Yealink Management Cloud Service
Service Provider Guide V3.7.0.1

Contents

About This Guide

This guide introduces Yealink Management Cloud Service (YMCS) and how to manage devices on it.

- Related Documentations

Related Documentations

Except for this guide, we also provide the following documents:

You can download the above documents from Yealink official website or in the top-right corner of the YMCS web page. The address of Yealink official website is as below: http://support.yealink.com/documentFront/forwardToDocumentDetailPage?documentId=254.

For more supports or services, contact Yealink channel or go to Yealink Technical Support online: http://support.yealink.com/.

Summary of Changes

Changes for Release 37, Guide Version V3.7.0.1

Starting from this version, we apply a new user interface design. For other new features, see the following.

The following sections are new for this version:

- Auto Provisioning
- Device Managing Features and Their Supported Devices

Major updates have occurred to the following sections:

- Supported Device Models
- Configuring the Common.cfg File
- Connecting Phone Devices and Room Systems (Except for MVC/ZVC)
- Connecting MVC/ZVC Room Systems
- Device Status
- Managing Sites
- Taking the Screenshot of the Device

Changes for Release 36, Guide Version V3.6.0.30

The following sections are new for this version:

- Viewing the Devices Statistics
- Enabling Login Protection

Major updates have occurred to the following sections:

- Logging into YMCS
- Managing SIP Devices-Searching for Devices
- Pushing Configuration Files to Devices
- Managing USB Devices-Searching for Devices
- Managing Room System-Searching for Devices
- Viewing the Detailed Information of Phone Devices
- Adding Firmware
- Adding Resource Files
- Adding Configuration Templates
- Uploading Configuration Files
- Capturing Packets
- Viewing Alarms
- Viewing Call Quality Statistics
- Assigning the Data Permission
- Editing the Account Information

Changes for Release 36, Guide Version V3.6.0.20

Major updates have occurred to the following sections:

- Supported Device Models
- Viewing Recordings
- Taking the Screenshot of the Device

Changes for Release 36, Guide Version V3.6.0.10

The following sections are new for this version:

- Resetting the Devices to Factory
- Enabling Automatic Synchronization
- Backing up Configuration Files

Major updates have occurred to the following sections:

- Adding the Group Configuration
- Viewing the Information of Connected Accessories
- Synchronizing Devices
- Adding and Managing Roles
- Viewing Alarms

Changes for Release 36, Guide Version V3.6.0.1

The following sections are new for this version:

- Deploying YMCS Agent
- Getting the Device Log

Major updates have occurred to the following sections:

- Supported Device Models
- Port Requirements
- Adding Devices
- Viewing the Detailed Information of Phone Devices
- Adding Timer Tasks
- Diagnosing Devices
- Starting Diagnosing
- Viewing the CPU and the Memory Status
- Download the Device Log
- Viewing Alarms
- Viewing the Call Data

Changes for Release 35, Guide Version V3.5.0.20

Major updates have occurred to the following sections:

- Hardware and Software Requirements
- Supported Device Models
- Why the Browser Prompts That the Security Certificate of the Website Is not Trusted When You Access the Login Page?

Changes for Release 35, Guide Version V3.5.0.10

The following sections are new for this version:

- Alarm Statistics
- Filtering the Alarms
- Exporting Alarm Records

Major updates have occurred to the following sections:

- Supported Device Models
- Adding Alarm Strategies
- Managing Alarm Strategies

Changes for Release 35, Guide Version V3.5.0.1

Major updates have occurred to the following sections:

- Managing Tasks

Changes for Release 34, Guide Version V3.4.0.10

The following sections are new for this version:

- Pushing Configuration Files to Devices
- Pushing Firmware to Devices
- Pushing Resource Files to Devices
- Diagnosing Devices
- Managing the Site Configuration
- Setting Parameters
- Exporting the Packets, Logs, and Configuration Files by One Click
- Viewing the Account Code

Major updates have occurred to the following sections:

- Logging into YMCS
- Configuring the Common.cfg File
- Adding Sites
- Starting Diagnosing

Introduction of Yealink Management Cloud Service

Yealink Management Cloud Service (YMCS), based on cloud architecture, possesses the centralized deployment, the management, the analysis, the alarm monitoring, the device diagnosis, the account registration, the RPS service, the order management, and other features. The management platform allows enterprise administrators to deploy and configure Yealink devices used in an enterprise, to use the RPS feature to manage the devices.

- Browser Requirements
- Supported Device Models
- Port Requirements

Browser Requirements

YMCS supports the following browsers:

Browser	Version
Firebox	55 or later
Chrome	55 or later
Internet Explorer	11 or later
Safari	10 or later

Supported Device Models

You can manage the following devices via YMCS:

Device Types	Supported Device Models	Version Requirements
Voice Communication Phone	T27P/T27G/ T29G/T41P/T41S/T42G/T42S/ T42U/T46G/ T46S/T48G/T48S/T52S/T54S	XX.83.0.30 or later (except for XX.84.0.10). XX represents the fixed number for each device model.
	T56A/T58	58.83.0.5 or later.
	T53/T53W	95.84.0.10 or later.
	T54W	96.84.0.10 or later.
	T57W	97.84.0.30 or later.
	T42U/T43U/T46U/T48U	108.84.0.30 or later.
	T30/T30P/T31/T31P/T31G/T33P/ T33G	124.85.0.10 or later.
DECT Phone	W60B	77.85.0.25 or later.
Conference Phone	CP960	73.83.0.10 or later.
	CP920	78.84.0.15 or later.
Video Phone	VP59	91.283.0.10 or later.
Zoom Phone	CP960	73.30.0.10 or later.
Microsoft Skype for Business Desk Phone	T41S/T42S/T46S/T48S	66.9.0.45 or later (except for 66.9.0.46).
	T58/T56A/T55A	55.9.0.6 or later.
	CP960	73.8.0.27 or later.
	MP56	122.9.0.1 or later.
	MP54/MP58	122.9.0.5 or later.
Microsoft Teams Desk Phones	CP960	73.15.0.20 or later.
	T56A/T58	58.15.0.20 or later.
	T55A	58.15.0.36 or later.
	VP59	91.15.0.16 or later.
	MP56	122.15.0.9 or later.
	MP54/MP58	122.15.0.25 or later.
	MP52	145.15.0.4 or later.
	VC210	118.15.0.20 or later.
Microsoft Teams Collaboration Bar	MeetingBar A20	133.15.0.20 or later.
	MeetingBar A30	133.15.0.42 or later.

Device Types	Supported Device Models	Version Requirements
Zoom Rooms Collaboration Bar	MeetingBar A20/A30	133.30.0.35 or later.
Microsoft Teams Room System/Zoom Rooms Kit (MVC/ZVC Room System)	MVC500/MVC800/MVC300/ CP960-UVC Zoom Rooms Kit/ VP59 Zoom Rooms Kit	XX.11.0.10 or later.
	MVC840/MVC640/MVC940	262.410.0.10 or later
	MVC400	2.2.23.0 or later
VC Room System	VC200/VC500/VC800/VC880	XX.32.10.25/XX.32.0.25 or later. XX represents the fixed number for each device model.
	PVT950/PVT980	1345.32.10.40 or later.
	PVT940/PVT960	120.43.0.25 or later.
	VP59	91.332.0.10 or later.
	MeetingEye 600/MeetingEye 400	120.43.0.5 or later.
	VC200-E/VC210 Pro	118.50.0.10 or later
	VC210	118.43.0.1 or later.

Note:

- Microsoft Teams devices are not available for managing the accounts and viewing the call quality.

Port Requirements

You need to open 6 ports for YMCS: 443, 9989, 8446, 80, 8443, and 8445. We do not recommend that you modify these ports.

Port	Description
443	It is used for accessing the device management platform and reporting the device information to the platform via HTTPS.
9989	It is used for the phone to download the configuration files.
8446	It is used for mutual authentication between YMCS and the devices when pushing the configuration, the firmware, and the resource files to the devices.
80	It is used for accessing the platform via HTTP.
8443	It is used for calling the API of YMCS for RPS Enterprise.
8445	It is used for calling the API of YMCS for Enterprise.

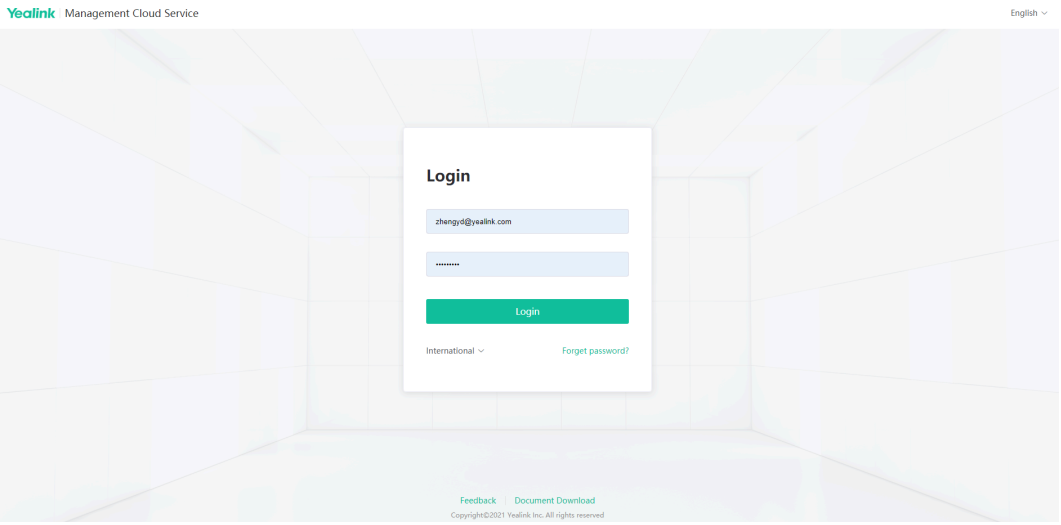
Getting Started

Logging into YMCS

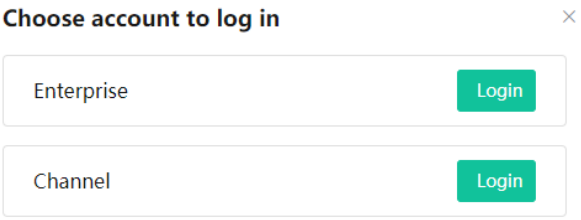
The accounts of YMCS for the service provider are created by Yealink, and you can get the login username and the password from the email.

Procedure

1. Enter the address of YMCS (https://ymcs.yealink.com) in the browser address box, and then press Enter.

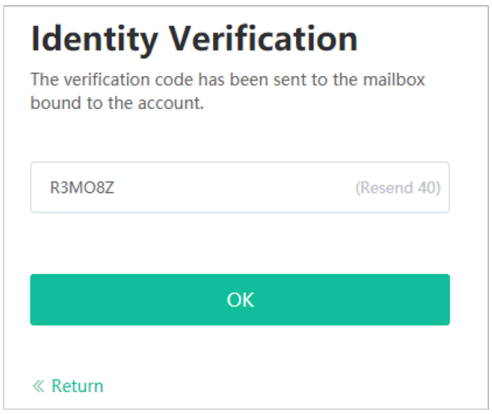


2. Select the desired language from the drop-down menu of **Language** in the top-right corner.
3. Enter your username and the password.
4. Click **International** to select the desired site.
5. Click **Login**.
6. If you register the enterprise account and the channel account with the same email, select the desired account to log in.

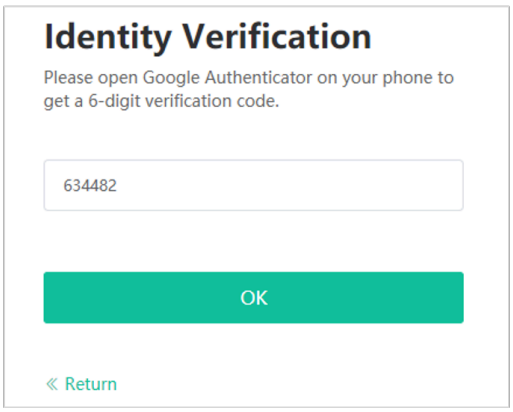


7. If you want to enable the login protection feature for dual identify authentication, refer to Enabling Login Protection.

If you enable the login protection of **Email**, the page is shown as below:



If you enable the login protection of **Virtual MFA Device**, the page is shown as below:

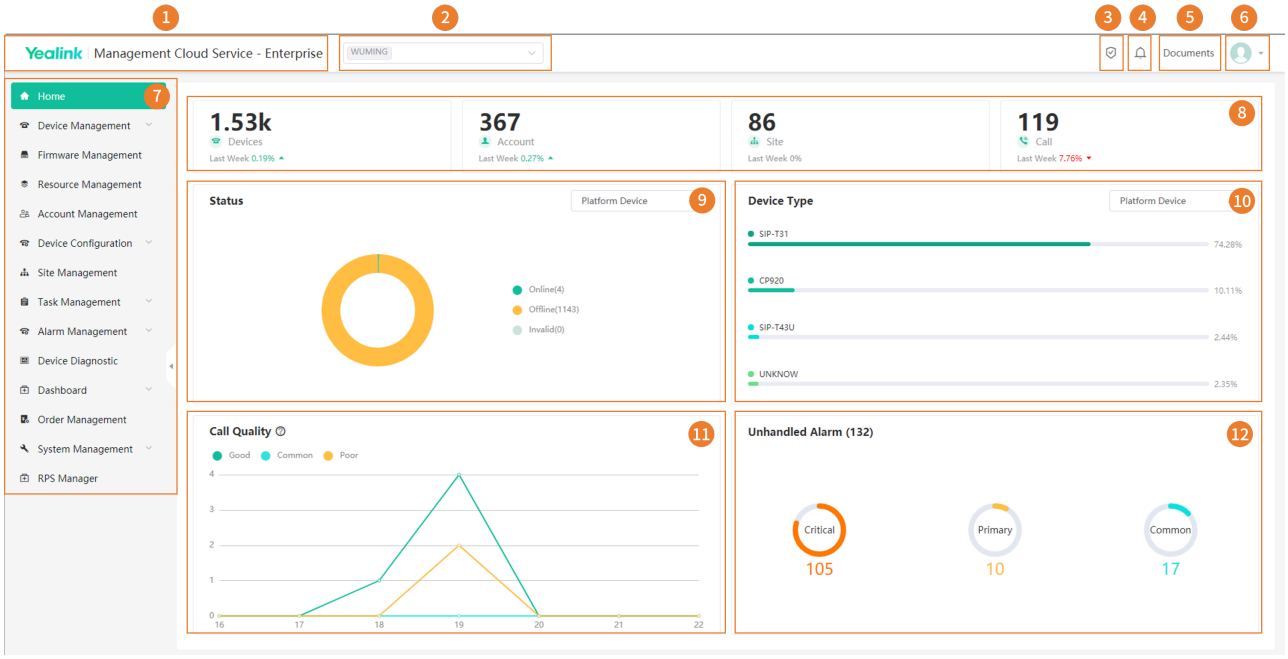


8. If you log into YMCS for the first time, the system will remind you to change the password, click **Change** to go to the homepage.

Note: If you enter the correct username and password, but you fail to log in. You can change the site and log in again.

Home Page

After logging into YMCS, you can see the home page displayed as below:



Number	Description
1	The platform name.
2	Select a site.

Number	Description
3	: you have authorized a channel to manage your platform for you. : you do not authorize any channel to manage your platform for you. For more information, refer to Authorizing/Un-authorizing the Management to the Channel.
4	Display number of unread alarms and the type of alarms.
5	Go to the website of Yealink Support to download documents.
6	Go to the page of setting the administrator account.
7	Navigation pane.
8	**Overview:** • Display the number of devices, accounts, sites, and calls. • Click the desired module to go to the corresponding module.
9	**Status:** • Select a device type. • Display the number of online, offline, and invalid devices. • Click the corresponding device status to go to the page that lists the devices of this status.
10	**Device Type:** • Select a device type. • Display the number of devices in each model. • Click the corresponding model to go to the page that lists the devices in this model.
11	**Call Quality:** • Display the number of calls with good, bad or poor call quality. • You can click the desired module to view the call statistics. **Note:** It is not available for the basic package. You can contact your distributor/reseller to subscribe to the advanced package if you need. You can view the details of the subscribed package on the page of Managing Orders.
12	**Unhandled Alarms:** • Display the number of critical, major, and minor alarms. • Click the corresponding alarm level to go to the page that lists the alarm in this level. **Note:** It is not available for the basic package. You can contact your distributor/reseller to subscribe to the advanced package if you need. You can view the details of the subscribed package on the page of Managing Orders.

Logging out of YMCS

Procedure

Hover your mouse on the account avatar in the top-right corner, and click **Exit**.
You will log out of the current account and return to the Login page.

Deploying YMCS Agent

This chapter introduces how to install and deploy YMCS Agent.

If your enterprise deploying YMCS Agent, you can enjoy the following features:

- You can connect devices to Agent and get the firmware or resource files on Agent, thereby improving the access speed.
- The device log can be saved on Agent for 7 days.

Basic Requirements of Hardware and Software

For virtual machine, we support VMware ESXi in version 6.5 or later. For Linux operating system, we support CentOS7.5 and CentOS8.1.

Requirements for installing Agent:

Table 1: Basic Requirements of Hardware

Device Quantity	CPU	RAM	Hard Drive	Outbound Bandwidth
0~5000	Dual core , 2.4 GHz	4 GB	50G	10M
5000~20000	Quad-core , 2.4 GHz	8 GB	50G	50M

Note: The above requirements of hard drive is only used for deploying Agent. For storing logs and the firmware or resource files, you need to create two individual partitions. For more information, refer to Installing Agent.

Port Requirements

You need to open port 80 and 9990 for YMSC Agent. We do not recommend that you modify these ports.

Table 2: Port Requirements

Port	Description
80	It is used for accessing Agent via HTTP.
9990	It is used for connecting the phone to Agent.

Installing Agent

Before you begin

You should configure your environment for installing Agent as below:

- Create two individual partitions (fox example, vdb or vdc) for storing the log and the firmware or resource files respectively. First of all, add two hard drives to the virtual machine, and then run the following commands.

```
echo '- - -' > /sys/class/scsi_host/host0/scan        ##San the added hard drives##
lsblk                                                 ##Check whether the hard drives are added successfully##
```

- Run the following commands to create two folders for storing the log and the firmware or resource files respectively. You can customize the names for the two folders.

```
mkdir /data/log          ##/data/log is the directory for saving the log##
mkdir /data/resource     ##/data/resource is the directory for saving the firmware or resource
 files##
```

- Run the following commands to mount partitions.

```
mkfs.xfs /dev/vdb                  ##Format the partition and vdb is the name of the partition for
 storing device logs under the directory of /dev/##
mkfs.xfs /dev/vdc                  ##Format the partition and vdc is the name of the partition for
 storing firmware or resource files under the directory of /dev/##
mount /dev/vdb /data/log           ##Mount the partition to the directory of /data/log##
mount /dev/vdc /data/resource      ##Mount the partition to the directory of /data/resource##
df -h                              ##Check whether you succeed in mounting the partition##
```

- The above mounted partitions become invalid if you reboot the system. Edit the *fstab* file in the directory of */etc/*, add the following commands to the file to realize automatic mounting after rebooting.

```
/dev/vdb                  /data/log          xfs     defaults        0 0
/dev/vdc                  /data/resource         xfs     defaults        0 0
```

Procedure

1. Click **System Management** > **Agent Management** > **Download Agent** to download the installation package.
2. Use SecureCRT to go to the command interface of the root account via SSH.
3. Run the following command to go to the directory (/usr/local).

```
cd /usr/local
```

4. Run the command *rz* and upload the desired installation package on the pop-up window.

```
yum install -y lrzsz
rz
```

5. Unzip the installation package:

```
tar zxvf DM_AGENT-release-x.x.x.x.tar.gz     ##unzip the installation package (change x.x.x.x to the
 version number you want to install)##
cd yealink_install/                  ##go to the installation directory##
tar zxvf install.tar.gz              ## nzip the installation script##
```

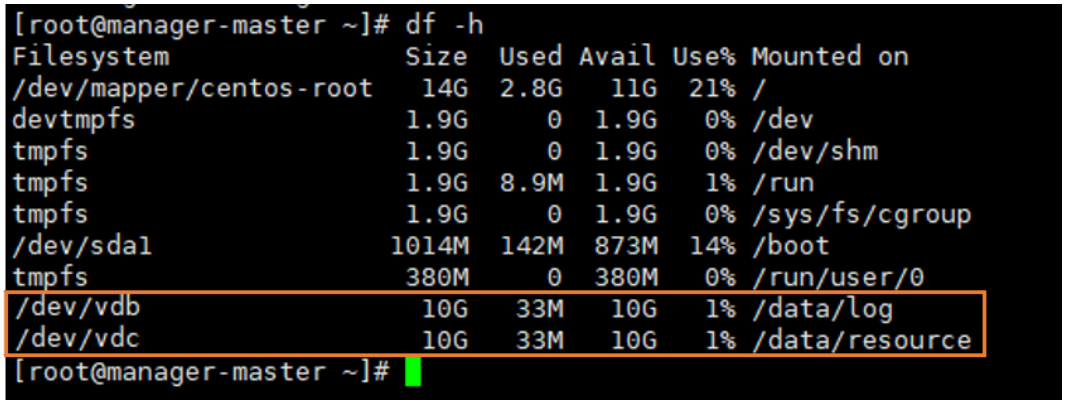
6. Install Agent:

```
cd /usr/local/yealink_install/
./install
```

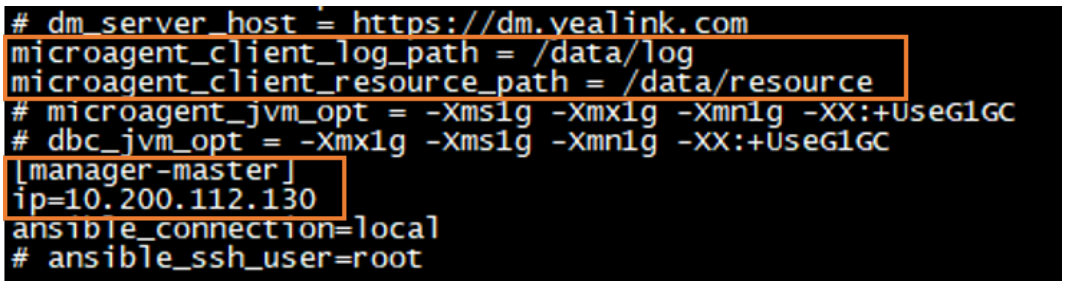
Enter the Agent address, the directory for storing log, and the directory for storing the firmware and resource files respectively according to the prompts.

Note: If it prompts installation failed, check the following:

a. Check whether you succeed in mounting the partition.



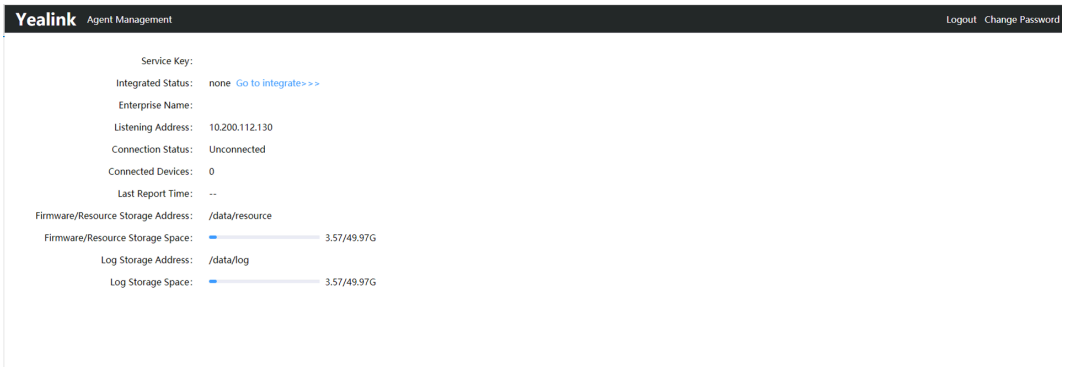
b. Check whether you correctly configure the parameters in the *install.conf* file in the directory of */usr/local/yealink/data/*. When you are installing Agent, the parameters with yellow frame in the following picture will be written to the configuration file.



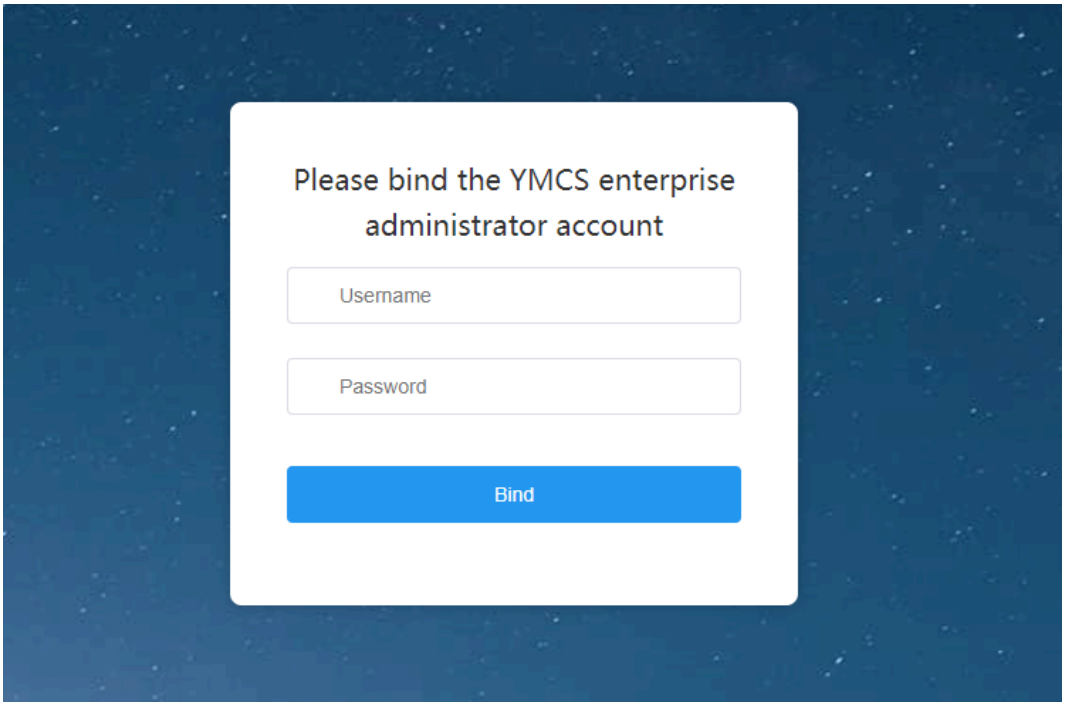
Integrating Agent with YMCS

Procedure

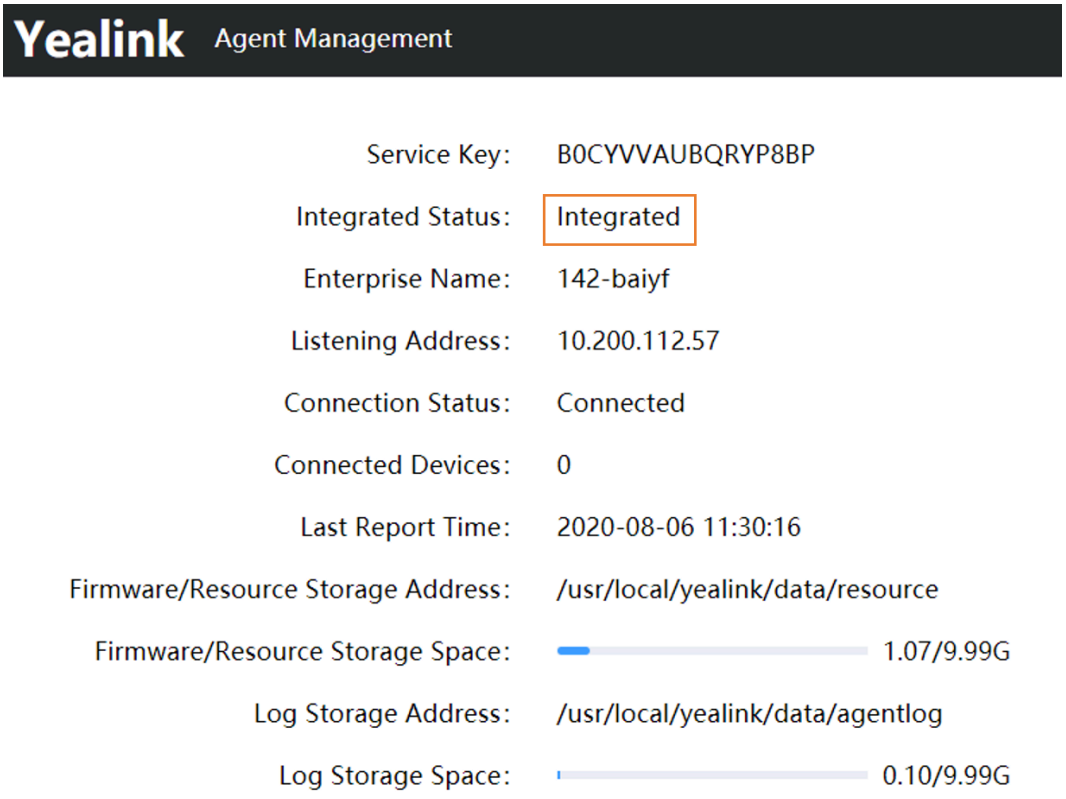
1. Open a browser and enter the Agent IP address in the address bar.
2. Enter the username (default: admin) and the password (default: admin) and click **Login**.
3. Click **Go to Integrate**.



