Yealink Device Management Platform Administrator Guide V3.6.0.20

Contents

About This Guide 7
Related Documentations 7

Summary of Changes 7
Changes for Release 36, Guide Version V3.6.0.20 7
Changes for Release 36, Guide Version V3.6.0.10 8
Changes for Release 36, Guide Version V3.6.0.1 8
Changes for Release 35, Guide Version V3.5.0.21 8
Changes for Release 35, Guide Version V3.5.0.20 8
Changes for Release 35, Guide Version V3.5.0.11 9
Changes for Release 35, Guide Version V3.5.0.10 9
Changes for Release 35, Guide Version V3.5.0.1 9
Changes for Release 34, Guide Version V3.4.0.10 9

Introduction of Yealink Device Management Platform 10
Browser Requirements 10
Supported Device Models 10
Port Requirements 11

Deploying YDMP 12
Hardware and Software Requirements 12
Updating YDMP (from V2.0 to V3.1) 13
Restoring YDMP (from V3.1 to V2.0) 13
Installing YDMP 3.X (3.5.0.11 or Earlier Versions) 14
Installing YDMP 3.X (3.5.0.20 or later Versions) 15
Downloading the Installation Package 15
Closing the Firewall Came with the Linux System 16
Unzipping the Installation Package 16
Installing YDMP 16
Importing the HTTPS Certificate 18
Updating YDMP (from V3.1 to V3.X) 19
Installing the Diagnostic Script 20
Activating the License 21
Importing the Device Certificate 21
Activating the License Online 22
Activating the License Offline 22
Updating the Configuration 23
Uninstalling YDMP 23

Getting Started 23
Logging in to YDMP 23
Home Page 24
Logging out of YDMP 25

Connecting to YDMP.....25
Connecting SIP Device.....26
Using Certificates for Mutual TLS Authentication.....26
Configuring the Common.cfg File.....27
Deploying Devices on the RPS (Redirection & Provisioning Server) Management Platform...28
Configuring the Server Address.....28
Connecting USB Devices.....28
Connecting Room System.....29

Managing Devices.....29
Device Status.....29
Running State Page.....30
Managing SIP Devices.....30
Editing the Device Information.....31
Exporting the Device Information.....31
Viewing the Information of SIP Device.....31
Searching for Devices.....32
Assigning Accounts to Devices.....32
Setting the Sites.....33
Pushing Configuration Files to Devices.....34
Pushing Firmware to Devices.....34
Pushing Resource Files to Devices.....35
Diagnosing Devices.....36
Enabling/Disabling DND.....37
Sending Messages to Devices.....38
Rebooting Devices.....38
Resetting the Devices to Factory.....39
Deleting Devices.....40
Managing USB Devices.....40
Editing the Device Information.....40
Exporting the Device Information.....41
Viewing the USB Device.....41
Searching for Devices.....41
Setting the Sites.....42
Deleting Devices.....42
Managing Room System.....42
Editing the Device Information.....43
Viewing the Information of the Room System.....43
Searching for Devices.....44
Setting the Sites.....44
Rebooting Devices.....45
Pushing Firmware to Devices.....45
Resetting the Devices to Factory.....46
Deleting Devices.....46
Managing Firmware.....47
Adding Firmware.....47
Pushing Firmware to Devices.....48
Editing the Firmware.....49
Downloading the Firmware.....49
Deleting Firmware.....49
Managing Resources.....50
Adding Resource Files.....50
Pushing Resource Files to Devices.....50

Editing Resource Files....51
Downloading the Resource Files....51
Deleting Resource Files....52

Managing Accounts....52
Adding Accounts....52
Importing Accounts....52
Editing the Account Information....53
Exporting Accounts....53
Deleting Accounts....53

Managing the Device Configuration....54
Managing Model Configuration....54
Adding Configuration Templates....55
Setting Parameters....55
Pushing Configuration to Devices....58
Editing Configuration Templates....59
Downloading the Model File....59
Viewing Parameters....59
Deleting Templates....60
Managing the Site Configuration....60
Adding Site Configuration Templates....60
Setting Parameters....60
Pushing the Site Configuration to Devices....63
Editing the Site Configuration Template....64
Downloading the Site Configuration Template....64
Deleting Site Configuration Templates....64
Managing the Group Configuration....64
Adding the Group Configuration....65
Setting Parameters....66
Editing Groups....68
Pushing the Group Configuration....69
Viewing Parameters....70
Downloading Configuration File....71
Deleting Groups....71
Managing the MAC Configuration....71
Uploading Backup Files....71
Generating Configuration Files....72
Setting Parameters....72
Pushing Backup Files to Devices....74
Downloading the Configuration Files....74
Exporting the Configuration Files....74
Deleting Backup Files....74
Configuring Global Parameters....74

Managing Sites....75
Adding Sites....75
Importing Sites....76
Editing Sites....76
Deleting Sites....77

Managing Tasks....78

Adding Scheduled Tasks....79
Editing Scheduled Tasks....80
Pausing or Resuming Scheduled Tasks....81
Ending Scheduled Tasks....81
Searching for Scheduled Tasks....81
Viewing Scheduled Tasks....82
Viewing Tasks....82
Searching for Executed Tasks....83

Diagnosing Devices....83
Starting Diagnosing....84
Exporting the Packets, Logs, and Configuration Files by One Click....85
Capturing Packets....86
Diagnosing the Network....87
Exporting System Logs....88
Exporting the Configuration Files....89
Viewing the CPU and the Memory Status....89
Viewing Recording Files....90
Taking the Screenshot of the Device....91
Getting the Device Log....92
Setting the Log Level....92
Download the Device Log....92
Backing up Configuration Files....93
Diagnostic Assistance....93
Ending the Diagnostic....93

Managing Alarm....93
Alarm Statistics....94
Adding Alarm Strategies....95
Managing Alarm Strategies....98
Viewing Alarms....99
Filtering the Alarms....103
Customizing Filters....103
Filtering the Alarms....104
Exporting Alarm Records....104

Viewing Call Quality Statistics....105
Customizing the Indicators of Call Quality Detail....105
Viewing the Call Data....105

Managing System....107
Viewing Operation Logs....107
Exporting the Server Log....108
Configuring the SMTP Mailbox....108
Uploading DST Rules....110
Obtaining the Accesskey....110

Managing Administrator Accounts....110
Adding and Managing Groups....110
Adding and Managing Roles....111
Assigning the Function Permission....112

Assigning the Data Permission..... 113
Adding and Managing Sub-Administrator Accounts..... 114
Editing the Account Information..... 114
Viewing the Account Code..... 115

Troubleshooting..... 116
Forget the Login Password?..... 116
Why You Cannot Access the Login Page?..... 116
Why the Browser Prompts That the Security Certificate of the Website Is not Trusted When You Access the Login Page?..... 117

About This Guide

This guide introduces Yealink Device Management Platform (YDMP) and how to manage devices on it.

- *Related Documentations*

Related Documentations

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

- Quick Start Guide introduces how to deploy devices and configure the most basic features available on devices.
- User Guide introduces the basic and advanced features available on devices.
- Administrator Guide introduces how to deploy the devices.
- Auto Provisioning Guide introduces how to deploy devices by using the configuration and the boot files. The purpose of Auto Provisioning Guide is to serve as basic guidance for provisioning Yealink phones in a provisioning server. If you are new to this, it is helpful to read this guide.
- API documents introduces how to call the API.

You can download the above documents from Yealink official website or in the top-right corner of the YDMP web page. The address of Yealink official website is as below: *http://support.yealink.com/documentFront/forwardToDocumentDetailPage?documentId=242*.

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

Summary of Changes

- *Changes for Release 36, Guide Version V3.6.0.20*
- *Changes for Release 36, Guide Version V3.6.0.10*
- *Changes for Release 36, Guide Version V3.6.0.1*
- *Changes for Release 35, Guide Version V3.5.0.21*
- *Changes for Release 35, Guide Version V3.5.0.20*
- *Changes for Release 35, Guide Version V3.5.0.11*
- *Changes for Release 35, Guide Version V3.5.0.10*
- *Changes for Release 35, Guide Version V3.5.0.1*
- *Changes for Release 34, Guide Version V3.4.0.10*

Changes for Release 36, Guide Version V3.6.0.20

Major updates have occurred to the following sections:

- *Supported Device Models*
- *Viewing Recording Files*
- *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*
- *Backing up Configuration Files*

Major updates have occurred to the following sections:

- *Adding the Group Configuration*
- *Viewing the Information of the Room System*
- *Adding and Managing Roles*
- *Viewing Alarms*

Changes for Release 36, Guide Version V3.6.0.1

The following sections are new for this version:

- *Getting the Device Log*

Major updates have occurred to the following sections:

- *Supported Device Models*
- *Viewing the Information of SIP Device*
- *Adding Scheduled 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 V3.5.0.21

Major updates have occurred to the following sections:

- *Importing the HTTPS Certificate*
- *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 V3.5.0.20

The following sections are new for this version:

- *Installing YDMP 3.X (3.5.0.20 or later Versions)*

Major updates have occurred to the following sections:

- *Hardware and Software Requirements*
- *Supported Device Models*
- *Updating YDMP (from V3.1 to V3.X)*

- *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 V3.5.0.11

Major updates have occurred to the following sections:

- *Supported Device Models*
- *Deploying YDMP*
- *Viewing Alarms*

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

The following sections are new for this version:

- *Uploading DST Rules*

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:

- *Configuring the Common.cfg File*
- *Adding Sites*

- *Starting Diagnosing*

Introduction of Yealink Device Management Platform

Yealink Device Management Platform (YDMP) possesses the centralized deployment, the management, the analysis, the alarm monitoring, the device diagnosis, the account registration, and other features. The management platform allows administrators to deploy and configure Yealink devices used in an enterprise.

- *Browser Requirements*
- *Supported Device Models*
- *Port Requirements*

Browser Requirements

YDMP 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 YDMP:

Device Types	Supported Device Models	Version Requirements
SIP IP Phones	SIP-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.
	SIP-T56A/T58	58.83.0.5 or later.
	SIP-CP960	73.83.0.10 or later.
	SIP-CP920	78.84.0.15 or later.
	SIP-T53/T53W	95.84.0.10 or later.
	SIP-T54W	96.84.0.10 or later.
	SIP-T57W	97.84.0.30 or later.
	VP59	91.283.0.10 or later.
	SIP-T42U/T43U/T46U/T48U	108.84.0.30 or later.
	SIP-T30/T30P/T31/T31P/T31G/ T33P/T33G	124.85.0.10 or later.

Device Types	Supported Device Models	Version Requirements
	W60B	77.85.0.20 or later.
Skype for Business HD IP phones	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.
Teams phones (It is not available for managing the accounts and viewing the call quality)	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.
	VC210	118.15.0.20 or later.
Video Conferencing Systems	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.
	VP59	91.332.0.10 or later.
	PVT940/PVT960	120.43.0.25 or later.
Zoom phones	CP960	73.30.0.10 or later.
Room System	MVC500/MVC800/MVC300/ CP960-UVC Zoom Rooms Kit/ VP59 Zoom Rooms Kit	XX.11.0.10 or later.
	MVC400	2.2.23.0 or later

Note: If your YDMP is upgraded from a lower version, you must import the latest parameter configuration file. Otherwise, you cannot use some device models. For more information about the corresponding configuration, refer to *Updating the Configuration* .

Port Requirements

You need to open 5 ports for YDMP: 443, 9989, 8446, 9090, and 80. We do not recommend that you modify these ports.

Port	Description
443	It is used for accessing the device management platform via HTTPS.
9989	It is used for the phone to download the configuration files and calling the API.
9090	TCP persistent connection. It is used for reporting the device information.

Port	Description
8446	It is used for mutual authentication between YDMP 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.

Deploying YDMP

This chapter introduces how to install and deploy YDMP.

- *Hardware and Software Requirements*
- *Updating YDMP (from V2.0 to V3.1)*
- *Restoring YDMP (from V3.1 to V2.0)*
- *Installing YDMP 3.X (3.5.0.11 or Earlier Versions)*
- *Installing YDMP 3.X (3.5.0.20 or later Versions)*
- *Updating YDMP (from V3.1 to V3.X)*
- *Installing the Diagnostic Script*
- *Activating the License*
- *Updating the Configuration*
- *Uninstalling YDMP*

Hardware and Software Requirements

YDMP supports the stand-alone installation and the cluster installation since version 3.5.0.20. YDMP has different hardware and software requirements for different installation methods.

For virtual machine, we support VMware ESXi in version 6.5 or later. For Linux operating system, we support CentOS7.5 and CentOS8.1 (supported since version 3.5.0.20)

Requirements for stand-alone installation:

Device Quantity	CPU	RAM	Hard Drive
0~6000	8-core	16G	At least 250G, and the capacity of the hard drive increases by 30G with every 1000 devices added.
6000~15000	16-core	32G	
15000~30000	32-core	64G	

Requirements for each server in the cluster installation (3 servers are required and the requirements for each server are the same):

Device Quantity	CPU	RAM	Hard Drive
0~30000	8-core	16G	At least 250G for 6000 devices, and the capacity of the hard drive increases by 30G with every 1000 devices added.
30000~50000	8-core	24G	
50000~100000	16-core	24G	

Note:

- The partition /usr/local/ is used for installing YDMP. You can run command df -h /usr/local/ to check the available space in this partition. Make sure that there are at least 200G available in this partition.
- The partition /var is used for storing the service log. You can run command df -h /var to check the available space in this partition. Make sure that there are at least 50G available in this partition.
- For other partitions, make sure they have available space.

Updating YDMP (from V2.0 to V3.1)

The following is an example of updating YDMP from V2.0.0.14 to V3.1.0.13.

Before you begin

- Obtain the installation package of YDMP from the Yealink distributor or SE and then save it at the path of /usr/local.
- Meet the following requirements: *Hardware and Software Requirements* and *Port Requirements* .

Procedure

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

```
cd /usr/local
tar -zxf DM_3.1.0.13.tar.gz
cd yealink_install&& tar -zxf install.tar.gz
./upgrade_v2_to_v3.sh
```

3. According to the prompts, enter *1* which means updating.
4. According to the prompts, enter the server IP address and enter *Y* to confirm the IP address.

Results

YDMP will be upgraded to the corresponding version if it is upgraded successfully.

Note: Upgrading the version has no influence on the devices connected to YDMP.

Restoring YDMP (from V3.1 to V2.0)

Procedure

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

```
cd /usr/local/yealink_install/
./upgrade_v2_to_v3.sh
```

3. According to the prompts, enter *2* which means restoring.
4. According to the prompts, enter the password *Yealink1105*.
5. According to the prompts, enter *Y* to confirm restoring.
6. According to the prompts, enter *Y* to clean up the data.

   When the restoring is completed, YDMP will be restored to V2.0.

Attention: Note that if you enter the wrong password, do not restore YDMP again, because it will delete all the data on YDMP. However, you can follow the steps below:

1. Run the command:

```
cd /usr/local/
mv yealink yealink_bak #it means making a data backup for V2.0
cd yealink_install/
./uninstall  #it means uninstalling V3.0
```

2. According to the prompts, enter the password *Yealink1105*.
3. According to the prompts, enter *Y* to confirm to uninstall.
4. According to the prompts, enter *Y* to clean up the data.
5. After uninstalling, run the command below:

```
cd /usr/local/
mv yealink_bak/ yealink #it means restoring the data for V2.0
#create the contents that are deleted
cd /var/log/yealink/
mkdir dm
cd dm/
mkdir tomcat_dm
cd tomcat_dm/
touch catalina.out
#Run the command below to start the corresponding services of V2.0:
systemctl start mariadb
systemctl start redis
systemctl start rabbitmq-server
systemctl start tcp-server
systemctl start tomcat_dm
```

YDMP will be restored to V2.0.

Installing YDMP 3.X (3.5.0.11 or Earlier Versions)

The following is an example of installing V3.5.0.1.

Before you begin

- Obtain the installation package of YDMP from the Yealink distributor or SE and then save it at the path of /usr/local.
- Meet the following requirements: *Hardware and Software Requirements* and *Port Requirements* . When you install YDMP in the version 3.3.0.0 or later for the first time, if your hardware does not meet the basic requirements for installing YDMP, your installation will be forbidden. Change your hardware and re-install YDMP according to the prompts.

Procedure

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

```
cd /usr/local
tar -zxf DM_3.5.0.1.tar.gz
cd yealink_install&& tar -zxf install.tar.gz
./install --host the internal IP or the external IP
##If it is the deployment of a single NIC (the internal network or the external network), run this
 command. ##
./install --host the internal IP -e nat_ip=the external IP behind NAT
```

##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this command.## This command is only applicable to 3.3.0.0 or later versions.
Make sure that the default gateway is the gateway of the external NIC.
Run the command “ip route” to request the default gateway.
Run the command “*ip route add default via* gateway IP *dev* external NIC name” to edit the default gateway. ##
./install --host the internal IP -e nat_ip=the external IP behind NAT
##If it is the deployment of dual NIC (the internal and the external network), run this command. This command is only applicable to 3.3.0.0 or later versions. ##

3. It defaults to select A as the installation method.

Results
The installation starts and takes some time to finish.

Installing YDMP 3.X (3.5.0.20 or later Versions)

YDMP installation method includes the stand-alone installation and the cluster installation.

- *Downloading the Installation Package*
- *Closing the Firewall Came with the Linux System*
- *Unzipping the Installation Package*
- *Installing YDMP*
- *Importing the HTTPS Certificate*

Downloading the Installation Package

- The server can access the external network

1. Run the following command to go to the directory (/usr/local):

```
cd /usr/local
```

2. Run the following command to download the installation package:

```
wget address     # replace address with the address you obtain from Yealink technical support engineers to download the installation package#
```

- The server cannot access the external network

1. Manually download the installation package, which you obtain from Yealink technical support engineers.
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.

Closing the Firewall Came with the Linux System

Run the following command to close the firewall:

```
systemctl status firewalld.service
systemctl stop firewalld.service
systemctl disable firewalld.service
```

Unzipping the Installation Package

Run the following command:

```
tar zxvf DM-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                      ##unzip the installation script##
```

Installing YDMP

This chapter introduces how to run the command to install stand-alone YDMP and cluster YDMP.

Before you begin

- Meet the following requirements: *Hardware and Software Requirements* and *Port Requirements* . When you install YDMP for the first time, if your hardware does not meet the basic requirements for installing YDMP, your installation will be forbidden. Change your hardware and re-install YDMP according to the prompts.
- For cluster deployment, you need 3 servers.

Procedure

1. Run the command:

```
cd /usr/local/yealink_install/
./install
##If it is the single NIC deployment (internal or external), run this command.##
./install -e nat_ip=the external IP behind NAT IP
##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this
 command.
Make sure that the default gateway is the gateway of the external NIC.
Run the command "ip route" to request the default gateway.
Run the command "ip route add default via gateway IP dev external NIC name" to edit the
 default gateway. ##
./install -e nat_ip=the external IP
##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this
 command.##
```

2. Do one of the following:

- For the stand-alone installation, select A. If you do not select one within 30 seconds, the system will select A automatically.

  It prompts you to enter the IP address when you install stand-alone YDMP for the first time. After typing the IP address, press Enter.

  Note: If the server has only one IP address, enter it. If the server has several IP addresses, enter the internal IP address.

- For the cluster deployment, select B. The system automatically generates the configuration template *usr/local/yealink/data/install.conf*.

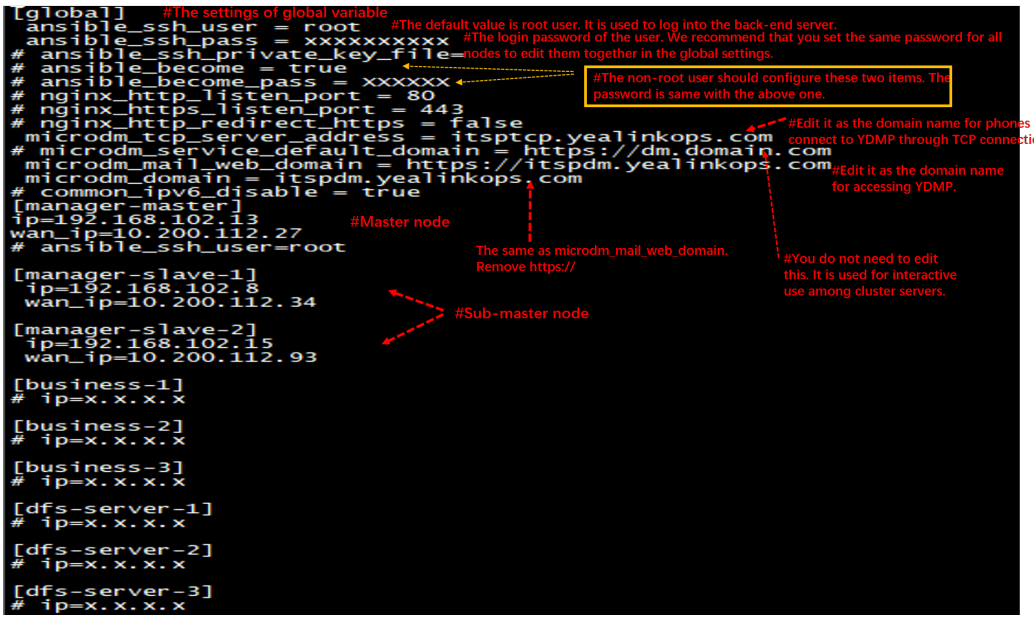
  Run command *vi*, edit the configuration template, and fill in the desired cluster information. Run *./install* again.

Note:

- If it is the deployment of single NIC (the internal or external network), you only need to edit the *ip=x.x.x.x* in the master node.
- If it is the deployment of dual NIC (the internal and the external network), you need to edit *ip=x.x.x.x* as the internal IP address and *wan_ip=x.x.x.x* as the external IP address. You need to edit the internal and the external IP address in the corresponding fields.
- After editing the parameter, you need to delete the comment symbol # in front of the parameter.
- You need to employ the domain name for the following configuration:

  ```
  microdm_tcp_server_address
  ```

```
microdm_mail_web_domain
microdm_domain
```



Results

The installation starts and takes some time to finish. For the cluster deployment, you can use the domain name to log into YDMP if your installation successes.

Importing the HTTPS Certificate

For the cluster deployment, you need to import HTTPS certificate. Otherwise, it will affect the mutual authentication between the phone and the server and cause the failure of pushing the configuration and firmware.

Procedure

1. Upload the custom HTTPS certificate to the certificate directory.

   ```
   cd /usr/local/yealink/nginx/conf/ssl/
   rz    ##run command rz to upload the custom HTTPS certificate##
   ```

2. Edit the *yealink.conf* file in the directory of */usr/local/yealink/nginx/conf/http.conf.d/*, and change the corresponding certificate names of *ssl_certificate* and *ssl_certificate_key* of port 443 to *ssl/xxxxx.pem* (the name of the custom HTTPS certificate).

```
#server
server {
    server_name "_";
    listen        443 ssl;
    ssl_certificate      ssl/nginx.pem;
    ssl_certificate_key  ssl/nginx.pem;

    ssl_verify_depth 2;
    client_max_body_size 10240m;
    proxy_http_version 1.1;
    proxy_set_header   Upgrade $http_upgrade;
    proxy_set_header   Connection $connection_upgrade;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Real-Port $remote_port;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Protocol "$scheme";
    #proxy_set_header Apollo-Forwarded "edge";
    proxy_set_header apollo-server-addr "$server_addr";
    add_header Strict-Transport-Security "max-age=16000000;includeSubDomains;preload;" al
    add_header Referrer-Policy "no-referrer-when-downgrade" always;
    add_header X-Content-Type-Options "nosniff" always;
    add_header X-XSS-Protection "1;mode=block" always;
    proxy_set_header Client-DN $ssl_client_s_dn;
    add_header Set-Cookie "HttpOnly";
    add_header Set-Cookie "secure";
    add_header X-Frame-Options "SAMEORIGIN";

    location / {
        proxy_pass https://server_frontend_manager;
    }
```

3. Run the following command.

```
systemctl restart nginx
```

4. After you change the certificate of port 443 to the custom one, you need to change the server address that devices use for obtaining the configuration (dm.cfg) to *http://IP or domain name:9989/dm.cfg*.

Updating YDMP (from V3.1 to V3.X)

Before you begin

- Obtain the installation package of YDMP from the Yealink distributor or technical support engineers and then save it at the path of /usr/local.
- Meet the following requirements: *Hardware and Software Requirements* and *Port Requirements* .

Procedure

1. Log into CentOS as the root user and open the terminal.
2. Do one of the following:
   - If you want to upgrade YDMP to the version earlier than 3.4.0.10 (not including 3.4.0.10), run the following command:

```
cd /usr/local
rm -rf yealink_install
tar -xvzf DM_3.3.0.0.tar.gz
cd yealink_install&& tar -xvzf install.tar.gz
./upgrade --host internal IP or the external IP
##If it is the deployment of a single NIC (the internal or the external network), run this
 command.##
./upgrade --host the internal IP -e nat_ip=the external IP behind NAT
```

```
##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this
 command This command is only applicable to 3.3.0.0 or later versions. ##
./upgrade --host the internal IP -e nat_ip=the external IP behind NAT
##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this
 command. This command is only applicable to 3.3.0.0 or later versions. ##
```

- If you want to upgrade YDMP to the version later than 3.4.0.10 (including 3.4.0.10), firstly, run the following command:

```
cd /usr/local
rm -rf yealink_install
tar -xvzf DM_3.5.0.1.tar.gz
cd yealink_install&& tar -xvzf install.tar.gz
./install -m upgrade
###If it is the deployment of a single NIC (the internal network or the external network), run this
 command.##
./install –m upgrade –e nat_ip=the external IP behind NAT
###If it is the deployment of dual NIC (the internal and the external network) and NAT, run this
 command. This command is only applicable to 3.3.0.0 or later versions. ##
./install –m upgrade –e nat_ip=the external IP
###If it is the deployment of dual NIC (the internal and the external network), run this command.
 This command is only applicable to 3.3.0.0 or later versions. ##
```

- If you want to upgrade YDMP to the version later than 3.5.0.20 (including 3.5.0.20), you can install it directly (refer to *Installing YDMP 3.X (3.5.0.20 or later Versions)*).

Results

YDMP will be upgraded to the corresponding version if it is upgraded successfully.

Note: Upgrading the version has no influence on the devices connected to YDMP.

Installing the Diagnostic Script

If you fail to install YDMP or some exceptions occur to the service, you can run the diagnostic script to collect the related environment and service information of YDMP, and pack the file named *ydmp_diag_time.tar.gz*. And then, you can provide the developers or operation and maintenance engineers with the file.

About this task

This script is packed in the file *local install.tar.gz* in the directory of */usr/local*.

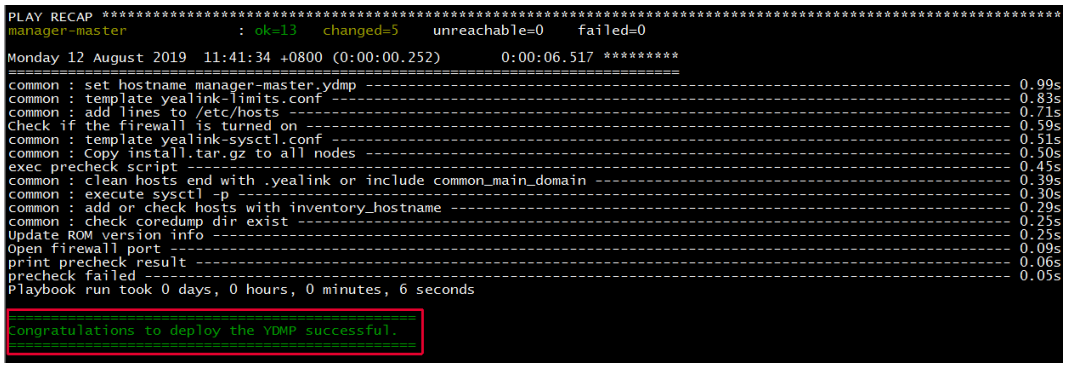
Procedure

Unzip and run the script.

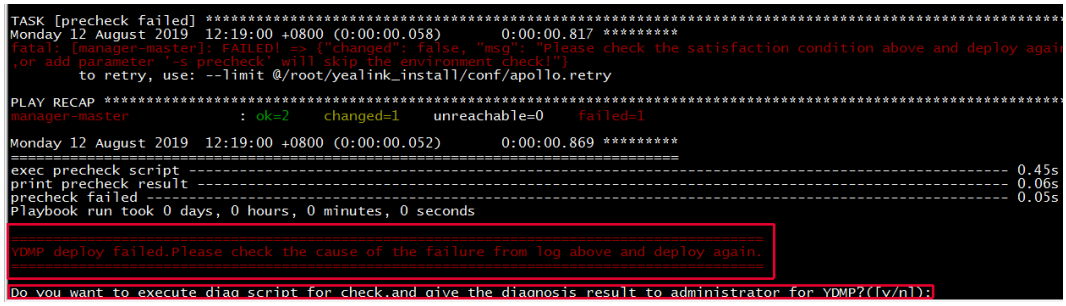
```
[root@manager-master yealink_install]# ./diag
Starting to execute diag script ...
```

Results

If you succeed in installing, the page is shown as below:



If you fail to install, the page is shown as below:



Activating the License

Before managing your devices on YDMP, you need purchase the license from your supplier and activate it.

Procedure

1. *Importing the Device Certificate* .
2. *Activating the License Online* or *Activating the License Offline* .

- *Importing the Device Certificate*
- *Activating the License Online*
- *Activating the License Offline*

Importing the Device Certificate

You need to import a device certificate which is associated with the server uniquely.

Before you begin

You provide the enterprise name, the distributor and the country for Yealink. Yealink will generate a device certificate according to the information you provide.

Procedure

1. Click **System Management** > **License**.
2. Select a device certificate.

Note: Note that one device certificate for one server, that is, if you have imported the device certificate to one server, you cannot import the certificate to another server.

If the association between the device ID and the server succeeds, the page will display as below:

Activating the License Online

If your server can access the public network, you can activate the license online.

Before you begin

- If *Importing the Device Certificate* is finished, the hardware information will be sent to Yealink License server automatically.
- You provide the device ID, the license type, the concurrent number and the validity for Yealink. Yealink will generate a license according to the information you provide.

Procedure

Click **System Management** > **License** > **Refresh**.
After Yealink authorizes the license, you can see the license in the list.

Activating the License Offline

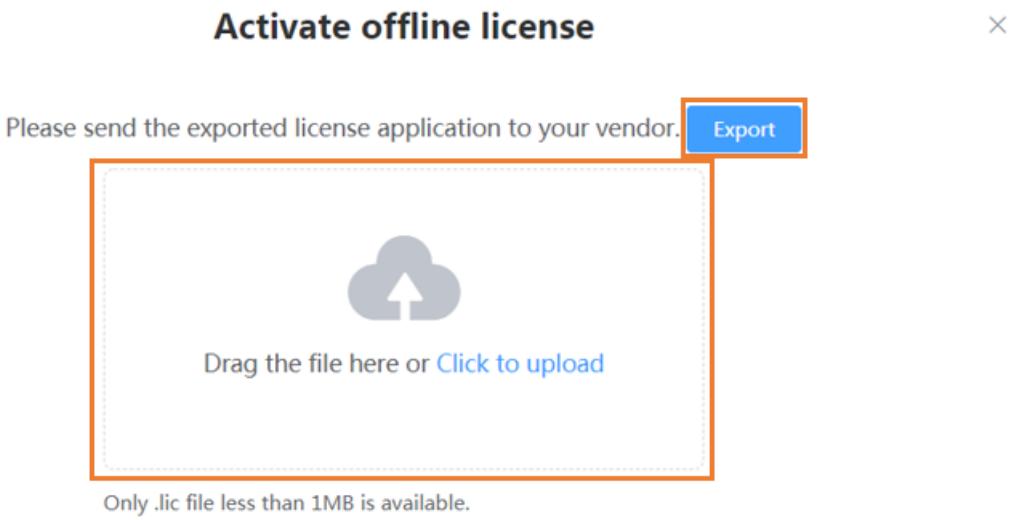
If your server cannot access the public network, you can activate the license offline.

