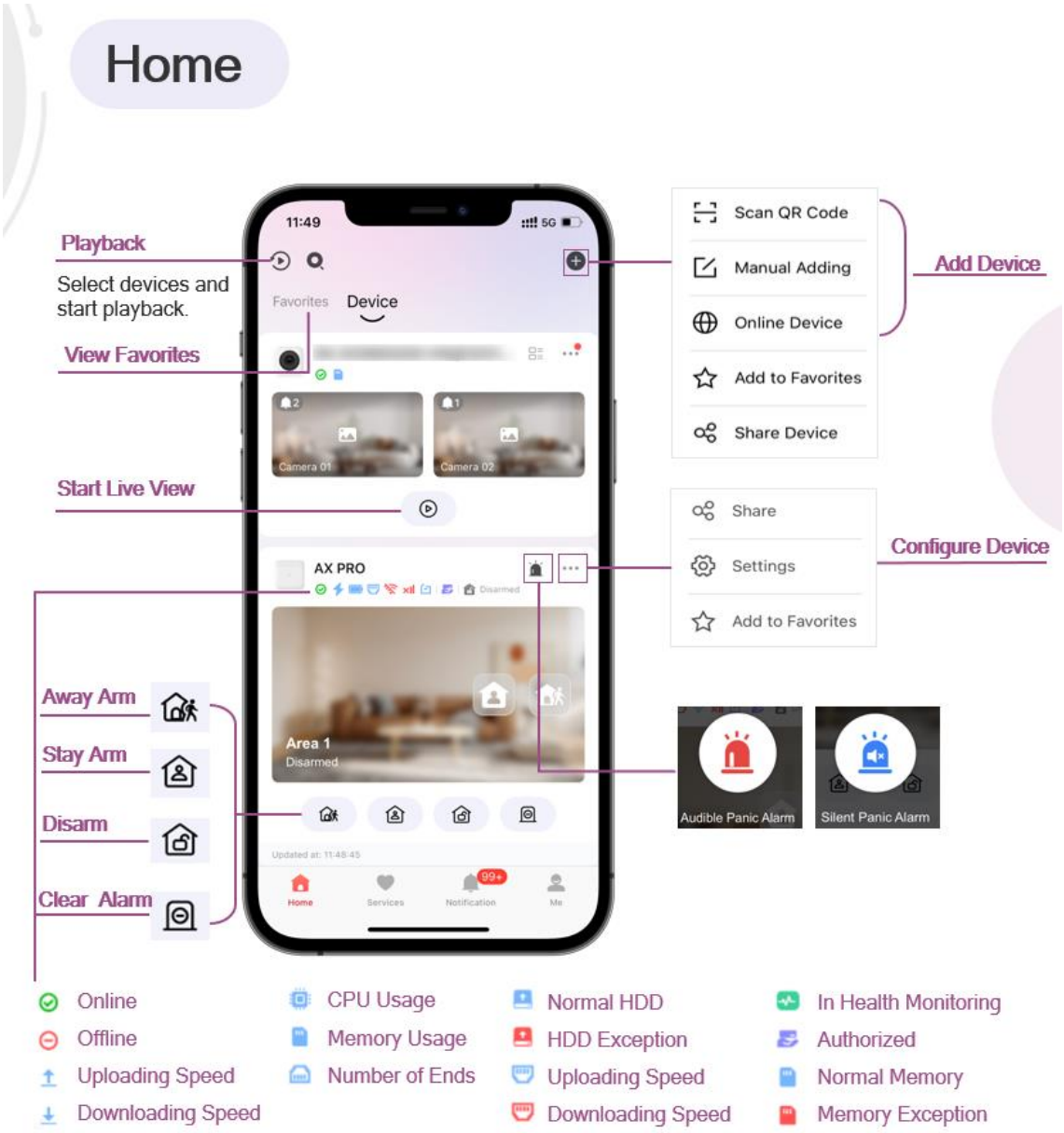
LTS Connect Mobile Client

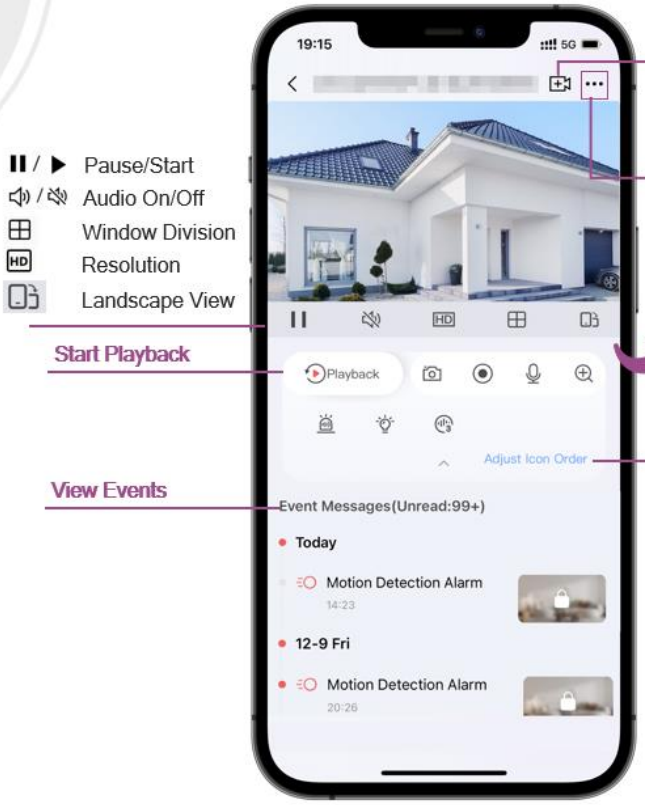
User Manual

Contents

Chapter 1 Quick Start Guide



Live View



Pause/Start

Audio On/Off

Window Division

Resolution

Landscape View

Start Playback

View Events

Add Device for Live View

Add a device and swipe the live view image to view the live image of another device

Share — **Share the Device**

Settings — **Set Device Parameters**

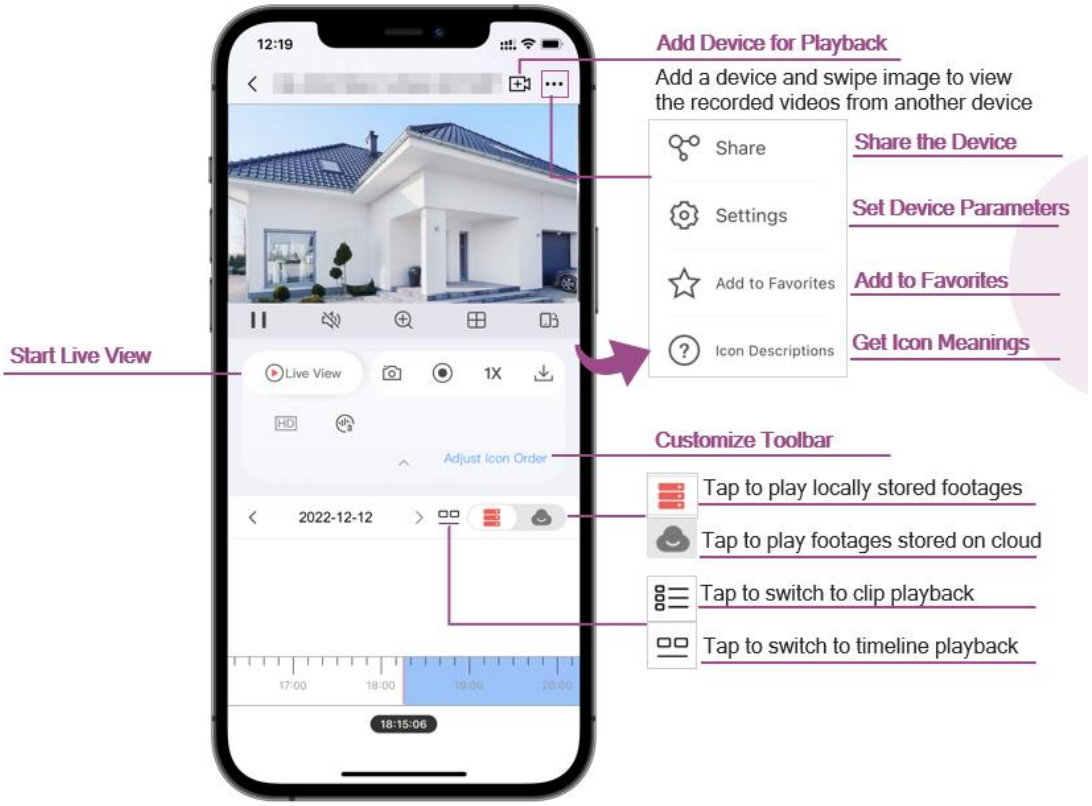
Add to Favorites — **Add to Favorites**

Icon Descriptions — **Get Icon Meanings**

Customize Toolbar

Note:
When there are multiple windows, double tap a window to enlarge it, and double tap again to go back to multiple windows.

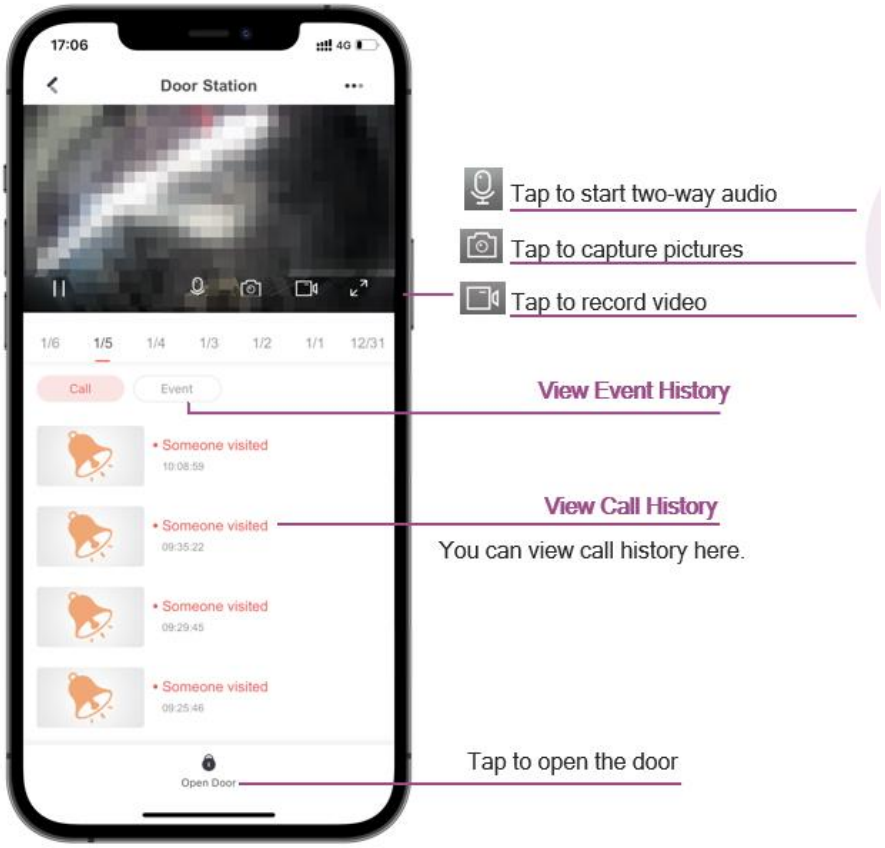
Playback


Add Device for Playback
Add a device and swipe image to view the recorded videos from another device
Share
Share the Device
Settings
Set Device Parameters
Add to Favorites
Add to Favorites
Icon Descriptions
Get Icon Meanings
Start Live View
Live View
1X
HD
Adjust Icon Order
Customize Toolbar
2022-12-12
Tap to play locally stored footages
Tap to play footages stored on cloud
Tap to switch to clip playback
Tap to switch to timeline playback
17:00
18:00
19:00
20:00
18:15:06


Security Control
Share Device
Configure Device
Check System Faults
Audible Panic Alarm
Silent Panic Alarm
View Areas
View Peripherals and Detectors
View Security Panel Status
Arm or Disarm an Area
Add Area
Multiple selection
Away Arm
Stay Arm
Disarm
Clear Alarms
16:07
AXPRO
Area
Device
Status
Area 1
Stay
Area 2
Stay
Area 3
Stay
Area 4
Stay

Access Control

Intercom


17:06
Door Station
Tap to start two-way audio
Tap to capture pictures
Tap to record video
1/6 1/5 1/4 1/3 1/2 1/1 12/31
Call
Event
View Event History
• Someone visited
10:08:59
• Someone visited
09:35:22
View Call History
You can view call history here.
• Someone visited
09:29:45
• Someone visited
09:25:46
Open Door
Tap to open the door

Chapter 2 About LTS Connect

LTS Connect is used to remotely control devices (NVRs, DVRs, network cameras, indoor stations, doorbells, security control panels, access control devices, etc.) via Wi-Fi or cellular network.
The Mobile Client provides access to the LTS Connect service, which is a cloud service developed by LTS, to manage your devices.

Note

Network traffic charges may be incurred during the use of the Mobile Client. Consult your local carriers for details.

2.1 System Requirements and Conventions

System Requirement

Android 5.0 / iOS 10.0 or later.

Conventions

In the following chapters, this manual simplifies LTS Connect Mobile Client as "Mobile Client", device such as DVR, NVR, encoder, and network camera as "device", and device which supports being added to LTS Connect service as "LTS Connect Device".

2.2 Summary of Changes

See detailed descriptions on feature changes on the Mobile Client in ***LTS Connect Mobile Client Release Notes***.

Chapter 3 Device Management

You need to add devices to the Mobile Client before you can do further remote operations such as live view and playback.
The devices added to the Mobile Client will be displayed in the device list.

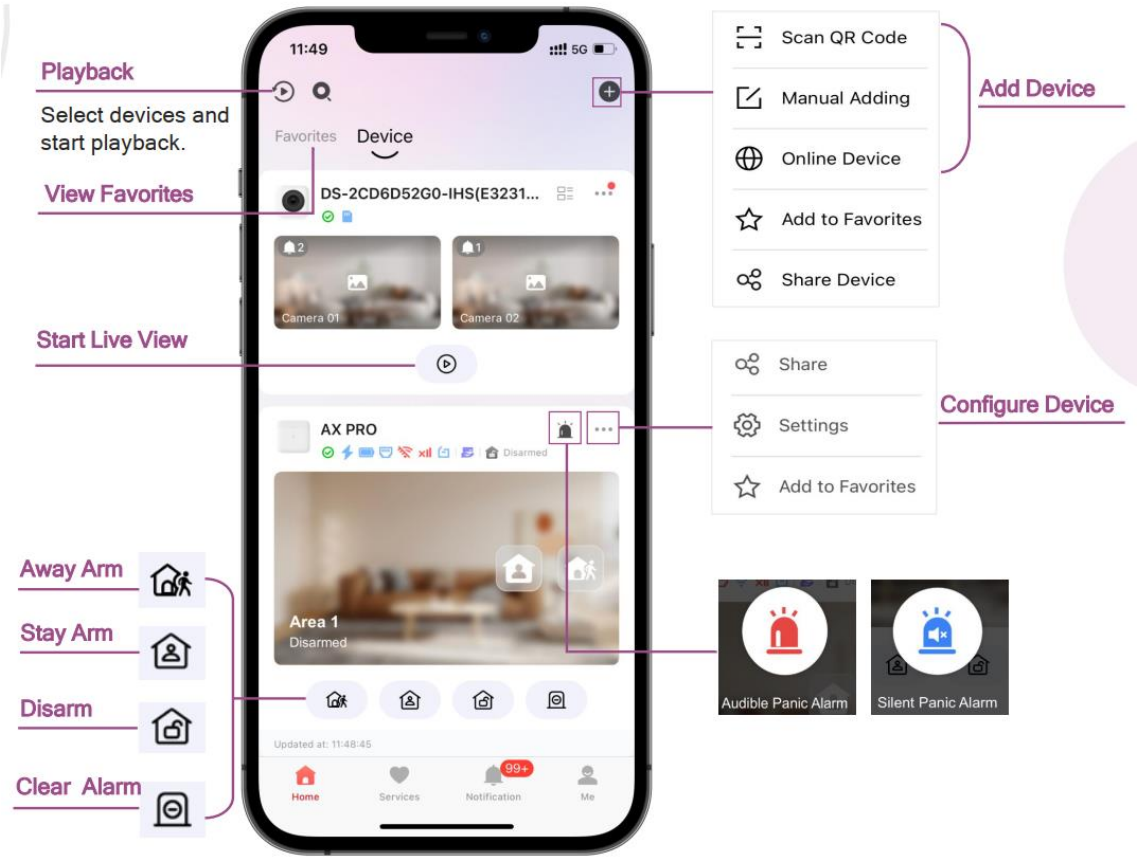


Figure 3-1 Device List

3.1 Add Device for Management

You need to add devices to the Mobile Client first so that subsequent operations such as live view and playback can be available. If you want to receive alarm event information from a device, you should add it by scanning QR code or LTS Connect domain.

Note

- For details about adding Pyronix control panel, see ***Add Pyronix Control Panel to Mobile Client***.
- For details about managing alarm event information, see ***Notification***.

3.1.1 Add an Online Device

The Mobile Client can detect the online devices in the same local area network with your phone or tablet, and you can add the detected online devices to the Mobile Client.

Before You Start

Make sure the devices are connected to the same local area network with the phone or tablet.

Steps

1. On the device list page, tap ⊕ → **Online Device** to enter the Online Device page.
   All detected online devices will be in the list.
2. Select a device for adding.

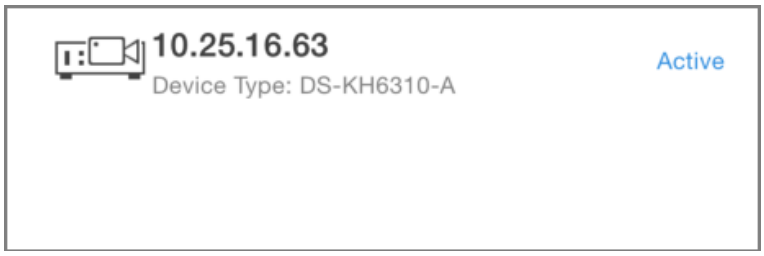


Figure 3-2 Online Device

Note

- For network cameras, make sure the device Multicast Discovery function is enabled so that the online network camera can be automatically detected via private multicast protocol in the LAN. For details, see User Manual of the network camera.
- For the inactive device (excluding the access control device), tap **Active** to create a password for it before you can add the device properly. For more information about the device activation, see ***Set a Password to Activate a Device***.

3. Optional: Edit the network information.
   1) Tap ✎.
   2) Change the device IP address to the same LAN as your phone's by either editing the IP address manually or enabling the device DHCP function.
   3) Tap 💾 and input the admin password of the device to save the settings.
4. Tap **Add**.
5. Enter the required information, including device alias, user name and the password.
6. Tap 💾.
7. Optional: Tap the device name or tap ⋯, and then tap **Delete Device**.

3.1.2 Add Device(s) by Scanning Device QR Code

You can add the device by scanning the device's QR code. You can also add device(s) by scanning

the QR code obtained via the web page of the device.

Steps

1. On the device list page, tap → **Scan QR Code** to enter the Scan QR Code page.
2. Scan the QR code / bar code.
   – Scan the QR code or bar code by aligning the QR Code with the scanning frame.

   Note
   - Usually, the device QR code is printed on the label, which is on the back cover of the device.
   - Tap to enable the flashlight if the scanning environment is too dark.

   – If there are QR codes in photo album of the phone, tap to extract QR code from local album.
3. Optional: Perform the following operations if the following situations occur.
   – If the system fails to recognize the QR code, tap to add the device manually.
   – If the device has been added to another account, you should unbind the device from the account first. See ***Unbind Device from Its Original Account*** for details.
   – If the device is offline, you should connect a network for the device. For details, see ***Connect Offline Device to Network*** for details.
   – If the device is not activated, the Activate Device page will pop up (excluding the access control device). You should activate the device. For details, see ***Set a Password to Activate a Device*** for details.
   – If the LTS Connect service is disabled for the device, you should enable the function (excluding the access control device). For details, see ***Enable LTS Connect Service When Adding Device on Mobile Client*** for details.
4. Tap **Add** on the Result page.
5. Enter the device verification code.
   The device will be added successfully.

   Note
   - The default device verification code is usually on the device label. If no verification code found, enter the device verification code you created when enabling LTS Connect service.
   - For details about enabling LTS Connect service, see ***Enable LTS Connect Service for Device***.

6. Optional: Tap **Configure DDNS** to configure DDNS.

   Note
   - See ***Set DDNS*** for details.
   - After DDNS being enabled, the device will be accessed via IP address in priority, so that remote configuration of the device will be supported and the streaming speed will be faster than streaming via LTS Connect service.
   - If you skip this step, the device will be accessed via LTS Connect service.

7. Tap **Finish**.

3.1.3 Add a Device by IP/Domain

You can add the device by fixed IP address or domain name. The streaming speed of devices added by IP/domain is faster than those added by LTS Connect domain.

Before You Start

If you want to add the access control device, activate it before adding. See the user manual of the access control device for details.

Steps

1. Tap ⊕ and select **Manual Adding**.
2. Select **IP/Domain** as the adding type.
3. Enter the required information, such as alias, address, user name, camera No. and device password.

   Address

   Device IP address or domain name.

   Camera No.

   The number of the camera(s) under the device can be obtained after the device is successfully added.
4. Tap 💾 to add the device.

Note

- If the device is offline, you should connect the device to a network. For details, see ***Connect Offline Device to Network***.
- If the device is not activated, the Activate Device page will be popped up (exclude the access control device). You should activate the device. For details, see ***Set a Password to Activate a Device***.

3.1.4 Add a Device by LTS Connect Domain

For devices which support LTS Connect service (a cloud service provided by LTS), you can add them manually by LTS Connect domain.

Before You Start

Make sure the device is powered on.

Steps

1. On the device list page, tap ⊕ → **Manual Adding** to enter the Add Device page.
2. Select **LTS Connect Domain** as the adding type.
3. Enter the device serial No. manually.

Note

- By default, the device serial No. is on the device label.

- For the video intercom devices, when entering the serial No. of the indoor station, the corresponding door station will also be added to the Mobile Client automatically.
- An indoor station can be linked to multiple door stations.

4. Tap .

Note

- If the device has been added to another account, you should unbind the device from the account first. See ***Unbind Device from Its Original Account*** for details.
- If the device is offline, you should connect a network for the device. For details, see ***Connect Offline Device to Network*** for details.
- If the device is not activated, the Activate Device page will pop up (excluding the access control device). You should activate the device. For details, see ***Set a Password to Activate a Device*** for details.
- If LTS Connect service is disabled for the device, you should enable the function (excluding the access control device). For details, see ***Enable LTS Connect Service When Adding Device on Mobile Client*** for details.

5. Tap **Add** on the Result page.
6. Enter the device verification code.
   The device will be added successfully.

Note

- The default device verification code is usually on the device label. If no verification code found, enter the device verification code you created when enabling LTS Connect service.
- For details about enabling LTS Connect service, see ***Enable LTS Connect Service for Device***.

7. Optional: Tap **Configure DDNS** to configure DDNS.

Note

- See ***Set DDNS*** for details.
- After DDNS being enabled, the device will be accessed via IP address in priority, so that remote configuration of the device will be supported, and the streaming speed will be faster than streaming via LTS Connect service.
- If you skip this step, the device will be accessed via LTS Connect service.

8. Tap **Finish**.

3.2 Set a Password to Activate a Device

When adding a device, if the device is not activated, a window will pop up to ask you to activate

the device.

Before You Start

The device to be activated and the phone running the Mobile Client should be on the same LAN.

Steps

1. Add a device.
2. On the Activate Device page, tap **Set Device Password**.
3. Create a password.

Note

If you forget the password in the future, you might need to reset the device.

4. Tap **Activate** to activate the device.
5. Enable DHCP or manually configure network if you enter the Network Configuration page.

3.3 Connect Offline Device to Network

When adding a device to the Mobile Client, if the device is offline, you should connect the device to a network first. The Mobile Client provides the following four methods for connecting offline devices to networks.

Connect to Wired Network

Use this method if a router is available for the device to connect to.

Note

Make sure the device is powered on.

Connect to Wireless Network

Use this method if a wireless network is available for the device to connect to. "Device" here excludes wireless doorbell, wireless security control panel, and Mini Trooper (a kind of battery camera).

Note

- Make sure your phone has connected to a Wi-Fi network before using the method.
- The device should support connecting to wireless network.

Connect to Network by Wi-Fi Configuration

You can use this method to connect wireless doorbell to the network by using the doorbell to scan the QR code generated by the Mobile Client.

Tap **Connect to a Network** on the Result page and then follow the instructions on the subsequent pages to connect the device to the network.

Connect to Network by Access Point

In the Mobile Client, Access Point (AP) refers to a networking hardware device (e.g., wireless doorbell or wireless security control panel), which can provide a Wi-Fi network for the phone to connect to.

Note

Make sure you have turned on WLAN in the phone's operation system.

Tap **Connect to a Network** on the Result page, select **Wireless Connection** as the connection type, and then follow the instructions on the subsequent pages to complete the connection process.

3.4 Enable LTS Connect Service for Device

LTS Connect service is a cloud service provided by LTS. When adding a device via LTS Connect Domain or scanning QR code, the service should be enabled. You can enable the service via the Mobile Client, the device web page, or Lts-Partner Pro client software. This section introduces how to enable the service via the former two methods.

3.4.1 Enable LTS Connect Service When Adding Device on Mobile Client

When adding a device via LTS Connect domain or scanning QR code, if the LTS Connect service is not enabled for the device, the Enable LTS Connect Service window will pop up to remind you to enable the service first.

Perform the following task to enable the LTS Connect service in this case.

Steps

1. Add a device via LTS Connect domain or scanning QR code.

   Note

   See ***Add a Device by LTS Connect Domain*** or ***Add Device(s) by Scanning Device QR Code*** for details.

   If the device's LTS Connect service is not enabled, the following window pops up.
2. On the Enable LTS Connect Service window, tap **LTS Connect Terms of Service** to read the terms of service.
3. Check **Read and Agree LTS Connect Terms of Service**.
4. Tap **Next**.
5. Create a device verification code.

   Note

   You can change the device verification code. See ***Change Device's Verification Code*** for details.

6. Tap **Enable LTS Connect Service**.

What to do next

Continue the process for adding the device. See ***Add a Device by LTS Connect Domain*** or ***Add Device(s) by Scanning Device QR Code*** for details.

3.4.2 Enable LTS Connect Service on Device Web Page

You can enable LTS Connect service for a device on the device web page.

Steps

1. Visit the device IP address on the web browser.
2. Enter the device user name and device password to log in to the device web page.
3. Tap **Configuration** → **Network** → **Advanced Settings** → **Platform Access** to enter the Platform Access page.

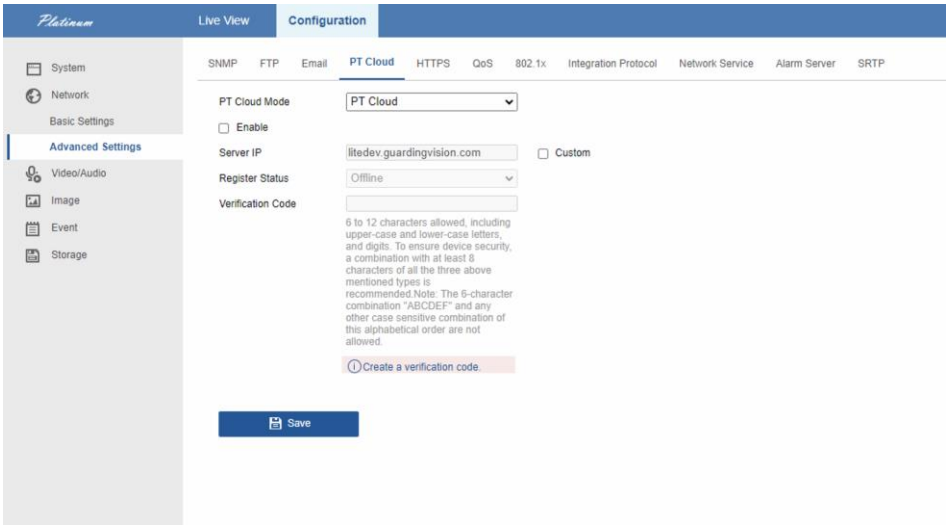


Figure 3-3 The Platform Access Page

4. Check **Enable**.
   The system will set LTS Connect as the platform access mode by default.
5. Optional: If it is the first time to enable the LTS Connect service, create a device verification code.
6. Tap **Save**.

