LTS Platinum Partner Web Portal

User Manual

Contents

Chapter 1. Introduction

The LTS Platinum Partner is a one-stop security service platform that partners efficient customer and device management tools and extended value-added services with round-the-clock convenience. LTS Platinum Partner also serves as a convergent, cloud-based security solution, helping partners manage services for their customers and expand their businesses using subscription offers. Partners can monitor the system health status of customers' sites, resolve problems remotely, and customize security solutions with fully converged LTS devices, covering video, access, intercom, and more.

Read the following sections to learn more about LTS Platinum Partner.

- ***Clients***
- ***Relationship Among LTS Platinum Partner and LTS Connect***

Clients

LTS Platinum Partner provides various clients for partners (service providers) and their customers.

Table 1-1 Client Description

Client	Description
LTS Platinum Partner Web Portal	Portal for service providers logging in to LTS Platinum Partner to manage their security businesses, such as permissions and employee’s management, site management, device management and device health monitoring.
LTS Platinum Partner Mobile Client	Mobile Client for service providers logging in to LTS Platinum Partner to manage site, apply for site information management permission from end users, manage and configure devices, submit RMAs (Return Material Authorization) requests, 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 for site information management permissions, etc.
LTS Connect Web Portal	Portal for customers to manage their employees' access levels and attendance after setting an attendance system for them via the LTS Platinum Partner Portal.

Relationship between LTS Platinum Partner and LTS Connect

LTS Platinum Partner provides certain value-added services related to LTS Connect. You can activate these value-added services to benefit yourselves or your customers (i.e., end users). For more information about the value-added services and how they relate to LTS Connect, see ***Value-Added Services*** and its sections.

1.1 Target Audience

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

This manual describes how to manage the permission and employees of your company, add new or existing sites for management, apply for site authorization and device permissions from your customers, manage and configure devices belonging to a site, and check the device health status for further maintenance.

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

Sites

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 Sites

For individual users, 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 Sites

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, attendance check, 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 and services of the site.

Site Owner

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

1.3 Operating Environment

The following are recommended for running the Portal.

Operating System

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

CPU

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

RAM

8 GB and above (4 GB at least).

Graphics Card

NVIDIA® GeForce GT 730

Web Browser

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

1.4 Function Availability

Table 1-2 Functions

Module	Function(s)
Account Management	● ***Register an Installer Admin Account*** ● ***Manage Company Information*** ● ***Set Account Information***

Module	Function(s)
Site Management	● ***Add Personal Site*** ● ***Hand Over Personal Site by Transferring*** ● ***Apply for Site Authorization from Site Owner*** ● ***Site Collaboration***
Device Management	● Add Device • ***Add Detected LAN Device*** • ***Add Device by Entering Serial No.; Add Devices by IP Address or Domain Name*** • ***Batch Add Devices*** ● ***Apply for Device Permission*** ● ***Release Permission for Devices*** ● ***Synchronize Devices with LTS Connect Account*** ● ***Enable Device to Send Notifications*** ● ***Upgrade Device*** ● ***Batch Upgrade Devices on LAN*** ● ***Configure DDNS for Devices*** ● ***Remote Configuration*** ● ***Reset Device Password*** ● ***Unbind a Device from Its Current Account***
Video	● ***View Live Video*** ● ***Play Back Video Footage***
Log	***Search Operation Log***
Tool	***Tools***
Explore	● View, Search, Like, Share, and Comment on Feeds, and Add to Favorites ● View, Search, Like, Share, and Comment on How To, and Add to Favorites ● View, Search, Like, Share, and Comment on Videos, and Add to Favorites ● Receive and View Notices ● Register for and Participate in Events

1.5 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.
ℹ**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.

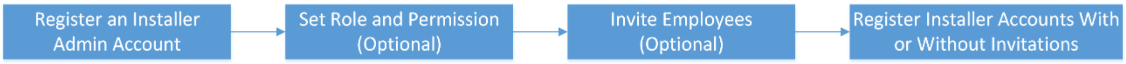
Installer Admin

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 permissions 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, and then employees can be invited to register Installer accounts, or they can register Installer accounts without invitation by applying to join existing companies on registration.
The flow chart of the whole process is shown as follows.



Register an Installer Admin Account → Set Role and Permission (Optional) → Invite Employees (Optional) → Register Installer Accounts With or Without Invitations

Figure 2-1 Flow Chart of Account Management

- **Register an Installer Admin Account:** You should 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 Employee***.
- **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 Register an Installer Admin Account

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

Steps

Note

You can click **Try Free Demo** on the login page to see what LTS Platinum Partner can do for you, without registering any account. The data displayed in the demo is for demonstration only, and you cannot perform any operations.

1. In the address bar of the web browser, enter ***https://www.ltsplatinumpartner.com***.
   The Login page of LTS Platinum Partner will show.
2. On the Login page, click **Register** to register an account.

   Note

   If your account has been registered, you can click **Login** to log in to LTS Platinum Partner. For details about login, refer to ***Login***.

3. Select your identity and service provider type.
4. Select whether you are to register by email or by phone number.
5. 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) Click **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, click **Create Company** to continue registering an Installer Admin account.

   You will receive confirmation that you have registered successfully, and the **Company Authentication** window will pop up.
6. Click **Authenticate Now** or **Later** to enter either of the following processes.
   - Click **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. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in the agreements.
3. Click **Confirm** to submit the application and enter LTS Platinum Partner.

– Click **Later** to go to the Complete Information page.

1. Send the required information (address, etc.).
2. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in the agreements.
3. Click **Confirm** to enter LTS Platinum Partner.

Note

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

2.2 Manage Roles and Permissions

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

Steps

Note

- 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.
  - **Administrator**: Setting company information, managing employees, checking operation logs of all the employees, and managing all the sites.
  - **Technician**: Managing assigned sites, adding, configuring, and deleting devices, and activating valued services for end users of assigned sites.
  - **IT Manager**: Managing all the sites, assigning sites to other employees, activating or editing valued service for all the end users, and viewing operation logs of all the employees.

1. Click **My Partner** → **Company Management** → **Role and Permission** to display all the roles.
2. Add a role.

   1.) Click **Add Role** to open the Add Role panel.

   2) Enter the role name and select permissions for the role.

   Manage All Sites

   Managing all sites, including adding and editing sites, assigning sites to site managers, handing over sites, applying for site authorization, searching sites, applying for device permissions, adding, deleting, editing, and upgrading devices on the sites, and health monitoring.

If you select this permission, you can continue to configure device permissions of this role, including:

- Remote Configuration, Live View, Playback, Invite Customers (for sharing devices to more customers)

Manage Assigned Site

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

Note

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

Manage Account and Role

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

3) Optional: Enter remarks of the role in the **Description** field.
4) Click **OK**.

3. Optional: Check added roles and click **Delete** to delete the selected role(s).

Note

You cannot delete a role which has been assigned to an employee.

2.3 Invite Employees

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

1. Open the Add Employee pane.
   - Click **Company** → **Employee** → **Add Employee**
   - On the Home page, click **Company** → **Role and Permission** and then click **Add Employee** in the Operation column.
2. Enter the email of the to-be-invited employee.
3. Select a role for the employee.

Note

You can also create a new role. For details, refer to ***Manage Role and Permission***.

The permissions of the role will be displayed.

4. Click **Add**.

   The invited employee will receive an email delivering a link in the entered email box. The employee needs to click the link to register an account, after which the employee's information will be displayed in the employee list.

5. Optional: Perform the following operations after adding employees.

Enable/Disable Employee Acct.

Click ✓/⊖ in the Operation column to enable or disable the employee account.

Note

- Once disabled, the employee cannot log in to the platform via this account.
- You cannot disable your own account and the Installer Admin account.

Remove Account Limits

Note

- 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 ***Purchase Employee Account Add-On***.

To remove the account limits, you can 1.) click 👤 in the Operation column, or 2) hover your mouse cursor over ⓘ in the Status column and click **Remove Limit**.

Delete Employee Accts.

Check one or more employees and click **Delete** to delete the selected employee(s) acct. if needed.

Note

- 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 ***Become an LTS Platinum Partner User After Product Upgrade*** for details.

View Employee Details

Click an employee to open the Employee Details pane to view the employee's contact number, email address, role permissions, and so on.

Edit Role Assigned to Employee

Click an employee to open the Employee Details pane and click ✎ in the Role field to enter the Edit Role pane. Then you can click **Add** to add a new role or select another role for the employee.

Note

You cannot edit roles assigned to your own account and the Installer Admin account.

View Sites Managed by Employee

Click an employee to open the Employee Details pane or click the information in the Managed column to view the list of all sites managed by the employee. You can click a site to view the site details.

Note

The above operation is supported only when the employee has site(s) to be managed.

2.4 Register an Installer Account With 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 who has permission to **Manage Account and Role** should invite the employee first. For details about inviting employees, refer to ***Invite Employee***.

1. After you are invited to join a company as an employee, you will receive an email from LTS Platinum Partner.
2. Click the button or the link in the email.
3. Click **Register** to open the Create Account page.
4. Set the type, name, verification code (for verifying the email address), and password.
5. Check **By clicking Register, I agree to LTS Privacy Policy.**

6. Click **Register**.

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

2.5 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.

Before You Start

Make sure you have registered an account. See ***Register an Installer Admin Account*** or ***Register an Installer Account With or Without an Invitation*** for details about registration.

Steps

1. In the address bar of the web browser, enter ***https://www.ltsplatinumpartner.com***.
   The login page of LTS Platinum Partner will show.
2. Enter the registered email and password.
5. Optional: Reset the password if you have forgotten the password.
   1.) Click **Forgot Password** to enter the resetting password page.
   2) Click **Get Verification Code**.
      You will receive a verification code sent by the Portal in your email box.
   3) Enter the received verification code in the **Verification Code** field.
   4) Enter the new password and confirm the password.
   5) Click **OK**.
      By default, you will be required to log in with the new password.
6. Click **Sign In** or **Login**.

Note

If you have completed company merging and your account still exists in more than one company, or if the companies in which your account exists are all kept on LTS Platinum Partner, you need to select one company for login. You can also click **Switch Company** on the Company Information page to switch to another company. For details, refer to ***Become an LTS Platinum Partner User After Product Upgrade***.

2.6 Set Account Information

After logging in, you can edit the basic information of the current account and change password if necessary. Click the name at the upper-right corner and select **Account Settings**.

Set Basic Information

Set the basic information of the current account, including the name of the Installer, email address, phone number, etc.

Note

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

Click to set the profile of the current account.

Manage My QR Code

Hover over 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 click **Add Your Company Logo to the QR Code** to upload your company logo.

Click to download the QR code.

Change Password

Click to change the password of the current account.

Change Account's Bound Email

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

1. In the Basic Information page of the account settings, click .
2. Enter a new email address in the **New Email** field.
3. Click **Verify**.
   In the new email address, you will receive an email with a verification code.
4. Enter the received verification code in the **Verification Code** field.
5. Enter the password of the current account.
6. Click **Save**.

Delete Installer Admin Account

For Installer Admin, if the account is no longer used, you can delete it in the Basic Information page of the account settings.

Note

- Deleting the 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. In the Basic Information page of the account settings, click **Delete Installer Admin Account**.
2. Enter the password of your Installer Admin account and click **Next**.
3. Click **Delete Installer Admin Account** to confirm deleting.

Chapter 3. Company Management

After registering an Installer Admin account, you can edit your company information, authenticate your company to purchase value-added services and use more features, and merge companies into one for efficient management. In addition, you can also view the efficiency statistics and search for operation logs of all employees.

3.1 Manage Company Information

After registering an Installer Admin account, you can manage and edit your company information.

Steps

Note

- Before your company is authenticated, the Installer Admin can manage and edit all the company information; when your company authentication application is approved, the Installer Admin can submit the information change request, and the information will be edited successfully after approval.
- You can link your Installer Admin account to a distributor via the LTS Platinum Partner Mobile Client to get support and help from the distributor. For details, see *LTS Platinum Partner Mobile Client User Manual*.

1. Go to **Company** → **Company Information**
2. Enter the name of your company.
3. Enter other information of your company, such as the address, GPS information, postal code, phone number, email, and user type.
4. Optional: If you want to upload the company logo, click **+** to upload the picture of your company logo, or click **Edit** to re-upload a picture to update the logo.

Note

- The picture should be in JPG, JPEG, or PNG format.
- Recommended picture size: Height = 200px, 200px ≤ Width ≤ 600px.
- You are not allowed to enable the Co-Branding function if you have not set the company logo. For details about Co-Branding, see ***Co-Branding***.

5. Optional: Enter the website of your company.
6. Optional: Enter or edit the description information, which will be displayed on LTS Connect Mobile Client.
7. Click **Save** to save the configurations.

Note

You can check the percentage of completed information after saving.

3.2 Authenticate Company

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

By Entering Authentication Code

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

1. Go to **Company Management** → **Company Information**, and click **Authenticate Now**.
   Optional: If you have no authentication code, click **Get Authentication Code**, 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 ID, company name, and phone number, to LTS or the distributor, and apply for one authentication code.

Note

- You can click ✎ to edit the information in the template. The edited contents will be updated in the company information.
- If the email server is not configured or the recipient's address is not completed automatically, you can copy the content and send it to LTS or the distributor by your own email box.

2. Once you receive the authentication code, enter it on the account authentication page and click **OK** to authenticate your account.

By Submitting Online Application

In this way, you need to complete 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 login.

1. Go to **My Company Management** → **Company Information** page and click **Authenticate Now**. Review and edit the company information already filled in and set other required information, such as company name, address, city, etc.
2. Click + to upload a picture (e.g., business license and business card) as evidence.
3. Enter the distributor if you have bought LTS products.

4. Click **Authenticate Now**.
   The application information will be sent.

Note

After your application is approved, you will be notified via push notification and email.

3.3 View Employee Efficiency Statistics

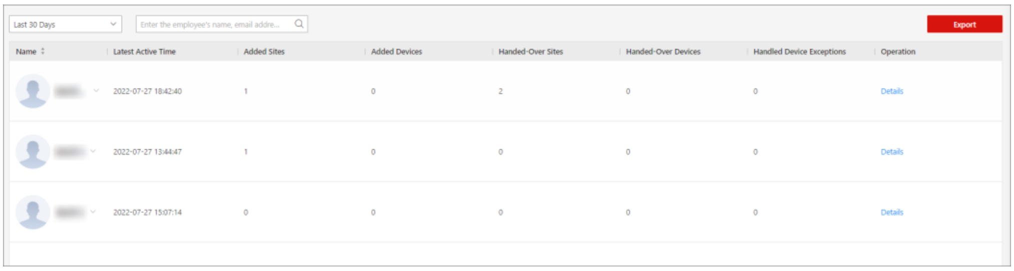
You can view the efficiency statistics of all employees, including the latest active time, added sites, added devices, handed-over sites, handed-over devices, and handled device exceptions. You can also perform operations such as exporting efficiency statistics.

Note

This is supported only if you have permission to manage the employees.

You can enter the Employee Efficiency Statistics page via the following methods:

- Go to **Company** → **Employee Efficiency Statistics**.
- Click **View All** in the Employee Efficiency Overview section.



Name	Latest Active Time	Added Sites	Added Devices	Handed-Over Sites	Handed-Over Devices	Handled Device Exceptions	Operation
[redacted]	2022-07-27 18:42:40	1	0	2	0	0	Details
[redacted]	2022-07-27 13:44:47	1	0	0	0	0	Details
[redacted]	2022-07-27 15:07:14	0	0	0	0	0	Details

Figure 3-14 Employee Efficiency Statistics Page

You can perform the following operations if needed.

Table 3-1 Supported Operations

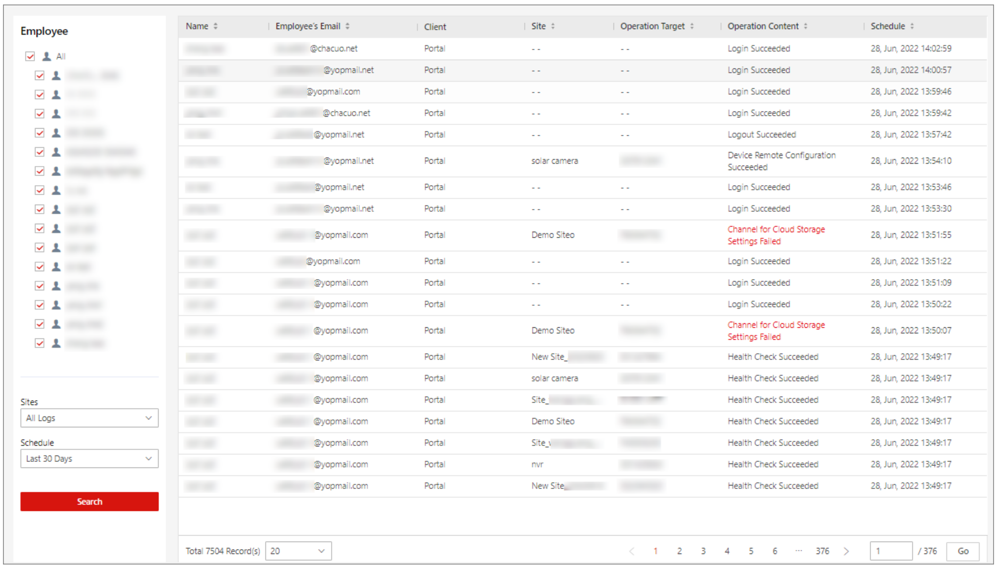
Operation	Description
View Operation Logs of an Employee	Click **Details** in the Operation column to switch to the Operation Log page to view the operation logs of the corresponding employee.
Filter Statistics	Click ⌄ to filter the efficiency statistics by time period (i.e., today, yesterday, this week, last 7 days, last 30 days, or custom time period).
Search for Statistics	Enter the employee's name, email address, or phone number in the search box to search for statistics.
Export Statistics	Click **Export** to export statistics in XLSX or CSV format.

3.4 Search Operation Log

Operations information (including the operator, operating time, site, operation target and result, etc.) of the employees (referring to Installer Admin and Installers) will be recorded. You can search for the operation logs of any employee within 90 days for troubleshooting the sites and devices. Click **Company Management → Operation Log** to display the employee list and all the operation logs. You can search for logs by the employee, site, and time.

Note

- Logs of all accounts are available to accounts with the permission to manage accounts and roles. For accounts without permission to manage accounts and roles, they can only view their own logs.
- Logs of all sites are available to accounts with the permission to manage all sites. For accounts without permission to manage all sites, they can only view the logs of assigned sites.
- Logs within 90 days are available.



Employee

☑ All
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]

Sites: All Logs

Schedule: Last 30 Days

Name	Employee's Email	Client	Site	Operation Target	Operation Content	Schedule
[redacted]	[redacted]@chacuo.net	Portal	- -	- -	Login Succeeded	28, Jun, 2022 14:02:59
[redacted]	[redacted]@yopmail.net	Portal	- -	- -	Login Succeeded	28, Jun, 2022 14:00:57
[redacted]	[redacted]@yopmail.com	Portal	- -	- -	Login Succeeded	28, Jun, 2022 13:59:46
[redacted]	[redacted]@chacuo.net	Portal	- -	- -	Login Succeeded	28, Jun, 2022 13:59:42
[redacted]	[redacted]@yopmail.net	Portal	- -	- -	Logout Succeeded	28, Jun, 2022 13:57:42
[redacted]	[redacted]@yopmail.net	Portal	solar camera	[redacted]	Device Remote Configuration Succeeded	28, Jun, 2022 13:54:10
[redacted]	[redacted]@yopmail.net	Portal	- -	- -	Login Succeeded	28, Jun, 2022 13:53:46
[redacted]	[redacted]@yopmail.net	Portal	- -	- -	Login Succeeded	28, Jun, 2022 13:53:30
[redacted]	[redacted]@yopmail.com	Portal	Demo Siteo	[redacted]	Channel for Cloud Storage Settings Failed	28, Jun, 2022 13:51:55
[redacted]	[redacted]@yopmail.com	Portal	- -	- -	Login Succeeded	28, Jun, 2022 13:51:22
[redacted]	[redacted]@yopmail.com	Portal	- -	- -	Login Succeeded	28, Jun, 2022 13:51:09
[redacted]	[redacted]@yopmail.com	Portal	- -	- -	Login Succeeded	28, Jun, 2022 13:50:22
[redacted]	[redacted]@yopmail.com	Portal	Demo Siteo	[redacted]	Channel for Cloud Storage Settings Failed	28, Jun, 2022 13:50:07
[redacted]	[redacted]@yopmail.com	Portal	New Site_[redacted]	[redacted]	Health Check Succeeded	28, Jun, 2022 13:49:17
[redacted]	[redacted]@yopmail.com	Portal	solar camera	[redacted]	Health Check Succeeded	28, Jun, 2022 13:49:17
[redacted]	[redacted]@yopmail.com	Portal	Site_[redacted]	[redacted]	Health Check Succeeded	28, Jun, 2022 13:49:17
[redacted]	[redacted]@yopmail.com	Portal	Demo Siteo	[redacted]	Health Check Succeeded	28, Jun, 2022 13:49:17
[redacted]	[redacted]@yopmail.com	Portal	Site_[redacted]	[redacted]	Health Check Succeeded	28, Jun, 2022 13:49:17
[redacted]	[redacted]@yopmail.com	Portal	nvr	[redacted]	Health Check Succeeded	28, Jun, 2022 13:49:17
[redacted]	[redacted]@yopmail.com	Portal	New Site[redacted]	[redacted]	Health Check Succeeded	28, Jun, 2022 13:49:17

Total 7504 Record(s) 20

Figure 3-15 Search Operation Logs

Chapter 4. LTS Platinum Partner Portal Overview

LTS Platinum Partner Portal is a B/S portal of the LTS Platinum Partner platform. The service providers (e.g., installation company) can register an Installer Admin account on LTS Platinum Partner, and then the Installer Admin can invite employees to register Installer accounts. Each company has only one Installer Admin but can have multiple Installers.
After registering, the Installer Admin and Installers can log into the LTS Platinum Partner via the web browser and the Home page of the LTS Platinum Partner Portal will show.

4.1 Main Modules

The LTS Platinum Partner Portal is divided into several main modules. You can access these modules via tabs at the top.

Home Page

On the Home page, you can check the number of added sites or devices, view the wizard about how to add and manage devices, view the number of abnormal devices and total devices, check the number of not-yet-handled and to-be-followed-up exceptions, check the efficiency statistics of all employees, view some banners showing key features, functions, and important information, have an overview of your services, manage services, set more value-added services for devices, and view video tutorials and documents to learn more about the platform and the proper ways of using the platform.
If you have any issues or suggestions when using LTS Platinum Partner, you can report them via Case or Feedback. You can also use some online tools to improve your work efficiency and quickly access some pages such as the site adding page, device adding page, and health monitoring page. Refer to ***Home Page*** for details.

Company Management

Company Information

View and manage the company information. See ***Manage Company Information*** for details.

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 various permissions to employees according to actual needs. Installers with permission to **Manage Account and Role** can also invite other employees to be Installers by registering Installer accounts. See ***Invite Employee*** for details.

Employee Efficiency Statistics

See the efficiency statistics of all employees, including the latest active time, added sites, added devices, handed-over sites, handed-over devices, and handled device exceptions here.

See ***View Employee Efficiency Statistics*** for details.

Manage My Agreements

Distributors can manage and sign contract agreements of partner programs with resellers and LTS on LTS Platinum Partner.

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. See ***Manage Role and Permission*** for details.

Operation Log

View the operation logs of your accounts and sites in the current company. See ***Search Operation Log*** for details.

Co-Branding

Enable the displaying of a company logo on the LTS Connect Mobile Client for brand promotion to end users. For details about how to get the co-branding service for free and enable the service, refer to ***Co-Branding***.

Account Information

My Profile

Edit your account information, including profile photo, name, email address, password, and phone number. Refer to ***Set Account Information*** for details.

My Favorites / My Comments

View your past comments on news and how-to articles, and view the news, how-to articles, and solutions that are added to your Favorites.

4.1.1 Home Page

Table 4-2 Home Page Description

Name	Introduction
Site & Device Overview	View the total number of sites/devices & the number of abnormal sites/devices. Click **Add Site** to add a new site. For details, refer to ***Add Personal Site***. Click **Add Device** to add a device. You can also click ? in the top right corner of the Site & Device Overview pane to open the wizard about adding devices, handing over devices to customers, and remote configuration. Click **Add Device Now** to start adding a device. For details, refer to ***Add Device***. The recently visited sites will be displayed on the Site & Device

Name	Introduction
	Overview pane and you can click a site name to enter the site details page. **Note** ● If there are no sites or devices added, the wizard will automatically be displayed on this panel. ● A prompt will appear at the top of this pane to show the number of notifications to be handled, and you can click **Handle Now** to enter the Notification Center module to handle these notifications.
Health Monitoring Overview	You can view the number of abnormal devices and total devices, including devices overall and each device type respectively. **Note** You can click **More** to enter the Health Status page to check the details about device status. For detailed instructions about Health Status, refer to ***View Status of Devices in All Sites*** and ***View Status of Devices in a Specific Site***.
Exception Notification Overview	You can view the number of not-yet-handled and to-be-followed-up exceptions and numbers of top 5 types of those exceptions. You can click a number on a chart to enter the Exception Center page and the exceptions will be filtered correspondingly. For example, if you click the number on the “Not Handled” chart, the exceptions will be filtered by the status of Not Handled on the Exception Center page. **Note** ● To receive exception notifications, you need to configure the recipient when setting the exception rule. For details, refer to ***Add Exception Rule***. ● The number of exceptions you view here may not be the same as that in the Exception Center. You can click **More** to enter the Exception Center page to see received exceptions. For detailed instructions about Exception Center, refer to ***Exception Center***.
Employee Efficiency Overview	You can view the efficiency statistics of all employees, including the numbers of added sites and handed-over sites, the numbers of added devices and handed-over devices, the number of device exceptions,

Name	Introduction
	the exception handling rate, and the numbers of handled and to-be-handled exceptions. You can also filter statistics data by this month, this week, and today, or click **Refresh** to display the latest statistics data. If you want to view more data, click **More** to enter the Employee Efficiency Statistics page. For details, refer to ***View Employee Efficiency Statistics***. **Note** This is only supported only if you have permission to manage the employees.
My Service Overview	You can have an overview of your services and manage the services.

