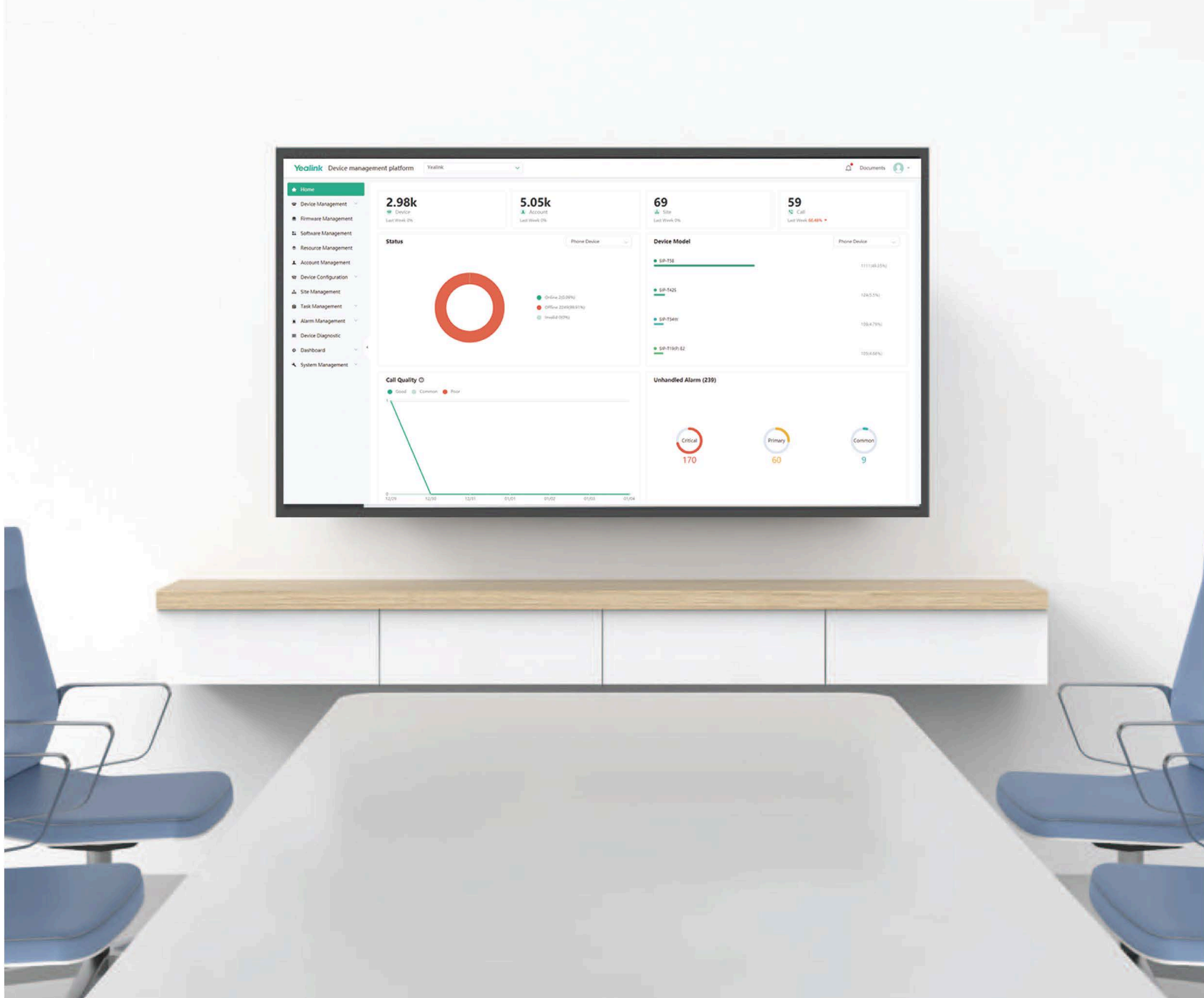
Yealink Device Management Platform Administrator Guide

V38.10.0.2 | February 2023



Contents

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.

For more supports or services, go to Yealink Technical Support online.

Summary of Changes

- Changes for Release 38, Guide Version V38.10.0.2
- Changes for Release 38, Guide Version V38.10.0.0
- Changes for Release 38, Guide Version V38.8.0.0
- Changes for Release 38, Guide Version V38.5.0.0
- Changes for Release 38, Guide Version V38.2.0.0
- Changes for Release 38, Guide Version V38.1.0.0
- Changes for Release 38, Guide Version V3.8.0.0
- Changes for Release 37, Guide Version V3.7.0.30
- Changes for Release 37, Guide Version V3.7.0.20
- Changes for Release 37, Guide Version V3.7.0.10
- Changes for Release 37, Guide Version V3.7.0.1
- Changes for Release 36, Guide Version V3.6.0.30
- 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 38, Guide Version V38.10.0.2

Major updates have occurred to the following sections:

- Viewing Alarms
- Home Page

Changes for Release 38, Guide Version V38.10.0.0

The following section is new for this version:

- Enabling Login Protection

Major updates have occurred to the following sections:

- Verifying the Installation Package
- Hardware and Software Requirements
- Logging into YDMP
- Adding and Managing Sub-Administrator Accounts

Changes for Release 38, Guide Version V38.8.0.0

Major updates have occurred to the following section:

- Home Page
- Verifying the Installation Package

Changes for Release 38, Guide Version V38.5.0.0

The following section is new for this version:

Verifying the Installation Package

Major updates have occurred to the following section:

- Supported Device Models
- Updating YDMP (from V3.1 to V3.X)

Changes for Release 38, Guide Version V38.2.0.0

Major updates have occurred to the following sections:

- Hardware and Software Requirements
- Supported Device Models
- Pushing Configuration Files to Devices
- Connecting Phone Devices and Room Systems (Except for MVC/ZVC)
- Viewing Alarms

Changes for Release 38, Guide Version V38.1.0.0

The following sections are new for this version:

- Exporting Sites
- Setting the Configuration Policy

Major updates have occurred to the following sections:

- Supported Device Models
- Exporting the Device Information
- Device Managing Features and Their Supported Devices
- Adding Alarm Strategies
- Viewing Alarms
- Taking the Screenshot of the Device

Changes for Release 38, Guide Version V3.8.0.0

The following sections are new for this version:

- Making Parameters Mandatory and Pushing Them to Devices
- Pushing SkypeSettings Files to Microsoft Teams Rooms

Major updates have occurred to the following sections:

- Supported Device Models
- Adding Sites
- Device Managing Features and Their Supported Devices
- How to Change/Customize Port 443 If It Is Occupied
- Viewing the Detailed Information of Phone Devices

Changes for Release 37, Guide Version V3.7.0.30

Major updates have occurred to the following sections:

- Pushing Firmware to Devices

Changes for Release 37, Guide Version V3.7.0.20

From this version, we support manage Wordskpace devices and Yealink USB Connect software.