4. Enter the username and password of YMCS and click **Bind**.



The page is displayed as below when you succeed in integrating Agent with YMCS:



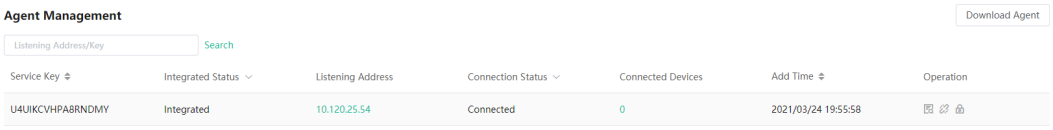
Connecting Device to Agent

If you deploy Agent in your enterprise, you can connect devices to YMCS via Agent. The address that the devices are connected to Agent is *http://AgentIPaddress/agent.cfg*. The method for connecting devices to Agent is the same as the one of YMCS, refer to Connecting to YMCS.

Managing Agent

Procedure

1. Click **System Management** > **Agent Management**.
   The page displays all the integrated Agent and each enterprise can integrate with 10 Agent at most.



2. Do one of the following:
   - Click to view the Agent status and you can enable or disable the feature of 7-Day Log.
   - Click to cancel the integration with the enterprise. After that, you cannot integrate the Agent with any enterprises unless you uninstall Agent (Uninstalling Agent) and install it again. Click to delete the records.
   - Click to reset the password of Agent.

Uninstalling Agent

Procedure

1. Log into CentOS as the root user and open the terminal.
2. Run the command:

```
cd /usr/local/yealink_install
./uninstall
```

3. According to the prompts, enter the password Yealink1105.
   Agent will be uninstalled from CentOS.

Connecting to YMCS

Before using YMCS to manage devices, you need to connect the devices to YMCS.

- Connecting Phone Devices and Room Systems (Except for MVC/ZVC)
- Connecting USB Devices
- Connecting MVC/ZVC Room Systems

Connecting Phone Devices and Room Systems (Except for MVC/ZVC)

The devices are redirected to YMCS through the RPS feature by default, and will be automatically connected to YMCS after powered on. If the automatic deployment fails, you need to manually deploy the devices.

Before you begin

Note: Note that the firmware version of the device should meet the requirement of connecting to YMCS. Otherwise, you should upgrade the device firmware first.

Procedure

1. If there is a provisioning server you are using in your environment, configure the common cfg file (refer to Configuring the Common.cfg File).
2. If there is no provisioning server, you need to configure the devices to obtain the provisioning server address in one of the following ways:
   - DHCP option 66, 43, 160 or 161.

     The DHCP option must meet the following format: https://dm.yealink.com/dm.cfg.
   - Configuring the Server Address, and deploy a single phone.
3. If you are a RPS user, you can use the RPS feature to deploy the devices.

Results

The device will be successfully connected to YMCS.

Note:

1. If the device is disconnected from YMCS, you need to reboot it to reconnect it to YMCS.
2. After the device is automatically connected to YMCS through RPS feature, the RPS feature is disabled automatically.

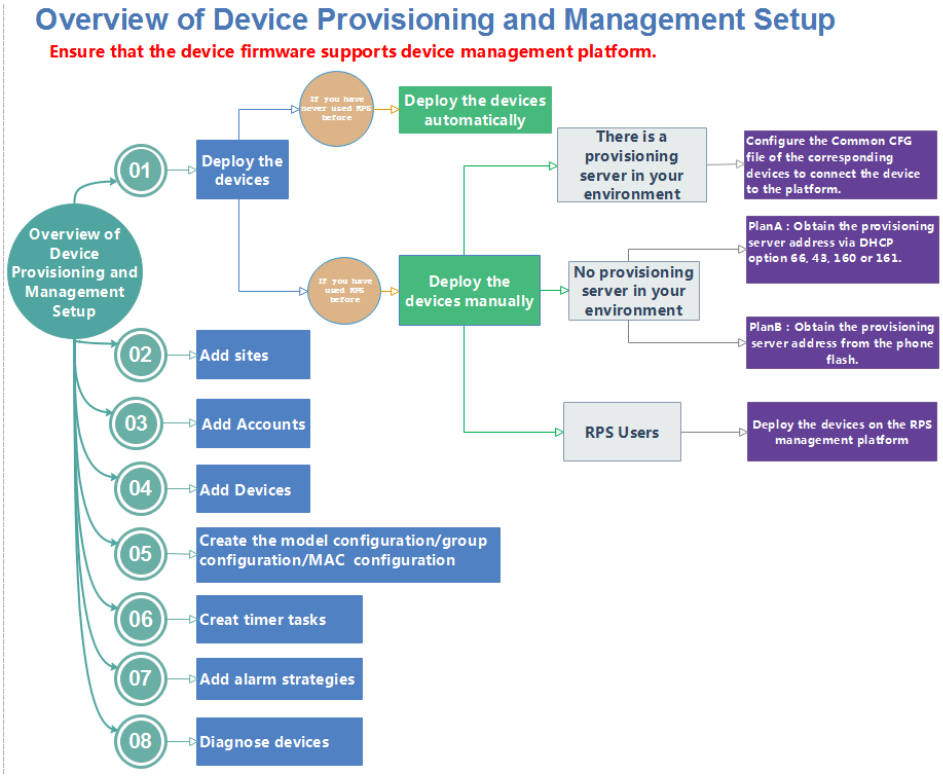
- Overview of Device Deployment and Management
- Configuring the Common.cfg File
- Deploying Devices via YMCS for RPS Enterprise
- Configuring the Server Address

Related concepts

Supported Device Models

Overview of Device Deployment and Management

The processes of the device deployment and management are shown as below:

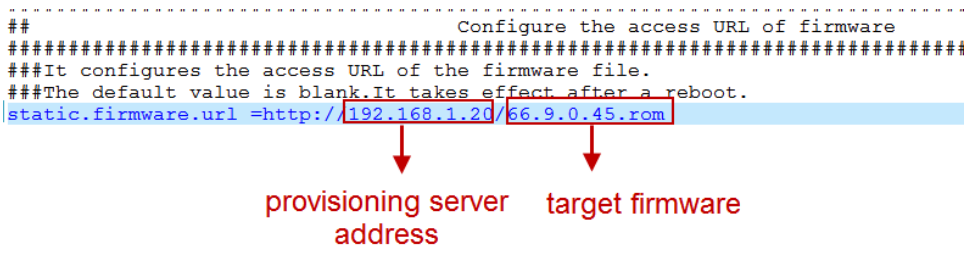


Configuring the Common.cfg File

If you want to use your auto-provisioning server to deploy devices but your firmware versions are lower than the requirement of YMCS, you need to upgrade the device firmware first and connect them to YMCS. For easy deployment, you can configure the parameters of upgrading the firmware and the access URL of YMCS in the Common.cfg file.

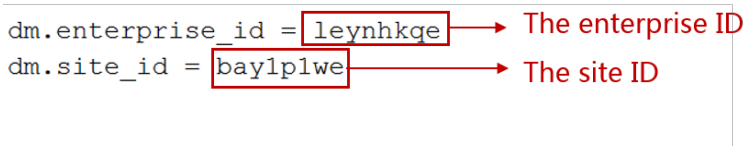
Procedure

1. Open the Common.cfg file of the corresponding device.
2. If your device firmware does not support the YMCS, upgrade the firmware of the device.



3. Configure the URL of the auto-provisioning server to connect the devices to YMCS.

4. Optional: Add the following configuration to your Common.cfg file, to make the device automatically connected to the corresponding site of the desired enterprise.



Note:

- Only the specific device and firmware version support this feature. For detailed information, contact Yealink technical support engineers.

  The supported device and firmware version are as below:

Device Type	Model	Version
DECT Phone	W60B	77.85.0.25 or later
	Desk Phone	T27G
T30, T30P, T31, T31P, T31G, T33P, T33G		124.86.0.5 or later
T41S, T42S, T46S, T48S		66.86.0.5 or later
T41U, T42U, T46U, T48U		108.86.0.10 or later
T53, T53C, T53W, T54W, T57W		96.86.0.10 or later
Conference Phone	CP960	73.86.0.5 or later
	CP920	78.86.0.10 or later
Video phones	VP59	91.86.0.5 or later
For Zoom Rooms Collaboration Bars	MeetingBar A20, MeetingBar A30	133.30.0.35 or later

- The priority (the devices automatically connected to the site) in the descending order is site IP setting (see Adding Sites), and then the site setting in the Common.cfg file.

5. Save the file.

Results
After auto-provisioning, the devices will be connected to YMCS.
Related concepts
Supported Device Models
Related tasks
Viewing the Account Code

Deploying Devices via YMCS for RPS Enterprise

If you deploy the device through the RPS management platform for the first time, after the devices are powered on and connected into the network, the RPS management platform pushes the address of YMCS (https://dm.yealink.com/dm.cfg) to the devices so that they can be connected to YMCS.

Procedure

1. Log in to YMCS for RPS Enterprise.
2. On the **Server Management** page, add the server URL.

3. On the **Device Management** page, add or edit the device information.
   After the device sends an RPS request, the device will be connected to YMCS.

   Note: You can use the RPS feature on YMCS in the version 3.4.0.0 or later, for more information, refer to Managing RPS.

Related tasks
Logging into YMCS
Adding Servers
Adding Devices
Importing Devices

Configuring the Server Address

Before deploying the device, if the DHCP server is not available, you need to configure the server address to make the device connected to YMCS.

Procedure

1. Log into the web user interface of the device.
2. Click **Settings** > **Auto Provision**.
3. Enter the provisioning server URL in the **Server URL** field.

   The URL should be set as https://dm.yealink.com/dm.cfg.
4. Click **Auto Provision Now**.
   The device will be connected to YMCS successfully.

Connecting USB Devices

Before you begin
Install USB Device Manager client on the PC that is connected to the USB device.

About this task

For more information about the configuration of USB Device Manager client, refer to Yealink USB Device Manager Client User Guide.

Procedure

Open USB Device Manager client, go to **Config DM Server**, and complete the correspond configuration.
The device will be connected to YMCS automatically.

Connecting MVC/ZVC Room Systems

About this task

For more information about deploying Room System, refer to Yealink RoomConnect User Guide.

Procedure

On your MTouch, open Yealink RoomConnect, go to **Remote Management**, and configure the related parameters.
The device will be connected to YMCS automatically.

Managing Devices

After connecting devices to YMCS, you need to add the devices so you can see them in the device list. You can manage phone devices, USB devices, room systems, and workspace devices (available from version 37 SP2).

Note:

Phone devices include

The maximum number of devices that you can manage on YMCS depends on the number in the package you purchased from the reseller or the distributor. You are not able to add new devices once the upper limit is reached. When some of your invalid orders cause some of the devices unable to manage, the device status will be invalid and you cannot manage it. If you still want to use this service, contact your superior channel.

Device Status

Before managing devices, you can familiarize yourself with the device status.

Status	Description
Online	The device is connected to YMCS.
Offline	The device is disconnected from YMCS.
Invalid	The server license expires, or the number of the devices reported to the platform exceeds the number allowed in the license.

Device Managing Features and Their Supported Devices

Following is the available features and their supported device type.

Supported Feature	Devices
Adding Devices	Phone device, Room System (only applicable to VC Room System)
Importing Devices	Phone device, Room System (only applicable to VC Room System)
Exporting the Device Information	Phone device, Room System, USB device
Editing the Device Information	Phone device, Room System, USB device
Viewing the Detailed Information of Phone Devices	Phone device
Searching for Devices	Phone device, Room System, USB device
Assigning Accounts to Devices	Phone device, Room System (only applicable to VC Room System and Zoom Rooms Kits)
Setting the Sites	Phone device, Room System, USB device
Pushing Configuration Files to Devices	Phone device, Room System (only applicable to VC Room System)
Pushing Firmware to Devices	Phone device, Room System, USB device
Pushing Resource Files to Devices	Phone device, Room System (only applicable to VC Room System)
Diagnosing Devices	Phone device, Room System, Workspace device, USB device
Enabling/Disabling DND	Phone device, Room System (only applicable to VC Room System)
Sending Messages to Devices	Phone device, Room System (only applicable to VC Room System)
Rebooting Devices	Phone device, Room System
Resetting the Devices to Factory	Phone device, Room System
Deleting Devices	Phone device, Room System, USB device
Auto Provisioning	Phone device
Viewing the Information of Connected Accessories	Room System

Adding Devices

After you connect the devices to YMCS, you need to add the devices so you can see them on the device list.

About this task

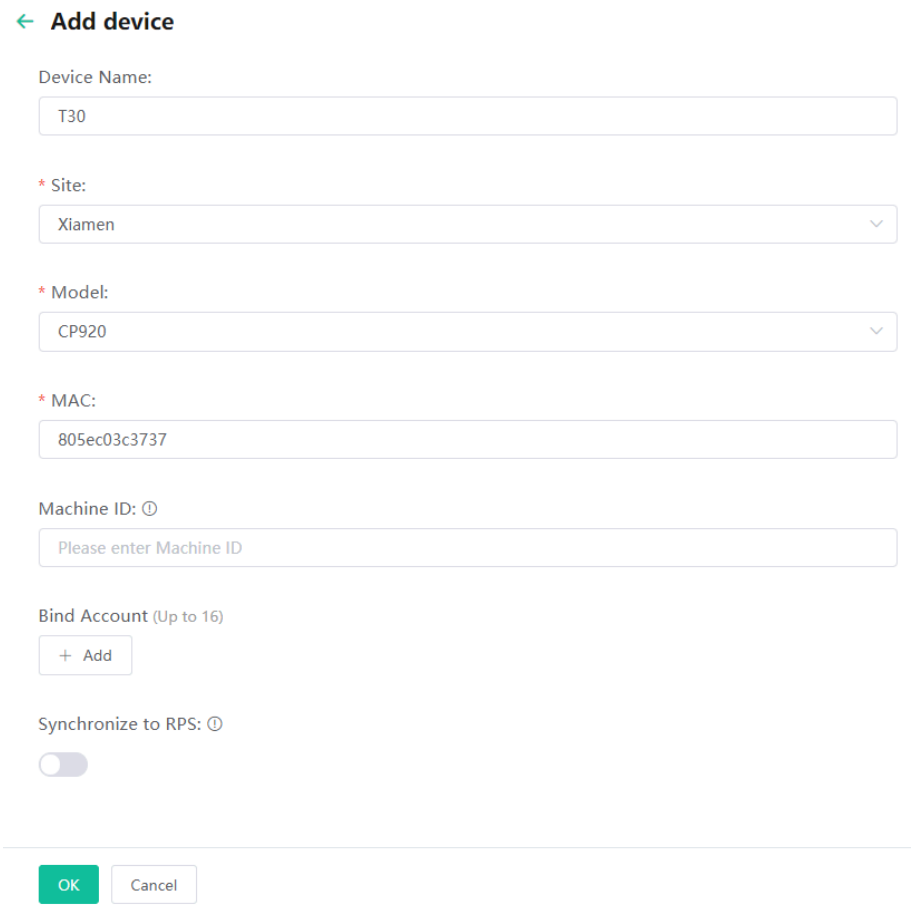
Note:

- You do not need to add USB device after connecting them to YMCS.
- If you deploy Agent and use it to connect devices to YMCS, you do not need to add devices.

Procedure

1. Click **Device Management** > **Phone Device/Room System** > **Add device**.
2. Set and save the parameters.

   Take the image of phone device as an example.



3. Optional: On the right side of the **Bind Account** field, click **Add**, and select an account and the account type to assign the account to the device.

   Note: This parameter is only applicable to phone devices.

4. Optional: If you want to use the RPS feature on YMCS, enable **Synchronize to RPS**, and set the related parameters of RPS.

   If you already have an RPS account, you can Binding RPS Accounts first, and enable **Synchronize to RPS**. After that, the device on YMCS will be synchronized with the devices on the RPS device management platform.

Related tasks

Assigning Accounts to Devices

Adding Accounts

Setting the Sites

Importing Devices

If you want to add devices quickly, you can import them in batch. You need to download the template, edit the devices information in the template and then import the template to YMCS.

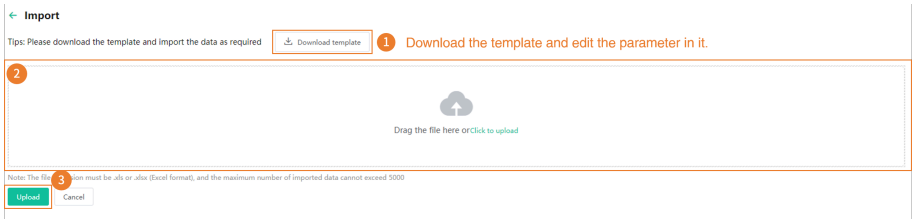
About this task

Before deploying the device, note the following:

- This feature is not applicable to USB and Workspace devices.
- If the device MAC address exists, the imported template will cover the previous account information, if you need to add new accounts, follow the note in the template.
- Only one account can be assigned to the SfB device, if there are multiple accounts, the first account is used by default.
- The number of accounts that can be linked to each device is different. If the number of accounts exceeds the limit, the exceeded accounts cannot be added by default.
- If a device with an account assigned to exists on the platform, and you import another device of the same model, the account information of the former device will be removed.
- If you enable **Synchronize to RPS**, make sure you enter the name of the server that you have already added.

Procedure

Click **Device Management** > **Phone Device/Room System** > **Import**.



Editing the Device Information

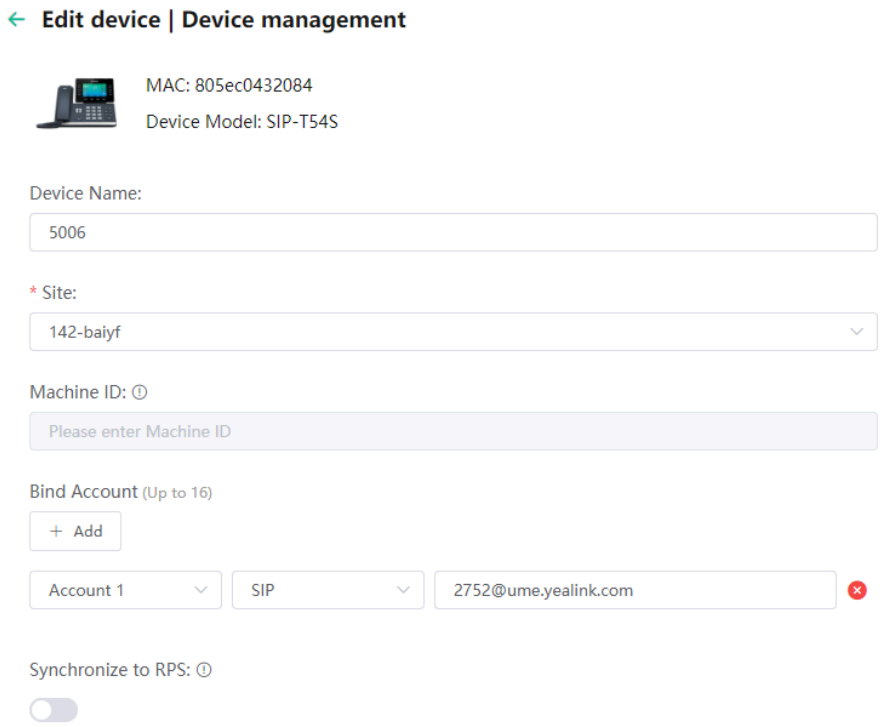
You can edit the device name and the site, or re-assign an account to the device.

Procedure

1. Click **Device Management** > **Phone Device/USB Device/Room System**.
2. Click beside the desired device.

3. Edit the device information and save it.

   Take the image of phone device as an example.



4. Optional: If you want to use the RPS feature on YMCS, enable **Synchronize to RPS**, and set the related parameters of RPS.

   If you already have an RPS account, you can Binding RPS Accounts first, and enable **Synchronize to RPS**. After that, the device on YMCS will be synchronized with the devices on the RPS device management platform.

Related tasks

Adding Accounts

Setting the Sites

Exporting the Device Information

You can export the basic information of phone device, USB device, and room system.

Procedure

Click **Device Management** > **Phone Device/USB Device/Room System** > **Export**.

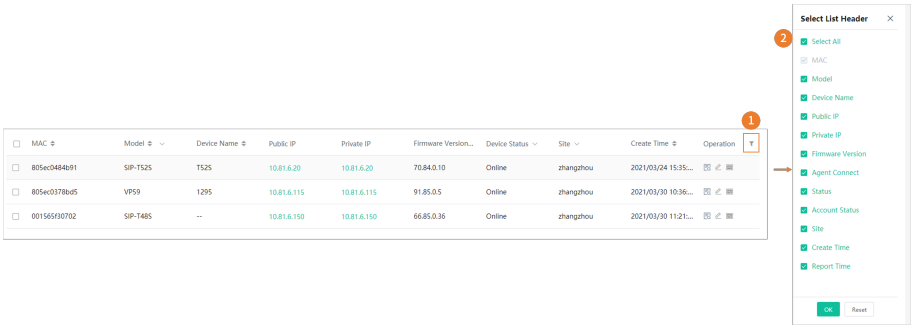
Viewing the Detailed Information of Phone Devices

You can view the device information, including the MAC address, the model, the name, the IP, the firmware version, the status, the site , the report time and so no. You can customize the desired information. If you deploy Agent in your enterprise, you can also view the connecting status between devices and Agent.

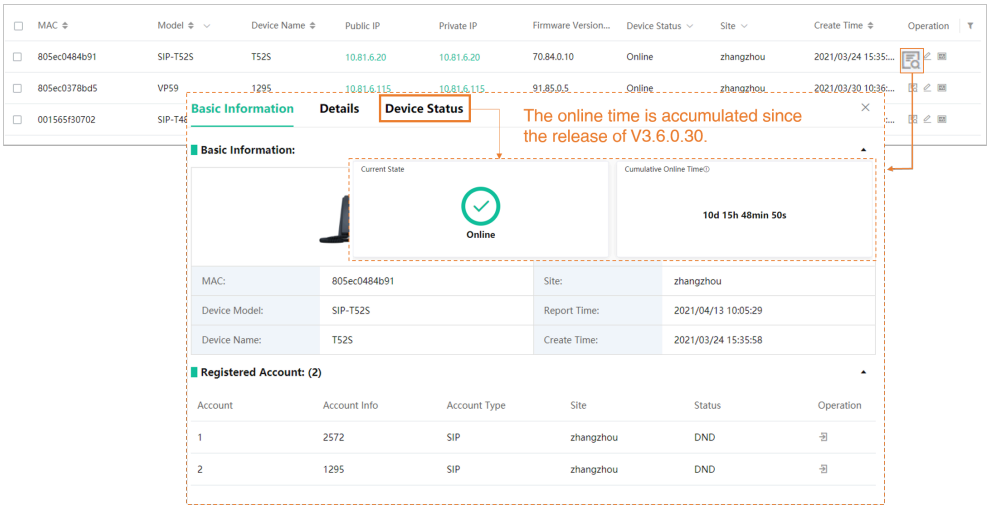
Procedure

1. Click **Device Management** > **Phone Device**.

2. Click on the right side of the page and select the desired filter.



3. Click beside the desired device.



Related concepts

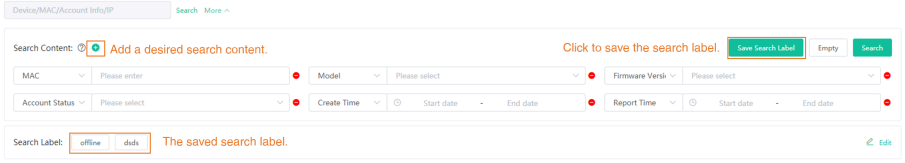
Device Status

Searching for Devices

You can use the search bar or the filters to search for the desired devices.

Procedure

Click **Device Management** > **Phone Device/USB Device/Room System**.



The search results are displayed in the device list.

Assigning Accounts to Devices

You can assign accounts to the device and YMCS will push the account information to the device.

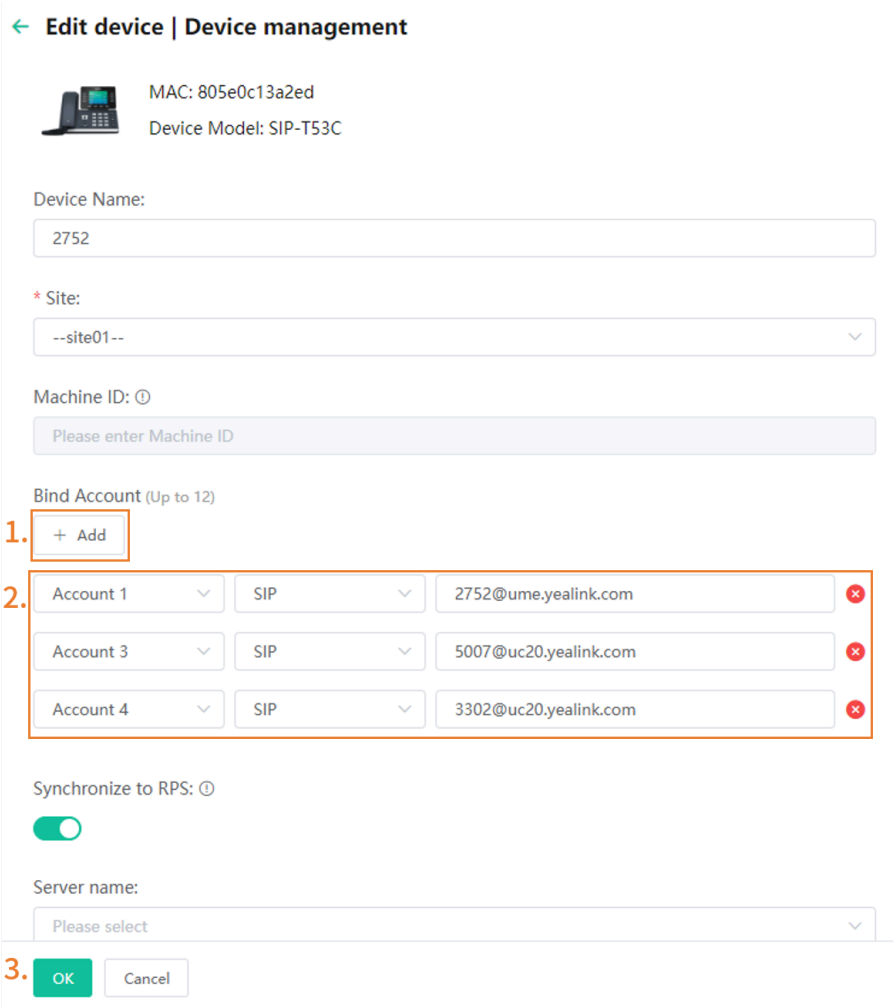
About this task

This feature is only applicable to phone devices and room system (not including MVC devices).

Procedure

1. Click **Device Management** > **Phone Device/Room System**.
2. Click beside the desired device, edit and save the corresponding parameter.

   Take the image of phone device as an example.



   The account information is sent to the device.

Note:

- When the device is offline, the account information will not be push to the device. When the device is online, it will be pushed.
- You can also see the account information you configure for the devices in other platforms on YMCS.

Related tasks
Adding Accounts

Setting the Sites

When editing the device information, you can edit the site which the device belongs to. You can put one device to a site or put multiple devices to the same site.

