

LTS Platinum Partner Mobile Client

User Manual

Contents

Chapter 1. Introduction	1
1.1 Target Audience	1
1.2 Entities in LTS Platinum Partner	2
1.3 Operating Environment.....	3
1.4 Function Availability.....	3
1.5 Downloading the Mobile Client	4
1.6 Symbol Conventions.....	4
Chapter 2. Account Management	5
2.1 Registering with an LTS Connect Account	5
2.2 Registering an Installer Admin Account	6
2.3 Managing Roles & Permissions	9
2.4 Inviting Employees	10
2.5 Registering an Installer Account With or Without an Invitation.....	12
2.6 Logging In.....	14
2.7 Editing Account Information.....	15
Chapter 3. Company Management	17
3.1 Managing Company Information.....	17
3.2 Authenticating a Company	18
Chapter 4. LTS Platinum Partner Mobile Client Overview	19
Chapter 5. Site Management	22
5.1 Common Site Transfer Scenario	22
5.2 Site Page Introduction.....	22
5.3 Creating Site Groups.....	24
5.4 Adding a Personal Site	26
5.5 Adding a Team Site.....	28
5.6 Assigning Site to Installer	30
5.7 Handing Over Personal Site via Transfer	32
5.8 Handing Over Personal Site via Sharing	33
5.9 Handing Over a Team Site.....	37

5.10 Applying for Site Authorization from Site Owner	38
5.11 Accepting a Device Management Invitation from Your Customer	39
5.12 Site Collaboration	41
5.12.1 Site Collaboration During Handover	42
5.12.2 Accepting a Site Collaboration	43
5.12.3 Features Available to MSP/ISP on a Collaborated Site	44
Chapter 6. Using IP Portal Tool for On-Site Configuration	46
6.1 Searching for Devices on a LAN	47
6.2 Initializing an NVR on a LAN	47
6.3 Initializing Devices on a LAN (Excluding NVRs)	48
6.4 Batch Activating Devices	49
6.4.1 Batch Activating One NVR Together with One or More Network Cameras	49
6.4.2 Batch Activating Other Combinations of Devices	50
6.5 Adding Channels to Activated NVR	50
6.5.1 Automatically Adding Channels to NVR	50
6.5.2 Manually Selecting Channels to Add to NVR	51
6.6 Configuring & Managing NVRs, DVRs, & Network Camera Channels on the Live View Page	51
6.7 Sorting NVR Channels	58
6.8 Setting Verification Method for Password Reset	59
6.9 Adding Devices on LAN (via IP Portal Tool)	61
6.10 Resetting Device Password via IP Portal Tool	61
6.10.1 Resetting Password by Entering Old Password	61
6.10.2 Resetting Password via Reserved Email	62
6.10.3 Resetting Password by Answering Security Questions	63
6.10.4 Resetting Password by Submitting Case	64
6.10.5 Resetting Password by Sending Email to Technical Support	65
6.11 Adding Devices to LTS Connect	67
6.12 More Features of the IP Portal Tool	68
Chapter 7. Device Management	71
7.1 Batch Configuring Devices on LAN	71
7.1.1 Batch Activating Devices and Assign IP Addresses for Them	73

7.1.2 Batch Linking Channels to NVR and DVR.....	74
7.1.3 Creating Templates for Setting Parameters.....	75
7.1.4 Batch Setting Parameters for Devices.....	76
7.2 Adding Devices.....	76
7.2.1 Adding Devices After Batch Configuring Them on LAN.....	79
7.2.2 Connecting an Offline Device to Network.....	80
7.2.3 Adding Devices by Scanning QR Code.....	80
7.2.4 Adding Devices by Entering Serial No.	82
7.2.5 Adding Devices on LAN (via IP Portal Tool).....	83
7.2.6 Adding Devices by IP Address or Domain Name.....	84
7.2.7 Synchronizing Devices with LTS Connect Account.....	86
7.3 Activating the Health Monitoring Service.....	87
7.4 Managing Device Permissions.....	89
7.4.1 Applying for Device Permission.....	89
7.4.2 Release Permissions for Devices.....	90
7.5 Moving Devices.....	90
7.7 Resetting Device Password.....	93
7.8 Enabling Remote Log Collection.....	96
7.9 Viewing Video Feeds.....	98
7.9.1 Live Video.....	98
7.9.2 Playing Back Video Footage.....	98
7.10 Managing Network Devices.....	99
7.10.1 Adding Network Devices and Initializing Network.....	100
7.10.2 Network Switch Operations.....	101
7.10.3 Network Topology.....	105
7.11 Other Management.....	107
7.11.1 Unbinding a Device from Its Current Account.....	107
7.11.2 Configuring DDNS for Devices.....	107
7.11.3 Remote Configuration.....	109
Chapter 8. Health Monitoring.....	110
8.1 Checking the Status of Devices on All Sites.....	112

8.2 Checking the Status of Devices on One Site	115
8.3 Network Topology	119
Chapter 9. Notification Center	125
9.1 Business Notifications	125
9.2 Exception Center	127
9.3 System Messages	131
Chapter 10. Value-Added Services	133
10.1 Viewing and Purchasing Value-Added Services	133
10.2 Viewing and Managing My Services	133
10.3 Co-Branding	134
Chapter 11. Support	135

Chapter 1. Introduction

LTS Platinum Partner is a convergent, cloud-based security solution that helps manage services for your customers and expand your business by subscription offers. You can monitor the system health status of your customers' sites (even resolving problems) remotely, using a simple and reliable platform. LTS Platinum Partner solution enables you to customize security solutions for customers with fully converged LTS devices, covering video, intrusion, access, intercom, and more. LTS Platinum Partner solution provides different ways/clients for service providers' customers.

Table 1-1 Client Description

Client	Description
LTS Platinum Partner Portal	Portal for Installer Admin and Installers logging into LTS Platinum Partner to manage the security business, such as permission and employee management, site management, device management and devices health monitoring, etc.
LTS Platinum Partner Mobile Client	Mobile Client for service providers logging into LTS Platinum Partner to manage site, apply for site information management permission from end user, manage and configure the devices etc.
LTS Connect Mobile Client	Mobile Client for customers to manage their devices, accept the site handover from the service provider as the site owner, approve the Installer's application of site information management permission, etc.
LTS Connect Portal	Portal for customers to manage their employees' access level and attendance data after you set an attendance system for them via the LTS Platinum Partner Portal.

1.1 Target Audience

This manual provides service providers (i.e., Installers, Systems Integrators, Distributors, Resellers) with the essential information and instructions about how to use the LTS Platinum Partner Mobile Client to manage the security business.

This manual describes how to manage permissions and employees of a company, add new or existing sites for management, apply for site authorization and device permissions from customers, manage and configure devices belonging to the site, select products, check the device health status for further maintenance, and more. Keep this document as long as you use the related products and/or services. Check the LTS website for updates from time to time.

1.2 Entities in LTS Platinum Partner

Here we introduce the entities (any physical or conceptual object) involved in LTS Platinum Partner.

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.

Systems Integrator

Integrates multiple systems to provide solutions for customers.

End User

Those who have purchased or rented LTS devices (e.g., network cameras, DVRs, 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 LTS 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 LTS 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 control, and device maintenance on both LTS 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 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.

1.3 Operating Environment

The following is the recommended system requirement for operation the Mobile Client.

System Requirements

For iOS: iOS 12 or later versions

For Android: Android 5.0 or later versions

Memory

For iOS: 1 GB or more

For Android: 2 GB or more

1.4 Function Availability

The following table shows the functions on the Mobile Client.

Table 1-2 Free Functions on the Mobile Client

Module	Function(s)
Account Management	<ul style="list-style-type: none"> ● <u>Register an Installer Admin Account</u> ● <u>Manage Company Information</u>
Site Management	<ul style="list-style-type: none"> ● <u>Add Personal Site</u> ● <u>Hand Over Personal Site by Transferring</u> ● <u>Apply for Site Authorization from Site Owner</u> ● <u>Site Collaboration</u>
Device Management	<ul style="list-style-type: none"> ● Add Device <ul style="list-style-type: none"> ○ <u>Add Device by Scanning QR Code</u> ○ <u>Add Device by Entering Serial No.</u> ○ <u>Add Device by IP Address or Domain Name</u> ● <u>Apply for Device Permission</u> ● <u>Release the Permission for Devices</u> ● <u>Synchronize Devices with LTS Connect Account</u> ● <u>Enable Device to Send Notifications</u> ● <u>Upgrade Device</u> ● <u>Batch Upgrade Devices on LAN</u> ● <u>Configure DDNS for Devices</u> ● <u>Remote Configuration</u> ● <u>Reset Device Password</u>

Module	Function(s)
	<ul style="list-style-type: none"> ● <u>Unbind a Device from Its Current Account</u> ● <u>Manage Network Devices</u>
Video	<ul style="list-style-type: none"> ● <u>View Live Video</u> ● <u>Play Back Video Footage</u>

1.5 Downloading the Mobile Client

You can download the LTS Platinum Partner Mobile Client via the Portal, QR code, and online mobile application stores. The ways listed below are available to download the Mobile Client.

- Portal: Visit the landing page <https://www.itsplatinumpartner.com>
- Portal: Log in and click the account name or profile photo in the top right corner of the Portal to open the drop-down list, click **About** to access the About page and scan the QR code with your mobile phone to download the LTS Platinum Partner Mobile Client.
- App Stores: Enter LTS Platinum Partner as the keyword to search in the Apple App Store and/or Google Play.

1.6 Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Chapter 2. Account Management

There are two types of accounts: Installer Admin and Installer. Each company has only one Installer Admin account but can have multiple Installer accounts.

Installer Admin

The Installer Admin has full access to the functions in the system. Usually, the Installer Admin can be the manager of the installation company.

Installer

Installers are "sub-accounts" to the Installer Admin and are controlled by permission for what they can do. For example, they may only be able to manage the sites that are assigned to them. Usually, the Installers are the employees of the installation company.

The installation company should first register an Installer Admin account to create a company, then employees can be invited to register Installer accounts or register Installer accounts without an invitation by applying to join existing companies on the registration.

The flow chart of the whole process is shown as follows.



Figure 2-1 Flow Chart of Account Management

- **Register an Installer Admin Account:** First, register an Installer Admin account before accessing any functions of LTS Platinum Partner. For details, refer to [Register an Installer Admin Account](#).
- **Set Role and Permission (Optional):** Before adding an employee to the system, you can create different roles with different permissions for accessing system resources. There are also three predefined roles. For details, refer to [Manage Role and Permission](#).
- **Invite Employees (Optional):** You can invite employees to register Installer accounts and assign different roles to employees to grant the permissions to them. For details, refer to [Invite Employees](#).
- **Register Installer Accounts With or Without Invitations:** The employees can accept invitations to register Installer accounts, or register Installer accounts without invitations to apply to join existing companies. For details, refer to [Register an Installer Account With or Without an Invitation](#).

2.1 Registering with an LTS Connect Account

If you already have an LTS Connect account, you can register an Installer Admin account by the LTS Connect account.

Before You Start

- Make sure you have registered an LTS Connect account.

- Make sure the account to be registered is in the same region with the LTS Connect account.

Steps

1. Start the Mobile Client.
The Login page will show.
2. Tap LTS Connect on the lower side of the page.
You will access the authorizing and login page.
3. Authorize LTS Platinum Partner to get the account information of LTS Connect.
 - Enter your phone number and password for authorization.
 - Enter your email address/username and password for authorization.

Note

Check **Get Your Account and Device Information** to allow LTS Platinum Partner to get this information.

4. Tap **Authorize and Login**.
5. Register an Installer Admin account.

Note

For details about the registration process, refer to the ***Register an Installer Admin Account***.

6. Optional: After you finish registration and log in to LTS Platinum Partner, synchronize devices in your LTS Connect account with this account.

Note

For details, refer to ***Synchronize Devices with LTS Connect Account***.

What to do next

On the login page, enter the email address and password to log in to the LTS Platinum Partner Mobile Client.

2.2 Registering an Installer Admin Account

The Installation company should register an Installer Admin account before accessing any functions of LTS Platinum Partner.

Steps

1. Start the Mobile Client.
2. If you start the Mobile Client for the first time, select your country/region of your company and then tap **OK**.

 **Note**

You cannot change the selected country/region after registration.

3. In the Login page, tap **Register** to register an account.
-

 **Note**

If your account has been registered, you can tap **Log In** to log in to LTS Platinum Partner. For details about logging in, refer to [Login](#).

4. Select your identity and service provider type (installer, system integrator, distributor, reseller).
-

 **Note**

- In some countries/regions, you can only set the service provider type to Installer, Systems Integrator and Distributor.
 - For details about the identities and service provider types, refer to [Entities in LTS Platinum Partner](#).
-

5. Select whether you are to register by email or by phone number.
-

 **Note**

In some countries/regions, only registration by email is supported.

6. Register an account.

1) Set your name (first name and last name), company name, email, phone number, verification code (for verifying the email address) / SMS code (for verifying the phone number), and password.

2) Check **I agree to LTS Privacy Policy**, if you accept the details in the **Privacy Policy**.

3) Tap **Register**.

 **Note**

If there are existing companies with names similar to the company name you just entered, these companies will be listed and displayed so that employees can select and join their companies to register Installer accounts without invitation (refer to [Register an Installer Account With or Without an Invitation](#) for details). If you are to register an Installer Admin account and create a company, tap **Create Company** to continue registering an Installer Admin account.

You will be prompted that you have registered successfully, and the **Company Authentication** page will pop up.

7. Tap **Authenticate Now** or **Later** to enter either of the following processes.
- Tap **Authenticate Now** to submit the company authentication application.
 1. Set the required information and review the information already filled in (company name, address, email, phone, etc.).

 **Note**

For details, refer to ***Authenticate Company***.

2. (Optional) Check **I would like to receive marketing information about services and activities from LTS Platinum Partner via email. I understand that I can unsubscribe at any time.**

 **Note**

- If the subscription was successful, you will receive a confirmation email in a few minutes. You can unsubscribe by clicking the URL in the email if needed.
 - After the subscription, we will send emails about the latest product introduction, service introduction, questionnaires, and special offers, to the email address which is used for your account registration.
-

3. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in the agreements.
4. Tap **Confirm** to submit the application and access LTS Platinum Partner.

- Tap **Later** to go to the Complete Information page.

1. Enter the required information (address, etc.).
 2. (Optional) Check **I would like to receive marketing information about services and activities from LTS Platinum Partner via email. I understand that I can unsubscribe at any time.**
-

 **Note**

- If the subscription was successful, you will receive a confirmation email in a few minutes. You can unsubscribe by clicking the URL in the email if needed.
 - After the subscription, we will send emails about the latest product introduction, service introduction, questionnaires, and special offers, to the email address which is used for your account registration.
-

3. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in the agreements.
 4. Tap **Confirm** to access LTS Platinum Partner.
-

 **Note**

If you tap **Cancel**, the **Company Authentication** page will still pop up after you log in to the new account.

Result

You can log in to LTS Platinum Partner with this account and perform other operations such as site management.

2.3 Managing Roles & Permissions

Before adding an employee to the system, you can create different roles with different permissions for accessing system resources and then assign roles to corresponding employees to grant the permissions to them. Or you can give a predefined role to an employee without creating one. An employee can have only one role.

Steps

- There are three predefined roles in the system: Administrator, Site Manager, and IT Manager. The permissions of the three roles are as follows. The three roles cannot be deleted by anyone.
 - **Administrator:** Setting company information, managing employees, checking operation logs of all the employees, and managing all the sites.
 - **Site Manager:** Managing assigned sites, adding, configuring, and deleting devices, and enabling valued services for end users of assigned sites.
 - **IT Manager:** Managing all the sites, assigning sites to other employees, enabling or editing valued service for all the end users, and viewing operation logs of all the employees.
-

1. Tap **Me** → **Company Management** → **Role and Permission**.
2. Tap **+** in the upper-right corner of the Role and Permission page to open the Add Role page.
3. Enter the role name and select permission(s) for the role.

Manage All Sites

Managing all sites, including adding and editing site, assigning site to Site Manager, handing over sites, applying for site authorization, searching sites, managing devices in the site (adding, deleting, editing, upgrading), applying for device permission, and health monitoring. Up to 100 employees can be assigned this permission.

Manage Assigned Site

Managing site(s) assigned to the employee, including editing site, handing over sites, applying for site information management permission, adding existing site, adding a new site, managing devices in the site (adding, deleting, editing, and upgrading), and deleting site.

Note

You must give an employee this permission before assigning the employee a site.

Manage Account and Role

Accessing the Employee page and the Role and Permission page, adding and deleting accounts and roles. The Employee page and the Role and Permission page will not show without this permission.

Manage Company Information

Accessing company information page and edit company information (e.g. name, logo, addresses, etc.). Company information page will not show without this permission.

- Optional: Enter remarks of the role in the **Description** field.
- Tap **OK**.
- Optional: Perform the following operations after adding roles.

View Role Details	Tap an added role to access the role details page to view the role information and permissions.
Edit Roles	Tap an added role to access the role details page and tap  to edit the role information and permissions.
Delete Roles	Tap  in the upper-right corner and select the added role(s) to delete them. <hr/>  Note You cannot delete a role which has been assigned to an employee. <hr/>

2.4 Inviting Employees

Installer Admin and Installer with the role permission for managing account and role can invite employees to manage resources in the system.

Steps

- Tap **Me** → **Company Management** → **Employee**.
- Tap  in the upper-right corner of the Employee page to open the Add Employee page.
- Enter the email of the to-be-invited employee.
- Select a role for the employee.

Note

You can tap  in the upper-right corner of the Select Role page to create a new role. For details about managing roles, refer to **Manage Role and Permission**.

The permissions of the role will be displayed.

- Tap **Add**.
The invited employee will receive an email delivering a link at the email address entered. The employee needs to tap the link to register an account, after which the employee's information will be displayed in the employee list.
- Optional: Perform the following operations after adding employees.

<p>Enable/Disable Employee</p>	<p>Set the switch to on or off to enable or disable the employee account.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> ● Once disabled, the employee cannot log in to the system via this account. ● You cannot disable your own account and the Installer Admin account. <hr/>
<p>Remove Account Limits</p>	<hr/> <p> Note</p> <ul style="list-style-type: none"> ● The status of employees is limited by default and some operations are unavailable to them such as creating sites, adding devices, viewing records in the Employee Efficiency Statistics module, and viewing operation logs. ● Installer Admin and Installers with employee management permission can remove account limits for employees, which requires the employee account add-on for each employee. See details in <u>View and Purchase Value-Added Services</u>. <hr/> <p>Tap an employee to open the Employee Details pane, tap the account limit message on the top, and tap Remove Limit on the pop-up.</p>
<p>Delete Employees</p>	<p>Tap  in the upper-right corner and select the added employee(s) to delete them.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> ● You cannot delete your own account, the Installer Admin account and the Site Manager account. ● If the employee has not merged account data or become an LTS Platinum Partner user, you cannot delete their account. Refer to <u>Become an LTS Platinum Partner User After Product Upgrade</u> for details. <hr/>
<p>View Employee Details</p>	<p>In the employee list, you can view the employee's contact number, email address, role permissions, and numbers of sites and devices the employee managed.</p>
<p>Edit Role Assigned to Employee</p>	<p>Tap an employee to open the Employee Details pane and tap  in the role field to access the Select Role page. Then you can tap  to add a new role or select another role for the employee.</p>

	<hr/>  Note You cannot edit roles assigned to your own account and the Installer Admin account. <hr/>
View Sites Managed by Employee	Tap numbers of sites and devices in the employee list or tap an employee to open the Employee Details page to view the list of all sites managed by the employee. You can tap a site to view the site details. <hr/>  Note The above operation is supported only when the employee has site(s) to be managed. <hr/>

2.5 Registering an Installer Account With or Without an Invitation

The Installer accounts are "sub-accounts" to the Installer Admin account and are controlled by permissions for what they can do. Usually, the employees in a company will use the Installer accounts and can register the Installer accounts with or without invitations.

Register with an Invitation

As an employee, after you are invited to register the Installer account, you can accept the invitation and register an Installer account to manage sites and devices.

Note

The Installer Admin or Installer whose role contains permission to **Manage Account and Role** should invite the employee first. For details, refer to [*Invite Employees*](#).

After you are invited to join a company as an employee, you will receive an email from LTS Platinum Partner. You can complete your Installer account registration through the link or button in the email, for details about the registration process, refer to the *LTS Platinum Partner Portal User Manual*.

After registration, you can log in to LTS Platinum Partner with this Installer account and perform other operations such as site management and configuration.

Register Without an Invitation

As an employee of a company, you can also join the company upon registration without an invitation. The registration process is like that for the Installer Admin. Refer to [*Register an*](#)

Installer Admin Account for details.

After you fill in the required information (company name, etc.) and tap **Register** on the registration page, if there are existing companies with names like the company name you just entered, these companies will be listed and displayed, and you can apply to join one of them. After your application is approved by your company's administrator, you can log in to LTS Platinum Partner with this Installer account and perform other operations such as site management and configuration.

 **Note**

- You can contact your company's administrator to ask them to approve your application in Notification Center (**Business Notifications**).
- Only authenticated companies and companies which have submitted authentication applications can be listed and displayed.
- If your company is not listed and displayed, you will not be able to register an Installer account without an invitation. Consult the section **Register with an Invitation**.
- After you submit your joining application to an existing company and before it is approved by the company's administrator, you can withdraw the application.

Join Company

If you are an employee from one of the following companies, please select and join the company. Or if you are a company owner, you can create a company. [Create Company](#)

all-gardiner limited

 Admin: all-gardiner limited *****

all-gardiner limited

 Admin: 786-432 0 *****

all-gardiner limited

 Admin: 61,ADHALL *****

all-gardiner limited

 Admin: 786-432 0 *****

Figure 2-3 Select and Join a Company

2.6 Logging In

After logging in with an Installer Admin account or Installer account, you can manage resources (including sites, devices, roles, etc.) and perform health monitoring and so on.

Make sure you have registered an account. See **[Register with LTS Connect Account](#)**, **[Register an Installer Admin Account](#)**, for details about registration.

2.7 Editing Account Information

After logging in, you can edit your account information of the current account and change password if required.

Tap **Me** at the bottom and then tap the profile photo on the top-left corner to access the Me page. You can view and edit your account information of the current account, including the profile photo, name, email, phone number, etc. You can also view your HIK ID on this page, but you cannot edit it.

Note

For accounts registered in countries which support registration with phone number, the phone number information cannot be edited.

Change Profile Photo

You can change your profile photo to another one if required.

1. Tap the profile photo.
2. Choose a photo from the photo albums on your phone.
3. Optional: Drag, crop and rotate the photo to change the position and size of your profile photo.
4. Tap **OK**.

Edit Name

You can edit the name if required.

1. Tap the name to access the Edit Name page.
2. Enter the first name and last name.

Note

The last name and first name should contain 1 to 32 characters, excluding emoji and special characters including: * ? " < > |.

3. Tap **Save**.

Manage My QR Code

Tap  to show My QR Code, which your customers can scan to add you as the service provider and authorize you to manage devices.

If you have uploaded your company logo, your company logo will be displayed in the center of the QR code. Or you can tap **Add Your Company Logo to the QR Code** to upload your company logo.

Tap  to download the QR code.

Change Email

You can change the current bound email address of the account to another one if required.

1. Tap the email to access the Change Email page.
2. Enter the password for the current account and tap **Confirm** to verify your identity.

3. Enter a new email address in the **Email** field.
4. Tap **Verify**.
An email with a verification code will be sent to your new email address.
5. Enter the received verification code in the **Verification Code** field.
6. Enter the password of the current account.
7. Tap **Confirm**.

Edit Phone Number

You can edit the phone number if required.

1. Tap the phone number.
2. Choose the area code of your country/region and enter a phone number.
3. Tap **Save**.

Change Password

Change the password of the current account.

Delete Installer Admin Account

For Installer Admin, if the account is no longer used, you can delete it on the Settings page.

Note

- Deleting an Installer Admin account is irreversible. The company information and accounts CANNOT be restored once deleted. Back up the required data before deleting the account.
 - If there are authorized site(s) or employee account(s) under the current account, you cannot delete it.
-

1. Tap **Me** → .
2. Tap **Delete Installer Admin Account**.
3. Tap **Delete Account**.
4. Enter the password of your Installer Admin account, and tap **Verify**.
5. Tap **Confirm** to confirm deleting.

Chapter 3. Company Management

After registering an Installer Admin account, you can bind your company information with this account for better service, authenticate your company to purchase value-added services and use more features using LTS Platinum Partner.

3.1 Managing Company Information

After registering an Installer Admin account, LTS recommends you bind your company information (including company name, phone number, email, etc.) with this account for better service.

Steps

Note

When your company is not authenticated, the Installer Admin can manage and edit all the company information. If you enter an authentication code to authenticate your company, you can directly edit the company information instead of waiting for the approval of the information change request.

1. Go to the Company Information page.
2. Tap .
3. Enter the name of your company.
4. Optional: Enter the website of your company.
5. Enter your address.
6. Enter the city of your company.
7. Enter an email address which will be bound with the Installer Admin account after registration.
8. Enter other information of your company, such as state/province/region, and postal code.
9. Enter your phone number.
10. Enter the VAT number.
11. Tap **OK**.

Note

You can check the percentage of completed information after saving.

3.2 Authenticating a Company

After you register an Installer Admin account, you can authenticate your account/company to purchase value-added services and use more features (besides the basic features) in LTS Platinum Partner.

At least one of the following account authentication methods is supported, depending on your country or region:

By Entering an Authentication Code

In this way, you will need to get an authentication code from LTS or the distributor first, and then enter the authentication code to authenticate your account.

1. Go to **Me** → **Authenticate Now**. (Optional) If you have no authentication code, tap **Get Authentication Code**, and send the application email with the predefined content template, including your email address (the one used when registering your Installer Admin account) and company information, such as company name, VAT No., and phone number, to LTS or the distributor to apply for an authentication code.

Note

If the email server is not configured or the recipient's address is not entered automatically, you can copy the content and send it to LTS or the distributor by your own email box.

2. Enter the authentication code on the account authentication page, and tap **Authenticate Now** to authenticate your account.

By Submitting an Online Application

You can fill in and submit the online application information to authenticate your account directly. After your application is approved, your account will be authenticated.

Note

If your company is not authenticated and you have permission to submit the authentication application, you may be prompted and guided to authenticate your company by submitting the application after logging in.

1. Go to **Me** → **Authenticate Now**. Review and edit the company information already filled in and set other required information, such as company name, address, city, etc.
2. Select the distributor if you have bought LTS products.
3. Tap **+** to upload a image (e.g., business license and business card) as evidence.
4. Tap **Authenticate Now**.
The application information will be sent.

Note

After your application is approved, you will be notified with push notifications and emails.

