-Partner Pro and the device are on the same LAN.	a. (Optional) Tap the device with the LAN icon. b. Tap **Reset Password** to send the application to your customer. c. Wait until your customer reset the password on their Hik-Connect.
The device is handed over and you have the site authorization. Also, your customer's Hik-Connect and the device are on the same LAN.	a. (Optional) Tap the device. b. The application is auto sent to your customer. c. Wait until your customer reset the password on their Hik-Connect.

5.2.3 Reset Password by Submitting Case

Submit Password Reset Case Using the Mobile Client

1. Enter the Submit Case page via either of the ways.
   - On the **Me** page or in the application center, go to **Support → Online Support Case → New Case → Device Password Reset** .
   - On the **Me** page or in the application center, **Support → Reset Password → Submit Case** .
2. Fill in the fields as required.
3. Tap **Confirm**.
4. After you receive the reply which contains the reset code/string from our technical support, enter the code or import the string file to reset the password using the SADP software on the PC.

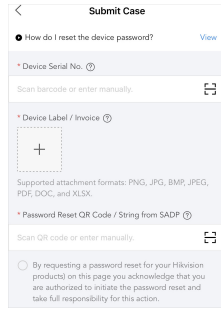


Figure 5-1 Device Password Reset Case

5.2.4 Reset Password via Old Password

Reset Password via Old Password Using the Mobile Client

1. If your device and your phone are on the same LAN, go to the SADP page by tapping ⊕ → **SADP** .
2. Tap ··· → **Reset Password** → **Know Password** .
3. Enter the old password and set the new password.
4. Tap **OK**.

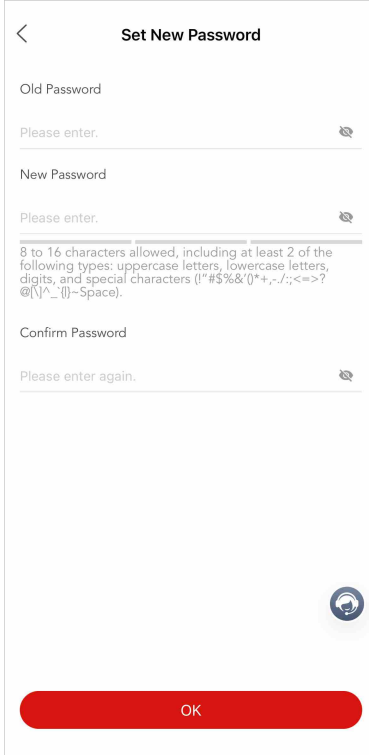
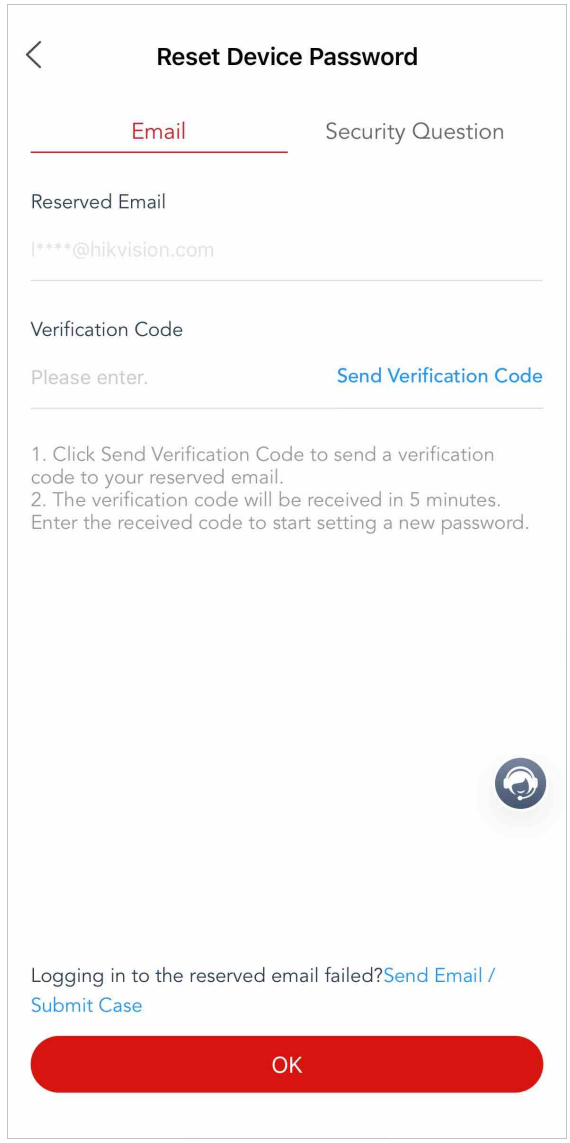


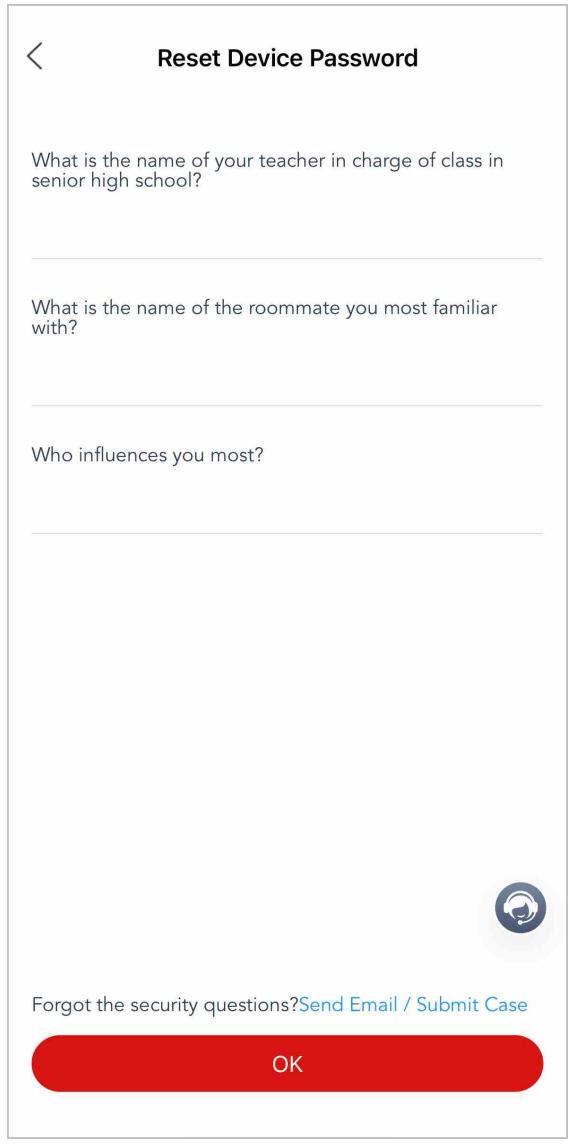
Figure 5-2 Reset Password via Old Password

5.2.5 Reset Password via Reserved Email / Security Questions

Reset Password via Reserved Email Using the Mobile Client

1. If your device and your phone are on the same LAN, go to the SADP page by tapping ⊕ → **SADP** .
2. Tap ··· → **Reset Password** → **Forgot Password** on the SADP page.
3. Read carefully the Privacy Policy, and tap **Agree** to continue.
4. Select **Forgot Password**.
5. Set a new password via reserved email or by answering the predefined security questions.


Reset Device Password
Email
Security Question
Reserved Email
l****@hikvision.com
Verification Code
Please enter.
Send Verification Code
1. Click Send Verification Code to send a verification code to your reserved email.
2. The verification code will be received in 5 minutes. Enter the received code to start setting a new password.
Logging in to the reserved email failed?Send Email / Submit Case
OK



How to Set Verification Method for Password Reset Using the Mobile Client

Note

Setting the verification method is available only when the device is not added to Hik-Partner Pro and no verification method is set for the device.

1. If your device and your phone are on the same LAN, go to the SADP page by tapping ⊕ → **SADP** .
2. Tap ··· → **Settings** on the SADP page.
3. Set either or both of the reserved email and the answers to 3 security questions.
4. Tap **OK**.

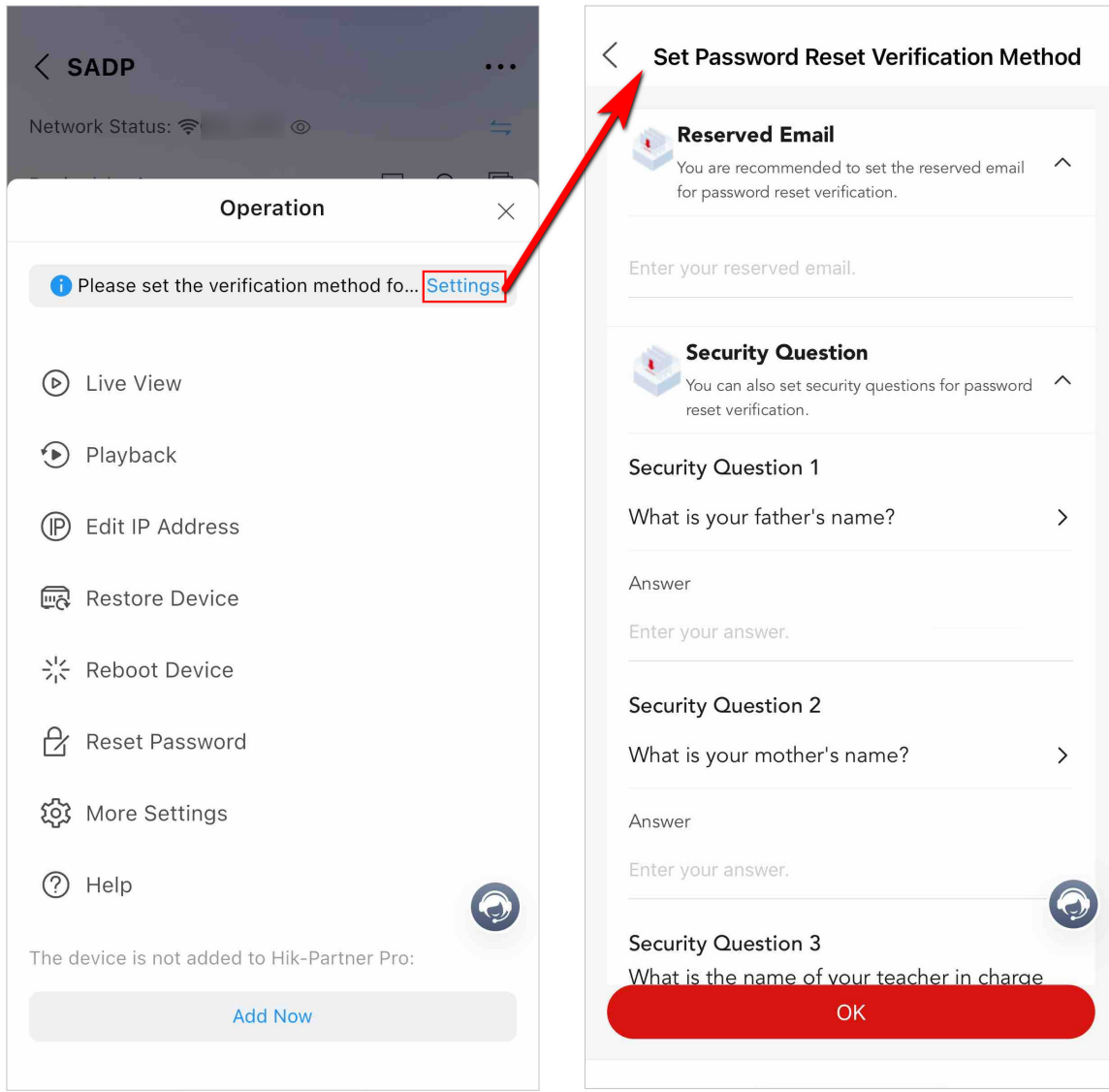


Figure 5-3 Set Verification Method

5.2.6 Reset Password by Sending Email to Technical Support

Send Email to Technical Support for Password Reset Using the Mobile Client

1. If your device and your phone are on the same LAN, go to the SADP page by tapping ⊕ → **SADP** .
2. Tap ··· → **Reset Password** → **Forgot Password** on the SADP page.
3. Upload the picture of the device label / Invoice, confirm and check the statement, and tap **Send Email** to send the email to technical support.

Note

The password reset QR code / string from SADP is filled in automatically and cannot be edited.

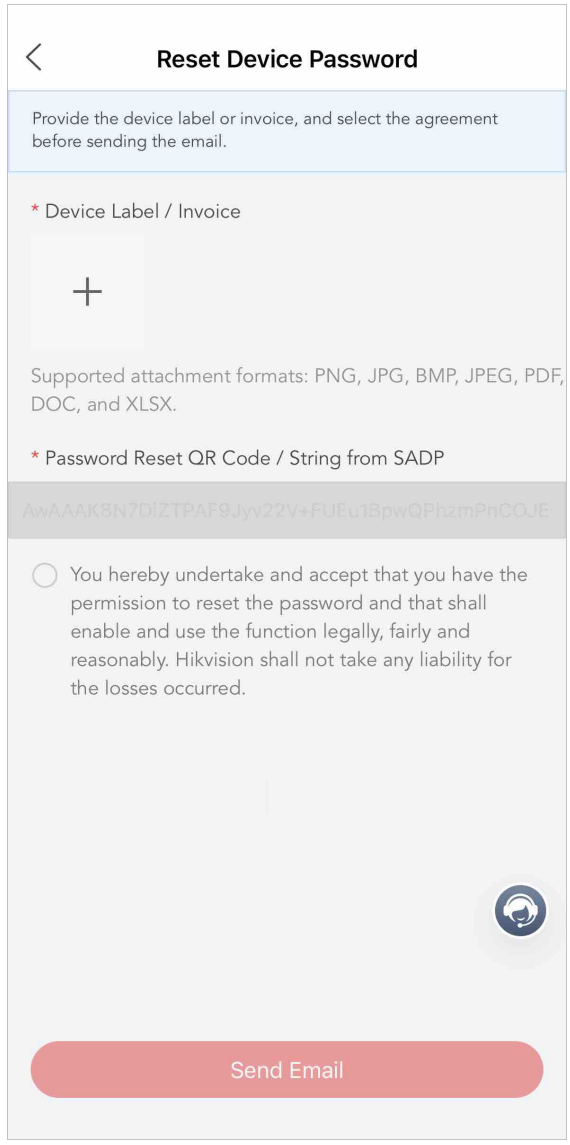


Figure 5-4 Reset Password via Technical Support

4. After you receive the reset code/string from technical support, enter the reset code/string on the Reset Device Password page, set the new password, and tap **OK**. Tap **Send Again** if you do not receive a reply.

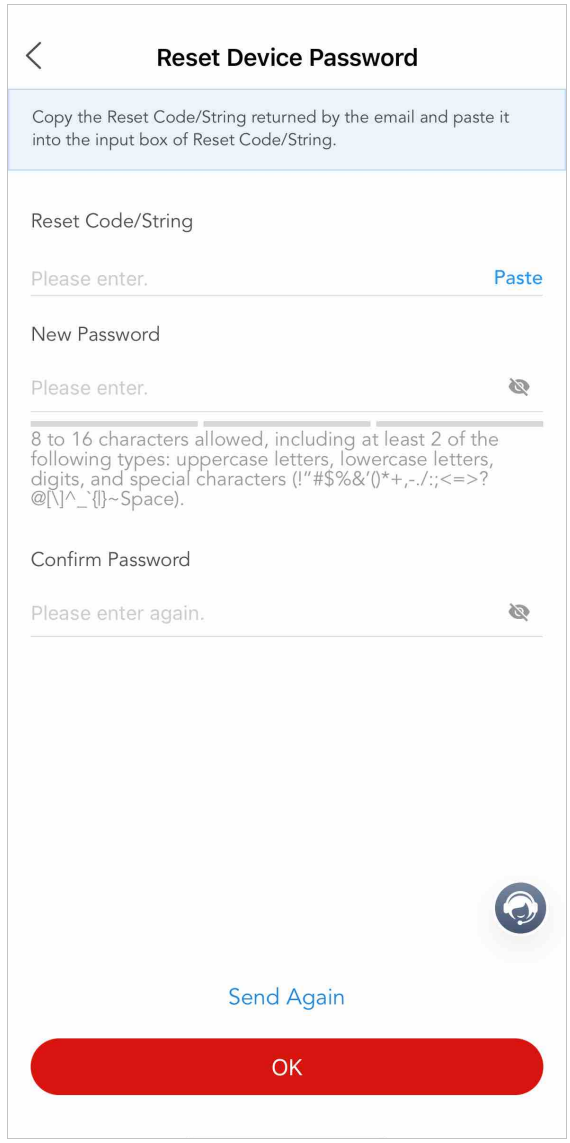


Figure 5-5 Set New Password

5.3 How to Upgrade Devices

Table 5-1 Situations and Corresponding Solutions

Your Situation	Solution	Supported Devices
Devices are on the same LAN of Hik-Partner Pro.	***Batch Upgrade Device on LAN***	Security Control Panels, Doorbells, Network Cameras,

Your Situation	Solution	Supported Devices
		NVRs, DVRs, Hik-ProConnect Boxes
Devices are added to Hik-Partner Pro and are online.	***Upgrade Device Automatically***	Security Control Panels, Doorbells, Hik-ProConnect Boxes, DVRs, NVRs, Network Cameras
	Upgrade Device Manually by Uploading Firmware Package	NVRs, DVRs, Network Cameras

5.3.1 Batch Upgrade Device on LAN

You can batch upgrade devices (security control panels, encoding devices, doorbells, etc.) on the same LAN to make the devices compatible with Hik-Partner Pro, if there are new firmware versions of the devices.

Batch Upgrade Device on LAN Using the Portal

1. Click **Site & Device → Install & Config → On-Site Batch Upgrade** .
2. Select devices that need to be upgraded.
3. Click **Upgrade Online** or **Upgrade by Local File** to upgrade the selected devices.

Batch Upgrade Device on LAN Using the Mobile Client

1. On Home page, tap **More → On-Site Batch Upgrade** , or tap **On-Site Batch Upgrade** on the Home page.
2. Select devices that need to be upgraded.
3. Tap **Upgrade Online** to upgrade the selected devices.

5.3.2 Upgrade Device Automatically

If Hik-Partner Pro detects new firmware of devices including security control panels, doorbells, Hik-ProConnect boxes, DVRs/NVRs that support cloud storage, and certain models of network cameras, you can upgrade the devices automatically.

Upgrade Device Automatically Using the Portal

1. Go to **Site & Device → Customer Site** .
2. In **Device Mode**, click **Upgrade Device**, and select upgradable devices. Or in **Site Mode**, click a site to enter its site details page, and click **Upgrade Device** to select upgradable devices.
3. Click **Upgrade**.

Note

- If there are devices which have enabled EN50131 Compliant mode, enter the device passwords and click **OK**.
- Once started, the upgrade cannot be stopped. Make sure a power failure or network disconnection does not happen during the upgrade.
- For the device failed to be upgraded, you can click to download the upgrade firmware package, and then upgrade the device on the remote configuration page of device or via manual upgrade.

Upgrade Device Automatically Using the Mobile Client

1. Tap **Site**, and tap a site to enter its site details page.
2. Tap a device name to enter the device details page.
3. Tap **Upgrade Device**.

Note

- If there are devices which have enabled EN50131 Compliant mode, enter the device passwords and click **OK**.
- Once started, the upgrade cannot be stopped. Make sure a power failure or network disconnection does not happen during the upgrade.
- For the device failed to be upgraded, you can tap **Share Download Link** to share the download link via Email, Facebook, etc. You can then open the link to download the upgrade firmware and upgrade the device on the remote configuration page of the device or via manual upgrade.

5.3.3 Upgrade Device Manually by Uploading Firmware Package

If a device with the new firmware version to be upgraded and the PC running with the Portal are not on the same LAN (Local Area Network), you can upload firmware packages from the local PC for manually upgrading the device to make the device more compatible with Hik-Partner Pro.

Note

- Make sure you have the permission for remotely configuring devices.
- This function is only available for some DVRs, NVRs, and network cameras.

Upgrade Device Manually Using the Portal

1. Go to **Site & Device → Customer Site** .
2. Find the device, and click or → **Manual Upgrade** .

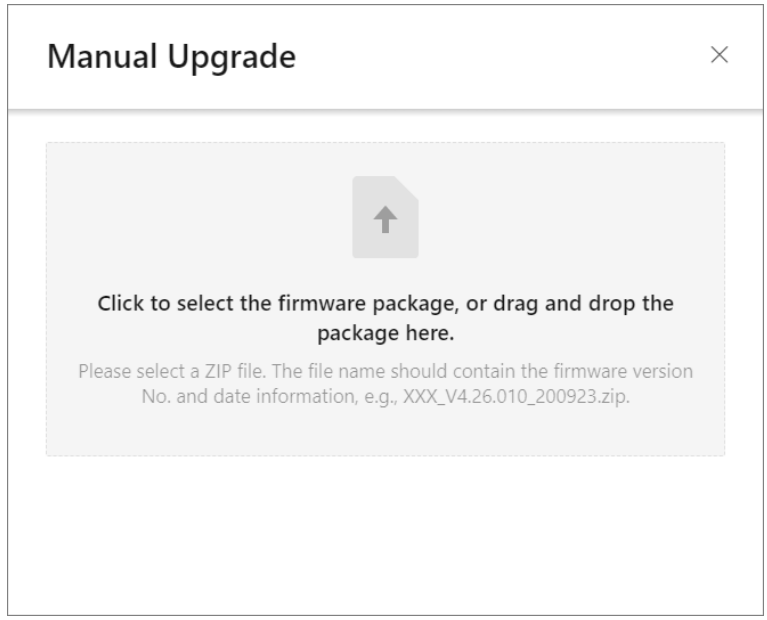


Figure 5-6 Manual Upgrade Pane

3. Click **Firmware Update Search** to search for and download the firmware package of the current device.
4. Click to select the firmware package in ZIP format from the local PC or drag it to the gray area.

Note

Make sure the package is consistent with **Details of This Device**, and the file name matches one of the followings, otherwise, errors will occur.

Supported File Name Format	Example
{custom name}_V{firmware version No.}_{date}.zip	test_V4.26.10_230316.zip
{custom name}_V|v{firmware version No.}_Build_{date}.zip	NVR_V5.0.0_Build_220210.zip
Format 3: {custom name}_V{firmware version No.}_build{date}.zip	DVR_V4.26.500_build200518.zip

5. Click to reselect an upgrade package as you needed.

Note

If you click × to close the Manual Upgrade pane, the selected package will still be kept for the next time you open the pane.

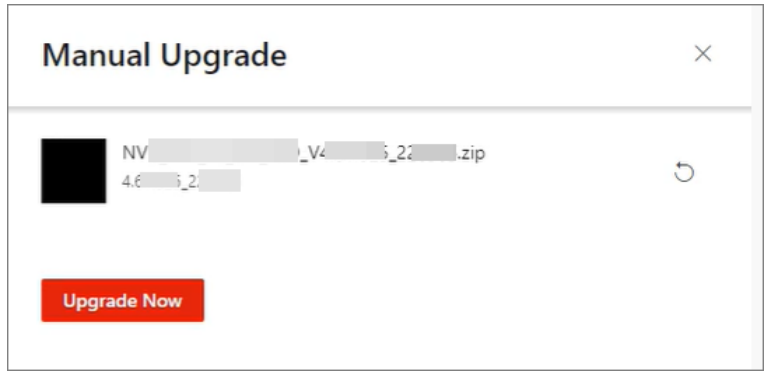


Figure 5-7 After Selecting Firmware Package

6. Click **Upgrade Now** and a risk prompt will pop up.
7. Click **OK** to start upgrading the device.

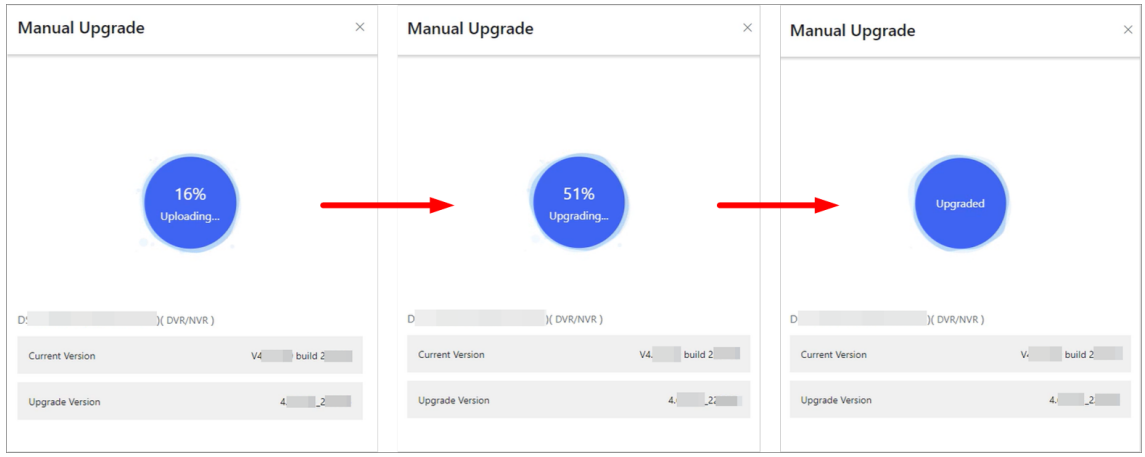


Figure 5-8 Upgrade Progress

5.4 How to Unbind Devices?

When you add a device by scanning QR code or add it manually by entering the serial number, or when you add detected online devices, if the adding result page shows it has been added to another account, you need to unbind it from its current account first before you can add it to your account. The device unbinding functionality is useful when you need to add a device to a new account but have no access to delete it from the old account (e.g., if you forgot the password of the old account).

Unbind Devices Using the Portal

1. On the adding result page, click in the Operation column.
2. Enter the device password and click **OK** to unbind it from its current account.

Note

If the device firmware does not support device unbinding, you are required to enter a CAPTCHA code after entering the device password.

3. When the device is unbound, you can click ⊕ in the Operation column to add the device to your account.

Unbind Devices Using the Mobile Client

1. Tap **Unbind** on the adding result page.
2. Enter the device password and tap **Finish** to unbind it from its currently-added account.

Note

If the device firmware does not support device unbinding, you are required to enter a CAPTCHA code after entering the device password.

3. When the device is unbound, you can add it to your account.

Limitations

- Make sure the Mobile Client or the Portal runs on the same LAN with the device. Otherwise, unbinding will be unavailable.
- Some devices only supports unbinding on the Mobile Clients, e.g., AX HOME security control panels.
- For a site that is handed over to your customer by sharing, you cannot unbind the devices added to this site.

5.5 How to Set Linkages to Trigger Actions When Events Occur?

You can set up a linkage to trigger certain device actions when the specified event occurs. You can add a linkage using the predefined template or customize a linkage. The linkages can be used for purposes such as notifying the security personnel, upgrading the security level, and recording evidences when specific events occur.

Note

What Is A Linkage and How to Set One

A linkage refers to the process where an event detected by **Resource A** triggers actions of **Resource B**, **Resource C**, **Resource D**, etc.
To set a linkage, you need to define the following five elements.

Table 5-2 Five Elements of a Linkage

Element	Description
Source	The resource that detects the **Triggering Event**.
Triggering Event	The event detected by the **Source** for triggering the **Linkage Actions**.
Linked Resources	The resources that are to perform the **Linkage Actions**.
Linkage Actions	Actions that the **Linked Resources** perform when the **Triggering Event** occurs.
Linkage Schedule	The scheduled time during which the linkage is activated.

Table 5-3 Overall Process of Setting a Linkage

Steps	Instructions
1. Add resources to Hik-Partner Pro you need them to be the **Source** and **Linked Resources**.	• ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** • ***Available Triggering Events for Different Source Devices*** • ***Available Linkage Actions for Different Linked Resources*** • ***What Are the Six Template Linkages For?***
2. Set the triggering event on the source device (resource), and some linkage actions also need to be set on the linked resources (devices) in advance.	• User manuals of the devices (resources). • ***Available Triggering Events for Different Source Devices*** • ***Available Linkage Actions for Different Linked Resources*** • ***What Are the Six Template Linkages For?***
3. Add and enable a linkage.	***Add and Enable a Linkage***
4. Enable **Notification** for the **Source** device.	***Enable Notification for the Source Device***

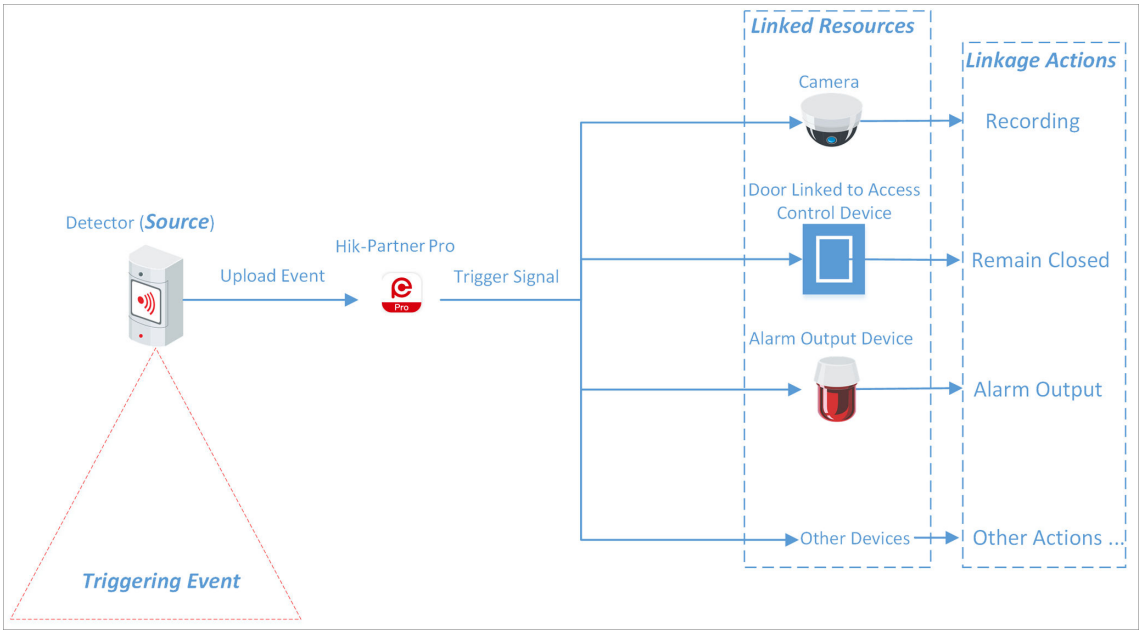


Figure 5-9 Linkage

Example

Upgrade Security Level for a Jewelry Store

Your customer is the manager of a jewelry store, who needs to upgrade the store's security level during non-business hours. The store has been installed with a PIR detector linked to a security control panel, a sounder linked to the security control panel, and several network cameras.

In this case, you can set a linkage to trigger alarm output and recording in the store when objects in motion are detected during non-business hours. The following elements need to be defined:

- **Source**: The PIR detector in the store.
- **Triggering Event**: The motion detection event.
- **Linked Resources**: The alarm output (the sounder in this case) and the network cameras in the store.
- **Linkage Actions**:
  - For sounder: Sends out audible alarm.
  - For network cameras: Start recording.
- **Linkage Schedule**: Non-business hours every day.

5.5.1 Add and Enable a Linkage

Hik-Partner Pro offers 6 predefined templates (Intrusion, Forced Entry Alarm, Back to Home/Office, Away, Visitor Calling, and Perimeter Zone Alarm), designed for 6 typical applications of linkages. You can also customize the linkage for your customer.

Note

Make sure you have the configuration permission for the devices.

Add and Enable a Linkage Using the Portal

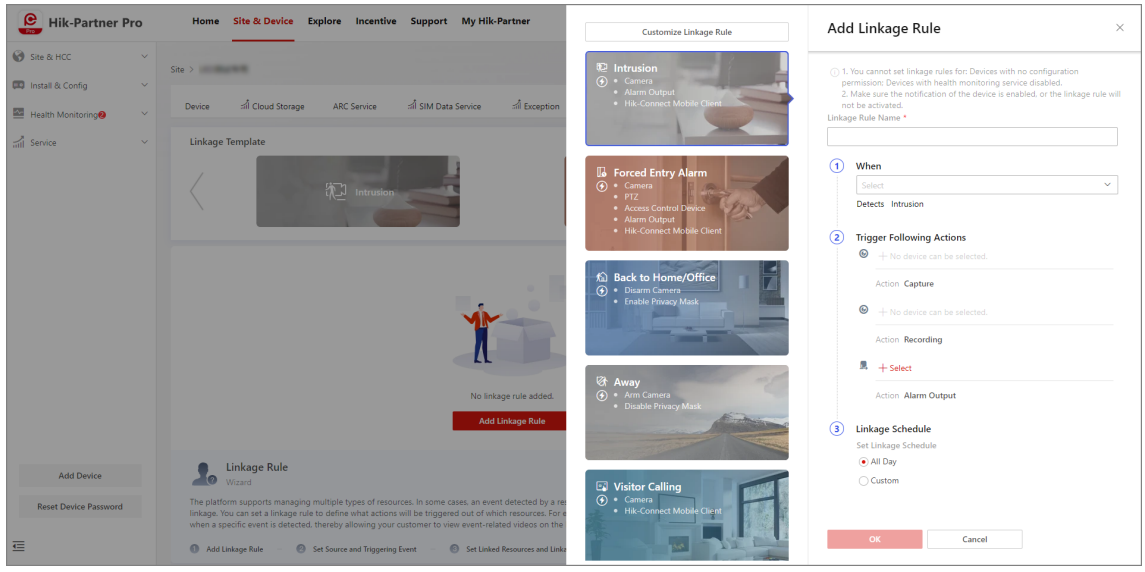
1. Go to **Site & Device → Customer Site** .
2. Open the **Add Linkage Rule** page in one of the following ways:
   - Click a site to enter its site details page, and click **Linkage Rule**.
   - In the site list (site mode) or in the device list (device mode), click in the Operation column.
3. Choose either ways to set a linkage:
   - To add a linkage based on a template, select a template on the left, and set the required information.

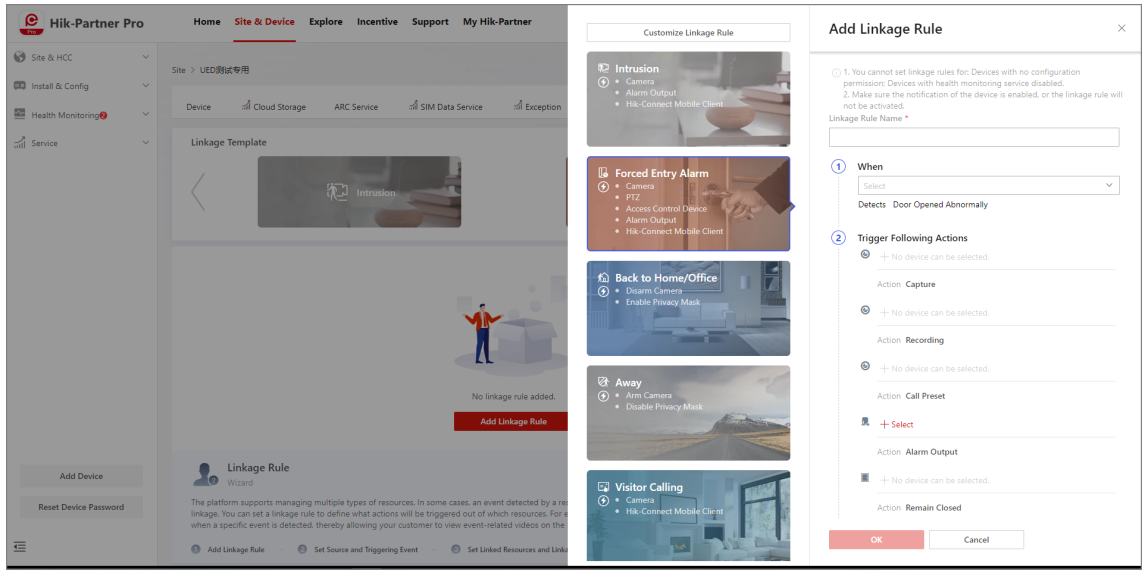
Parameter	Description
Linkage Rule Name	Set a name for the linkage.
When	Select a resource as the **Source** for detecting the triggering event defined in the template.
Trigger Following Actions	Select the **Linked Resources** for performing the linkage action. **Note** You can set only one linkage action.
Linkage Schedule	Set the scheduled time during which the linkage is activated.

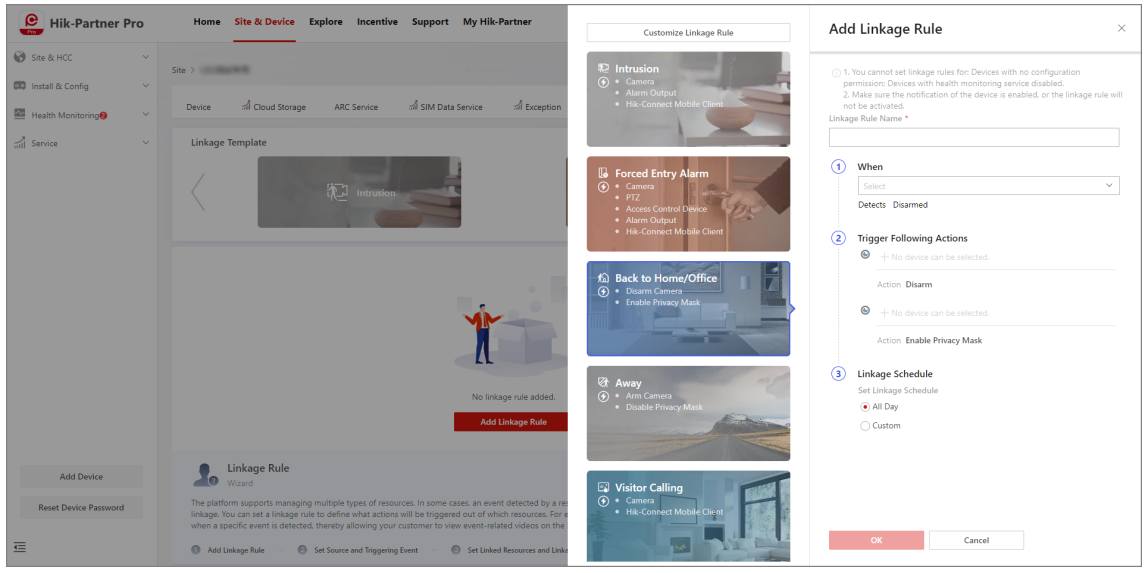
   - To customize a linkage, click **Customize Linkage Rule**, and set the required information.

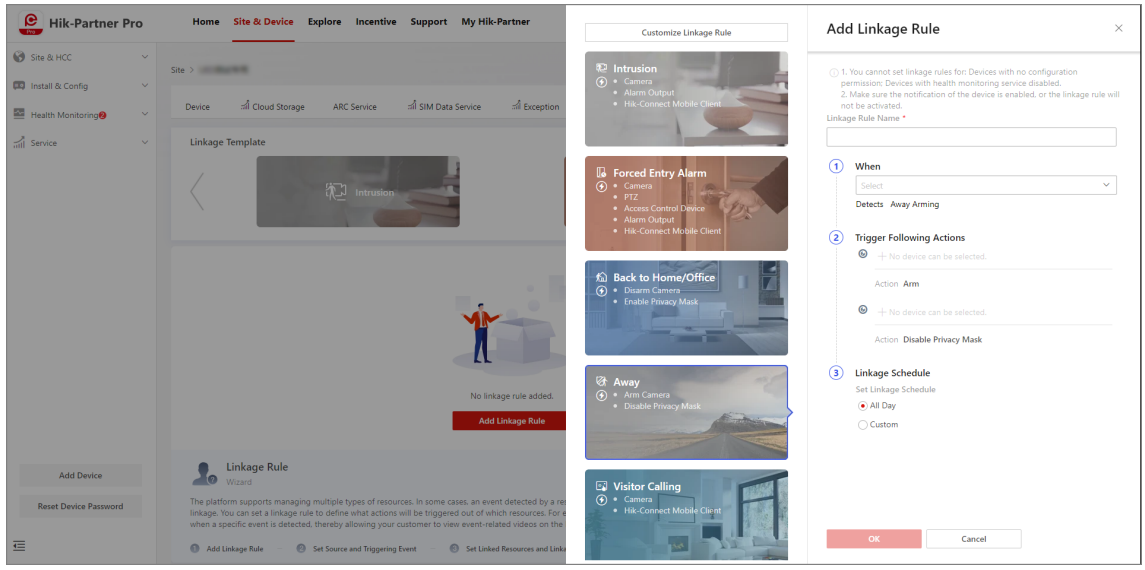
Parameter	Description
Linkage Rule Name	Set a name for the linkage.
Trigger	Set the **Source** and the **Triggering Event** for triggering the linkage action. **Note** Make sure that the triggering event has been configured on the selected device. For details about configuring event on device, see the user manual of the device.

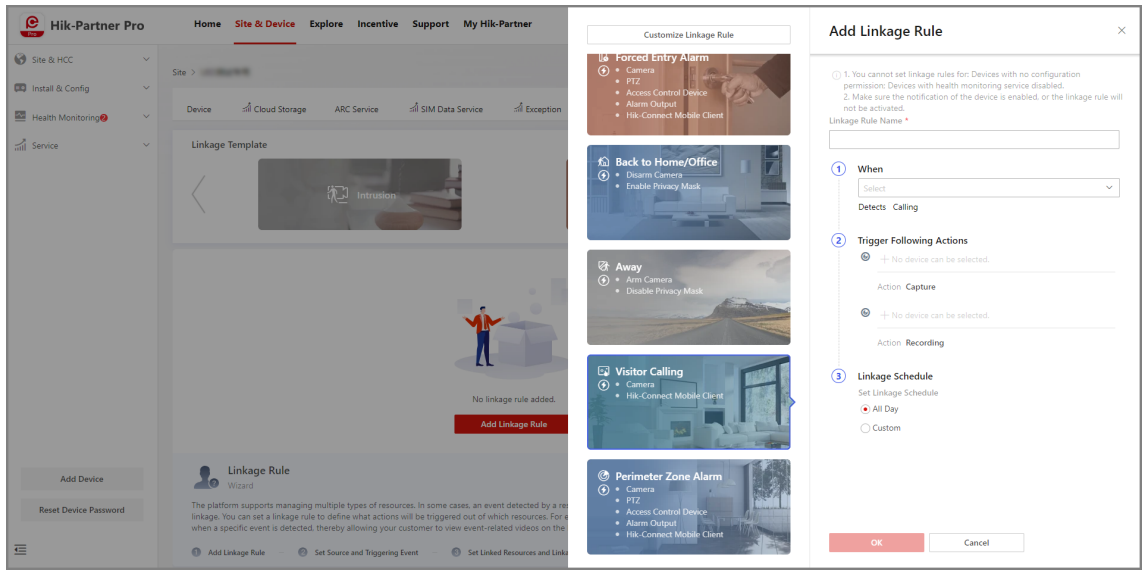
Parameter	Description
Linkage	Click **Add** to select **Linkage Actions** and **Linked Resources**. **Note** - Up to 128 Linkage Actions or 10 Linked Resources can be selected. - You can set up to 4 **Linkage Actions** for cameras as the **Linked Resources**. For example, if you have set the picture capturing and recording for camera 1, you can only set two more **Linkage Actions**, e.g., capturing picture and recording for camera 2.
Linkage Schedule	Set the scheduled time during which the linkage is activated.




Hik-Partner Pro
Home
Site & Device
Explore
Incentive
Support
My Hik-Partner
Site & HCC
Install & Config
Health Monitoring
Service
Linkage Template
Intrusion
No linkage rule added.
Add Linkage Rule
Add Device
Reset Device Password
Linkage Rule
Wizard
Customize Linkage Rule
Intrusion
Camera
Alarm Output
Hik-Connect Mobile Client
Forced Entry Alarm
Camera
PTZ
Access Control Device
Alarm Output
Hik-Connect Mobile Client
Back to Home/Office
Disarm Camera
Enable Privacy Mask
Away
Arm Camera
Disable Privacy Mask
Visitor Calling
Camera
Hik-Connect Mobile Client
Add Linkage Rule
1. You cannot set linkage rules for: Devices with no configuration permission; Devices with health monitoring service disabled.
2. Make sure the notification of the device is enabled, or the linkage rule will not be activated.
Linkage Rule Name *
When
Detects Door Opened Abnormally
Trigger Following Actions
Action Capture
Action Recording
Action Call Preset
Select
Action Alarm Output
Action Remain Closed
OK
Cancel


Hik-Partner Pro
Home
Site & Device
Explore
Incentive
Support
My Hik-Partner
Site & HCC
Install & Config
Health Monitoring
Service
Linkage Template
Intrusion
No linkage rule added.
Add Linkage Rule
Add Device
Reset Device Password
Linkage Rule
Wizard
Customize Linkage Rule
Intrusion
Camera
Alarm Output
Hik-Connect Mobile Client
Forced Entry Alarm
Camera
PTZ
Access Control Device
Alarm Output
Hik-Connect Mobile Client
Back to Home/Office
Disarm Camera
Enable Privacy Mask
Away
Arm Camera
Disable Privacy Mask
Visitor Calling
Camera
Hik-Connect Mobile Client
Add Linkage Rule
1. You cannot set linkage rules for: Devices with no configuration permission; Devices with health monitoring service disabled.
2. Make sure the notification of the device is enabled, or the linkage rule will not be activated.
Linkage Rule Name *
When
Detects Disarmed
Trigger Following Actions
Action Disarm
Action Enable Privacy Mask
Linkage Schedule
Set Linkage Schedule
All Day
Custom
OK
Cancel


Hik-Partner Pro
Home
Site & Device
Explore
Incentive
Support
My Hik-Partner
Site & HCC
Install & Config
Health Monitoring
Service
Device
Cloud Storage
ARC Service
SIM Data Service
Exception
Linkage Template
Intrusion
No linkage rule added.
Add Linkage Rule
Linkage Rule
Wizard
Add Device
Reset Device Password
Customize Linkage Rule
Intrusion
Camera
Alarm Output
Hik-Connect Mobile Client
Forced Entry Alarm
Camera
PTZ
Access Control Device
Alarm Output
Hik-Connect Mobile Client
Back to Home/Office
Disarm Camera
Enable Privacy Mask
Away
Arm Camera
Disable Privacy Mask
Visitor Calling
Camera
Hik-Connect Mobile Client
Add Linkage Rule
1. You cannot set linkage rules for: Devices with no configuration permission; Devices with health monitoring service disabled.
2. Make sure the notification of the device is enabled, or the linkage rule will not be activated.
Linkage Rule Name *
When
Select
Detects Away Arming
Trigger Following Actions
No device can be selected.
Action Arm
No device can be selected.
Action Disable Privacy Mask
Linkage Schedule
Set Linkage Schedule
All Day
Custom
OK
Cancel


Hik-Partner Pro
Home
Site & Device
Explore
Incentive
Support
My Hik-Partner
Site & HCC
Install & Config
Health Monitoring
Service
Device
Cloud Storage
ARC Service
SIM Data Service
Exception
Linkage Template
Intrusion
No linkage rule added.
Add Linkage Rule
Linkage Rule
Wizard
Add Device
Reset Device Password
Customize Linkage Rule
Forced Entry Alarm
Camera
PTZ
Access Control Device
Alarm Output
Hik-Connect Mobile Client
Back to Home/Office
Disarm Camera
Enable Privacy Mask
Away
Arm Camera
Disable Privacy Mask
Visitor Calling
Camera
Hik-Connect Mobile Client
Perimeter Zone Alarm
Camera
PTZ
Access Control Device
Alarm Output
Hik-Connect Mobile Client
Add Linkage Rule
1. You cannot set linkage rules for: Devices with no configuration permission; Devices with health monitoring service disabled.
2. Make sure the notification of the device is enabled, or the linkage rule will not be activated.
Linkage Rule Name *
When
Select
Detects Calling
Trigger Following Actions
No device can be selected.
Action Capture
No device can be selected.
Action Recording
Linkage Schedule
Set Linkage Schedule
All Day
Custom
OK
Cancel

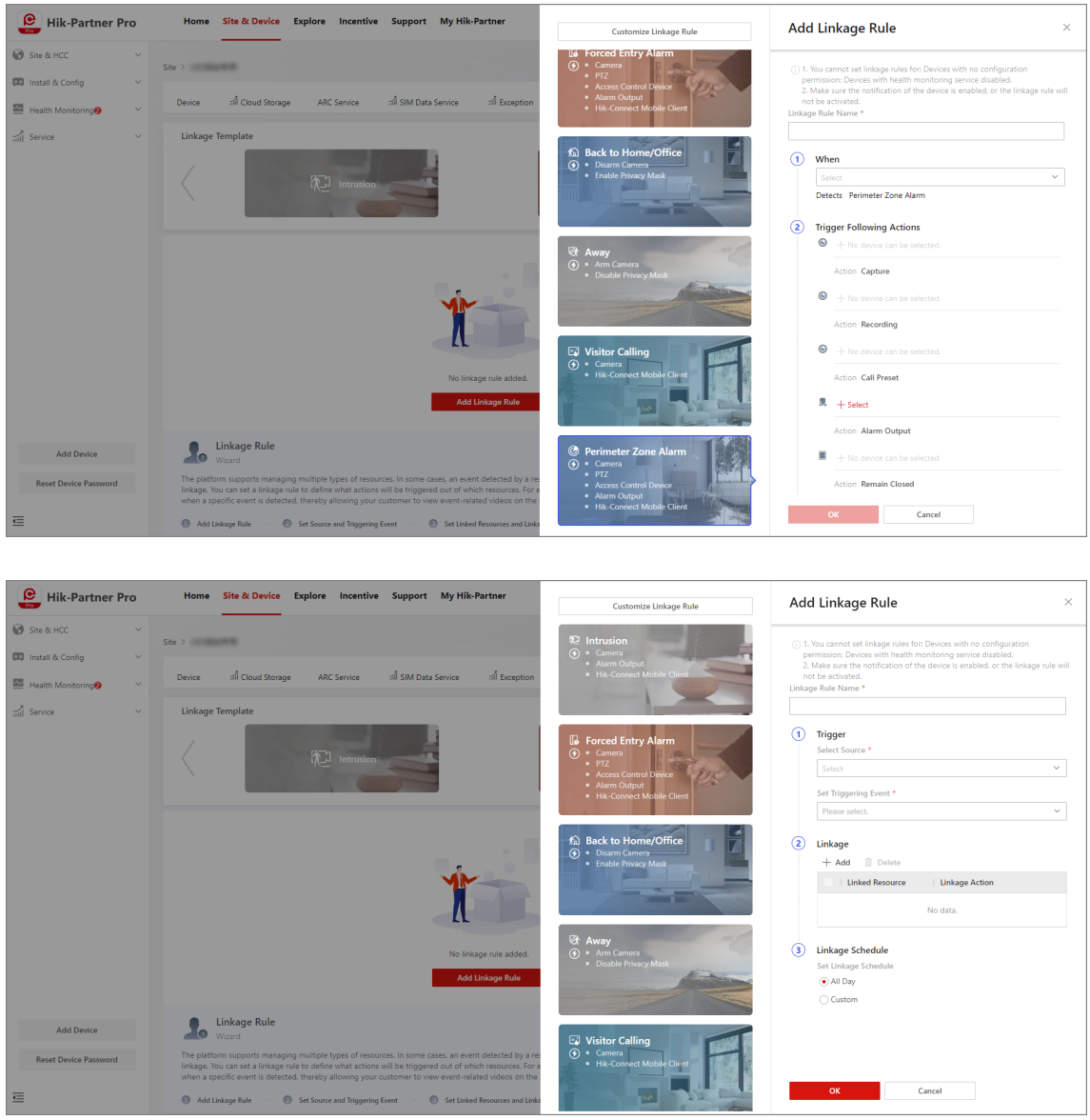


Figure 5-10 Add Linkage Rule Using the Portal

4. Click **OK**.

Add and Enable a Linkage Using the Mobile Client

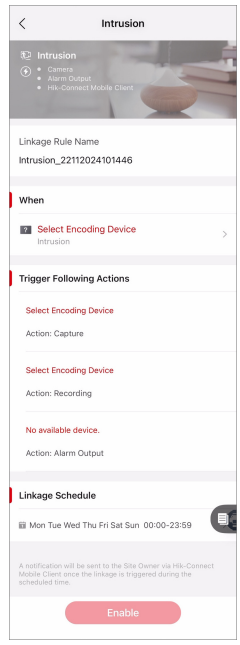
1. Tap **Site**.
2. Tap **Linkage Rule**.
3. Choose either ways to set a linkage:
   - To add a linkage based on a template, tap a template on the top, and set the required information.

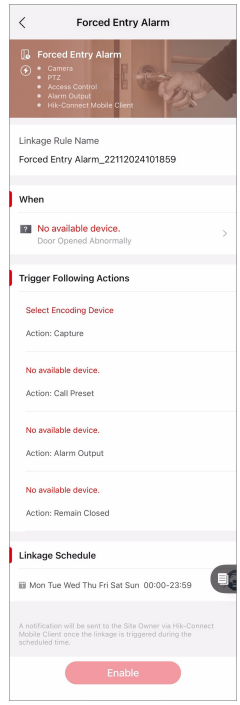
Parameter	Description
Linkage Rule Name	Set a name for the linkage.
When	Select a resource as the **Source** for detecting the triggering event defined in the template.
Trigger Following Actions	Select the **Linked Resources** for performing the linkage action. **Note** You can set only one linkage action.
Linkage Schedule	Set the scheduled time during which the linkage is activated.

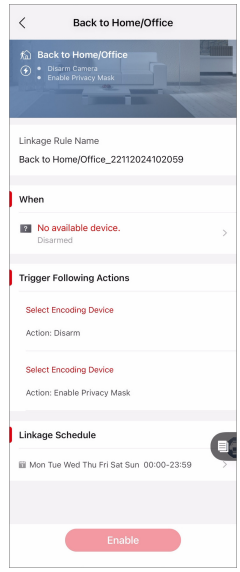
- To customize a linkage, tap **Add Linkage Rule** on the bottom, and set the required information.