The following sections are new for this version:

- Connecting Workspace Devices
- Updating Software of USB Devices
- Managing USB Software
- How to Change/Customize Port 443 If It Is Occupied
- Uploading Multilingual Template for Importing Devices

Major updates have occurred to the following sections:

- Supported Device Models
- Hardware and Software Requirements

- Home Page
- Device Managing Features and Their Supported Devices
- Editing the Device Information
- Assigning Accounts to Devices
- Pushing Configuration Files to Devices
- Pushing Firmware to Devices
- Pushing Resource Files to Devices
- Resetting the Devices to Factory

Changes for Release 37, Guide Version V3.7.0.10

Major updates have occurred to the following sections:

- Home Page
- Capturing Packets
- Setting the Log Level
- Download the Device Log

Changes for Release 37, Guide Version V3.7.0.1

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

The following sections are new for this version:

- Auto Provisioning
- Device Managing Features and Their Supported Devices

Major updates have occurred to the following sections:

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

Changes for Release 36, Guide Version V3.6.0.30

The following sections are new for this version:

- Viewing the Devices Statistics

Major updates have occurred to the following sections:

- Managing SIP Devices-Searching for Devices
- Pushing Configuration Files to Devices
- Managing USB Devices-Searching for Devices
- Managing Room System-Searching for Devices
- Viewing the Detailed Information of Phone Devices
- Adding Firmware
- Adding Resource Files

- Adding Configuration Templates
- Uploading Configuration Files
- Capturing Packets
- Viewing Alarms
- Viewing Call Quality Statistics
- Assigning the Data Permission
- Editing the Account Information

Changes for Release 36, Guide Version V3.6.0.20

Major updates have occurred to the following sections:

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

Changes for Release 36, Guide Version V3.6.0.10

The following sections are new for this version:

- Resetting the Devices to Factory
- Backing up Configuration Files

Major updates have occurred to the following sections:

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

Changes for Release 36, Guide Version V3.6.0.1

The following sections are new for this version:

- Setting the Device Log

Major updates have occurred to the following sections:

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

Changes for Release 35, Guide Version V3.5.0.21

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 section is 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:

Note:

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

Device Types	Supported Device Models	Version Requirements
Voice Communication Phone	T27P/T27G/ T29G/T41P/T41S/T42G/T42S/ T42U/T46G/ T46S/T48G/T48S/T52S/T54S	XX.83.0.30 or later (except for XX.84.0.10). XX represents the fixed number for each device model.
	T56A/T58	58.83.0.5 or later.
	T53/T53W	95.84.0.10 or later.
	T54W	96.84.0.10 or later.
	T57W	97.84.0.30 or later.
	T42U/T43U/T46U/T48U	108.84.0.30 or later.
	T30/T30P/T31/T31P/T31G/T33P/ T33G	124.85.0.10 or later.
	T53C	96.86.0.20 or later.
	T58W	150.86.0.5 or later.
DECT Phone	W60B	77.85.0.25 or later.
	W70B	146.85.0.20 or later.
	W80DM	103.83.0.20 or later.
	W90DM	130.85.0.20 or later.
Conference Phone	CP960	73.83.0.10 or later.
	CP920	78.84.0.15 or later.
	CP925	149.85.254.26 or later.
	CP965	148.85.254.31 or later.
	CP935W	143.85.254.32 or later.
Video Phone	VP59	91.283.0.10 or later.
Zoom Phone	CP960	73.30.0.10 or later.
	MP54, MP56, MP58	122.30.0.10 or later.
	VP59	91.30.0.20 or later.
Microsoft Skype for Business Desk Phone	T41S/T42S/T46S/T48S	66.9.0.45 or later (except for 66.9.0.46).
	T58/T56A/T55A	55.9.0.6 or later.
	CP960	73.8.0.27 or later.
	MP56	122.9.0.1 or later.
	MP54/MP58	122.9.0.5 or later.

Device Types	Supported Device Models	Version Requirements
Microsoft Teams Desk Phones	CP960	73.15.0.20 or later.
	T56A/T58	58.15.0.20 or later.
	T55A	58.15.0.36 or later.
	VP59	91.15.0.16 or later.
	MP56	122.15.0.9 or later.
	MP54/MP58	122.15.0.25 or later.
	MP52	145.15.0.4 or later.
	VC210	118.15.0.20 or later.
Microsoft Teams Collaboration Bar	MeetingBar A20	133.15.0.20 or later.
	MeetingBar A30	133.15.0.42 or later.
Zoom Rooms Collaboration Bar	MeetingBar A20/A30	133.30.0.35 or later.
Microsoft Teams Room System/ Zoom Rooms Kit/ RingCentral Room Kit/ Bluejeans Room Kit	MVC500/MVC800/MVC300/ CP960-UVC Zoom Rooms Kit/ VP59 Zoom Rooms Kit	XX.11.0.10 or later.
	MVC840/MVC640/MVC940	UVC84: 262.410.0.10 or later.
	MVC400	UVC40: 2.2.23.0 or later.
	MVC320	UVC30: 105.422.0.10 or later.
	MVC660/MVC860	UVC86: 151.410.0.20 or later.
	MeetingBar A20/A30 (Tencent)	133.50.400.11 or later.
	MeetingBar A20/A30 (BlueJeans)	133.50.401.2 or later.
	MeetingBar A20/A30 (RingCentral)	133.50.25.15 or later.
VC Room System	VC200/VC500/VC800/VC880	XX.32.10.25/XX.32.0.25 or later. XX represents the fixed number for each device model.
	PVT950/PVT980	1345.32.10.40 or later.
	PVT940/PVT960	120.43.0.25 or later.
	VP59	91.332.0.10 or later.
	MeetingEye 600/MeetingEye 400	120.43.0.5 or later.
	MeetingEye 400 Pro	YMS: 133.352.0.1 or later Cloud: 133.352.1000.1 or later
	MeetingEye 800	129.351.0.10 or later.
	VC200-E/VC210 Pro	118.50.0.10 or later.
	VC210	118.43.0.1 or later.
	PVT920	118.351.0.1 or later.
Intelligent Room Device	RoomCast	144.350.0.20 or later.