Chapter 4. LTS Platinum Partner Mobile Client Overview

The LTS Platinum Partner Mobile Client provides access to LTS Platinum Partner from your smart phone. After logging in to LTS Platinum Partner via the Mobile Client, the Home page will show:

Main Modules

The LTS Platinum Partner Mobile Client is divided into the following main modules. You can access these modules via the tab bar on the bottom.

Table 4-1 Main Modules of LTS Platinum Partner Mobile Client

Module	Description
Home	On the Home page, you can view the overview of your sites and devices, and other quick entries for health monitoring, IP Portal tool, on-site config, account linking, tools, recently visited sites, etc.
Site	In the Site module, the site list will show. A site represents a physical location where devices are installed and through which the Installer Admin / Installer can manage the devices.
Health	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;">  Note For countries/regions that support the Explore and Products modules, this module cannot be accessed via the Health tab at the bottom, but can be accessed via Health Monitoring or More → Health Monitoring on the Home page, or via Site → Health Monitoring. </div> <p>Includes the following sub-modules:</p> <ul style="list-style-type: none"> ● Health Status: Provides near-real-time information about the status of devices (including the encoding device, access control device, etc.,) added to the sites. You can view device status of a specific site or all sites. ● Exception Center: Shows all the history notifications of device exceptions and channel exceptions.
Me	<p>View and Edit Account Information: You can view the information of the current account, including name, authentication status (Authenticated and Not Authenticated), and your QR code. You can also tap the profile photo to view or edit the profile photo, name, email, phone number, QR code, password, etc.</p> <p>: Tap  in the top right corner to access the Support page.</p>

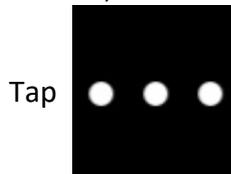
Module	Description
	<ul style="list-style-type: none"> ● Contact Us: You can contact us by calling or sending emails to us, and our address is also shown in Contact Us.
	<p>⚙️: Tap ⚙️ to access Settings.</p> <ul style="list-style-type: none"> ● About: You can view the version of the current platform, unsubscribe from marketing communications, and read the agreements including legal terms, privacy policy, and open-source license. ● Logout: Log out of the current account and return to the login page. ● Delete Installer Admin Account: If you are the Installer Admin and the account is no longer used, you can delete the Installer Admin account.
	<ul style="list-style-type: none"> ● Company Management: Tap Company Management to access the Company page. <ul style="list-style-type: none"> ○ Company Information: View company information, including company ID, country/region, address, email, etc. Tap  in the upper-right corner to edit company information if needed. ○ Co-Branding: This function helps to enhance brand awareness. Once enabled, your customers can view your company logo, address, and phone number via the LTS Connect Mobile Client. For details about how to get the co-branding service for free and enable the service, refer to <i>Co-Branding</i>. ○ Employee: Each company has only one Installer Admin but can have multiple Installers. The Installer Admin can invite the company's employees to register Installer accounts and assign different permissions to employees according to actual needs. Installer whose role contains permission Manage Account and Role can also invite other employees to be Installers by registering Installer accounts. ○ Role and Permission: A role defines one employee's rights to the functions in the system. After creating a role and specifying the role's permission, you can assign it to the employees according to actual needs.
<p>Help Center:</p> <ul style="list-style-type: none"> ● Help: Open the user manual of the LTS Platinum Partner Mobile Client. You can enter keywords to search the information you want in the user manual for help. ● Display Demo: Displays brief introductions to the five features of the Mobile Client such as "What is Site?" and "What is Exception?". ● Wizard: You can view the detailed explanations and operation guidance of some important functions of the LTS Platinum Partner 	

Module	Description
	Mobile Client. Follow the guidance as prompted to add a site, add a device, configure a device remotely, view live view of the device, etc.
	Link with LTS Connect Account: Link your account with LTS Connect accounts to synchronize devices automatically from the linked LTS Connect accounts.

Home Page Introduction

Scan QR Code

You can scan the QR code to add devices, add sites, reset passwords, check the firmware version, check the device batch, etc.



Tap  → **Help** on the top right corner to view the details about different types of QR

codes and their functions.

1. Scan the QR code generated by LTS Connect which contains the site information to add a site. For details about adding a site, refer to **Add Personal Site**.
2. Scan the QR code on the device to add it. For details about adding device, refer to **Add Device by Scanning QR Code**.
3. Scan the QR code generated by NVMS V3 to add multiple devices. For details about adding devices, refer to **Add Device by Scanning QR Code**.
4. Scan other QR codes such as the QR code of marketing communications to access the related web pages for more operations.

Add Device Manually

Add a device by entering the serial number or IP/domain.

Refer to **Add Device by Entering Serial No.** and **Add Device by IP Address or Domain Name**.

Synchronize Devices from LTS Connect

Refer to **Synchronize Devices with LTS Connect Account**.

IP Portal

Installation and configuration tool.

Refer to **Use IP Portal Tool for On-Site Configuration**.

Chapter 5. Site Management

A site can be regarded as an area or location with an actual time zone and address. There are two types of sites on LTS Platinum Partner, including personal site and team site. Personal site is for individual users and applicable to households and independent stores. Team site is for enterprise users and applicable to scenes where multi-user management is required such as chain stores, offices, and communities. You can create a site on LTS Platinum Partner to manage devices on it. Moreover, after you complete installing and setting up devices on a site, you can hand over the site and devices to your customer.

5.1 Common Site Transfer Scenario

A typical site transfer scenario is where the devices are owned by customers, and the installer provides 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. For more information, see [**Hand Over Personal Site by Transferring**](#).

5.2 Site Page Introduction

On the Site page, you can view the sites that are assigned to you (the Installer Admin as well as Installers with Manage All Sites permission can view all the sites of the company), and perform some operations for the sites, such as searching for sites, adding sites, and handing over sites. There are different statuses for the sites in the Site list.

Not Handed Over

The site is newly added, and you have not handed over it to the customer.

Not Registered

The handover must be sent to a customer who has not registered an LTS Connect account.

To Be Accepted

The handover application has been sent but has not been accepted by the customer who has registered an LTS Connect account.

Handed Over, Not Authorized (Shown as No Commission Authorization)

The site is handed over to the customer by transferring, but the installer is not authorized to manage the site.

Authorized and Monitoring (Shown as Email Address or Phone Number)

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.

Note

According to site status, the Installer Admin and Installers with related permissions can perform the following operations in the table.

Table 5-1 Supported Operations in Different Status

Supported Operations	Not Handed Over	To Be Accepted Not Registered	Handed Over, Not Authorized (Shown as No Commission Authorization)	Authorized and Monitoring (Shown as Email Address or Phone Number)	Shared	Disbanded
Search Site	✓	✓	✓	✓	✓	✓
Assign Site	✓	✓	✓	✓	✓	×
Hand Over Site via Transfer	✓	×	×	×	×	×
Hand Over via Sharing	✓	×	×	×	×	×
Manage Devices	✓	✓	×	✓	✓	×
Edit Site	✓	✓	×	✓	✓	×
Delete Site	✓	✓	×	×	✓	✓
Apply for Device Permissions	×	×	✓	✓	✓	×
Site Collaboration	✓	×	×	✓	×	×
Batch Share Devices	×	×	×	×	✓	×
Move to Group	✓	✓	✓	✓	✓	×

Note

If there are abnormal devices on sites, you can view a red icon indicating the number of abnormal devices beside **Site**. If the number of abnormal devices equals or exceeds 100, you can view the icon . Also, you can tap the abnormal device prompt above the site list to view all abnormal devices.

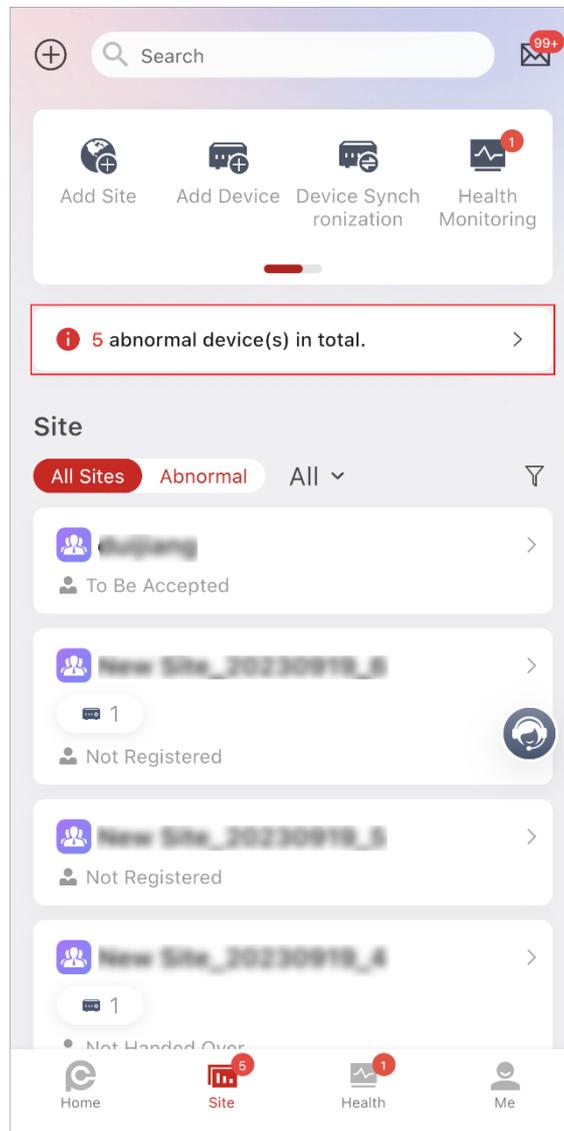


Figure 5-6 All Abnormal Devices

5.3 Creating Site Groups

You can create site groups and move sites to the groups.

Note

You can only create site groups for personal sites.

If you need to manage customers from different cities, or if there is a customer who has many sites, such as chain stores, you can create site groups by cities or create a site group for such a customer who has many sites, thus managing your customers more efficiently.

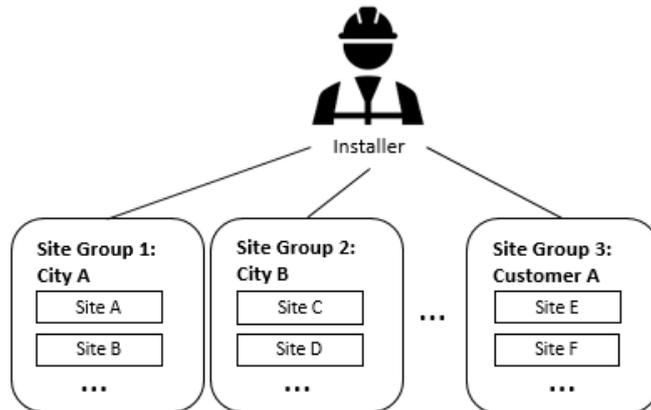


Figure 5-7 Site Grouping Scenario

There are three ways for you to create a site group.

Note

One site can be added to only one site group.

- If there is no site group, tap **Create Group** above the site list, enter the group name, tap **+** to select sites from the site list (optional), and tap **Complete**.
- If there are already created site groups, you can tap **▼** above the site list to pop up the Group pane, tap **Add Group**, enter the group name, tap **+** to select sites from the site list (optional), and tap **Complete**.
- You can also create site groups when you add sites. On the Add New Site page, check **Move to Group**, tap **>** or the group name, tap **Create Group**, enter the group name, and tap **OK**.

The following operations are supported after adding site groups.

Description	Operation
Edit Site Group	Tap ▼ above the site list to pop up the Group pane, tap Edit , and select a site group to edit the site group name and add/delete the sites.
Delete Site Group	Tap ▼ above the site list to pop up the Group pane, tap Edit in the upper-right corner, swipe a site group to the left, and tap 🗑️ to delete it.
Search for Site Group	Tap ▼ above the to pop up the Group pane, tap Edit in the upper-right corner, and enter keywords in the search box to search for the site groups.

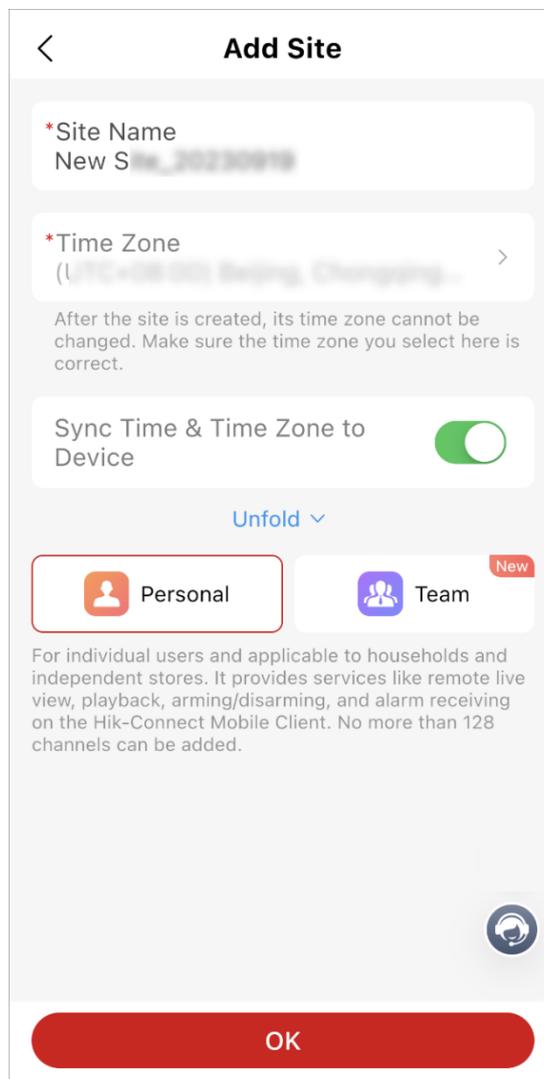
5.4 Adding a Personal Site

Personal sites are used for individual users and applicable to households and independent stores. When such a customer wants the installation company to provide the installation and maintenance service or the installation company assigns devices of a customer to employees to install and maintain the devices, the Installer Admin or Installer with related permission needs to create a personal site for managing these devices of the customer.

Steps

1. Enter the Add Site page.

- Tap the **Site** tab at the bottom to access the Site page. Tap  to access the Add New Site page.
- Tap **Add** → **Add New Site** in the Site & Device area on the Home page.



Add Site

*Site Name
New S...

*Time Zone
(UTC+08:00) Beijing, Chongqing... >

After the site is created, its time zone cannot be changed. Make sure the time zone you select here is correct.

Sync Time & Time Zone to Device

Unfold ▾

 Personal  Team New

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.



OK

Figure 5-8 Add New Site

2. Set the site name and time zone.

 **Note**

Select the correct time zone where the devices are located; a time zone cannot be changed after the site is added.

3. Optional: Enable **Sync Time & Time Zone to Device** to synchronize the time and time zone of the site to the devices added to the site.

4. Optional: Tap **Unfold** to set more information including scene, site address, city, and state/province/region.

 **Note**

- The Installer can select different configuration plans for the site and devices according to the selected scene.
 - You can tap  to set the location of the site on the map.
-

5. Optional: Enable **Move to Group** and select a group in the drop-down list to move the site to this group.

 **Note**

You can tap **Create Group** to create a new group. For details about creating site group, refer to [**Create Site Group**](#).

6. Optional: Enter the customer information, such as contact number and maintenance records as the remark.

 **Note**

The customer can view the remarks via LTS Connect Mobile Client.

7. Select **Personal** as the site type.

8. Tap **OK**.

You will access the site details page.

9. Optional: On the site details page, perform further operations.

View Site Details	Tap Detail or  → Site Details in the upper-right corner to view the site information including site name, site ID, site manager, etc.
Add Device	Tap Add Device or  → Add Device in the upper-right corner and select a method to add devices.

	<hr/>  Note For details, refer to <u>Add Device by Scanning QR Code</u> , <u>Add Device by Entering Serial No.</u> , <u>Add Device by IP Address or Domain Name</u> , <u>Synchronize Devices with LTS Connect Account</u> , and <u>Add Devices on LAN (via IP Portal Tool)</u> . <hr/>
Hand Over Site	After adding devices to the site, tap Hand Over Site → Hand Over by Transferring or Hand Over Site → Hand Over by Sharing to hand over the site. <hr/>  Note For details, refer to <u>Hand Over Personal Site by Sharing</u> and <u>Hand Over Personal Site by Transferring</u> . <hr/>
Delete Site	Tap  → Delete Site in the upper-right corner to delete the site.

5.5 Adding a Team Site

Team site is used for enterprise users and applicable to the scenes such as chain stores, offices, and communities. When such customers want the installation company to provide the installation and maintenance service, the Installer / Installer Admin needs to create a team site for managing these devices of the customers.

Steps

- Enter the Add Site page.
 - Tap the **Site** tab at the bottom to access the Site page and tap  .
 - Tap **Add** → **Add New Site** in the Site & Device area on the Home page.
- Set the site name and time zone.

Note

- Select the correct time zone where the devices are located; a time zone cannot be changed after the site is added.
 - The name of team site cannot be the same as that of personal site.
-

- Optional: Enable **Sync Time & Time Zone to Device** to synchronize the time and time zone of the site to the devices added to the site.
- Optional: Tap **Unfold** to set more information including scene, site address, city, and state.

 **Note**

- The Installer can select different configuration plans for the site and devices according to the selected scene.
 - You can tap  to set the location of the site on the map.
-

5. Optional: Enter the customer information, such as contact number and maintenance records as the remark.
-

 **Note**

The customer can view the remarks via LTS Connect Mobile Client.

6. Select **Team** as the site type.
7. Optional: Select one or more services to activate.
-

 **Note**

LTS recommends you select **Analysis Report** service together with **Video Management** service.

8. Tap **OK**.
The Add Device panel pops up.
9. Optional: Add devices on the Add Device panel.
- Tap **Scan QR Code** to add devices by scanning QR codes. For details, refer to [**Add Device by Scanning QR Code**](#).
 - Tap **Add Manually** to add devices by serial No. For details, refer to [**Add Device by Entering Serial No.**](#).
 - Tap **IP Portal** to add devices on LAN via IP Portal tool. For details, refer to [**Add Devices on LAN \(via IP Portal Tool\)**](#).
10. Optional: On the site details page, perform the following operations.

Add Device	Tap Add Device or  → Add Device in the upper-right corner to add devices to the site. For details, refer to Step 9.
Hand Over Site	After activating services, tap Hand Over Site to access the Handover List page, and hand over the site to the customer. <hr/> <p> Note</p> <p>For details, refer to <u>Hand Over Team Site</u>.</p> <hr/>
Activate Service	Tap All to access the All Services page. <ul style="list-style-type: none">● If you have activated a service when adding the site, tap Activate and Expand to activate and expand the service.● If you have not activated any service when adding the site, tap

	<p>Activate to activate a service. After activation, you can tap the service to view its details and perform different operations for different types of services.</p> <ul style="list-style-type: none"> ○ For video management, access control & attendance, and video intercom services, you can view the free channel(s) you have, and tap Activate and Expand to activate and expand the service or tap Get Free Trial to upgrade to trial plan. ○ For people counting and heat analysis services, tap Renew to renew the service or tap Get Free Trial to upgrade to trial plan.
View Site Details	Tap  → Site Details in the upper- right corner to view site details such as site name, site ID, and site manager.
Delete Site	Tap  → Delete Site in the upper-right corner to delete the site.

5.6 Assigning Site to Installer

The Installer Admin or the Installers with the Manage All Sites permission can assign a site to the specified Installer as site manager responsible for configurations of the devices on the site.

Before You Start

Make sure you have the Manage All Sites permission.

Steps

1. Tap the **Site** tab at the bottom to access the Site page.
2. Tap  to access the Assign page.

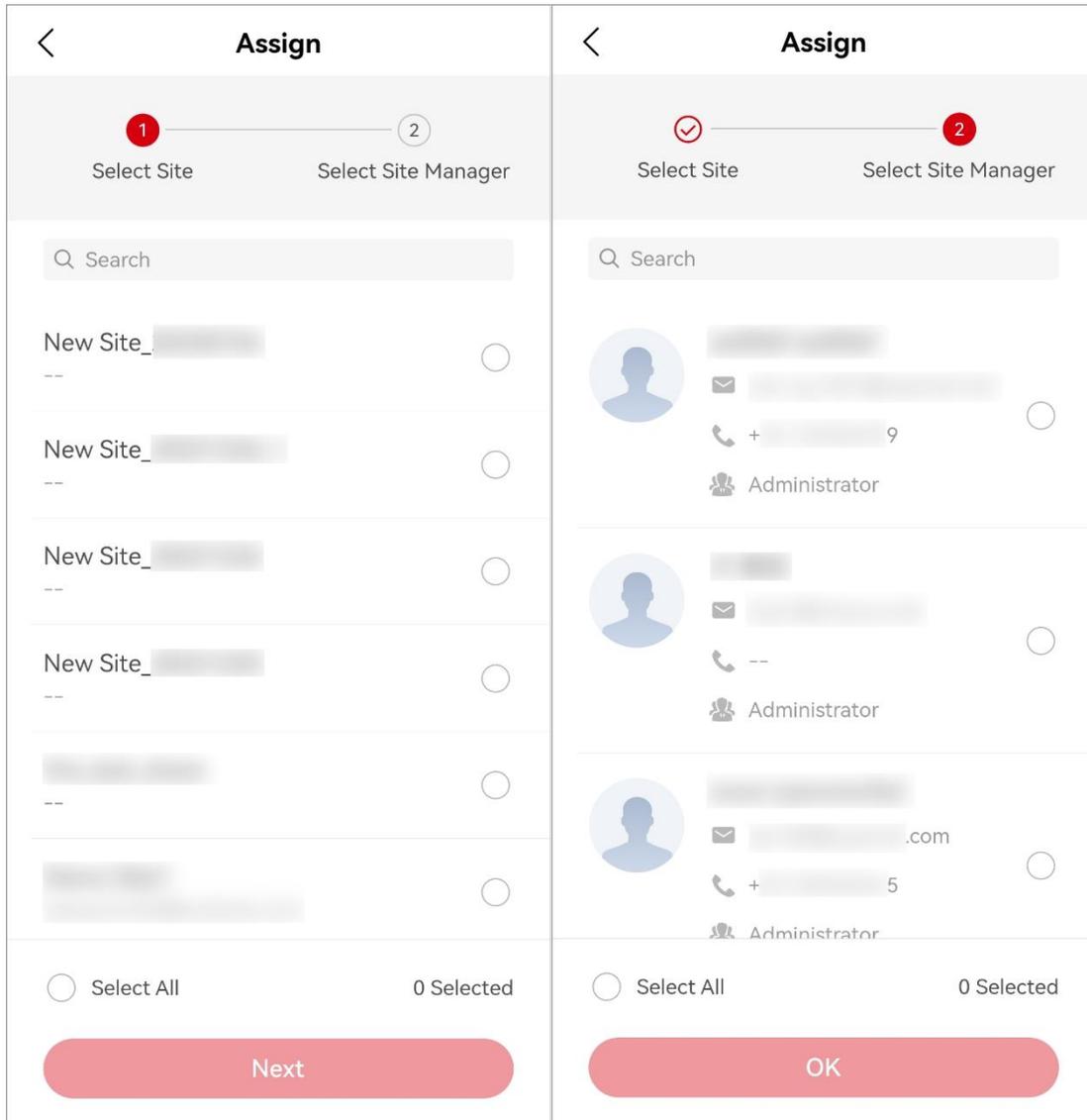


Figure 5-9 Assign Site to Installer

3. Select one or multiple sites for assignment and tap **Next**.

Note

- You can check **Select All** to select all the sites.
 - You can search for specific sites by entering keywords in the **Search** field.
-

4. Select one or multiple Installers as the site manager(s) of the selected site(s).

Note

- You can check **Select All** to select all the site managers.
 - You can search for specific site managers by entering keywords in the **Search** field.
 - No more than 100 site managers can be assigned to each site.
-

5. Tap **OK**.

The site manager of assigned sites can enter site details and perform related operations, such as adding devices.

5.7 Handing Over Personal Site via Transfer

After the installation company completed the installation, the Installer can hand over the site to a customer by transferring. After the site is handed over by transferring, the customer takes ownership of the devices, and usually the devices are owned by the customers. If required, the Installer can also apply for specified permissions for further device maintenance when handing over the site.

Before You Start

Make sure the site status is **Not Handed Over**; the devices are added to the site; and you have the permission for site management, such as managing all sites and assigned sites.

Steps

Note

You can only hand over personal sites by transferring.

1. In the site list, tap a site to access the Site Details page.
2. Tap **Hand Over Site** → **Hand Over by Transferring**.
3. Optional: Select the permissions for which you need to apply from your customer to maintain the devices.

Note

- If you have no permission to manage devices, or no devices are added to the site, you cannot select the permissions of configuration, live view, and playback when handing over the site.
 - If the following permissions are selected, when your customer accepts the handover, the permissions will be granted to the you. You do not need to apply for authorization from your customer again.
 - You can tap **Permission** or **Validity Period** to batch select the permissions and validity periods for all devices on the site.
-

Site Information Management

The permission to manage the site information.

Configuration

The permission to configure selected devices on the site.

Live View

The permission to stream the live video from the selected devices on the site.

Playback

The permission to play back videos of the selected devices on the site.

4. Tap **Next**.

5. Select a handover method.

- Tap **Hand Over via QR Code**, then show the QR code to customer in person, or tap  to share the QR code via a third-party application. Then ask your customer to scan the QR code with LTS Connect (V5.2.3 or later) to finish the handover.
- Tap **Hand Over via Phone/Email**, tap **Phone Number** or **Email**, enter the email address or phone number of the customer, enter the remarks (optional), and tap **Submit Application**.
- If you select **Hand Over via Phone/Email**, your customer will receive the handover application in their email box or via short message with a download link of the LTS Connect Mobile Client.
- If your customer has not registered an LTS Connect account, they must register an LTS Connect account first. After registering the account and accepting the handover via the LTS Connect Mobile Client, your customer will become the site owner.

Note

Please inform your customers to download or update the LTS Connect Mobile Client (V5.2.3 or later).

- If your customer wants you to manage and maintain more of their devices, after your customer accepts the handover via the LTS Connect Mobile Client and becomes the site owner, they must authorize related permissions to you.
6. Optional: For **Not Registered** or **To Be Accepted** sites, you can submit the handover application again.

Note

You can send the handover application up to five times in one day; the previous handover will be invalid if you send a new one.

5.8 Handing Over Personal Site via Sharing

If the devices are owned by your company, you can hand over the devices to your customers by sharing without transferring ownership of the devices. To hand over devices by sharing, you can choose between applying for permissions from your customer (Mode A) and NOT applying for permissions from your customer (Mode B).

Before You Start

- Make sure the site status is **Not Handed Over**, and you have the permission for site management, such as managing all sites and assigning sites.
- Make sure the devices are added to the site. The supported devices include access control devices, encoding devices, video intercom devices.