Free Package (Adding Devices + Remote Configuration)

- Display number of managed devices and devices that can be added.
- Display the entrances for adding devices and synchronizing devices from LTS Connect.

Co-Branding

Display the company logo when co-branding is enabled and the entrance for enabling the co-branding.

Health Monitoring Service

- Display the numbers of used and available service packages and the entrance for activating the service.
- Display the number of devices with expiring or expired service and the entrance for details, if there are devices with the service expiring within 30 days.
- Display the numbers of device exception notifications and scheduled reports if there are devices using the health monitoring service.
- Display the entrance for renewing/expanding.
- Display the entrance for getting the free health monitoring packages (if any).
- Display the entrances for enabling the device exception notifications and configuring the scheduled reports.

Employee Account Add-On

- Display used and available employee accounts.
- Display the expiry time when the service is expiring within 30 days and displaying the entrance for renewing the service
- Display entrances for inviting employees and managing employees.

4.1.2 Site & Device Module

The Site & Device module is divided into several sections. You can access these sections via the navigation pane on the left.

Note

- You can click 📌 to pin or unpin the navigation pane on the left of the page.

Table 4-3 Site & Device Module

Name	Introduction
Dashboard	You can check the total number of sites / devices, view the wizard about how to add and manage devices, view the number of abnormal devices and total devices, check the number of Not Handled and To Be Followed Up exceptions, check the efficiency statistics of all employees, have an overview of your services, manage services, set more value-added services for devices, and view online documents to learn more about the platform and the proper ways of using the platform.

Customer Site

A site represents a physical location where devices are installed and through which the Installer Admin/Installer can manage the devices.

Site Map

If sites are configured with the GPS information, they can be displayed on the map for viewing the site details, such as the site name, site owner, site location, and number of online/offline/abnormal devices.

Health Status

The Installer can view the devices overall, normal, and abnormal status, locate the abnormal devices, and perform troubleshooting quickly.

Exception Center

After setting the exception rules, when an exception occurs on the device, the device will push a notification to the Portal and you can view all the received notifications of exceptions in the Exception Center.

4.2 Other Modules

Global Search

Click 🔍 in the top right corner of the Portal to open a search pane. Select **All**, **Sites**, **Device**, **Feeds**, or **How To** and enter the corresponding keyword to search for sites, devices, feeds, or how-to documents/videos.

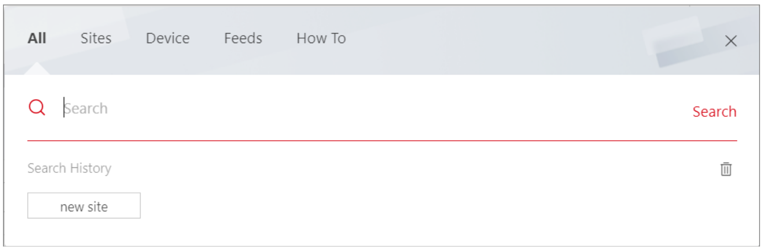


Figure 4-3 Global Search Pane

The search results will be listed on a new page. You can view the site information (including the site owner, phone number of the site owner, site address, site type, and site manager), the device information (including device name, device type, device serial no., online status, and health monitoring status), and the short descriptions of feeds or how to. You can also click a result item to enter the corresponding details page.

The search history will be displayed on the search pane, and you can click a historical keyword to search again or clear the search history.

Switch Company

If you have upgraded and become an LTS Platinum Partner user and your account still exists in more than one company, click ⇄ in the top right corner of the Portal to switch companies for logging in.

Notification Center

See all historical business notifications (including device management invitations, site sharing notifications, etc.), notifications of device/channel exceptions, new features of the system messages, and the latest deals and offers. For more details about the notification center, refer to ***Notification Center***.

Help

Click ? in the top right corner of the Portal to show a drop-down list.

User Manual

Provides an entrance for viewing the user manual of the LTS Platinum Partner Portal online.

Wizard

View a wizard that guides you through the process of configurations and operations.

Click **Next** or **Previous** to go through the introductions in the wizard. You can click the image on the right to view the large image and check the details on the image if necessary.

Click **Skip** to close the wizard.

After-Sales Authorization Code

Provides access for you to view the after-sales authorization code(s) 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 configure devices, perform health monitoring, etc.

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

A 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.

Profile Photo and Account Name

In the upper-right corner of the Portal, click the account name or profile photo to open the drop-down list.

Account Settings and Upgrades

Access for editing the basic information of the account or deleting the Installer Admin account if it is no longer used. For details, refer to ***Set Account Information***.

Link with LTS Connect Account

Access for linking your LTS Platinum Partner account with multiple LTS Connect accounts, so the devices managed in the LTS Connect account can be synchronized to an LTS Platinum Partner account automatically. For details, refer to ***Synchronize Devices with LTS Connect Account***.

My QR Code

Provides access for downloading your QR code so your customers can scan via the LTS Connect Mobile Client to add you as the service provider and authorize you to manage devices.
You can also go to **Account Information** → **My Profile** page to view your QR code.

Note

This feature is only supported by accounts with the Manage Assigned Sites permission.

About

View the version of the current system, and read the agreements, including terms of service, privacy policy, and open-source license. You can also scan the QR code with your mobile phone to download the LTS Platinum Partner Mobile Client.

Switch Company

Provides access for switching companies when logging in if you have completed company merging and your account still exists in more than one company, or if the companies in which your account exists are all kept on the LTS Platinum Partner.

Log Out

Log out of the current account and return to the login page.

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: personal and team. Personal sites are for individual users and apply to households and independent stores. Team sites are for enterprise users and apply to scenes where multi-user management is required, such as chain stores, offices, and communities. You can create a site 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 Transferred-Site Scenario

A typical transferred site scenario is where the devices are owned by customers, and the installer provides the device installation and maintenance service for the customers. The devices will be available to the installer only if the customer grants the installer the corresponding device permissions.
For more information, see ***Hand Over Personal Site by Transferring***.

5.2 Common Tenant-(or Shared-)Site Scenario

A typical tenant (or “shared”) site scenario is where the devices are owned by the installer, or the property management company, and the installer helps the property management company provide the device installation and maintenance service for the customers (tenants).The devices will be available to the customers only during the service periods. For more information, see ***Hand Over Personal Site by Sharing***.

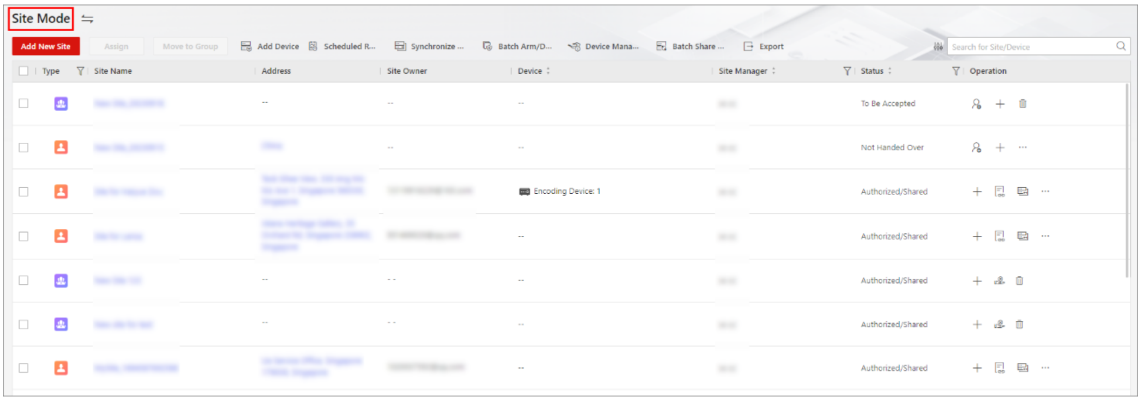
5.3 Site Page Overview

On the site page, you can switch between site mode and device mode. In site mode, you can view 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 operations for the sites, such as searching for sites, adding sites, handing over sites, and assigning sites. In the device mode, you can view all the devices in all the sites, and perform operations for the devices, such as batch refreshing devices which are in different sites and filtering devices.

Move your cursor to the **Site & Device** tab. Click **Customer Site** to enter the site page.

Select **Site Mode** or **Device Mode** as needed and perform more operations.

Site Mode



□	Type	Site Name	Address	Site Owner	Device	Site Manager	Status	Operation
□		[redacted]	--	--	--	[redacted]	To Be Accepted	
□		[redacted]	[redacted]	--	--	[redacted]	Not Handed Over	···
□		[redacted]	[redacted]	[redacted]	Encoding Device: 1	[redacted]	Authorized/Shared	···
□		[redacted]	[redacted]	[redacted]	--	[redacted]	Authorized/Shared	···
□		[redacted]	--	- -	--	[redacted]	Authorized/Shared	
□		[redacted]	--	- -	--	[redacted]	Authorized/Shared	
□		[redacted]	[redacted]	[redacted]	--	[redacted]	Authorized/Shared	···

Figure 5-6 Site Page

Note

- In the Site mode, you can click the search box or beside **Status** to search for or filter the sites in the site list.
- You can click to customize the columns to be displayed and change the order if needed.

There are different statuses for the sites.

Not Handed Over

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

Not Registered

The handover has been sent to a customer who has not registered 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

The site is handed over to a customer by transfer, but the installer is not (yet) authorized to manage the site.

Authorized and Monitoring

The site is handed over by transfer and the Installer gets the site authorization from the customer.

Shared

The site is handed over to customers by sharing.

Note

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

Table 5-1 Supported Operations for Sites in Each Status

Supported Operations	Not Handed Over	To Be Accepted Not Registered	Handed Over, Not Authorized	Authorized and Monitoring	Shared	Disbanded
Search Site	✓	✓	✓	✓	✓	✓
Assign Site	✓	✓	✓	✓	✓	×
Hand Over via Transfer	✓	×	×	×	×	×
Hand Over via Sharing	✓	×	×	×	×	×
Manage Device	✓	✓	×	✓	✓	×
Edit Site	✓	✓	×	✓	✓	×
Delete Site	✓	✓	✓	✓	✓	✓
Apply for Site Authorization	×	×	√	×	×	×
Apply for Device Permissions	×	×	✓	✓	✓	×
Site Collaboration	✓	×	×	✓	×	×
Batch-Share Devices	×	×	×	×	✓	×
Move to Group	✓	✓	✓	✓	✓	×

Device Mode

In this mode, there are two view modes. You can switch between card view and list view.

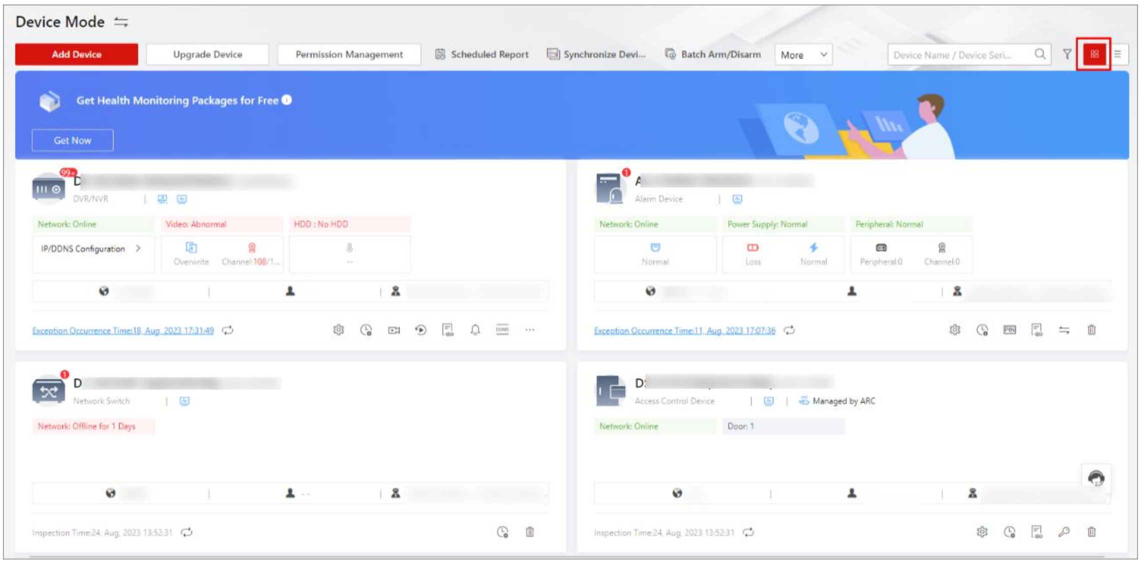
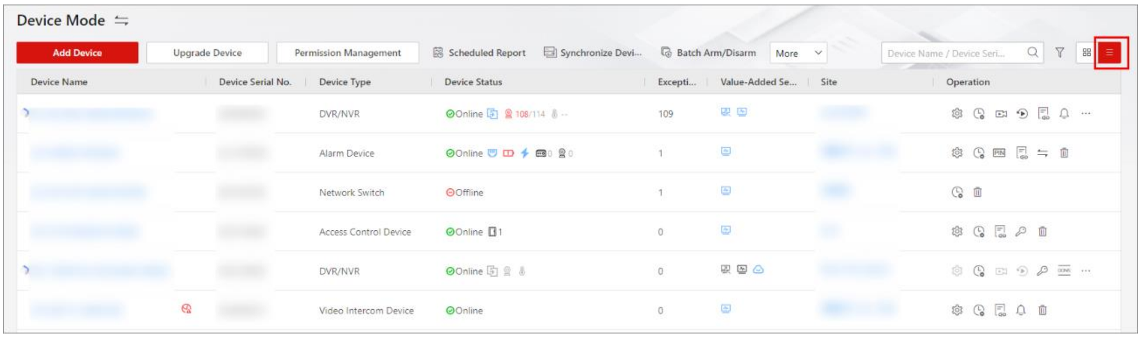


Figure 5-7 Card View



Device Name	Device Serial No.	Device Type	Device Status	Excepti...	Value-Added Se...	Site	Operation
[redacted]	[redacted]	DVR/NVR	Online 108/114	109		[redacted]	
[redacted]	[redacted]	Alarm Device	Online 0 0	1		[redacted]	
[redacted]	[redacted]	Network Switch	Offline	1		[redacted]	
[redacted]	[redacted]	Access Control Device	Online 1	0		[redacted]	
[redacted]	[redacted]	DVR/NVR	Online	0		[redacted]	
[redacted]	[redacted]	Video Intercom Device	Online	0		[redacted]	

Figure 5-8 List View

Table 5-2 Supported Operations for Devices

Description	Operation
View Device Details	View the device name, device serial number, site name, device status, health monitoring status, etc.
Add Device	Click **Add Device** to go to Add Device page, add device(s) via one of the methods. For details, refer to ***Add Device***.
Upgrade Device	Click **Upgrade Device** to upgrade device(s) if there is/are upgradable device(s).
Apply for Device Permission	Click **Permission Management**, select the needed permission, and then select the device(s) for which you want to apply for the corresponding permission. For details, refer to ***Apply for Device Permission***.
Send Scheduled Report	Click **Scheduled Report** or **More** → **Scheduled Report** to enter the Scheduled Report page, configure schedules to generate, and send device health check reports to the specified email addresses

Description	Operation
	automatically. For details, refer to ***Send Report Regularly***.
Synchronize Devices from LTS Connect	Click **Synchronize Devices from LTS Connect** or **More** → **Synchronize Devices from LTS Connect** to synchronize devices in your LTS Connect account with devices in the LTS Platinum Partner account. For details, refer to ***Synchronize Devices with LTS Connect Account***.
Batch Arm/Disarm Devices	Click **Batch Arm/Disarm** or **More** → **Batch Arm/Disarm** to batch arm/disarm devices.
Device Management Invitation from Customer	Click **Device Management Invitation from Customer** or **More** → **Device Management Invitation from Customer** to view the introduction of how your customer authorize you to manage devices in her/his LTS Connect account.
Refresh Device	Click **Refresh** or **More** → **Refresh** to refresh all the devices.
Search Device	Enter keywords (device name or serial number) in the search box to search for the needed devices.
Filter Device	Click ▽ to filter devices by setting the needed condition(s).
Switch Between Card/List View	Click ⊞ or ≡ to display device list in card or list view.
Other Operations	For a single device, you can configure the device remotely, start live view and playback of the device, reset device admin password, refresh the device, etc.

5.4 Create Site Group

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

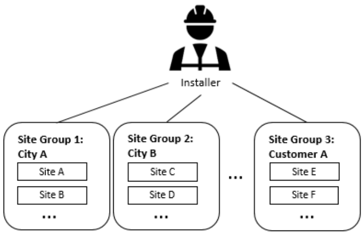


Figure 5-9 Site Grouping Scenario

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, you can create one: check one or more sites, click **Move to Group**, click **Create Group** on the pop-up prompt, enter the group name, select sites from the site list (optional), and click **Confirm**.
- If there are already created site groups, you can click + in the site group list which is to the left of the site list, enter the group name, select sites from the site list (optional), and click **Confirm**.
- You can also create site groups when you add sites. On the **Add New Site** page, check **Move to Group**, click **Create Group**, enter the group name, and click **Confirm**.

The following operations are supported after adding site groups.

Description	Operation
Add Site to Site Group	Select sites in the site list, click **Move to Group**, select a site group, and click **Confirm**.
Edit Site Group	Click a site group in the list; click ✎ to edit the site group name and/or add/delete the sites.
Delete Site Group	Click a site group in the list; click 🗑 to delete it.
Search for Site Group	Enter keywords in the search box to search for the site groups.

5.5 Add Personal Site

Personal sites are for individual users and apply to households and independent stores. When such a customer wants the installation company to provide installation and maintenance services, 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 New Site page.
   – Go to **Site & Device** → **Customer Site** → **Site Mode** → **Add New Site**

– Click **Add Site** on the Home page

2. Set the site name and the time zone where devices locate.

Note

The time zone *cannot be changed* after the site is added.

3. Optional: Check **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: Click **Unfold** to set more information including the scene, site address, city, and state.

Note

- The Installer can make unique installation plans depending on the specific scene
- To set the address, click on the map or enter keywords in the search box

5. Optional: Check **Move to Group** to move the site to a group.
6. Optional: Enter the customer information as Remarks, such as contact information and maintenance records. The customer can view the remarks via LTS Connect Mobile Client.
7. Select **Personal** as the site type.
8. Click **OK**. You will then enter the Add Device page.

What to do next

Refer to the following related topics.

- ***Add Device***
- ***Create Site Group***
- ***Hand Over Personal Site by Transferring***
- ***Hand Over Personal Site by Sharing***
- ***Site Collaboration Before Handover***
- ***Site Collaboration After Handover***

5.6 Add Team Site

Team sites are for enterprise users and apply to chain stores, offices, and communities. When such customers want the installation company to provide installation and maintenance services, the Installer / Installer Admin needs to create a team site for managing the devices of these customers.

Steps

1. Enter the Add New Site page.
   – Move your cursor to the **Site & Device** tab. Click **Customer Site** and switch to the **Site Mode**. And then click **Add New Site**.
   – Click **Add Site** on the Home page.
2. Set the site name and time zone.

Note

- You should select the correct time zone where the devices are located. The time zone *cannot be changed* after the site is added.
- The name of team site cannot be the same as a personal site.

3. Optional: Click **Unfold** to set more information including scene, site address, city, and state.

Note

- When setting the site address, you can click on the map to locate a place, or you can enter keywords in the search box to locate a place on the map.
- The Installer can select different configuration plans for the site and devices according to the selected scene.

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

You should select **Analysis Report** service together with **Video Management** service.

8. Click **OK** to finish adding the new team site.
   You will enter the Add Device page.
9. On the Add Device page, perform one of the following.
   - Add online devices or add devices by serial No. For details about adding devices, refer to ***Add Detected LAN Device*** or ***Add Device by Entering Serial No.***.
   - Click **Cancel** to cancel adding devices and enter the site details page.
10. Optional: On the site details page, perform the following operations.

Edit Site Information	Click ✎ in the upper-right corner to edit the site information such as site name and scene.
Add Device	Click **Add Device** to add online devices or add devices by serial No. For details, refer to ***Add Detected LAN Device*** or ***Add Device by Entering Serial No.***.
Activate Service	● If you have activated a service when adding the site, click **Activate**

and Expand to activate and expand the service.

- If you have not activated any services when adding the site, click **Activate** to activate a service. After activation, you can click the service to view its details and perform various operations for different types of services.
  - For video management, access control & attendance, and video intercom services, you can view the free channel(s) you have, and click **Activate and Expand** to activate and expand the service – or click **Get Free Trial** to upgrade to trial plan.
  - For people counting and heat mapping services, click **Renew** to renew the service – or click **Get Free Trial** to upgrade to trial plan.

Hand Over Site

Click **Hand Over by Transferring** in the lower-right corner to hand over the site.

Note

For details, refer to Section **5.8**.

5.7 Assign 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

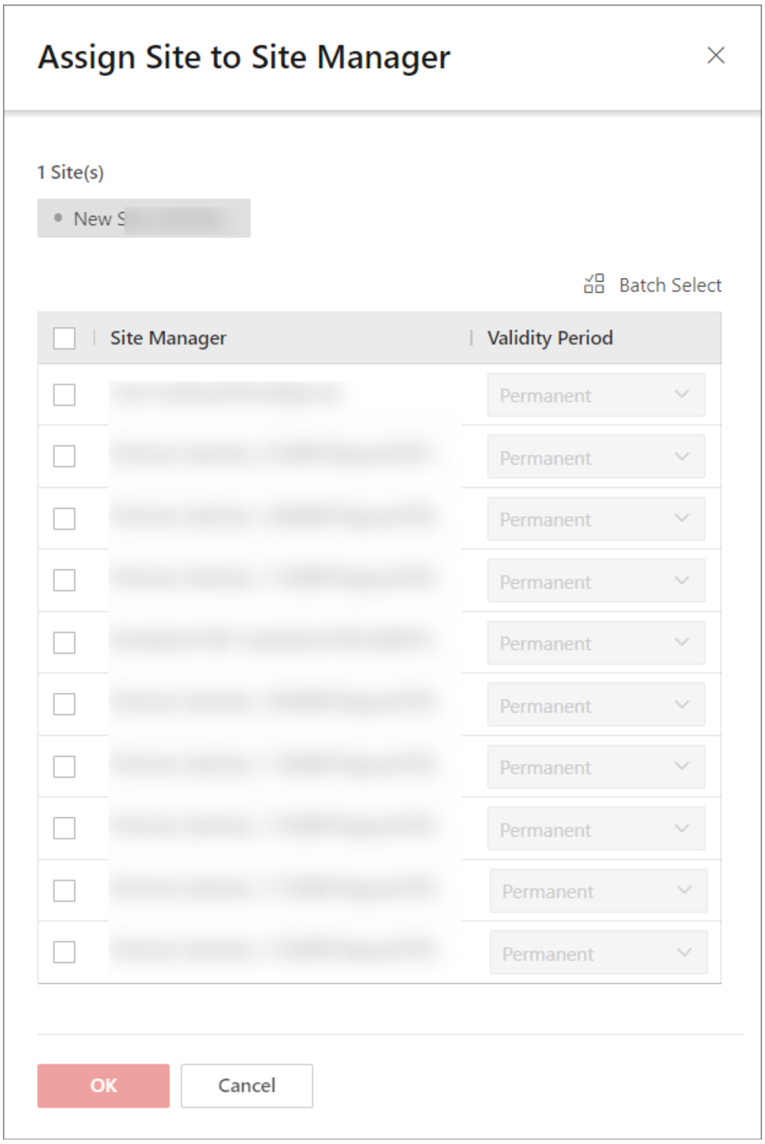
Make sure you have the Manage All Sites permission.

Steps

1. Move your cursor to the **Site & Device** tab. Select **Customer Site** to enter the Site page. And click ⇆ to switch to site mode.
2. Select one or multiple sites for assignment.
3. Click **Assign**.
4. On the Assign Site to Site Manager pane, check one or multiple Installers as the site manager(s) of the selected site(s).

Note

No more than 100 site managers can be assigned to each site.



Assign Site to Site Manager

1 Site(s)

New S[redacted]

Batch Select

☐	Site Manager	Validity Period
☐	[redacted]	Permanent
☐	[redacted]	Permanent
☐	[redacted]	Permanent
☐	[redacted]	Permanent
☐	[redacted]	Permanent
☐	[redacted]	Permanent
☐	[redacted]	Permanent
☐	[redacted]	Permanent
☐	[redacted]	Permanent
☐	[redacted]	Permanent

Figure 5-11 Assign Site to Site Manager

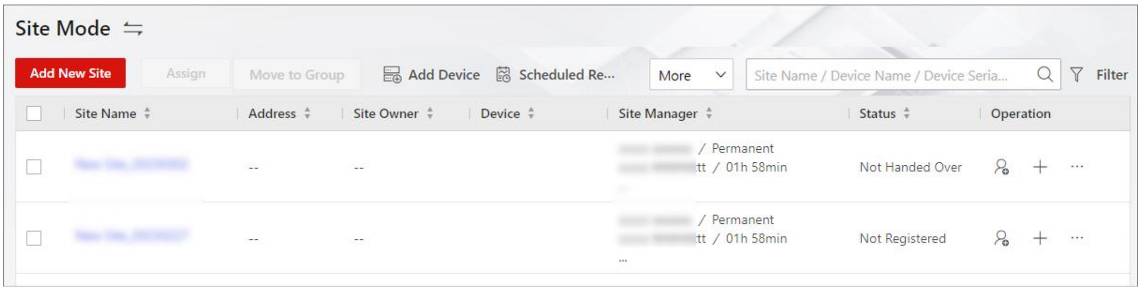
5. Optional: In the Validity Period column, select a validity period for each site manager.

Note

- You can also click **Batch Select** on the top right and then select a validity period for them in a batch.
- At least one site manager's validity period should be Permanent.
- By default, the validity period of site managers with the permission for managing all sites is Permanent and cannot be edited.