Procedure

1. Click **Device Management** > **Phone Device/USB Device/Room System**.
2. Select the corresponding devices and click **Site Settings**.
3. In the pop-up window, select the desired site and click **OK**.

Note: After setting the site, you can see the task details, refer to Viewing Executed Tasks.

Related tasks
Adding Sites

Pushing Configuration Files to Devices

You can push the configuration files to one or multiple devices.

Before you begin
If there are no desired configuration files, you can refer to Managing the Device Configuration to add one first.

About this task

Note:

- This feature is only applicable to phone device and VC room systems.
- When the device is in a call, the configuration file will not be pushed until the call is finished.
- When the device is offline or invalid, the configuration file cannot be pushed.
- When the device is unregistered, online or registered, the configuration file will be pushed.

  For more information about the device status, refer to Device Status.

Procedure

1. Click **Device Management** > **Phone Device/Room System**.
2. Select the corresponding devices and click **Update Configuration File**.
3. In the pop-up window, select the desired update content and the execution mode, then click **OK**.

Note:

- If you select **Update CFG by model template** and both the current site and the parent site have site configuration, the devices access both the configuration. The priority of the configuration in ascending order is the parent site and the current site.
- After updating the configuration file, you can see the task details, refer to Viewing Executed Tasks.

Related concepts
Managing the Device Configuration

Pushing Firmware to Devices

You can push the firmware to one or multiple devices.

Before you begin

If there is no desired firmware, you need to Adding Firmware.

About this task

- When the device is in a call, the firmware will not be pushed until the call is finished.
- When the device is offline or invalid, the firmware cannot be pushed.
- When the device is unregistered, online or registered, the firmware will be pushed.

  For more information about the device status, refer to Device Status.

Procedure

1. Click **Device Management** > **Phone Device/USB Device/Room System**.
2. Select the corresponding devices and click**Update Firmware**.
3. In the pop-up window, select the desired firmware version and the execution mode, then click **OK**.

Note:

- Note that the firmware must be applicable to all selected devices.
- After updating the firmware, you can see the task details, refer to Viewing Executed Tasks.

Related concepts

Managing Firmware

Pushing Resource Files to Devices

You can push resource files to one or multiple devices.

Before you begin

If there are no desired resource files, you need to Adding Resource Files.

About this task

- This feature is not applicable to USB devices.
- When the device is in a call, the resource file will not be pushed until the call is finished.
- When the device is offline or invalid, the resource file cannot be pushed.
- When the device is unregistered, online or registered, the resource file will be pushed.

  For more information about the device status, refer to Device Status.

Procedure

1. Click **Device Management** > **Phone Device/Room System**.
2. Select the corresponding devices and click **Update Resource File**.
3. In the pop-up window, select the desired resource type and file, select the execution mode, then click **OK**.

Note:

- The resource file you select must be applicable to all the selected devices. Otherwise, the device that not support the resource file fails to update.

- After updating the resource file, you can see the task details, refer to Viewing Executed Tasks.

Related concepts

Managing Resources

Diagnosing Devices

You can diagnose devices. You can diagnose up to 5 devices at the same time.

About this task

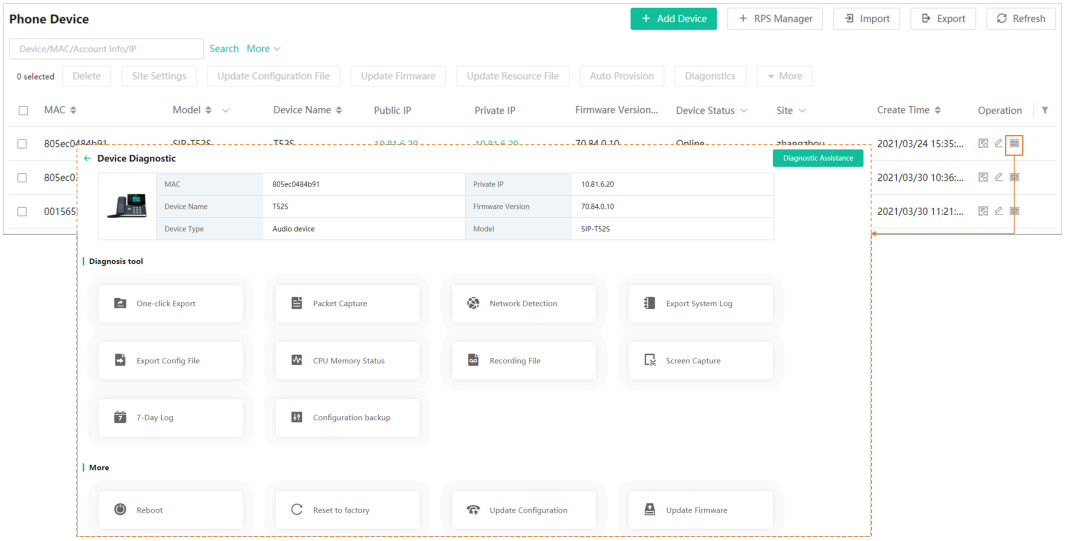
Note:

- For phone devices, you can diagnose a single device or up to 5 devices at the same time.
- For USB and room system devices, you cannot diagnose multiple devices at the same time.
- This feature is not applicable to the offline and invalid devices. For more information about the device status, refer to Device Status.

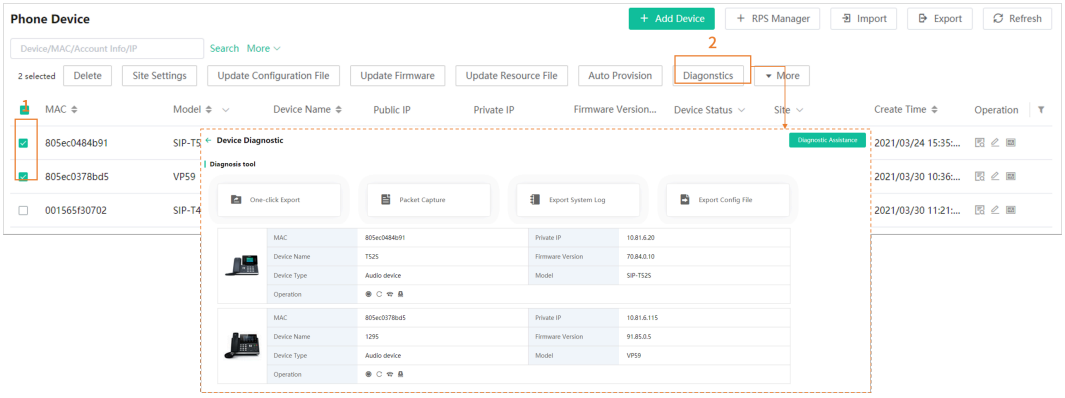
Procedure

1. Click **Device Management** > **Phone Device/USB Device/Room System**.

2. Diagnose the device.
   - Diagnose a single device.



   - Diagnose multiple devices



3. Select the desired diagnostic tool to diagnose the device.
4. After diagnosing, click **End Diagnostic**.

Related concepts

Diagnosing Devices

Enabling/Disabling DND

If your boss doesn't want to be disturbed during the break, you can enable DND for the boss's phone, and then cancel DND during office hours; if you need to make such settings every day, you can set it as a periodic task.

About this task

This feature is only applicable to phone devices and VC room systems.

Procedure

1. Click **Device Management** > **Phone Device/Room System**.
2. Select the corresponding devices and click **More→ DND/Cancel DND**.

3. In the pop-up window, select the desired execution mode and click **OK**.

   Note: After enabling/disabling DND, you can see the task details, refer to Viewing Executed Tasks.

Sending Messages to Devices

If you need to perform operations, for example, updating the firmware for the device, and you want to notify the device owner in advance, you can send a message to the device through YMCS. YMCS supports sending messages to one or multiple devices.

About this task

This feature is only applicable to phone devices and VC room systems.

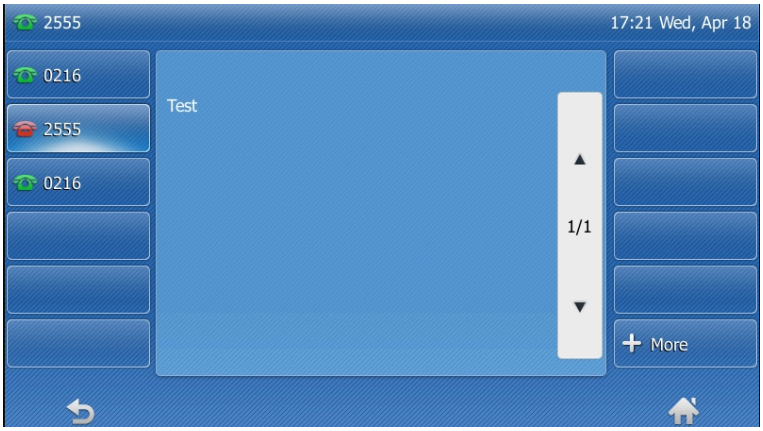
Procedure

1. Click **Device Management** > **Phone Device/Room System**.
2. Select the corresponding devices and click **More** > **Send Message**.
3. In the pop-up window, set the duration and the message content, then click **OK**.

   Note: After sending the messages, you can see the task details, refer to Viewing Executed Tasks.

Results

The message will pop up on the device screen. Take the T48S IP phone as an example:



Rebooting Devices

This feature is only applicable to phone device and room system.

Procedure

1. Click **Device Management** > **Phone Device/Room System**.
2. Select the corresponding devices and click **More**→ **Reboot**
3. In the pop-up window, select the desired execution mode and click **OK**.

   Note: After rebooting the device, you can see the task details, refer to Viewing Executed Tasks.

Resetting the Devices to Factory

About this task

This feature is only applicable to phone devices and room systems.

Procedure

1. Click **Device Management** > **Phone Device/Room System/Workspace Device**.
2. Select the corresponding devices and click **More→ Reset to factory**.
3. In the pop-up window, select the desired execution mode and click **OK**.

Note: After resetting the device, you can see the task details, refer to Viewing Executed Tasks.

Results

- After you reset the device, the account information, personal settings, or call history on the devices will be deleted.

Note:

- After you reset the device, the device status becomes offline on YMCS. You need to re-deploy the device (Connecting Phone Devices and Room Systems (Except for MVC/ZVC)) to make the device connect to YMCS.
- If you do not delete the reset devices on YMCS, when the devices are reconnected to YMCS, they will automatically obtain the configuration saved on YMCS.

Deleting Devices

Procedure

1. Click **Device Management** > **Phone Device/USB Device/Room System**.
2. Select the corresponding devices and click **Delete**.
3. Click **OK**.

Auto Provisioning

You can perform auto provisioning for a single or multiple devices on the platform.

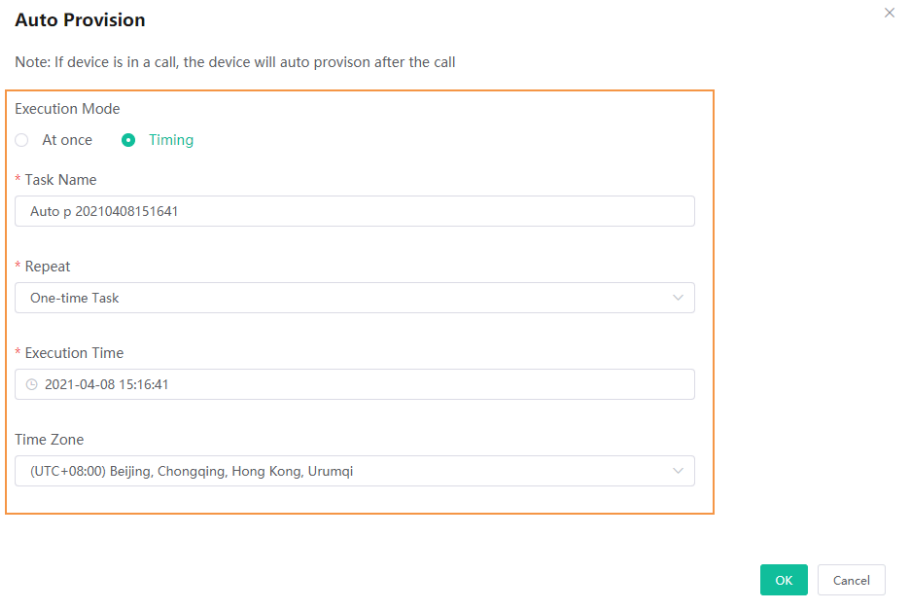
About this task

Note: This feature is only applicable to phone devices.

Procedure

1. Click **Device Management** > **Phone Device** > **Auto Provision**.
2. Select the corresponding devices and click **Auto Provision**.

3. Set the parameter and click **OK**.

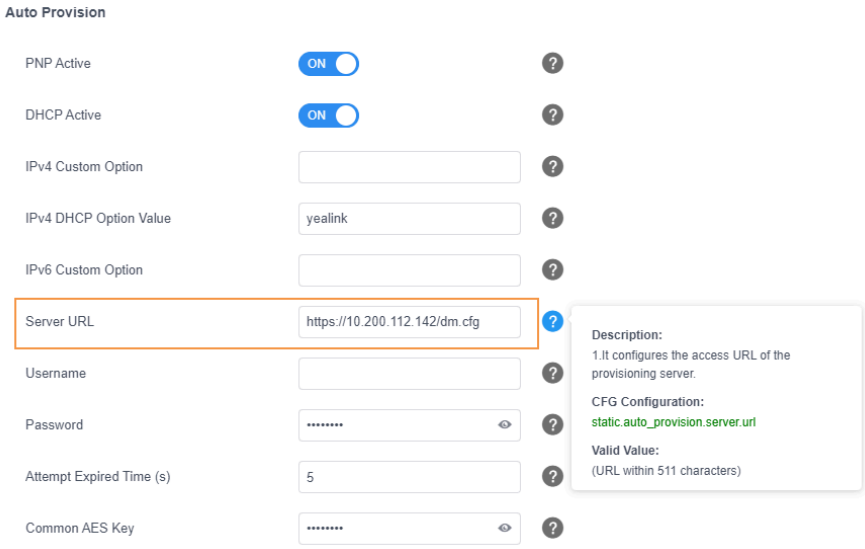


Note: After performing auto provisioning, you can see the task details, refer to Viewing Executed Tasks.

Results

The device will access the server URL to get the device configuration.

Note: The server URL is the address that you set on the device web user interface. Take VP59 as an example (log into the web user interface as an administrator and go to **Settings** > **Auto Provision**).



Viewing the Information of Connected Accessories

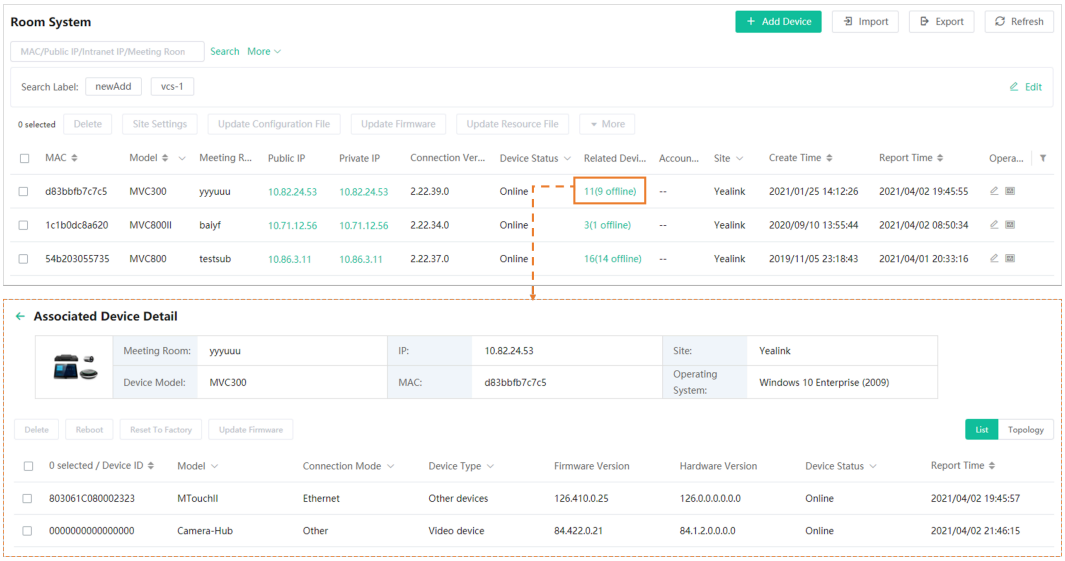
You can view the information of accessories connected to the Room System, including the name, the MAC address, the model, the meeting room name, the IP, the operating system, the status, the site and the report time.

About this task

Note: This feature is only applicable to room system.

Procedure

1. Click **Device Management** > **Room System**.
2. Click the blue font under the **Associated Device** tab and you can view the detailed information of the associated device of the room system.

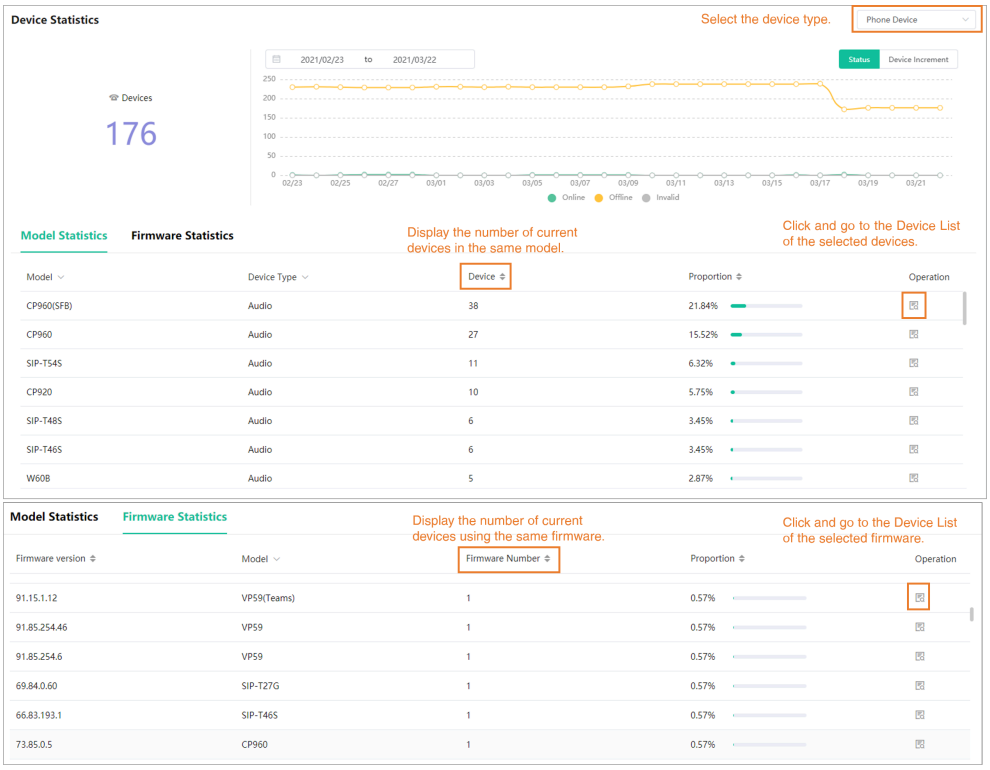


Viewing the Devices Statistics

The Device Statistics page displays the total number of current devices. Through the page, you can also view the statistics of phone devices, USB devices, and room systems, including the number of devices in the same model, the number of devices using the same firmware, the changes of device number/device status over time, and so on.

Procedure

Click **Dashboard** > **Devices Statistics**.



Managing Firmware

You can manage all the device firmware on YMCS.

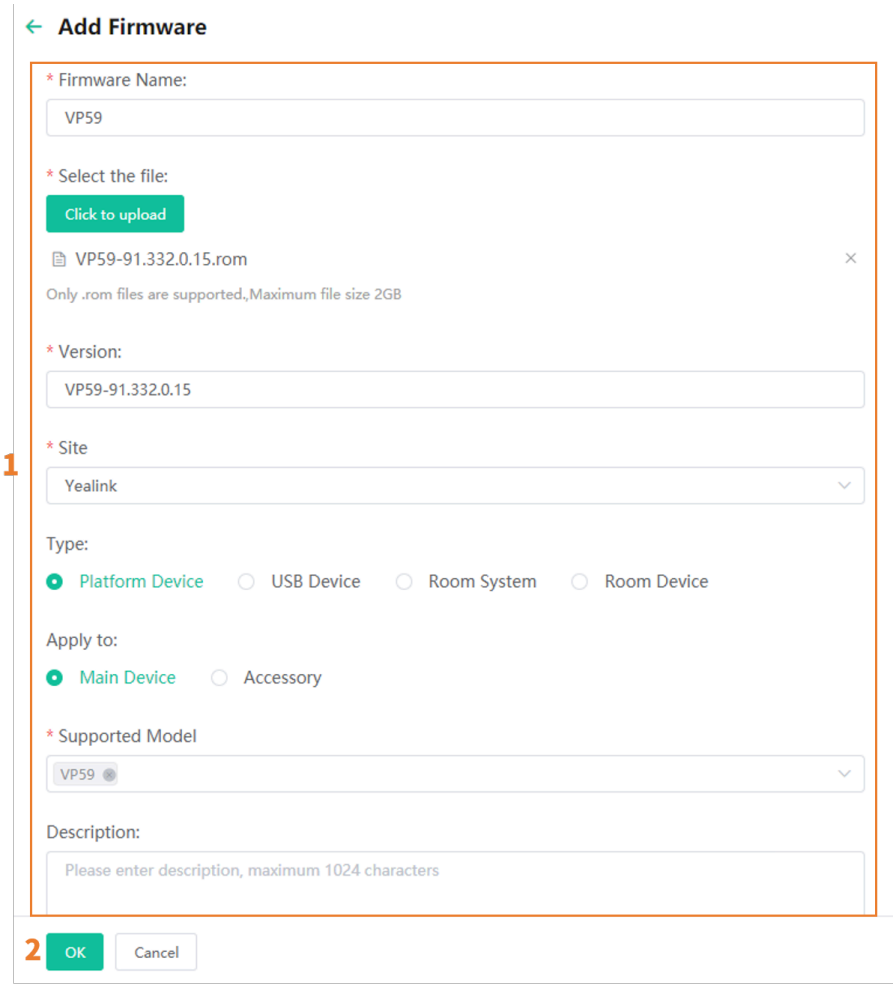
- Adding Firmware
- Sharing Firmware
- Pushing Firmware to Devices
- Editing the Firmware
- Downloading the Firmware
- Deleting Firmware

Adding Firmware

Procedure

1. Click **Firmware Management** > **Add Firmware**.

2. Enter the corresponding information and save it.



Sharing Firmware

You can share the desired firmware to others by sending the firmware address.

Procedure

1. Click **Firmware Management**.
2. Click beside the desired firmware.
3. Paste and share the firmware address to the desired person.

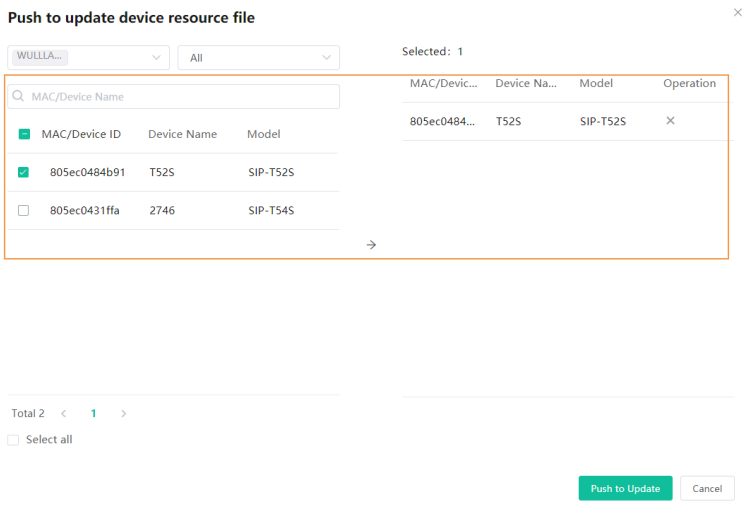
Pushing Firmware to Devices

When you need to update the device firmware, you can push the new firmware to the device. If it is not convenient for the device user to update the device during working time, you can set a timing task.

Procedure

1. Click **Firmware Management**.

2. Click beside the desired firmware.
3. Select the desired devices in the pop-up window and click **Push to Update**.



4. Select the desired execution mode.

Tip: You can also select the desired device in the Device List, click **Update Firmware**, and select the corresponding firmware version to update. For more information, refer to Pushing Firmware to Devices.

Note:

- Note that the firmware must be applicable to all selected devices.
- After updating the firmware, you can see the task details, refer to Viewing Executed Tasks.

Editing the Firmware

You can modify the firmware information, for example, the name and the version, or upload a new firmware to replace the old one.

Procedure

1. Click **Firmware Management**.
2. Click beside the desired firmware.
3. Edit ans save the corresponding parameters.

Downloading the Firmware

Procedure

1. Click **Firmware Management**.

2. Click beside the desired firmware.

Deleting Firmware

Procedure

1. Click **Firmware Management**.
2. Select the desired firmware.
3. Click **Delete**.
4. Click **OK** according to the prompts.

Results
After the firmware is deleted, the timer task associated with this firmware fails to execute.

Managing Resources

You can add and edit resource files, push resource files to devices or download them to your local system.

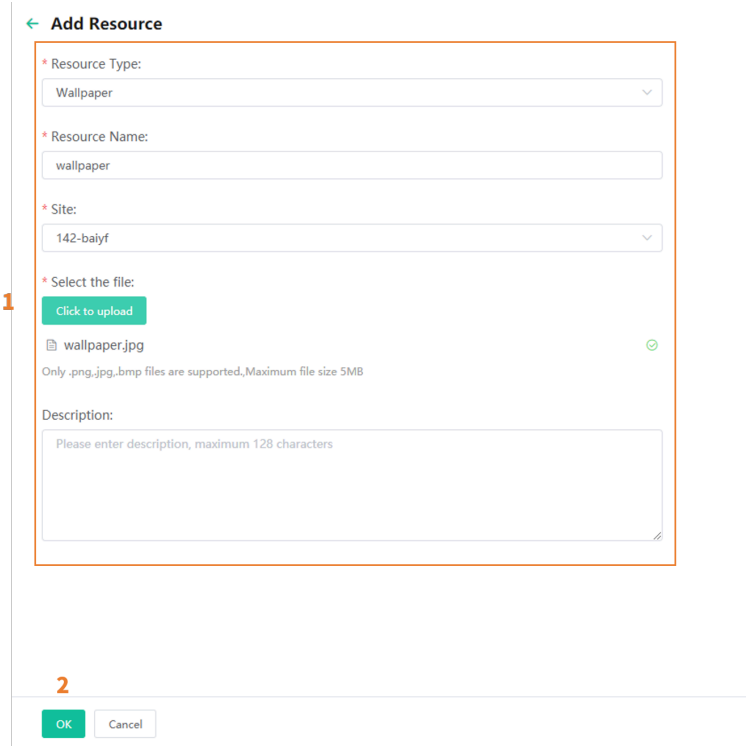
- Adding Resource Files
- Pushing Resource Files to Devices
- Editing Resource Files
- Downloading the Resource Files
- Deleting Resource Files

Adding Resource Files

Procedure

1. Click **Resource Management** > **Add Resource**.

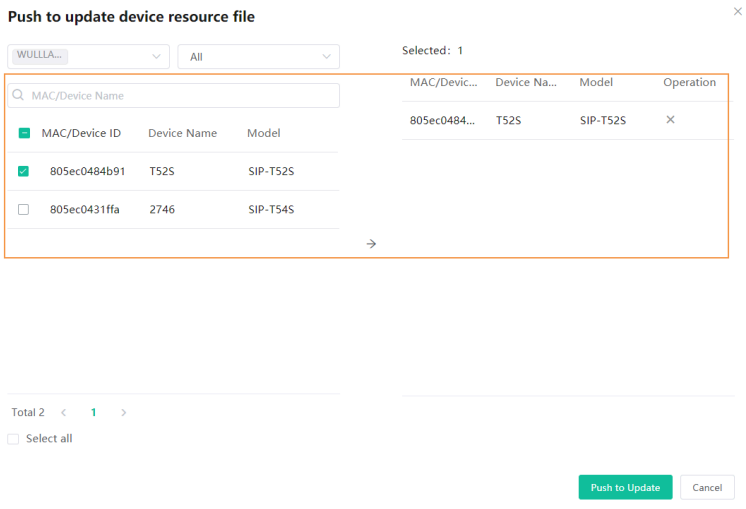
2. Add a resource file.