Steps

Note

You can only hand over personal sites by sharing.

1. In the site list, tap a site to access the site details page.
2. Tap **Hand Over Site** → **Hand Over by Sharing**.
3. Select the resources and permissions to be shared with your customer.
4. Tap **Next**.
5. 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**.
In this mode, you must set the permissions to apply for from your customer and their validity periods. The permissions include configuration, live view, playback, and sub permissions. The configuration permissions are selected by default and cannot be deselected.
 - Mode B: Enable **I Have All Device Permissions** to confirm that you have all permissions for the devices and do not need to apply for permissions from your customer for remote maintenance.

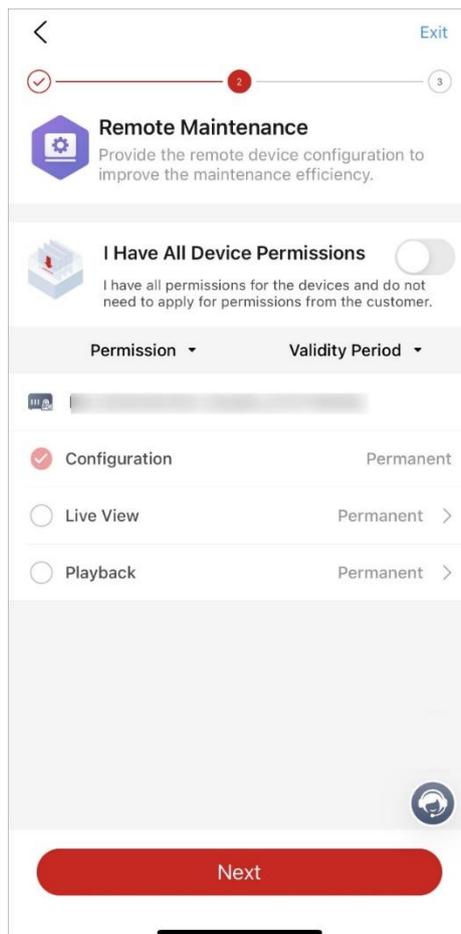


Figure 5-11 Enable "I Have All Device Permissions" or Not

6. Tap **Next**.

Note

For the following steps, you must choose between to hand over to only one customer or to hand over to multiple customers.

7. Optional: Hand over to only one customer.

Note

- For Mode A, only one customer will be the customer administrator who reviews your application for permissions.
- To accept the handover (by sharing), your customer's LTS Connect must be V5.4.0 or later.

- Tap **Hand Over via QR Code**, then show the QR code to customer in person, or tap  to share the QR code via a third-party application. Then ask your customer to scan the QR code with LTS Connect (V5.2.3 or later) to finish the handover.
- Tap **Hand Over via Phone/Email**, tap **Phone Number** or **Email**, enter the email address or phone number of the customer, enter the remarks (optional), and tap **Submit Application**.

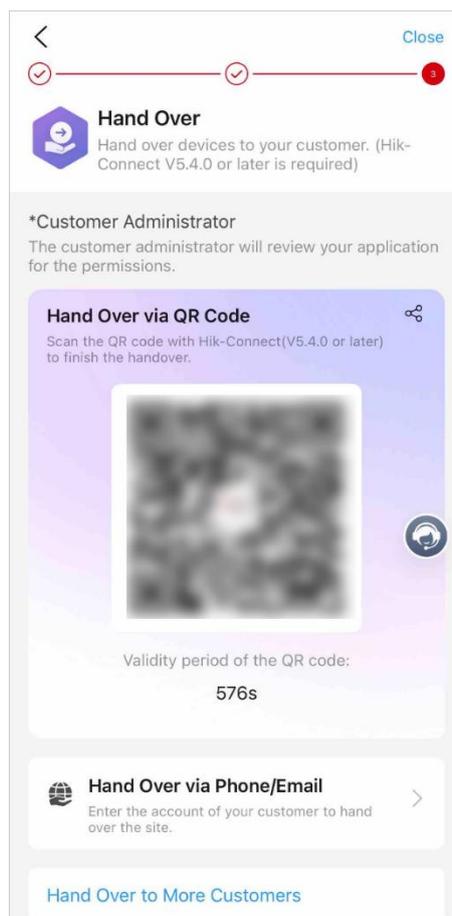


Figure 5-12 Add Customer Account

8. Optional: To hand over to multiple customers, tap **Hand Over to More Customers** at the bottom of the page.

 **Note**

- For Mode A, if you add more than one customer account to share with, you will be asked to select one customer as the customer administrator who reviews your application for device permissions.
- One device can be shared with no more than 10 customers.
- To accept the handover (by sharing), your customer's LTS Connect must be V5.4.0 or later.

- Tap **Hand Over via QR Code** and ask multiple customers to scan the QR code with LTS Connect (V5.4.0 or later) to finish the handover.
- Tap **Hand Over via Phone/Email**, tap  to add more customers' phones/emails, enter remarks (optional), and tap **Submit Application**.

9. Optional: After sites are shared, you can perform the following operations:

Check Sharing Details	Tap a shared site, and tap  → Customer to check sharing details including customer accounts and sharing statuses.
Share Again	Tap a shared site, and tap  → Customer . If rejected or expired, you can tap Share Again to share the site again.
Cancel Sharing	Tap a shared site, and tap  → Customer . For sharing items that are to be accepted or already accepted, you can tap  → Cancel Sharing to cancel sharing.
View and Edit Shared Resources and Permissions	Tap a shared site, tap  → Customer , and tap the customer card to view and edit the resources and permissions that are shared with the customer.
Edit Customer Account	Tap a shared site, tap  → Customer , and tap  → Edit Account to edit the customer account. <hr/>  Note In Mode A, if the customer administrator accepts the sharing handover, you will not be able to edit their account, but you can tap Cancel Sharing send an application to the customer administrator to cancel sharing. <hr/>
Add New Sharing	Tap a shared site, and tap  → Customer . Tap  in the upper-right corner to add new customer accounts to share with them.
Add New Devices to	After a site has been shared with customers, you can still add new

Shared Sites	devices to the site. By default, these newly added devices will not be shared with any customer, but you can tap the customer cards to select these devices and their permissions to share them with the corresponding customers. The customers do not need to accept the sharing once again.
---------------------	---

5.9 Handing Over a Team Site

After the installation company completes the installation, the Installer can hand over the team site to the customer. After the site is handed over, the customer takes ownership of the devices, and usually the devices are owned by the customers. If required, the Installer can also apply for specified permissions for further device maintenance when handing over the site.

Before You Start

Make sure the site status is **Not Handed Over**, the service(s) have been activated on the site, and you have the permission for site management, such as managing all sites and assigned sites.

Steps

1. Tap **Site** to access site list page.
2. Tap a site to access the site details page.
3. Tap **Hand Over Site** to access the Handover List page.
You can view the activated services, devices added to the site (if any), etc., on the Handover List page.
4. Tap **Hand Over Site** to pop up the Hand Over Site panel.
5. Select **Email** or **Mobile** as the account type.
 - If you select **Email**, set customer's email (required), name, phone number, and remarks.
 - If you select **Mobile**, set customer's phone number (required), name, and remarks.
6. Tap **Confirm**.
 - Your customer will receive the handover application in their email box or via short message with a download link of the LTS Connect Mobile Client.
 - If your customer has not registered an LTS Connect account, tap **Send** to send a registration message to the customer. After registering the account and accepting the handover via the LTS Connect Mobile Client, your customer will become the site owner.

Note

Please inform your customers to download or update the LTS Connect Mobile Client (V5.2.3 or later).

5.10 Applying for Site Authorization from Site Owner

After the site (no permission selected when handing over site) is handed over by transferring to a site owner, if the site owner wants the Installer to maintain the devices for them, the Installer needs to send an application to the site owner to ask for authorization. After the application is approved, the Installer can get the permission to manage and configure the devices on the site. Besides, the site owner can add a device on the LTS Connect Mobile Client and authorize the Installer for further management and configuration.

Steps

Note

Only the site that is handed over by transferring supports this function.

1. Tap **Site** to access the site list page.
2. Enter the Apply for Authorization page.
 - Tap **Apply Again** in the site list.
 - Tap a site to access the Site Details page. Tap **⋮** → **Apply for Authorization** in the top right corner.
3. Enter the remarks and tap **OK** to confirm the operation.
 - The Site Owner will receive and handle the application via LTS Connect Mobile Client. After the Site Owner approves the application, the Installer will have the authorization of the Site and perform some operations.
 - If there are maintenance requirements for the devices added in LTS Connect Mobile Client, but not added and managed in the Site by the Installer yet, after consensus, the Site Owner can select the devices and authorize the permissions of the devices to the Installer.

Note

- Please inform your end users to download or update the LTS Connect Mobile Client (Version 4.5.4 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.
 - For more details about operations on LTS Connect Mobile Client, refer to the User Manual of LTS Connect Mobile Client.
-

4. Optional: On the Site Details page, tap **⋮** → **Discard Authorization** to discard authorization of the Site.

Note

For Sites with Allow Me to Disable LTS Platinum Partner Service function enabled when handing over to Installer, discarding authorization is not supported.

5.11 Accepting a Device Management Invitation from Your Customer

You can accept a device management invitation from your customer (i.e., an LTS Connect user) to manage a device that has already been added to an LTS 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 LTS Platinum Partner. Compared with migrating the device from LTS Connect to LTS Platinum Partner, which requires your customer to share their LTS 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 sections below:

- **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 LTS Connect user) has already added one device to their LTS Connect account, the customer can use the LTS 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 LTS Connect username 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 LTS Platinum Partner.

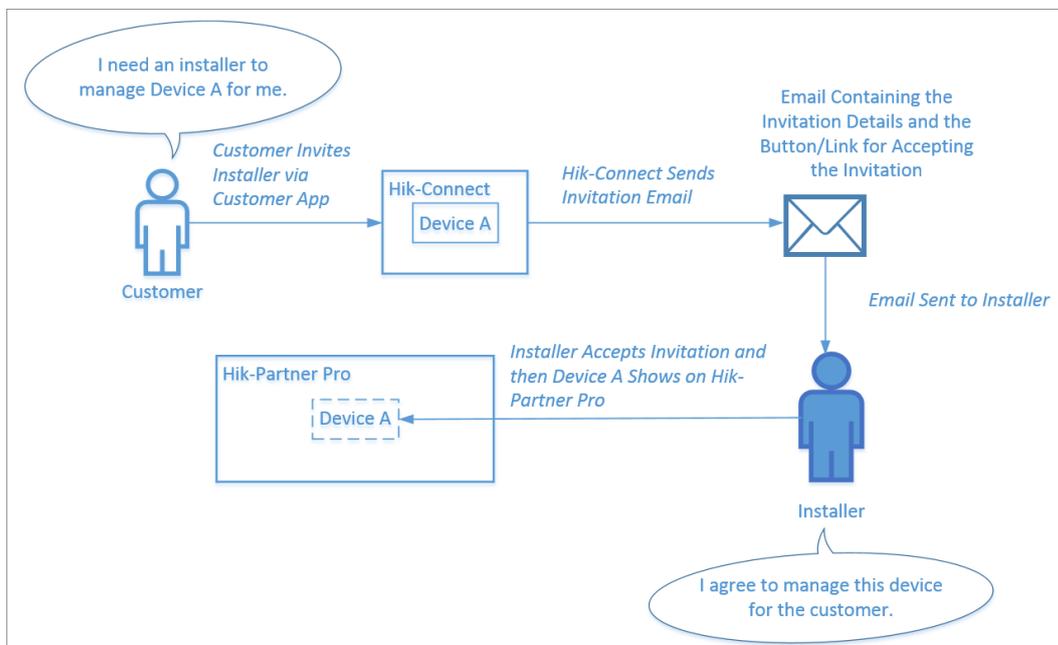


Figure 5-13 Process Diagram

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 LTS Connect Mobile Client to invite you to manage their device. It should be noted that you will need to provide your LTS Platinum Partner account (email address) to your customer first to let them specify you as the Installer who manages their device.

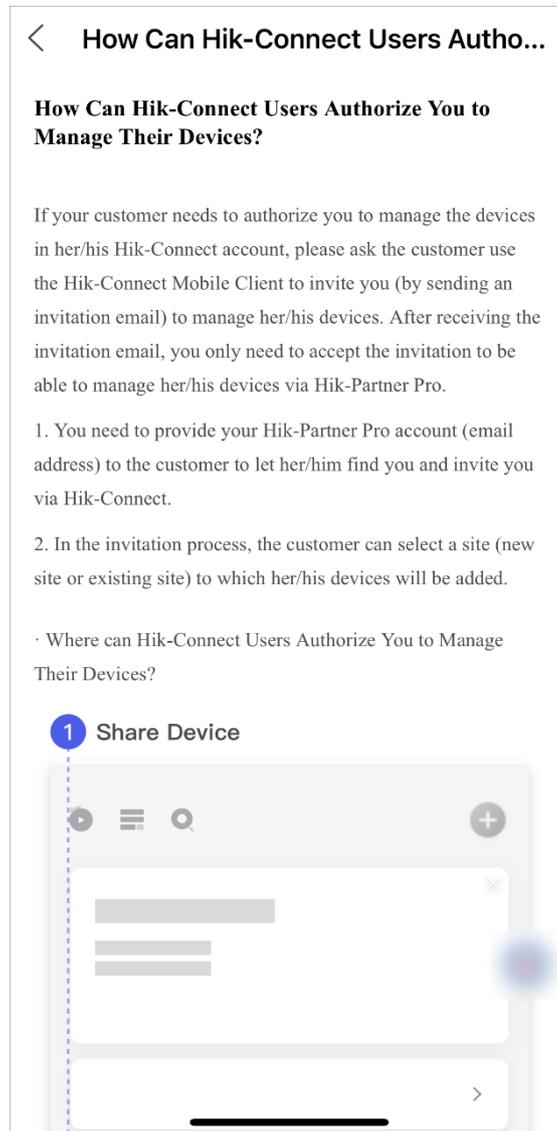


Figure 5-14 How Can LTS Connect User Authorize You to Manage Their Device

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, LTS Connect user account, and the time of invitation. If you agree to manage the device(s) for your customer, you will need to accept the invitation within 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 LTS Connect user account, and the time of invitation. If you agree to manage the device(s) for your customer, you will need to accept the invitation within three days, otherwise the invitation will be invalid.

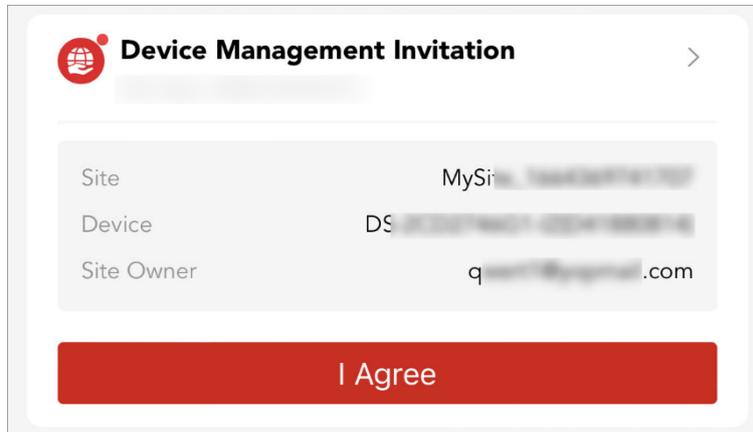


Figure 5-15 Sample Notification

5.12 Site Collaboration

Before the site handover, you can invite your installation service partner (ISP) to collaborate with you on the site so that they can help you add and hand over devices. After the site handover (by transferring), you can invite your maintenance service partner (MSP) to collaborate with you on the site in providing device management/maintenance services for your customer, especially in offering technical support. For the ISP, they have all permissions for devices on a collaborated site before the site handover, and their device permissions will be removed after the site is handed over or the collaboration is canceled. For the MSP, you can determine the permissions for them to access devices on the collaborated site, and after inviting your MSP to collaborate with you on the site, you can change the MSP's permissions.

Note

- Site collaboration that is after handover is not supported by sites handed over by sharing.
- If you change the MSP's permissions, your customer will receive a notification about it on the LTS Connect Mobile Client.
- If the site is handed over by the ISP to your customer, the handover email/message your customer receives will only contain your company's information and will not contain any information about the ISP.
- 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. For details, refer to *LTS Platinum Partner Portal User Manual*.

5.12.1 Site Collaboration During Handover

You can apply for site authorization and select permissions for the maintenance service partner at the same time when you hand over the site, to invite your maintenance service partner to collaborate with you for managing and maintaining the site together.

Before You Start

Make sure the site status is **Not Handed Over** and you have the permission to manage all sites or assigned sites.

Steps

Note

- The maintenance service partner's LTS Platinum Partner account should be an Installer Admin account, of which the country/region should be the same as that of your account.
- You cannot invite the account of any employee in your company to collaborate with you on the site.
- Only the site that is handed over by transferring supports site collaboration.

-
1. Enter the Hand Over Site page. Refer to [Hand Over Personal Site by Transferring](#) for details.
 2. In the Site Collaboration section, switch on **Apply for Site Authorization for Maintenance Service Partner**.
 3. Enter the maintenance service partner's LTS Platinum Partner account.

Note

If the account has been linked with two or more companies, select a company.

-
4. Select permissions for the maintenance service partner.

Note

- You can set the validity period for the permissions of configuration, live view, and playback, and select the device(s).
 - If you have no permission to manage devices, or no devices are added to the site, you cannot select the permissions of configuration, live view, and playback when handing over the site.
 - If the following permissions are selected, when your customer accepts the handover and the maintenance service partner accepts site collaboration, the permissions will be authorized to the maintenance service partner.
-

Site Information Management

The permission to manage the site information.

Configuration

The permission to configure selected devices on the site.

Live View

The permission to stream the live video from the selected devices on the site.

Playback

The permission to play back videos of the selected devices on the site.

5. Configure other settings on the Hand Over Site page. Refer to **Hand Over Personal Site by Transferring** for details.

6. Tap **OK**.

7. Optional: After your customer accepts the handover and the maintenance service partner accepts the site collaboration, perform the operations below.

View Information About the Maintenance Service Partner	You can view the status of site collaboration and the email address of the maintenance service partner on the site details page.
Cancel Site Collaboration	You can cancel site collaboration on the Site Collaboration page.
Change Permissions for the Maintenance Service Partner	<p>You can change permissions for the maintenance service partner on the Site Collaboration page.</p> <hr/> <p> Note</p> <p>You can only change the permissions that have already been granted to the maintenance service partner by your customer, and your customer will receive a notification on their LTS Connect Mobile Client if the permissions are changed.</p> <hr/>

5.12.2 Accepting a Site Collaboration

If you are the maintenance/installation service partner (MSP/ISP), you can receive and handle the site collaboration application in the Notification Center on LTS Platinum Partner.

Before You Start

- If you are the MSP, make sure the site owner has agreed to the device permission application on the LTS Connect Mobile Client.
- Make sure you (MSP/ISP) have logged in to the LTS Platinum Partner.

Steps

Note

If you (ISP) are invited to collaborate on a site, all accounts of your company can view the site collaboration application in the Notification Center, but only the ISP account specified in the site collaboration application and the accounts with the Manage All Sites permission can handle the application.

1. Tap  in the upper-right corner of the page to access the Notification Center page.
2. Tap the **Business Notification** tab.
3. Tap **I Agree** to accept the site collaboration.

For MSPs, you can manage and maintain devices on the collaborated site; for ISPs, you can add, configure, and hand over devices on the collaborated site.

5.12.3 Features Available to MSP/ISP on a Collaborated Site

After the maintenance/installation service partner (MSP/ISP) accepts the site collaboration, the MSP can perform configurations and operations which the customer authorized on the collaborated site, and the ISP can add, configure, and hand over devices on the collaborated site. The MSP can also release device permissions, and both the MSP and ISP can cancel the site collaboration. If the MSP is authorized to manage the site, the MSP can directly apply from the customer for device permissions.

Note

The MSP/ISP who accepted the site collaboration cannot invite another MSP/ISP for collaboration on the site.

Customer Site

For MSP

Live view and playback, arming and disarming, remote configuration, device upgrade, linkage rule configuration, DDNS configuration, password reset, exception notification configuration, and deleting the site.

Note

If the MSP deletes the site, it indicates that the site authorization is discarded by the MSP, but the installer can still manage the sites and their devices.

For ISP

Adding and deleting devices, live view and playback, arming and disarming, remote configuration, linkage rule configuration, DDNS configuration, exception notification configuration, device upgrade, remote log collection, editing device names, editing site information (except the site name), and site handover.

Health Monitoring

Viewing the statuses of devices on the collaborated sites, device remote configuration, refreshing device status, live view, playback, manually inspecting devices, exporting health check reports, and device upgrade.

Exception Center

Receiving device exceptions and exporting exception records.

Send Report Regularly

Configuring report settings to send reports regularly.



Note

This feature is not available to the ISP.

My Service

Viewing the validity periods, expiration time, and status of activated services of the collaborated site and their corresponding resources.



Note

- The MSP cannot activate or transfer services on the collaborated site.
 - This feature is not available to the ISP.
-

MSP Applies from Customer for Device Permissions

If the MSP is authorized to manage the site, the MSP can directly apply from the customer for device permissions. The installer who invited the MSP for collaboration on the site will receive the notification after the MSP sends the application for device permissions.

For how the MSP applies from the customer for device permissions, refer to [**Apply for Device Permission**](#).

MSP Releases Device Permissions

If the MSP does not need device permissions, or the MSP finished the device configuration task earlier than the planned time, the MSP can release the permission.

For how the MSP releases device permissions, refer to [**Release the Permission for Devices**](#).

MSP/ISP Cancels Site Collaboration

The MSP/ISP can cancel the site collaboration. After the site collaboration is canceled, the site (and also the devices on the site) will be deleted from the MSP/ISP's LTS Platinum Partner account, and the granted permissions will be removed.

Chapter 6. Using IP Portal Tool for On-Site Configuration

The IP Portal 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 LTS Platinum Partner, and hand over the devices to customers. Most of these are done automatically and all are done smoothly, with just the LTS Platinum Partner Mobile Client, and no need for a computer or monitor, which greatly increases the installers' work efficiency.

This article contains the following sections:

- **[IP Portal Tool Overview](#)**
- **[Prepare the Devices](#)**
- **[Search for Devices on LAN](#)**
- **[Initialize NVR on LAN](#)**
- **[Initialize Device on LAN \(Excluding NVRs\)](#)**
- **[Batch Activate Devices](#)**
 - **[Batch Activate One NVR Together with One or More Network Cameras](#)**
 - **[Batch Activate Other Combinations of Devices](#)**
- **[Add Channels to Activated NVR](#)**
- **[Configure and Manage NVR / DVR / Network Camera Channels on the Live View Page](#)**
 - **[Set Image Parameters](#)**
 - **[Set Video Parameters](#)**
 - **[Edit Channel Name and Information](#)**
- **[Sort NVR Channels](#)**
- **[Set Verification Method for Password Reset](#)**
- **[Add Devices on LAN \(via IP Portal Tool\)](#)**
- **[Reset Device Password via IP Portal Tool](#)**
 - **[Reset Password by Entering Old Password](#)**
 - **[Reset Password via Reserved Email](#)**
 - **[Reset Password by Answering Security Questions](#)**
 - **[Reset Password by Submitting Case](#)**
 - **[Reset Password by Sending Email to Technical Support](#)**
- **[Add Devices to LTS Connect](#)**
- **[More Features with IP Portal Tool](#)**

IP Portal Tool Overview

Prepare the Devices

To use the IP Portal tool on the Mobile Client, make sure the devices are powered on and connected to the LAN. Connect your phone to the same LAN as the devices via Wi-Fi or adapter.

6.1 Searching for Devices on a LAN

The IP Portal tool searches for LAN devices automatically and constantly in the background.

- After you log in to the LTS Platinum Partner Mobile Client and when your phone is connected to the LAN, the IP Portal tool will search for LAN devices in the background automatically and constantly.
- When new devices are detected, the tool will check if there are any issues with the devices.
- The tool tests and displays the ping values and levels in real time. A 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
 - : 50 ms to 200 ms
 - : More than 200 ms
- When the IP Portal tool detects inactivated devices on the LAN, the window of inactivated devices will pop up.

6.2 Initializing an NVR on a LAN

Steps

1. Tap **Activate** on the IP Portal page or the pop-up window of the inactivated NVR.
2. The window for setting the device password and verification code pops up.

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 access the Device Initialization page.
4. The Device Initialization page shows the whole process of the automatic NVR initialization, which includes the following configurations:

- Activate the NVR.

The IP Portal tool checks for device batch issues during the activation, and the activation can be completed only if there is no batch issue. (The check starts right away once the tool detects the device.)

After the NVR is activated, and if there are detected inactivated network cameras, the IP Portal tool will automatically activate the network cameras and automatically add them to the NVR. (This operation will not be performed if it is a PoE NVR and the PoE channels are enabled by default.)

- Configure the device network based on your phone's network settings.
DLCP (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.

- Check the firmware update.
- Synchronize the phone time and time format to the device.
- Initialize the HDD / SD card.

The HDDs or SD cards will be initialized automatically if they are new and not initialized. If any data is stored on the HDDs and SD cards, they will not be initialized.

5. After the initialization is completed, 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.)

What to do next

After the initialization is completed, 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.)

Refer to [**Add Channels to Activated NVR**](#), [**Sort NVR Channels**](#), [**Add Devices on LAN \(via IP Portal Tool\)**](#), and [**Add Devices to LTS Connect**](#).

6.3 Initializing Devices on a LAN (Excluding NVRs)

Besides NVRs, you can use the IP Portal tool to initialize network cameras (including PTZ cameras and thermal cameras), DVRs, access control devices, video intercom devices, and network switches.



Note

To initialize NVRs via the IP Portal tool, refer to [**Initialize NVR on LAN**](#).

Steps

1. Tap **Activate** on the IP Portal page or on the pop-up window of the inactivated device.
2. The window for setting the device password and verification code pops up.

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 access the Device Initialization page.
4. The Device Initialization page shows the whole process of the automatic initialization, which includes the following automatic configurations:

- Activate the device.
The IP Portal tool checks for device batch issues during the activation, and the activation can be completed only if there is no batch issue. (The check starts right away once the tool detects the device.)
- Configure the device network based on your phone's network settings.
 - For network switches (except for EI-series switches) and all DVRs, DLCP is enabled automatically.
For network cameras, DLCP is disabled automatically, in case IP address changes lead to the device going offline.

For other devices, DLCP 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 the firmware update.
- Synchronize the phone time and time format to the device.
- Initialize the HDD / SD card.

The HDDs or SD cards will be initialized automatically if they are new and not initialized. If any data is stored on the HDDs and SD cards, they will not be initialized.