Before you begin

- *Importing the Device Certificate* is done.
- You provide the device ID, the license type, the concurrent number and the validity for Yealink. Yealink will generate a license according to the information you provide.

Procedure

1. Click **System Management** > **License** > **Activate offline license**.
2. Click **Export Config File**. Send the exported REQ file to Yealink. Yealink will generate a license according to the file you provide. Yealink will generate the LIC authentication file and send it to you.
3. Click the field of the dotted box to upload the authorization file obtained from Yealink.



Note: The authentication file is unique, that is, different servers use different authentication files. You cannot activate your server by importing the authentication files of other servers.

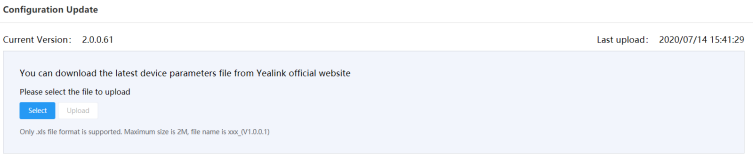
Results
The authorized license is displayed on the page.

Updating the Configuration

If your YDMP is upgraded from a lower version, you must import the latest configuration file. Otherwise, you cannot use some device models. You can update the configuration by downloading the latest configuration file from Yealink official website. If the configuration is updated, the parameters in the template will be updated synchronously. You can download the latest configuration file from *http://support.yealink.com/documentFront/forwardToDocumentDetailPage?documentId=242*.

Procedure

1. Click **Device Configuration** > **Configuration Update**.
2. Click **Select** and select the desired file to upload.



Only the XLS file is supported and the size should be less than 2M.

3. Click **Upload**.

Uninstalling YDMP

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*.
YDMP will be uninstalled from the CentOS.

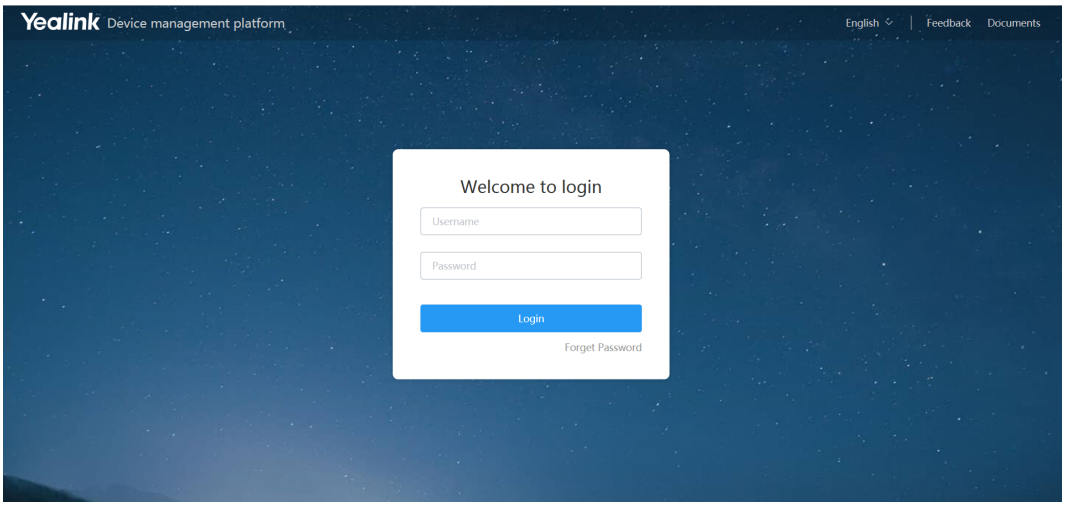
Getting Started

- *Logging in to YDMP*
- *Home Page*
- *Logging out of YDMP*

Logging in to YDMP

Procedure

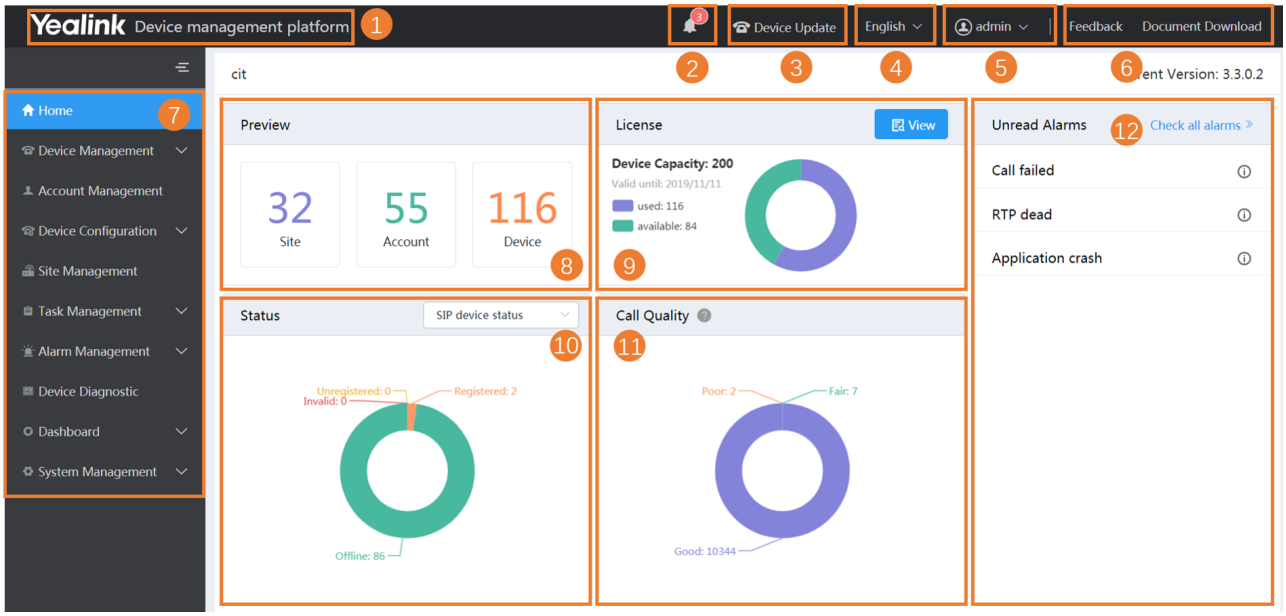
1. Enter https://<IP address>/(for example, https: //10.2.62.12/) in the address box, and then press Enter.



2. Select the desired language from the drop-down menu of **Language** in the top-right corner.
3. Enter your username (default: admin) and the password (default: v123456789).
4. Click **Login**.
5. When the first time you use the default password to log in, the system will remind you to change the password, click **Change** to go to the home page of YDMP .

Home Page

After logging in YDMP, you can see the home page displayed as below:



Number	Description
1	Go to the home page quickly when you are browsing other pages.
2	Display the number of unread alarms and the type of alarms.
3	Go to the Device List page quickly.

Number	Description
4	Change the display language.
5	Go to the page of setting the administrator account.
6	Go to the page of sending feedback or downloading a document.
7	Navigation pane.
8	**Data preview:** • Display the number of sites, accounts and devices. • Click the desired module to go to the corresponding module.
9	**License:** Display the current number of manageable devices.
10	**Device status:** • Select a device type. • Display the number of the unregistered, the registered, the invalid and the offline devices. • Click the corresponding device status to go to the page that lists all the devices of this status.
11	**Call quality:** • Display the number of the good, the bad or the poor call quality. • You can click the desired module to view the call statistics.
12	**Unread Alarms:** • Click **Check all alarms** to go to the Alarm List page. • Hover the mouse over the icon ⓘ to view the alarm details.

Logging out of YDMP

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.

Connecting to YDMP

- *Connecting SIP Device*
- *Connecting USB Devices*
- *Connecting Room System*

Connecting SIP Device

Before you begin

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

Procedure

1. *Using Certificates for Mutual TLS Authentication* .
2. If there is a provisioning server you are using in your environment, configure the common cfg file (refer to *Configuring the Common.cfg File*).
3. 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://<IP address>/dm.cfg.

     (for example, https://10.2.62.12/dm.cfg)
   - *Deploying Devices on the RPS (Redirection & Provisioning Server) Management Platform* , and configure the server address.
   - *Configuring the Server Address* , and deploy a single phone.

Results

After the device is connected to the YDMP-SP, the device information will be displayed in the device list.

- *Using Certificates for Mutual TLS Authentication*
- *Configuring the Common.cfg File*
- *Deploying Devices on the RPS (Redirection & Provisioning Server) Management Platform*
- *Configuring the Server Address*

Related concepts

Supported Device Models

Using Certificates for Mutual TLS Authentication

To allow YDMP and the device to authenticate with each other, YDMP supports mutual TLS authentication by using default certificates.

- **Configuring Server Certificates**

  When YDMP sends a TLS connection request to the device, YDMP needs to verify whether the device can be trusted. The device will send the default device certificate to YDMP.

  Procedure

  1. Log into the web user interface of the device.
  2. Click **Security** > **Server Certificates**.
  3. Select **Default Certificates** from the drop-down menu of **Device Certificates**.

     The device will send the default device certificate to YDMP for authentication.

- **Configuring Trusted Certificates**

  When a device sends a SSL connection request to YDMP, the device needs to verify whether YDMP can be trusted. YDMP sends its certificate to the device and the device verifies this certificate based on its trusted certificates list.

Procedure

1. Log into the web user interface of the device.
2. Click **Security** > **Trusted Certificates**.
3. Select **Enabled** from the drop-down menu of **Only Accept Trusted Certificates**.

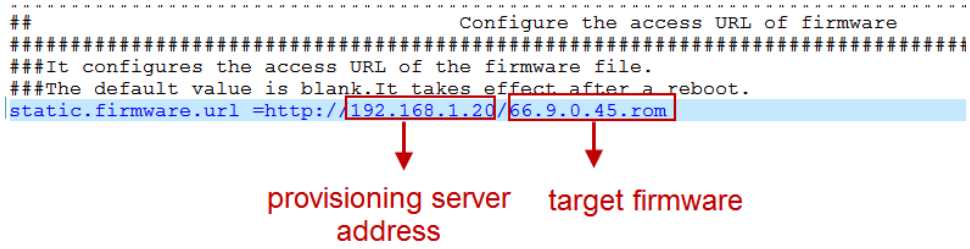
   Only when the authentication succeeds will the device trust YDMP.

Configuring the Common.cfg File

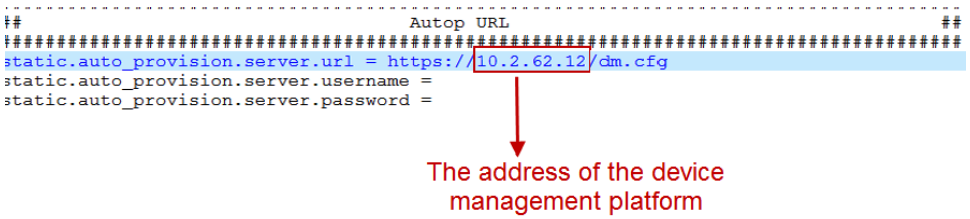
If you want to use your auto-provisioning server to deploy devices but your firmware versions are lower than the requirement of YDMP-SP, you need to upgrade the device firmware first and connect them to YDMP. For easy deployment, you can configure the parameters of upgrading the firmware and the access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

Procedure

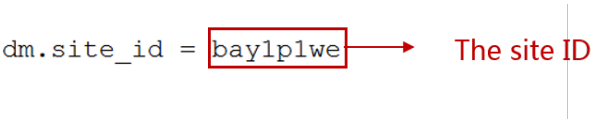
1. Open the Common.cfg file of the corresponding device.
2. If your device firmware does not support the YDMP, upgrade the firmware of the device.



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



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



Note:

- Only the specific firmware version supports this feature. For more information, contact Yealink technical support engineers.

  The supported device models are as below: CP960 (73.84.0.21), T58V (58.84.0.26), VP59 (91.283.0.47), T4xS/T5xW (x.84.0.102), and W60B (77.83.0.72).
- 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 YDMP.

Related concepts
Supported Device Models
Related tasks
Viewing the Account Code

Deploying Devices on the RPS (Redirection & Provisioning Server) Management Platform

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 YDMP to the devices so that they can be connected to YDMP.

Procedure

1. Log in to YMCS for RPS Enterprise.
   The address of the RPS management platform is *https://dm.yealink.com/manager/login*.
2. On the **Server Management** page, add the server URL.
3. On the **Device Management** page, add or edit the device information.

   The server URL must meet the following format: https://<IP address>/dm.cfg

   (for example, https://10.2.62.12/dm.cfg)

Results
After the device sends an RPS request, the device will be connected to YDMP.

Note: For more information on how to use the RPS management platform, refer to *Yealink Management Cloud Service for RPS Administrator Guide*.

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 YDMP.

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 must meet the following format: https://<IP address>/dm.cfg

   (for example, https://10.2.62.12/dm.cfg).
4. Click **Auto Provision Now**.
   The device will be connected to YDMP 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 YDMP automatically.

Connecting Room System

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 YDMP automatically.

Managing Devices

After connecting devices to YDMP, you can see the devices in the device list and manage them.

Note: The maximum number of devices that you can manage on YDMP depends on the number in the license you purchased from the service provider. 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 service provider.

- *Device Status*
- *Running State Page*
- *Managing SIP Devices*
- *Managing USB Devices*
- *Managing Room System*
- *Managing Firmware*
- *Managing Resources*

Device Status

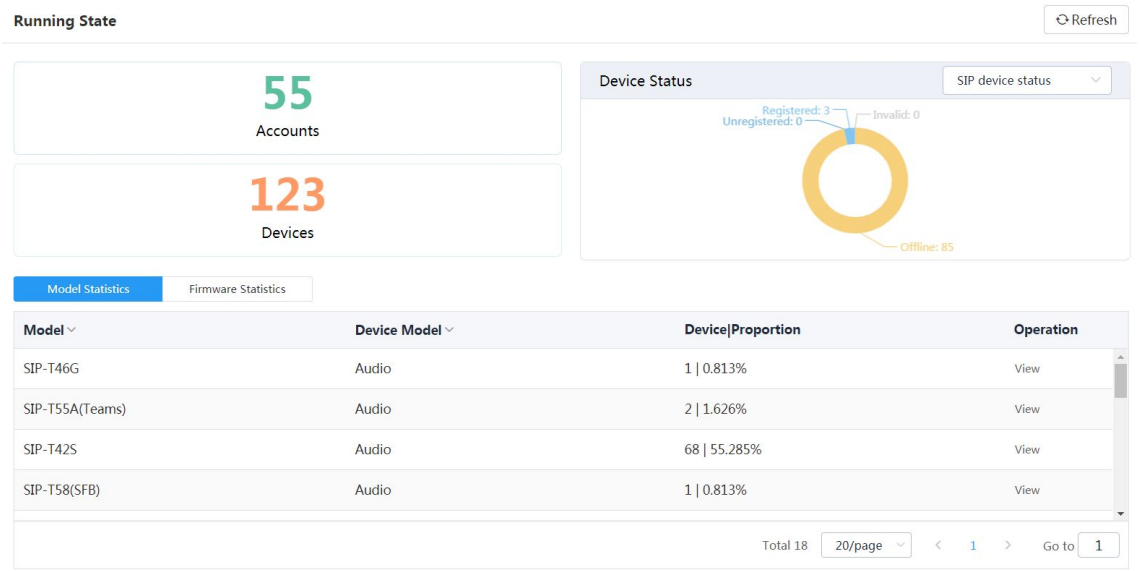
Before managing devices, you can familiarize yourself with the device status.

- Device status of the SIP device
  - Registered: the device is online with an account registered in. You can use it and click it to view the account information.
  - Unregistered: the device is online without an account registered in.
  - Offline: the device is offline.
  - Invalid: the server license expires, or the number of the devices reported to the platform exceeds the number allowed in the license.
- Device status of the USB device and the Room System
  - Online: the application connected to the USB device/Room System is connected to YDMP.

- Offline: the USB device/Room System is disconnected, or the application connected to the USB device/Room System is disconnected to the platform.
- Invalid: the server license expires, or the number of the devices reported to the platform exceeds the number allowed in the license.

Running State Page

Click **Dashboard** > **Running state** to go to the Running State page. You can view the number of accounts and devices, the device status, the statistics of the model and the firmware. It is displayed as below:



- Click **Accounts** to go to the Account Management page, then you can manage the account directly.
- Click **Devices** to go to the Device Management page, then you can manage devices directly.
- In the **Device Status** module, select the device type, click the corresponding status (offline, registered, invalid, and unregistered) to go to the Device List page, and then you can update the device status directly.
- Click **Model Statistics** to view all the device information, including the model and the proportion. Click **View** beside the desired device to go to the Device Management page, then you can view the device information or update this device.
- Click **Firmware Statistics** to view all the running firmware. Click **View** beside the desired firmware to go to the Device Management page, then you can view the device information or update this device.

Managing SIP Devices

- *Editing the Device Information*
- *Exporting the Device Information*
- *Viewing the Information of SIP Device*
- *Searching for Devices*
- *Assigning Accounts to Devices*
- *Setting the Sites*
- *Pushing Configuration Files to Devices*
- *Pushing Firmware to Devices*
- *Pushing Resource Files to Devices*

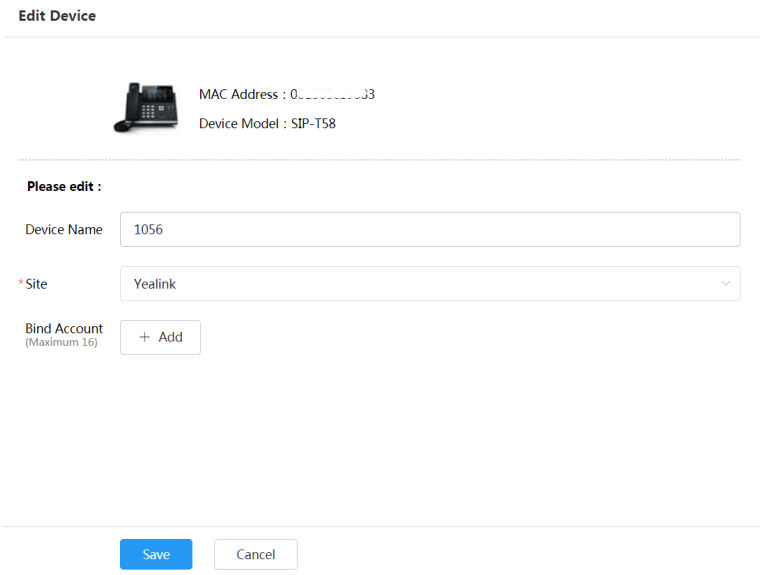
- *Diagnosing Devices*
- *Enabling/Disabling DND*
- *Sending Messages to Devices*
- *Rebooting Devices*
- *Resetting the Devices to Factory*
- *Deleting Devices*

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** > **SIP Device List**.
2. Click beside the desired device.
3. Edit the device information and save it.



Related tasks

Adding Accounts
Setting the Sites

Exporting the Device Information

You can export the basic information of all devices.

Procedure

Click **Device Management** > **SIP Device ListExport**.

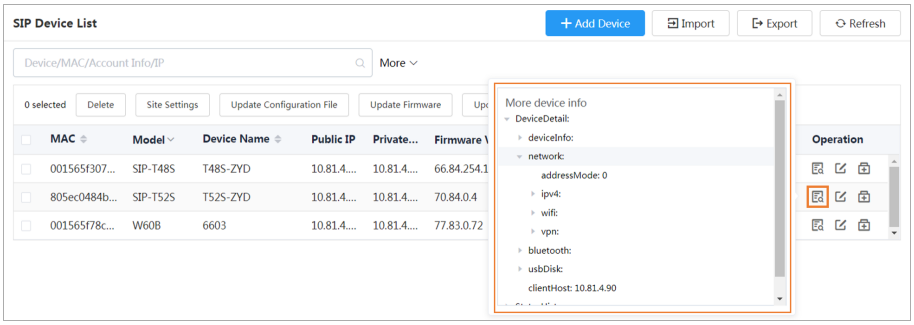
Viewing the Information of SIP Device

You can view the information of SIP devices, including the MAC address, the model, the name, the IP, the firmware version, the status, the site and the report time.

Procedure

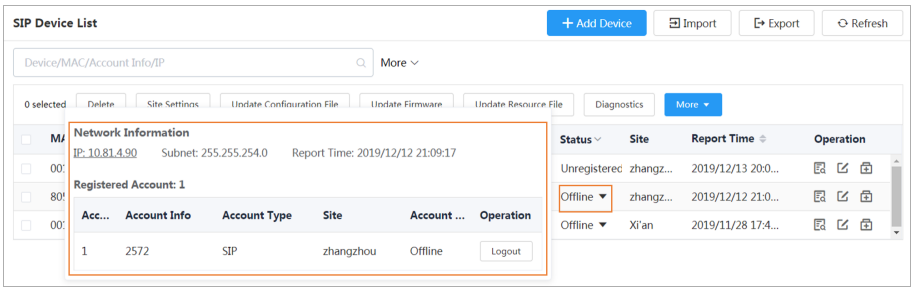
1. Click **Device Management** > **SIP Device List**.
   You can click **Refresh** in the top-right corner to obtain the latest device information,

2. Click beside the desired device.



Note: The devices report their information in real time. Therefore, you cannot view the device information of the offline devices.

3. Optional: Click the status of the desired device under the **Status** tab and you can view the network information and the registered account information.



Note: This feature is not applicable to invalid devices.

Related concepts

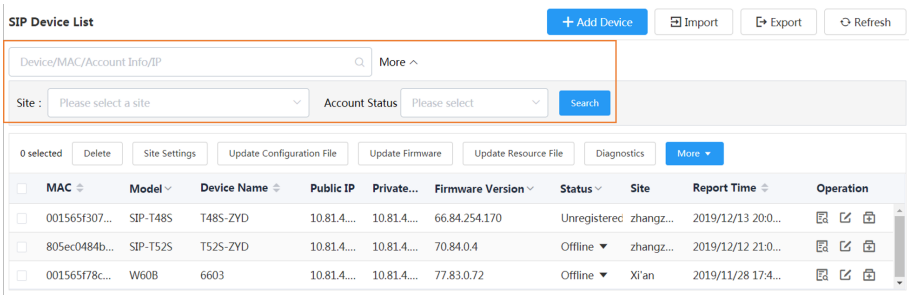
Device Status

Searching for Devices

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

Procedure

Click **Device Management** > **SIP Device List**.



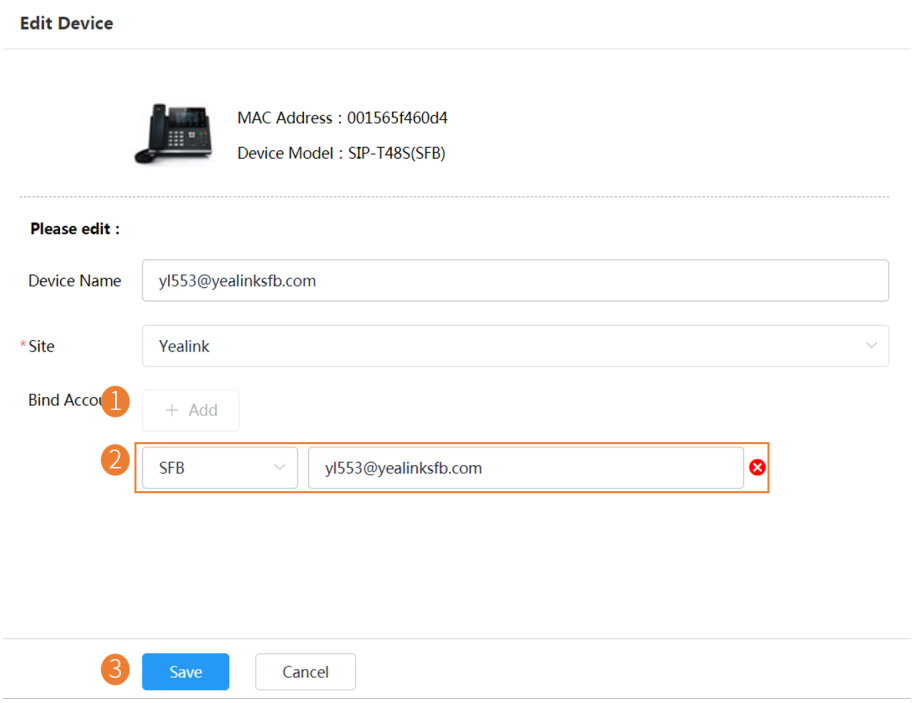
The search results are displayed in the list.

Assigning Accounts to Devices

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

Procedure

Click **Device Management** > **SIP Device List**.



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 YDMP.

Related tasks

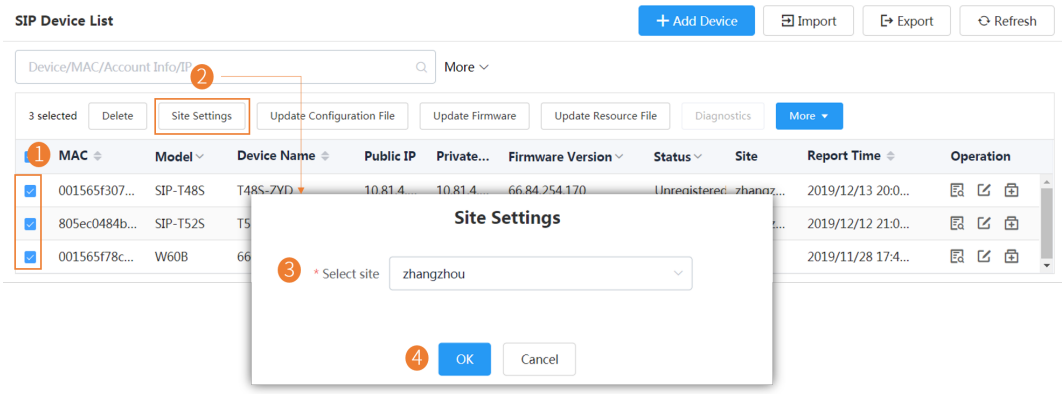
Adding Accounts

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

Click **Device Management** > **SIP Device List**.



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

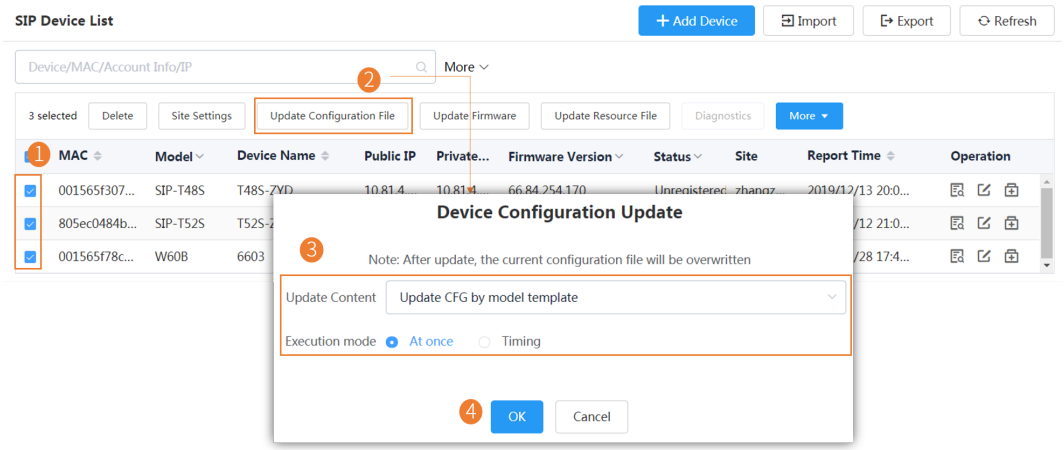
About this task

- 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** > **SIP Device List**.
2. Push the configuration file to the selected devices.



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

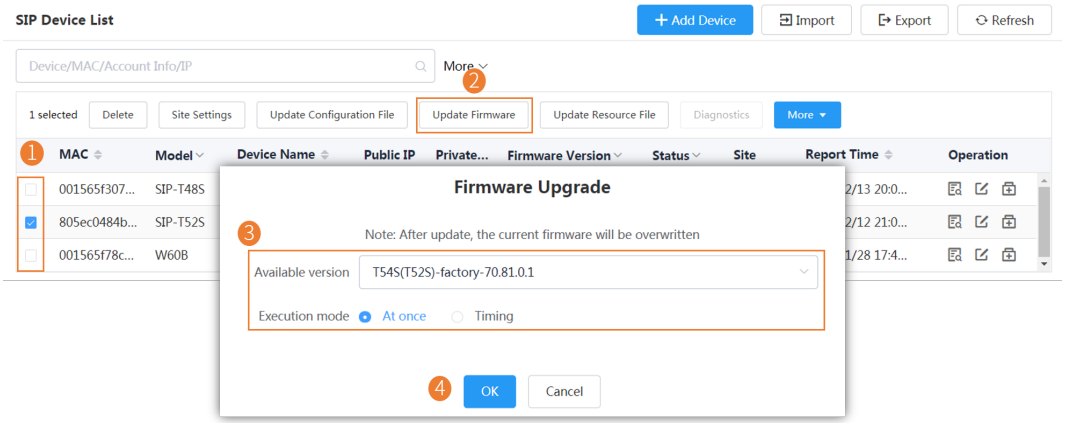
About this task

- 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** > **SIP Device List**.
2. Push the firmware to the selected 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 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* .

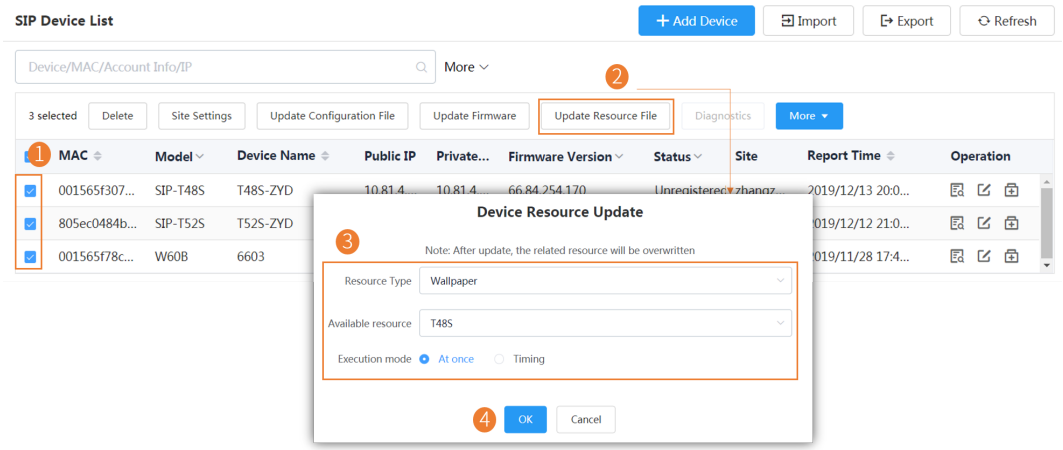
About this task

- 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** > **SIP Device List**.
2. Push the resource file.