Device Types	Supported Device Models	Version Requirements
	RoomCast (Zoom)	144.30.0.3 or later.
	RoomPanel	147.510.0.10 or later.
	RoomPanel (Teams)	147.15.0.7 or later.
	RoomPanel (Zoom)	147.30.0.10 or later.
USB Device	BH72, BH76, BT50, CP700, CP900. MP50, UH33 E2, UH34, UH36, UH38, UVC20, UVC34, UVC50, UVC80, WH63, WH66, WH67	The software version of Yealink USB connect should be higher than 0.33.32.0.
	UVC84, UVC86	The software version of Yealink RoomConnect should be higher than 282.24.42.0. UVC84: 262.423.0.72 or later UVC86: 151.410.0.26 or later
	BT51	The software version of Yealink USB connect should be higher than 0.34.0.10.

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.
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.

Note: If you want to change the 443 port, refer to How to Change/Customize Port 443 If It Is Occupied.

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:

- CentOS: 7.5, 7.9, and 8.1 (supported since version 3.5.0.20)
- Red Hat Enterprise Linux: 7.5, 7.9, 8.0, 8.5 (supported since version 38.2.0.0), and 8.6 (supported since version 38.10.0.0)

Requirements for stand-alone installation:

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

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	20 G	At least 250 G for 6000 devices, and the capacity of the hard drive increases by 30 G with every 1000 devices added.
30000~50000	8-core	24 G	
50000~100000	16-core	24 G	

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 200 G 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 50 G 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 commands:

```
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 commands:

```
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 commands:

   ```
   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 commands 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.

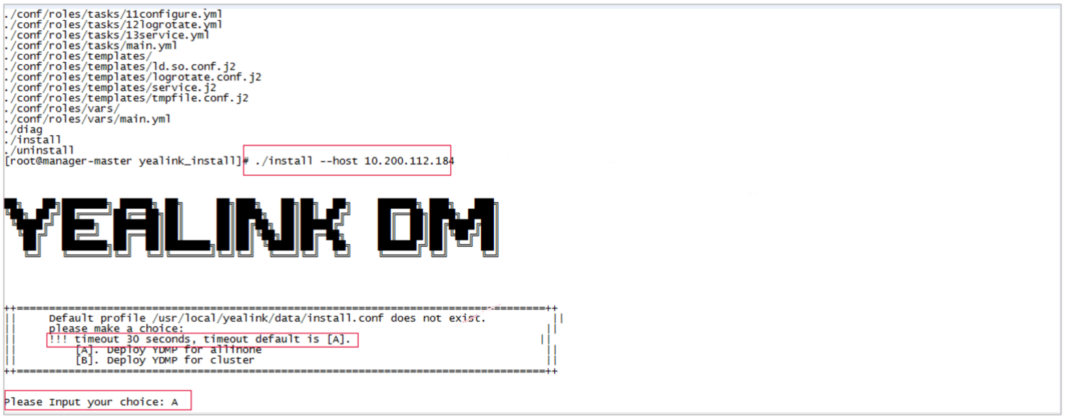
Procedure

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

   ```
   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. Only
 3.3.0.0 or later versions can be supported. ##
```

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



```
./conf/roles/tasks/11configure.yml
./conf/roles/tasks/12logrotate.yml
./conf/roles/tasks/13service.yml
./conf/roles/tasks/main.yml
./conf/roles/templates/
./conf/roles/templates/ld.so.conf.j2
./conf/roles/templates/logrotate.conf.j2
./conf/roles/templates/service.j2
./conf/roles/templates/tmpfile.conf.j2
./conf/roles/vars/
./conf/roles/vars/main.yml
./diag
./install
./uninstall
[root@manager-master yealink_install]# ./install --host 10.200.112.184

YEALINK DM

++==========================================================================++
||     Default profile /usr/local/yealink/data/install.conf does not exist.  ||
||     please make a choice:                                                 ||
||     !!! timeout 30 seconds, timeout default is [A].                      ||
||         [A]. Deploy YDMP for allinone                                     ||
||         [B]. Deploy YDMP for cluster                                      ||
++==========================================================================++

Please Input your choice: A
```

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
- Verifying the Installation Package
- 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 of */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 of */usr/local*.

```
cd /usr/local
```

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

Verifying the Installation Package

Since version 38.5.0.0, YDMP provides SHA1 (stands for Secure Hash Algorithm) and MD5 (stands for Message Digest) algorithms to use the verification codes to verify the authenticity and integrity of the installation package.

About this task

Note that the verification codes are unique and vary from each version.

The SHA1 and MD5 verification codes for each version are as below:

Version	Codes
38.5.0.0	• **SHA1**: 07e255d9688621c71168bb227cceedacf22bd7a8 • **MD5**: df7db2835c37862b7bd98fdd04865e51
38.8.0.0	• **SHA1:** 48533c407988b0b3a115602201095cbc528ef03b • **MD5:** 0f00bfbc56ee5ffff84b0851a43c5653
38.10.0.0	• **SHA1:**fa8fe965e7c76a53c5d25dfd18738d4d3c9799b6 • **MD5:** 80c61321af9863013dce62ef4b68bdac

Procedure

1. Upload Uploadthe installation package to *cd /usr/local*.
2. Run the following commands:

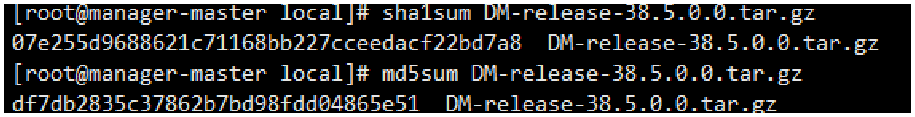
```
sha1sum DM-release-38.5.0.0.tar.gz
```

or

```
md5sum DM-release-38.5.0.0.tar.gz
```

Results

If the verification code you get is the same as the preceding one, it is the authentic installation package for YDMP. Otherwise, unauthorized people might have tempered with it.