- The LTS Connect service will be automatically enabled if it is supported by the device.
- If the device is a network camera, the following configurations will be done automatically:
 - Enable **Motion Detection 2.0** automatically. All the area is set as the detection area and **Notify Surveillance Center** is enabled.
 - Set the encoding format. 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.

5. Tap **Complete Initialization**.

6.4 Batch Activating Devices

Using the IP Portal tool, you can automatically batch activate multiple devices. The configuration details are different according to different combinations of devices.

This article contains the following sections.

- **[Batch Activate One NVR Together with One or More Network Cameras](#)**
- **[Batch Activate Other Combinations of Devices](#)**

6.4.1 Batch Activating One NVR Together with One or More Network Cameras

Steps

1. Tap → **Batch Activate** on the IP Portal page, select devices to activate, and tap **Next**. Or tap **Activate** on the pop-up window of the inactivated devices.

2. The window for setting the device password and verification code pops up.

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**.

4. Tap **Yes** or **No** in the pop-up window to set whether to add the activated network cameras as channels of the NVR.

5. The Device Initialization page shows the whole process of the automatic NVR initialization.

- You can close the page and tap other devices to show the corresponding Device Initialization pages.
- For details about the automatic initialization process, refer to **[Initialize NVR on LAN](#)** and

Initialize Device on LAN (Excluding NVRs).

6. After the initialization completes, tap **Next**.

If you select **Yes** in Step 4 to add the activated channels automatically, the page for automatic adding channels will be displayed.

7. Enter the device-adding process.

Refer to **Add Devices on LAN (via IP Portal Tool)** and **Add Devices to LTS Connect**.

6.4.2 Batch Activating Other Combinations of Devices

Steps

1. Tap  → **Batch Activate** on the IP Portal page, select devices to activate, and tap **Next**. Or tap **Activate** on the pop-up window of the inactivated devices.

2. The window for setting the device password and verification code pops up.

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 automatic initialization process.

For details about the automatic initialization process, refer to **Initialize NVR on LAN** and **Initialize Device on LAN (Excluding NVRs)**.

6.5 Adding Channels to Activated NVR

You can automatically add inactivated cameras as NVR channels, or manually select both activated and inactivated cameras to add as channels.

This article contains the following sections.

- **Automatically Add Channels to NVR**
- **Manually Select Channels to Add to NVR**

6.5.1 Automatically Adding Channels to NVR

Only inactivated cameras will be automatically activated and added to the NVR in this method.

Steps

1. Initialize the NVR.

2. Tap  → **Auto Add** or  →  **Add Channel** → **Auto Add** on the device card of the IP Portal page or tap **Auto Add** on the pop-up window named Add Chanel after the NVR initialization.

3. All inactivated cameras are automatically added to the NVR.

- During the channel-adding process, the IP Portal tool activates the cameras, sets IP addresses, disables DLCP, checks firmware updates, and then adds them to the NVR.
- After the channels are added, the IP Portal tool enables **Motion Detection 2.0** automatically if

it is supported by the cameras and **Notify Surveillance Center** is enabled.

4. Drag the channels to sort them. (If the total number of channels of the NVR is more than 1 after you add the channels, you will access the Sort Channels page.)

Note

- Channel sorting is supported only by some NVR models.
 - Refer to [***Sort NVR Channels***](#).
-

6.5.2 Manually Selecting Channels to Add to NVR

You can select both inactivated and activated cameras to add them to the NVR, and the inactivated cameras will be automatically activated.

Steps

1. Initialize the NVR.
2. Tap  → **Manually Select** or  →  **Add Channel** → **Manually Select** on the device card of the IP Portal page or tap **Manually Select** on the pop-up window named Add Chanel after the NVR initialization.
3. Select the cameras to be added as channels, and tap **Confirm**.
4. The selected cameras are automatically added to the NVR.
 - During the channel-adding process, the IP Portal tool activates the inactivated cameras, sets IP addresses, disables DLCP, and checks firmware updates. Then it adds all the selected cameras to the NVR.
 - After the channels are added, the IP Portal tool enables **Motion Detection 2.0** automatically if it is supported by the cameras and **Notify Surveillance Center** is enabled.
5. Drag the channels to sort them if you access the Sort Channels page. (If the total number of channels of the NVR is more than 1 after you add the channels, you will access the Sort Channels page.)

Note

- Channel sorting is supported only by some NVR models.
 - Refer to [***Sort NVR Channels***](#).
-

6.6 Configuring & Managing NVRs, DVRs, & Network Camera Channels on the Live View Page

The IP Portal 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, username, and password), sort

channels, add channels, and delete channels.

Note

The available parameters and operations vary according to the device's capabilities.

Enter the channel management page (also the live view page) by one of the following ways.

- Tap  or  →  **Live View** on the device card of an NVR / DVR / network camera.
- Tap an activated NVR / DVR / network camera on the IP Portal page, and then select the **Channel** tab.
- Tap  or  →  **Playback** on the device card of an NVR / DVR / network camera, and then tap **Live View**.

Refer to the following sections to learn more.

- [Set Image Parameters](#)
- [Set Video Parameters](#)
- [Edit Channel Name and Information](#)

Set Image Parameters

With image parameters, you can control the exposure and color effects of the video image produced by your camera.

On a channel card, tap  or  →  **Image Parameters**.

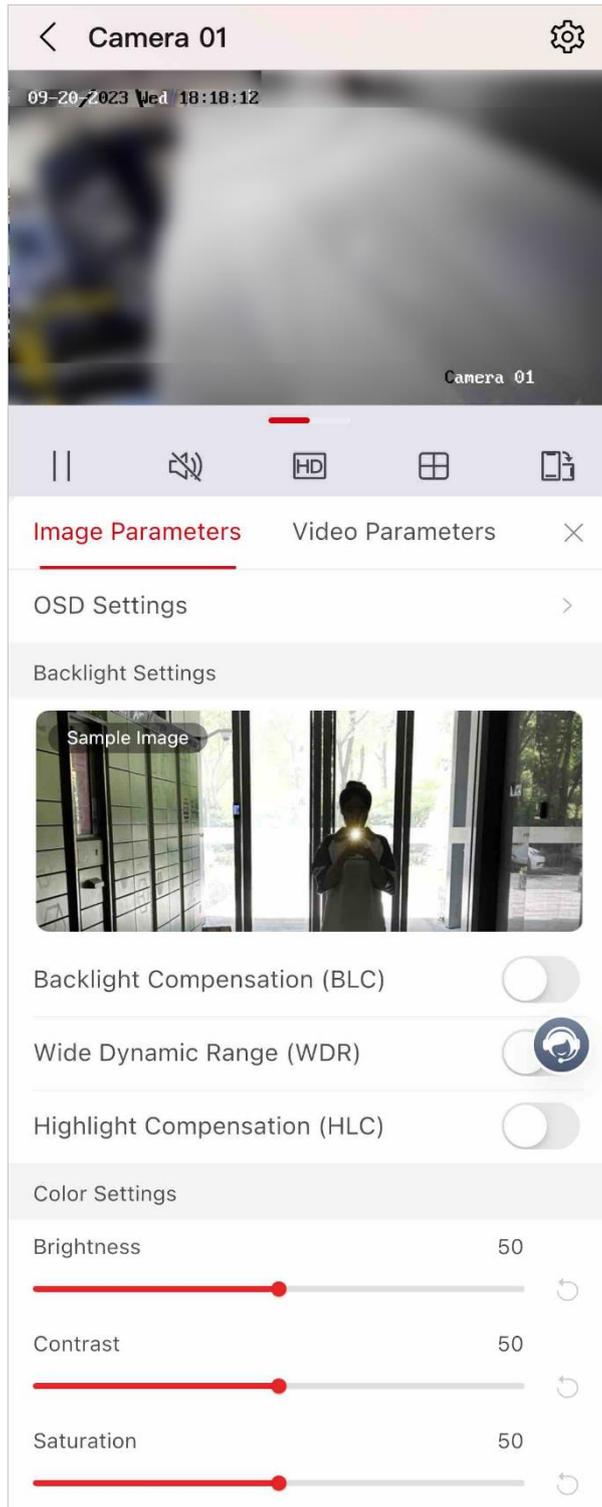


Figure 6-7 Image Parameters

Scene Direction

Select the rotating direction of the camera. You can set it to **Up/Down**, **Left/Right**, or **Center**, or you can select **Restore Default** to restore to the default direction.

OSD Settings

Set whether to display the camera and time information on the video, and way they are displayed.

Camera

Enable/disable **Display Name** to display or to not display the camera name on the video. You can tap **Camera Name** to edit the camera name and set where on the video it is displayed by setting the **Position** to **Lower Right**, **Lower Left**, **Upper Left**, or **Upper Right**.

Time

Enable/disable **Display Time** to display or to not display the time on the video. You can tap **Date Format** to set the format of the displayed date (eg., YYYY-MM-DD), tap **Time Format** to set it to **24-Hour** or **12-Hour**, set where on the video it is displayed by setting the **Position** to **Lower Right**, **Lower Left**, **Upper Left**, or **Upper Right**, and set whether to display the day of the week together with the date by enabling/disabling **Display Day of Week**.

Backlight Settings

If your camera video contains areas that are either too dark or too bright, you can adjust the exposure of the image via the BLC, WDR, or HLC settings to end up with a cleaner and more detailed image. BLC and HLC compensate for uneven brightness via digital adjustments, whereas WDR uses the camera's hardware to provide even brightness.

While adjusting the backlight settings, you can refer to the sample image to preview the effect of your settings.

Note

Only one of BLC, WDR, and HLC can be enabled at the same time.

Backlight Compensation (BLC)

Backlight compensation (BLC) is a setting that allows you to select the **BLC Area** where the light is too strong to reduce exposure of this area, thus increasing the exposure of other dark areas, so you can see details in other comparatively dark areas.

After **Backlight Compensation (BLC)** is enabled, you can tap **BLC Area** to set it to **Auto**, **Up**, **Down**, **Left**, **Right**, or **Center**. When you set it to **Auto**, the intelligent algorithm will recognize the area with too strong light automatically for compensation.

Wide Dynamic Range (WDR)

By enabling **Wide Dynamic Range (WDR)**, you can have proper brightness on both the darker and brighter parts of the image, so you can see more details across a wider dynamic range between the shadows and highlights.

When **Wide Dynamic Range (WDR)** is enabled, you can also adjust the strength of the WDR by adjusting the WDR value. The higher the value, the less contrast there will be between the

darker and brighter parts. Adjust this setting sparingly, as the higher the WDR value, the lower quality video your camera will produce. By enabling **Auto Adjust WDR**, the WDR value will be automatically adjusted based on the actual environment.

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, so that you can see details in brighter parts of the video that would otherwise be overexposed.

When **Highlight Compensation (HLC)** is enabled, you can also adjust the strength of HLC by adjusting the compensation value. The higher the value, the darker the image will be. Adjust the compensation value sparingly until you can see enough detail in the brighter parts of the video.

Color Settings

By adjusting the basic camera parameters including **Brightness, Contrast, Saturation, and Sharpness**, you can make your camera produce the video image according to your needs.

Set Video Parameters

Set the parameters related to video streaming.

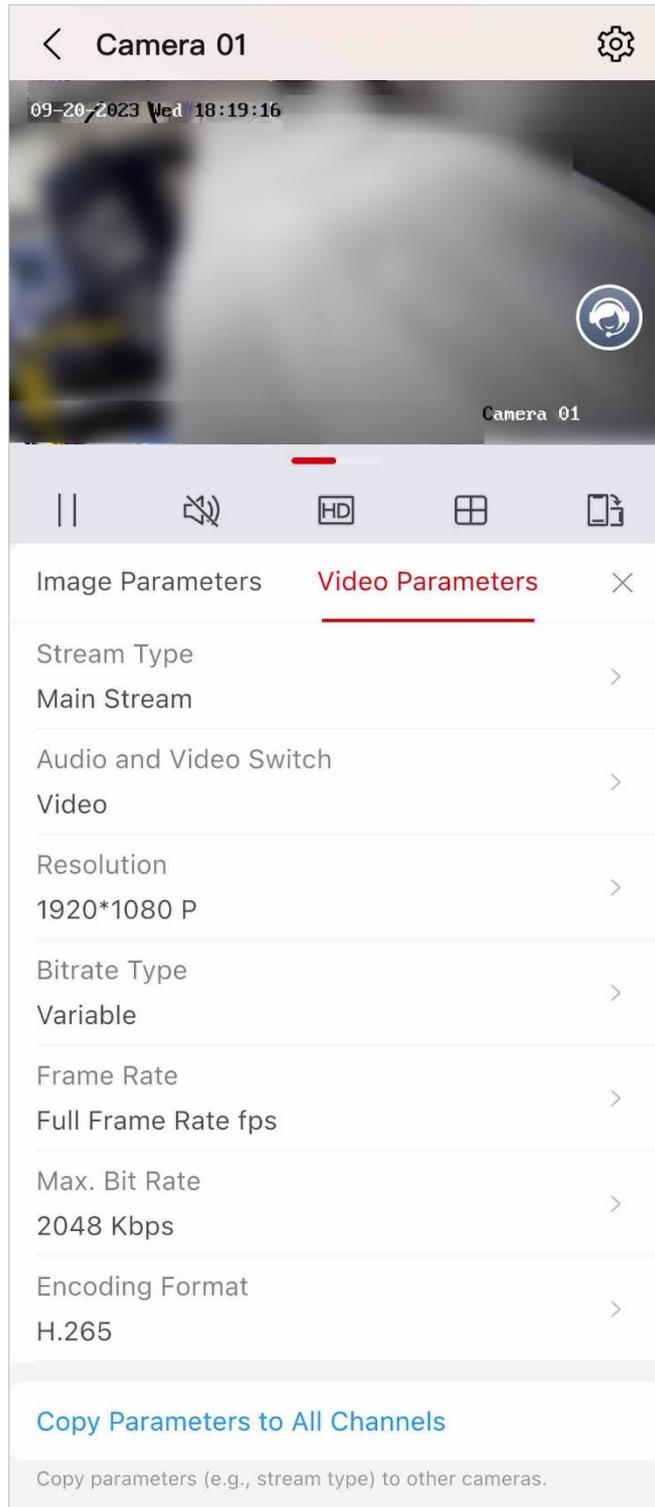


Figure 6-8 Video Parameters

Stream Type

For devices that support more than one stream, you can specify parameters for each stream type.

Main Stream

The main stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But a high resolution or a high frame rate usually means larger storage space and higher bandwidth requirements.

Sub Stream

The sub stream usually offers comparatively low resolution options and consumes less bandwidth and storage space.

Audio and Video Switch

Select the content (only video or both video and audio) that is contained in the stream.

Resolution

Select the video resolution according to your actual needs. A higher resolution requires higher bandwidth and larger storage.

Bitrate Type

Constant Bitrate

It means that the stream is compressed and transmitted at a comparatively fixed bitrate. The compression speed is fast with the constant bitrate, but mosaic may occur across the image.

Variable Bitrate

It means that the device automatically adjusts the bitrate under the set **Max. Bitrate**. The compression speed is slower than that of the constant bitrate. But it guarantees the image quality of complex scenes.

Frame Rate

The frame rate is the frequency at which the video stream is updated, and it is measured by frames per second (fps).

A higher frame rate is advantageous when there is movement in the video stream, as it guarantees image quality throughout. Note that a higher frame rate requires higher bandwidth and larger storage space.

Max. Bitrate

The maximum bitrate is to limit the compression speed and guarantee image quality.

Encoding Format

The compression standard the device adopts for video encoding. The options are **H.264**, **H.265**, **H.264+**, or **H.265+**. The options vary according to the device's capabilities. For details about various compression standards, refer to the camera user manuals.

Copy Parameters to All Channels

After you set the parameters, you can tap **Copy Parameters to All Channels**, and then tap

Confirm, to copy the parameters to all other channels of the current device.

Edit Channel Name and Information

Tap **...** → **Edit Name** to edit the channel name.

Tap **...** → **Edit** to edit the channel information including the IP address, management port, username, and password.

6.7 Sorting NVR Channels

After you add channels to an NVR, you can sort the channels.

Steps

Note

Channel sorting is supported only by some NVR models.

1. Enter the Sort Channels page.
 - After you add channels to an NVR, and if the total number of channels of the NVR is more than 1, you will navigate to 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 access the Sort Channels page.
2. Drag and drop the channels to sort them.

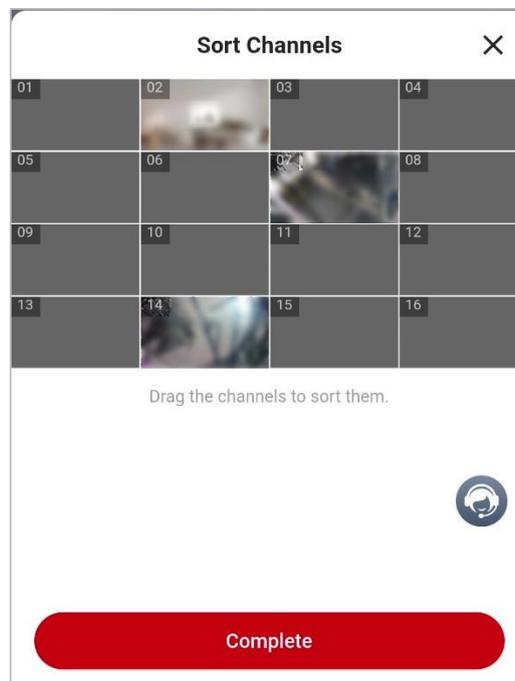


Figure 6-10 Sort Channels

3. Tap **Complete** to finish sorting.

6.8 Setting Verification Method for Password Reset

After the device is activated or initialized, you are recommended to set the verification method for password reset.

Steps

1. Initialize the device.
2. Tap  → **Settings** on the IP Portal page.

Note

Setting the verification method is available only when the device is not added to LTS Platinum Partner and no verification method is set for the device.

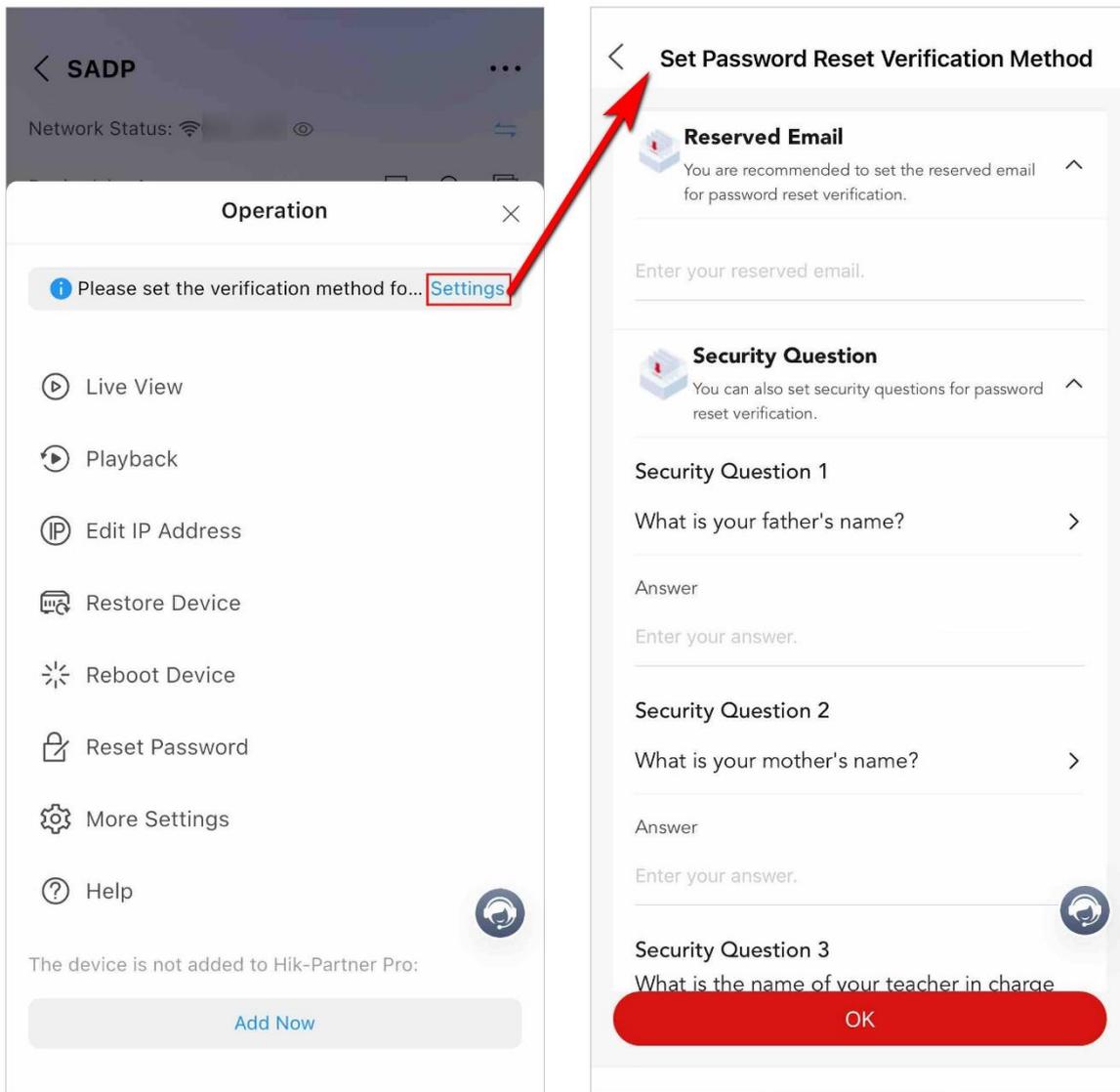


Figure 6-11 Set Verification Method

3. Set either or both of the reserved email and the answers to 3 security questions.
4. Tap **OK**.

What to do next

After the verification method is set successfully, you can reset the device password via the reserved email or the security questions. Refer to ***Reset Device Password via IP Portal Tool***.

6.9 Adding Devices on LAN (via IP Portal Tool)

You can add devices to the Mobile Client via IP Portal.

Steps

1. Enter the device adding page.
 - Tap **Add** in the Site & Device area on the Home page.
 - Tap **Site** on the bottom, and then tap **Add Device** above the site list.
 - Tap **Site** on the bottom, tap a site to access its details page, and tap **Add Device** or  → **Add Device**.
 - Tap  in the upper-left corner on the Home page.
2. Tap **IP Portal**.
3. Optional: Tap **Activate** to activate and initialize the devices to be added if they are not activated. Refer to [Initialize NVR on LAN](#), [Initialize Device on LAN \(Excluding NVRs\)](#), and [Batch Activate Devices](#) for details.
4. Tap **Complete** to access the Add to LTS Platinum Partner page.
5. Optional: 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 a new, automatically created site.
6. Select the devices to be added and tap **OK**.
7. Optional: Tap **Complete** and the added devices are displayed on the page of the site.

6.10 Resetting Device Password via IP Portal Tool

The IP Portal tool offers various ways of password reset, and there is always one way to suit your situation, regardless of whether you have forgot the password or not, whether you have set the verification method for password reset or not, and whether submitting support cases is supported in your country/region or not.

This article contains the following sections.

- [Reset Password by Entering Old Password](#)
- [Reset Password via Reserved Email](#)
- [Reset Password by Answering Security Questions](#)
- [Reset Password by Submitting Case](#)
- [Reset Password by Sending Email to Technical Support](#)

6.10.1 Resetting Password by Entering Old Password

If you do not forget the password, you can reset it by entering the old password.

Steps

1. Tap  →  **Reset Password** on the IP Portal page.
2. Select **Know Password** if you know the old password.

< Set New Password

Old Password

Please enter. 

New Password

Please enter. 

8 to 16 characters allowed, including at least 2 of the following types: uppercase letters, lowercase letters, digits, and special characters (!\"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~Space).

Confirm Password

Please enter again. 



OK

Figure 6-12 Reset Password via Old Password

3. Enter the old password and the new password.
4. Enter the new password again to confirm.
5. Tap **OK**.

6.10.2 Resetting Password via Reserved Email

If you forgot the password, and if you have set a reserved email, you can reset the password via reserved email.

Steps

1. Tap **...** → **Reset Password** → **Forgot Password** on the IP Portal page.
2. Read carefully the Privacy Policy, and tap **Agree** to continue.
3. Select **Forgot Password**.

4. Enter the reserved email and tap **Send Verification Code**.
5. Enter the received verification code and tap **OK**.
6. Set a new device password and tap **OK**.

6.10.3 Resetting Password by Answering Security Questions

If you forgot the password, and if you have set answers to security questions, you can reset the password by answering the questions.

Steps

1. Tap **⋮** → **Reset Password** → **Forgot Password** on the IP Portal page.
2. Optional: If you have also set the reserved email, read carefully the Privacy Policy, tap **Agree** to continue, and select **Security Questions**.
3. Enter the answers to the 3 security questions and tap **OK**.

< **Reset Device Password**

What is the name of your teacher in charge of class in senior high school?

What is the name of the roommate you most familiar with?

Who influences you most?

Forgot the security questions? [Send Email / Submit Case](#)

OK

Figure 6-14 Reset Password via Security Questions

4. Set a new device password and tap **OK**.

6.10.4 Resetting Password by Submitting Case

If you have not set the reserved email or security questions and have forgot the password, and the Case module is supported in your country/region, you can reset the password by submitting a device password reset case.

Steps

1. Tap **...** → **Reset Password** → **Forgot Password** on the IP Portal page.
2. Upload the image of the device label / Invoice, confirm and check the statement, and tap **OK**.

 **Note**

- The serial No. and the password reset QR code / string from IP Portal are filled in automatically and cannot be edited.
 - Refer to **[Submit Device Password Reset Case](#)** for more details about the cases.
-

6.10.5 Resetting Password by Sending Email to Technical Support

If you have not set the reserved email or security questions and have forgot the password, and the Case module is not supported in your country/region, you can reset the password by sending an email to technical support.

Steps

1. Tap  →  **Reset Password** → **Forgot Password** on the IP Portal page.

Figure 6-15 Reset Password via Technical Support

2. Upload the image 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 IP Portal is filled in automatically and cannot be edited.

3. 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**.

 **Note**

If you do not receive a reply, you can tap **Send Again** to send the email again.

Reset Device Password

Copy the Reset Code/String returned by the email and paste it into the input box of Reset Code/String.

Reset Code/String

Please enter. [Paste](#)

New Password

Please enter.

8 to 16 characters allowed, including at least 2 of the following types: uppercase letters, lowercase letters, digits, and special characters (!"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~Space).

Confirm Password

Please enter again.

[Send Again](#)

OK

Figure 6-16 Set New Password

6.11 Adding Devices to LTS Connect

After devices are activated or initialized, you can choose to directly add them to your or your customer's LTS Connect.