3.5 Enable DHCP Function on Device Web Page

You can enable DHCP by following the steps below to allow allocating DNS address automatically.

Steps

1. Visit the IP address of the device.
2. Enter the device user name and device password and log in to the device's web page.
3. Click **Configuration** → **Network** → **Basic Settings** to enter the Basic Settings page.

4. Enable **DHCP**.
   DNS address will be allocated automatically.
5. Click **Save**.

3.6 Unbind Device from Its Original Account

When adding a device by scanning QR code or LTS Connect domain, if the result shows that the device has been added to another account, you should unbind it from the account before you can add it to your account.

Before You Start

Make sure the device and the phone running the Mobile Client are in the same local area network.

Steps

1. Add the device by scanning QR code or LTS Connect domain.

   See ***Add Device(s) by Scanning Device QR Code*** or ***Add a Device by LTS Connect Domain*** for details.
2. On the Result page, tap **Unbind Device** to start unbind the device from its account.
3. Optional: If the network exception occurs, perform the following operations.
   – Tap **Connect to Wi-Fi** to connect the phone to the Wi-Fi network and make sure the device is in the same local area network with the phone.
   – Tap **Or you can unbind the device from its account in local GUI** to unbind the device via local GUI.

   Note

   Unbinding the device via local GUI should be supported by the device.
4. On the Unbind Device page, enter the device password and the verification code displayed on the image.
5. Tap **Finish**.

3.7 Device Sharing

You can share devices to other users. The recipient can access the devices according to the permissions you grant them. You can also receive and use the devices shared by other users.

3.7.1 Share a Device via Its QR Code

You can share a device to another LTS Connect user via the device's QR code. You can also select the device permissions granted to the recipient to determine which operations the recipient can

perform on the device.

Steps

1. In the device list, find a device you want to share, and tap ··· → **Share** on the device card.
2. Tap **Share with User**.

Note

You can share the device with a service provider to let the service provider set up and manage your device. See details in ***Invite a Service Provider to Manage Devices***.

3. Tap **Share via QR Code**.
4. Select the device permissions to be shared with the recipient.
   – Check **All Permissions** to grant all available permissions to the recipient.
   – Tap the device name, and then select permissions to grant the selected ones to the recipient, and finally tap .

   Example

   For example, if you select Live View and Remote Playback, the recipient will have the permissions to view live video and play back the video footage of the device.
5. Let the recipient use the LTS Connect Mobile Client to scan the QR code.
   The recipient needs to send a device sharing application to you. You will receive a notification about the application on your Mobile Client.
6. Agree the device sharing application from the recipient.
   - The device will be shared to the recipient. The recipient will be able to view the device on the device list.
   - The next time you want to share devices to this recipient, you can select the recipient in the History Recipient list.
7. Optional: Perform further operations.

Edit Device Permissions	1. Go to **Me** → **Manage Sharing Settings**. 2. Tap the device and then edit the device permissions granted to the recipient.
Stop Sharing	1. Go to **Me** → **Manage Sharing Settings**. 2. Tap the device to enter the Sharing Details page and then tap **Delete**.

3.7.2 Share Multiple Devices by Scanning Recipient's Account QR Code

You can share multiple devices to another LTS Connect user. You can also set the device permissions granted to the recipient to determine which operations the recipient can perform on

the device.

Steps

1. Tap ⊕ → **Share Device**.
2. Tap **Share with User**.

> **Note**
>
> You can share the device with a service provider to let the service provider set up and manage your device. See details in ***Invite a Service Provider to Manage Devices***.

3. Tap **Scan QR Code**.
4. Scan the QR code of the recipient's account.

> **Note**
>
> The recipient needs to go to **Me** → **Account Management** → **My QR Code** on the Mobile Client to get the QR code of his/her account.

5. Select the devices you want to share, and then tap **Next**.

> **Note**
>
> For devices linked with multiple cameras, you can select the cameras for sharing.

6. Select the device permissions to be shared with the recipient.
   - Check **All Permissions** on the Sharing Details page to select all the permissions.
   - Tap the device displayed on the Sharing Details page, and then select permission(s) and tap 💾.

   Example

   For example, if you select Live View and Remote Playback, the recipient will have the permissions to view live video and play back the video footage of the device.
7. Tap **Finish** to finish sharing.
   A notification about the sharing will appear on the recipient's Mobile Client. The recipient needs to accept the shared devices.
8. Optional: Perform further operations.

Edit Device Permissions	1. Go to **Me** → **Manage Sharing Settings**. 2. Tap a device and then edit the device permissions granted to the recipient.
Stop Sharing	1. Go to **Me** → **Manage Sharing Settings**. 2. Tap a device to enter the Sharing Details page and then tap **Delete**.

3.7.3 Silenced Mode for Devices Shared by Others

You can enable Silenced mode for the devices shared by others if you don't want to be disturbed by the devices' alarm notifications. When enabled, all the alarm notifications triggered by the device(s) will be silenced. And you can still check the information of all the silenced alarm notifications from the devices on the notification list.
Tap ··· → **Settings** to enter the Settings page of the device and then enable the Silenced mode.

3.8 Favorites Management

You can add the frequently-used camera(s) to the favorites so that you can access them conveniently.

3.8.1 Add Cameras to Favorites on Home Page

On the device list page, you can add the frequently-used camera(s) to the favorites so that you can access them conveniently.

Steps

1. You can add one or more devices to Favorites.
   – On the home page, tap ⊕ → **Add to Favorites**, and select devices and cameras.
   – On a specific device card, tap ··· → **Add to Favorites** to add a selected device to Favorites.
2. Select devices and cameras on the Select Camera page.
3. Tap **OK**.
4. Create a name for the Favorites and then tap **OK**.

Note

- Up to 32 favorites can be added.
- The favorites name should be no more than 32 characters.

   The Favorites tab will be displayed near the Device page.
5. Optional: Tap the Favorites name on the Favorites page to edit name and involved cameras.
6. Optional: Tap the ··· → **Sort** on the Favorites page to sort favorites.

3.8.2 Add Cameras to Favorites During Live View

On the live view page, you can add frequently-used cameras to Favorites so that you can access them conveniently

Steps

1. Enter the Live View page.

Note

For details about how to enter the Live View page, see ***Start and Stop Live View***

2. Tap ••• and tap **Add to Favorites**.
3. Add cameras to favorites.
   – Create a new favorites in the pop-up window and tap **OK**.
   – Add to an existing favorites group. Tap **Add to Existing Favorites** in the pop-up window. Then select a Favorites folder in the list.

Note

- Up to 32 Favorites can be added.
- The favorites name should be no more than 32 characters.

4. Optional: Tap the Favorites on the device list page to view the cameras' live videos.

3.8.3 Remove Cameras from Favorites

You can delete cameras in the favorites.

Steps

1. Tap **Favorites** on the Home page.
2. Tap a Favorites folder.
   Cameras that are added to the favorites folder are displayed.
3. Tap ⊖ and then **Delete** to remove a camera from Favorites.

3.9 Configure Your Device

On the Settings page of a device, you can view and edit the device's basic information, delete the device, upgrade device firmware, and configure other functions such as video and image encryption and changing device verification code.

Note

The available functions on the Settings page vary with different device types and device models.

3.9.1 Change Device's Verification Code

The device verification code is used for verifying user identity, as well as encrypting a device's videos (including live videos and recorded video files) and captured pictures. You can change the device verification code for the network camera and Mini Trooper (a kind of camera powered by

battery).

Steps

Note

For details about how to encrypt a device's videos and captured pictures, see ***Set Video and Image Encryption***.

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Tap **Change Verification Code**, and then tap **Edit** on the pop-up Window to enter the Change Verification Code page.
3. Enter the old verification code, and then tap **Next**.
4. Create a new verification code, and then confirm it.

Note

If you have enabled the Video and Image Encryption function, new pictures and videos will be encrypted by the new verification code. However, the earlier encrypted pictures and videos still use the old verification code.

3.9.2 Set Video and Image Encryption

For security reasons, you can set the video and image encryption function to encrypt the videos or the pictures.

Steps

Note

- If you set the video and image encryption function, the device's live video, recorded video, and pictures in event information will be encrypted. You should enter the device verification code the first time you entering these pages.
- If you log in to the Mobile Client with the same account on another phone, you should enter the device verification code again to view the live video, the recorded video, and pictures in event information.

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Set the Video and Image Encryption switch to ON to enable the function.
3. Optional: Change the encryption password (device verification code).
   1) Tap **Change Password**.
   2) Tap **Edit** in the pop-up window to enter the Change Password page.
   3) Follow the instructions on the page to change the device verification code.

Note

The default device verification code is usually on the device label. If no verification code found, enter the device verification code you created when enabling LTS Connect service. For details about enabling LTS Connect service, see ***Enable LTS Connect Service for Device***.

3.9.3 Set DDNS

For a device added via LTS Connect Domain or Scanning QR code, if DDNS is enabled, the device's streams will be accessed via IP address in priority. In this case, you can remotely configure device and the speed of streaming will be faster than that of streaming via LTS Connect service.

Steps

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. On the Settings page, tap **Configure DDNS** to enter the Configure DDNS page.
3. Set the required information.

Device Domain Name

The default device domain name is the serial number of the device. If you want to edit it, the edited domain name should contain 1 to 64 characters, including numbers, lowercase letters, and dashes. And it should start with a lowercase letter and cannot end with a dash.

Port Mapping Mode

For details about setting port mapping, tap **How to Set Port Mapping**.

Note

The entered port number should be from 1 to 65535.

User Name

Enter the device user name.

Password

Enter the device password.

4. Tap .

3.9.4 Upgrade Device Firmware

You can upgrade the firmware of a device to its latest version. If the latest version is detected, a red dot will appear on the Device Version field of the Settings page of the device.

Steps

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Tap **Device Version** to enter the Device Version page.
3. Tap **Upgrade**.

The Mobile Client will download the upgrade file first and then start upgrading the device.

Note

You can also enable the Mobile Client to automatically download the upgrade file in Wi-Fi networks once a new device version is detected.

3.9.5 Set Custom Audio

You can select a recorded audio file and set it as the custom audio prompt for the alarms sent from the channels linked to specific models of DVR.

Steps

Note

The device should support this function.

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Tap **Custom Audio** to enter the Select Channel page.
3. Select channel(s), and then tap **Next Step**.
   The available audio file(s) will appear.
4. Optional: Tap the Play icon to play the audio file.
5. Select an audio file or record an audio file yourself, and then tap **OK**.

3.9.6 Use Mobile Client as Device's Remote Controller

For a device added via IP/Domain, you can use the Mobile Client as the device's remote controller.

Steps

Note

- The function should be supported by the device.
- The remote controller function is supported when your phone or tablet is connected to a Wi-Fi network, and the network latency should be less than 200ms.

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Tap ⋯ and tap **Remote Controller** to enter the following page.

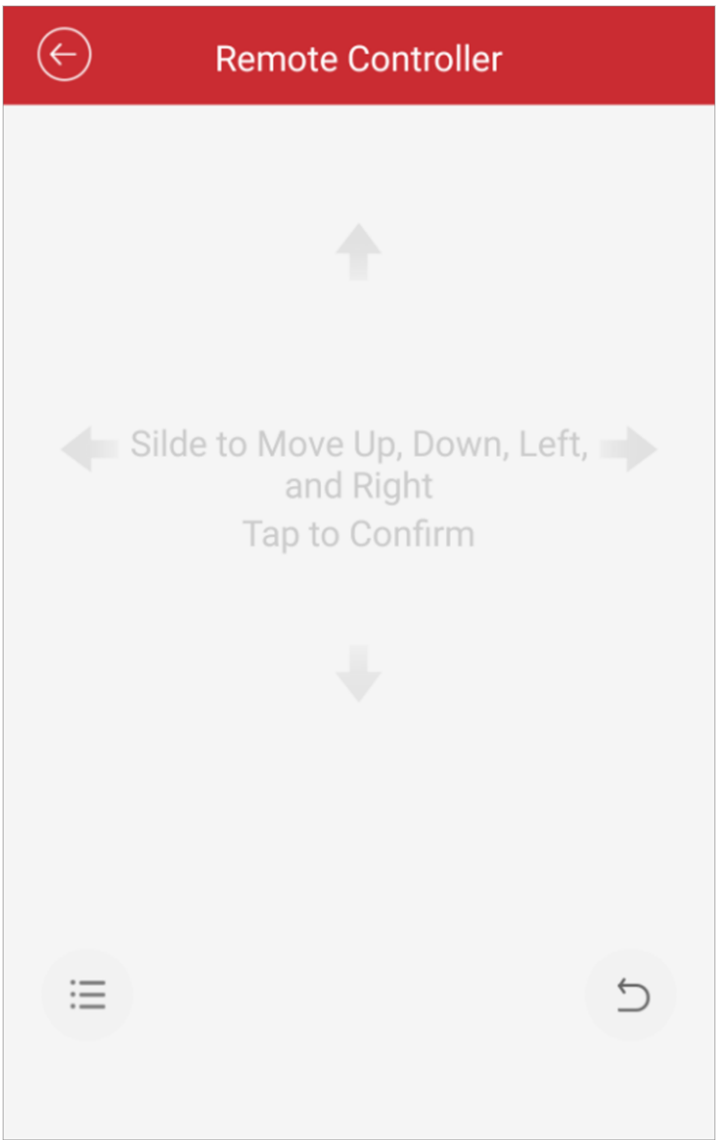


Figure 3-4 Remote Controller Page

3. Swipe the screen to perform remote-control operations such as moving up, down, left, and right.
4. Tap the screen to confirm.
5. Optional: Tap to cancel and return to the previous menu of the device.
6. Optional: Tap to open the main menu of the device.

3.9.7 Remote Configuration

After adding a device, you can set the parameters of the device, including basic information, time settings, recording schedule, etc.

View and Edit Basic Information

You can view and edit the basic information of a device.

Steps

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Enter the Remote Configuration page.
   – For a device added via IP/Domain, tap ⋯ → **Remote Configuration**.

   Note

   For details about adding device via IP/Domain, see ***Add a Device by IP/Domain***.

   – For a device added via other methods, tap **Remote Configuration** on the Settings page.

   Note

   You should have configured DDNS for the device first. See ***Set DDNS***.

3. Tap **Basic Information** to enter the Basic Information page.
4. Tap ✎ to enter the Edit Device page.
5. Edit the basic information of the device.
6. Tap 💾 to save the settings.

Set Recording Schedule

You can set a recording schedule for a channel of a specific device.

Steps

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Enter the Remote Configuration page.
   – For a device added via IP/Domain, tap ⋯ → **Remote Configuration**.

   Note

   For details about adding device via IP/Domain, see ***Add a Device by IP/Domain***.

   – For a device added via other methods, tap **Remote Configuration** on the Settings page.

   Note

   Make sure you have configured DDNS for the device first. See ***Set DDNS***.

3. Tap **Recording Schedule** to enter the Recording Schedule page.
4. Select a channel if the device has multiple channels.
5. Set the switch to ON to enable recording schedule.
6. Set a recording schedule for a day in the week.
   1) Tap a day in the week to enter the schedule settings page.
   2) Tap a time period to set the recording type, start time, and end time.

      Continuous

The video will be recorded automatically according to the time of the schedule.

Motion Detection

The video will be recorded when the motion is detected.

Alarm

The video will be recorded when the alarm is triggered via the external alarm input channels.

Motion Detection or Alarm

The video will be recorded when the external alarm is triggered or the motion is detected.

Motion Detection and Alarm

The video will be recorded when the motion and alarm are triggered at the same time.

Event

The video will be recorded when any event is detected.

Note

You can also set the recording type to detailed event type, which should be supported by the device. For details, refer to the user manual of the device.

3) Tap **OK** to save the settings of the time period.
4) Set other time periods in the day.

Note

Up to 8 time periods can be configured for each day. And the time periods cannot be overlapped with each other.

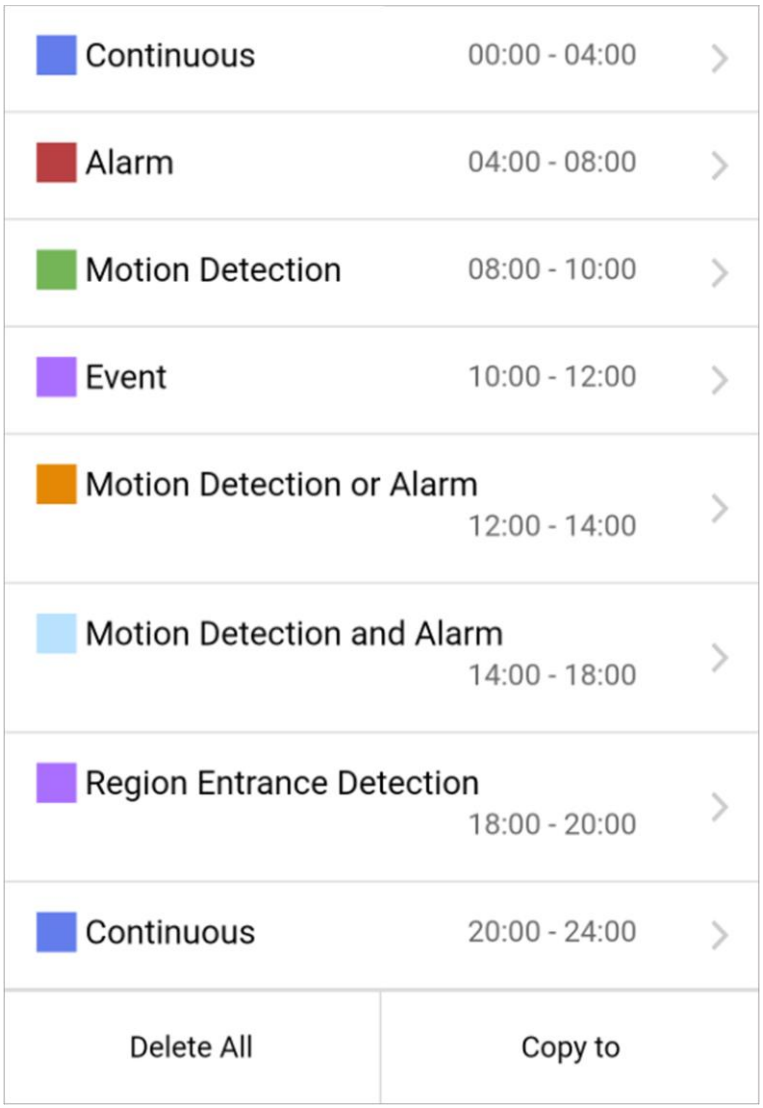


Figure 3-5 Setting Multiple Time Periods in a Day

7. Optional: Perform the following operations after saving the time periods in one day.

Copy to Other Days	Tap **Copy to** to copy all the time periods settings to the other days in the week.
Delete All	Tap **Delete All** to clear all the configured time periods.

8. Tap to save the settings.

Configure Time Settings

You can select the time zone and set the time synchronization mode to Manual or NTP mode for the added device.

Steps

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.

2. Enter the Remote Configuration page.
   – For a device added via IP/Domain, tap ⋯ → **Remote Configuration**.

   Note

   For details about adding devices via IP/Domain, see ***Add a Device by IP/Domain***.

   – For a device added via other methods, tap **Remote Configuration** on the Settings page.

   Note

   You should have configured DDNS for the device first. See ***Set DDNS***.

3. Tap **Time Configuration** to enter the Time Configuration page.
4. Select the time zone in which the device locates.
   The device time will be adjusted automatically.
5. Select the time synchronization mode.
   – Select **NTP Synchronization**. And then set the interval for synchronizing the device time with the NTP server.

   NTP Synchronization

   Synchronize time at a specific interval with the NTP server.

   Note

   For details about setting the NTP server details, refer to the user manual of the device.

   –
   – Select **Manual Synchronization**. And then tap **Synchronize with Phone** to synchronize the device time with the OS (Operation System) time of your phone.
6. Tap 💾 to save the settings.

Change Device Password

You can change the password of a device via the Mobile Client.

Steps

1. On the device list page, tap ••• → **Settings** to enter the Settings page of the device.
2. Enter the Remote Configuration page.
   – For a device added via IP/Domain, tap ⋯ → **Remote Configuration**.

   Note

   For details about adding device via IP/Domain, see ***Add a Device by IP/Domain***.

   – For a device added via other methods, tap **Remote Configuration** on the Settings page.

   Note

   You should have configured DDNS for the device first. See ***Set DDNS***.

3. Tap **Change Password** to enter the Change Password page.

4. Enter the old password of the device
5. Create a new 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) in order 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 installer and/or end-user.

6. Confirm the password.
7. Tap to save the changes.

Configure Normal Event

You can enable a device's normal event such as motion detection, video tampering alarm, video loss alarm, for the channels of the device.

Steps

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Enter the Remote Configuration page.
   – For a device added via IP/Domain, tap → **Remote Configuration**.

   Note

   For details about adding device via IP/Domain, see ***Add a Device by IP/Domain***

   – For a device added via other methods, tap **Remote Configuration** on the Settings page.

   Note

   You should have configured DDNS for the device first. See ***Set DDNS***.

3. Tap **Normal Event** to enter the Normal Event page.
4. Optional: Select a channel if the device has multiple channels.
5. Set the switch(es) to ON to enable the event(s).

Configure Smart Event

You can enable the smart event for the channels of a device, including audio exception detection,

face detection, and intrusion detection, etc.

Steps

Note

The supported event types of smart event vary according to different devices.

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Enter the Remote Configuration page.
   – For a device added via IP/Domain, tap → **Remote Configuration**.

   Note

   For details about adding device via IP/Domain, see ***Add a Device by IP/Domain***.

   – For a device added via other methods, tap **Remote Configuration** on the Settings page.

   Note

   You should have configured DDNS for the device first. See ***Set DDNS*** for details.
3. Tap **Smart Event** to enter the Smart Event page.
4. Optional: Select a channel if the device has multiple channels.
5. Set the switch(es) to ON to enable event(s).

Enable Temperature Measurement

You can enable the temperature measurement function for the thermal camera on the Mobile Client.

Steps

Note

This function is only available to the thermal camera.

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Enter the Remote Configuration page.
   – For a device added via IP/Domain, tap → **Remote Configuration**.

   Note

   For details about adding device via IP/Domain, see ***Add a Device by IP/Domain***.

   – For a device added via other methods, tap **Remote Configuration** on the Settings page.

   Note

   You should have configured DDNS for the device first. See ***Set DDNS***.
3. Tap **Temperature Measurement** to enter the Temperature Measurement page.

4. Optional: Select a camera if camera(s) are linked to the device.
5. Set the switch to ON to enable temperature measurement.

Chapter 4 Camera / NVR / DVR

The Mobile Client supports adding cameras, NVRs, and DVRs. After you add the devices, you can start live view, playback on the client. You can also link cameras with NVR/DVR, set motion detection alarms for network cameras, and reset password of NVRs or DVRs, etc.

4.1 Manage Solar Camera

After adding a solar camera to the Mobile Client, you can control and manage it remotely. The supported functions include waking up the device, viewing its network signal strength, switching power consumption mode, etc.

Wake Up Solar Camera

Unlike using other network cameras, you need to wake up a solar camera before you can control it. You can wake it up in the following two ways:

- On the device list page, tap to enter the device settings page. Once you enter this page, the camera will start waking up.
- On the device list, tap the device to enter its live view page. Once you enter this page, the camera will start waking up.

View Network Signal Strength

Enter the device settings page of the solar camera, and then tap **Network Strength** to view its network strength level.

Switch Power Consumption Mode

Enter the device settings page of the solar camera, tap **Power Consumption Mode** and then select a mode.

Note

After switching power consumption mode, you need to reboot the solar camera to make the new settings take effect on the device.

4.2 Set Light for Floodlight Camera

You can set light for the Floodlight camera.

Before You Start

Make sure you have added a Floodlight camera to the Mobile Client.

Steps

1. On the device list page, tap to enter the Settings page of a Floodlight camera.

2. Tap **Light Settings** to enter the Light Settings page.
3. Set the parameters.

Adjust Brightness

Adjust the brightness of the camera light.

Light Linkage

If enabled, when activities of human beings or animals are detected at night in the areas specified by you (see **Light Linkage Area Settings**, the camera light will be automatically turned on.

Light Linkage Area Settings

Tap the areas to specify them as the light linkage areas.

4.3 Edit Settings of Cameras Linked to NVR/DVR

For cameras linked to NVR/DVR, you can edit their names, hide or show them in the device list, and enable camera cascading.

Steps

1. On the device list page, tap to enter the Settings page of a NVR or DVR.
2. Tap **Linked Camera** to enter the Linked Camera page, and then edit camera settings.

Edit Camera Name	Tap › to enter the camera details page, and then tap **Channel Name** to edit the camera name, and finally tap to save the settings.
Hide/Show Camera	Tap or to hide or show the camera on the device list respectively.

4.4 Set Motion Detection Alarm for Network Camera

Motion detection is a way of detecting motion in a surveillance scene by analyzing image data and differences in a series of images. After setting motion detection area within the field of view of the network camera, the network camera will be able to detect the objects in motion within the area you set and at the same the Mobile Client will receive an event notification about the motion detection alarm.

Steps

1. On the device list page, tap to enter the Settings page of the network camera.
2. Tap **Notification** to enter the Notification page.
3. Draw motion detection area.
   1) Tap **Draw Motion Detection Area** to enter the motion detection area settings page.
   2) Swipe on the screen to draw the motion detection area.

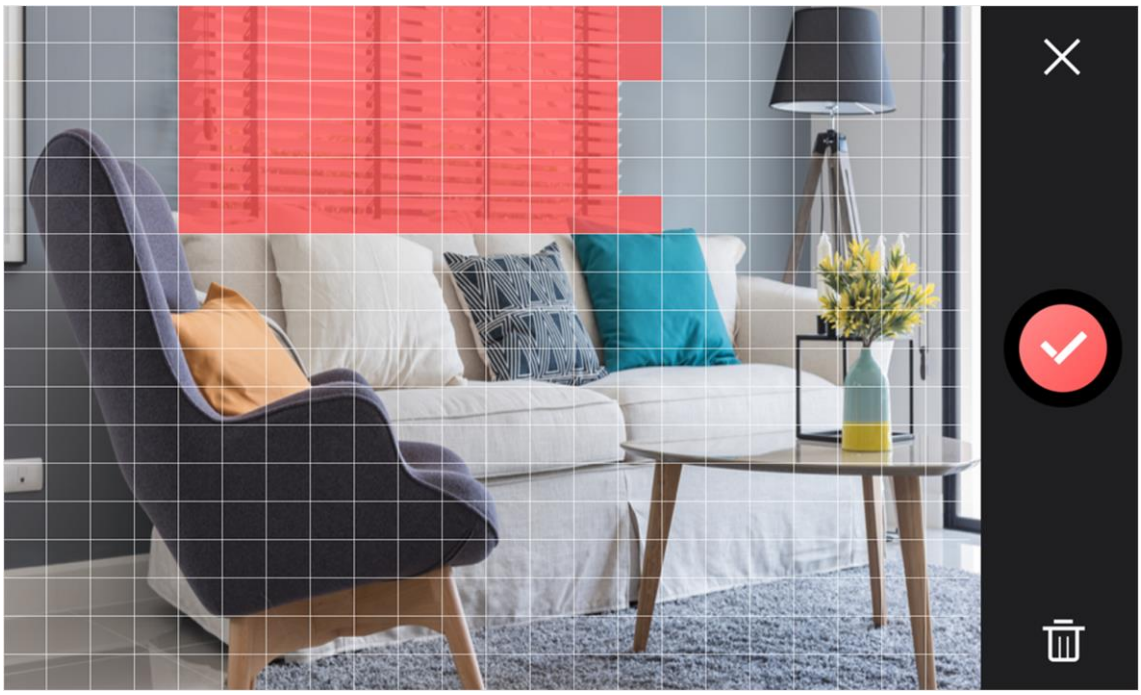


Figure 4-1 Draw Motion Detection Area

3) Optional: Tap to undo the drawing.