```
[root@manager-master local]# sha1sum DM-release-38.5.0.0.tar.gz
07e255d9688621c71168bb227cceedacf22bd7a8  DM-release-38.5.0.0.tar.gz
[root@manager-master local]# md5sum DM-release-38.5.0.0.tar.gz
df7db2835c37862b7bd98fdd04865e51  DM-release-38.5.0.0.tar.gz
```

Unzipping the Installation Package

Run the following commands:

```
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.

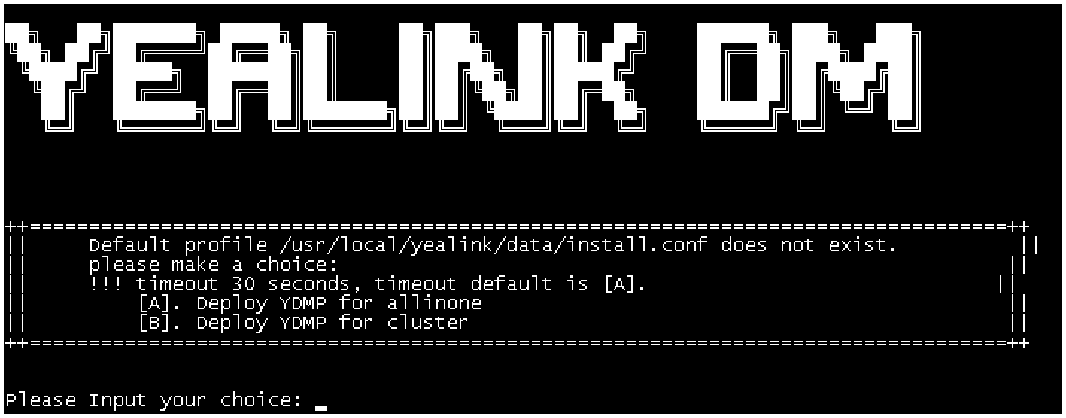
Before you begin

- 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 commands:

```
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.##
```



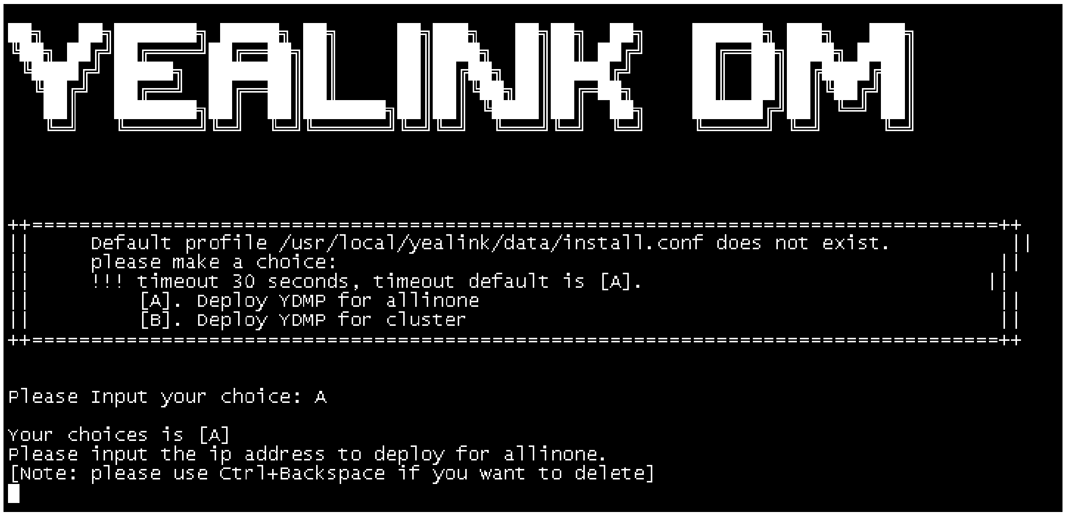
```
++==========================================================================++
||     Default profile /usr/local/yealink/data/install.conf does not exist.   ||
||     please make a choice:                                                ||
||     !!! timeout 30 seconds, timeout default is [A].                     ||
||         [A]. Deploy YDMP for allinone                                    ||
||         [B]. Deploy YDMP for cluster                                     ||
++==========================================================================++

Please Input your choice: _
```

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.

      ```
      ++====================================================================================++
      ||      Default profile /usr/local/yealink/data/install.conf does not exist.             ||
      ||      please make a choice:                                                           ||
      ||      !!! timeout 30 seconds, timeout default is [A].                                ||
      ||          [A]. Deploy YDMP for allinone                                               ||
      ||          [B]. Deploy YDMP for cluster                                                ||
      ++====================================================================================++


      Please Input your choice: A

      Your choices is [A]
      Please input the ip address to deploy for allinone.
      [Note: please use Ctrl+Backspace if you want to delete]
      ```