Pushing Resource Files to Devices

Procedure

1. Click **Resource Management**.
2. Click  beside the desired resource.
3. Select the desired devices in the pop-up window.



4. Click **Push to Update**.

5. Select the desired execution mode.

6. Click **OK**.

Tip: You can also select the desired devices in the Device List, click **Update Resource File**, and select the corresponding resource type to update.

Note:

- The resource file you select must be applicable to all the selected devices. Otherwise, the device that not support the resource file fails to update.
- After updating the resource file, you can see the task details, refer to Viewing Executed Tasks.

Editing Resource Files

Procedure

1. Click **Resource Management**.
2. Click beside the desired resource.
3. Edit the related information of the resource file in the corresponding field.
4. Click **Confirm**.

Downloading the Resource Files

Procedure

1. Click **Resource Management**.
2. Click beside the desired resource.
3. The file will be downloaded to your computer.

Deleting Resource Files

Procedure

1. Click **Resource Management**.
2. Select the desired resource.
3. Click **Delete**.
4. Click **OK** according to the prompts.

Results

After the resource is deleted, the timer task associated with this resource file fails to execute.

Managing Accounts

You can manage different devices on YMCS. Different devices may use different types of login accounts, so we divide the accounts into the SFB account, the SIP account, the YMS account, the Cloud account and the H.323 account for better management.

Note: This feature is not applicable to the Room System and the Teams phone.

Adding Accounts

Procedure

1. Click **Account Management**.
2. In the top-right corner of the page, click **Add Account** > **Add SFB account/Add SIP account/Add YMS account/Add CLOUD account/Add H323 account**.
3. Configure the account information.
4. Click **Confirm**.

Related tasks

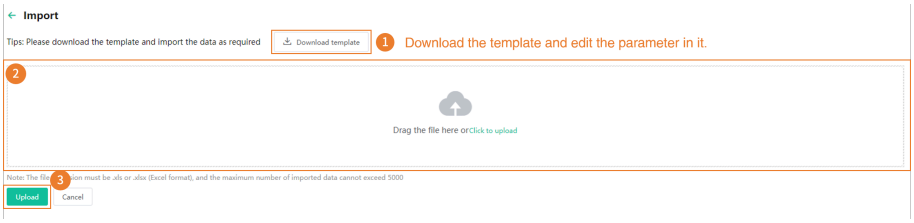
Assigning Accounts to Devices

Importing Accounts

You can import the template to add multiple accounts quickly. You need to download the template, add a batch of accounts, and then import the template to YMCS.

Procedure

1. Click **Account Management**.
2. In the top-right corner, click **Import** > **Import SFB account/Import SIP account/Import YMS account/Import CLOUD account/Import H323 account**.



Editing the Account Information

Procedure

1. Click **Account Management**.
2. Click beside the desired account.
3. Edit the account information.
4. Click **Confirm**.

Exporting Accounts

You can export the basic information of all accounts. The exported files are classified by different account types.

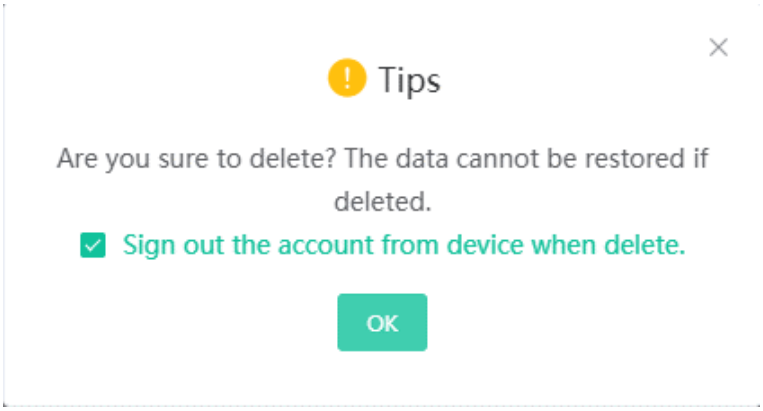
Procedure

1. Click **Account Management**.
2. In the top-right corner, click **Export**.
   The files are automatically saved to the local system, then you can view the basic information of all accounts.

Deleting Accounts

Procedure

1. Click **Account Management**.
2. Select the desired accounts.
3. Click **Delete** and confirm the action.
   If you select **Sign out the account from device when delete**, the account will be deleted from YMCS and signed out from the device. If you select **Sign out the account from device when delete**, the account will only be deleted from YMCS but not signed out from the device.



Managing the Device Configuration

You can manage the configuration file by model, by site, by group, or by MAC on YMCS, for example, creating or pushing the configuration file.

Introduction of obtaining the configuration:

- **Automatically obtaining the configuration:**

  After the devices are connected to YMCS, the devices can automatically obtain the configuration on YMCS if the following scenario occurs:

  - When you connect the device to the platform for the first time
  - When you reset the device (For devices in version 84 or before, you need to enable **Synchronize to RPS**, and enable **Redirection** on the devices; for devices in version 84 or later, they can obtain the configuration automatically. For the detailed device version, contact Yealink technical support.)

  The priority of obtaining the configuration in ascending order is RPS, global, model, site, MAC. The group configuration can only be updated manually.

  If both the current site and the parent site have site configuration, the devices access both the configuration. The priority of the configuration in ascending order is the parent site and the current site.

- **Manually obtaining the configuration:**

  For the devices existing on YMCS, they would not automatically obtain the updated configuration. Therefore, you need to push the configuration to them.

Managing Model Configuration

You can customize the configuration template according to the device model, that is, one template for one device model configuration. You can update the device configuration by setting the parameters in the template or editing the model configuration in the text.

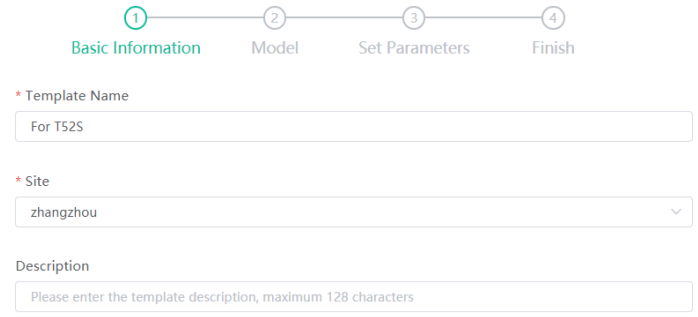
Adding Configuration Templates

You can add configuration templates to manage the corresponding device models.

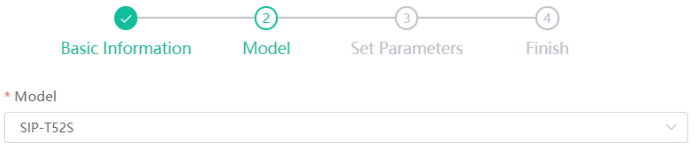
Procedure

1. Click **Device Configuration** > **Model Management** > **Add Template**.

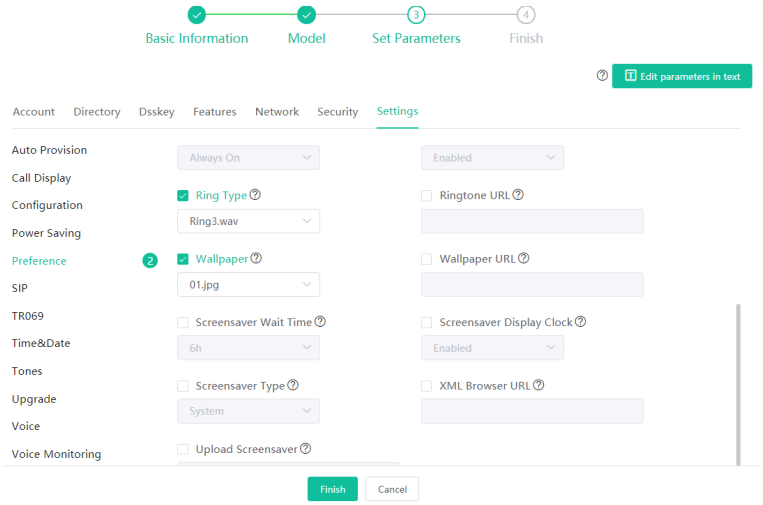
2. Set the basic information and click **Next step**.



3. Select the device model and click **Next step**.



4. Set the parameter and click **Finish**.



Setting Parameters

About this task

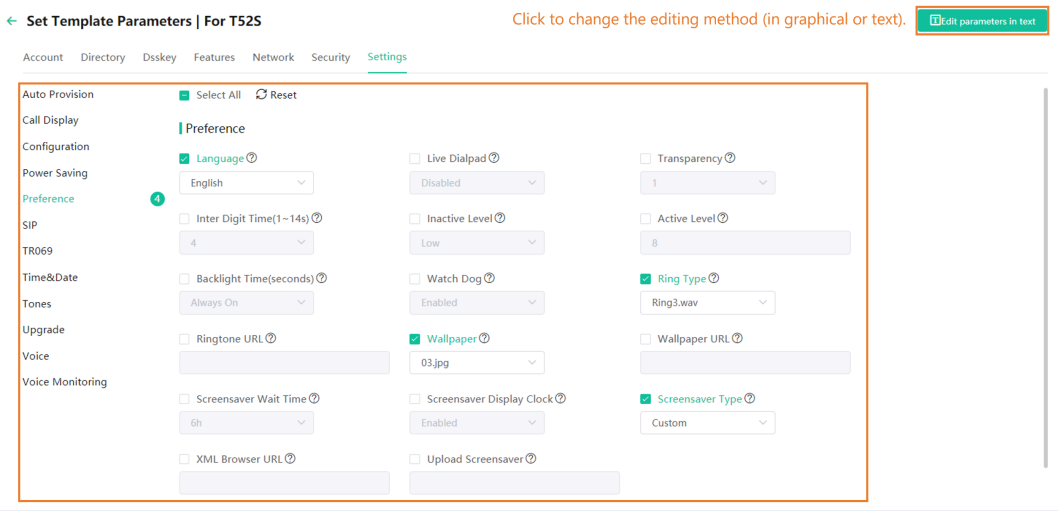
You can choose one of the following methods to configure the parameters:

- Edit parameters in the text: you can edit any parameter supported by the device in the text.
- Edit parameters on the graphical editing page: you can edit the corresponding template parameters on the graphical editing page.

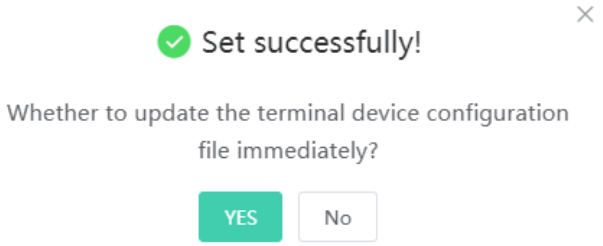
Procedure

1.
2. Click / on the right side of the desired template.

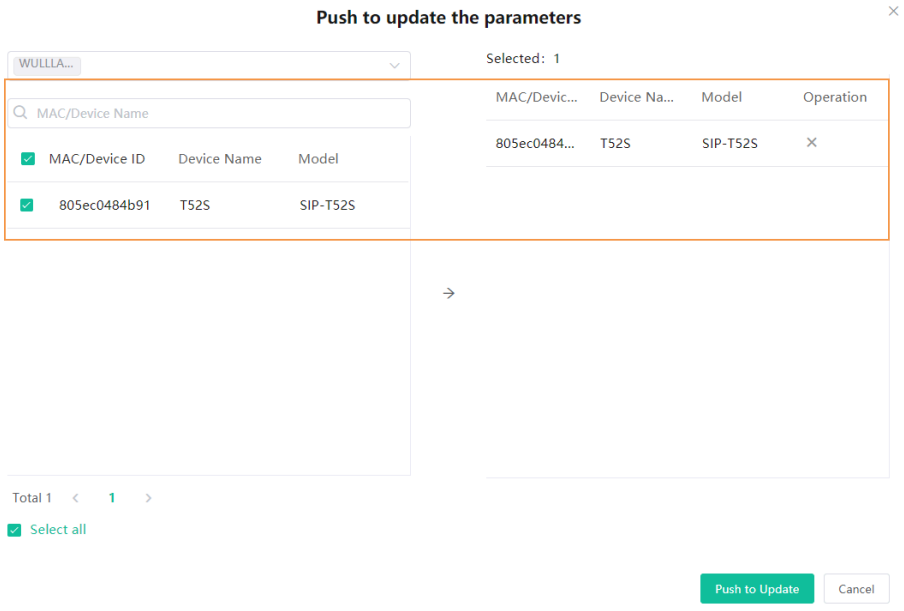
3. Set the parameters and click **Save** .



4. On the pop-up window, select **Yes** to push the edited configuration immediately, or **No** to save the edited configuration.



5. Push the selected configuration.



6. Select the desired execution mode.

Note:

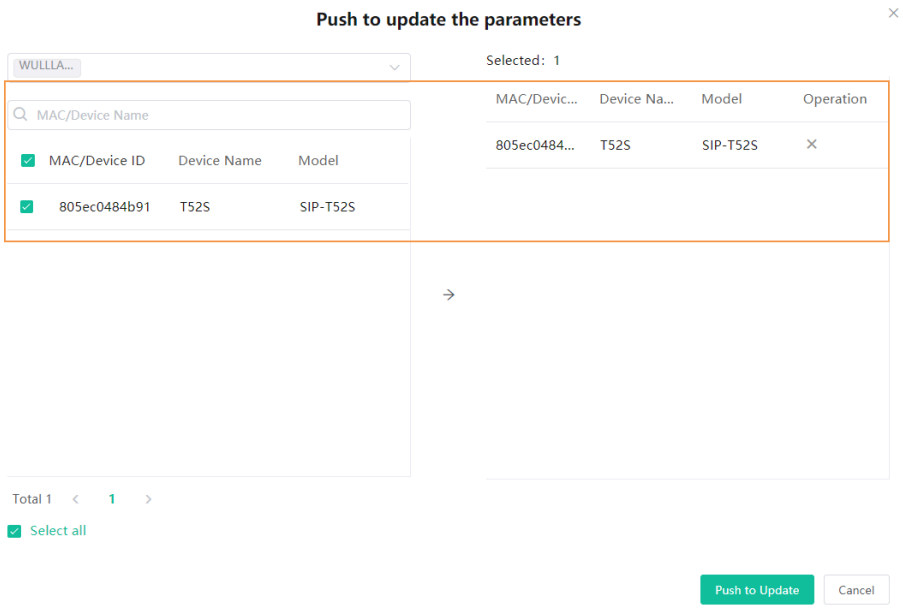
- If you select **At once**, the configuration will be pushed to the selected devices immediately.
- If you select **Timing**, the configuration will be pushed to the selected devices at the time you set.
- If the edited templates are involved, the timer tasks will be executed according to the last template that you edit and save.

Pushing Configuration to Devices

You can push the configuration to devices if you have updated the configuration in the text or in the template.

Procedure

1. Click **Device Configuration** > **Model Management**.
2. Click on the right side of the desired template.
3. Push the selected configuration.



4. Select the desired execution mode.

Note:

- You can also select the desired devices in the Device List, click **Update Configuration File**, select **Update CFG by model template** to update.

- After updating the configuration file, you can see the task details, refer to Viewing Executed Tasks.

Editing Template Information

You can edit the name and the description of the configuration templates, but you cannot edit the device model.

Procedure

1. Click **Device Configuration** > **Model Management**.
2. Click  on the right side of the desired template.
3. Edit and save the parameters.

Downloading the Model File

You can download the configuration template to your computer to view the configuration parameters.

Procedure

1. Click **Device Configuration** > **Model Management**.
2. Click  on the right side of the desired template.

Deleting Templates

Procedure

1. Click **Device Configuration** > **Model Management**.
2. Select the desired templates.
3. Click **Delete**.
4. Click **OK** according to the prompts.

Results

After you delete the template, the timer tasks involving this template will fail to execute.

Managing the Site Configuration

You can customize and manage the configuration according to the site that the devices belong to. Site configuration applies to all the offline devices in the site and its sub-sites.

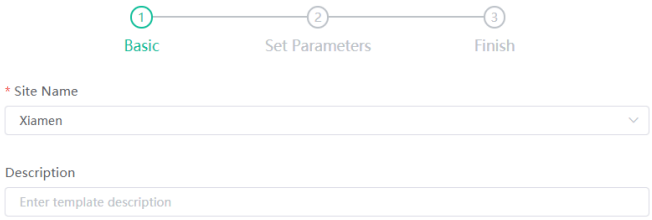
- Adding Site Configuration Templates
- Setting Parameters
- Pushing the Site Configuration to Devices
- Editing the Site Configuration Template
- Downloading the Site Configuration Template
- Deleting Site Configuration Templates

Adding Site Configuration Templates

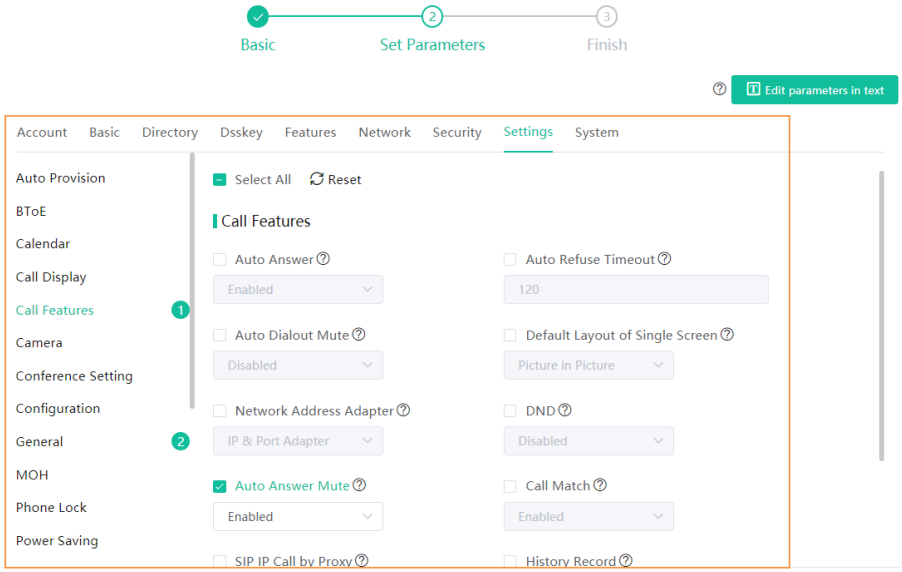
Procedure

1. Click **Device Configuration** > **Site Configuration** > **Add Template**.

2. Set the site name and click **Next**.



3. Set the parameter and click **Finish**.



Setting Parameters

About this task

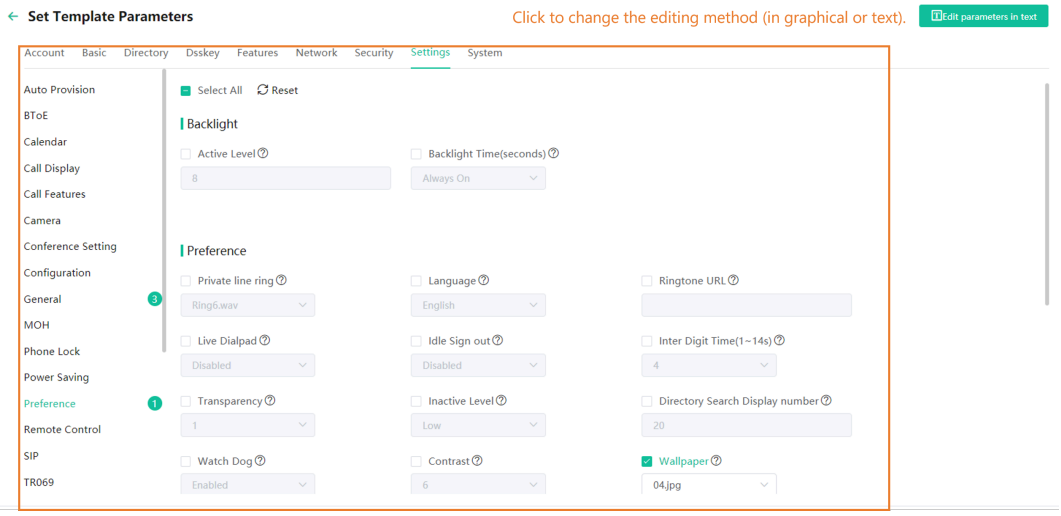
You can choose one of the following methods to configure the parameters:

- Edit parameters in the text: you can edit any parameter supported by the device in the text.
- Edit parameters on the graphical editing page: you can edit the corresponding template parameters on the graphical editing page.

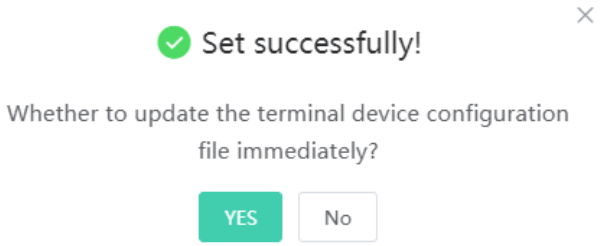
Procedure

1. Click **Device Configuration** > **Site Configuration**.
2. Click / on the right side of the desired template.

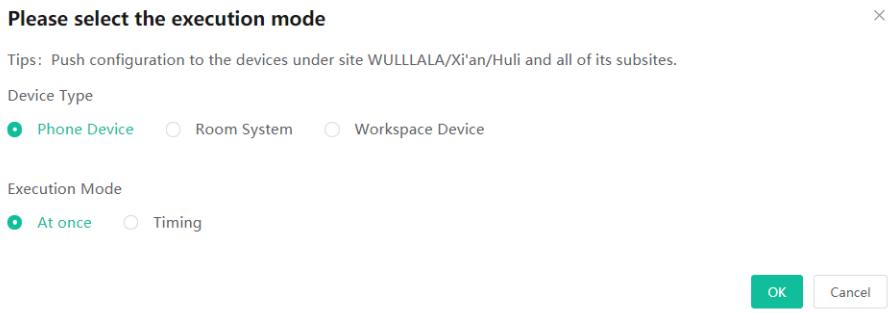
3. Set the parameters and click **Save** .



4. On the pop-up window, select **Yes** to push the edited configuration immediately, or **No** to save the edited configuration.



5. Select the desired device type and executing mode.



Note:

- If you select **At once**, the configuration will be pushed to the selected devices immediately.
- If you select **Timing**, the configuration will be pushed to the selected devices at the time you set.
- If the edited templates are involved, the timer tasks will be executed according to the last template that you edit and save.

Pushing the Site Configuration to Devices

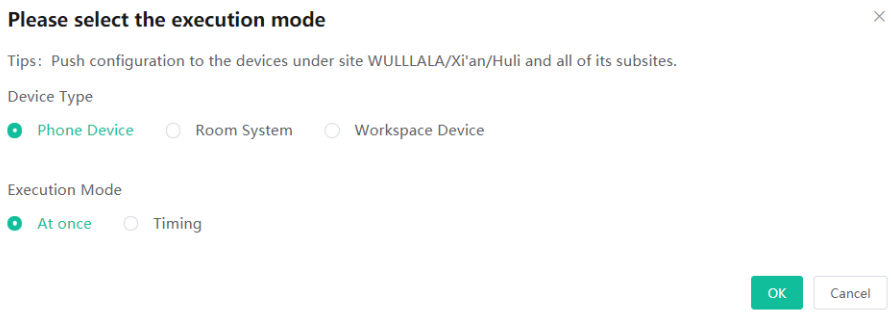
You can select the desired configuration and push it to all the devices in the corresponding site and the sub-sites.

About this task

If the sub-sites have their configuration files, their configuration files will cover the configuration files of their parent sites.

Procedure

1. Click **Device Configuration** > **Site Configuration**.
2. Click beside the desired template.
3. Select the desired device type and executing mode.



Note: After updating the configuration file, you can see the task details, refer to Viewing Executed Tasks.

Editing the Site Configuration Template

You can only edit the description of the site configuration template.

Procedure

1. Click **Device Configuration** > **Site Configuration**.
2. Click on the right side of the desired template.
3. Edit and save the parameters.

Downloading the Site Configuration Template

You can download the configuration template to your computer to view the configuration parameters.

About this task

Procedure

1. Click **Device Configuration** > **Site Configuration**.
2. Click on the right side of the desired template.

Deleting Site Configuration Templates

Procedure

1. Click **Device Configuration** > **Site Configuration**.
2. Select the desired template.
3. Click **Delete**.
4. Click **OK**.

Results

After you delete the template, the timer tasks involving this template will fail to execute.

Managing the Group Configuration

You can customize the group configuration for different departments of your company (for example marketing department and product department). When you push the configuration, online (registered or unregistered) devices are updated in real time when they receive updates.

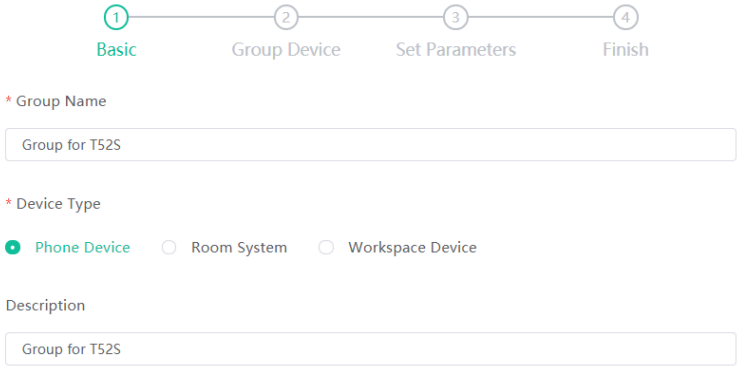
- Adding the Group Configuration
- Setting Parameters
- Editing the Group Configuration Template
- Pushing the Group Configuration
- Downloading Configuration File
- Deleting Groups

Adding the Group Configuration

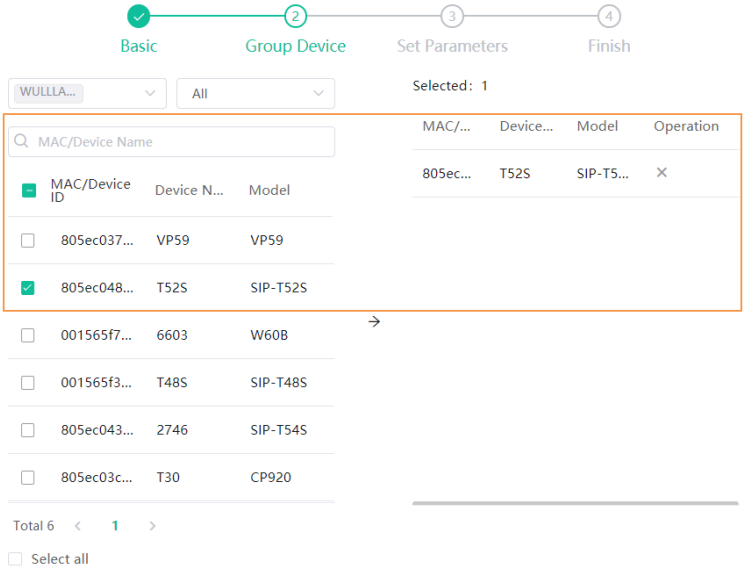
You can add the name and description, select devices and customize the device setting for a group configuration.

Procedure

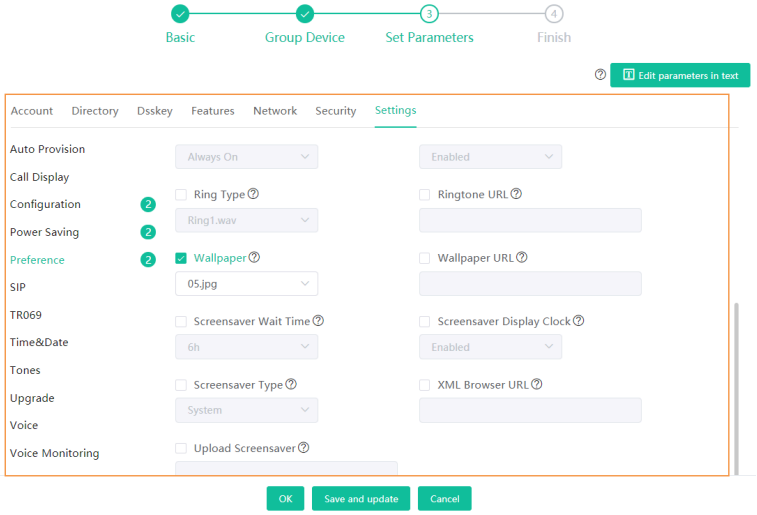
1. Click **Device Configuration** > **Group Configuration** > **Add Group**.
2. Set the group name, select the device type, and click **Next step**.