6. Click **OK**.

The Installers assigned with sites will receive a notification on the Mobile Client. In the Site Manager column, the names of site managers and validity period countdown of the permission will be displayed.



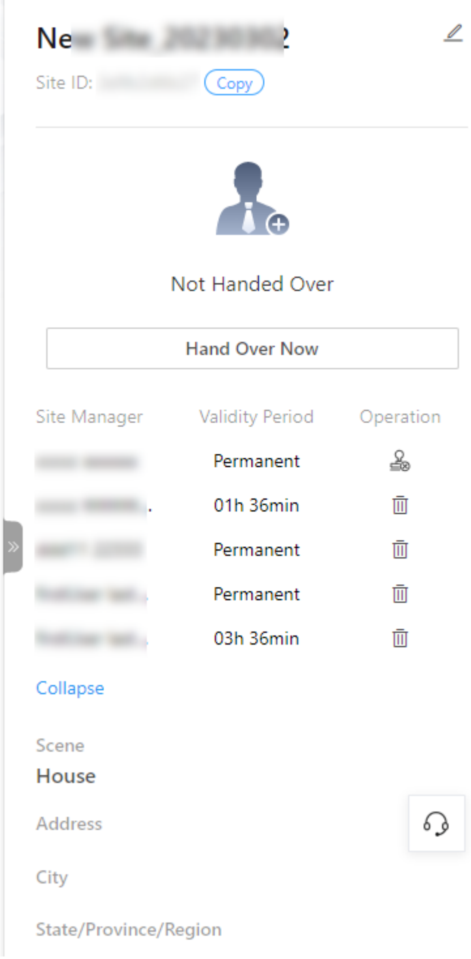
Site Mode ⇆

□	Site Name	Address	Site Owner	Device	Site Manager	Status	Operation
□	[redacted]	--	--		[redacted] / Permanent [redacted]tt / 01h 58min ...	Not Handed Over	+ ···
□	[redacted]	--	--		[redacted] / Permanent [redacted]tt / 01h 58min ...	Not Registered	+ ···

Figure 5-12 Current Site Page

7. Optional: Click a site name to show the site details. The basic information about the site will be displayed on the right, including site managers and their validity period. You can perform the following operations.

- Click 👤 to remove current account from the site manager list.
- Click 🗑 to remove other account from the site manager list.
- Click ✎ and select a new validity period for the site manager from the drop-down list.



Ne[redacted]

Site ID: [redacted] Copy

Not Handed Over

Site Manager	Validity Period	Operation
[redacted]	Permanent	👤
[redacted]	01h 36min	🗑
[redacted]	Permanent	🗑
[redacted]	Permanent	🗑
[redacted]	03h 36min	🗑

Collapse

Scene

House

Address

City

State/Province/Region

Figure 5-13 Site Details

Note

- An account without permission for managing all sites can only remove its own account from the site manager list, while an account with the permission for managing all sites can remove all accounts from the site manager list.
- When the site managers or validity periods are changed, the corresponding site managers will receive notifications on the Portal and Mobile Client.

5.8 Hand Over Personal Site by Transferring

After the installation company has 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

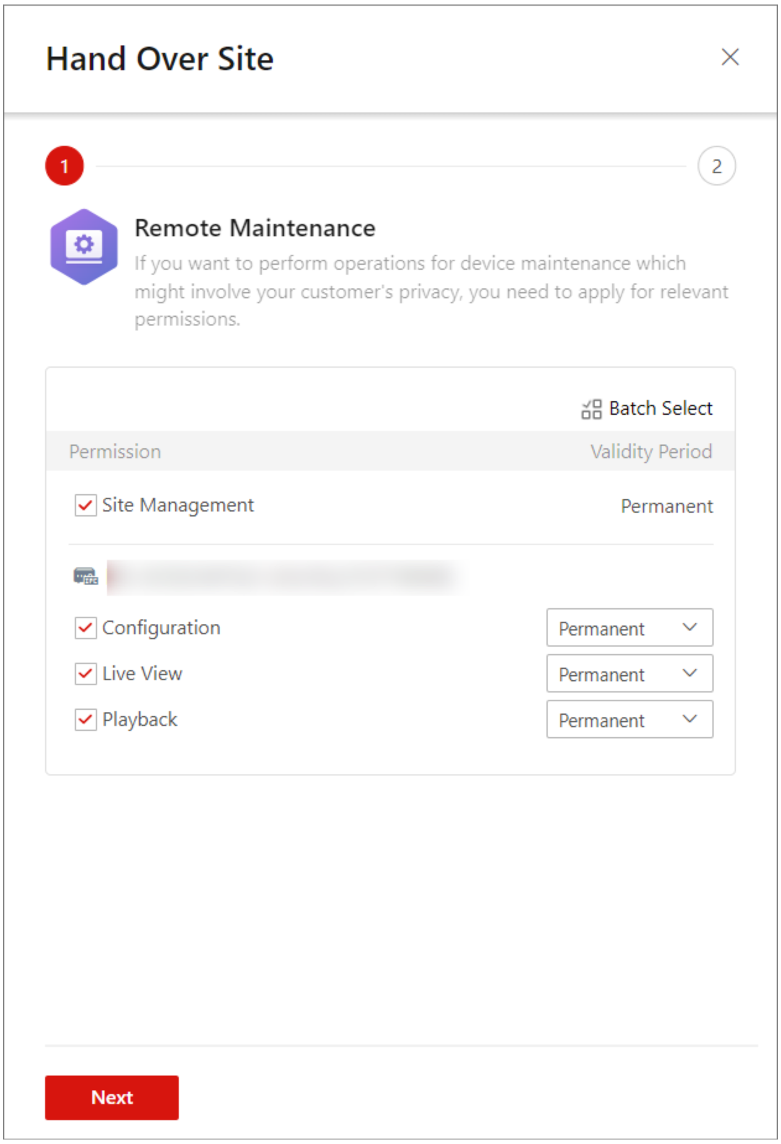
Make sure the site status is **Not Handed Over**, the devices are added to the site, and you have permission for site management, such as managing all sites and assigned sites.

Steps

Note

You can only hand over personal sites by transferring.

1. Move your cursor to the **Site & Device** tab.
2. Click **Customer Site**, and switch to the **Site Mode**.
3. Select a site to be handed over.
   - Select a site and click → **Transfer** in the Operation column.
   - Click the site name to enter the Site Details page and click **Hand Over by Transferring** in the lower-right corner.
4. Optional: Select the permissions for which you need to apply from your customer to maintain the devices.



Hand Over Site

Remote Maintenance

If you want to perform operations for device maintenance which might involve your customer's privacy, you need to apply for relevant permissions.

Permission	Validity Period
☑ Site Management	Permanent
☑ Configuration	Permanent
☑ Live View	Permanent
☑ Playback	Permanent

Figure 5-14 Hand Over Site by Transferring

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 you. You do not need to apply for authorization from your customer again.
- You can click **Batch Select** to batch select 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 selected devices on the site.

5. Click **Next**.

6. Select **Email** or **Phone Number** as the handover method.

7. Enter the site owner's email address or phone number.

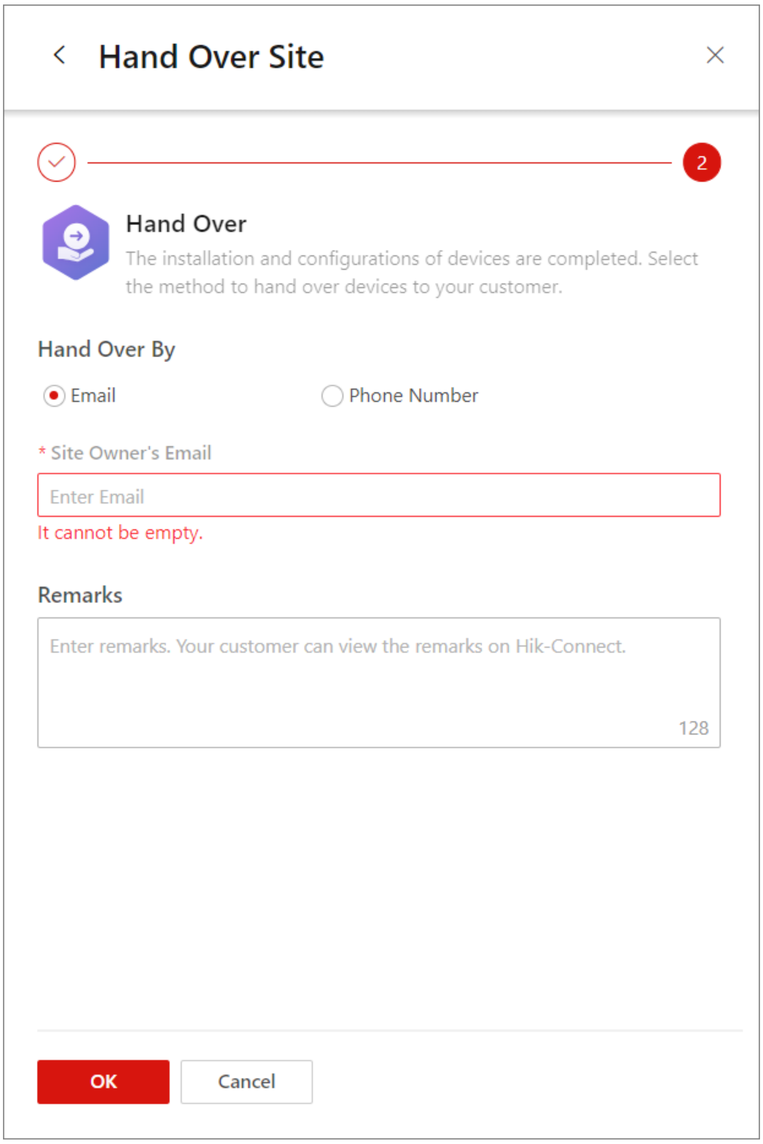
8. Optional: Enter the remarks, such as the reason for the handover, which your customer can view when they receive the handover via the LTS Connect Mobile Client.

9. Click **OK** to send the handover application.

   - 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 need to 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.

     - 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 need to authorize related permissions to you.


Hand Over Site

Hand Over

The installation and configurations of devices are completed. Select the method to hand over devices to your customer.

Hand Over By

● Email ○ Phone Number

* Site Owner's Email

Enter Email

It cannot be empty.

Remarks

Enter remarks. Your customer can view the remarks on Hik-Connect.

128

Figure 5-15 Hand Over Site by Transferring

Note

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

10. 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; a previous handover will be invalid if you send a new handover.

5.9 Hand Over Personal Site by 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 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.

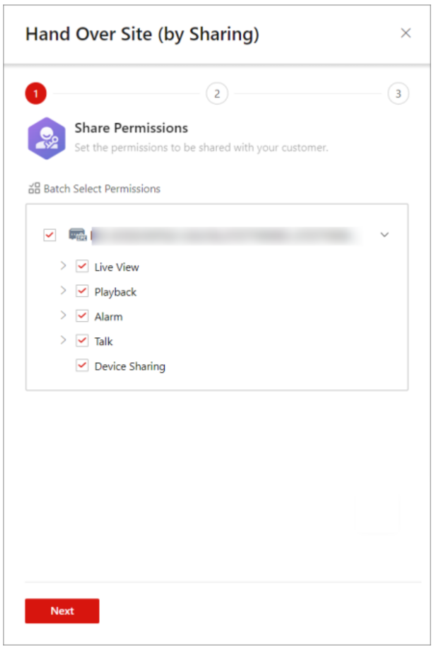
Steps

Note

You can only hand over personal sites by sharing.

1. Move your cursor to the **Site & Device** tab.
2. Click **Customer Site**, and switch to the **Site Mode**.
3. Select a site to be handed over.
   - Select a site and click → **Share** in the Operation column.
   - Click the site name to enter the Site Details page and click **Hand Over by Sharing** in the lower-right corner.

   You will enter the Hand Over Site (by Sharing) page.
4. Select the resources and permissions to be shared with your customer.



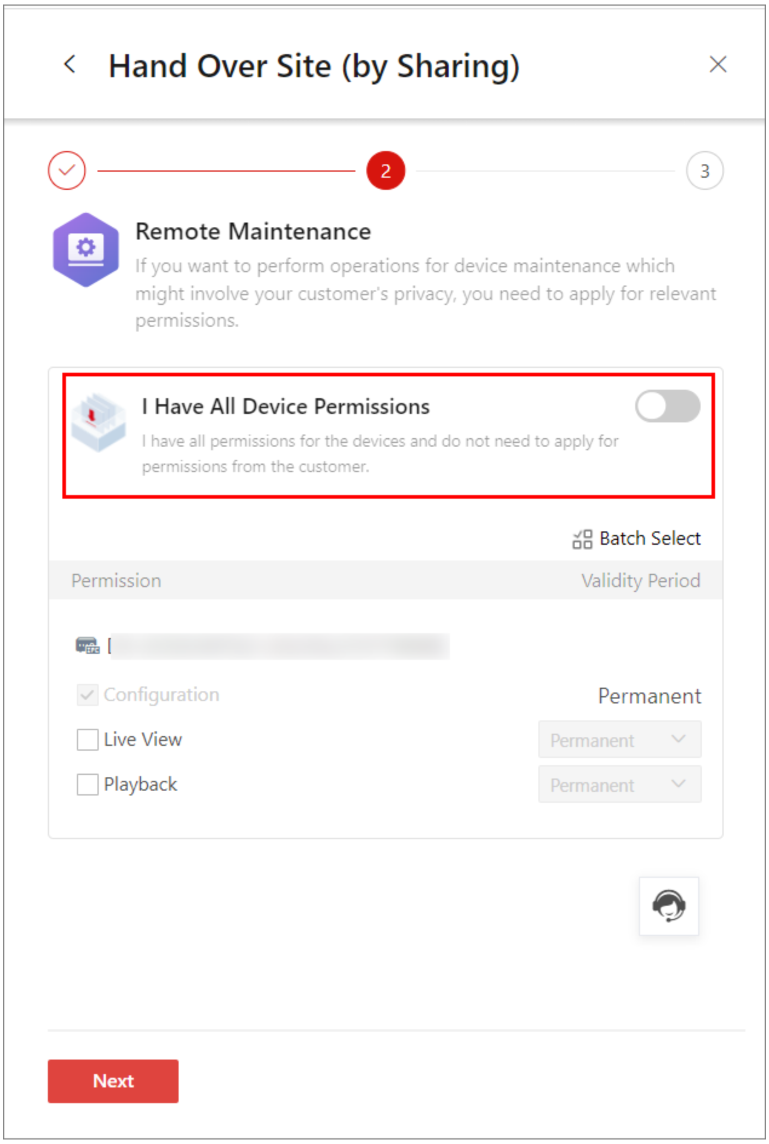
Set the permissions to be shared with your customer.

☑ [redacted]
- ☑ Live View
- ☑ Playback
- ☑ Alarm
- ☑ Talk
- ☑ Device Sharing

Figure 5-16 Share Resources and Permissions

5. Click **Next**.
6. 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 need to 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.



Remote Maintenance

If you want to perform operations for device maintenance which might involve your customer's privacy, you need to apply for relevant permissions.

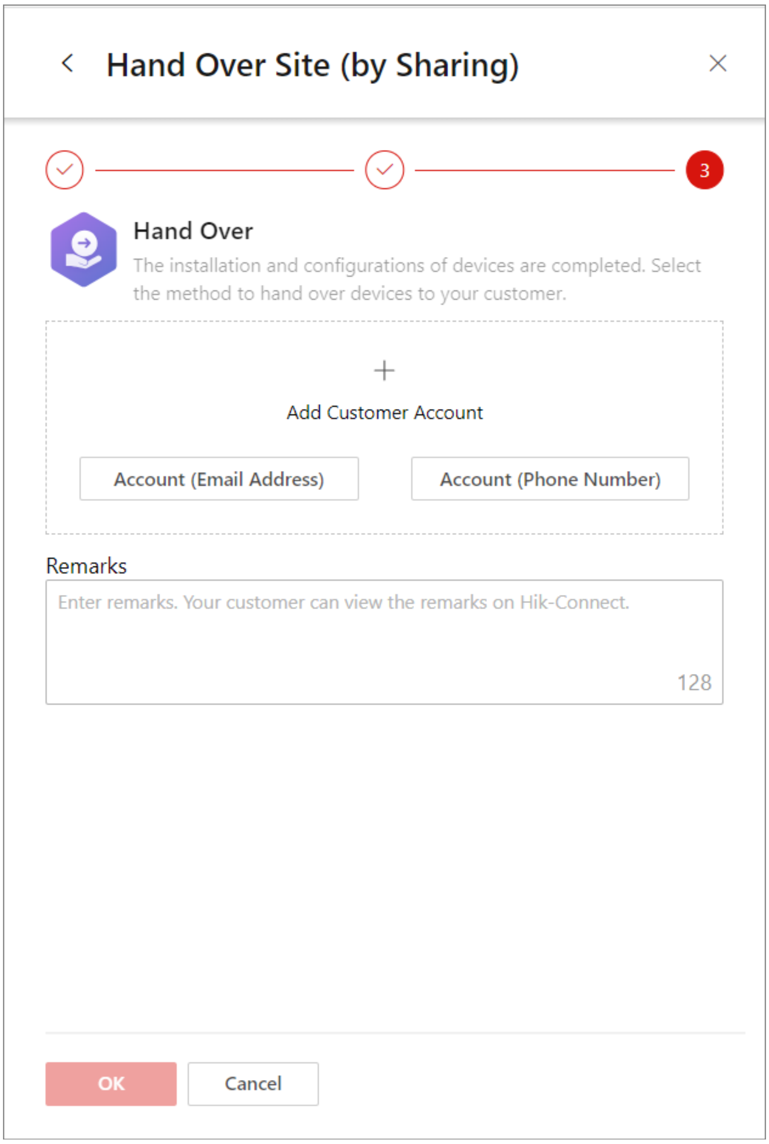
I Have All Device Permissions

I have all permissions for the devices and do not need to apply for permissions from the customer.

Permission	Validity Period
[redacted]	
☑ Configuration	Permanent
□ Live View	Permanent
□ Playback	Permanent

Figure 5-17 Enable "I Have All Device Permissions" or Not

7. Click **Next**.
8. Click **Account (Email Address)** or **Account (Phone Number)**, then enter the email address or phone number to add the customer account.



Hand Over Site (by Sharing)

Hand Over

The installation and configurations of devices are completed. Select the method to hand over devices to your customer.

Remarks

Enter remarks. Your customer can view the remarks on Hik-Connect.

Figure 5-18 Add Customer Account

Note

- For Mode A, there is a customer administrator who will review your application for permissions. If you add only one customer account in this step, then this customer will be the customer administrator. If you add more than one customer account, you will be asked to select one customer as the customer administrator.
- For both Mode A and B, you can add multiple customer accounts for handing over the devices. All the added customers will receive the handover application on their LTS Connect.
- One device can be shared with no more than 10 customers.
- To accept the handover (by sharing), your customer's LTS Connect must be V5.4.4 or later.

9. Optional: Enter the remarks.
10. Click **OK**.

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

Check Sharing Details	Click a shared site, and under the Customer tab, you can check sharing details including customer accounts and sharing status.
Share Again	Click a shared site, and under the Customer tab, for sharing that are rejected and expired, you can click **Share Again** to share the site again.
Cancel Sharing	Click a shared site, and under the Customer tab, for sharing that are accepted and to be accepted, you can click ··· → **Cancel Sharing** to cancel sharing.
View and Edit Shared Resources and Permissions	Click a shared site, and under the Customer tab, you can click the customer card to view and edit the resources and permissions that are shared with the customer.
Edit Customer Account	Click a shared site, and under the Customer tab, you can click ··· → **Edit Account** to edit the customer account. **Note** In Mode A, if the customer administrator accepts the sharing handover, you will not be able to edit their account, but you can click **Cancel Sharing** to send an application to the customer administrator to cancel sharing.
Add New Sharing	Click a shared site, and under the Customer tab, you can click **New Sharing** to add new customer accounts to share with them.
Add New Devices to Shared Sites	After a site is shared with customers, you can still add new devices to the site. By default, these newly added devices will not be shared with any customer, but you can click the customer cards to select these devices and their permissions to share them with the corresponding customers. The customers do not need to accept sharing again.
Batch Share Devices / Batch Cancel Sharing Devices	After sites are shared, you can batch-share or batch-cancel sharing the devices on these shared sites with multiple customers. In Site Mode, above the site list, click **More** → **Batch Share Devices**. On the Batch Share Devices page, select devices on the list of shared sites and devices, enable **Share With** and/or **Cancel Sharing With**, enter your customers' accounts (click ⊕ to add more accounts), and click **Confirm**.

5.10 Hand Over Team Sites

After the installation company has completed 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 the devices are usually 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. Move your cursor to the **Site & Device** tab.
2. Click **Customer Site**, and switch to the **Site Mode**.
3. Enter the Handover List page.
   - Select a site and click 👤 → **Transfer** in the Operation column.
   - Click the site name to enter the Site Details page and click **Hand Over by Transferring** in the lower-right corner.

   You can view activated services, devices added to the site (if any), etc., on the Handover List page.
4. Click **Hand Over** to enter the Hand Over System page.
5. Configure the related parameters including account type (required), customer name, phone, and remarks.

   Account Type

   Select **Email** or **Phone Number** and enter the site owner's email or phone number.
6. Click **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, they need to 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).

5.11 Apply for Site Authorization from Site Owner

After the site is handed over by transferring to a site owner (but no permission selected when handing over site), 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 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

Sites that are handed over by sharing do not support this function.

1. Move your cursor to the **Site & Device** tab.
2. Click **Customer Site**, and switch to the **Site Mode**.
3. Select a Site.
4. Enter Apply for Authorization page.
   - Select a Site and click on Operation column.
   - Click the Site name to enter Site Details page and click **Apply for Authorization**.
5. Enter the remarks and click **OK** to send the application.
   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 (V 4.15.0 or later). You can send the QR code to them.

6. Optional: Perform the following operations.

Apply for Device Permission	Click the Site name to enter Site Details page and apply for permissions.
Discard Authorization	On the Site list page, click ⋯ → to discard authorization or the Site.

5.12 Accept a Device Management Invitation from an LTS Connect User

You can accept a device management invitation from your customer (i.e., an LTS Connect user) to manage a device already 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 the device on LTS Platinum Partner. Compared with synchronizing the device in LTS Connect with the device in LTS Platinum Partner, which requires your customer to share their LTS Connect account name and password with you, this way is more privacy-friendly and easier to accept. To learn more about the device management invitation, read the sections below:

- ***Overall Process***
- ***Introduction About the Device Management Invitation on LTS Platinum Partner***
- ***The Email of Device Management Invitation***
- ***The Notification of Device Management Invitation***
- ***How Can Your Customer Invite You to Manage Their Device via LTS Connect***

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 **Notification Center** → **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.

Introduction to the Device Management Invitation on LTS Platinum Partner

You can go to the site list page, and then click **Device Management Invitation from Customer** to open the window shown below. This shows how your customer uses the LTS Connect Mobile Client to invite you to manage their device. It should be noted that you need to provide your LTS Platinum Partner account (email address) to your customer first to let them specify you as the Service Provider who manages their device.

The Device Management Invitation Email

The email shows the invitation details including device name, device serial no., 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 need to accept the invitation in three days, otherwise the invitation will be invalid.

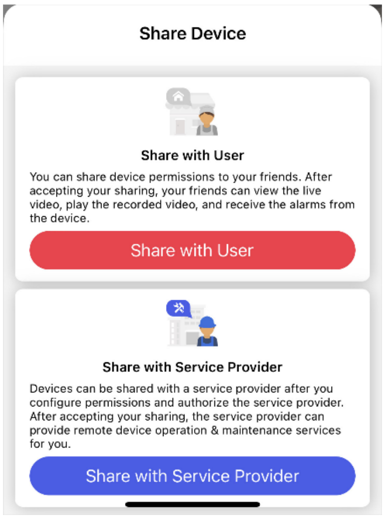
The Device Management Invitation Notification

The notification shows the invitation details including name of the site where the device(s) is/are added, device name, device serial no., and the LTS Connect user account. If you agree to manage the device(s) for your customer, you need to accept the invitation within three days, otherwise the invitation will be invalid.

How Your Customer Can Invite You to Manage Their Device via LTS Connect

Refer to the following steps for details about how your customer can invite you to manage their device via the LTS Connect Mobile Client.

1. In the device list, tap ⋖ of the device and the Share Device page will pop up. Or select **Me** → **Manage Sharing Settings** → **Share Device** to show the Share Device page.



Share Device

Share with User

You can share device permissions to your friends. After accepting your sharing, your friends can view the live video, play the recorded video, and receive the alarms from the device.

Share with Service Provider

Devices can be shared with a service provider after you configure permissions and authorize the service provider. After accepting your sharing, the service provider can provide remote device operation & maintenance services for you.

Figure 5-22 Share Device

Note

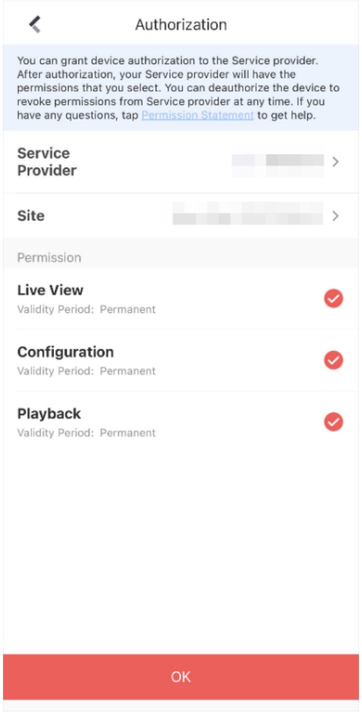
If this page does not appear, it means the device cannot be managed by a Service Provider and can only be shared with another LTS Connect user.
Possible reasons: the device is shared from another; the device is already managed by a Service Provider; the device is not enabled with the LTS Connect service.