4) Tap to save the motion detection area settings.

4. Tap to go back to the Notification page and tap **Motion Detection Sensitivity**, and then adjust the slider to adjust the motion detection sensitivity.

Low

Moving persons, large moving pets, and any other large moving objects in the motion detection area will trigger the alarm, while smaller objects will not.

Medium

Moving small pets and any other medium-sized moving objects in the motion detection area will trigger the alarm, while smaller objects will not.

High

Moving insects, moving leaves, and any other larger objects will trigger the alarm.

What to do next

Go back to the Notification page and make sure **Notification** is enabled.

Note

For details about how to enabling notification, see ***Enable Notifications***

4.5 View Network Topology of NVR

You can view network topology of the cameras connected to an NVR.

Note

The NVR should support the network topology functionality.

On the device list page, tap to enter the Settings page of the NVR, and then tap **Network Camera Topology** to enter the topology page. On the page, you can perform the following operations.

View Network Status

On the topology, you can know the type of the network connection between each node (i.e., an NVR or a network camera) by the type of the line between the two nodes: solid line represents wired connection, dotted line Wi-Fi connection.
You can also view network status of the cameras. If a camera icon is grayed out, the camera is offline.

Zoom In/Out

You can pinch fingers together to zoom in, and spread them apart to zoom out.

Refresh Topology Structure

Tap in the upper right corner to refresh the topology structure.

Show/Hide Cascaded Camera

You can enable the topology to display a specific camera's cascaded camera(s).

Note

The NVR should support this function.

1. On the device list page, tap to enter the Settings page of the device, and then tap **Linked Camera** to enter the Linked Camera page.
2. Tap a camera on the Linked Camera page to enter the Details page.
3. Turn on**Cascading Status** to display cascaded camera(s) of a specific camera in the topology. Turn off to hide.

4.6 Reset Password of DVR or NVR via the Mobile Client

If you forgot the admin password of a DVR or NVR, you can reset the password by using the Mobile Client to scan the QR code generated on the local GUI of the device.
Two verification methods are provided for resetting the password of DVR or NVR: verifying by reserved email or verifying by LTS Connect.

Procedures of Resetting Password via LTS Connect Verification

It is recommended that you use this way to reset the password of DVR or NVR, which is comparatively simpler and more convenient. For details, see ***Reset Password by LTS Connect***.

Procedures of Resetting Password via Email Verification

The flow chart below shows the procedures of resetting password by email verification.

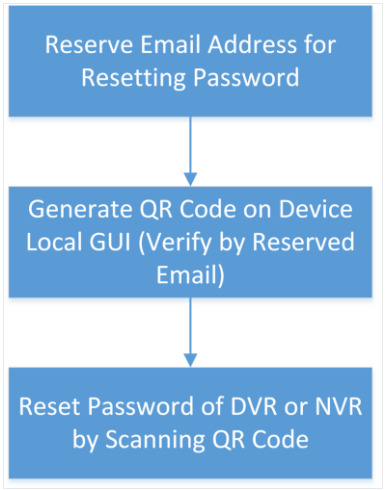


Figure 4-2 Flow Chart

- Reserve Email Address for Resetting Password: See ***Reserve Email Address for Resetting Password*** for details.
- Generate QR Code on Device Local GUI (Verify by Reserved Email): See ***Generate QR Code by Reserved Email*** for details.
- Reset Password of DVR or NVR by Scanning QR Code: See ***Reset Password by Reserved Email*** for details.

4.6.1 Reset Password by LTS Connect

You can reset the password of DVR or NVR via LTS Connect.

Steps

1. On the user login interface of the device, click **Forgot Password**.
2. On the password reset type interface, select **Verify by LTS Connect**.
   The QR code will be generated on the local GUI of the device.
3. Go to the LTS Connect Mobile Client, and then tap **Me** → **Reset Device Password** to enter the Reset Device Password page.
4. Scan the QR code.
   A verification code will be displayed on the Mobile Client.
5. Go to the local GUI of the device and enter the received verification code, and then click **OK** to continue.
6. Create a new password and then confirm the password on the local GUI of the device.

4.6.2 Reserve Email Address for Resetting Password

Make sure you have reserved email address for resetting the admin password of NVR or DVR if you want to change the password by scanning QR code.

Before You Start

- Upgrade the firmware of the NVR or DVR to make the device support self-service password reset.
- If the device is inactivated, check **Reserved Email Settings** when activate it. For details about activating NVR or DVR, see the user manual of the device.

Steps

Note

The DVR or NVR should support the function.

1. Go to **Configuration** → **User** on the local GUI of the device.
2. Select admin user and then click **Edit**.
3. Enter the password of the device in the Old Password field.
4. Click the Settings icon in Reserved E-mail Settings field.
5. Enter an email address for receiving verification code, and then click **OK**.

4.6.3 Generate QR Code by Reserved Email

If you forgot the admin password of the DVR or NVR, you can generate a QR code on the device's local GUI and then scan the QR code via the Mobile Client to reset the admin password.

Before You Start

Make sure you have reserved an email address for resetting password.

Steps

Note

The DVR or NVR should support this function.

1. On the login page of the device's local GUI, click **Forgot Password**.
2. Select **Verify by Reserved Email** and then click **OK**.
3. Read and agree the Legal Disclaimer, and click **OK** to continue.
   The QR code for resetting password pops up.

4.6.4 Reset Password by Reserved Email

If you forgot the admin password of DVR or NVR, you can reset the password by scanning the QR

code generated on the local GUI of the device.

Before You Start

- Make sure you have allowed the Mobile Client to access your phone's camera.
- Make sure you have reserved email address for resetting device password and generated QR code on the device's local GUI. For details, see ***Reserve Email Address for Resetting Password*** and ***Generate QR Code by Reserved Email*** for details.

Steps

1. Tap **Me** → **Reset Device Password** to enter the Reset Device Password page.
2. Scan the QR code on the local GUI of the DVR or NVR.
   A verification code will be sent to the reserved email address.

Note

- The verification code will be valid for 48 hours.
- If you reboot the device or change the reserved email address, the verification code would be invalid.

3. Go to the device's local GUI.
4. Enter the received verification code on the Verify by Reserved Email window and then click **OK** to reset the password.

Chapter 5 Video & Cloud Storage

With the Mobile Client, you can remotely view live videos of the added encoding devices (e.g., cameras, NVRs, and DVRs) and play back their video footage. If cloud storage is activated on the video devices, you can browse, search, play back, and download the video footage on cloud.

5.1 Live View

You can view live video of the devices' connected cameras. And some basic operations are supported during live view, including picture capturing, manual recording, PTZ control, etc.

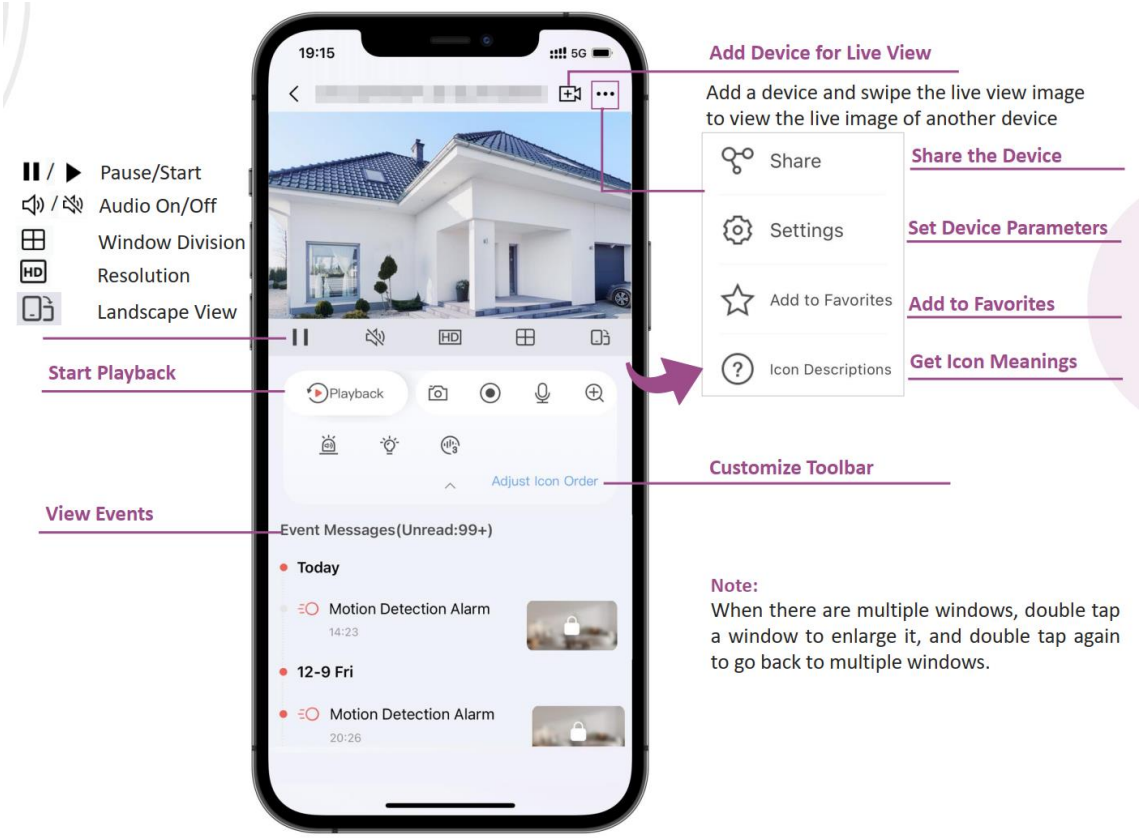


Figure 5-1 Live View

5.1.1 Start and Stop Live View

Live view shows you the live video getting from cameras. Perform the following task to start and stop live view.

Steps

1. Tap a camera to enter the Live View page.

- If the Video and Image Encryption function is disabled, the live video will start playing automatically.
- If the Video and Image Encryption function is enabled, you should enter the device verification code before the live video starting playing.

Note

- For details about Video and Image Encryption function, see ***Set Video and Image Encryption***.
- The default device verification code is usually on the device label. If no verification code found, enter the device verification code you created when enabling LTS Connect service.
- The live video from the video intercom device lasts 5 minutes.
- Up to 6 users can view the live video of a same door station simultaneously. If the upper-limit is reached, other users can only use the audio function of the door station.

2. Optional: Perform the following operations.

View Full Screen Live Video	Rotate the phone to view live video in full screen mode.
Switch Camera	Swipe the live view page to the left or right to switch camera and view its live video.
Reselect Device for Live View	1. Tap to reselect device(s) for live view. 2. Reselect cameras and then tap **OK**. **Note** You can select up to 256 cameras.
Switch to Playback	Tap **Playback** to switch to playback. **Note** For details about playback, see ***Playback***.

3. Stop live view of a camera.
   1) Press and hold a window under live view.
   2) Drag the window upwards to the appearing at the top of the page.

5.1.2 Set Window Division

You can adjust window division in different scenarios.
Tap to set the window division mode to 1-window, 4-window, 9-window, 12-window, or 16-window respectively.

If the added camera number is more than the window division number, you can swipe left or right to see the rest.

5.1.3 Digital Zoom

Digital zoom adopts encoding technology to enlarge the image which will result in image quality damage. You can zoom in or zoom out the live video image as desired.
Tap ⊕ to zoom in or zoom out the image.
Or spread two fingers apart to zoom in, and pinch them together to zoom out.

5.1.4 PTZ Control

PTZ is an abbreviation for "Pan, Tilt, and Zoom". With the PTZ Control functionality provided by the Mobile Client, you can make the cameras pan and tilt to the required positions, and zoom in or out the live video images. For some network cameras, you can also enable auto-tracking to make the camera pan, tilt, and zoom to track the detected moving objects.
Tap to start PTZ.

Note

PTZ control should be supported by the camera.

Pan and Tilt a Camera

The Mobile Client allows you to pan and tilt a camera's view.

Steps

1. Start live view of a camera supports PTZ control.

   Note

   For details about how to start live view, see ***Start and Stop Live View***.

2. Select a live view window on the Live View page.
3. Tap to open the PTZ Control panel.

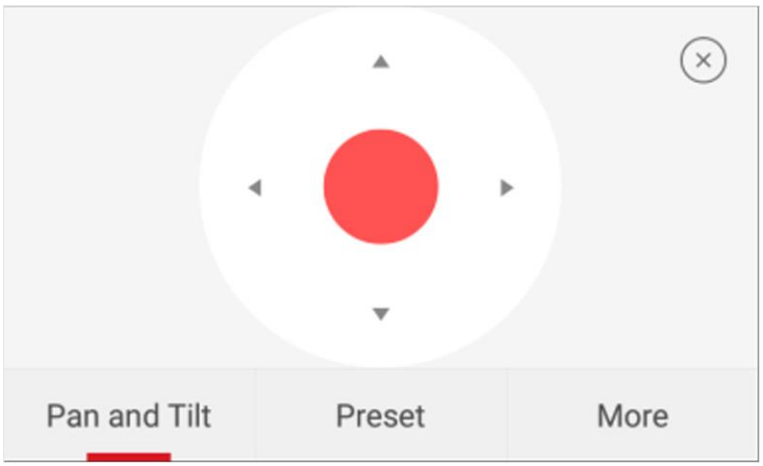


Figure 5-2 PTZ Control Panel

4. Tap **Pan and Tilt**.
5. Drag the circle button at the center of the PTZ Control panel to pan and tilt the camera.

Set a Preset

A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. You can also set a virtual preset after enabling digital zoom. After you set a preset, you can call the preset and then the camera will move to the programmed position.

Steps

1. Pan and tilt a camera to move the camera direction to a desired position.

Note

See ***Pan and Tilt a Camera*** for details.

2. In the PTZ Control panel, tap **Add Preset** to open the following window.

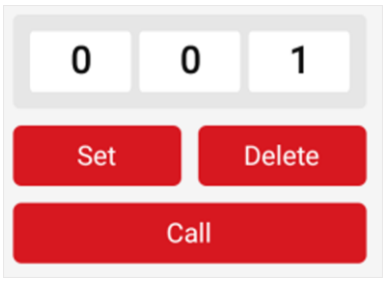


Figure 5-3 Set a Preset

3. Swipe the number up or down to set the preset No.

Note

The preset No. should be between 1 and 256.

4. Tap **Set** to complete setting the preset.
5. Tap **Call** to call the preset.
6. Optional: Tap **Delete** to delete the preset.

Adjust PTZ Speed

You can adjust the PTZ speed.

Steps

1. Start live view of a camera which supports PTZ control.
2. Tap to open the PTZ control panel.
3. Tap **More** → to open the PTZ speed panel.
4. Drag the slider to adjust the PTZ speed.

Other Functions

The PTZ Control panels provide other functions such as PTZ speed adjustment, auto-scan, focus control, iris control, and auto-tracking.
Tap **More** on the PTZ Control panel to view the functions.

Table 5-1 Other Functions

Icon	Description
	Start/stop the auto-scan, which means to make the speed dome pan, tilt, and (or) zoom by a predefined route. **Note** ● You can define the route on the device. For details, see the user manual of the device. ● The function should be supported by the device.
	Zoom control: Zoom+/ Zoom-
	Focus control: Focus +/ Focus -
	Iris control: Iris +/ Iris -
	Adjust PTZ speed.
	Enable/Disable auto-tracking. After enabled, when the camera detects a moving object, the camera will pan, tilt, and zoom to track the object until the object moves out of the field

Icon	Description
	of view of the camera. **Note** The function should be supported by the device.

5.1.5 Start Two-Way Audio

Two-way audio function enables the voice talk between the Mobile Client and devices. You can get and play not only the live video but also the real-time audio from the devices, and the devices can also get and play the real-time audio from the Mobile Client.

Steps

Note

- The function should be supported by the device.
- The devices added by LTS Connect domain or by scanning QR code do not support this function.

1. Start live view of the device.

Note

See ***Start and Stop Live View*** for details.

2. Tap in the toolbar to turn on the two-way audio.
3. If the device is a NVR, select the device or its linked network camera as the two-way audio channel.

Note

If not, skip this step.

- If the device is full duplex, two-way audio will be started automatically.
- If the device is half-duplex, you have to tap and hold to talk, and release to listen.

4. Tap to turn off two-way audio.

5.1.6 Capturing and Recording

During live view, you can capture pictures of the live video and record video footage.

Steps

1. Start live view of a camera.

> **Note**
>
> See ***Start and Stop Live View*** for details.

2. Capture a picture or record video footage.

Capture Picture	Tap to capture a picture.
Record Video Footage	Tap to start recording video footage, tap again to stop.

The captured pictures and recorded videos will be saved in **Me** → **Pictures and Videos**.

5.1.7 Set Image Quality for Device Added by IP/Domain

For devices added via IP/Domain, you can set its image quality to Fluent or Clear. You can also customize image quality for the devices.

Steps

> **Note**
>
> - If you change the image quality, the live view and recording of the device may be affected due to the new settings.
> - In multi-window mode, you can only set the image quality to Fluent, or customize the image quality and the stream type can only be Sub Stream.

1. Start live view of a device added via IP/Domain.

> **Note**
>
> See ***Start and Stop Live View*** for details.

2. Tap BASIC on the live view page to enter the quality switching panel.

> **Note**
>
> The icon vary with the actual video quality.

3. Set the image quality as desired.
   - Tap **Clear** to set the image quality as Clear.
   - Tap **Fluent** to set the image quality as Fluent.

– Tap **Custom** to open the Custom Settings window, and then configure the parameters and tap **Confirm** to confirm the custom settings.

Note

- The live view effect is related to the performance of your network and hardware of your network and phone and tablet. If the live view is not fluent or the image appears blurred, reduce the resolution, frame rate and bitrate of the camera in custom mode, or set the image quality as fluent mode.
- The following table shows the recommended Android and iOS frame rate and bitrate configuration for different resolution at H.264, H.264+ and H.265 video compression by Moto X Pro (CPU: Snapdragon805, Android 5.0.2).

Table 5-2 Android Recommended Configuration

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
H.264 (Software Decoding)				
1080P	√	√		Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264 (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264+ (Software Decoding)				
1080P	√	√		Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
H.264+ (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
H.265 (Software Decoding. Hardware decoding is not supported.)				
1080P	√	√		Frame rate: 25fps; Bit rate: 2Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 256Mbps

Table 5-3 iOS Recommended Configuration

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
H.264 (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264 (Software Decoding)				
720P	√	√		Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264+ (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
H.264+ (Software Decoding)				
720P	√	√		Frame rate: 25fps; Bit rate: 2Mbps
H.265 (Software Decoding. Hardware decoding is not supported.)				
1080P	√			Frame rate: 25fps; Bit rate: 2Mbps
720P	√	√		Frame rate: 25fps; Bit rate: 1Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 256Kbps

5.1.8 Set Image Quality for LTS Connect Device

Usually three pre-defined image qualities are provided in the Mobile Client for LTS Connect device: Basic, Standard, and High Definition.

Steps

Note

The provided image quality types may vary with different devices.

1. Start live view of a LTS Connect device.

Note

See ***Start and Stop Live View*** for details.

2. Tap BASIC to enter the quality switching panel.

Note

The icon may vary with the actual image quality.

3. Set image quality.

Basic

Basic image quality.

Note

Basic is the default image quality.

Standard

Standard image quality (the image quality is higher than that of Basic and lower than that of HD).

HD

High definition image quality (the image quality is the highest of the three).

5.1.9 Live View for Fisheye Camera

In the fisheye view mode, the whole wide-angle view of the fisheye camera is displayed. Fisheye expansion can expand images in five modes: 180° panorama, 360° panorama, 4-PTZ, semisphere, and cylindrical-surface.

Steps

Note

The function is only supported by fisheye camera.

1. Start live view of a fisheye camera.

Note

See ***Start and Stop Live View*** for details.

2. Tap to show the fisheye expansion panel.
3. Select mounting type.

Table 5-4 Mounting Type

Icon	Description
	Wall Mounting
	Ceiling Mounting

4. Select fisheye expansion mode.

Table 5-5 Fisheye Expansion Mode

Icon	Description
	Fisheye view for ceiling mounting and wall mounting. In the Fisheye view mode, the whole wide-angle view of the camera is displayed. The mode is the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image. In this mode, you can pinch the fingers together to zoom out the image, and spread them apart to zoom in.
	Dual-180° panorama view for ceiling mounting. The distorted fisheye image is transformed to normal perspective image. In this mode, you can swipe to the left or to the right to adjust the field of view.
	360° panorama view for ceiling mounting and wall mounting. The distorted fisheye image is transformed to normal perspective image. In this mode, you can swipe to the left or to the right to adjust the field of view.
	4 PTZ Views for ceiling mounting and wall mounting. The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view. In this mode, you can pinch the fingers together to zoom out the image, and spread them apart to zoom in. You can also swipe the screen to perform pan and tilt movement.
	Semisphere-shaped view for wall mounting. In this mode, the whole wide-angle view of the camera is displayed. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image. In this mode, you can drag the image to adjust the view angle, and pinch the fingers together to zoom out the image, and spread them apart to zoom in.

Icon	Description
	Cylindrical-surface-shaped view for wall mounting. In this mode, the whole wide-angle view of the camera is displayed. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image. In this mode, you can drag the image to adjust the view angle, swipe to the left or to the right to adjust the field of view, as well as pinch the fingers together to zoom out the image and spread them apart to zoom in.

5.1.10 Open Door During Live View

You can open or close the door when viewing the live video of a video intercom device, a face recognition terminal, or a related camera of an access control device. This function allows you to check the visitor or the situation nearby the door before you open it.

Note

- The device should support this function.
- For face recognition terminals, you can enabling opening door by fingerprint authentication or facial authentication. For details, see ***Manage Access Control Devices***.

For the access control device's related cameras, select a live view window and tap **Open Door**, and then enter the device verification code to open the door.
For the video intercom device, select a live view window and tap , and then enter the device verification code to open the door.

Note

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

5.1.11 Check Events During Live View

You can select an event and then play back the event-related video footage. Duration playback, you can also save the event-related picture if it has been captured by the camera.

Before You Start

Make sure you have configured events for the selected camera.

Steps

1. Start live view.

Note

For details, see ***Live View***.

2. Tap an event to view the event-related footage.

5.2 Playback

You can search the recorded video files stored in the added device for remote playback.

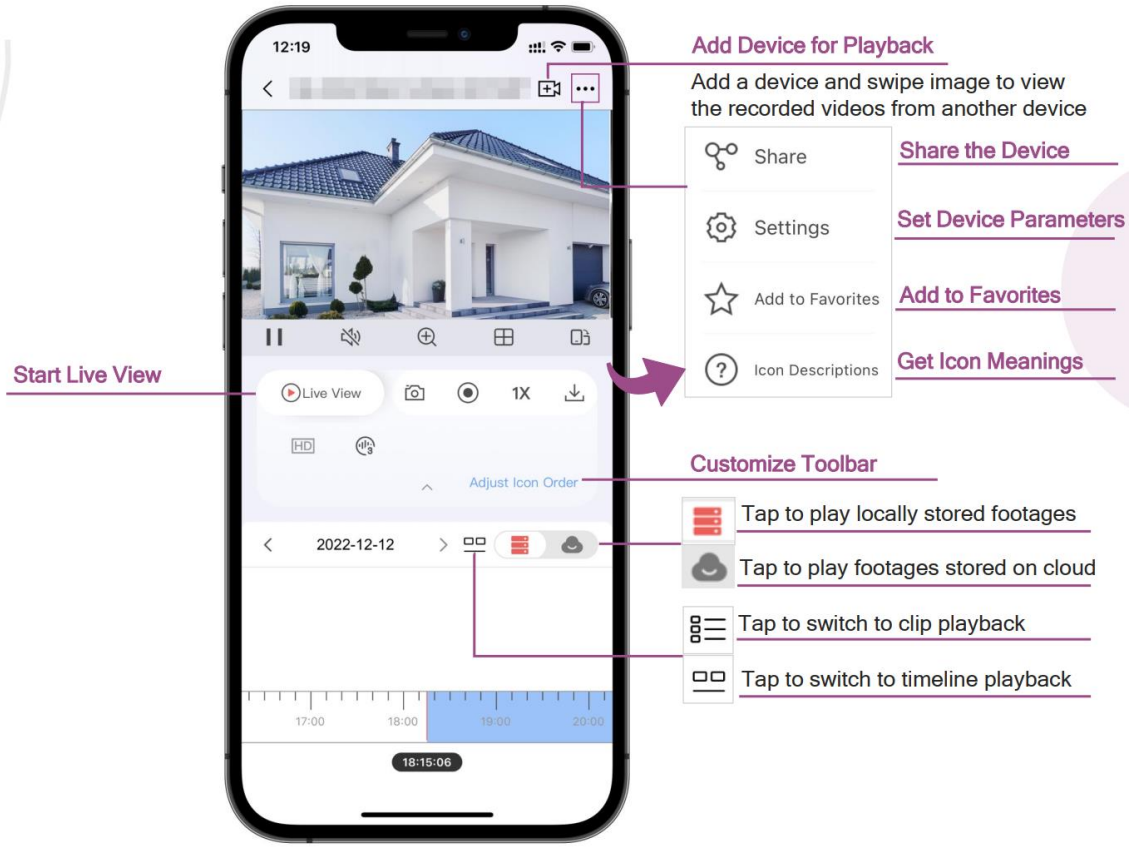


Figure 5-4 Playback

5.2.1 Normal Playback

Normal playback refers to the playback based on timeline. You can search the camera's recorded video files in a selected time period and then start playback.

Steps

1. On the device list page, tap in the upper-left corner to enter the Select Item(s) page.
2. Set the date and time for playback.

Playback Date

Select a date.

Note

The date during which video files were recorded is marked with a yellow dot.

Playback Time

Set the start time point for the playback in the selected date.

3. Select camera(s).

Note

You can select up to 4 cameras.

4. Tap **Start Playback** to enter the Playback page.
5. Optional: Perform the following operations.

Play Video Footage Stored on Cloud	Tap on the playback page to play back video footage stored on cloud. **Note** See details in ***Play Back Video Footage on Cloud***.
Play Video Footage Stored on Local	Tap on the playback page to play back video footage stored locally.
Clip Playback	Tap to switch to clip playback.
Adjust Playback Time	Tap to switch timeline playback. Slide the timeline to adjust the playback time. Spread two fingers apart to scale up the timeline or pinch them together to scale down. **Note** represents continuous recording and represents event-triggered recording. You can determine the recording type (continuous or event-triggered) when setting recording schedule. For details, see ***Set Recording Schedule***.

5.2.2 Capturing and Recording

During playback, you can capture pictures and record video footage.

Steps

1. Start playback.

Note

See ***Normal Playback*** for details.

2. Capture a picture or record video footage.

Capture a Picture	Tap to capture a picture.
Record Video Footage	Tap to start recording video footage, tap again to stop.

The captured pictures and recorded videos will be saved in **Me** → **Pictures and Videos**.

5.2.3 Set Playback Quality for Device Added by IP/Domain

For devices added by IP/Domain, you can set the image quality of playback for them.