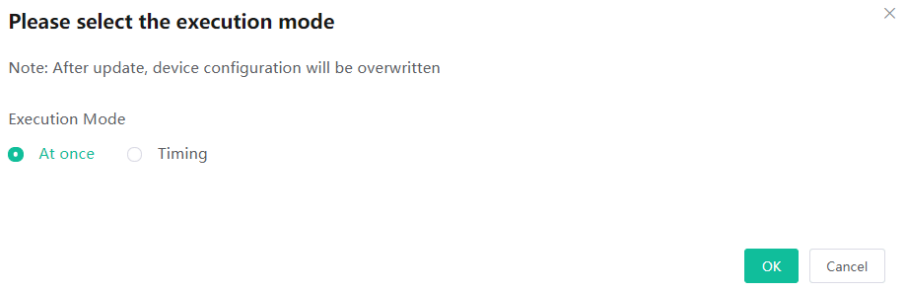
3. Select the desired device to the group.



4. Set the parameter and click **Save and update**.



5. Select the desired execution mode and click **OK**.



Note:

- If you select **At once**, the configuration will be pushed to the selected devices immediately.
- If you select **Timing**, the configuration will be pushed to the selected devices at the time you set.

- After updating the configuration file, you can see the task details, refer to Viewing Executed Tasks.

Setting Parameters

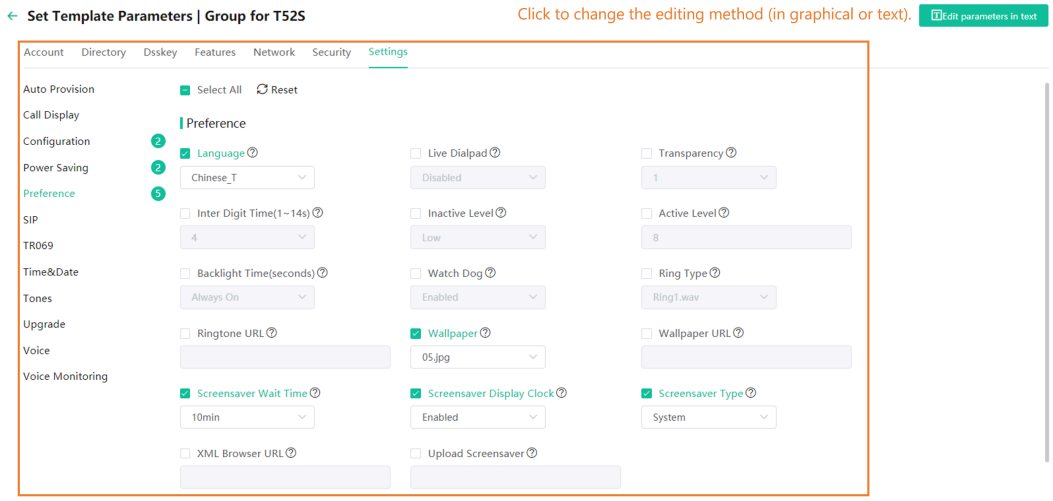
About this task

You can choose one of the following methods to configure the parameters:

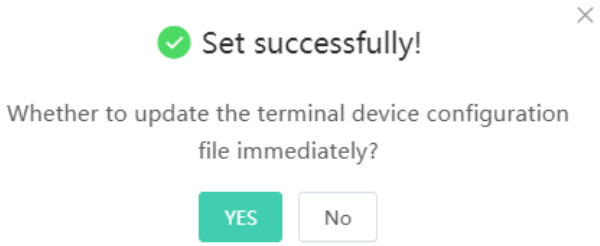
- Edit parameters in the text: you can edit any parameter supported by the device in the text.
- Edit parameters on the graphical editing page: you can edit the corresponding template parameters on the graphical editing page.

Procedure

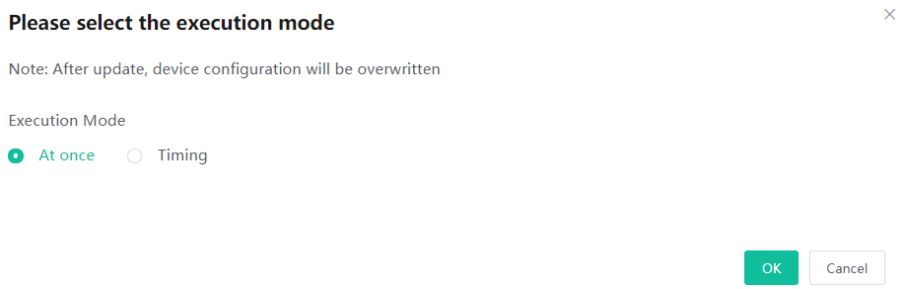
1. Click **Device Configuration** > **Group Configuration**.
2. Click / on the right side of the desired template.
3. Set the parameters and click **Save** .



4. On the pop-up window, select **Yes** to push the edited configuration immediately, or **No** to save the edited configuration.



5. Select the desired execution mode and click **OK**.



Note:

- If you select **At once**, the configuration will be pushed to the selected devices immediately.
- If you select **Timing**, the configuration will be pushed to the selected devices at the time you set.
- If the edited templates are involved, the timer tasks will be executed according to the last template that you edit and save.

Editing the Group Configuration Template

You can edit the name and the description, reselect the devices and reset the device parameters for the group.

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Click on the right side of the desired template.
3. Edit and save the parameters.

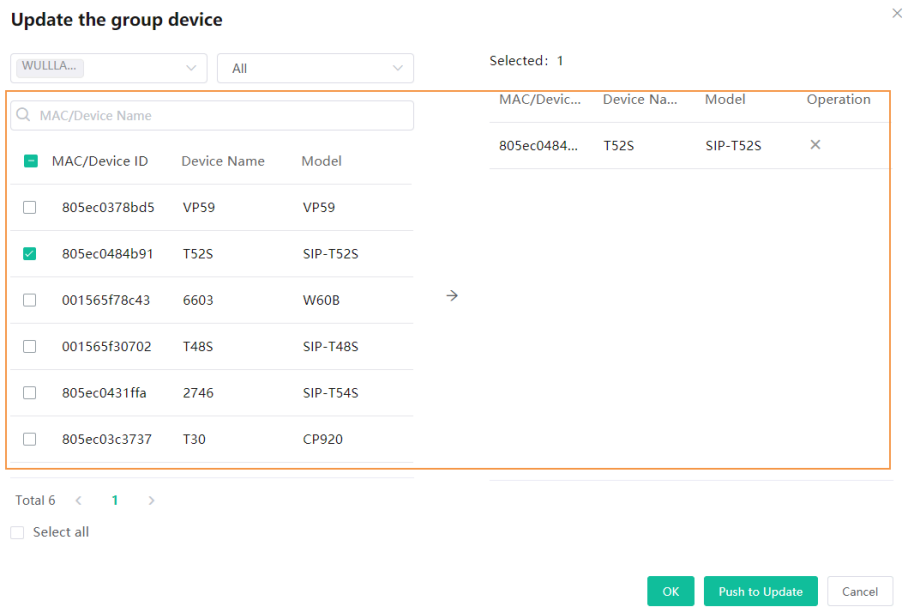
Pushing the Group Configuration

When you need to add or remove devices in your group, you can update the group device and choose to save the group configuration directly or push the parameters to the selected devices immediately.

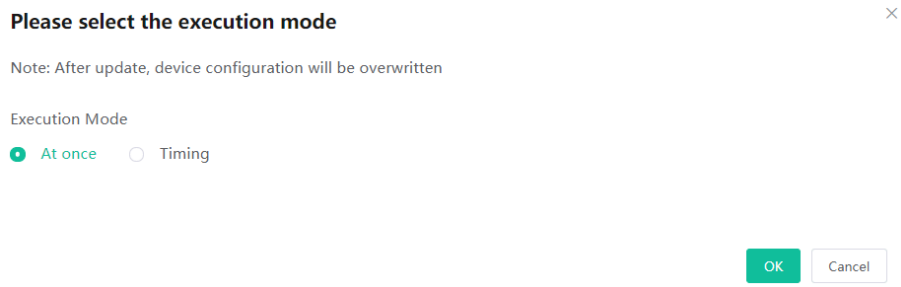
Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Click beside the desired template.

3. Select the desired device.



4. Select the desired execution mode.



Note: After updating the configuration file, you can see the task details, refer to Viewing Executed Tasks.

Downloading Configuration File

You can download the configuration template to your computer to view the configuration parameters.

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Click on the right side of the desired template.

Deleting Groups

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Select the desired group template.
3. Click **Delete**.
4. Click **OK** according to the prompts.

Results

After you delete the template, the timer tasks involving this template will fail to execute.

Managing the MAC Configuration

You can upload, generate, download and export the configuration file, you can also push the backup files to devices.

- Uploading Configuration Files
- Generating Configuration Files
- Pushing Backup Files to Devices
- Downloading the Configuration Files
- Exporting the Configuration Files
- Deleting Backup Files

Uploading Configuration Files

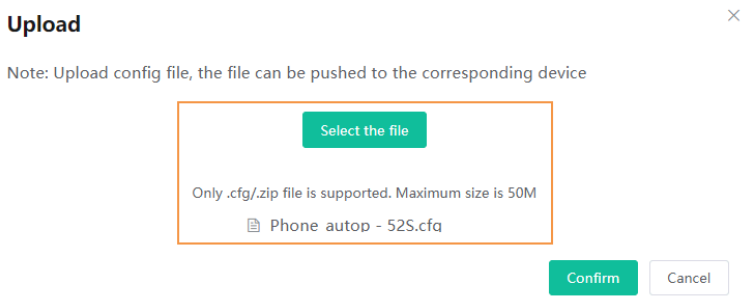
You can update the configuration for one or more devices by uploading the configuration file.

About this task

Note: If the uploaded configuration file is within the data permission range of the current account, the site is displayed as the site to which the device belongs. If the site is displayed as "--", it means that the device has not been added.

Procedure

1. Click **Device Configuration** > **MAC Configuration** > **Upload**.
2. Upload the desire file and click **Confirm**.



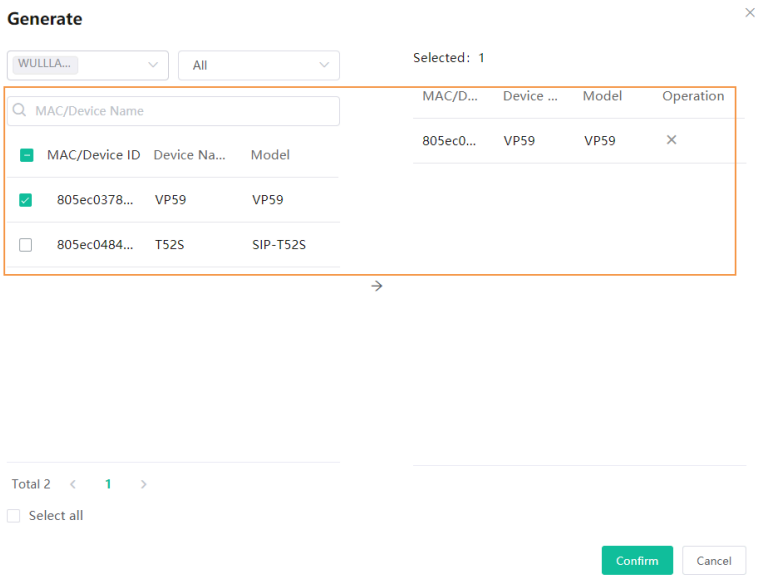
Generating Configuration Files

You can generate configuration files to back up the configuration on YMCS.

Procedure

1. Click **Device Configuration** > **MAC Configuration** > **Generate**.

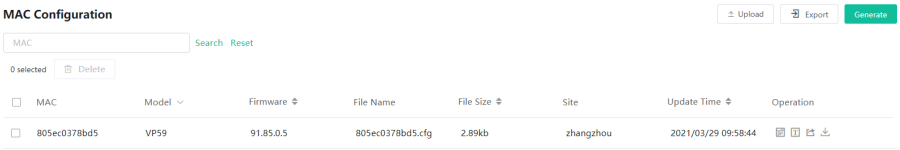
2. Select the desired devices on the pop-up window and click **Confirm**.



If the device has already generated a configuration file, click **Replace** to generate a new configuration file.

Results

The generated files are in the list as below:



Pushing Backup Files to Devices

Procedure

1. Click **Device Configuration** > **MAC Configuration**.
2. Click beside the desired MAC configuration.

Note: After updating the configuration file, you can see the task details, refer to Viewing Executed Tasks.

Downloading the Configuration Files

You can download the backup files to your local system.

Procedure

1. Click **Device Configuration** > **MAC Configuration**.
2. Click beside the desired MAC configuration to download the backup to your local system.

Exporting the Configuration Files

You can export all device configuration files by one click.

Procedure

1. Click **Device Configuration** > **MAC Configuration**.
2. In the top-right corner, click **Export**.

   This will export all MAC configuration files.

Deleting Backup Files

Procedure

1. Click **Device Configuration** > **MAC Configuration**.
2. Select the desired backup file.
3. Click **Delete**.
4. Click **OK** according to the prompts.

Results

After you delete the template, the timer tasks involving this template will fail to execute.

Configuring Global Parameters

The global parameter applies to all devices connected to the device management platform.

Procedure

1. Click **Device Configuration** > **Global Parameters Settings**.
2. Set and save the parameters.

   Note:

   - You can also click **Save and update,** and click **OK** to update the global parameters to all devices.
   - After updating the global parameters, you can see the task details, refer to Viewing Executed Tasks.

Managing Sites

You can set sites according to your enterprise organization, and manage the devices in the same site.

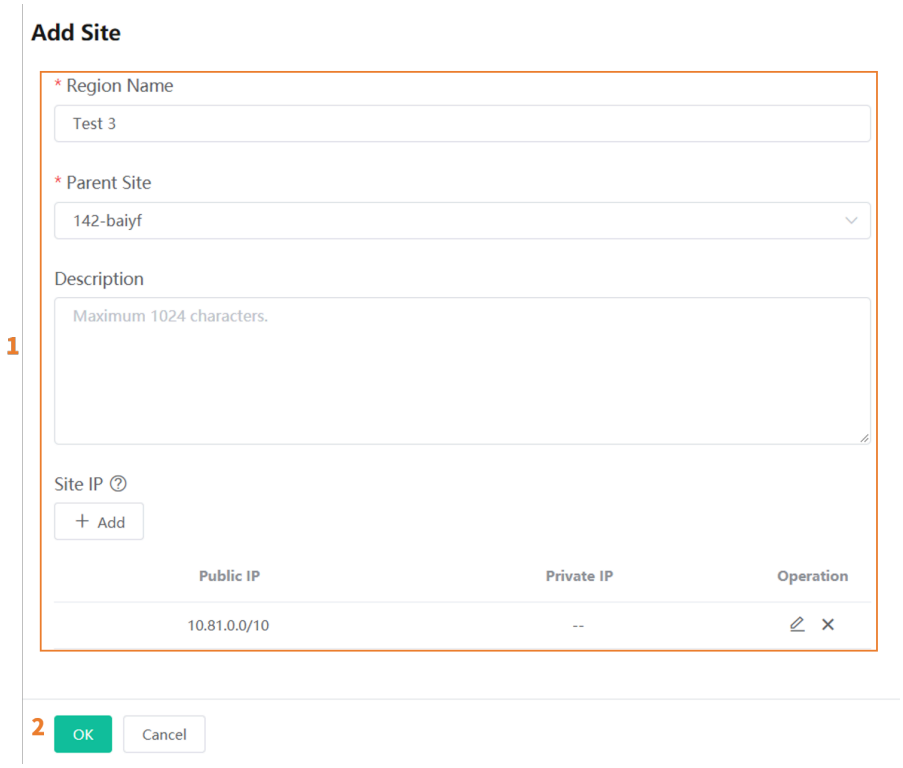
Note: The default site named after your company name is added when the system is initialized.

- Adding Sites
- Importing Sites
- Managing Sites

Adding Sites

Procedure

1. Click **Site Management** > **Add Site**.
2. Set and save the parameters.



Tip: You can enter 0.0.0.0 in the **Public IP** field, which means all IP addresses are acceptable.

Results

After adding sites, you can move devices to the site and manage the devices. Setting site IP makes the devices automatically assigned to the corresponding site if the device IP addresses are in the site IP range.

Note:

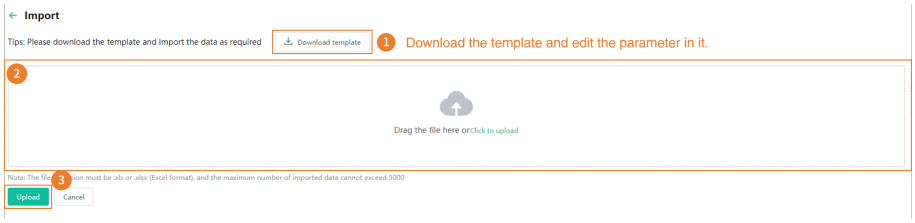
- The priority (the devices automatically connected to the site) in the descending order is site IP setting, the site setting in the Common.cfg file, the site setting in importing a batch of devices.
- When a device is in the IP range of a sub-site and a superior site, the device goes to the sub-site with priority.
- For sites at the same level, if site A is configured with both the public and the private IP while the site B is configured with only the public IP, the device goes to site A with priority.

Importing Sites

You can import a template to add multiple sites quickly. You need to download the template, edit the information in the template and then import the template to YMCS.

Procedure

Click **Site Management** > **Import**.



Managing Sites

After adding or import site, you can edit the site name/IP, organize or delete the site.

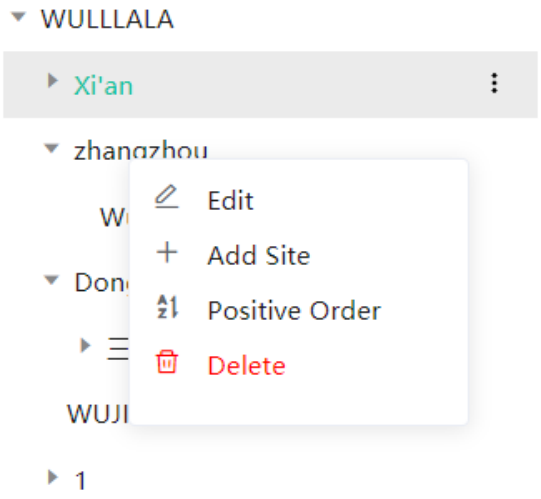
Procedure

1. Click **Site Management**.
2. Hover your mouse on the desired site, click ⋮, and do one of the following:
   - Click the desired site and drag the site to the desired position.

     Note:

     - For site of the same level, you can move the site up or down but cannot change its parent site, one position at a time.

    - When you move a site that has sub-sites, the whole sub-tree is moved.
- Select **Edit** to edit the site information.
- Select **Add Site** to add sub-site under the selected site.
- Select **Positive Order** rearrange the site in alphabetical order. If you want to cancel the positive order, select **Cancel**.
- Select **Delete** to delete the site. Note that if the site or its sub-site has devices, you cannot delete the site.



Managing Tasks

The Scheduled Task page displays the added timer tasks and allows you to add, view, or edit timer tasks on this page. The Executed Task page displays the executed tasks and allows you to view all the executed tasks, view the details of the failed execution, and retry the failed tasks.

Execution mode	• At once: the task is executed immediately. • Timing: the task is executed at the time you set.

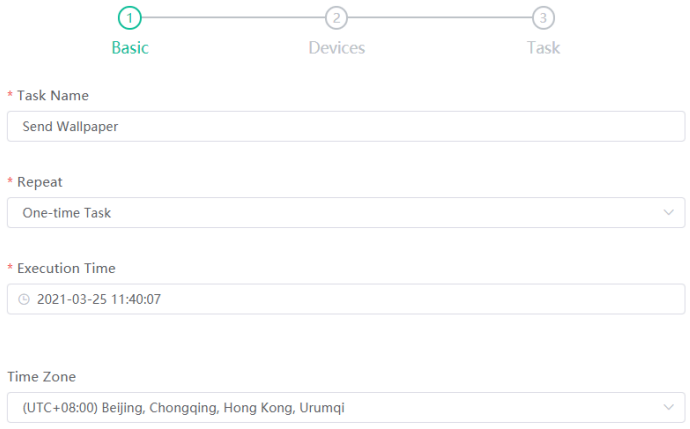
Tasks and Rules	• Update resource file: you can only push one file of the same resource type at a time. Only the resource file supported by the selected device can be pushed.
	• Upgrade firmware: if you select devices of different models, only the firmware applicable to all the devices can be pushed.
	• Update config file:
	  • Update CFG by model template: the system will push the configuration of the corresponding model template to the selected device. If the corresponding model temple does not exist, no push is performed.
	  • Update CFG by factory defaults: the system will push the system default configuration to the selected device.
	• DND/Cancel DND: DND is enabled or disabled for the registered accounts you select on the selected device.
	• Push global parameters: the system will push the global parameter to the selected devices.
	• Send message: the system will send messages to the selected devices.

	• Reboot/Reset to factory: the system will reboot the selected devices or reset the selected devices to factory. • Update site configuration: the system will push the site configuration you select to the selected devices. • Update group configuration: the system will push the group configuration you select to the selected devices. • Push MAC config: the system will push the MAC configuration you select to the selected devices.

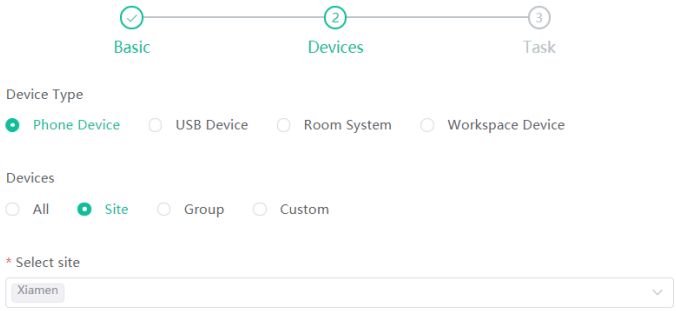
Adding Timer Tasks

Procedure

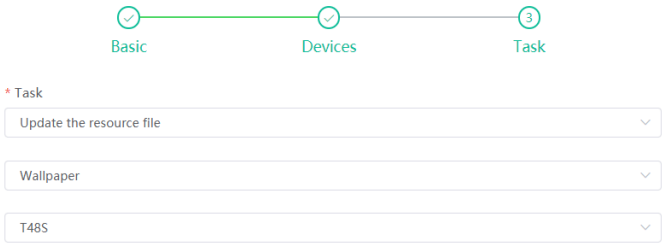
1. Click **Task Management** > **Scheduled Task** > **Add Scheduled**.
2. Set the task name, the executing type and time, then click **Next step**.



3. Select the device type and device range, then click **Next step**.



4. Select the task type and click **Finish**.



Tip: If your country supports DST, you can enable or disable DST in the field of **Time Zone**.

Note:

- If you add multiple tasks for one device, those tasks are lined up to run in order of their configured execution time.
- If the device is offline, the task will not be executed. If the device is reconnected to YMCS before the task expires, the task will be executed.

Related tasks

Editing Timer Tasks
Pausing or Resuming Timer Tasks
Ending Timer Tasks
Viewing Timer Tasks
Viewing Executed Tasks

Editing Timer Tasks

You can edit the timer tasks in the status of pending or suspending, but you cannot edit the tasks in the status of executing or finished.

Procedure

1. Click **Task Management** > **Scheduled Task**.
2. Click beside the desired task.
3. Edit and save the parameters.

Tip: If your country supports DST, you can enable or disable DST in the field of **Time Zone**.

Pausing or Resuming Timer Tasks

You can pause or resume the periodic timer tasks. After resumed, the task can still be executed according to the time.

Procedure

1. Click **Task Management** > **Scheduled Task**.
2. Click / beside the desired task to pause/resume the task.

Ending Timer Tasks

If you end the Executing timer task, the task can still be executed until it is finished. If you end the periodic timer task, they will no longer be executed.

Procedure

1. Click **Task Management** > **Scheduled Task**.
2. Click on the right side of the desired task to end the task.

Note: If you end the timer task before the task execution time (for the periodic timer task, before the first execution time), the task would not be displayed in the page of Executed Task.

Related tasks

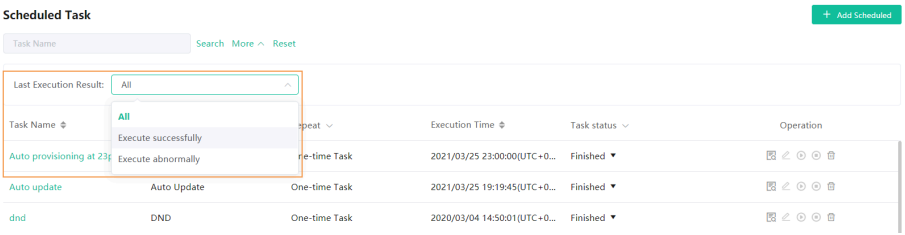
Viewing Timer Tasks
Viewing Executed Tasks

Searching for Timer Tasks

You can search for timer tasks by entering the task name or selecting the execution result.

Procedure

Click **Task Management** > **Scheduled Task**.



Results

The search results are displayed in the list.

Viewing Timer Tasks

Procedure

1. Click **Task Management** > **Scheduled Task**.

2. Click the desired task name or click beside the desired task name.

Results

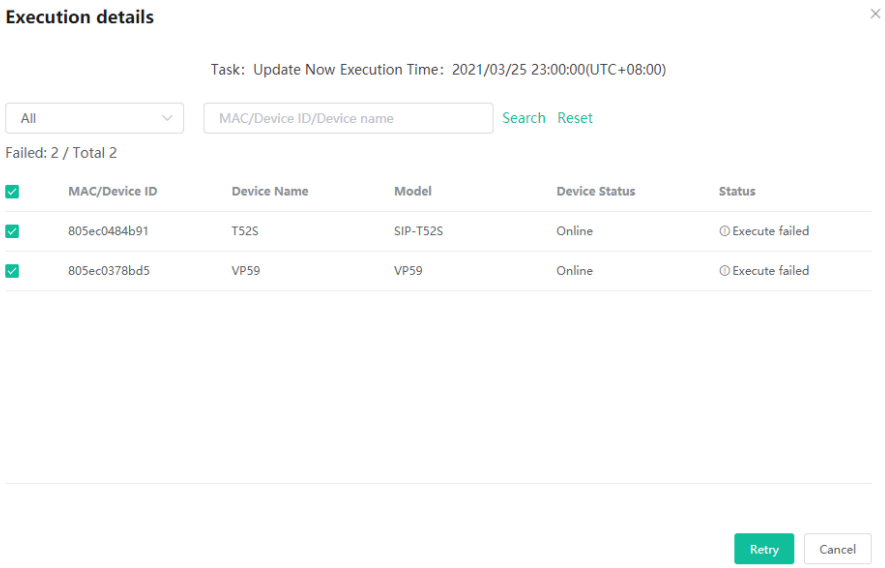
It goes to the Executed task page and you can view the execution details.

Viewing Executed Tasks

You can view the task details including the type, the time and the related device information. If the task is failed or executed exceptionally, you can check the reason or re-execute the task.

Procedure

1. Click **Task Management** > **Executed Task**.
2. Click beside the desired task name.



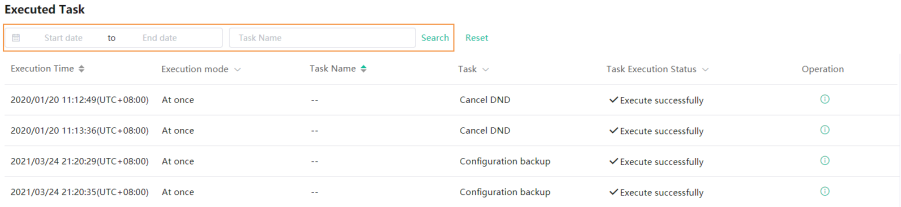
3. Optional: Select the exceptional devices, and then click **Retry** to re-execute the task.

Searching for Executed Tasks

You can search for executed tasks by directly entering the task name or selecting the start time and the end time.

Procedure

Click **Task Management** > **Executed Task**.