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

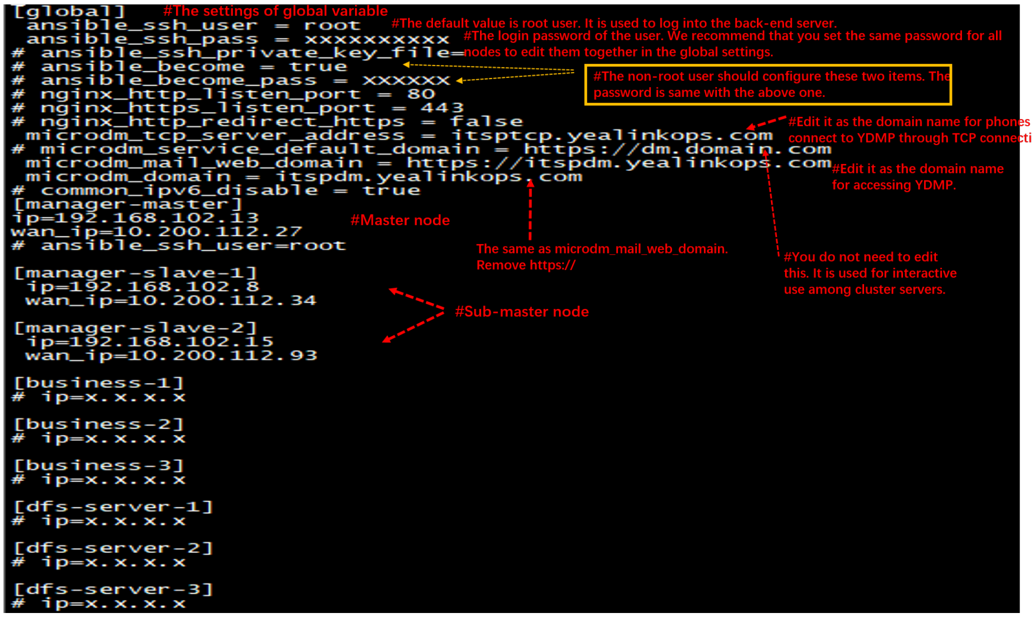
      Run command *vi*, edit the configuration template, and fill in the desired cluster information. Run *./ install* again.

    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
```



```
[global]
 ansible_ssh_user = root
 ansible_ssh_pass = xxxxxxxxxx
# ansible_ssh_private_key_file=
# ansible_become = true
# ansible_become_pass = xxxxxx
# nginx_http_listen_port = 80
# nginx_https_listen_port = 443
# nginx_http_redirect_https = false
 microdm_tcp_server_address = itsptcp.yealinkops.com
# microdm_service_default_domain = https://dm.domain.com
 microdm_mail_web_domain = https://itspdm.yealinkops.com
 microdm_domain = itspdm.yealinkops.com
# common_ipv6_disable = true
[manager-master]
ip=192.168.102.13
wan_ip=10.200.112.27
# ansible_ssh_user=root

[manager-slave-1]
 ip=192.168.102.8
 wan_ip=10.200.112.34

[manager-slave-2]
 ip=192.168.102.15
 wan_ip=10.200.112.93

[business-1]
# ip=x.x.x.x

[business-2]
# ip=x.x.x.x

[business-3]
# ip=x.x.x.x

[dfs-server-1]
# ip=x.x.x.x

[dfs-server-2]
# ip=x.x.x.x

[dfs-server-3]
# ip=x.x.x.x
```

#The settings of global variable

#The default value is root user. It is used to log into the back-end server.

#The login password of the user. We recommend that you set the same password for all nodes to edit them together in the global settings.

#The non-root user should configure these two items. The password is same with the above one.

#Edit it as the domain name for phones to connect to YDMP through TCP connection.

#Edit it as the domain name for accessing YDMP.

#Master node

The same as microdm_mail_web_domain. Remove https://

#You do not need to edit this. It is used for interactive use among cluster servers.

#Sub-master node

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

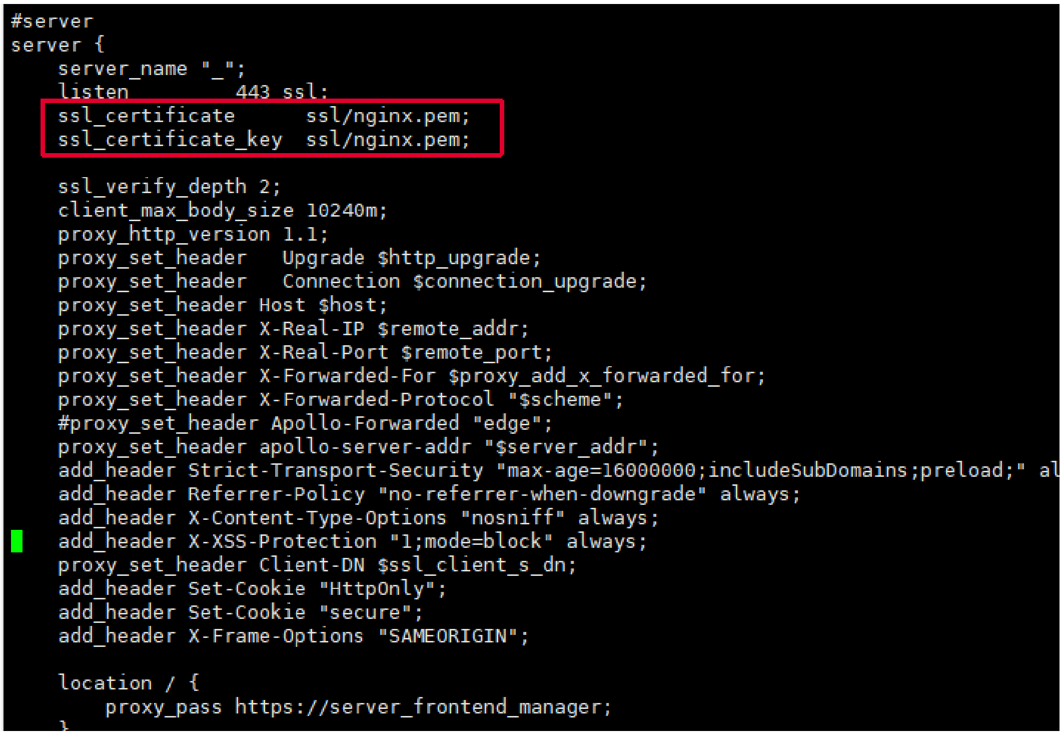
For the cluster deployment, you need to import HTTPS certificate. Otherwise, it will affect the mutual authentication between the phone and the server and cause the failure of pushing the configuration and firmware.

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*.
- Verify the authenticity and integrity of the installation package if the YDMP version is later than 38.5.0.0 (including 38.5.0.0).
- 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 commands:

      ```
      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 commands:

```
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

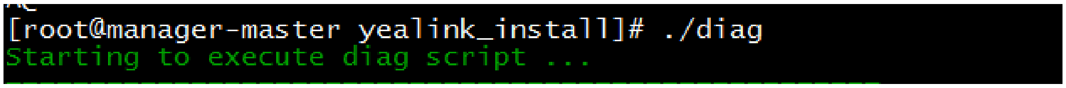
If you fail to install YDMP or some exceptions occur to the service, you can run the diagnostic script to collect the related environment and service information of YDMP, and pack the file named *ydmp_diag_time.tar.gz*. And then, you can provide the developers or operation and maintenance engineers with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

About this task

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

Procedure

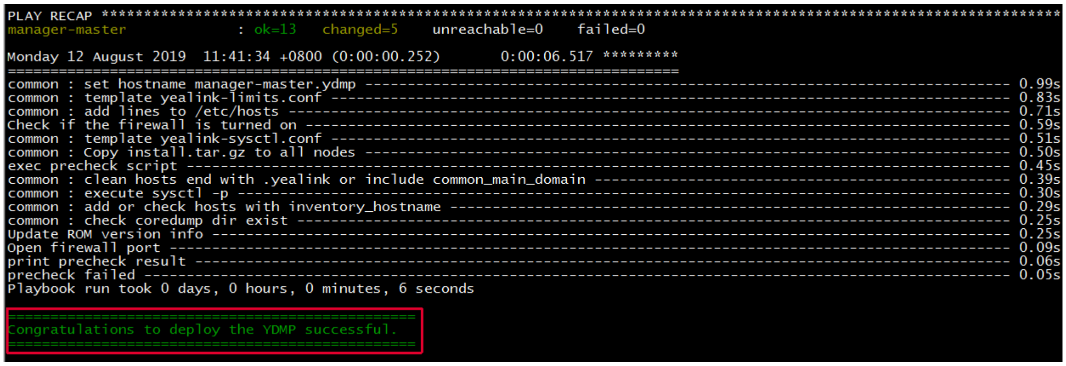
Unzip and run the script.



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

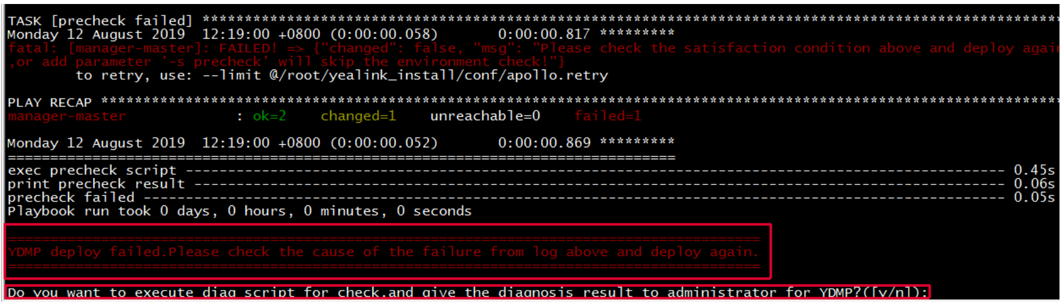
Results

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



```
PLAY RECAP ******************************************************************************************************
manager-master             : ok=13   changed=5    unreachable=0    failed=0

Monday 12 August 2019  11:41:34 +0800 (0:00:00.252)       0:00:06.517 *********
===============================================================================
common : set hostname manager-master.ydmp ------------------------------------------------------------------ 0.99s
common : template yealink-limits.conf ---------------------------------------------------------------------- 0.83s
common : add lines to /etc/hosts --------------------------------------------------------------------------- 0.71s
Check if the firewall is turned on ------------------------------------------------------------------------- 0.59s
common : template yealink-sysctl.conf ---------------------------------------------------------------------- 0.51s
common : Copy install.tar.gz to all nodes ------------------------------------------------------------------ 0.50s
exec precheck script --------------------------------------------------------------------------------------- 0.45s
common : clean hosts end with .yealink or include common_main_domain --------------------------------------- 0.39s
common : execute sysctl -p --------------------------------------------------------------------------------- 0.30s
common : add or check hosts with inventory_hostname -------------------------------------------------------- 0.29s
common : check coredump dir exist -------------------------------------------------------------------------- 0.25s
Update ROM version info ------------------------------------------------------------------------------------ 0.25s
Open firewall port ----------------------------------------------------------------------------------------- 0.09s
print precheck result -------------------------------------------------------------------------------------- 0.06s
precheck failed -------------------------------------------------------------------------------------------- 0.05s
Playbook run took 0 days, 0 hours, 0 minutes, 6 seconds

================================================
Congratulations to deploy the YDMP successful.
================================================
```

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



```
TASK [precheck failed] ******************************************************************************************
Monday 12 August 2019  12:19:00 +0800 (0:00:00.058)       0:00:00.817 *********
fatal: [manager-master]: FAILED! => {"changed": false, "msg": "Please check the satisfaction condition above and deploy agai
,or add parameter '-s precheck' will skip the environment check!"}
        to retry, use: --limit @/root/yealink_install/conf/apollo.retry

PLAY RECAP ******************************************************************************************************
manager-master             : ok=2    changed=1    unreachable=0    failed=1

Monday 12 August 2019  12:19:00 +0800 (0:00:00.052)       0:00:00.869 *********
===============================================================================
exec precheck script --------------------------------------------------------------------------------------- 0.45s
print precheck result -------------------------------------------------------------------------------------- 0.06s
precheck failed -------------------------------------------------------------------------------------------- 0.05s
Playbook run took 0 days, 0 hours, 0 minutes, 0 seconds

================================================================================
YDMP deploy failed.Please check the cause of the failure from log above and deploy again.
================================================================================

Do you want to execute diag script for check.and give the diagnosis result to administrator for YDMP?([y/n]):
```

Activating the License

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

Procedure

1. Importing the Device Certificate.
2. Activating the License Onlineor 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.