Steps

1. Enter the device adding page.
 - Tap **Add** in the Site & Device area on the Home page.
 - Tap **Site** on the bottom, and then tap **Add Device** above the site list.
 - Tap **Site** on the bottom, tap a site to access its details page, and tap **Add Device** or →

Add Device.

- Tap  in the upper-left corner on the Home page.
2. Tap **IP Portal**.
3. Optional: Tap **Activate** to activate and initialize the devices to be added if they are not activated. Refer to [Initialize NVR on LAN](#), [Initialize Device on LAN \(Excluding NVRs\)](#), and [Batch Activate Devices](#) for details.
4. Tap **Complete** to access the Add to LTS Platinum Partner page.
5. Tap **Add to LTS Connect** to switch to the page for adding devices to LTS Connect.
6. Select the devices to be added and tap **OK**.
7. Scan the device QR codes with your LTS Connect Mobile Client to finish the device adding.

6.12 More Features of the IP Portal Tool

- [Manage Default Device Password](#)
- [Check Network Status of Phone and Switch Networks](#)
- [Switch Between Device Card View and Device List View](#)
- [Search for Devices](#)
- [Edit IP Addresses](#)
- [Restore and Reboot Devices](#)
- [Live View and Playback](#)
- [More Settings](#)
- [Help](#)

Manage Default Device Password

On the top right of the IP Portal page, tap  → **Manage Default Device Password** to set a default device password and a default verification code.

During device initialization, the default password and verification code will be automatically filled in, but you can still edit and set a different password and verification code for the devices.

Check Network Status of Phone and Switch Networks

You can check the network connection details of your phone and switch networks on your phone as shown below.

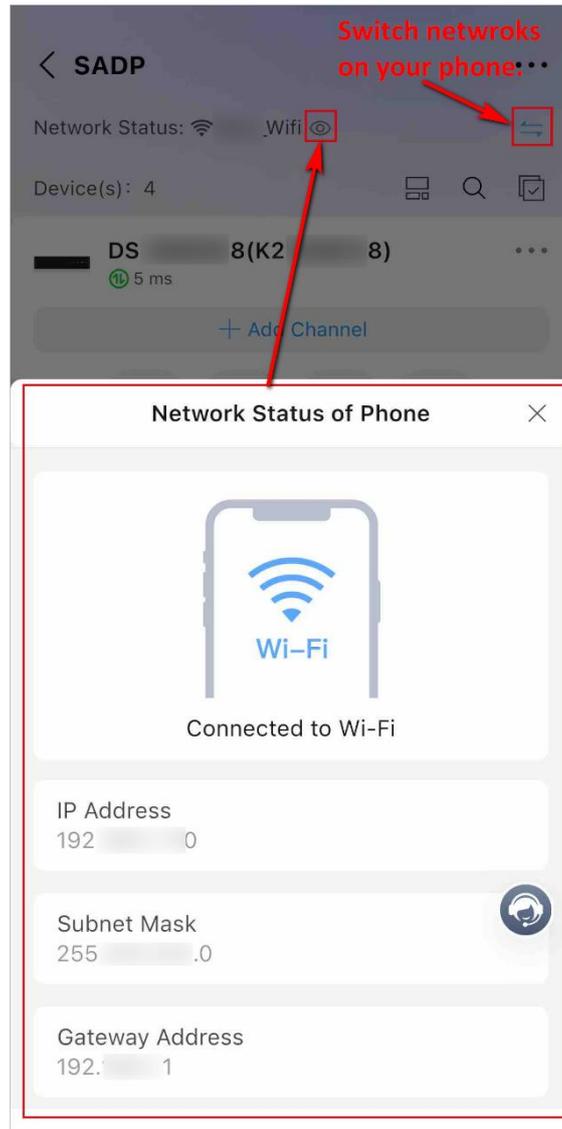


Figure 6-17 Check Network Status and Switch Networks

Switch Between Device Card View and Device List View

You can switch between the device card view and list view by tapping  and .

Both the card and list views display thumbnail images of the channels so that you can easily recognize the devices. Moreover, in card view, the device card of an NVR/DVR displays thumbnail images of all channels, and you can swipe left and right to view all the thumbnail images.

You can check the device type icon, device name, device serial number, IP address, whether DLCP is enabled, thumbnail images of channels (for encoding devices), whether the device is added to LTS Platinum Partner, real-time ping, and device exceptions.

Search for Devices

Tap  and enter keywords of the device model and serial number to search for devices.

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 **DLCP** to automatically assign the IP address, gateway address, subnet mask, and DNS address, or disable **DLCP** 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 devices, tap  or  →  **Restore Device** on a device card to restore a single device, or tap  → **Batch Restore** to batch restore multiple devices.

To reboot devices, tap  →  **Reboot Device** on a device card to reboot a single device, or tap  → **Batch Reboot** to batch reboot multiple devices.

Live View and Playback

For live view, tap  or  →  **Live View** on a device card to view the live video.

For playback, tap  or  →  **Playback** on a device card to play back videos.

Refer to [View Live Video](#) and [Play Back Video Footage](#) for more details.

More Settings

Tap  →  **More Settings** to set more parameters of the corresponding device.

For more details, check the user manuals of the devices.

Help

Tap  →  **Help** to get more instructions about the device, including the device description, parameters, documents, etc.

Chapter 7. Device Management

LTS Platinum Partner supports multiple device types, including encoding device (e.g., solar camera), video intercom device, access control device, NVR/DVR. After adding them to the system, you can manage them and configure parameters, including remotely configuring device parameters, configuring exception rule and linkage rule, etc. After adding people counting cameras and temperature screening devices, you can also activate these services and set related parameters on the Portal.

Note

Some features may not be available in all countries or regions.

7.1 Batch Configuring Devices on LAN

You can batch configure online devices on the same Local Area Network (LAN) with the phone on which the LTS Platinum Partner Mobile Client operates. 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

- This 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 phone on which the LTS Platinum Partner Mobile Client operates.
-

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

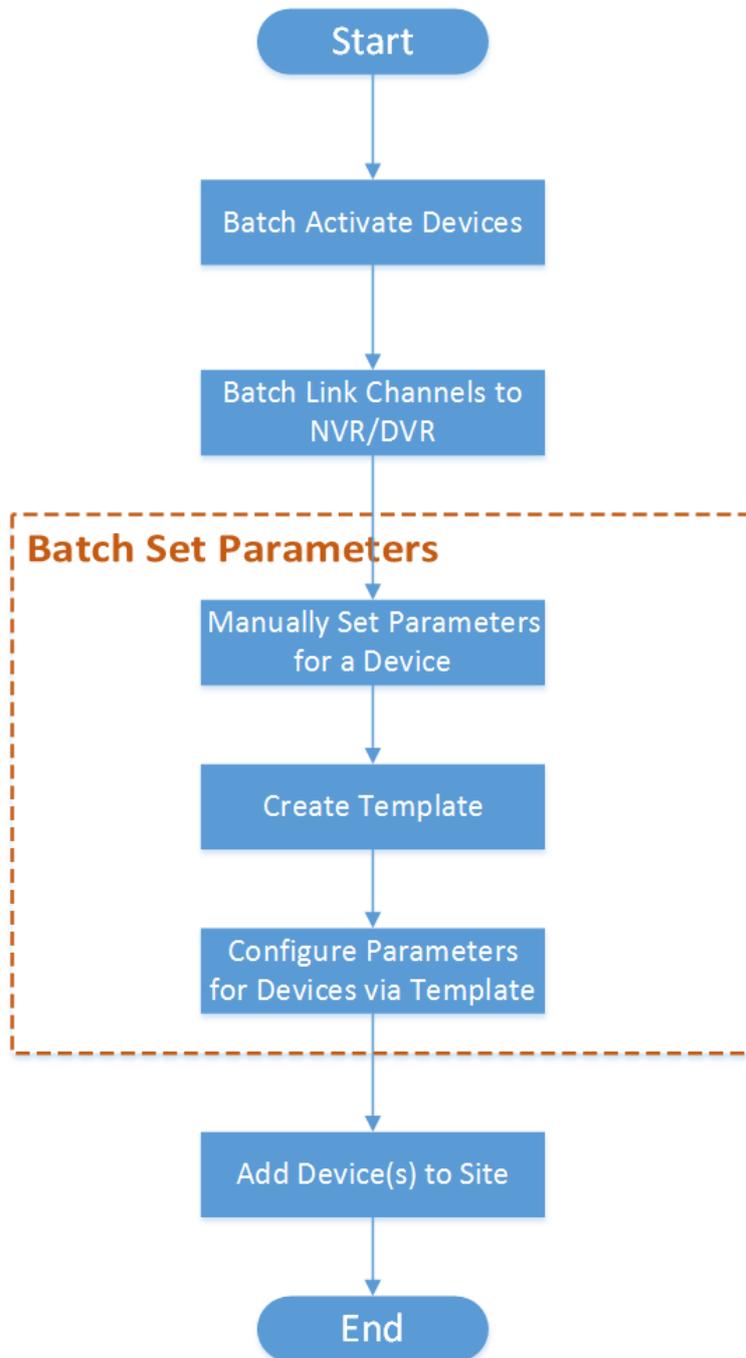


Figure 7-1 Flow Chart

Table 7-1 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 phone on which the LTS Platinum Partner Mobile Client operates and assign IP addresses for the activated devices. See <u>Batch Activate Devices and Assign IP Addresses for Them</u> for details.
Batch Link Channels to the NVR/DVR	N/A	If the activated devices include NVR/DVR, link channels to NVR/DVR. See <u>Batch Link Channels to NVR and DVR</u> for details.
Batch Set Device Parameters	Manually Set Parameters for a Device	Select an activated device and set its parameters manually. See <u>Create Templates for Setting Parameters</u> for details.
	Create Template	Created a template based on the manually configured device. See <u>Create Templates for Setting Parameters</u> for details.
	Configure Parameters for Devices via Template	Batch configure parameters for multiple devices via a selected template. See <u>Batch Set Parameters for Devices</u> for details.
Add Device(s) to Site	N/A	If required, add the activated and configured device(s) to a Site. See <u>Add Device by Scanning QR Code</u> , <u>Add Device by Entering Serial No.</u> , or <u>Add Device by IP Address or Domain Name</u> for details.

7.1.1 Batch Activating Devices and Assign IP Addresses for Them

The Mobile Client can detect available devices connected to the same network with the client, and you can activate devices and assign IP addresses 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. On the Home page, tap **On-Site Config** or **More** → **Tools** → **On-Site Config** to access the configuration page.
2. Optional: Tap **Show Inactivated Devices Only** to hide the activated devices.
3. Select the detected online devices to be activated.
4. Tap **Activate and Assign IP Address** to open the Activate and Assign IP Address window.
5. Enter the device admin password and confirm the password.
6. Tap **Activate and Assign IP Address**.

Note

- The inactivated 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, device port, HTTP port, subnet mask, gateway are assigned by the client.

The time of the mobile phone will be synchronized to the activated devices.

7. Optional: Enable **Time Synchronization** to synchronize the time from the mobile phone to the device.
8. Tap **OK**.

What to do next

After activating the devices, you can batch add channels to NVR and DVR. For details, refer to [**Batch Link Channels to NVR and DVR**](#).

7.1.2 Batch Linking Channels to NVR and DVR

If there are online NVR, DVR, and network camera on the same LAN, you can batch link the network cameras to the NVR or 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.

Steps

Note

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

1. On the Link Channel page, tap the NVR or DVR to access its details page.

 **Note**

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

2. Enter the Link Channel page.
 - Select the NVR or DVR and tap **Link Channel**.
 - Tap the NVR or DVR name.
3. In the available device list, select a device and tap  to link the device. The linked channel will be displayed in the linked channel list.
4. Optional: On the NVR or DVR details page, perform the following operations.

Edit NVR/DVR Name	On the top of NVR / DVR details page, tap Rename to edit the NVR name.
Sort Channels	Select a channel, press  and drag to change its position.
Replace Device	Select a channel and swipe left. Tap Replace Device to unlink this channel and link a new device.
Unlink Device	Select a channel and swipe left. Tap Delete to unlink channel.

7.1.3 Creating Templates for Setting Parameters

Before batch configuring parameters for devices, you may want to create a template. After creating a template, you can batch apply it to other 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. In the Parameter Template field of Configuration page, select an NVR and tap  → **Parameter Configuration** to access the remote configuration page.
2. On the remote configuration page, set parameters for the device.
3. Tap **Save as Template** on the top right.
4. Select parameters you want to save in the template and tap **Next**.
5. Enter the template name and tap **Complete** to save the template.
6. Optional: Add a new template based on device with configured parameters.
 - 1) In the Parameter Template field of Configuration page, tap **Show All** to access the Manage Template page.
 - 2) Tap **Create Template**.
 - 3) Select a device of which the parameters will be saved as the new template and tap **Next**.
 - 4) Select the parameters you want to save in the template and tap **OK**.
 - 5) Enter template name and tap **Complete** to create the template.

- 6) Optional: On the Manage Template page, select a template and swipe left, and tap **Delete** to delete a template.

7.1.4 Batch Setting Parameters for Devices

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 Templates for Setting Parameters](#) for details.

Steps

1. Enter the Select Template page.
 - Select a device and tap .
 - Select a device and tap  → **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 and tap **Apply Parameters**.
The application process and application results will be displayed.
3. Optional: Perform the following operations.

Add Device to Site	Tap Complete on the top right and add devices to Sites. See Add Device for details.
Manage Template	Tap Show All to access the Manage Template page. You can add new template or delete template. See Create Templates for Setting Parameters for details.
Edit NVR Name	Select an NVR, and tap  → Rename to edit name of NVR.
Synchronize Phone Time to Device	On the top of Parameter Configuration page, tap Synchronize to synchronize the mobile phone time to all devices.

7.2 Adding Devices

LTS Platinum Partner accesses devices by two modes: LTS Connect (P2P) and Device IP Address/Domain Name. The former provides securer data communications (between the platform and devices) and full access to features based on the LTS Connect service, such as device handover and exception notification; the latter provides faster data communications but no access to the

features based on the LTS Connect service.

Device Adding Methods

The table below shows the device adding methods for the two access modes respectively.

Access Mode	Device Adding Method
LTS Connect (P2P)	<ul style="list-style-type: none"> ● <u>Add Devices on LAN (via IP Portal Tool)</u><u>Add Device by Scanning QR Code</u> ● <u>Add Device by Entering Serial No.</u> ● <u>Synchronize Devices with LTS Connect Account</u>
Device IP Address/Domain Name	<u>Add Device by IP Address or Domain Name</u>

Following Operations

Perform the following operations after adding the device.

Operation	Description
Activate Health Monitoring Service	<p>Tap Activate Health Monitoring Service on the results page to activate the health monitoring service. See <u>Activate the Health Monitoring Service</u> for details.</p> <hr/> <p> Note</p> <p>If the service is not activated, some features such as device health monitoring and device exception notification will be unavailable.</p> <hr/>
Remote Configuration	<p>Tap the device and then tap  to remotely configure its parameters.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> ● For details, see the user manual of the device. <hr/>

Operation	Description
Delete Device	<p>On the device page, tap ● ● ● → Delete Device to delete the device.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> ● Deleting devices (except devices added by IP/Domain) is not supported if the site is authorized.
Generate Device QR Code	<ul style="list-style-type: none"> ● If a device is added by scanning the QR code generated by NVMS V3, you can generate a QR code of the device. If an end user did not add the device to his/her LTS Connect account, he/she can add it to the LTS Connect account by scanning this QR code using the LTS Connect Mobile Client. ● On the top right of a device page, tap ● ● ● → Generate QR Code to open the Generate QR Code window. ● Optional: (Optional) Enter the password to encrypt the QR code, and then tap Next. <hr/> <p> Note</p> <p>It is highly recommended that you encrypt the device QR code for security reasons.</p> <hr/> <ul style="list-style-type: none"> ● Tap Save to save the generated QR code to your phone.
Set Type for Unknown Device	<p>If the LTS Platinum Partner cannot recognize a device's type after you add it, you can manually set a device type for it.</p> <ol style="list-style-type: none"> 1. Enter a device details page, tap  of the Device Type to access the Device Type page. 2. Select a type for the device. <p>You can edit it again after the selection.</p>
Edit Device Information	<p>For devices added by scanning QR code generated by NVMS V3, if the device's information changed, or a network exception occurs, you can edit its information accordingly.</p>

Operation	Description
	Enter a device page, then tap IP/Domain to edit the device's name, IP address, port number, username, or password, then tap Save .

7.2.1 Adding Devices After Batch Configuring Them on LAN

After batch configuring devices, you can batch add these devices to the Mobile Client.

Before You Start

Make sure you have batch configured devices. For details, refer to [Batch Configure Devices on LAN](#).

After you batch configured devices, a prompt pops up about whether to add devices or not. Tap **OK** to access the Add Devices page.

Steps

1. Select a Site as the target to which devices will be added.

Note

You can select an existing Site, or you can add a new Site. For details about adding a new Site, refer to [Add Personal Site](#).

2. Select the device(s) to be added.
3. Tap **Next**.
4. Batch enter the device password, then tap **Complete**.

Note

The password will be applied to all the devices to be added. You can also edit the password for a single device.

5. Tap **Next**.

If there is a wrong password prompt, you can edit the password as prompted, or you can skip the prompt and go to the next step.

6. Configure device verification code.
 - Tap **Configure Verification Code**, and batch configure a verification code for all the devices.

Note

You can customize the verification code as needed.

- Tap **Enter Verification Code**, then enter the verification code for each device to be added.

 **Note**

You can get the verification code from the bottom of the device.

7. Tap **Next**.

The device compatibility test starts.

 **Note**

Only when all devices' compatibilities have been tested, can you add them to LTS Platinum Partner.

8. Add devices.

 **Note**

For details about adding devices, see [**Add Device by Scanning QR Code**](#) or [**Add Device by Entering Serial No.**](#).

- If there are no upgradeable devices, tap **Add** to add the selected devices.
 - If there are upgradeable devices, tap **Add and Upgrade** to add all devices and upgrade the upgradeable devices.
-

 **Note**

- If there are devices that failed to be upgraded, you can tap **Details** to view failure details.
 - Devices that failed to be upgraded can also be added to the target Sites.
-

7.2.2 Connecting an Offline Device to Network

If you want to add an offline device to the Mobile Client, connect the device to a network first.

Before You Start

Ensure that the device is powered on.

Steps

1. Add a device to the Mobile Client.
2. When the device's status indicator light flashes green, join the device LAN.
3. Choose a 2.4Ghz Wi-Fi from the nearby Wi-Fi list and enter the password.

7.2.3 Adding Devices by Scanning QR Code

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 NVMS V3.

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. Enter the adding device page.
 - Tap **Add** in the Site & Device area on the Home page.
 - Tap **Site** on the bottom, and then tap **Add Device** above the site list.
 - Tap **Site** on the bottom, tap a site to access its details page, and tap **Add Device** or  → **Add Device**.
 - Tap  in the upper-left corner on the Home or Site page.
2. Select **Scan QR Code** as the adding mode.
3. Scan QR code to add device(s) to a site.
 - Scan a QR code on a device. You can scan the QR code by aligning the QR code with the scanning frame. If there is a device QR code in the phone album, tap **Album** to extract the QR code from the local album. In this mode, you can add only one device to a site at a time.

Note

- Usually, the QR code is printed on the label, which is on the back cover of the device.
- Tap  to enable the flashlight if the scanning environment is too dark.
- Please allow the Mobile Client to access the photo album of the phone.

-
- Scan a QR code generated by NVMS V3. After scanning the QR code, you will access the page for selecting to-be-added devices. Check devices and tap **OK** to add the selected devices to site. By this mode, you can add multiple devices to site at a time.
4. Tap **Add to Site** to select a site to which the device(s) will be added.

Note

- If you have selected the site in Step 1, skip this step.
- You can add the device to an existing site, or, tap **Add New Site** to add the device to a new site.

-
5. Optional: Perform the following operations if the following situations occur.
 - If the QR code only contains the information on device serial No., you will access the add manually page. Add the device manually in this case. See **Add Device by Entering Serial No.** for details.
 - If the device is offline, you can connect to a network for the device. For details, see **Connect Offline Device to Network.**
 - If the device is not activated, tap **Activate** on the pop-up window, and then create a device admin password and tap **Activate** to activate the device.

Note

During activation, Dynamic Host Configuration Protocol (DHCP) will be automatically enabled for allocating IP addresses for the device.

-
- If the LTS Connect service is disabled for the device, tap **Enable** on the pop-up window, and then create a device verification code and tap **Enable** to enable the service.

 **Note**

Please inform your customers to download or update the LTS 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 of Portal to them.

The device will appear on the device list.

 **Note**

- After the device is added, the LTS Platinum Partner starts detecting whether the device firmware version is compatible. Some functions (including health monitoring, linkage rule, and remote configuration) are unavailable if the device is not compatible with the LTS Platinum Partner.
-

7.2.4 Adding Devices by Entering Serial No.

If a device is connected to LTS Connect Service, you can manually add it to a site by entering the device serial number and device verification code.

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. Enter the adding device page.
 - Tap **Add** in the Site & Device area on the Home page.
 - Tap **Site** on the bottom, and then tap **Add Device** above the site list.
 - Tap **Site** on the bottom, tap a site to access its details page, and tap **Add Device** or  → **Add Device**.
 - Tap  in the upper-left corner on the Home or Site page.
 2. Tap **Add Device Manually** to access the adding device page.
 3. Enter the device serial number.
-

 **Note**

The device's serial number is usually on the device label.

4. Tap **Add to Site** to select a site to which the device will be added.
-

 **Note**

- If you have selected the site in Step 1, skip this step.
 - You can add the device to an existing site, or, tap **Add New Site** to add the device to a new site.
-

5. Tap **Add**.

 **Note**

- After adding the device, the LTS Platinum Partner starts detecting whether the device firmware version is compatible. Some functions (including health monitoring, linkage rule, and remote configuration) are unavailable if the device is not compatible with the LTS Platinum Partner. Devices incompatible with the LTS Platinum Partner likely need to be upgraded. Tap **Add and Upgrade** to upgrade and add the device. For some devices, you may need to enter the device username and password. You can also upgrade the device on the device page.
-

6. Optional: Perform the following operations if the following situations occur.

- If the device is offline, you can connect to a network for the device. For details, see [***Connect Offline Device to Network***](#).
 - If the device is not activated, tap **Activate** on the pop-up window, and then create a device admin password and tap **Activate** to activate the device.
-

 **Note**

During activation, Dynamic Host Configuration Protocol (DHCP) will be automatically enabled for allocating IP addresses for the device.

- If the LTS Connect service is disabled for the device, tap **Enable** on the pop-up window, and then create a device verification code and tap **Enable** to enable the service.
 - If Enter Verification Code window pops up, enter the device verification code.
-

 **Note**

The default device verification code is usually on the device label. If no device verification code is found, enter the verification code you created when enabling the LTS Connect service.

The device will appear in the device list.

7.2.5 Adding Devices on LAN (via IP Portal Tool)

You can add devices to the Mobile Client via IP Portal.

Steps

1. Enter the device adding page.
 - Tap **Add** in the Site & Device area on the Home page.
 - Tap **Site** on the bottom, and then tap **Add Device** above the site list.
 - Tap **Site** on the bottom, tap a site to access its details page, and tap **Add Device** or  → **Add Device**.
 - Tap  in the upper-left corner on the Home page.
2. Tap **IP Portal**.

3. Optional: Tap **Activate** to activate and initialize the devices to be added if they are not activated. Refer to [Initialize NVR on LAN](#), [Initialize Device on LAN \(Excluding NVRs\)](#), and [Batch Activate Devices](#) for details.
4. Tap **Complete** to access the Add to LTS Platinum Partner page.
5. Optional: 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 a new, automatically created site.
6. Select the devices to be added and tap **OK**.
7. Optional: Tap **Complete** and the added devices are displayed on the page of the site.

7.2.6 Adding Devices by IP Address or Domain Name

If you know the IP address or domain name of a device, you can add it to LTS Platinum Partner by specifying its IP address/domain name, username, password, etc. Once a device is added in this way, you can generate a QR code containing the device information. After completing device setup, you can share the QR code to your customer. And then your customer can scan the QR code via the LTS Connect Mobile Client to add the device to her/his LTS Connect account.

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

Note

- Devices added in this method do NOT support the device handover process. If you need to hand over a device to your customer after completing the device setup work, please add it in one of the following two methods: [Add Device by Scanning QR Code](#) and [Add Device by Entering Serial No.](#)
 - Only encoding devices mapped in WAN support this function.
 - Ask your customers to download or update the LTS 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.
-

1. Enter the adding device page.
 - Tap **Add** in the Site & Device area on the Home page.
 - Tap **Site** on the bottom, and then tap **Add Device** above the site list.
 - Tap **Site** on the bottom, tap a site to access its details page, and tap **Add Device** or  → **Add Device**.
 - Tap  in the upper-left corner on the Home or Site page.
 2. Tap **Add Device Manually** → **IP/Domain**.
 3. Enter the device name, device's IP address, port number, username, and password.
 4. Tap **Add to Site** to select a site to which the device will be added.
-

Note

- If you have selected the site in Step 1, skip this step.

- You can add the device to an existing site, or, tap **Add New Site** to add the device to a new site.

5. Tap **Add**.

 **Caution**

The password strength of the device can be automatically checked. We highly recommend you change to a password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6. Optional: Perform the following operations.

Operations	Description
Edit Device Information	For devices added by IP/Domain, if the device's information changed, or a network exception occurs, you can edit its information accordingly. Enter a device page, then tap IP/Domain to edit the device's name, IP address, port number, username, or password, and then tap Save .
Generate Device QR Code	<ol style="list-style-type: none"> 3. On the top right of a device page, tap ••• → Generate QR Code to open the Generate QR Code window. 4. Optional: (Optional) Enter the password to encrypt the QR code, and then tap Next. <hr/> <p> Note It is highly recommended that you encrypt the device QR code for security reasons.</p> <hr/> <ol style="list-style-type: none"> 5. Tap Save to save the generated QR code to your phone.
Set Type for Unknown Device	If the LTS Platinum Partner cannot recognize a device's type after you add it, you can manually set a device type for it. <ol style="list-style-type: none"> 1. Enter a device details page, tap  of the Device Type to access the Device Type page. 2. Select a type for the device. You can edit it again after the selection.
Delete Device	On the device page, tap ••• → Delete Device .

7.2.7 Synchronizing Devices with LTS Connect Account

You can synchronize the devices, including devices shared by others and the ones added by you, in your LTS Connect account with those in the LTS Platinum Partner account to provide better device management and maintenance services to your customers.

Steps

1. Log in to the LTS Connect page.
 - Tap **Site** → **Device Synchronization**.
 - Tap **Me** → **Link With LTS Connect Account** → **Link With Account** / .
 - Tap **Account Linking** or **More** → **Tools** → **Account Linking** / .
2. Log in to your LTS Connect account.