Results
The search results are displayed in the executed task list.

Diagnosing Devices

You can troubleshoot the device by using the log files and the captured packet and so on. Make sure that the device is connected to YMCS before you diagnose the device. You can diagnose up to 5 SIP devices at the same time. This feature is not applicable to USB devices and Room System devices.

Note: The device diagnosis is the advanced feature, not supported by the basic package. If you want to use the advanced features, you can contact your distributor/reseller to subscribe to the advanced package. You can view the details of the subscribed package on the page of Managing Orders.

Start Diagnosing

About this task

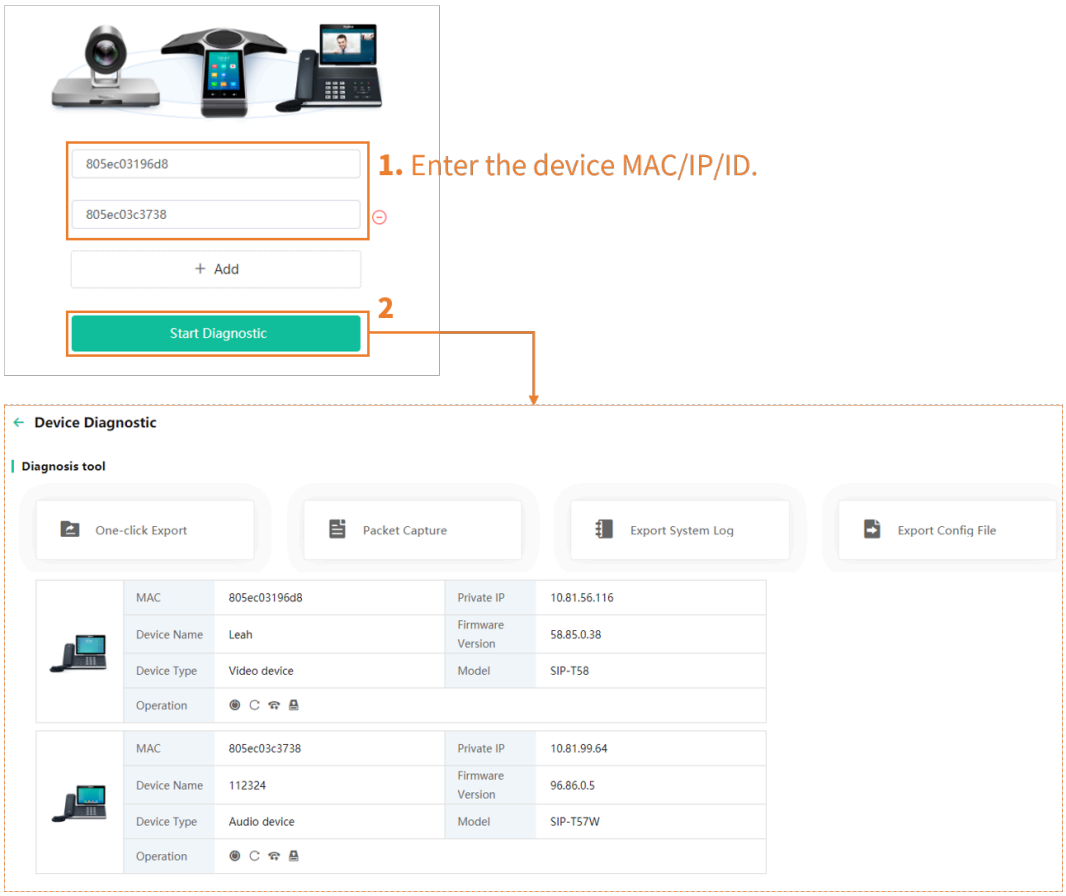
Note:

- Currently, diagnosing multiple devices only applies to phone devices. Up to 5 phone devices can be diagnosed at the same time.
- This feature is not applicable to the offline and invalid devices.
- You can diagnose the same devices at the same time except for capturing packets. The later request of capturing packets will automatically disable the former one.

Procedure

Diagnose a single/multiple devices.

Take the image of phone device as an example.



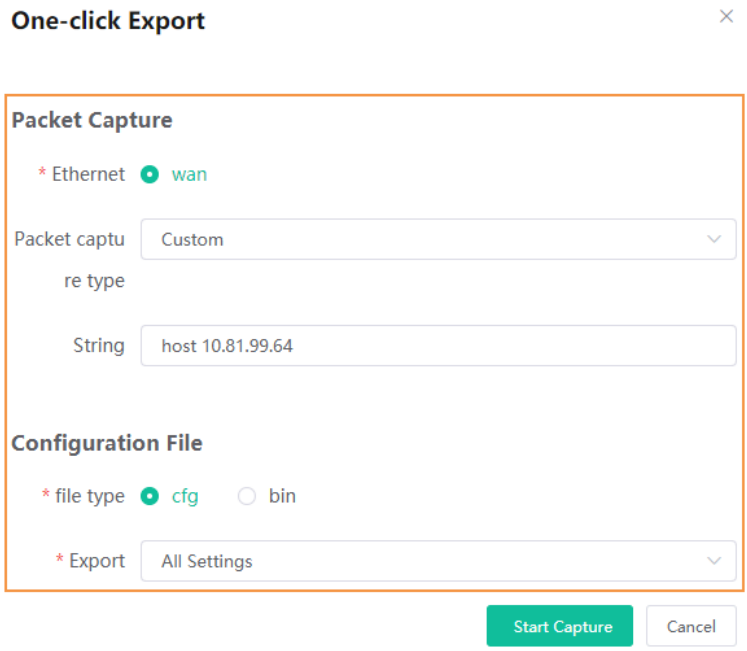
Exporting the Packets, Logs, and Configuration Files by One Click

You can use the **One-click Export** feature to export the packets, logs, and configuration files of one or multiple devices at the same time.

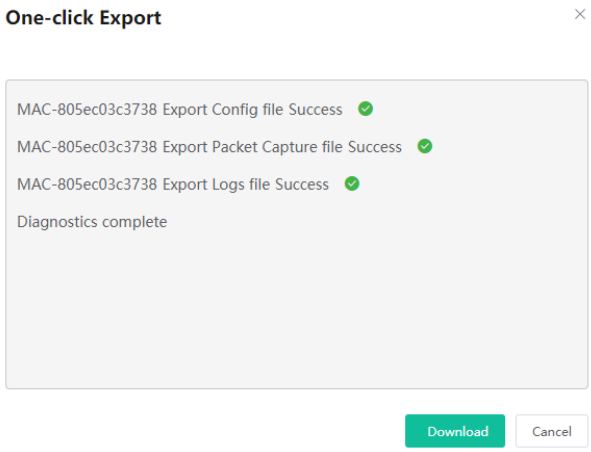
Procedure

1. On the Device Diagnostics page, click **One-click Export**.

2. Set the parameters and click **Start Capture**.



3. Reproduce the problem during the packet capturing.
4. If you finish reproducing the problem, click **End Capture** and the file is generated automatically.



5. Click **Download** to download the files to your local system.

Capturing Packets

About this task

This feature is not applicable to USB devices.

Here, we list some frequently used rules for packet capturing.

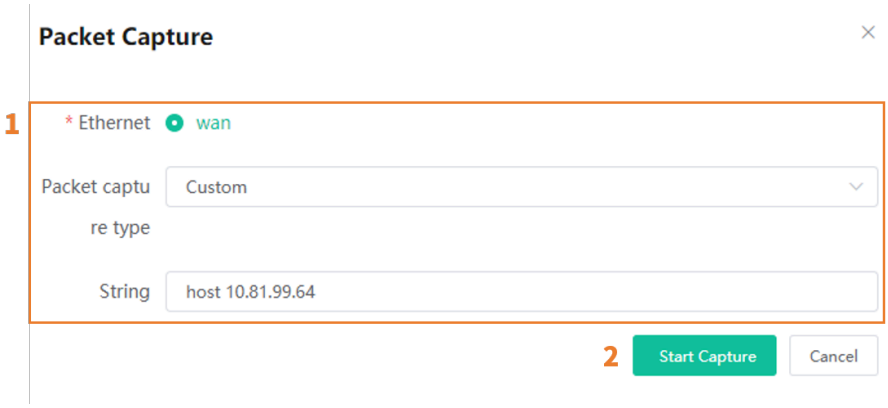
String	Example	Introduction
host IP	host 10.81.36.16	Only see the incoming and outgoing traffic of a specific IP.

String	Example	Introduction
Port number	port 90	Only see the incoming and outgoing traffic of a specific port.
Portrange value1-value2	portrange 21-23	Only see the traffic belonging to a specific port range.
tcp port 23 and host IP	tcp port 23 and host 10.81.36.16.	Check who controls the phone via telnet.
port 80	/	Check the packets of the requests received and the responses sent by your phone web user interface.
net IP/mask	net 10.91.33.0/24	Only capture the packet from the resource IP address or the destination IP address.
src	src host 10.81.36.16	Only capture the packet send by the IP 10.81.36.16.
	src port 80	Only capture the packet send by port 80.
	src portrange 21-23	Only capture the packet send by the port number from 21 to 23.
dst	dst host 10.81.36.16	Only capture the packet received by the IP 10.81.36.16.
	dst port 80	Only capture the packet received by the port number 80.
	dst portrange 21-23	Only capture the packet received by the port number from 21 to 23.
and	host 10.81.33.32 and (10.81.33.12 or 10.81.33.56)	Both of the objects before or after and. This example means that capturing the packet of IP 10.81.36.16 and IP 10.81.36.18 or 10.81.33.56.
or	(10.81.33.12 or 10.81.33.56)	Either the objects before or after or. This example means IP 10.81.36.16 or 10.81.33.56.
and !, and not	ip host 10.81.36.16 and ! 10.81.36.18, ip host 10.81.36.16 and not 10.81.36.18	Neither of them. This example means that not capturing the packet of IP 10.81.36.16 and IP 10.81.36.18.

Procedure

1. On the Device Diagnostics page, click **Packet Capture**.

2. Select the desired Ethernet and type, and then enter the string.



Note: You cannot enter the string for packet capturing unless you set the type as **Custom**. Besides, if you do not enter the string, the system will capture all the data packets.

3. Reproduce the problem during the packet capturing.
4. If you finish reproducing the problem, click **End Capture** to stop capturing, and the file is generated automatically.
5. Click **Download** to save the file to your computer.
   If it takes more than 1 hour to capture packets, the packet capturing will be automatically ended.

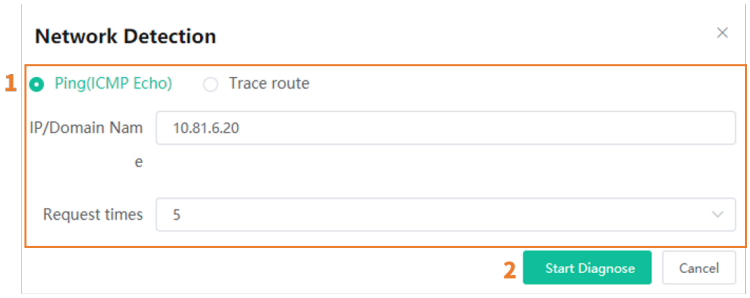
Diagnosing the Network

About this task

- This feature is not applicable to USB devices.
- Network diagnostics include: Ping (ICMP Echo) and Trace Route.
  - **Ping (ICMP Echo)**: by sending a data packet to the remote party and requesting the party to return a data packet in the same size, this method can identify whether those two devices are connected. The diagnostic results include a brief summary of the received packets, as well as the minimum, the maximum, and the average round trip times of the packets.
  - **Trace Route**: this method records the route from the local device to the remote device. If this test succeeds, you can view the network node and the time took from one node to the other, to check whether or not there is a network congestion.

Procedure

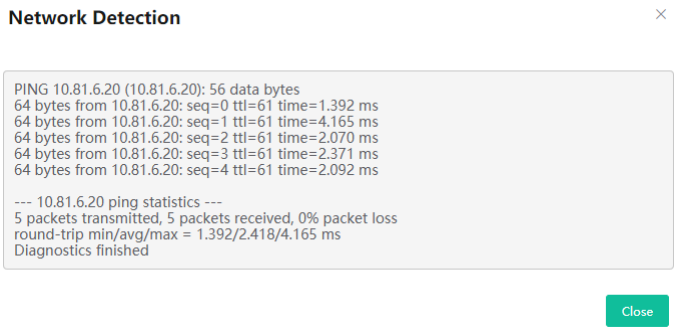
On the Device Diagnostics page, click **Network Detection**.



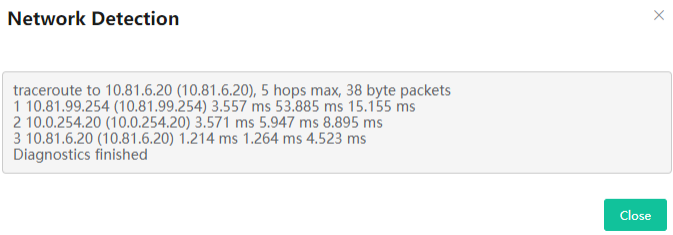
The value of IP/Domain Name is the address of YMCS by default.

Results

- If you select Ping, following is the example result



- If you select Trace Route, following is the example result



Exporting System Logs

You can export the current system logs to diagnose the device. It is not available for offline devices.

Procedure

1. On the Device Diagnostics page, click **Export System Log**.
2. Save the file to your local computer.

Exporting the Configuration Files

You can export the cfg files or the bin files. For cfg files, you can choose to export static setting files, non-static setting files or all setting files. You cannot export configuration files of the offline devices.

About this task

This feature is not applicable to USB devices.

Procedure

On the Device Diagnostics page, click **Export Config File**.

Viewing the CPU and the Memory Status

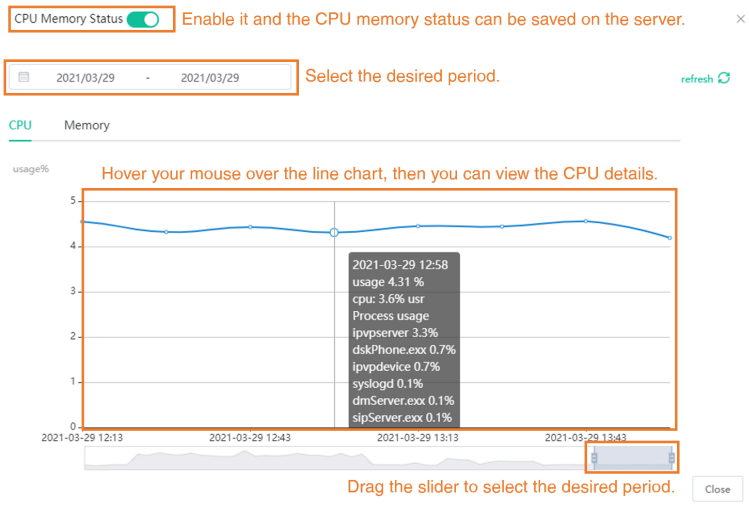
The device will regularly report its CPU and memory information to YMCS, so you can view the latest information. You can also view the memory information by copying it to Microsoft Word.

About this task

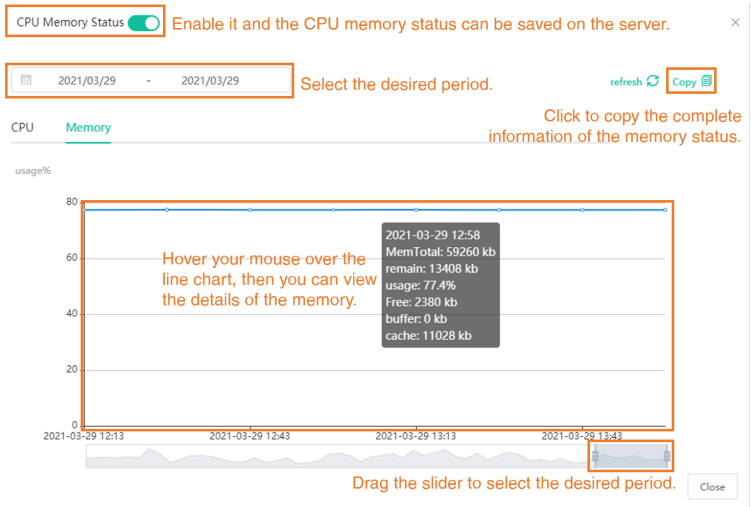
This feature is not applicable to USB devices.

Procedure

1. On the Device Diagnostics page, click **CPU Memory Status**.
2. Do one of the following:
   - Click **CPU** to view the CPU usage.



   - Click **Memory** to view the memory usage.

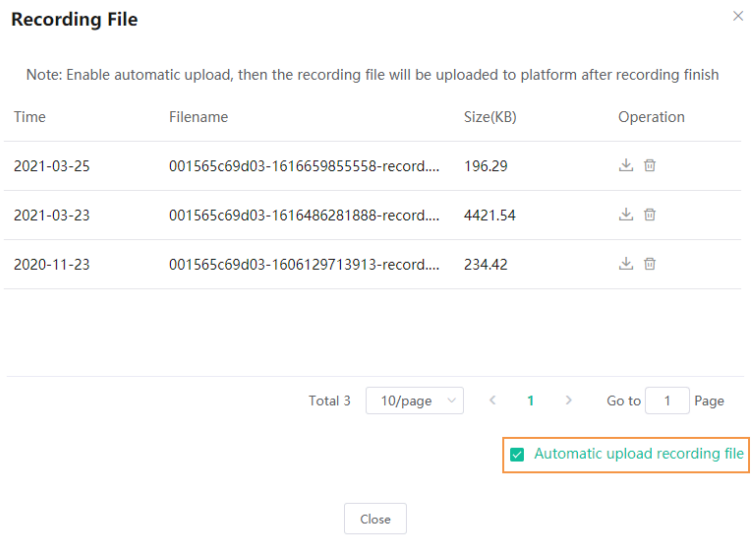


Viewing Recordings

Before you begin

- Go to Device Diagnostics page of the desire device, click **Recording File**, and select the **Automatic upload recording file** check box to enable the automatic uploading. Therefore, the recording file will be uploaded to the platform automatically.

  Note: If the device owner does not allow your request, the device would not upload the recording file.



- The device has recording files and uploads them to the platform.

About this task

This feature is not applicable to USB devices.

Procedure

On the Device Diagnostics page, click **Recording File**.

Note: You can click to download the recording file or click to delete the recording file.

Taking the Screenshot of the Device

About this task

Note:

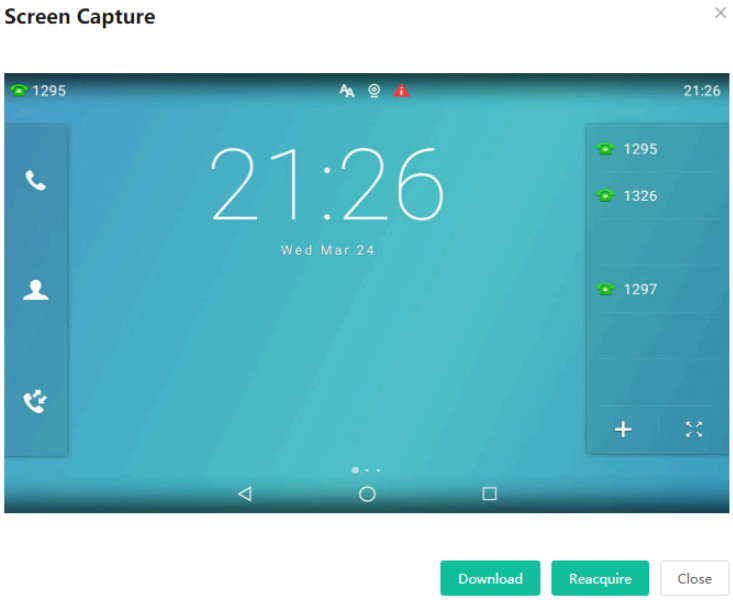
- If you want to take the screenshot of Microsoft Teams Rooms System, you should use Yealink RoomConnect in version 2.23.XX.0 (soon to be released) or later to connect the Teams Rooms System to the platform. Otherwise, you cannot use it.
- This feature is not applicable to USB devices.

Procedure

On the Device Diagnostics page, click **Screen Capture**.

Results

Note: If the device owner does not allow your request for taking screenshots of the device, you cannot take the screenshot.



Note: You can click **Reacquire** to acquire the latest screenshot.

Getting the Device Log

About this task

Note:

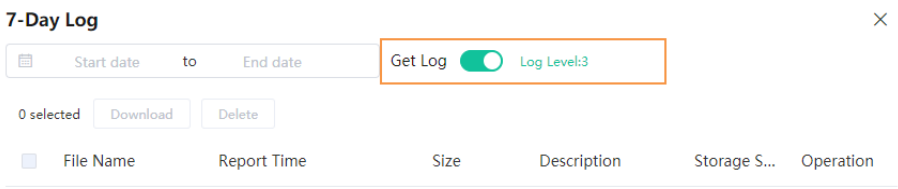
This feature is not applicable to USB devices.

If you deploy Agent and use it to connect the device to YMCS without enabling the feature of getting log, the device log will be saved to the Agent automatically.

Procedure

1. On the Device Diagnostics page, click **7-Day Log**.
2. Enable **Get Log**.

3. Click **Log Level** to set the desired log level.



When each time the size of obtained logs reaches 100M, this feature will be disabled automatically. After that, YMCS would not save the device logs any longer.

Download the Device Log

If you configure devices to report device logs to YMCS, you can download the logs saved on YMCS.

Before you begin

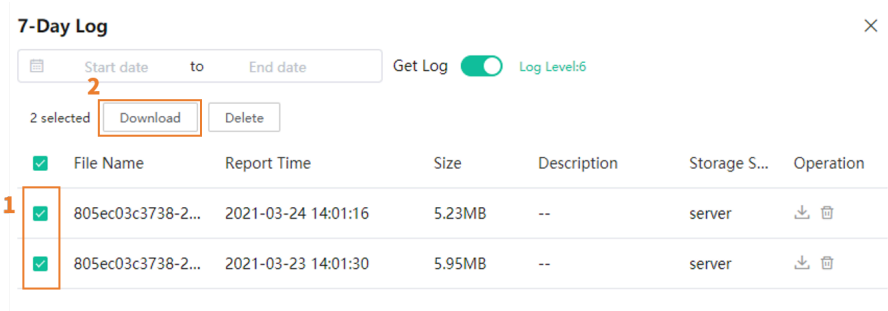
Getting the Device Log

About this task

If you do not allow the USB device to upload device log to YMCS, you cannot download their log on YMCS. For more information about setting the USB device to upload log, refer to Yealink USB Device Manager Client User Guide.

Procedure

On the Device Diagnostics page, click **7-Day Log**.



Note: You can also click to download the desired log.

Backing up Configuration Files

You can back up 5 historical configuration files at most.

About this task

This feature is not applicable to USB devices.

Procedure

1. On the Device Diagnostics page, click **Configuration Backup**.

2. Click **Backup Now**.

   The Configuration backup list displays the backup records. You can view, push, download, or delete the corresponding configuration file.

   Additionally, YMCS allows you to create a scheduled task for backing up or restoring the configuration file. For more information, refer to Adding Timer Tasks.

Managing Alarm

When the devices are abnormal, they will send alarm to YDMP-SP so that you can detect and solve problems such as network or server problems in time.

- Alarm Statistics
- Adding Alarm Strategies
- Managing Alarm Strategies
- Viewing Alarms
- Filtering the Alarms
- Exporting Alarm Records

Alarm Statistics

You can view the alarm statistics of the selected sites on the page of Alarm Statistics.

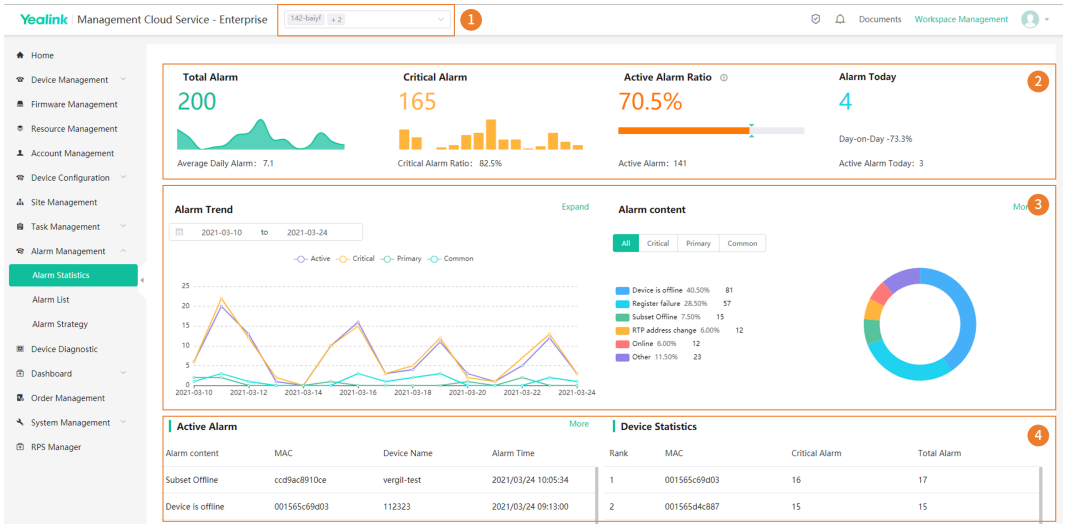


Table 3:

No.	Feature	Description
1	Select the sites.	After you select the sites, the chart displays the statistics of the selected sites. The default value is all sites. **Note:** You can only select the sites which your account has the permission to.
2	Total Alarm	This chart displays the trend of the alarms in the recent 15 days.
	Critical Alarm	This chart displays the distribution of the critical alarms in the recent 15 days.

No.	Feature	Description
	Active Alarm Ratio	1. When the ratio is below 30%, the color of the scale bar is green. 2. When the ratio is between 30% ~ 70%, the color of the scale bar is yellow. 3. When the ratio is above 70%, the color of the scale bar is red.
	Alarm Today	The number of alarms today, the ratio of the alarms compared between today and yesterday, the number of active alarms today.
3	Alarm Trend	1. The statistics of the chart can select any rage within a half year. The default value is the statistics in the recent 15 days. 2. Click  to view in a larger screen. You can use this feature to view the statistics within a longer time scale. 3. Display or hide the trend of the statistics. The default value is displaying the trend of all statistics. 4. Move your mouse to the corresponding date to display the detailed data.
	Alarm Content	This chart displays the ratio and the number of each alarm content.
4	Active Alarm	Display the content of the active alarms of devices.
	Device Statistics	1. The devices ranks based on the number of critical alarms and the total number of alarms. 2. Click Critical Alarm. The devices ranks based on the number of the critical alarms in positive or negative sequence. 3. Click Total Alarm. The devices ranks based on the number of the total alarms in positive or negative sequence.

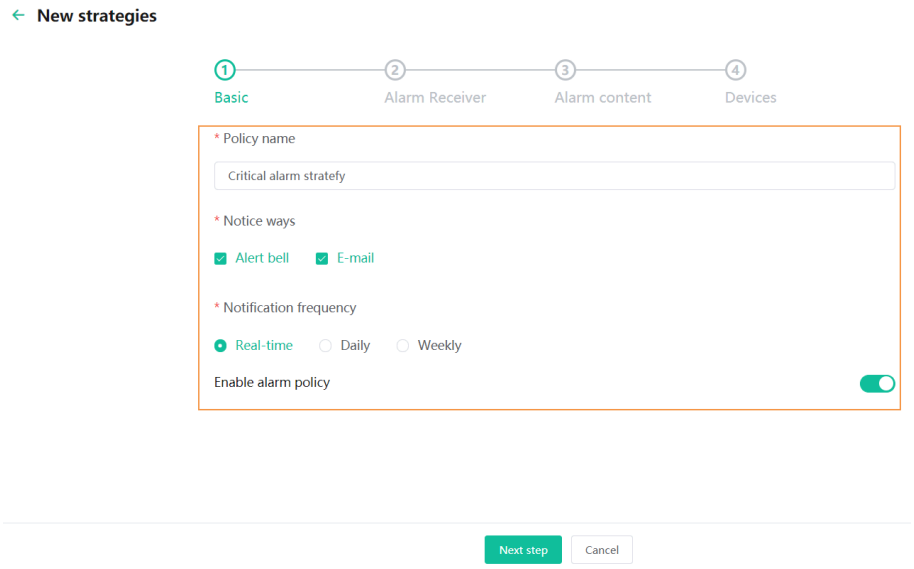
Adding Alarm Strategies

You can add alarm strategies. When there are alarms, you will receive the reminds by email or on the platform (Homepage→ the alarm icon in the top-right corner).