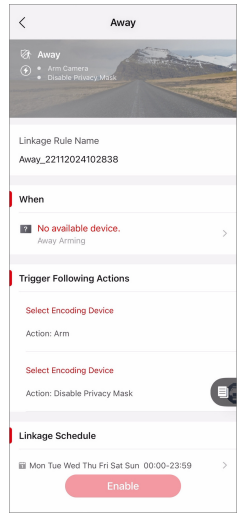
Parameter	Description
Trigger	Set the **Source** and the **Triggering Event** for triggering the linkage action. **Note** Make sure that the triggering event has been configured on the selected device. For details about configuring event on device, see the user manual of the device.
Linkage	Tap **Add Linkage** to select **Linkage Actions** and **Linked Resources**. **Note** - Up to 128 Linkage Actions or 10 Linked Resources can be selected. - You can set up to 4 **Linkage Actions** for cameras as the **Linked Resources**. For example, if you have set the picture capturing and recording for camera 1, you can only set two more **Linkage Actions**, e.g., capturing picture and recording for camera 2.

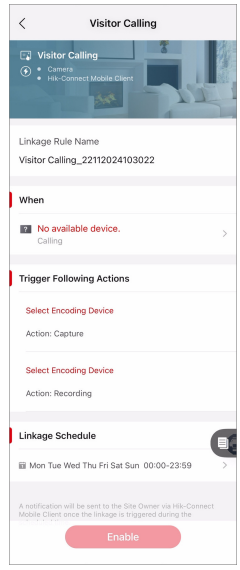
Parameter	Description
Linkage Schedule	Set the scheduled time during which the linkage is activated.
Linkage Rule Name	Set a name for the linkage.

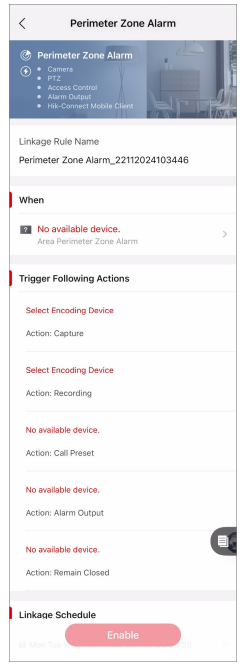





Back to Home/Office
Back to Home/Office
Disarm Camera
Enable Privacy Mask
Linkage Rule Name
Back to Home/Office_22112024102059
When
No available device.
Disarmed
Trigger Following Actions
Select Encoding Device
Action: Disarm
Select Encoding Device
Action: Enable Privacy Mask
Linkage Schedule
Mon Tue Wed Thu Fri Sat Sun 00:00-23:59
Enable


Away
Away
Arm Camera
Disable Privacy Mask
Linkage Rule Name
Away_22112024102838
When
No available device.
Away Arming
Trigger Following Actions
Select Encoding Device
Action: Arm
Select Encoding Device
Action: Disable Privacy Mask
Linkage Schedule
Mon Tue Wed Thu Fri Sat Sun 00:00-23:59
Enable


Visitor Calling
Visitor Calling
Camera
Hik-Connect Mobile Client
Linkage Rule Name
Visitor Calling_22112024103022
When
No available device.
Calling
Trigger Following Actions
Select Encoding Device
Action: Capture
Select Encoding Device
Action: Recording
Linkage Schedule
Mon Tue Wed Thu Fri Sat Sun 00:00-23:59
A notification will be sent to the Site Owner via Hik-Connect Mobile Client once the linkage is triggered during the
Enable


Perimeter Zone Alarm
Perimeter Zone Alarm
Camera
PTZ
Access Control
Alarm Output
Hik-Connect Mobile Client
Linkage Rule Name
Perimeter Zone Alarm_22112024103446
When
No available device.
Area Perimeter Zone Alarm
Trigger Following Actions
Select Encoding Device
Action: Capture
Select Encoding Device
Action: Recording
No available device.
Action: Call Preset
No available device.
Action: Alarm Output
No available device.
Action: Remain Closed
Linkage Schedule
Enable

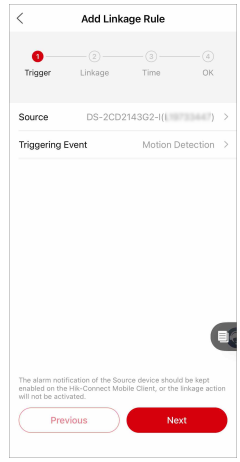


Figure 5-11 Add Linkage Rule Using the Mobile Client

4. Tap **Enable** or **OK**.

5.5.2 Enable Notification for the Source Device

After adding and enabling a linkage rule, you should make sure the Notification functionality of the Source device is enabled so that the events detected by the Source device can be uploaded to the Hik-Partner Pro system, which is the prerequisite to trigger the linkage actions in the related linkage rules.

Enable Notification for the Source Device Using the Portal

1. Go to **Site & Device → Customer Site** .
2. Find the device, and click on the device card or in the Operation column.
3. Switch on **Notification** and set the **Notification Schedule** for uploading the events detected by the **Source** device to Hik-Partner Pro.
4. Click **OK**.

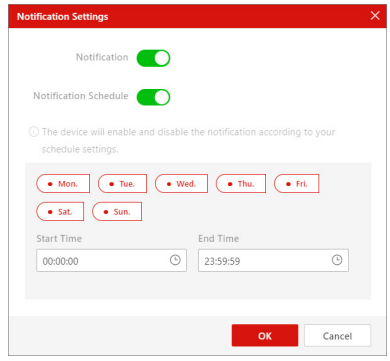


Figure 5-12 Notification Settings

Enable Notification for the Source Device Using the Mobile Client

1. Tap **Site**.
2. Find the device, and tap it to enter its device details page.
3. Tap ••• → **Notification** .
4. Switch on **Notification** and set the **Notification Schedule** for uploading the events detected by the **Source** device to Hik-Partner Pro.

5.5.3 What Are the Six Template Linkages For?

Template	Description
Intrusion	Used for improving the security level by triggering the linkage actions including capture, recording, and alarm output, when the intrusion event (people, vehicles, or other objects enter a predefined area) occurs.
Forced Entry Alarm	Used for improving the security level by triggering the linkage actions including capture, recording, door remaining closed, alarm output, and calling preset when a door is opened abnormally.
Back to Home/Office	Used for lowering the security level and enabling privacy protection by triggering the linkage actions including disarming and enabling privacy mask, when you are back to your home or office from outside.
Away	Used for improving the security level and canceling privacy protection by triggering the linkage actions including arming and disabling privacy mask when you leave your home or office.
Visitor Calling	Used for improving the security level by triggering the linkage actions including capture and recording when visitors are calling from the door station.
Perimeter Zone Alarm	Used for improving the security level by triggering the linkage actions including capture, recording, calling preset, alarm output, and remaining door closed, if people or other objects are detected in all accesses (including doors, windows, cellar doors, etc.) to a property.

5.5.4 Available Triggering Events for Different Source Devices

Table 5-4 Available Triggering Events for Different Resource Types

Source	Triggering Event
Camera	• Motion Detection • Face Detection • Intrusion • Line Crossing Detection
Access Control Device	• Network Disconnected • Tampering Alarm
Door Linked to Access Control Device	• Door Opened Normally **Note** Capture or Recording cannot be set as the linkage action for the triggering event Door Opened Normally. • Door Opened Abnormally • Tampering Alarm
Door Station	• Calling
Area of Security Control Panel	• Away Arming • Disarmed • Stay Arming • Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm.
Zone (Detector) Linked to Security Control Panel	• Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm.
Doorbell	• Calling • PIR Detection

5.5.5 Available Linkage Actions for Different Linked Resources

Table 5-5 Linkage Action Description

Linked Resource	Linkage Action	Description
Camera (Channel)	Capture Picture	The camera will capture a picture when the Triggering Event is detected.
	Recording	The camera will record video footage when the Triggering Event is detected. **Note** The recorded video footage starts from 5 s before the detection of the Triggering Event, and lasts 30 s.
	Call Preset	Select a preset from the Preset drop-down list to specify it as the preset which will be called when the Triggering Event is detected. A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. By calling a preset, the PTZ camera will move to the predefined image position. **Note** Make sure you have configured presets for the PTZ camera. For details, see the user manual of the PTZ camera.
	Call Patrol	S elect a patrol from the Patrol drop-down list to specify it as the patrol which will be called when the Triggering Event is detected. A patrol is a predefined PTZ movement path consisted of a series of key points (i.e., presets) that have their own designated sequence. By calling a patrol, the PTZ camera will travel to all the key points in the set speed so as to provide a dynamic view. **Note** Make sure you have configured patrols for the PTZ camera. For details, see the user manual of the PTZ camera.

Linked Resource	Linkage Action	Description
	Call Pattern	Select a pattern from the Pattern drop-down list tot specify it as the pattern which will be called when the Triggering Event is detected. A pattern is a predefined PTZ movement path with a certain dwell-time configured for a certain position. By calling a pattern, the PTZ camera moves according the predefined path. **Note** Make sure you have configured patterns for the PTZ camera. For details, see the user manual of the PTZ camera.
	Arm	The camera will be armed and hence the events related to the camera will be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected.
	Disarm	The camera will be disarmed and hence the events related to the camera will not be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected.
	Enable Privacy Mask	Privacy mask will be displayed on the live images of the camera when the Triggering Event is detected. **Note** Make sure you have configured privacy mask for the camera. For details, see the user manual of the camera.
	Disable Privacy Mask	Privacy mask will NOT be displayed on the live images of the camera when the Triggering Event is detected.
Alarm Output	Alarm Output	The alarm output of the Linked Resource will be triggered when the Triggering Event is detected.
Area of Security Control Panel	Stay Arm	The arming status of the area of the security control panel will switch to Stay when the Triggering Event is detected.
	Away Arm	The arming status of the area of the security control panel will switch to Away when the Triggering Event is detected.
	Disarm	The area of the security control panel will be disarmed when the Triggering Event is detected.
Door Linked to Access Control Device	Open Door	The door related to the access control device will be opened when the Triggering Event is detected.

Linked Resource	Linkage Action	Description
	Remain Open	The door related to the access control device will remain open when the Triggering Event is detected.
	Remain Closed	The door related to the access control device will remain closed when the Triggering Event is detected.
Door Station	Open Door	The door linked to the door station will be automatically opened when the Triggering Event is detected.
Alarm Input	Arm Alarm Input	The alarm input will be armed and hence events related to it will be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected.
	Disarm Alarm Input	The alarm input will be disarmed and hence events related to it will NOT be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected.

5.6 How to Set Up Exception Rules to Receive Exception Notifications?

You can set up an exception rule to specify how, when, and where you want to receive exception notifications of a device or channel.

What Is An Exception Rule and How to Set One

An exception rule is used to monitor the status of managed resources in real time: When an exception of a resource occurs, the resource will push a notification to Hik-Partner Pro to notify the specified Installers about this exception.
To set an exception rule to define such a notification, you need to define the following five elements.

Table 5-6 Five Elements of an Exception Rule

Element	Description
Source	The resource (device, channel, zones, peripherals, etc.) on which an **Exception** occurs.
Exception	The event/exception occurring on the **Source** for triggering the notification.
Received By	Portal, Mobile Client, email.
Recipient	Who can receive the notification.
Schedule	When to receive the notification.

Table 5-7 Overall Process of Setting a Exception Rule

Steps	Instructions
1. Add resources to Hik-Partner Pro you need them to be the **Source** of exceptions.	***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance***
2. Add the exception notification rule.	***Add an Exception Rule***
3. Enable **Notification** for the **Source** device.	***Enable Notification for the Source Device***

5.6.1 Add an Exception Rule

Add an Exception Rule Using the Portal

1. Go to **Site & Device → Customer Site** .
2. Click a site to enter its site details page, and then click **Exception**.
3. Click to set the elements for triggering a notification of a device. Or click **Batch Edit** to set for multiple devices.

Parameter	Description
Exception	Select the types of exceptions you need to monitor. For **Offline**, you can set the threshold of the offline duration. You will only be notified of **Offline** longer than the threshold.
Received By	Where to receive: Hik-Partner Pro Portal, Hik-Partner Pro App, Hik-Connect App, or Recipients' Emails.
Recipient	Site manager and/or Installer Admin.
Schedule	Set when the recipient can receive the notification.

4. Switch on **Enable** to enable the exception rule. You also click **Copy To** to copy the exception notification settings to the resources of the same type.

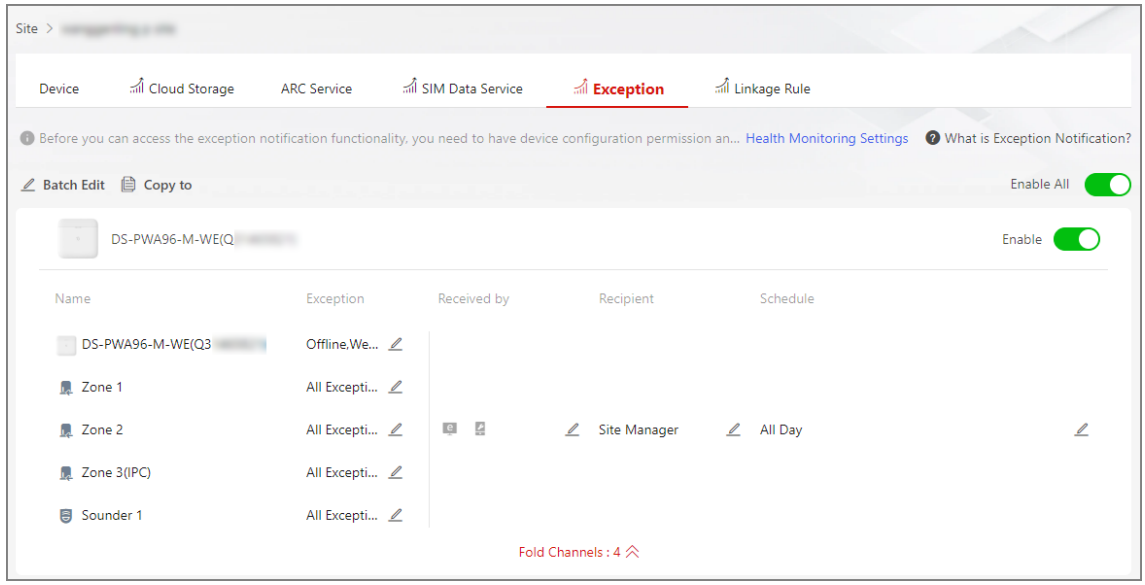


Figure 5-13 Exception Settings

Add an Exception Rule Using the Mobile Client

1. Tap **Site**.
2. Tap a site to enter its site details page, and then tap **Exception**.
3. Tap **Device/Channel Exception** and **How to Receive** to set the elements for triggering a notification of a device. Or tap to batch set for multiple devices.

Parameter	Description
Device/Channel Exception	Select the types of exceptions you need to monitor. For **Offline**, you can set the threshold of the offline duration. You will only be notified of **Offline** longer than the threshold.
Recipient	Site manager and/or Installer Admin.
Received By	Where to receive: Hik-Partner Pro Portal, Hik-Partner Pro App, Hik-Connect App, or Recipients' Emails.
Schedule	Set when the recipient can receive the notification.

4. Switch on the button on the device card to enable the exception rule. You also tap to copy the exception notification settings to the resources of the same type.

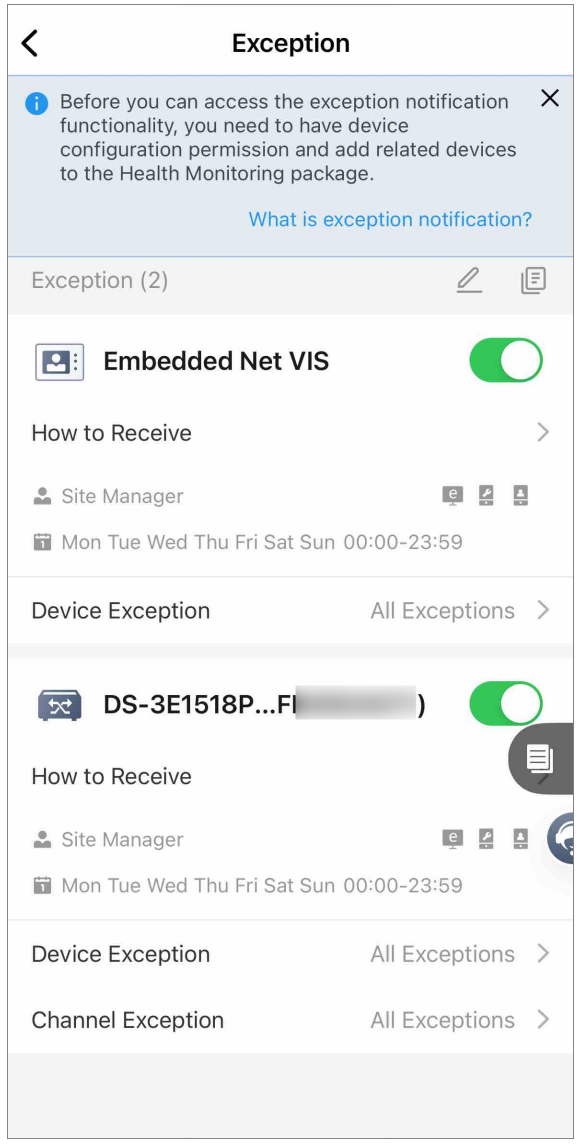


Figure 5-14 Exception Settings

5.6.2 Enable Notification for the Source Device

After adding and enabling an exception rule, you should make sure the Notification functionality of the Source device is enabled so that the events detected by the device can be uploaded to the Hik-Partner Pro system and the Hik-Connect Mobile Client, which is the prerequisite to trigger the exception rules defined in related exception rules.

Enable Notification for the Source Device Using the Portal

1. Go to **Site & Device → Customer Site** .
2. Find the device, and click on the device card or in the Operation column.
3. Switch on **Notification** and set the **Notification Schedule** for uploading the events detected by the **Source** device to Hik-Partner Pro.
4. Click **OK**.

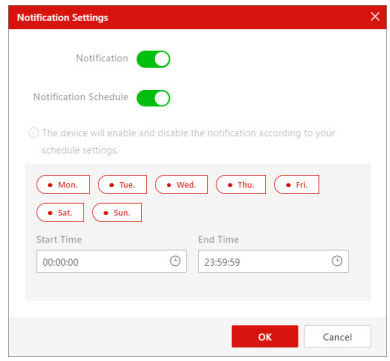


Figure 5-15 Notification Settings

Enable Notification for the Source Device Using the Mobile Client

1. Tap **Site**.
2. Find the device, and tap it to enter its device details page.
3. Tap → **Notification** .
4. Switch on **Notification** and set the **Notification Schedule** for uploading the events detected by the **Source** device to Hik-Partner Pro.

5.7 How to Configure Device Offline Delay?

You can set the allowed offline duration for the device. Hik-Partner Pro, ARC, and Hik-Connect will receive offline exceptions only if the device is offline for longer than the configured duration.

- This feature only supports devices that are connected to Hik-Connect services (P2P).
- Make sure you have activated health monitoring services and configured **Offline** as an exception type on the site details page. For security control devices, if your only need ARC and Hik-Connect to receive notifications, you do not need to activate health monitoring services.

Configure Device Offline Delay Using the Portal

1. Go to **Site & Device → Customer Site** .
2. Open the Configure Offline Delay pane via one of the following ways.
   - Find the device, and click on the device card/list.

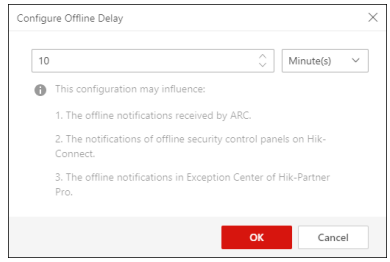


Figure 5-16 Configure Offline Delay

- Find and click the site, click **Exception**, click on the device card in the **Exception** column.

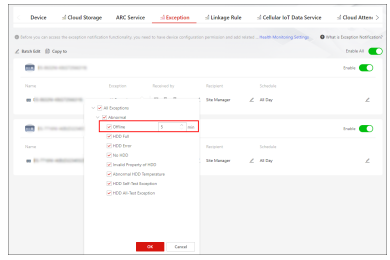


Figure 5-17 Configure Device Offline Delay on Site Details Page

3. Specify the delay duration (5 minutes to 24 hours).
4. Click **OK**.

Configure Device Offline Delay Using the Mobile Client

1. Tap **Site** .
2. Tap the site to enter the site details page, and tap **Exception**.
3. Tap **Device/Channel Exception → Exception** .

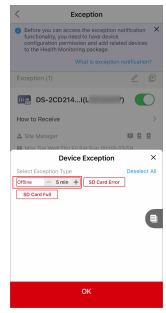


Figure 5-18 Configure Device Offline Delay

4. Specify the delay duration (5 minutes to 24 hours).
5. Tap **OK**.

5.8 How to View Device Health Status in Real Time?

Note

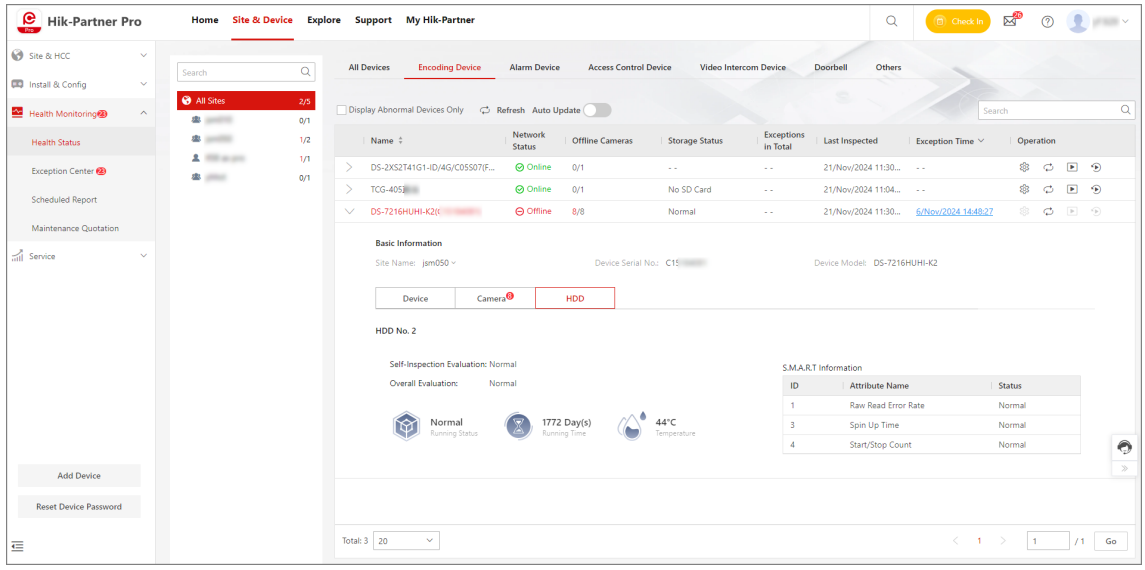
Make sure you have activated the health monitoring service.

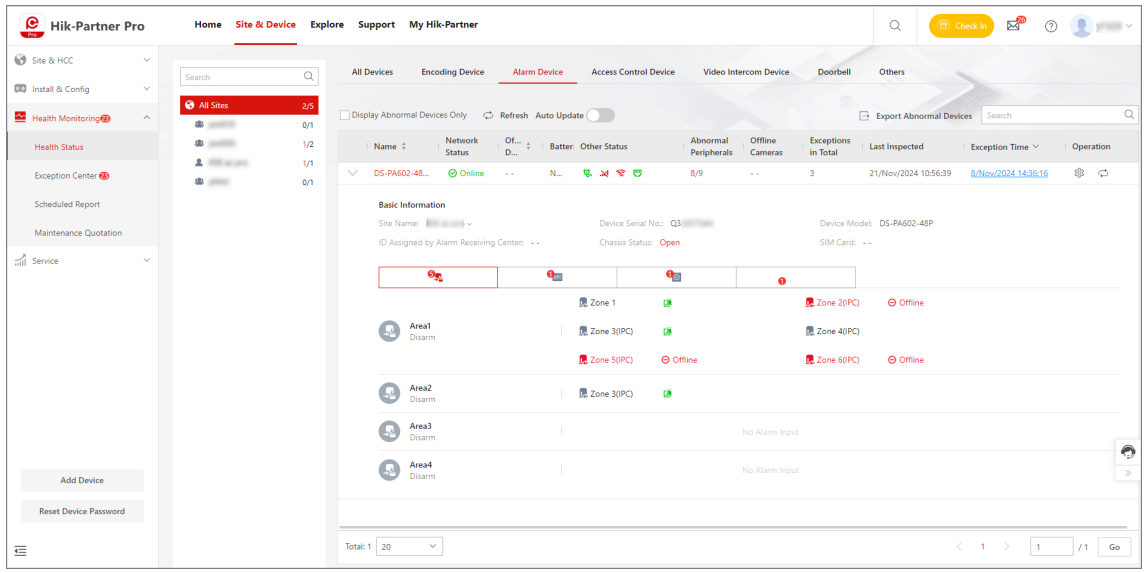
5.8.1 View Devices Health Status

View Device Health Status Using the Portal

1. Go to **Site & Device → Health Monitoring → Health Status** .
2. - To view all devices on all sites by device type, click **All Sites**, and select a device type.
   - To view all devices on a specific site, select a site.
3. View the device status and perform related operations. See ***Supported Device Status and Operations for Different Device Types*** for more supported status and operations.

Button	Description
	Perform remote configuration.
	Perform health check/inspection to get the latest device status.
	Live view.
	Playback.
Auto Update	Switch on **Auto Update** so that the latest exceptions and status will be displayed in real time.


Hik-Partner Pro
Home
Site & Device
Explore
Support
My Hik-Partner
Check In
Site & HCC
Install & Config
Health Monitoring
Health Status
Exception Center
Scheduled Report
Maintenance Quotation
Service
Add Device
Reset Device Password
Search
All Sites
All Devices
Encoding Device
Alarm Device
Access Control Device
Video Intercom Device
Doorbell
Others
Display Abnormal Devices Only
Refresh
Auto Update
Name
Network Status
Offline Cameras
Storage Status
Exceptions in Total
Last Inspected
Exception Time
Operation
Basic Information
Device
Camera
HDD
HDD No. 2
Self-Inspection Evaluation: Normal
Overall Evaluation: Normal
S.M.A.R.T Information
ID
Attribute Name
Status
Raw Read Error Rate
Spin Up Time
Start/Stop Count
Normal
1772 Day(s)
44°C
Total: 3
20
Go


Hik-Partner Pro
Home
Site & Device
Explore
Support
My Hik-Partner
Check In
Site & HCC
Install & Config
Health Monitoring
Health Status
Exception Center
Scheduled Report
Maintenance Quotation
Service
Add Device
Reset Device Password
Search
All Sites
All Devices
Encoding Device
Alarm Device
Access Control Device
Video Intercom Device
Doorbell
Others
Display Abnormal Devices Only
Refresh
Auto Update
Export Abnormal Devices
Name
Network Status
Other Status
Abnormal Peripherals
Offline Cameras
Exceptions in Total
Last Inspected
Exception Time
Operation
Basic Information
Zone 1
Zone 2(IPC)
Offline
Area1
Disarm
Zone 3(IPC)
Zone 4(IPC)
Zone 5(IPC)
Offline
Zone 6(IPC)
Offline
Area2
Disarm
Zone 3(IPC)
Area3
Disarm
No Alarm Input
Area4
Disarm
No Alarm Input
Total: 1
20
Go

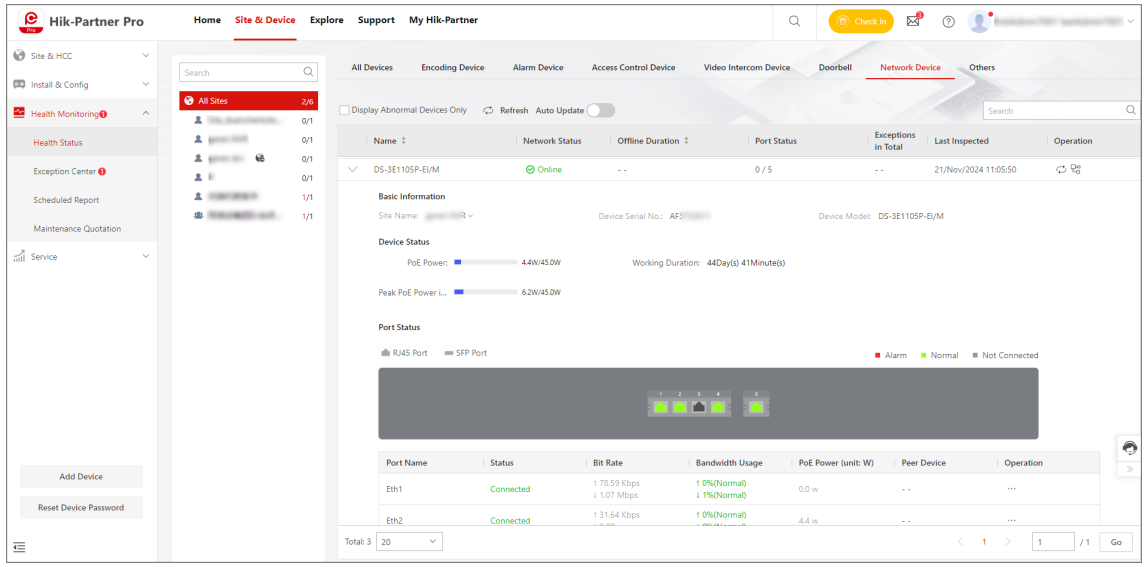


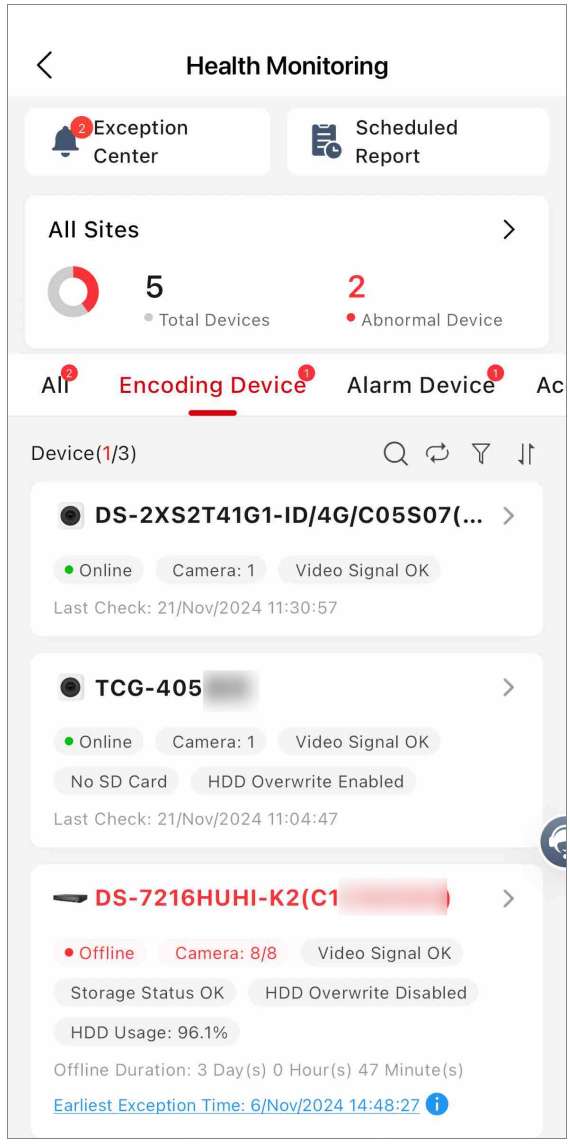
Figure 5-19 Health Status on the Portal

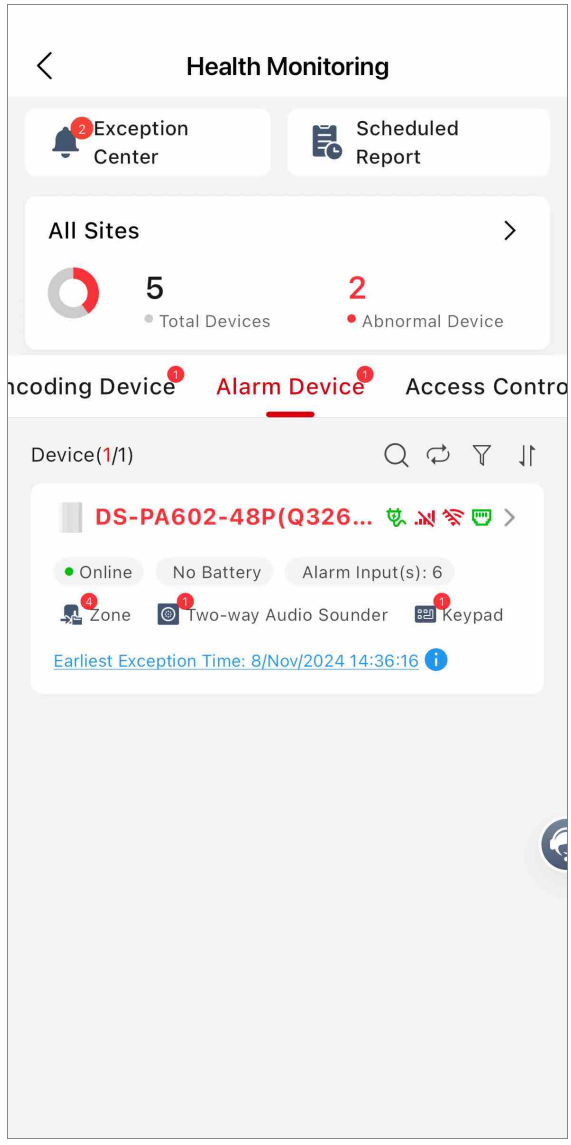
View Device Health Status Using the Mobile Client

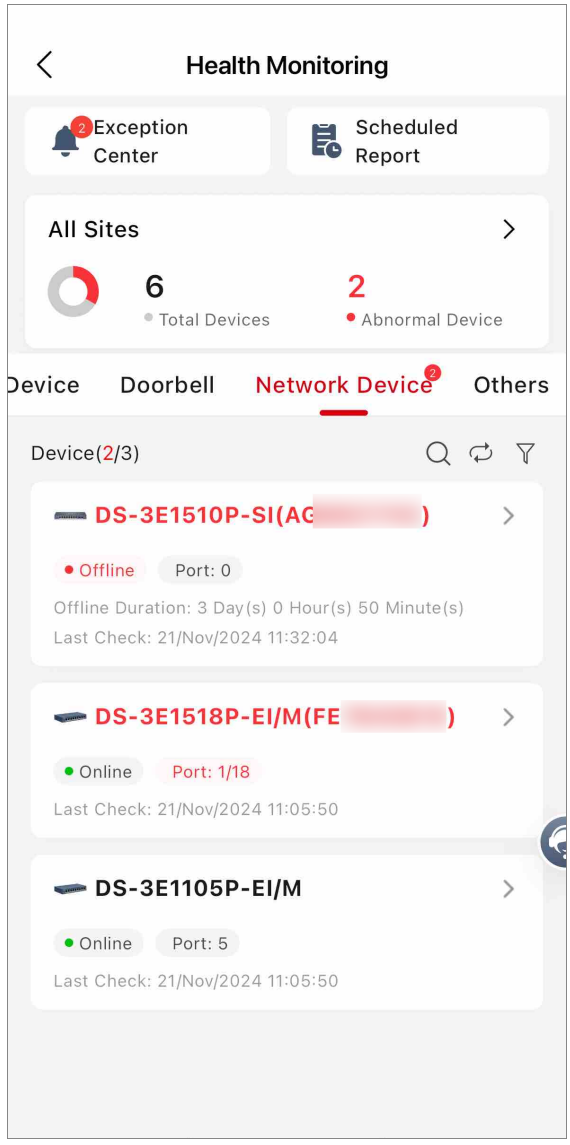
Tap **Site & Device → Health Monitoring → Health Status** , select **All Sites** to view device health status by device type, or select a specific site to view the devices of this site.

1. Tap **Site → Health Monitoring** .
2. - To view all devices on all sites by device type, select a device type.
   - To view all devices on a specific site, tap **All Sites**, and select a site.
3. View the device status and perform related operations. See ***Supported Device Status and Operations for Different Device Types*** for more supported status and operations.

Button	Description
	Perform remote configuration.
	Perform health check/inspection to get the latest device status.
	Live view.
	Playback.
Auto Update	Switch on **Auto Update** so that the latest exceptions and status will be displayed in real time.


Health Monitoring
Exception Center
Scheduled Report
All Sites
5
Total Devices
2
Abnormal Device
All
Encoding Device
Alarm Device
Ac
Device(1/3)
DS-2XS2T41G1-ID/4G/C05S07(...
Online
Camera: 1
Video Signal OK
Last Check: 21/Nov/2024 11:30:57
TCG-405
Online
Camera: 1
Video Signal OK
No SD Card
HDD Overwrite Enabled
Last Check: 21/Nov/2024 11:04:47
DS-7216HUHI-K2(C1
Offline
Camera: 8/8
Video Signal OK
Storage Status OK
HDD Overwrite Disabled
HDD Usage: 96.1%
Offline Duration: 3 Day(s) 0 Hour(s) 47 Minute(s)
Earliest Exception Time: 6/Nov/2024 14:48:27


Health Monitoring
Exception Center
Scheduled Report
All Sites
5
Total Devices
2
Abnormal Device
ncoding Device
Alarm Device
Access Contro
Device(1/1)
DS-PA602-48P(Q326...
Online
No Battery
Alarm Input(s): 6
Zone
Two-way Audio Sounder
Keypad
Earliest Exception Time: 8/Nov/2024 14:36:16


Health Monitoring
Exception Center
Scheduled Report
All Sites
6
Total Devices
2
Abnormal Device
Device
Doorbell
Network Device
Others
Device(2/3)
DS-3E1510P-SI(AG)
Offline
Port: 0
Offline Duration: 3 Day(s) 0 Hour(s) 50 Minute(s)
Last Check: 21/Nov/2024 11:32:04
DS-3E1518P-EI/M(FE)
Online
Port: 1/18
Last Check: 21/Nov/2024 11:05:50
DS-3E1105P-EI/M
Online
Port: 5
Last Check: 21/Nov/2024 11:05:50

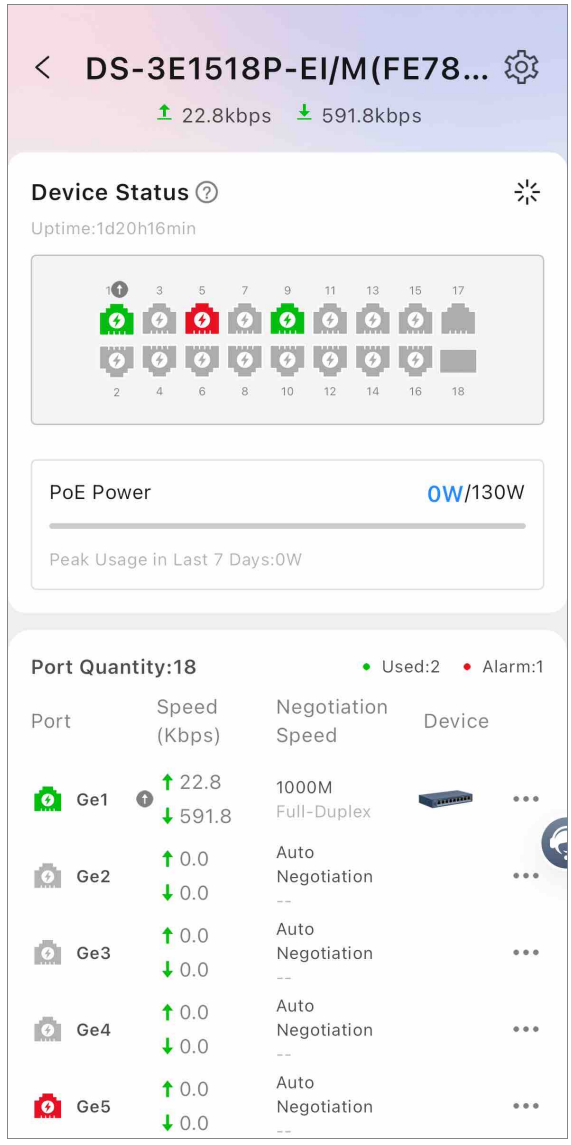


Figure 5-20 Health Status on the Mobile Client

5.8.2 Supported Device Status and Operations for Different Device Types

Device Type	Device Status	Device Operations
Encoding Device	• Device: Network Status, Storage Status, Video Signal, HDD Usage, Overwritten Recording Status	Live View, Playback, Remote Configuration

Device Type	Device Status	Device Operations
	appears beside the device name when you have no configuration permission for it, the IP/domain is invalid, or DDNS is invalid. You can fix these issues via . • Channel: Network Status • HDD: Self-Inspection Evaluation Result, Overall Evaluation Result, Running Status, Running Time, Temperature, S.M.A.R.T Information	
Alarm Device	• Device: Network Status, Offline Duration, Battery Status, Power Supply Status, Mobile Network Status, Wireless Network Status, Network Cable Status, Quantity of Abnormal Peripherals, Chassis Status, SIM Card Status appears beside the device name when firmware update is available. You can upgrade firmware via . appears beside the device name when EN50131 Compliant mode has been enabled on the device, or you have no configuration permission for it. For the former, authenticate the device via so you can view the device status. • Area (Zones) and Peripheral:	Remote Configuration

Device Type	Device Status	Device Operations
	Network Status, Zone Triggering Status, Tampering Status, etc.	
Hik-ProConnect Box	Network Status, Quantity of Offline Channels	Remote Configuration
Access Control Device	Network Status, Offline Duration, Door Quantity appears beside the device name when you have no configuration permission for it. You can fix the issue via . • : Sufficient battery power. • : Insufficient battery power. • : Normal strength of the communication signals between the peripheral device and the security control panel. • : Weak strength of the communication signals between the peripheral device and the security control panel. • : Alarm triggered. • : Device tampered. • : Zone bypassed. • : Trigger exception.	Remote Configuration
Video Intercom Device	Network Status appears beside the device name when you have no configuration permission for it.	Remote Configuration
Doorbell	Network Status, SD Card Status appears beside the device name when firmware update is	Live View, Remote Configuration

Device Type	Device Status	Device Operations
	available. You can upgrade firmware via .	
Network Device	Network Status, Offline Duration, Quantity of Online Ports, Memory Usage, CPU Usage, PoE Power, Peak PoE Power, Working Duration, Port Status, Network Topology	• Remote Configuration • : View Topology • : Remotely Reboot Device • → **Clear Alarm** : Clear Alarms of Ports • → **Restart Port** : Restart Port • → **Enable Extend Mode** : Extend Transmission Range of Port **Note** When enabled, the transmission range of the port will be extended from 200 to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.

5.9 Health Monitoring: AI Diagnostics & One-Click Fix Guide

5.9.1 Feature Overview

Based on Health Monitoring exception detection, Hik-Partner Pro introduces AI-powered troubleshooting to automatically generate targeted diagnostic and resolution recommendations. This helps users quickly identify root causes and take effective actions. For certain simple issues (such as time zone exceptions), a one-click fix is also supported to further improve resolution efficiency.

5.9.2 Applicable Scenarios

When device exceptions are detected through Health Monitoring, such as offline status, battery issues, weak signal, high temperature, or time zone exceptions, users can leverage **AI Diagnostics** to obtain intelligent diagnostic guidance or perform one-click fixes.

5.9.3 Prerequisites

- You have purchased the Health Monitoring value-added service.
- You have enabled Health Monitoring on the target devices.
- You have remote configuration permission for the devices.

5.9.4 Supported Device Types

AI Diagnostics supports all device types that enable Health Monitoring, including but not limited to:

- Encoding Devices
- Alarm Devices
- Video Intercom Devices
- Access Control Devices
- Doorbells
- Cloud Storage Boxes
- Network Devices
- Other Health Monitoring Enabled Devices

5.9.5 AI Diagnostics Workflow

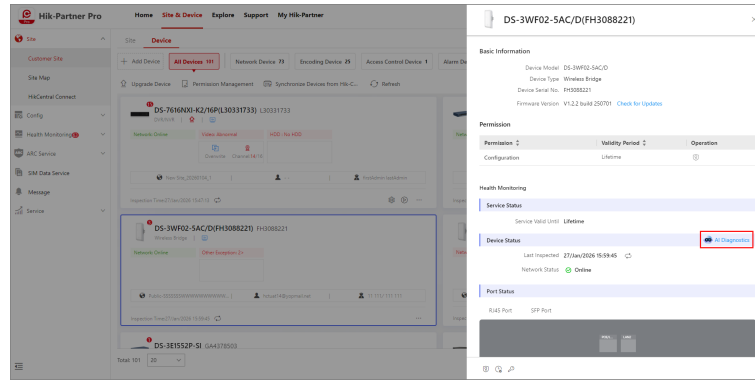
1. The **AI Diagnostics** entry is available on the following pages.

Note

AI Diagnostics is available only when **Health Monitoring** is enabled for the device.

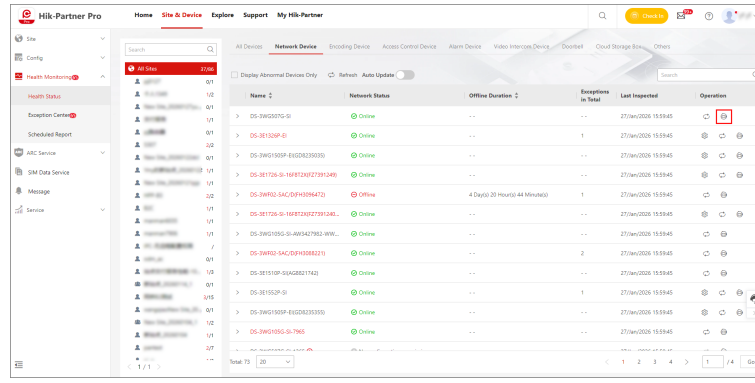
Device Details Page:

In **Customer Site**, select a device, and click **AI Diagnostics**.



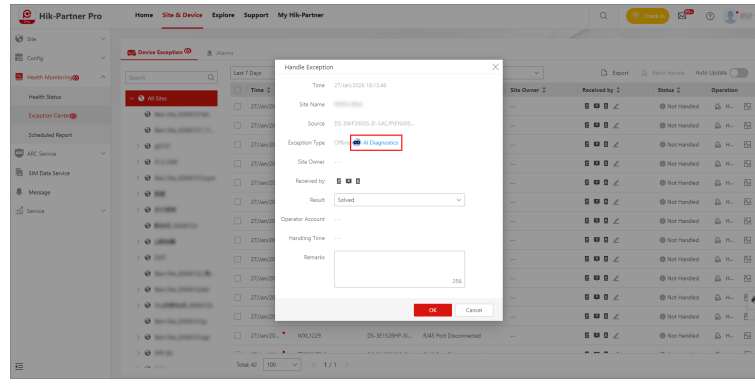
Health Status

In **Health Monitoring → Health Status** , click in the Operation column of the corresponding device.



Exception Center

In **Exception Center → Device Exception** , click **Handle** in the Operation column of the corresponding device, and then click **AI Diagnostics** .



5.10 How to Export Device Health Report and Set Scheduled Report Delivery?

Note

- Make sure you have activated the health monitoring service or remote maintenance Pro service.
- Health check reports only support encoding devices and security control panels.

Your Intention	Report Scope	Instructions
To Perform Health Check and Export the Report Manually	For All Devices of a Site	***Export Reports Manually of a Site***
Reports Being Sent Automatically and Regularly to You and Your Customers	For All Devices of a Site or a Site Group	***Set Scheduled Report Delivery***

Device Health Report Template

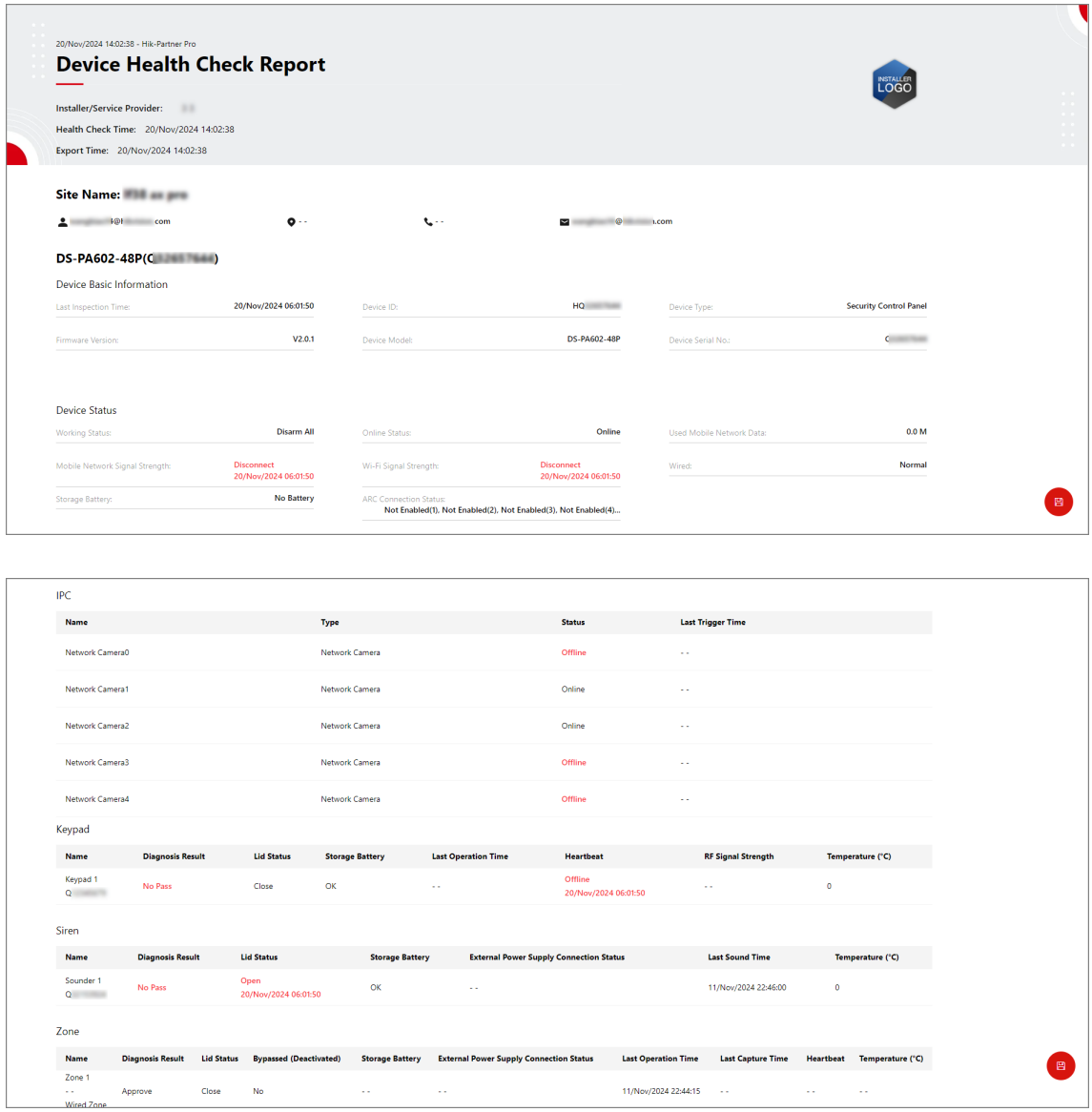


Figure 5-21 Device Health Report Template

5.10.1 Export Reports Manually of a Site

Export Reports Manually of a Site Using the Portal

1. Go to **Site & Device → Health Monitoring → Health Status** , or go to **Site & Device → Customer Site** .
2. Select a site from the list for which you need to export the report.
3. Click **Health Check**.
4. Click **Check Now** to check the health status of the devices on the site and generate a report.
5. To export the report of a device, click **View Report**. To export the report of all devices on the site, click **Export Report**.

Export Reports Manually of a Site Using the Mobile Client

1. Tap **Site → Health Monitoring** .
2. Tap **All Sites**, and select a site for which you need to export the report.
3. Tap **Health Check**.
4. Tap **Check Now** to check the health status of the devices on the site and generate a report.
5. To export the report of a device, tap . To export the report of all devices on the site, tap **View All Reports**.

5.10.2 Set Scheduled Report Delivery

Set Scheduled Report Delivery Using the Portal

1. Go to **Site & Device → Health Monitoring → Scheduled Report** .
2. Select **Site Report** or **Site Group Report**, and configure the report delivery settings.

Report Type	Description	Steps
Site Report	One report for one site.	Click **Edit** to set for a site, or click **Batch Configure** and select sites to set for multiple sites.
Site Group Report	One report for a group of sites. For how to group sites, see ***Group Sites to Manage Multiple Sites More Efficiently*** .	Click **Edit** or click **Add** to set for a site group.

Delivery Parameter	Description
Device	Devices to be included in the report.
Schedule	Set the frequency and specific time for sending the report. Supports annually, quarterly, monthly, weekly, and daily.
Recipient Email Address	Enter one or more email addresses to set recipients.
Report Language	Choose a language for the report.

3. Click **OK** or **Add**.
4. To enable the scheduled delivery settings, switch on **Enable** or **Enable All**.

Set Scheduled Report Delivery Using the Mobile Client

1. Tap **Site → Health Monitoring → Scheduled Report** .
2. Select **Site Report** or **Site Group Report**, and configure the report delivery settings.

Report Type	Description	Steps
Site Report	One report for one site.	Tap a site card to set for a site, or tap **Batch Configure** and select sites to set for multiple sites.
Site Group Report	One report for a group of sites. For how to group sites, see ***Group Sites to Manage Multiple Sites More Efficiently*** .	Tap a site group card or tap **Add** to set for a site group.