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 Tasks* .

Related concepts

Managing Resources

Diagnosing Devices

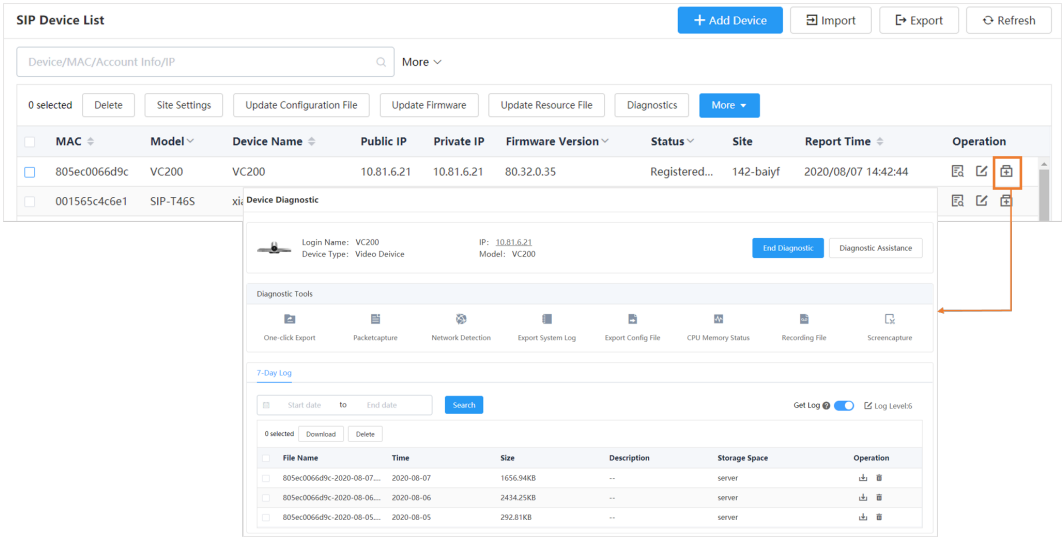
You can diagnose one or multiple devices. You can diagnose up to 5 devices at the same time.

About this task

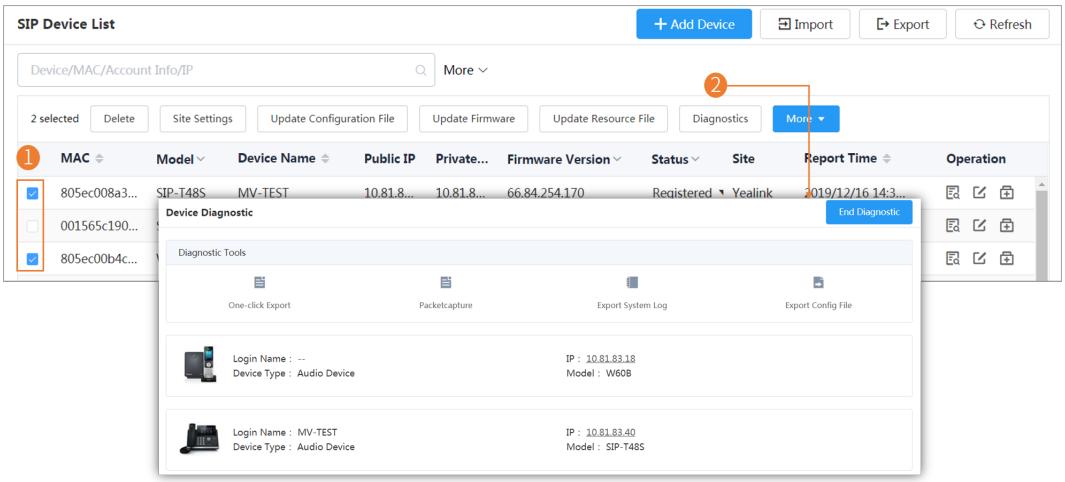
This feature is not applicable to the offline and invalid devices. For more information about the device status, refer to *Device Status* .

Procedure

1. Click **Device Management** > **SIP Device List**.
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

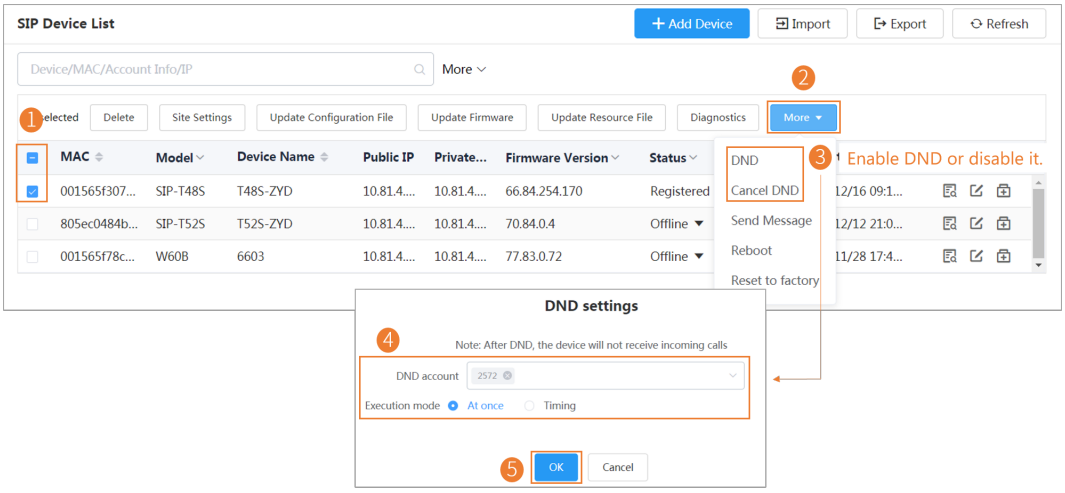
Diagnosing Devices

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.

Procedure

1. Click **Device Management** > **SIP Device List**.
2. Select the corresponding devices and click **More→ DND/Cancel DND**.
3. According to the prompts, select the desired execution mode, and click **OK**.



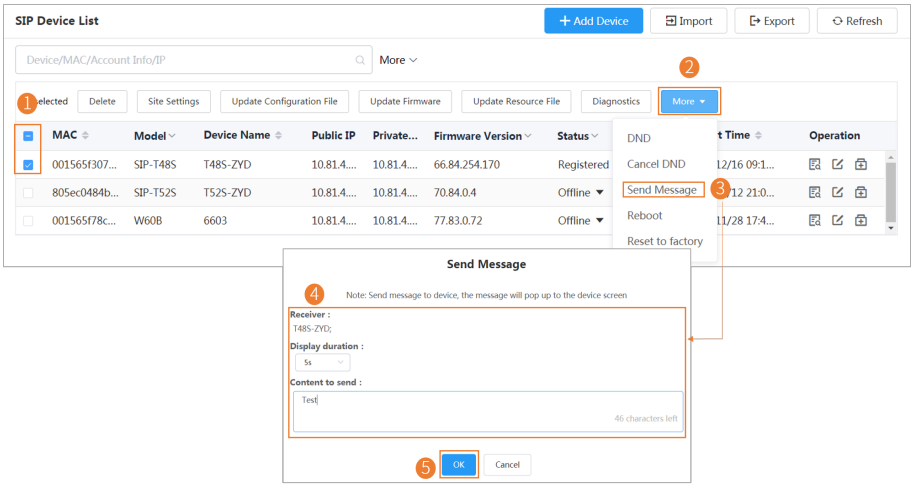
Note: After enabling/disabling DND, you can see the task details, refer to *Viewing Tasks* .

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 YDMP. YDMP supports sending messages to one or multiple devices.

Procedure

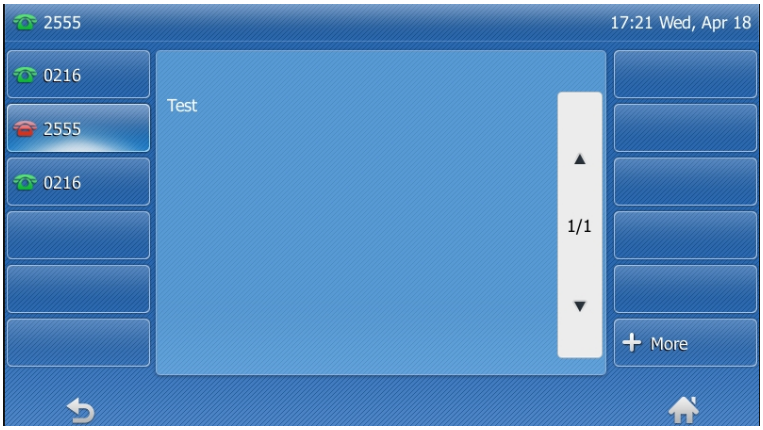
Click **Device Management** > **SIP Device List**.



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

Results

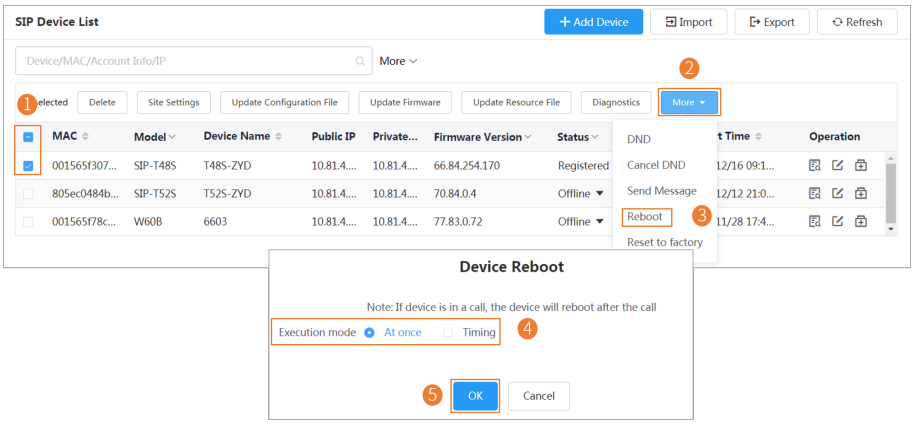
The message will pop up on the device screen. Take the T48S IP phone as an example:



Rebooting Devices

Procedure

1. Click **Device Management** > **SIP Device List**.
2. Select the corresponding devices and click **More→ Reboot**
3. According to the prompts, select the desired execution mode, and click **OK**.

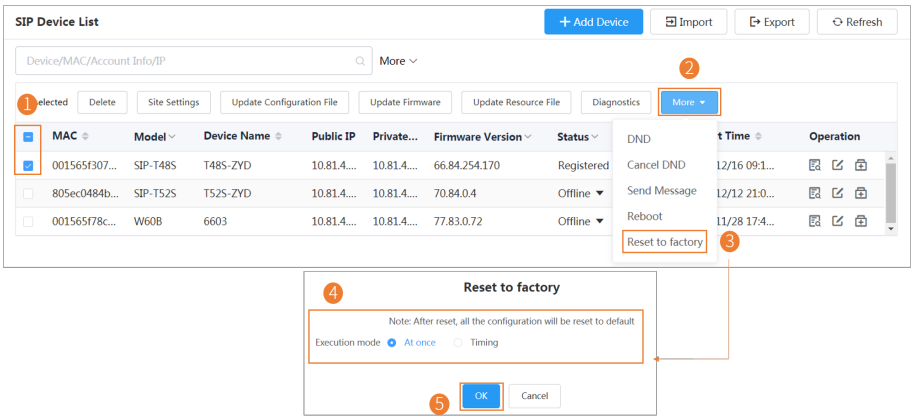


Note: After rebooting the device, you can see the task details, refer to *Viewing Tasks* .

Resetting the Devices to Factory

Procedure

1. Click **Device Management** > **SIP Device List**.
2. Select the corresponding devices and click **More→ Reset to factory**.
3. According to the prompts, select the desired execution mode, and click **OK**.



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

Results

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

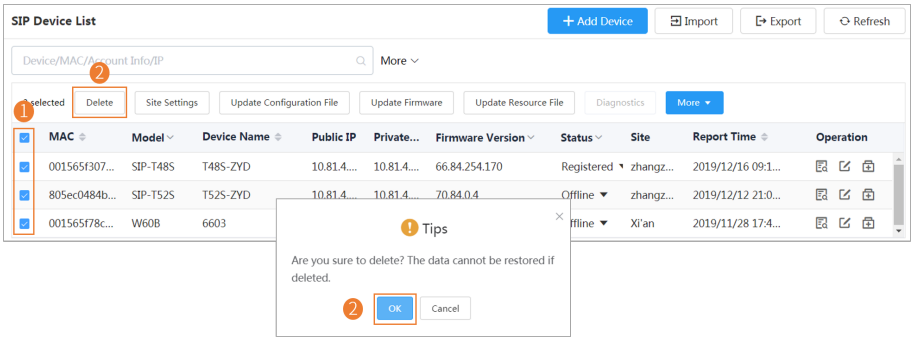
Note:

- After you reset the device, the device status becomes offline on YDMP. You need to re-deploy the device (*Connecting SIP Device*) to make the device connect to YDMP.
- If you do not delete the reset devices on YDMP, when the devices are reconnected to YDMP, they will automatically obtain the configuration saved on YDMP.

Deleting Devices

Procedure

1. Click **Device Management** > **SIP Device List**.
2. Select the corresponding devices and click **Delete**.
3. Click **OK**.



Managing USB Devices

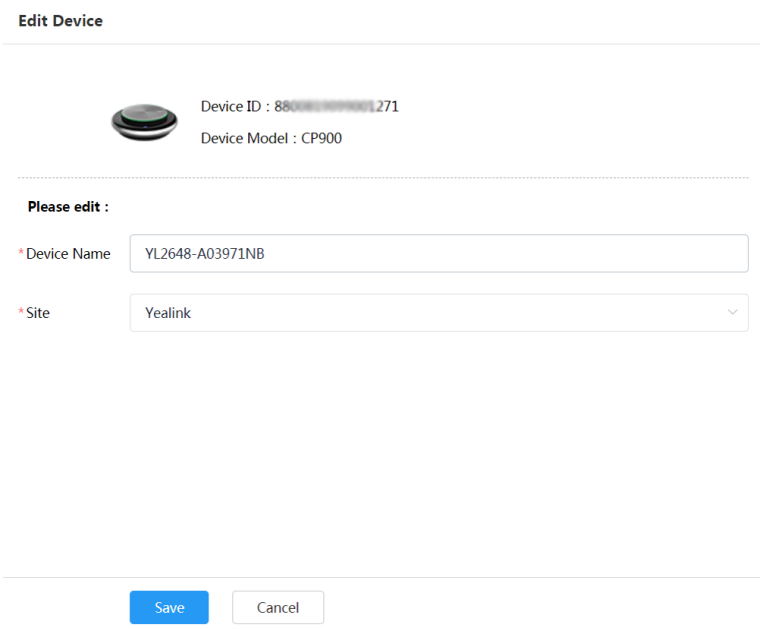
- *Editing the Device Information*
- *Exporting the Device Information*
- *Viewing the USB Device*
- *Searching for Devices*
- *Setting the Sites*
- *Deleting Devices*

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** > **USB Device List**.
2. Click beside the desired device.
3. Edit the device information and save it.



Exporting the Device Information

You can export the basic information of all devices.

Procedure

Click **Device Management** > **USB Device ListImport**.

Viewing the USB Device

You can view the information of the USB device, including the model, the device ID, the device name, the IP, the firmware version, the status, the site and the report time.

Procedure

Click **Device Management** > **USB Device List**.

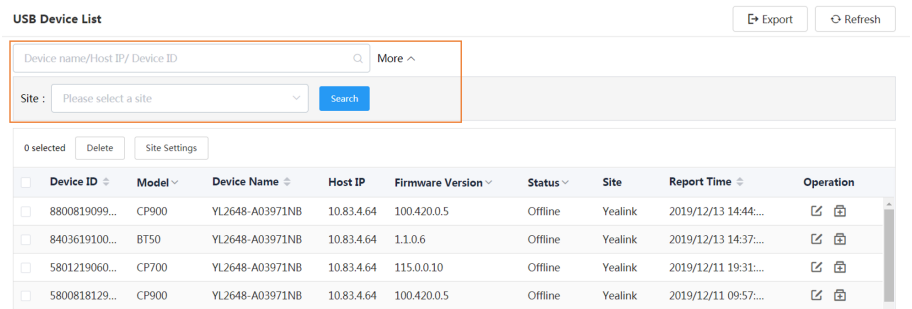
You can click **Refresh** in the top-right corner to obtain the latest device information,

Searching for Devices

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

Procedure

Click **Device Management** > **USB Device List**.



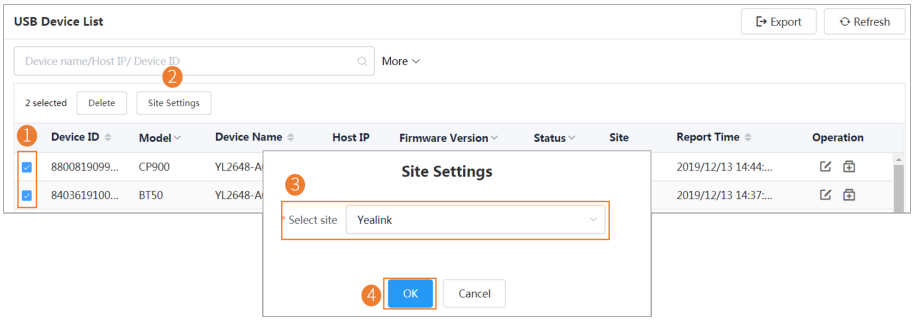
The search results are displayed in the list.

Setting the Sites

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

Procedure

Click **Device Management** > **USB Device List**.



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

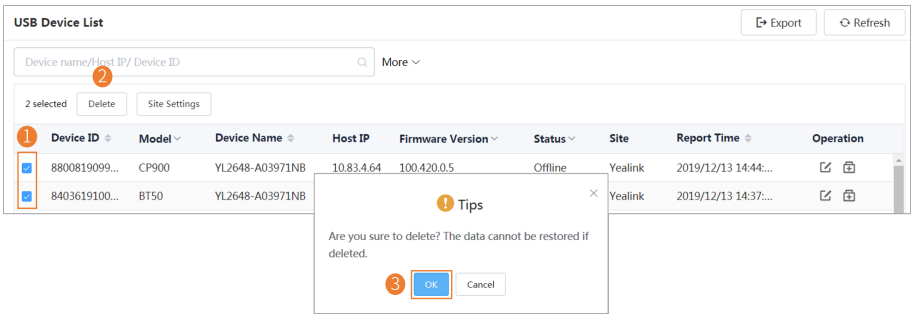
Related tasks

Adding Sites

Deleting Devices

Procedure

1. Click **Device Management** > **USB Device List**.
2. Select the corresponding devices and click **Delete**.
3. Click **OK**.



Managing Room System

- *Editing the Device Information*
- *Viewing the Information of the Room System*
- *Searching for Devices*
- *Setting the Sites*
- *Rebooting Devices*
- *Pushing Firmware to Devices*

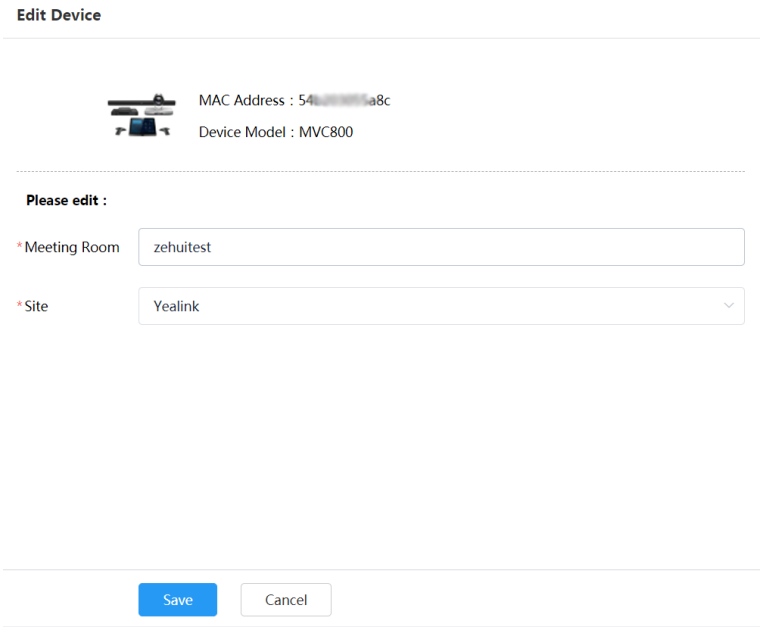
- *Resetting the Devices to Factory*
- *Deleting Devices*

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** > **Room System**.
2. Click beside the desired device.
3. Edit the device information and save it.

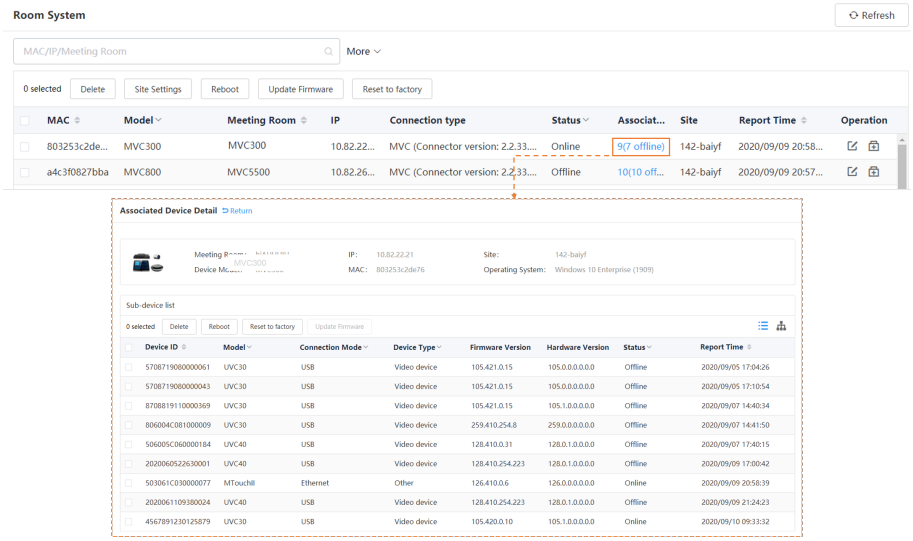


Viewing the Information of the Room System

You can view the information of 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.

Procedure

1. Click **Device Management** > **Room System**.
   You can click **Refresh** in the top-right corner to obtain the latest device information,
2. Optional: Click the blue font under the **Associated Device** tab and you can view the detailed information of the associated device of the room system.

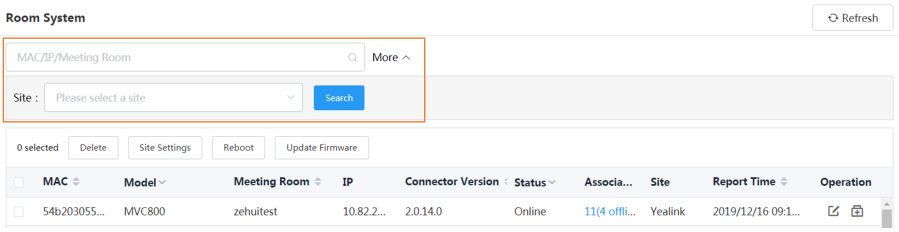


Searching for Devices

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

Procedure

Click **Device Management** > **Room System**.



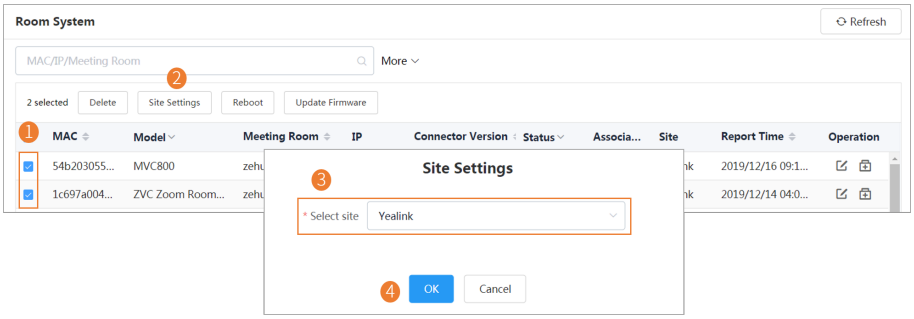
The search results are displayed in the list.

Setting the Sites

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

Procedure

Click **Device Management** > **Room System**.



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

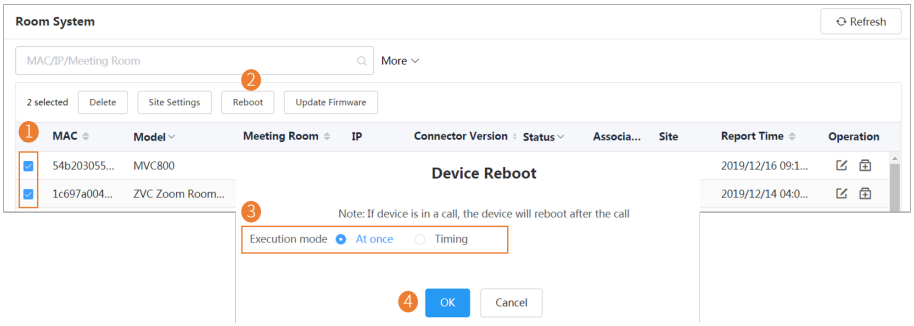
Related tasks

Adding Sites

Rebooting Devices

Procedure

1. Click **Device Management** > **Room System**.
2. Select the corresponding devices and click **Reboot**.
3. According to the prompts, select the desired execution mode, and click **OK**.



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

Pushing Firmware to Devices

Before you begin

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

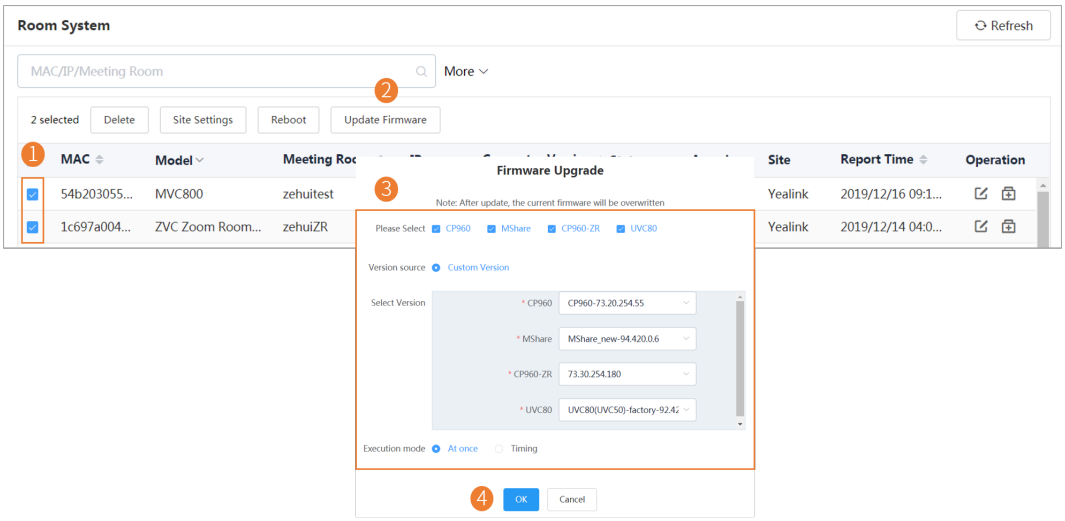
About this task

- 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** > **Room System**.
2. Push the firmware to the selected 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 Tasks* .

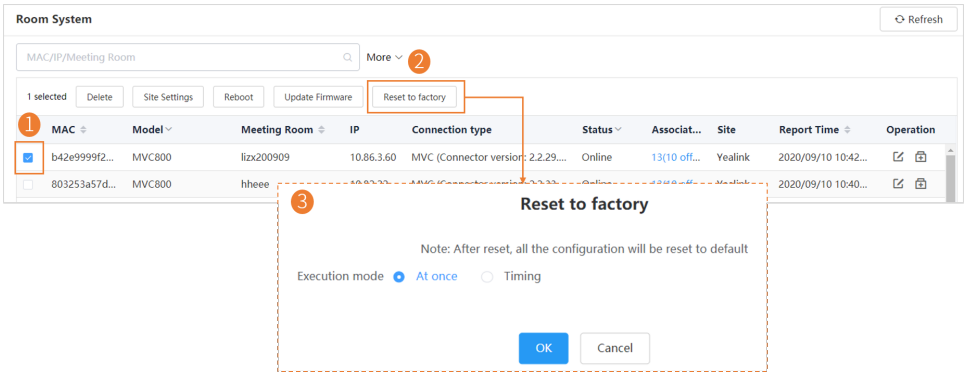
Related concepts

Managing Firmware

Resetting the Devices to Factory

Procedure

1. Click **Device Management** > **Room System**.
2. Select the corresponding devices and click **Reset to factory**.
3. According to the prompts, select the desired execution mode, and click **OK**.

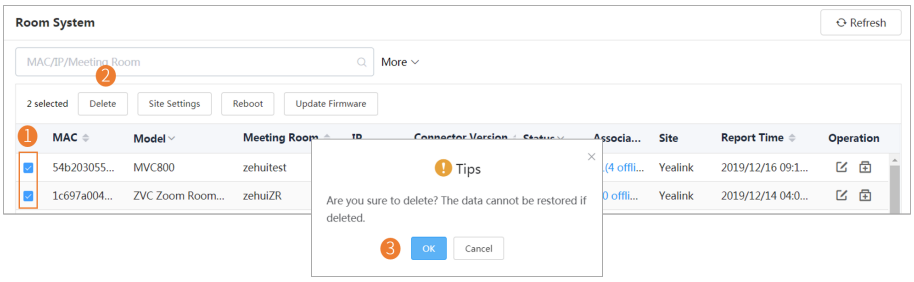


Note: After resetting the device, you can see the task details, refer to *Viewing Tasks* .