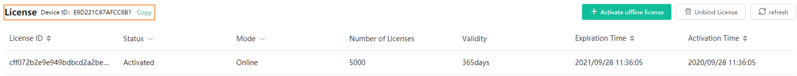
Procedure

1. Click **System Management** > **License**.

2. Select the desired 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:



License ID	Status	Mode	Number of Licenses	Validity	Expiration Time	Activation Time
cff072b2e9e949bdbcd2a2be...	Activated	Online	5000	365days	2021/09/28 11:36:05	2020/09/28 11:36:05

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.

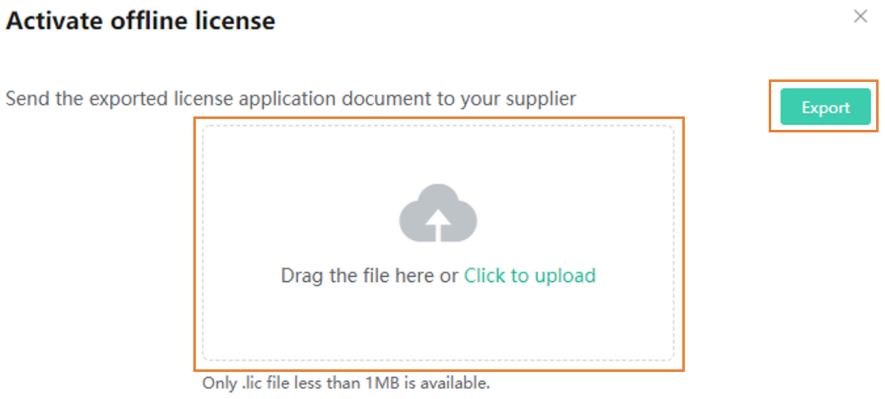
Before you begin

- 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**. 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.



Activate offline license

Send the exported license application document to your supplier

Drag the file here or Click to upload

Only .lic file less than 1MB is available.

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

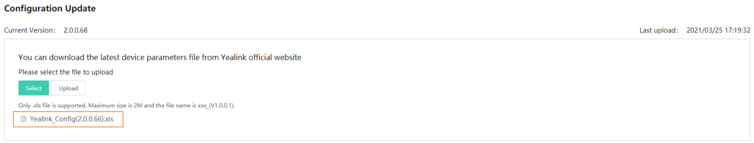
The authorized license is displayed on the page.

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 Yealink Support.

Procedure

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



Configuration Update

Current Version: 2.0.0.68

Last upload: 2021/03/25 17:19:32

You can download the latest device parameters file from Yealink official website

Please select the file to upload

Only .xls file is supported. Maximum size is 2M and the file name is xxx_(V1.0.0.1).

Yealink_Config(2.0.0.66).xls

   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.

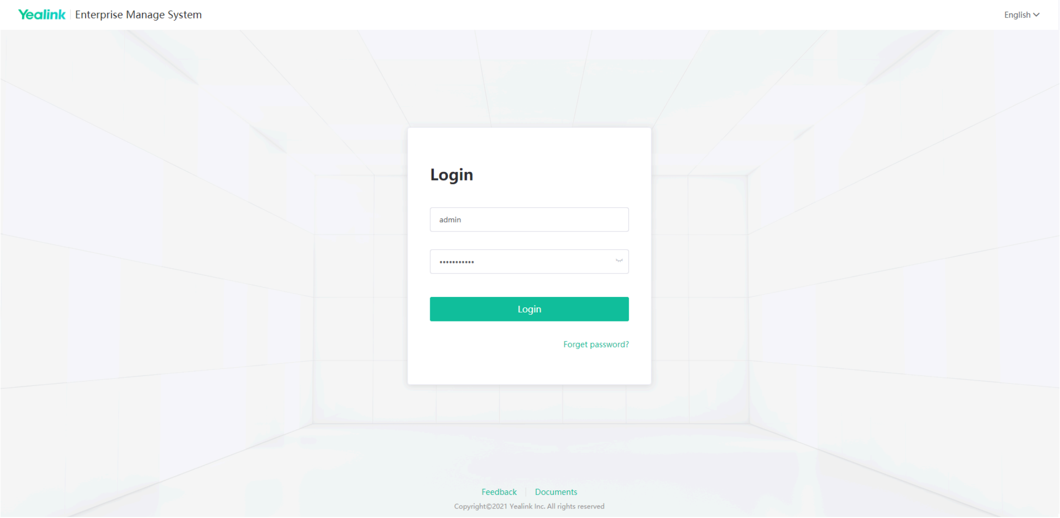
Getting Started

- Logging into YDMP
- Home Page
- Logging out of YDMP

Logging into YDMP

Procedure

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



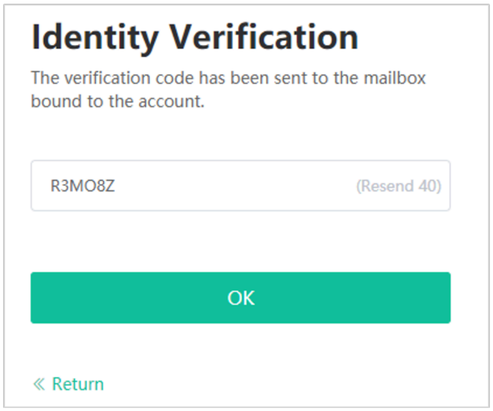
admin

•••••••••••

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. If it is the first time you log in, please change the password according to the system prompts.

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

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

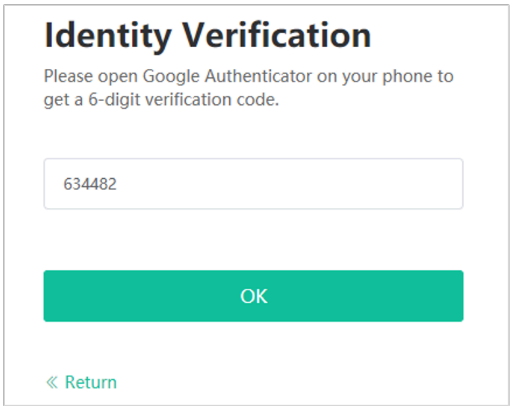


Identity Verification

The verification code has been sent to the mailbox bound to the account.