Delivery Parameter	Description
Device	Devices to be included in the report.
Schedule	Set the frequency and specific time for sending the report. Supports annually, quarterly, monthly, weekly, and daily.
Recipient Email Address	Enter one or more email addresses to set recipients.
Report Language	Choose a language for the report.

3. Tap **Save**.
4. To enable the scheduled delivery settings, switch on the button.

5.11 How to Create Maintenance Quotation?

To provide customers with regular and professional device maintenance services, you can use the tool for after-sales maintenance quotation, with which you can standardize the service process, improve customer satisfaction, and expand your business.

Note

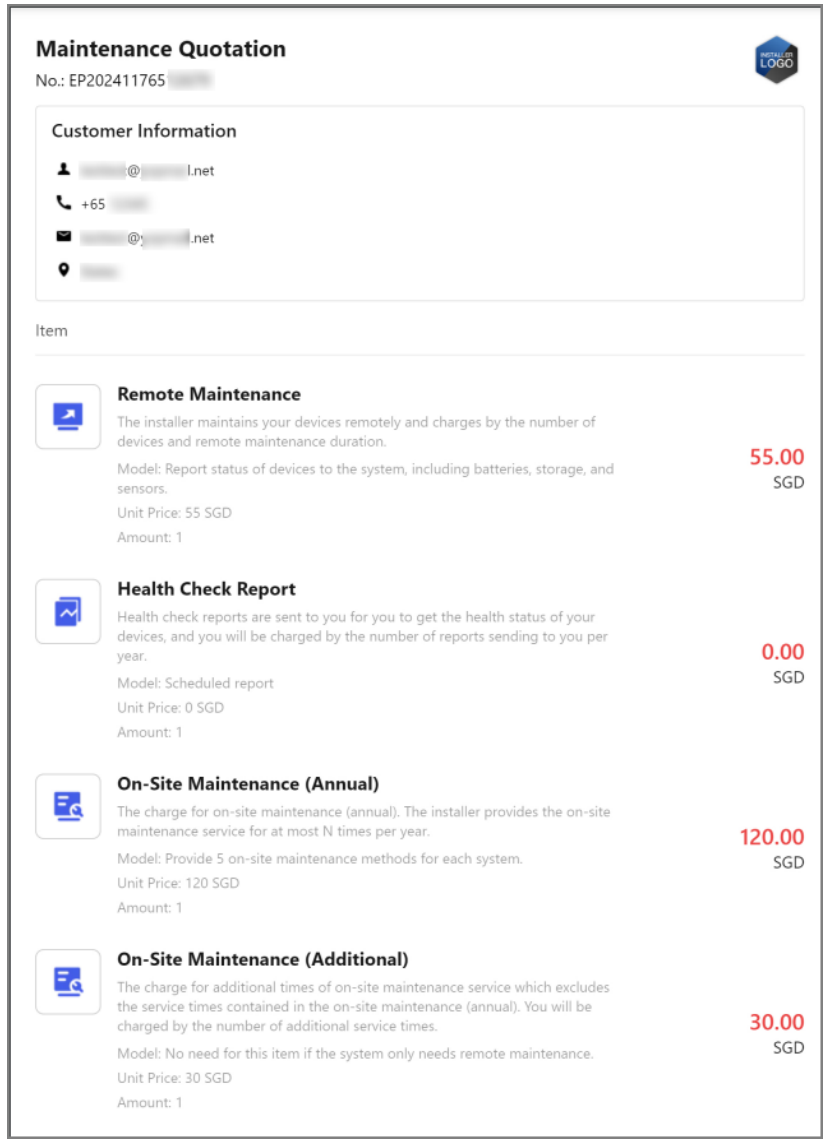
You can create unlimited number of quotations if you activate the health monitoring service or remote maintenance Pro service. Otherwise, you can create only 3 quotes.

Create a Maintenance Quotation Using the Portal

1. Go to **Site & Device → Health Monitoring → Maintenance Quotation** .
2. Click **Create Quotation**.
3. Set the required information.

Parameter	Description
Quotation Details	Quotation name and quotation No.
Customer Information	Customer's name, email, phone, and address. Or click **Get from Site** and select a site to auto sync the info.
Item	Click **Add Item** to add the default or custom items. Then, set the device model, unit price, and quantity.
Set Discount	If needed, set a discount for your customer.
Set VAT Rate	If needed, set the VAT rate.
Service Provider Information	Service provider's name, email, phone number, address, and company logo.

4. Click **Preview/Export** to see and export it as a PDF file.
5. Click **Save**.



Maintenance Quotation

No.: EP202411765

Customer Information

Item

Remote Maintenance

The installer maintains your devices remotely and charges by the number of devices and remote maintenance duration.

Model: Report status of devices to the system, including batteries, storage, and sensors.

Unit Price: 55 SGD

Amount: 1

55.00 SGD

Health Check Report

Health check reports are sent to you for you to get the health status of your devices, and you will be charged by the number of reports sending to you per year.

Model: Scheduled report

Unit Price: 0 SGD

Amount: 1

0.00 SGD

On-Site Maintenance (Annual)

The charge for on-site maintenance (annual). The installer provides the on-site maintenance service for at most N times per year.

Model: Provide 5 on-site maintenance methods for each system.

Unit Price: 120 SGD

Amount: 1

120.00 SGD

On-Site Maintenance (Additional)

The charge for additional times of on-site maintenance service which excludes the service times contained in the on-site maintenance (annual). You will be charged by the number of additional service times.

Model: No need for this item if the system only needs remote maintenance.

Unit Price: 30 SGD

Amount: 1

30.00 SGD

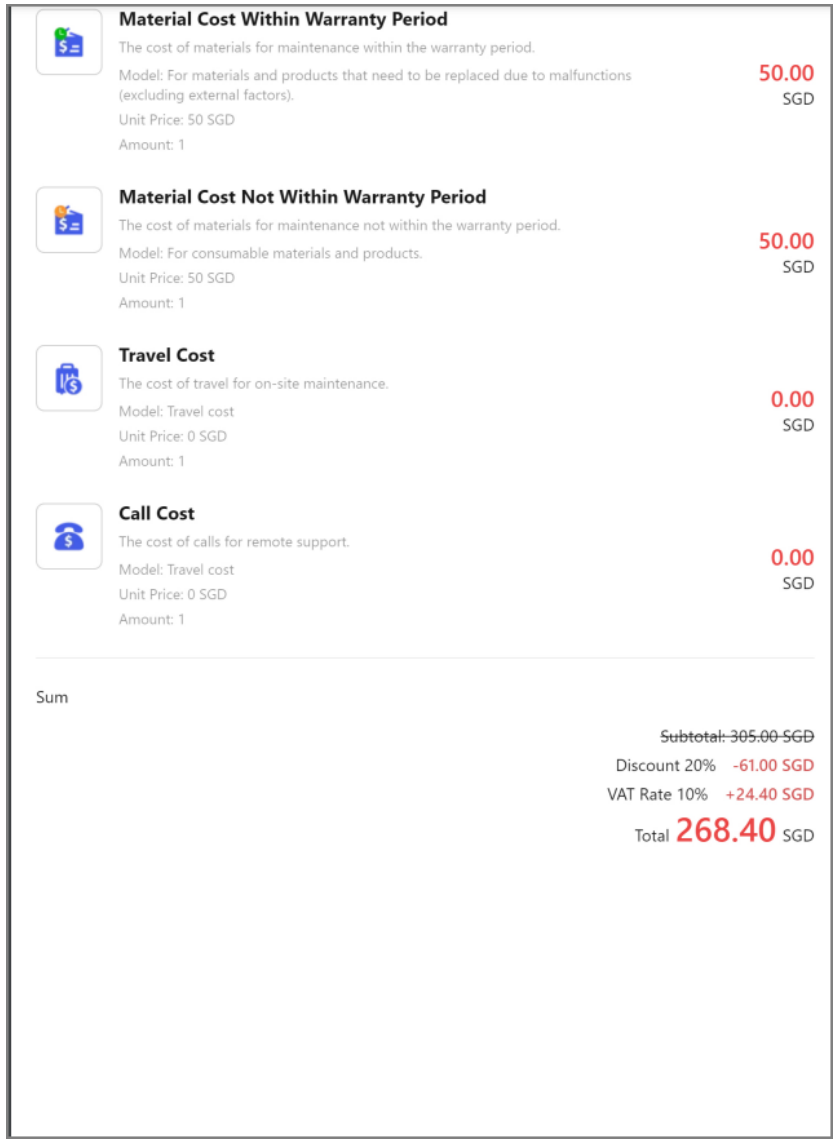

Material Cost Within Warranty Period
The cost of materials for maintenance within the warranty period.
Model: For materials and products that need to be replaced due to malfunctions (excluding external factors).
Unit Price: 50 SGD
Amount: 1
50.00
SGD
Material Cost Not Within Warranty Period
The cost of materials for maintenance not within the warranty period.
Model: For consumable materials and products.
Unit Price: 50 SGD
Amount: 1
50.00
SGD
Travel Cost
The cost of travel for on-site maintenance.
Model: Travel cost
Unit Price: 0 SGD
Amount: 1
0.00
SGD
Call Cost
The cost of calls for remote support.
Model: Travel cost
Unit Price: 0 SGD
Amount: 1
0.00
SGD
Sum
Subtotal: 305.00 SGD
Discount 20% -61.00 SGD
VAT Rate 10% +24.40 SGD
Total 268.40 SGD



Figure 5-22 Maintenance Quotation Template

5.12 How to Get Operations Logs of Employees for Troubleshooting?

Operation logs (the operator, time, site, target, result, etc.) of all employees (Installer Admin and Installers) will be recorded and you can search for the operation logs of any employee within 90 days for troubleshooting the sites and devices.

Note

- This feature is not available to authenticated channel partners.
- Logs of all employees are available to those with the permission to manage accounts and roles. For those without this permission, they can only view their own logs.
- Logs of all sites are available to those with the permission to manage all sites. For those without this permission, they can only view the logs of the sites assigned to them.
- Logs within up to 90 days are available.

Search Operation Logs Using the Portal

To access the operation logs, click **My Hik-Partner → Company Management → Operation Log** . You can search for operation logs by the employee, site, and time.

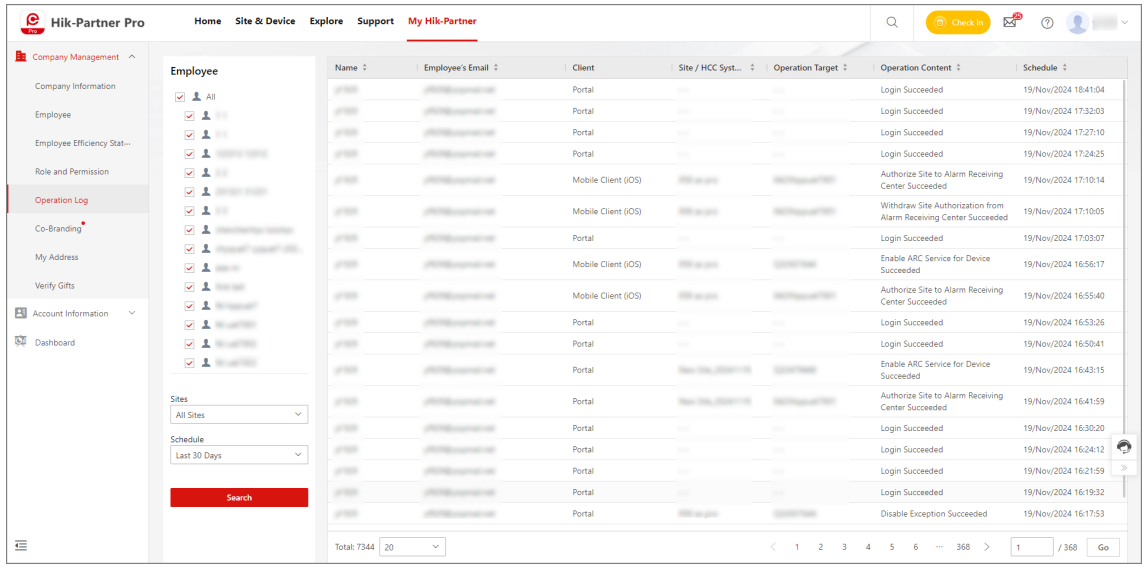


Figure 5-23 Search Operation Logs

5.13 How to Provide an ARC Service on Hik-Partner Pro to Expand Your Business?

5.13.1 Feature Overview

Alarm Receiving Centers (ARC) is a facility that receives and reacts quickly to alarms from systems of companies, schools, factories, etc., for the security purpose. Hik-Partner Pro offers a list of authenticated professional ARCs, from which installers can select to provide 24/7 remote alarm receiving service for their customers.

Note

The ARC service is available in only some countries and regions.

5.13.2 Overall Instruction

Table 5-8 Overall Instruction

Your Role	Description	Related Topics
ARC Service Provider	Add your company to Hik-Partner Pro's ARC list. After that, all other Hik-Partner Pro users can be your potential customers. This promotes brand awareness for your company and provides great possibility to expand business. And you can manage your ARC service using Hik-Partner Pro if it is supported in your region/ country. **Note** The ARC service is only supported by the devices added by Hik-Connect (P2P). The supported device types include cameras, NVRs, and security control panels.	• ***Step 1: ARC Company Joins the ARC List of Hik-Partner Pro*** • ***Step 3: ARC Service Provider Accepts Devices Entrusted by Installers*** • ***Step 4: ARC Manages Entrusted Devices*** • ***Step 5: ARC Establishes Communications Between ARC Software and Devices Using IP Receiver Pro*** • ***How to Integrate with Hik-Partner Pro?***
Installer or Other Hik-Partner Pro Users	Select from Hik-Partner Pro's ARC list to provide 24/7 remote alarm receiving service for your customers.	• ***Step 2: Installer Enables ARC Service for Customer's Devices*** • ***Authorization Rules for ARC Service***

5.13.3 View of Authorizing an ARC Service Provider

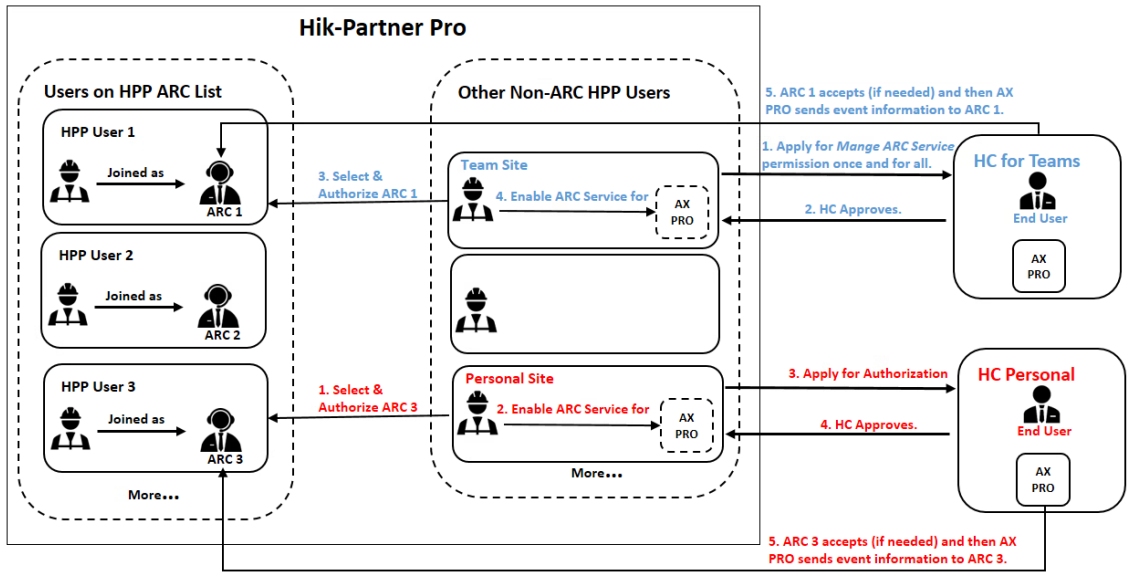


Figure 5-24 View of Authorizing an ARC Service Provider

5.13.4 Authorization Rules for ARC Service

When installers authorize an ARC service provider and enable the ARC service for a device, the required authorization process varies depending on whether the site is handed over and the site type.

Scenario	Site Type	Authorization Requirement
Handed Over	**Personal Site**	Each time ARC service is enabled for a device, approval is required from both the ARC side (if supported) and the Hik-Connect personal user side.
	Team Site	Each time ARC service is enabled for a device, only approval from the ARC side is required (if supported), provided the user has the **Manage ARC Service** permission. ***How to Apply for Manage ARC Service Permission for a Team Site***
Not Handed Over	Both **Personal Site** and **Team Site**	Each time ARC service is enabled for a device, only approval from the ARC side is required (if supported).Each time ARC is enabled for a device, only approval from the ARC side is required (if supported).

Note

- "ARC side approval" refers to acceptance performed by the ARC service provider. This feature is supported only in some regions/countries.
- "Hik-Connect personal user approval" refers to authorization confirmation from the device end user (customer) using a Hik-Connect personal account.

How to Apply for Manage ARC Service Permission for a Team Site

You can apply for **Manage ARC Service** permission when you hand over the team site (either by transferring or sharing).

Using the Portal

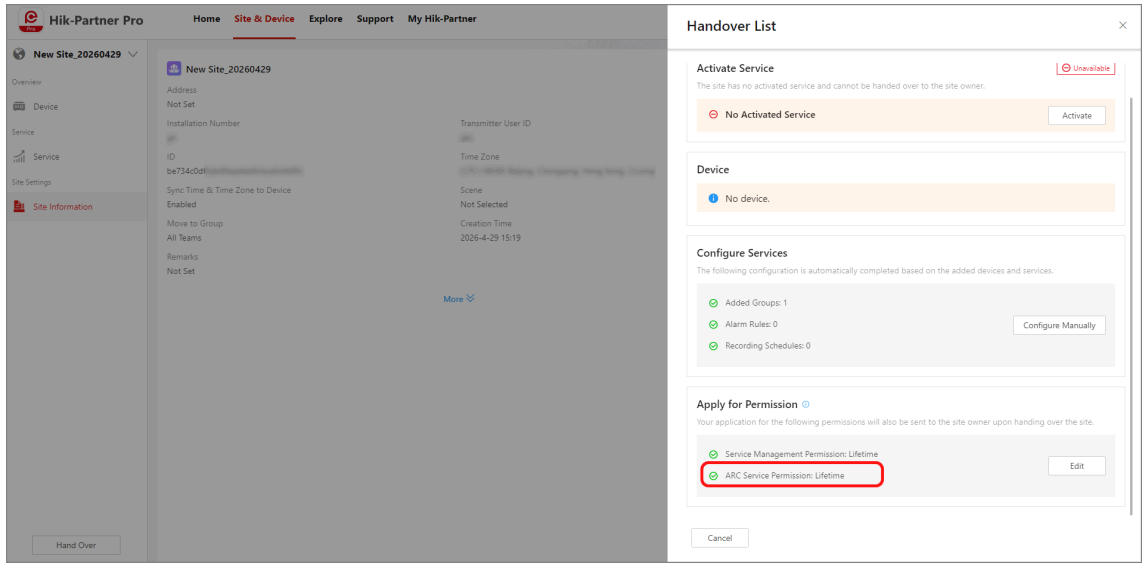


Figure 5-25 Apply for Manage ARC Service Permission

Using the Mobile Client

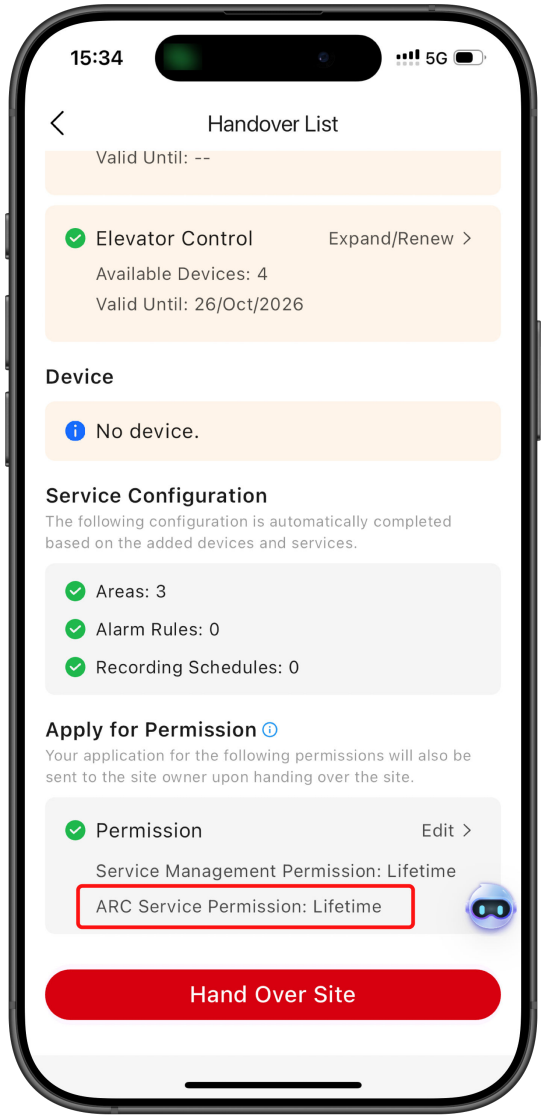


Figure 5-26 Apply for Manage ARC Service Permission

5.13.5 Step 1: ARC Company Joins the ARC List of Hik-Partner Pro

ARC Company Joins the ARC List of Hik-Partner Pro Using the Portal

Before joining as ARC, make sure the type of your company is ARC on your company information page.

1. Go to **My Hik-Partner → Company → Company Information** .

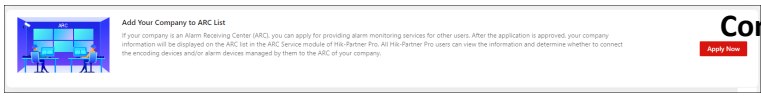


Figure 5-27 Entry

2. Click **Apply Now**.

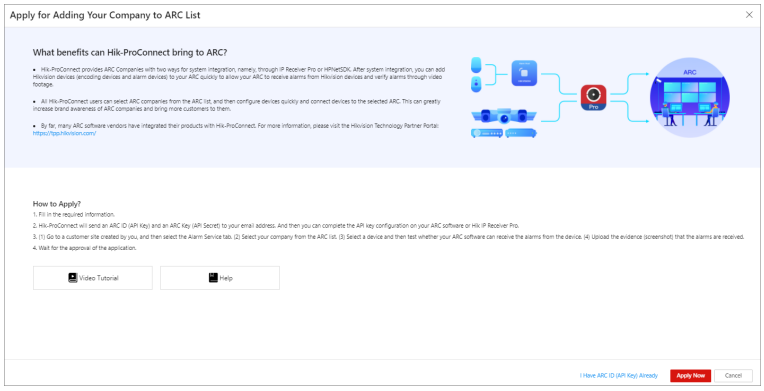


Figure 5-28 Introduction Page of Joining as ARC

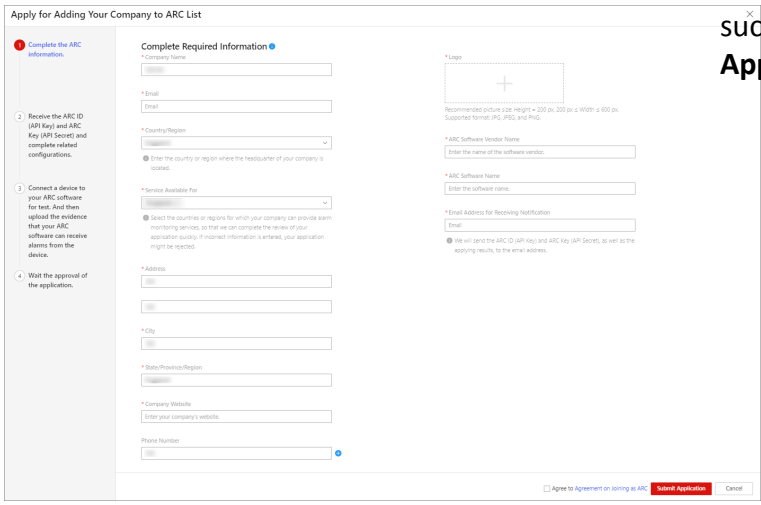


Figure 5-29 Fill in Information

3. Complete the required company information such as the email address, and click **Submit Application**.

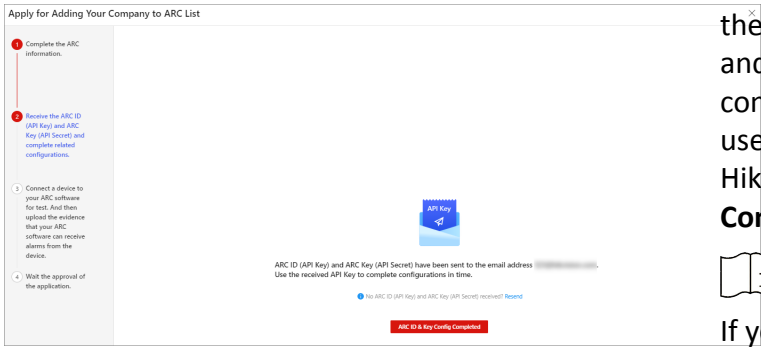


Figure 5-30 ARC ID & Ket Sent

4. Make sure you receive an email containing the ARC ID (API Key) and ARC Key (API Secret), and then complete the ARC ID and ARC Key configuration on your ARC software (software used by your company for receiving alarms) or Hik IP Receiver Pro. Last, click **ARC ID & Key Config Completed**.

Note

If you have any questions about the ARC ID and ARC Key configuration, refer to **Agreement on Joining as ARC** and find the email for getting help.

5.13.6 Step 2: Installer Enables ARC Service for Customer's Devices

You can authorize a site to an ARC, and then enable the ARC service for devices on the site to allow the staff of the ARC to receive events from the devices, respond to the events, and send out emergency dispatches (if needed) around the clock.

Note

The ARC service is only supported by the devices added by Hik-Connect (P2P). The supported device types include cameras, NVRs, and security control panels.

Enable ARC Service for Devices Using the Portal

1. Go to **Site & Device → Customer Site** , and click the site to enter its site details page.
2. Click **ARC Service**.
3. Click **Select ARC** to show the ARC list. You can check the ARC's information.
4. Select an ARC, and click **Authorize**. Devices on this site available for the ARC service will show.
5. Enable the ARC service for a specific device. After the ARC confirms, events detected by the device and device exceptions will be sent to the ARC.
   a. Turn on the button on the device card.
   b. To help the ARC identify the device, set the account number.
   c. Click **Next**.
   d. Set the types of notifications (events) that can be received by the ARC.
   e. Click **OK**.
   f. Waiting for required confirmation and authorization if needed.

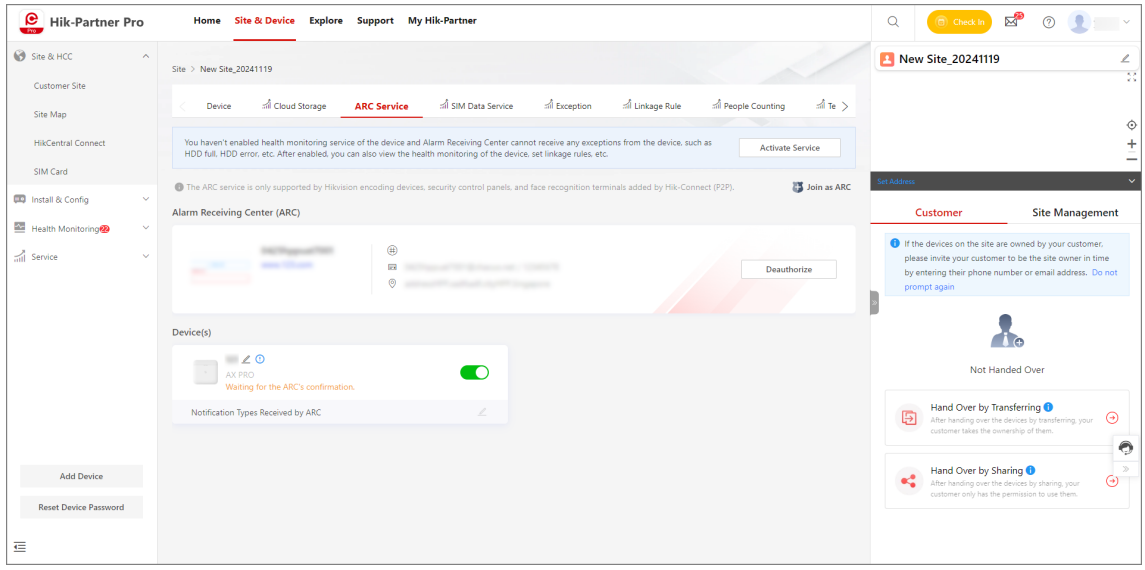


Figure 5-31 Enable ARC Service for Devices Using the Portal

Enable ARC Service for Devices Using the Mobile Client

Note

Enabling ARC service for team sites is only supported on the Portal.

1. Tap **Site**, and tap the site to enter its site details page.
2. Tap **ARC Service**.
3. Tap to show the ARC list. You can check the ARC's information.

4. Choose and tap an ARC, and tap **Authorize**. Devices on this site available for the ARC service will show.
5. Enable the ARC service for a specific device. After the ARC confirms, events detected by the device and device exceptions will be sent to the ARC.
   a. Tap a device.
   b. Turn on the ARC Service button.
   c. To help the ARC identify the device, set the account number.
   d. Tap **Next**.
   e. Set the types of notifications (events) that can be received by the ARC.
   f. Tap **OK**.
   g. Waiting for required confirmation and authorization if needed.

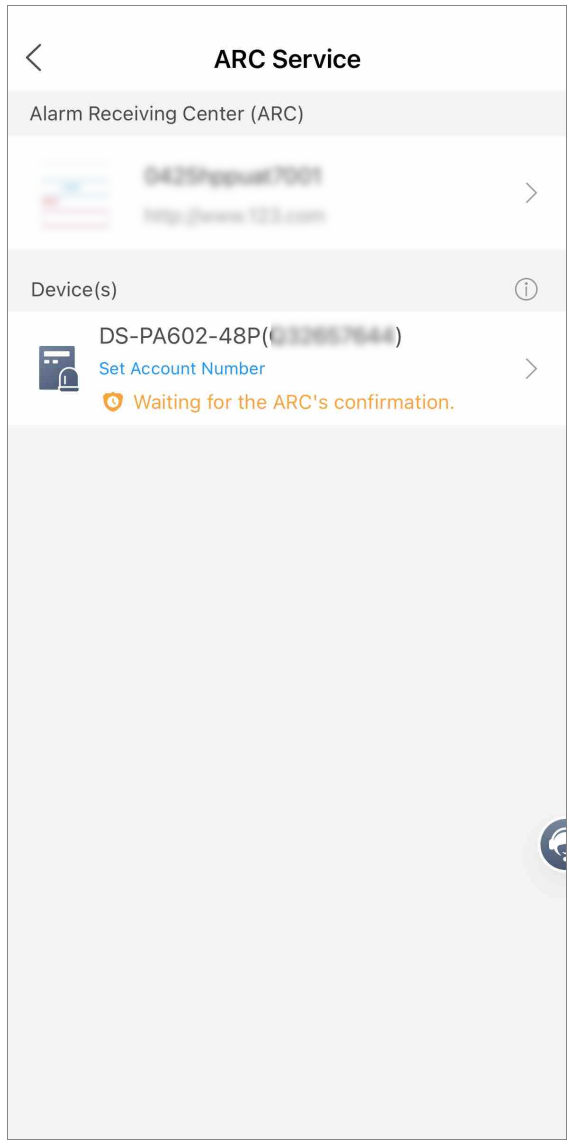


Figure 5-32 Enable ARC Service for Devices Using the Mobile Client

5.13.7 Step 3: ARC Service Provider Accepts Devices Entrusted by Installers

When installers entrust devices to ARC users, ARC users can now receive notifications via Hik-Partner Pro, and choose to accept or reject them.

Note

In some regions/countries, this Step is not supported and is skipped. The ARC service is enabled for the devices after Step 2.

Accept Devices Using the Portal

1. On the top right of the Portal, click , and then **ARC Message**.
2. Click **Accept**.

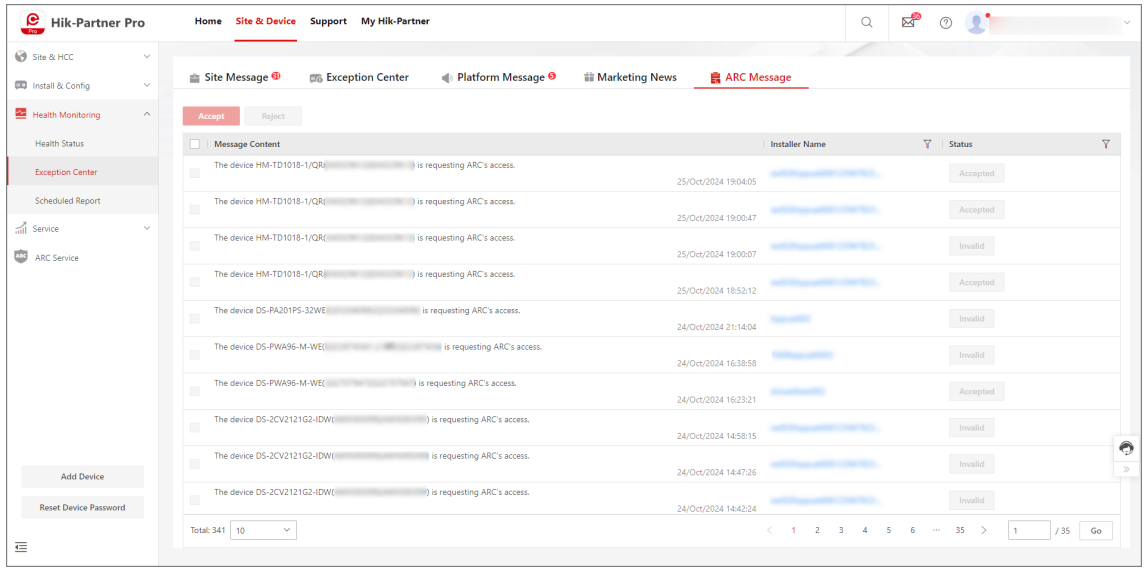
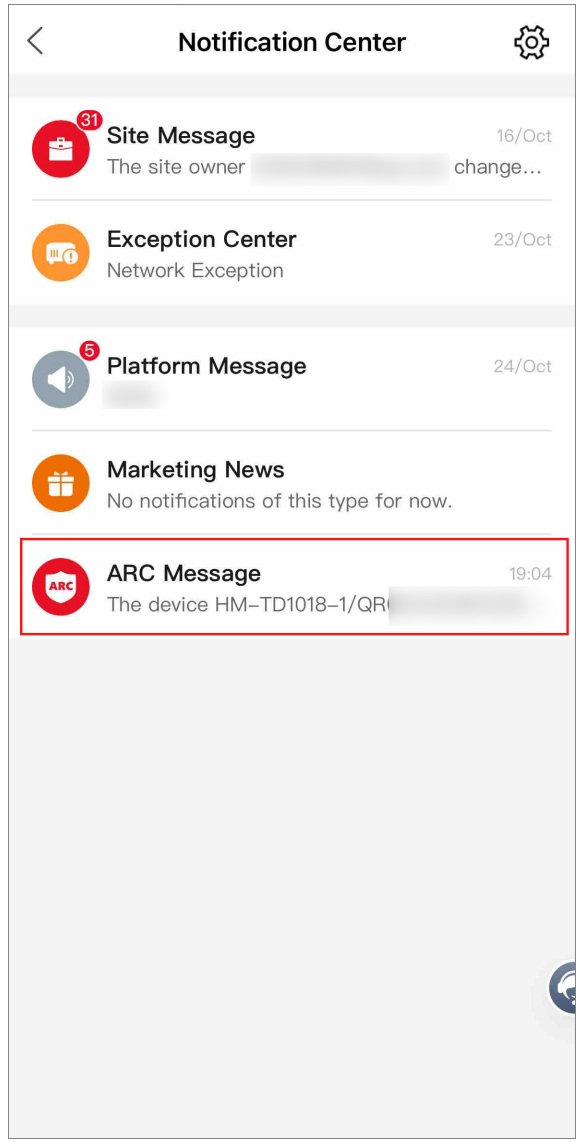


Figure 5-33 ARC Message on the Portal

Accept Devices Using the Mobile Client

1. On the top right of the Mobile Client, tap , and then **ARC Message**.
2. Tap **Accept**.


Notification Center
31
Site Message
16/Oct
The site owner change...
Exception Center
23/Oct
Network Exception
5
Platform Message
24/Oct
Marketing News
No notifications of this type for now.
ARC Message
19:04
The device HM-TD1018-1/QR

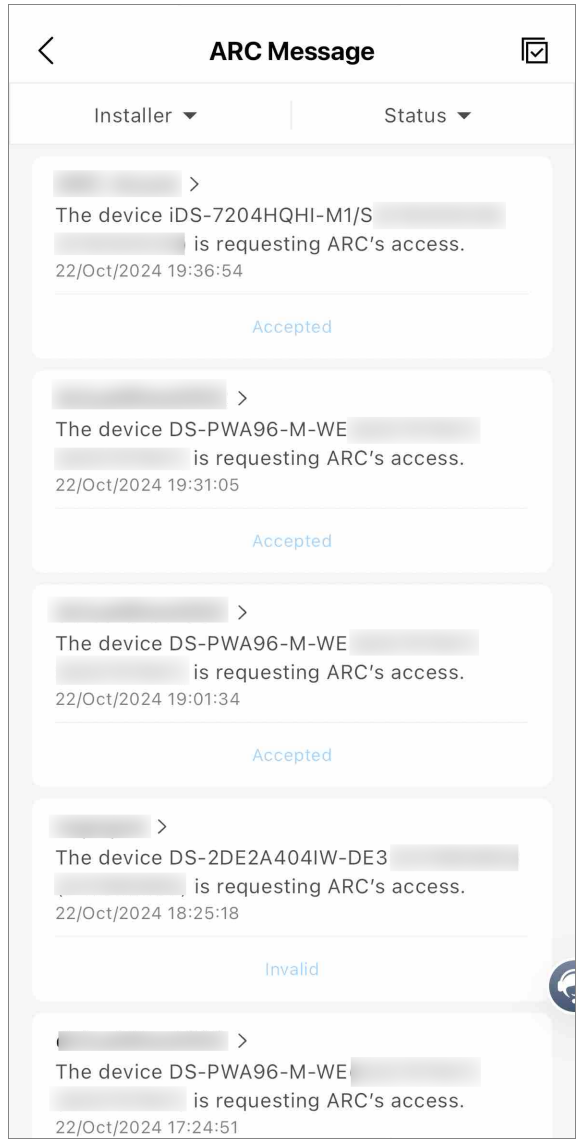


Figure 5-34 ARC Message on the Mobile Client

5.13.8 Step 4: ARC Manages Entrusted Devices

ARC users can log in to Hik-Partner Pro to manage devices with ARC service enabled.

Note

In some countries/regions, this feature is not supported.

On the ARC Service page, devices are listed, and ARC users can suspend/resume selected devices to stop/restart providing ARC services, modify the types of events they can receive, and modify the account numbers of devices.

Manage Entrusted Devices Using the Portal

Go to **Site & Device → ARC Service** .

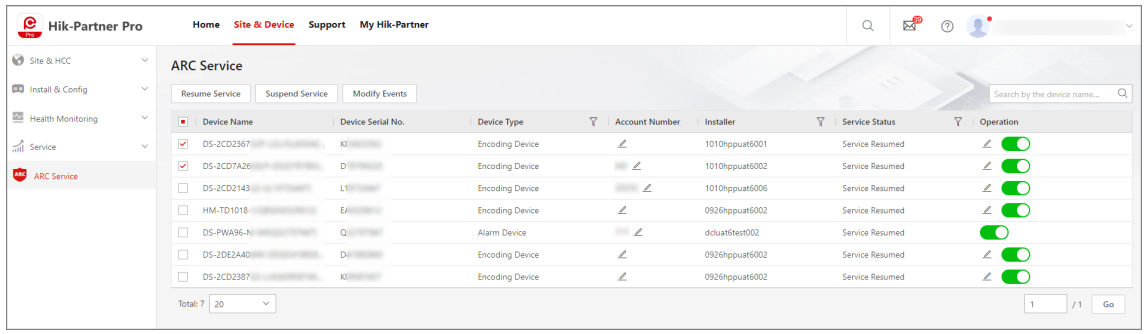
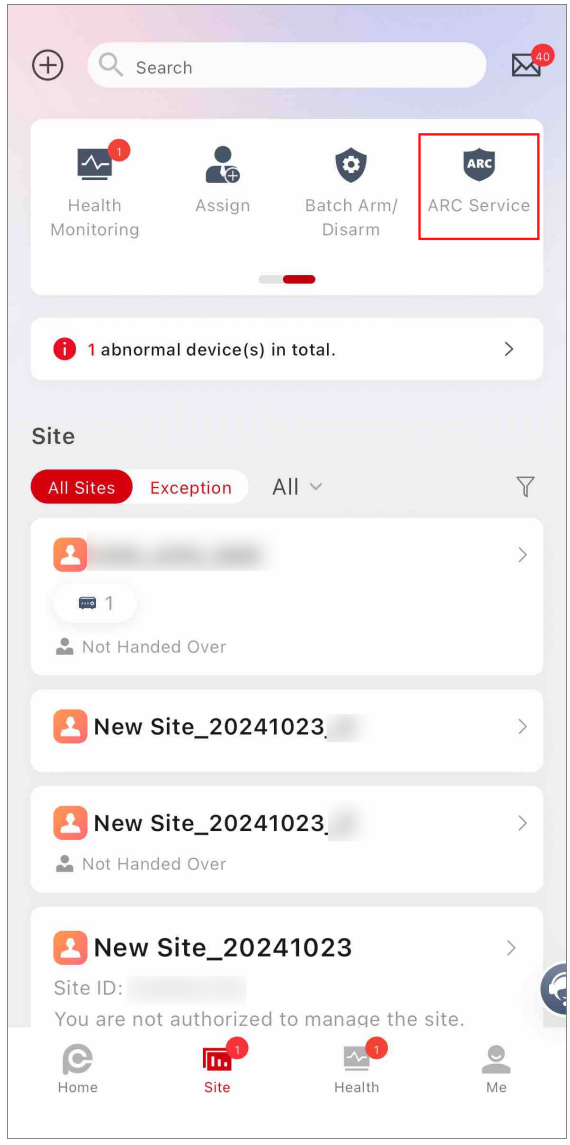


Figure 5-35 ARC Device Management on the Portal

Intention	Steps
Modify Types of Events Received (of Encoding Devices)	Select devices and click **Modify Events** to batch modify, or click in the Operation column to modify. Notifications will be sent to customers or installers for approval.
Modify Account Number for Device for Easier Management	Click in the Account Number column.
Stop/Restart Providing ARC Services for Selected Devices	Select devices and click **Suspend Service** or **Resume Service**, or switch off/on the button in the Operation column.

Manage Entrusted Devices Using the Mobile Client

Tap **Site**, and then **ARC Service**.


Search
40
Health Monitoring
Assign
Batch Arm/ Disarm
ARC Service
1 abnormal device(s) in total.
Site
All Sites
Exception
All
1
Not Handed Over
New Site_20241023
New Site_20241023
Not Handed Over
New Site_20241023
Site ID:
You are not authorized to manage the site.
Home
Site
Health
Me

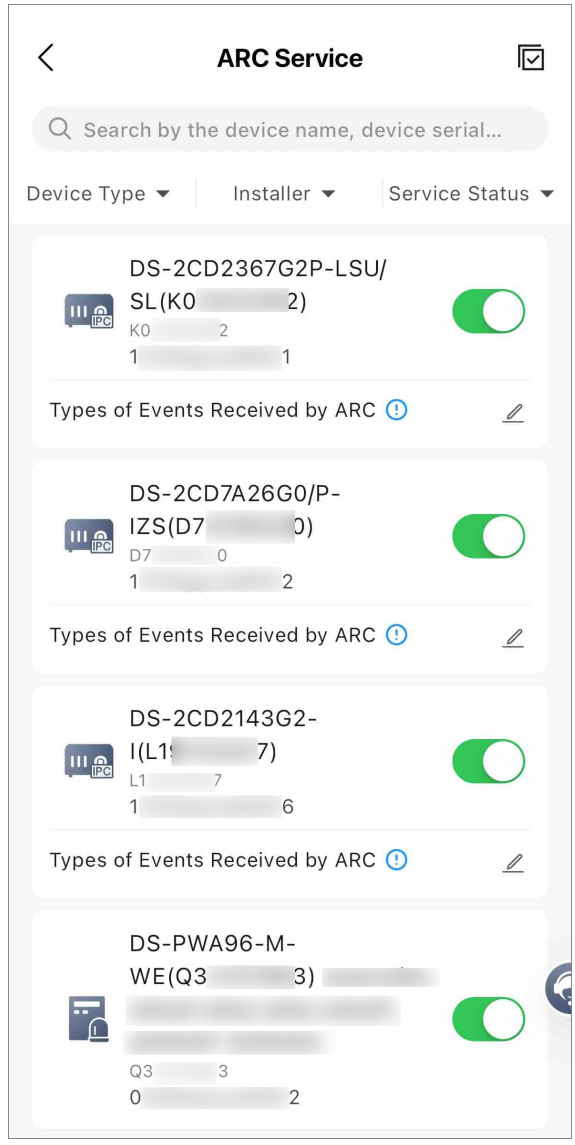


Figure 5-36 ARC Device Management on the Mobile Client

Intention	Steps
Modify Types of Events Received (of Encoding Devices)	Tap , select devices, and tap **Modify Events** to batch modify, or tap on the device card to modify.

Intention	Steps
	Notifications will be sent to customers or installers for approval.
Modify Account Number for Device for Easier Management	Tap a device card, and tap **Account Number** to modify.
Stop/Restart Providing ARC Services for Selected Devices	Tap , select devices, and tap **Suspend Service** or **Resume Service**, or switch off/on the button on the device card.

5.13.9 Step 5: ARC Establishes Communications Between ARC Software and Devices Using IP Receiver Pro

1. Install and activate the IPRP (the medium for transmitting alarms and related videos from the device to the ARC). Refer to ***the user manual of IPRP*** .
2. Configure supported protocols for transmitting events from devices to the ARC on the IPRP. Refer to ***the user manual of IPRP*** .
3. If you have enabled the ARC service for a security control panel in the previous steps and the ARC accesses the device via IP Receiver Pro, click/tap the device to open the configuration pane, and then set the way to connect the device to IP Receiver Pro (the medium for transmitting alarms and related videos from the device to the ARC).

Note

If the device is armed, disarm it first.

Ways to Connect to IP Receiver Pro

Connect Directly or by Hik-Partner Pro Server

Direct connection will be used in priority. When direct connection is abnormal, the device will be connected to IP Receiver Pro by Hik-Partner Pro server. If direct connection is restored, it will auto switch back to direct connection.

This mechanism ensures the stability of data transmission from the device to the ARC.

Connect by Hik-Partner Pro Server

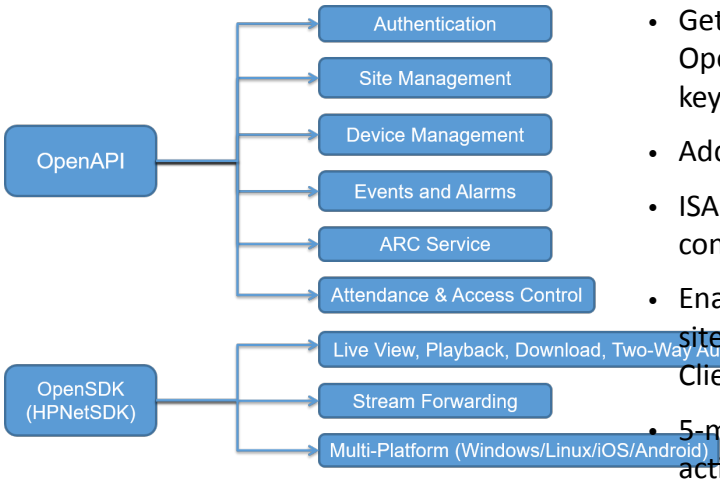
The device will be connected to IP Receiver Pro byHik-Partner Pro server constantly.

The stability of data transmission is lower compared with **Connect Directly or by Hik-Partner Pro Server**

5.14 How to Integrate with Hik-Partner Pro?

Integration guide for alarm receiving centers (ARC), third-party VSaaS vendors, and cloud-based time-attendance vendors.

Step 1: Check the Capabilities for Integration



- Get the access token (call credential of OpenAPIs) using the developer account (API key and API secret).
- Add a site before adding the device.
- ISAPI transparent transmission and allowlist control.
- Enable the ARC service for the device on the site using the Hik-Partner Pro Portal or Mobile Client.
- 5-minute free streaming. Purchase and activate by channels for unlimited streaming.

Step 2: Get a Developer Account

The developer account (API key) and password (API secret) are used for getting the access token (call credential of OpenAPIs).

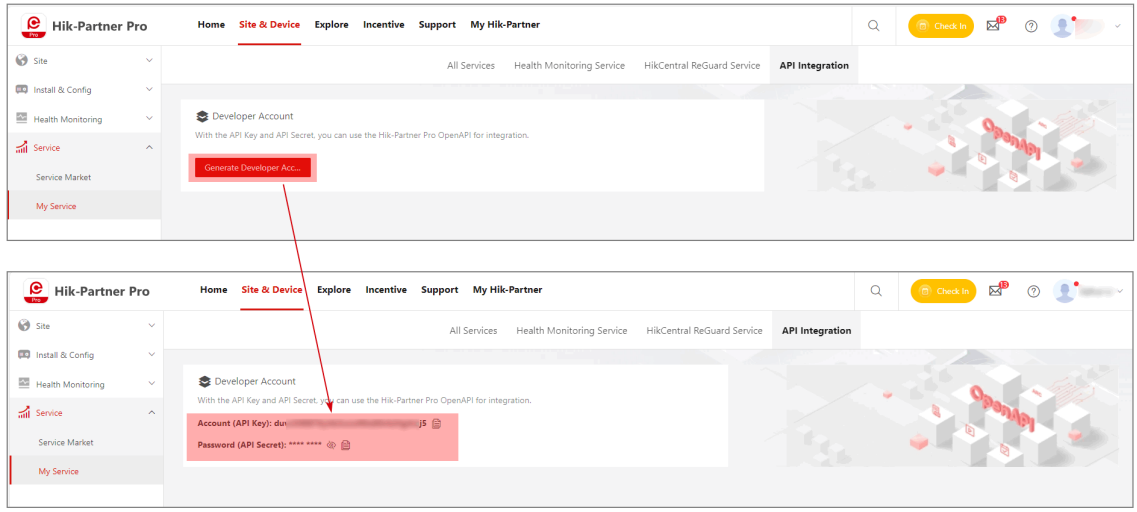
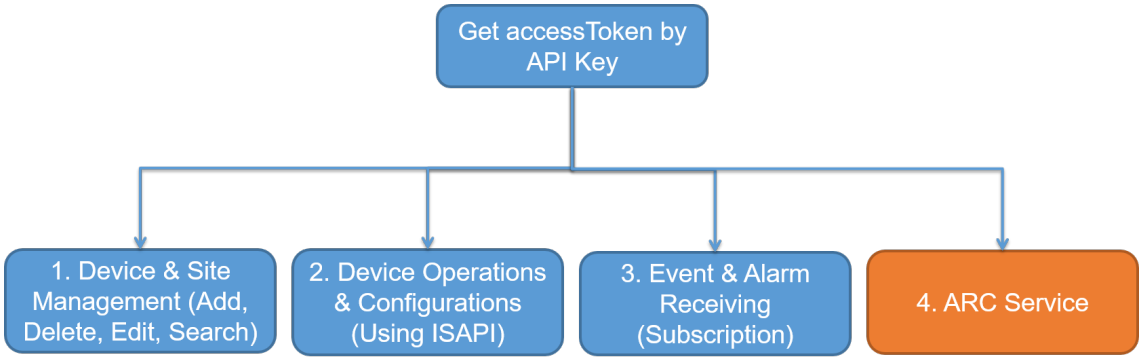


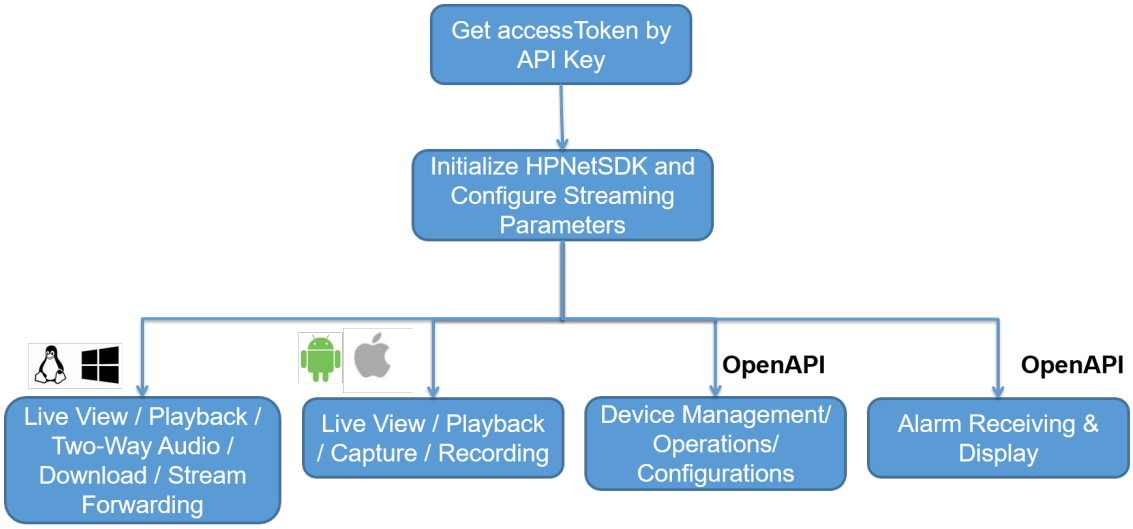
Figure 5-37 Generate a Developer Account

Step 3: (Optional) ARC Integration Process



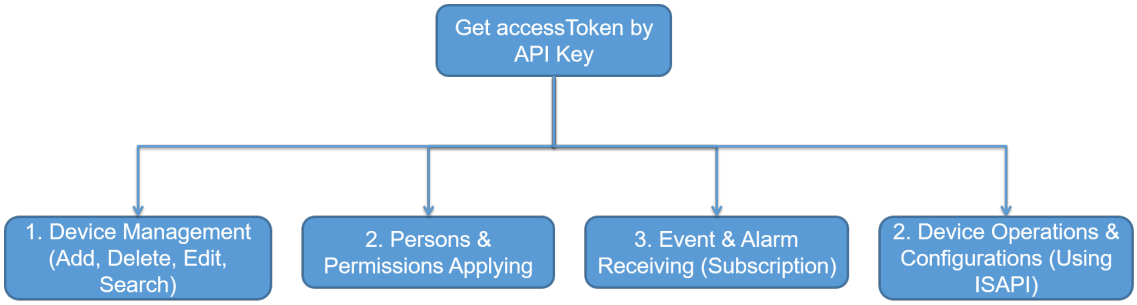
- Link the API key to the devices.on sites of Hik-Partner Pro companies.
- Perform operations & configurations for devices that you are authorized by other Hik-Partner Procompanies to manage.
- Subscribe to the events and alarms of devices owned or managed by your company.
- Access the devices that you are authorized by other companies to manage.