Deleting Devices

Procedure

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



Managing Firmware

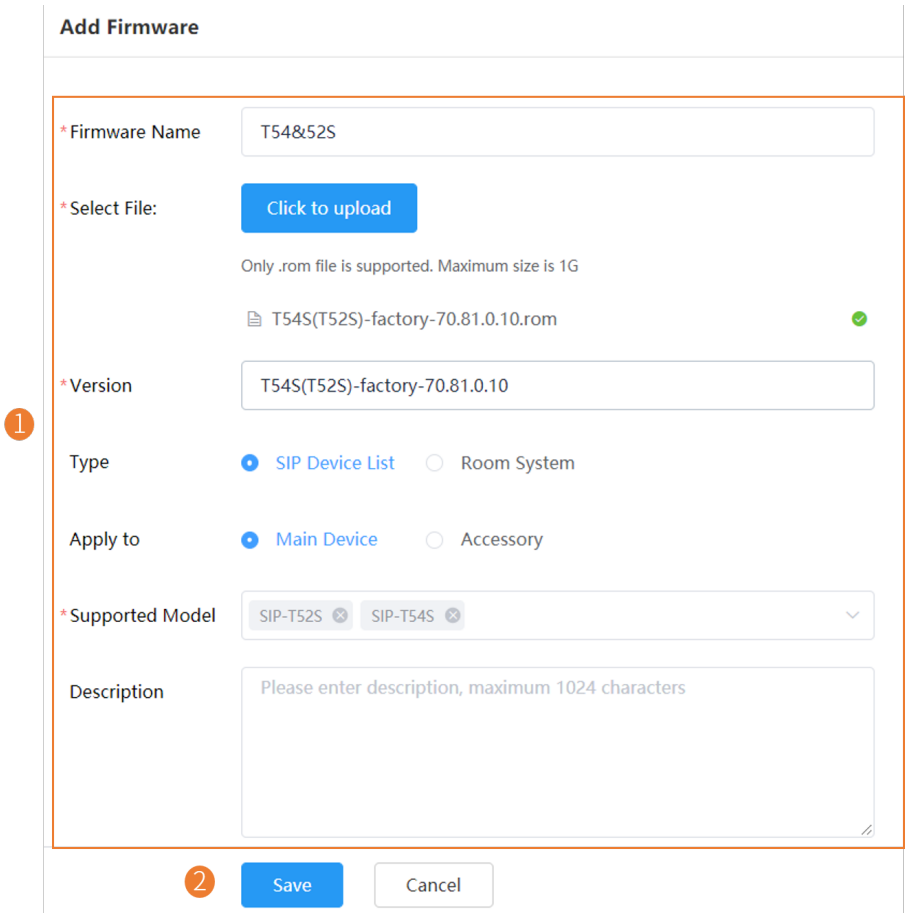
You can manage all the device firmware on YDMP.

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

Adding Firmware

Procedure

1. Click **Device Management** > **Firmware Management** > **Add Firmware**.
2. Enter the corresponding information and save it.

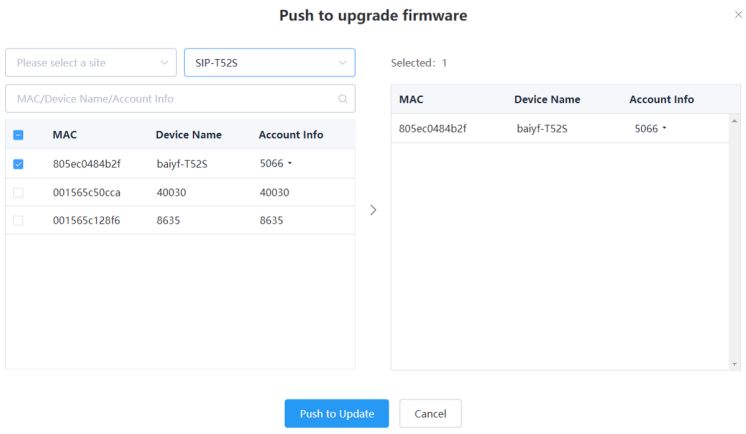


Pushing Firmware to Devices

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.

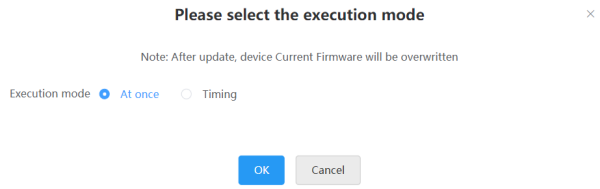
Procedure

1. Click **Device Management** > **Firmware Management**.
2. Click beside the desired firmware.
3. Select the desired devices in the pop-up window.



4. Click **Push to Update**.

5. 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.

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 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 **Device Management** > **Firmware Management**.
2. Click beside the desired firmware.
3. Edit the corresponding information.
4. Click **Confirm**.

Downloading the Firmware

Procedure

1. Click **Device Management** > **Firmware Management**.
2. Click beside the desired firmware.
3. The file will be downloaded to your computer.

Deleting Firmware

Procedure

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

Results

After the firmware is deleted, the scheduled task associated with this firmware will fail to execute.

Managing Resources

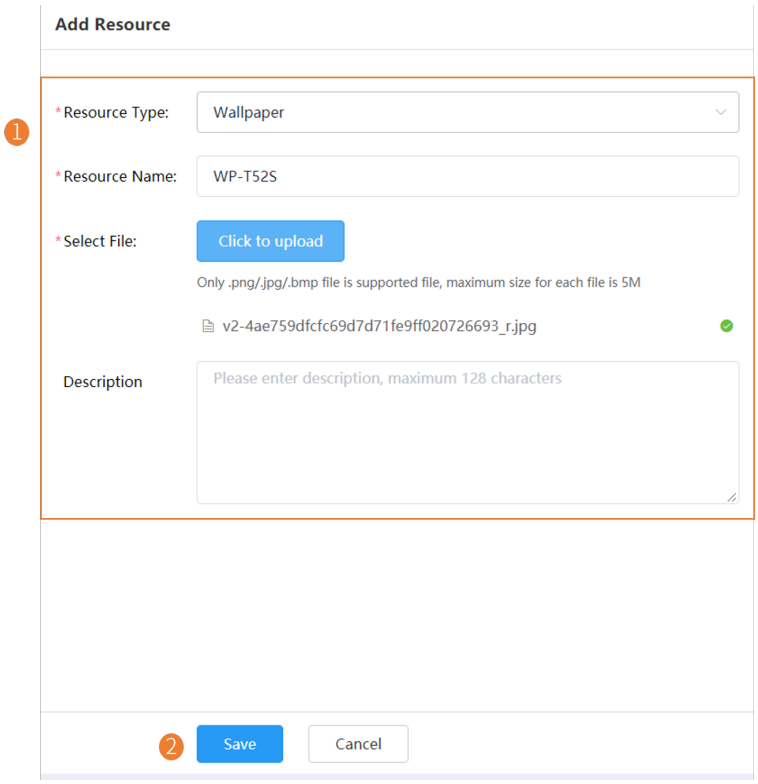
You can add and edit resource files, push resource files to devices or download them to your local system.

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

Adding Resource Files

Procedure

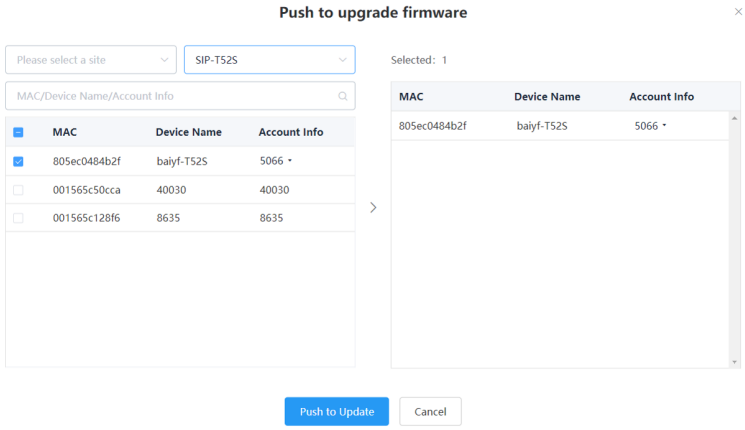
1. Click **Device Management Resource ManagementAdd Resource**.
2. Add a resource file.



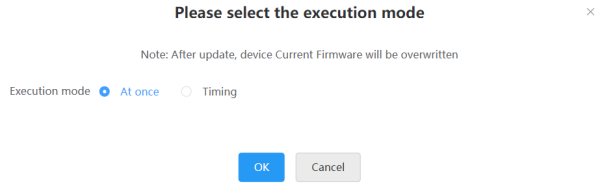
Pushing Resource Files to Devices

Procedure

1. Click **Device Management** > **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 Tasks* .

Editing Resource Files

Procedure

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

Deleting Resource Files

Procedure

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

Results

After the resource is deleted, the scheduled task associated with this resource file will fail to execute.

Managing Accounts

You can manage different devices on YDMP. 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*
- *Importing Accounts*
- *Editing the Account Information*
- *Exporting Accounts*
- *Deleting Accounts*

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 H.323 account**.
3. Configure the account information.
4. Click **Confirm**.

Related tasks

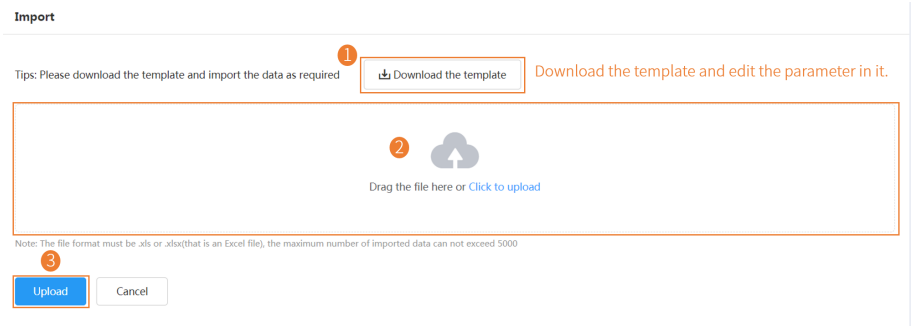
Assigning Accounts to Devices

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 YDMP.

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 H.323 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**.

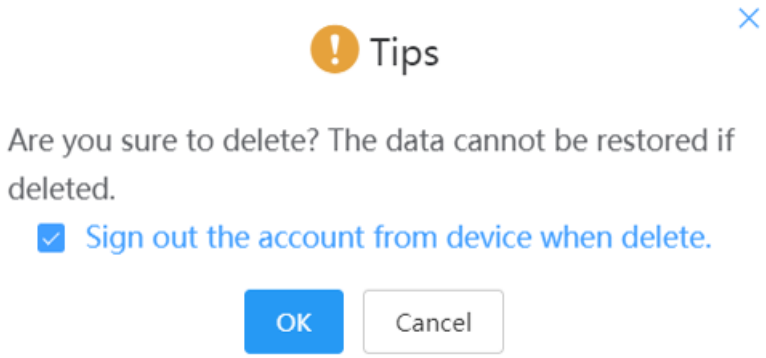
   The files are automatically saved to the local system, then you can view the basic information of all accounts.

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 YDMP and signed out from the device. If you select **Sign out the account from device when delete**, the account will only be deleted from YDMP 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 YDMP, for example, creating or pushing the configuration file.

Introduction of obtaining the configuration:

- **Automatically obtaining the configuration:**

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

  - When you connect the device to the platform for the first time
  - When you reset the device (It is only applicable to devices in version 84 or later. For the detailed device version, contact Yealink technical support.)

  The priority of obtaining the configuration in ascending order is 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 YDMP, they would not automatically obtain the updated configuration. Therefore, you need to push the configuration to them.

- *Managing Model Configuration*
- *Managing the Site Configuration*
- *Managing the Group Configuration*
- *Managing the MAC Configuration*
- *Configuring Global Parameters*

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*
- *Setting Parameters*

- *Pushing Configuration to Devices*
- *Editing Configuration Templates*
- *Downloading the Model File*
- *Viewing Parameters*
- *Deleting Templates*

Adding Configuration Templates

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

Procedure

1. Click **Device Configuration** > **Model Configuration** > **Add Template**.
2. Set and save the parameters.

Setting Parameters

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.

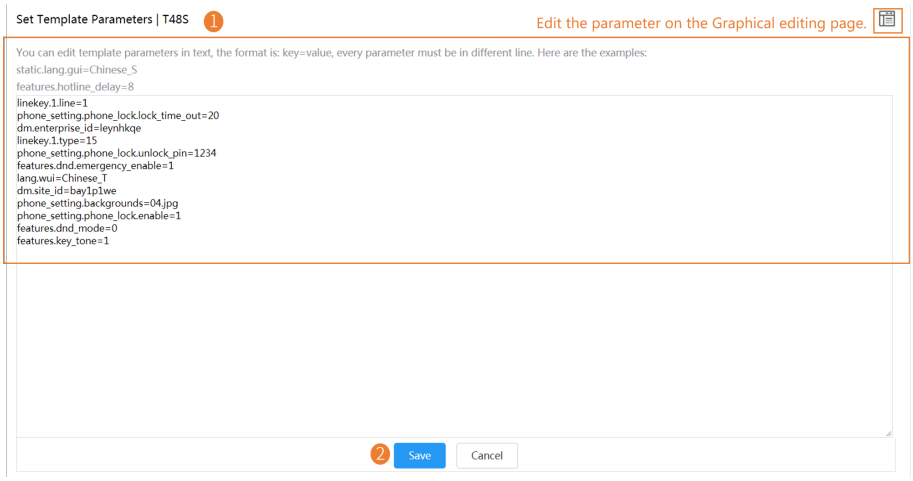
- *Setting Parameters in the Text*
- *Setting Parameters on the Graphical Editing Page*

Setting Parameters in the Text

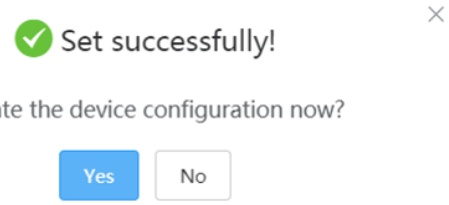
You can customize any parameters supported by the devices in the text and push the parameters to the device after editing.

Procedure

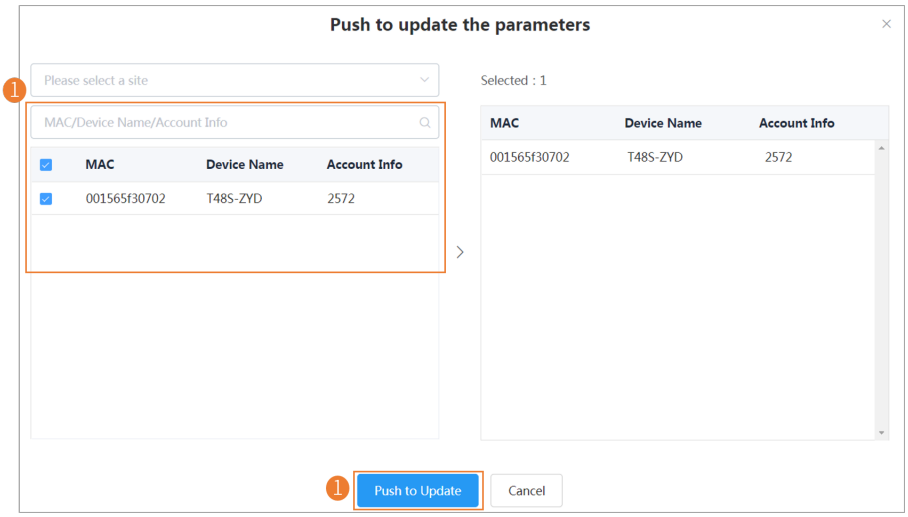
1. Click **Device Configuration** > **Model Configuration**.
2. Click "" on the right side of the desired template, and select **Edit Parameters in text** from the drop-down menu.
3. Set and save the parameters.



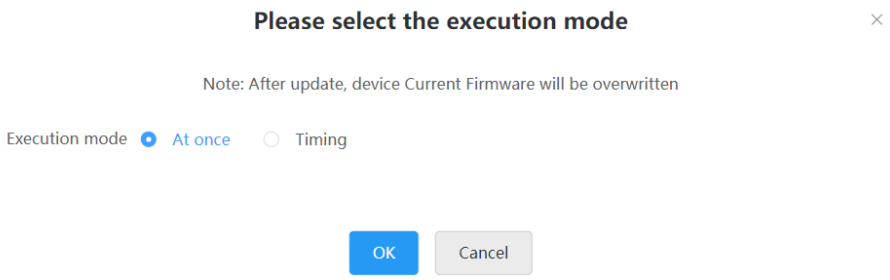
4. On the pop-up window, select **Yes** to push the edited configuration immediately, or **No** to save the edited configuration.



5. Push the selected configuration.



6. Select the desired execution mode.



Note:

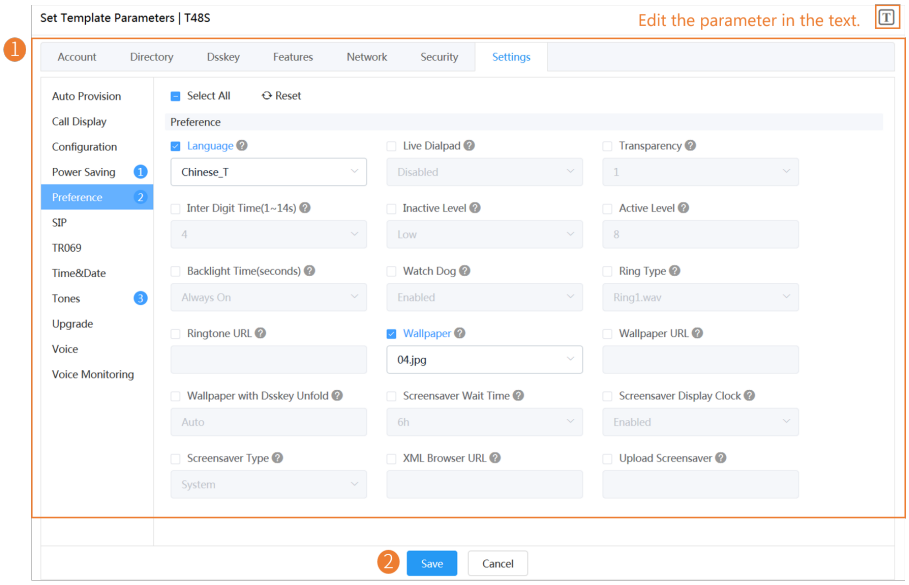
- If you select **At once**, the configuration will be pushed to the selected devices immediately.
- If you select **Timing**, the configuration will be pushed to the selected devices at the time you set.
- If the edited templates are involved, the scheduled tasks will be executed according to the last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

Setting Parameters on the Graphical Editing Page

You can edit the parameter supported in the template, and push the edited parameter to the device.

Procedure

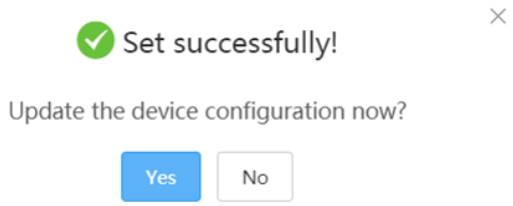
1. Click **Device Configuration** > **Model Configuration**.
2. Click beside the desired template.
3. Set and save the parameters.



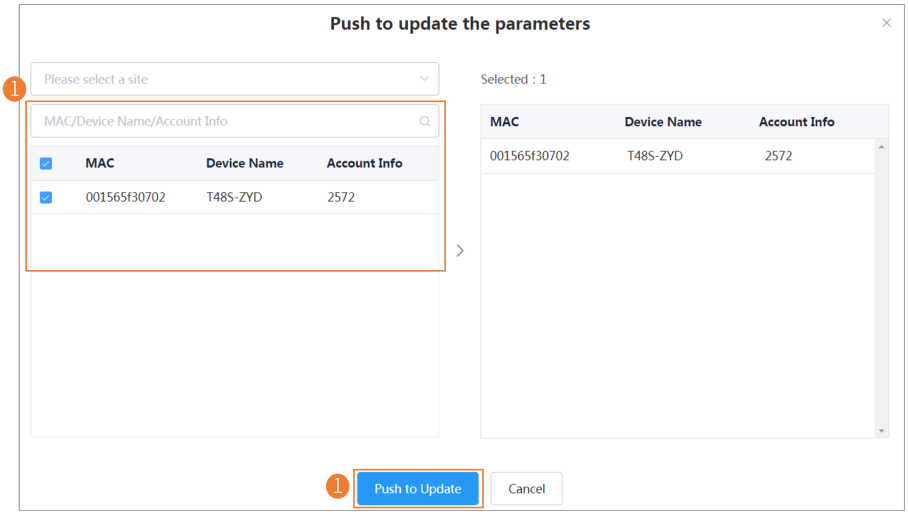
Tip:

- You can select the edited configuration, and push it to the desired devices.
- You can click **Reset** to reset the configuration on this page to the value before modification.

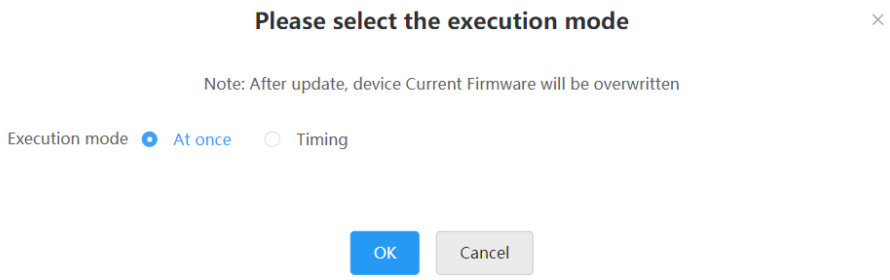
4. On the pop-up window, select **Yes** to push the edited configuration immediately, or **No** to save the edited configuration.



5. Push the selected configuration.



6. Select the desired execution mode.



Note:

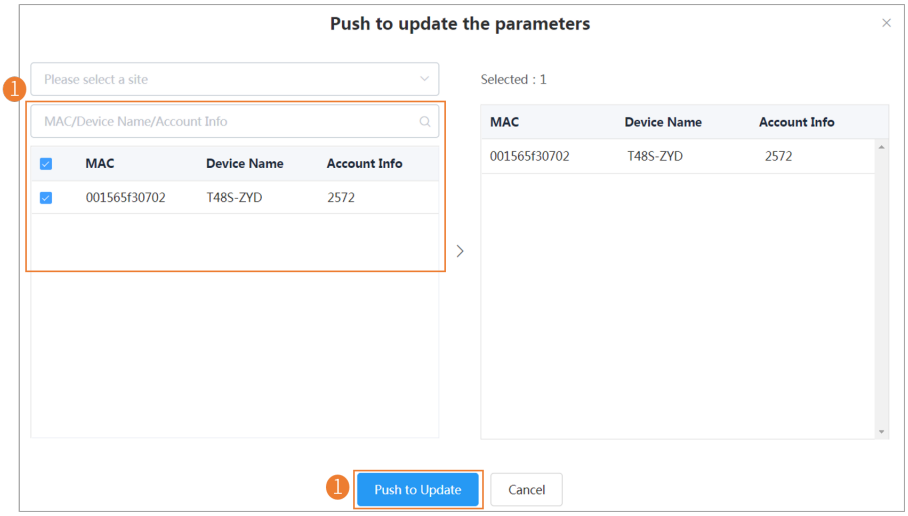
- If you select **At once**, the configuration will be pushed to the selected devices immediately.
- If you select **Timing**, the configuration will be pushed to the selected devices at the time you set.
- If the edited templates are involved, the scheduled tasks will be executed according to the last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

Pushing Configuration to Devices

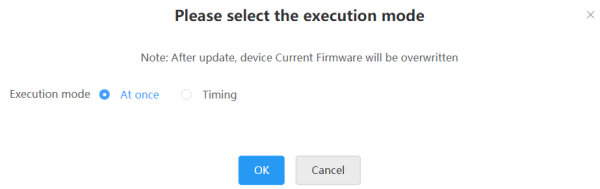
You can push the configuration to devices if you have updated the configuration in the text or in the template.

Procedure

1. Click **Device Configuration** > **Model Configuration**.
2. Click beside the desired template.
3. Push the selected configuration.



4. Select the desired execution mode.



Note:

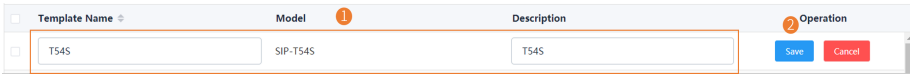
- You can also select the desired devices in the Device List, click **Update Configuration File**, select **Update CFG by model template** to update.
- After updating the configuration file, you can see the task details, refer to *Viewing Tasks* .

Editing Configuration Templates

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 Configuration**.
2. Click ··· on the right side of the desired template, and select **Edit Template** from the drop-down menu.
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

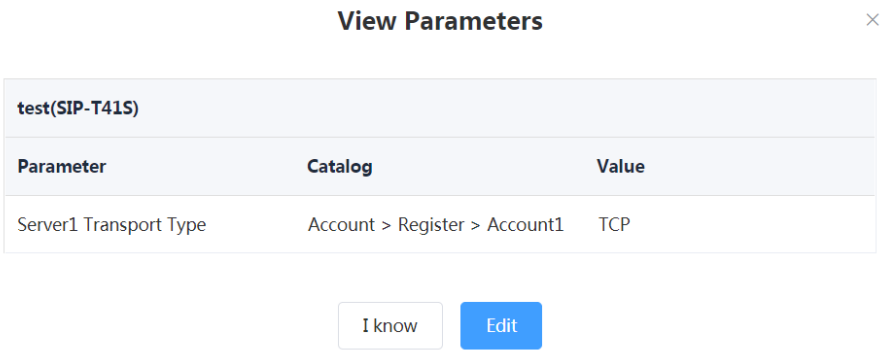
1. Click **Device Configuration** > **Model Configuration**.
2. Click ··· on the right side of the desired template, and select **Download config file** from the drop-down menu.

Viewing Parameters

You can view the configured parameter in the template but the parameters you customize in the text are not displayed in the template.

Procedure

1. Click **Device Configuration** > **Model Configuration**.
2. Click beside the desired template to view the parameters.



You can also click **Edit** to edit the parameters in the text.

Deleting Templates

Procedure

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

Results

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

Managing the Site Configuration

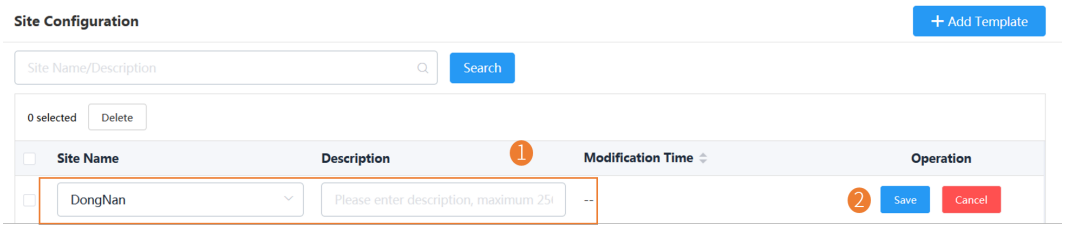
You can customize and manage the configuration according to the site that the devices belong to. Site configuration applies to all the offline devices in the site and its sub-sites.

- *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 and save the parameters.



Setting Parameters

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.

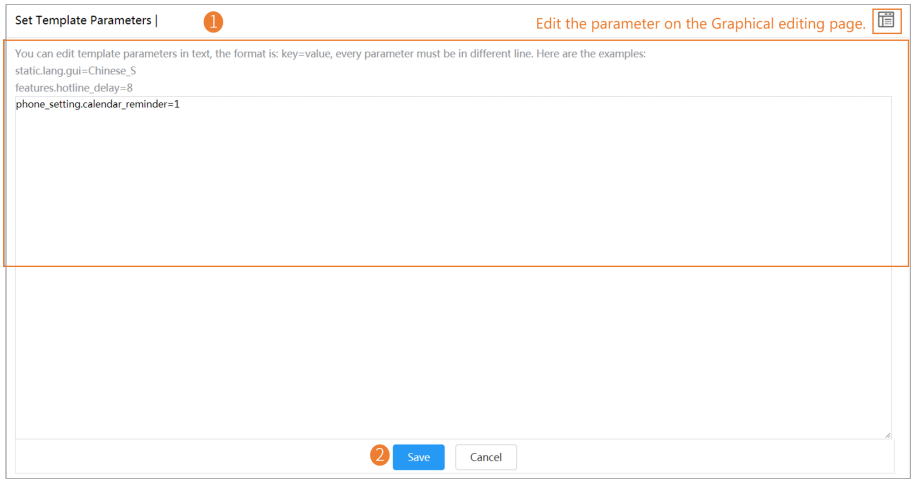
- *Setting Parameters in the Text*
- *Setting Parameters on the Graphical Editing Page*

Setting Parameters in the Text

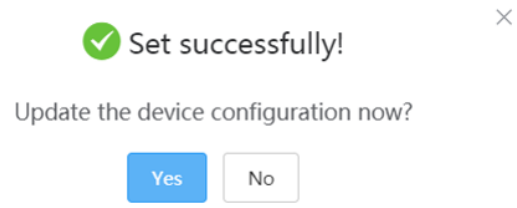
You can customize any parameters supported by the devices in the text and push the parameters to the device after editing.

Procedure

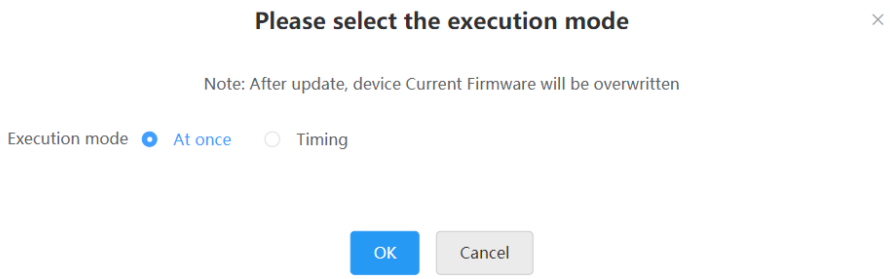
1. Click **Device Configuration** > **Site Configuration**.
2. Click ··· on the right side of the desired template, and select **Edit Parameters in text** from the drop-down menu.
3. Set and save the parameters.



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.



Note:

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

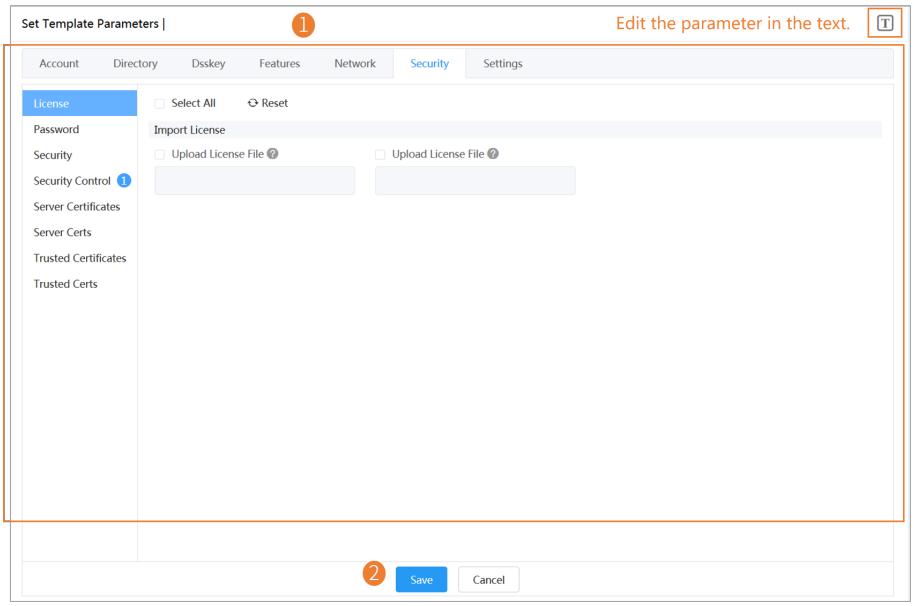
- If the edited templates are involved, the scheduled tasks will be executed according to the last template that you edit and save.

Setting Parameters on the Graphical Editing Page

You can edit the parameter supported in the template, and push the edited parameter to the device.

Procedure

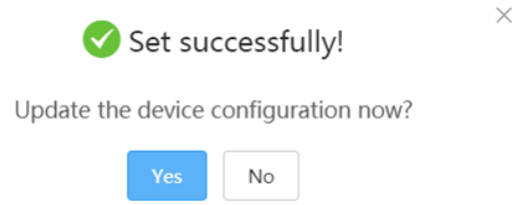
1. Click **Device Configuration** > **Site Configuration**.
2. Click beside the desired template.
3. Set and save the parameters.