2. Tap **Share with Service Provider**.
3. Tap **New Service Provider** and enter the Service Provider's account to share device permissions with a new Service Provider; or select an existing Service Provider.

Note

After entering the new Service Provider's account, if the account has been linked with two or more companies, you should select a company to share device permissions with.

4. Select the Site where the device will be added and the device permissions to be granted to the Service Provider.



Authorization

You can grant device authorization to the Service provider. After authorization, your Service provider will have the permissions that you select. You can deauthorize the device to revoke permissions from Service provider at any time. If you have any questions, tap Permission Statement to get help.

Service Provider [redacted] >

Site [redacted] >

Permission

Live View ✓
Validity Period: Permanent

Configuration ✓
Validity Period: Permanent

Playback ✓
Validity Period: Permanent

OK

Figure 5-23 Authorization

5.13 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.

Please see the following sections to learn the limitations of site collaboration:

Limitations

- You can only invite these accounts to collaborate with you on the site: your MSP's Installer Admin account, and your ISP's account with the Manage All Sites or Manage Assigned Sites permission.
- Your account and the account which you invite need to be in the same country/region.
- You cannot invite any Installer account of your company.

5.13.1 Site Collaboration Before Handover

Before the site handover, you can invite your installation service partner (ISP) to collaborate with you on the site for adding and handing over devices.

Before You Start

- Make sure site collaboration is supported both in your country/region and the ISP's country/region, and by both accounts.
- Make sure the site status is **Not Handed Over** and you have the permission to manage all sites or assigned sites.
- The ISP's account should have the Manage All Sites or Manage Assigned Sites permission and should not be an account of your company.
- Your account and the ISP's account need to be in the same country/region.

Steps

1. Move your cursor to the **Site & Device** tab.
2. Click **Customer Site**, and switch to the **Site Mode**.
3. Go to the Site Collaboration page.
   – On the site list, select ··· → 🌐
   – Click a site to go to the site details page, click **Site Collaboration** on the top left of the page
4. Enter the ISP's LTS Platinum Partner account.

   Note

   Make sure the account you enter has permission to Manage All Sites or Manage Assigned Sites, otherwise it will not be able to manage the site.

5. Select the validity period for the permission granted to the ISP.

   Note

   - When the configured validity period ends, site collaboration will be automatically canceled.
   - Before the validity period ends, the ISP has all permissions for devices on the collaborated site if the site collaboration is not canceled and the site is not handed over.

6. Optional: Enter the remarks.
7. Click **OK**.

Note

- The site collaboration will be canceled automatically, and all device permissions will be removed from the ISP's account, if the set permission validity period ends, the site is handed over to the customer, or the site is deleted.
- You will receive notifications in the Notification Center when the ISP accepts / rejects / cancels the collaboration.

8. Optional: Perform the operation(s) below if needed.

View Site Collaboration	You can enter the Site Collaboration page to view the site status, the ISP's account, and the validity period.
Cancel Site Collaboration	After the ISP accepts/rejects the site collaboration, you can cancel site collaboration.
Invite Again	After the ISP rejects the site collaboration or if the site collaboration is to be accepted, you can go to the site collaboration page, and edit the ISP's account and/or the validity period to invite the ISP again.

5.13.2 Site Collaboration After Handover

After a site is handed over by transferring, you can invite your maintenance service partner to collaborate with you for managing and maintaining the site together.

Before You Start

Make sure the site is handed over by transferring 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.
- Only the site that is handed over by transferring supports site collaboration.

1. Move your cursor to the **Site & Device** tab.
2. Click **Customer Site**, and switch to the **Site Mode**.
3. Select a site for site collaboration.
4. Enter the Site Collaboration page.
   – Move the cursor to ··· in the Operation column and click 🌐
   – Click the site name to enter the site details page and click **Site Collaboration**.
5. Enter the maintenance service partner's LTS Platinum Partner account.

Note

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

6. 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.
- If the following permissions are selected, when your customer accepts the permission application 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.

7. Enter the remarks, such as the reason for site collaboration.
8. Click **OK**.
9. Optional: After your customer accepts the application 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	You can change permissions for the maintenance service partner on the Site Collaboration page.

	Note 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 the LTS Connect Mobile Client if the permissions are changed.

5.13.3 Accept 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 authorization 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. In the upper-right corner of the page, click 🔔 to enter the Notification Center.
2. Click the **Business Notification** tab.
3. Click **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.

5.13.4 Features Available to MSPs & ISPs 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 Sites

For MSPs

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 ISPs

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

Exceptions Center

Receiving device exceptions and exporting exception records.

Send Reports 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.

To learn 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 completed the device configuration task earlier than the planned time, the MSP can release permission.

To learn how the MSP releases device permissions, refer to ***Release Permission for Devices***.

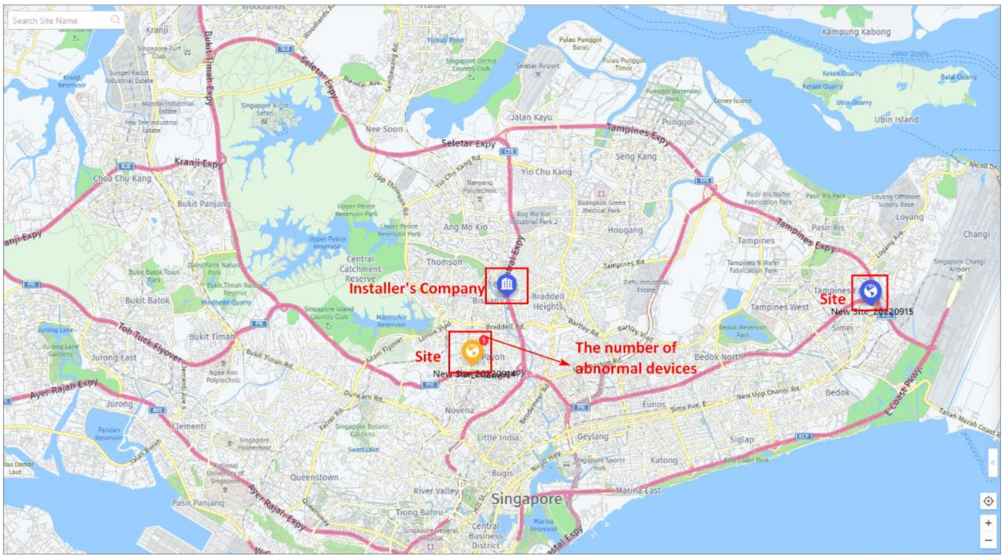
MSP/ISP Can Cancel Site Collaboration

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

5.14 View Sites on the Map

If you have configured GPS information for the sites, you can view them on the map.

Move your cursor to the **Site & Device** tab. Select **Site Map** to enter the Site Map page.



Installer's Company

Site

The number of abnormal devices

Site

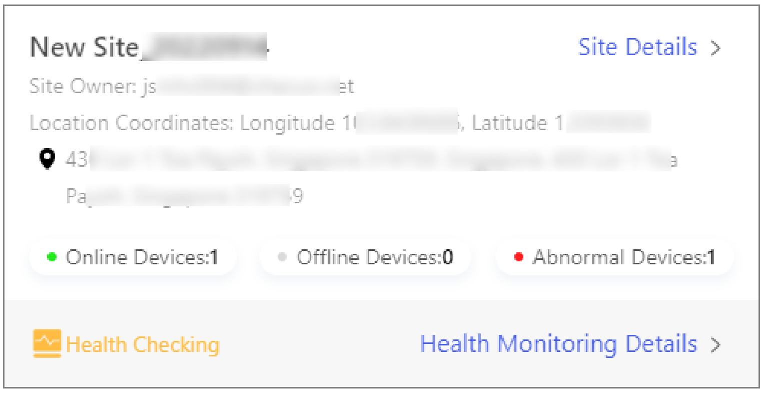
Figure 5-28 Site Map

Note

- Installer's company is at the center of the map by default.
- 📍: There are device(s) that have activated the health monitoring service in this site.
- 📍: No device has activated the health monitoring service in this site.

You can perform the following on this page.

- You can view companies and sites whose GPS information has been configured on the map. For details about configuring GPS information for companies and sites, refer to ***Add Personal Site*** and ***Manage Company Information***.
- You can click a site to view its information, including site name, site owner, site location, the number of online/offline/abnormal devices, etc. Also, you can click **Site Details** to enter the site details page to view more information about the site. You can click **Health Monitoring Details** to enter the health status page and view the health status of all the devices added to this site.



New Site_[redacted]

Site Owner: js[redacted]et

Location Coordinates: Longitude 1[redacted], Latitude 1[redacted]

43[redacted]a

Pa[redacted]9

● Online Devices:1

● Offline Devices:0

● Abnormal Devices:1

Figure 5-29 Site Information

- You can drag the map as needed. You can scroll the mouse or click + / − in the lower-right corner to zoom in/out the map. Also, you can click ⊙ to view the company's location on the map.
- You can enter keyword(s) in the search box in the upper-left corner to search for the site name.

Chapter 6. Device Management

LTS Platinum Partner supports multiple device types, including encoding device (e.g., solar cameras), security control panels, video intercom devices, access control devices, and doorbells. After adding them to the system, you can manage them and configure settings, including remotely configuring device parameters, configuring exception rules, linkage rules, etc.

6.1 Batch Configure Devices on LAN

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

Note

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

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

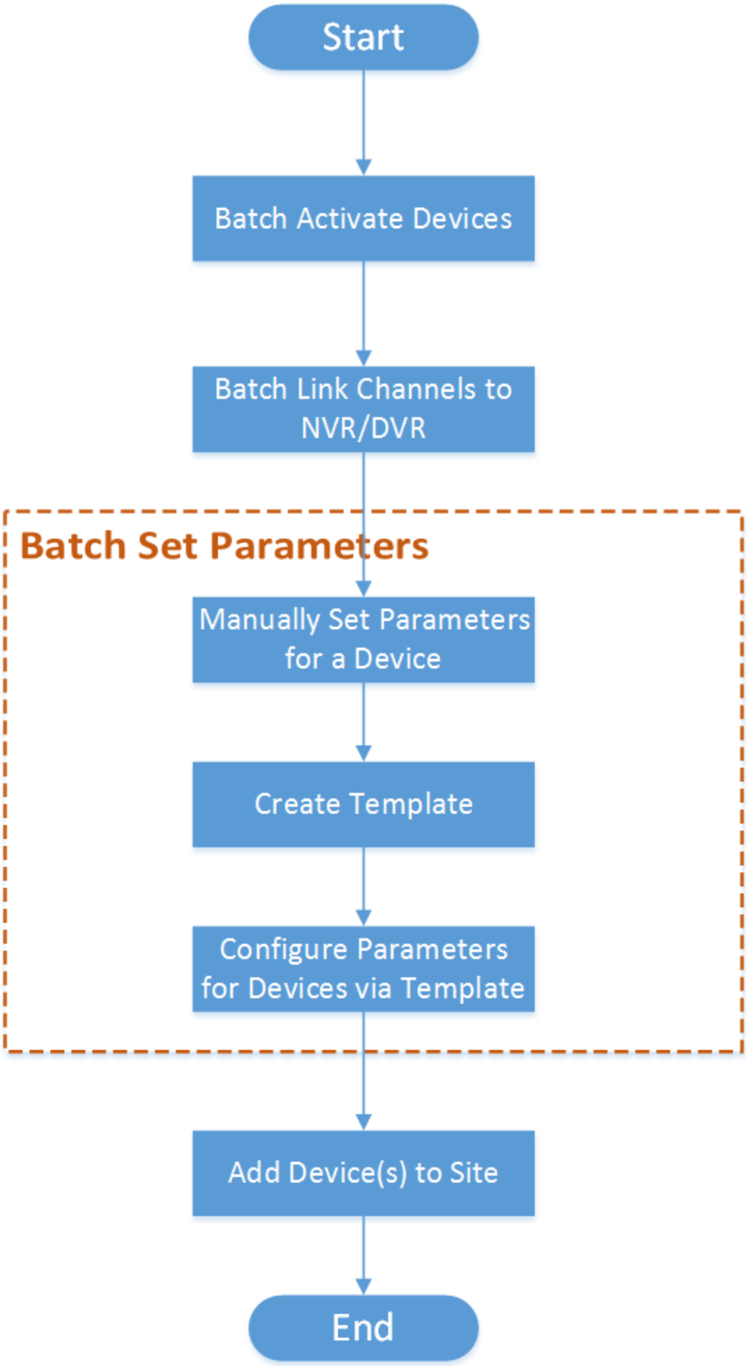

Start
Batch Activate Devices
Batch Link Channels to NVR/DVR
Batch Set Parameters
Manually Set Parameters for a Device
Create Template
Configure Parameters for Devices via Template
Add Device(s) to Site
End

Figure 6-1 Flow Chart

Table 6-1 Flow Chart Description

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

6.1.1 Batch Activate Devices and Assign IP Addresses for Them

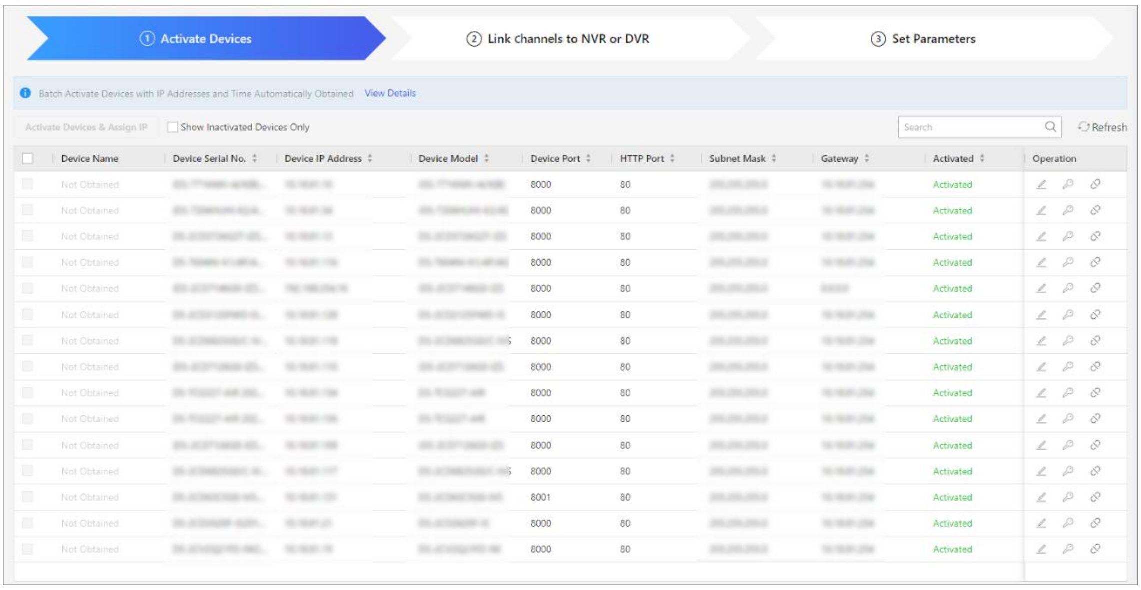
The Portal can detect available devices connected to the same network with the Portal, then you can activate devices and assign an IP address for them.

Before You Start

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

Steps

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


① Activate Devices

② Link channels to NVR or DVR

③ Set Parameters

Batch Activate Devices with IP Addresses and Time Automatically Obtained View Details

Activate Devices & Assign IP ☐ Show Inactivated Devices Only Search Refresh

☐	Device Name	Device Serial No.	Device IP Address	Device Model	Device Port	HTTP Port	Subnet Mask	Gateway	Activated	Operation
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8001	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗
☐	Not Obtained	[redacted]	[redacted]	[redacted]	8000	80	[redacted]	[redacted]	Activated	✎ 🔑 🔗

Figure 6-2 Batch Device Configuration

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

Note

- The non-activated devices and activated devices with no assigned IP address will be displayed as **Not Obtained** in the **Device Name** column.
- For activated devices and those assigned with an IP address, hovering the mouse over the IP address will display a note that the IP address has been automatically assigned.

The devices are activated, and the device IP address are assigned by the Portal.
The time of the computer will be synchronized to the activated devices.

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

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

What to do next

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

6.1.2 Batch Link Channels to NVR and DVR

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

Before You Start

Make sure you have activated the NVRs, DVRs, and/or network cameras. See ***Batch Activate Devices and Assign IP Addresses for Them*** for details.

Steps

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

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

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

2. Click **Next**.
   Channels that have been linked will be displayed in the middle.

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

3. Click **Link Channel** to open the Link Channel panel.

4. Optional: Select a device and click ⇅ to log in to the device and get device information.

5. Click **+** to link the device.

6. Optional: Perform the following operations.

Edit NVR / DVR / Channel Name	Click ✎ to edit the NVR / DVR / channel name.
Sort Channels	Click ↑ or ↓ to sort the channels.

Replace Device	Click **Replace Device** to unlink this channel and link a new device.
Unlink Device	Click 🗑 to unlink channel.

What to do next

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

6.1.3 Create Template for Setting Parameters

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

Before You Start

Make sure you have activated devices and linked channels to any NVR or DVR. See ***Batch Activate Devices and Assign IP Addresses for Them*** and ***Batch Link Channels to NVR and DVR*** for details.

Steps

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

7. Optional: Click 🗑 to delete a template.

6.1.4 Batch Set Parameters for Devices via Template

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

Before You Start

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

Steps

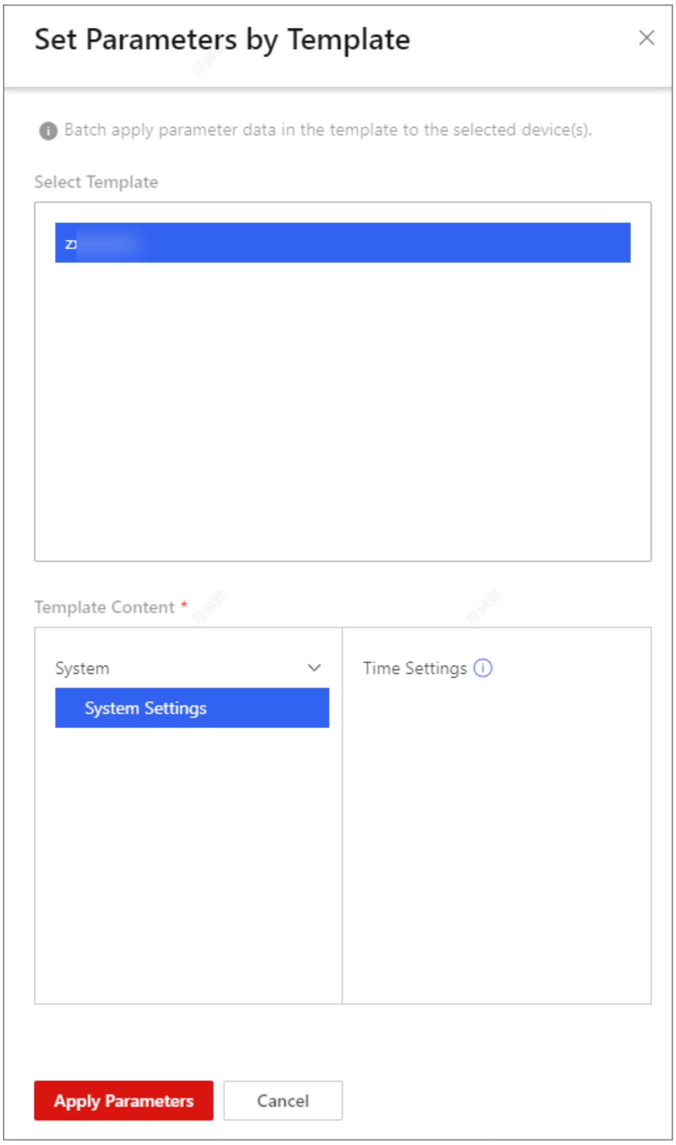
1. Check device(s) and click **Set Parameters by Template**.

Note

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

---

2. Select a template.
3. Click **Apply Parameters** to apply the configured parameters to devices.



Set Parameters by Template

Batch apply parameter data in the template to the selected device(s).

Select Template: z[redacted]

Template Content *

Figure 6-6 Set Parameters by Template

The application process and application results will be displayed.

4. Optional: Perform the following operations.

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

6.2 Add Device

LTS Platinum Partner accesses devices by two modes: LTS Connect (P2P) and Device IP Address / Domain Name. The former provides securer data communication (between LTS Platinum Partner 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 communication but no access to the features based on 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)	● ***Add Detected LAN Device*** ● ***Add Device by Entering Serial No.*** ● ***Synchronize Devices with LTS Connect Account*** ● ***Add Devices Without Support for the LTS Connect Service***
Device IP Address/Domain Name	● ***Add Devices by IP Address or Domain Name*** ● ***Batch Add Devices***

Following Operations

After adding devices to the Portal, you can perform the following operations if required.

Operation	Description
Configure Linkage Rule	Click to configure linkage rule for the device. **Note** For details, see ***Add Custom Linkage Rule***.
Activate Health Monitoring Service	Click **Activate Service** on the adding result page. Or hover the cursor onto on the device card on the site details page, and then click **Activate Service**. **Note** For details about how to activate the health monitoring service, see ***Activate the Health Monitoring Service for Devices***. For details about Health Monitoring service, see ***Health Monitoring Service***.
Delete Device	Click ⋯ → 🗑 to delete the device. **Note** Deleting device (except devices added by IP/domain) is not supported if the site is authorized.
Upgrade Device Firmware	When device adding completes, the platform will start 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. For devices incompatible with the LTS Platinum Partner, you need to upgrade them. 1. Select **Upgrade to Compatible Version** on the **Upgrade or Not** column, then click **Add and Upgrade**. 2. Enter device username and password to add and upgrade the device.
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. Click **Set Device Type** and select a device type from the drop-down list. You can edit it again after the selection.
Unbind Device from Its Current Account	If the adding result page shows that a device fails to be added and has been added to another account, you can click to unbind it. When the device is unbound, you can add it to your account. For details about unbinding device, see ***Unbind a Device from Its Current Account***.

6.2.1 Add Device(s) after Batch Configuring Them

After batch configuring devices, you can add the device(s) to the existing site or a new site.
Select one of the following ways to enter the Add Device page.

- After batch configuring device(s), click **Add Device** in the prompt box.

  Note

  For details about batch configuring devices, refer to ***Batch Configure Devices on LAN***.

- On the Home page, click **Add Device**.
- On the navigation pane, click **Site & Device** → **Customer Site**
  - In Device Mode of the Customer Site page, click **Add Device** on the top.
  - In Site Mode of the Customer Site page, 1.) click **Add Device** on the top of the site list; 2) click + in the Operation column of the site list; 3) click the site name to enter the site details page, and then go to **Device** → **Add Device**.

Select **Scan for Devices on LAN**, **Enter Serial no., Enter IP Address / Domain**, **Batch Import**, or **Synchronize devices from LTS Connect** as the adding method.
Select the device(s) to be added, then perform one of the following two ways to add the device(s) to the site.

- Select **Existing Site** and then click the site in the drop-down list.
- Select **New Site** and edit the following parameters to create a new site.

  Site Name

  The name of the site, which can describe the site location, function, etc.

  Time Zone

  Select the time zone in the drop-down list according to the location the site belongs to.

  Scene

  Select the scene of the site in the drop-down list according to the usage scene, such as house, department, villa, and store.

  Site Address

  Enter the site address, such as street and number, apartment suite, unit, building, floor, etc.

  City

  Enter the city of the site.

  State

  Enter the state of the site.

  Sync Time & Time Zone to Device

  After checking, the time and time zone will be synchronized to the device from the site.

Click **Next** and perform the operations according to the prompts on the page. For more details, refer to ***Add Device***.

6.2.2 Add Detected LAN Device

The Portal can detect available devices connected to the same network with the Portal, which makes the devices' information (e.g., IP address) about themselves recognized by the Portal. Based on the information, you can add the devices quickly.

Note

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.
- You can add up to 15 detected LAN devices simultaneously.

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

- On the Home page, click **Add Device**.
- On the navigation pane, click **Site & Device** → **Customer Site**
  - In Device Mode of the Customer Site page, click **Add Device** on the top.
  - In Site Mode of the Customer Site page, 1.) click **Add Device** on the top of the site list; 2) click + in the Operation column of the site list; 3) click the site name to enter the site details page, and then go to **Device** → **Add Device**.

On the Add Device page, click **Scan for Devices on LAN**. The device(s) connected to the same LAN with the Portal will be displayed on the device list. You can view information including device serial no., device IP address, activation status (activated or not), LTS Connect status (connected to LTS Connect service or not), etc.

Check the LAN device(s) to be added and click **Next**. Perform part or all the following 4 steps based on the status of the selected devices before you can add them.

Table 6-2 Step Description

Step	Description
1. Activate Device	If there are device(s) not activated, activate them. See ***Activate Device*** for details. **Note** If a device is activated, the platform will automatically assign a fixed IP address for it.
2. Enter Device Password	Enter admin password of the device. See ***Enter Device Password*** for details.
3. Automatically Connect to LTS Connect Service	Connect device(s) to the LTS Connect service. See ***Connect to LTS Connect Service*** for details.

Step	Description
4. Set Device Verification Code	If a device is connected to the LTS Connect service successfully, the platform will automatically get device verification code from device. If not, you need to set verification code for it. See ***Set Device Verification Code*** for details.

Activate Device

If there are inactivated device(s) in the selected devices, create a device admin password for all the inactivated device(s) on the pop-up window to activate them.

Enter Device Password

For devices which are activated but not connected to the LTS Connect service, you should enter its admin password on the pop-up window. The admin password is created when you activate the device.

If multiple devices share the same password, enable **Batch Enter Admin Password** to enter the password for all the devices in a batch. If any device passwords are incorrect, a notification will appear showing these device(s) for you to enter the correct password(s).

Note

Before entering admin password, you should make sure that no repeated device IP address exists, or one of the devices with the same IP address will fail to be added. You can click ✎ in the Operation column, and then edit the device IP address.

Connect to LTS Connect Service

After entering device admin passwords, the platform will automatically start connecting the device(s) to the LTS Connect service. Devices that fail to be connected to the LTS Connect service cannot be added.