Step 3: (Optional) VSaaS Integration Process



- Use HPNetSDK for Windows/Linux.
- Use HPNetSDK for Android & iOS.
- Call OpenAPIs or get from the third-party server.
- The third-party server forwards alarms and by calling OpenAPIs receives alarms.

Step 3 (Optional) Attendance Integration Process



- By calling OpenAPIs, create sites first and then add devices.
- Or using the Hik-Partner Pro Portal or Mobile Client to create sites and add devices, and then by calling OpenAPIs access the device list.

- Add, delete, and edit persons.
- Apply access levels.

- Supported types of events and alarms are controlled by the allowlist.

- Supported ISAPI protocols are controlled by the allowlist.

Related Documents

- ***Hik-Partner Pro OpenAPI Developer Guide***
- Hik-Partner Pro Network SDK (Windows)
- Hik-Partner Pro Network SDK (Linux)
- Hik-Partner Pro Network SDK (iOS)
- Hik-Partner Pro Network SDK (Android)

Chapter 6 Provide Value-Added Services: Expand Your Business

Hik-Partner Pro provides various value-added services to help partners to expand their businesses and meet the demands of all types of customers.

Value-Added Service	Customer Type
Health Monitoring Service: Better Maintenance for Your Customers	Individual users: Households, independent stores. etc.
Remote Maintenance Pro Service: Better Maintenance for Your Customers **Note** Available in only the United Kingdom and Ireland.	
Cloud Storage Service: Secure & Expand Your Customers' Storage	
SIM Data Service: Connect Devices to 4G Network	
Hik-Connect for Teams Services: Provide VSaaS Solution for Enterprise Customers	Enterprise users: Chain stores, offices, communities, etc.
HikCentral ReGuard Service: Security Management Solution for Customers	Remote monitoring center.

6.1 Health Monitoring Service: Better Maintenance for Your Customers

Note

For the United Kingdom and Ireland, the health monitoring service is replaced by ***Remote Maintenance Pro Service: Better Maintenance for Your Customers*** .

Pain Points and What Customers Want From Installers

Pain Points of Customers & Installers	What Customers Want from Installers
Customers: • Do not know if the devices need any maintenance. • Do not know if any exceptions occur. • Lack of professional device maintenance. **Installers:** • On-site visit is time consuming, laborious, and with high travel & operational costs. • Cannot spot device exceptions promptly.	• They want the installers to spot device exceptions as quickly as possible. • They want the installers to handle the exceptions as quickly as possible, anytime and anywhere.

What You Can Sell & Offer to Your Customers

Hik-Partner Pro offers a free package containing a suite of features such as device online/offline status. In some cases, these free features are insufficient for you to satisfy higher level needs of your customers. Compared with the free package, the health monitoring package offers much more as follows.

Table 6-1 Free Package VS Health Monitoring Package

Functionality	Free Package	Health Monitoring Package
Site and Customer Management	Supported	Supported
Site Map	Supported	Supported
Add Devices to Hik-Partner Pro	Supported Capacity: 1024 Devices	Supported **Capacity: Unlimited Devices**
On-Site Config	Supported	Supported
On-Site Batch Upgrade	Supported	Supported
Device Status	Supported	Supported
Batch Arm and Disarm Alarm Devices	Supported	Supported
Employee Account	Supported Unlimited Number of Employee Accounts	Supported Unlimited Number of Employee Accounts

Functionality	Free Package	Health Monitoring Package
	Employee accounts with permission to manage devices shall be purchased additionally.	Employee accounts with permission to manage devices shall be purchased additionally.
Maintenance Quotation	Supported Capacity: 3 Maintenance Quotations	Supported **Capacity: Unlimited Maintenance Quotations**
Remote Configuration	Supported	Supported
Remote Live View, Playback, and Video Download	Supported	Supported
Remote Device Upgrade	Supported	Supported
Remote Batch Upgrade	Supported	Supported
Real-Time Health Monitoring	NOT Supported	**Supported**
Device Exception Notification	NOT Supported	**Supported**
Exception Handling	NOT Supported	**Supported**
Scheduled Health Check Reports	NOT Supported	**Supported**
Linkage Rule	NOT Supported	**Supported**

6.1.1 Step 1: Get Health Monitoring Packages

You can purchase the health monitoring packages online in the Service Market in Hik-Partner Pro, or purchase a service key from the local distributor first and then activate by the service key to get the purchased service packages.

Note

The supported purchase methods vary depending on your country/region. Contact the local distributor for details.

Purchase Online Using the Portal

1. Go to **Site & Device → Service Market** .
2. In the Health Monitoring Package area, click **Online Purchase** to enter the Purchase Health Monitoring Package page.
3. Select the package based on the number of devices requiring proactive health monitoring, and click **Purchase**.

Premium Package

Health monitoring up to 50 devices.

Professional Package

Health monitoring up to 200 devices.

Expert Package

Health monitoring up to 500 devices.

Custom

If you need health monitoring for more devices, click **Contact Us**, and contact our sales representatives to customize the package.

4. Select the effective duration.
5. Enter the distributor invitation code and the code from Hikvision sales.

Note

By entering the codes when you purchase services online, you may get some discounts and the distributor/reseller can earn some rebates. For details, refer to ***How to Earn Commissions as a Distributor/Reseller*** .

6. Enter your VAT number. The VAT number will be displayed in the payment receipt.
7. Select **Credit/Debit Cards** as the payment method.
8. Click **Checkout** to enter the payment page and finish the payment.

Purchase Online Using the Mobile Client

1. Go to **Me → Service Market** .
2. In the Health Monitoring Service area, tap **Buy Now**.
3. Select the package based on the number of devices requiring proactive health monitoring, and tap **Purchase**.

Premium Package

Health monitoring up to 50 devices.

Professional Package

Health monitoring up to 200 devices.

Expert Package

Health monitoring up to 500 devices.

Custom

If you need health monitoring for more devices, click **Contact Us**, and contact our sales representatives to customize the package.

4. Select the effective duration.
5. Enter the distributor invitation code and the code from Hikvision sales.

Note

By entering the codes when you purchase services online, you may get some discounts and the distributor/reseller can earn some rebates. For details, refer to ***How to Earn Commissions as a Distributor/Reseller*** .

6. Tap **Payment Agreement** at the bottom to read the agreement and check **Before paying, please agree to Payment Agreement** if you agree with the terms.
7. Tap **Checkout** to enter the payment page and finish the payment.

Get Packages by Service Key Using the Portal

1. Contact your local distributor and purchase a service key from them.
2. Go to **Site & Device → Service Market** .
3. In the Health Monitoring Package area, click **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Click **OK**.

Get Packages by Service Key Using the Mobile Client

1. Contact your local distributor and purchase a service key from them.
2. Go to **Me → Service Market** .
3. In the Health Monitoring Service area, tap **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Tap **OK**.

6.1.2 Step 2: Activate Health Monitoring Service for Customers' Devices

After you get the health monitoring package, you can activate the health monitoring service for any types of devices, as long as the number of devices is within your current package's limit. Once the service is activated, features such as device health monitoring and device exception notifications will be available for these devices.

Activate the Service for Devices Using the Portal

Choose one of the following ways to activate the health monitoring service for the devices.

- Go to **Site & Device → Service → My Service → Health Monitoring Service** . Toggle on the switch in the Operation column to activate for one device, or select multiple devices and click **Batch Activate Health Monitoring Service for Devices**.
- Go to **Site & Device → Customer Site** , find the device, hover the cursor onto on the device card, and then click **Activate Service**.
- When you add devices successfully, on the adding result page, click **Activate Service**.

Note

- If the firmware version of a device is obsolete, or its device type cannot be recognized by Hik-Partner Pro, activating health monitoring service for the device is not supported.
- If the number of devices with activated health monitoring service reached the package's limit, you can click **Upgrade Service** to upgrade to a package of higher device capacity.

Activate the Service for Devices Using the Mobile Client

Choose one of the following ways to activate the health monitoring service for the devices.

- Go to **Me → My Service** , and tap **Detail** in the Health Monitoring section. Tap **Activate Service**, and select devices to activate the service.
- Tap **Site**, tap a site, tap a device, and tap **Health Monitoring Service** to activate the service for it.
- When you add devices successfully, on the adding result page, tap **Activate Service**.

Note

- If the firmware version of a device is obsolete, or its device type cannot be recognized by Hik-Partner Pro, activating health monitoring service for the device is not supported.
- If the number of devices with activated health monitoring service reached the package's limit, you can tap **Upgrade Service** to upgrade to a package of higher device capacity.

6.1.3 Step 3: Manage Health Monitoring Packages

Manage Health Monitoring Service Using the Portal

Go to **Site & Device → Service → My Service → Health Monitoring Service** .

Package

On this page, you can manage your premium, professional, and expert packages.

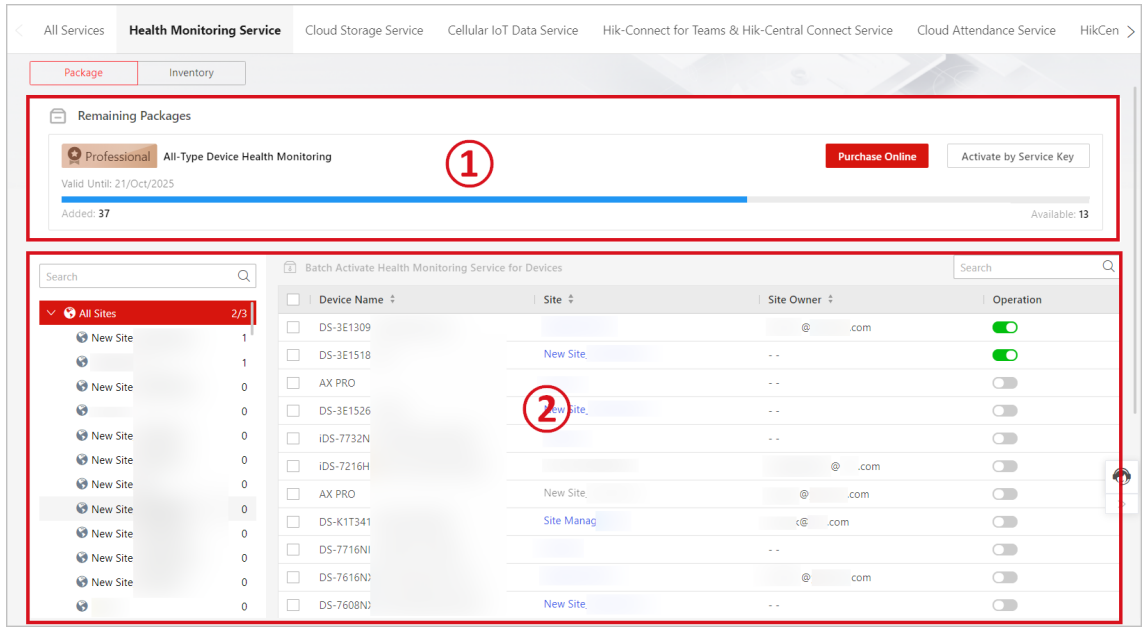


Figure 6-1 Manage Your Health Monitoring Service (Package)

Table 6-2 Available Operations

Area No.	Operation	Description
1	View Remaining Packages & Purchase More	You can check the current number of devices for which the health monitoring service is activated, and the remaining number of devices for which the service can still be activated. Click **Activate by Service Key** or **Online Purchase** to get more packages.
2	Activate Service	Toggle on the switch in the Operation column to activate the service for the device. Or select multiple devices, and then click **Batch Activate Health Monitoring Service for Devices**.

Inventory

On this page, you can manage your remaining all-type device monthly/annual packages, and network camera monthly/annual packages. If you do not have these remaining packages, this page will not be available to you.

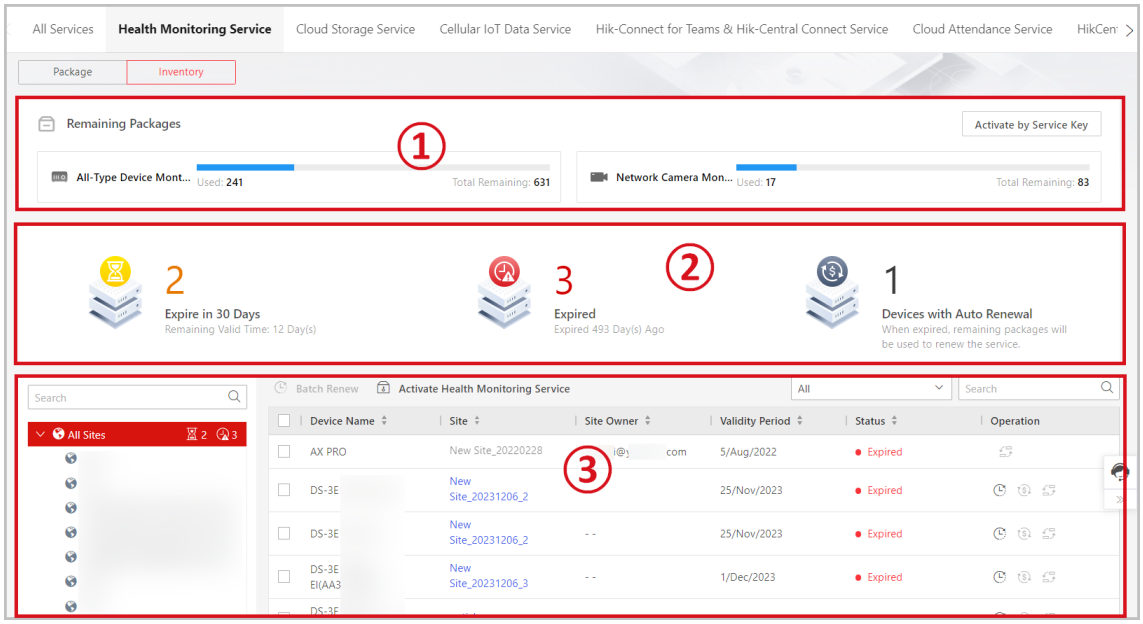


Figure 6-2 Manage Your Health Monitoring Service

Table 6-3 Available Features

Area No.	Operation	Description
1	View Remaining Packages & Purchase More	View the used number and remaining numbers of each type of heath monitoring packages. Click **Activate by Service Key** to get more all-type device monthly/annual packages, and network camera monthly/annual packages.
2	View Expiration and Auto Renewal Information	View numbers of devices whose services are expiring in 30 days, expired, and with enabled auto renewal.
3	Activate Service	Click **Activate Health Monitoring Service** to activate the service for selected devices.
3	Renew Service	Select devices and then click **Batch Renew**, or click in the Operation column.
3	Transfer Service	Click in the Operation column to transfer the remaining service time from the current device to another.
3	Enable Service Auto Renewal	Click in the Operation column, switch on **Auto Renewal**, and then select a type of service packages for auto renewing the service.

Manage Health Monitoring Service Using the Mobile Client

Tap **Me** at the bottom right, tap **My Service**, and tap **Detail** in the Health Monitoring Service section.

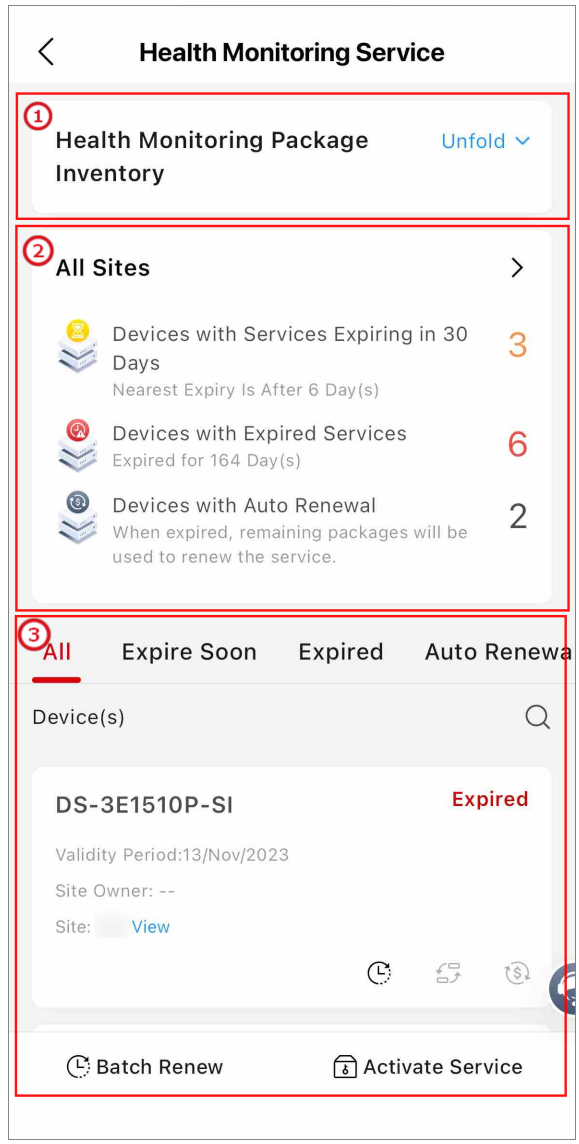


Figure 6-3 My Service: Health Monitoring Service

Table 6-4 Available Operations

Area No.	Operation	Description
1	View Remaining Packages & Purchase More	Check the usage details of your health monitoring packages.

Area No.	Operation	Description
		Tap **Activate by Service Key** or **Buy Now** to get more packages.
2	View Expiration and Auto Renewal Information	View numbers of devices whose services are expiring in 30 days, expired, and with enabled auto renewal.
3	Activate Service	Tap **Activate Service**, and select multiple devices to activate.
3	Renew Service	Tap **Batch Renew**, and select devices to renew. Or tap on the device card.
3	Transfer Service	Tap on the device card to transfer the remaining service time from the current device to another.
3	Enable Service Auto Renewal	Tap on the device card, and select a type of service packages for auto renewing the health monitoring service.

6.2 Remote Maintenance Pro Service: Better Maintenance for Your Customers

Note

The remote maintenance Pro service is available to only the United Kingdom and Ireland.

Pain Points and What Customers Want From Installers

Pain Points of Customers & Installers	What Customers Want from Installers
Customers: • Do not know if the devices need any maintenance. • Do not know if any exceptions occur. • Lack of professional device maintenance. **Installers:** • On-site visit is time consuming, laborious, and with high travel & operational costs. • Cannot spot device exceptions promptly.	• They want the installers to spot device exceptions as quickly as possible. • They want the installers to handle the exceptions as quickly as possible, anytime and anywhere.

What You Can Sell & Offer to Your Customers

Hik-Partner Pro offers a free package containing a suite of features such as device online/offline status. In some cases, these free features are insufficient for you to satisfy higher level needs of your customers. Compared with the free package, the remote maintenance Pro package offers much more as follows.

Table 6-5 Free Package VS Remote Maintenance Pro Package

Functionality	Free Package	Remote Maintenance Pro Package
Site and Customer Management	Supported	Supported
Site Map	Supported	Supported
Add Devices to Hik-Partner Pro	Supported Capacity: 1024 Devices	Supported **Capacity: Unlimited Devices**
On-Site Config	Supported	Supported
On-Site Batch Upgrade	Supported	Supported
Device Status	Supported	Supported
Batch Arm and Disarm Alarm Devices	Supported	Supported
Employee Account	Supported Unlimited Number of Employee Accounts Employee accounts with permission to manage devices shall be purchased additionally.	Supported Unlimited Number of Employee Accounts Employee accounts with permission to manage devices shall be purchased additionally.
Maintenance Quotation	Supported Capacity: 3 Maintenance Quotations	Supported **Capacity: Unlimited Maintenance Quotations**
Remote Configuration	NOT Supported	**Supported**
Remote Live View, Playback, and Video Download	NOT Supported	**Supported**
Remote Device Upgrade	NOT Supported	**Supported**
Remote Batch Upgrade	NOT Supported	**Supported**
Real-Time Health Monitoring	NOT Supported	**Supported**

Functionality	Free Package	Remote Maintenance Pro Package
Device Exception Notification	NOT Supported	**Supported**
Exception Handling	NOT Supported	**Supported**
Scheduled Health Check Reports	NOT Supported	**Supported**
Linkage Rule	NOT Supported	**Supported**

6.2.1 Step 1: Get Remote Maintenance Pro Packages

You can purchase the remote maintenance Pro packages online in the Service Market in Hik-Partner Pro, or purchase a service key from the local distributor first and then activate by the service key to get the purchased service packages.

Note

The supported purchase methods vary depending on your country/region. Contact the local distributor for details.

Purchase Online Using the Portal

1. Go to **Site & Device → Service Market** .
2. In the Remote Maintenance Pro Service area, click **Online Purchase** to enter the Purchase Remote Maintenance Pro Package page.
3. Select service packages and set the number of service packages that you want to purchase.

   Back-End Recorder Monthly Package

   One package for one device of nearly any type. And the activated service lasts one month.

   Applicable to DVRs, NVRs, network cameras, PTZ cameras, access control devices, alarm devices, video intercom devices, doorbells, Hik-ProConnect boxes, thermal devices, and network switches.

   Back-End Recorder Annual Package

   One package for one device of nearly any type. And the activated service lasts one year.

   Applicable to DVRs, NVRs, network cameras, PTZ cameras, access control devices, alarm devices, video intercom devices, doorbells, Hik-ProConnect boxes, thermal devices, and network switches.

   Back-End Recorder Annual Package * 20

   20 back-end recorder annual packages sold as a batch. Set the number of batches to purchase.

   Back-End Recorder Annual Package * 100

100 back-end recorder annual package sold as a batch. Set the number of batches to purchase.

Camera Monthly Package

One package for one camera. And the activated service lasts one month.

Camera Annual Package

One package for one camera. And the activated service lasts one year.

Camera Annal Package * 20

20 camera annual packages sold as a batch. Set the number of batches to purchase.

Camera Annual Package * 100

100 camera annual packages sold as a batch. Set the number of batches to purchase.

4. Enter the distributor invitation code and the code from Hikvision sales.

Note

By entering the codes when you purchase services online, you may get some discounts and the distributor/reseller can earn some rebates. For details, refer to ***How to Earn Commissions as a Distributor/Reseller*** .

5. Enter your VAT number. The VAT number will be displayed in the payment receipt.
6. Select **Credit/Debit Cards** as the payment method.
7. Click **Checkout** to enter the payment page and finish the payment.

Purchase Online Using the Mobile Client

1. Go to **Me → Service Market** .
2. In the Remote Maintenance Pro Service area, tap **Buy Now**.
3. Select service packages and set the number of service packages that you want to purchase.

Back-End Recorder Monthly Package

One package for one device of nearly any type. And the activated service lasts one month.

Applicable to DVRs, NVRs, network cameras, PTZ cameras, access control devices, alarm devices, video intercom devices, doorbells, Hik-ProConnect boxes, thermal devices, and network switches.

Back-End Recorder Annual Package

One package for one device of nearly any type. And the activated service lasts one year.

Applicable to DVRs, NVRs, network cameras, PTZ cameras, access control devices, alarm devices, video intercom devices, doorbells, Hik-ProConnect boxes, thermal devices, and network switches.

Back-End Recorder Annual Package * 20

20 back-end recorder annual packages sold as a batch. Set the number of batches to purchase.

Back-End Recorder Annual Package * 100

100 back-end recorder annual package sold as a batch. Set the number of batches to purchase.

Camera Monthly Package

One package for one camera. And the activated service lasts one month.

Camera Annual Package

One package for one camera. And the activated service lasts one year.

Camera Annal Package * 20

20 camera annual packages sold as a batch. Set the number of batches to purchase.

Camera Annual Package * 100

100 camera annual packages sold as a batch. Set the number of batches to purchase.

4. Enter the distributor invitation code and the code from Hikvision sales.

Note

By entering the codes when you purchase services online, you may get some discounts and the distributor/reseller can earn some rebates. For details, refer to ***How to Earn Commissions as a Distributor/Reseller*** .

5. Tap **Payment Agreement** at the bottom to read the agreement and check **Before paying, please agree to Payment Agreement** if you agree with the terms.
6. Tap **Checkout** to enter the payment page and finish the payment.

Get Packages by Service Key Using the Portal

1. Contact your local distributor and purchase a service key from them.
2. Go to **Site & Device → Service Market** .
3. In the Remote Maintenance Pro Service area, click **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Click **OK**.

Get Packages by Service Key Using the Mobile Client

1. Contact your local distributor and purchase a service key from them.
2. Go to **Me → Service Market** .
3. In the Remote Maintenance Pro Service area, tap **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Tap **OK**.

6.2.2 Step 2: Activate Remote Maintenance Pro Service for Customers' Devices

After you get the remote maintenance pro packages, you can activate the service for devices. Once the service is activated, features such as device health monitoring and device exception notifications will be available for these devices.

Activate the Service for Devices Using the Portal

Choose one of the following ways to activate the remote maintenance Pro service for the devices.

- Go to **Site & Device → Service → My Service → Remote Maintenance Pro Service → Activate Remote Maintenance Pro Service** . Select the devices and the activation type to activate the service.
- Go to **Site & Device → Customer Site** , find the device, hover the cursor onto on the device card, and then click **Activate Service**.
- When you add devices successfully, on the adding result page, click **Activate Service**.

Note

If the firmware version of a device is obsolete, or its device type cannot be recognized by Hik-Partner Pro, activating remote maintenance Pro service for the device is not supported.

Activate the Service for Devices Using the Mobile Client

Choose one of the following ways to activate the remote maintenance Pro service for the devices.

- Go to **Me → My Service** , and tap **Detail** in the Remote Maintenance Pro Service section. Tap **Activate Service**, and select the devices and activation type to activate the service.
- Tap **Site**, tap a site, tap a device, and tap **Remote Maintenance Pro Service** to activate the service for it.
- When you add devices successfully, on the adding result page, tap **Activate Service**.

Note

If the firmware version of a device is obsolete, or its device type cannot be recognized by Hik-Partner Pro, activating remote maintenance Pro service for the device is not supported.

6.2.3 Step 3: Manage Remote Maintenance Pro Packages

Manage Remote Maintenance Pro Service Using the Portal

Go to **Site & Device → Service → My Service → Remote Maintenance Pro Service** .

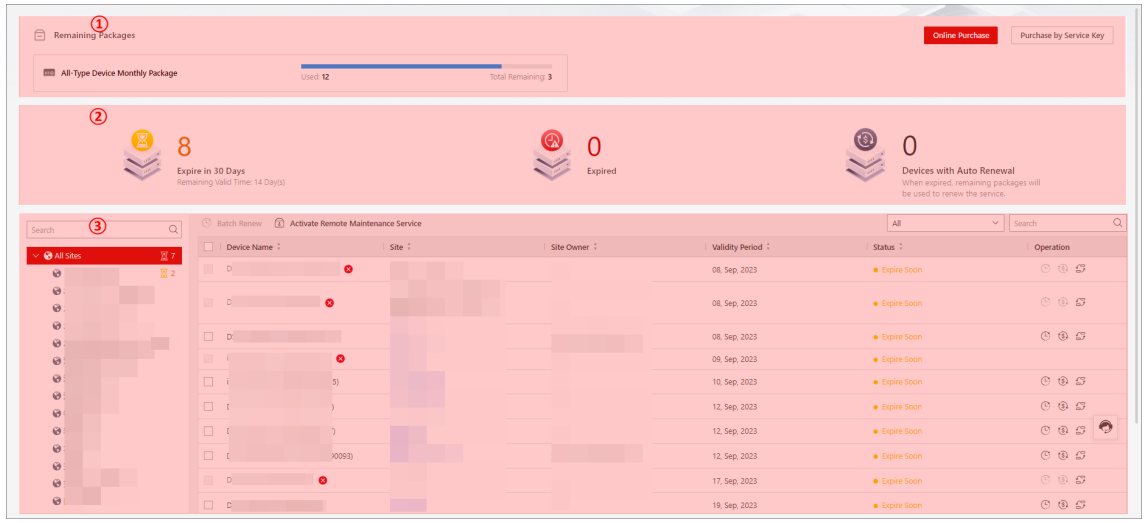


Figure 6-4 Manage Your Remote Maintenance Pro Service

Table 6-6 Available Features

Area No.	Operation	Description
1	View Remaining Packages & Purchase More	View the used number and remaining numbers of each type of remote maintenance Pro packages. Click **Activate by Service Key** or **Online Purchase** to get more packages.
2	View Expiration and Auto Renewal Information	View numbers of devices whose services are expiring in 30 days, expired, and with enabled auto renewal.
3	Activate Service	Click **Activate Remote Maintenance Pro Service** to activate the service for selected devices.
3	Renew Service	Select devices and then click **Batch Renew**, or click in the Operation column.
3	Transfer Service	Click in the Operation column to transfer the remaining service time from the current device to another.
3	Enable Service Auto Renewal	Click in the Operation column, switch on **Auto Renewal**, and then select a type of service packages for auto renewing the service.

Manage Remote Maintenance Pro Service Using the Mobile Client

Tap **Me** at the bottom right, tap **My Service**, and tap **Detail** in the Remote Maintenance Pro Service section.

Table 6-7 Available Operations

Operation	Description
View Remaining Packages & Purchase More	Check the usage details of your remote maintenance Pro packages. Tap **Activate by Service Key** or **Buy Now** to get more packages.
View Expiration and Auto Renewal Information	View numbers of devices whose services are expiring in 30 days, expired, and with enabled auto renewal.
Activate Service	Tap **Activate Service**, and select multiple devices to activate.
Renew Service	Tap **Batch Renew**, and select devices to renew. Or tap on the device card.
Transfer Service	Tap on the device card to transfer the remaining service time from the current device to another.
Enable Service Auto Renewal	Tap on the device card, and select a type of service packages for auto renewing the service.

6.3 Cloud Storage Service: Secure & Expand Your Customers' Storage

Customers' Pain Points and What They Want

Pain Points of Customers (End Users)	What They Want
• Limited storage capacity. • Data loss risk. • Complex data management. • Restricted access and sharing. • High infrastructure or hardware costs.	• Scalable and flexible storage. • Cost efficiency. • Guaranteed data security and privacy. • Real-time access.

What You Can Sell & Offer to Your Customers

Hik-Partner Pro offers a comprehensive cloud storage solution of both event-related recording and 24/7 recording.

- **Scalability and flexibility:** Cloud storage solutions can easily scale to accommodate large volumes of data, providing flexibility as data storage needs fluctuate.
- **Cost savings:** Cloud storage eliminates the need for expensive on-premises hardware and reduces maintenance costs.
- **Lower risk of data loss:** Recordings are synchronously stored on the cloud.

- **Certified security with data protection:** Only users can access their own cloud stored videos.
- **Improved usability and accessibility:** Easy downloading and retrieval of videos anytime and anywhere.

6.3.1 Device Compatibility for Cloud Storage Service

Check Device Compatibility for Cloud Storage Service Using the Portal

1. Visit the Portal and scroll down to the bottom of the Portal. Click **Device Compatibility List**.

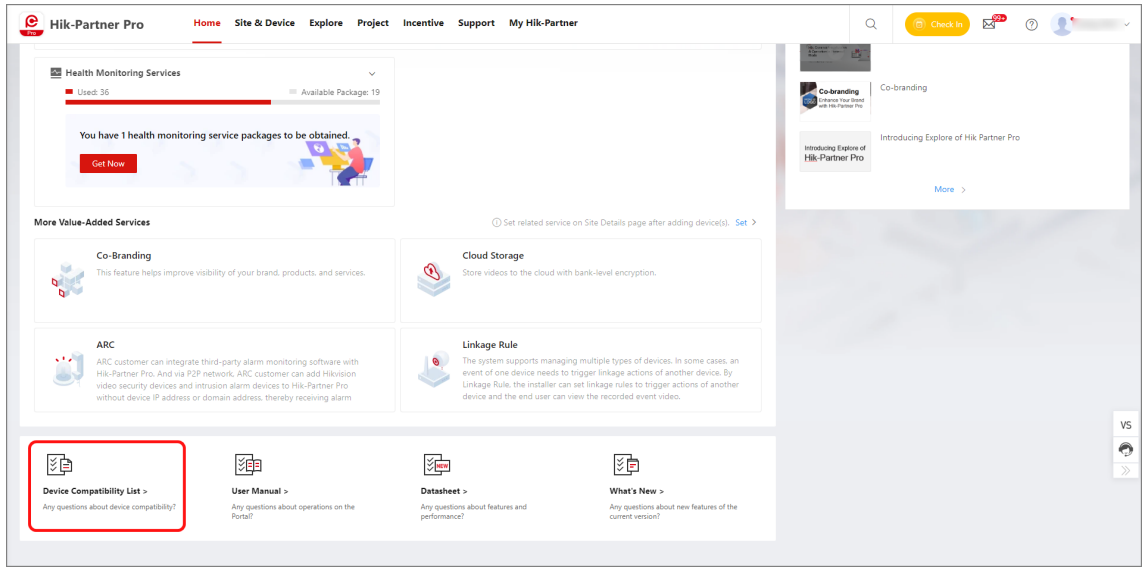


Figure 6-5 Device Compatibility List

2. Click **Cloud Storage**, and search for a NVR / DVR / network camera model to check whether it supports the cloud storage service.

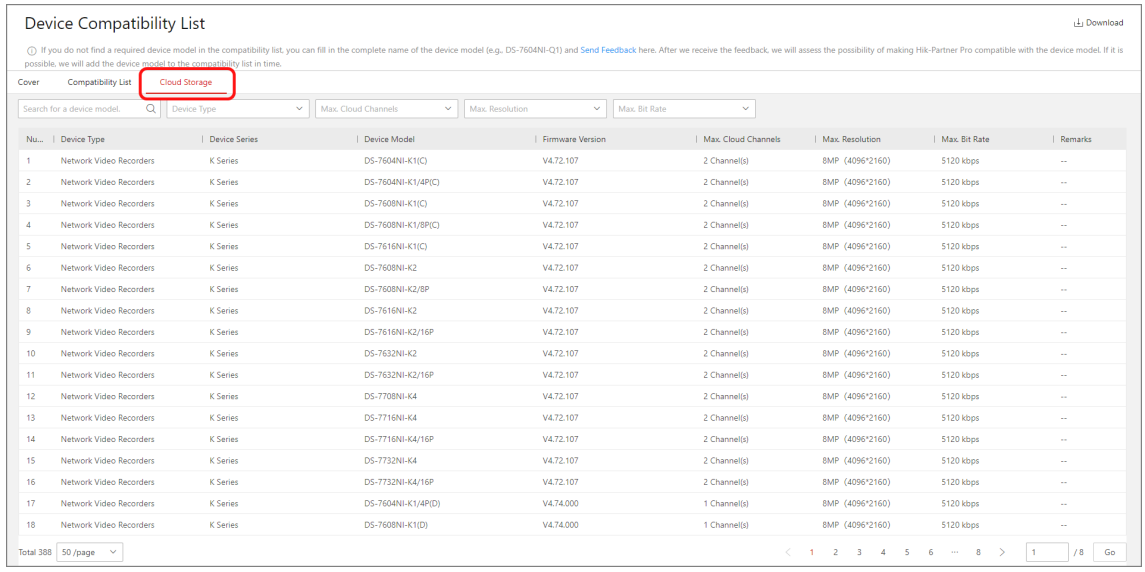


Figure 6-6 Compatibility List

Check Device Compatibility for Cloud Storage Service Using the Mobile Client

1. Log in to the Mobile Client, tap **Me → Tutorial Center** .

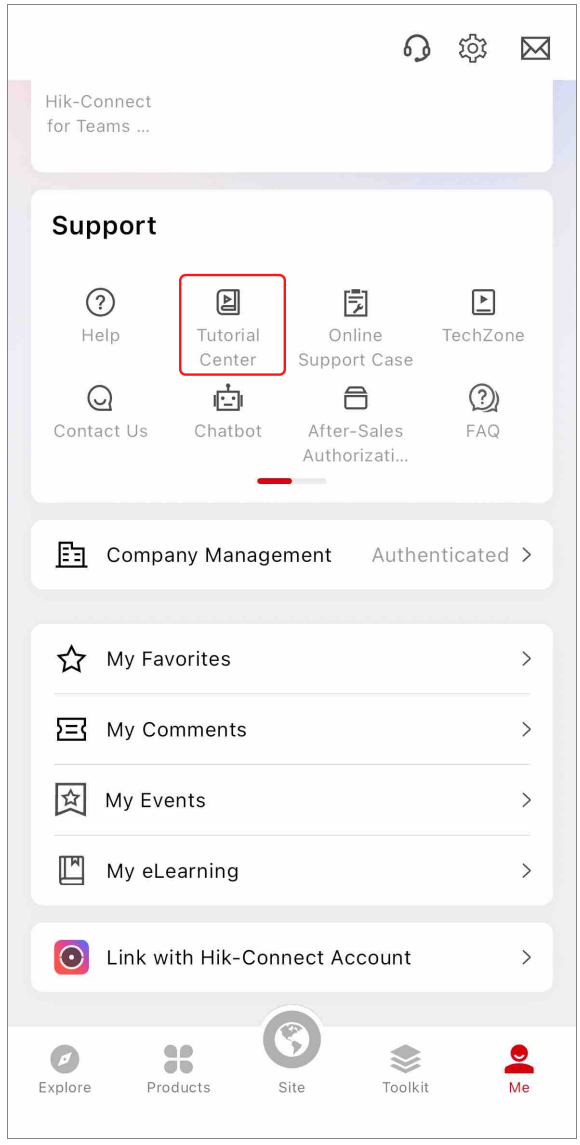


Figure 6-7 Tutorial Center

2. Tap **Technical Guidance → Hik-Partner Pro Device Compatibility List** .

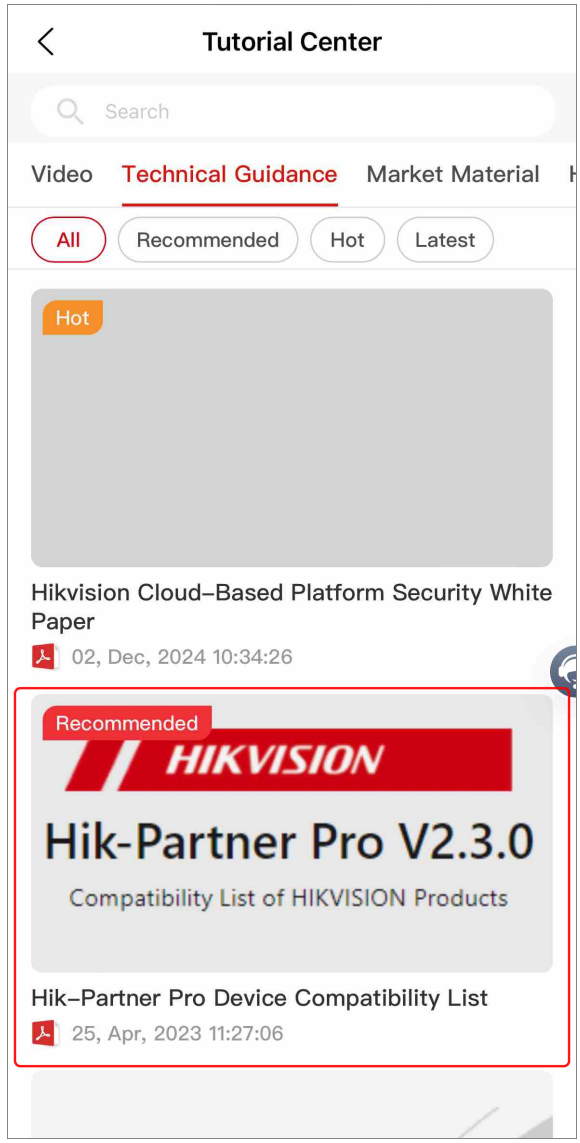


Figure 6-8 Compatibility List

3. Tap **Cloud Storage**, and search for a NVR / DVR / network camera model to check whether it supports the cloud storage service.

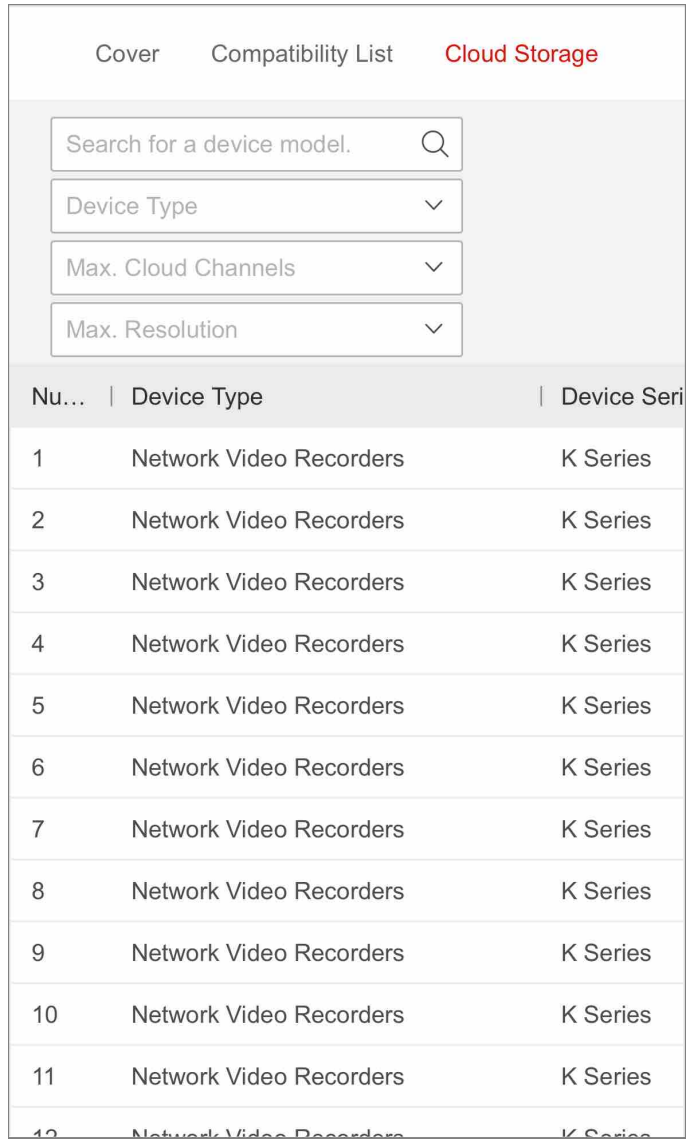


Figure 6-9 Cloud Storage Compatibility

6.3.2 Step 1: Get Cloud Storage Service Packages

You can purchase the cloud storage service packages online in the Service Market in Hik-Partner Pro, or purchase a service key from the local distributor first and then activate by the service key to get the purchased service packages.

Note

The supported purchase methods vary depending on your country/region. Contact the local distributor for details.

Purchase Online Using the Portal

1. Go to **Site & Device → Service Market** .
2. In the Cloud Storage Service area, click **Online Purchase**.
3. Set the number of packages to purchase. You can purchase one or more types of packages at a time.
   The number before "Day" (e.g. 7-Day, 30-Day, 90-Day, 180-Day, 365-Day) refers to the retention period of video footage on the cloud. **Monthly** and **Annual** refer to how long the service will last after activation.
   For example, if you select **7-Day Monthly Package**, the video footage can be saved on the cloud for 7 days, and it will be covered by new video footage from the 8th day; and the service will last for a month after activation.
4. Enter the distributor invitation code and the code from Hikvision sales.

   Note

   By entering the codes when you purchase services online, you may get some discounts and the distributor/reseller can earn some rebates. For details, refer to ***How to Earn Commissions as a Distributor/Reseller*** .
5. Enter your VAT number. The VAT number will be displayed in the payment receipt.
6. Select **Credit/Debit Cards** as the payment method.
7. Click **Checkout** to enter the payment page and finish the payment.

Get Packages by Service Key Using the Portal

1. Contact your local distributor and purchase a service key from them.
2. Go to **Site & Device → Service Market** .
3. In the Cloud Storage Service area, click **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Click **OK**.

Get Packages by Service Key Using the Mobile Client

1. Contact your local distributor and purchase a service key from them.
2. Go to **Me → Service Market** .
3. In the Cloud Storage Service area, tap **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Tap **OK**.

6.3.3 (Optional) Step 2: Perform Uplink Bandwidth Test

Before you set cloud storage for devices, it is recommended that you perform the uplink bandwidth test first, so you can refer to the test result to decide the quantity of cloud storage channels to set and their definitions.

Perform Uplink Bandwidth Test Using the Portal

1. Add a Hik-ProConnect box or an NVR/DVR/camera with the cloud storage capability to a site.

   Note

   Refer to ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** . Do not add the device by IP / domain name, or its cloud storage functionality will be unavailable.
2. Go to **Site & Device → Customer Site** .
3. Find the device and click it to enter its details page.
4. Click **Uplink Bandwidth Test**.
5. Click **Start**. When it completes, the recommended quantity and resolution are shown on the test page.

Perform Uplink Bandwidth Test Using the Mobile Client

1. Add a Hik-ProConnect box or an NVR/DVR/camera with the cloud storage capability to a site.

   Note

   Refer to ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** . Do not add the device by IP / domain name, or its cloud storage functionality will be unavailable.
2. Tap **Site** .
3. Find the device and tap it to enter its details page.
4. Tap **Cloud Storage → Uplink Bandwidth Test** .
5. Tap **Start Testing**. When it completes, the recommended quantity and resolution are shown on the test page.

6.3.4 Step 3: Configure Cloud Storage and Activate Service for Devices

Hik-Partner Pro provides a seamless configuration process that contains enabling cloud storage, service activation, and event settings.

Scenario	Instruction
If your NVRs/DVRs/cameras have cloud storage capabilities themselves, you can directly set cloud storage for them.	**For NVRs/DVRs:** • ***Set Cloud Storage Service for NVRs/DVRs Using the Portal*** • ***Set Cloud Storage Service for NVRs/DVRs Using the Mobile Client*** **For Cameras:**

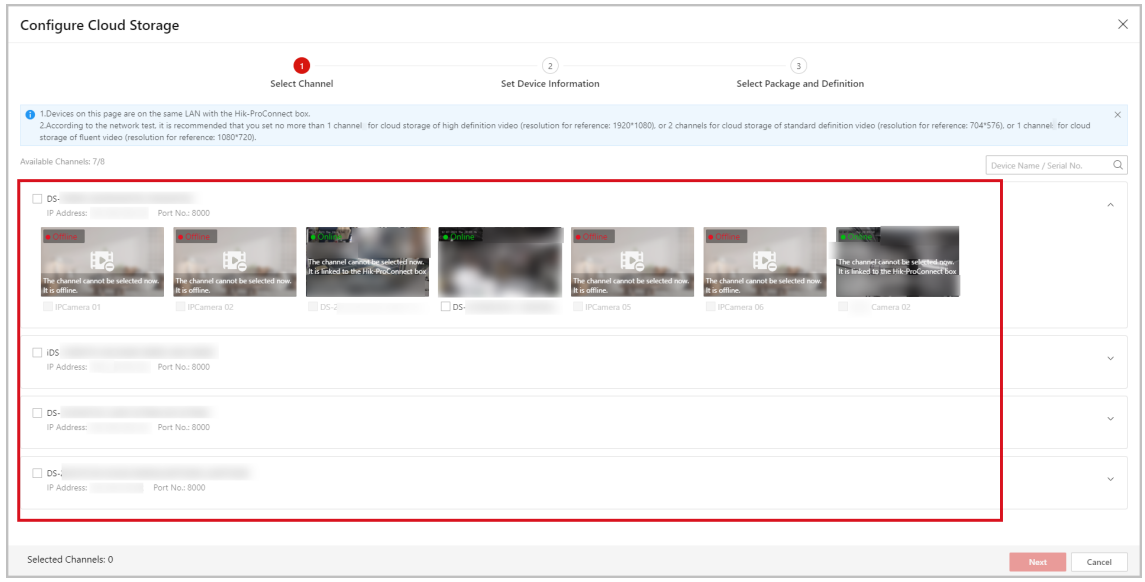
Scenario	Instruction
	• ***Set Cloud Storage Service for Cameras Using the Portal*** • ***Set Cloud Storage Service for Cameras Using the Mobile Client***
If your NVRs/DVRs/cameras do not have cloud storage capabilities themselves, you should use a Hik-ProConnect box to help the NVRs/DVRs/ cameras to upload videos to the cloud.	• ***Set Cloud Storage Service for Hik-ProConnect Boxes Using the Portal*** • ***Set Cloud Storage Service for Hik-ProConnect Boxes Using the Mobile Client***

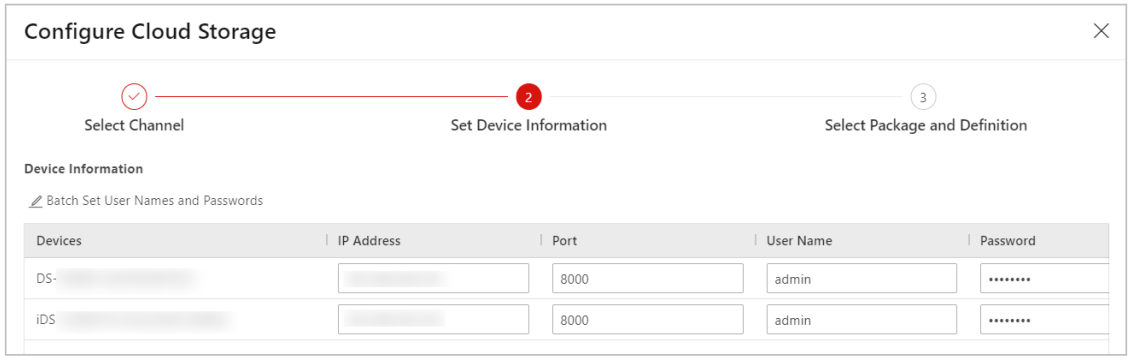
Set Cloud Storage Service for Hik-ProConnect Boxes Using the Portal

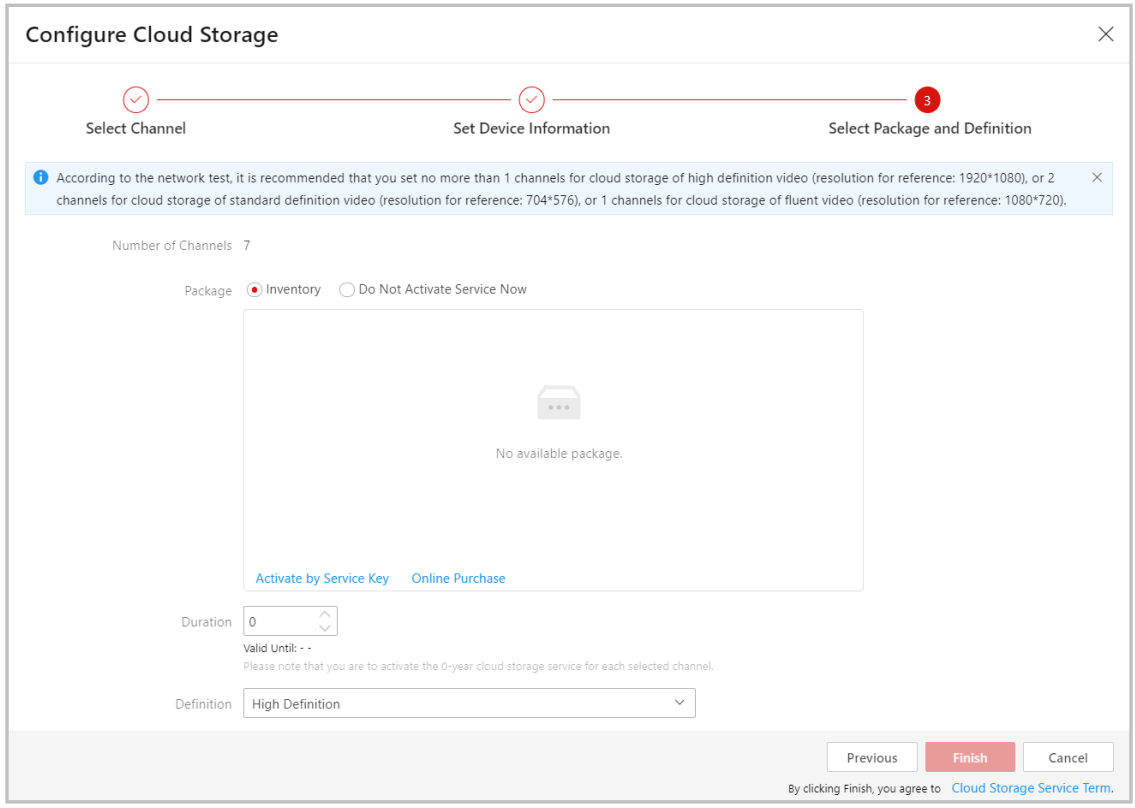
1. Add a Hik-ProConnect box and the NVRs/DVRs/cameras to the same site (also need to be on the same LAN).