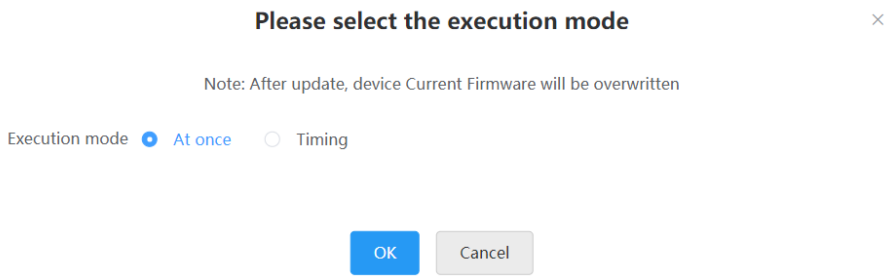
Tip:

- You can select the edited configuration, and push it to the desired devices.
- You can click **Reset** to reset the configuration on this page to the value before modification.

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.



Note:

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

Pushing the Site Configuration to Devices

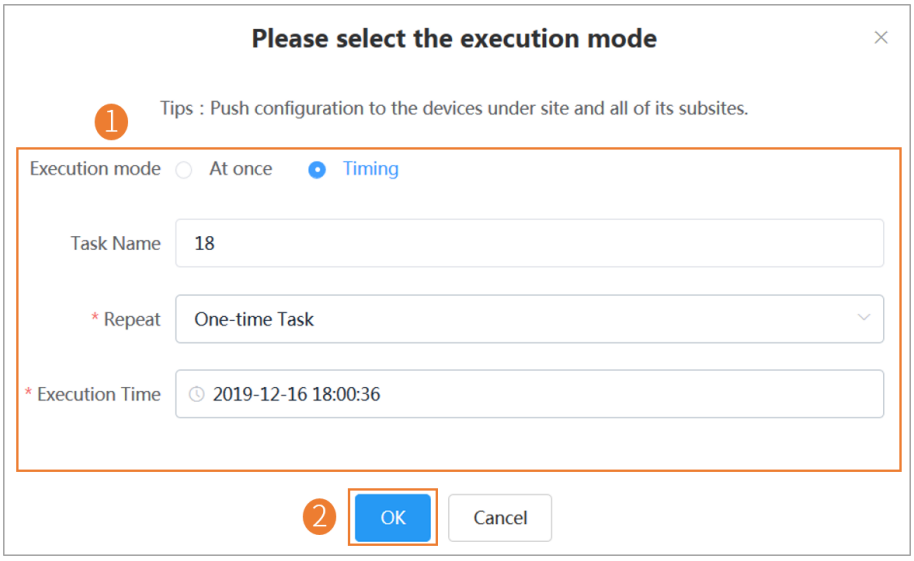
You can select the desired configuration and push it to all the devices in the corresponding site and the sub-sites.

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 a desired execution mode on the pop-up window.



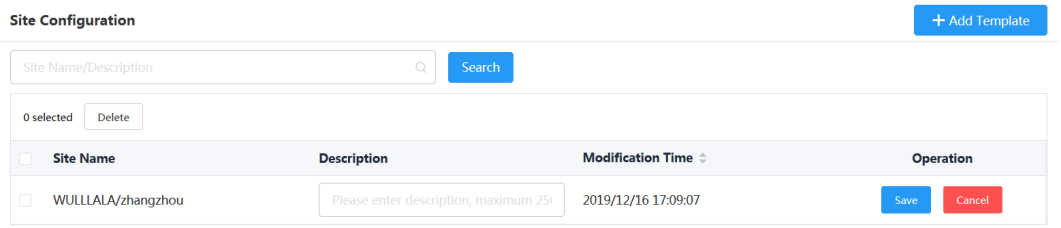
Note: After updating the configuration file, you can see the task details, refer to *Viewing Tasks* .

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, and select **Edit Template** from the drop-down menu.
3. Edit and save the description.



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, and select **Download config file** from the drop-down menu.

Deleting Site Configuration Templates

Procedure

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

Results

After you delete the template, the scheduled 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 Groups*
- *Pushing the Group Configuration*
- *Viewing Parameters*

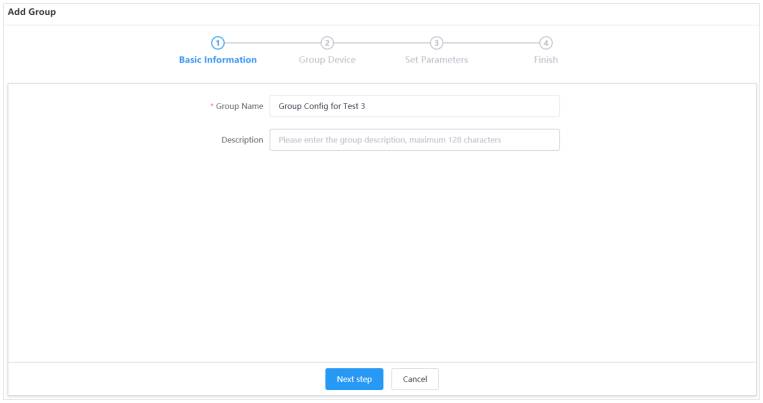
- *Downloading Configuration File*
- *Deleting Groups*

Adding the Group Configuration

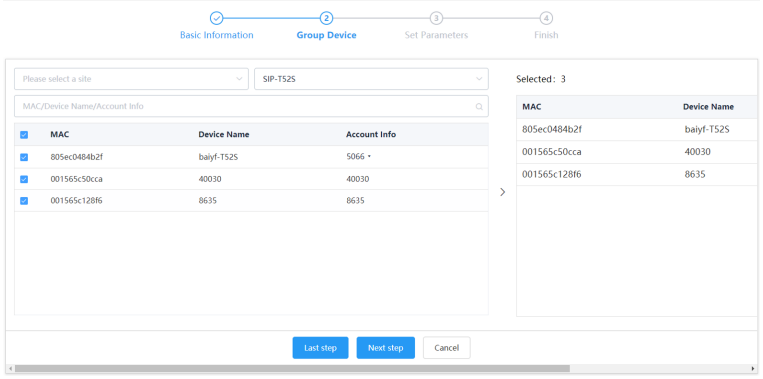
You can add the name and description, select devices, and customize the device setting for a group configuration.

Procedure

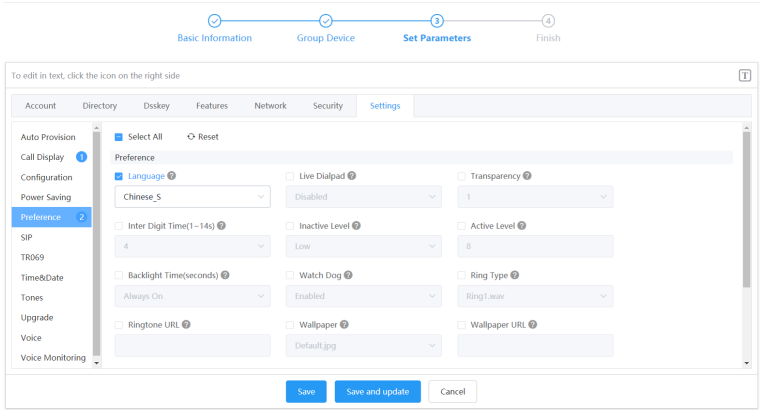
1. Click **Device Configuration** > **Group Configuration** > **Add Group**.
2. Enter the information.



3. Optional: Select the desired device to the group.



4. Set the parameters.



5. Click **Save** to only save the configuration, or click **Save and update** to push the updated parameters to the selected devices.

Setting Parameters

You can choose one of the following methods to configure the group 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.

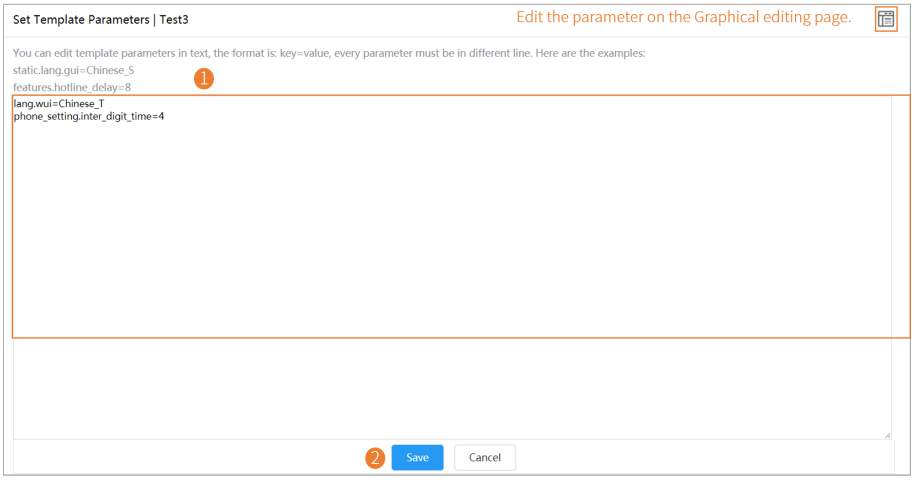
- *Setting Parameters in the Text*
- *Setting Parameters on the Graphical Editing Page*

Setting Parameters in the Text

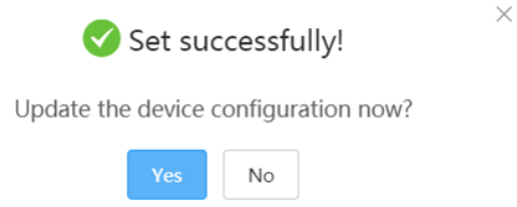
You can customize any parameters supported by the devices in the text and push the parameters to the device after editing.

Procedure

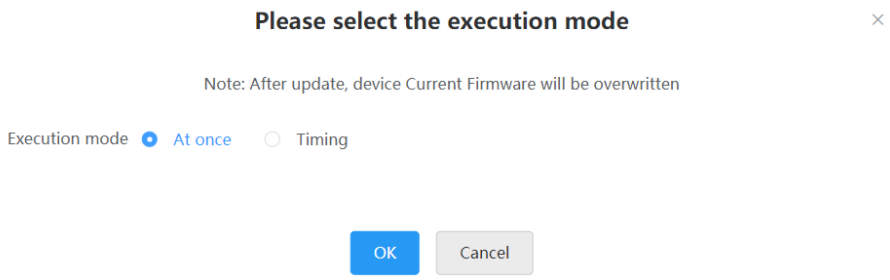
1. Click **Device Configuration** > **Group Configuration**.
2. Click "" on the right side of the desired template, and select **Edit Parameters in text** from the drop-down menu.
3. Set and save the parameters.



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.



Note:

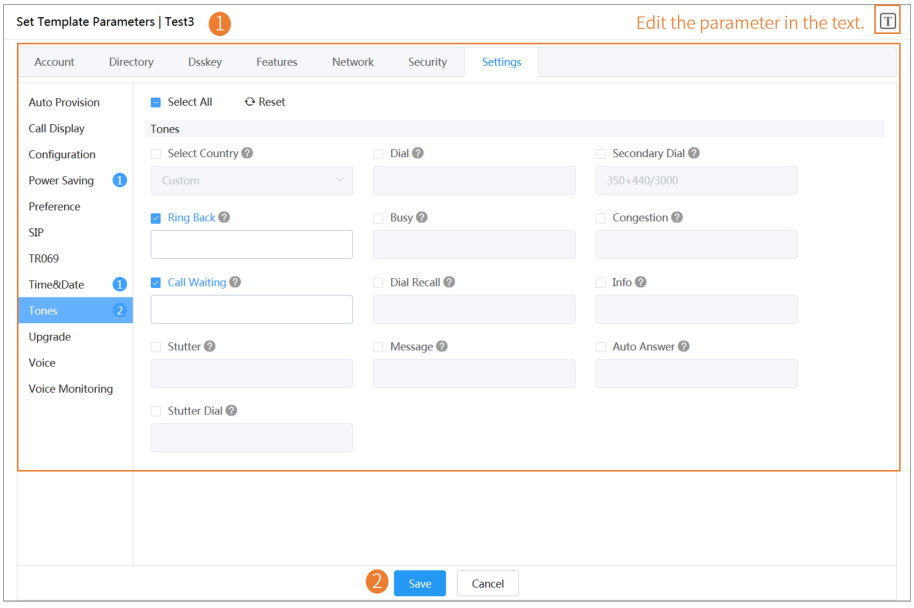
- If you select **At once**, the configuration will be pushed to all the devices in this group immediately.
- If you select **Timing**, the configuration will be pushed to all the devices in this group at the time you set.
- If the edited templates are involved, the scheduled tasks will be executed according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

Setting Parameters on the Graphical Editing Page

You can edit the parameter supported in the template, and push the edited parameter to the device.

Procedure

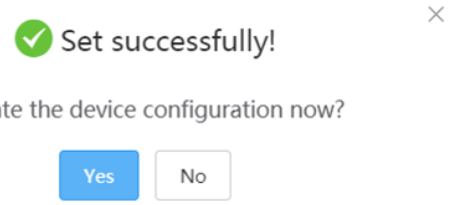
1. Click **Device Configuration** > **Group Configuration**.
2. Click beside the desired template.
3. Set and save the parameters.



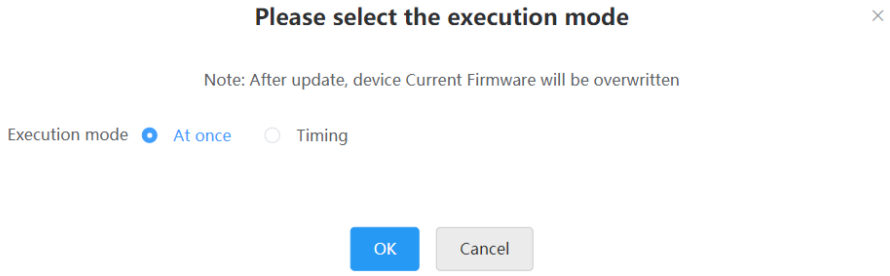
Tip:

- You can select the edited configuration, and push it to the desired devices.
- You can click **Reset** to reset the configuration on this page to the value before modification.

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.



Note:

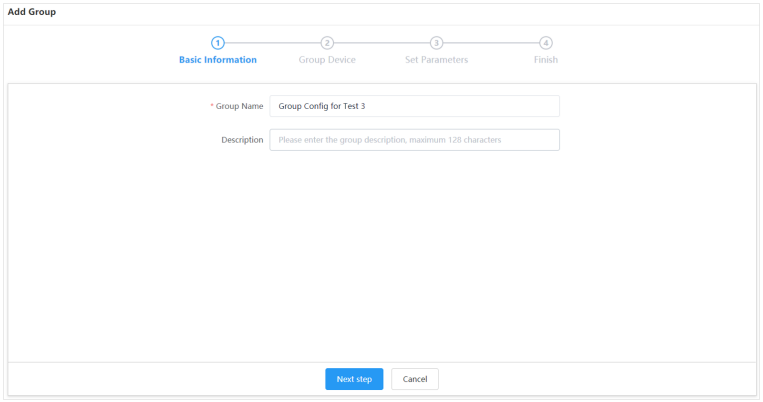
- If you select **At once**, the configuration will be pushed to all the devices in this group immediately.
- If you select **Timing**, the configuration will be pushed to all the devices in this group at the time you set.
- If the edited templates are involved, the scheduled tasks will be executed according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

Editing Groups

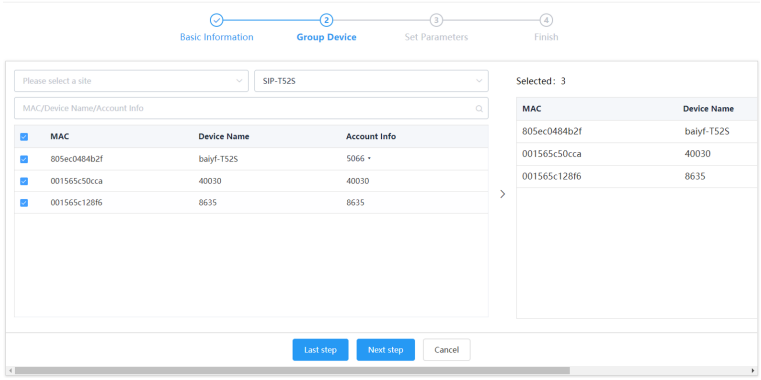
You can edit the name and the description, reselect the devices and reset the device parameters for the group.

Procedure

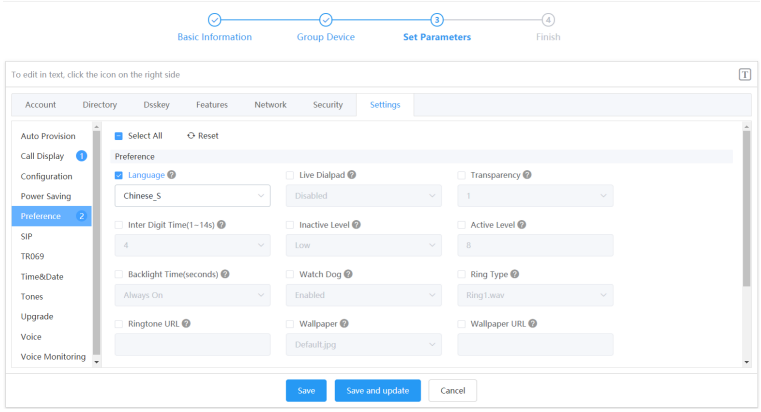
1. Click **Device Configuration** > **Group Configuration**.
2. Click ··· on the right side of the desired template, and select Edit Group from the drop-down menu.
3. Edit the information.



4. Select the desired device to the group.



5. Edit the device parameters.



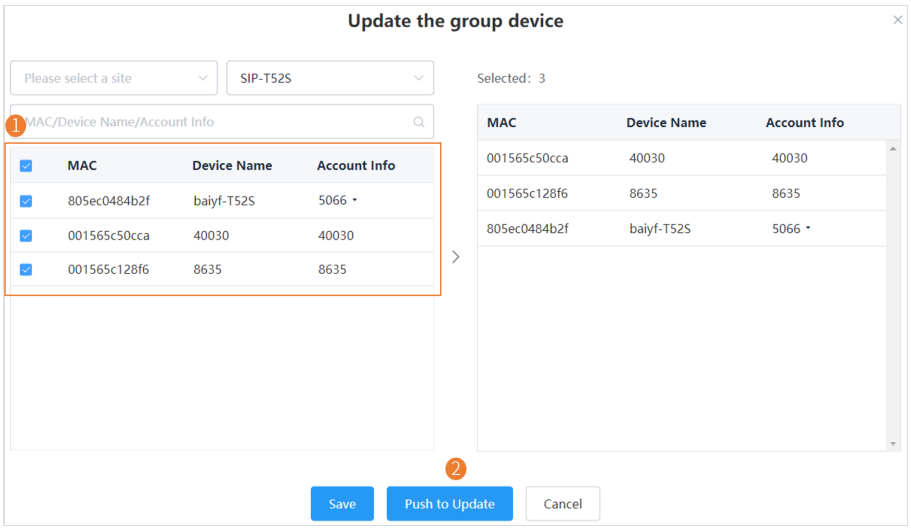
6. Click **Save** to only save the configuration, or click **Save and update** to push the updated parameters to the selected devices.

Pushing the Group Configuration

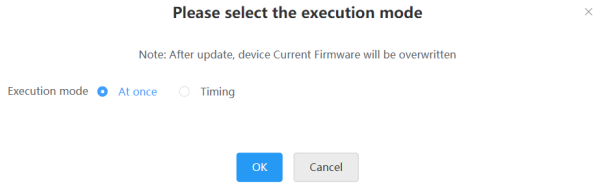
When you need to add or remove devices in your group, you can update the group device and choose to save the group configuration directly or push the parameters to the selected devices immediately.

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Click beside the desired group.
3. Select the desired device.



4. Select the desired execution mode.



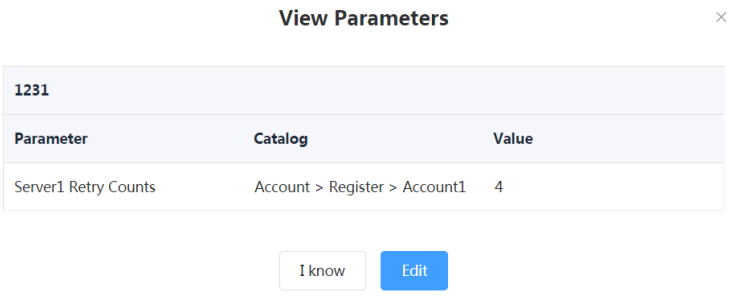
Note: After updating the configuration file, you can see the task details, refer to *Viewing Tasks* .

Viewing Parameters

You can view the configured parameter in the template but the parameters you customize in the text are not displayed in the template.

Procedure

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



You can click **Edit** to edit the parameters.

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, and select **Download config file** from the drop-down menu.

Deleting Groups

Procedure

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

Results

After you delete the template, the scheduled 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.

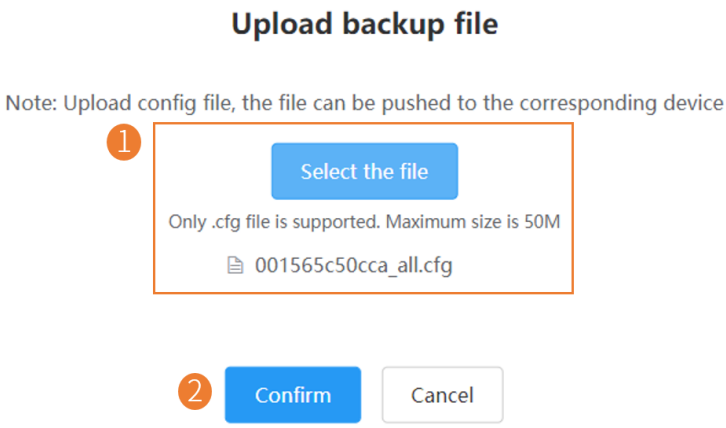
- *Uploading Backup Files*
- *Generating Configuration Files*
- *Setting Parameters*
- *Pushing Backup Files to Devices*
- *Downloading the Configuration Files*
- *Exporting the Configuration Files*
- *Deleting Backup Files*

Uploading Backup Files

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

Procedure

Click **Device Configuration** > **MAC Configuration** > **Upload backup files**.

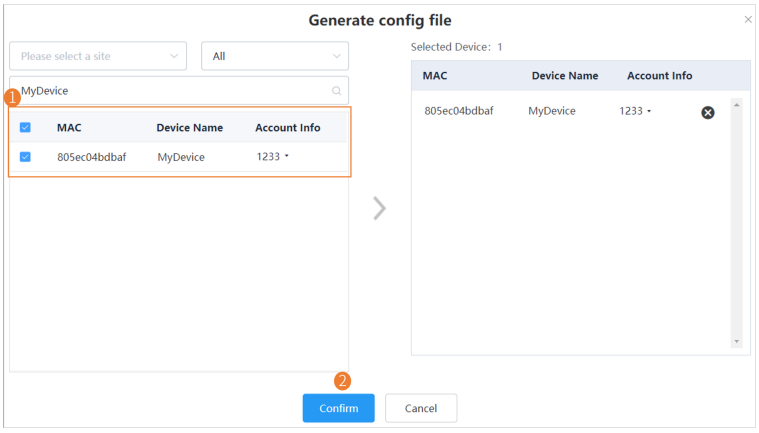


Generating Configuration Files

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

Procedure

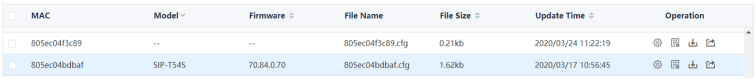
1. Click **Device Configuration** > **MAC Configuration** > **Generate config file**.
2. Select the desired devices on the pop-up window and click **Confirm**.



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:



Setting Parameters

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.

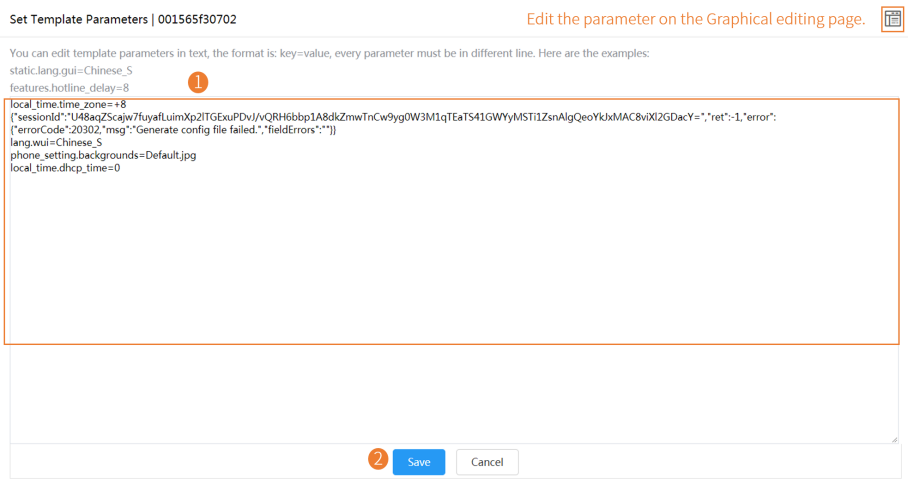
- *Setting Parameters in the Text*
- *Setting Parameters on the Graphical Editing Page*

Setting Parameters in the Text

You can customize any parameters supported by the devices in the text.

Procedure

1. Click **Device Configuration** > **MAC Configuration**.
2. Click beside the desired template.
3. Set and save the parameters.

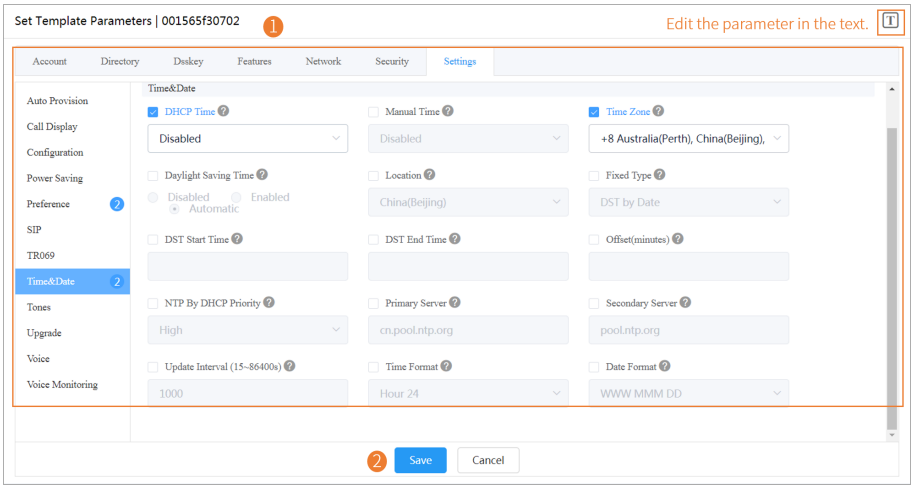


Setting Parameters on the Graphical Editing Page

You can edit the parameter supported in the template.

Procedure

1. Click **Device Configuration** > **MAC Configuration**.
2. Click beside the desired template.
3. Set and save the parameters.



Tip:

- You can select the edited configuration, and push it to the desired devices.
- You can click **Reset** to reset the configuration on this page to the value before modification.

Pushing Backup Files to Devices

Procedure

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

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

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 scheduled 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**.
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 Tasks* .

Managing Sites

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

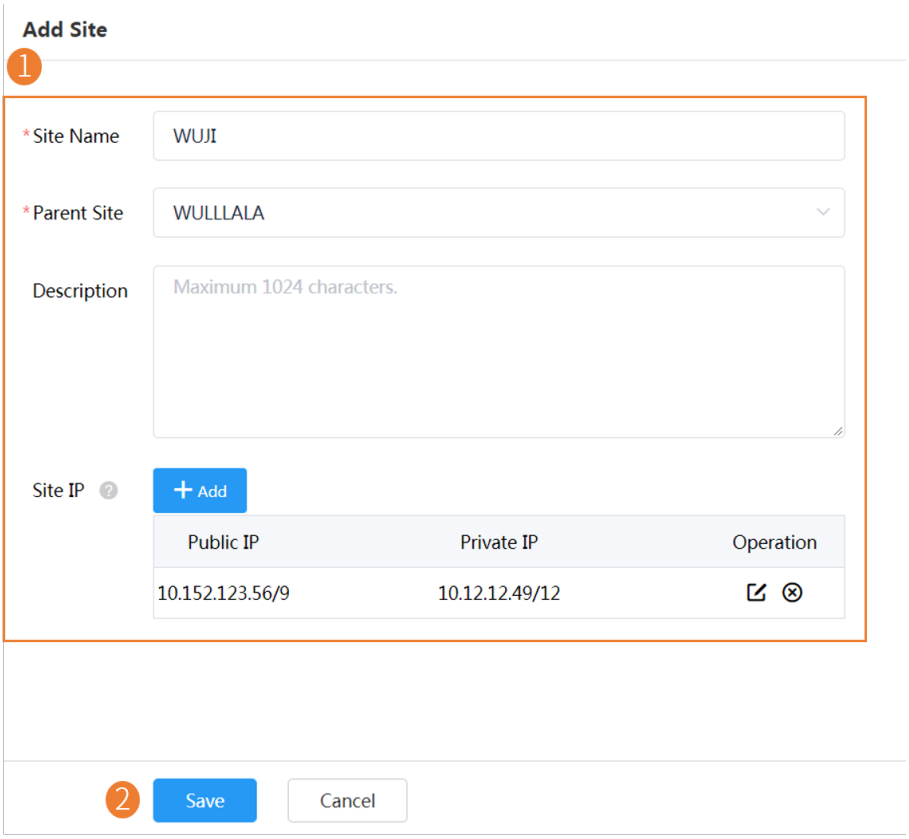
Note: The default site named after your company name is added when the system is initialized.

- *Adding Sites*
- *Importing Sites*
- *Editing Sites*
- *Deleting Sites*

Adding Sites

Procedure

1. Click **Site ManagementAdd 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:

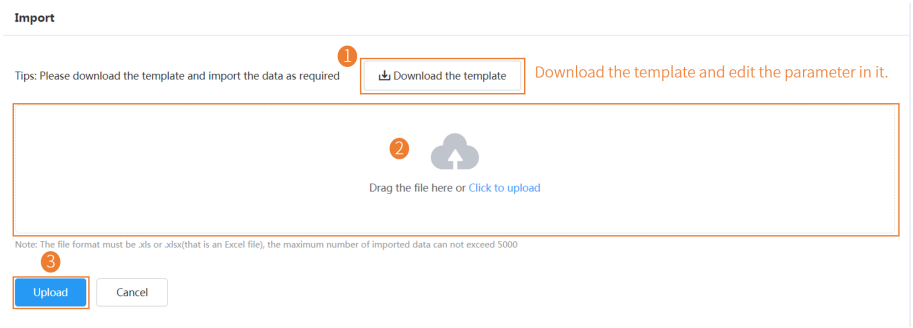
- The priority (the devices automatically connected to the site) in the descending order is site IP setting, the site setting in the Common.cfg file, the site setting in importing a batch of devices.
- When a device is in the IP range of a sub-site and a superior site, the device goes to the sub-site 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 YDMP.