Steps

Note

For details about adding device by IP/Domain, see ***Add a Device by IP/Domain***.

1. Select a device added by IP/Domain on the device list and then start playback.

Note

For details about starting playback, see ***Normal Playback***.

2. Tap on the playback page to enter the quality switching panel.

Note

The icon may vary with the actual video quality.

3. Set the image quality as desired.
   - Tap **Clear** to tap the image quality to Clear.
   - Tap **Custom** to open the Custom Settings window, and then configure the parameters (Resolution, Frame Rate, and Bitrate) and tap **Confirm** to confirm the custom settings.

Note

- The image effect is related to the performance of your network and phone or tablet. If the

image is not fluent or the screen appears blurred, reduce the resolution, frame rate and bitrate of the camera in custom mode.

- The following table shows the recommended Android and iOS frame rate and bitrate configuration for different resolution at H.264, H.264+ and H.265 video compression by Moto X Pro (CPU: Snapdragon805, Android 5.0.2).

Table 5-6 Android Recommended Configuration

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
H.264 (Software Decoding)				
1080P	√	√		Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264 (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264+ (Software Decoding)				
1080P	√	√		Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
H.264+ (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
H.265 (Software Decoding. Hardware decoding is not supported.)				
1080P	√	√		Frame rate: 25fps; Bit rate: 2Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 256Mbps

Table 5-7 iOS Recommended Configuration

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
H.264 (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264 (Software Decoding)				
720P	√	√		Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264+ (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
H.264+ (Software Decoding)				
720P	√	√		Frame rate: 25fps; Bit rate: 2Mbps
H.265 (Software Decoding. Hardware decoding is not supported.)				
1080P	√			Frame rate: 25fps; Bit rate: 2Mbps
720P	√	√		Frame rate: 25fps; Bit rate: 1Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 256Kbps

5.2.4 Adjust Playback Speed

For the cameras linked to a DVR or NVR, you can adjust the playback speed for them as required.

Note

The function should be supported by the device.

During playback, you can swipe the toolbar at the bottom to view the hidden icons, and then tap 1X to set the playback speed to 1/8 X, 1/4 X, 1/2 X, 1X, 2X, 4X, and 8X. X here refers to the original playback speed.

5.2.5 Download Video Segment from Device

During playback of the cameras linked to a DVR or NVR, you can download a specific video segment as evidence if it contains important information about incidents such as violent crimes in

case of the need for settling disputes or legal cases.

Steps

Note

The function should be supported by the device.

1. Start playback.
2. Tap ⬇ if important information occurs on the image.
   By default, the video segment which lasts 130 seconds (from 10 seconds before the tapping, to 120 seconds after that) will be automatically selected for download. For example, if you tap ⬇ when the video footage is played to 00:00:30, the segment from 00:00:20 to 00:02:30 will be selected.

Note

In special occasions when 130-seconds duration is not available to be selected following the above-mentioned rule, the segment will extend afterwards or backwards until the segment duration reaches 130 seconds. For example, if you start downloading from the very beginning of the video footage, the selected segment will be from 00:00:00 to 00:02:10.

3. Optional: Drag the slider(s) to lessen the duration of the segment for download.

Note

The duration should not be shorter than 10 seconds.

4. Optional: Tap the Play icon to preview the selected segment.

Note

If the segment is encrypted, you should enter the device verification code before you can preview it. For details about video encryption, see ***Set Video and Image Encryption***.

5. Tap **Download** to start downloading.

Note

Downloading at the background is supported. Download task(s) continues if you exit the Download page or the Mobile Client.

6. Optional: Go to **Me** → **Pictures and Videos** to view the downloaded video segment.

5.3 Cloud Storage

With cloud storage, your cameras, DVRs, and NVRs can upload recorded video clips to the cloud

automatically. You can easily access, play, and download the video footage of your video devices on cloud.

Note

Cloud storage service is not available in all countries or regions.

5.3.1 Enable/Disable Cloud Storage Service for a Channel

You can enable/disable cloud storage service for a specific channel of a device supporting storing video footage on cloud. You can also view details of the cloud storage service package, including service package type, effective period, and status (activated or expired).

Before You Start

Make sure your Service Provider has activated the cloud storage service for your device. Otherwise, you cannot enable cloud storage.

Steps

1. Enter the settings page of the device.
2. Tap **Cloud Storage** to enter the Cloud Storage page.

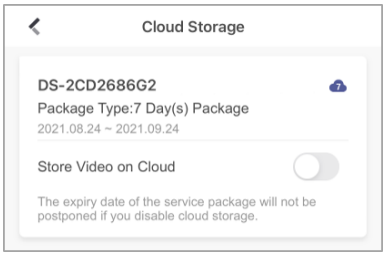


Figure 5-5 Cloud Storage

3. Switch on/off to enable/disable the cloud storage service of a specific channel.

5.3.2 Play Back Video Footage on Cloud

You can play back video footage stored on cloud.

Note

Make sure your Service Provider has activate cloud storage service for your devices and you have enabled it.
See details in ***Enable/Disable Cloud Storage Service for a Channel***.

To play back the video footage on cloud:

1. Start playing back the recorded video footage of a video device.

   Note

   See instructions in ***Normal Playback***.

2. Tap to play back video footage stored on cloud.

Note

You can adjust the playback speed to up to 8 times faster.

5.3.3 Download Video Footage from Cloud

The Mobile Client allows you to browse through the video footage stored on cloud of each date to quickly locate the footage you need. And you can download the video footage to your phone.

Before You Start

Note

Make sure your Service Provider has activate cloud storage service for your devices and you have enable it.
See details in ***Enable/Disable Cloud Storage Service for a Channel***.

Steps

1. Start playing back video footage stored on cloud.

   Note

   See details in ***Play Back Video Footage on Cloud***.

2. Tap to play video stored on cloud.
3. Tap to enter the Download Video page.
4. Select a date.

   Note

   The date marked with a blue dot is the date during which video footage is recorded.

5. Tap , and then select the video footage you want to download.
6. Tap to download the selected video footage to your phone.

Chapter 6 Notification

On the Notification tab, you can view event notifications, call logs of video intercom devices, and alarm information related to security control panels.

Note

In the mobile client, each device can only send one alarm per minute. It's a mechanism to not overload the servers. So for example, a camera will send a notification about a line crossing but if someone crosses the same line 20 seconds later on the same camera, it won't send another alert/notification. It can only send 1 alert per device, per minute.

6.1 Enable Notifications

You can allow the Mobile Client to receive and push notifications of the events detected by a device, services, exceptions, etc. If you want to block notifications during specific time, you can set a notification schedule to define the time period(s) during which the Mobile Client is allowed to receive event information and push them to you. You can also set notification mode to avoid the disturbance of push notifications (and the audio and strobe light alarm) while still being able to receive information on the Notifications page.

Before You Start

Make sure you have configured event settings on device (except for the video intercom device). See the user manual of the device for details.

Steps

Note

- For Android, make sure your phone supports Google Play service, or notifications may fail to be pushed to you.
- For iOS, when Critical Alerts is enabled, you will get notifications on critical alerts even if your device is muted or in Do Not Disturb mode. You can enable Critical Alerts for the Mobile Client in **Settings** → **Notifications** of iOS.

  Note

  Critical Alerts requires iOS 12 or later.

- The Mobile Client will ignore alarm events triggered out of the time period defined by the notification schedule.
- The security control panel does not support setting notification schedule.
- For specific thermal device, you can also set custom voice prompt for the detected events, such as fire detection.

1. On the device list page, tap ··· → **Settings** to enter the Settings page of the device.
2. Tap **Notifications** to enter the Notification page.
3. Turn on **Notifications** to allow the Mobile Client receive and push notifications of events detected by device all the time.
4. Select a notification mode.
   - For normal devices, select one of the following two modes.

     Receive Events and Push Notifications

     The Mobile Client will receive event information from the device and push related notifications in real time. In other words, you can not only get notified by the push notifications, but also view all the received event information in Notification page.

     Receive Events but NOT Push Notifications

     The Mobile Client will receive event information in real time from the device but NOT push related notifications. In other words, although you will NOT be disturbed by the event-related push notifications, you can view all the received event information in the Notification page.
   - For audible strobe light, select one of the following two modes.

     Receive events and push notifications, and allow Audio and Strobe Light alarms on device

     The Mobile Client will receive event information from the device, and push related notifications in real time. And the audio and strobe light alarm is allowed to be triggered on the device once an event is detected. In other words, you can not only get notified by the push notifications and the audio and strobe light alarms, but also view all the received event information in the Notification page.

     Receive events but NOT push notifications, and NOT allow Audio and Strobe Light alarms on device

     The Mobile Client will receive event information from the device in real time, but NOT push related notification. And the audio and strobe light alarm is NOT allowed to be triggered on the device once an event is detected. In other words, although you will NOT be disturbed by the event-related push notifications and the audio and strobe light alarms, you can view all the received event information in the Notification page.
5. Optional: Enable notification schedule to set a time schedule for receiving event information from the device and push related notifications (if allowed in the previous step).
   1) Tap **Notification Schedule**.
   2) Tap **Set a Time Schedule** to enter the Schedule Settings page.

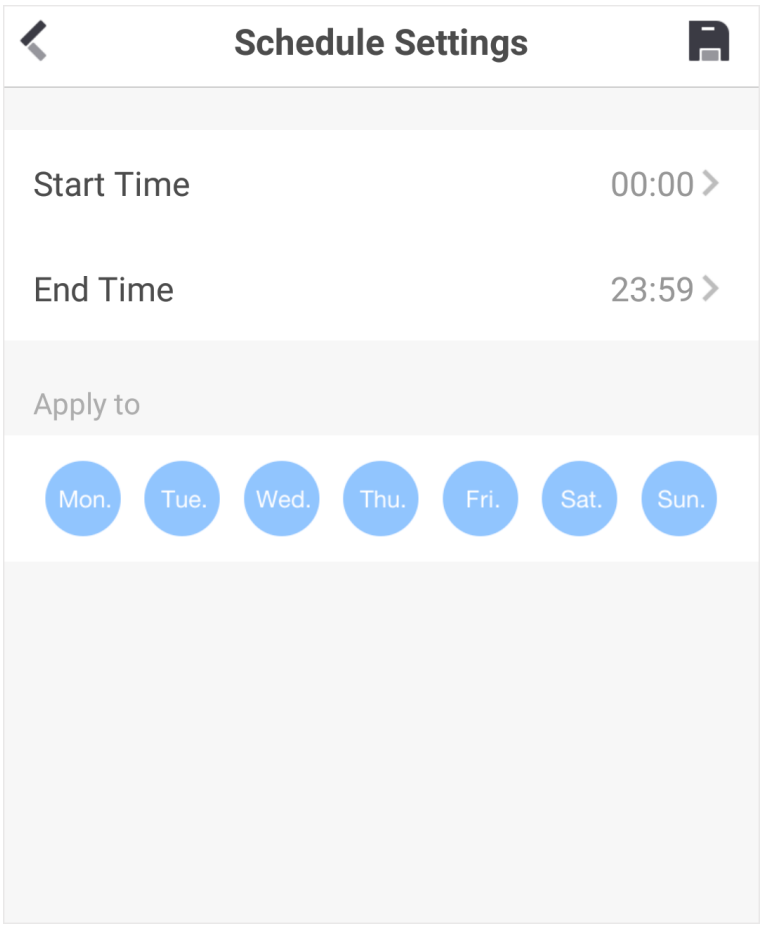


Figure 6-1 Schedule Settings Page

3) Set the start time and the end time.
4) Select the date(s) to which the configured time period applies to.

Note

The date(s) marked in blue is selected.

5) Tap .
6) Optional: Tap the configured schedule to enter the Schedule Settings page, and then edit the start time, end time, and the date(s) to which the configured time period applies to. Or tap **Delete** to delete the schedule.
7) Go back to the Notification page.

6. Optional: Tap **Notification Sound Mode** and then select one of the following sound mode and tap to set a notification sound mode for the detected intrusion.

Note

The function should be supported by the device.

Intensive

Intense warning for the intrusion.

Soft

Soft warning for the intrusion.

Mute

No audible warning.

6.2 Check Event Notifications

You can check event notifications on the Notification page when events are detected by the devices. The unread notifications are marked with a red dot.

Before You Start

- Set event parameters for the device and arm the device. For details, see the user manual of the device.
- For indoor station, it should have been linked to the sensor. For details, see the user manual of the video intercom device.

Steps

1. Tap **Notifications** → **Event** to enter the Event Notifications page.
2. Optional: Tap and then select a date and (or) select a device to filter the events.
3. Tap an event notification to show the detailed information such as time and source.

View and Download Event-related Picture	If there are multiple event-related pictures, you can swipe left/right to switch pictures. You can also tap a picture and then tap to download the picture.
Zoom In/Out Event-related Picture	Tap the picture, and then spread two fingers apart to zoom in the picture and pinch them together to zoom out, or double-tap the picture to zoom in or zoom out.
	Note ● Make sure you have configured the event linkage action for capturing event-related picture for the device. See the user manual of the device for details. ● If you have enabled Video and Image Encryption for the device, you need to enter the device verification code before you can view the picture.
View Event-related Video Footage	Tap **Playback** to view the video footage.

Note

Make sure you have configured the event linkage action for recording video for the device. See the user manual of the device for details.

View Live Video

Tap **Live View** to view the live video of the device.

Note

The device should support this function.

View External Linked Video

Tap **External Linked Video** to view the video footage recorded by the device's externally linked device.
For example, if a camera is linked to a detector, once the detector detects an event, the camera will record video footage.

4. Optional: Go back to the Notifications page and then edit the event information.

Mark All Events as Read

Tap ··· → **Mark as All Read**, and then tap to mark all event information as "already read".

Clear All Events

Tap ··· → **Edit** → **Clear All** to clear all event notifications.

Delete a Specific Event

Tap and hold an event notification until a prompt pops up, and then tap **Delete** to the prompt to delete the notification.
Or, swipe from the right end of the card that displays the event notification towards the left, and then delete this event notification.

6.3 Check Pyronix Notifications

You can check Pyronix notifications on the Notifications page when there are any Pyronix notifications. The unread notifications are marked with a red dot.

Steps

1. Tap **Notifications** → **Pyronix** to enter the Pyronix Notifications page.
2. Optional: Tap and then select a date, event type, and (or) select a device to filter the notifications.
3. Optional: Go back to the Notifications page and then edit the event information.

Mark All Events as Read

Tap ··· → **Mark as All Read**, and then tap to mark all event information as "already read".

Clear All Events	Tap ··· → **Edit** → **Clear All** to clear all event notifications.
Delete a Specific Event	Tap and hold an event notification until a prompt pops up, and then tap **Delete** to the prompt to delete the notification. Or, swipe from the right end of the card that displays the event notification towards the left, and then delete this event notification.

6.4 Check Call Notifications

You can check call notifications on the Notifications page when someone calls. The unread notifications are marked with a red dot.

Steps

1. Tap **Notifications** → **Call** to enter the call notifications page.
2. Optional: Tap and then select a date and (or) select a device to filter the notifications.
3. Optional: Go back to the Notifications page and then edit the event information.

Mark All Events as Read	Tap ··· → **Mark as All Read**, and then tap to mark all event information as "already read".
Clear All Events	Tap ··· → **Edit** → **Clear All** to clear all event notifications.
Delete a Specific Event	Tap and hold an event notification until a prompt pops up, and then tap **Delete** to the prompt to delete the notification. Or, swipe from the right end of the card that displays the event notification towards the left, and then delete this event notification.

6.5.1 Accept Invitation to Be Site Owner

You can accept the invitation from the Service Provider to be the owner of a specific site.
Go to **Notifications** → **Service**.
You can tap on an invitation to view the details such as the site and the devices authorized to the Service Provider, and then tap **Agree** to accept the invitation and therefore become the owner of the site.

6.5.2 Approve Device Handover and Authorization Application

If a Service Provider hands over devices to you or applies for device permissions on the Lts-Partner Pro platform, you will receive an application notification. After you approve the application, the Service Provider will be able to provide device configuration and maintenance services based on the permissions you granted.

- If the Service Provider hands over devices to you, you will receive device handover and authorization applications.

- If the Service Provider applies for device permissions, you will receive device authorization applications.

Steps

1. Go to **Notifications** → **Service**.
2. Tap on a Device Handover and Authorization Application notification.
3. Accept device handover.

Note

After handover, your Service Provider does not have any permissions to operate or configure the devices. Service Provider usually applies for device permissions so as to configure and maintain the devices for you. If your Service Provider has applied for the permissions, you need to accept it in device authorization application.

4. Open the Device Authorization Application.
   - If the Service Provider has applied for device permissions when handing over the devices, the device authorization application will show up right after you accept device handover.
   - If the Service Provider has not applied for device permissions, open the application after the Service Provider sends one.

Note

- In device authorization application, you can view details such as Service Provider information, permissions that the Service Provider applies for, and the Alarm Receiving Center (ARC) information.
- For more details on Alarm Receiving Center, see ***ARC Service***.

5. Select the permissions you want to grant to the Service Provider.

Note

- If the Service Provider enabled ARC service for you, you can check **ARC Service** to activate it.
- If you activate ARC service, the ARC will provide 24/7 alarm responding service for you, including receiving events from devices, responding to events, and sending out emergency dispatches (if needed).

6. Tap **Agree** to approve the application.

6.5.3 Notification about Availability of a Rent Device

If a device that you rent from the Service Provider is blocked or unblocked by the Service Provider,

you will receive a notification about that.

Note

If a rent device is blocked by the Service Provider, you are not allowed to operate the device via the Mobile Client. In this case, you can contact the Service Provider and ask her/him to unblock the device if required.

For such a notification, you can view the Service Provider who block/unblock the device and the site where the device is added.

6.6 Check Device Exception Notifications

You can receive and view the exception notifications of your devices that are managed by the Service Provider.
After your Service Provider handles an exception, you will also be notified of the handling result.
You can see all exception notifications in **Notifications** → **Exception**.

6.7 Check System Notifications

Under system notifications, you can view linkage notifications. Linkage refers to the process in which an event detected by a resource triggers actions in other resources. The linkage can be used for notifying security personnel, upgrading security level, saving evidence, etc., when specific events happen. You can view notifications about linkages in Service Notifications.

Note

- This feature is not available in all countries or regions.
- The linkage can only be set by the Service Provider via the Lts-Partner Pro platform.

Go to **Notifications** → **System** to view linkage notifications. You can tap on each notification to view the detected event, event time, devices in the linkage, and triggered actions.

Chapter 7 Service Management

In Services section, you can manage or access services related to Lts-Partner Pro, which is a cloud service platform for Service Providers (installation companies). Service Providers can provide services such as device configuration and device maintenance for you if granted with device authorization and permissions.
Cloud Service page includes the following modules.

Service Notifications

Check cloud-related notifications and respond requests from Lts-Partner Pro, such as applications from the Service Provider, including applications for device handover, device authorization and permissions, and device password reset.

Device Authorization

Manage device authorization, device permissions, and ARC authorization, check Service Provider information, and transfer devices to another user.

Deauthorized Devices

Check the devices that are deauthorized from the Service Provider and re-authorize to a new or existing Service Provider.

Cloud Features

Access the features activated by your Service Provider via Lts-Partner Pro, including Access & Attendance, People Counting, and Temperature Screening.

Note

- Cloud features are not available in all countries or regions.
- Service Provider can also activate cloud storage for your devices. With cloud storage, you can easily access the video footage of your video devices stored on cloud. See details in ***Cloud Storage***.

7.1 Invite a Service Provider to Manage Devices

You can invite and authorize a Service Provider to help you set up and manage the devices in your account.

Steps

1. In the device list, tap of the device and the Share Device page will pop up.
2. Tap **Share with Service Provider**.

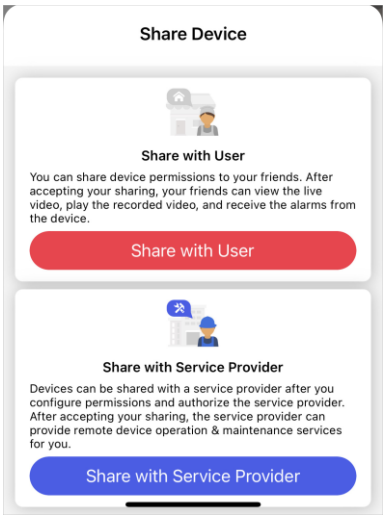


Figure 7-1 Select Service Provider

3. Tap **New Service Provider** and enter the Service Provider's account if you want to share device permissions with a new Service Provider or you do not have a Service Provider before. You can also select an existing Service Provider if you have authorized one or more Service Providers to manage your other devices before.
4. Select the site which the device will be added to and the device permissions you want to grant to the Service Provider.

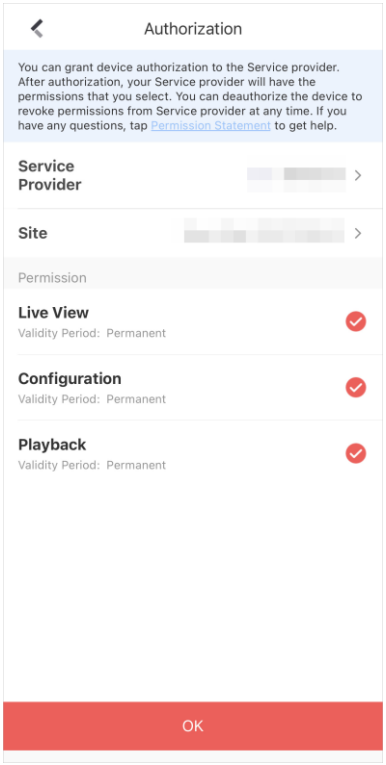


Figure 7-2 Authorization

Note

- If the Service Provider has not created any site for your devices, a new site will be created.
- **What's a Site?** A site is like an area where your devices are located, such as your home, office, etc. Your Service Provider uses sites to group, batch configure, and provide cloud features for your devices.

5. Tap **OK** to invite the Service Provider.
   Your Service Provider will receive an email about the authorization and need to accept it before managing your device on Lts-Partner Pro.

7.2 Device Authorization Management

You can grant authorization and permissions of the devices in your LTS Connect account to a Service Provider. With device authorization and permissions, the Service Provider is able to control and configure the devices, thereby managing and maintaining the devices for you.
You can manage device authorization in **Services** → **Device Authorization**.

Note

Authorized devices are grouped in "Sites" which are created by your Service Provider.

Grant Device Authorization and Permissions to Service Provider

- If your Service Provider has sent device authorization application to you, you can grant authorization by approving the application. See ***Approve Device Handover and Authorization Application*** for details.
- To authorize a Service Provider with more devices, follow the steps below.
  - Tap **Services** → **Authorize More**.
  - Select devices and permissions.
  - Tap **OK** and the devices will be authorized to the Service Provider and added to the Site.

Edit Device Permissions

You can edit devices permissions for Service Provider in the following two ways.

- Bulk Edit the Permissions of Devices in a Site:
  Tap **Services**, and you can see all Service Providers.
  Tap a Service Provider, and tap **Edit** to edit device permissions.
- Edit the Permissions of a Single Device:
  Go to the Home page, in the device list, tap ··· → **Settings** of a device to enter the device settings page. Tap **Authorization Service** → **Edit** to edit device permissions.

Cancel Device Authorization

Tap **Services**, you can see all Service Providers, and tap a Service Provider.
Tap ··· → **Cancel Authorization** to cancel the authorization of ALL devices in the Site.

You can keep the Site if there are value-added services activated.

View Service Details

Tap **Services**, and you can see all Service Providers.
The number of service times is displayed, and tap it to view details.

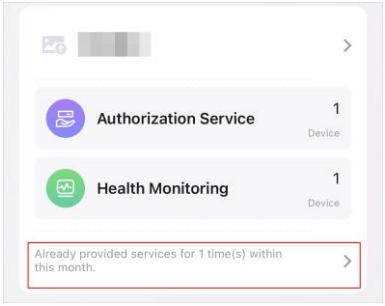


Figure 7-3 Service Details

You can filter by date to view service details.

7.3 Reset Password of Device in Authorization

You can reset the password of a device with the assistance of Service Provider.

Note

This feature requires device support.

Refer to the flow chart below for the whole process of resetting the password of a device that you authorized Service Provider with.

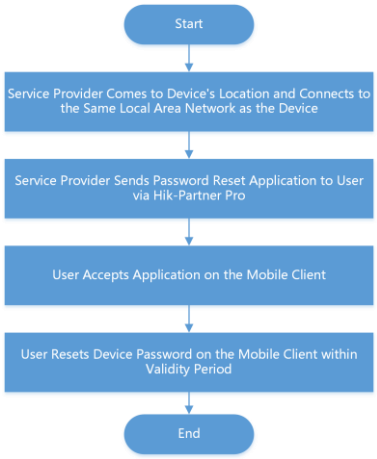


Figure 7-4 Flow Chart of Resetting Device Password

Note

- The validity period of password reset application is 5 minutes.
- You will be notified whether password reset is completed or failed.

Example

User can ask the Service Provider for a password reset if the password of an authorized device is lost. The Service Provider has to go to the device's location and connect to the same local area network before sending a password reset application to the user. After the Service Provider sends the password reset application, user can set a new password for the device.

7.4 Transfer Device to Others

You can transfer the devices in your account to another account. Once transferred, the devices will be unavailable to you, and the target account will have all configuration and operation permissions of the devices.

Steps

1. Tap **Services**, and you can see all Service Providers.
2. Tap a service provider, and tap ··· → **Transfer Device**.

Note

Only supports transferring devices in a Site altogether. Site is created by your Service Provider to group your devices.

3. Enter the mobile phone number or e-mail address of the target account.
4. Tap **OK** to start transferring.

Note

- The Site becomes unavailable during transfer process.
- The recipient will receive a device transfer application. You can cancel device transfer before the target user accept the application. Once the recipient accepts it, you will no longer have any access or permission towards the devices.
- If the devices are managed by a Service Provider, the recipient can choose to keep the authorization service or cancel it.
  If the recipient choose to keep the current authorization, the Service Provider managing the device will still have the device permissions after the transfer.
  If the recipient choose to cancel the authorization, the Service Provider will not have any permission of the device after the transfer.

7.5 ARC Service

ARC stands for Alarm Receiving Center. ARC provides round-the-clock alarm monitoring and responding service for you. ARC can receive event notifications sent from your devices and respond to these events. In case of emergency, such as intrusions or fires, ARC sends out

dispatches or contact the police on your behalf to address security issues to protect people and property.

Activate ARC Service

Note

ARC service is not available in all countries or regions.

Your Service Provider can enable ARC service for you with your approval.
To enable ARC service, the Service Provider needs to apply for ARC authorization and permissions.
After the Service Provider sends an application, you need to accept it to activate the ARC service.
To check the currently active ARC service, go to **Services** → **ARC Service**.

Deactivate ARC Service

You can deactivate ARC service by deauthorizing ARC.
To deauthorize ARC, go to **Services** page, and tap a service provider.
Tap **Alarm Receiving Center (ARC)** and tap **Deauthorize ARC**.
After deauthorization, the ARC will lose all device permissions you granted previously and cease to provide ARC service for you.

7.6 Cloud Attendance

Cloud Attendance works with MinMoe access control devices. It is designed for bringing higher security and improved efficiency to access control and attendance tracking. Persons in a cloud attendance system (usually employees in an organization) can use Cloud Attendance on the Mobile Client to check attendance records, control doors and turnstiles, and check in/out.

Note

- Cloud Attendance is not available in all countries or regions.
- If applicable, make sure you have evaluated the impact on data protection before using Cloud Attendance.
- Select your role and read the part you need.
  - If you are the employee who needs to check attendance records and control doors, read the ***For Employee*** section.
  - If you are the administrator who needs to set up the Cloud Attendance system, read the ***For Administrator*** section.

For Employee

Go to **Services** → **Cloud Attendance**.