   Note

   Refer to ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** . Do not add the device by IP / domain name, or its cloud storage functionality will be unavailable.
2. Enter the Configure Cloud Storage page by one of the following ways.
   - On the adding result page, click **Cloud Storage Settings**.
   - Go to **Site & Device → Customer Site** , find the Hik-ProConnect box, and click on the device card.
   - Go to **Site & Device → Customer Site** , click the Hik-ProConnect box to enter its details page, and click **Configure Cloud Storage**.
   - Go to **Site & Device → Customer Site** , click the site, and go to **Cloud Storage → Configure Cloud Storage /** .
3. Set required information: Select channels to be configured, set device information (user name, password, IP address, port No.), select cloud storage package for service activation, and select definitions.


Configure Cloud Storage
Select Channel
Set Device Information
Select Package and Definition
Available Channels: 7/8
Selected Channels: 0
Next
Cancel


Configure Cloud Storage
Select Channel
Set Device Information
Select Package and Definition
Device Information
Batch Set User Names and Passwords
Devices
IP Address
Port
User Name
Password
8000
admin
8000
admin



4. Wait for the configuration to complete. You can click **Run in Background** to hide the page. Settings completed automatically in the background include:
   - Linking the selected channels to the Hik-ProConnect box.
   - Enabling SVC.
   - Enabling the device's cloud storage capability.
   - Setting motion detection events and enabling **Notify Surveillance Center**.
   - Activating the cloud storage service.
5. On the result page, click **Event Settings** to continue to set events.

Set Cloud Storage Service for Hik-ProConnect Boxes Using the Mobile Client

1. Add a Hik-ProConnect box and the NVRs/DVRs/cameras to the same site (also need to be on the same LAN).

   Note

   Refer to ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** . Do not add the device by IP / domain name, or its cloud storage functionality will be unavailable.
2. Enter the Configure Cloud Storage page by one of the following ways.
   - On the adding result page, tap **Cloud Storage Settings**.
   - Tap **Site**, select the site, find the Hik-ProConnect box, and tap on the device card.

- Tap **Site**, select the site, tap the Hik-ProConnect box to enter its details page, and tap **Cloud Storage → Cloud Storage Settings** .
- Tap **Site**, select the site, and go to **Cloud Storage → Configure Cloud Storage /** .

3. Set required information: Select channels to be configured, set device information (user name, password, IP address, port No.), select cloud storage package for service activation, and select definitions.
4. Wait for the configuration to complete. You can tap **Run in Background** to hide the page. Settings completed automatically in the background include:
   - Linking the selected channels to the Hik-ProConnect box.
   - Enabling SVC.
   - Enabling the device's cloud storage capability.
   - Setting motion detection events and enabling **Notify Surveillance Center**.
   - Activating the cloud storage service.
5. On the result page, tap **Event Settings** to continue to set events.

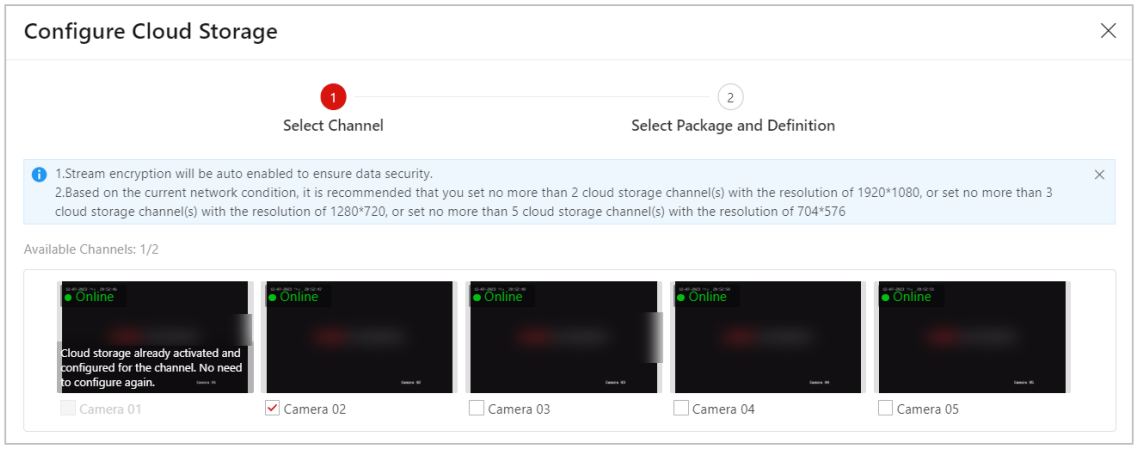
Set Cloud Storage Service for NVRs/DVRs Using the Portal

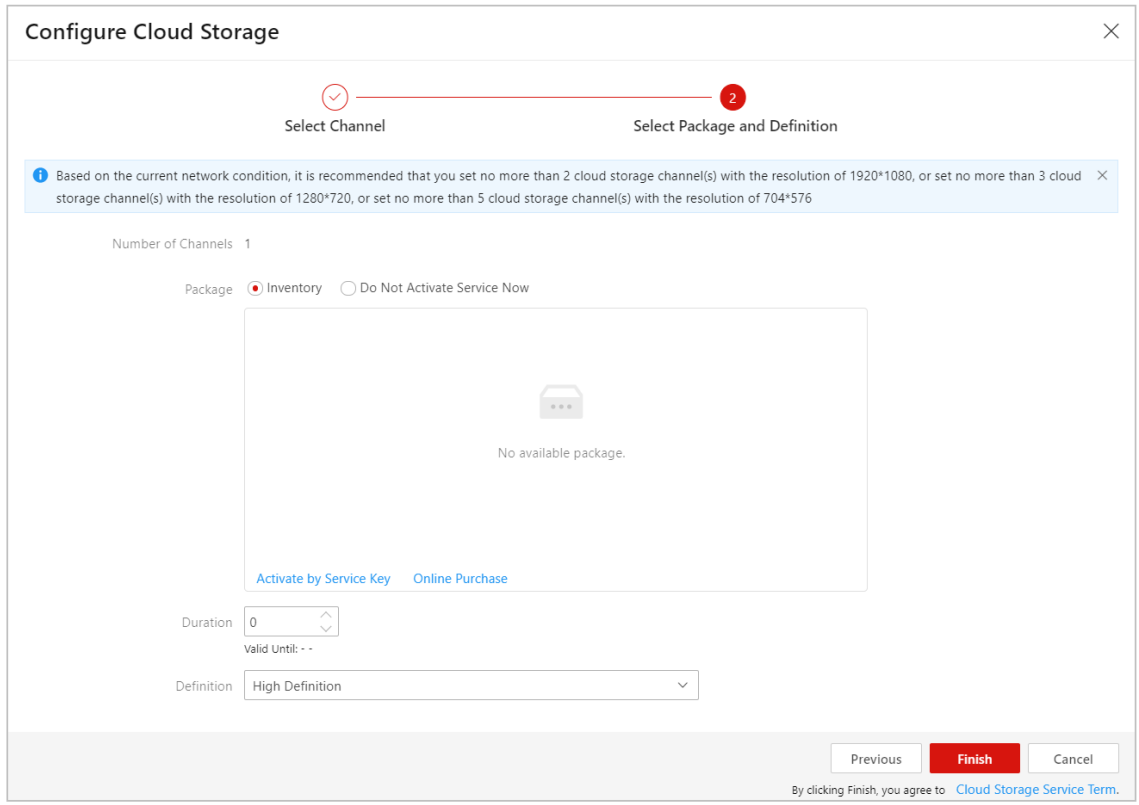
1. Add the NVR/DVR with the cloud storage capability itself to a site.

   Note

   Refer to ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** . Do not add the device by IP / domain name, or its cloud storage functionality will be unavailable.

2. Enter the Configure Cloud Storage page by one of the following ways.
   - On the adding result page, click **Cloud Storage Settings**.
   - Go to **Site & Device → Customer Site** , find the NVR/DVR, and click on the device card.
   - Go to **Site & Device → Customer Site** , click the NVR/DVR to enter its details page, and click **Configure Cloud Storage**.
   - Go to **Site & Device → Customer Site** , click the site, and go to **Cloud Storage → Configure Cloud Storage /** .
3. Set required information: Select channels to be configured, select cloud storage package for service activation, and select definitions.





4. Wait for the configuration to complete. You can click **Run in Background** to hide the page. Settings completed automatically in the background include:
   - Disabling Smart H.264+/H.265+ encoding and enabling SVC.
   - Enabling the device's cloud storage capability.
   - Setting motion detection events and enabling **Notify Surveillance Center**.
   - Activating the cloud storage service.
5. On the result page, click **Event Settings** to continue to set events.

Set Cloud Storage Service for NVRs/DVRs Using the Mobile Client

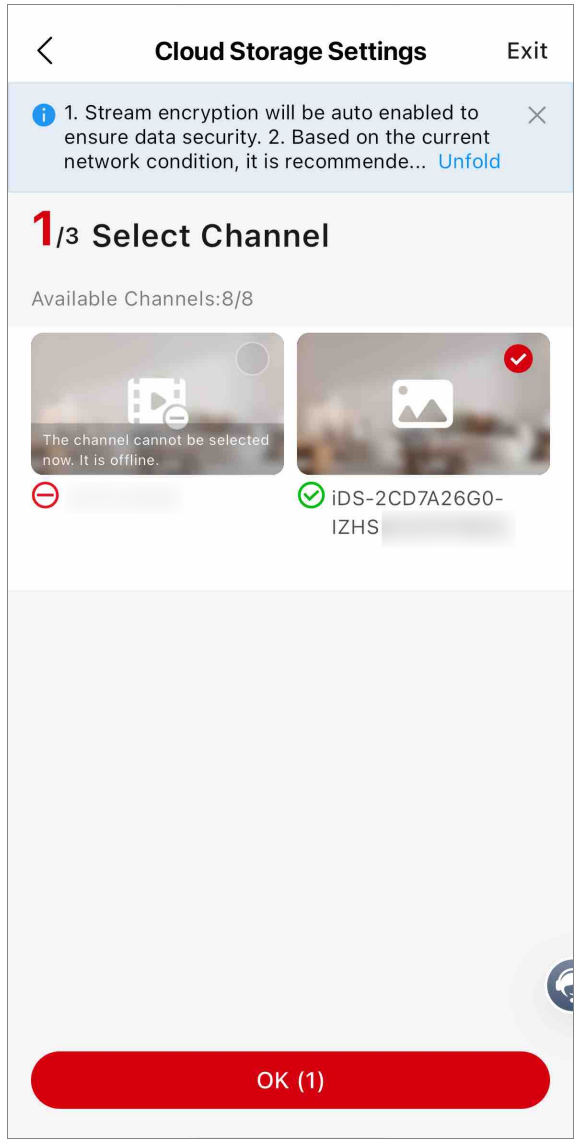
1. Add the NVR/DVR with the cloud storage capability itself to a site.

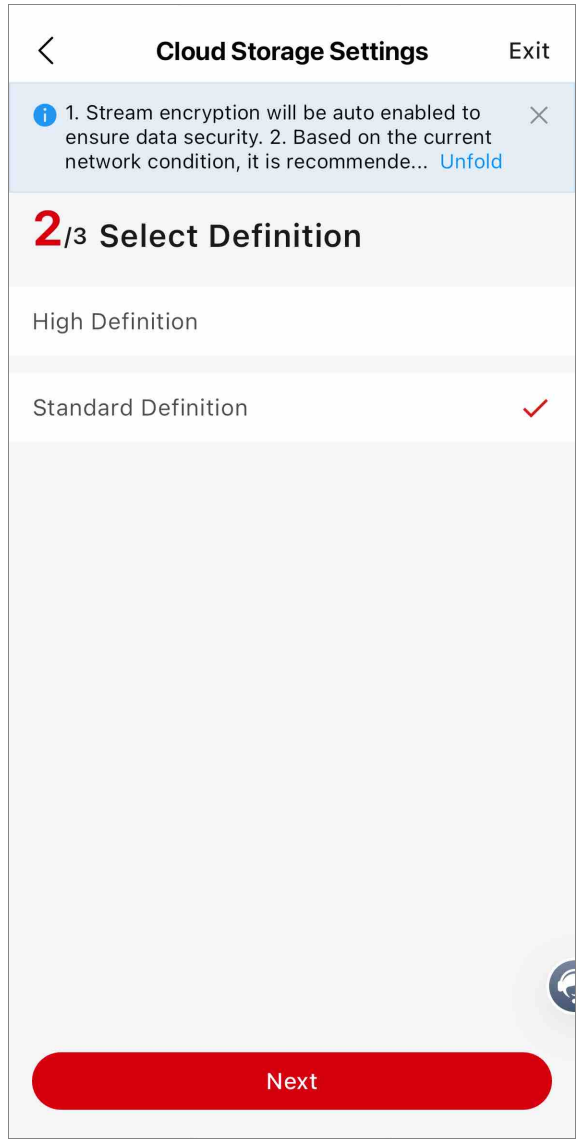
   Note

   Refer to ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** . Do not add the device by IP / domain name, or its cloud storage functionality will be unavailable.

2. Enter the Configure Cloud Storage page by one of the following ways.
   - On the adding result page, tap **Cloud Storage Settings**.
   - Tap **Site**, select the site, find the NVR/DVR, and tap on the device card.
   - Tap **Site**, select the site, tap the NVR/DVR to enter its details page, and tap **Cloud Storage → Cloud Storage Settings** .
   - Tap **Site**, select the site, and go to **Cloud Storage → Configure Cloud Storage /** .

3. Set required information: Select channels to be configured, select cloud storage package for service activation, and select definitions.




Cloud Storage Settings
Exit
1. Stream encryption will be auto enabled to ensure data security. 2. Based on the current network condition, it is recommende... Unfold
2/3 Select Definition
High Definition
Standard Definition
Next

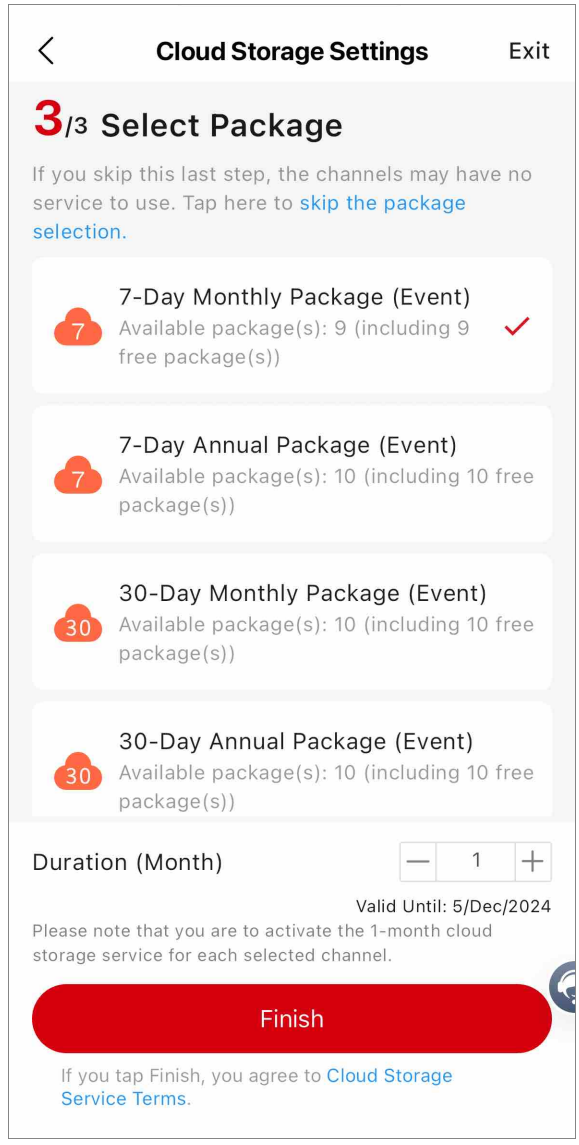


Figure 6-10 Cloud Storage Config

4. Wait for the configuration to complete. You can tap **Run in Background** to hide the page. Settings completed automatically in the background include:
   - Disabling Smart H.264+/H.265+ encoding and enabling SVC.
   - Enabling the device's cloud storage capability.
   - Setting motion detection events and enabling **Notify Surveillance Center**.
   - Activating the cloud storage service.
5. On the result page, tap **Event Settings** to continue to set events.

Set Cloud Storage Service for Cameras Using the Portal

1. Add the camera with the cloud storage capability itself to a site.

Note

Refer to ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** . Do not add the device by IP / domain name, or its cloud storage functionality will be unavailable.

2. Enter the Configure Cloud Storage page by one of the following ways.
   - On the adding result page, click **Cloud Storage Settings**.
   - Go to **Site & Device → Customer Site** , find the camera, and click on the device card.
   - Go to **Site & Device → Customer Site** , click the camera to enter its details page, and click **Configure Cloud Storage**.
   - Go to **Site & Device → Customer Site** , click the site, and go to **Cloud Storage → Configure Cloud Storage /** .
3. Set required information: Select the cloud storage package for service activation, and select the definition.
4. Wait for the configuration to complete. You can click **Run in Background** to hide the page. Settings completed automatically in the background include:
   - Disabling Smart H.264+/H.265+ encoding and enabling SVC.
   - Enabling the device's cloud storage capability.
   - Setting motion detection events and enabling **Notify Surveillance Center**.
   - Activating the cloud storage service.
5. On the result page, click **Event Settings** to continue to set events.

Set Cloud Storage Service for Cameras Using the Mobile Client

1. Add the camera with the cloud storage capability itself to a site.

Note

Refer to ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** . Do not add the device by IP / domain name, or its cloud storage functionality will be unavailable.

2. Enter the Configure Cloud Storage page by one of the following ways.
   - On the adding result page, tap **Cloud Storage Settings**.
   - Tap **Site**, select the site, find the camera, and tap on the device card.
   - Tap **Site**, select the site, tap the camera to enter its details page, and tap **Cloud Storage → Cloud Storage Settings** .
   - Tap **Site**, select the site, and go to **Cloud Storage → Configure Cloud Storage /** .
3. Set required information: Select the cloud storage package for service activation, and select the definition.
4. Wait for the configuration to complete. You can tap **Run in Background** to hide the page. Settings completed automatically in the background include:
   - Disabling Smart H.264+/H.265+ encoding and enabling SVC.
   - Enabling the device's cloud storage capability.
   - Setting motion detection events and enabling **Notify Surveillance Center**.
   - Activating the cloud storage service.
5. On the result page, tap **Event Settings** to continue to set events.

6.3.5 Step 4: Manage Cloud Storage Service Packages

Manage Cloud Storage Service Using the Portal

Go to **Site & Device → Service → My Service → Cloud Storage Service** .

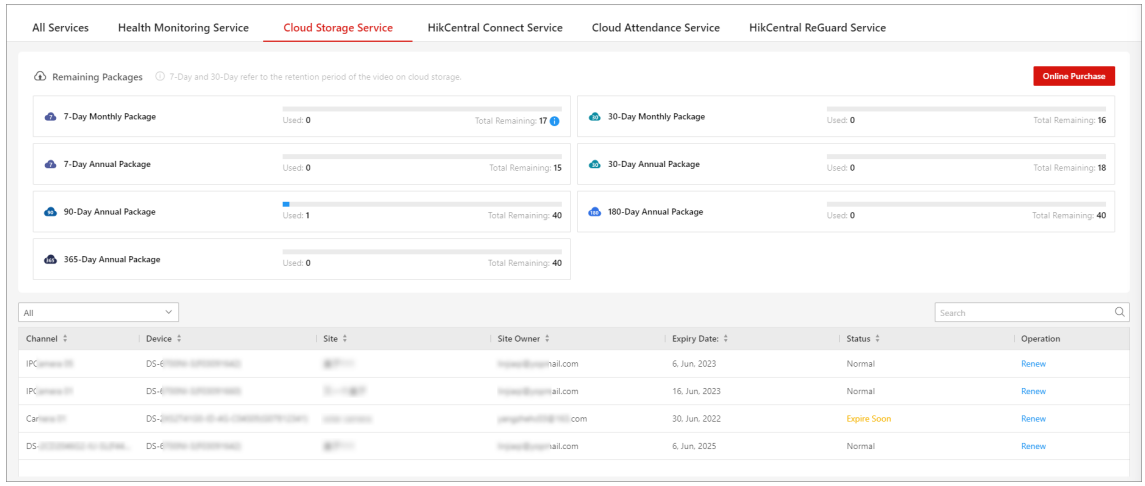


Figure 6-11 Manage Your Cloud Storage Service

Table 6-8 Available Features

Operation	Description
View Remaining Packages & Purchase More	View the used number and remaining numbers of each type of cloud storage packages. Click **Online Purchase** or **Activate by Service Key** to get more packages.
View Expiry Dates	View service expiry dates of each channel.
Renew Service	Click in the Operation column.
Transfer Service	Click in the Operation column to transfer the remaining service time from the current device to another.

Manage Health Monitoring Service Using the Mobile Client

Tap **Me** at the bottom right, tap **My Service**, and tap **Detail** in the Cloud Storage Service section.

Table 6-9 Available Features

Operation	Description
View Remaining Packages & Purchase More	View the used number and remaining numbers of each type of cloud storage packages.

Operation	Description
	Tap **Buy Now** or **Activate by Service Key** to get more packages.
View Expiry Dates	View service expiry dates of each channel.
Renew Service	Tap on the device card.
Transfer Service	Tap on the device card to transfer the remaining service time from the current device to another.

6.4 SIM Data Service: Connect Devices to 4G Network

Pain Points and What Customers Want From Installers

Pain Points of Customers	What Customers Want from Installers
• Remote or hard-to reach areas where traditional networks may fail. • Network downtime such as a primary network failure.	• Reliable and secure connectivity anytime and anywhere. • Data plans easy to purchase and manage. • Help manage multiple SIM cards.

What You Can Sell & Offer to Your Customers

- **Clear Service Plan and Easy to Purchase**: Hik-Partner Pro saves you the hassle of going to stores in person to purchase data plans. You can get service packages directly online. Data plans offered by Hik-Partner Pro are no-contract and data-only, which can be canceled at any time.
- **A Wide Variety of Options**: You can choose from monthly packages that contain different amount of data to suit your customers' needs.
- **Multi-Carrier IoT Connectivity**: The SIM cards support extensive connections to multiple carriers, and support switching among carriers for optimal signal strength.
- **Simple to Manage**: You can manage the service packages and data usage details of all your SIM cards on the Portal, and receive reminders promptly when data is about to run out or expire.
- **Data Security**: Data privacy protection for ensuring data security for your customers.

6.4.1 Step 1: Get SIM Card and Set APN on Devices

To use the data service on a device, you need a SIM card and set the APN on the device.

1. Get a SIM card from your distributor. Some devices themselves include SIM cards already.
2. Open the device's back cover, and insert the SIM card into the device's slot.

Note

The slot's position may vary depending on the specific model.

3. Set the APN according to the first 6 digits of the SIM card number.

Note

On some devices, APN is automatically set when you insert a SIM card into the device.

- **For wireless security control panels:**
  On the device configuration page, go to **Configuration → Network Settings → Cellular Data Network → Network Parameters** , enter the APN.
- **For 4G cameras:**
  On the device configuration page, go to **Configuration → Network Settings → Wireless Dial Settings → Private Network** , enter the APN.

First 6 Digits of Card No.	APN
890010	data.apn.name
891039	data.apn.name
893204	bicsapn
898830	super

6.4.2 Step 2: Get SIM Data Service Packages

You can purchase the SIM data service packages online in the Service Market in Hik-Partner Pro, or purchase a service key from the local distributor first and then activate by the service key to get the purchased service packages.

Note

The supported purchase methods vary depending on your country/region. Contact the local distributor for details.

Purchase Online Using the Portal

1. **Go to Site & Device → Service Market .**
2. In the SIM Data Service area, click **Online Purchase** to enter the Purchase SIM Data Service Package page.
3. Select the package based on the data amount and SMS allowance and set the quantity of packages to purchase.

Note

Packages that contain SMS allowance are exclusive to SIM cards of which the card numbers starting with 898830.

4. Enter the distributor invitation code and the code from Hikvision sales.

Note

By entering the codes when you purchase services online, you may get some discounts and the distributor/reseller can earn some rebates. For details, refer to ***How to Earn Commissions as a Distributor/Reseller*** .

5. Enter your VAT number. The VAT number will be displayed in the payment receipt.
6. Select **Credit/Debit Cards** as the payment method.
7. Click **Checkout** to enter the payment page and finish the payment.

Get Packages by Service Key Using the Portal

1. Contact your local distributor and purchase a service key from them.
2. Go to **Site & Device → Service Market** .
3. In the SIM Data Service area, click **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Click **OK**.

6.4.3 Step 3: Activate SIM Data Service for SIM Card

Activate the Service for SIM Card Using the Portal

1. Add the SIM card to Hik-Partner Pro by one of the following ways.

Method	Steps
Auto Add SIM Card This method is only applicable to SIM cards inserted in devices which are already added to the site.	a. Go to **Site & Device → Customer Site** . b. Click the site. c. Click **SIM Data Service → Auto Add SIM Card** . d. Wait for cards to be auto added to the site. Click **OK**.
Add SIM Card Manually Enter the card No. to add SIM cards one by one.	**To add a SIM card to Hik-Partner Pro:** a. Go to **Site & Device → SIM Card** . b. Click **Add SIM Card Manually**. c. Enter the card number. d. Click **Confirm**.
	To add a SIM card to a specific site on Hik-Partner Pro:

Method	Steps
	a. Go to **Site & Device → Customer Site** . b. Click the site. c. Click **SIM Data Service → Add SIM Card Manually** . d. Enter the card number. e. Click **Confirm**.

2. Turn on **Activate**.
3. Select a type of service package.
4. Turn on **Auto Renewal**.
5. Click **Confirm**.

6.4.4 Step 4: Manage SIM Cards and SIM Data Service Packages

Manage SIM Data Cards Using the Portal

Go to **Site & Device → SIM Card** .

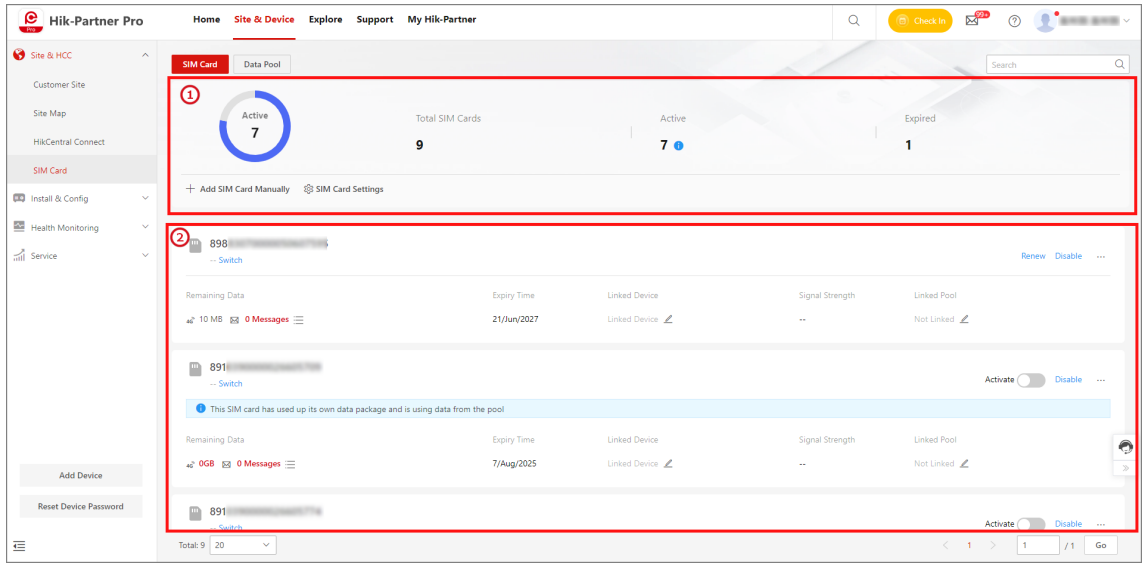


Figure 6-12 SIM Card Management

Table 6-10 Available Operations

Area No.	Operation	Description
1	View SIM Card Status	View the number of SIM cards with active/expired data service.
1	Add SIM Card Manually	Add a SIM card by entering the SIM card number.

Area No.	Operation	Description
2	View SIM Card Details	View remaining data, expiry time, signal strength, etc.
2	Activate/Renew Service	Turn on **Activate** or click **Renew** to activate/renew the SIM data service for the card.
2	Suspend/Resume SIM Card	Click **Suspend**/**Resume** to suspend/resume the data service for the SIM card.
2	Enable Service Auto Renewal	Click ··· → **Auto Renewal** .
2	Check Usage Details	Click ··· → **Details** to view data usage details in the last 30 days.

Manage SIM Data Service Packages Using the Portal

Go to **Site & Device → Service → My Service → SIM Data Service** .

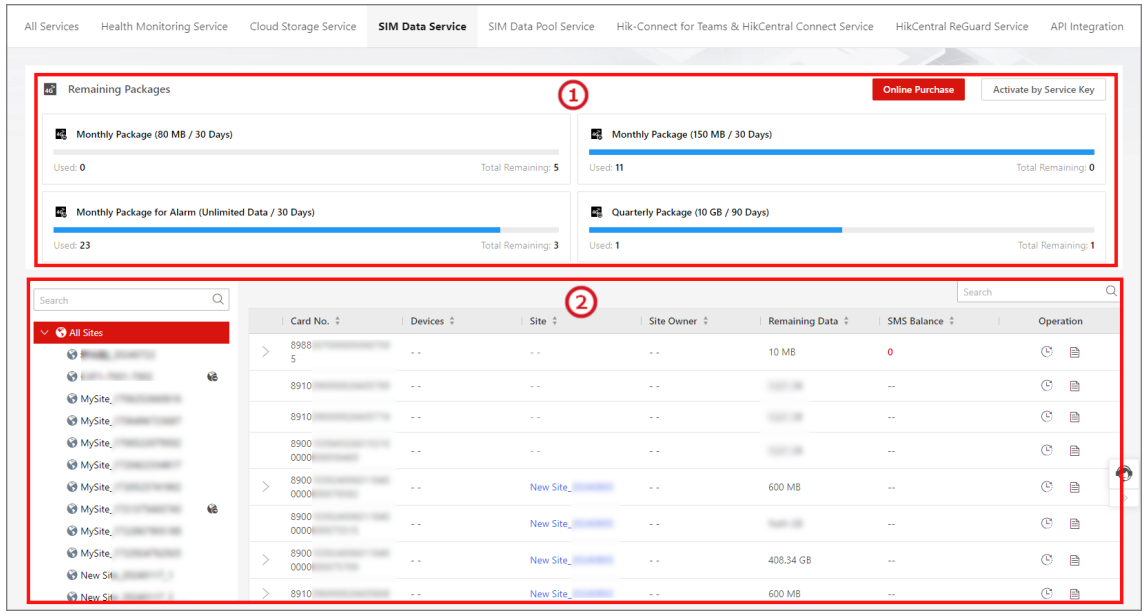


Figure 6-13 Manage Your SIM Data Service Packages

Table 6-11 Available Operations

Area No.	Operation	Description
1	View Remaining Packages & Purchase More	View the used number and remaining numbers of each type of packages.

Area No.	Operation	Description
		Click **Activate by Service Key** or **Online Purchase** to get more packages.
2	View Data Balance	View the remaining data of each SIM card.
2	Renew Service	Click in the Operation column. You can choose to enable **Auto Renewal**.
2	Check Usage Details	Click in the Operation column to data usage details in the last 30 days.

6.5 SIM Data Pool Service: Cards Share Data in a Pool

This service allows multiple SIM cards in one data pool to share data.

Pain Points and What Customers Want From Installers

Pain Points of Customers & Installers	What Customers Want from Installers
• Hard to avoid overage fees of SIM cards. • Complex bill management. • Hard to manage and allocate data for multiple SIM cards.	• Help manage multiple SIM cards and bills. • Help avoid overage fees.

What You Can Sell & Offer to Your Customers

- **Cost Savings**: Centralized data management to avoid overage fees of the SIM cards.
- **Flexibility**: Allocate data based on demand, improving efficiency.
- **Simplified Financial Management**: One bill covers all SIM cards.
- **Convenience**: Ideal for households or enterprises for centralized management and control.

How to Use SIM Data Pool Service

Table 6-12 How to Use SIM Data Pool Service

Steps	Related Topics
1. **Add SIM cards to pools** so as to use purchased data pool service packages. Only SIM cards for which the **SIM data service** is already activated (not expired) can be added to	• ***SIM Data Service: Connect Devices to 4G Network*** • ***Step 1: Add SIM Cards to Data Pool***

Steps	Related Topics
pools. They start using data from the pool if their own data are used up.	
2. **Get SIM data pool service packages** by online purchase or purchasing service keys from distributors.	***Step 2: Get SIM Data Pool Service Packages***
3. **Replenish the pool** with shareable data quota.	***Step 3: Activate SIM Data Pool Service for Pool***
4. Enable auto renewal, add SIM cards, check usage details, etc.	***Step 4: Manage Data Pools and SIM Data Pool Service Packages***

6.5.1 Step 1: Add SIM Cards to Data Pool

Only SIM cards for which the SIM data service is already activated (not expired) can be added to pools. They start using data from the pool if their own data are used up.

Add SIM Cards to Data Pool Using the Portal

1. Go to **Site & Device → SIM Card → Data Pool** .
2. Add a pool.
   a. Click **Add Pool**.
   b. Enter the pool name.
   c. Click **OK**.
3. Add SIM cards to the pool.
   a. Click **Add SIM Card Manually**.
   b. Select SIM cards to add them to the pool, or click **Manual Adding** to add by entering the card number.
   c. Click **OK**.

6.5.2 Step 2: Get SIM Data Pool Service Packages

You can purchase the SIM data pool service packages online in the Service Market in Hik-Partner Pro, or purchase a service key from the local distributor first and then activate by the service key to get the purchased service packages.

Note

The supported purchase methods vary depending on your country/region. Contact the local distributor for details.

Purchase Online Using the Portal

1. Go to **Site & Device → Service Market** .
2. In the SIM Data Pool Service area, click **Online Purchase** to enter the Purchase SIM Data Pool Service Package page.
3. Select the package based on the data amount and SMS allowance and set the quantity of packages to purchase.
4. Enter the distributor invitation code and the code from Hikvision sales.

   Note

   By entering the codes when you purchase services online, you may get some discounts and the distributor/reseller can earn some rebates. For details, refer to ***How to Earn Commissions as a Distributor/Reseller*** .
5. Enter your VAT number. The VAT number will be displayed in the payment receipt.
6. Select **Credit/Debit Cards** as the payment method.
7. Click **Checkout** to enter the payment page and finish the payment.

Get Packages by Service Key Using the Portal

1. Contact your local distributor and purchase a service key from them.
2. Go to **Site & Device → Service Market** .
3. In the SIM Data Pool Service area, click **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Click **OK**.

6.5.3 Step 3: Activate SIM Data Pool Service for Pool

Activate the Service for Your Pool Using the Portal

1. Go to **Site & Device → SIM Card → Data Pool** .
2. Click **Activate**.
3. Select a type of service package.
4. Turn on **Auto Renewal**.
5. Click **Confirm**.

6.5.4 Step 4: Manage Data Pools and SIM Data Pool Service Packages

Manage Data Pools Using the Portal

Go to **Site & Device → SIM Card → Data Pool** .

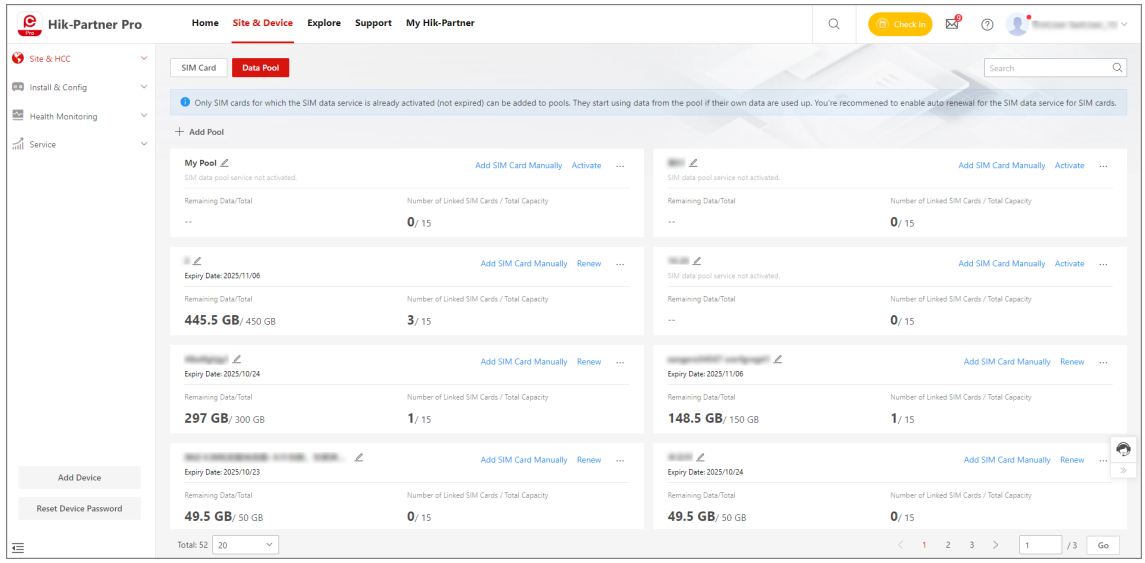


Figure 6-14 Data Pool Management

Table 6-13 Available Operations

Operation	Description
View Data Pool Details	View the remaining data of the pool and number of added SIM cards.
Add SIM Card	Click **Add SIM Card Manually**. Select SIM cards or enter a SIM card number to add to a pool.
Activate/Renew Service	Click **Activate** or **Renew** to activate/renew the SIM data pool service for the pool.
Enable Service Auto Renewal	Click ··· → **Auto Renewal** .
Check Usage Details	Click ··· → **Details** to view data usage details of the pool in the last 30 days.

Manage SIM Data Pool Service Packages Using the Portal

Go to **Site & Device → Service → My Service → SIM Data Pool Service** .

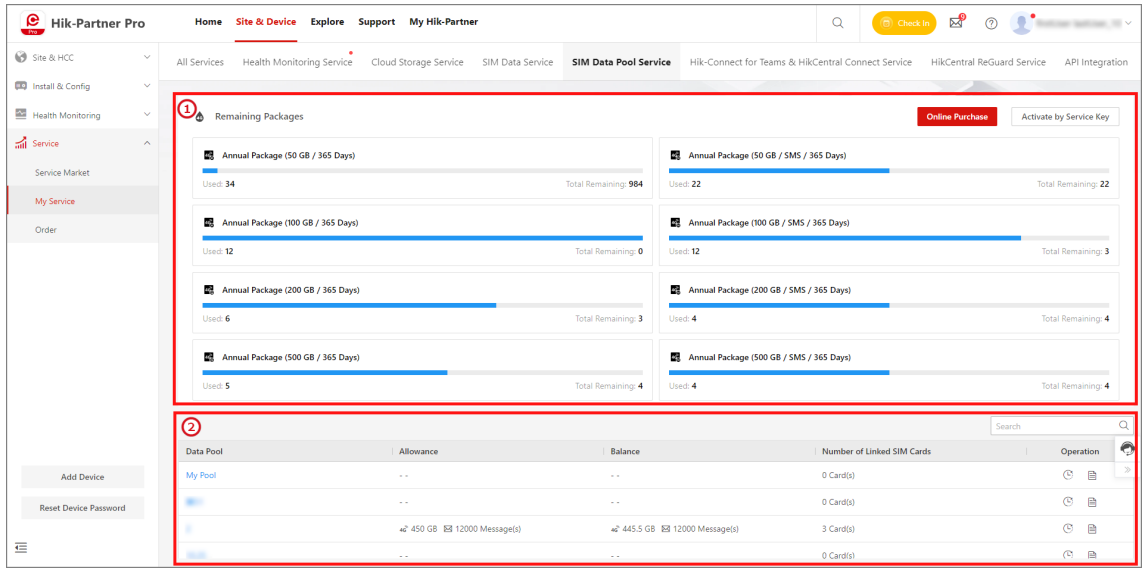


Figure 6-15 Manage Your SIM Data Pool Service Packages

Table 6-14 Available Operations

Area No.	Operation	Description
1	View Remaining Packages & Purchase More	View the used number and remaining numbers of each type of packages. Click **Activate by Service Key** or **Online Purchase** to get more packages.
2	View Data Balance	View the data balance of each data pool.
2	Renew Service	Click in the Operation column. You can choose to enable **Auto Renewal**.
2	Check Usage Details	Click in the Operation column to data usage details in the last 30 days.

6.6 Hik-Connect for Teams Services: Provide VSaaS Solution for Enterprise Customers

Hik-Connect for Teams (HCT) services are offered by the HCT Portal and Mobile Client, which provide a Video Security as a Service (VSaaS) solution for enterprise users.

Note

The availability of HCT services varies depending on the country/region.

What to Offer to Your Customers & Core Benefits for You

For What Kind of Customers
Enterprise users, also for chain stores, offices, communities, etc.

What You Can Offer to Customers

You can help enterprise customers install, set up, and hand over a system using Hik-Partner Pro to provide services like person and permission management, video security, access control, attendance check, and device maintenance.

Note

Except for basic features, customers can only pay for the services they need.

- **Basic features for HCT systems:**
  - Unlimited channels and devices.
  - Access via HCT Portal and Mobile Client.
  - Enterprise-level management, multi-location management.
  - Multi-account management (unlimited user), multi-level permissions for different user roles.
  - Maintenance and OpenAPI.
- **Video management:** Live view, playback, 3 auxiliary screens, intelligent video search, video clip & alarm information archiving to cloud storage, etc.
- **Access control & attendance:**
  - Remote door control, personnel management, access level management, temporary pass assignment, entry or exit logs with detailed info, event management, etc.
  - Timetable, schedule, and shift settings. Diverse attendance reports. Mobile attendance for clocking.
- **Intrusion:** Support alarm devices. Arming, disarming, alarm handling, linkage between alarms and videos, etc.
- **Intercom:** Remote video intercom, building/room/resident management, and temporary pass.
- **Analysis report:** Support people counting and heat maps.
- **On-board monitoring:** Real-time monitoring, GPS location, and playback of on-board devices, alarms on drivers' behaviors, driving reports, etc.
- **ANPR:** License plate management, vehicle allowlists, passing vehicle records, barrier gate control, etc.
- **Health monitoring:** Device health monitoring overview and scheduled health check report delivery.

Core Benefits for You (Installers, Service Providers, etc.)
• **Cloud-based, easy deployment:** Simplify the installation process with Hik-Partner Pro. **No more** complex server deployment, public IP, domain, or VPN requirements. • **Unlock profitable opportunities:** Expand your business, generate continuing revenue for you via multiple subscription service options, including cloud-based VMS, access control & attendance, intercom, and cloud storage solutions.

Overall Instructions for Service Providers to Provide HCT Services

Role / Platform	Description	Related Topics
Service Providers (Installers, etc.) on Hik-Partner Pro	1. Create a team site and select desired services.	***Step 1: Create an HCT System (Team Site) and Select Desired Services***
	2. Add devices to the team site.	***Step 2: Add Devices to Team Site***
	3. Activate the service, configure users, devices & scenarios for the site, and hand over the team site to customers.	• ***Step 3: Get HCT Packages*** • ***Step 4: Activate/Renew HCT Services*** • ***Step 5: Hand Over a Team Site*** • ***Hik-Connect for Teams Portal User Manual***
	4. Manage services and access the system to help customers maintain the services.	• ***Step 6: Manage Devices, Services & Users for a Team Site*** • ***Step 7: Manage HCT Services for All Team Sites***
Customers (i.e., Enterprise Users) on Hik-Connect for Teams	1. Receive an email after the installer hands over the site, which contains a login link. 2. Log in to the HCT system and accept the devices. 3. Use the services in HCT.	• ***Hik-Connect for Teams Portal User Manual*** • ***Hik-Connect for Teams Mobile Client User Manual***

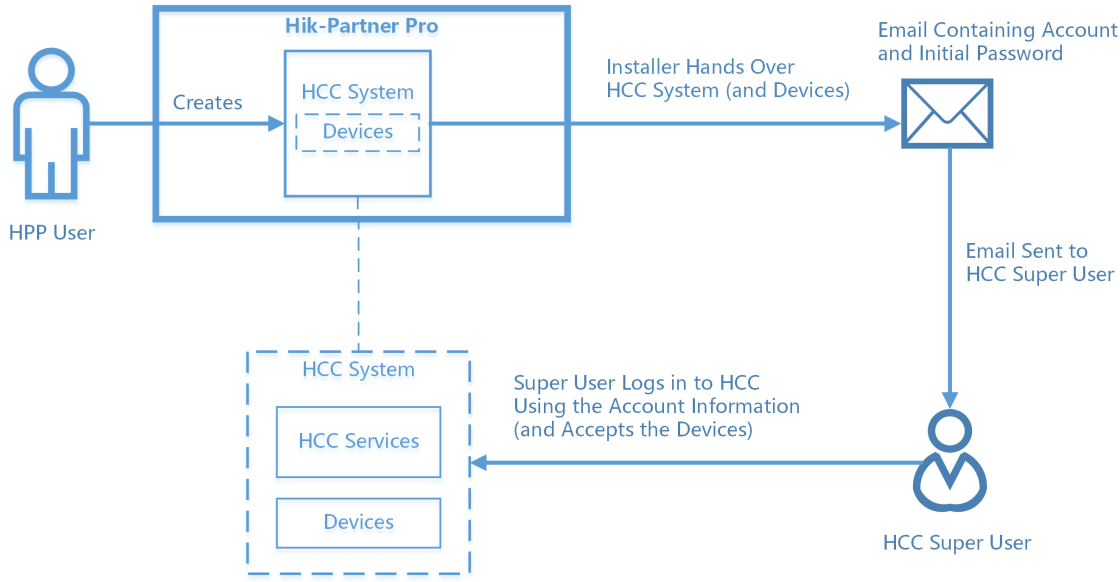


Figure 6-16 How an HCT System Is Created on Hik-Partner Pro and Handed Over

6.6.1 Step 1: Create an HCT System (Team Site) and Select Desired Services

Add a Team Site Using the Portal

1. Go to **Site & Device → Customer Site** .
2. Switch to **Site Mode**.
3. Click **Add New Site**.
4. Set the site name and time zone.
5. Click **More** to set more information such as the scene and site address.
6. Select **Team** as the site type.
7. Select desired services to activate for your customer.

Note

For some services, Hik-Partner Pro offers both the capacity-umlimited trial for some time period and the free lifetime capacity. Details vary depending on the country/region.

8. Click **OK**.

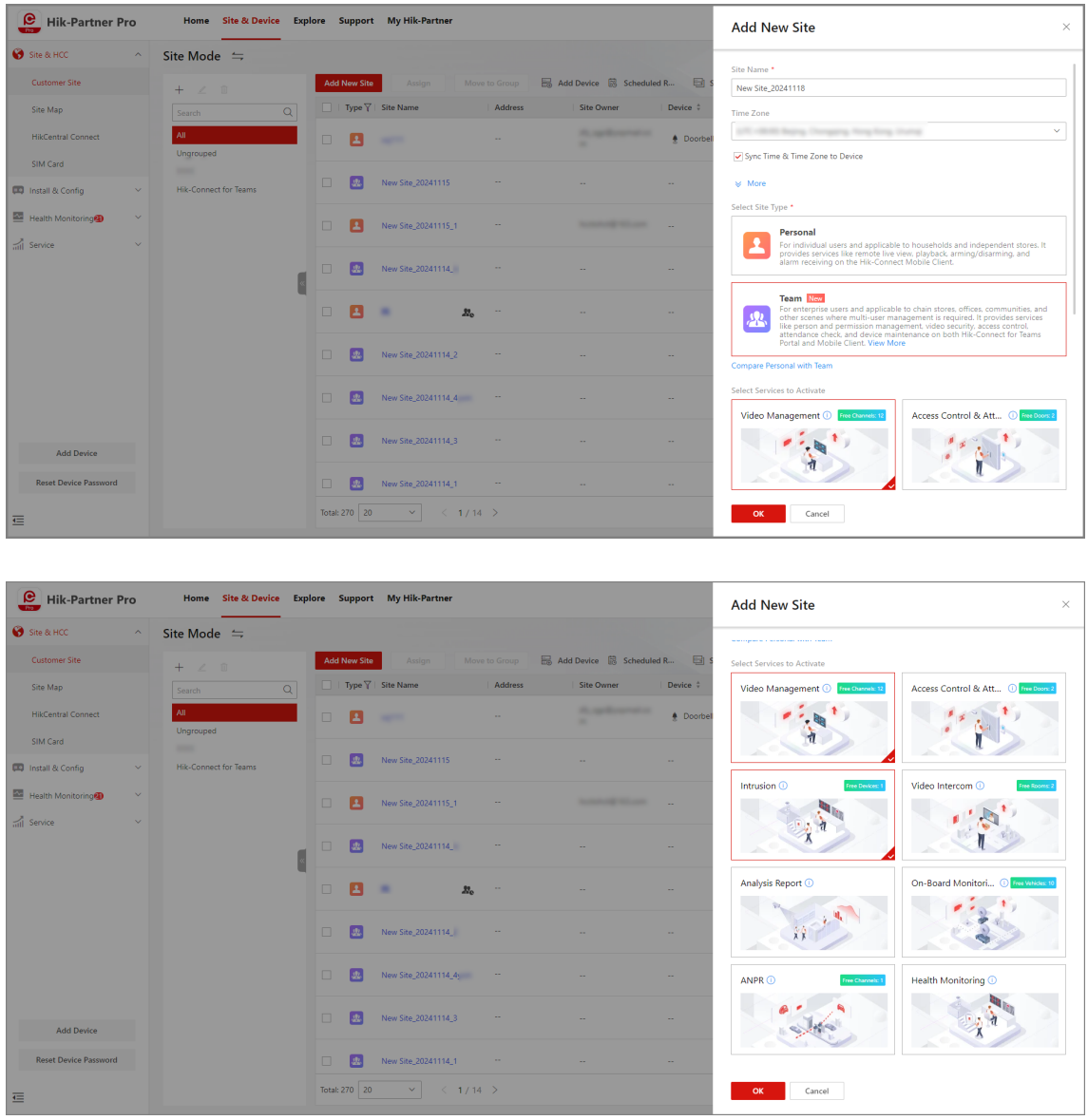


Figure 6-17 Add New Team Site Using the Portal

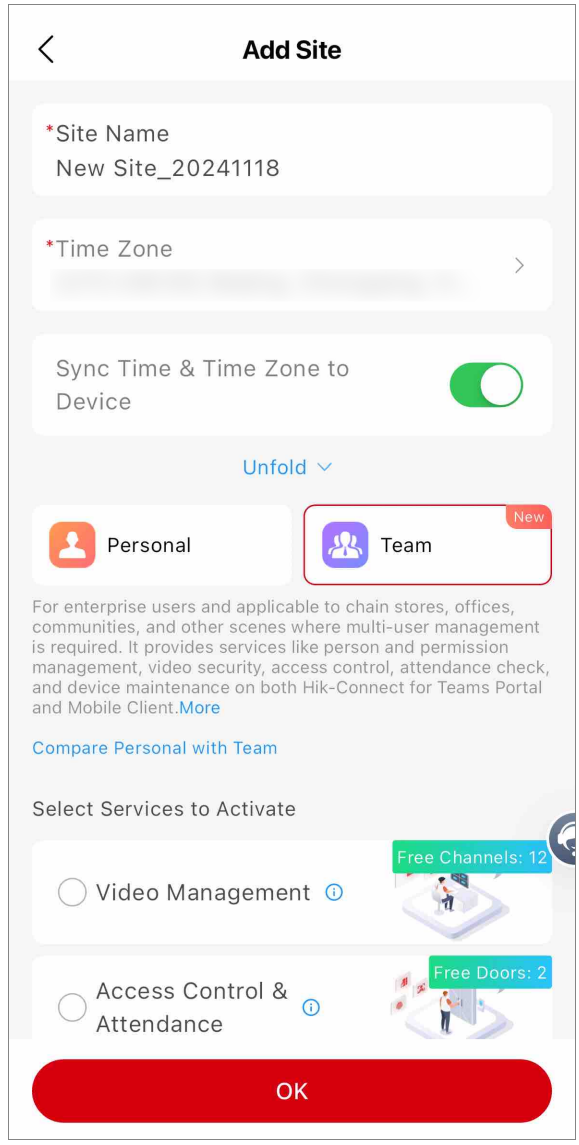
Create a Team Site Using the Mobile Client

1. Go to **Site**.
2. Tap **Add Site**.
3. Set the site name and time zone.
4. Tap **Unfold** to set more information such as the scene and site address.
5. Select **Team** as the site type.
6. Select desired services to activate for your customer.

Note

For some services, Hik-Partner Pro offers both the capacity-umlimited trial for some time period and the free lifetime capacity. Details vary depending on the country/region.