Procedure

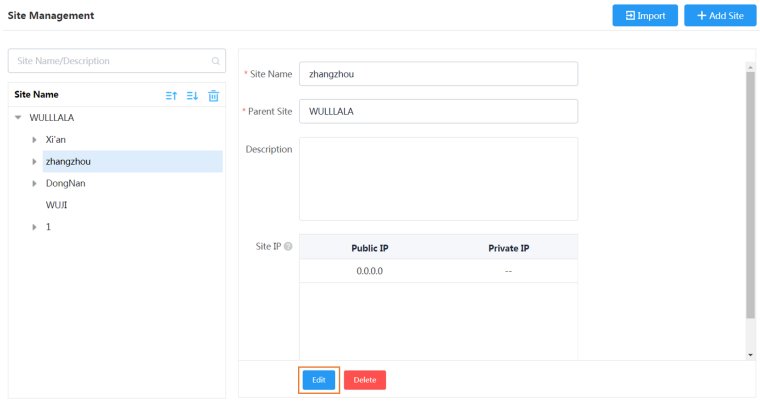
Click **Site ManagementImport**.



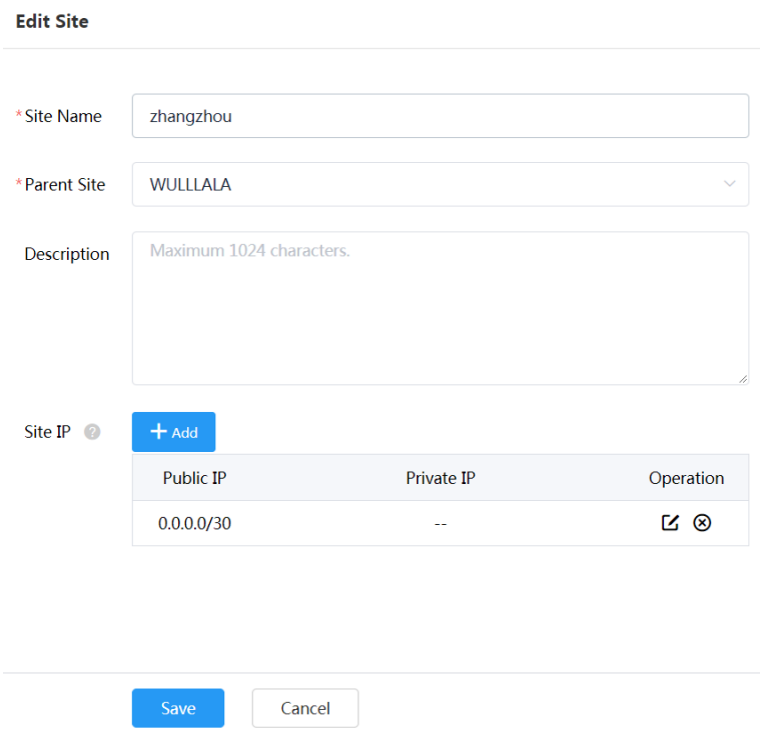
Editing Sites

Procedure

1. Click **Site Management**.
2. Select a desired site in the Site Name list, and click **Edit**.



3. Set and save the parameters.



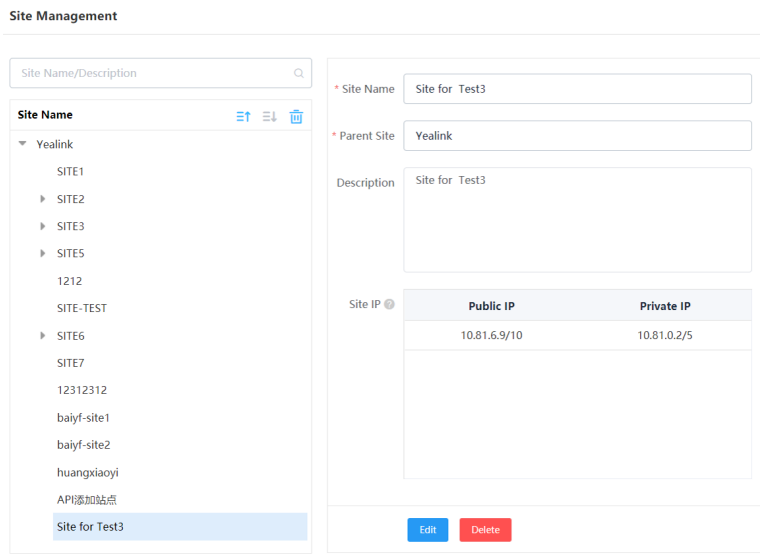
Deleting Sites

About this task

- You can delete sites created by your own, but you cannot delete the default site named after your company name.
- The site cannot be deleted if there are devices under it.
- If a site does not have any sub-sites and the sub-site do not have devices, when you delete the site, its sub-sites will be deleted too.

Procedure

1. Click **Site Management**.
2. Select a desired site in the Site Name list.
3. Click **Delete** or click .



4. Click **OK** according to the prompts.

Managing Tasks

The Scheduled Task page displays the added tasks and allows you to add, view, or edit scheduled 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.

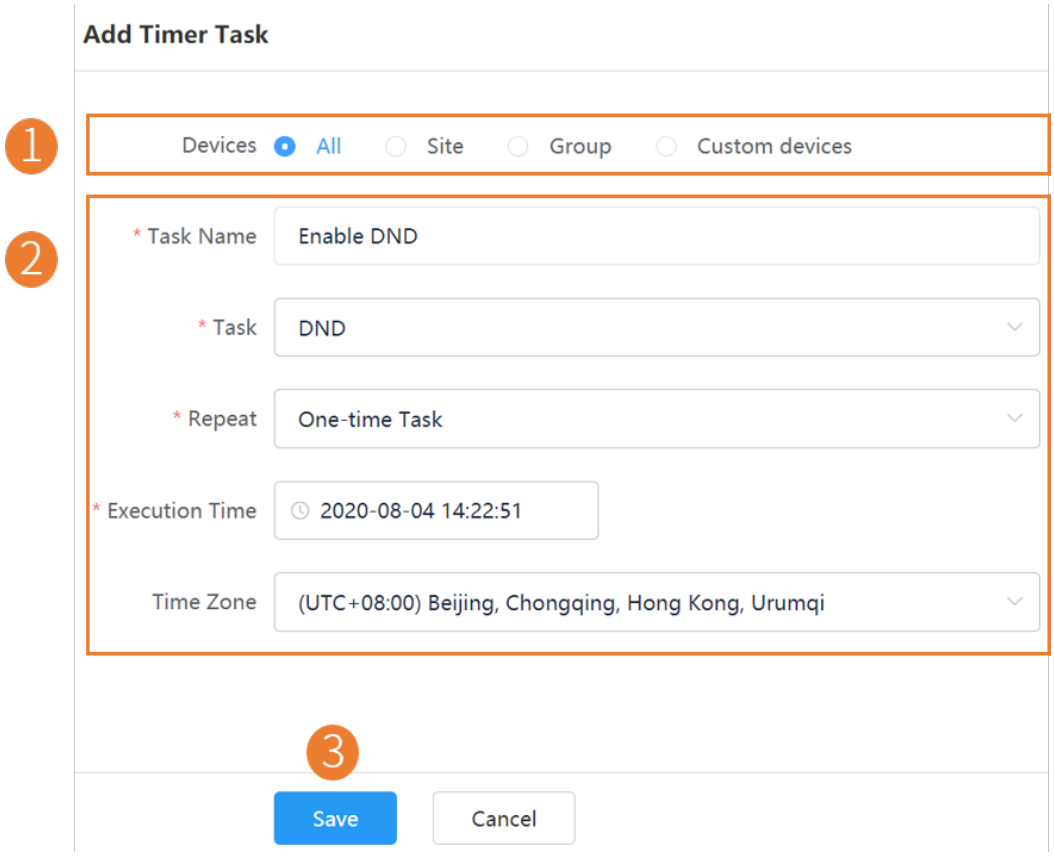
	• Push MAC config: the system will push the MAC configuration you select to the selected devices.

- *Adding Scheduled Tasks*
- *Editing Scheduled Tasks*
- *Pausing or Resuming Scheduled Tasks*
- *Ending Scheduled Tasks*
- *Searching for Scheduled Tasks*
- *Viewing Scheduled Tasks*
- *Viewing Tasks*
- *Searching for Executed Tasks*

Adding Scheduled Tasks

Procedure

Click **Task Management** > **Scheduled Task** > **Add Timer Task**.



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 YDMP before the task expires, the task will be executed.

Related tasks

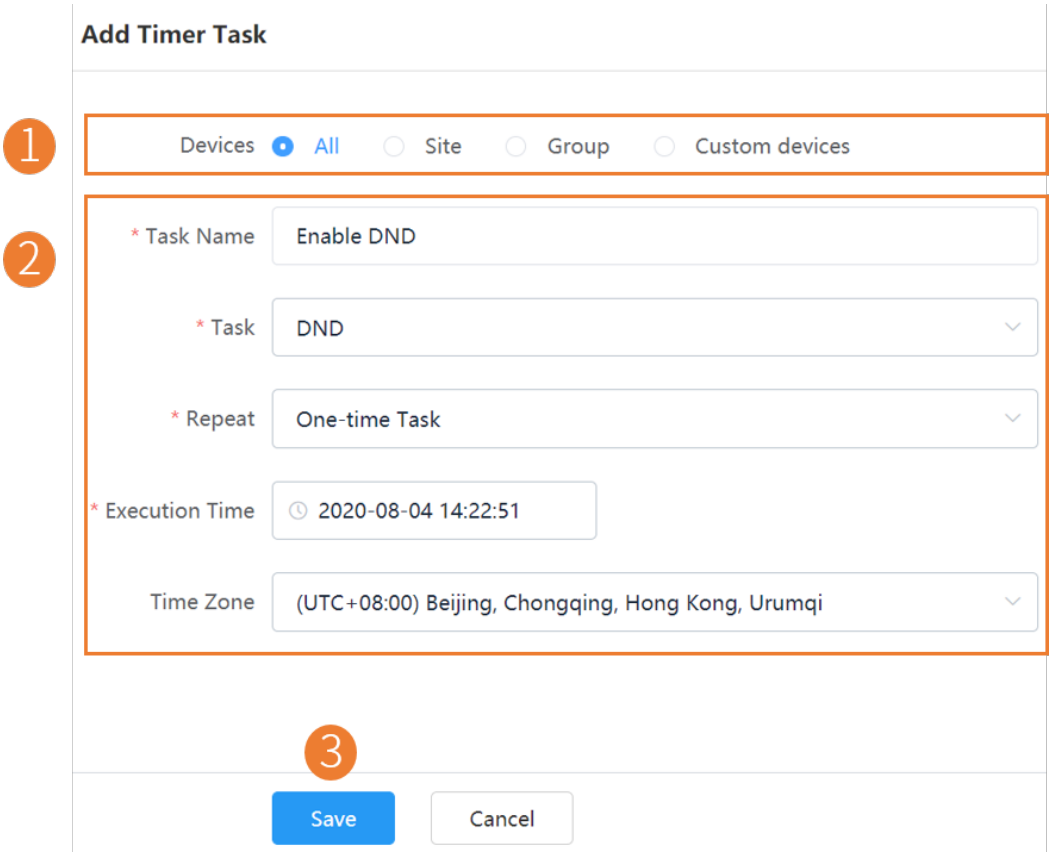
Editing Scheduled Tasks
Pausing or Resuming Scheduled Tasks
Ending Scheduled Tasks
Viewing Scheduled Tasks
Viewing Tasks

Editing Scheduled Tasks

You can edit the scheduled 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 Scheduled Tasks

You can pause or resume the periodic scheduled 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 Scheduled Tasks

If you end the scheduled tasks in the status of executing, the task scan still be executed until they are finished. If you end the periodic scheduled tasks, 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 scheduled tasks before the task execution time (for the periodic scheduled tasks, before the first execution time), the tasks would not be displayed in the page of Executed Task.

Related tasks

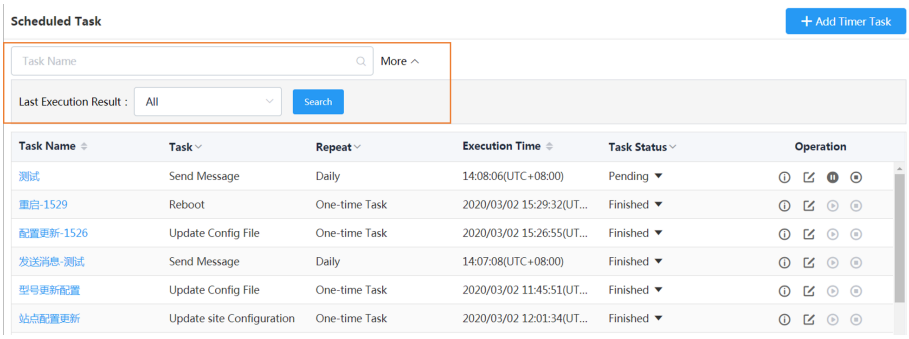
Viewing Scheduled Tasks
Viewing Tasks

Searching for Scheduled Tasks

You can search for scheduled 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.

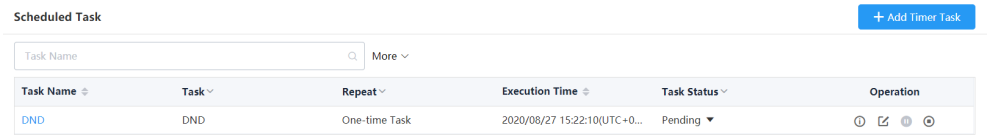
Viewing Scheduled Tasks

Procedure

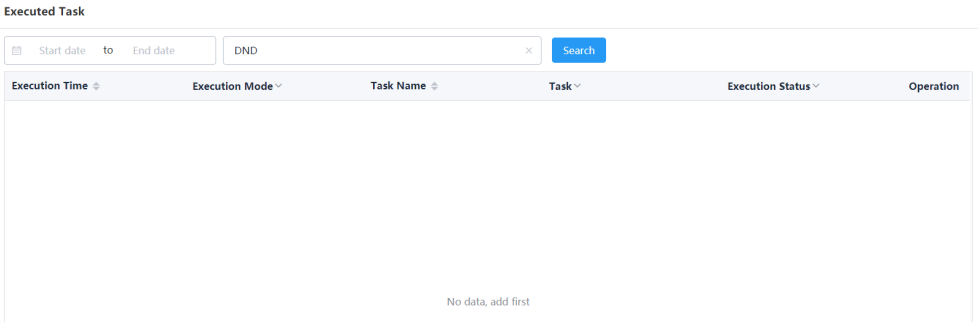
1. Click **Task Management** > **Scheduled Task**.
2. Click the desired task name or click ⓘ beside the desired task name.

Results

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



Note: For the pending task you end before their execution time, there is no data.

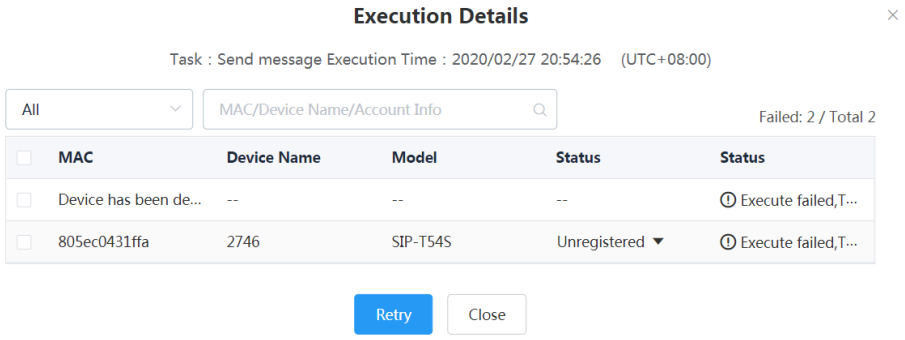


Viewing Tasks

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** > **Scheduled Task**.
2. Click ⓘ beside the desired task name.



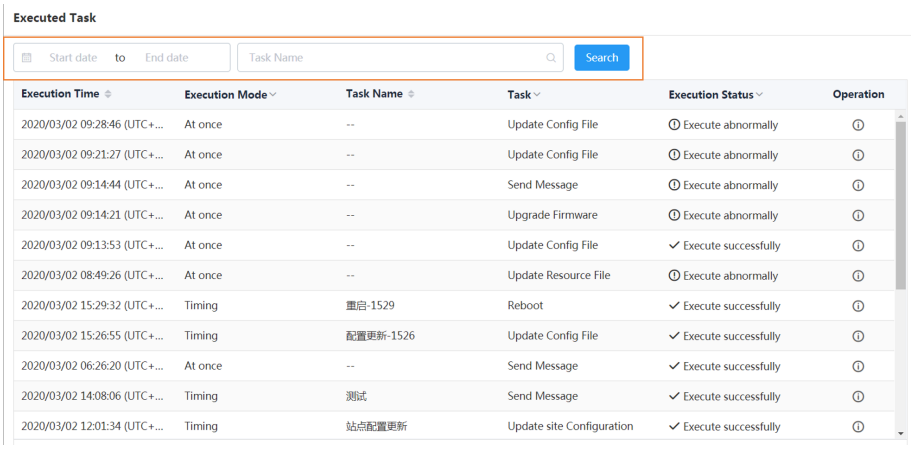
3. Optional: Select the exceptional devices, and then click **Retry** to re-execute the task.

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** > **Scheduled Task**.



Results

The search results are displayed in the executed task list.

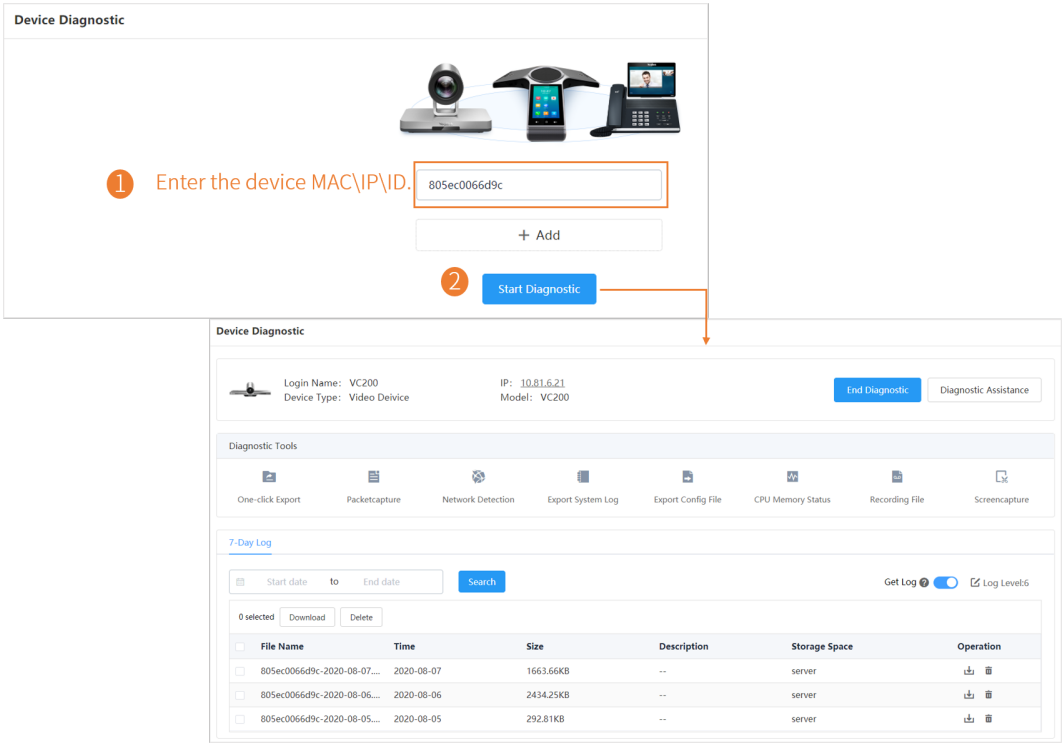
Diagnosing Devices

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 YDMP 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.

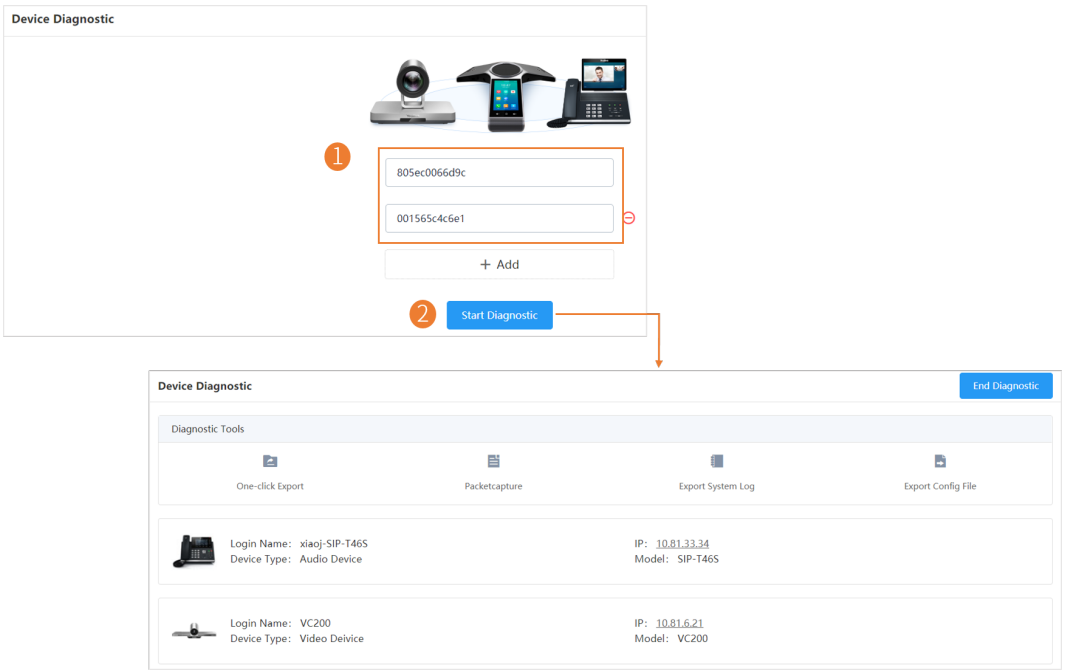
- *Starting Diagnosing*
- *Exporting the Packets, Logs, and Configuration Files by One Click*
- *Capturing Packets*
- *Diagnosing the Network*
- *Exporting System Logs*
- *Exporting the Configuration Files*
- *Viewing the CPU and the Memory Status*
- *Viewing Recording Files*
- *Taking the Screenshot of the Device*
- *Getting the Device Log*
- *Setting the Log Level*
- *Download the Device Log*
- *Backing up Configuration Files*
- *Diagnostic Assistance*
- *Ending the Diagnostic*

Starting Diagnosing

- Diagnosing a single device (taking the SIP device as an example)



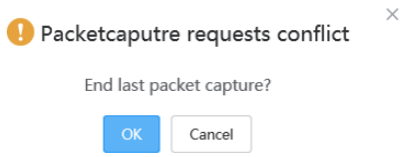
- Diagnosing multiple devices (now this feature is only applicable to SIP devices. Up to 5 SIP devices can be diagnosed at the same time)



Note:

- This feature is not applicable to the offline and invalid devices.

- Users 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.

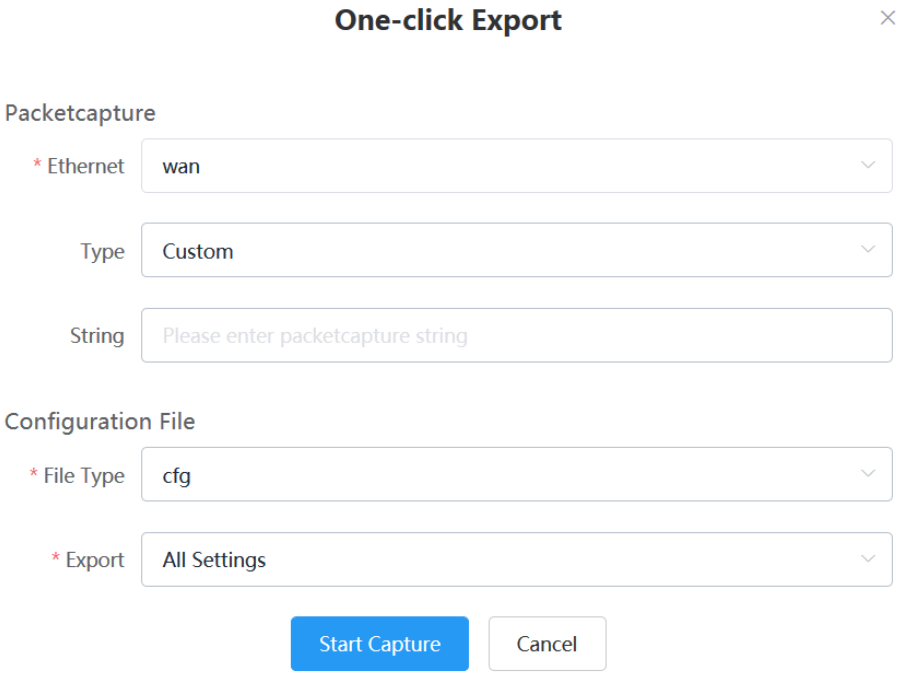


Exporting the Packets, Logs, and Configuration Files by One Click

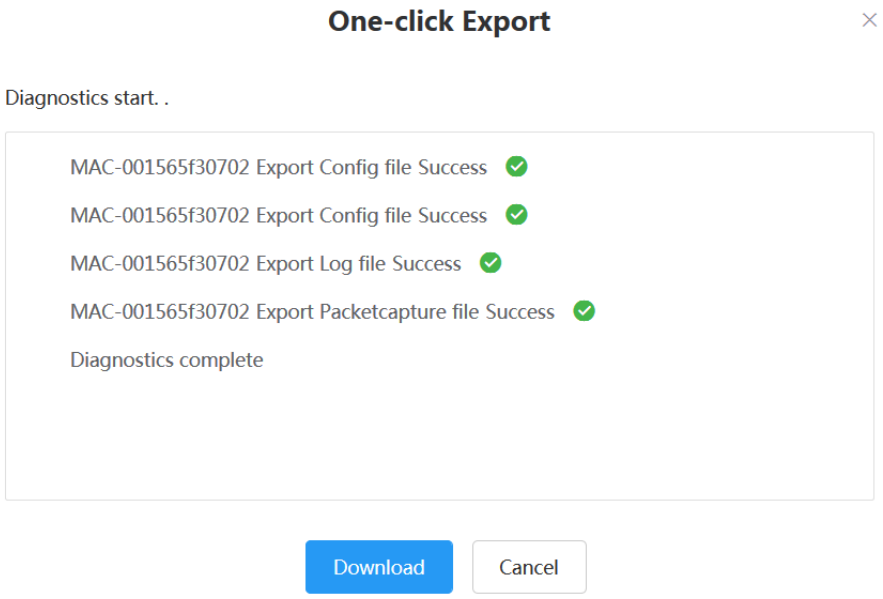
You can use the **One-click Export** feature to export the packets, logs, and configuration files of one or multiple devices at the same time.

Procedure

1. On the Device Diagnostics page, click **One-click Export**.
2. Set the parameters and click **Start Capture**. You can customize the time for packet capturing.



3. Click **End Capture** and the file is generated automatically.



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

Capturing Packets

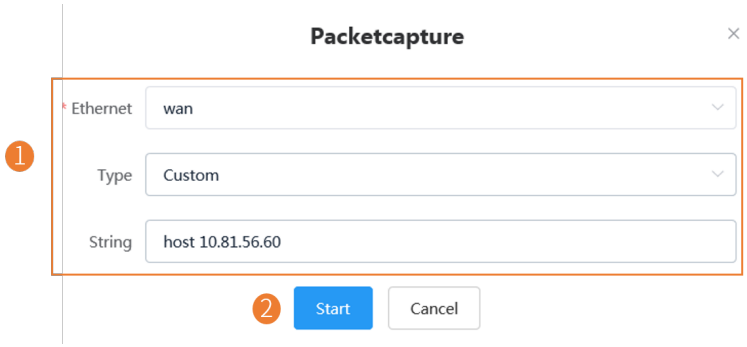
About this task
Here, we list some frequently used rules for packet capturing.

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

String	Example	Introduction
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 **Packetcapture**.



Note:

- Customize the time for capturing.
- You can enter the string only when you select **Custom** from the drop-down menu of the **Type**.

2. Click **Finish** to stop capturing, and the file is generated automatically.
3. 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

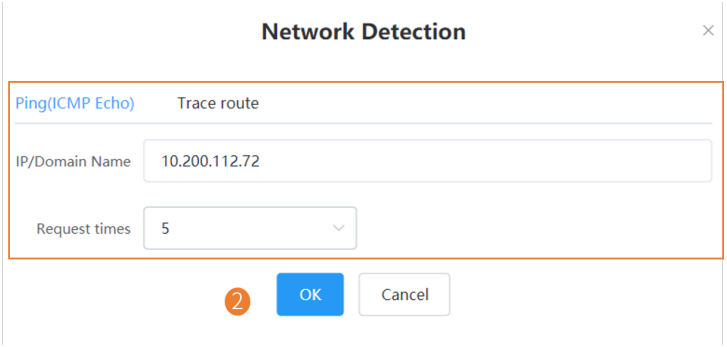
About this task

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

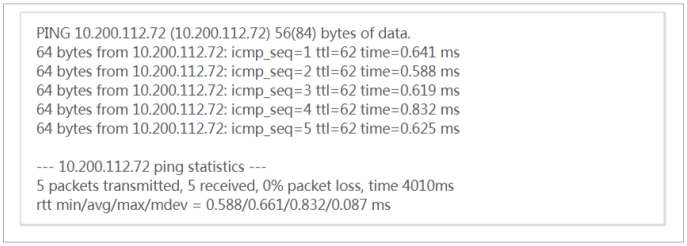
On the Device Diagnostics page, click **Network detection**.



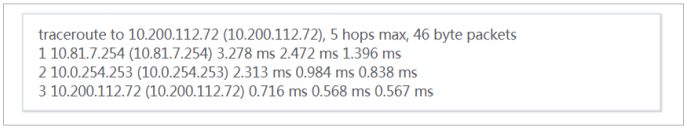
The value of IP/Domain Name is the address of YDMP by default.

Results

- If you select Ping, the example result is below



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



Exporting System Logs

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

Procedure

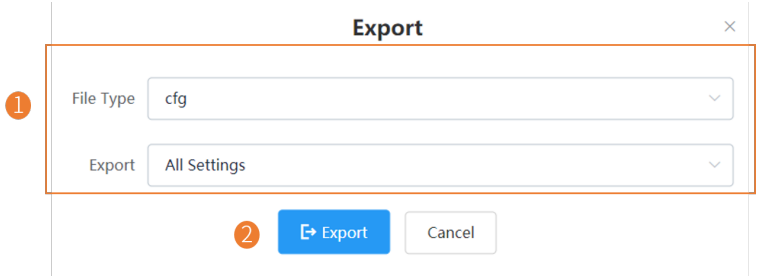
1. On the Device Diagnostics page, click **Export System Log**.
2. Save the file to your local computer.

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.