Note

If you cannot see Cloud Attendance in the Cloud Service tab, you are not in a Cloud Attendance system. Ask the administrator of the Cloud Attendance system for help.

Cloud Attendance has three tabs:

Attendance Report

Check your attendance status and records.

Check In

Check in or check out directly on the Mobile Client without actually presenting and authenticating at the attendance check devices. See details in ***Check In/Out Remotely***.

Door Control

See the live view of an access control device and open door remotely. See details in ***Open Door Remotely***.

For Administrator

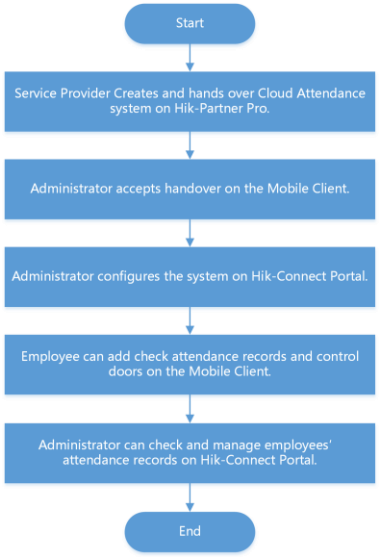
If you are the administrator who manages employees' attendance, you need to set up the Cloud Attendance system before the employees can use Cloud Attendance via the LTS Connect Mobile Client. The system contains the access control devices, person information, shift settings, and access permission settings.

Note

A Service Provider can create such a system, add access control devices into the system, and hand it over to you. Contact your Service Provider if you want to deploy Cloud Attendance in your organization.

To set up the Cloud Attendance system, you need to add persons (employees and sub-administrators) to the system, assign persons to access groups, allow check-in/out on app, and assign shift schedules to persons on the LTS Connect Portal. For details, please visit https://www.LTS Connect.com/views/login/userManual/LTS Connect_en/index.html.
The following is the flow chart for deploying Cloud Attendance:

Figure 7-5 Flow Chart for Deploying Cloud Attendance



7.6.1 Check In/Out Remotely

You can check in or check out directly on the Mobile Client without actually presenting or authenticating at an attendance check device.

Ask Administrator to Enable Check-In/Out on Mobile Client

If you cannot see the **Check In** tab, it means that you do not have the permission to check in/out on the Mobile Client yet.

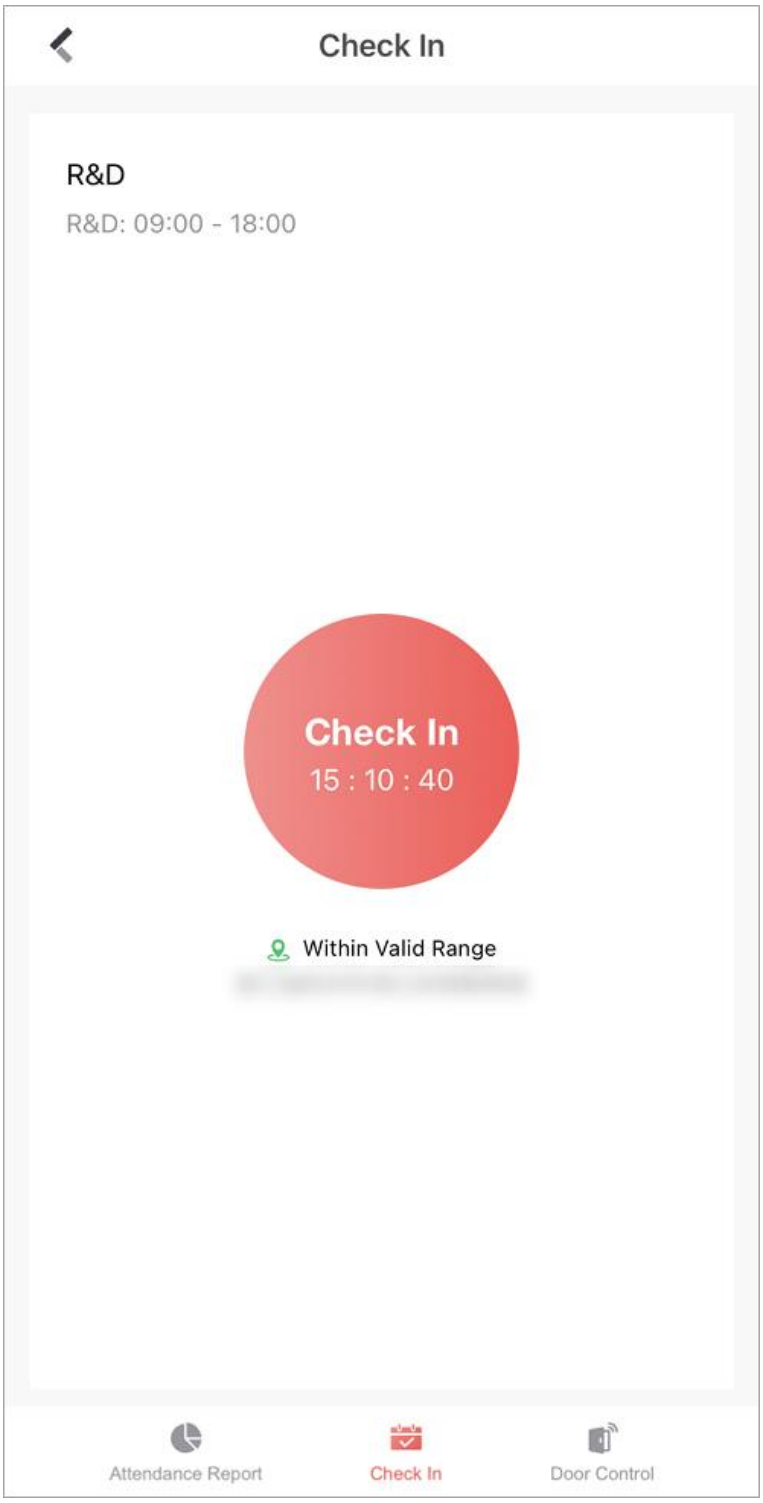


Figure 7-6 Check In Tab in Cloud Attendance

You can ask the administrator of the attendance system to enable **Check-In/Out by Mobile Client** for you on the LTS Connect Portal. The administrator also needs to set the locations of each attendance site and the valid check-in range.

If the attendance system has no attendance check device added, you cannot check in/out on the

Mobile Client even if the feature is enabled for you.

Figure 7-7 No Attendance Check Device

Check In/Out on the Mobile Client

If you have acquired the permission to check in on the Mobile Client, you can tap **Check In** whenever you are within the valid check-in range of any attendance site.
After checking in/out, you can view the recent attendance records.

Figure 7-8 Pop-Up Notice on Recent Check-In/Out

If You are not Within Valid Range...

If you are not within the valid check-in range of any attendance site, check-in/out will be unavailable.

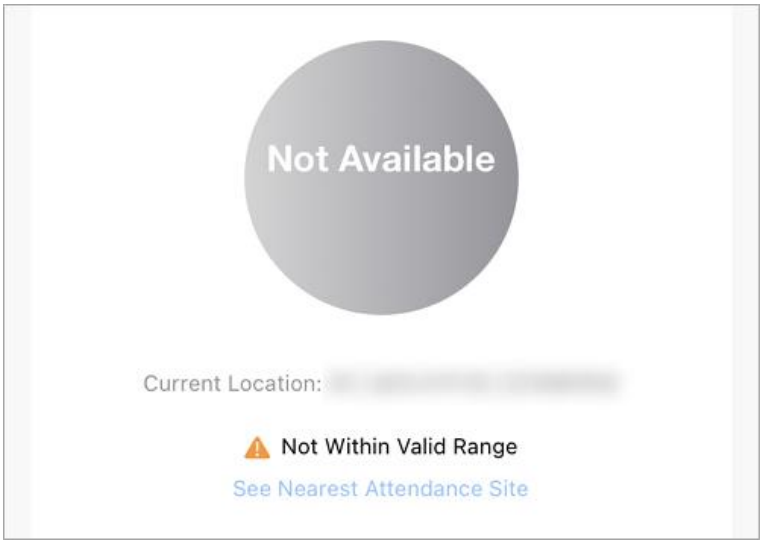


Figure 7-9 Check-In/Out Unavailable

You can tap **See Nearest Attendance Site** to check the nearest site for checking in/out.

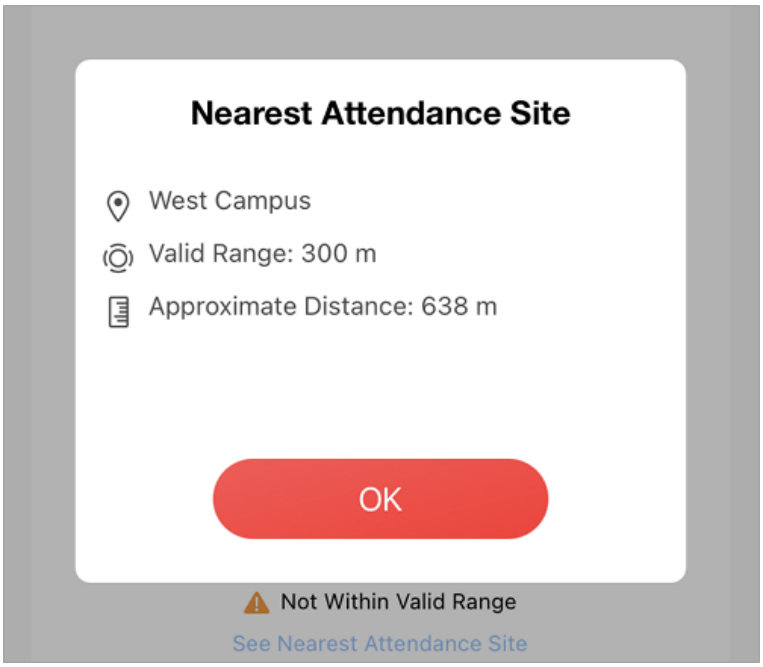


Figure 7-10 See Nearest Attendance Site

If You are Working from Home or on a Business Trip...

If you are not required to work at a fixed location, the administrator can enable **Allow Offsite Check-In** for you.
You can tap **Check In Offsite** to check in outside the valid check-in range of any attendance site.

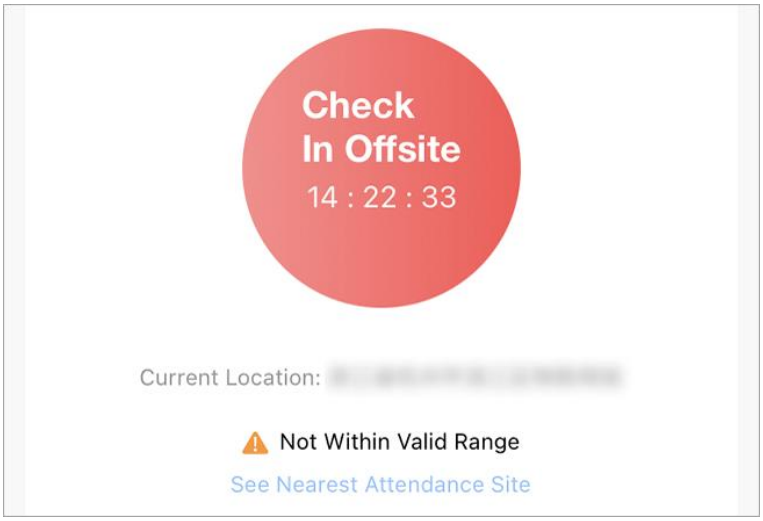


Figure 7-11 Check In Offsite

7.6.2 Open Door Remotely

You can control the status of doors in the Cloud Attendance system. You can also see the live

video of a door before you open it.

Before You Start

Make sure the administrator has granted the following permissions to you: Remotely Open Door and Remote Live View.

Steps

1. Go to **Cloud Service** → **Cloud Attendance** → **Door Control**.
   You can see the live view of the access control devices.
2. Control door status.

   Remain Open

   Keep the door open.

   Open Door

   Open the door temporarily.

   Remain Closed

   Keep the door closed.

7.6.3 Add Face Picture for Face Recognition

The administrator of the Cloud Attendance system can add a face picture in your person information, so that you can use face recognition for access control and time attendance. If the administrator did not add a face picture for you, you can add it by yourself.

Steps

Note

If you are the administrator of the Cloud Attendance system, use LTS Connect Portal to add employees' face pictures. You shall ensure that you have obtained the explicit consent from the data subject before you upload the face image and that you have performed the DPIA (Data Protection Impact Assessment) where applicable beforehand.

1. Go to **Cloud Service** → **Cloud Attendance**.
2. Tap to enter person information page.
3. Tap **Add Face Picture** and follow the instructions on screen to finish the process.

7.7 People Counting

People Counting works with people counting cameras. It is designed for monitoring crowd density in order to achieve "social distancing" in workplaces, businesses, and public spaces. On the LTS Connect Mobile Client, you can see the real-time number of people staying in an area, set the maximum number of people allowed to stay in the area, and get alerts when more people are

present.

Note

Contact your Service Provider if you want to deploy People Counting in your space.

To check over-limit records, tap **Message and Report**. You can filter the records by dates and people counting groups.

Note

- An over-limit record contains information such as the name of people counting group, device name, alarm time, actual number of people, and the alarm threshold you set.
- Over-limit records can be kept for up to 30 days.

To send a copy of the records, tap and enter your email address.

Note

The records will be saved as an Excel file.

7.8 Temperature Screening

Temperature Screening works with temperature screening devices and thermographic cameras. It is designed for contact-less skin-surface temperature measurement and detection of protective face masks so as to achieve preliminary screening in public areas with high efficiency. On LTS Connect Mobile Client, you can see the screening results in real-time, set a threshold temperature, and receive abnormal temperature alarms and no-mask alarms.

Figure 7-12 Temperature Screening and Mask Detection

Note

- Temperature Screening is not available in all countries or regions.
- Contact your Service Provider if you want to deploy Temperature Screening in your space.

To check the records of abnormal temperature alarms and no-mask alarms, tap **Message and Report**. You can filter the records by dates, alarm types, and devices.

Note

An alarm contains information such as device name, alarm time, alarm type, and body temperature.

To send a copy of the records, tap and enter your email address.

Note

The records will be saved into an Excel file.

Chapter 9 Manage Access Control Devices

Access control is the selective restriction of access to a place or other resources. After adding access control devices to the Mobile Client, you can remotely control the doors, and configure duration in which the doors remain open. You can also filter and view access control device's logs, which provide the information of access events and related alarms, such as access controller tampering alarms.

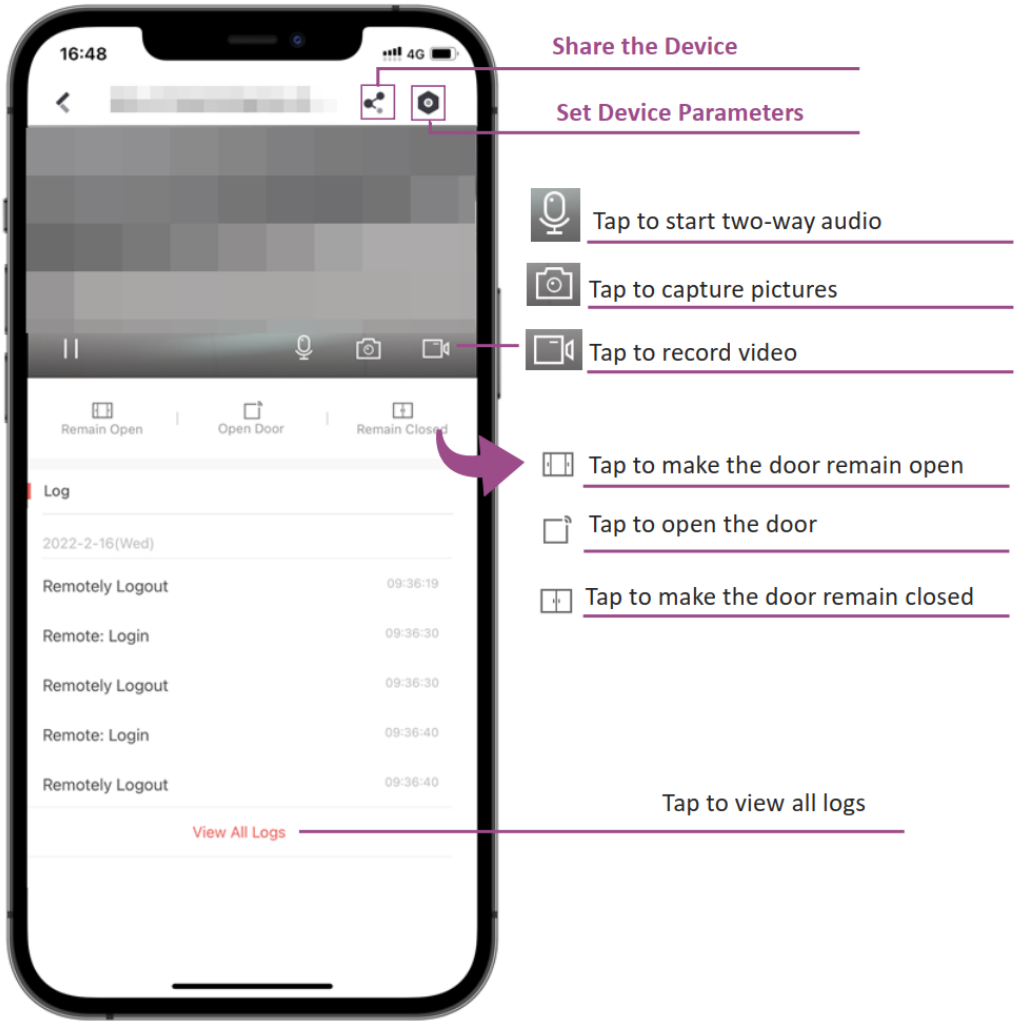


Figure 9-1 Access Control

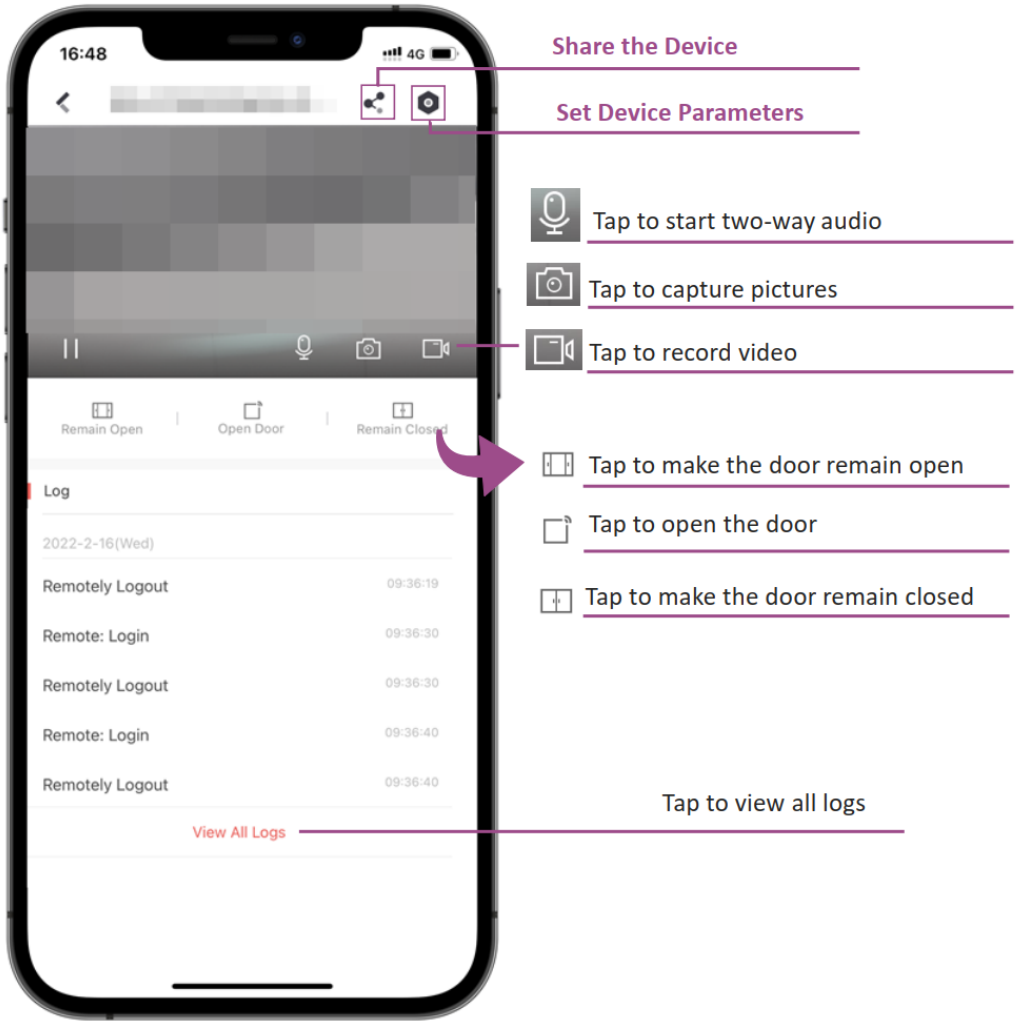


Figure 9-2 Access Control

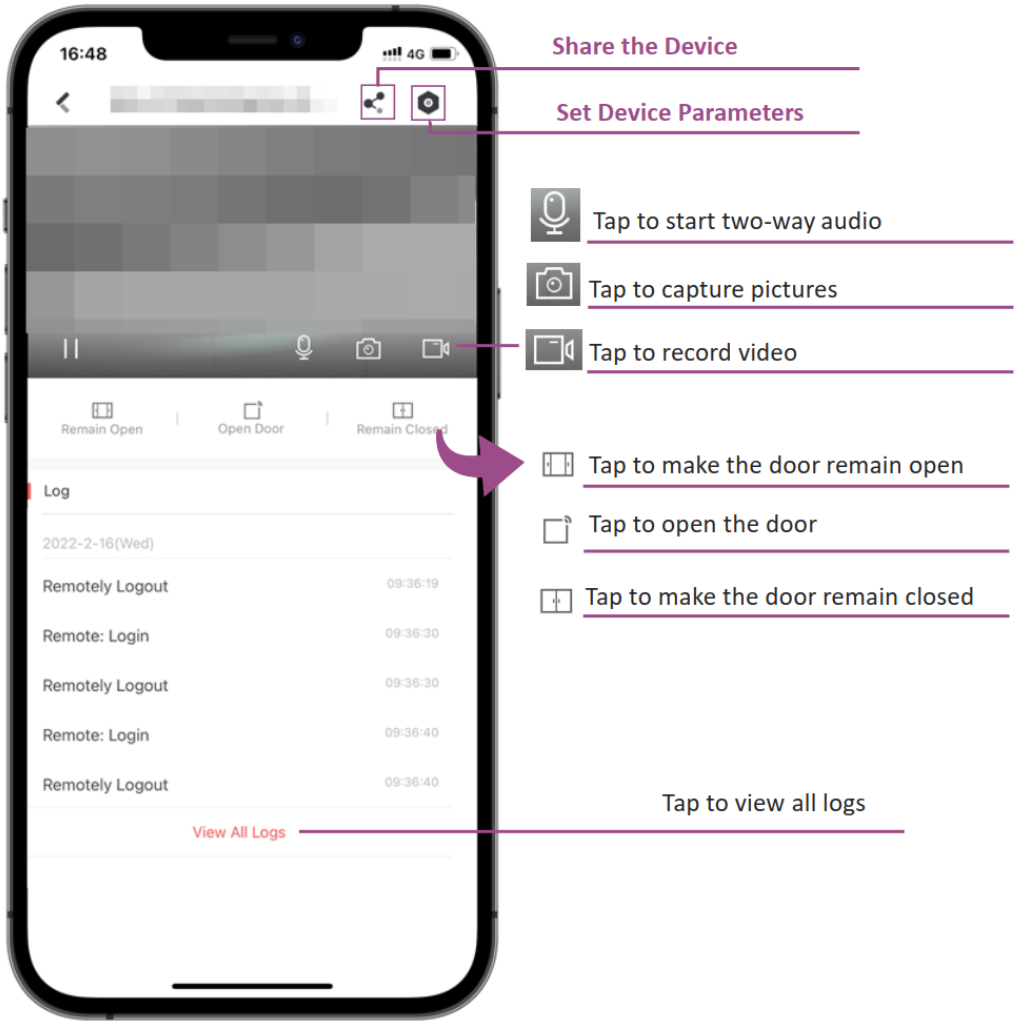


Figure 9-3 Access Control

Besides the above-mentioned functionality, you can change the supper password of the access control device. And for face recognition terminals, you can enable fingerprint authentication or facial authentication to open doors.

9.1 Control Door Status

The Mobile Clientsupports controlling the status of the access control devices' related doors by the super password of the device.

Steps

Note

You can change the super password. See ***Change Super Password*** for details.

1. On the device list page, tap  on the right of the access control device to enter the door control page.

Note

The door icon varies with different door status.

2. Control the door status.

Remain Open

Keep the door open.

Open Door

Open the door for a configurable time period. When the time period expires, the door will close.

Note

For details about configuring the time period, see ***Set Door Open Duration***.

Remain Closed

Keep the door closed. In this status, the door can only be opened by super card or super password.

Note

For details about super card, see the user manual of the access control device.

3. Enter the super password.

Note

- For face recognition terminal, this step is not required. You can control door status directly in step 2.
- By default, the super password is the device verification code. You can change the super password. See ***Change Super Password*** for details.

The door status will change.

9.2 Set Door Open Duration

You can set the door open duration for the access control device. When the duration expires, the

door will close automatically.

Steps

1. On the device list page, tap to enter the Settings page of the access control device.
2. Tap **Door Open Duration** to open the Door Open Duration list.
3. Select a duration from the list.
4. Tap to confirm the selection.
   If you tap **Open Door** in the door control page, the door will open for the configured time duration.

Note

For details about controlling door status, see ***Control Door Status***.

9.3 Change Super Password

The Mobile Client allows you to change the super password of the access control device, which can be used to open all the access control points (e.g., doors), even when the access control point is in remaining closed status.

Steps

Note

For details about super password of the access control device, see the user manual of the device.

1. On the device list page, tap to enter the Settings page of the device.
2. Tap **Change Password** to enter the Change Password page.
3. Enter the old password and tap **Next**.

Note

If it is the first time to set the super password, skip this step.

4. Create a new password and then tap **Finish**.

Note

The password should contain 6 numbers.

9.4 View Access Control Logs

You can view the access control device's logs including the access control events and alarm

information. You can also filter the logs.

Steps

1. On the device list page, tap the door icon on the right of the access control device to enter the door control page.

Figure 9-4 The Icon Representing Door

   The log list will be displayed on the Log section of the page.
2. Perform the following operations.

Refresh Log List	Swipe the log list downward to refresh it.
View All Logs	Tap **View All Logs** to enter the Log page and view all access control device logs.
Filter Logs	On the Log page, tap **Filter** and then set the filtering condition (time and event type) to filter.

9.5 Enable Opening Door via Touch ID (or Face ID) Authentication

After adding face recognition terminals to the Mobile Client, you can enable opening door via Touch ID authentication or Face ID authentication.

Note

Your phone or tablet should support Touch ID authentication or Face ID authentication.

After adding a face recognition terminal, when you open the device's related door for the first time, a prompt will pop up asking you whether to enable opening door via Touch ID authentication or Face ID authentication or not. You can follow the prompt to enable this function.
If you have ignored the above-mentioned prompt, you can tap to enter the Settings page, and then switch on the function.

Chapter 10 Video Intercom

The Mobile Client supports video intercom functions. Video intercom is an audiovisual communication and security technique used in a building or a small collection of buildings. With microphones and video cameras at both sides, it enables the intercommunication via video and audio signals.