Note

- Check **Get Your Account and Device Information** to allow LTS Platinum Partner to acquire necessary information for device synchronization.
-

3. Tap **Authorize and Login**.
4. Select the devices you want to synchronize and tap **Next**.
5. Configure Sites for the devices.
 - 1) Tap **Site Time Zone** to set the default time zone for Sites.
 - 2) Tap **My Devices** or **Others' Devices**.
 - 3) Tap **Assign Site** to select device allocation mode.

Auto Allocate to Sites

For My Devices, this will create different Sites by the names of the accounts that you share devices with, and then allocate devices to these Sites accordingly.

For Others' Devices, this will create different Sites by the name of the accounts that share devices to you, and then allocate devices to these Sites accordingly.

Same Site

Allocate all devices to a single Site named by your LTS Connect account.

- 4) View and edit the configurations of each Site. Tap on each Site to view or edit information such as Site name, time zone, devices to be synchronized, and device permissions.
- 5) Tap **Finish** to save the settings.
6. Tap **Synchronize** to start device synchronization.

Note

- For Others' Devices, the platform will send an application to the belonging accounts for device authorization. You will obtain device permissions and be able to configure, operate, and manage these devices in LTS Platinum Partner upon approval.

- After synchronization, you can still manage the devices in your LTS Connect account and access LTS Connect services.
-

7. Optional: If you have authorized automatic device synchronization, view the linked account(s) and tap  → **Unlink** to unlink an account if needed.
- On the Home page, go to **Account Linking** or **More** → **Tools** → **Account Linking**.
 - Tap **Me** → **Link With LTS Connect Account**.

7.3 Activating the Health Monitoring Service

After purchasing health monitoring packages, you can use them to activate the health monitoring service for specific devices. Once the service is activated, features such as device health monitoring and device exception notifications will be available for these devices.

Before You Start

Make sure you have purchased health monitoring packages.

Note

Contact the local distributor for details about whether your country/region supports service keys. If supported, you can purchase a service key from the distributor, and then go to the Service Market on the Mobile Client to purchase health monitoring packages by the service key. If not supported, go to the Service Market on the Portal to purchase health monitoring packages online first (see *LTS Platinum Partner Portal User Manual* for details).

Steps

Note

Multiple entries are available for activating the service, including:

- The results page of adding a device by scanning QR code or by LTS Connect (P2P).
- The results page of batch adding devices.
- The device details page.

Here we only introduce activating the service via the last entry, i.e., the device details page.

1. Tap **Site** to access the site details page.
 2. Tap a device to access the device details page.
 3. Switch on **Health Monitoring Service** to access the Select Activation Type page.
-

Note

If the firmware version of a device is obsolete, or its device type cannot be recognized by LTS Platinum Partner, activating health monitoring service for the device is not supported

4. Set the number of months/years that the service lasts for each selected device, then set other parameters.

Use All Device Package Only

When enabled, you can only select All Device Packages (All Device Monthly Package or All Device Annual Package) for network cameras to activate the service for them.

Auto Renewal

When enabled, if the service for a device expires, the service will be automatically renewed using the same service package in the previous activation. For example, assume that you activated a 1-month health monitoring service for an NVR using an All-Device Monthly Package on 5/14/2021, the 1-month service will be automatically renewed using another All Device Monthly Package on 6/14/2021.

The following list shows the description of each package type.

All-Device Monthly Package

An All-Device Monthly Package can be used to activate the service for almost all types of devices. And the activated service lasts one month.

"All Device" here means that the service package is applicable to nearly all device types, including DVR, NVR, network cameras, PTZ cameras, access control devices, video intercom devices, and network switches.

"Monthly" here means that the service term is one month. The service term starts when you activate the service.

All-Device Annual Package

An All-Device Annual Package can be used to activate the service for a device of nearly any type. And the activated service lasts one year.

"All Device" here means that the service package is applicable to nearly all device types, including DVR, NVR, network cameras, PTZ cameras, access control devices, video intercom devices and network switches.

"Annual" here means that the service term is one year. The service term starts when you activate the service.

Network Camera Monthly Package

A Network Camera Monthly Package can be used to activate the service for a network camera. And the activated service lasts one month.

"Network Camera" here means that the service package is only applicable to network cameras.

"Monthly" here means that the service term is one month. The service term starts when you activate the service.

Network Camera Annual Package

A Network Camera Annual Package can be used to activate the service for a network camera. And the activated service lasts one year.

"Network Camera" here means that the service package is only applicable to network cameras.

"Annual" here means that the service term is one year. The service term starts when you activate the service.

5. Tap **OK**.

6. Optional: Go to the device details page to perform the following operations if needed.

View Service Expiry Date	View the service expiry date shown beside Health Monitoring Service .
Renew the Service	Tap Health Monitoring Service to renew the service for the device.
Enable Auto Renewing the Service	Switch on Auto Renewal , and then select a type of service packages for auto renewal.
Transfer the Service	Tap Transfer , and then select a device to transfer the remaining service time from the current device to the selected device.

7.4 Managing Device Permissions

By handing over the site and applying for site authorization, you have already acquired some device permissions. You can still apply for additional device permissions afterward or release device permissions if needed.

7.4.1 Applying for Device Permission

After handing over a site to the customer, if you need to view the live view or playback of device(s) added to the site or configure the device(s) added to the site, you can apply for the permission accordingly from the customer.

Steps

1. Tap **Site** in the bottom to access the site list page.
2. Tap a site to access the site details page.

Note

You can either apply for permission for one device (refer to Step 3) or apply for permission for multiple devices (refer to Step 4).

3. Optional: Apply for permission for one device.
 - 1) Tap a device to access the device details page.
 - 2) In the Available Permission area, tap ⓘ beside **Configuration**, **Live View**, or **Playback** to access the Set Permission page.
 - 3) Set the validity period for the permission.
 - 4) Optional: Enter the remarks.
 - 5) Tap **OK** to send the application to the customer.

If the customer approves your application, you will be able to view the live view, playback of the device and configure device.

4. Optional: Apply for permissions for multiple devices.

- 1) Tap **Manage Permission** on the top.
- 2) 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.

3) Optional: Enter the remarks.

4) Tap **OK** to send the application to the customer.

If the customer approves your application, you will be able to view the live view, playback of the devices and configure devices.

7.4.2 Release Permissions for 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.

Before You Start

Make sure the site of the devices has been authorized to you.

Steps

1. Tap a site in the site list to access the site details page.
2. Tap a device on the site details page to access the device details page.
3. In the Permission area, select a permission, and tap **• • • → Release Permission → Release Permission** to release the permission.

 **Note**

- Upon release, the permission will be unavailable to you. You may need to apply for it again.
 - You do not have to release permission if the permission validity is **Permanent**.
-

7.5 Moving Devices

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.

Steps

 **Note**

- The feature is only supported by a device matches the following conditions:
 - The original Site where the device belongs needs to have been authorized to you.
 - The device needs to be added by serial No. 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 will 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, network switch settings, etc., will be affected. You also need to configure these related configurations again.
-

1. Tap **Site** at the bottom to access the Site page.
2. Tap an authorized Site to access its details page.
3. Tap **⋮** in the upper right corner, and then tap **Move Device** to open the following pane.
4. Tap **Select Device** to access the Select Device page.

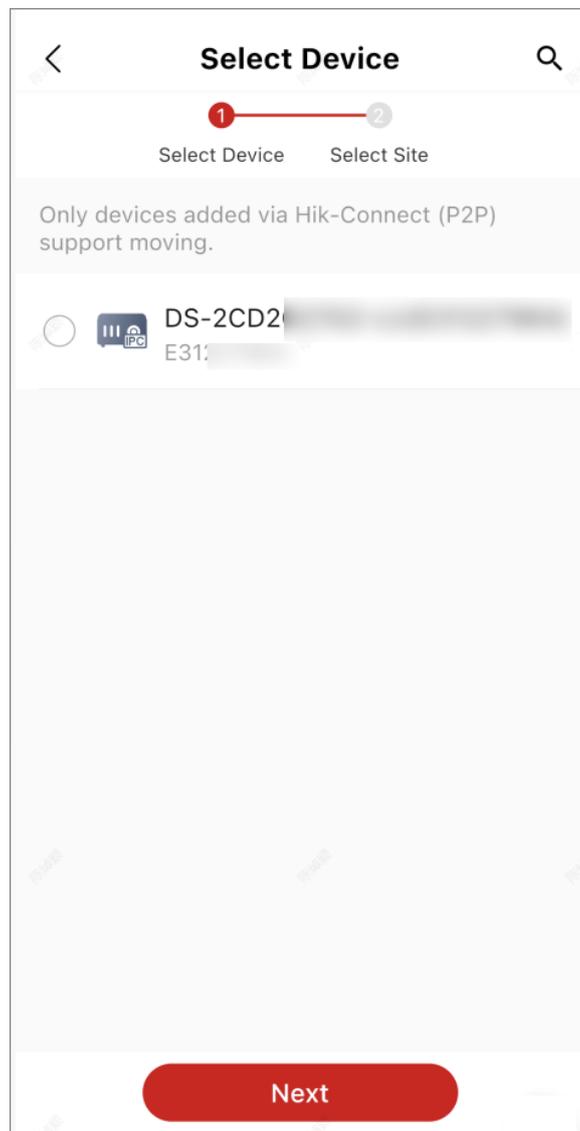


Figure 7-2 Select Device

5. Select device(s) and tap **Next** to access the Select Site page.

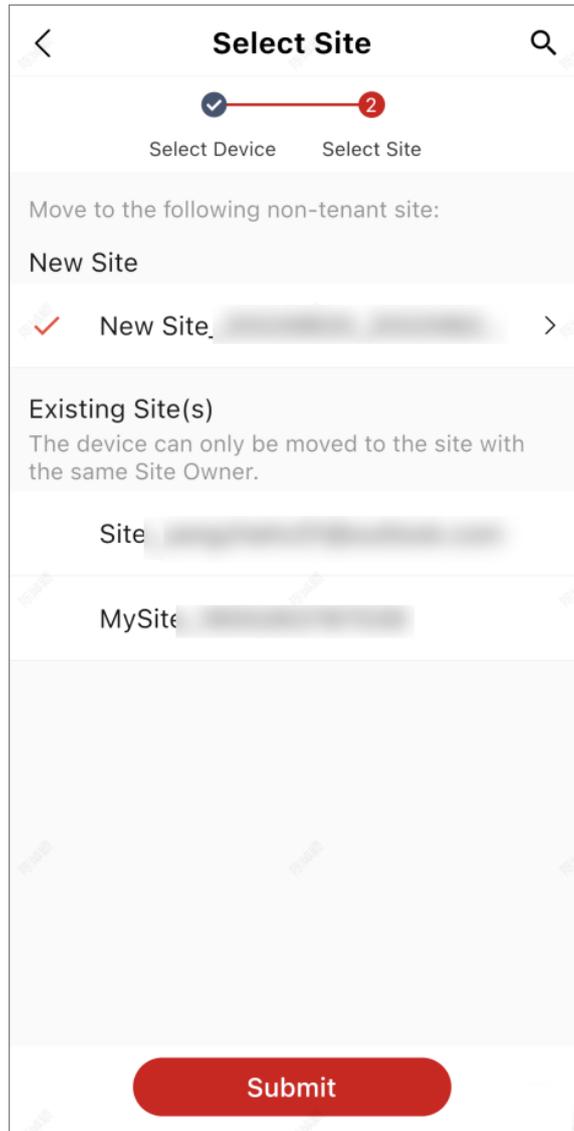


Figure 7-3 Select Site

6. Select a Site.

New Site: If you select **New Site**, you will need to create a name for the Site and set its time zone.

Existing Site: If you select **Existing Site**, you will need to select a Site that shares the same Site Owner with the current one. Under the condition that two sites are handed over to the same LTS Connect user by email and phone number respectively, you can also move devices between the two sites.

7. Tap **Submit**.

 **Note**

The application will expire if not handled within 7 days.

8. Optional: Tap **View Device Movement Records** and perform the following operation(s).

Apply Again	Tap an expired (🕒) or rejected (❌) application to access its details page, and then tap Apply Again to send the application again.
View Details	Tap an application record to access its details page to see the details.
Move More	Tap an approved (✅) or sent (📧) application to access its details page, and then tap Move More to move more devices.

7.7 Resetting Device Password

Three ways of resetting the device password are available: scanning the QR code acquired from the device's local GUI, sending the password reset application to LTS Connect (the Mobile Client for your customers), and using the IP Portal tool.

 **Note**

Resetting the password via LTS Platinum Partner is not supported by every device type/model.

Access the Password Reset function via either of the following ways.

- Tap **Site** at the bottom and access the site where the device is located. Tap the device to access the device details page and then tap **Reset Password**.
 - On the Home page, tap **More** → **Support** → **Reset Password** to open the Reset Password pane.
-

 **Note**

You can also tap **Submit Case** on the Reset Password pane and submit a device password reset case. Refer to [***Submit Device Password Reset Case***](#) for details

You may access automatically or choose one of the following three processes for password reset.

- **Nearby Device (Scanning)**
- **Device on LTS Platinum Partner**
- **LAN Device (IP Portal)**

Nearby Device (Scanning)

If you can get the password reset QR code by tapping **Forget Password** → **Verify by LTS Connect** on the local GUI of the device, you can select this method.

Scan the password reset QR code via the LTS Platinum Partner Mobile Client, then you can get a verification code for password reset. Enter the verification code in the local GUI to reset the device password.

Device on LTS Platinum Partner

If the device is on LTS Platinum Partner, you can select this method to reset the device password directly or by sending password reset applications to your customer's LTS Connect.

- For a device not handed over:

Note

Make sure that the LTS Platinum Partner Mobile Client and the device are on the same LAN.

You can reset the password by entering and confirming a new password directly on LTS Platinum Partner.

- For a device that is handed over:

Note

Make sure you are granted the site authorization. For details about how to get site authorization, see ***[Apply for Site Authorization from Site Owner](#)***.

- When you are not at the site:

Note

Make sure that your customer's LTS Connect app and the device are on the same LAN and that the version of LTS Connect is V 4.15.0 or later.

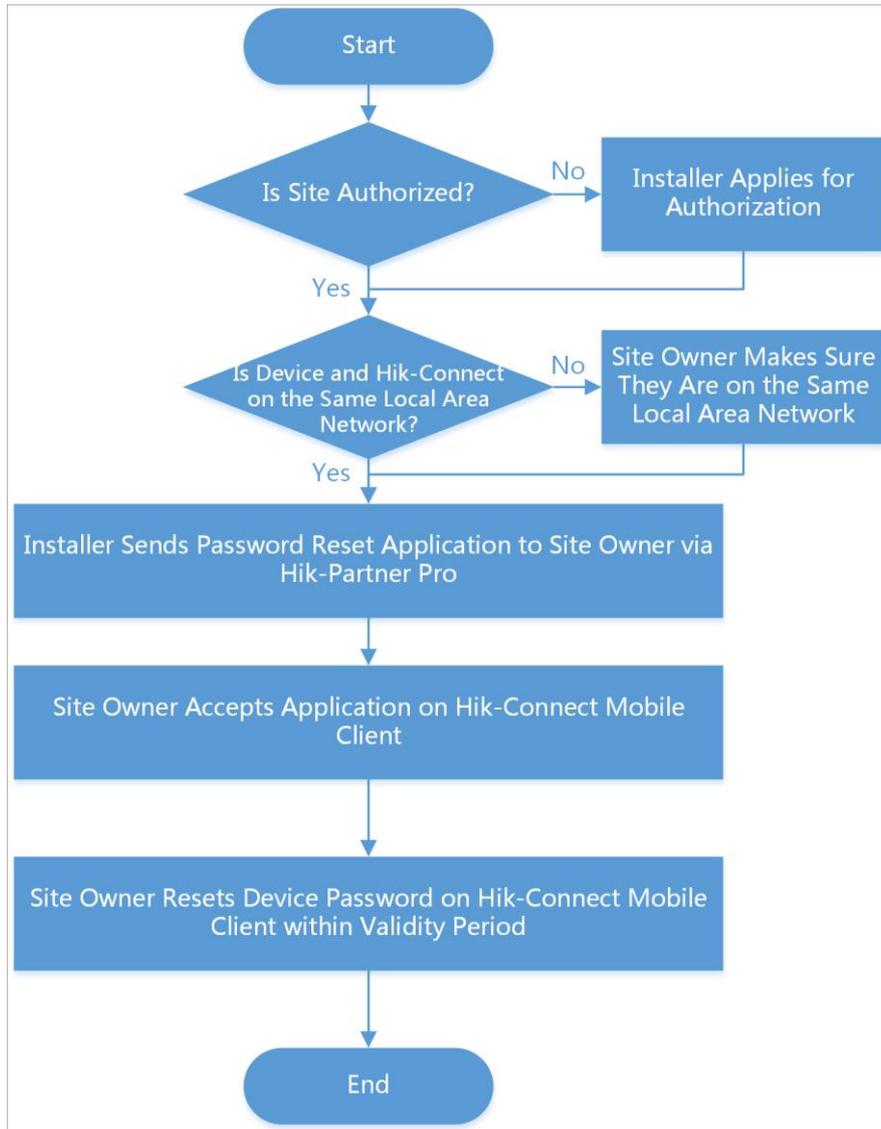


Figure 7-7 Flow Chart of Resetting Device Password Offsite

- o When you are at the site:

Note

Make sure that the LTS Platinum Partner Mobile Client and the device are on the same LAN.

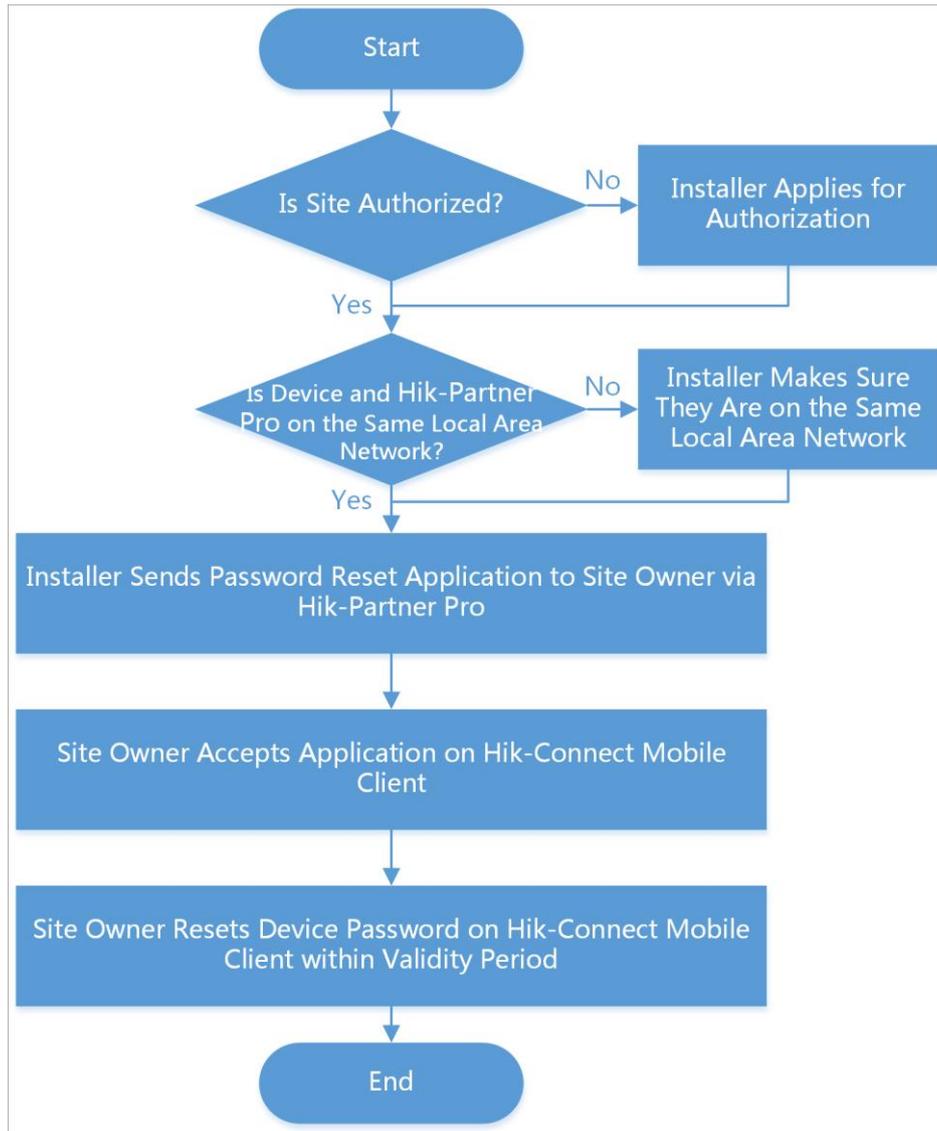


Figure 7-8 Flow Chart of Resetting Device Password Onsite

LAN Device (IP Portal)

If the device that requires password reset and your phone are on the same LAN, you can select this method.

Refer to ***Reset Device Password via IP Portal Tool.***

7.8 Enabling Remote Log Collection

Remote Log Collection is for getting device logs. When this function is enabled, the technical support can collect device logs remotely for troubleshooting. You can set the validity period for collecting remote logs as needed, and this function will be automatically disabled when the

validity period expires.

Before You Start

Make sure you have added the device which supports remote log collection to the site, and the site has not been handed over to the end user. If the site has been handed over to the end user, you will need to contact the end user to enable the Remote Log Collection function on LTS Connect.

Steps

1. Tap a site to access the site list page.
2. Tap a device to access the device details page.
3. Tap **⋮** in the upper right corner.
4. Tap **Remote Log Collection** to access Remote Log Collection page.
5. Optional: For enabling this function for the first time, tap **Enable** to confirm enabling the function.
6. Switch on **Log Collection**.

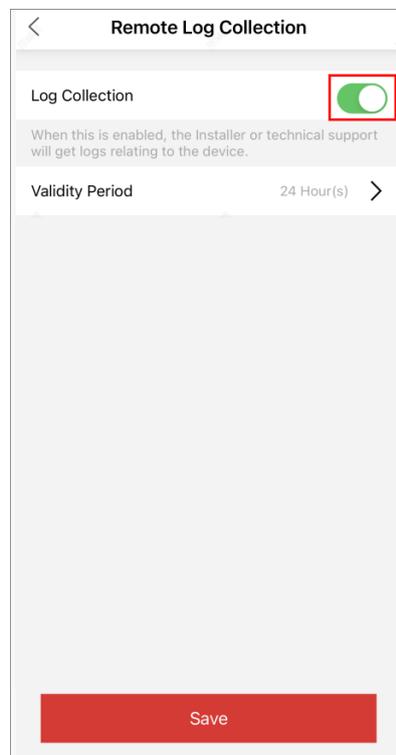


Figure 7-9 Remote Log Collection

7. Select the validity period.

Note

The function of remote log collection will be automatically disabled when the validity period expires. The default validity period is 24 hours.

8. Tap **Save**.

9. Optional: Disable the function.

- 1) Tap **Remote Log Collection** to access Remote Log Collection page.
- 2) Switch off **Log Collection**.
- 3) Tap **Save** to save the settings.
- 4) Tap **OK** to confirm the operation.

7.9 Viewing Video Feeds

You can view the live video and the recorded video footage of the added encoding device(s).

7.9.1 Live Video

By LTS Platinum Partner Mobile Client, you can view live view of managed cameras and perform related operations.

Tap  to launch the live view of the last 5 minutes of an encoding device. During live view, you can perform PTZ control (except Pattern), enable wiper to clean the camera lens, and tap **High Definition** to switch image quality. For devices added by LTS Connect Service without configuring DDNS, the live view will work for up to five minutes; for devices added by IP/Domain Name and devices added by LTS Connect Service with DDNS configured, the live view duration is not limited.

Note

- If Image and Video Encryption has been enabled for the device on the LTS 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 *LTS Connect Mobile Client User Manual*.
 - Please inform your end users to download or update the LTS 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 of Portal to them.
 - For those who have no permission for live view: If you are on site, tap **I Am at the Site** in the pop-up window of no-permission prompt, to connect your mobile phone to the same Wi-Fi with the encoding device and log into the device to start live view; if you are off site, tap **Apply for Permission** in the pop-up window to apply for permission for live view. See details in [**Apply for Device Permission**](#).
 - Make sure the device is online, otherwise the function cannot be used.
-

7.9.2 Playing Back Video Footage

You can start playback to view the recorded video footage of a device.

Enter a site page, select a device and tap  to access the playback page. You can also access the playback page on the live view page.

 **Note**

- For those who have no permission for playback: If you are on site, tap **I Am at the Site** in the pop-up window of no-permission prompt, to connect your mobile phone to the same Wi-Fi with the encoding device and log into the device to start playback; if you are off site, tap **Apply for Permission** in the pop-up window to apply for permission for playback. See details in [**Apply for Device Permission**](#).
 - This function should be supported by the device.
-

Tap the date below the playback window to select a date for playback.

On the playback tool bar, tap the following icons to perform functions you need.

For devices added by LTS Connect P2P, the video files are displayed by different color: the time-based video files are marked in blue in the time bar and the event-based video files are marked in yellow in the time bar.

	Tap the icon to select a channel for playback.
	Tap the icon to download the video footage to your mobile phone.
	Tap the icon to turn on/off the playback sound.
	Tap the icon to pause the playback.
	Tap the icon to select a speed for playing video footage.
	Tap the icon to perform digital zoom.
	Tap the icon to capture a image.
	Tap the icon to clip the video footage and download it to your PC.

7.10 Managing Network Devices

Setting up network devices like the access point (AP), and network switch, and cameras together allows for seamless integration and 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.

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 manages 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. **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.

7.10.1 Adding Network Devices and Initializing Network

With LTS Platinum Partner, you can activate the network switches on the same LAN together and configure the network settings.

Before You Start

- Connect and power on your network switches.

Steps

1. Connect to the network devices.
 - 1) Optional: In **Add Device Manually** mode, enter the serial number 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 LTS Platinum Partner can find the AC router and switches.
2. Tap **Activate All** to activate the AC router and network switches by setting the device username, password, and verification code.

Note

The verification code is set for only the network switches to enable the LTS 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.

DLCP

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.