Procedure

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

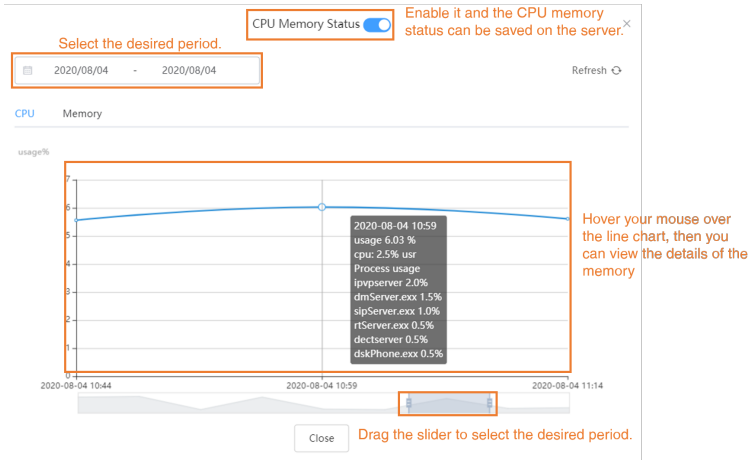


Viewing the CPU and the Memory Status

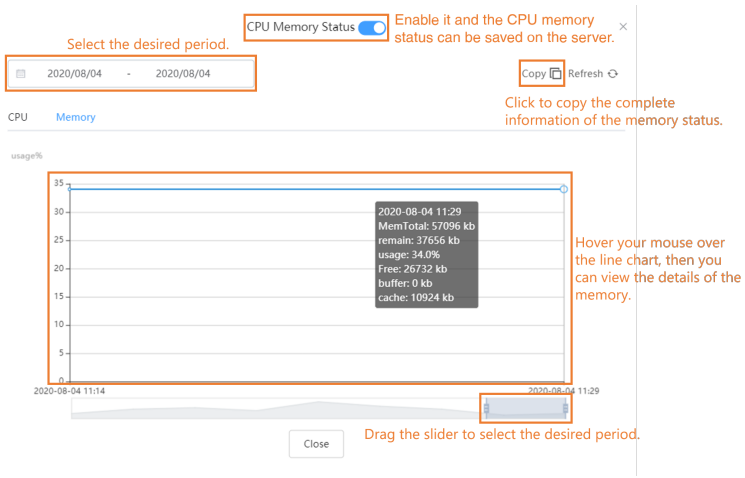
The device will regularly report its CPU and memory information to YDMP, so you can view the latest information. You can also view the memory information by copying it to Microsoft Word.

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.

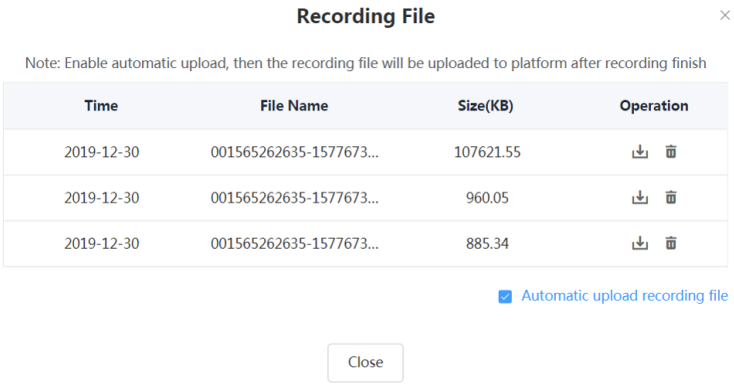


Viewing Recording Files

Before you begin

- There are recording files on the devices.
- You already select the **Automatic upload recording file** check box. Therefore, when the recording is finished, the device will upload the recording file to the platform automatically.

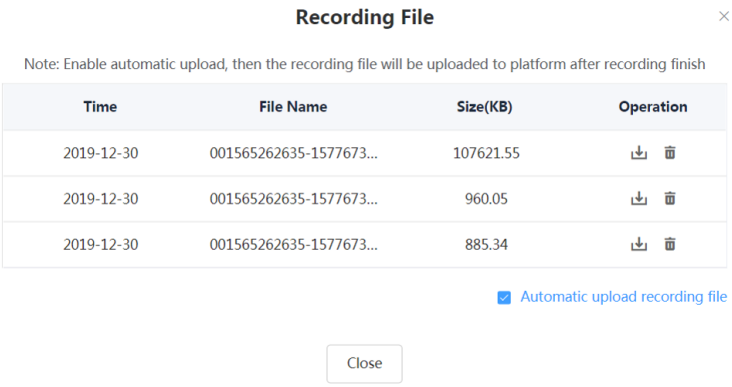
Note: If the device owner does not allow your request, the device would not upload the recording file.



Procedure

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

Results



Note: Click to download the recording file or click to delete the recording file.

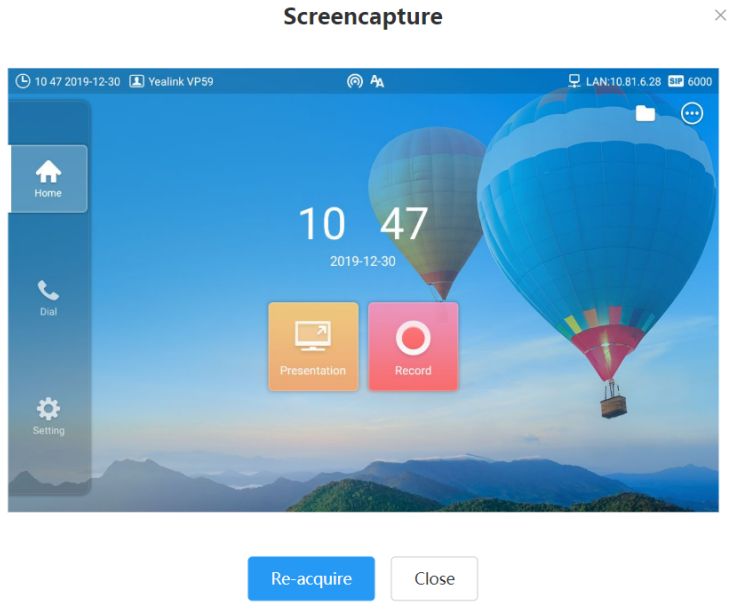
Taking the Screenshot of the Device

Procedure

On the Device Diagnostics page, click **Screencapture**.

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 **Re-acquire** to take the latest screenshot.

Getting the Device Log

About this task

Note:

Procedure

On the Device Diagnostics page, enable **Get Log**.

If you disable this feature, YDMP would not save the device logs any longer.

Setting the Log Level

Procedure

1. On the Device Diagnostics page, click **Log Level**.
2. Enter the desired value.
3. Click **Confirm**.

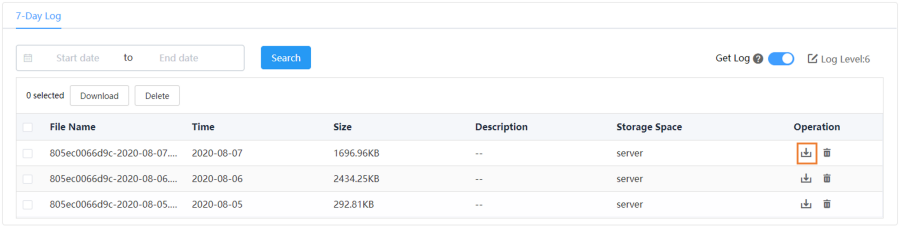
Download the Device Log

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

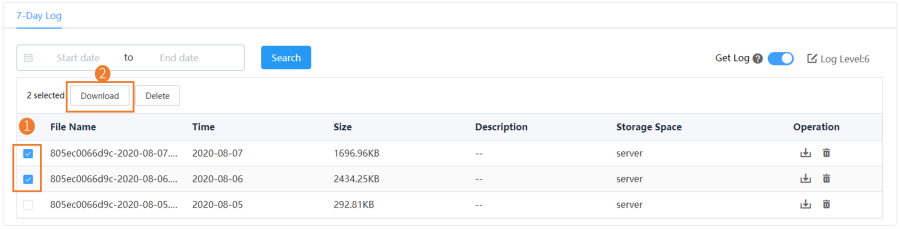
Procedure

On the Device Diagnostics page, do one of the following:

- Download a single device log:



- Download a batch of device logs:

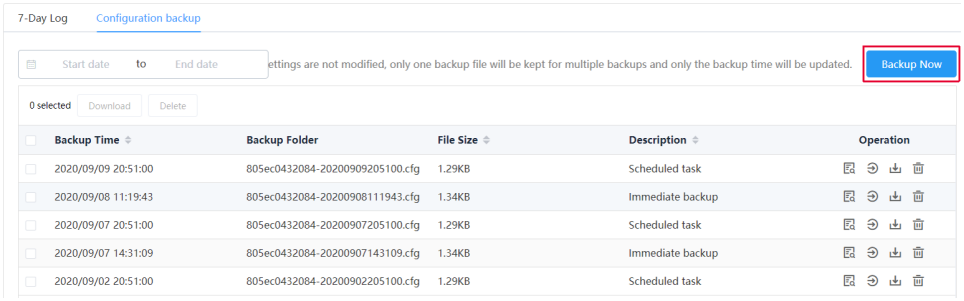


Backing up Configuration Files

You can back up 5 historical configuration files at most.

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, YDMP allows you to create a scheduled task for backing up or restoring the configuration file. For more information, refer to *Adding Scheduled Tasks* .

Diagnostic Assistance

If you cannot solve the problem by diagnosing the devices, you can click Diagnostic Assistance on the Device Diagnostics page to send the issue to Yealink.

Ending the Diagnostic

Procedure

On the Device Diagnostics page, click **End Diagnostic**.

Managing Alarm

When the devices are abnormal, they will send alarm to YDMP 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.

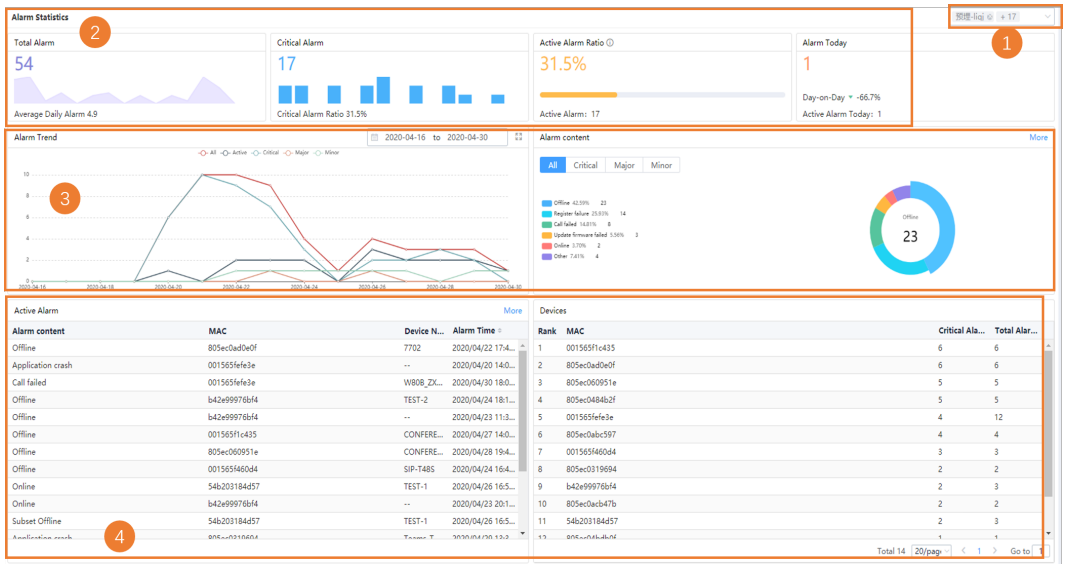


Table 1:

Number	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	The total alarms of the enterprises.	This chart displays the trend of the alarms in the recent 15 days.
	The critical alarms of the enterprises.	This chart displays the distribution of the critical alarms in the recent 15 days.
	The active alarm ratio and the total number of active alarms.	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.

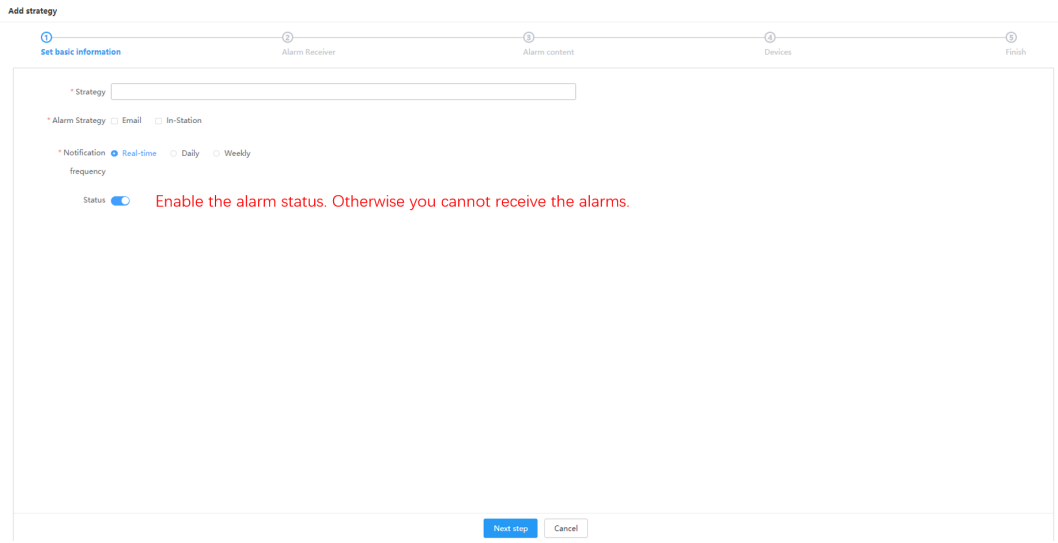
Number	Feature	Description
	The number of alarms today, the ratio of the alarms compared between today and yesterday, the number of active alarms today.	
3	The chart of the alarm trends.	1. The statistics of the chart can select any rage within a half year. The default value is the statistics in the 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.
	The alarm content.	This chart displays the ratio and the number of each alarm content.
4	The active alarm.	Display the content of the active alarms of devices.
	The devices.	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

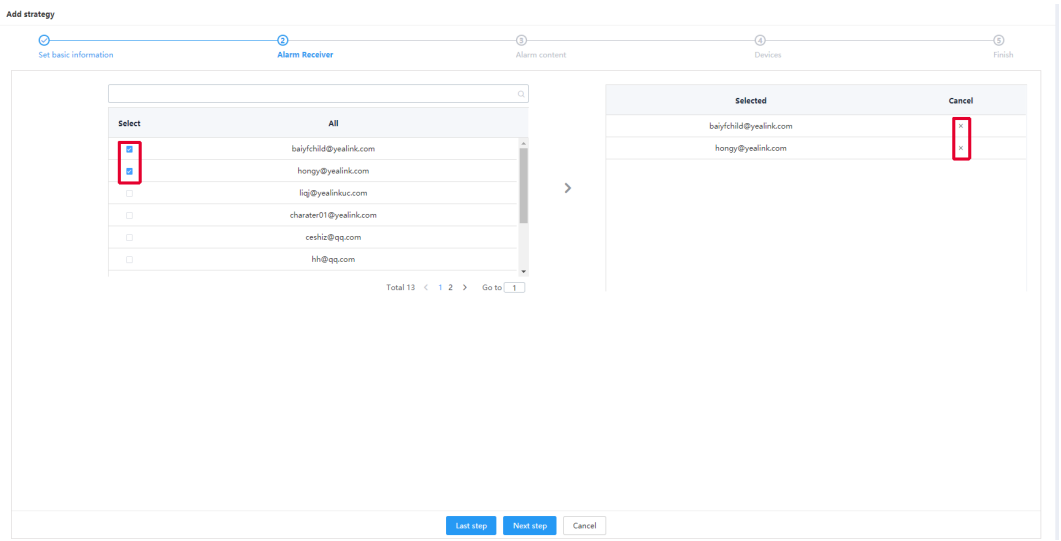
1. Click **Alarm Management** > **Alarm Strategy** > **Add Strategy**.
2. On the page of Set basic information, enter the corresponding information.



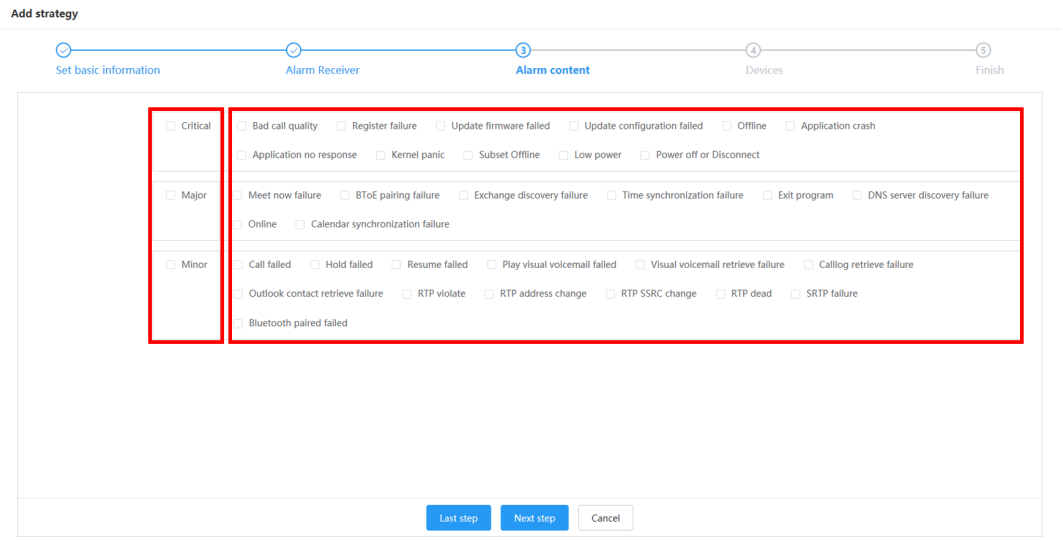
3. Click **Next step** to go to the page of Alarm Receiver.

   Note: The alarm receiver is the administrator by default, you can also select the sub-administrator as the receiver. For adding sub-administrators, refer to *Adding and Managing Sub-Administrator Accounts* 。

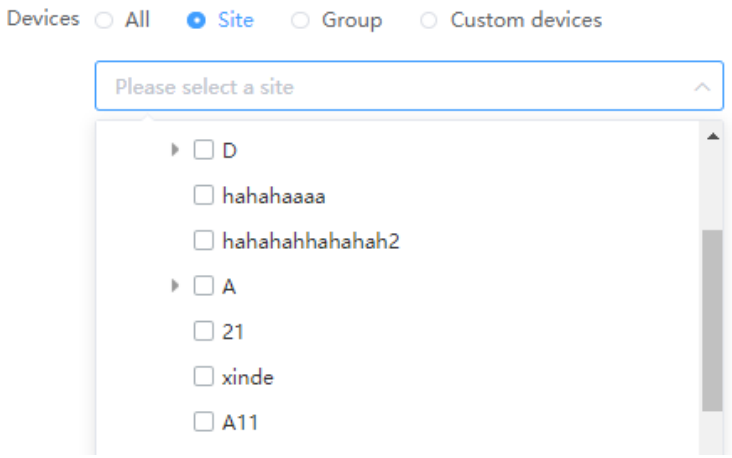
4. On the page of Alarm Receiver, select the desired alarm receivers, and the selected alarm receivers will display in the selected list on the right side of the page. If you want to delete the alarm receivers, click ✕ to delete.



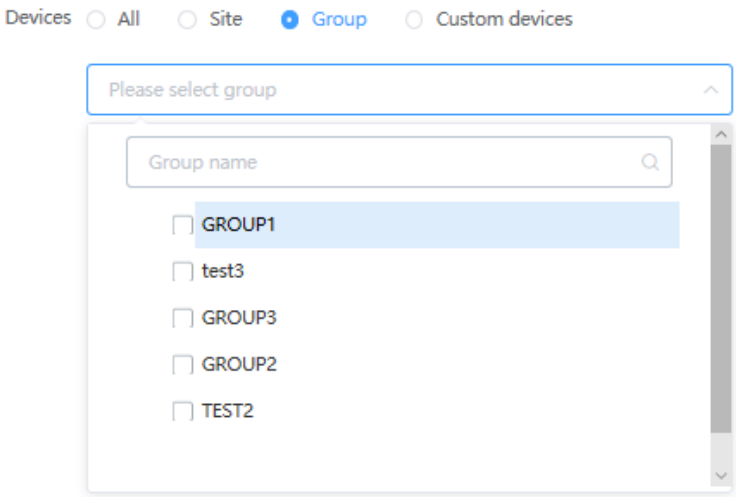
5. Click **Next step** to go to the page of Alarm content. If you want to go back to the former page, click **Last step** and you will go to the page of Set basic information.
6. On the page of Alarm content, select the alarm levels on the left side of the page, and select the desired corresponding alarm content beside the alarm levels.



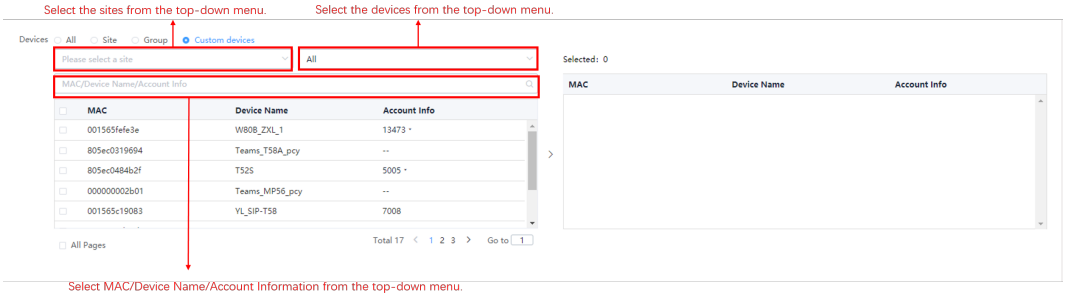
7. Click **Next step** to go to the page of Devices. I If you want to go back to the former page, click **Last step** and you will go to the page of Alarm content.
8. On the page of Devices, do one of the following:
   - Select All to display all alarms.
   - Select Site and select the desired sites from the top-down menu.



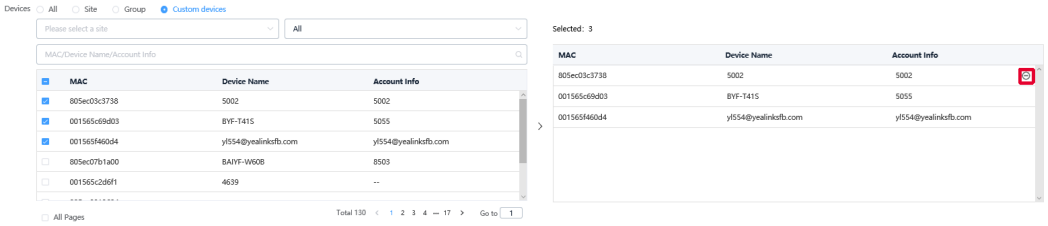
   - Select Group and select the desired groups from the top-down menu.



- Select Custom devices and enter the corresponding information.



If you want to delete the selected information, click ⊖ after the selected information on the right side of the page.

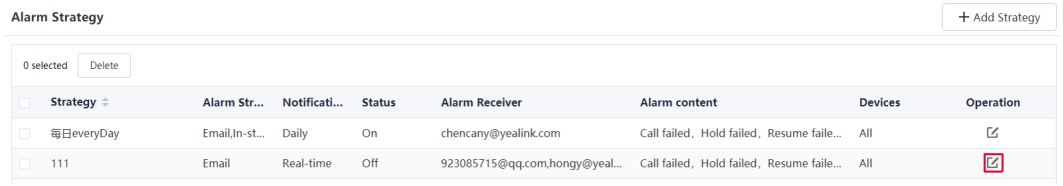


9. Click **Finish**. If you want to go back to the former page, click **Last step** and you will go to the page of Alarm content.

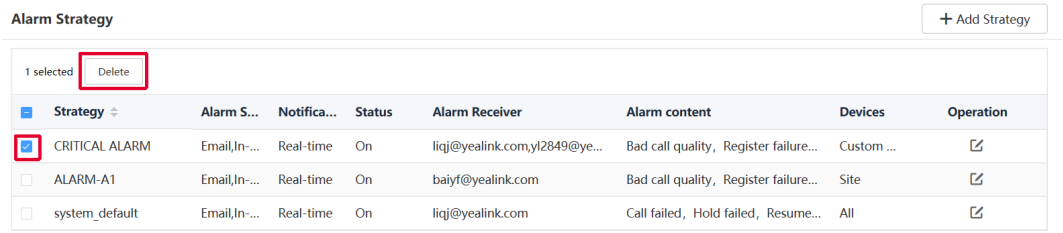
Managing Alarm Strategies

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**.

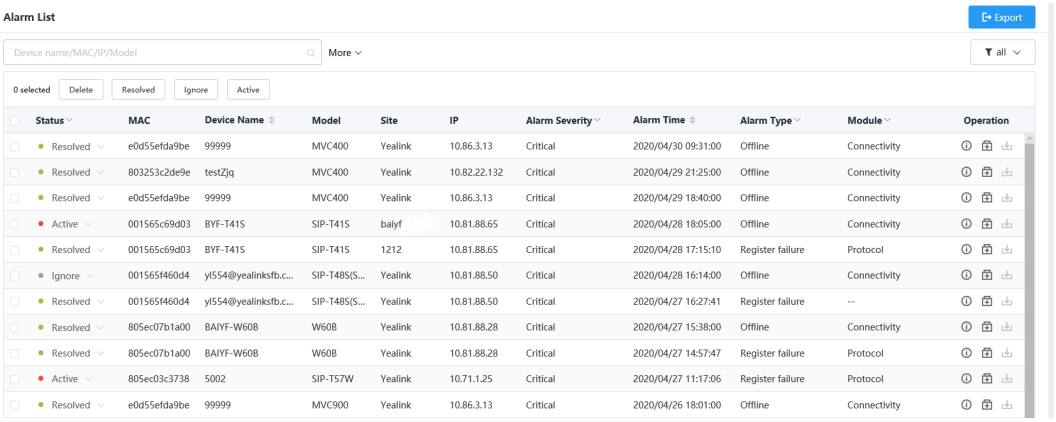


Viewing Alarms

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.

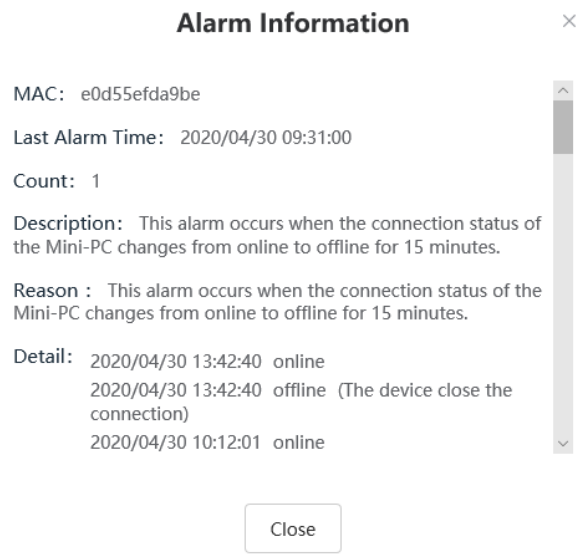
Procedure

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



2. Optional: Do one of the following:

- Click ⓘ on the right side of the desired alarm to view the details.



- Select the desired alarm, click the alarm status **Resolved** on the top of the page to exchange the alarm status as Resolved.

  Click the alarm status **Ignore** on the top of the page to exchange the alarm status as Ignore.

  Click the alarm status **Active** on the top of the page to exchange the alarm status as Active.

- 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	Recommended Solution	Supported device
Poor call quality	Critical	Make sure that the network connection status is good.	SIP IP Phones SfB HD IP phones Video Conferencing Systems
Register failure	Critical	Generally, it is caused by the server rather than the device. You can refer to the error codes and do the following: • Check whether you enter the correct account number. • Check whether the server and port configuration are correct. • Check whther the server is available and can response requests.	SIP IP Phones SfB HD IP phones Video Conferencing Systems

Alarm type	Severity	Recommended Solution	Supported device
Upgrade firmware failure	Critical	• Check whether the firmware matches the device model. • Check whether the firmware is damaged. • Check whether the firmware is protected by software.	SIP IP Phones SfB HD IP phones Video Conferencing Systems Teams phones
Update configuration failure	Critical	• Check whether the configuration file is correct without messy codes. • Check whther the configuration file is started with **#!version:1.0.0.1**.	SIP IP Phones SfB HD IP phones Video Conferencing Systems Teams phones
Offline	Critical	• Check whether the device network connection is available. • Check whether the device is connected to YDMP.	SIP IP Phones SfB HD IP phones Video Conferencing Systems Teams phones MVC Room System
System license is about to expire	Critical	Contact Yealink technical support.	N/A
Device capacity of license is insufficient	Critical	Contact Yealink technical support.	N/A
Subset Offline	Critical	Insert the accessories.	MVC Room System
Low power	Critical	Charge the device.	MVC Room System
Power off or Disconnect	Critical	Turn on the wireless microphone.	MVC Room System
Visual voicemail retrieve failure	Minor	• Check whether the server address is correct. • Check whether the server works well. • Check whether the network connection is available and the devices is connected to the server.	SfB HD IP phones
Hold failure	Minor	• Check the hold feature of the server. • Contact Yealink technical support.	SIP IP Phones SfB HD IP phones
Resume failure	Minor	• Check the hold feature of the server. • Contact Yealink technical support.	SIP IP Phones SfB HD IP phones

Alarm type	Severity	Recommended Solution	Supported device
RTP violate	Minor	• Change the phone codec to the one negotiated in a call. • Check whether the server uses the different codec from the negotiated codec in a call.	SIP IP Phones SfB HD IP phones
RTP address change	Minor	Check the server.	SIP IP Phones SfB HD IP phones
RTP dead	Minor	Make sure that the network connection status is good.	SIP IP Phones SfB HD IP phones Video Conferencing Systems
SRTP failure	Minor	Check whether the server RTP stream is encrypted.	SIP IP Phones SfB HD IP phones
Call log retrieve failure	Minor	• Check whether the server address is correct. • Check whether the server works well. • Check whether the network connection is available and the devices is connected to the server.	SfB HD IP phones
Outlook contact retrieve failure	Minor	• Check whether the server address is correct. • Check whether the server works well. • Check whether the network connection is available and the devices is connected to the server.	SfB HD IP phones
Call failed	Minor	You can refer to the error codes and do the following: • Check whether the callee device has account registered and DND is disabled. • Check whether the callee number exists. • Check whether the callee has codecs in common with the caller to establish a call.	SIP IP Phones SfB HD IP phones Video Conferencing Systems

Alarm type	Severity	Recommended Solution	Supported device
Calendar synchronization failure	Major	• Check whether the server address is correct. • Check whether the server works well. • Check whether the network connection is available and the devices is connected to the server.	SfB HD IP phones
Exchange discovery failure	Major	• Check whether the server address is correct. • Check whether the server works well. • Check whether the network connection is available and the devices is connected to the server.	SfB HD IP phones
Online	Major	N/A	MVC Room System

Related concepts

Managing Alarm

Filtering the Alarms

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

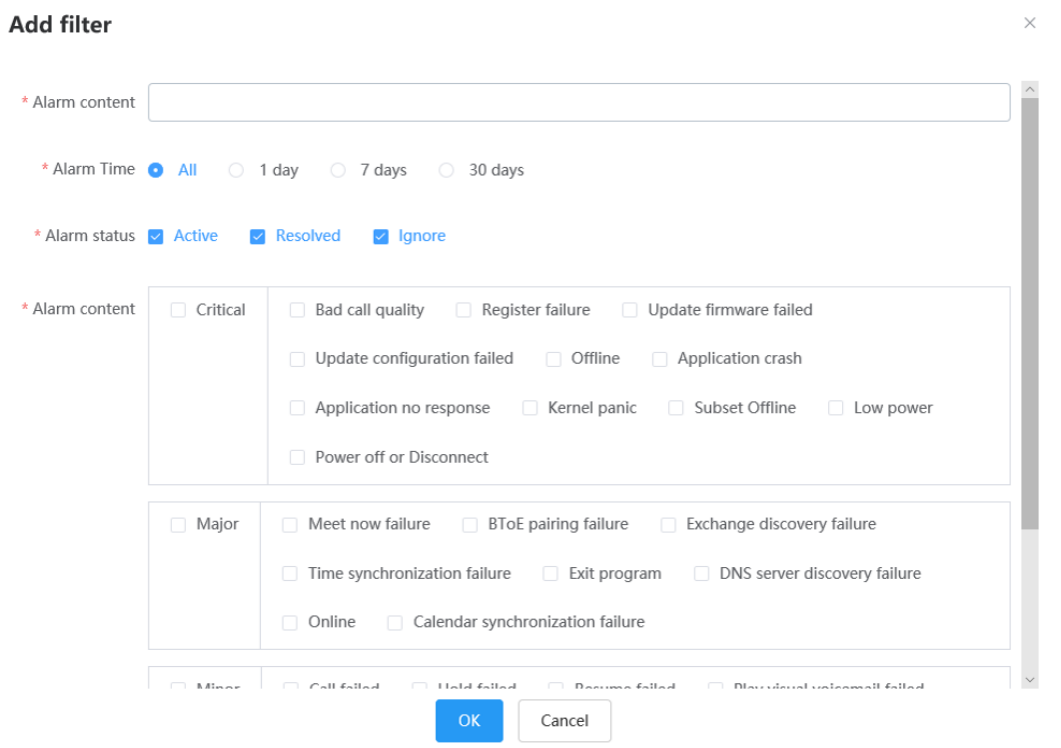
- *Customizing Filters*
- *Filtering the Alarms*

Customizing Filters

Procedure

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

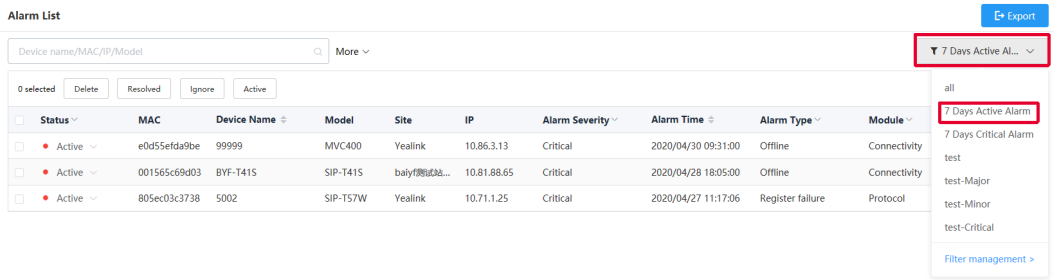
3. Click **Add filter**, enter the corresponding information, and click **OK**.