Note

Make sure that no repeated device IP address exists and that the IP addresses of the to-be-connected devices are in the same network segment with the PC running LTS Platinum Partner, or connection exception will occur. You can click ✎ in the Operation column, and then edit the device IP address.

Set Device Verification Code

- If a device is connected to the LTS Connect service successfully, the platform will automatically get device verification code from the device. If the platform failed to get the verification codes from any devices, you need to manually enter their verification codes.
  If multiple devices share the same verification code, enable **Batch Enter Verification Code** and

enter the verification code for all of them.

- If the device(s) fail(s) to be connected to the LTS Connect service, set a shared device verification code for multiple devices, or set verification codes for each device. After completing device verification settings, the device(s) will be connected the LTS Connect service.

6.2.3 Add Device 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.
- Make sure the device has been activated and connected to LTS Connect service.

Steps

1. Enter the Add Device page.
   - On the Home page, click **Add Device**.
     - On the navigation pane, click **Site & Device** → **Customer Site**
     - In Device Mode of the Customer Site page, click **Add Device** on the top.
     - In Site Mode of the Customer Site page, 1.) click **Add Device** on the top of the site list; 2.) click ＋ in the Operation column of the site list; 3.) click the site name to enter the site details page, and then go to **Device** → **Add Device**.
2. Select **Enter Serial No.** as the adding mode.
3. Enter the device serial number and device verification code.

Note

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

4. Click **Next**.

Note

LTS Platinum Partner will start detecting whether the device firmware version is compatible with the LTS Platinum Partner. Some functions (including health monitoring, linkage, and remote configuration) cannot be used if the device is not compatible with the LTS Platinum Partner. Firmware version detection will not happen if a site is authorized. For devices incompatible with the LTS Platinum Partner, you need to upgrade them.

   1.) Select **Upgrade to Compatible Version** on the **Upgrade or Not** column, then click **Add and Upgrade**.

   2) Enter device username and password to add and upgrade the device.

5. Check the device(s) to be added.

6. Click **Add**.

6.2.4 Add 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, LTS Platinum Partner will generate a QR code containing the device information. After completing device setup, you can share the QR code with 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 mode 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 following two methods: ***Add Detected LAN Device*** or ***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 Add Device page.
   - On the Home page, click **Add Device**.
     - On the navigation pane, click **Site & Device** → **Customer Site**
     - In Device Mode of the Customer Site page, click **Add Device** on the top.
     - In Site Mode of the Customer Site page, 1.) click **Add Device** on the top of the site list; 2.) click + in the Operation column of the site list; 3.) click the site name to enter the site details page, and then go to **Device** → **Add Device**.
2. Select **Enter IP Address / Domain** as the adding mode.
3. Enter the device's name, IP address/domain name, port number, username, and password.

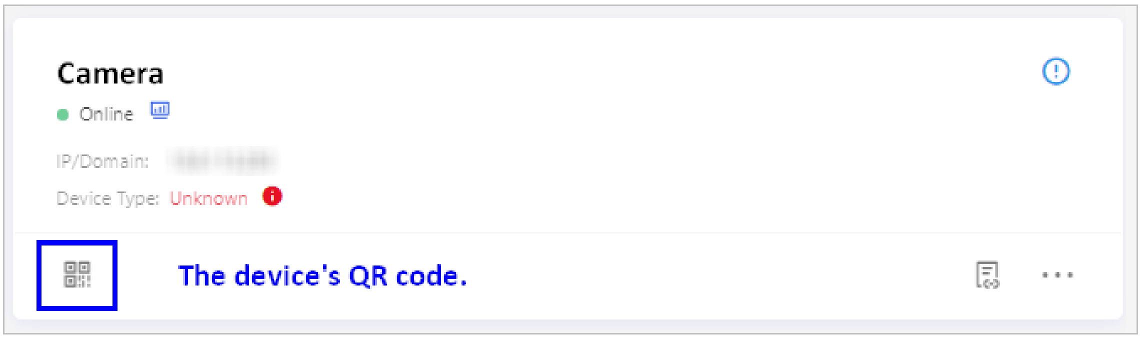
Caution

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.

4. Click **Add**.

   A QR code containing the device information will be generated and displayed in the device card on the site details page.



Camera

● Online

IP/Domain: [redacted]

Device Type: Unknown

Figure 6-7 The QR Code of the Added Device

6.2.5 Batch Add Devices

You can batch-add multiple devices to the LTS Platinum Partner by entering the device parameters in a predefined template.

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

- The devices added in this mode cannot be handed over to your customer. If you need to hand over a device to your customer after completing the device setup work, please add it by LTS Connect (P2P). For details, see ***Add Detected LAN Device*** or ***Add Device by Entering Serial No.***
- Only encoding devices mapped in WAN support this function.

1. Enter the Add Device page.
   - On the Home page, click **Add Device**.
     - ● On the navigation pane, click **Site & Device** → **Customer Site**
     - ● In Device Mode of the Customer Site page, click **Add Device** on the top.
     - ● In Site Mode of the Customer Site page, 1.) click **Add Device** on the top of the site list; 2.) click + in the Operation column of the site list; 3.) click the site name to enter the site details page, and then go to **Device** → **Add Device**.
2. Select **Batch Import** as the adding mode.
3. Click **Download Template** to save the predefined template (CSV file) on your PC.
4. Open the downloaded template file and enter the required information of the devices to be added in the corresponding column.
5. Click **Upload Template** to upload the edited template to LTS Platinum Partner.
6. Optional: Perform the following operations after adding the devices.

Encrypt Device QR Code	A QR code will be generated and displayed in the device information area. 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 LTS Connect. 1. Click ▦ to display the QR code. 2. Enter a password to encrypt the QR code, and then click **Save**.
Activate Health Monitoring Service	Hover the cursor onto ▣ on the device card on the site details page, and then click **Activate Service**. **Note** ● For details about how to activate the health monitoring service, see ***Activate the Health Monitoring Service for Devices***. For details about Health Monitoring service, see ***Health Monitoring Service***.
View and Edit Device Information	Click the device's IP address or domain name to view the device basic information. If the device's information changed, or a network exception occurs, you can edit its information accordingly. Select a device, then click ••• → ✎ to edit the device's name, IP address/domain name, port number, username, and password.
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. Click **Set Device Type** and select a device type from the drop-down list. You can edit it again after the selection.

Delete Device	Click ••• → 🗑. **Note** Deleting device (except devices added by IP/domain) is not supported if the site is authorized .

Note

- We highly recommend encrypting the device QR code for security reasons.
- 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 to them.

6.2.6 Synchronize Devices with LTS Connect Account

You can synchronize devices in your LTS Connect account with devices in the LTS Platinum Partner account. After synchronization, the devices are still managed in your LTS Connect account and you can continue to use LTS Connect service.

In the following two cases, you will need to synchronize devices in the LTS Connect account with devices in the LTS Platinum Partner account.

- **Case 1**: Before using LTS Platinum Partner, you managed the devices for the customer by the LTS Connect Mobile Client after the customer shares her/his devices to your LTS Connect account.
- **Case 2**: Before using LTS Platinum Partner, you already had an LTS Connect account and added device(s) to it.

Under the above two circumstances, you can synchronize these devices (including the ones the customers shared to you, or the ones added in your LTS Connect account) with the LTS Platinum Partner account for quick and convenient devices adding and better device management and maintenance.

There are three entries.

- On the Customer Site page, click **Synchronize Devices from LTS Connect** on the top.
- On the Add Device page, click **Synchronize Devices from LTS Connect**.
- Click the username in the upper-right corner, click **Link with LTS Connect Account** in the drop-down menu, and click **Link with Account**.

Log In to LTS Connect

First, you need to log into **LTS Connect** by entering your account or by scanning QR code.

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

Check **Authorize Automatic Device Synchronization from Your Account to the Current LTS Platinum Partner Account** to authorize automatic device synchronization. After authorization, devices newly added to LTS Connect will be automatically synchronized to LTS Platinum Partner.

Select Device for Synchronization

Secondly, you need to select the devices for synchronization.

After logging in, the devices added to your LTS Connect account, as well as the ones others shared to you, will be displayed in the device list.

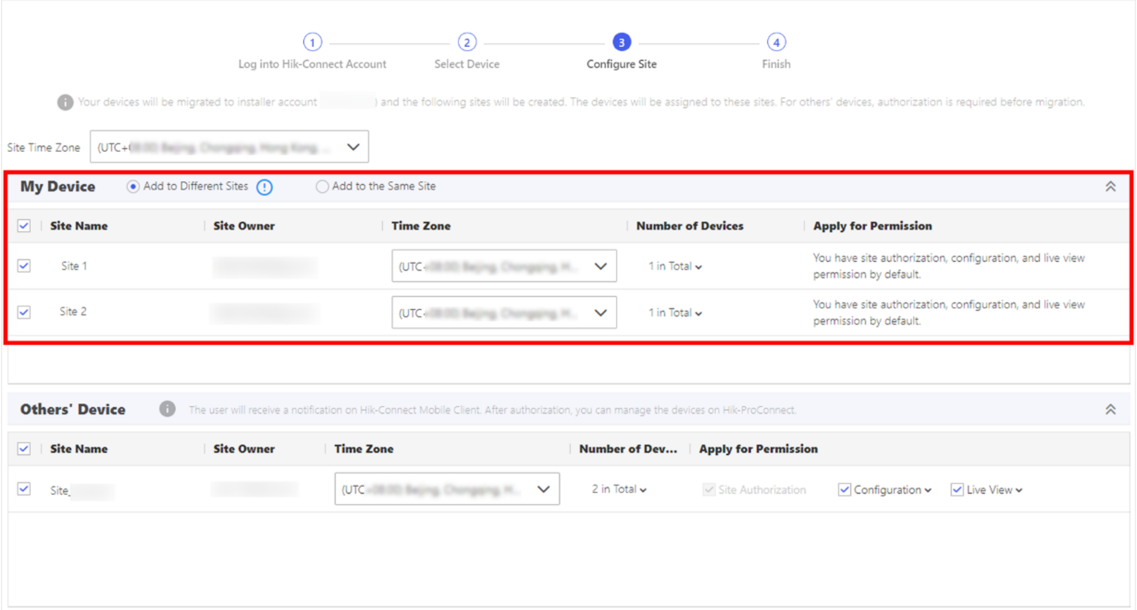
You can filter the devices by selecting **Show All Devices**, **Show My Devices Only** (the devices added to your LTS Connect account), or **Show Others' Devices Only** (the devices shared to your LTS Connect account from the customer) in the drop-down list.

Select the devices you want to synchronize with LTS Platinum Partner account, then click **Next**.

Configure Site for My Devices

Thirdly, you need to set the site information in LTS Platinum Partner for your devices to be synchronized.

For the devices added in your LTS Connect account (displayed in My Devices list), you can add them to different sites or to the same site according to your actual needs.



Your devices will be migrated to installer account [redacted] and the following sites will be created. The devices will be assigned to these sites. For others' devices, authorization is required before migration.

Site Time Zone (UTC+[redacted]

My Device ● Add to Different Sites ○ Add to the Same Site

☑ Site Name	Site Owner	Time Zone	Number of Devices	Apply for Permission
☑ Site 1	[redacted]	(UTC[redacted]	1 in Total	You have site authorization, configuration, and live view permission by default.
☑ Site 2	[redacted]	(UTC[redacted]	1 in Total	You have site authorization, configuration, and live view permission by default.

Others' Device The user will receive a notification on Hik-Connect Mobile Client. After authorization, you can manage the devices on Hik-ProConnect.

☑ Site Name	Site Owner	Time Zone	Number of Dev...	Apply for Permission
☑ Site_[redacted]	[redacted]	(UTC[redacted]	2 in Total	☑ Site Authorization ☑ Configuration ☑ Live View

Figure 6-10 Configure Site for My Devices

Add to Different Sites

If your devices are shared with different customers, select this option and you can add them to different sites.

For the devices which have been shared to the customers, the system will automatically create sites by the usernames of the customers, and then add the devices to these sites. If there already exists a site the site owner of which is the customer, the information of this site (site name and time zone) will be displayed, and the corresponding devices will be added to this site automatically.

For the devices which are not shared to anyone, the system will automatically create a site named after your LTS Connect account username, and then assign them to this site.

You can hover over the site name and click 🖉 to edit the site name.

Add to the Same Site

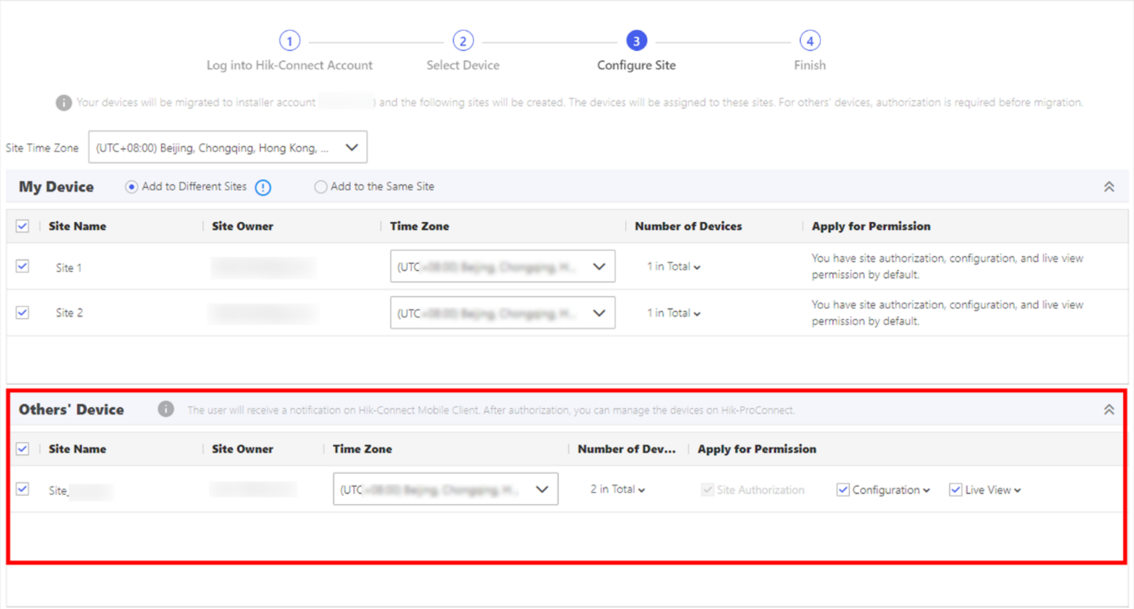
You can also add these devices to the same site. The system will automatically create a site named after your LTS Connect account username, and then add all these selected devices to this site.

You can hover over the site name and click ✎ to edit the site name.

By default, after synchronization, you will have site authorization permission of the automatically created site(s), and configuration as well as live view permission of the devices in My Devices list.

Configure Site and Permissions for Others' Devices

Fourthly, you need to set the site information in LTS Platinum Partner and set the device permission for the devices shared to you.



Your devices will be migrated to installer account [redacted]) and the following sites will be created. The devices will be assigned to these sites. For others' devices, authorization is required before migration.

Site Time Zone (UTC+08:00) Beijing, Chongqing, Hong Kong, ...

My Device ● Add to Different Sites ○ Add to the Same Site

☑ Site Name	Site Owner	Time Zone	Number of Devices	Apply for Permission
☑ Site 1	[redacted]	(UTC [redacted]	1 in Total	You have site authorization, configuration, and live view permission by default.
☑ Site 2	[redacted]	(UTC [redacted]	1 in Total	You have site authorization, configuration, and live view permission by default.

Others' Device The user will receive a notification on Hik-Connect Mobile Client. After authorization, you can manage the devices on Hik-ProConnect.

☑ Site Name	Site Owner	Time Zone	Number of Dev...	Apply for Permission
☑ Site_ [redacted]	[redacted]	(UTC [redacted]	2 in Total	☑ Site Authorization ☑ Configuration ☑ Live View

Figure 6-11 Configure Site and Permissions for Others' Devices

For the devices shared to you by others, usually customers, (displayed in Others' Devices list), they will be added to different sites. The system will automatically create sites named after the usernames of the customers, and then add all these selected devices to this site. If there already exists a site the site Owner of which is the customer, the information of this site (site name and time zone) will be displayed, and the corresponding devices will be added to this site automatically.

You can hover over the site name and click ✎ to edit the site name.

In the **Apply for Permission** list, you need to select the permissions that you want to apply from the customers for the devices. By default, you will have site authorization permission of the automatically created site(s). After synchronization, the customers will receive a notification on LTS Connect Mobile Client. After authorization by the customers, you can manage the devices on LTS Platinum Partner.

Set Time Zone

Fifthly, you can set the time zone of the devices if needed.

You can set the time zone for each device, or you can select a time zone in the **Set Time Zone** drop-down list at the upper-left corner to set a time zone for the devices in a batch.

Start Synchronization

Finally, start device synchronization.
After setting the sites and device permissions, select the devices in the My Devices and Others' Devices list, and click **Synchronize** to start synchronization.
For devices shared from the customers in Others' Devices list, the system will send a request to the customers. After the customers approve the authorization request, the devices will be synchronized successfully.
Click **Continue** to select other devices for synchronization or click **Finish and View** to view the devices synchronized after creating sites in the site list.

6.3 Move 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

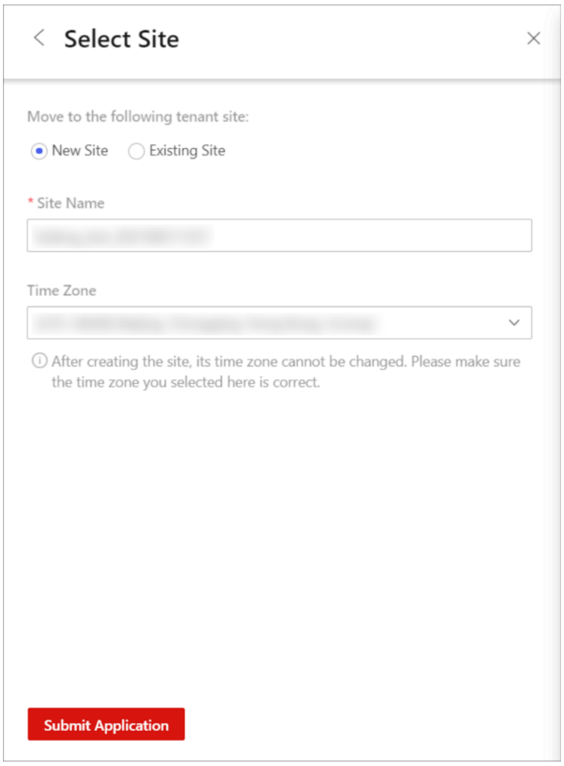
- This feature is only supported by a device that matches the following conditions:
  - The original Site where the device belongs must have been authorized to you.
  - The device needs to be added by LTS Connect (P2P). The devices added by IP address / domain name are not supported.
  - The original Site and the target Site should belong to the same Site Owner.
- Once a device is moved from its original Site, you need to configure the device again because all the original device configurations will be invalid. In addition, device related configurations including the linkage rules, exception rules, network switch settings, etc., will be affected. You need to configure these related configurations again also.

1. Go to **Site & Device → Customer Site**
2. Click ⇆ to switch to Site Mode.
3. Click the name of an authorized Site to enter its details page.
4. Click **Move Device** to open the Move Device pane.
5. Click **Select Device to Move**, select device(s), and click **Next**.
6. Select a Site.

Note

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



Select Site

Move to the following tenant site:

● New Site ○ Existing Site

* Site Name

[redacted]

Time Zone

[redacted]

ⓘ After creating the site, its time zone cannot be changed. Please make sure the time zone you selected here is correct.

Figure 6-14 Select Site

7. Click **Submit Application**.

Note

The application will expire if not handled within 7 days.

8. Optional: On the Move Device pane, click **View Device Movement Record** to enter the Device Movement Record page, and perform the following operation(s) if needed.

Apply Again	Click **Apply Again** to send an application for device movement again if the former one has been rejected or expired.
View Details	Click an application record to enter its details page to see the details.
Move More	Click an approved or sent application, and then click **Move More** to move more devices.

6.4 Manage 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.

6.4.1 Apply for Device Permission

After handing over a site to the customer, if you need to view the live/recorded videos of the devices added to the site or configure those devices, you can apply for the permission accordingly from the customer.

Steps

1. Go to **Site & Device** → **Customer Site**
2. Choose from the following based on whether the devices for which you are applying for permission belong to a single site or multiple sites.
   – Applying for permission for devices of a single site: Make sure you are in site mode. If not, click ⇆ next to **Device Mode** to switch to site mode. Click the name of a site to enter the site details page, and select the **Device** tab.
   – Applying for permission for devices of multiple sites: Make sure you are in device mode. If not, click ⇆ next to **Site Mode** to switch to device mode.
3. Enter the Permission Management page.
   – In both modes, if you are only applying for permission for a single device, you can click 🛡 on the device card (card view) or click 🛡 in the Operation column (list view).
   – In both modes, if you are applying for permissions for multiple devices, click **Permission Management**.
4. Select the needed permissions such as live view and playback.
5. Click ✎ to edit the validity period (Permanent, 1 Hour, 2 Hours, 4 Hours, or 8 Hours) for the permission.

Note

You can click **Batch Select** to select permissions and batch set a validity period for them.

6. Optional: Enter the remarks for the application.
7. Click **OK** to apply for the permission(s) from the customer.
   If the customer approves your application, you will get the corresponding permission(s).

6.4.2 Release Permission for Devices

If you do not need configuration and live view permissions for devices, or you complete the device configuration task earlier than the planned time, you can release Permissions manually.

Before You Begin

Make sure the site of the devices has been handed over to you.

Steps

1. Click a site in the site list to enter the site details page.
2. Click a device to show the device details page.
3. In the Permission section, select a permission, and click 🛡 → **OK** to release Permission.

Note

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

6.5 Linkage and Exception Rules

You can set up a linkage rule to trigger certain device actions when the triggering event occurs. You can configure an exception rule to specify how, when, and where you want to receive exception notifications of a device or channel.

Note

Make sure you have enabled the Notification functionality of the source device of the linkage/exception rule. If the function is disabled, events detected by the device cannot be reported and thus the linkage/exception rule cannot be triggered.

6.5.1 Add Linkage Rule

A linkage (see the picture below for reference) refers to the process in which an event detected by resource A triggers actions of resource B, resource C, resource D, etc. You can add a rule using the predefined template or customize a rule to define such a linkage. The rule contains five elements, including Source (resource A), Triggering Event (the event detected by resource A), Linked Resources (resource B, resource C, resource D, etc.), Linkage Actions (actions of resource B, resource C, resource D, etc.), and Linkage Schedule (the scheduled time during which the linkage is activated). These linkages can be used for purposes such as notifying security personnel, upgrading security levels, and saving evidence when specific events occur.

Add a Custom Linkage Rule

If the predefined templates cannot meet your needs, you can customize linkage rules as desired.

Steps

Note

- Make sure you have the permission for the configuration of the devices, or apply for the permission first. For details about applying for the permission, see ***Apply for Device Permission***.

- The Source and the Linked Resource cannot be the same resource.
- You cannot configure two identical linkage rules. In other words, you cannot configure two rules with the same Source, Triggering Event, Linked Resource, and Linkage Action.
- When the Source is a device added by IP/domain, the device added by LTS Connect cannot be set as the Linked Resource for triggering capture.

1. Go to **Site & Device** → **Customer Site**
2. Open the Add Linkage Rule pane.
   - Under site mode, select a site and click or··· → in its Operation column.
   - Under site mode, click the name of a site to enter the site details page, and then click **Linkage Rule** → **Add Linkage Rule**.
   - Under site mode, click the name of a site to enter the site details page, select a device, and then click in its Operation column or on its device card.
   - Under device mode, select a device, and then click in its Operation column or on its device card.

Note

To switch between device mode and site mode, click ⇆ at the top of the Customer Site page.

3. Set the required information.

Linkage Rule Name

Create a linkage rule name.

Trigger

Define the trigger for the linkage action.

Select Source

Select a resource as the Source.

Set Triggering Event

Select an event as the triggering event.

Note

Make sure that the triggering event has been configured on the selected device. For details about configuring event on device, see the user manual of the device.

Table 6-4 Available Triggering Events for Different Resource Types

Resource	Triggering Event
Camera	● Motion Detection ● Face Detection ● Intrusion ● Line Crossing Detection
Access Control Device	Tampering Alarm
Door Linked to Access Control Device	● Door Opened Normally **Note** Capture or Recording cannot be set as the linkage action for the triggering event "Door Opened Normally." ● Door Opened Abnormally ● Tampering Alarm
Door Station	Calling

Linkage

Click **Add** to select Linkage Action(s) and Linked Resource(s).

Note

- After selecting a Linkage Action, the resource(s) available to be set as Linked Resource(s) will appear.
- Up to 128 Linkage Actions or 10 Linked Resources can be selected.

Linkage Action

Select linkage action(s).