7.10.2 Network Switch Operations

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

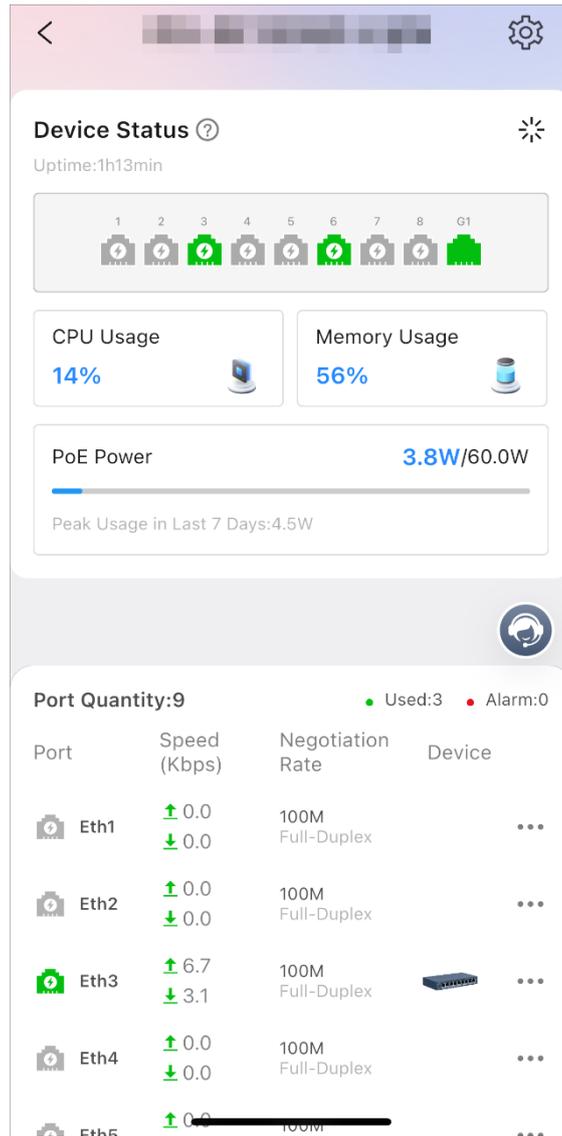


Figure 7-16 Network Switch Detail Page

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**, then select the desired ports.

 **Note**

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 for connecting devices that must 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 that port can only communicate with other devices.	None

Port Type	Description	Following Operation
TRUNK	Used for connecting 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 must 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 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	<p>Tap Enable Extend Mode/Disable Extend Mode to extend or not to extend the transmission range of this port.</p> <hr/> <p> 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.</p> <hr/>
Detect Cable Status	Tap  → Cable Detection , tap a port, and then tap Detect . When the detection is finished, you can view the detection results and cable length.

7.10.3 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 sources 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 [***Apply for Device Permission***](#).

Tap a site on the site list to access 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.

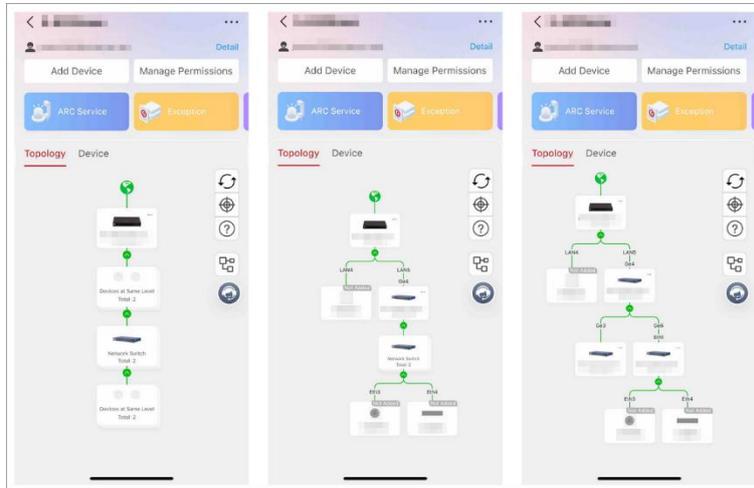


Figure 7-17 Topology Mode 1, 2 and 3

Table 7-6 Available Operations

Operation	Description
Set Root Node	<p>If you want to change the root node, you can select a device and tap ⋮ → Set Root Node.</p> <hr/> <p>Note</p> <p>You can set a third-party switch to the root node.</p> <hr/>
View Network Device Details	<p>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.</p>
View Details of Other Device	<p>Tap a device to view its details, such as device model and network status.</p> <hr/> <p>Note</p> <ul style="list-style-type: none"> ● Make sure you have the configuration permission for the device, otherwise you will 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

Operation	Description
	with the network switch, you cannot view its details.
View More Information	Tap  to view the connection type, connection status, and device status.

7.11 Other Management

You can perform more operations for device management, including upgrading device firmware, unbinding device from its current account, and configuring DDNS for devices added by LTS Connect service.

7.11.1 Unbinding a Device from Its Current Account

When you add a device by scanning a QR code or add it manually, if the results page shows it has been added to another account, you will 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).

Note

- Make sure the phone on which the Mobile Client operates is on the same LAN with the device. Otherwise, this function will be unavailable.
 - If you checked **Allow Me to Disable LTS Connect Mobile Client Remote Use** when you hand over a site to your customer, you cannot unbind the devices added to this Site. For details about site handover, see [***Hand Over Personal Site by Transferring.***](#)
-

Tap **Unbind** on the results page, and then enter the device password and tap **Finish** to unbind it from its currently added account. When the device is unbound, you can add it to your account.

Note

If the device firmware does not support device unbinding, you are required to enter a CAPTCHA code after entering device password.

7.11.2 Configuring DDNS for Devices

For devices with invalid or old firmware version, you can configure DDNS for them to make sure

they can be managed by LTS Platinum Partner properly.

Steps

Note

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

1. Tap a site on the site list to access the site details page.
-

Note

For devices with invalid or old firmware version and without DDNS configured, a red dot will be displayed beside the device name.

2. Tap a device to access the device page.
 3. Tap **DDNS Settings** to access the DDNS Settings page.
-

Note

You can tap **How to set port?** to learn the configuration.

4. Switch **Enable DDNS** on.
5. Enter the device's domain name.
6. Select **Port Mapping Mode**.

Auto

In this mode, 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.

7. Enter the username and password.
-

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

8. Tap **Save**.

7.11.3 Remote Configuration

You can configure parameters remotely for the added device such as doorbell and encoding device.

Tap  to set the device parameters. See device user manual for details about remote configuration.

Note

- For those who have no permission for remote configuration: If you are on site, tap **I Am at the Site** in the pop-up window of no-permission prompt, to connect your mobile phone to the same Wi-Fi with the encoding device and log into the device to perform remote configuration; if you are off site, tap **Apply for Permission** in the pop-up window to apply for permission for remote configuration. See details in [***Apply for Device Permission***](#).
 - Make sure the device is online.
-

Chapter 8. Health Monitoring

The Health Monitoring module includes Exception Center, Scheduled Report and Health Status, where you can view the device exceptions, configure the report schedule, and check a device's health status.

Exception Center

When any exception occurs during health monitoring, the notification will appear in the Exception Center under the Notification Center module. See details in [**Exception Center**](#).

Scheduled Report

With the scheduled report feature, the device status information will be sent to you or the corresponding user based on the configured schedule.

Health Status

Shows the near-real-time information about the status of the devices added to the sites. If you have added network switches to a site, you can view the device status and link status in a visualized way via network topology. The status information, which is important for the maintenance of devices managed across the LTS Platinum Partner platform as a whole, helps you locate the source of exceptions and determine troubleshooting methods in time, thus ensuring the smooth operation of these devices.

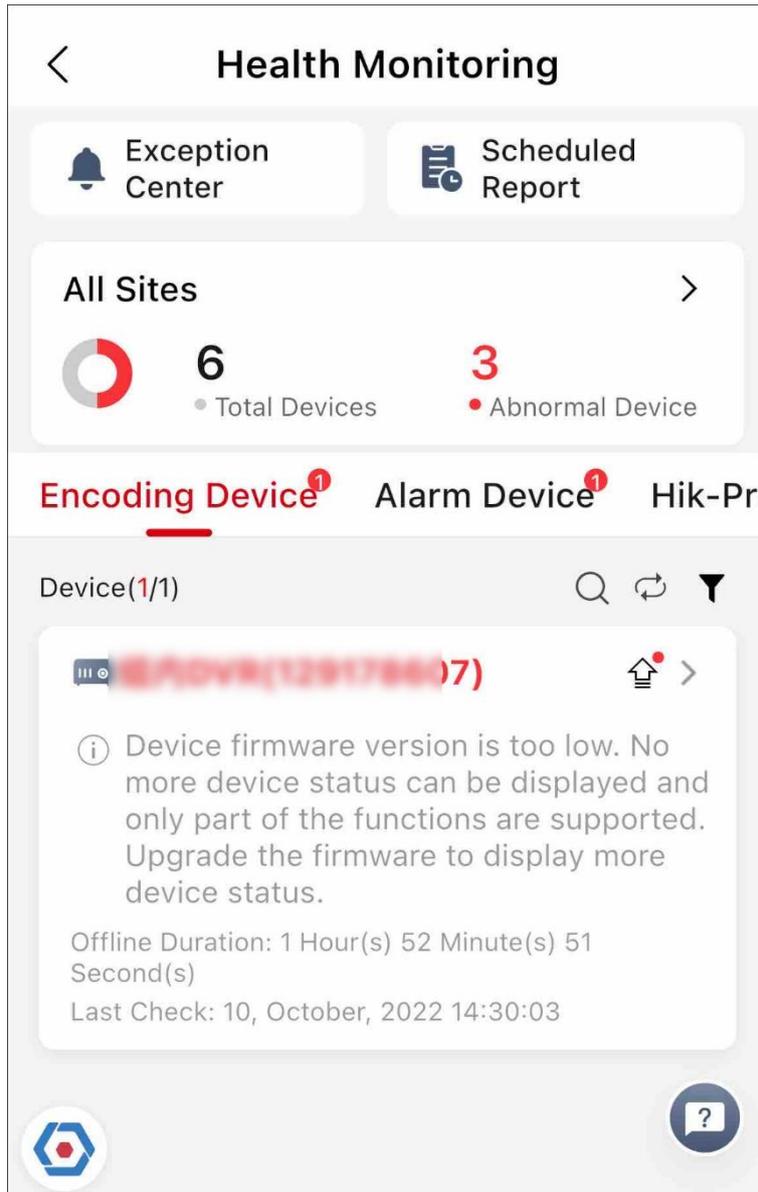


Figure 8-1 Health Monitoring Page

Note

- The link of video tutorial on how to check device health status will pop up on the bottom of the page when you first access the Health Monitoring module.
Tap  to make the video link pop up when you access Health Monitoring next time.
 - For Installer, you can only view the status information of devices on the site assigned to you. For Installer Admin, you can view the status information of devices on all sites.
-

8.1 Checking the Status of Devices on All Sites

For the Installer, you can view the status of each device type on all the sites which have been assigned to you. For the Installer Admin, you can view the status of each device type on all the sites.

On the Home page, tap **Health Monitoring** or **More** → **Maintenance** → **Health Monitoring**, or **Site** → **Health Monitoring** to access the Health Monitoring page, and you can view the total number of devices and the number of abnormal devices on all sites.

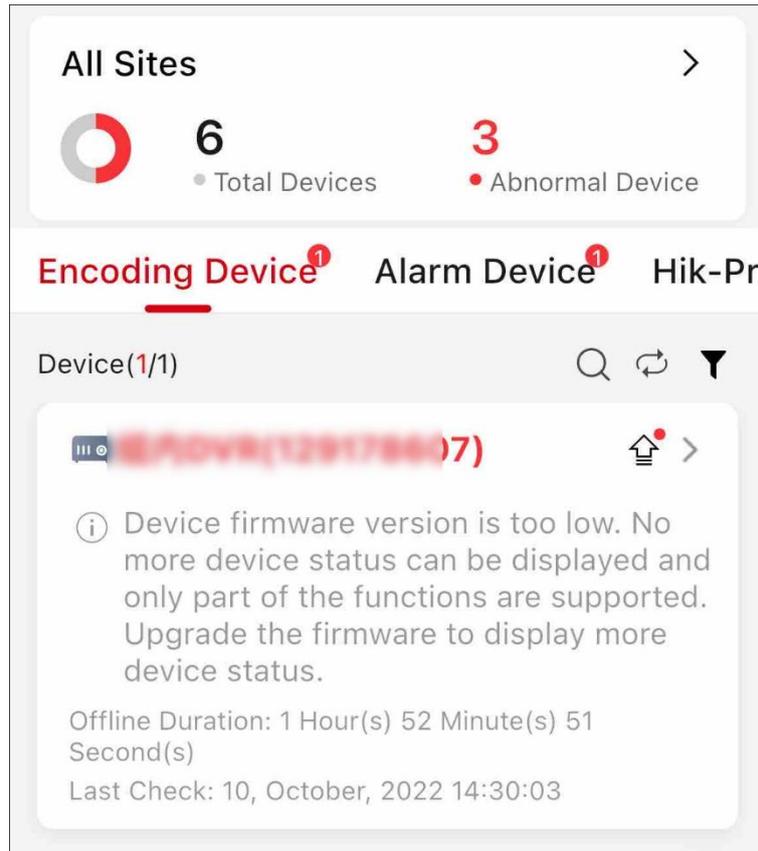


Figure 8-2 Device Status

Refer to the following to get the device descriptions and operations.

- For each device type, you can tap to inspect all the devices in the list; tap → **Display Abnormal Devices Only** to display the abnormal devices only; tap → **Display Authorized Devices Only** to display the devices whose configuration permission has been authorized to you.
- The Offline Duration column displays offline duration of devices in the format of "x Day(s) x Hour(s) x Minute(s)". If the offline duration is less than one day, the duration will be displayed as "x Hour(s) x Minute(s) x Second(s)".
- The icon beside the device name represents that you do not have the configuration permission for the device. You can tap the device and tap **Apply for Configuration Permission** to apply for the permission. For details, see [***Apply for Device Permission***](#).

- The icon  beside the device name represents that a new firmware is available. You can tap the device and tap **Upgrade** to upgrade the device. For details, see [Upgrade Device](#).

Encoding Device

You can view the device information including network status, the number of offline linked cameras, storage status, HDD usage, last check time, overwritten recording status, etc.

The icon  beside the device name represents that the IP address/domain set for the device is invalid or the DDNS is invalid, you can tap the device and tap **Edit Device Information** to edit the device information or tap **Configure DDNS** to reconfigure the device's DDNS.

Note

- For details about configuring device IP address/domain, see [Add Device by IP Address or Domain Name](#). For details about configuring DDNS, see [Configure DDNS for Devices](#).
-

Tap a device to access the Device Details page to view more basic information about the device, and perform the following operations.

Operation	Description
Inspect Device	Tap  to inspect the device manually.
Remotely Configure Device	Tap  to remotely configure the device parameters. For details, see the device user manual.
Live View	Tap  to view the live view of the device. <hr/>  Note <ul style="list-style-type: none"> • If you do not have the Live View permission, you can apply for the live view permission from the end user. For details, see Apply for Device Permission. • If the selected camera has been enabled with stream encryption, you must enter the device verification code before you can view its live view. <hr/>
View Playback	Tap  to view the playback of the device.
View Site Owner and Site Manager Information	Tap  beside site name to view the information about the Site Owner and Site Manager, such as name and phone number.
View Camera Status	Tap Camera to view the cameras linked to the

Operation	Description
	device and their online/offline status.
View DVR HDD Information	Tap HDD to view the HDD information about the DVR, including self-evaluation results, overall evaluation results, operating status, run time, HDD temperature, and S.M.A.R.T information.

Access Control Device

You can view the device information including device model, network status, last check time, etc. Tap a device to access Device Details page to view more basic information about the device and perform the following operations.

Operation	Description
Inspect Device	Tap  to inspect the device manually.
View Site Owner and Site Manager Information	Tap  beside the site name to view the information about the Site Owner and Site Manager, such as name and phone number.

Video Intercom Device

You can view the device information including network status, last check time, etc. Tap a device to access Device Details page to view more basic information about the device, and perform the following operations.

Operation	Description
Inspect Device	Tap  to inspect the device manually.
View Site Owner and Site Manager Information	Tap  beside the site name to view the information about the Site Owner and Site Manager, such as name and phone number.

Network Switch

View information including network status of the switch (online/offline), the number of online ports of the switch, and the last check time.

Tap a network switch to view its information, including working duration, the thumbnail of the switch, PoE Power, peak PoE power in last 7 days, port status (alarm, normal, not connected). You can tap the switch thumbnail to view its enlarged image.

 **Note**

Working duration refers to the time from when the switch is turned on till the current moment. If the switch is turned off, its working duration will be recounted when turned on again.

- Tap **...** → **Device Information** in the upper-right corner to view more basic information about the device, including device serial No., device model, device type, etc. You can tap **Reboot Device** at the bottom to reboot the device.
- Tap **...** → **Topology** in the upper-right corner to view the topology of this switch. For details about topology, refer to ***Network Topology***.

For the port with alarms, tap **Clear Alarm** to clear the alarms of this port.

Tap **Extend Mode** to extend the transmission range of this port. Tap **Extend Mode** (displayed in green) to disable extending the transmission range of the port.

 **Note**

When enabled, the transmission range of the port will be extended from 200 m to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.

8.2 Checking the Status of Devices on One Site

You can view the status of devices on a specific site which has been assigned to you.

Steps

1. On the Home page, tap **Health Monitoring** or **More** → **Maintenance** → **Health Monitoring**, or **Site** → **Health Monitoring** to access the Health Monitoring page, and you can view the total number of devices and the number of abnormal devices on all sites.
2. Tap **>** to access the site list page, then select a site from the list.

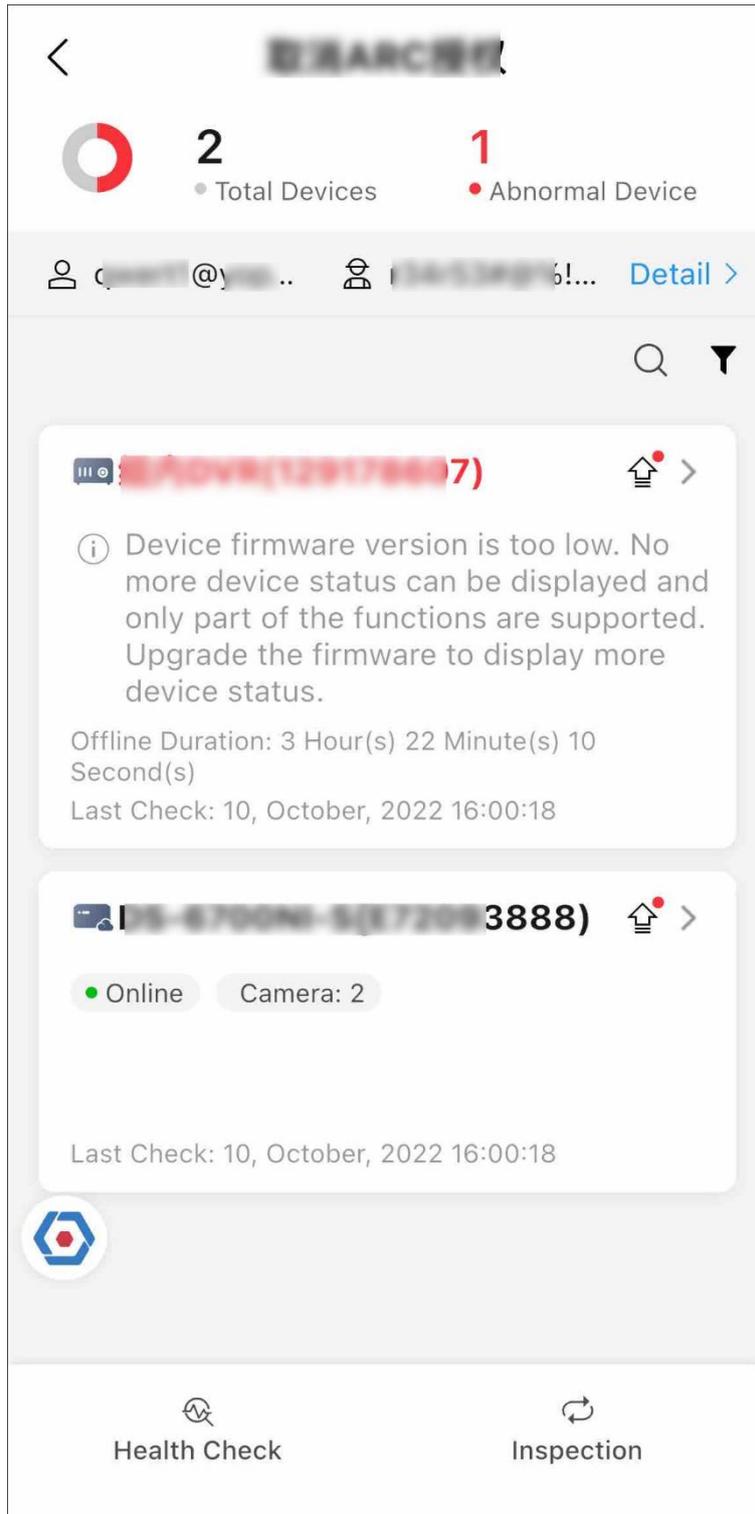


Figure 8-3 The Current Site

The status of the devices on the current site will be displayed.

3. Optional – Perform the following operations:

<p>Filter Data</p>	<ul style="list-style-type: none"> ● Tap  → Display Abnormal Devices Only to display the abnormal devices only. ● Tap  → Display Authorized Devices Only to display the devices whose configuration permission has been authorized to you.
<p>View Information About Site Owner & Site Manager</p>	<p>Tap Detail to view the information about the Site Owner and Site Manager, including the name, email address, and phone number. Up to 100 site managers can be displayed.</p>
<p>Inspect Devices</p>	<p>Tap Inspection at the bottom to inspect all the devices on the site.</p>
<p>Upgrade Device Firmware</p>	<p>If there are devices available for upgrade,  will appear. You can tap the device to access its details page, and tap Upgrade to upgrade it.</p> <hr/> <p> Note For details, see <u>Upgrade Device</u>.</p>
<p>Remote Configuration</p>	<p>Select a device and then tap  to remotely configure the device parameters.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> ● The device should be online. ● For details, see the user manual of the device.
<p>Inspect a Single Device</p>	<p>Select a device and then tap  to inspect it.</p>
<p>Reconfigure IP/Domain of Encoding Device</p>	<p>If the IP address/domain set for the device is invalid,  will appear. You can tap the device to access its details page, and tap Edit Device Information to reconfigure the device's IP/domain. For details about configuring IP/Domain, see <u>Add Device by IP Address or Domain Name</u>.</p>
<p>Reconfigure DDNS</p>	<p>If the DDNS of the device is invalid,  will appear. You can tap the device to access its details page, and tap Configure DDNS to reconfigure the device's DDNS. For details, see <u>Configure DDNS for Devices</u>.</p>
<p>View Encoding</p>	<p>You can view the network status, storage status, HDD usage, and</p>

<p>Device Details</p>	<p>overwritten recording status, etc.</p> <p>Also, you can tap the encoding device to view its details, including the basic information such as device type, serial No., and the network status of each linked camera. You can tap Camera to view all the linked cameras. If there is only one linked camera, tap  to view its live view. If there are multiple cameras, tap , and select one camera to view its live view.</p> <p>If the encoding device is a DVR, you can also view its HDD information, including self-evaluation results, overall evaluation results, operating status, run time, HDD temperature, and S.M.A.R.T information.</p> <p>For the analog camera, you can view if video loss occurs.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> ● If you do not have the Live View permission, you can apply for the live view permission from the end user. For details, see <u>Apply for Device Permission</u>. ● If a camera has been enabled with stream encryption, you must enter its device verification code in the pop-up window before you can view its live view. <hr/>
<p>View Access Control Device Details</p>	<p>Tap an access control device to view its details, including basic information such as device type, serial No., and the device status including network status and the number of its linked doors.</p>
<p>View Video Intercom Device Details</p>	<p>Tap a video intercom device to view its basic information and its network status.</p>
<p>View Network Switch Details</p>	<p>Tap a network switch to view its information, including working duration, the thumbnail of the switch, PoE Power, peak PoE power in last 7 days, port status (alarm, normal, not connected). You can tap the thumbnail of switch to view its enlarged image.</p> <hr/> <p> Note</p> <p>Working duration refers to the time from when the switch is turned on till the current moment. If the switch is turned off, its working duration will be recounted when turned on again.</p> <hr/> <p>Tap  → Device Information in the upper-right corner to view more basic information about the device, including device serial No., device model, device type, etc. You can tap Reboot Device at the bottom to reboot the device.</p>

	<p>Tap ... → Topology in the upper-right corner to view the topology of this switch. For details about topology, refer to <u>Network Topology</u>. For the port with alarms, tap Clear Alarm to clear the alarm(s) of this port.</p> <p>Tap Extend Mode to extend the transmission range of this port. Tap Extend Mode (displayed in green) to disable extending the transmission range of the port.</p> <hr/> <p> Note</p> <p>When enabled, the transmission range of the port will be extended from 200 m to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.</p> <hr/>
--	--

8.3 Network Topology

If you have added network switch(es) to a site and connected devices to the network switch(es), you can view these devices' network topology. Network topology displays network links between devices and shows the link exceptions and abnormal devices, helping you to locate the exception source and troubleshoot faults in a visualized way.

Note

- Make sure you have the configuration permission for the network switch. Otherwise, network topology will be unavailable. For details about applying for configuration permission, see **Apply for Device Permission**.
 - If you have not activated the health monitoring service for the network switch, some topology functions (e.g., viewing device status on the topology) will be unavailable. For details about activating the health monitoring service, see **Activate the Health Monitoring Service**.
-

On the Home page, tap **Health Monitoring** → **Scheduled Report** or **More** → **Maintenance** → **Health Monitoring** → **Scheduled Report**, or **Site** → **Health Monitoring** → **Scheduled Report**.

- Tap **>** beside All Sites, select a site from the list, and then tap **View Topology**.
- Tap **Network Switch**, tap a switch to access the device details page, and then tap **...** → **View Topology** in the upper-right corner.