Filtering the Alarms

Procedure

Click to filter the alarms, 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.

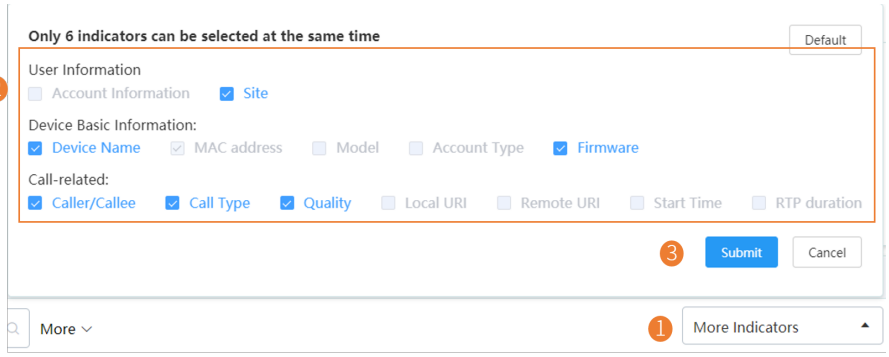
- *Customizing the Indicators of Call Quality Detail*
- *Viewing the Call Data*

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 6 indicators expect for the MAC address.

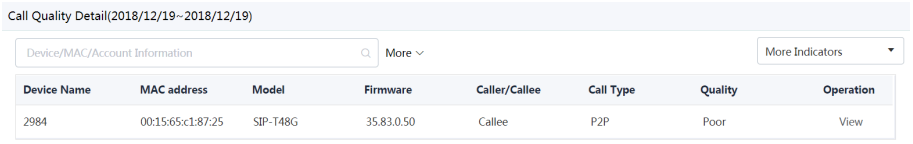
Procedure

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 **View** beside the desired call to go to the Call Data page.

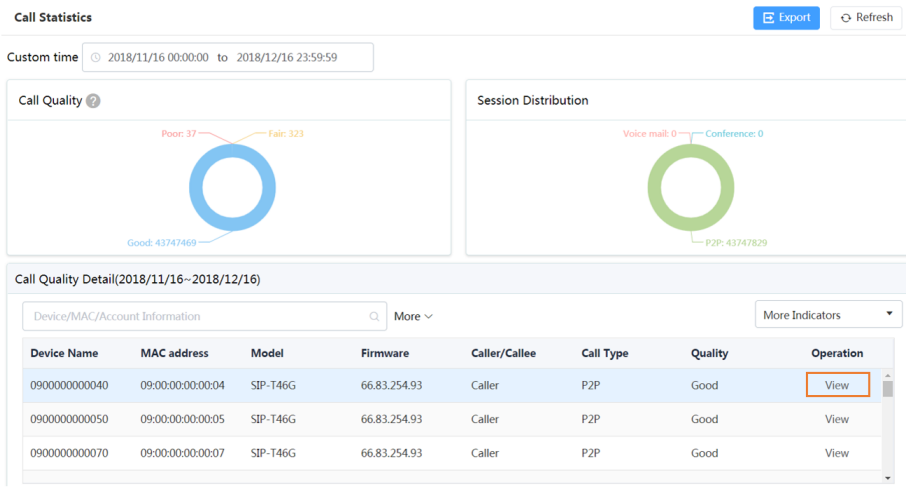


Table 2: Metrics of Call Data

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
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 3: 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 200ms

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

Managing System

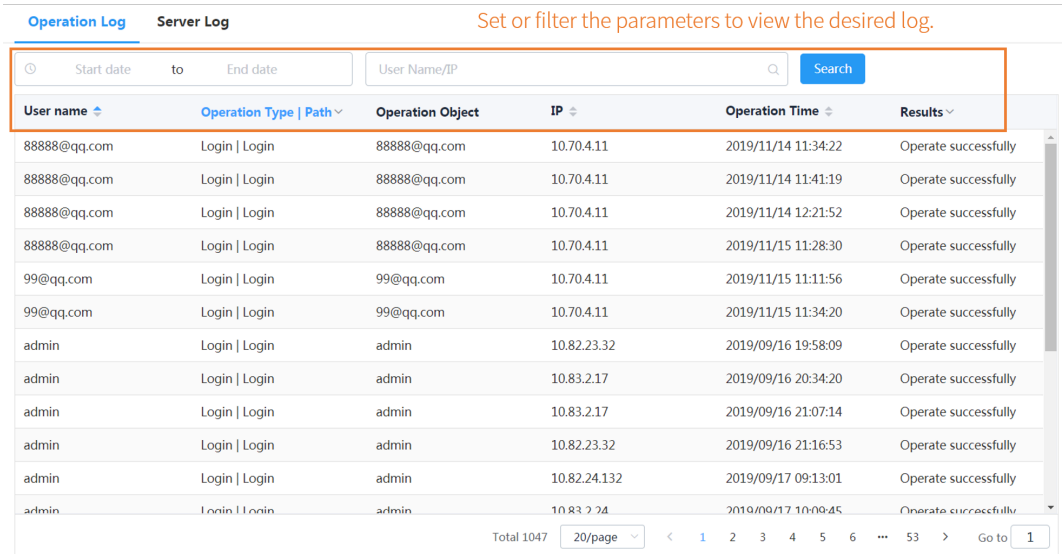
- *Viewing Operation Logs*
- *Exporting the Server Log*
- *Configuring the SMTP Mailbox*
- *Uploading DST Rules*
- *Obtaining the Accesskey*

Viewing Operation Logs

Operation logs record the operation performed by administrators and sub-administrators on YDMP. You can view the operation log.

Procedure

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

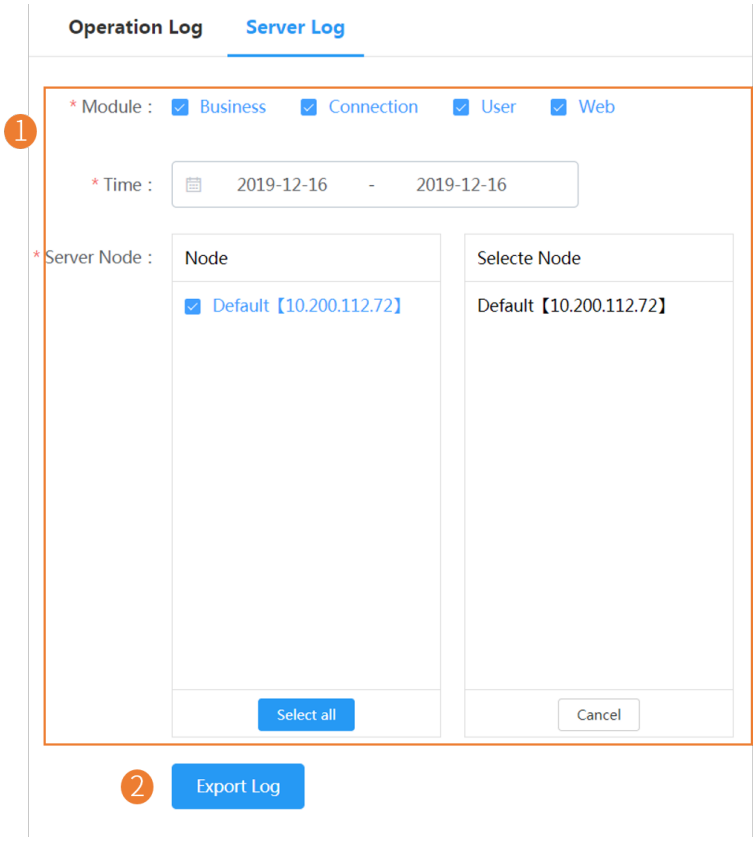


Exporting the Server Log

You can export the server log and provide Yealink technical support with the log for troubleshooting.

Procedure

1. Click **System Management** > **Log Management** > **Server Log**.
2. Export the log.

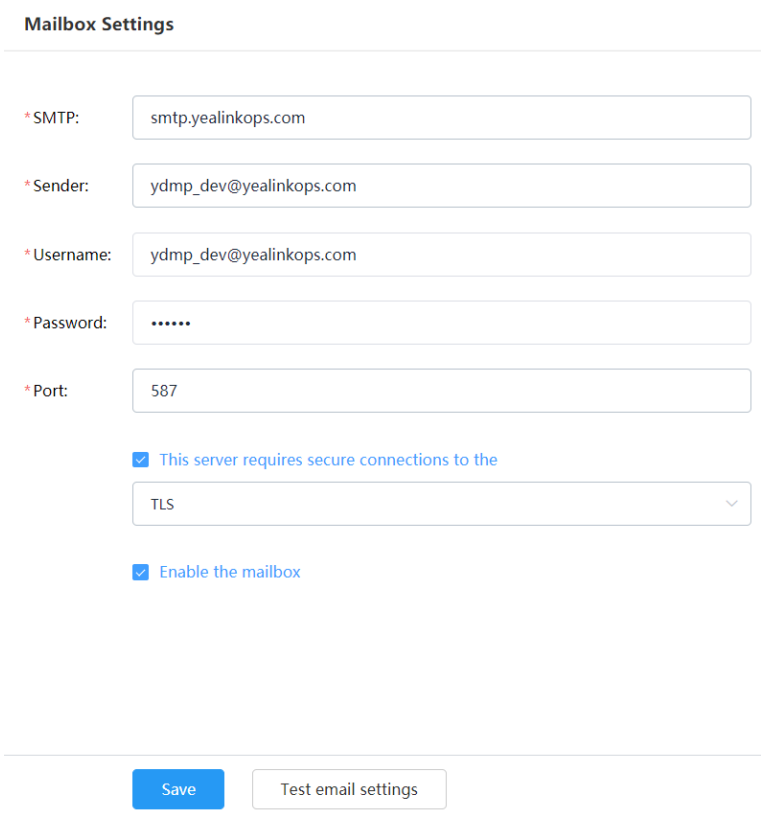


Configuring the SMTP Mailbox

The SMTP mailbox is used to send the alarm and the account information to administrators.

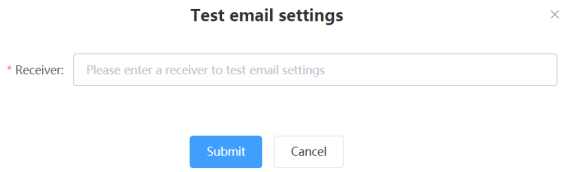
Procedure

1. Click **System Management** > **Mailbox Settings**.
2. Configure the parameters.



Parameter	Description
SMTP	Specifies the address of the SMTP server.
Sender	Configures the email address of the sender.
Account	Specifies the email username of the sender.
Password	Specifies the email password of the sender.
Port	Specifies the connection port.
This server requires a secure connection.	Enables or disables the secure connection: SSL or TLS (default)
Enable the mailbox	Enables or disables the mailbox.

3. Optional: Click **Test email settings**.



Enter the email address of a receiver and click **Submit** to test whether the email address you set is available. If the receiver does not receive the email, you can check the account and the password.

4. Click **Confirm**.

Uploading DST Rules

Procedure

1. Click **System Management** > **DST Template**.
2. Click **Select** and select the desired file to upload.

3. Click **Upload**.

Obtaining the Accesskey

YDMP 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 Device Management 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 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*
- *Adding and Managing Roles*
- *Assigning the Function Permission*
- *Assigning the Data Permission*
- *Adding and Managing Sub-Administrator Accounts*
- *Editing the Account Information*
- *Viewing the Account Code*

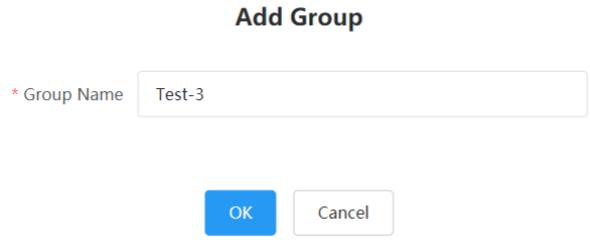
Adding and Managing Groups

You can manage the roles by the group.

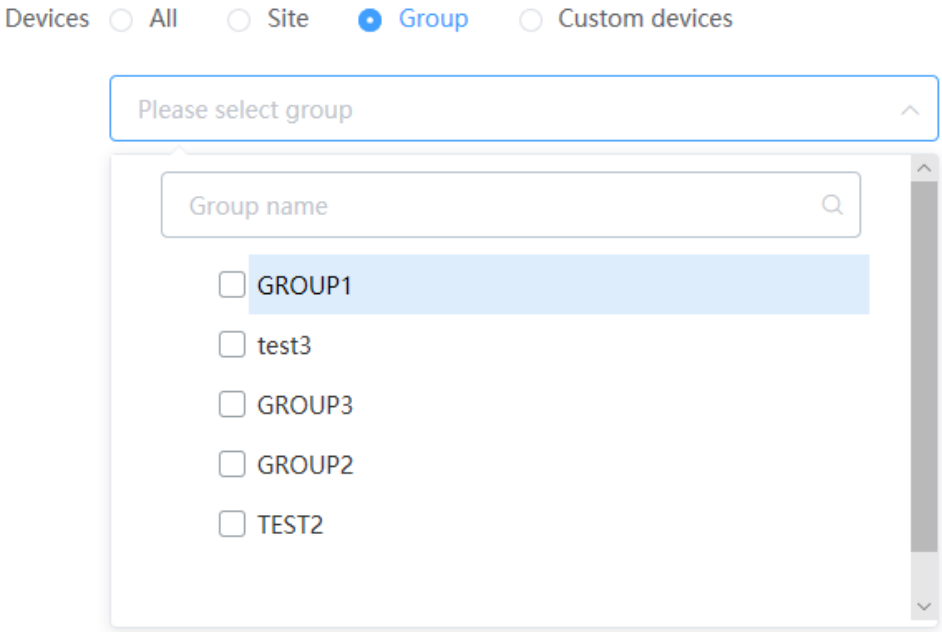
About this task
You cannot edit or delete the default group.

Procedure

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



After adding the group, click the corresponding icon on the right side of the desired group 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

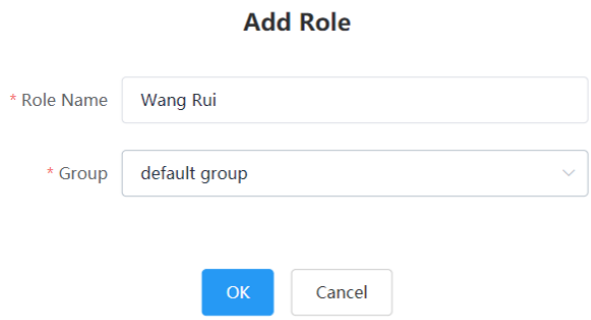
The default roles are as below, you cannot edit or delete them.

Table 4: Default role

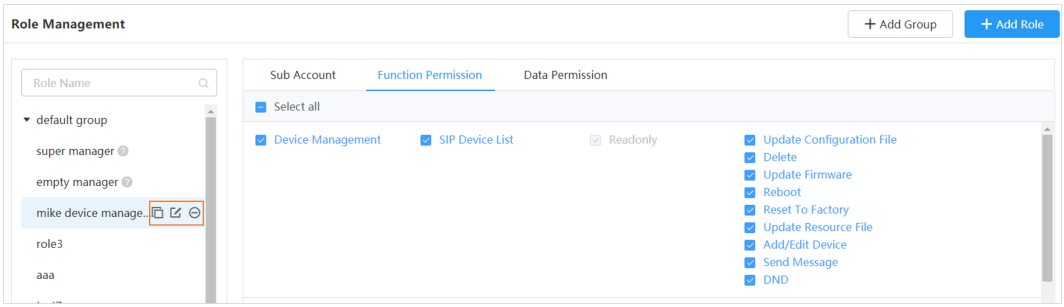
Name	Group	Function and data permission
Super manager	Default role group	All function and data permission
Empty manager	Default role group	Only the permission of logging in.

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.



After adding the role, you can also click **Add sub account** to add a sub-administrator account for the role.

Assigning the Function Permission

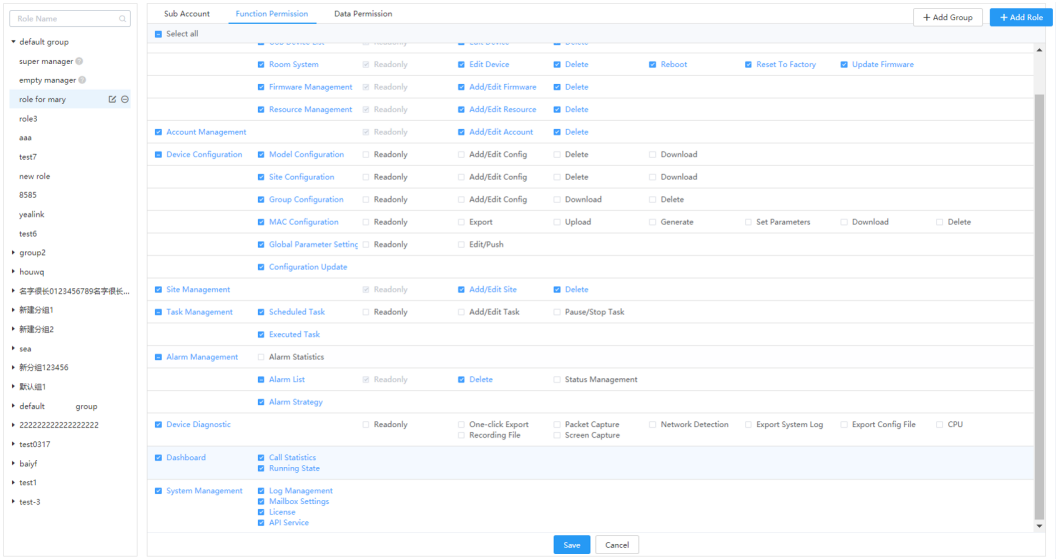
If you want to allow non-managers to use the sub-administrator account, for example, checking the call quality of the phone and diagnosing the devices, but you do not want them to add or delete devices, you can assign the limited function permission to them.

Before you begin

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

Procedure

1. Go to the page of Role Management, select the corresponding role, and click **Function Permission**.
2. If you only want to grant the Readonly permission, select the check boxes of **Readonly** on the right side of the corresponding functions; if you want to grant the operation permission, select the check boxes of the corresponding operations.



Assigning the Data Permission

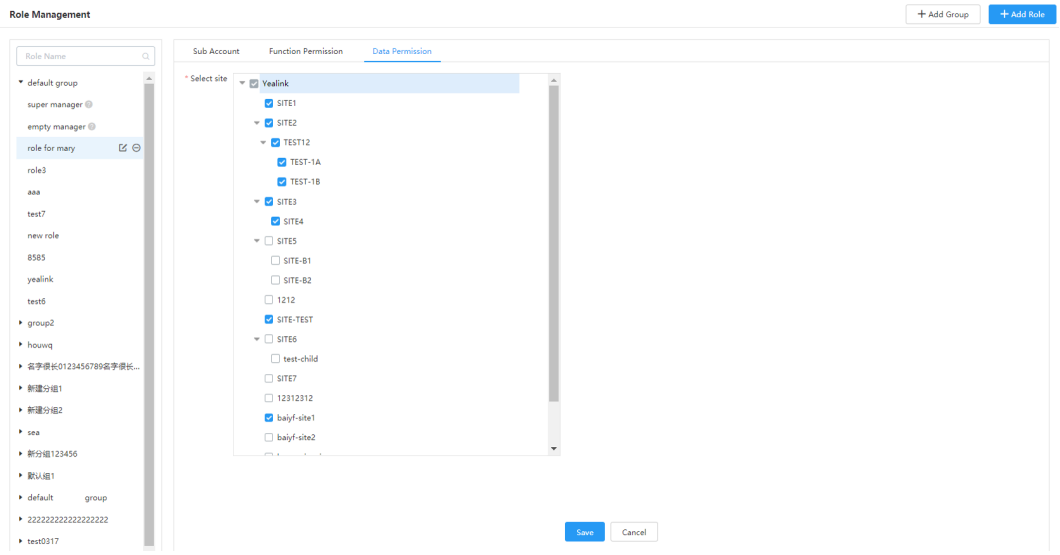
If you want to manage the device of your own site or of a certain amount sites, you can assign the data permission.

Before you begin

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

Procedure

1. Go to Role Management, select the corresponding role, and click **Data Permission**.
2. Select the checkbox of the site you want to manage.



Related tasks

Adding Sites

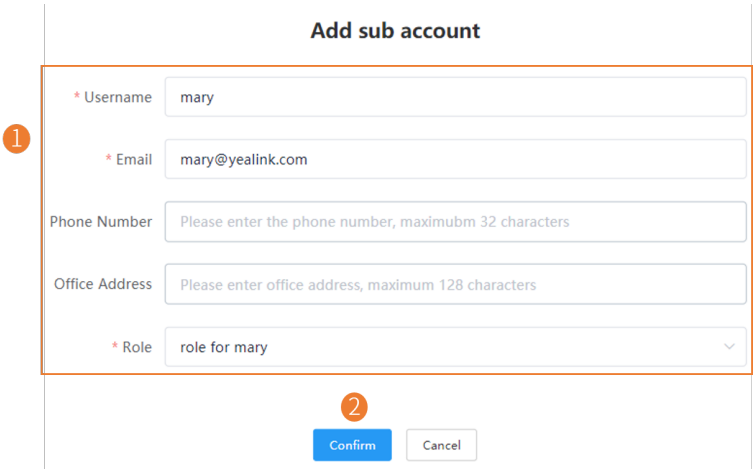
Adding and Managing Sub-Administrator Accounts

Before you begin

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

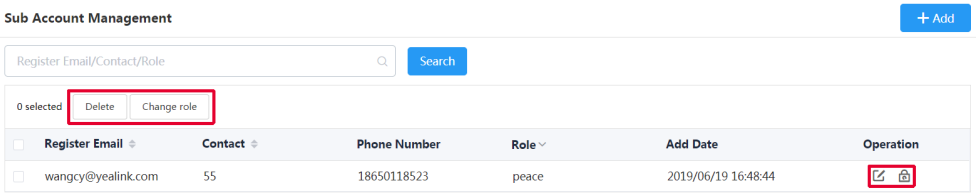
Procedure

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.



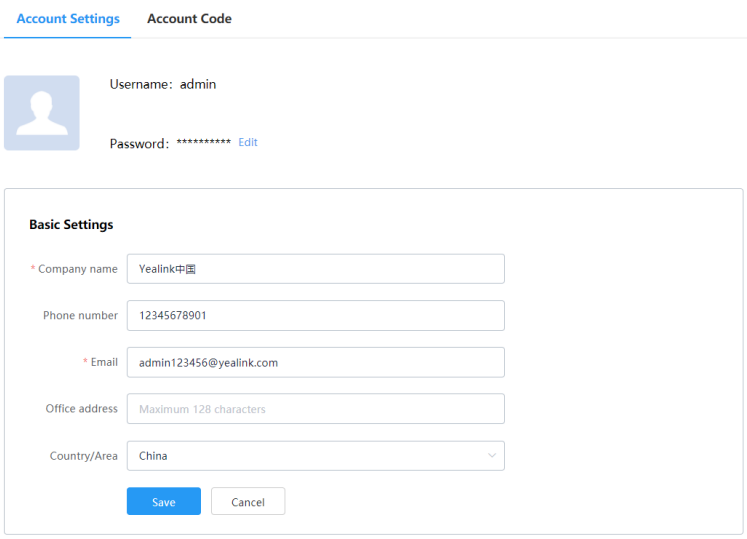
If you enable SMTP mailbox (refer to *Configuring the SMTP Mailbox*), the account information will be sent to the mailbox of the sub-administrator automatically.

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 the related information.



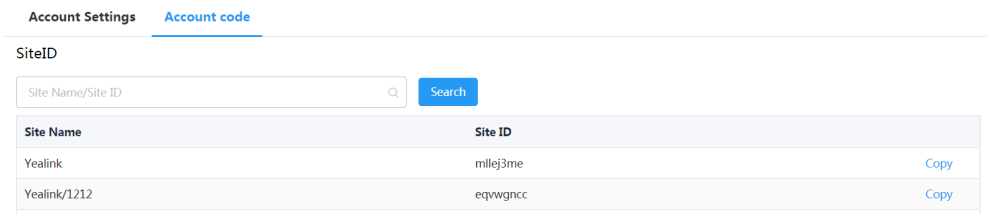
Parameter	Introduction
Password	The password of this account. Click **Edit** to change the password according to the prompt. For account security, we recommend that you change the password regularly.
Email	The mailbox is used to receive alarms and the account information.
Country/Area	You can change 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.

Viewing the Account Code

The account code is 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 of YDMP. 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 YDMP. Upon encountering a case not listed in this section, contact your Yealink reseller or technical support engineer for further support.

- *Forget the Login Password?*
- *Why You Cannot Access the Login Page?*
- *Why the Browser Prompts That the Security Certificate of the Website Is not Trusted When You Access the Login Page?*

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.

Why You Cannot Access the Login Page?

Server:

- Check the network connection of the devices.
- Check the server and the firewall.

Windows:

- Run Network Diagnostics of Window.

Check the firewall:

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

```
[root@localhost ~]# systemctl status firewalld
â firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2017-11-01 06:34:55 EDT; 9min ago
 Main PID: 23324 (firewalld)
   CGroup: /system.slice/firewalld.service
           ††23324 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Nov 01 06:34:54 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Nov 01 06:34:55 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
```

   - If you enable the firewall, you should run the following commands to enable the related ports in the firewall configuration:
   - firewall-cmd --permanent --zone=public --add-port=80/tcp
   - firewall-cmd --permanent --zone=public --add-port=443/tcp

- firewall-cmd --permanent --zone=public --add-port=9989/tcp
- firewall-cmd --permanent --zone=public --add-port=9090/tcp
- firewall-cmd --reload
- firewall-cmd --list-ports
- After you finish the configuration and refresh the page, you can access the login page of YDMP successfully.

Why the Browser Prompts That the Security Certificate of the Website Is not Trusted When You Access the Login Page?

1. The Yealink server has built-in certificates. For security considerations, the browser only trusts certificates issued by the professional certificate issuing authorities. Therefore, they do not trust self-signed certificates by default.
2. When you access the Login page for the first time, it will prompt you an insecure connection (certificate security issue), but you can still access the browser.
3. If you have purchased your own certificate, you can also replace our certificate with your own certificate.

Solution:

1. Edit the install.conf file under the directory of /usr/local/yealink/data/. Add the domain name of tcp and web in the [global] configuration field, see the following example

   microdm_tcp_server_address = tcp.yealinkops.com

   microdm_mail_web_domain = https://dm.yealinkops.com

   microdm_domain = dm.yealinkops.com
2. Run the command as below:

   ```
   cd /usr/local/yealink/nginx/conf/ssl/
   rz      ##run command rz to upload the custom HTTPS certificate##
   ```
3. Edit the *yealink.conf* file in the directory of */usr/local/yealink/nginx/conf/http.conf.d/*, and change the corresponding certificate names of *ssl_certificate* and *ssl_certificate_key* of port 443 to *ssl/xxxxx.pem* (the name of the custom HTTPS certificate).

```
#server
server {
    server_name "_";
    listen        443 ssl;
    ssl_certificate      ssl/nginx.pem;
    ssl_certificate_key  ssl/nginx.pem;

    ssl_verify_depth 2;
    client_max_body_size 10240m;
    proxy_http_version 1.1;
    proxy_set_header   Upgrade $http_upgrade;
    proxy_set_header   Connection $connection_upgrade;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Real-Port $remote_port;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Protocol "$scheme";
    #proxy_set_header Apollo-Forwarded "edge";
    proxy_set_header apollo-server-addr "$server_addr";
    add_header Strict-Transport-Security "max-age=16000000;includeSubDomains;preload;" al
    add_header Referrer-Policy "no-referrer-when-downgrade" always;
    add_header X-Content-Type-Options "nosniff" always;
    add_header X-XSS-Protection "1;mode=block" always;
    proxy_set_header Client-DN $ssl_client_s_dn;
    add_header Set-Cookie "HttpOnly";
    add_header Set-Cookie "secure";
    add_header X-Frame-Options "SAMEORIGIN";

    location / {
        proxy_pass https://server_frontend_manager;
    }
```

4. Run command *systemctl restart nginx* to take effect.
5. After you change the certificate of port 443 to the custom one, you need to change the server address that devices use for obtaining the configuration (dm.cfg) to *http://IP or domain name:9989/dm.cfg*.