Table 6-5 Linkage Action Description

Linked Resource	Linkage Action	Description
Camera (Channel)	**Capture**	The camera will capture a picture when the Triggering Event is detected.
	Recording	The camera will record video footage when the Triggering Event is detected. **Note** The recorded video footage starts from 5 sec. before the detection of the Triggering Event and lasts 30 secs.
	Call Preset	Select a preset from the Preset drop-down list to specify it as the preset which will be called when the Triggering Event is detected. A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. By calling a preset, the PTZ camera will move to the predefined image position. **Note** Make sure you have configured presets for the PTZ camera. For details, see the user manual of the PTZ camera.
	Call Patrol	Select a patrol from the Patrol drop-down list to specify it as the patrol which will be called when the Triggering Event is detected. A patrol is a predefined PTZ movement path consisting of a series of key points (i.e., presets) that have their own designated sequence. By calling a patrol, the PTZ camera will travels to all the key points in set speed so as to provide a dynamic view. **Note** Make sure you have configured patrols for the PTZ camera. For details, see the user manual of the PTZ camera.
	Call Pattern	Select a pattern from the Pattern drop-down list tot specify it as the pattern which will be called when the Triggering Event is detected. A pattern is a predefined PTZ movement path with a certain

Linked Resource	Linkage Action	Description
		dwell-time configured for a certain position. By calling a pattern, the PTZ camera moves according the predefined path. **Note** Make sure you have configured patterns for the PTZ camera. For details, see the user manual of the PTZ camera.
	Arm	The camera will be armed and hence the events related to the camera will be uploaded to the LTS Connect Mobile Client when the Triggering Event is detected.
	Disarm	The camera will be disarmed and hence the events related to the camera will not be uploaded to the LTS Connect Mobile Client when the Triggering Event is detected.
	Enable Privacy Mask	Privacy mask will be displayed on the live images of the camera when the Triggering Event is detected. **Note** Make sure you have configured privacy mask for the camera. For details, see the user manual of the camera.
	Disable Privacy Mask	Privacy mask will NOT be displayed on the live images of the camera when the Triggering Event is detected.
Alarm Output	**Alarm Output**	The alarm output of the Linked Resource will be triggered when the Triggering Event is detected.
Area of Security Control Panel	**Stay Arm**	The arming status of the area of the security control panel will switch to Stay when the Triggering Event is detected.
	Away Arm	The arming status of the area of the security control panel will switch to Away when the Triggering Event is detected.
	Disarm	The area of the security control panel will be disarmed when the Triggering Event is detected.
Door Linked to Access Control Device	**Open Door**	The door related to the access control device will be opened when the Triggering Event is detected.
	Remain Open	The door related to the access control device will remain open when the Triggering Event is detected.
	Remain Closed	The door related to the access control device will remain closed when the Triggering Event is detected.

Linked Resource	Linkage Action	Description
Door Station	**Open Door**	The door linked to the door station will be automatically opened when the Triggering Event is detected.
Alarm Input	**Arm Alarm Input**	The alarm input will be armed and hence events related to it will be uploaded to the LTS Connect Mobile Client when the Triggering Event is detected.
	Disarm Alarm Input	The alarm input will be disarmed and hence events related to it will NOT be uploaded to the LTS Connect Mobile Client when the Triggering Event is detected.

Linked Resource

Select resource(s) as the trigger source of the Linkage Action.

Note

When configuring Linkage Actions for the same Source, if its Linked Resources are cameras (i.e., channels), you can set at most four Linkage Actions. For example, if you have set capturing picture and recording (the two are considered as two Linkage Actions) as the Linkage Actions for camera 1, you can only set two more Linkage Actions, i.e., capturing picture and recording for camera 2, or capturing picture for channel 2 and recording for channel 3, or recording for channel 2 and capturing picture for channel 3.

Note

After selecting Linkage Action(s) and Linked Resource(s), you can check the box(es) and then click **Delete** to delete the selected Linked Action(s) and Linkage Resource(s).

Linkage Schedule

Define the scheduled time during which the linkage is activated.

All Days

The external linkage action is always activated from Monday to Sunday, 7 days × 24 hours.

Custom

Select date(s) within a week and then specify the start time and end time for each selected date.

Note

The date(s) marked blue is selected.

4. Click **OK**.
The linkage rule will appear on the Linkage Rule list.

5. Optional: Perform the following operations if required after adding linkage rules.

Edit Linkage Rule	Click ··· → ✎ to edit the linkage rule
Delete Linkage Rule	Click ··· → 🗑 to delete the linkage rule
Disable Linkage Rule	Set ● to ○ to disable the linkage rule

What to do next

If you have enabled the linkage rule, make sure the Notification functionality of the Source is enabled. For details about enabling the functionality, see ***Enable Device to Send Notifications***.

Note

- If the Notification functionality of the Source is disabled, the Linkage Action will NOT be activated whether the Triggering Event is detected by Source or not.
- Please notify the end user after handing over the site to him/her that notification of the Source should be kept enabled on the LTS Connect Mobile Client, or the Linkage Action will NOT be activated whether the Triggering Event is detected by Source or not. For details about enabling alarm notification for a specific device or channel, see the *LTS Connect Mobile Client User Manual*.
- Please notify 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 to them.

Add Linkage Rule Based on Predefined Template

You can use six predefined templates to add linkage rules, including Intrusion, Forced Entry Alarm, Back to Home/Office, Away, Visitor Calling, and Perimeter Zone Alarm. Each of the six templates is designed for a typical application (see the table below) of linkage rule.

Before You Start

Make sure you have the permission for the configuration of the devices. If not, you need to apply for the permissions first. For details about applying for permission, see ***Apply for Device Permission***.

Table 6-6 Template Description

Template	Description
Intrusion	The Intrusion Template: Used for improving security level by triggering the linkage actions including capture, recording, and alarm output, when the intrusion event (people, vehicles, or other objects enter a predefined area) occurs.

Template	Description
Forced Entry Alarm	The Forced Entry Alarm Template: Used for improving security level by triggering the linkage actions including capture, recording, remaining door closed, alarm output, and calling preset when a door is opened abnormally.
Back to Home / Office	The Back to Home/Office Template: Used for lowering the security level and enabling privacy protection by triggering the linkage actions including disarming and enabling privacy mask, when you are back to home or office.
Away	The Away Template: Used for improving security level and canceling privacy protection by triggering the linkage actions including arming and disabling privacy mask when you leave your home or office.
Visitor Calling	The Visitor Calling Template: Used for improving security level by triggering the linkage actions including capture and recording when visitor(s) are calling from the door station.
Perimeter Zone Alarm	The Perimeter Zone Alarm Template: Used for improving security level by triggering the linkage actions including capture, recording, calling preset, alarm output, and remaining door closed, if people or other objects are detected in all accesses (including doors, windows, cellar doors, etc.) to a property.

Steps

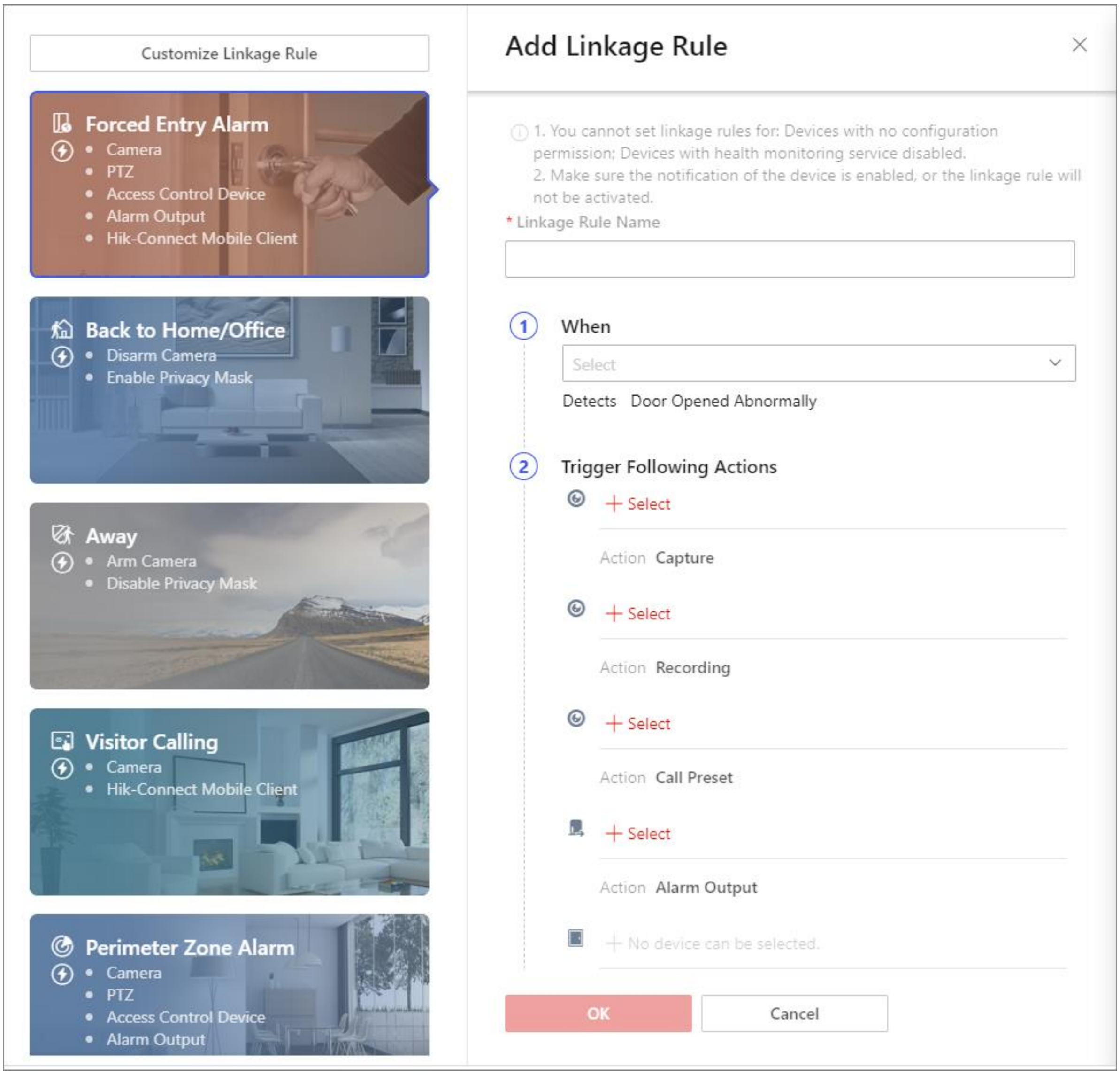
Note

Due to the similarity of adding linkage rules based on different templates, here we only introduce how to add a linkage rule based on the **Forced Entry Alarm** template.

1. Go to **Site & Device** → **Customer Site**
2. Open the Add Linkage Rule pane.
   - Under site mode, select a site and click or··· → in its Operation column, and then select the **Forced Entry Alarm** template from the left side of the Add Linkage Rule pane.
   - Under site mode, click the name of a site to enter the site details page, select the **Linkage Rule** tab, and then click the **Forced Entry Alarm** template in the Linkage Template area.
   - Under site mode, click the name of a site to enter the site details page, click **Add Linkage Rule** and then select the **Forced Entry Alarm** template from the left side of the Add Linkage Rule pane.
   - Under device mode, select a device, click in its Operation column or on its device card, and then select the **Forced Entry Alarm** template from the left side of the Add Linkage Rule pane.

Note

To switch between device mode and site mode, click ⇆ at the top of the Customer Site page.



Customize Linkage Rule

Forced Entry Alarm
- Camera
- PTZ
- Access Control Device
- Alarm Output
- Hik-Connect Mobile Client

Back to Home/Office
- Disarm Camera
- Enable Privacy Mask

Away
- Arm Camera
- Disable Privacy Mask

Visitor Calling
- Camera
- Hik-Connect Mobile Client

Perimeter Zone Alarm
- Camera
- PTZ
- Access Control Device
- Alarm Output

Add Linkage Rule

1. You cannot set linkage rules for: Devices with no configuration permission; Devices with health monitoring service disabled.
2. Make sure the notification of the device is enabled, or the linkage rule will not be activated.

* Linkage Rule Name

1 When

Select

Detects Door Opened Abnormally

2 Trigger Following Actions

+ Select

Action Capture

+ Select

Action Recording

+ Select

Action Call Preset

+ Select

Action Alarm Output

+ No device can be selected.

OK Cancel

Figure 6-16 Add Linkage Rule by Template

3. Set the required information.

Linkage Rule Name

Create a linkage rule name.

When

Select a resource as the Source for detecting line crossing event from the drop-down list.

Trigger the Following Actions

Click **Select** to select the Linked Resources used for triggering the linkage actions, and then click **Add**.

Note

- You can set only one linkage action.
- For details about the linkage actions, see ***Table 6-7***.

Linkage Schedule

Define the scheduled time during which the linkage is activated.

All Days

The linkage action is always activated from Monday to Sunday, 7 days × 24 hours.

Custom

Select date(s) within a week and then specify the start time and end time for each selected date.

Note

The date(s) marked blue is/are selected.

4. Click **OK**.
   The added linkage rule will be displayed in the linkage rule list.
5. Optional: Set ● to ○ to disable the linkage rule.

What to do next

If you have enabled the linkage rule, make sure the Notification functionality of the Source is enabled. For details, see ***Enable Device to Send Notifications***.

Note

- If the Notification functionality of the Source is disabled, the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not.
- Please notify the end user after handing over the site to him/her that notification of the Source should be kept enabled on the LTS Connect Mobile Client, or the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not. For details about enabling alarm notification for a specific device or channel, see the *LTS Connect Mobile Client User Manual*.
- Please notify 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 to them.

6.5.2 Add an Exception Rule

An exception rule is used to monitor the status of managed resources in real time. When the resource is an exception, the resource will push a notification to the LTS Platinum Partner to notify the specified Installer(s). Currently, the exceptions include two types: device and channel exceptions.

Before You Start

- Make sure you have the permission for configuration of the device. For applying configuration permission, refer to ***Apply for Device Permission***.
- Make sure you have enabled the device to send notifications to the system (if the device supports). For details, refer to ***Enable Device to Send Notifications***.

You can add a rule to define such a notification. The rule contains five elements, including **Source** (device A or channel A), **Exception** (the exception occurred on device A or channel A), **Received by** (the source pushes a notification to notify the recipient via certain ways), **Recipient** (who can receive the notification), as well as **Schedule** (when the recipient can receive the notification).

Steps

Note

This function is not supported by the solar camera.

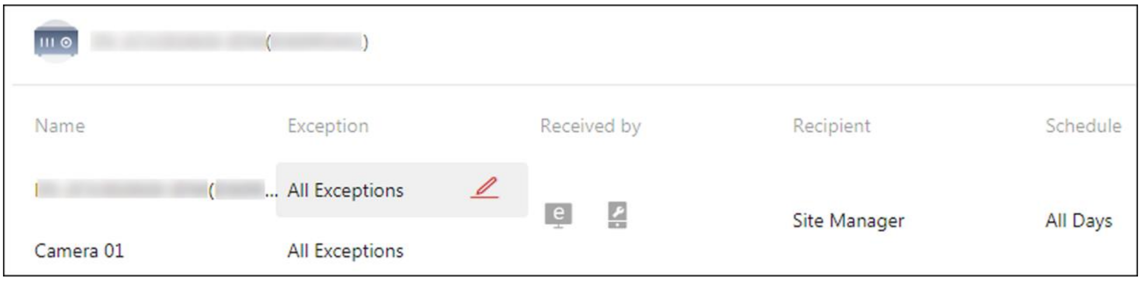
1. On the navigation pane, click **Site & Device** → **Customer Site**
2. Switch the mode to **Site Mode** if it is in Device Mode.
3. Click the name of a site to enter the site details page, and then click **Exception**. The exception rules of all the devices added in this site are displayed by default.
4. Optional: Click **Unfold Channels** to display all the channels of the device.

   Example

   For security control panels, all the zones and alarm outputs are displayed.

5. Set the types of exceptions which can trigger a notification.

   1.) Move the cursor to the **Exception** field of the device or channel and click ✎ .



[redacted] ([redacted])

Name	Exception	Received by	Recipient	Schedule
[redacted] ([redacted]...	All Exceptions ✎		Site Manager	All Days
Camera 01	All Exceptions			

Figure 6-17 Edit Exception

   2.) Check the exception type(s) that you want to set exception rules for.

Note

- For **Offline** exceptions, you can set a duration threshold. When the device or channel is offline for longer than this threshold, an offline exception will be triggered.
- The duration threshold of an offline device should be between 5 minutes and 24 hours (it is 5 minutes by default). You can also configure the device offline delay on the device card/list (See details in ***Configure Device Offline Delay***).
- The duration threshold for an offline channel should be between 5 and 120 minutes.
- For network switches, you can set exception rules for the following: PoE Port Power Off, SFP Port Disconnected, RJ45 Port Disconnected, Port Blocked, Port Busy, and PoE Power Exceeds Limit.

3.) Click **OK**.

6. Set where the notifications will be sent.

1.) Move the cursor to the **Received by** field and click ✎ .

2.) Check the receiving mode(s) according to actual needs.

Portal

When an exception is detected, the device will push a notification to the Portal in real time. The Portal is checked by default and cannot be edited.

Note

For checking received notifications in the Portal, refer to ***Exception Center***.

LTS Platinum Partner App

When an exception is detected, the device will push a notification to the LTS Platinum Partner Mobile Client in real time.

Email

When an exception is detected, the device will push a notification to the LTS Platinum Partner, and the system will send an email with the exception details to the email address(es) of the recipient(s) in real time.

LTS Connect App (Site Owner)

When an exception is detected, the device will push a notification to the LTS Connect Mobile Client, used by your customer in real time.

Note

For alarm devices, this option is enabled by default and cannot be disabled.

3.) Click **OK**.

7. Set who will receive the notification.

1.) Move the cursor to the **Recipient** field and click ✎ .

2.) Select **Site Manager** or **Installer Admin**. The recipient can receive the notification when the exception is detected in real time.

Note

- The Site Manager is checked by default and cannot be edited.
- If you select **LTS Connect App (Site Owner)** in the previous step, your customer will receive exception notifications.

3.) Click **OK**.

8. Set when the recipient can receive the notification.

1.) Move the cursor to the **Schedule** field and click ✎.

2.) Select the schedule.

All Day

The recipient can always receive notifications, 7 days a week and 24 hours a day.

Custom

Customize days and time periods on the selected days according to the actual needs.

3.) Click **OK**.

9. Optional: Set or edit the exception rules of the devices in the site in a batch.

1.) Click **Batch Edit**.

2.) Check the devices or channels on which to set the exception rules.

3.) Click ✎ in the bottom to set/edit the exception types, receiving mode, recipient, and notification time.

4) Click **OK** to save the settings.

10. Optional: After setting one rule, you can copy the rule settings to other devices or channels for quick settings.

1.) Click **Copy to**.

2.) In the **Copy Exception Settings from** field, select device(s) or channel(s) as the sources.

3.) In the **To** field, select the target resources of the same type as the selected sources.

4) Click **Copy** to copy the rule settings of the sources to the target resources and back to the exception rule list. Or you can click **Copy and Continue** to copy the rule settings and continue to copy other settings.

11. After setting an exception rule, you need to set the **Enable** switch in the upper-right corner of the rule to *"on"* to enable the device's exception rule; or, set the **Enable All** switch to *"on"* to enable the all devices' exception rules on the site.

After enabling the rule, it will be active and when an exception occurs, the device will push a notification according to the settings in the rule.

6.5.3 Enable Devices to Send Notifications

After adding and enabling a linkage rule or exception rule, you should make sure the Notification functionality of the Source device is enabled so that the events detected by the device can be uploaded to the LTS Platinum Partner system and the LTS Connect Mobile Client, which is the prerequisite to trigger the linkage actions and exception rules defined in the Source-device-related linkage rule(s) and exception rule(s) respectively.

Steps

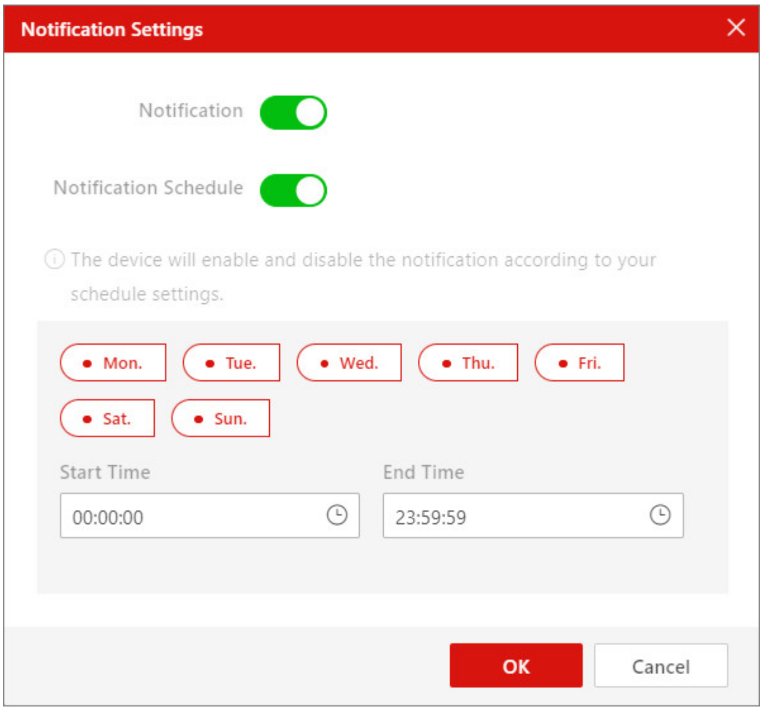
Note

The device should support this functionality. If you have activated the health monitoring service for the device, the Notification function of the device is enabled by default. For details about activating the health monitoring service, refer to ***Activate the Health Monitoring Service for Devices***.

1. Go to **Site & Device** → **Customer Site**
2. Open the Notification Settings window.
   - Under site mode, click the name of a site to enter the site details page, select a device under the **Device** tab, and then click 🔔 or ⋯ → 🔔 in its Operation column or on its device card.
   - Under device mode, select a device, and then click 🔔 or ⋯ → 🔔 in its Operation column or on its device card.

Note

To switch between device mode and site mode, click ⇆ at the top of the Customer Site page.



Notification Settings

Notification: on

Notification Schedule: on

The device will enable and disable the notification according to your schedule settings.

Mon. Tue. Wed. Thu. Fri. Sat. Sun.

Start Time: 00:00:00

End Time: 23:59:59

Figure 6-19 Notification Settings

3. Set the parameters.

   Notification

   Make sure the functionality is enabled.

   Notification Schedule

   After enabling the Notification functionality, set a time schedule for uploading the events detected by the Source to the LTS Platinum Partner system and the LTS Connect Mobile Client.
   You can select date(s) and then set the start time and end time for each selected date.
4. Click **OK**.

Note

- Please notify the end user after handing over the site to him/her that notification of the Source should be kept enabled on the LTS Connect Mobile Client, or the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not. For details about enabling alarm notification for a specific device or channel, see the *LTS Connect Mobile Client User Manual*.
- Please notify 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 to them.

6.6 Reset Device Password

You can reset the password of a device when you and the site owner both lost the password. Two methods of resetting device password are available: resetting passwords off-site or on-site.

Note

- Resetting passwords via the LTS Platinum Partner platform is not supported by every device type/model.
- To reset the device password via the Portal, make sure that the device is authorized by the Site Owner to you before resetting device password. For details, see ***Apply for Site Authorization from Site Owner***.
- More convenient password reset methods are available on the LTS Platinum Partner Mobile Client, such as by scanning the QR codes for password reset, using the SADP tool for LAN devices, and submitting password reset cases. Refer to the ***LTS Platinum Partner Mobile Client user manual*** for more details.

Go to **Site & Device** → **Customer Site**
Open the Reset Password window via one of the following ways:

- Under site mode, click the name of a site to enter the site details page, select a device under the **Device** tab, and then click 🔑 or ••• → 🔑 in its Operation column or on its device card.

- Under device mode, select a device, and then click 🔑 or ● ● ● → 🔑 in its Operation column or on its device card.

Note

To switch between device mode and site mode, click ⇆ at the top of the Customer Site page.

There are two methods to reset the device password.

- **Reset Password Offsite**: You do not need to travel to the site where the device is located to reset the device password. This method can be used when you are not at the site.

  Note

  Make sure that LTS Connect (the Mobile Client for your customers) and the device are on the same LAN and that the version of LTS Connect is V 4.15.0 or later.

- **Reset Password Onsite**: You need to go to the site where the device is located. This method can be used when you are at the site.

  Note

  Make sure that LTS Platinum Partner (the Installer platform) and the device are on the same LAN.

6.7 Enable 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 should contact the end user to enable the Remote Log Collection function on LTS Connect.

Steps

1. Go to **Site & Device** → **Customer Site**
2. Open the Remote Log Collection window.
   - Under site mode, click the name of a site to enter the site details page, select a device under the **Device** tab, and then click ✎ or ··· → ✎ in its Operation column or on its device card.
   - Under device mode, select a device, and then click ✎ or ··· → ✎ in its Operation column or on its device card.

   Note

   To switch between device mode and site mode, click ⇆ at the top of the Customer Site page.

3. Click **Authorize**.
4. Select the validity period from the drop-down list.

Note

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

5. Click **Enable** to enable the function.
   The Remote Log Collection icon turns from to .
6. Optional: Disable the function.
   1.) Click **Remote Log Collection**.
   2.) Click **Deauthorize** in the pop-up window.

6.8 View Video

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

6.8.1 View Live Video

By viewing live view of managed cameras, you can check whether the camera is installed and located properly by capturing pictures, recording, PTZ control, etc.

- Click **Encoding Device** on the top of the Site Detail page to show all the encoding devices of the site.
- Click **Customer Site** → ⇆ to change to the device mode and enter the device list page.

Select an encoding device and click to launch the live view. The live view will work for up to five minutes. When the live view ends, you can still start a new feed. Hover the cursor on the live view window and click icons on the tool bar to start recording, conduct digital zoom and PTZ control, capture a picture, switch image quality, and turn on/off audio. Double-click the live view image to enter the full-screen mode, then double-click the image again to exit full-screen mode.

Note

- Up to 16 live view windows are supported.
- 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 do not 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 to them.
- Make sure the device is online, otherwise the function cannot be used.

6.8.2 Play Back Video Footage

Video playback shows what happens when emergencies occur. If an end user approves your application for device playback permission, you will be able to play back the recorded video footage stored on the device.

Note

- Make sure your account has the permission for playback. Otherwise, you cannot enter the playback page. See ***Apply for Device Permission*** for details about applying device permission.
- This function needs to be supported by a device.
- Make sure you have configured recording schedule for the device and there is video footage stored in the device.

- Click **Encoding Device** on the top of the Site Detail page to show all the encoding devices of the site.
- Click **Customer Site** → ⇆ to change to the device mode and enter the device list page.

On the device list page, select a device and click ▶ to enter the playback page. You can select a date and time on the calendar to view the playback during a certain time range.