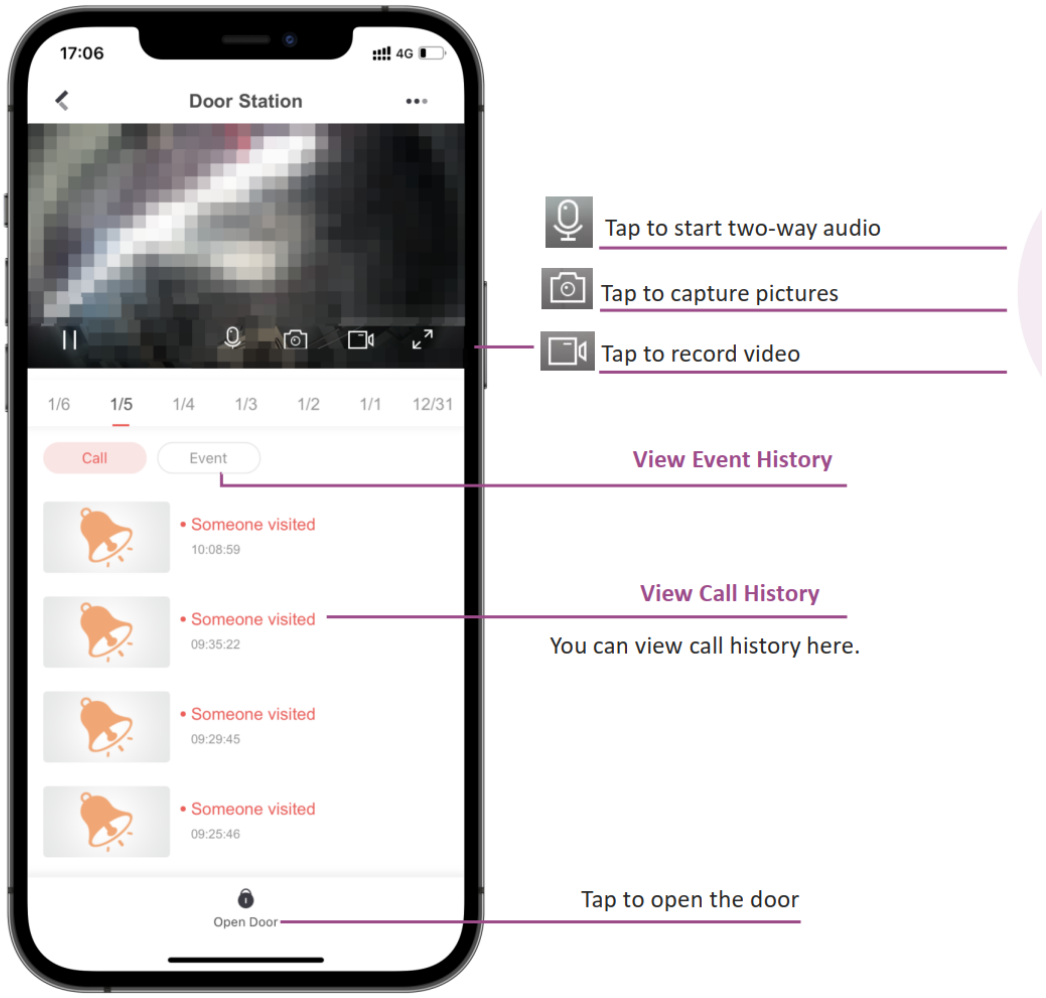


Figure 10-1 Video Intercom

10.1 Answer Call from Indoor Station

If no one answers the call via the indoor station for a while, the call will be forwarded to the Mobile Client. You can answer the call, view the live video of the door station, as well as open the

door.

Steps

Note

Up to 6 users can view the live video of the same door station at the same time. If there's already been 6 users viewing the live video, you can only use the audio function of the video intercom device.

1. Tap the call message to enter the following page.

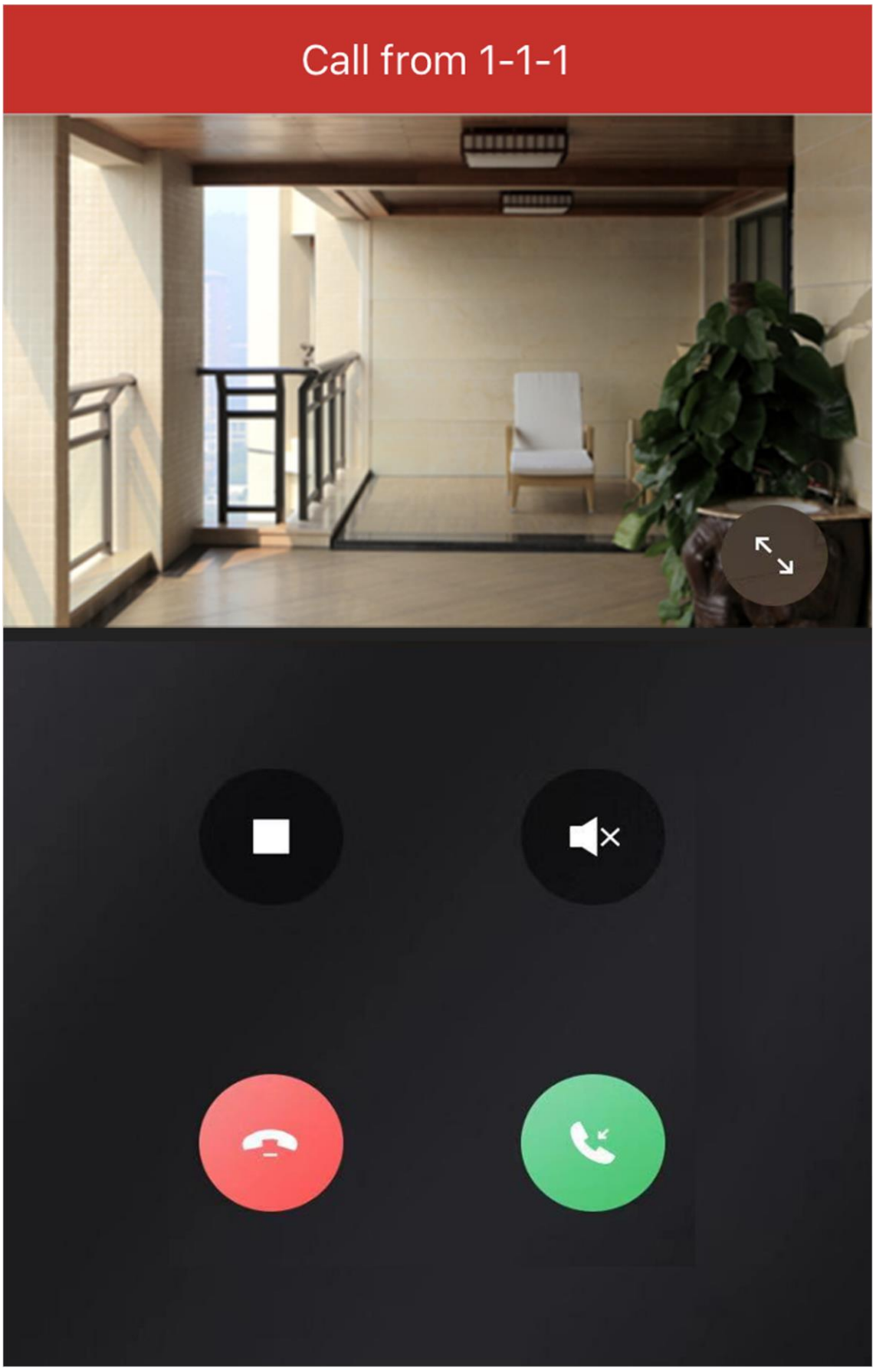

Call from 1-1-1

Figure 10-2 Call Page

2. Answer the call.
3. Optional: Perform the following operations.

Stop/Restart Live View	Tap to stop the live view. And tap to restart it.
Mute	Tap to mute the live video.
Open Door	Tap to open the door.
Digital Zoom	Pinch two fingers together to zoom in the live video image, and spread them apart to zoom out.

10.2 Operations on Device Details Page

On the device details page of the video intercom devices, you can perform the operations including viewing the live videos streamed from the cameras linked to the door stations or doorbells, starting two-way audio, playing back video footage, viewing call logs and history events, controlling doors linked to door stations, and controlling relays connected to the indoor station. Tap the video intercom device on the device list to enter the device page.

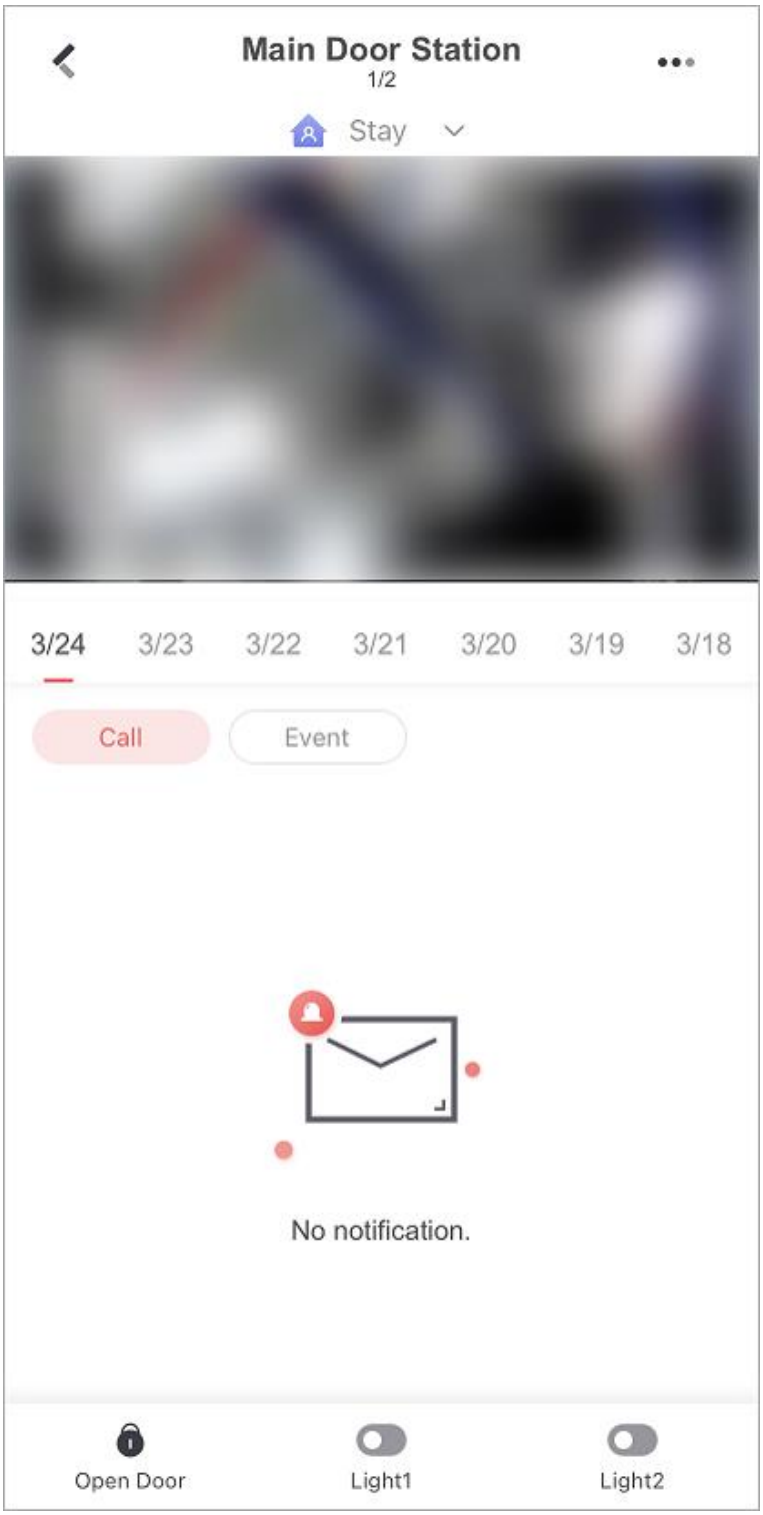


Figure 10-3 Video Intercom Device Page

Switch Scene

You can tap ⌄ to set **Stay**, **Away**, **Sleep**, or **Custom** as the scene for arming the detectors linked to the door station.

Stay

When the people stays inside the detection area, turn on the Stay mode to turn on all the perimeter burglary detection (such as perimeter detector, magnetic contacts, curtain detector in the balcony). At the meantime, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarm will not be triggered.

Away

When all the people in the detection area leave, turn on the Away mode to arm all zones in the area after the defined dwell time. For example, assume that you have set your apartment as a zone, you can set the zone status to Away when you go to work.

Sleep

The detectors in the bedroom is bypassed while the detectors in other rooms are armed. In this scene, all the perimeter burglary detection in other rooms are turned on, while no alarms will be triggered within the bedroom.

Live View

The live video will start playing when you enter the device details page. You switch live videos if multiple door stations are linked to the video intercom device.
During live view, you can tap the image to show the hidden icons, and then perform operations such as starting two-way audio, capturing picture, recording, full-screen live view, and setting image quality.

Note

For details about the above-mentioned operations during live view, see ***Start Two-Way Audio***, ***Capturing and Recording***, ***Set Image Quality for Device Added by IP/Domain***, and ***Set Image Quality for LTS Connect Device***.

Playback

Tap ••• → **Playback** to start playing back video footage.

View Call Logs and Events

You can view the call logs and device-related events in the latest 7 days (the events or call logs of the current day will be displayed by default).

Control Door

You can tap to control the door linked to the video intercom device.

Control Relay

You can tap to control the connected relays of an indoor station remotely.
To set up relay name and open duration, go to the Settings page of the video intercom device.
Open duration for a relay:

- Remain Open: The relay will not be closed automatically after you open it.
- 0-180s: The relay will be closed automatically after the open duration.

10.3 Set Motion Detection Alarm for Wi-Fi Doorbell

Motion detection is a way of detecting motion in a surveillance scene by analyzing image data and differences in a series of images. After setting motion detection area for Wi-Fi doorbell, the device will be able to detect the object in motion and at the same time the Mobile Client will receive an event notification about the motion detection alarm.

Steps

1. On the device list page, tap to enter the Settings page of the Wi-Fi doorbell.
2. Tap **Notification** to enter the Notification page.
3. Draw motion detection area.
   1) Tap **Draw Motion Detection Area** to enter the Motion Detection Area page.

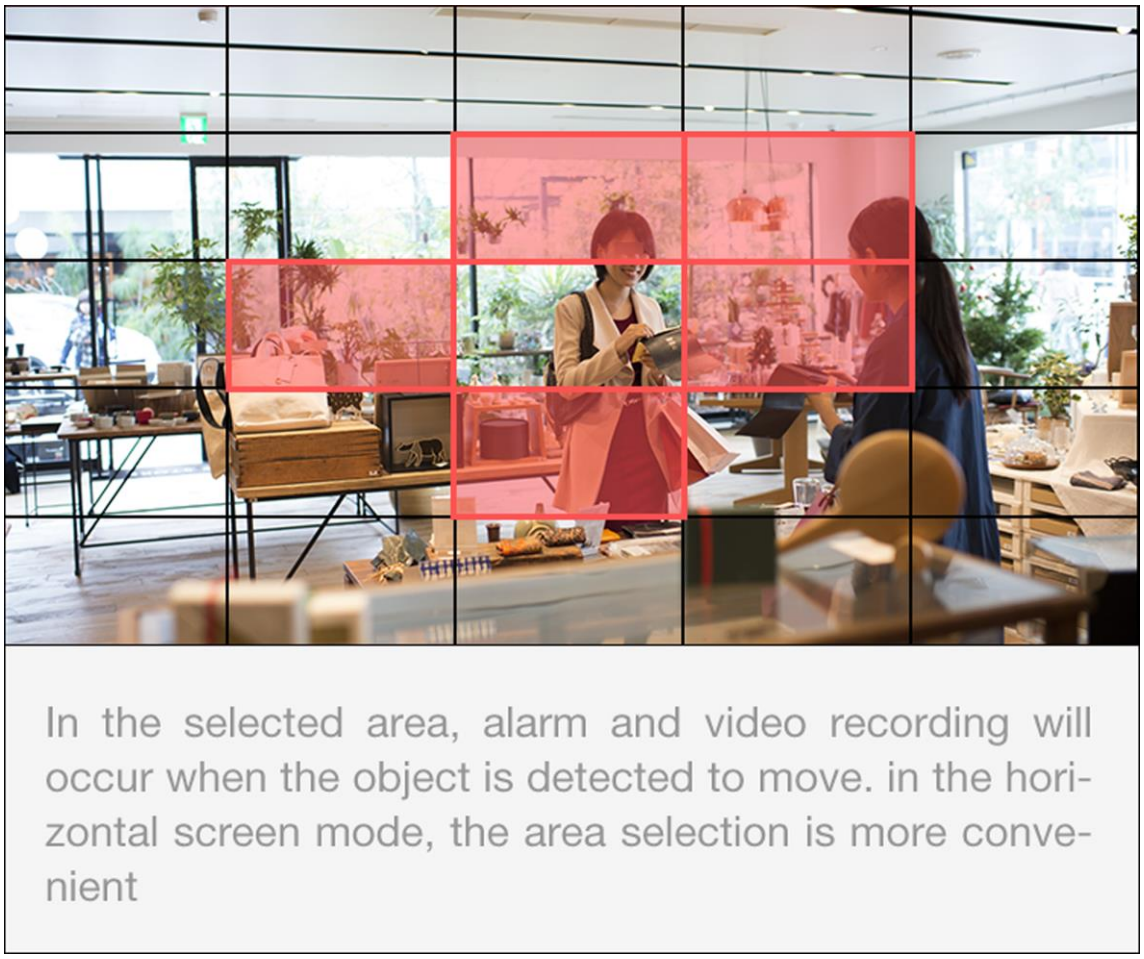


Figure 10-4 Draw Motion Detection Area

   2) Tap the grid(s) on the live video image to select the motion detection area.
   3) Tap to save the settings.
4. Tap **Motion Detection Sensitivity** on the Alarm Notification page and then drag the slider to adjust the sensitivity.

   Low

Moving persons, large moving pets, and any other large moving objects in the motion detection area will trigger the alarm, while smaller objects will not.

Medium

Moving small pets and any other medium-sized moving objects in the motion detection area will trigger the alarm, while smaller objects will not.

High

Moving insects, moving leaves, and any other larger objects will trigger the alarm.

What to do next

Go back to the Notification page and make sure **Notification** is enabled.

Note

For details about how to enabling notification, see ***Enable Notifications***

10.4 Set Volume for Video Intercom

You can set video intercom volume as required.

Steps

Note

Only video intercom devices support this function.

1. On the device list page, tap to enter the Settings page of a video intercom device.
2. Tap **Loudspeaker Volume** or **Microphone Volume** to adjust the loudspeaker and the microphone volume respectively.

10.5 Link Smart Chime with Doorbell

You can add a smart chime to the Mobile Client and link it with a doorbell so that the doorbell will standby for longer and be more responsive.

Add a Smart Chime

- To add an EZVIZ smart chime, tap → **Scan QR Code** on LTS Connect. Select Doorbell as the Device Type, enter the serial number, tap **Add**.
- You can also tap → **Manual Adding** to add a smart chime.

After adding a smart chime, you can tap the smart chime in the device list to mute all devices with one tap and enable/disable Ring Alert for linked doorbells.

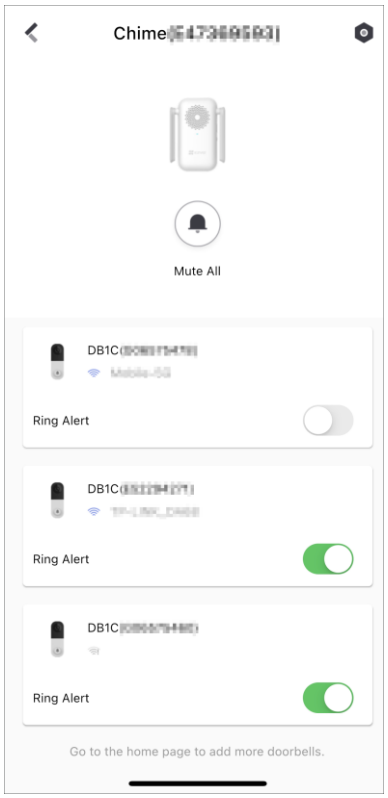


Figure 10-5 View Smart Chime

Link Smart Chime with Doorbell

- After successfully adding a smart chime, tap **Next** and link the smart chime with up to two doorbells.

Figure 10-6 Link Doorbell

- You can also go to the doorbell Settings page and tap **Chime Type** → **Smart Chime** to link a smart chime with the doorbell.

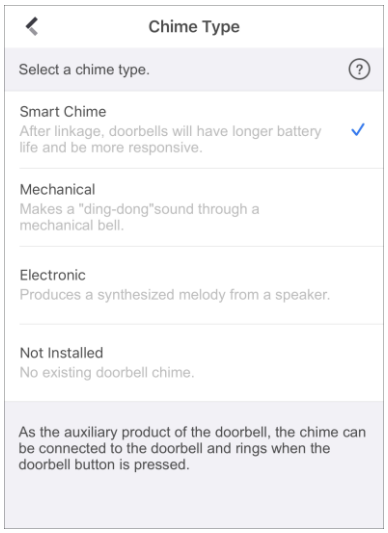


Figure 10-7 Link Smart Chime

Note

When you link a smart chime with a doorbell, make sure they are near to each other and they are both online.

Chapter 11 Router

You can establish a wireless network by setting up a LTS router.

Add and Set Up a Router

You can add a new router to the Mobile Client, so that you can set up your wireless network with just a few taps and manage the router right on your phone.
See details in ***Add and Set Up a Router***.

Check the Network Speed and Connected Devices

After adding the router, it will show up in the device list.

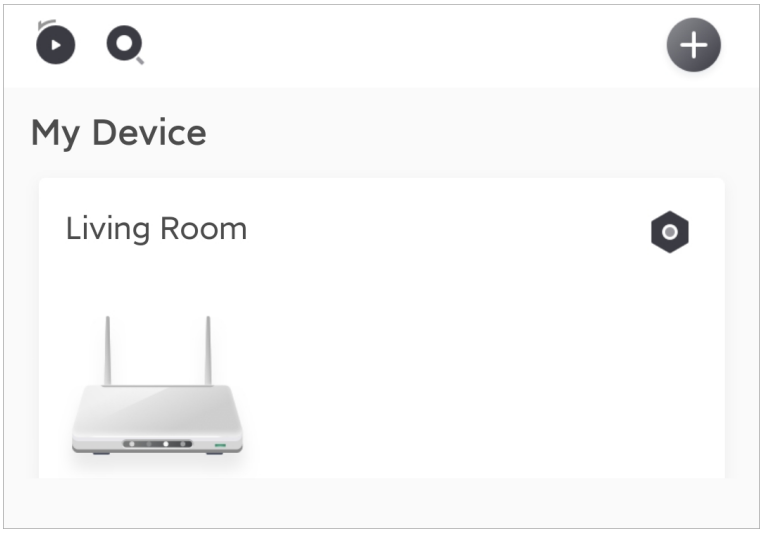


Figure 11-1 Device List

You can tap on the router to see its network speed and connected devices.

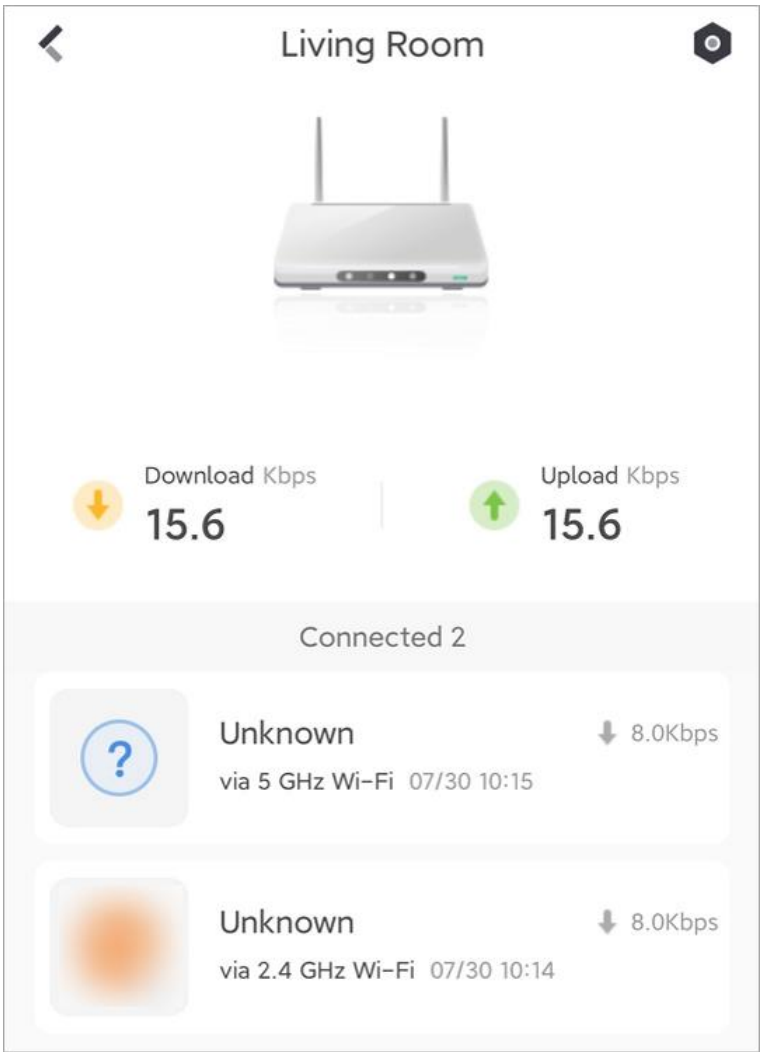


Figure 11-2 Connection Details

Tap on a connected device, you can see its connection details, limit the connection speed, or add the device to the blocklist.
See details in ***Manage the Devices Connected to a Router***.

Change the Wi-Fi Name, Security Mode, Password, and Bands

You can set theWi-Fi name, security mode, and password of a router in Wi-Fi settings. You can also hide the Wi-Fi from other people's Wi-Fi list. If your router supports the5 GHz Wi-Fi, you can also enable the5 GHz Wi-Fi for higher data rates.
See details in ***Wi-Fi Settings of a Router***.

Change the Internet Connection Type

You can set the Internet connection type to PPPoE, dynamic IP, or static IP in Internet Settings.
See details in ***Internet Settings of a Router***.

Set Up a Guest Wi-Fi for Visitors

You can set up a guest Wi-Fi to securely separate visitors' Wi-Fi connection from yours. You can

also control the validity period and bandwidth limit of the guest Wi-Fi.
See details in ***Set Up a Guest Wi-Fi for Visitors***.

Improve the Network Quality with Wi-Fi Speedup

If the Wi-Fi connection is slowing down and becoming unstable, you can use Wi-Fi Speedup to improve the network quality.
See details in ***Wi-Fi Speedup***.

Secure the Network with Security Checkup

Security Checkup examines the overall security level of your router and wireless network, and provides recommendations to guide you secure your network.
See details in ***Security Checkup***.

Check the Internet Connection Details

Tap **Status** on the settings page of your router. You can see the overall status, speed, duration, connection type, IP address, subnet mask, network gateway,and DNS of the Internet connection.