7. Tap **OK**.



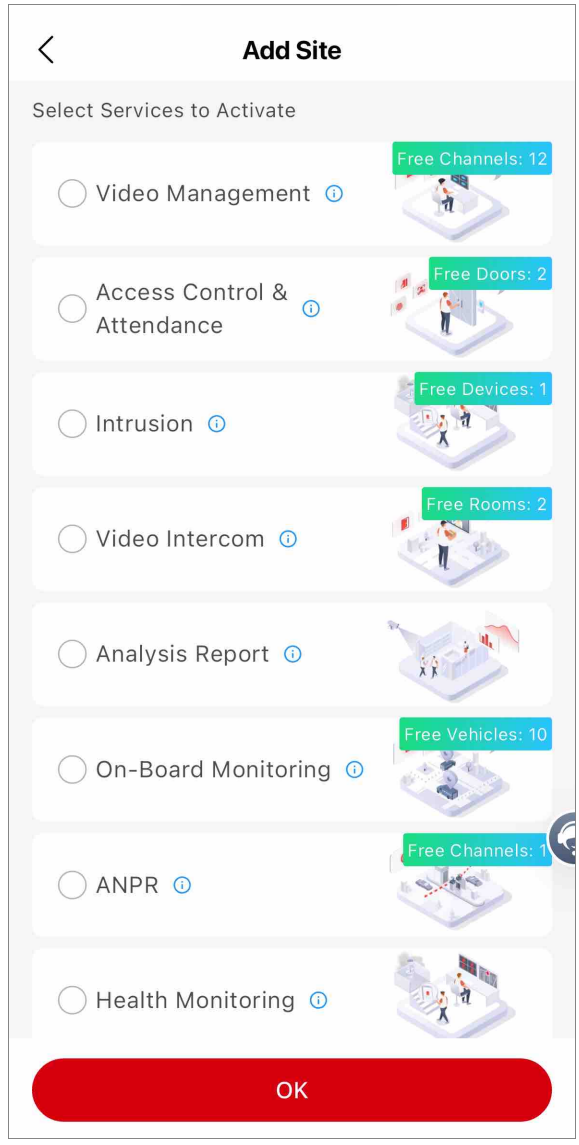


Figure 6-18 Add Team Site Using the Mobile Client

6.6.2 Step 2: Add Devices to Team Site

After you create a team site, you will immediately enter the Add Device process. Or you can add devices later. The team sites only supports adding device by scanning QR codes, by entering the serial numbers, and via the LAN (the SADP tool). For detailed instructions, refer to ***Quick Start Guide: Add Devices to Hik-Partner Pro for Remote Maintenance*** .

6.6.3 Step 3: Get HCT Packages

You can purchase the health monitoring packages online in the Service Market in Hik-Partner Pro, or purchase a service key from the local distributor first and then activate by the service key to get the purchased service packages.

Note

The supported purchase methods vary depending on your country/region. Contact the local distributor for details.

Purchase Online Using the Portal

1. Go to **Site & Device → Service Market** .
2. In the Hik-Connect for Teams Service area, click **Online Purchase** to enter the Purchase Hik-Connect for Teams Service Package page.
3. Set the package quantity of the services your customer needs.

   Video Management Service Package

   One monthly/annual package for one channel. You can select whether to include the cloud storage service.

   On-Board Monitoring Service Package

   One monthly/annual package for one vehicle.

   Intrusion Service Package

   One monthly/annual package for one alarm device.

   Access Control & Attendance Service Package

   One lifetime/annual package for 1/5/10 doors.

   Video Intercom Service

   One annual package for one room.

   Health Monitoring Service Package

   One monthly/annual package for one device.

   Note

   You can also activate the health monitoring service for devices on team sites using the health monitoring packages for personal sites.
4. Enter the distributor invitation code and the code from Hikvision sales.

   Note

   By entering the codes when you purchase services online, you may get some discounts and the distributor/reseller can earn some rebates. For details, refer to ***How to Earn Commissions as a Distributor/Reseller*** .
5. Enter your VAT number. The VAT number will be displayed in the payment receipt.

6. Select **Credit/Debit Cards** as the payment method.
7. Click **Checkout** to enter the payment page and finish the payment.

Get Packages by Service Key Using the Portal

1. Contact your local distributor and purchase a service key from them.
2. Go to **Site & Device → Service Market** .
3. In the Hik-Connect for Teams Service area, click **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Click **OK**.

Get Packages by Service Key Using the Mobile Client

1. Contact your local distributor and purchase a service key from them.
2. Go to **Me → Service Market** .
3. In the Hik-Connect for Teams Service area, tap **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Tap **OK**.

6.6.4 Step 4: Activate/Renew HCT Services

HCT services activation or renewal via the Hik-Partner Pro means to only expand the service capacities for customer's HCT system. Customers need to choose which resources to utilize the capacities on their HCT Portal or Mobile Client.

Activate/Renew HCT Services Using the Portal

1. Go to **Site & Device → Customer Site** , and click a team site to enter the site details page.
2. Click the service you are to activate/renew, and click **Expand** or click **Activate** first and then **Expand**.
3. Set the quantity and (if any) service duration.
4. Click **Confirm** to complete, or **Purchase and Activate** if remaining packages are insufficient.

Activate/Renew HCT Services Using the Mobile Client

1. Go to **Site**, and tap a team site to enter the site details page.
2. Tap the service you are to activate/renew, and tap **Activate and Expand** or tap **Activate** first and then **Activate and Expand**.
3. Set the quantity and (if any) service duration.
4. Tap **Confirm** to complete, or **Purchase and Activate** if remaining packages are insufficient.

6.6.5 Step 5: Hand Over a Team Site

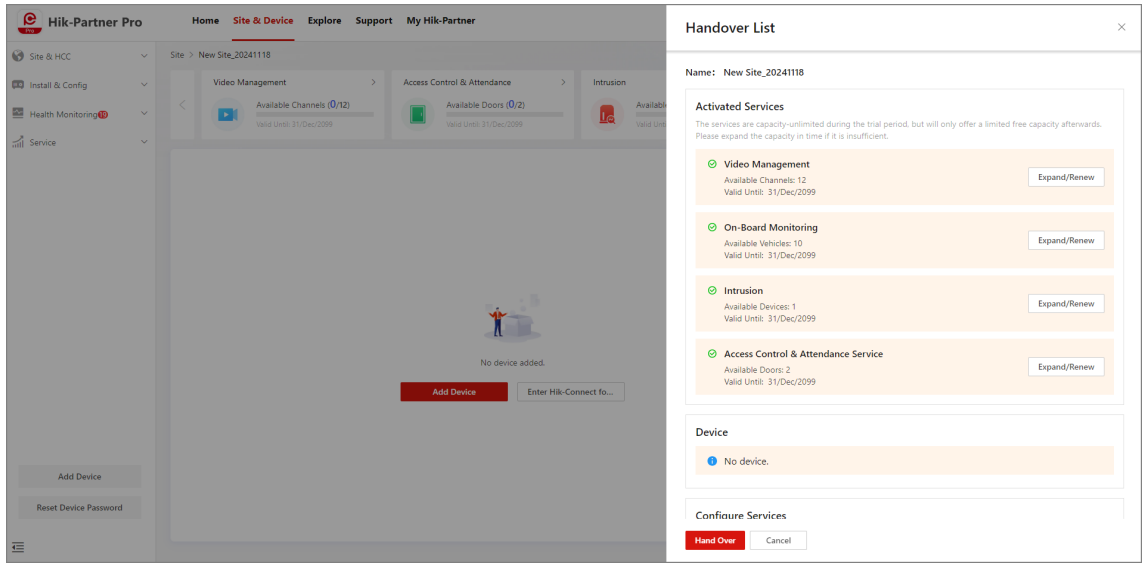
Hand Over a Team Site Using the Portal

1. Go to **Site & Device → Customer Site** , and switch to **Site Mode**.
2. To complete more configurations (users, devices and scenarios settings) before the handover, click **Enter Hik-Connect for Teams** to enter the HCT system of your customer.
3. Find the team site, and click in the Operation column, or click the team site to enter its details page and click **Hand Over by Transferring**.
4. Check and make adjustments to the handover list: the activated services and their capacities, added devices, completed configurations, and the permissions you are to apply for from the customer.

Note

- With the service management permission, you can activate, renew, and manage HCT services for this team site via Hik-Partner Pro.
- With the system access permission, you can access the HCT system remotely to help add, maintain, and configure devices.

5. Click **Hand Over**.
6. Select **Email** or **Phone Number**, and set customer information for handover.
7. Click **Confirm**. Your customer will receive the handover request via email or SMS.



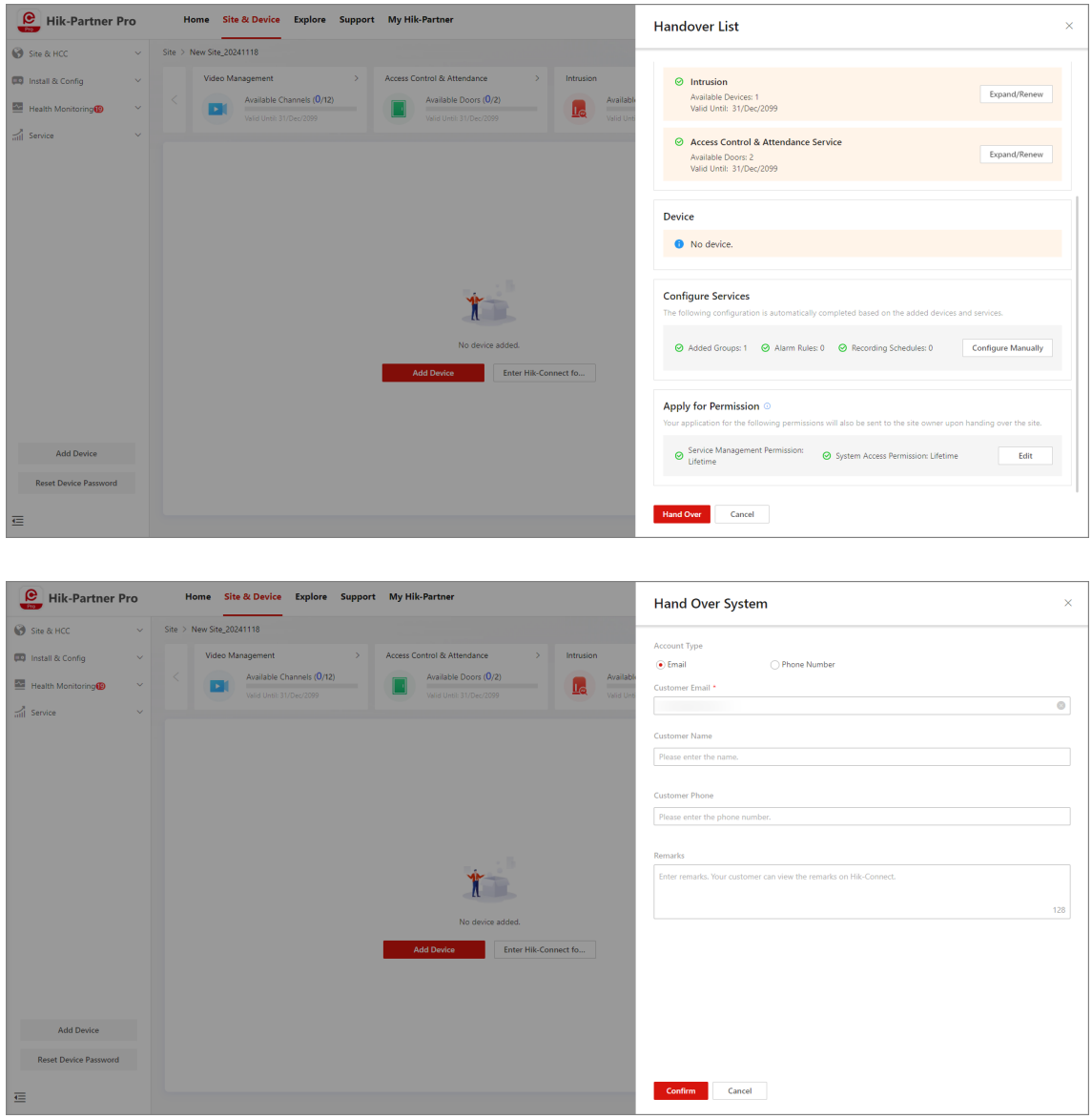


Figure 6-19 Hand Over Team Site Using the Portal

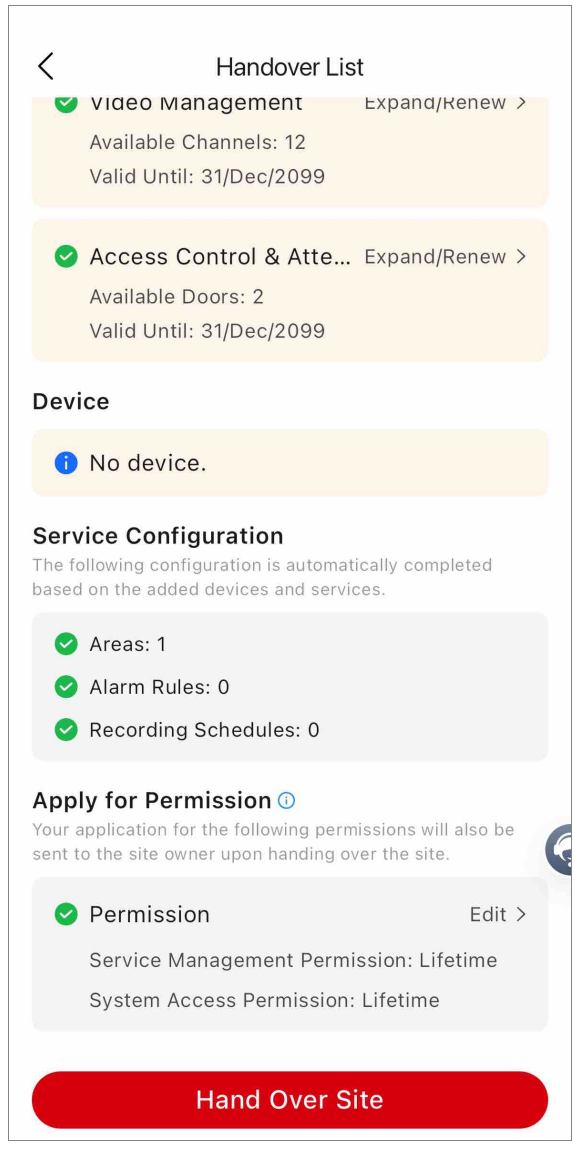
Hand Over a Team Site Using the Mobile Client

1. Tap **Site**.
2. Find and tap the team site to enter its details page, and tap **Hand Over Site**.
3. Check and make adjustments to the handover list: the activated services and their capacities, added devices, completed configurations, and the permissions you are to apply for from the customer.

Note

- With the service management permission, you can activate, renew, and manage HCT services for this team site via Hik-Partner Pro.
- With the system access permission, you can access the HCT system remotely to help add, maintain, and configure devices.

4. Tap **Hand Over Site**.
5. Select **Email** or **Phone Number**, and set customer information for handover.
6. Tap **Confirm**. Your customer will receive the handover request via email or SMS.



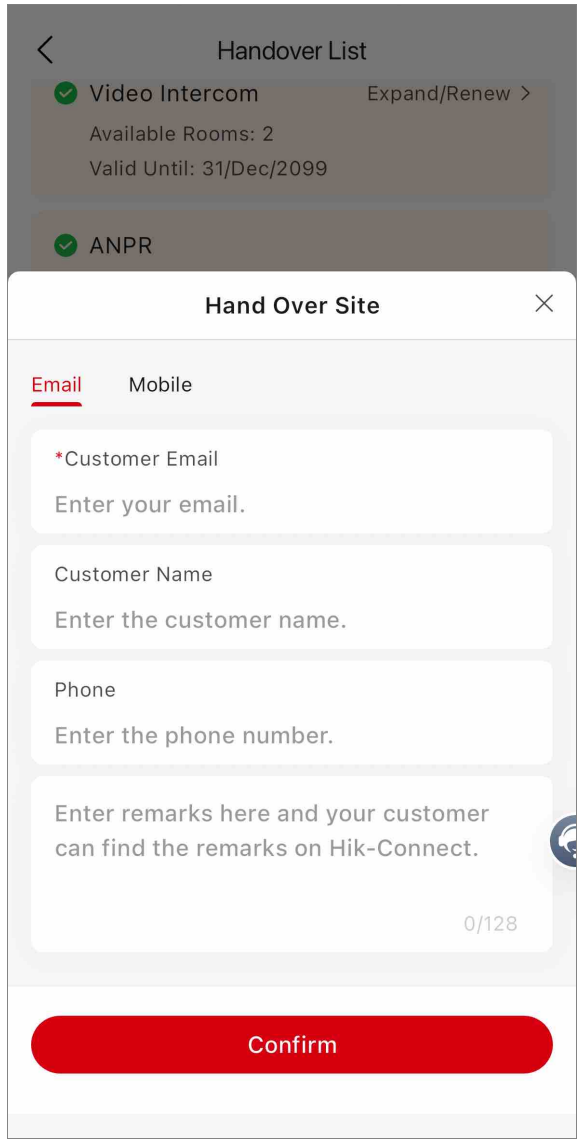


Figure 6-20 Hand Over Team Site Using the Mobile Client

6.6.6 Step 6: Manage Devices, Services & Users for a Team Site

Before you hand over the team site, or after you hand it over and if you are granted the service management permission and the system access permission by your customer, you can help manage devices, services and users for their team site.

Installer's Permission	With the Permission, Installers Can	Instructions
Service Management Permission	View service package information of the system, including activated service types, activated service quantities, expiry times, and used service quantities.	Enter a team site's details page to view its service details: • **Portal:** Click **Site & Device → Customer Site** , and click the team site. • **App:** Tap **Site**, and tap the team site.
	Activate services, renew the activated services, and expand the service capacity for the system.	***Step 4: Activate/Renew HCT Services***
System Access Permission	• View device information of the system, including the number of devices, device names, device serial numbers, and models. • Add devices to the system. • View live videos of cameras and perform PTZ controls (such as setting and calling presets and auto-switches). • Play recorded video clips. • Configure devices remotely. • Add, delete, edit and view user accounts on the remote configuration page of the device (with administrator password authenticated).	Enter a team site's details page to add and configure devices: • **Portal:** Click **Site & Device → Customer Site** , and click the team site. • **App:** Tap **Site**, and tap the team site.
	Access the system remotely as an administrator. All device configuration and operation permissions, and all system configuration and management permissions.	**Portal:** 1. Click **Site & Device → Customer Site** , and click the team site. 2. Click **Enter Hik-Connect for Teams** to enter the customer's HCT system.

6.6.7 Step 7: Manage HCT Services for All Team Sites

Manage HCT Services for All Team Sites Using the Portal

Go to **Site & Device → Service → My Service → Hik-Connect for Teams Service** .

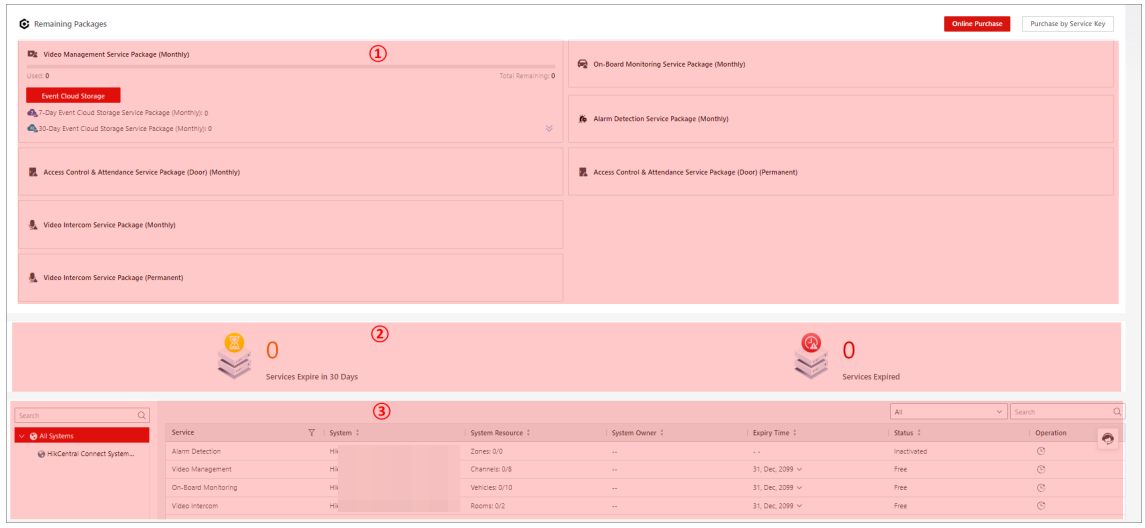


Figure 6-21 Manage Your HCT Services

Table 6-15 Available Features

Area	Operation	Description
1	Check Remaining Packages & Purchase More	You can check the number of used and remaining packages for each service. If needed, click **Online Purchase** or **Activate by Service Key** to get more packages.
2	View Overall Package Expiration Status	You can view the overall number of services that are going to expire within 30 days and those that have already expired. Click to view details of these services in the list below.
3	Activate Service	Click in the Operation column to activate the service for the corresponding HCT team site.

Manage HCT Services for All Team Sites Using the Mobile Client

Tap **Me** at the bottom right, tap **My Service**, and tap **Detail** in the Hik-Connect for Teams Service section.

You can check the number of used and remaining packages for each service.

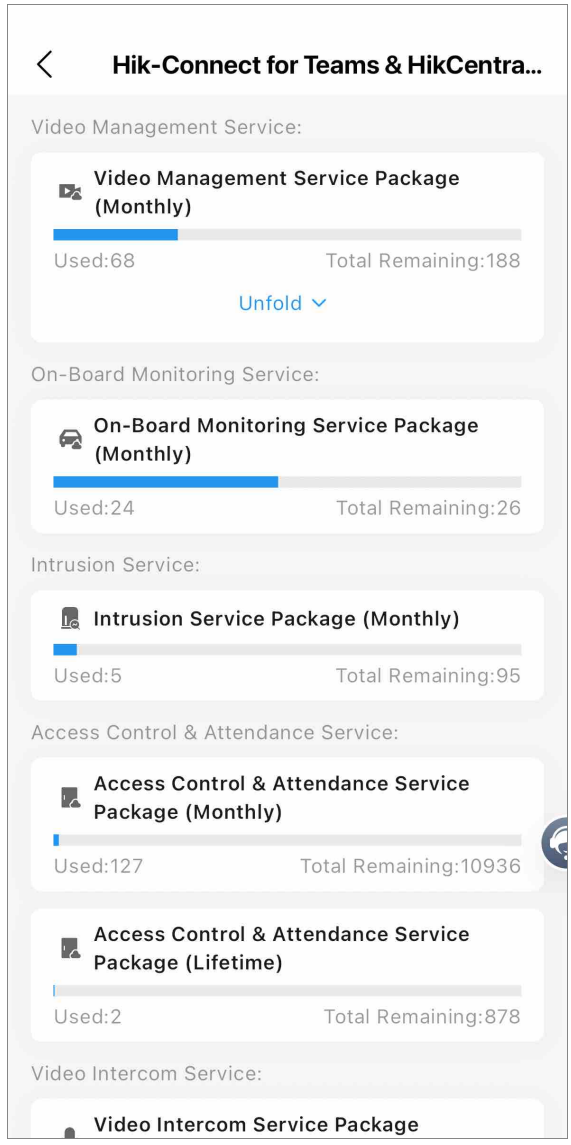


Figure 6-22 My Service: HCT Service

6.7 HikCentral ReGuard Service: Security Management Solution for Customers

HikCentral ReGuard (hereinafter referred to as HCRG) services are the value-added services offered by the HCRG. HCRG provides a security management solution that helps its users (i.e., remote monitoring center) with alarm receiving and handling.

Note

The HCRG services are supported only in some countries/regions. For details, contact the local distributors or after-sales.

For What Kind of Customers & What You Can Offer to Them

For What Kind of Customers
Remote Monitoring Centers (RMC) (for alarm receiving and handling, etc.).

What You Can Offer to Them
You can help customers install and set up a system with the following capabilities. • **Basic features for RMC systems:** ◦ Alarm receiving and verification (without videos or pictures). ◦ Configuration and application of alarm handling flows. ◦ Web Client & Control Client. ◦ 12-month maintenance service and 24/7 emergency support for critical faults. • **Visualized alarms:** ◦ Pop-up window for alarm videos and fast alarm verification. ◦ Alarm verification with details including captured pictures, live videos, and recorded videos. ◦ Quick live view and playback of all cameras of the alarm source location. ◦ Video monitoring module. ◦ Smart wall configuration and application. • **Virtual guard:** Management of scheduled virtual guard tours. • **Work order system:** Online work order system to assign and manage work orders and get device installation & maintenance support from installers. • **Operational enhancement:** Alarm statistics reports and alarm handling efficiency reports.

Overall Instructions for Service Providers to Provide HikCentral ReGuard Services

Role / Platform	Description	Related Topics
Service Providers (Installers, etc.) on Hik-Partner Pro	1. Purchase HCRG services and and generate an HCRG key on Hik-Partner Pro. 2. Give the HCRG key to customer for HCRG activation. 3. Receive the installation work orders from customers' HCRG, and go to the sites to	• ***Step 1: Get HikCentral ReGuard Services*** • ***Step 2: Generate HikCentral ReGuard Key for HCRG Activation*** • ***(Optional) Step 3: Receive and Handle Work Orders*** • ***Step 4: Manage HikCentral ReGuard Services***

Role / Platform	Description	Related Topics
	install devices and hand over to HCRG.	
Customers (i.e., Remote Monitoring Centers) on HikCentral ReGuard	1. Use the HCRG key given by the service provider to log in to HCRG and activate the services. 2. Create installation work orders and assign to service providers (installers). 3. Accept devices and use the services in HCRG.	• ***HikCentral ReGuard Web Client User Manual*** • ***HikCentral ReGuard Control Client User Manual***

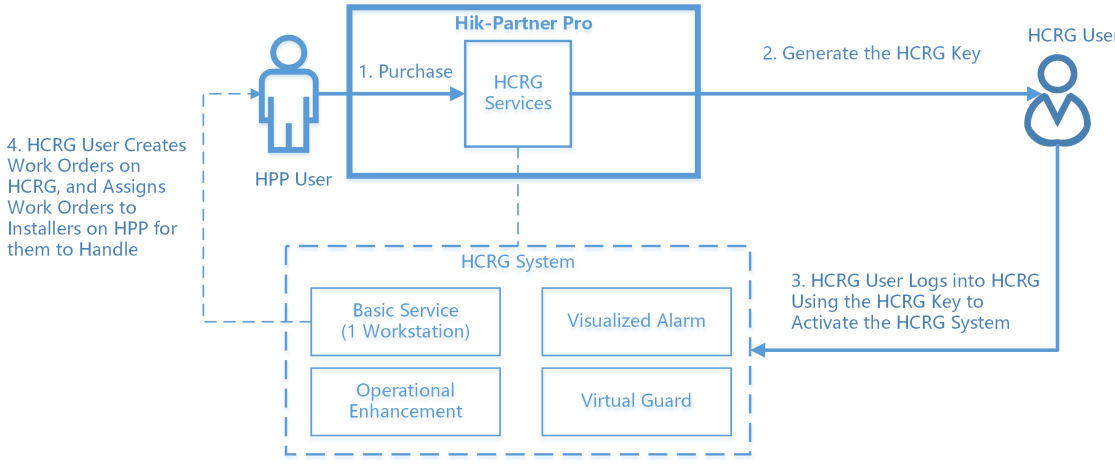


Figure 6-23 How HCRG Services Are Used

6.7.1 Step 1: Get HikCentral ReGuard Services

You can purchase a service key from the local distributor first and then activate by the service key to get the purchased services.

Get Services by Service Key Using the Portal

1. Contact your local distributor and purchase a service key from them.
2. Go to **Site & Device → Service Market** .
3. In the HikCentral ReGuard Services area, click **Activate by Service Key**.
4. In the **Service Key** field, enter the service key.
5. Click **OK**.

6.7.2 Step 2: Generate HikCentral ReGuard Key for HCRG Activation

After you get the HCRG services by service key, you can generate an HCRG key for activating the HCRG system. Users can use your HCRG key to activate the HCRG services.

Generate the HikCentral ReGuard Key Using the Portal

1. Go to **Site & Device → Service → My Service → HikCentral ReGuard Service** .

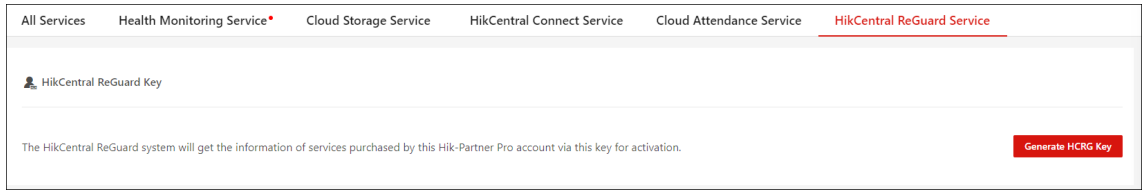


Figure 6-24 HikCentral ReGuard Service

2. Click **Generate**. The key will appear on this page and be sent to the email of Installer Admin.
3. Enter the key on HCRG to activate the services.

6.7.3 (Optional) Step 3: Receive and Handle Work Orders

If your customer (RMC) assign work orders to your company, all installers with the Manage All/ Assigned Site permission can receive the notifications, and can choose whether to handle the work orders.

Receive and Handle Work Orders Using the Mobile Client

1. Go to **Me →**  **→ Site Message** .
2. Find the work order and tap **Handle New**.
3. Go to the site, and install and configure the devices. After you complete, tap **submit** to submit the work order and hand over the devices to your customer's HCRG.

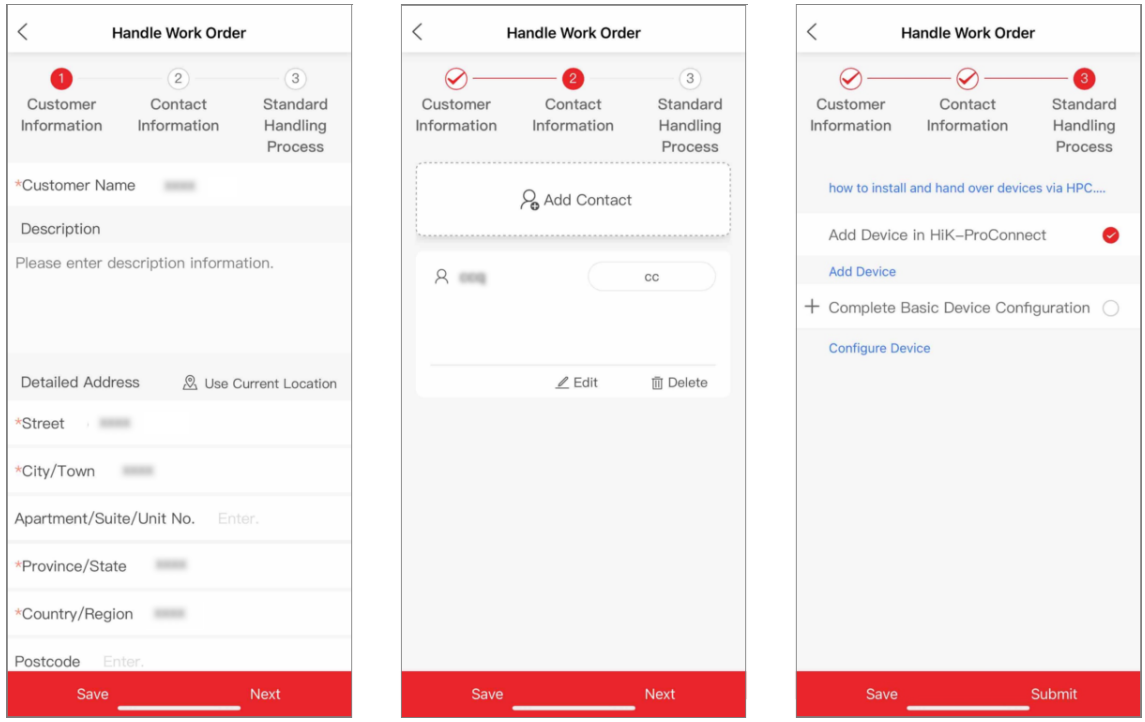


Figure 6-25 Handle a Work Order on the Mobile Client

6.7.4 Step 4: Manage HikCentral ReGuard Services

After purchasing and activating HCRG services, you can monitor the real-time status of HCRG services on Hik-Partner Pro, including the total number of valid workstations, the number of valid additional services, the number of services expiring within 30 days, and the number of expired services.

Manage HikCentral ReGuard Services Using the Portal

Go to **Site & Device → Service → My Service → Health Monitoring Service** .

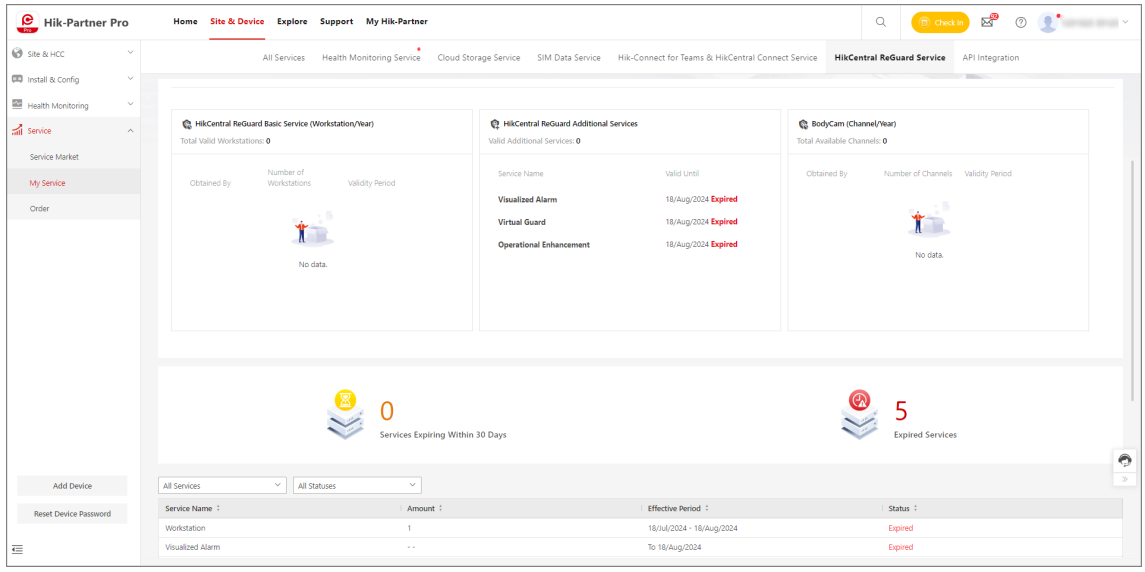


Figure 6-26 Manage HikCentral ReGuard Services Using the Portal

Chapter 7 Get Support & Incentives to Stay Connected with Hikvision

Hik-Partner Pro provides various features to help partners to get professional support and incentives for their businesses.

Features	Description	Related Roles
Online Support Cases	If you have any issues related to hardware, software, device password reset, etc., you can get professional help from our technical support via Online Support Case.	All
Return Material Authorization (RMA)	Return material authorization (RMA) is an arrangement in which installers can ship defected products back to distributors for an exchange or repair.	• Installer • Distributor
Partner Programs	Partner programs are rebate and incentive programs that encourage resellers (DPPs) to sell products by offering rebates. Three parties are involved here: Hikvision, reseller (DPP), and distributor.	• Reseller (DPP) • Distributor
Commissions	Distributors/resellers can earn commissions from successfully promoting value-added services of Hik-Partner Pro to their customers (e.g., installers). For installers, they can also get some discounts on purchasing the services.	• Distributor/Reseller
Compensations	For distributors who keep a supply of products from Hikvision at a fixed price in advance, but later sell products	• Distributor

Features	Description	Related Roles
	at a lower price due to getting project support, you may apply for compensation online.	
Reward Points	Hik-Partner Pro provides a reward point system to reward your trust and support.	• All
eCoupons	The eCoupons (quota eCoupons, cash eCoupons, and ratio eCoupons) can be used by buyers to get discounts when they purchase products.	• Installer or Other Buyers • Reseller, Distributor, or Other Providers
Sell-Out Promotions	Sell-out promotions are activities that offer buyers discounts or free products when discount conditions are met.	• Installer or Other Buyers • Reseller, Distributor, or Other Providers

7.1 How to Submit Online Support Cases to Get Help from Hikvision

If you have any issues related to hardware, software, device password reset, etc., you can get professional help from our technical support via Online Support Case. You can submit cases to report your issues to us and follow up on the cases you submit.

Note

- This feature is only available for some countries and regions.
- You can use this feature only if your company is authenticated. Refer to ***Authenticate Company to Use More Features*** .

Table 7-1 Case Types

Case Type	Description	Required Info	Where to Submit
Hardware Products	For issues related to device operations,	• Device Serial No. • Firmware Version • Issue Description	Portal / Mobile Client

Case Type	Description	Required Info	Where to Submit
	configurations, or faults.		
Software Products	For issues related to Hik-Connect and iVMS-4200.	• Software Name • Software Version • Issue Description	Portal / Mobile Client
Hik-Partner Pro	For issues related to Hik-Partner Pro • Account Management • Health Monitoring • Site Management • Cloud Storage • Co-Branding • Code Scanning and Reward Point Market • Solution and Projects • Others	• Issue Description • After-Sales Authorization Code Required when it is necessary for technical support to use the code to log in to your account for troubleshooting.	Portal / Mobile Client
Device Password Reset	Submit cases to reset device passwords according to the replies from the support team.	• Device Serial No. • Device Label / Invoice Upload label pictures or invoice files. • Password Reset QR Code / String from SADP Scan QR code or enter manually.	Mobile Client
Device Unbinding	Submit cases to unbind your devices from Hik-Connect according to the replies from the support team.	• Network Status (LAN device or not.) Serial No. and QR code / string from SADP are auto filled for LAN devices. • Device Serial No. • Device Label / Invoice	Mobile Client

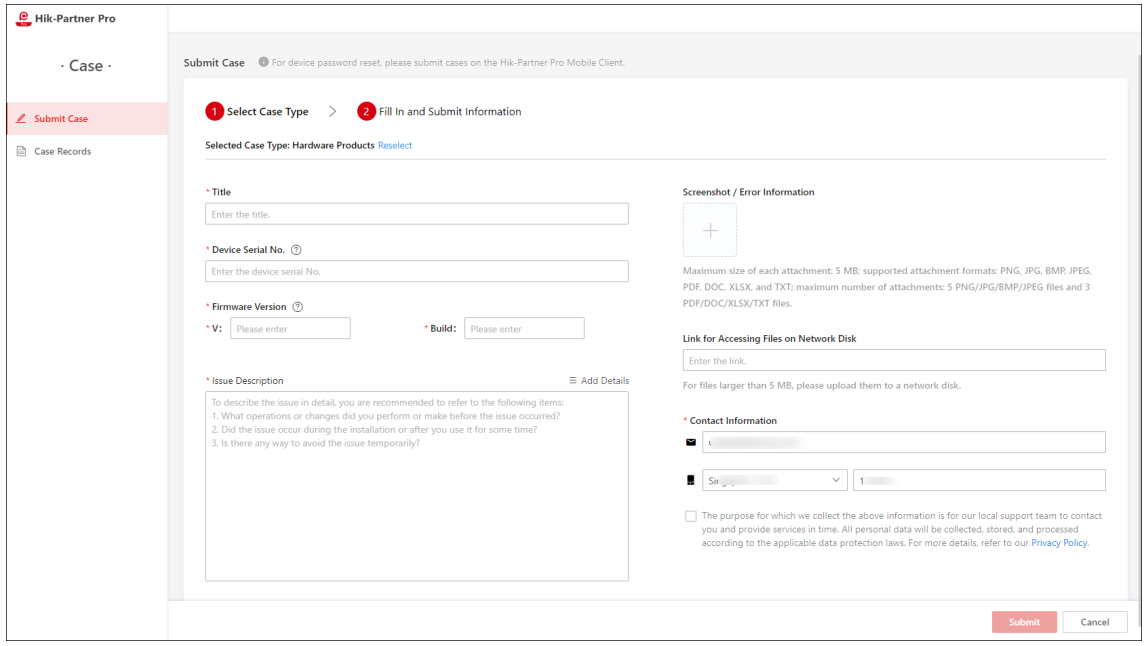
Case Type	Description	Required Info	Where to Submit
		Upload label pictures or invoice files. • Password Reset QR Code / String from SADP Scan/enter the QR code / string provided by SADP.	
Dedicated Customer Service	Only available for some installers, for focused troubleshooting from technical support.	• Language • Case Severity **Critical Business Down** Main functions which are critical to your business, such as logging in to the platform, creating sites, adding devices, receiving alarms, and handing over sites, are unavailable. **Business Impaired** Main functions work properly, but there are other function-related issues such as batch LAN configuration not working, probabilistic failure of remote configuration, and connection failure of some devices.	Portal / Mobile Client

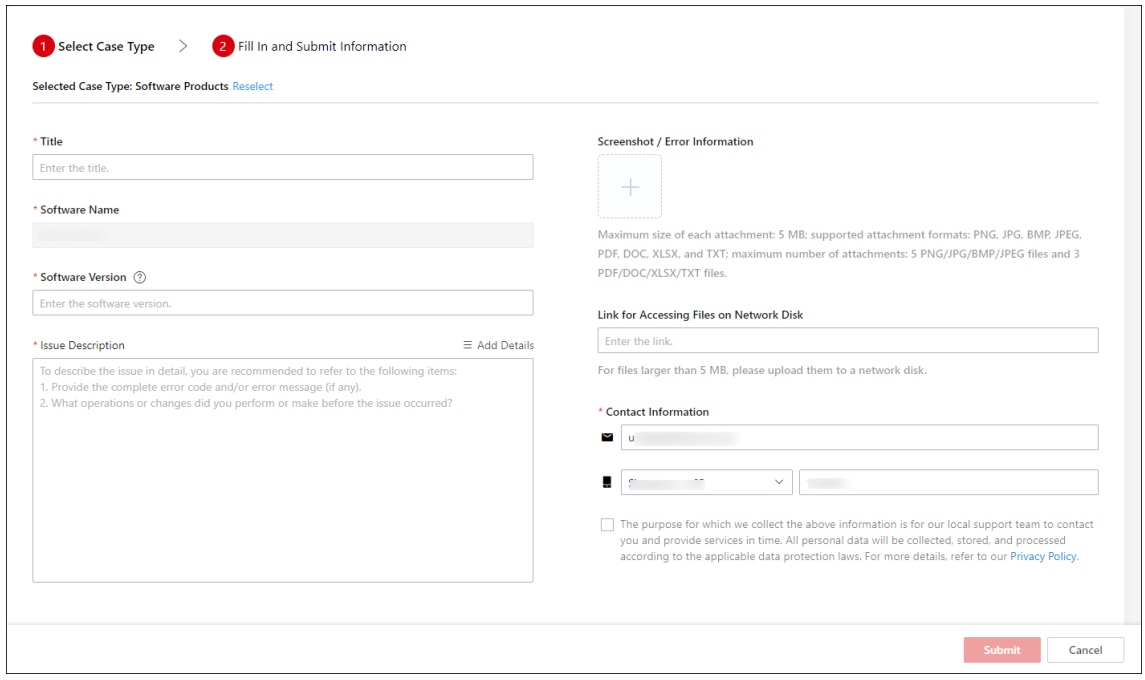
Case Type	Description	Required Info	Where to Submit
		Functional Defects There are some functional defects which do not affect your business or only affect your business slightly, such as wrong words on the page and high response latency. • Issue Description	

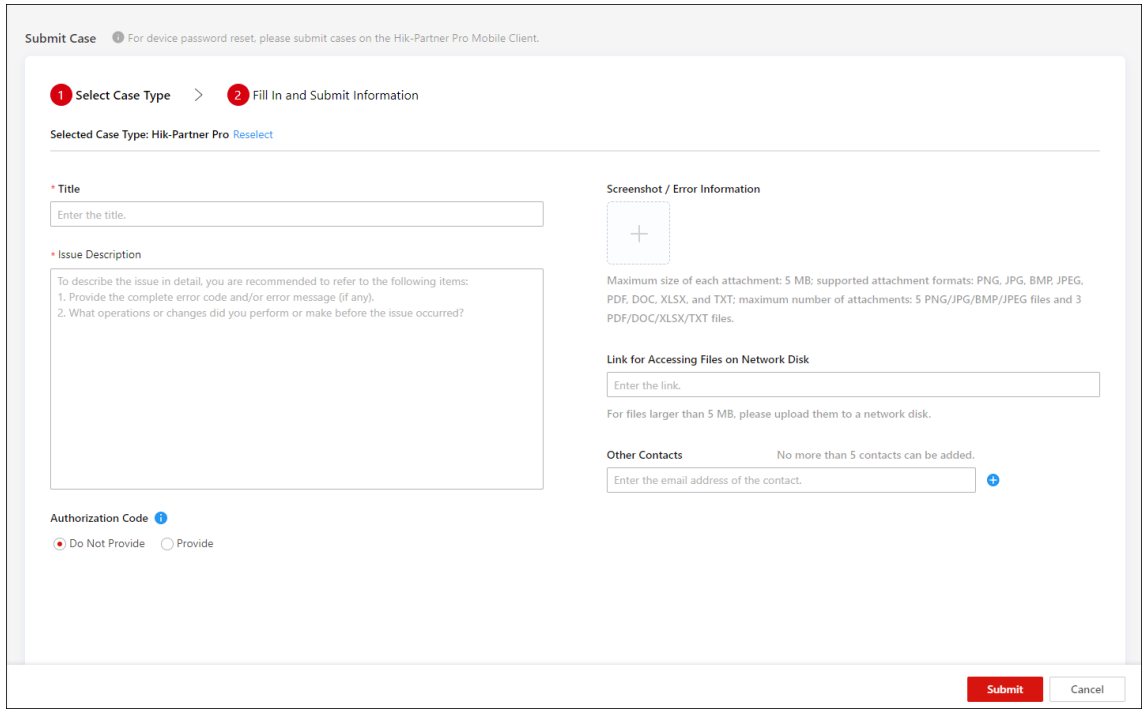
7.1.1 Submit and Track Online Support Cases

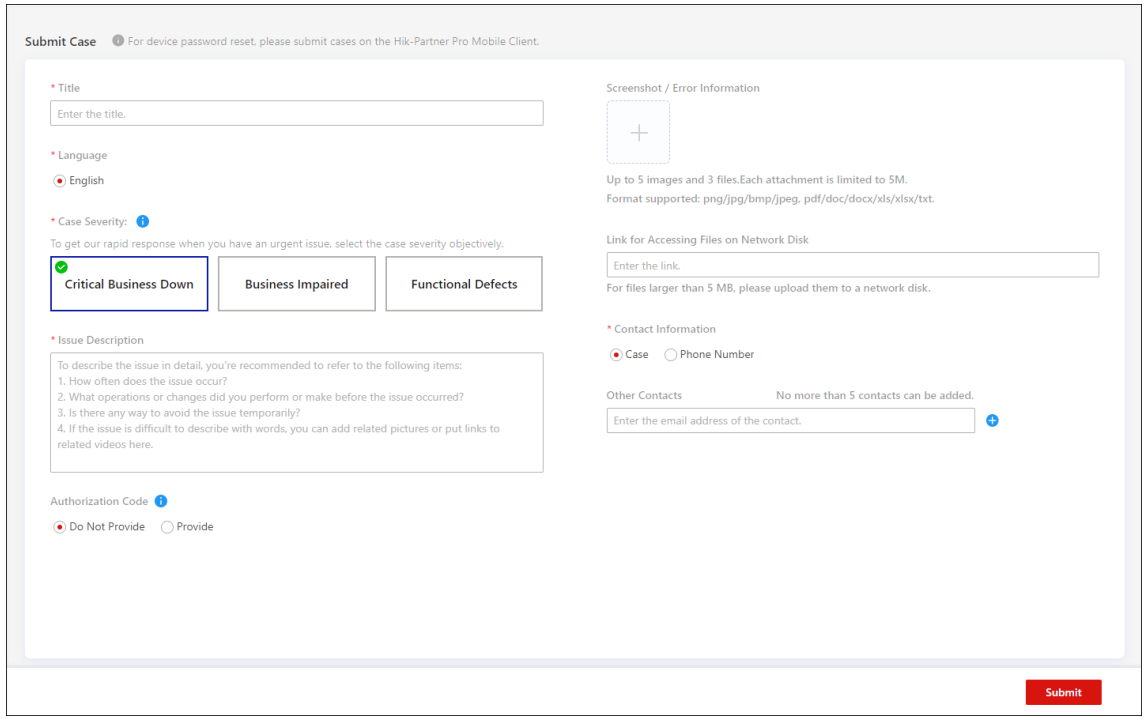
Submit and Track Online Support Cases Using the Portal

1. Access the Online Support Case module. Choose from:
   - Click **Support → Case** .
   - Click **Case** on the right side of the Home page.
   - Click → floating on the bottom right.
2. Click **Submit Case**.
3. Select a case type, and enter required information.


Hik-Partner Pro
· Case ·
Submit Case
Case Records
Submit Case
For device password reset, please submit cases on the Hik-Partner Pro Mobile Client.
1 Select Case Type
2 Fill In and Submit Information
Selected Case Type: Hardware Products Reselect
* Title
Enter the title.
* Device Serial No.
Enter the device serial No.
* Firmware Version
* V:
Please enter
* Build:
Please enter
* Issue Description
Add Details
To describe the issue in detail, you are recommended to refer to the following items:
1. What operations or changes did you perform or make before the issue occurred?
2. Did the issue occur during the installation or after you use it for some time?
3. Is there any way to avoid the issue temporarily?
Screenshot / Error Information
Maximum size of each attachment: 5 MB; supported attachment formats: PNG, JPG, BMP, JPEG, PDF, DOC, XLSX, and TXT; maximum number of attachments: 5 PNG/JPG/BMP/JPEG files and 3 PDF/DOC/XLSX/TXT files.
Link for Accessing Files on Network Disk
Enter the link.
For files larger than 5 MB, please upload them to a network disk.
* Contact Information
The purpose for which we collect the above information is for our local support team to contact you and provide services in time. All personal data will be collected, stored, and processed according to the applicable data protection laws. For more details, refer to our Privacy Policy.
Submit
Cancel


1 Select Case Type
2 Fill In and Submit Information
Selected Case Type: Software Products Reselect
* Title
Enter the title.
* Software Name
* Software Version
Enter the software version.
* Issue Description
Add Details
To describe the issue in detail, you are recommended to refer to the following items:
1. Provide the complete error code and/or error message (if any).
2. What operations or changes did you perform or make before the issue occurred?
Screenshot / Error Information
Maximum size of each attachment: 5 MB; supported attachment formats: PNG, JPG, BMP, JPEG, PDF, DOC, XLSX, and TXT; maximum number of attachments: 5 PNG/JPG/BMP/JPEG files and 3 PDF/DOC/XLSX/TXT files.
Link for Accessing Files on Network Disk
Enter the link.
For files larger than 5 MB, please upload them to a network disk.
* Contact Information
The purpose for which we collect the above information is for our local support team to contact you and provide services in time. All personal data will be collected, stored, and processed according to the applicable data protection laws. For more details, refer to our Privacy Policy.
Submit
Cancel





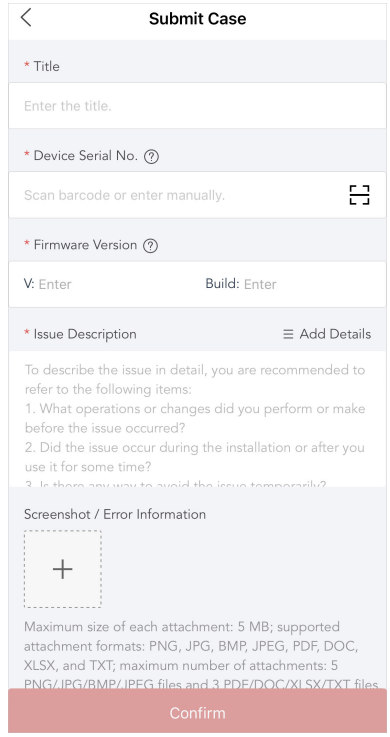
4. Click **Submit** to submit the case.
5. Go to **Case Records** to track all your submitted cases. You can track the replies from technical support, reply to them to provide more info, and close the cases if the issues are solved.

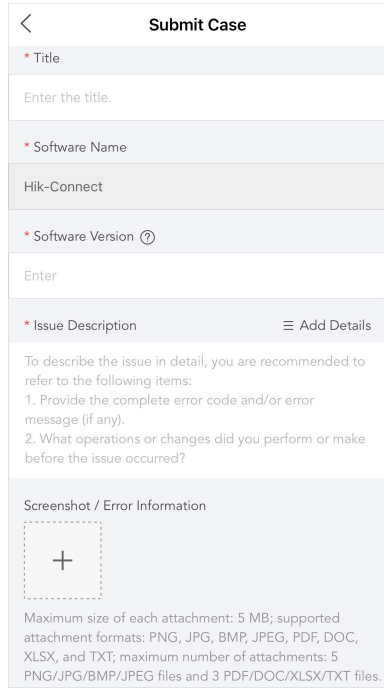
Note

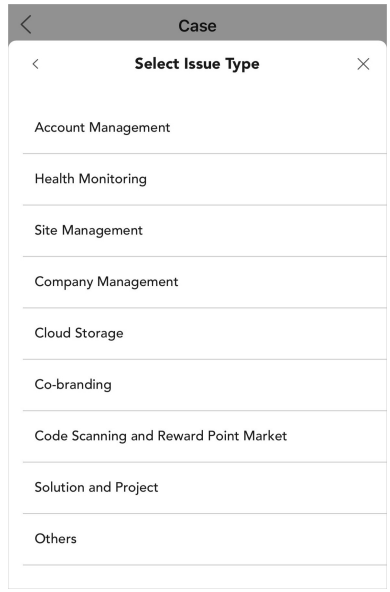
The case will be closed automatically if you do not reply within 14 days.