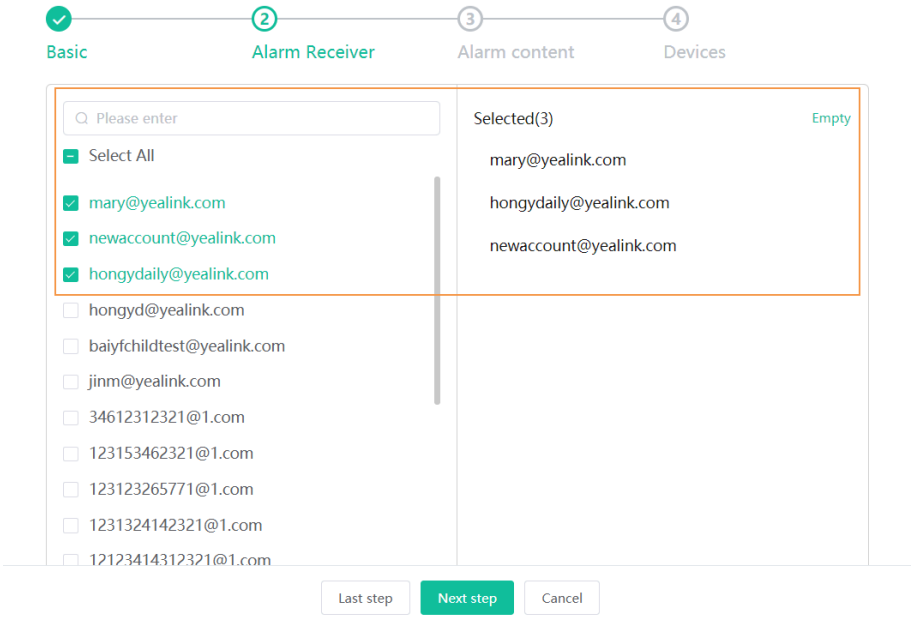
Procedure

1. Click **Alarm Management** > **Alarm Strategy** > **New strategies**.

2. Enter the corresponding information and click **Next step**.

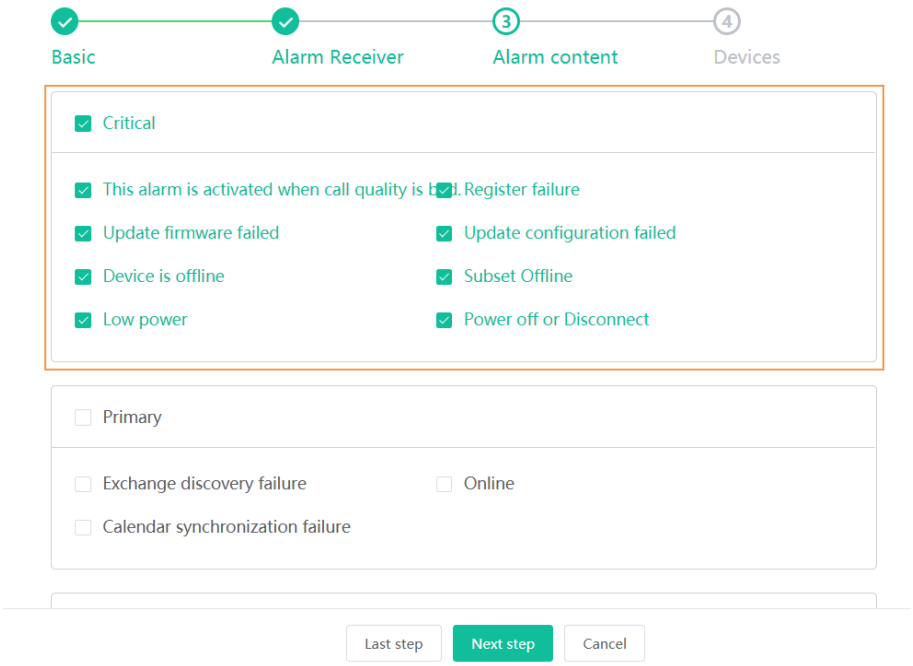


3. Select the alarm receiver and click **Next step**.

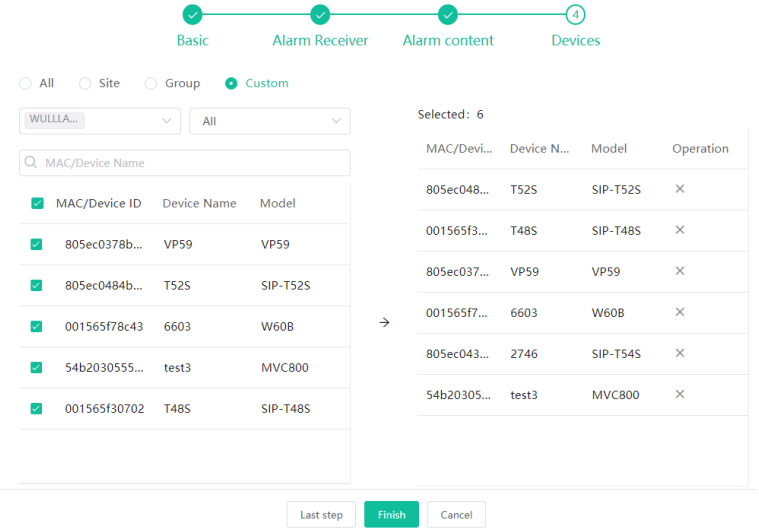


Note: If you want to add a sub-administrator as the receiver, refer to Adding and Managing Sub-Administrator Accounts.

4. Select the desired alarm level and content, and click **Next step**.



5. Select devices and click **Finish**.



6. Click **Finish**.

Managing Alarm Strategies

Procedure

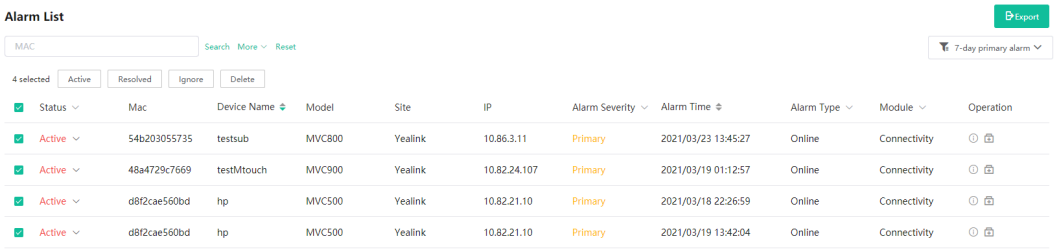
1. Click **Alarm Management** > **Alarm Strategy**.
2. Do one of the following:
   - Click  beside the desired strategy, edit the parameter and save it.
   - Select the corresponding strategy and click **Delete**.

Viewing Alarms

When a problem occurs to the device, for example the call failure or the registration failure, the problem will be reported to the server. You can quickly locate the problem by viewing the alarm details. If you have configured to receive the alarm by email, you can view the alarm in the email. Adding the alarm strategy does not affect the permission to access the alarm list.

Procedure

1. Click **Alarm Management** > **Alarm List**.



2. Optional: Do one of the following:
   - Click **Advanced Search**, select the alarm time to perform the search.
   - Click on the right side of the desired alarm to view the details.
   - Select the desired alarms, click **Resolved/Ignore/Active** to view the alarm of the selected status.
   - Click to diagnose the device and troubleshot the reason.
   - Click **Delete** to delete the alarm.

   The common alarm types are as below:

Alarm type	Severity	Device Model
Poor call quality	Critical	SIP Phones, SfB Phones, VC Room Systems
Register failure	Critical	SIP Phones, SfB Phones, VC Room Systems
Upgrade firmware failure	Critical	SIP Phones, SfB Phones, VC Room Systems, Teams Phones
Update configuration failure	Critical	SIP Phones, SfB Phones, VC Room Systems, Teams Phones
Offline	Critical	SIP Phones, SfB Phones, VC Room Systems, Teams Phones, MVC Room Systems
Associated device offline	Critical	MVC Room Systems
Wireless mic low power	Critical	MVC Room Systems
Wireless mic power off or disconnect	Critical	MVC Room Systems
Visual voicemail retrieve failure	Minor	SfB Phones
Hold failure	Minor	SIP Phones, SfB Phones
Resume failure	Minor	SIP Phones, SfB Phones

Alarm type	Severity	Device Model
RTP violate	Minor	SIP Phones, SfB Phones
RTP address change	Minor	SIP Phones, SfB Phones
RTP dead	Minor	SIP Phones, SfB Phones, VC Room Systems
SRTP failure	Minor	SIP Phones, SfB Phones
Call log retrieve failure	Minor	SfB Phones
Outlook contact retrieve failure	Minor	SfB Phones
Call failure	Minor	SIP Phones, SfB Phones, VC Room Systems
Calendar synchronization failure	Major	SfB HD IP phones
Exchange discovery failure	Major	SfB HD IP phones
Offline associated device back online	Major	MVC Room Systems

Related concepts

Managing Alarm

Filtering the Alarms

You can use the system built-in filter or customize the filters for filtering alarms.

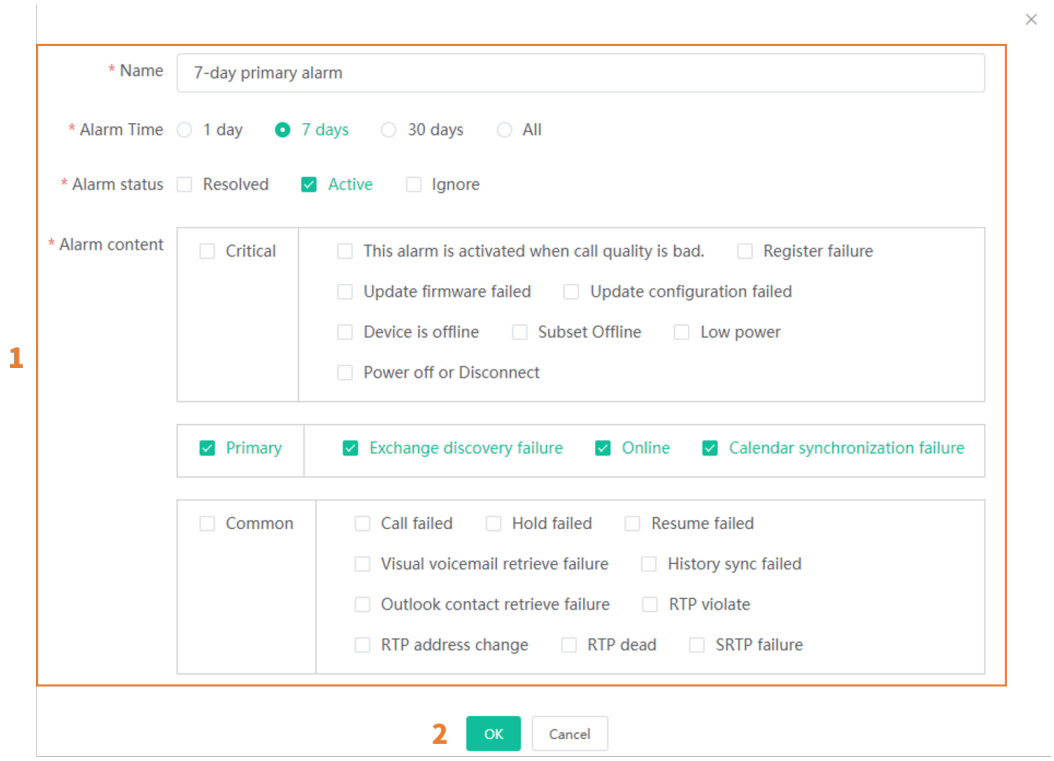
- Customizing Filters
- Filtering the Alarms

Customizing Filters

Procedure

1. Click **Alarm Management→ Alarm List**.
2. Click  in the top-right corner of the page, and select **Filter management**.

3. Click **Add filter**, enter the corresponding information, and click **OK**.



Filtering the Alarms

Procedure

1. Click **Alarm Management→ Alarm List**.
2. Click and select the desired filter to view the corresponding alarms.

Exporting Alarm Records

You can export the alarm records on the current page as Excel files.

Procedure

1. Click **Alarm Management→ Alarm List**.
2. Optional: Click in the top-right corner of the page to filter the desired alarm records.
3. Click **Export** to export the alarm records.

Viewing Call Quality Statistics

You can view the call quality and the session distribution on the Call statistics page. You can also view the details of the call quality, including the user information, the basic device information and the call-related information.

Note: The Teams phone does not support reporting the call statistics, so you are not available to view the call quality of the Teams phone.

The call quality is advanced feature, not supported by the basic package. If you want to use the advanced features, you can contact your distributor/reseller to subscribe to the advanced package. You can view the details of the subscribed package on the page of Managing Orders.

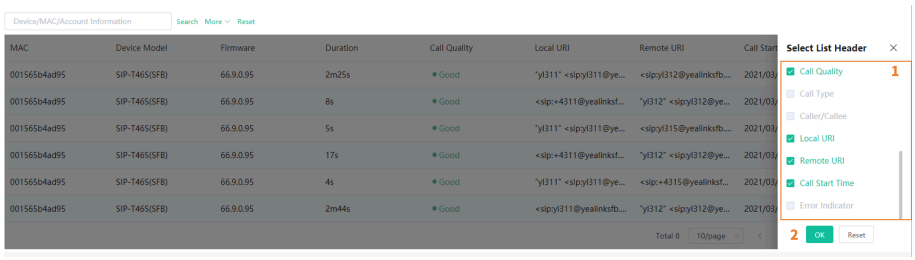
- Customizing the Indicators of Call Quality Detail
- Viewing the Call Data

Customizing the Indicators of Call Quality Detail

The device name, the model, the firmware, the caller/callee, the call type and the quality are displayed by default in the Call Quality Detail module, and you can customize up to 6 indicators expect for the MAC address.

Procedure

Click **Dashboard** > **Call Statistics** > .



Results

The selected indicators are shown in the list of call quality detail.

Viewing the Call Data

Procedure

1. Click **Dashboard** > **Call Statistics**.

2. Click beside the desired call to view the detailed call quality.

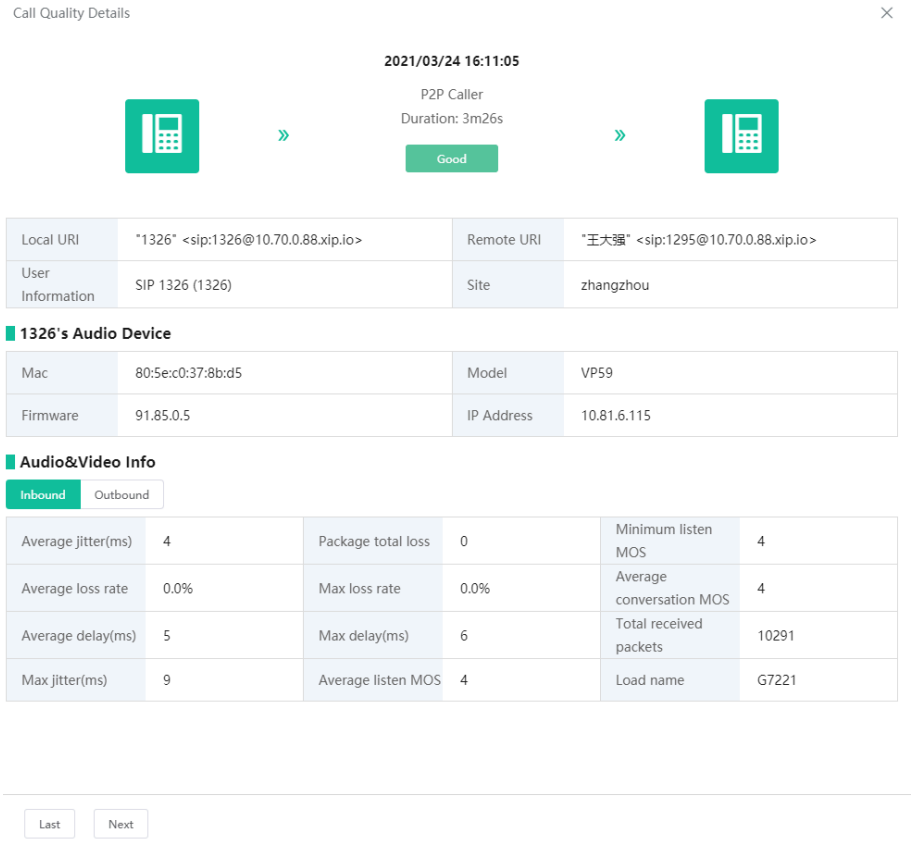


Table 4: Metrics of Call Data

Metrics	Description
Average jitter (ms)	The average jitter of the network delay
Package total loss	The amount of packet loss during a call
Minimum listen MOS	The minimum listen MOS value during a call, based on PESQ model. Its values can range from a low of 0.0 to a high of 5.0. Higher value indicates better call quality.
Max jitter (ms)	The maximum jitter, reflecting the degree of network delay
Average delay (ms)	The average value of network delay, reflecting the quality of the network
Average conversation MOS	The average conversation MOS value during a call, based on PESQ model. Its values can range from a low of 0.0 to a high of 5.0. Higher value indicates better call quality. The influence of hardware equipment on the audio is not considered.
Average loss rate	The average rate of packet loss during a call
Max delay (ms)	The maximum value of network delay, reflecting the quality of the network
Total received packets	The amount of received packets during a call
Max loss rate	The maximum rate of packet loss during a call

Metrics	Description
Average listen MOS	The average listen MOS value during a call, based on PESQ model. Its values can range from a low of 0.0 to a high of 5.0. Higher value indicates better call quality

Table 5: Evaluation Metrics of Call quality

Call quality	Metrics
Excellent (all metrics should be satisfied)	Delay: the average call delay should be less than or equal to 200 ms
	Packet loss: the average rate of packet loss should be less than or equal to 2%
	Jitter: The average call jitter should be less than or equal to 15 ms
Good (one of the following metrics should be satisfied)	Delay: the average call delay is more than 500 ms
	Packet loss: the average rate of packet loss is more than 2%
	Jitter: the average call jitter is more than 30 ms
Poor	Other situations

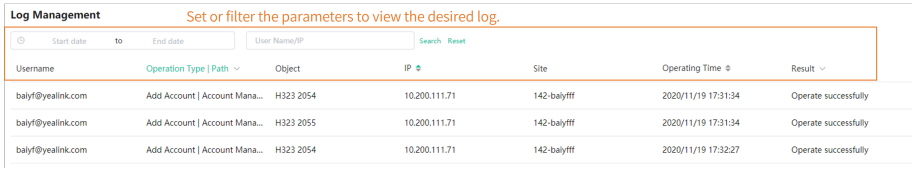
System Management

Viewing Operation Logs

Any operations performed by the administrator, the sub-administrator , or the superior channel on the YMCS are recorded as the operation logs. You can view the operation log.

Procedure

Click **System Management** > **Log Management**.



Obtaining the Accesskey

YMCS allows the third parties to call the API to integrate with their own system. Before calling the API, you need apply for the AccessKey for user authentication. For more information, refer to API for Yealink Management Cloud Service Platform.

Procedure

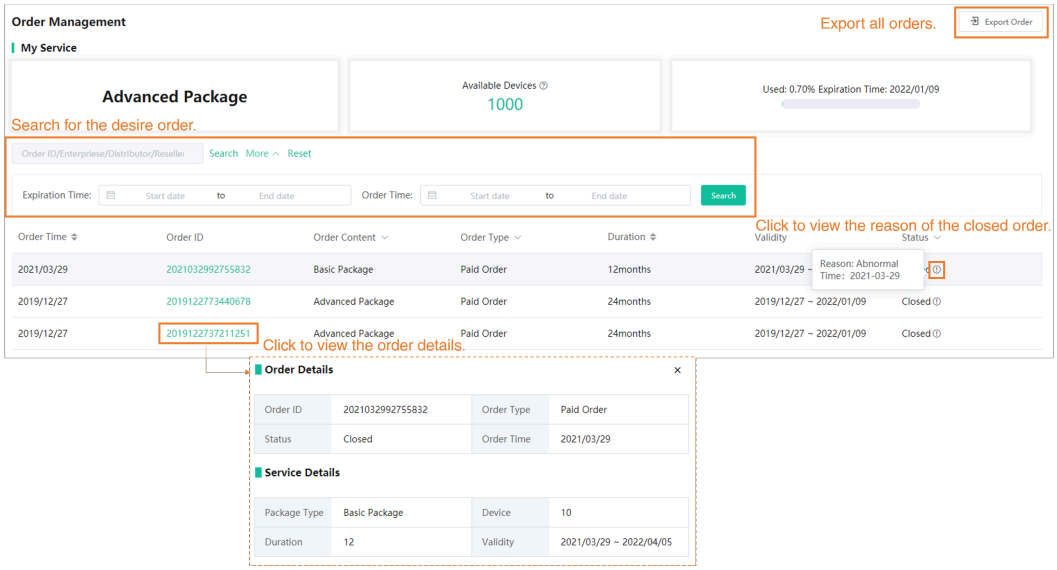
1. Click **System Management** > **API Service** .
2. If you want to call the interface of the alarm and the device diagnosis, enter the callback address.
3. Click **Acquire**, and then AccessKey ID and the AccessKey Secret will be generated by automatically.

Managing Orders

You can view the information of the basic package, including the package type, the amount of manageable devices for all placed orders, and the details of all orders. All orders in service can be superimposed during the validity. If an order is about to expire, you need to purchase the service from your distributor or reseller to continue using the service. When the order is closed, cancelled or expired, you can view the notifications of your order status on YMCS.

Procedure

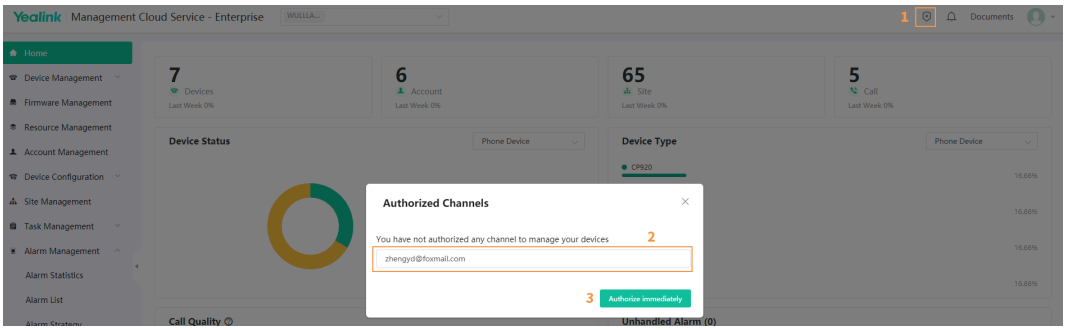
Click **Order Management**.



Authorizing/Un-authorizing the Management to the Channel

- **Authorizing**

  1. Click in the menu bar.
  2. Enter the email address of the channel account and click **Authorize immediately**.

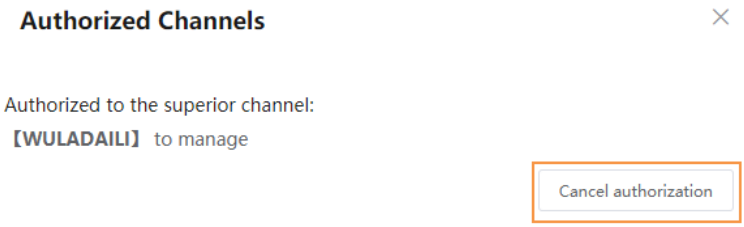


  3. Click **OK** in the pop-up window.

     Result: The icon changes from into .

- **Un-authorizing**

  1. Click in the menu bar.
  2. Click **Cancel authorization** in the pop-up window.



  3. Click **OK** in the pop-up window.

     Result: The icon changes from into .

Managing RPS

- Instruction for Old RPS Users
- Instructions for Users without RPS Account
- Binding RPS Accounts
- Synchronizing Devices
- Managing Devices
- Managing Servers

Instruction for Old RPS Users

For users who already have the RPS accounts, you can do the following two steps to migrate the data on the RPS device management platform to YMCS. After that, you can manage the device and use the RPS features on YMCS.

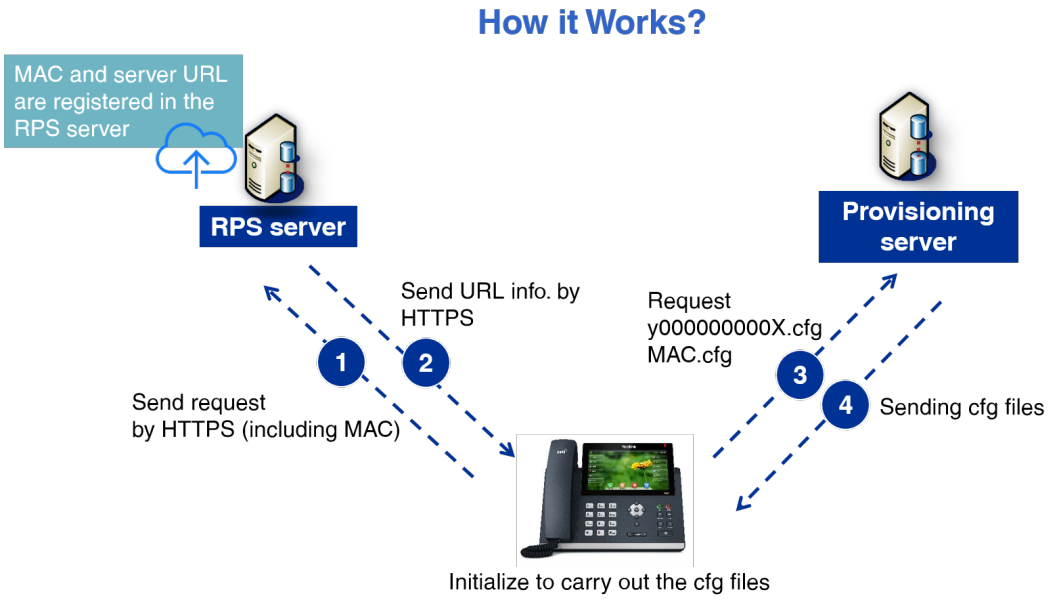
1. Binding RPS Accounts
2. Synchronizing Devices

Instructions for Users without RPS Account

If you do not have any RPS account, you can follow the step below to connect your device to YMCS via RPS server.

1. Adding Servers
2. Adding Devices
3. Initialize the device then the device will redirect to the RPS server.

   Generally, initializing refers to resetting the device to factory settings or when using a brand-new device.



- Adding Servers
- Adding Devices

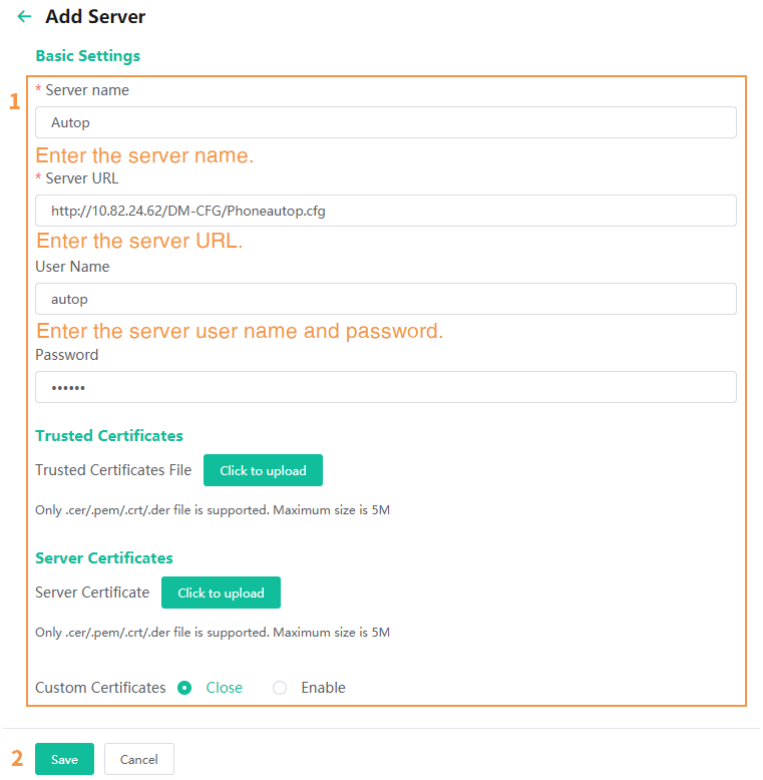
Adding Servers

If you want to save your configuration file on use your own server, you can add a server.