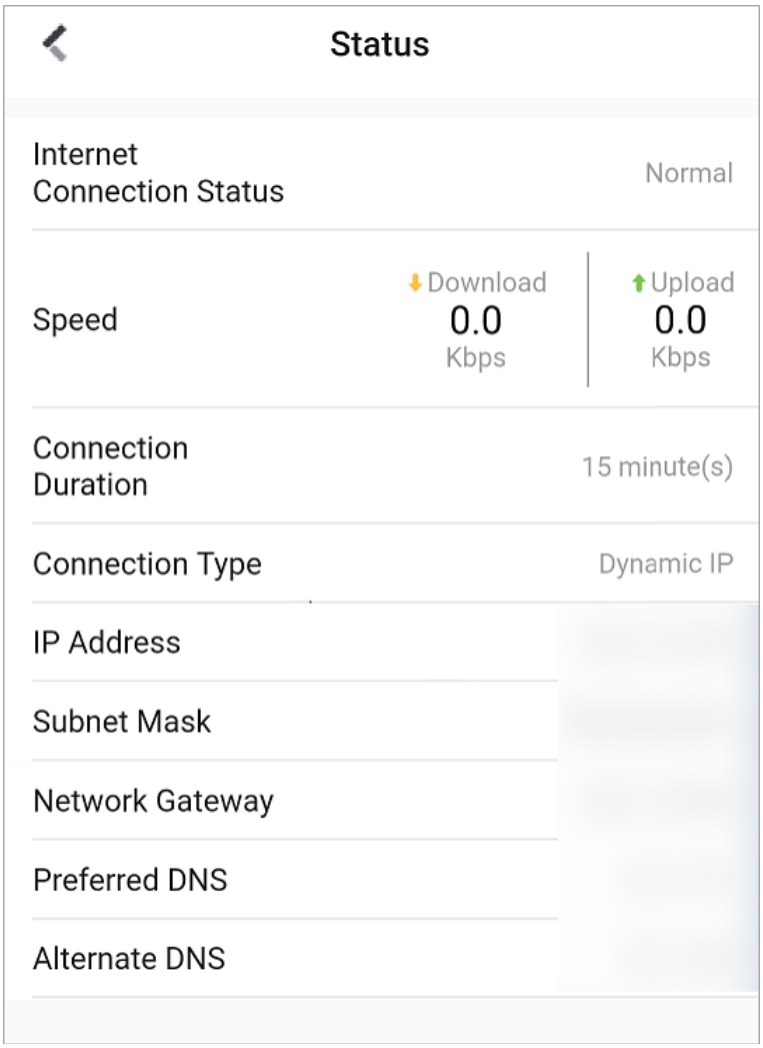


Figure 11-3 Status

Adjust the Wi-Fi Signal Strength

Tap **Wi-Fi Signal Strength** to select a signal strength mode: Power Saving, Standard, and High.

Set a Power-Off Schedule

Tap **Power-Off Schedule** on the settings page of your router to set a schedule to turn off the router during specific time periods in different days of a week.

Change the Admin Password

Tap **Change Admin Password** on the settings page of your router to set a new Admin password.

Restart the Router

Tap **Restart** on the settings page of your router to restart it.

Factory Reset the Router

Tap **Factory Reset** on the settings page of your router to reset the router to its factory state.

Note

A factory reset will erase all settings on the router. You have to add and activate the router again if you still want to manage the router on the Mobile Client.

11.1 Add and Set Up a Router

You can add a new router to the Mobile Client, so that you can set up your wireless network with just a few taps and manage the router right on your phone.
To add a LTS router, tap ⊕ → **Manual Adding**.
Select **Router** as the **Adding Type** and then join the Wi-Fi of the router (whose name usually starts with "LTS_").

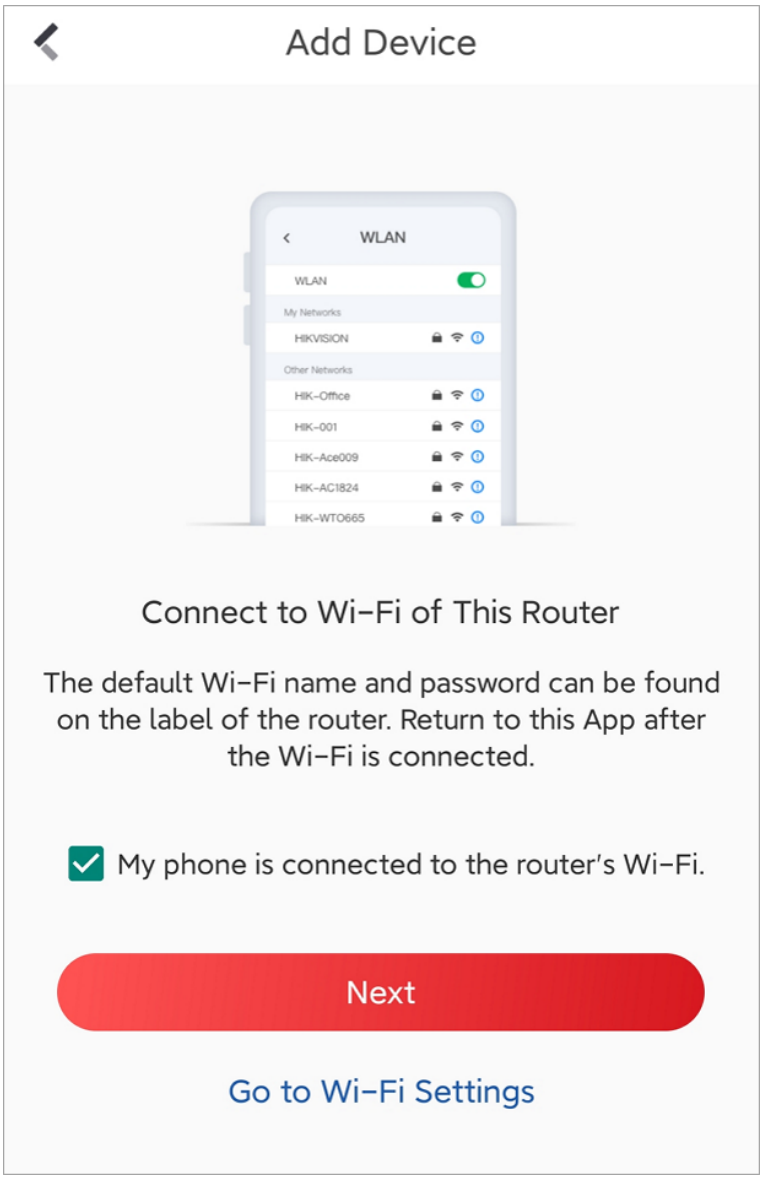


Figure 11-4 Add Device

During the process, you need to activate the router by setting an admin password, select the Internet connection mode (PPPoE, Static IP, or Dynamic IP), and set a Wi-Fi name and password.

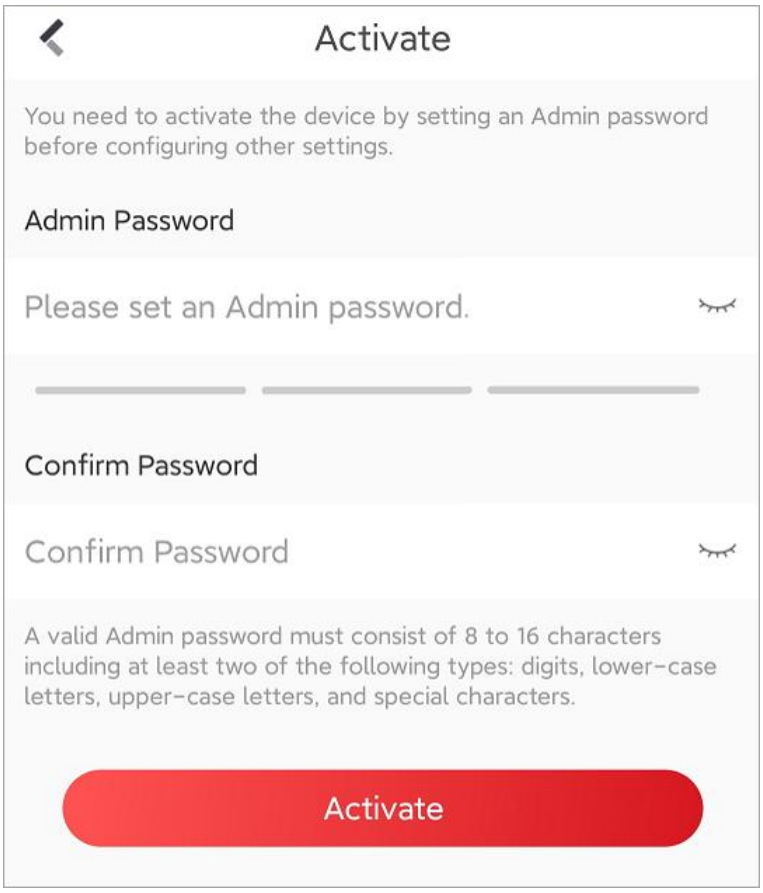


Figure 11-5 Activate Router

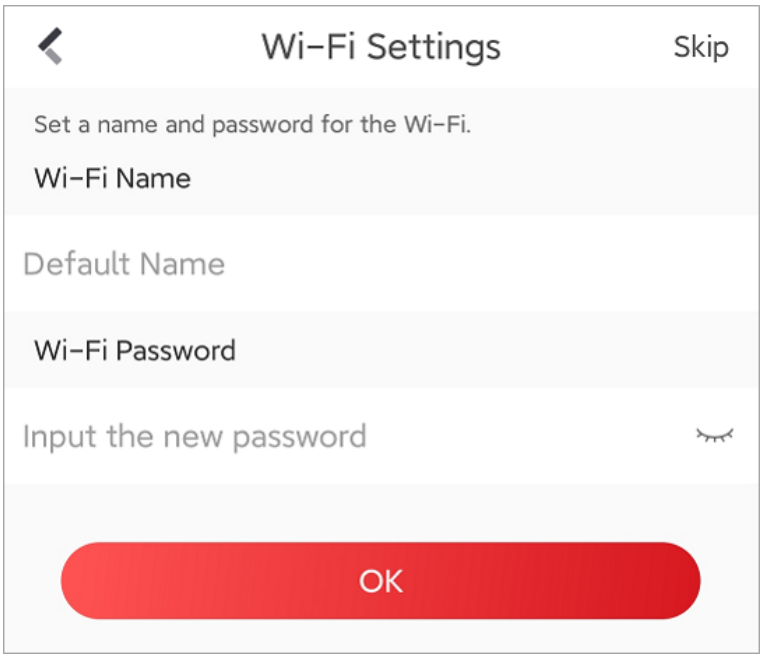


Figure 11-6 Set Wi-Fi Name and Password

Note

- Refer to ***Internet Settings of a Router*** if you need more information on Internet connection modes.
- After setting up the router, the router will restart. You need to re-connect to the Wi-Fi of the router before conducting further operations on the router.
- Routers are locally managed on the Mobile Client, so you can control or configure a router only when you connect your phone to the router's Wi-Fi.

11.2 Wi-Fi Settings of a Router

You can set theWi-Fi name, security mode, password, and bands of a router in Wi-Fi settings. You can also hide the Wi-Fi from other people's Wi-Fi lists.

Where is the Wi-Fi Settings?

Tap **Wi-Fi Settings** on the settings page of the router.

Options in Wi-Fi Settings

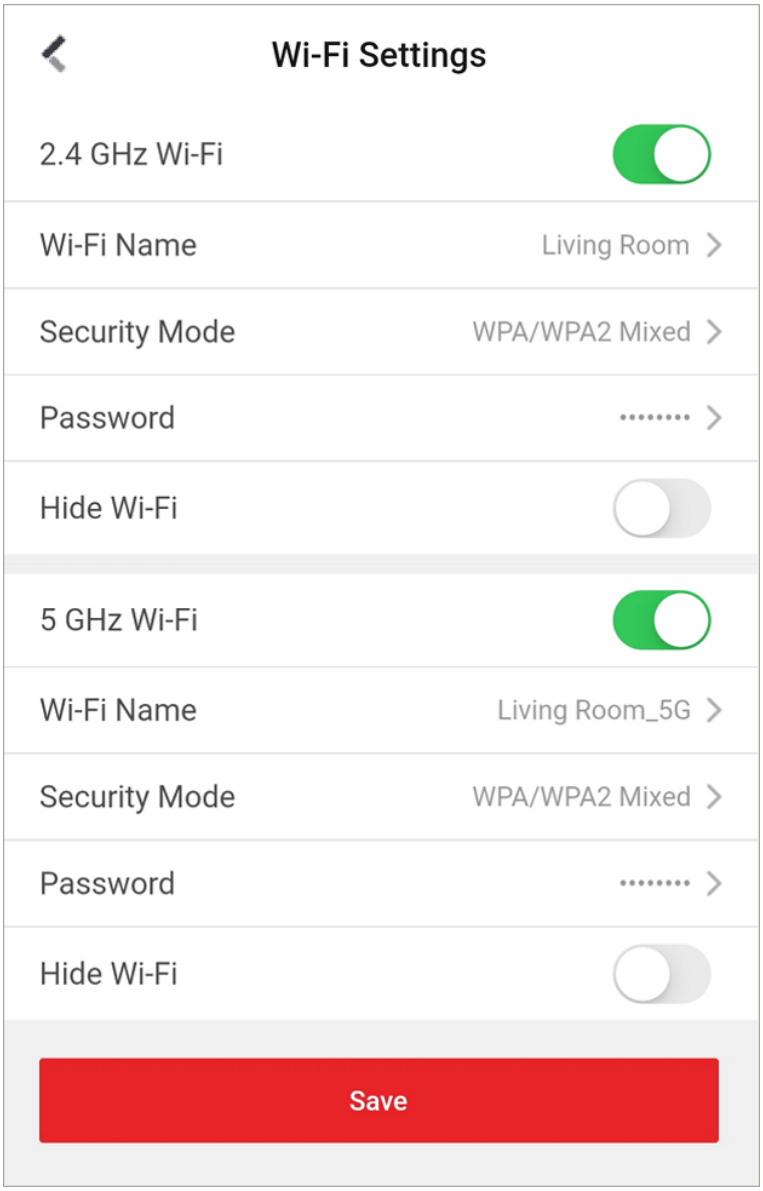


Figure 11-7 Wi-Fi Settings

2.4 GHz Wi-Fi / 5 GHz Wi-Fi

Enable or disable different bands of Wi-Fi signal.
Some models are equipped with the 5 GHz band, which supports a higher maximum data rates.
Tasks consuming a large amount of network traffic can benefit from the 5 GHz Wi-Fi network.

Wi-Fi Name

The Wi-Fi name will appear on the Wi-Fi list when you search for Wi-Fi connection.
TheWi-Fi name should contain 1 to 32 characters.

Security Mode

You can select None, WPA, WPA2, or WPA/WPA2 Mixed.

Caution

If you select **None**, your Wi-Fi network will be unprotected and open to anyone, which may cause security risks.

Password

Others must enter the password before connecting to the Wi-Fi.
The Wi-Fi password should contain 8 to 63 characters, excluding emoji or special characters.

Hide Wi-Fi

If you do not want your Wi-Fi network to appear on other people's Wi-Fi lists, you can hide the Wi-Fi.

11.3 Internet Settings of a Router

You can set the Internet connection type to PPPoE, dynamic IP, or static IP in Internet Settings.

Where is the Internet Settings?

Tap **Internet Settings** on the settings page of your router.

What Internet connection type should I select?

You need to select the type according to the current Internet service provided by your Internet Service Provider (ISP).

PPPoE

If your Internet service comes with an account name and password, select PPPoE.
ISP uses a PPPoE account to track the data traffic and bill each user. It is widely used in communities.

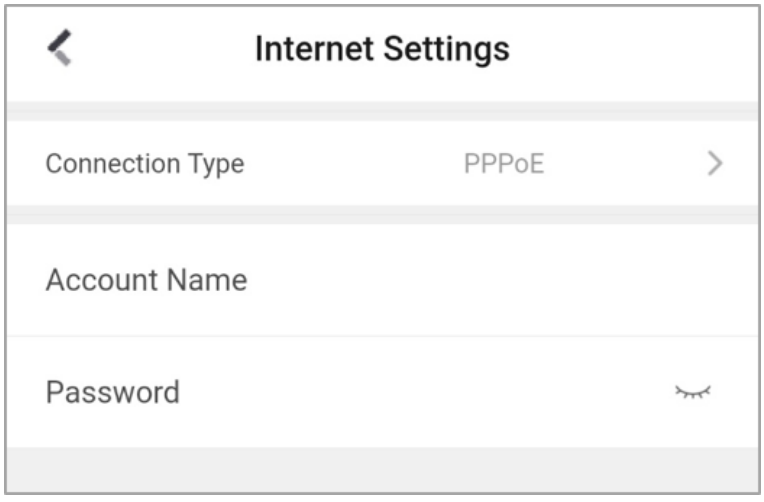


Figure 11-8 PPPoE

Dynamic IP

Also known as "DHCP". If your Internet service does not require any manual configurations to be connected, select Dynamic IP.

In this case, the ISP assigns a temporary IP address to you every time you try to connect to the Internet.

It is widely used in public spaces such as offices and hotels.

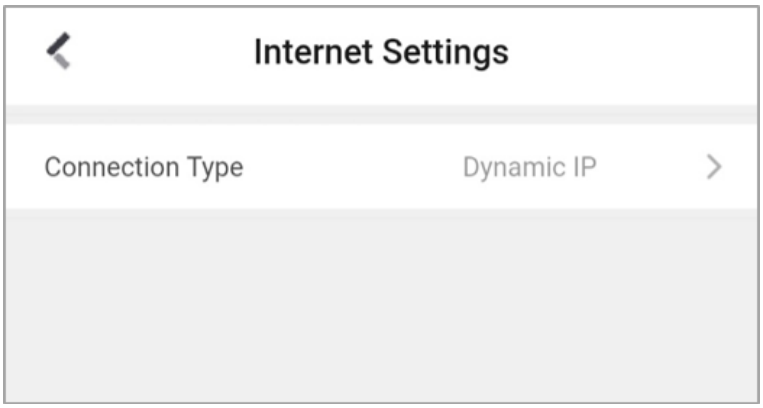


Figure 11-9 Dynamic IP

Static IP

If your ISP allocates a dedicated IP address to you, select **Static IP**.

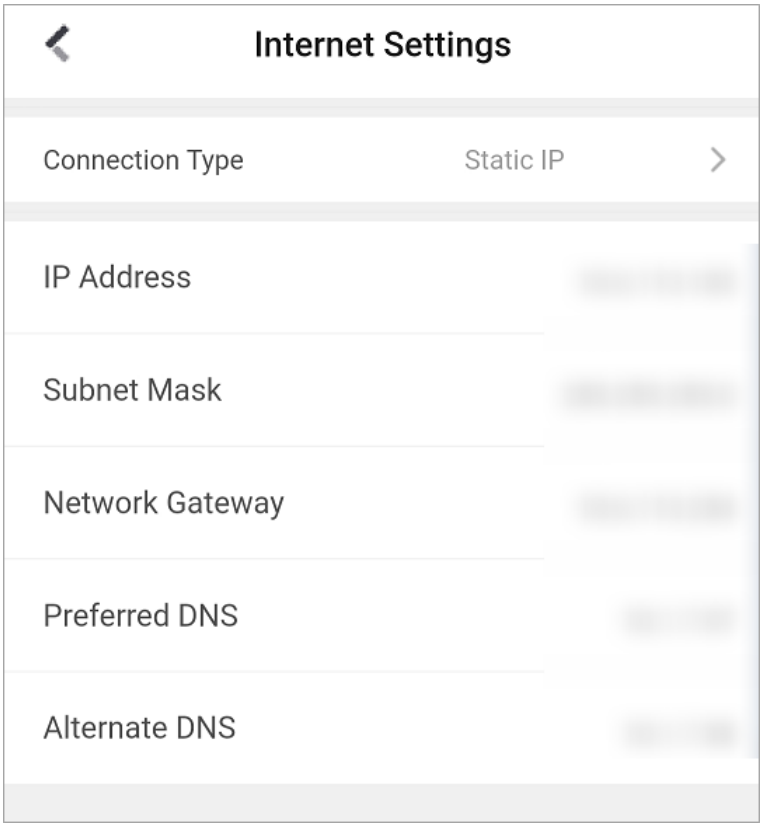


Figure 11-10 Static IP

11.4 Manage the Devices Connected to a Router

You can check which devices are connected to your router, and view the connection details of a particular device. You can limit the speed of the connected devices and add unwanted devices to the blocklist.

Where can I see the connected devices?

In the **My Device** list, tap on the router to see all devices connectedto it via the Wi-Fi or a network cable.

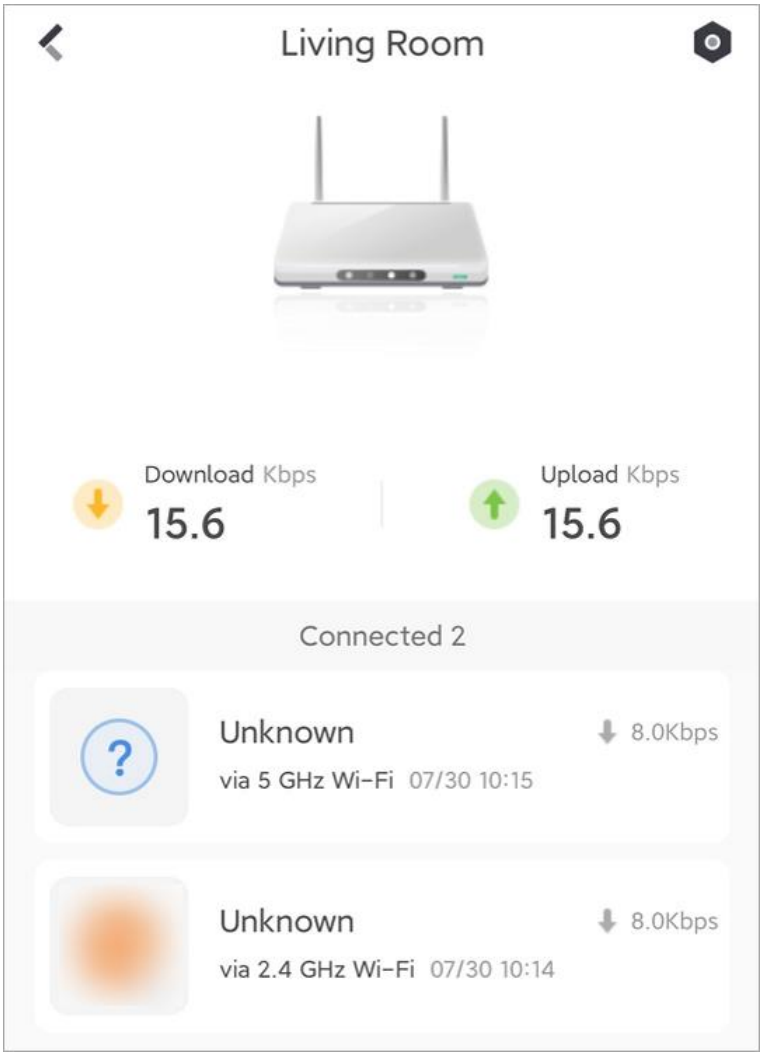


Figure 11-11 Connection Details

Check Device Connection Details

Tap on a connected device to see itsconnection details.

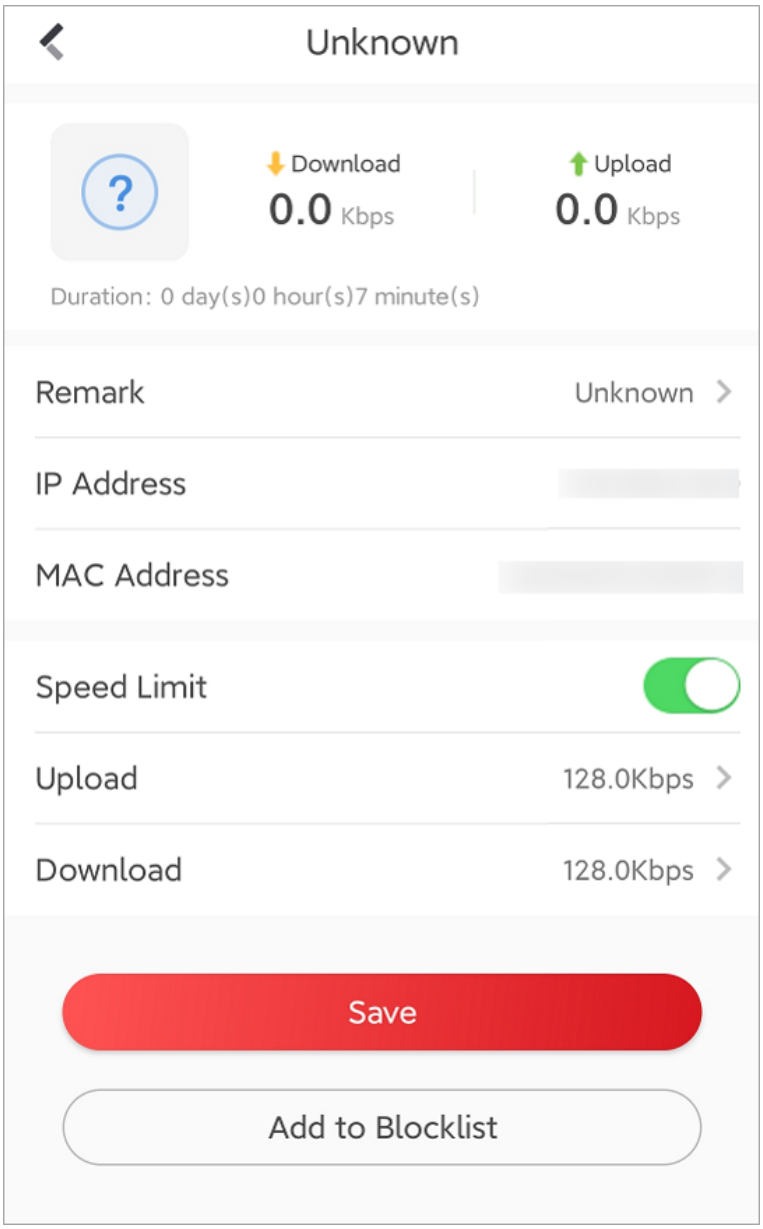


Figure 11-12 Device Connection Details

Limita Device's Connection Speed

You can switch on **Speed Limit** and set a limit for the download/upload speed of the device.

Add Device to the Blocklist

Tap **Add to Blocklist** so that the device cannot be connected to the Wi-Fiagain.
Tap **Remove from Blocklist** if you choose to allow the device to be connected to the router. You can also tap **Blocklist** on the settings page of the router to see all blocked devices.

11.5 Set Up a Guest Wi-Fi for Visitors

You can set up a guest Wi-Fi to securely separate visitors' Wi-Fi connection from yours.

Where can I set up the guest Wi-Fi?

To enable the guest Wi-Fi, go to the settings page of your router and tap **Guest Wi-Fi**.

Set Up the Guest Wi-Fi

In Guest Wi-Fi, you can set the name, password, validity period, and bandwidth limit of the guest Wi-Fi.

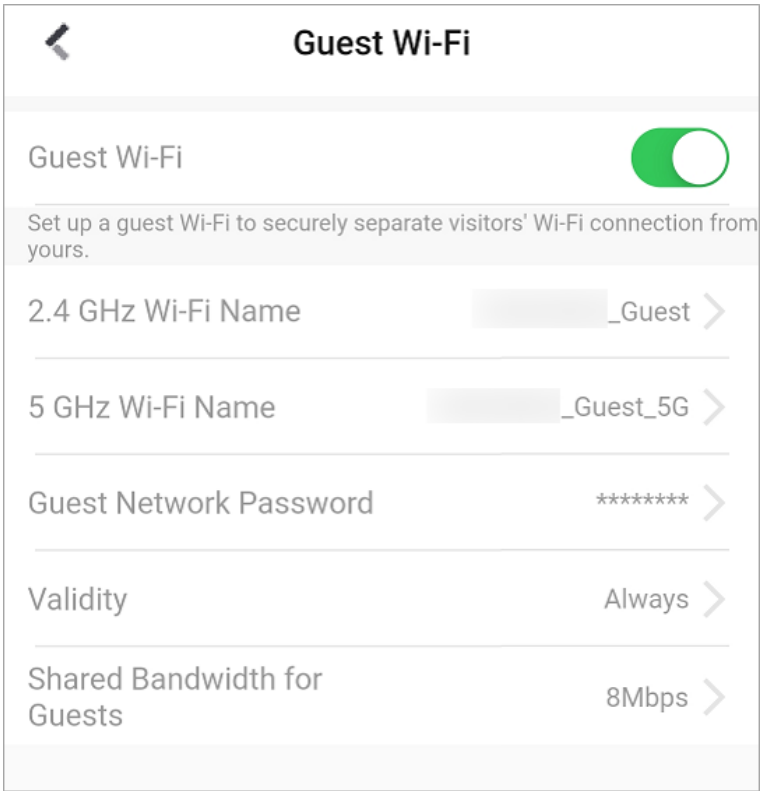


Figure 11-13 Guest Wi-Fi

11.6 Wi-Fi Speedup

If the Wi-Fi connection is slowing down and becoming unstable, you can use Wi-Fi Speedup to improve the network quality.