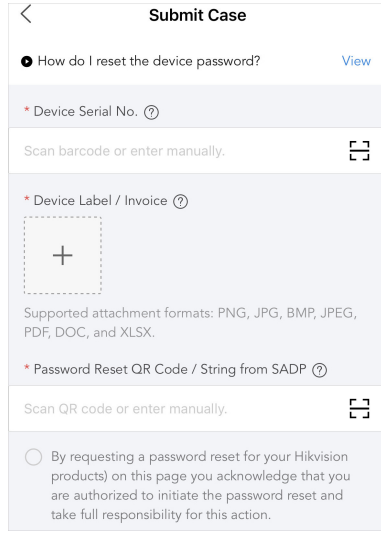
Submit and Track Online Support Cases Using the Mobile Client

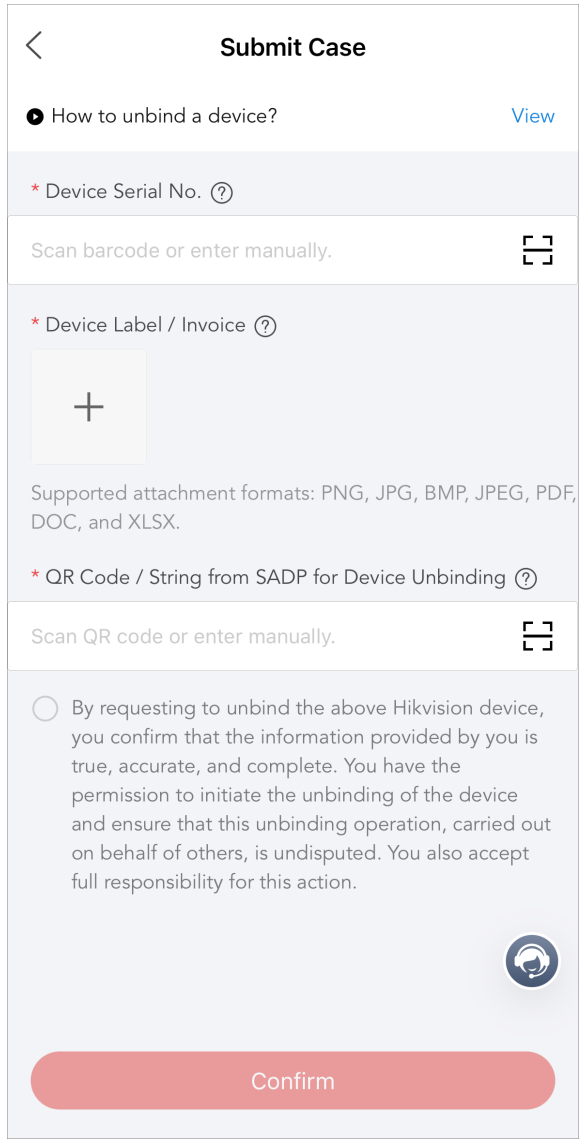
1. Access the Online Support Case module. Choose from:
   - Tap **Me → (at the top right) → Case** .
   - Tap **Home → More → Support → Case** .
   - Tap **(floating on the Mobile Client) → Support → Case** .
2. Tap **New Case**.
3. Select a case type, and enter required information.




Submit Case
* Title
Enter the title.
* Software Name
Hik-Connect
* Software Version
Enter
* Issue Description
Add Details
To describe the issue in detail, you are recommended to refer to the following items:
1. Provide the complete error code and/or error message (if any).
2. What operations or changes did you perform or make before the issue occurred?
Screenshot / Error Information
Maximum size of each attachment: 5 MB; supported attachment formats: PNG, JPG, BMP, JPEG, PDF, DOC, XLSX, and TXT; maximum number of attachments: 5 PNG/JPG/BMP/JPEG files and 3 PDF/DOC/XLSX/TXT files.


Case
Select Issue Type
Account Management
Health Monitoring
Site Management
Company Management
Cloud Storage
Co-branding
Code Scanning and Reward Point Market
Solution and Project
Others


Submit Case
How do I reset the device password?
View
* Device Serial No.
Scan barcode or enter manually.
* Device Label / Invoice
Supported attachment formats: PNG, JPG, BMP, JPEG, PDF, DOC, and XLSX.
* Password Reset QR Code / String from SADP
Scan QR code or enter manually.
By requesting a password reset for your Hikvision products) on this page you acknowledge that you are authorized to initiate the password reset and take full responsibility for this action.



4. Tap **Confirm** to submit the case.
5. On the case list, you can track all your submitted cases. You can track the replies from technical support, reply to them to provide more info, and close the cases if the issues are solved.

Note

The case will be closed automatically if you do not reply within 14 days.

7.2 How to Return Defected Products for Exchange or Repair (RMA)

Return material authorization (RMA) is an arrangement in which you can ship an item back for an exchange or repair due to a product defect or malfunction.

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

Your Role	Description	Related Topics
Installer	1. Submit RMA requests. 2. Send the defected products to the distributor. 3. Receive the repaired and debugged products.	• ***Submit RMA Requests*** • ***Track RMA Requests*** • ***Find Repair Stations***
Distributor	1. Repair the defected products after receiving RMA requests. 2. Return the repaired and debugged products.	/

7.2.1 Submit RMA Requests

You can register an RMA request for exchanging or repairing products. After registration, you can check real-time status of the RMA requests.

Submit RMA Requests Using the Portal

1. Go to **Support → RMA** .
2. Click **Add** to add products, and choose from:
   - Input the serial number of the products of interest, click **Add**, and enter fault description and reference. Click **Add Attachment** to add attachments if there are any.
   - Click **Download Template**, enter information of multiple products, and click **Upload Serial List** to batch upload products.

   Note

   It should be a Hikvision product sold in the current country or region.
3. After all products are added, click **Next** to set shipping information.
4. Set shipping information. The distributor is identified and auto-selected according to the product serial number, and the nearest repair station will be selected by default. The distributor and product info will show up in the list.
   If the distributor is not auto-identified:

Whether Your Country/Region Supports Trans-distributor Repair or Not	Description
Yes	- Click **Change Shipping Address** to choose a distributor by yourself. - You can also select among all stations of all distributors in the country.
No	The product cannot be added.

5. Check the information in the list, and click **Submit**.

Submit RMA Requests Using the Mobile Client

1. Tap **Me → (at the top right) → RMA** , or tap **Home → More → Support → RMA** .
2. Tap **Repair Request → +Add** , and enter the product serial No. or scan the product QR code to start the application.

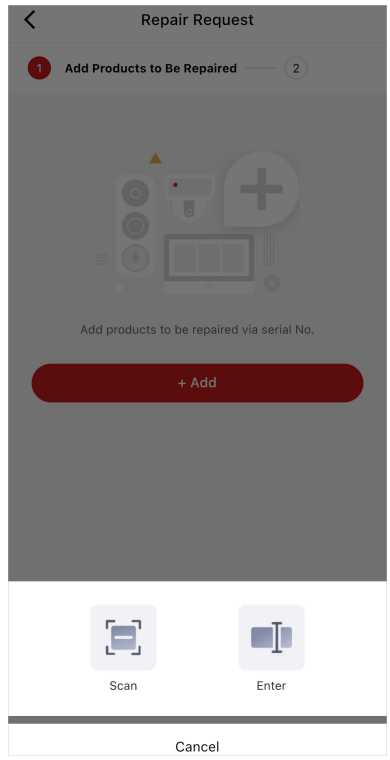


Figure 7-1 Add Products to Be Repaired

Note

It should be a Hikvision product sold in the current country or region.

3. Set shipping information. The distributor is identified and auto-selected according to the product serial number, and the nearest repair station will be selected by default. The distributor and product info will show up in the list.

If the distributor is not auto-identified:

Whether Your Country/Region Supports Trans-distributor Repair or Not	Description
Yes	- Tap to choose a distributor by yourself. - You can also select among all stations of all distributors in the country.
No	The product cannot be added.

4. If there are more devices to be repaired, tap **+Add** to add more devices, or you can tap **Confirm** to enter shipping information.
5. Tap **Add a New Address** to add a new shipping address or select an existing address, then tap **Submit**, and the status of the RMA request will turn to Requested.

Shipping Method	Description
Shipping Carrier	Tap **Ship to Distributor** to enter the shipping carrier and shipping order No.
By Myself	Confirm that the product is shipped, and then the status of the RMA request will turn to Shipped to Distributor.

7.2.2 Track RMA Requests

After an RMA request is submitted, you can track its status and perform further operations.

Track RMA Requests Using the Portal

Go to **Support → RMA** .

Operation	Description
Filter by Status	Click , and select among Saved, Unreceived, In Repair, Waiting For Customer Response, Ready for Shipment, and Completed.
View Details	Click **Detail** to view application details.
Download Document	Click **Download Document** to download the application file.

Track RMA Requests Using the Mobile Client

Tap **Me → (at the top right) → RMA** or tap **Home → More → Support → RMA** .

Note

- When the status is Requested:
  - If you select shipping carrier as the shipping method, you need to tap **Ship to Distributor** to enter shipping information (including shipping Carrier or shipping order No.).
  - If you select ship by myself as the shipping method, confirm that you have shipped the product.
  - You can tap **Cancel Request** to cancel the request.
- If the status is Repaired & Shipped, you can tap **Complete** to finish the request.

Operation	Description
Filter by Status	Tap **Filter** to filter requests by their status and time.
View Details	Tap an application to view details. Each to-be-repaired product has an RMA number.
Handle Requests Based on Their Status	**Requested** • If the shipping method is shipping carrier, tap **Ship to Distributor** to enter shipping information (including shipping Carrier or shipping order No.). • If the shipping method is by myself, confirm that you have shipped the product. • Tap **Cancel Request** to cancel the request. **Repaired & Shipped** Tap **Complete** to finish the request.

7.2.3 Find Repair Stations

You can view repair stations and their distances from you on the map, so you can choose which repair station you want to ship your products to.

Find Repair Stations Using the Mobile Client

1. Tap **Me → (at the top right) → RMA** , or tap **Home → More → Support → RMA** .
2. Tap **Repair Station Query**.
3. - On the map, your location and nearby repair stations are displayed.
   - In the list, the available repair stations are displayed according to their distances from your location.
   - The information about repair stations includes the station name, contributor name, station address, distance from you location to the station, and station phone number (Tap or tap **Make a Call** on the details page to make a phone call to the station staff for asking more information.)

7.3 How to Join Partner Programs

Partner programs are rebate and incentive programs that help resellers (DPPs) grow their businesses and encourage resellers to sell products, and rebates will be offered to resellers on their achieving the sales targets.

Note

- Contract agreements of partner programs where sales targets are set need to be signed by three parties (the reseller, distributor, and Hikvision).
- This function is not supported by some accounts or in some countries/regions.

Your Role	Description	Related Topics
Reseller (DPP)	1. Apply for partner programs, and make sure the contract agreements are signed by Hikvision either offline or online. 2. If your application is approved and your contract agreement is signed by all the three parties, you will get a program certificate. 3. Rebates will be offered to you on your achieving the sales targets.	• ***Resellers (DPPs) Submit Program Applications*** • ***Resellers (DPPs) Manage Certificates*** • ***Resellers (DPPs) Manage Programs***
Distributor	Manage and sign the program agreements on Hik-Partner Pro.	***Distributors Manage Agreements***

7.3.1 Resellers (DPPs) Submit Program Applications

As a reseller, you can apply for partner programs to get rebates on Hik-Partner Pro with the contract agreements signed either offline or online.

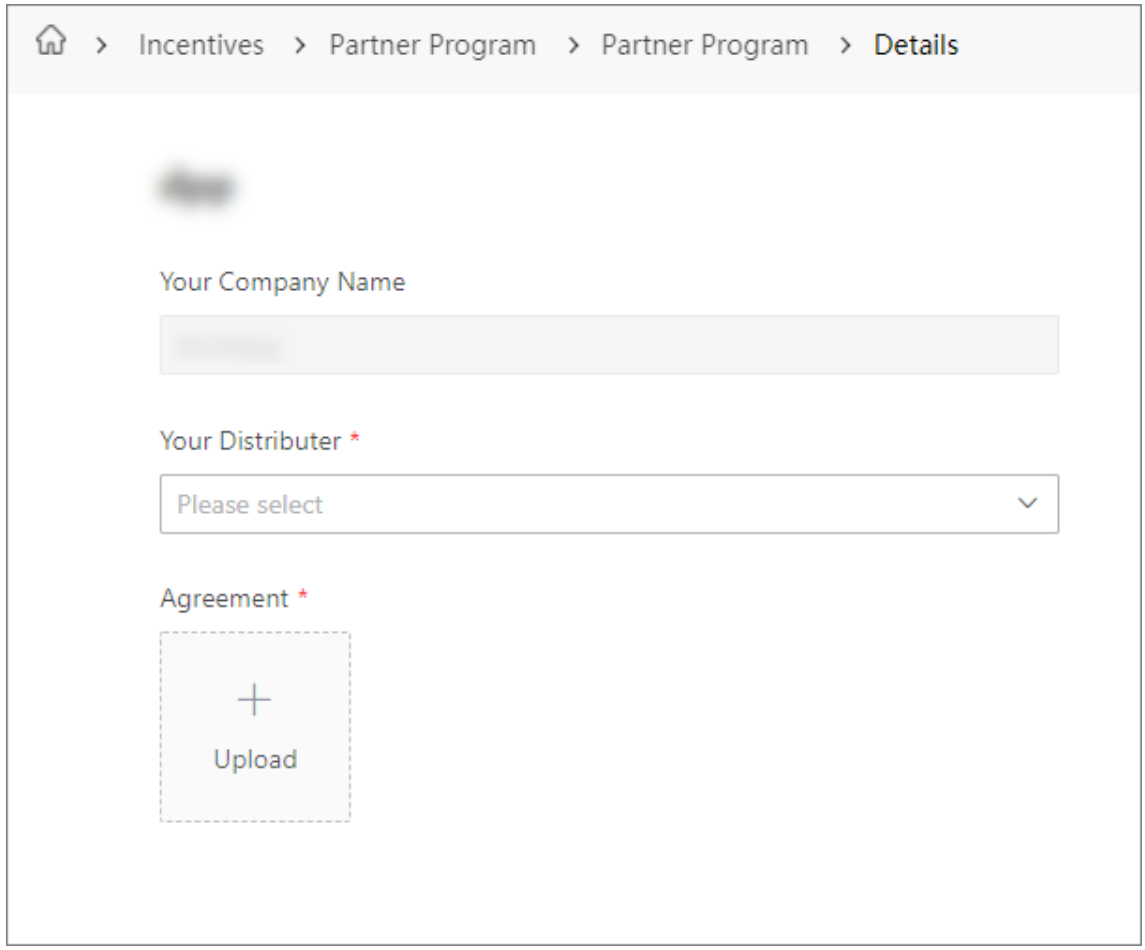
Submit Program Application Using the Portal

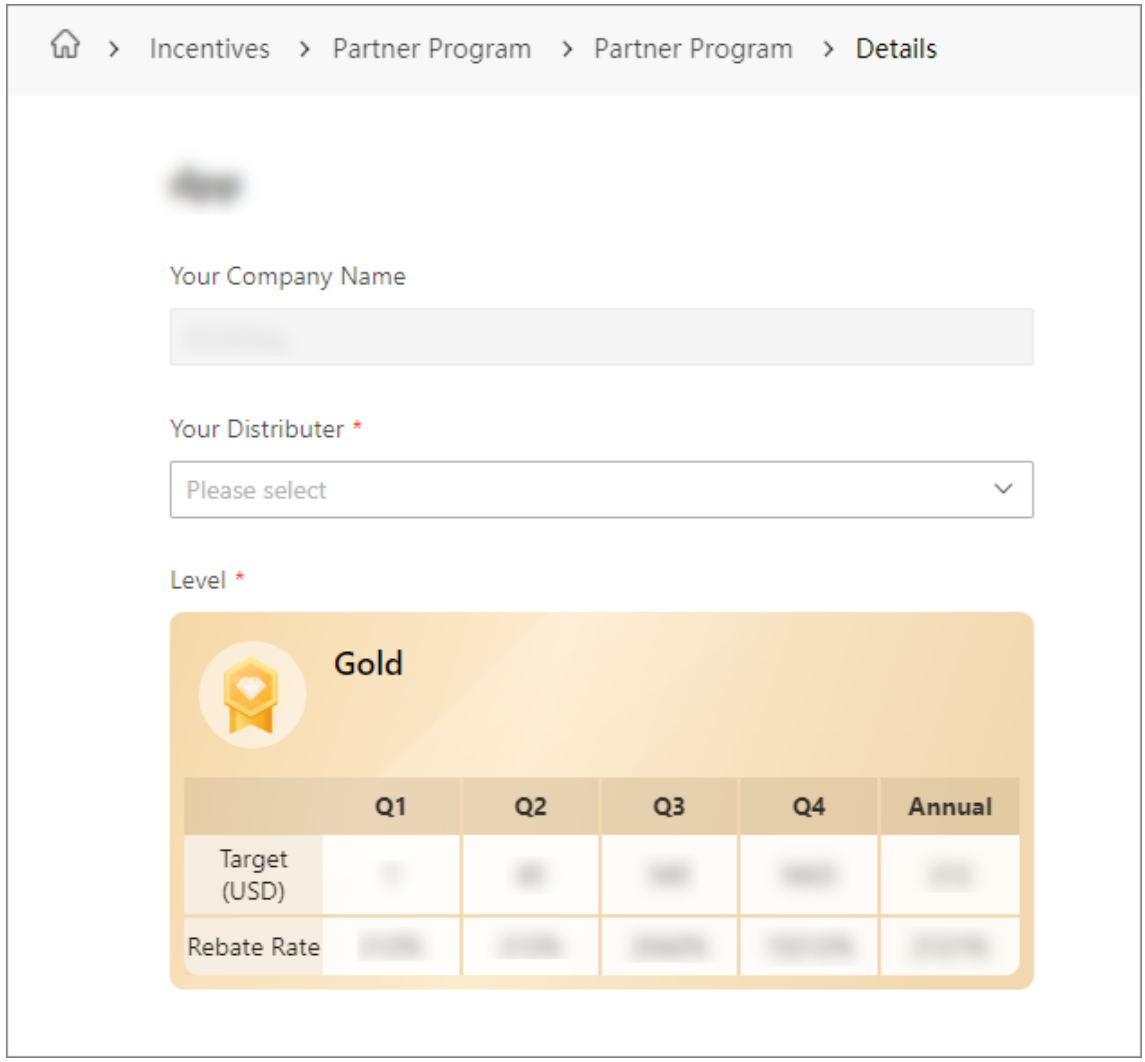
1. Go to **Incentive → Partner Program** , and click a program in the **Program Application** section.
2. Select your signing status in the pop-up window according to whether you have signed the agreement with Hikvision offline or not.
   The details and introduction about the partner program you are applying for will be shown.



Figure 7-2 Select Signing Status

3. Click **Next** to continue.
4. If you have signed the contract agreement with Hikvision offline, upload the signed contract agreement. If not, select the level you want to apply for.


Incentives
Partner Program
Partner Program
Details
Your Company Name
Your Distributer *
Please select
Agreement *
Upload



5. Click **Submit**.
6. If you have uploaded the signed agreement, the application process is completed after you click **Submit**. If not, you may enter one of the following processes:
   - If the level you select does not require you to communicate with Hikvision to confirm the targets offline, you will enter the Details page of the contract agreement. Check **I agree with and accept this agreement** and click **Submit** to submit the application.
   - If the level you select requires you to communicate with Hikvision to confirm the targets offline, choose one of the followings:
     - Communicate with the Hikvision sales representative offline, sign your contract agreement with them offline, and submit the application again online by yourself (you need to upload your signed contract agreement).
     - Communicate with the Hikvision sales representative offline, and they will initiate the signing process online for you. You need to sign the contract agreement online.

Submit Program Application Using the Mobile Client

1. Go to **Me → Partner Program** , and tap a program in the **Program Application** section.
2. Select your signing status in the pop-up window according to whether you have signed the agreement with Hikvision offline or not.
   The details and introduction about the partner program you are applying for will be shown.

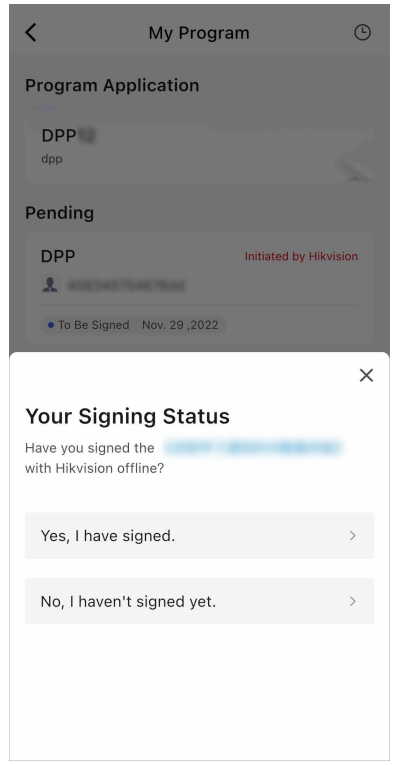
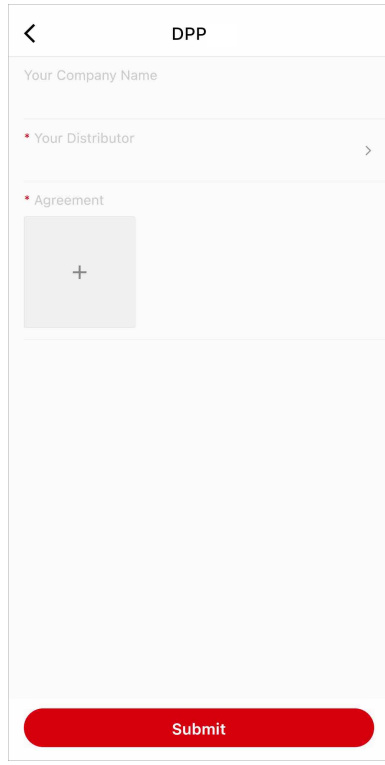
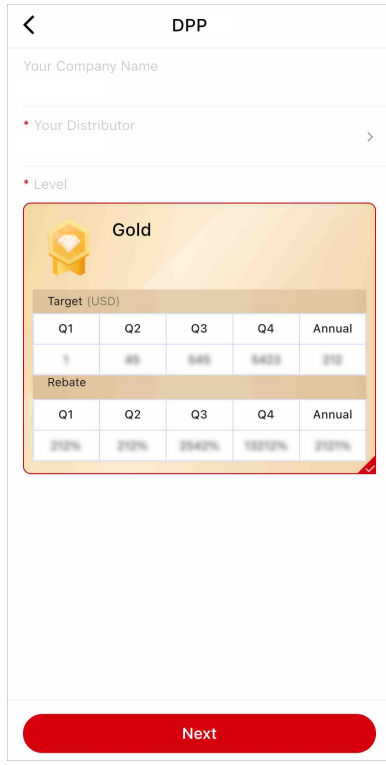


Figure 7-3 Select Signing Status

3. If you have signed the contract agreement with Hikvision offline, upload the signed contract agreement. If not, select the level you want to apply for.


DPP
Your Company Name
* Your Distributor
* Agreement
+
Submit


DPP
Your Company Name
* Your Distributor
* Level
Gold
Target (USD)
Q1
Q2
Q3
Q4
Annual
Rebate
Q1
Q2
Q3
Q4
Annual
Next

4. Tap **Submit** or **Next**.
5. If you have uploaded the signed agreement, the application process is completed after you tap **Submit**. If not, you may enter one of the following processes:
   - If the level you select does not require you to communicate with Hikvision to confirm the targets offline, you will enter the Details page of the contract agreement. Check **I agree with and accept this agreement** and tap **Next** to submit the application.
   - If the level you select requires you to communicate with Hikvision to confirm the targets offline, choose one of the followings:
     - Communicate with the Hikvision sales representative offline, sign your contract agreement with them offline, and submit the application again online by yourself (you need to upload your signed contract agreement).
     - Communicate with the Hikvision sales representative offline, and they will initiate the signing process online for you. You need to sign the contract agreement online.

7.3.2 Resellers (DPPs) Manage Certificates

As a reseller, after your program application is approved and the contract agreement is signed by all the three parties, the program certificate will be issued to you. You can view the details of all your certificates in My Certificate.

View Certificates Using the Portal

Go to **Incentive → Partner Program → My Certificate** .

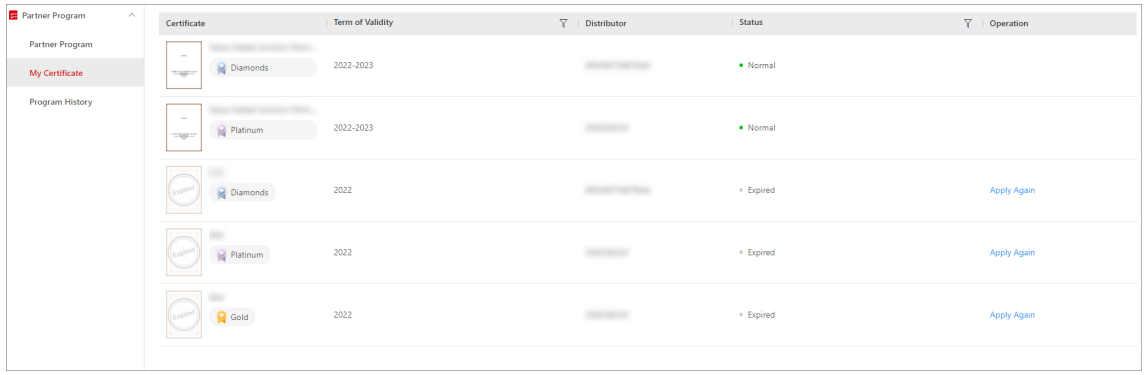


Figure 7-4 My Certificate

On the certificate list, you can view the program certificate name, certificate thumbnail, level, term of validity, distributor, and status (normal or expired).
Click **Apply Again** in the Operation column to apply for the partner program for which your certificate has expired.
Click the certificate thumbnail or name to enter the Certificate Details page. You can download the certificate and the contract agreement you signed on this page.

View Your Certificates Using the Mobile Client

Go to **Me → Partner Program** , you can swipe left and right to view the certificates in the My Certificate section, or tap **More** to enter the My Certificate page for more details and to perform more operations.

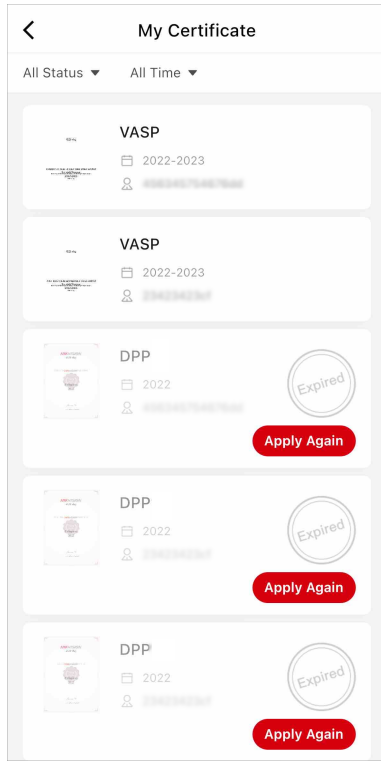


Figure 7-5 My Certificate

On the certificate list, you can view the program certificate name, certificate thumbnail, level, term of validity, distributor, and status (expired or not).
Tap **Apply Again** to apply for the partner program for which your certificate has expired.
Tap a certificate in the list to enter the Certificate Details page. You can download the contract agreement you signed on this page.

7.3.3 Resellers (DPPs) Manage Programs

As a reseller, after you submit your program application or if there are programs initiated by Hikvision for you, you can view all these programs in Program History.

Manage Programs Using the Portal

Go to **Incentive → Partner Program → Program History** .

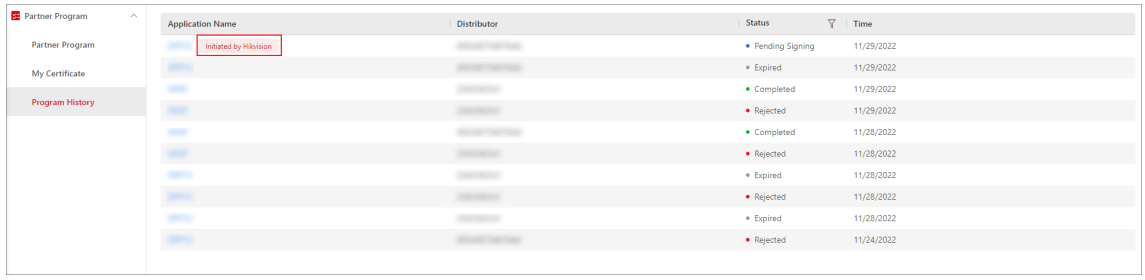


Figure 7-6 Program History

You can view the program name, application status (pending signing, completed, expired, and rejected), application time, and the distributor on the list.

Click an application record to enter the Details page. You can view the application status, program name, distributor name, level, and contract agreement.

For the program application of which the status is **Pending Signing**, click **Sign** on the right bottom of the Details page to sign the agreement online.

Manage Programs Using the Mobile Client

Go to **Me → Partner Program →** .

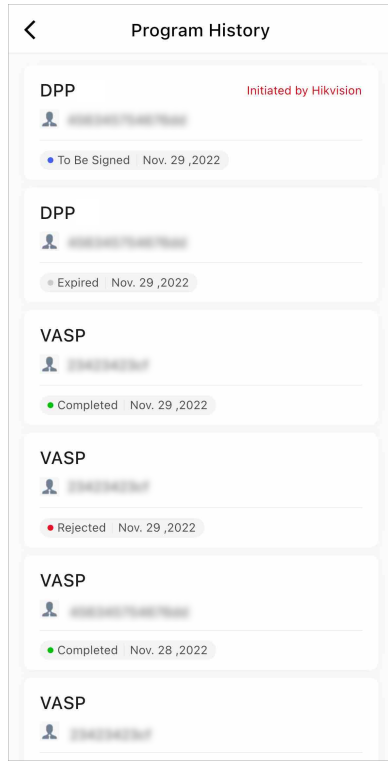


Figure 7-7 Program History

You can view the program name, application status (pending signing, completed, expired, and rejected), application time, and the distributor on the list.

Tap an application record to enter the details page of the program application. You can view the application status, program name, distributor name, level, and contract agreement.
For the program application of which the status is **Pending Signing**, tap **Sign** on the bottom of the details page to sign the agreement online.

7.3.4 Distributors Manage Agreements

As a distributor, you can manage and sign your contract agreements of partner programs with resellers and Hikvision on Hik-Partner Pro.

Manage Agreements Using the Portal

Go to **My Hik-Partner → Company Management → Agreement Management** .

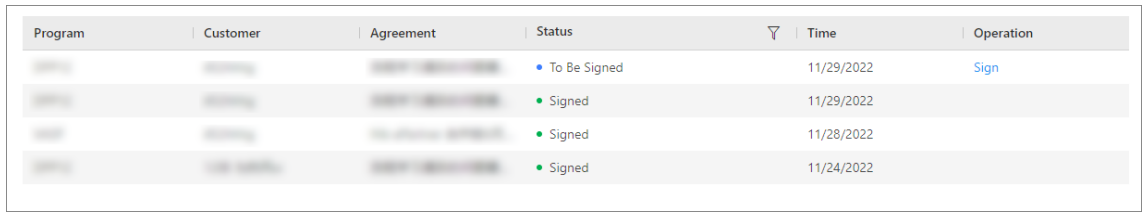


Figure 7-8 Agreement Management

You can view the program name, customer (i.e., reseller) name, agreement name, signing status (signed / to be signed), and the date when the signing process is initiated.
Click **Sign** to sign the contract agreement online.

Manage My Agreements Using the Mobile Client

Go to **Me → Agreement Management** to view your agreements.
You can view the program name, customer (i.e., reseller) name, agreement name, signing status (signed / to be signed), and the date when the signing process is initiated.
Tap **Sign** to sign the contract agreement online.

7.4 How to Earn Commissions as a Distributor/Reseller

For distributors/resellers, they can earn commissions from successfully promoting value-added services of Hik-Partner Pro to their customers (e.g., installers). For installers, they can also get some discounts on purchasing the services. Here we will introduce the process and the calculation method of earning commissions.

Note

This function is only available to some users in some countries/regions. For details, please contact Hikvision.

Example: Distributor/Resellers Earn Commissions

- Here we suppose that the price for 8 channels of 7-day annual event cloud storage is 360 EUR, which is only for reference. The actual prices on your page shall prevail.
- The discount for installers is not shown in the figure below.

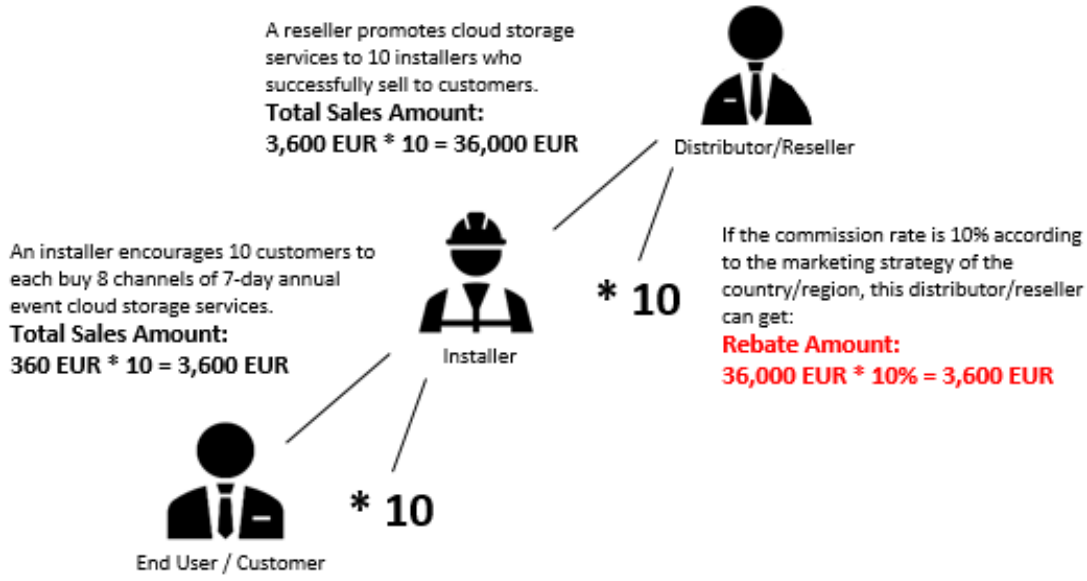


Figure 7-9 Example: Distributor/Resellers Earn Commissions

7.4.1 The Process of Earning Commissions

1. The distributor/reseller introduces and promotes the value-added services to installers when selling Hikvision devices.
   Value-added services include the health monitoring service, remote maintenance service, cloud storage service, cloud attendance service, employee account add-on, co-branding, cellular IoT data service, etc. The actual supported value-added services may vary according to your country/region.
2. The installer purchases services online via Hik-Partner Pro Portal / Mobile Client, and enters the **Distributor Invitation Code** (required for getting commissions) and the **Code from Hikvision Sales** (optional, and only for tracking sales performance).

Note

For distributors/resellers, you can get your **Distributor Invitation Code** via the Invite Friends task in the ***Rewards Store*** , and then ask the installer to enter it on the page of online purchase. The **Code from Hikvision Sales** can be any string created and given by the salesperson as long as it can represent this sales person for tracking their sales performance.

Note

Entering distributor invitation code is also supported on the Mobile Client. Due to UI similarity, here we only show the screenshot of the Portal.

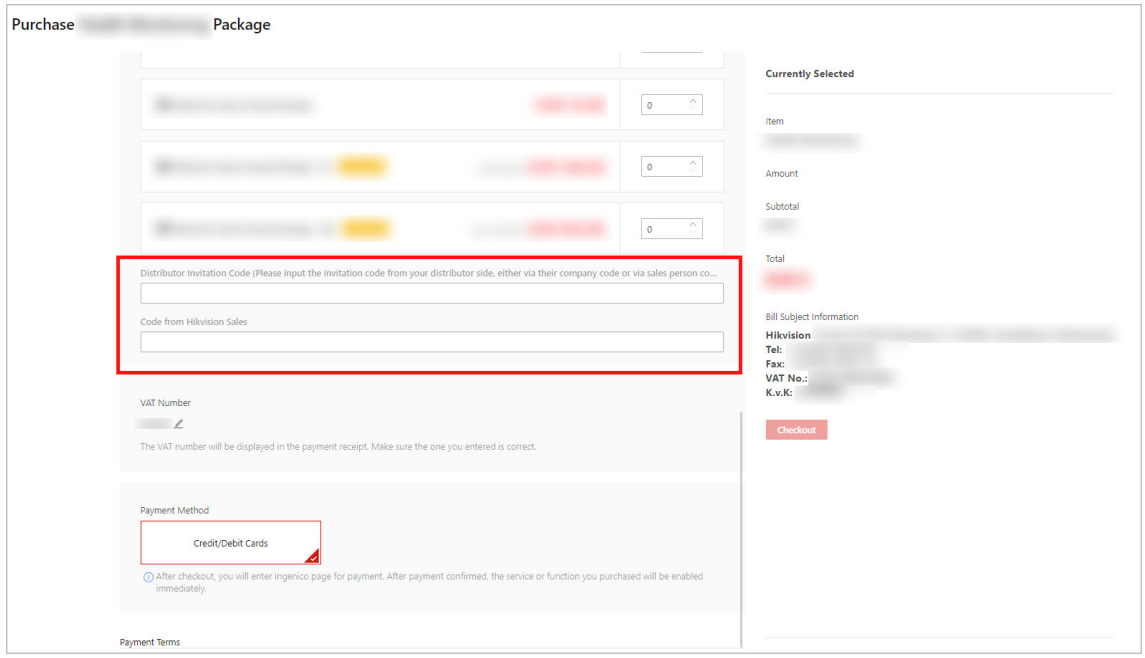


Figure 7-10 Enter Distributor Invitation Code Using the Portal

3. Hik-Partner Pro calculates the monthly commission amount based on the total sales amount of the distributor/reseller in the last month.

   Note

   The distributor/reseller can go to the Portal, and click **My Hik-Partner → Commission → Commission Settings** to view the calculation rules. Refer to ***The Way to Calculate Commission Amount*** for details.

4. The distributor/reseller gets the commission amount in the form of a credit note.

   Note

   The distributor/reseller can go to the Portal, and click **My Hik-Partner → Commission → Commission Details** to view information about the commissions they have earned. See ***View Commission Details Using the Portal*** for details.

7.4.2 The Way to Calculate Commission Amount

Go to the Hik-Partner Pro Portal, click **My Hik-Partner → Commission → Commission Settings** to view the calculation rules such as the commission rate.

Elements that Determine the Commission Amount

- **Total Sales Amount**
  The total sales amount of the orders linked to you via your distributor invitation code.
- **Commission Rate**
  The commission rate depends on the marketing strategy of the country/region.

Formula for Calculating the Commission Amount

Total Sales Amount in Previous Month × Commission Rate = Commission Amount for Previous Month

Note

The platform will calculate the commission amount of the previous month on a fixed day of each month.

7.4.3 View Commission Details Using the Portal

After distributors/resellers promote the value-added services to their customers (e.g., installers), they will earn a certain commission amount and they can view the details of their commissions.

Note

You can view the commissions of the current month after the calculation day of the next month. For example, if the calculation day is set to the 15th of each month, you can view the commissions of July on August 16th.

Go to **My Hik-Partner → Commission → Commission Details** .

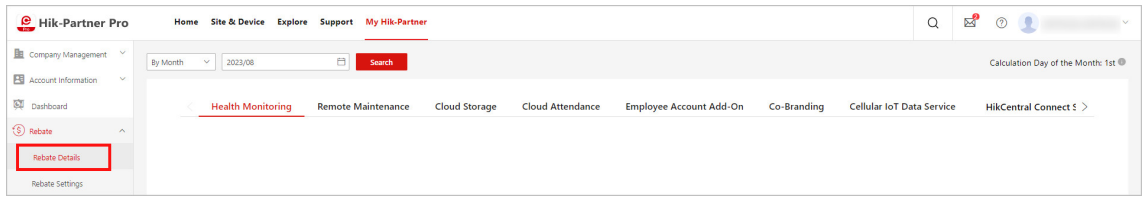


Figure 7-11 Commission Details

7.5 How to Apply for Compensation and Manage Applications

For distributors who keep a supply of products from Hikvision at a fixed price in advance, but later sell products at a lower price due to getting project support, you may apply for compensation online. After a compensation application is approved, the compensation amount may be issued to your e-wallet, or you may be compensated by credit notes against receivables or free items.

Note

- This feature is only available to authenticated channel partners.
- For details about projects, refer to .

7.5.1 Apply for Compensation Using the Portal

You can apply for compensation for projects that are either submitted by you or shared to you. Projects that support the submission of a compensation application should be in Closed Won status and the date of closing should be within three months.

1. Go to **Incentive → Compensation** , and select **Projects waiting for application**.

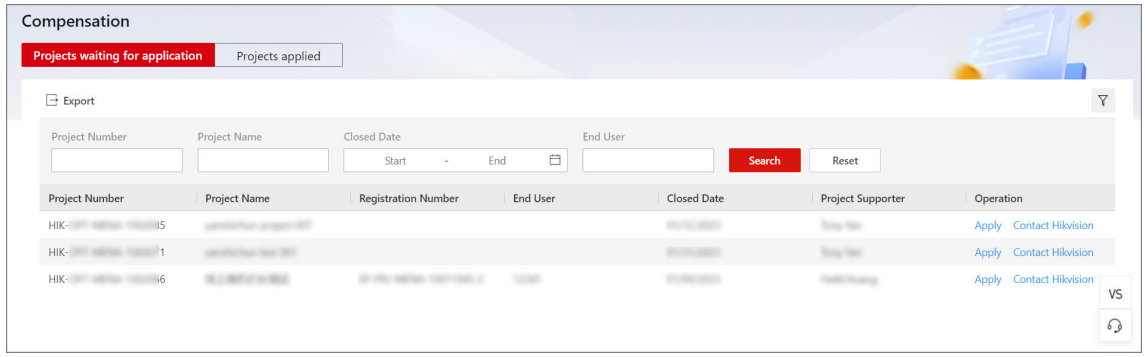


Figure 7-12 Projects Waiting for Compensation Application

2. (Optional) Click **Contact Hikvision** in the Operation column of a project to send an email to the project supporter (i.e., Hikvision sales representative), if you have any questions or there is something you would like to tell them before applying.
3. Click **Apply** in the Operation column of a project to enter the Input Price Information page.

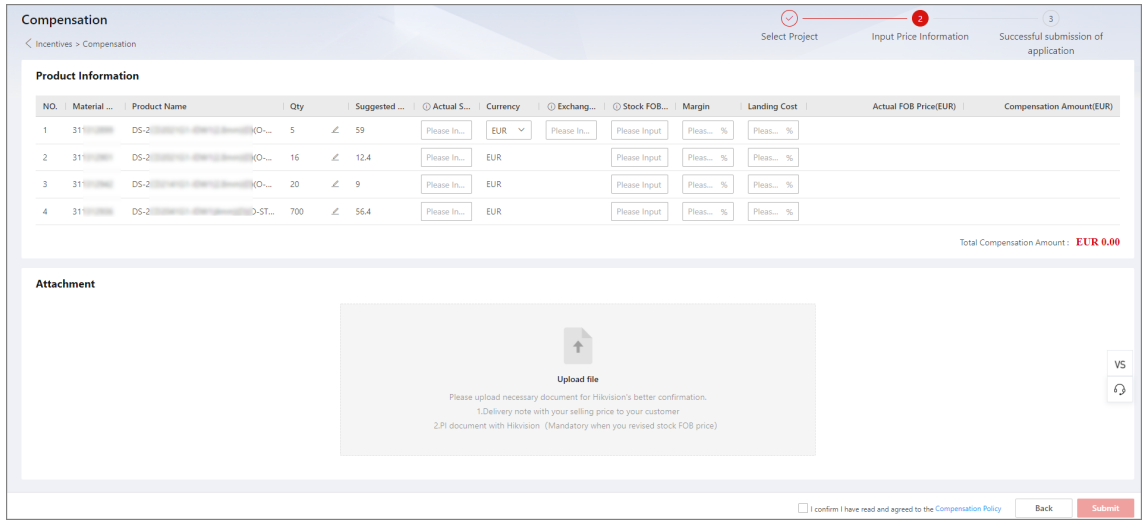


Figure 7-13 Compensation Application

4. In the Product Information field, enter or edit the following price related information accordingly for each product.

   Actual Sales Price

   If the currency of the actual transaction is different from that of the suggested sales price, enter this field according to your actual situation. Otherwise, the actual sales price should be the same as the suggested sales price.

   Currency

   Select the currency of the actual transaction.

   Exchange Rate

   If the currency of the actual transaction is different from that of the suggested sales price, enter the currency exchange rate at the time of the transaction.

   Note

   If the currencies are the same, exchange rate will be set to 1 and cannot be edited.

   Stock FOB Price

   Revise this field if you find a price displayed is incorrect.

   Margin

   Enter the handling fee of a transaction as a percentage (%).

   Landing Cost

   Enter the total landed cost for a product as a percentage (%).

5. (Optional) Upload the appropriate attachments (e.g., delivery notes with actual sales prices, PI documents, etc.) according to your actual situation to make it easier to get your application approved.

Note

If you have revised the stock FOB price for a product above, uploading a PI document is required here. Otherwise your application will be rejected.

6. Read the Compensation Policy, check the box for confirming policy agreement, and click **Submit**. A window will pop up for you to confirm the submission. After clicking **Confirm**, you will land on the successful submission page with relevant details of your application such as the application number, project number, and the total compensation amount.

Note

If your application fails to be submitted, please contact Hikvision. A failed submission will be saved in Draft status for you to edit and resubmit later.

7.5.2 Manage Submitted Compensation Applications Using the Portal

After you submit a compensation application, you can track the status of your application, edit draft and rejected applications for resubmission, and export all applications.

Go to **Incentive → Compensation** and select **Projects applied**.

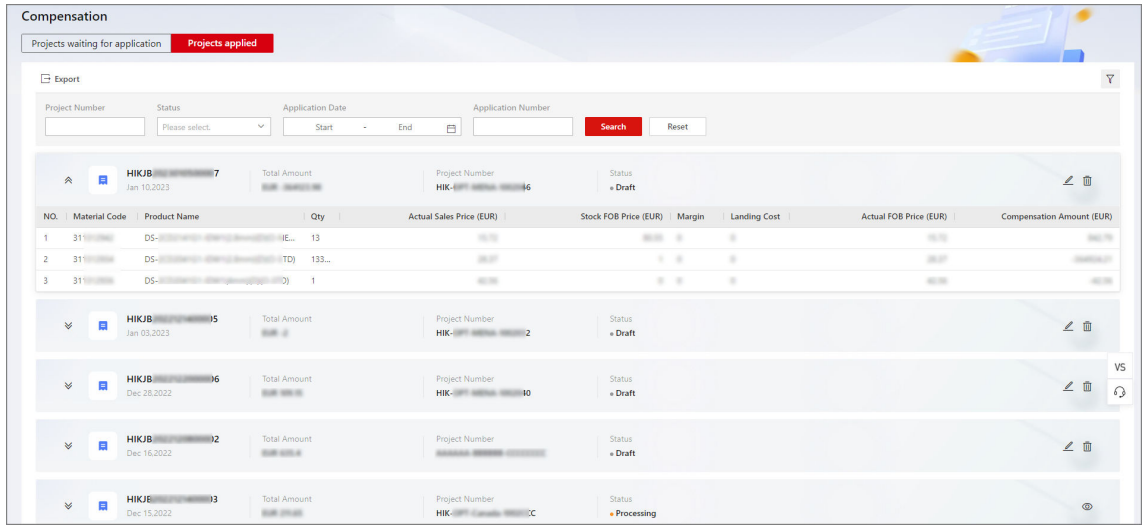


Figure 7-14 Submitted Compensation Applications

Application Status

Draft

The application has failed to be submitted. Information entered for the latest submission is saved for you to edit and resubmit.

Processing

The application has been submitted and is currently under review.

Rejected

The application has been reviewed by a Hikvision sales representative and is rejected. You can view remarks for your application, make changes to it, and resubmit if needed.

Completed

The application is approved. You will be compensated by one of the following methods: compensation amount issued to your e-wallet, credit notes, or free items.

7.6 How to Earn Reward Points and Redeem for Gifts

Hik-Partner Pro provides a reward point system to reward your trust and support. By completing specific tasks (e.g., check in, add devices, authenticate your company, invite friends, answer questions), you can get the reward points redeemable for lots of gifts (e.g., certain value-added services) in the Rewards Store.

Note

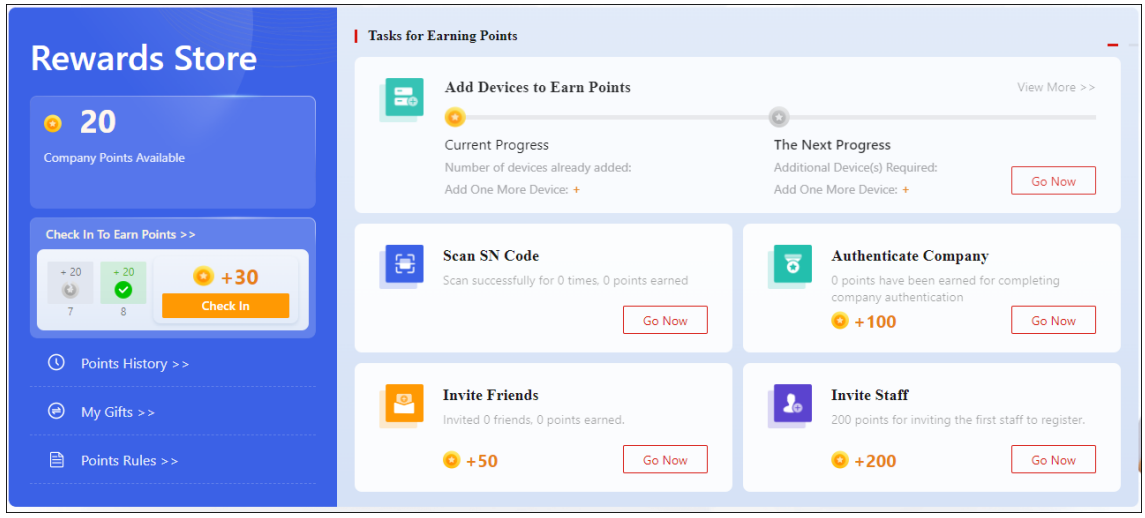
- The reward point system is only supported in some countries/regions.
- For some countries/regions, the reward points are available only when your company is authenticated. For details about company authentication, see ***Authenticate Company to Use More Features*** .

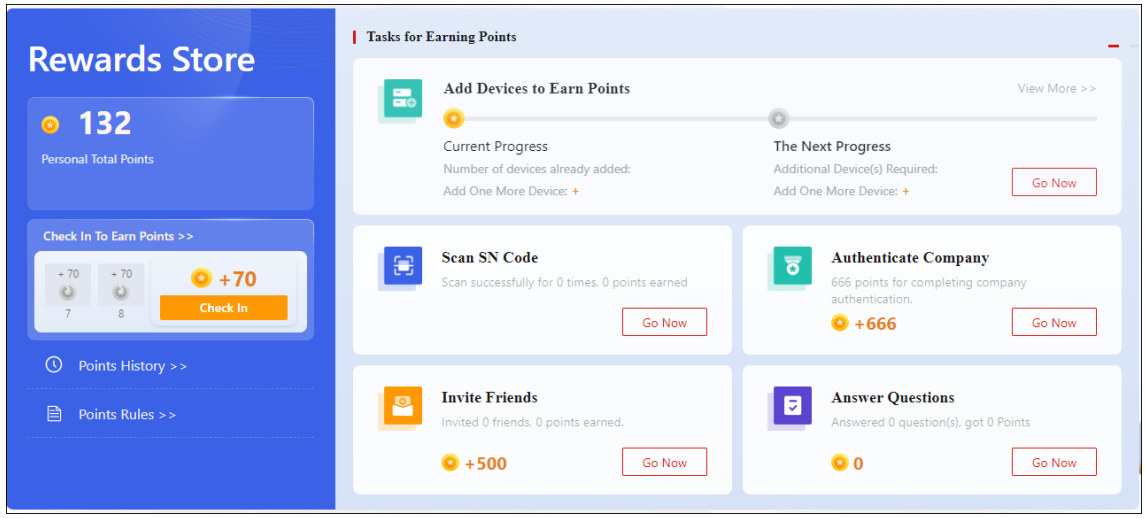
7.6.1 Earn Reward Points and Redeem for Gifts Using the Portal

1. Click **Incentive → Rewards Store** , or click **More** in the Rewards Store section on the right of the Home page.
2. On the task list, click **Go Now** to complete a task to earn points.

   Note

   You can click **Check In** on the top right of the Portal to earn points every day.





3. Select a gift, set the quantity, and click **Redeem** to redeem for it in the Gift Center below.

7.6.2 Earn Reward Points and Redeem for Gifts Using the Mobile Client

1. Enter the Rewards Store page.
   - Tap **Home → More → Rewards Store** .
   - Tap **Home → My Points** .
   - Tap **Me → Available Company Points** .
2. On the task list, tap **Go Now** to complete a task to earn points.

Note

You can tap **Check In** on the Home page to earn points every day.