You can select channels from the drop-down list on the top right. Drag the time bar at the bottom to jump to different video footage. Hover the cursor on the time bar and zoom in the time bar to select a more accurate time. Hover the cursor on a playback window and click icons on the tool bar to capture a picture, clip video footage, perform digital zoom, download video footage, and turn on the audio.

For devices (including the added online devices) added by LTS Connect Service without configuring DDNS, the playback will work for up to five minutes; for devices added by IP/Domain Name, and devices (including the added online devices) added by LTS Connect Service with DDNS configured, the playback duration is not limited.

Note

Up to four playback windows are supported.

6.9 Network Device Management

Setting up network devices like the access controller (AC), access point (AP) and switch, and security devices like security control panels 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 LTS Platinum Partner Mobile Client to add network devices, and the Portal Client to configure them.

6.9.1 Network Topology

If you have added network devices AC, AP, and switches to a site, and the devices connected to the network switch on the Mobile Client, 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 the configuration permission of the network switch, otherwise network topology will be unavailable. For details about applying for the 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 heath monitoring service for devices, see ***Activate the Health Monitoring Service for Devices***.

You can enter the network topology page in the following ways:

- Select **Site & Device** → **Consumer Site**. Select a site on the site list to enter the detail page, select the **Device** tab, and then select **More** → **View Topology**. You can perform the following operations on the network topology.

  Note

  If you have NOT enabled the Health Monitoring service for the network switch, you can enter the network topology page in this way only.

- On the navigation bar, click **Site & Device** → **Health Monitoring** → **Health Status**, select **All Sites** from the site list, and then select **Network Switch**, and then click in the Operation column in the network switch list.
- On the navigation bar, click **Site & Device** → **Health Monitoring** → **Health Status**, select a site from the site list to enter the site details page, and then click **Topology**.

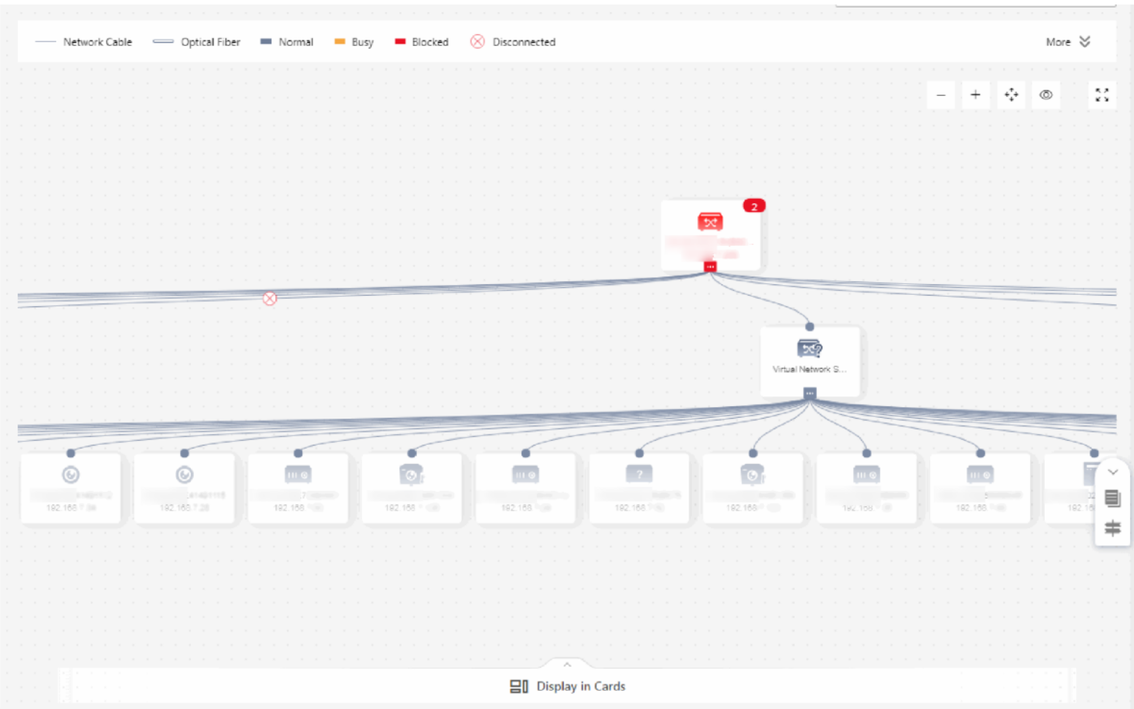


Figure 6-29 Network Topology

The following table shows the descriptions of the operations available on the network topology.

Table 6-7 Available Operations

Operation	Description
Set Root Node	If you want to change the root node, you can select a device and select ✎ to set a device to a root node. **Note** You can set third-party devices to the root node.
View Network Device Details	● Click an AC device on the topology to view its device status and basic information. ● Click a switch device to view its basic information, device status, and port status. **Note** You cannot view details of a virtual network switch.

Operation	Description
View Details of Other Devices	Tap a device to view its details, such as device model and network status. **Note** ● Make sure you have the configuration permission for the device, otherwise you need to apply for the permission first. ● If the device is not added to the same site with the network switch, you cannot view its details.
View More Information	In the upper-right corner of the topology, select **More** to view the introduction of the device type and device status.

6.10 Other Management

You can perform more operations for device management, including upgrading device firmware, unbinding a device from its current account, configuring DDNS for devices added by LTS Connect service, and remotely configure parameters for devices such as encoding devices and security control devices.

6.10.1 Upgrading Devices

On the device list page, ⬆ will appear beside the name of a device if it is upgradable. You can upgrade the device to make it compatible with the LTS Platinum Partner.

Steps

Note

- The function is supported by devices such as certain models of network cameras and DVRs / NVRs.
- The system supports upgrading encoding devices, some access control devices, and video intercom devices connected to the same LAN with the PC where the platform runs.
- You can also upgrade devices in the Health Monitoring module. For details, see ***Health Monitoring***.
- You can also upgrade devices when you add them. See ***Add Detected LAN Device*** and ***Add Device by Entering Serial No.*** for details.

1. Select upgradable device(s).
   – Click a site name to enter the site details page. Hover over ⬆, click **Upgrade Device** and then

select upgradable device(s).
  - Click **Customer Site** → ⇆ to switch to the device mode, click **Upgrade** and then select upgradable device(s).
2. Click **Upgrade**.
   A window will pop up showing the upgrade progress. If there are devices that failed to be upgraded, the causes will be displayed on the window.

6.10.2 Batch Upgrading Devices on a LAN

You can batch upgrade devices (encoding devices, etc.) on the same LAN to make the devices compatible with LTS Platinum Partner, if there are new firmware versions for the devices.

1. Click **Install & Config** → **On-Site Batch Upgrade**.
2. Select device(s) that need to be upgraded.
3. Click **Upgrade by Local File** to upgrade the selected device(s).

6.10.3 Upgrading Devices Manually by Uploading Firmware Package

If a device with the new firmware version to be upgraded and the PC running with the Portal are not on the same LAN (Local Area Network), you can upload firmware packages from the local PC for manually upgrading the device to make the device more compatible with LTS Platinum Partner.

Before You Start

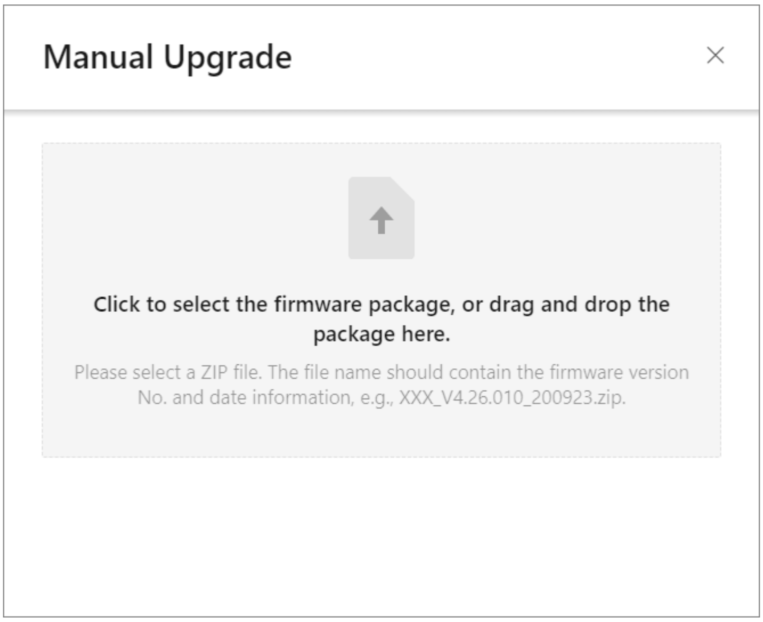
- Make sure you have permission to remotely configuring devices.
- This function is only available for some DVRs and NVRs.

Steps

Note

If a device and the PC running with the Portal are on the same LAN, you can directly go to the remote configuration page of the device to upgrade the device. For details about the remote configuration, refer to ***Remote Configuration***.

1. Go to the Customer Site page.
2. Open the Manual Upgrade pane of an upgradable device.
   - In Site Mode, click a site name to enter the site details page, and then select a device and click ⋯ → **Manual Upgrade**.
   - In Device Mode, click ⋯ → **Manual Upgrade**.



Manual Upgrade

Click to select the firmware package, or drag and drop the package here.

Please select a ZIP file. The file name should contain the firmware version No. and date information, e.g., XXX_V4.26.010_200923.zip.

Figure 6-33 Manual Upgrade Pane

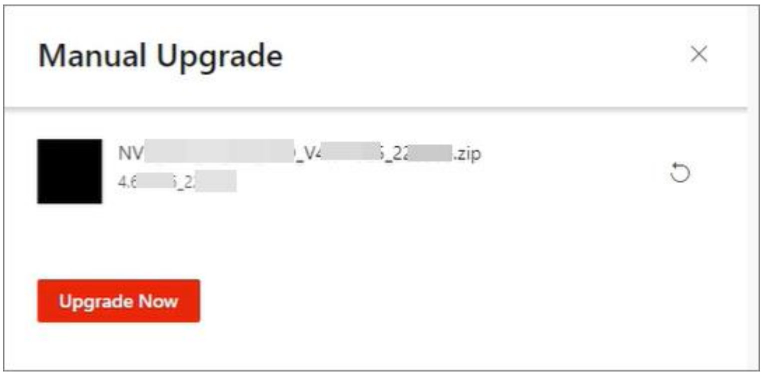
3. Click ↑ to select a firmware package in ZIP format from the local PC or drag a package to the gray area.

Note

The package file should be named by one of the following formats:

- Format 1: {custom name}_V{firmware version No.}_{date}.zip. For example, "test_V4.26.10_230316.zip".
- Format 2: {custom name}_V|v{firmware version No.}_Build_{date}.zip. For example, "NVR_V5.0.0_Build_220210.zip" or "NVR_v5.0.0_Build_220210.zip".
- Format 3: {custom name}_V{firmware version No.}_build{date}.zip. For example, "DVR_V4.26.500_build200518".

If the uploaded file name does not match any one of the above formats, you will be prompted with an error message.



Manual Upgrade

NV[redacted]_V4[redacted]_22[redacted].zip

4.6[redacted]_2[redacted]

Figure 6-34 After Selecting Firmware Package

4. Optional: Click ↻ to reselect an upgrade package as you needed.

Note

If you click × to close the Manual Upgrade pane, the selected package will still be kept for the next time you open the pane.

5. Click **Upgrade Now** and a risk prompt will pop up.
6. Click **OK** to start upgrading the device.

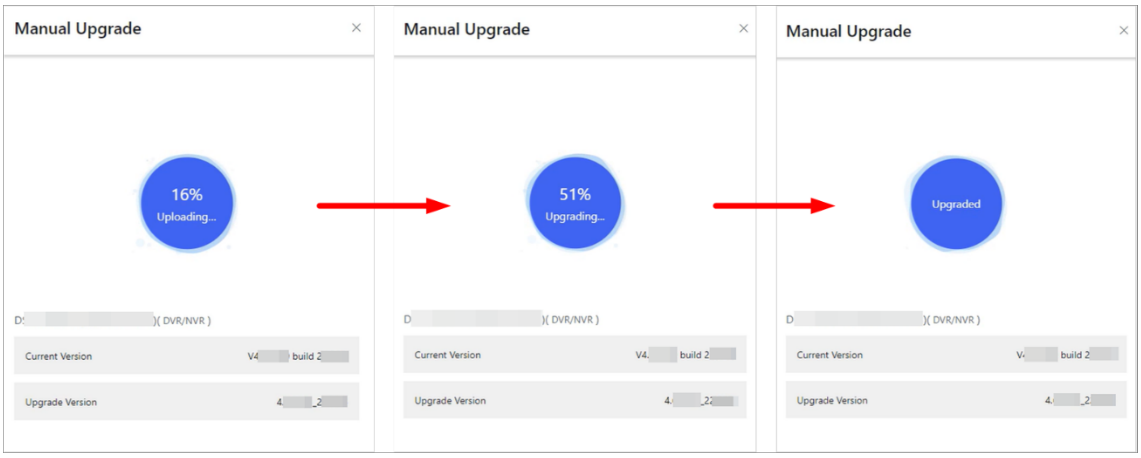


Figure 6-35 Upgrade Result

The status (including Uploading, Upgrading, Upgraded, and Upgrading Failed), the upgrading progress, the current firmware version, and the upgrade firmware version will be displayed on the Manual Upgrade pane.

6.10.4 Unbind a Device from Its Current Account

When you add detected device(s) online and the results page shows that a device has been added to another account, you need to unbind it 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 lost the password for the old account).

Note

- For details about adding detected LAN devices, see ***Add Detected LAN Device***.
- If handing over a Site to your customer by sharing, you cannot unbind the devices added to this Site. For details about Site handover, see ***Hand Over Personal Site by Transferring***.

On the adding results page, click 🔗 in the Operation column, and then enter the device password, then click **OK** to unbind it from its current account. When the device is unbound, you can click ⊕ in the Operation column to add the device 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.

6.10.5 Configure DDNS for Devices

For devices with invalid or outdated firmware, you can configure DDNS for them to make sure they can be properly managed by the LTS Platinum Partner.

Steps

Note

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

1. On the navigation pane, click **Customer Site** → ⇆ to switch modes.
   - For site mode, click a site to enter the site details page, and click **Device** to enter the device list page.
   - For device mode, all devices are displayed on the page.
2. Select a device, and click • • • → ▦ to open the DDNS Settings window.
3. Switch **Enable DDNS** on to show the DDNS parameters.

Note

You can click **How to set port?** to learn more about configuration.

4. 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

   You enter the service port and HTTP port manually.

5. Enter the device's domain name.
6. 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.

7. Click **OK**.

6.10.6 Configure Device Offline Delay

You can set the allowed offline duration for the device. Notifications about device offline exceptions will be received on LTS Platinum Partner, ARC, and LTS Connect only if the device is offline for longer than the configured duration.

Before You Start

- Make sure you have added device(s) that are connected to LTS Connect services (P2P).
- For NON security control panels, make sure you have activated health monitoring services and configured **Offline** as an exception type on the site details page. See details in ***Activate the Health Monitoring Service for Devices*** and ***Add Exception Rule***.

Note

- You can also configure the device's offline delay duration directly on the site details page.
- For security control panels, you need to activate health monitoring services and configure **Offline** as an exception type only if you need to receive exception notifications on LTS Platinum Partner (it is not required to activate health monitoring services for receiving exception notifications on LTS Connect).

Steps

1. On the navigation pane, click **Customer Site**
2. Open the Configure Offline Delay pane.
   – In Device Mode, click ◷ on the device card/list.
   – In Site Mode, enter the detail page of a site and click ◷ on the device card/list.
3. Specify the delay duration.

Note

The duration should be between 5 minutes and 24 hours.

4. Click **OK**

6.10.7 Remote Configuration

You can perform remote device configuration when needed.

Note

Only a site manager can perform the following operations and configurations of a site. See ***Assign Site to Installer*** for details about assigning site.

On the navigation bar, click **Site & Device** → **Customer Site** to enter the Site page. And then click ⇆ to switch to site mode. Click a site's name to enter the site's page. And then click **Device** tab to show the site's devices.

Note

In Device mode, all devices in the platform will be displayed.

Click ⚙ to open the remote configuration page of the device and set the device's parameters.

Note

- Only encoding devices and indoor stations support remote configuration.
- Make sure the device is online, otherwise the function cannot be used.
- For doorbells, you do not need to enter the device username and password before accessing the remote configuration page.
- For encoding devices, if you have already entered the device's username and password when adding it, you will not need to enter the information before remote configuration. For NVR and DVR, operations including rebooting, HDD formatting, and network settings are supported.
- If the device is not in the same local area network with the Portal, some operations in the remote configuration (such as device account management, enabling LTS Connect, and restoring device, etc.) are not available.
- See device user manual for details about remote configuration.
- If you have changed device parameters by other software or client (such as the device page, LTS Platinum Partner Mobile Client, etc.), and the parameters on the Portal's remote configuration page are not updated to the latest firmware, click **Clear Cache** in the drop-down list on the top right of the remote configuration page; this will update the device parameters.

Chapter 7. Health Monitoring

The Health Status module provides 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 of importance 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.

Note

- A video tutorial on how to check device health status will pop up in the lower-right corner of the page when you enter the Health Status module.
- For Installers, you can only view the status information of devices on the site assigned to you. For an Installer Admin, you can view the status information of devices on all sites.
- 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***.

7.1 View Status of Devices in All Sites

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

Click **Site & Device** → **Health Monitoring** → **Health Status** on the navigation bar to enter the Health Monitoring page, and then select **All Sites** from the site list.

You can view the total number of devices and the number of abnormal devices of each device type.

Refer to the following table to get to the device description and operations.

Table 7-1 Links of Different Device Types

Encoding Device	Refer to ***Encoding Device***.
Access Control Device	Refer to ***Access Control Device***.
Video Intercom Device	Refer to ***Video Intercom Device***.
Network Switch	Refer to ***Network Switch***.

Encoding Devices

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

Note

For analog cameras, you can view the status if video loss occurs.

Offline Cameras

The number on the left of the slash represents the number of offline/total cameras linked to the device.

Offline Duration

The 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)". You can click **Offline Duration** to sort devices by offline duration.

You can perform the following operations.

Operation	Description
View Device Name and Version	Hover the cursor over the device name to view its device type and device version.
Remotely Configure Device	Click ⚙ in the Operation column to remotely configure the device parameters. For details, see the device user manual.
Inspect All Encoding Devices	Click **Refresh** to inspect all the encoding devices in all sites.
Inspect Selected Encoding Device	Click ⟲ in the Operation column to inspect the selected encoding device manually.
Display Abnormal Devices	Check **Display Abnormal Devices Only** to display the abnormal devices only.
Display Authorized Devices	Check **Display Authorized Devices Only** to display the devices of which configuration permission has been authorized to you.
View Camera Status	Click › to show the cameras linked to the device, and then you can view the online/offline status of each camera.
View HDD Information of DVR	Click › to show the HDD information of the DVR, including self-inspection evaluation result, overall evaluation result, running status, running time, HDD temperature, and S.M.A.R.T information.
View Site Owner and Site Manager Information	Move the cursor to 👤 in the Site column to view the information of the Site Owner and Site Manager, such as name and phone no.
Live View	Click 🎥 in the Operation column and then select camera(s) to view live video(s).

Operation	Description
	Note ● If you have no permission to view the live video, you can apply for the live view permission from the end user. For details, see ***Apply for Device Permission***. ● If a selected camera has enabled stream encryption, you should enter the device verification code before you can view its live video. ● The device verification code is created when you connect the device to the LTS Connect service. For details, see ***Add Detected LAN Device***.
Playback	Click ▶ in the Operation column and then select camera(s) to playback video(s). **Note** ● If you have no permission to view the video playback, you can apply for the playback permission from the end user. For details, see ***Apply for Device Permission***. ● If a selected camera has enabled stream encryption, you should enter the device verification code before you can view its video playback. ● The device verification code is created when you connect the device to the LTS Connect service. For details, see ***Add Detected LAN Device***.
Apply for Permission or Reconfigure Device	❗ appearing beside the device name represents that you have no configuration permission for it, the IP address/domain set for the device is invalid, or DDNS is invalid. You can hover the cursor on the icon, and then apply for the permission from the end user, reconfigure its IP address/domain, or reconfigure DDNS respectively based on the prompts.

Operation	Description
	Note ● For details about applying for configuration permission, see ***Apply for Device Permission***. ● For details about configuring device IP address/domain, see ***Add Devices by IP Address or Domain Name***.For details about configuring DDNS, see ***Configure DDNS for Devices***.
Search for a Device	Enter keywords in the search field and click 🔍 to search for specific devices.
Auto Update	You can switch on **Auto Update** so that the latest device exceptions and status received by the Portal will be displayed in real time.

Access Control Devices

You can view statuses including network status, door number, last inspected time, etc.
You can perform the following operations.

Operation	Description
View Device Name and Version	Hover the cursor over the device name to view its device type and device version.
Inspect All Access Control Devices	Click **Refresh** to inspect all access control devices.
Inspect Selected Access Control Device	Click ⟳ in the Operation column to inspect the selected access control device manually.
Display Abnormal Devices	Check **Display Abnormal Devices Only** to display the abnormal devices only.
Display Authorized Devices	Check **Display Authorized Devices Only** to display the devices of which configuration permission has been authorized to you.
View Site Owner and Site Manager Information	Move the cursor to ✓ in the Site column to view the information of the Site Owner and Site Manager, such as name and phone

Operation	Description
	number.
Apply for Permission or Reconfigure a Device	❗ appearing beside the device name represents that you have no configuration permission for it. You can apply for the permission from the end user. **Note** For details about applying for configuration permission, see ***Apply for Device Permission***.
Search for a Device	Enter the keywords in the search field and click 🔍 to search for specific devices.
Auto Update	You can switch on **Auto Update** so that the latest device exceptions and status received by the Portal will be displayed in real time.

Video Intercom Devices

You can view the status such as network status and last inspected time.
You can perform the following operations.

Operation	Description
View Device Name and Version	Hover the cursor over the device name to view its device type and device version.
Inspect All Video Intercom Devices	Click **Refresh** to inspect all video intercom devices.
Inspect Selected Video Intercom Device	Click 🔄 in the Operation column to inspect the selected device manually.
Display Abnormal Devices	Check **Display Abnormal Devices Only** to display the abnormal devices only.
Display Authorized Devices	Check **Display Authorized Devices Only** to display the devices of which configuration permission has been authorized to you.
Apply for Permission or Reconfigure Device	❗ appearing beside the device name represents that you have no configuration permission for it. You can apply for the permission from the end user.

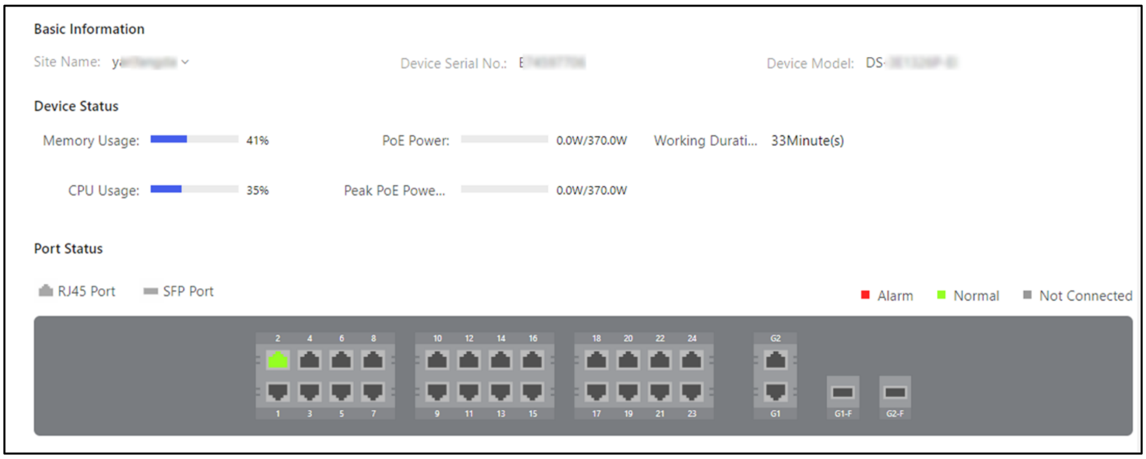
Operation	Description
	Note For details about applying for configuration permission, see ***Apply for Device Permission***.
Search for a Device	Enter the keywords in the search field and click 🔍 to search for specific devices.
Auto Update	You can switch on **Auto Update** so that the latest device exceptions and status received by the Portal will be displayed in real time.

Network Switch

View information including network status of the switch (online/offline), the number of online ports of the switch, and the latest time when the device was inspected.

You can also perform the following operations:

Operation	Description
Inspect Selected Device	Click ⇄ in the Operation column to inspect the selected device manually.
Remotely Reboot Device	Click © in the Operation column to reboot the network switch remotely.
View Typology	Click ⊞ in the Operation column to view the topology of this switch. For details about topology, refer to ***Network Topology***.
View Switch Details	Click › to view the detailed information of the switch, including the memory usage, CPU usage, POE power, peak POE power, working duration, port status (alarm, normal, not connected). **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.



Basic Information

Site Name: [redacted]

Device Serial No.: [redacted]

Device Model: [redacted]

Device Status

Memory Usage: 41%

PoE Power: 0.0W/370.0W

Working Durati... 33Minute(s)

CPU Usage: 35%

Peak PoE Powe... 0.0W/370.0W

Port Status

RJ45 Port
SFP Port
🟥 Alarm
🟩 Normal
■ Not Connected
2 4 6 8 10 12 14 16 18 20 22 24 G2
1 3 5 7 9 11 13 15 17 19 21 23 G1
G1-F
G2-F

Figure 7-1 Switch Details

On the Switch Details page, you can perform the following operations:

Operation	Description
View Enlarged Port Image	Hover the cursor over the switch image to view the enlarged picture of the ports.
Clear Alarm	For port with alarm(s), click ··· → **Clear Alarm** to clear the alarm(s) of this port.
Restart Port	For an abnormal port, click ··· → **Restart Port** to restart.
Extend Port Transmission Range	Click ··· → **Enable Extend Mode/Disable Extend Mode** to extend the transmission range of this port or not. **Note** When enabled, the transmission range of the port will be extended from 200 to 300 meters. Meanwhile, its bandwidth will be limited within 10 Mbps.