Procedure

1. Click **RPS Manager** > **Server Management** > **Add Server**.

2. Set and save the parameters.



Note:

- If the device needs to verify the server and requires a custom certificate, upload the trusted certificate.
- If the server needs to verify the device and requires a custom certificate, upload the server certificate.
- If the server requires the device to upload its custom certificate, enable **Custom Certificates**. It is disabled by default and the device will send the default certificate to the server for verification.

Adding Devices

When adding a device, if you select an added server and enter a unique server URL which is different from the URL of the added server, the RPS management platform performs the redirection according to the unique URL you entered. Otherwise, the platform performs the redirection according to the URL of the added server.

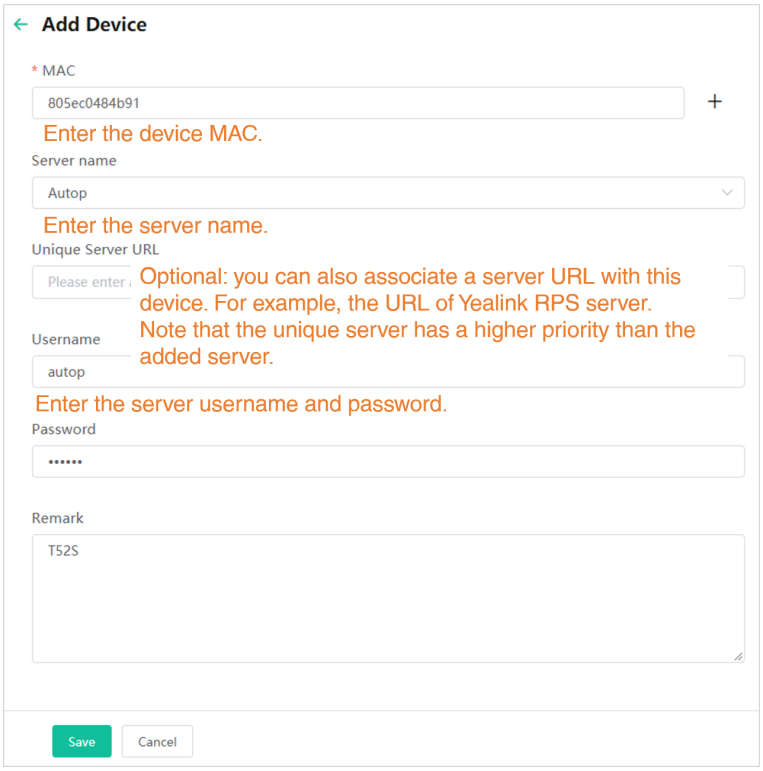
Before you begin

Binding RPS Accounts

Procedure

1. Click **RPS Manager** > **RPS Device** > **Add**.

2. Set and save the parameters.



If it prompts that other enterprises use the MAC address you entered, check your MAC address or file an appeal to Yealink if necessary.

Binding RPS Accounts

If you bind an RPS account, you can see the devices on the RPS device management platform, and manage those devices through YMCS.

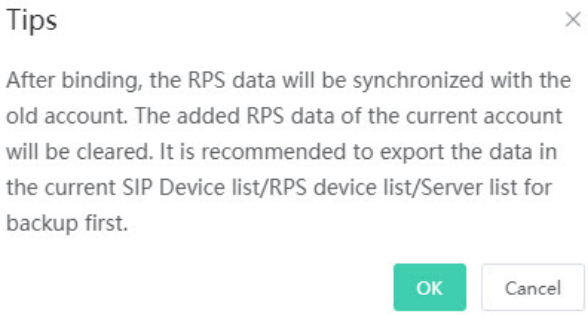
Before you begin

- You already have an RPS account.
- After you bind an RPS account, the existing RPS data of your account will be deleted. Therefore, we recommend that you export the data to make a backup.

Procedure

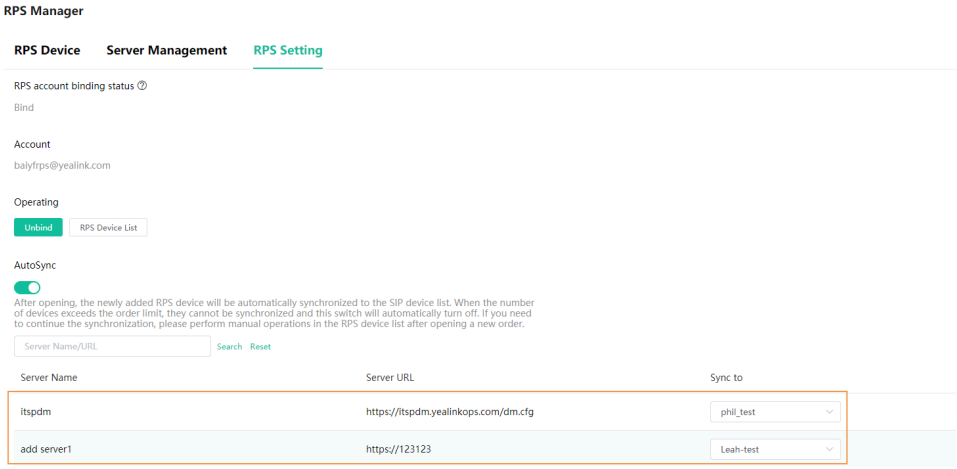
1. Click **RPS Manager** > **RPS Setting**.
2. Click **Bind**.

3. If your account does not have any existing data, click **OK**. If your account does have, you can make a backup first, and click **OK**. Otherwise, the data will be deleted.



4. Enter the user name and the password of the existing RPS account and click **OK**.

5. Optional: Enable **Auto Sync** and select the desired site for each RPS server for synchronizing devices from the server to the selected site.



Results

If you succeed in binding an RPS account, click **View device**, and you can view the synchronized devices.

Note: If you unbind the RPS account, the data on the pages of RPS Device and RPS Server will be removed.

Synchronizing Devices

If you want to use the feature of Managing Devices, you can synchronize the devices in the RPS Device List to the SIP Device List. In addition, you can select the desired site when synchronization.

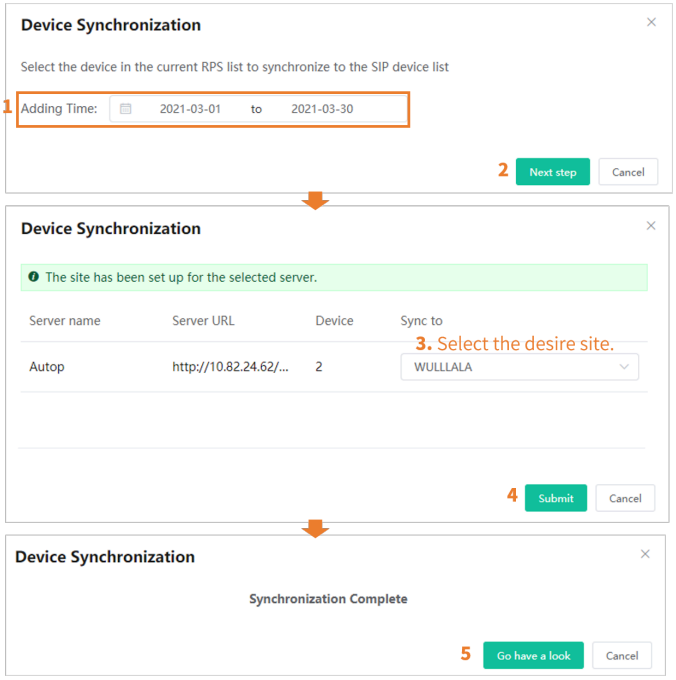
Before you begin

The RPS server has unsynchronized devices.

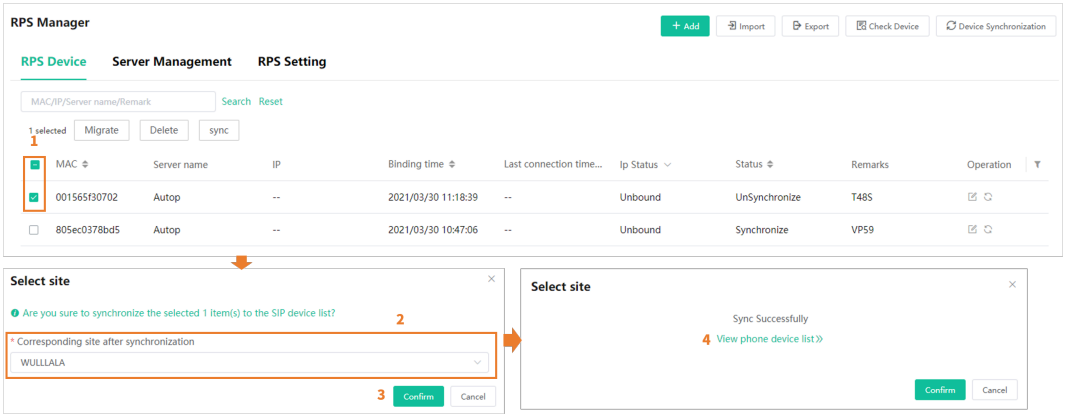
Procedure

1. Click **RPS Manager** > **RPS Device**.

2. Do one of the following:
   - Click **Device Sync** and do the following.

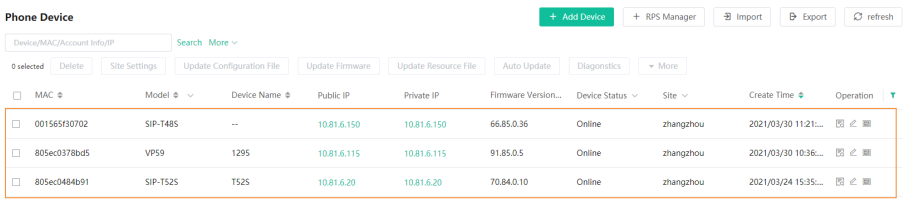


   - Select the desired unsynchronized device, click **Sync**.



Results

You can see the synchronized device on the device list.



Managing Devices

Importing Devices

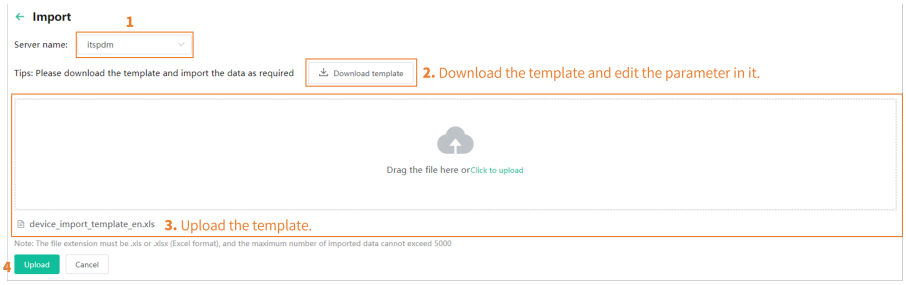
If you want to quickly add multiple devices, you can import them in batch. You need to download the template, edit the information in the template and then import the template to YMCS.

Before you begin

Binding RPS Accounts

Procedure

Click **RPS Manager** > **RPS Device** > **Import**.



Exporting Devices

You can export a batch of the device information to check the device backup information, or whether the device is sold and so on. If the device is linked to a server, it means the device is sold, otherwise it is not.

Procedure

1. Click **RPS Manager** > **RPS Device**.
2. In the top-right corner, click **Export**. The file will be saved in your local system.

Editing the Device Information

You can edit the device information, for example, the server or the unique server URL.

Procedure

1. Click **RPS Manager** > **RPS Device**.
2. Click beside the desired device.
3. Edit and save the parameters.

Migrating Devices to Another Server

You can migrate a single device or multiple devices to another server at once.

Procedure

1. Click **RPS Manager** > **RPS Device**.
2. Select the check boxes of the desired devices.
3. Click **Migrate**.
4. Select the targeted server.
5. Click **Confirm**.

Checking the Linking Status Between the Device and the Server

About this task

You can check the device linking status, which contains the following:

- Bound: the device MAC address belongs to your enterprise and is linked to the server successfully.
- Unbound: the device MAC address belongs to your enterprise but is not linked to the server.
- The device MAC address belongs to other enterprises.
- The query fails: the device does not exist or cannot be found on YMCS.

Procedure

1. Click **RPS Manager** > **RPS Device** > **Check Device**.
2. Enter the device MAC and click **Confirm**.

Results

It shows the result of the device linking status.

If it prompts that other enterprises use the MAC address you entered, check your MAC address or file an appeal to Yealink(https://ticket.yealink.com/) if necessary.

Deleting Devices

Procedure

1. Click **RPS Manager** > **RPS Device**.
2. Select the desired devices.
3. Click **Delete**.
4. Click **OK** according to the prompts.

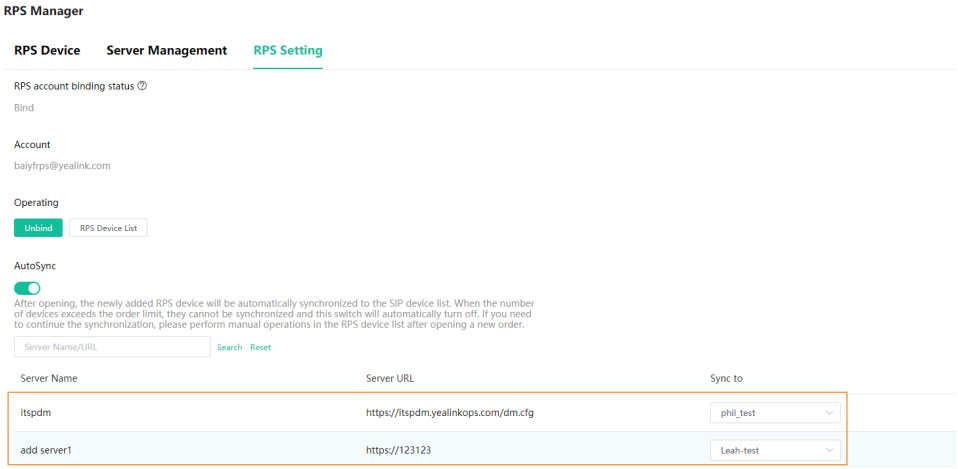
Enabling Automatic Synchronization

After associated with a RPS account, YMCS can automatically synchronize the newly added devices in the RPS Device List to the SIP Device List.

Procedure

1. Click **RPS Manager** > **RPS Setting**.
2. Enable **AutoSync**.

3. Optional: Select the desired site for each RPS server for synchronizing devices from the server to the selected site.



Managing Servers

Editing Servers

Procedure

1. Click **RPS Manager** > **Server Management**.
2. Click beside the desired server.
3. Edit and save the parameters.

Searching for Servers

You can search for the server by entering the server name or the URL.

Procedure

1. Click **RPS Manager** > **Server Management**.
2. Enter the server name or the URL in the search box.
3. Click **Search**.
   The search results are displayed in the server list.

Deleting Servers

Procedure

1. Click **RPS Manager** > **Server Management**.
2. Select the check boxes of the desired servers and click **Delete**.
3. Click **OK** according to the prompts.

Managing Administrator Accounts

This chapter allows the administrator to view, add, edit sub-administrator accounts, and manage role privileges. The administrator also can edit his account information. By default, the administrator has all privileges and can assign different role privileges for sub-administrator accounts.

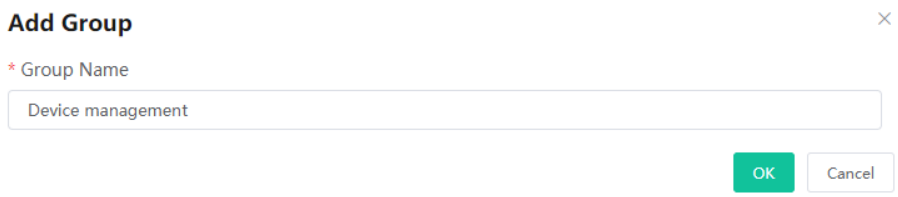
Adding and Managing Groups

You can manage the roles by the group.

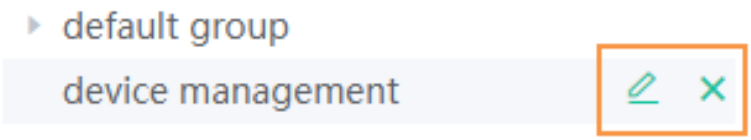
About this task
You cannot edit or delete the default group.

Procedure

Click **System Management** > **Role Management** > **Add Group**.



After adding the group, click the edit icon or the delete icon on the right side to edit or delete the group.



Adding and Managing Roles

You can customize roles first, configure the corresponding function permission for the roles, and then assign roles to the sub-administrator accounts.

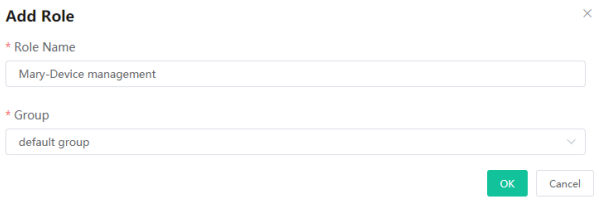
About this task
The default roles are as below, you cannot edit or delete them.

Table 6: Default role

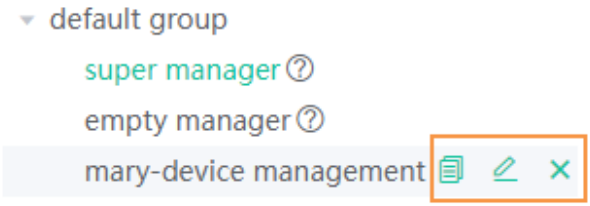
Name	Group	Function and data permission
Super manager	Default role group	All function and data permission
Empty manager	Default role group	Only the permission of logging in.

Procedure

Click **System Management** > **Role Management** > **Add Role**.



After adding the role, click the corresponding icon on the right side of the desired role to copy, edit, or delete the role.



You can also click **Add sub account** to add sub administrator for this role.

Assigning the Function Permission

If you want to allow non-managers to use the sub-administrator account, for example, checking the call quality of the phone and diagnosing the devices, but you do not want them to add or delete devices, you can assign the limited function permission to them.

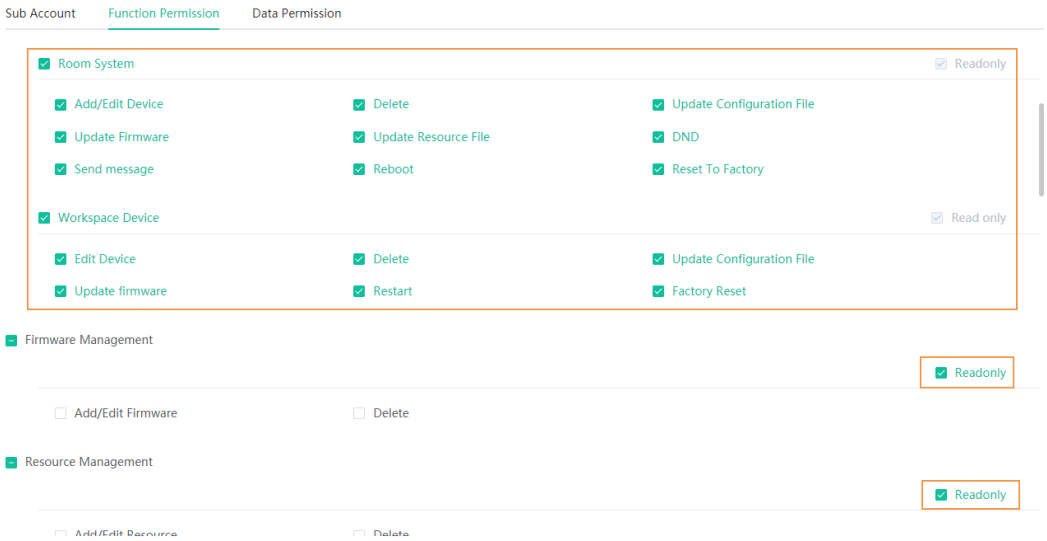
Before you begin

You have added roles, refer to Adding and Managing Roles.

Procedure

1. Click **System Management** > **Role Management**.
2. Select the corresponding role and click **Function Permission**.

3. If you only want to grant the Readonly permission, select the check boxes of **Readonly** on the right side of the corresponding functions. Otherwise, select the check boxes of the corresponding operations.



Assigning the Data Permission

If you want to manage the device of your own site or of a certain amount sites, you can assign the data permission.

Before you begin

Add roles, refer to Adding and Managing Roles.

Procedure

1. Click **System Management** > **Role Management**.
2. Select the corresponding role and click **Data Permission**.
3. Select the check box of the site you want to manage.
   - ☐ If you have assigned the function permission to the sub-administrator (Assigning the Function Permission), the sub-administrator can only view/use the firmware, resources, accounts, and configuration of this site, but cannot modify/delete them.
   - ☑ If you have assigned the function permission to the sub-administrator (Assigning the Function Permission), the sub-administrator can view/use/modify/delete the firmware, resources, accounts, and configuration of this site.

Related tasks

Adding Sites
Adding Accounts
Adding Firmware
Adding Resource Files
Adding Configuration Templates

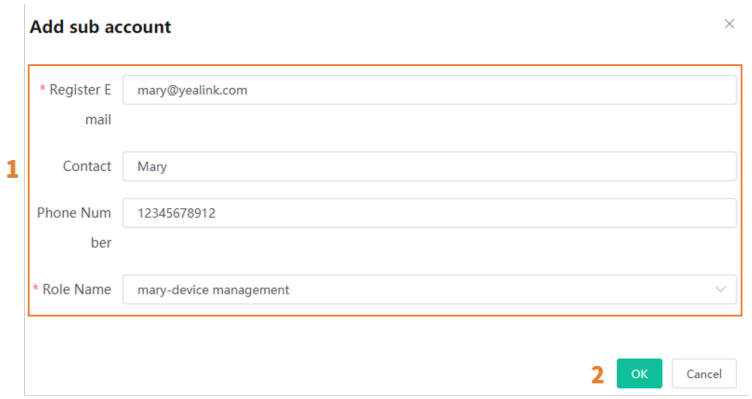
Adding and Managing Sub-Administrator Accounts

Before you begin

You have added roles, refer to Adding and Managing Roles.

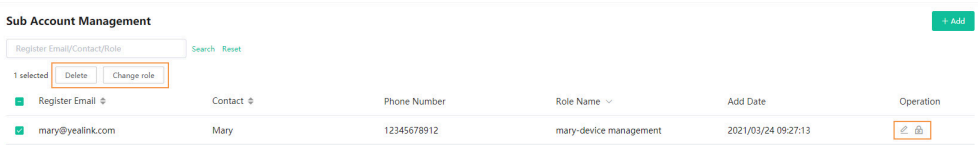
Procedure

Click **System Management** > **Sub Account Management** > **Add**.



Note:

After adding the sub-administrator account, you can change the role, reset the password or do other operations.



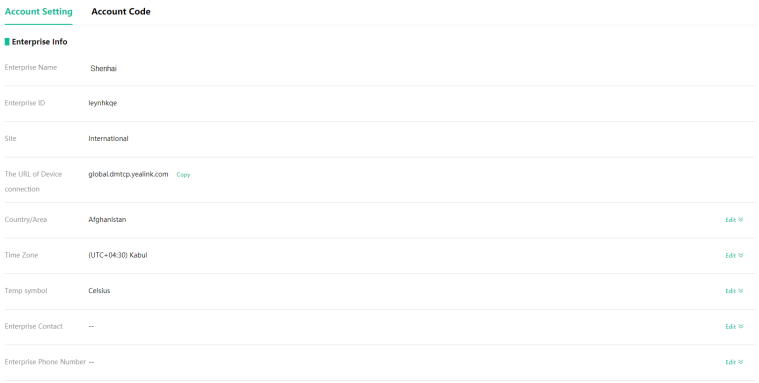
Editing the Account Information

You can edit the account information.

Procedure

1. Hover your mouse over the account avatar in the top-right corner, and then click **Account Settings**.

2. Edit and save the related information.



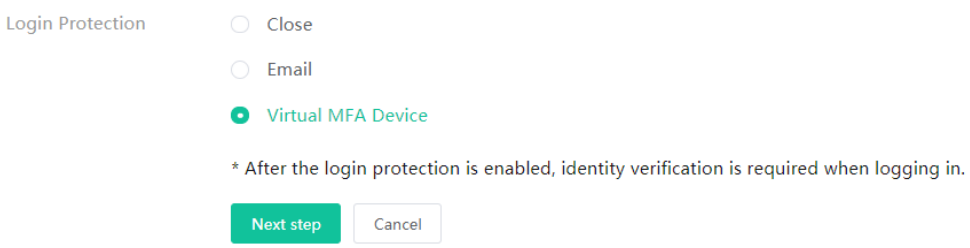
Parameter	Introduction
Password	The password of this account. Click **Edit** to change the password according to the prompt. For account security, we recommend that you change the password regularly.
Email	The mailbox is used to receive alarms and the account information. If you need to change your registered email, contact your superior channel.
Country/Area	You can change your current country/area to other countries/areas under the same site, for example in the international site. However, changing countries over two different site are not allowed.
The URL of Device connection	When you manage devices among different sites, you can configure this URL in the device to make the devices connected to the site.
Login Protection	When logging into YMCS, support using multi-factor authentication (MFA) or email for identity authentication. For more information, refer to Enabling Login Protection.

Enabling Login Protection

For single factor authentication, the passwords are easily cracked by brute force. To solve that, YMCS supports multi-factor authentication (MFA), requiring users to pass two authentications before they can log into YMCS.

Procedure

1. Hover your mouse over the account avatar in the top-right corner of the page, and then click **Account Settings**.
2. In the **Login Protection** field, click **Edit**.



3. Select **Virtual MFA Device** or **Email**, complete the operation according to the on-screen prompts.

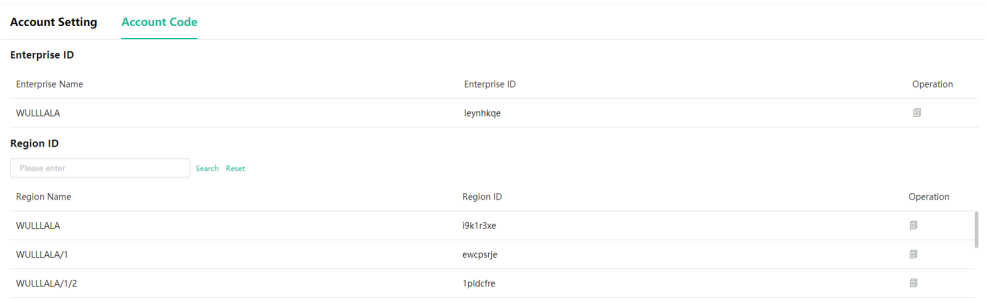
   If the page prompts “Login expired, please log in again", you need to use the new verification method to complete the login.

Viewing the Account Code

The account code is the enterprise ID and the site ID. You can put the account code into the Common.cfg file and push the file to the device, to make the device automatically connected to the corresponding site under the desired enterprise. For more information, refer to Configuring the Common.cfg File.

Procedure

1. Hover your mouse over the account avatar in the top-right corner of the page, and then click **Account Settings**.
2. Click **Account Code**.



Troubleshooting

This chapter provides you with general information for troubleshooting some common problems while using YMCS. Upon encountering a case not listed in this section, contact your Yealink reseller or technical support engineer for further support.

Forget the Login Password?

If you forget the password, you can reset it via email.

Procedure

1. On the Login page, click **Forget Password**.
2. Enter the email and the verification code in the corresponding fields.
3. Click **OK**.
4. Click **OK** according to the prompts.
5. Log into your email, click the resetting link, and rest the password according to the prompts.

The Devices Cannot Connect to YMCS

- Make sure the firmware version of the device supports YMCS. If the firmware version does not support, refer to Supported Device Models to upgrade the firmware first.
- Make sure you connect to the address https://dm.yealink.com/dm.cfg.

The Offline Device Reconnects to the YMCS

Reasons that the device is offline are as below:

- The device is disconnected from the network.
- The device is powered off.
- The device is reset to the factory and disconnected from YMCS.

Reconnect to YMCS:

- If the device has been reported to YMCS, the device will be automatically connected to it after being powered on or connected to the network.
- If the device has not been reported to YMCS, you need to deploy the device first. For more information on how to deploy the devices, refer to Connecting Phone Devices and Room Systems (Except for MVC/ZVC).