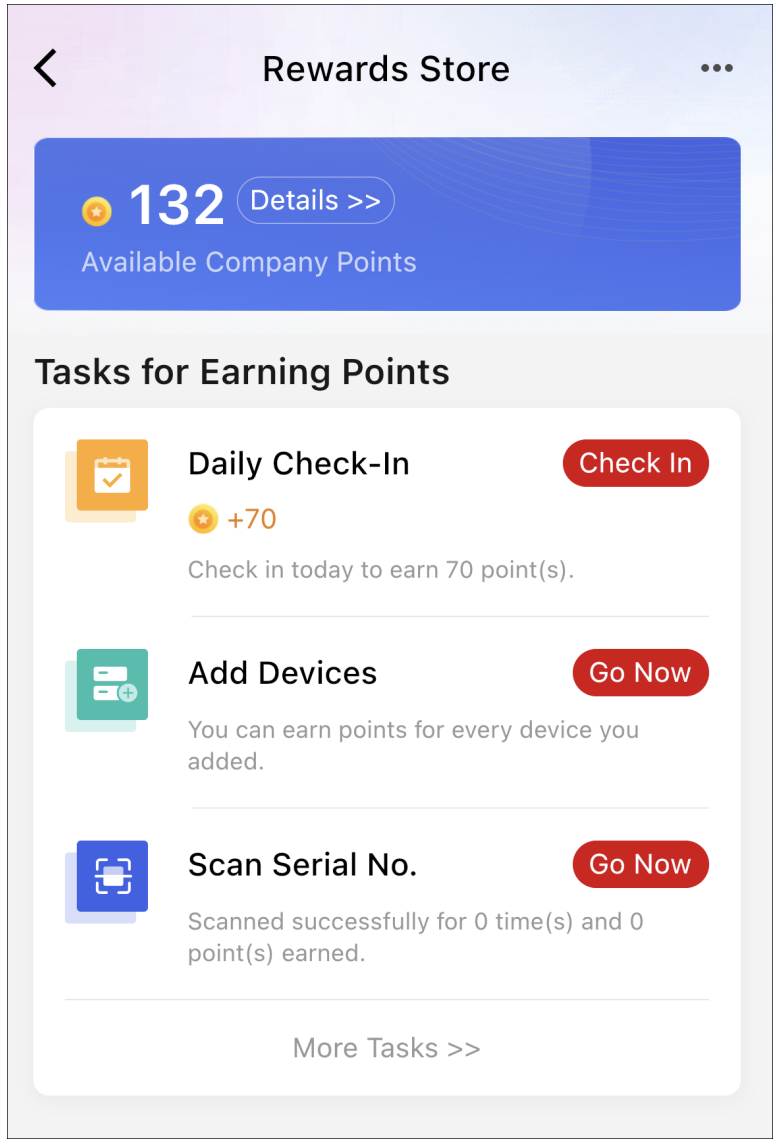


Figure 7-15 Rewards Store

3. Select a gift, set the quantity, and tap **Redeem** to redeem for it in the Gift Center below.

7.7 How to Claim and Verify eCoupons

The eCoupons (quota eCoupons, cash eCoupons, and ratio eCoupons) can be used by buyers to get discounts when they purchase products.

Note

This feature is only available to some users in some countries/regions.

Your Role	Description	Related Topics
Installer or Other Buyers	Claim eCoupons, and go to the corresponding providers to get the eCoupons verified to get discounts.	***Step 1: Buyers Claim eCoupons Using the Mobile Client***
Reseller, Distributor, or Other Providers	Verify buyers' eCoupons using Hik-Partner Pro and the verified amount will be reimbursed by Hikvision.	***Step 2: Providers Verify eCoupons Using the Mobile Client***

7.7.1 Step 1: Buyers Claim eCoupons Using the Mobile Client

Ways to Claim eCoupons

There are 3 ways to claim eCoupons.

- On the Home page, tap ⊕ →  in the upper-left corner, and scan the QR code of the eCoupon.
- Find the entry for claiming eCoupons in the Application Center, in the Banner area, or under the Event tab.
- Also, you may get eCoupons automatically.

View My eCoupons

After claiming eCoupons or getting eCoupons automatically, you can view all your eCoupons in **Me → My eCoupons** .

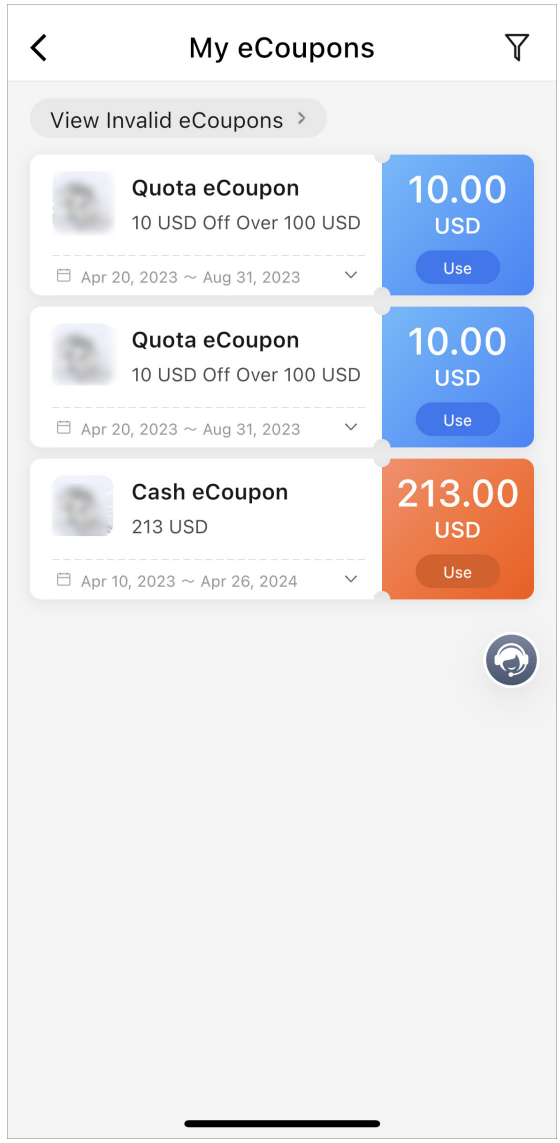


Figure 7-16 My eCoupons

On the My eCoupons page, you can:

- View eCoupon information such as the eCoupon type (quota eCoupon, cash eCoupon, or ratio eCoupon), discount rule, and validity period.
- Tap **View Invalid eCoupons** to view used or expired eCoupons.
- Tap ⌄ to view the number of eCoupons that are verified and whether you have reached the quantity limit of eCoupon verification.
- Tap an eCoupon to view its details.

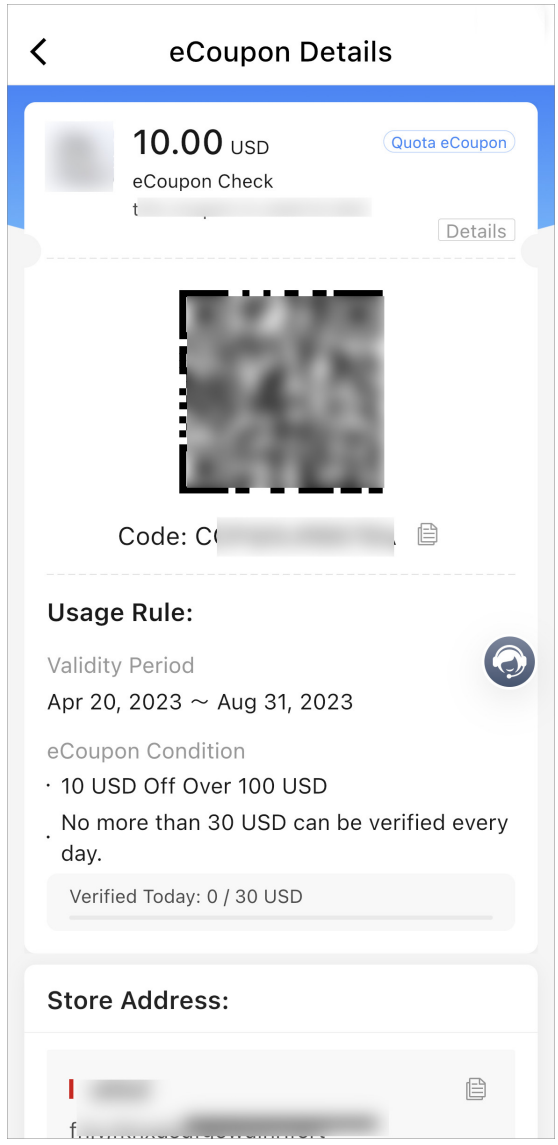


Figure 7-17 eCoupon Details

7.7.2 Step 2: Providers Verify eCoupons Using the Mobile Client

Note

If your company are granted the verification permission by Hikvision, all employees in your company can verify eCoupons. For details, please contact Hikvision.

1. Go to **Me → eCoupon Verification** .

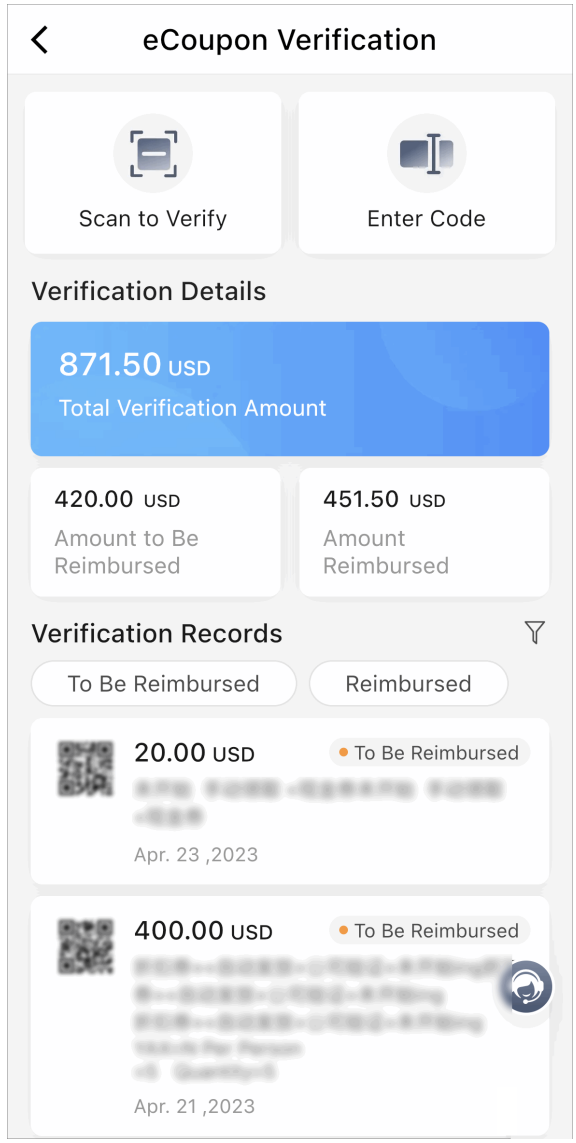


Figure 7-18 eCoupon Verification Page

2. Tap **Scan to Verify** or **Enter Code** to verify eCoupons.
3. (Optional) You can view the verification records and filter by whether eCoupons are reimbursed and by the reimbursement period.

7.8 How to Join Sell-Out Promotions

Sell-out promotions are activities that offer buyers discounts or free products when discount conditions are met.

Note

- This feature is only available to some users in some countries/regions.
- Only the Installer Admin account can access this feature.

Your Role	Description	Related Topics
Installer or Other Buyers	1. Submit purchase intentions to providers. 2. If intentions are confirmed, you can go to the providers offline and purchase the products with discounts.	***Step 1: Buyers Submit and Modify Intentions***
Reseller, Distributor, or Other Providers	1. Receive, manage, and confirm purchase intentions submitted by buyers. 2. After you confirm an intention, the intention submitter may come to you and purchase the products from you.	***Step 2: Providers Confirm Intentions from Buyers***

7.8.1 Step 1: Buyers Submit and Modify Intentions

On the sell-out promotion page, you can view the promotional rules and products, add the products to your cart, and submit your purchase intentions to selected providers (resellers or distributors). After your intentions are confirmed, you can go to the providers offline and purchase the products according to the prices of your intentions.

For Buyers: Submit and Modify Purchase Intentions Using the Portal

1. Find the entry for a sell-out promotion on the Event page or on the banner of the Home page. On the sell-out promotion page, you can view the promotion validity period, promotional discounts, and details about each product (product picture, product model, discount conditions, price, available quantity, etc.).

   Note

   A combo product is for selling a bundle of individual (single) products as one product.

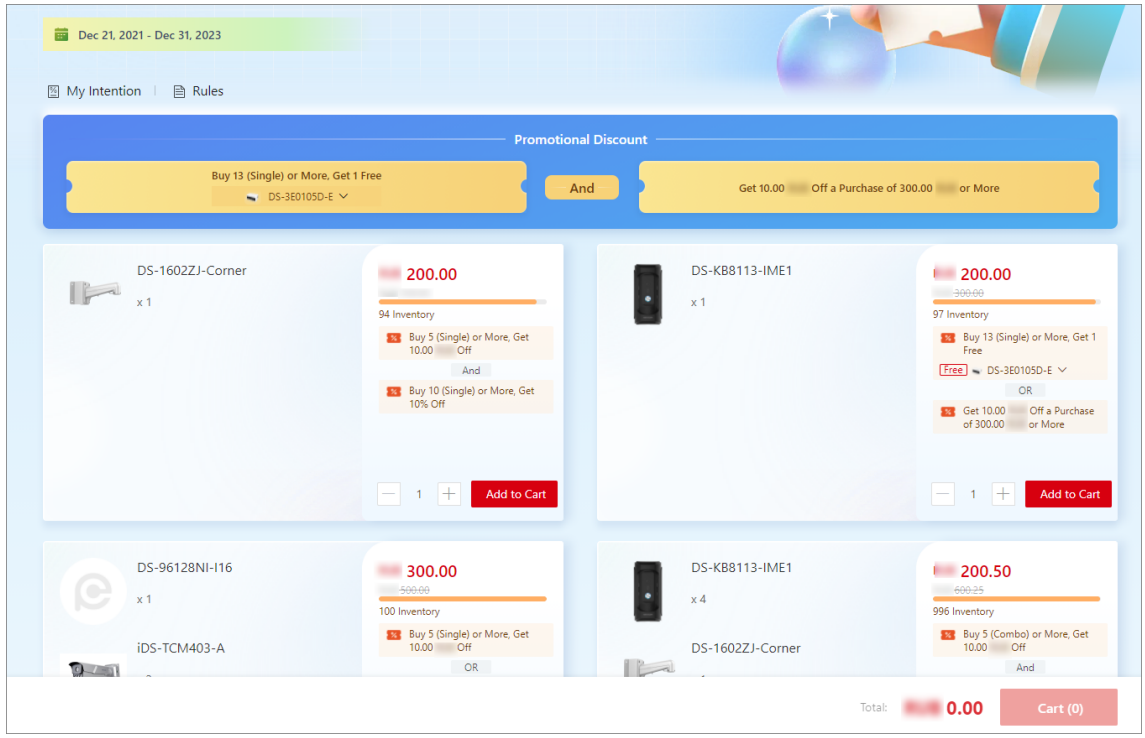


Figure 7-19 Example Sell-Out Promotion

2. (Optional) Click Rules to view the promotional rules, which offer detailed descriptions of the conditions you have to meet in order to get discounts and free products.
3. On each product card, click Add to Cart to add a specific number of products to your cart.
4. Click Cart to manage added products in your cart and to continue the submitting process. For each product, ⊙ indicates that the following discount condition is satisfied and you can get the corresponding discount or free products.

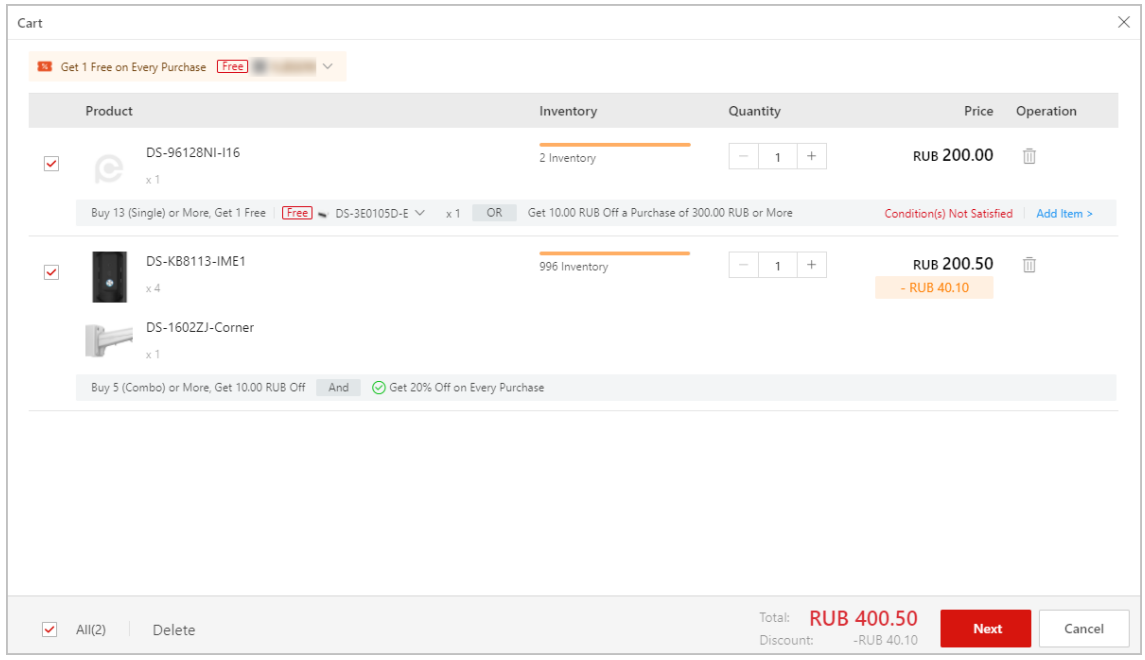


Figure 7-20 Cart for Sell-Out Promotion

5. Check the products and click Next to go to the Confirm Intention page. Select a distributor or reseller to purchase the products.

Note

The quantity in the summary contains the number of free gift products, the number of individual products in combo products, and the number of single products.

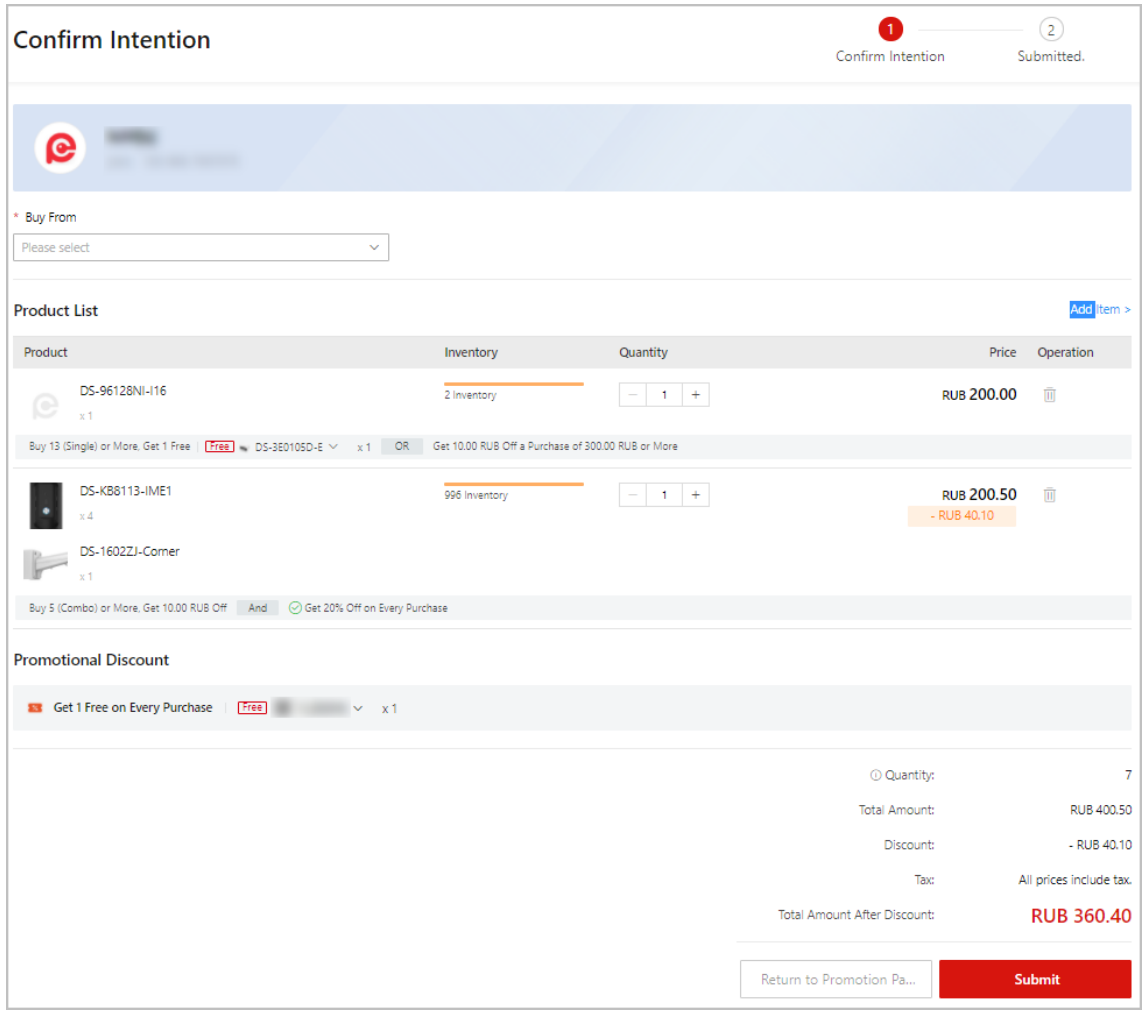
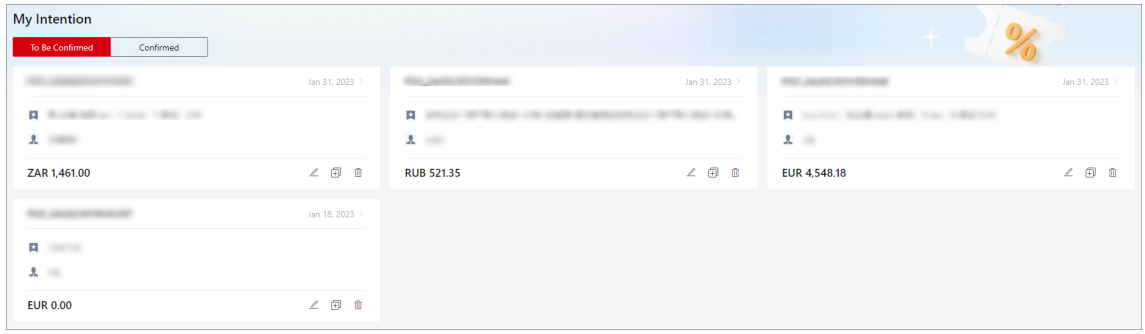


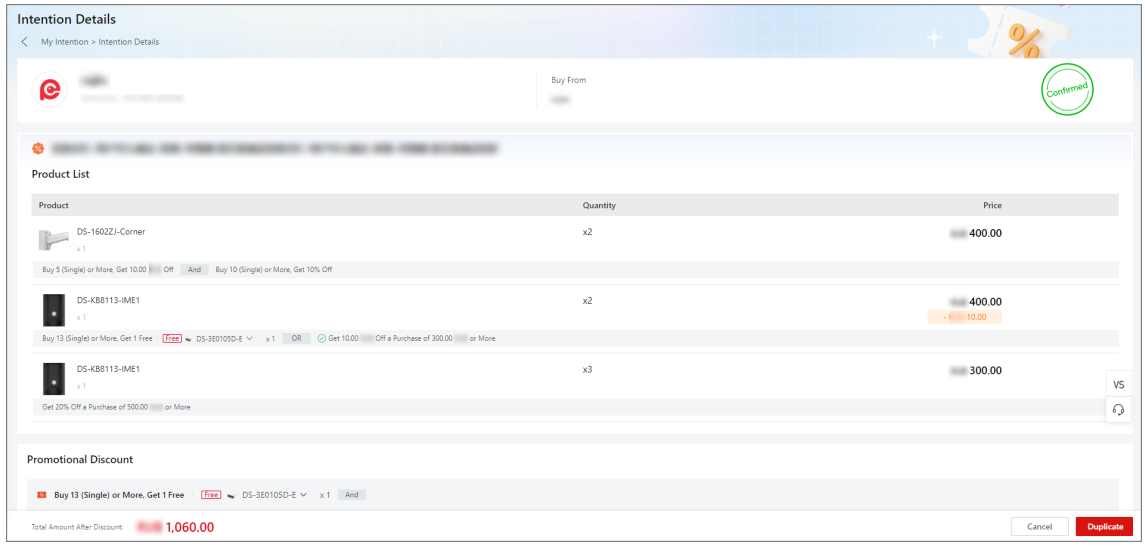
Figure 7-21 Confirm Intention

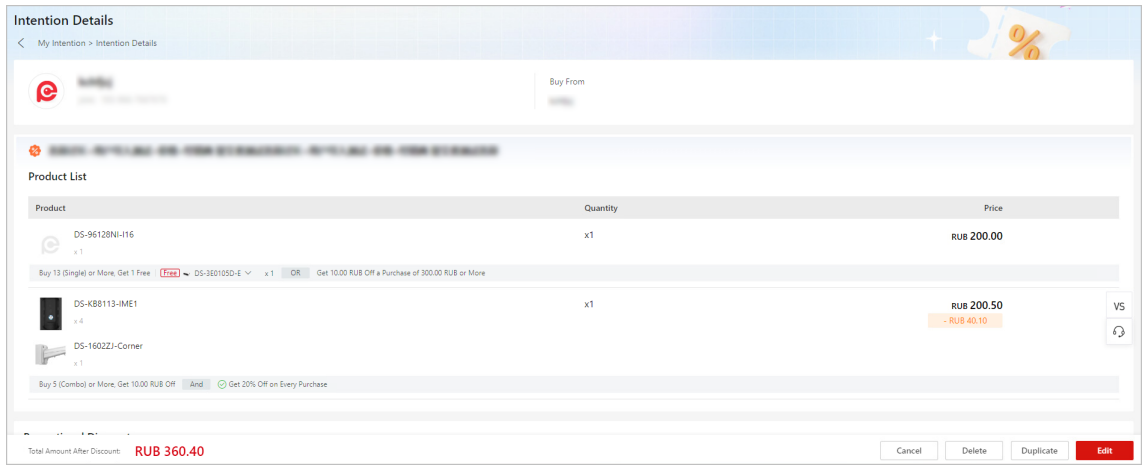
6. Click Submit to submit your intention.
7. (Optional) Click My Intention to modify your intentions before the provider confirms it.

Note

To go to the My Intention page, you can also click **My Intention** on the promotion page, or go to **My Hik-Partner → Account Information → My Intention** .







For Buyers: Submit and Modify Purchase Intentions Using the Mobile Client

1. Find the entry for a sell-out promotion on the Event page or on the banner of the Home page.

On the sell-out promotion page, you can view the promotion validity period, promotional discounts, and details about each product (product picture, product model, discount conditions, price, available quantity, etc.).

Note

A combo product is for selling a bundle of individual (single) products as one product.

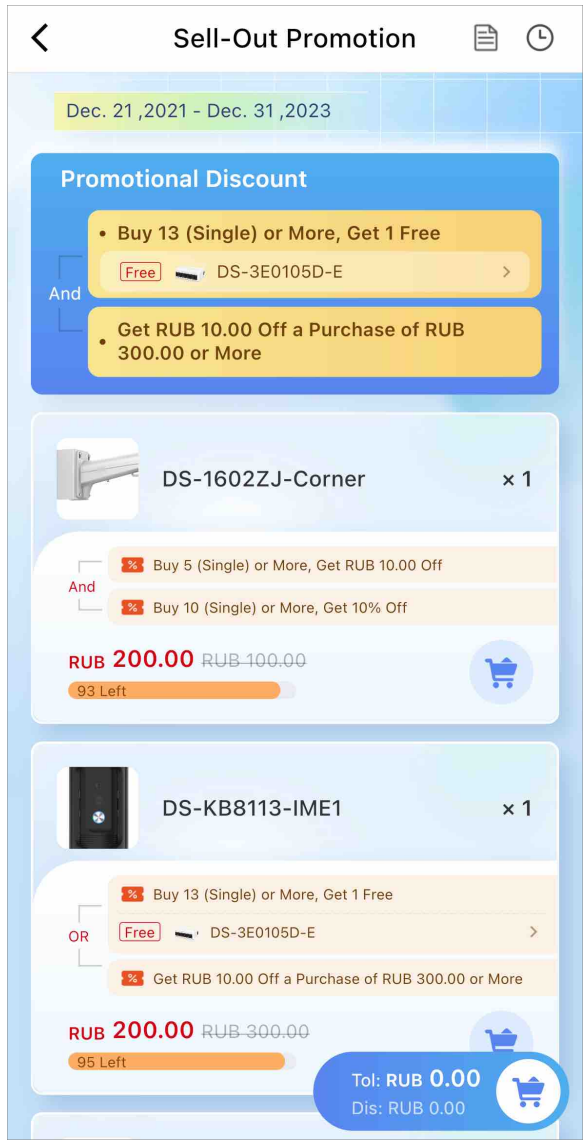


Figure 7-22 Example Sell-Out Promotion

2. (Optional) Tap to view the promotional rules, which offer detailed descriptions of the conditions you have to meet in order to get discounts and free products.
3. On each product card, tap to add one product to your cart. Tap again to add one more.

4. Tap to manage added products in your cart and to continue the submitting process.
For each product, indicates that the following discount condition is satisfied and you can get the corresponding discount or free products.

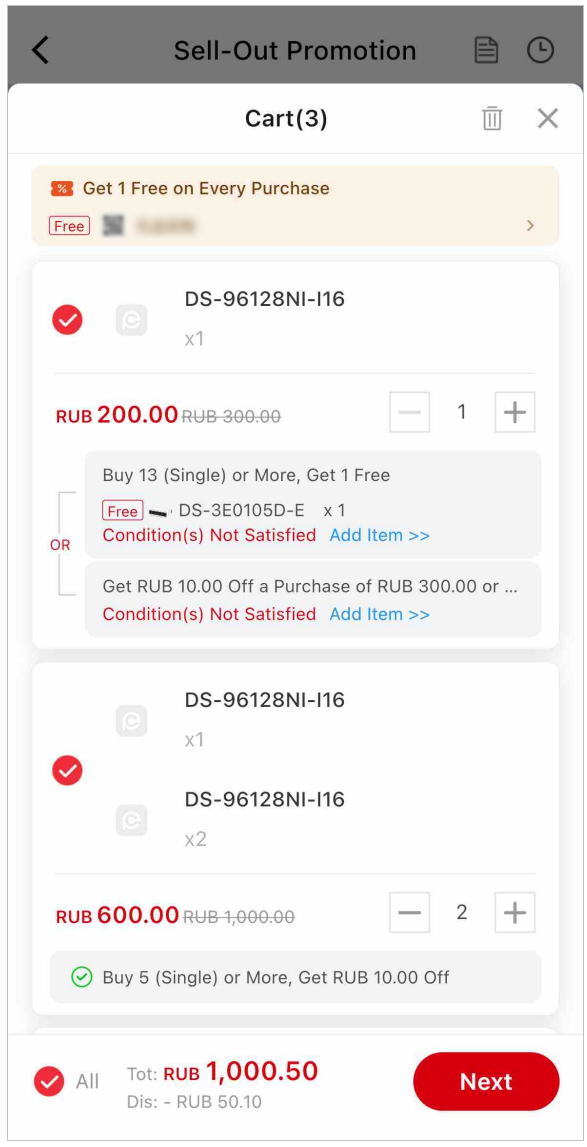


Figure 7-23 Cart for Sell-Out Promotion

5. Check the products and tap **Next** to go to the Confirm Intention page. Select a distributor or reseller to purchase the products.

Note

The quantity in the summary contains the number of free gift products, the number of individual products in combo products, and the number of single products.

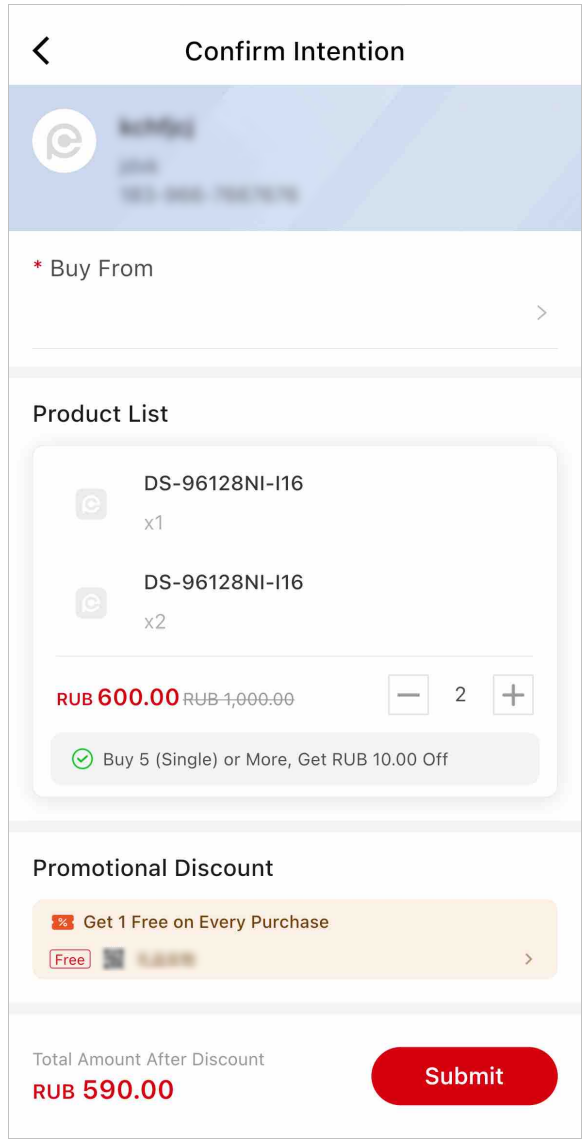
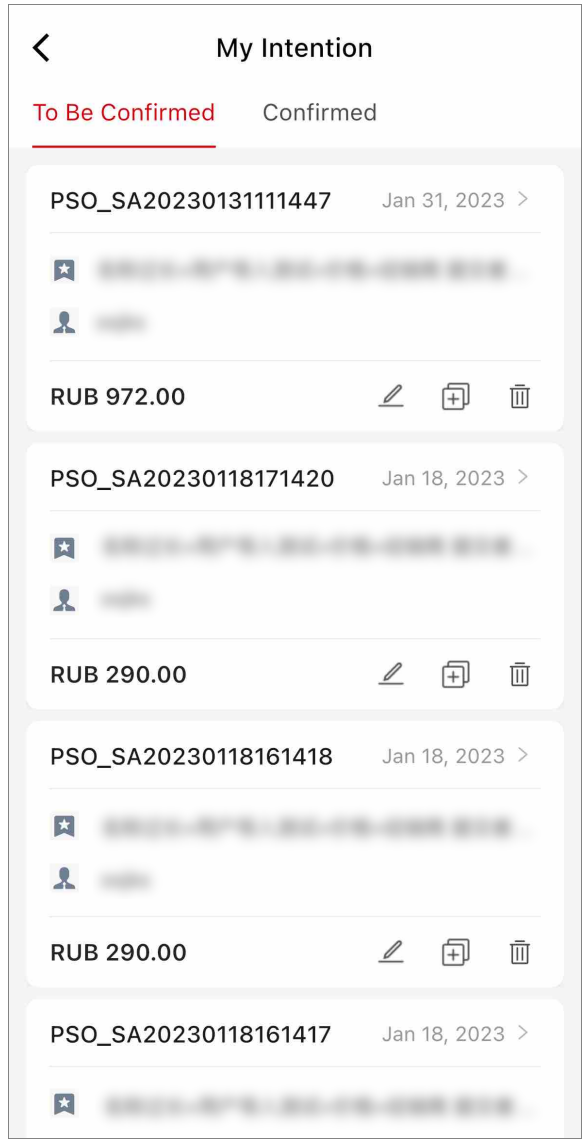


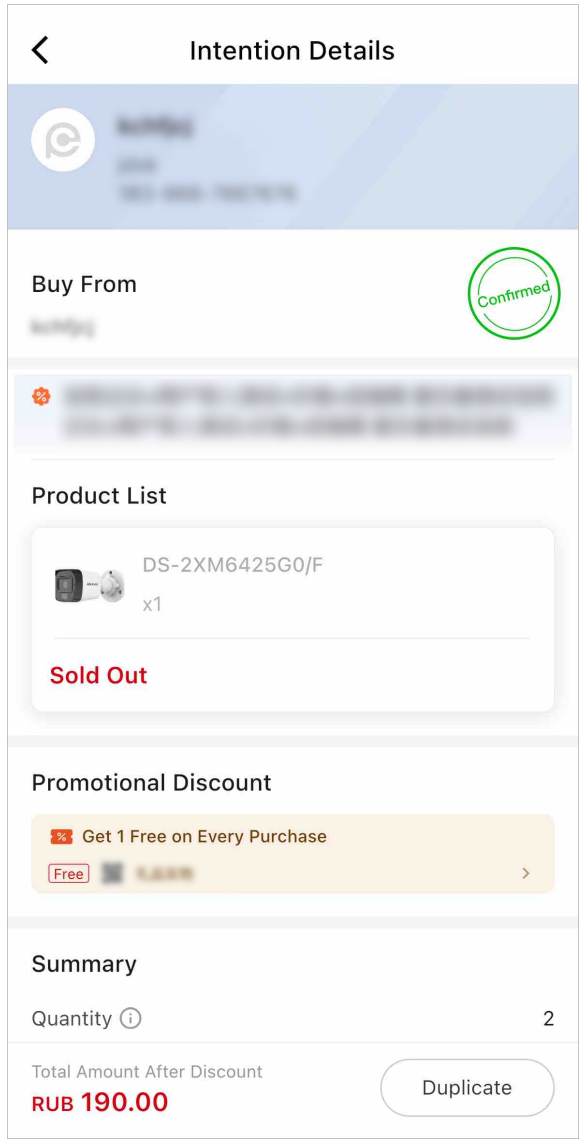
Figure 7-24 Confirm Intention

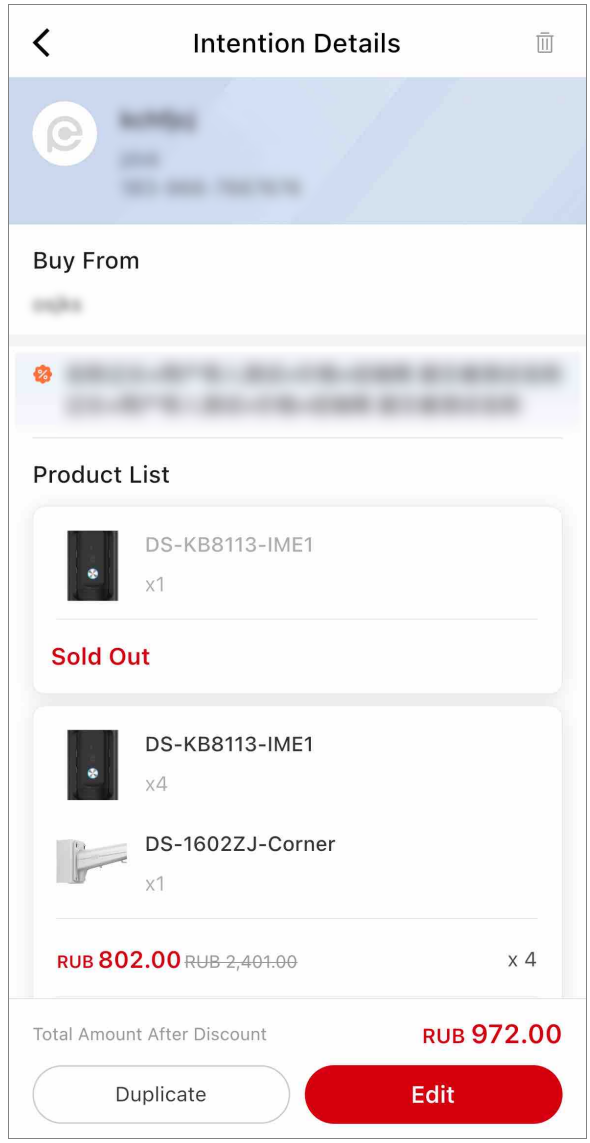
6. Tap **Submit** to submit your intention.
7. (Optional) Tap **My Intention** to modify your intention before the provider confirms it.

Note

To go to the My Intention page, you can also tap on the promotion page, or go to **Me → My Intention** .


My Intention
To Be Confirmed
Confirmed
PSO_SA20230131111447
Jan 31, 2023
RUB 972.00
PSO_SA20230118171420
Jan 18, 2023
RUB 290.00
PSO_SA20230118161418
Jan 18, 2023
RUB 290.00
PSO_SA20230118161417
Jan 18, 2023


Intention Details
Buy From
Confirmed
Product List
DS-2XM6425G0/F
x1
Sold Out
Promotional Discount
Get 1 Free on Every Purchase
Free
Summary
Quantity
2
Total Amount After Discount
RUB 190.00
Duplicate



7.8.2 Step 2: Providers Confirm Intentions from Buyers

If you are a distributor or reseller who is on the provider list for the sell-out promotion, you will be able to receive purchase intentions. You can decide whether to confirm a purchase intention, so the submitter can come to you and purchase the products.

For Providers: Confirm Intentions Using the Portal

1. Click **My Hik-Partner → Company Management → My Promotion** .

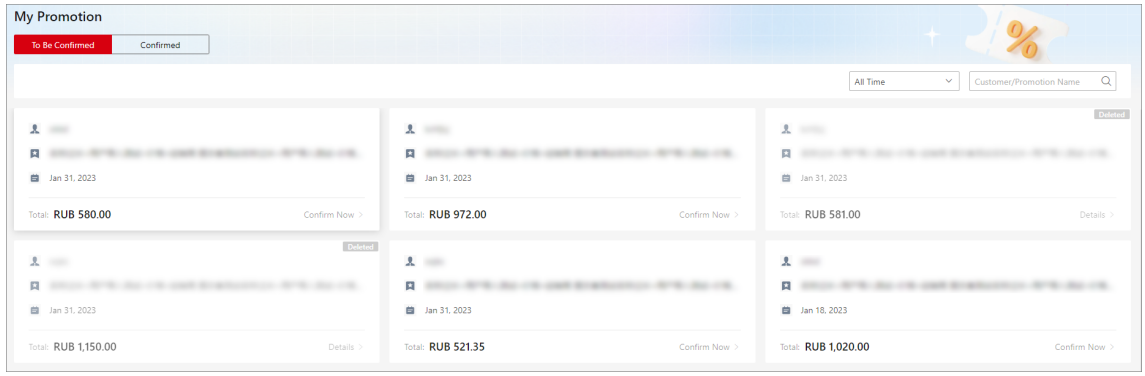
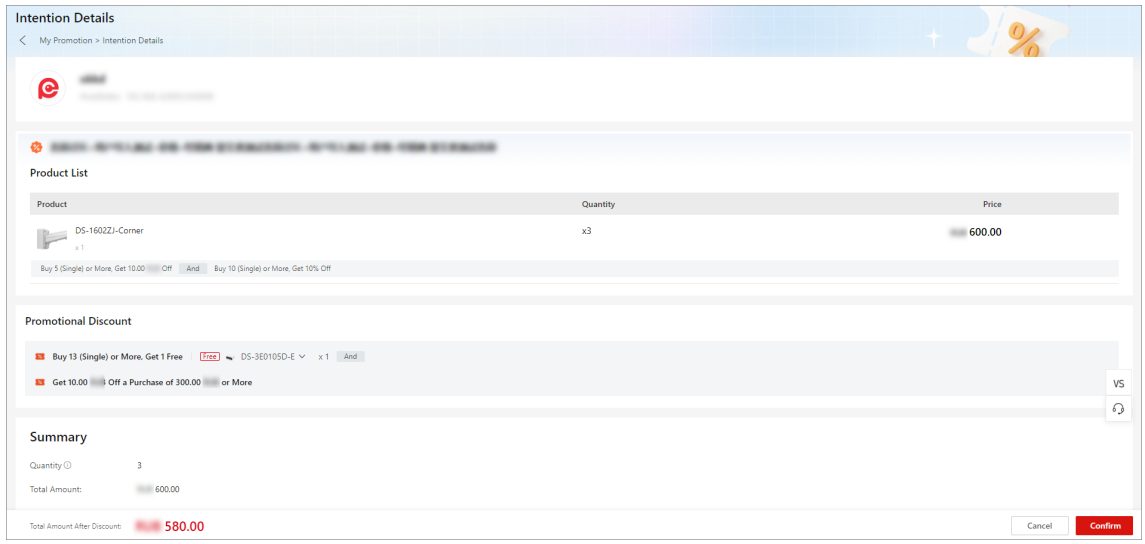
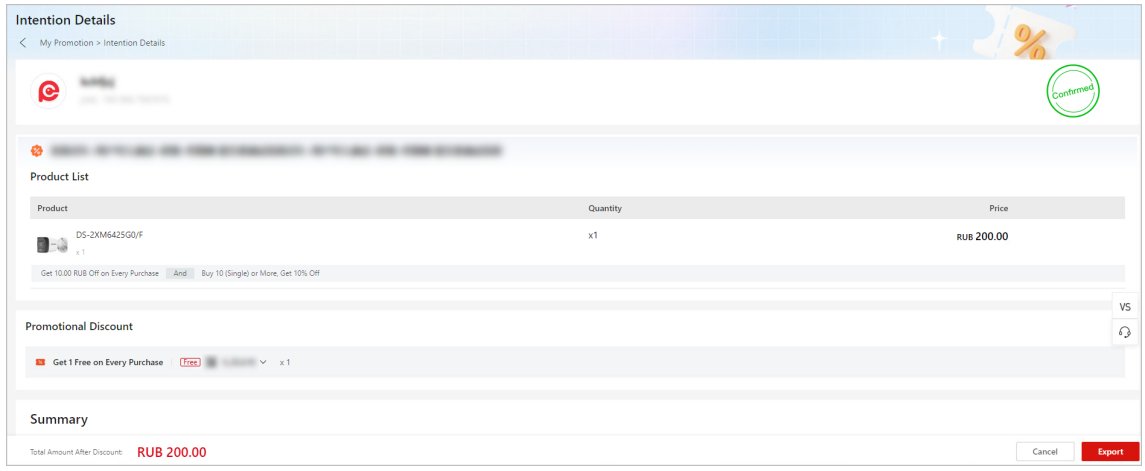


Figure 7-25 My Promotion

2. Click an intention card, check the intention details (product list, promotional discount, total amount after discount, etc.), and then click **Confirm** to confirm the intention.
   For confirmed intentions, you can click **Export** to export them to XLSX files.





For Providers: Confirm Intentions Using the Mobile Client

1. Tap **Me → My Promotion** .

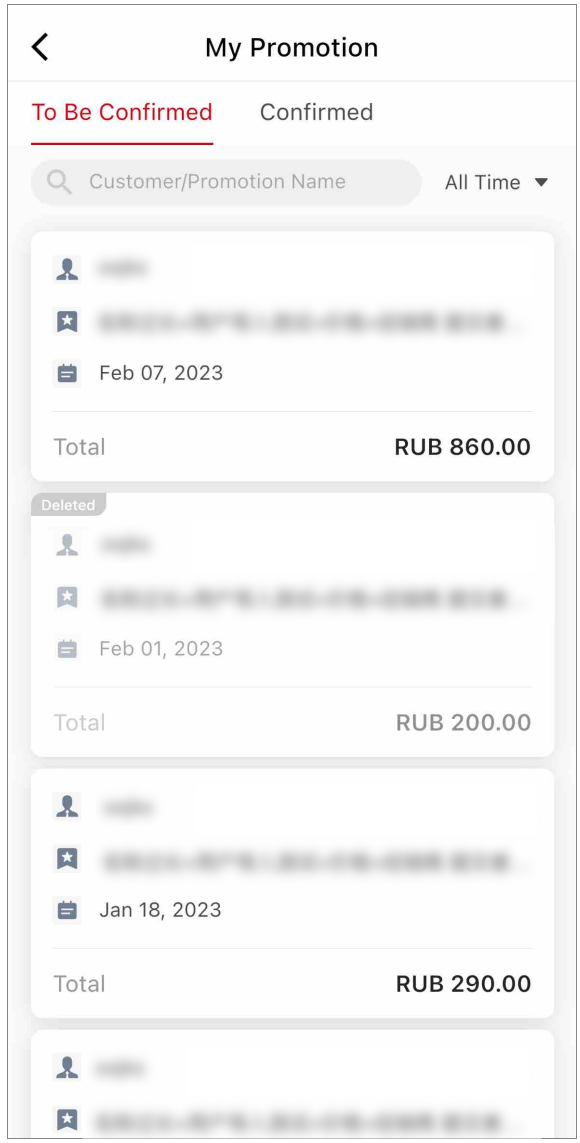
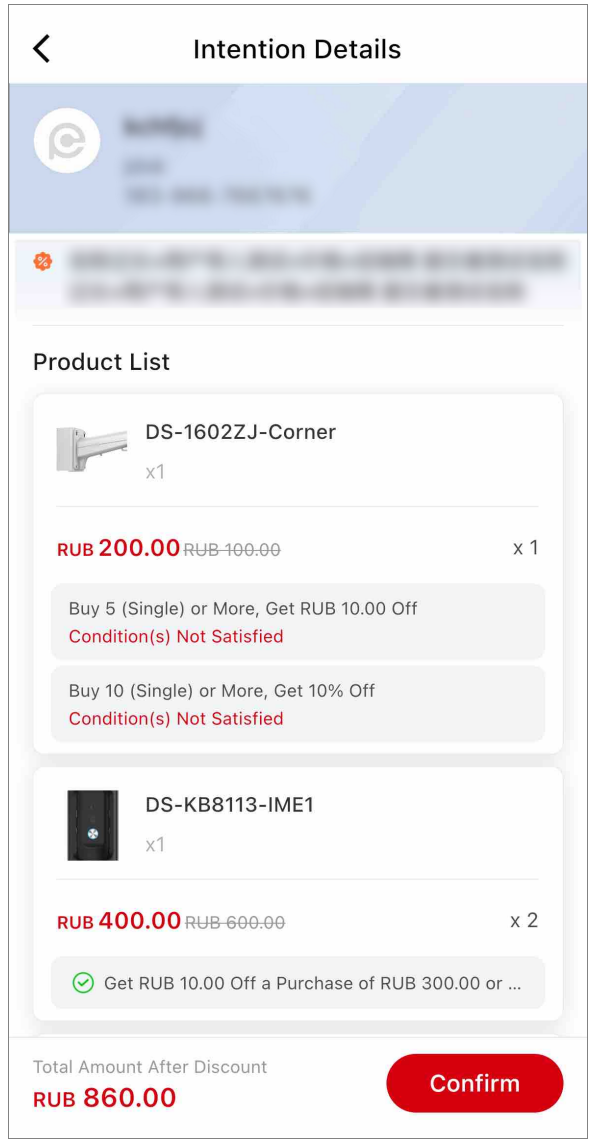
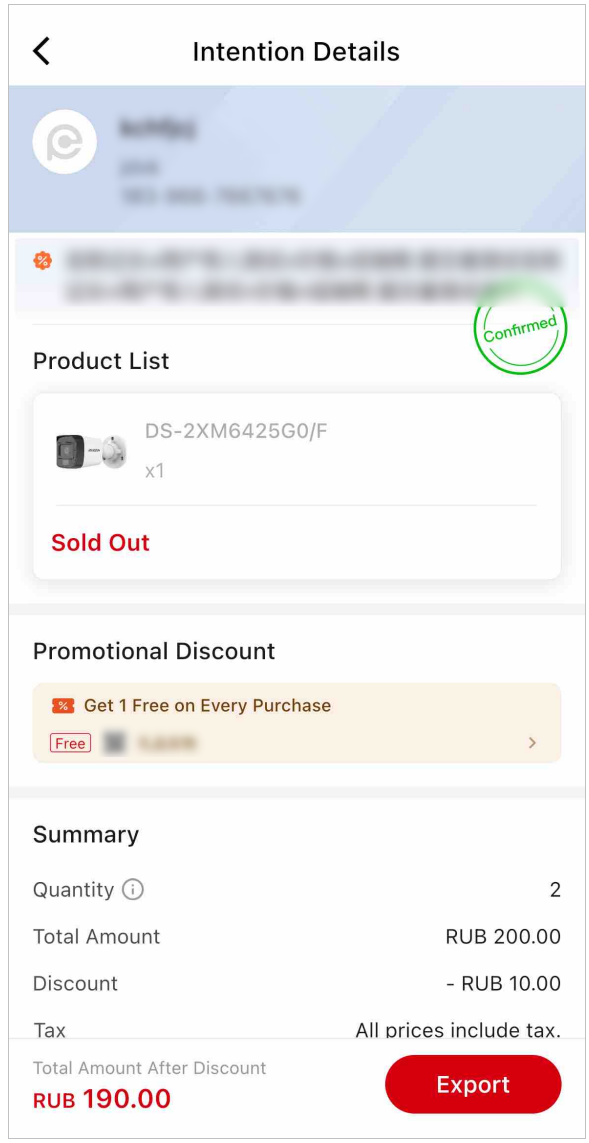


Figure 7-26 My Promotion

2. Tap an intention card, check the intention details (product list, promotional discount, total amount after discount, etc.), and then tap **Confirm** to confirm the intention.
   For confirmed intentions, you can tap **Export** to export them to XLSX files.


Intention Details
Product List
DS-1602ZJ-Corner
x1
RUB 200.00 RUB 100.00
x 1
Buy 5 (Single) or More, Get RUB 10.00 Off
Condition(s) Not Satisfied
Buy 10 (Single) or More, Get 10% Off
Condition(s) Not Satisfied
DS-KB8113-IME1
x1
RUB 400.00 RUB 600.00
x 2
Get RUB 10.00 Off a Purchase of RUB 300.00 or ...
Total Amount After Discount
RUB 860.00
Confirm


Intention Details
Confirmed
Product List
DS-2XM6425G0/F
x1
Sold Out
Promotional Discount
Get 1 Free on Every Purchase
Free
Summary
Quantity
2
Total Amount
RUB 200.00
Discount
- RUB 10.00
Tax
All prices include tax.
Total Amount After Discount
RUB 190.00
Export