7.2 View Status of Devices in a Specific Site

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

Steps

1. Click **Site & Device** → **Health Monitoring** → **Health Status** on the Navigation panel to enter the Health Status page.
2. Select a specific site from the site list. The status of the devices in the site will be displayed.

3. Optional: Perform the following operations.

Filter Data	Check **Display Abnormal Devices Only** to display abnormal device(s) only. Check **Display Authorized Devices Only** to display the device(s) of which configuration permission has been authorized to you only.
Auto Update	You can switch on Auto Update so that the latest device exceptions and statuses received by the Portal will be displayed in real time.
Upgrade Device Firmware	A number in red will be displayed on **Upgrade** showing the number of upgradable device(s). You can click **Upgrade**, select the upgradable device(s), and then click **Upgrade** to upgrade them. Select a device to view its basic information. If the device firmware is upgradable, you can click **Upgrade** in the Firmware Version field to upgrade it. **Note** For details, see ***Upgrade Device***.
Diagnose Devices of the Site	Click **Health Check** to open the Health Check window, and click **Check Now** to diagnose the devices of the site. When the checking completed, you can view the status of each device in the site. For NVR, and DVR, you can click **View Report** to export the diagnostics report as a PDF file to the local PC.
View Site Owner Information	Click **Site Owner** to view the Site Owner information, including name, email address, and phone number.
View Site Manager Information	Click **Site Manager** to view the Site Manager information, including name, email address and phone number. Up to 100 site managers can be displayed.
Inspect Devices in the Sites	Click **Refresh** to inspect all the devices in the site.
Remote Configuration	Select a device and then click **Remote Configuration** to remotely configure the parameters of the device. **Note** ● The device should be online, or remote configuration will be unavailable. ● For details, see the user manual of the device.

Inspect a Single Device	Select a device and then click ⇄ to inspect it.
Search for Device	Enter the keywords in the search field and click 🔍 to search for specific devices.
Reconfigure IP or Domain of Encoding Device	Move the cursor to ❗, and then click **Edit IP/Domain** to reconfigure the device's IP/domain. For details about configuring IP/Domain, see ***Add Devices by IP Address or Domain Name***.
Reconfigure DDNS	Move the cursor to ❗, and then click **Configure DDNS** to reconfigure the device's DDNS. For details about configuring DDNS, see ***Configure DDNS for Devices***.
View Encoding Device Details	You can view the network status, storage status, HDD usage, and overwritten recording status, etc. You also click the encoding device to view its details, including basic information such as device type and serial no., and the network status of each camera linked to it. You can click 🎥 and select linked cameras, and then click ✓ to view live videos. If the encoding device is a DVR, you can also view its HDD information, including self-inspection evaluation result, overall evaluation result, running status, running time, HDD temperature, and S.M.A.R.T information. For analog cameras, you can determine if video loss occurs. **Note** ● If you have no permission to view the live video, you can apply for the live view permission from the end user. For details, see ***Apply for Device Permission***. ● If a camera has enabled stream encryption, you should enter its device verification code in the pop-up window before you can view its live video. ● The device verification code is created when you connecting the camera to the LTS Connect service. For details, see ***Add Detected LAN Device***.
View Access Control Device Details	Click an access control device to view its details, including basic information such as device type and serial no., and the device status including network status and the number of its linked doors.
View Video Intercom Device Details	Click a video intercom device to view its basic information and its network status.

View Network Switch Details	The network switches are displayed by card. Click a switch to view its information, including the device model, device type, device serial no., the time of last inspection, network status, memory usage, CPU usage, PoE Power, peak PoE power in latest 70 days, working duration, port status (alarm, normal, not connected). **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. Hover the cursor onto the picture of switch to view the enlarged picture of the switch. Click ⊞ **Topology** at the top of the page to view the topology of this switch. For details about topology, refer to ***Network Topology***. Click ⟲ in the Operation column to inspect the device manually. For port with alarm(s), click ⋯ → **Clear Alarm** to clear the alarm(s) of this port. For the abnormal port, click ⋯ → **Restart Port** to restart this port. Click ⋯ → **Enable Extend Mode/Disable Extend Mode** to extend the transmission range of this port or not. **Note** When enabled, the transmission range of the port will be extended to 200 to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.

7.3 Send Regular Reports

You can set up schedules for the platform to generate and send device health check reports to the specified email addresses automatically, so that recipients get regular updates on the health status of important devices and compare the reports of each period.

Before You Start

Make sure you have activated the Health Monitoring service.

Steps

1. Enter the Scheduled Report page.
   - Go to **Site & Device** → **Health Monitoring** → **Scheduled Report**.

- Click **Site & Device** → **Customer Site** → **Scheduled Report**.

Note

- All sites available for this feature are shown on the page automatically.
- The platform only supports automatically sending health check reports of encoding devices on authorized sites.
- Sites without the above-mentioned types of devices or sites that are not authorized to you will NOT be shown on the page.

2. Enter the editing mode.
   - To configure the report sending schedule for a single site, click **Edit** on the right side of a site.
   - To configure the report sending schedule for multiple sites, click **Batch Configure** and then select the sites you want to configure.
3. Configure the report sending settings.

   Device

   Select the device(s) to be health-checked and included in the report.

   Send At

   Specify the frequency, date, and time of sending the reports. You can set the frequency to Daily, Weekly, Monthly, Quarterly, Semiannually, or Annually.

   Recipient Email Address

   Add and edit the email addresses of the recipients.

   Note

   - You can check **Site Owner's Email** to send a copy of the report to your customer.
   - Up to 4 email addresses can be added.

   Report Language

   Choose a language for the report. The report is now available in 39 languages.
4. Click **OK**.
5. Enable the settings.
   - To enable the settings for one site, switch on **Enable** for the site.
   - To enable the settings for all sites, switch on **Enable All** in the upper-right corner.

   The platform will generate and send reports according to the settings.

Note

If there are more than three site owners, only the first three can be displayed on the report while the others will be displayed as "…".

6. Optional: On the Search filled, enter the keywords and click 🔍 to search for specific sites.
7. Optional: Click **Report Sample** to view a report sample.

7.4 Network Topology

If you have added network switch(es) to a site and connected devices to the network switch(es), you can view their network topology. Network topology displays the network links between devices and shows link exceptions and abnormal devices, which helps you to locate exception sources and troubleshoot faults visually.

Note

- Make sure you have the configuration permission of the network switch, otherwise network topology will be unavailable. For details about applying for the 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 heath monitoring service for devices, see ***Activate the Health Monitoring Service for Devices***.

You can enter the network topology page in the following ways:

- Move your cursor to the **Site & Device** tab. Select **Customer Site** to enter the Site page. And click ⇆ to switch to site mode. Then click the name of a site to enter the site details page, and then click **View Topology**.

  Note

  If you have NOT enabled the Health Monitoring service for the network switch, you can enter the network topology page in this way only.

- On the navigation bar, click **Site & Device** → **Health Monitoring** → **Health Status**, select **All Sites** from the site list, and then select **Network Switch**, and then click ⊞ in the Operation column in the network switch list.
- On the navigation bar, click **Site & Device** → **Health Monitoring** → **Health Status**, select a site from the site list to enter the site details page, and then click **Topology**.

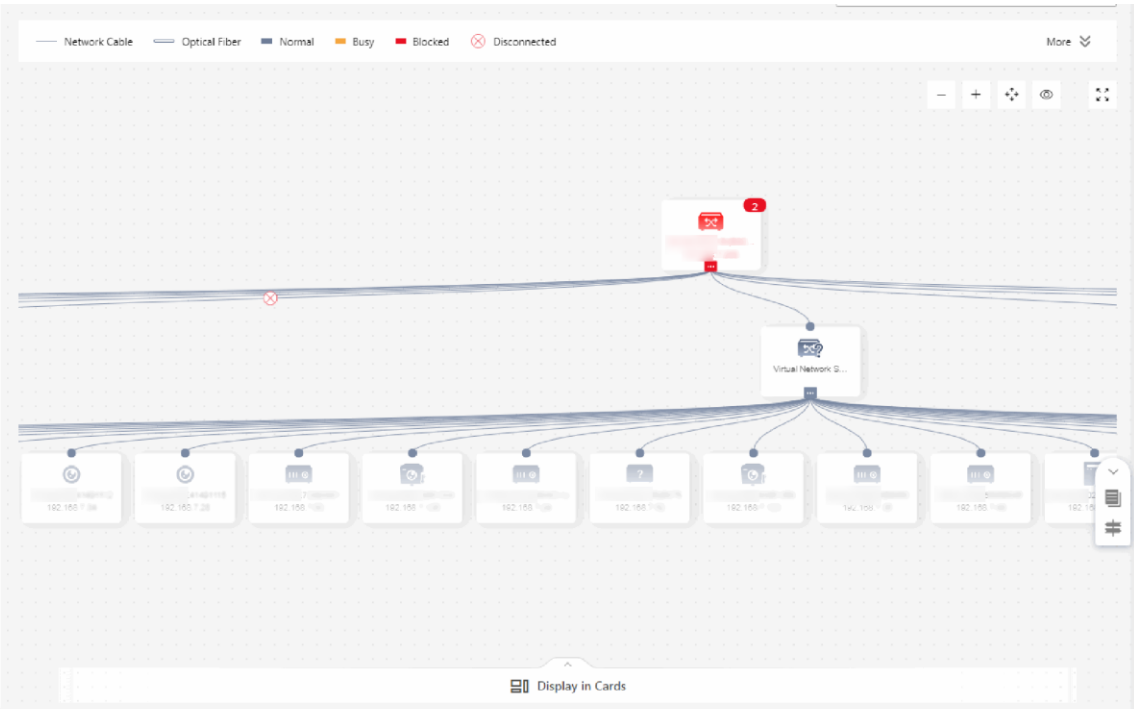
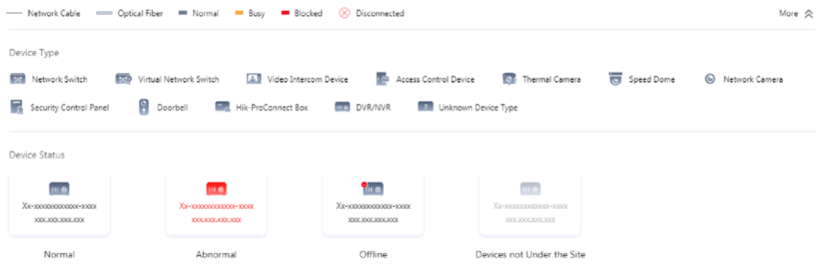
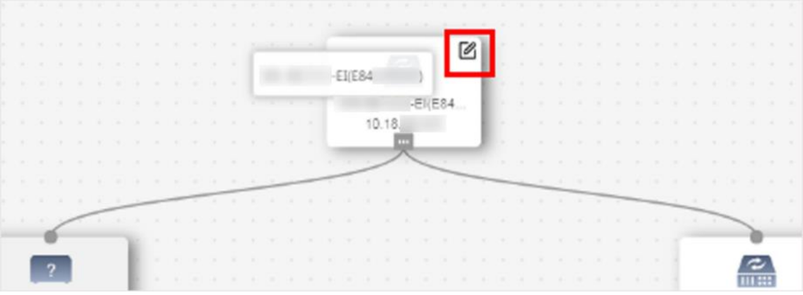
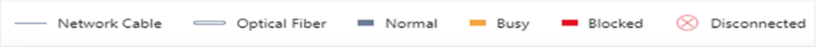


Figure 7-2 Network Topology

The following table shows the descriptions of the available operations on network topology.

Table 7-2 Available Operations

Operation	Description
View Legend	You can click ︾ next to **More** to view the legends.  Network Cable Optical Fiber Normal Busy Blocked Disconnected More Device Type Network Switch Virtual Network Switch Video Intercom Device Access Control Device Thermal Camera Speed Dome Network Camera Security Control Panel Doorbell Hik-ProConnect Box DVR/NVR Unknown Device Type Device Status Normal Abnormal Offline Devices not Under the Site **Figure 7-3 Legend**
Edit Root Node	When multiple network switches are added to a site, the platform will randomly select one of them as the root node by default for the network topology. If the randomly selected network switch is not the real root node, you can hover the cursor over the current root node, and then click ✎ to select a network switch as the root node.

Operation	Description
	 **Figure 7-4 Edit Root Node**
Refresh Topology	Click **Refresh** to refresh the topology structure. **Note** The device status will not be refreshed.
Display in Cards	If you want to view more device status information of all the devices connected to the network switch(es), click **Display in Cards** to display device information in cards.
Move Network Topology	Drag the network topology to move it.
Zoom In/Out	You can click +/ − in the upper left corner to zoom in/out the topology.
Adjust Topology Size	You can click ✥ in the upper left corner to fit the topology size into the display window. You can click ⛶ in the upper left corner to display the topology in full-screen mode.
Display Thumbnail	If you have zoomed in the topology to a large scale, you can click 👁 to show the thumbnail which shows the current cursor location on the topology.
Search Devices in Topology	You can enter the keyword of a device to search for it on the topology. Once the device is found, the topology will pan and zoom automatically to display the found device.
View Link Information	You can view link information based on the legends shown in the figure below.  Network Cable Optical Fiber Normal Busy Blocked Disconnected **Figure 7-5 Link Legend**

Operation	Description
View Link Details	You can hover the cursor over a specific link to view its details, such as the upstream, downstream, port name, and port status.
Apply for Configuration Permission	If you do not have the permission to configure a device, a prompt will pop up asking you to apply for the permission first. You can click **Apply for Permission** to apply for it. **Note** If you do not have the permission, the position of the device in the network topology might be incorrect.
View Network Switch Details and Control It	You can click a network switch on the topology to view the information about the network switch, including basic information, device status, and port status. You can also perform operations such as rebooting the network switch and restarting the port. For details, see ***Network Switch*** and ***View Status of Devices in a Specific Site***. **Note** You cannot view details of a virtual network switch.
View Another Device's Details and Configure It	If an online device is connected to the network switch and added to the same site with the network switch, its device icon and device serial number will be displayed. And you can click the device to view its information including the basic information (e.g., device model) and device status (e.g., network status). You can also click ⚙ to configure device parameters. **Note** ● If an unknown device (e.g., a PC) is connected to the network switch, it will be displayed as . And you cannot view its information. ● If an online device is connected to the network switch but is NOT added to the same site with the network switch, its serial number displayed will be a randomly generated virtual serial number. Its information will be invisible.

Chapter 8. Notification Center

The Notification Center module shows all historical notifications – including device management invitations, site sharing notifications, etc. – and notifications of device or channel exceptions, which help you respond in a timely manner for fluid operation. The module also keeps you informed about system messages – such as the latest version of the system, newly added features, and successful company authentication – as well as the latest deals and offers – such as complimentary service packages and more.

8.1 Exception Center

The Exception Center shows all notifications of device exceptions and channel exceptions.

Note

- 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 in the site which has been assigned to you.
- Device exception messages can be preserved for up to 90 days.
- You need to set the exception rule first. For details, refer to ***Add Exception Rule***.

Go to the **Notification Center** page. Click **Exception Center** to enter the Exception Center page.

Filter Exceptions

You can filter exceptions according to your actual needs.

1. Select a site in the site list to view device exceptions at this site. You can also select a device or a channel to view exceptions that occurred on the device or channel.
2. Set the time period. The exceptions received during this time period will be displayed.
3. Set the handling result from **All Status**, **Not Handled**, **Solved**, **False Alarm**, and **To Be Checked**.
4. Select the exception types that you want to check. The exception types include alarm, exception, and operation.

You can switch on **Auto-Update** so that the latest exceptions received by the Portal will be displayed in the table in real time.

Note

The auto-update will be invalid when viewing history records (including records after page 1 and records received before today).

Handle an Exception

When you have solved an exception or you want to mark it for further examinations, you can select the handling result 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 result on LTS Connect.

Follow the steps below to handle an exception.

1. Click **Handle** in the Operation column to show the Handle Exception pop-up window.
2. Select a handling result in **Result**. You can select from **Solved**, **To Be Checked**, and **False Alarm**.
3. Click **OK** to save the changes.

Batch Handle Exceptions

If the handling results of several devices are the same, you can select multiple exception items and click **Batch Handle** to batch handle them.

Jump to Device Health Monitoring

Click in the Operation column to jump to the device's health monitoring page to troubleshoot the exceptions.

Export Exception Records

After filtering the exceptions, click **Export** and select the format of the file to export these exception records to your local PC.

Note

Currently, the supported formats of the exported file include CSV, Excel, and PDF.

Open in New Window

Click **Open in New Window** in the upper-right corner to open a new window of the browser to view the Exception Center. With this function, you can view the Exception Center and other pages at the same time.

8.2 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).

On the top right of the page, click 🔔 to go to the Notification Center. Click **System Message** to enter the 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.

Employee Joining Application Approved

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

Chapter 9 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.

9.1 Health Monitoring Service

LTS Platinum Partner offers a free package containing a suite of basic features such as viewing the device online/offline status once your complete account registration. In some cases, for the capacity and functionality limitation of the free package, these basic features are insufficient for you to satisfy the higher-level needs of your customers (i.e., end users), such as the maintenance of many devices. Compared with the free package, the health monitoring package not only allows you to add an unlimited number of devices to LTS Platinum Partner, but also monitor the health status of your customers' devices.

The following table shows the comparison of the free package and the health monitoring package.

Table 11-1 Comparison of the Free Package and Health Monitoring Package

Functionality	Free Package	Health Monitoring Package
Site and Customer Management	Supported	Supported
Site Map	Supported	Supported
Add Devices to LTS Platinum Partner	Supported Capacity: 1,024 Devices	Supported Capacity: Unlimited Devices
On-Site Config	Supported	Supported
On-Site Batch Upgrade	Supported	Supported
Device Status	Supported	Supported
Employee Accounts	Supported Unlimited Number of Employee Accounts Employee accounts with permission to manage devices shall be purchased additionally.	Supported Unlimited Number of Employee Accounts Employee accounts with permission to manage devices shall be purchased additionally.
Remote Configuration	Supported	Supported
Remote Live View, Playback, and Video Download	Supported	Supported

Functionality	Free Package	Health Monitoring Package
Remote Device Upgrade	Supported	Supported
Remote Batch Upgrade	Supported	Supported
Real-Time Health Monitoring	NOT Supported	Supported
Device Exception Notification	NOT Supported	Supported
Exception Handling	NOT Supported	Supported
Scheduled Health Check Reports	NOT Supported	Supported
Linkage Rule	NOT Supported	Supported

9.1.1 Purchase Health Monitoring Service

You can purchase the health monitoring service packages from LTS and then activate the service key to get the health monitoring service packages in LPP.

Steps

1. Purchase a service key from LTS
2. click **Activate by Service Key** to get the service package.

Note

- You can activate the health monitoring service for any device types, but the number of devices cannot exceed your package's limit, or you will not be able to use the health monitoring service.
- You can add an unlimited number of devices to LTS Platinum Partner and perform remote configuration, live view, and playback freely.

9.1.2 Activate the Health Monitoring Service for Devices

After purchasing the health monitoring package, you can activate the health monitoring service for any type of devices, if the number of devices is within your current package's limit. Once the service is activated, features such as device health monitoring and device exception notifications will be available for these devices.

Before You Start

Make sure you have purchased health monitoring packages. For details, see ***Purchase Health Monitoring Service***.

Steps

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.

1. Enter the Activate Health Monitoring Service page in one of the following ways.
   - Click the **Site & Device** tab. Go to **Service** → **My Service** → **Health Monitoring Service**. Toggle on the switch in the Operation column to activate a device, or select multiple devices and click **Batch Activate Health Monitoring Service for Devices**.
   - Go to the site details page, hover the cursor over on the device card, then click **Activate Service** on the pop-up dialog.
   - Go to the site details page, click on a device to show the device details panel, then hover the cursor onto on the panel and click **Activate Service**.
   - Click **Activate Service** on the adding result page after adding detected online devices or adding a device by LTS Connect (P2P). See ***Add Detected LAN Device*** or ***Add Device by Entering Serial No.*** for details.

   The health monitoring service is activated, and the notifications of all exceptions will be enabled by default.
2. Optional: If the number of devices with activated health monitoring service reached the package's limit, you can click **Upgrade Service** to purchase a package of higher device capacity.
3. Optional: Perform the following operations on the site details page after activating the service for devices.

View Health Status of Devices	View health status of all devices on the device list, and view health status of a specific device on the device details panel. For details, refer to ***View Status of Devices in All Sites*** and ***View Status of Devices in a Specific Site***.
Inspect Devices	● Click **Refresh** to inspect all the devices in the site. ● Select a device and then click to inspect it.
Diagnose Devices of the Site	Click **Health Check** to open the Health Check window, and click **Check Now** to diagnose the devices of the site. When the checking completed, you can view the status of each device in the site. For NVR, and DVR, you can click **View Report** to export the diagnostics report as a PDF file to the local PC.

9.1.3 Manage Your Health Monitoring Service

In My Service, you can manage your health monitoring packages.

Go to **Service** → **My Service** → **Health Monitoring Service** to enter the health monitoring service page.

Package

On this page, you can manage your premium, professional, and expert packages.

Table 11-2 Available Features

Area No.	Feature	Description
1	View Remaining Packages & Purchase More	You can check the current number of devices for which the health monitoring service is activated, and the remaining number of devices for which the service can still be activated. Click **Activate by Service Key** or **Online Purchase** to purchase more premium, professional, and expert packages. For details, see ***Purchase Health Monitoring Service***.
2	Search by Keywords	Select a site from the site list on the left, and then enter keywords to search for devices.
2	Activate Service	Toggle on the switch in the Operation column to activate the service for the device. Or select multiple devices, and then click **Batch Activate Health Monitoring Service for Devices**.

Inventory

On this page, you can manage remaining monthly / annual packages for all devices, and/or network camera monthly / annual packages. If you do not have these remaining packages, this page will not be available to you.

Table 11-3 Available Features

Area No.	Feature	Description
1	View Remaining Packages & Purchase More	View the used number and remaining numbers of each type of heath monitoring packages. Click **Activate by Service Key** to purchase more all-type device monthly/annual packages, and network camera monthly/annual packages.
2	View Expiration and Auto Renewal Information	● **Expires in 30 Days**: The number of devices whose health monitoring services expire in 30 days. You can click **Expires in 30 Days** to view these devices in the device list below. ● **Expired**: The number the devices whose health monitoring services have expired. You can click **Expired** to view these devices in the device list below. ● **Devices with Auto Renewal**: The number of

Area No.	Feature	Description
		devices for which you have enabled service auto-renewal. You can click **Devices with Auto Renewal** to view these devices.
3	Filter Devices or Search by Keywords	Select a site from the site list on the left, and then select filter criteria (All, Expire in 30 Days, Expired, or Devices with Auto Renewal) from the drop-down list to filter devices. Or enter keywords to search for devices.
3	Activate Service	Click **Activate Health Monitoring Service** to activate the heath monitoring service for specific devices.
3	Batch Renew Service for Devices	Select devices and then click **Batch Renew** to renew the service for the selected devices. The process of renewing the service is similar to that of activating the service.
3	Renew Service for a Device	Click 🕒 in the Operation column to renew service for a device. The process of renewing the service is similar to that of activating the service.
3	Transfer Service	Click ⇄ in the Operation column to transfer the remaining service time from the current device to another.
3	Enable Service Auto Renewal	Click 🔄 in the Operation column to open the Auto Renew window, switch on **Auto Renewal**, and then select a type of service packages for auto renewing the health monitoring service.

9.2 Purchase Employee Account Add-On

LTS Platinum Partner offers only one Installer Admin account for your company to manage resources in the system. You can invite more employees to join LTS Platinum Partner to work collaboratively. By default, the status of employees is limited and some operations like managing sites are not available to them. However, the account limits can be removed by purchasing the employee account add-on. You can purchase the employee account add-on from LTS and then activate the employee account add-on by the service key.

9.3 Co-Branding

This feature helps improve the visibility of your brand, products, and services. It allows your customers to view some basic information of your company on the startup and live view page of NVRs / DVRs and the LTS Connect Mobile Client.

- A window with notifications about getting the co-branding service for free will pop up when your co-branding service expires in 2 months.
- You can get the co-branding service for free after purchasing the annual type of health monitoring packages (including All Device Annual Package and Network Camera Annual Package) for the first time. For details about how to purchase health monitoring packages, see ***Purchase Health Monitoring Service***.

9.3.1 Purchase Co-Branding

You can purchase co-branding service packages from LTS and activate them by entering service keys.

Note

- Make sure you get your company authenticated. For details, see ***Authenticate Company***.

Go to **Service** → **Company Management**. In the Co-Branding area, purchase the service packages online or activate the services by service keys.

9.3.2 Enable Co-Branding

If you enable the co-branding service, customers such as end users can view your company information, including logo, address, and phone number, on the startup and live view pages of NVRs / DVRs and the LTS Connect Mobile Client.
Go to **Company Management** → **Co-Branding**. Switch on **Service Status**, and then hover the cursor onto the Logo area to show the **Edit** button. And finally click **Edit** to upload your company logo.

Note

- If all the devices of your customer are managed by the same installation company, the installation company's logo will be displayed on the startup and live view page of NVR/DVR, the login page and About page of your customer's LTS Connect Mobile Client.
- If your customer's devices are managed by different installation companies, your customer can go to the device details page on the startup and live view page of NVR/DVR, LTS Connect Mobile Client to view the companies' logo and details.

Chapter 10 Support

In the Support module, you can find tools to improve your work efficiency.

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

10.1 Tools

LTS Platinum Partner provides tools to help you improve your work efficiency.
On the LTS Platinum Partner page, click **Tools** on the left pane to enter your tools page.

Disk Calculator

The tool is used to calculate the recording time and recording space by setting related parameters.

Bandwidth Calculator

The tool is used to calculate the required bandwidth of a network camera or NVR by setting parameters such as channel number and resolution.