Where is Wi-Fi Speedup?

To use Wi-Fi Speedup, go to the settings page of your router and tap **Wi-Fi Speedup**.

How does Wi-Fi Speedup work?

Wi-Fi Speedup analyzes the signal interference, channel congestion, transmission speed, and

signal quality of your Wi-Fi network.
When the network condition is poor, you can optimize your Wi-Fi network with just one tap.

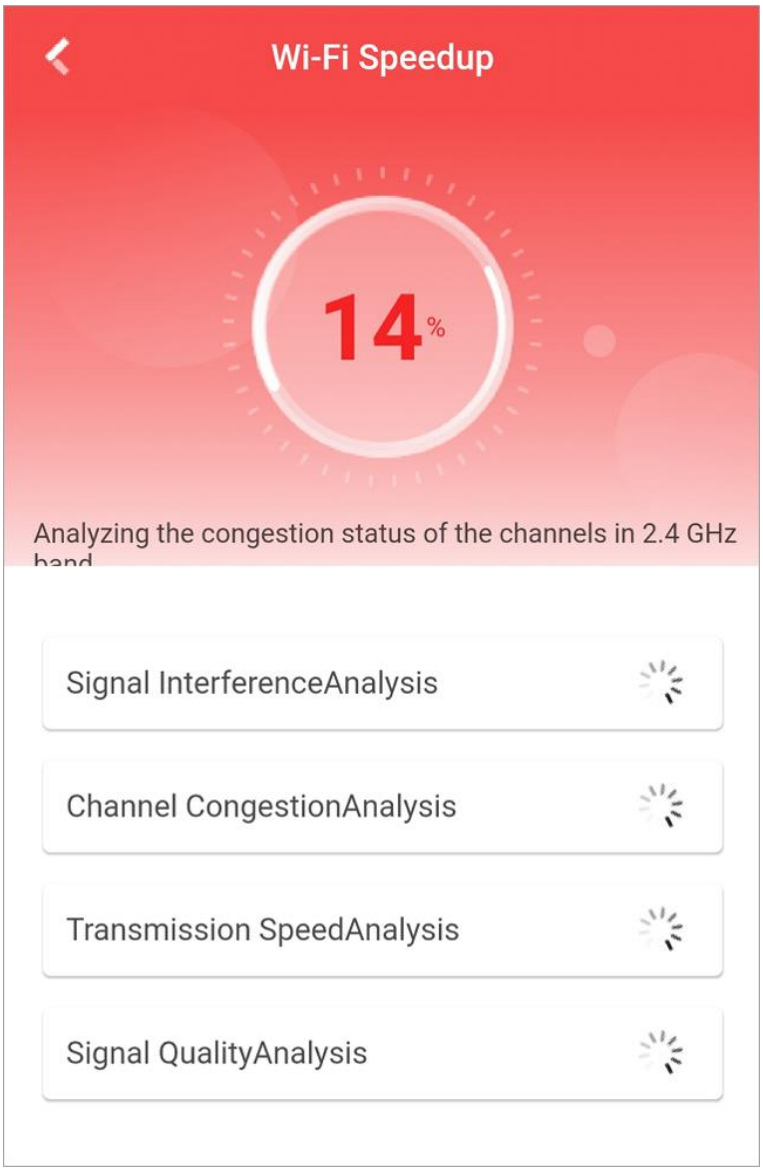


Figure 11-14 Wi-Fi Speedup

11.7 Security Checkup

Security Checkup examines the overall security level of your router and wireless network, and provides recommendations to guide you secure your network.

Where is Security Checkup?

To use Security Checkup, go to the settings pageof your router and tap **Security Checkup**.

How does Security Checkup work?

Security Checkup examines your password settings to prevent brute-force attacks onthe Wi-Fi password and admin password. Security Checkup also prevents system attacks, DNS hijacking, and redirection to phishing or malicious websites.

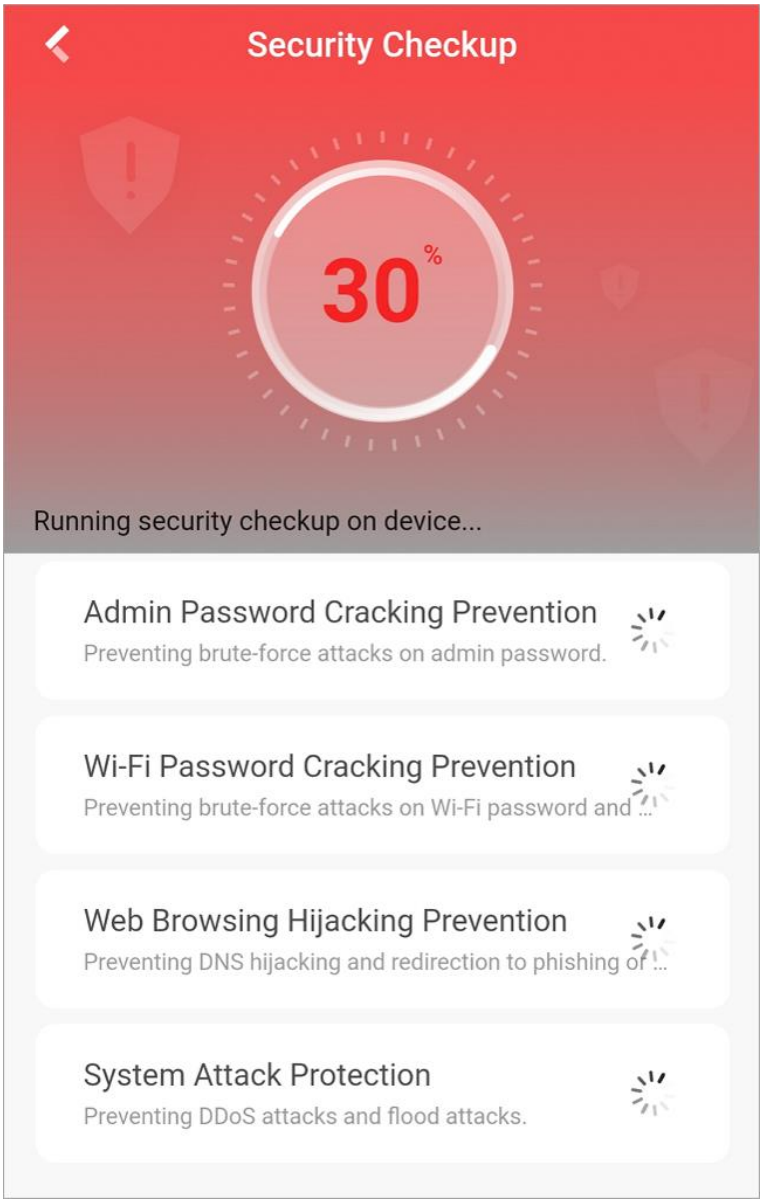


Figure 11-15 Security Checkup

If security threats are detected, Security Checkup will provide recommendations to guide you secure your network.

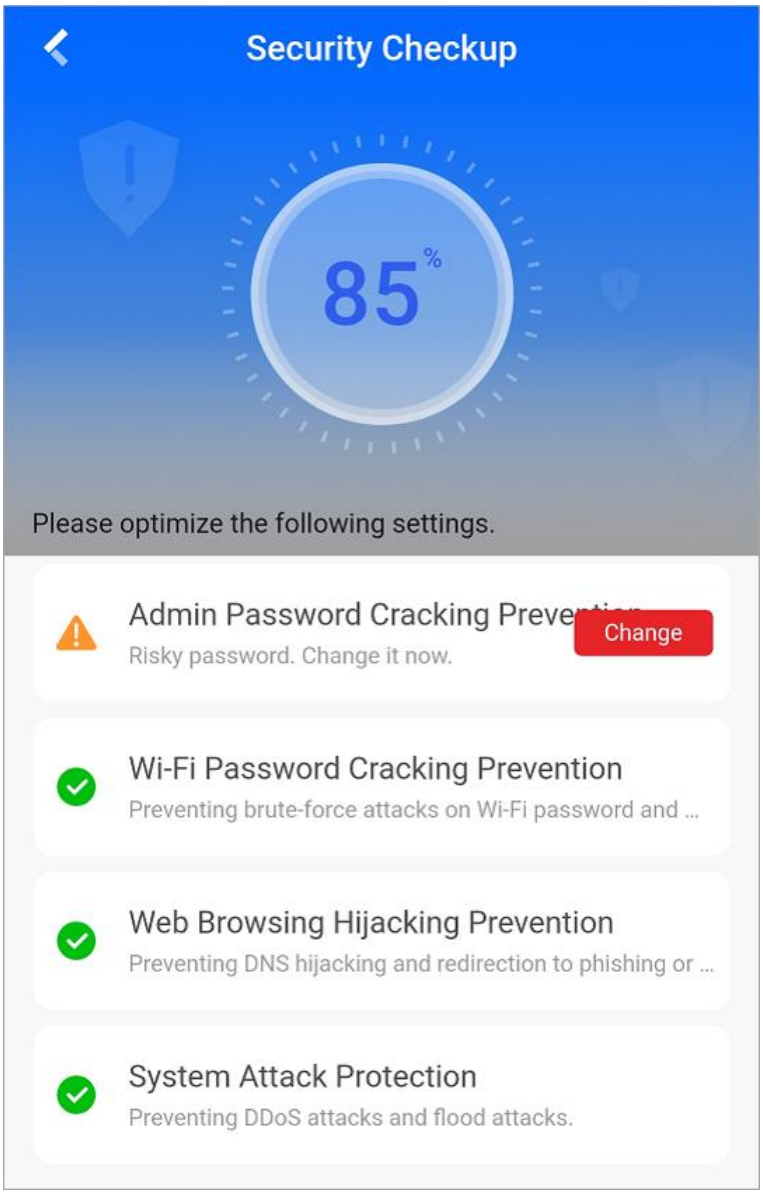


Figure 11-16 Result

Chapter 12 Network Switch

Network switches help to expand device connectivity, improve data distribution efficiency, and reduce network bandwidth stress, thus streamlining the deployment and maintenance of larger-scale video security network. You can view the status of network switches in the Mobile Client.

Note

Network switches need to be added on Lts-Partner Pro by Installer and then handed over to you. You cannot add network switches by yourself via LTS Connect.

After your Installer hands over network switches to you, you can view them in the device list on the Home page.
You can tap on a network switch to check its status.
When port connection changes or an exception occurs/restores, you will be notified. You can check the details on Notification tab.

Table 12-1 Supported Status and Operations of Network Switch

Status	Operation
● Device Uptime ● Port Status ● CPU Usage ● Memory Usage ● PoE Power	● Edit device name. ● Check device firmware version. ● Configure DDNS. ● Change remote configuration. ● Delete device.

Chapter 13 Account

You need a LTS Connect account to manage your devices online, use the cloud features, and share devices with others. You can use the visitor mode to experience the app with a temporary account and register an account of your own later.

13.1 Select Region at First Time Running

The first time you run the Mobile Client, you should select the region where your devices are located. Otherwise, the live view, playback and alarm notification of the devices will fail.

Note

You should select the region where your devices are located, or subsequent operations may be affected.

After running the Mobile Client, tap **Select Region** to select a region.

13.2 Registration

You can register an account by your mobile phone number or your email address. With a registered account, you can log in to the Mobile Clients running on different mobile phones, which provides convenience for managing your devices.

Note

You can use visitor mode to manage your devices without registration. See ***Visitor Mode*** for details.

13.2.1 Register by Email Address

You can register an account by your email address.

Steps

1. Tap **Login/Register** on the Home page.
2. Tap **Register** to enter the Join Us page.
3. Tap **Terms of Service** and **Privacy Policy** to read the relevant content and then tap **Agree** to continue.
4. Select the region where your devices locate.
5. In the Register page, enter your email address and then create a password.

Note

We highly recommend you to create a strong 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) in order 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.

6. Tap **Get Security Code** to get the security code for verification.
7. Enter the security code you received, and then tap **Finish**.

13.2.2 Register by Mobile Phone Number

You can register an account by your mobile phone number.

Steps

1. Tap **Login/Register** on the Home page.
2. Tap **Register** to enter the Join Us page.
3. Tap **Terms of Service** and **Privacy Policy** to read the relevant content and then tap **Agree** to continue.
4. Select the region where your devices locate.
5. In the Register page, tap **Register by Mobile Phone Number**.
6. Enter your mobile phone number and then create a password.

Note

We highly recommend you to create a strong 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) in order 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.

7. Tap **Get Security Code** to get the security code for verification.
8. Enter the security code you received, and then tap **Finish**.

13.3 Visitor Mode

Visitor mode allows you to manage devices on the Mobile Client without registration. When you log in as a visitor, a visitor account will be created for you automatically, and the account will not change on the same phone.

Caution

For information security, please use visitor mode cautiously, which is NOT password-protected.

Note

In visitor mode, you can only manage your devices on a same phone. To avoid this inconvenience, you can register an account. For details about registering account in visitor mode, see ***Register an Account in Visitor Mode***.

13.3.1 Functions in Visitor Mode

Most of the functions supported in a registered account are supported in visitor mode.
Tap **Visitor Mode** on the Home page or the Login page to enter visitor mode.
The followings are the functions supported in visitor mode.

Device Management

Add devices to the Mobile Client and configure device settings. See ***Add Device for Management*** and ***Configure Your Device*** for details.

Sharing Device

Tap ⊕ → **Scan QR Code** to scan the QR code of another visitor account to share device(s) to the account. For details about sharing device, see ***Device Sharing***.

Note

To get the QR code of a visitor account, go to **Me** → **Account Management**.

Live View and Playback

View live video of the added devices and play back the videos. See ***Live View*** and ***Playback*** for details.

Access Control

Control door status and check access control events. See ***Manage Access Control Devices*** for details.

Note

Make sure you have added access control devices to the Mobile Client.

Security Control Panel Management

Manage partitions (areas) and zones for the security control panel. See ***Security Control*** for details.

Alarm Configuration

Configure the alarm notifications on Alarm Notification page. See ***Notification*** for details.

13.3.2 Register an Account in Visitor Mode

Though the visitor mode allows you to manage devices without registration, you can only manage your devices on one phone or tablet. With a registered account, you can manage devices on different phones or tablets.

Steps

1. Tap **Visitor Mode** on the Login page or Home page to enter the visitor mode.
2. Tap **Me** → **Register an Account** to open the Join Us window.
3. Tap **Terms of Service** and **Privacy Policy** to read the relevant information.
4. Tap **Agree** if you accept our terms of service and privacy policy.
5. Register an account by mobile phone number or email address.

Note

See ***Register by Email Address*** and ***Register by Mobile Phone Number*** for details.

Chapter 14 Configure Your System

This section introduces system settings of the Mobile Client, and the parameters include custom audio management, generate QR code, hard-decoding preferred, traffic statistics, Wi-Fi settings,

display channel-zero, etc.

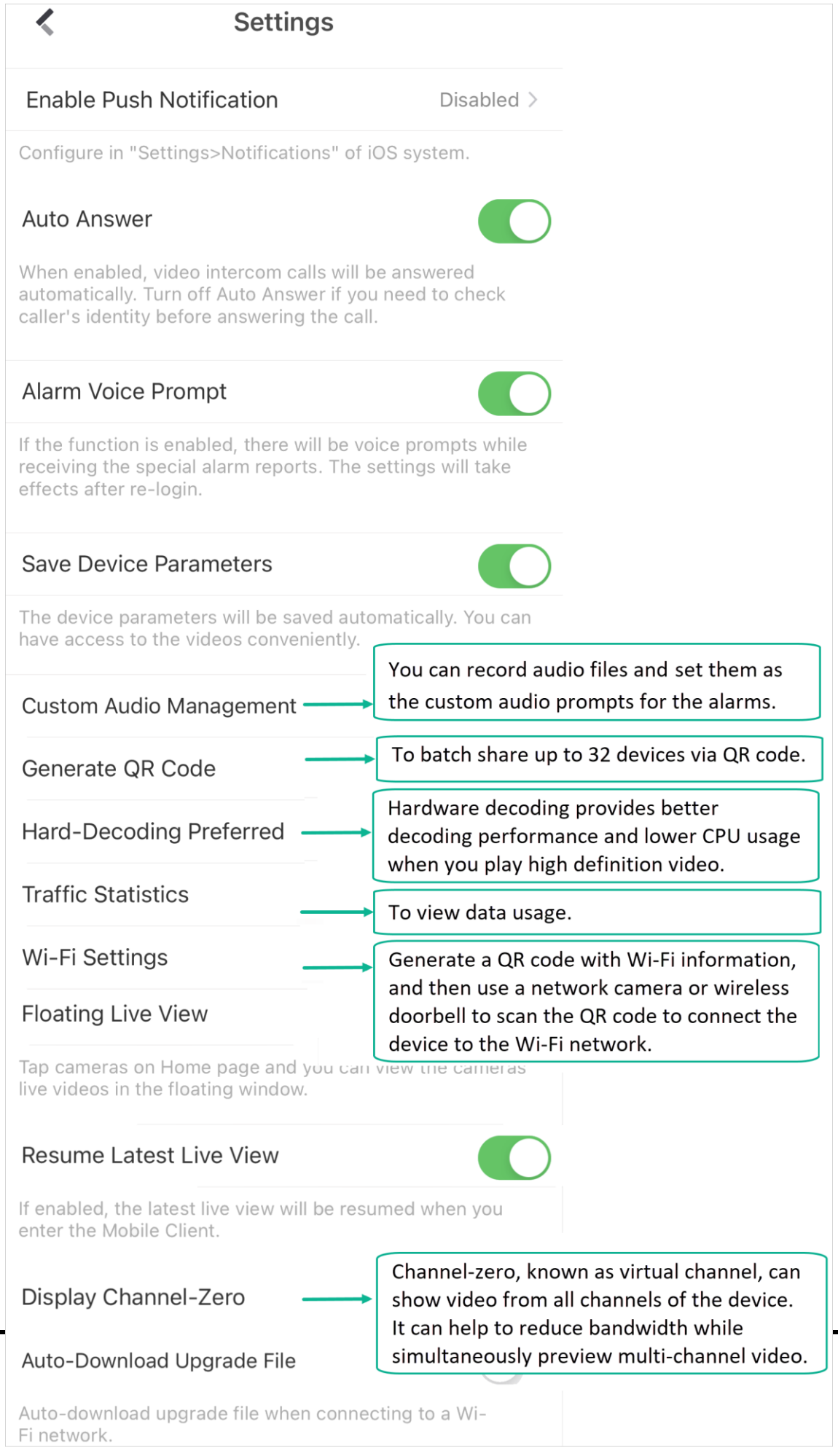

Settings
Enable Push Notification
Disabled
Configure in "Settings>Notifications" of iOS system.
Auto Answer
When enabled, video intercom calls will be answered automatically. Turn off Auto Answer if you need to check caller's identity before answering the call.
Alarm Voice Prompt
If the function is enabled, there will be voice prompts while receiving the special alarm reports. The settings will take effects after re-login.
Save Device Parameters
The device parameters will be saved automatically. You can have access to the videos conveniently.
Custom Audio Management
You can record audio files and set them as the custom audio prompts for the alarms.
Generate QR Code
To batch share up to 32 devices via QR code.
Hard-Decoding Preferred
Hardware decoding provides better decoding performance and lower CPU usage when you play high definition video.
Traffic Statistics
To view data usage.
Wi-Fi Settings
Generate a QR code with Wi-Fi information, and then use a network camera or wireless doorbell to scan the QR code to connect the device to the Wi-Fi network.
Floating Live View
Tap cameras on Home page and you can view the cameras live videos in the floating window.
Resume Latest Live View
If enabled, the latest live view will be resumed when you enter the Mobile Client.
Display Channel-Zero
Channel-zero, known as virtual channel, can show video from all channels of the device. It can help to reduce bandwidth while simultaneously preview multi-channel video.
Auto-Download Upgrade File
Auto-download upgrade file when connecting to a Wi-Fi network.

Figure 14-1 System Settings

14.1 Enable Push Notification

If push notification is enabled, the Mobile Client will push alarm notifications related to the added devices to you.

Note

For details about alarm notifications, see ***Notification*** for details.

Tap **Me** → **Settings** to enter the Settings page, and then enable the push notification.

14.2 Save Device Parameters

If the function is enabled, the Mobile Client will remember the device parameters you set. Take video and image encryption for an example, you only need to enter the device verification code for once to view the encrypted live view, playback, or picture.

Note

- For details about video and image encryption, see ***Set Video and Image Encryption***.
- For details about setting device parameters via the Mobile Client, see ***Configure Your Device***.

Tap **Me** → **Settings** to enter the Settings page, and then enable the function.

14.3 Auto-Receive Alarm after Power-on

If you enable this function, the Mobile Client will run automatically and receive alarm event information when the phone or tablet is powered on.
Tap **Me** → **Settings** to enter the Settings page and then enable the function.

Note

The power consumption of the phone or tablet may increase.

14.4 Generate a QR Code with Device Information

For devices added via IP/domain, the Mobile Client allows you to generate a QR code containing the information of up to 32 devices. The QR code can be used to quickly add multiple devices. For example, if user A has generated a QR code containing the information of 10 devices, user B can

scan the QR code to batch add the 10 devices to his or her account.

Steps

Note

Only devices added by IP/domain support this function.

1. Tap **Me** → **Settings** to enter the Settings page.
2. Tap **Generate QR Code**.
3. Tap **Generate QR Code** in the IP/Domain field to enter the Select Device page.
4. Select device(s).
5. Tap **Generate QR Code**.
   The QR code picture will be generated.
6. Tap **Save** to save the picture to the photo album of your phone.

14.5 Hardware Decoding

Hardware decoding provides better decoding performance and lower CPU usage when you play high definition videos during live view or playback.
Tap **Me** → **Settings** to enter the Settings page, and then enable the function.

Note

- Hardware decoding is only supported when the resolution is 704*576, 704*480, 640*480, 1024*768, 1280*720, 1280*960, 1920*1080, 2048*1536, or 2560*1920. For other resolutions, only software decoding is supported.
- For H.265 video compression, hardware decoding is not supported.
- Hardware decoding should be supported by the device. If not, the device will adopt software decoding by default.

14.6 View Traffic Statistics

The Mobile Client automatically calculates the network traffic consumed during live view and playback. You can check the mobile network traffic and Wi-Fi network traffic separately.
Tap **Me** → **Settings** to enter the Settings page, and then tap **Traffic Statistics**.

14.7 Generate a QR Code with Wi-Fi Information

You can generate a QR code with Wi-Fi information, and then use a network camera or wireless

doorbell to scan the QR code to connect the device to the Wi-Fi network.

Steps

Note

Connecting device to a Wi-Fi network by scanning QR code should be supported by the device.

1. Tap **Me** → **Settings** to enter the Settings page.
2. Tap **Wi-Fi Settings** to enter the Wi-Fi Settings page.
3. Set the required information.

Wi-Fi Name

Enter the SSID of the Wi-Fi network.

Password

Enter the password of the Wi-Fi network.

Encryption

Select the encryption type as the one you set for the router.

Note

If you select NONE as the encryption type, the password of the Wi-Fi network is not required.

4. Tap **Generate** to generate a QR code for the Wi-Fi network.

What to do next

Use a network camera or wireless doorbell to scan the QR code to connect the device to the Wi-Fi network.

14.8 Floating Live View

If you enable this function, floating live view window(s) will be displayed on the device list page when you select one or more device(s). You can preview the live video(s) in the floating window(s).

Note

- If you select more than 16 cameras, the number of the selected cameras will be displayed.
- Up to 256 cameras can be displayed as floating windows.

Tap **Me** → **Settings** to enter the Settings page and then enable the function.

14.9 Resume Latest Live View

If you enable the function, the latest live view will be resumed each time you enter the Mobile Client. The window division mode, and the live view windows' sequence (if in multiple-window

mode) will also be restored.
Tap **Me** → **Settings** to enter the Settings page, and then enable the function.

14.10 Tablet Mode

If the Mobile Client is installed on an Android tablet, you can enable tablet mode so that the interfaces will be displayed in landscape mode by default.
Tap **Me** → **Settings** to enter the Settings page and then enable the function.

Note

After enabling tablet mode, you should restart the Mobile Client to make the settings effective.

14.11 Display/Hide Channel-Zero

Channel-zero, known as virtual channel, can show the videos from all channels of the device, reducing the bandwidth while simultaneously previewing from multi-channel. It can acquire image information and save bandwidth for transmission through encoding and configuring output images.
Tap **Me** → **Settings** and then enable the Mobile Client to display channel-zero.

14.12 Auto-Download Upgrade File

If you enable Auto-Download Upgrade File, the Mobile Client will automatically download the upgrade file in Wi-Fi networks, which helps speed up the device upgrade process.

Note

For details about upgrading device, see ***Upgrade Device Firmware***.
Tap **Me** → **Settings** to enter the Settings page and then enable the function.

14.13 Manage Custom Audio

You can record audio files for setting them as the custom audio prompts for the alarms sent from the channels linked to specific models of DVR.

Perform this task to record an audio file.

Steps

1. Tap **Me** → **Settings** → **Custom Audio Management**.
2. Tap **Start Recording** to start recording, and then tap **Stop Recording**.
   The Complete Recording dialog pops up.

3. Optional: Create a name for the audio file.

Note

By default, the file name is the time (accurate to second) when recording stops.

4. Tap **Confirm**.
5. Optional: Perform further operations.

Rename Audio	Swipe left and then tap to rename the audio file.
Delete Audio	Swipe left and then tap to delete the audio file.

What to do next

Set custom audio prompt for the alarms sent from the channels linked to specific models of DVR. For details, see ***Set Custom Audio***.

Chapter 15 Other Functions

The Mobile Client provides other functions, including Touch ID or Face ID authentication and management of the recorded videos and captured pictures.

15.1 Pictures and Videos

In Picture and Video Management module, you can view and manage the recorded (or clipped) video footage and the captured pictures.
Tap **Me** → **Pictures and Videos** to enter the Pictures and Videos page and then you can perform the following operations.

- Play Video File
- : Tap a video file and then tap to play it.
  You can rotate the phone to view the video in landscape mode.
- Save to Local Album
- : Tap a video file or a picture, and then tap to save the video file or picture to the album of your phone or tablet.
- Delete a Video File or Picture
- : Tap a video file or a picture, and then tap to delete it.
- Share a Picture or Video File to Another Application
- : Tap a video file or a picture, and then tap to share it to another application.
- Batch Delete Video Files and (or) Pictures
- : Tap **Edit** and select video files and (or) pictures, and then tap to delete them.
- Batch Share Pictures and (or) Video Files to Another Application
- : Tap **Edit** and select pictures and (or) video files, and then tap to share it to another application.

15.2 Share LTS Connect

You can show the QR Code for downloading the Mobile Client to others.
Tap **Me** → **Share LTS Connect** to view the QR code. After that, you can let others scan the QR code to download the Mobile Client.

Symbol Conventions

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

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