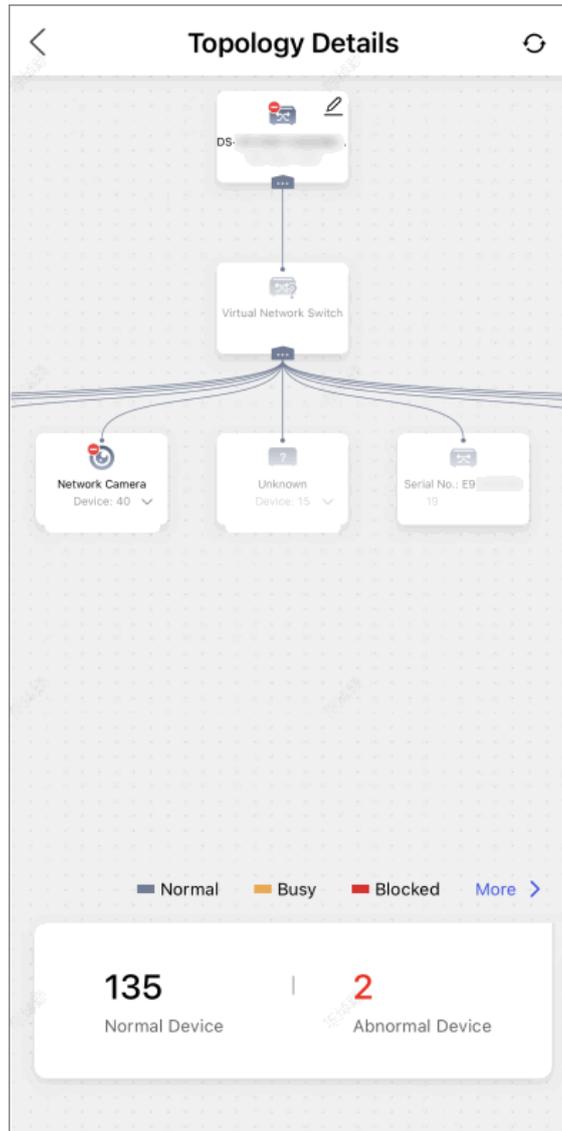


Figure 8-4 Topology Details

For detailed operations and descriptions about topology, refer to **Network Topology**.

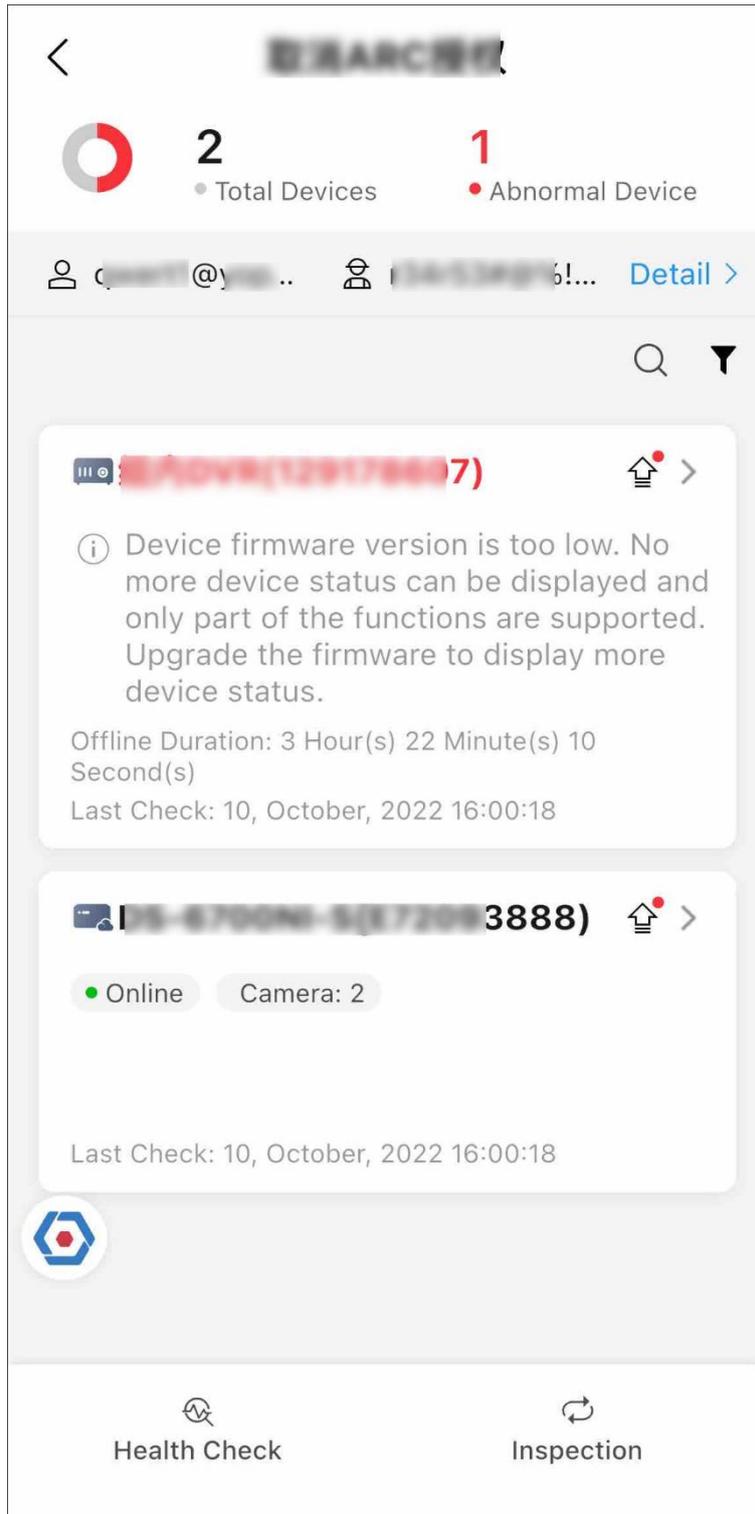


Figure 8-6 The Current Site

The status of the devices on the current site will be displayed.

3. Optional – Perform the following operations:

<p>Filter Data</p>	<ul style="list-style-type: none"> ● Tap  → Display Abnormal Devices Only to display the abnormal devices only. ● Tap  → Display Authorized Devices Only to display the devices whose configuration permission has been authorized to you.
<p>View Information About Site Owner & Site Manager</p>	<p>Tap Detail to view the information about the Site Owner and Site Manager, including the name, email address, and phone number. Up to 100 site managers can be displayed.</p>
<p>Inspect Devices</p>	<p>Tap Inspection at the bottom to inspect all the devices on the site.</p>
<p>Upgrade Device Firmware</p>	<p>If there are devices available for upgrade,  will appear. You can tap the device to access its details page, then tap Upgrade to upgrade it.</p> <hr/> <p> Note</p> <p>For details, see <u>Upgrade Device</u>.</p>
<p>Remote Configuration</p>	<p>Select a device and then tap  to remotely configure the device parameters.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> ● The device should be online. ● For details, see the user manual of the device.
<p>Inspect a Single Device</p>	<p>Select a device and then tap  to inspect it.</p>
<p>Reconfigure IP/Domain of Encoding Device</p>	<p>If the IP address/domain set for the device is invalid,  will appear. You can tap the device to access its details page, and tap Edit Device Information to reconfigure the device's IP/domain. For details about configuring IP/Domain, see <u>Add Device by IP Address or Domain Name</u>.</p>
<p>Reconfigure DDNS</p>	<p>If the DDNS of the device is invalid,  will appear. You can tap the device to access its details page, and tap Configure DDNS to reconfigure the device's DDNS. For details, see <u>Configure DDNS for Devices</u>.</p>
<p>View Encoding</p>	<p>You can view the network status, storage status, HDD usage, and</p>

<p>Device Details</p>	<p>overwritten recording status, etc.</p> <p>Also, you can tap the encoding device to view its details, including the basic information such as device type, serial No., and the network status of each linked camera. You can tap Camera to view all the linked cameras. If there is only one linked camera, tap  to view its live view. If there are multiple cameras, tap , and select one camera to view its live view.</p> <p>If the encoding device is a DVR, you can also view its HDD information, including self-evaluation results, overall evaluation results, operating status, run time, HDD temperature, and S.M.A.R.T information.</p> <p>For the analog camera, you can view if video loss occurs.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> ● If you do not have the Live View permission, you can apply for the live view permission from the end user. For details, see <u>Apply for Device Permission</u>. ● If a camera has been enabled with stream encryption, you must enter its device verification code in the pop-up window before you can view its live view. <hr/>
<p>View Access Control Device Details</p>	<p>Tap an access control device to view its details, including basic information such as device type, serial No., and the device status including network status and the number of its linked doors.</p>
<p>View Video Intercom Device Details</p>	<p>Tap a video intercom device to view its basic information and its network status.</p>
<p>View Network Switch Details</p>	<p>Tap a network switch to view its information, including working duration, the thumbnail of the switch, PoE Power, peak PoE power in last 7 days, port status (alarm, normal, not connected). You can tap the thumbnail of switch to view its enlarged image.</p> <hr/> <p> Note</p> <p>Working duration refers to the time from when the switch is turned on till the current moment. If the switch is turned off, its working duration will be recounted when turned on again.</p> <hr/> <p>Tap  → Device Information in the upper-right corner to view more basic information about the device, including device serial No., device model, device type, etc. You can tap Reboot Device at the bottom to reboot the device.</p>

Tap **...** → **Topology** in the upper-right corner to view the topology of this switch. For details about topology, refer to **Network Topology**. For the port with alarms, tap **Clear Alarm** to clear the alarm(s) of this port.

Tap **Extend Mode** to extend the transmission range of this port. Tap **Extend Mode** (displayed in green) to disable extending the transmission range of the port.

 **Note**

When enabled, the transmission range of the port will be extended from 200 m to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.

Chapter 9. Notification Center

The Notification Center module shows all the history business notifications and notifications of device/channel exceptions, which help you take reactions in time for the smooth operation of the devices. The module also keeps you informed about the system messages (such as the latest version of the system, newly added features, and successful company authentication) and the latest deals and offers (such as complimentary service packages).

Note

- All types of notifications received in the Notification Center can be sent as push notifications on your mobile device if you have push notifications enabled for the Mobile Client. Tap on a push notification to go straight to the corresponding details page.
 - The total number of unread notifications is displayed as a red badge on the top right corner of the Mobile Client icon.
-

9.1 Business Notifications

In the Business Notification module, you can receive the device management invitations from LTS Connect users for device management on LTS Platinum Partner, notifications concerning site sharing with the Maintenance Service Partner, etc.

In the upper-right corner of the page, tap  → **Business Notification** to access the Business Notification page.

Device Management Invitations

Besides receiving the device management invitation from LTS Connect users through an email, you can also receive it in the Business Notification on LTS Platinum Partner. After accepting the invitation, you will be able to manage the device on LTS Platinum Partner.

For details about accepting the invitation, refer to [**Accept a Device Management Invitation from Your Customer**](#).

Site Sharing Notifications

Both the person who shares sites and the person who accepts site sharing (MSP/ISP) can view the notifications concerning site sharing.

For the person who shares sites, you can receive site sharing notifications involving the customers and/or the MSP/ISP. For example, when the MSP/ISP accepts or cancels the site sharing, when the customer cancels the site sharing authorization to you and/or the MSP, or when the customer modifies your and/or the MSP's device management permissions.

For MSPs, you can receive site sharing notifications involving the Installer and/or the customers. For example, when the Installer cancels the site sharing, when the Installer shares a site with you and modifies your device management permissions, when the customer cancels the site sharing authorization to you and/or the Installer, or when the customer modifies your and/or the

Installer's device management permissions.

For details about accepting site sharing, refer to [**Accept Site Collaboration**](#).

Site Manager Change

When site managers change, for example, sites are assigned to new managers or site assignments expire, the corresponding site managers will receive notifications about the site manager changes.

Employee Joining Application

You can receive and view employees' applications to join the company in the app. Only those with employee management permission can approve/deny the applications.

If the application is approved, you can assign a role to grant the permissions to them. By default, the role administrator is selected.

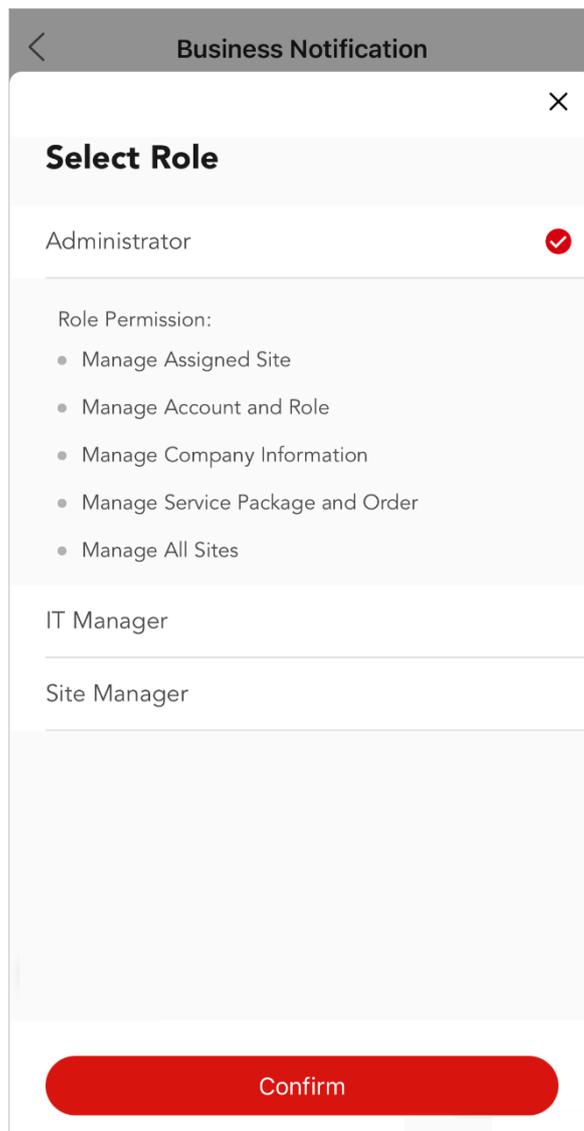


Figure 9-4 Select Role Upon Approving Employee Joining Application

9.2 Exception Center

If you have enabled device exception detection, real-time notifications will be sent to the Mobile Client or email when device exception occurs. The Exception Center shows all the history notifications of device exceptions and channel exceptions.

Note

- This feature is available only when you have activated the Health Monitoring Service.
 - For Installer Admin, you can view all the exceptions of the devices in all the added sites. For Installers, you can view the exceptions of the devices on the site which has been assigned to you.
 - You must set the exception rule first. For details, refer to [***Add Exception Rule***](#).
-

You can access the Exception Center page in the following ways:

- On the Home page, tap  → **Exception Center**.
- On the Home page, tap **More** → **Maintenance** → **Health Monitoring** → **Exception Center**.
- On the Home page, tap **Health Monitoring** → **Exception Center**.
- Tap **Site** → **Health Monitoring** → **Exception Center** to access the Exception Center page.

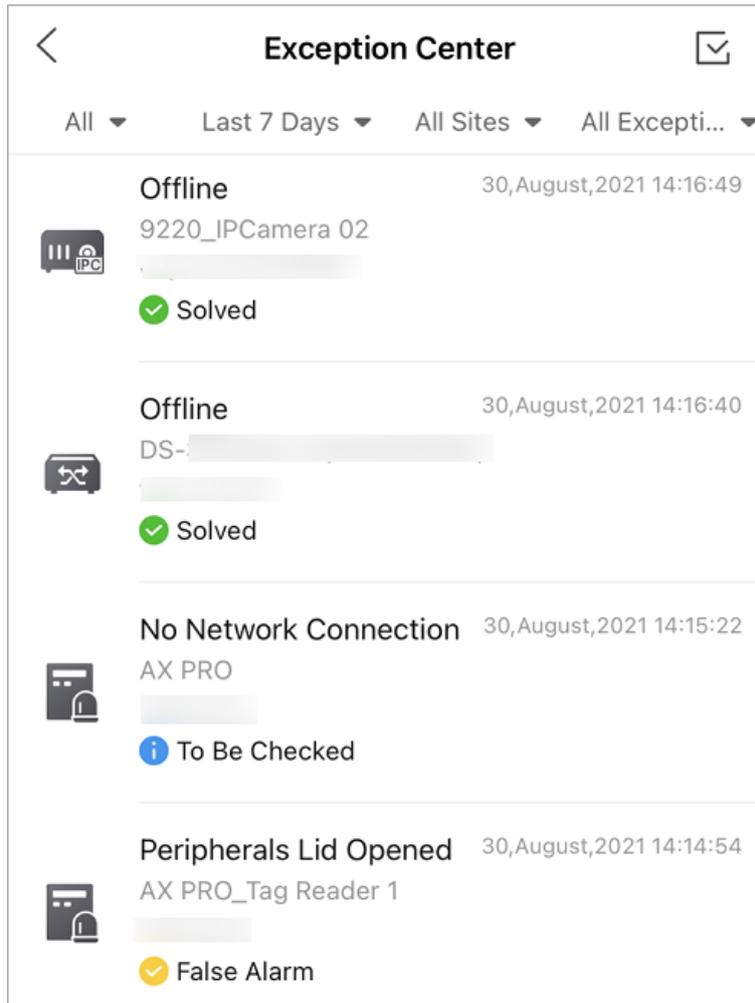


Figure 9-5 Exception Center

You can perform the following operations for the Exception Center.

Filter the Exceptions

You can filter the exceptions according to your actual needs.

1. Set the handling results from *all*, *unhandled*, *solved*, *to be checked*, and *false alarm*.
2. Set the time period as Today, Last 7 days, Last 30 Days, Last 60 Days, or Last 90 Days, or customize a specific one. The exceptions received during the set time period will be displayed.
3. Select a source (including site, device, and channel) from the drop-down list to view the corresponding exceptions.
4. Select the exception types that you want to check. The exception types include device exception and channel exception.

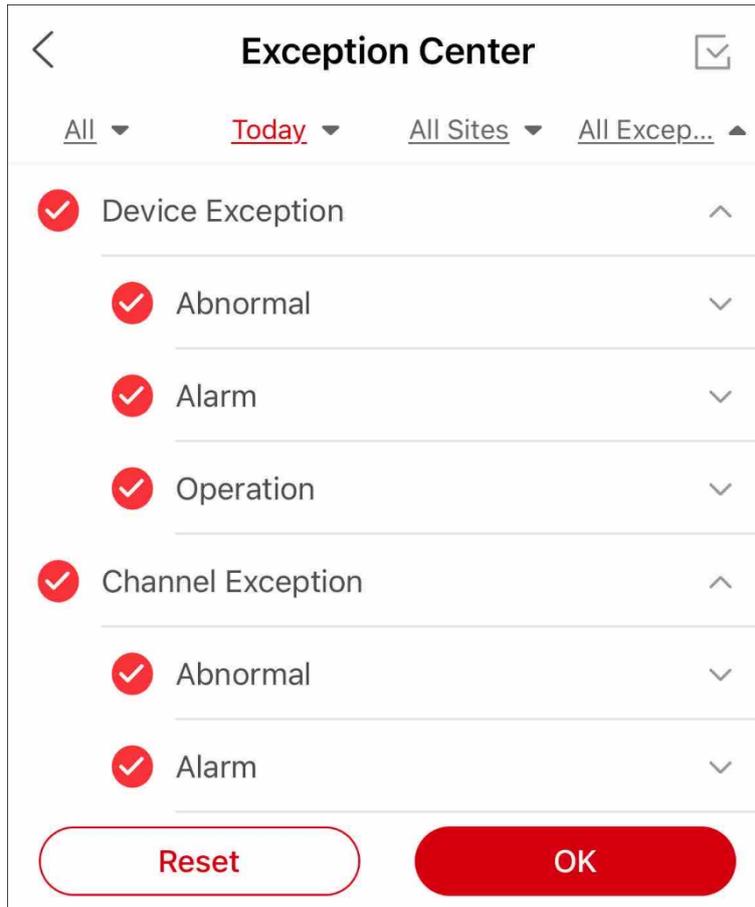


Figure 9-6 Exception Types

Handle an Exception

When you have solved an exception or you want to mark it for further examinations, you can select the handling results on LTS Platinum Partner. By handling the exceptions, you can better sort the exception list and avoid leaving some exceptions unattended. Your customer (the Site Owner) will also be informed of the handling results on LTS Connect.

Follow the steps below to handle an exception.

1. Tap on the exception to show the Handle Exception page.

Handle Exception ✕

Time	27,June,2022 19:33:34
Site Name	
Source	AX PRO 0554_Wireless Zone 1
Exception Type	Network Exception
Site Owner	
Received by	
Operator Account	--
Handling Time	--
Result	✔ Solved >

Handle

View Health Monitoring

Figure 9-7 Handle Exception

2. Select a handling results in **Result**. You can select from **Solved**, **To Be Checked**, and **False Alarm**.
3. Tap **Handle** to save the changes.

Jump to Device Health Monitoring

On the Handle Exception page, you can tap **View Health Monitoring** to jump to the device's health monitoring page to troubleshoot the exceptions.

9.3 System Messages

The System Message tab of the Notification Center supports displaying system messages to keep you informed of any system-related information. You can view basic information of the messages in the list, including the message title, time when it was generated, the read/unread status, and the message content (in the form of texts or images).

In the upper-right corner of the page, tap  → **System Message** to access the System Message page.

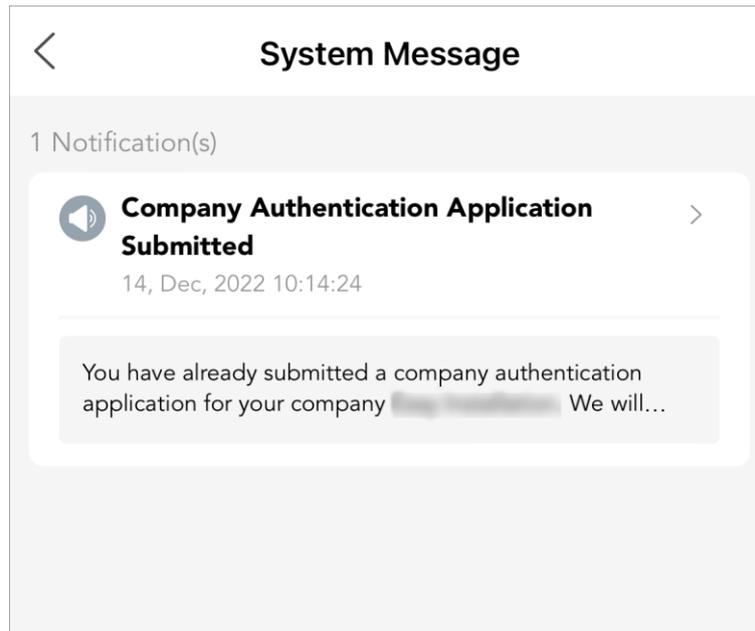


Figure 9-8 System Message Page

Feature and Version Updates

You can receive and view messages of system version updates and newly added features.

Complimentary Service Packages

You can receive and view messages notifying you of the complimentary value-added service packages issued to your account, which tell you the type of service packages and the total quantity.

Company Authentication Application Related

You can receive and view messages related to company authentication applications, which include status change information such as application submitted, application approved, and application declined. You can also receive and view the message when the authentication status of your company turns from authenticated to unauthenticated due to incomplete company information or company information expiration.

Note

- These are relevant for online applications only. If you are authenticating your account with an

authentication code, status change information will not be displayed here.

- Only users who have the permission to manage company information can view messages of company authentication status change.
-

Employee Joining Application Approved

You can receive a notification after you successfully join a company.

Chapter 10. Value-Added Services

LTS Platinum Partner provides multiple value-added services for you to better serve your customers, including the health monitoring service, co-branding service, and employee account add-on.

10.1 Viewing and Purchasing Value-Added Services

You can view the information of the following value-added services in the Service Market of the Mobile Client. Tap **Me** → **Service Market** to access the Service Market page to view details of the value-added services and activate by service key.

For purchasing other services by service key, you must go to the Portal.

Steps

1. Tap **Activate by Service Key** on the Health Monitoring Package card to open the Purchase by Service Key page.
2. Enter a service key or multiple service keys (separated by commas) purchased from LTS.
3. Tap **OK**.

10.2 Viewing and Managing My Services

On the My Service page, you can conveniently view and manage all your services.

Tap **Me** at the bottom right and tap **My Service** to access the My Service page.

The service section introduces a service and shows the numbers of used and remaining service packages (or employee accounts as for employee account add-on).

The My Service page shows the following sections.

Trial Period Information

The page shows this section only during the trial period.

This section presents the description and the end time of the trial period.

Free Package Information

This section presents the description of the free package, maximum number of manageable devices, and number of managed devices.

You can tap **Detail** in this section to view the differences between the free package and health monitoring package, and purchase health monitoring service packages by service keys.

Services Expiring Soon

The page shows this section only if there are services expiring soon.

You can tap **View** to go to the detail page for the service to renew it.

Health Monitoring Service

On the detail page for the health monitoring service, you can conveniently view the devices with services expiring in 30 days, devices with expired services, and devices with auto renewal, and perform operations as follows.

Table 12-1 Supported Operations on Details Page for Health Monitoring Service

Operation	Description
Filter Devices by Site	Tap All Sites and select a site to view the devices on the site and perform renewal / batch renewal, activation, etc.
Filter Devices by Service Status	Tap All , Expire Soon , Expired , or Auto Renewal to view devices with each service status.
Renew Service for Device	Tap  to renew the service for one device.
Transfer Service	Tap  to transfer the remaining service time to another device.
Enable/Disable Auto Renewal	Tap  to enable/disable auto renewal for the device.
Batch Renew for Devices	Tap Batch Renew at the bottom, select devices, and tap OK to batch renew.
Activate Service	Tap Activate Service , select devices, select activation type, and tap OK .

Employee Account Add-On

On the detail page for the employee account add-on, you can conveniently view the added employees, and add, delete, enable, and disable employees.

10.3 Co-Branding

After you purchase the co-branding service, you can enable this service to allow your customers to view your company information, such as logo, email address, and phone number on the LTS Connect Mobile Client. This will help promote awareness of your company brand, products, and services.

Step 1: Purchase Co-Branding Service

Tap **Activate by Service key**, enter one or multiple keys (separated by commas), and tap **OK**. (Optional) Upload your company logo for increased brand visibility. If no company logo is uploaded, your company name, instead of your company logo, will be displayed on the startup and live view page of NVR/DVR and LTS Connect Mobile Client.

Step 2: Enable Co-Branding

Tap **Me** → **Company Management** → **Co-Branding** and enable this feature.

Chapter 11. Support

In the Support module, you can find tools, tutorials, documentation, solutions, etc., to get support and improve your work efficiency.

- **Tools**

Provides tools that may improve your work efficiency during the device installation and maintenance.

You can access Tools by tapping in the Application Center.

- **Contact Us**

You can get the contacts (i.e., address, phone, and email) of our headquarter and the local office, and the email address of your sales representative.

You can access the Contact Us page in the Application Center or on the Me page.

- **After-Sales Authorization Code**

Provides an entrance for you to view the after-sales authorization code of your company. The after-sales authorization code is exclusive to the technical support staff for troubleshooting only. You can give your authorization code to the staff when it is necessary to log in to your account for troubleshooting. The staff can log in to your account via the authorization code to view or edit the information about the company (name, type, etc.), manage sites, remotely devices, perform health monitoring, etc.

You can access the After-Sales Authorization Code page in the Application Center or on the Me page.

Set the validity period, check the statement, and tap **Generate** to generate a code. You can click **Extend** to extend the validity period for the current authorization code or click **Invalidate Authorization Code** to invalidate the code right away.

 **Note**

One company can only have one valid after-sales authorization code. If the code is invalidated or your company has no authorization code, you can choose to generate one.

- **Reset Device Password**

Provides convenient ways to reset device passwords.