R3MO8Z (Resend 40)

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



Identity Verification

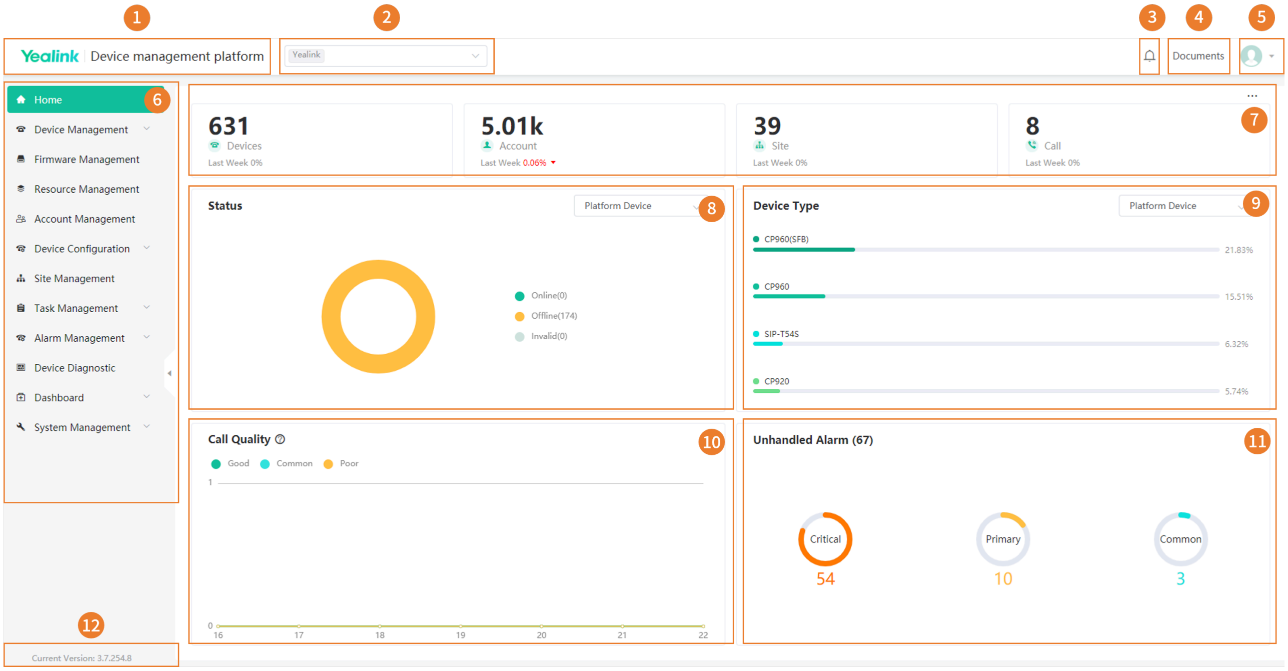
Please open Google Authenticator on your phone to get a 6-digit verification code.

634482

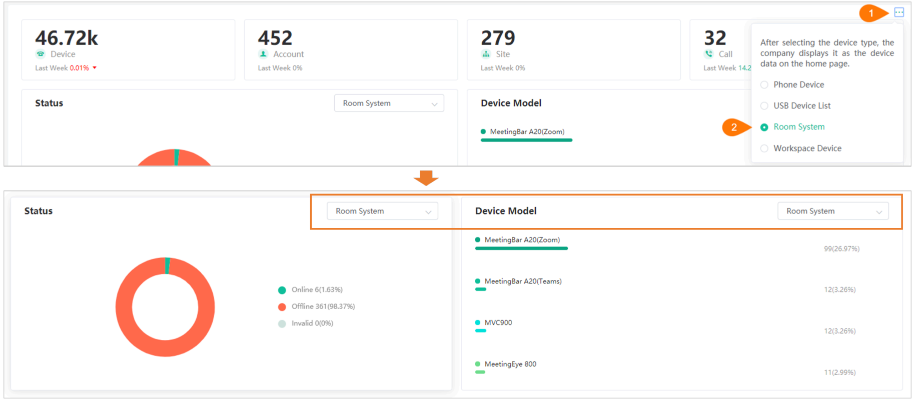
7. After finishing the preceding procedures, you will go to the YDMP homepage.

Home Page

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



Number	Description
1	The platform name.
2	Select a site. After you select a site, the Call Quality module on the home page will only display the data related to the selected site.
3	Display number of unread alarms and the type of alarms.

Number	Description
4	Go to the website of Yealink Support to download documents.
5	Go to the page of setting the administrator account. You can also change the desired display language. Now, we support Simplified Chinese, English, Español, Portugués (Brazil), and Deutsch.
6	Navigation pane.
7	**Overview:** • Display the number of devices, accounts, sites, and calls. • Click the desired module to go to the corresponding module. • For enterprise administrators, you can set the default device display type for the **Status** and **Device Model** modules on the Home page. After you set the default device type, all accounts in the enterprise can see the default device type on the **Status** and **Device Model** modules after they sign in to the platform.  After selecting the device type, the company displays it as the device data on the home page. ○ Phone Device ○ USB Device List ● Room System ○ Workspace Device 46.72k Device Last Week 0.01% 452 Account Last Week 0% 279 Site Last Week 0% 32 Call Last Week 14.2 1 2 Status Room System Device Model MeetingBar A20(Zoom) Status Room System Online 6(1.63%) Offline 361(98.37%) Invalid 0(0%) Device Model Room System MeetingBar A20(Zoom) 99(26.97%) MeetingBar A20(Teams) 12(3.26%) MVC900 12(3.26%) MeetingEye 800 11(2.99%)
8	**Status:** • Select a device type. • Display the number of online, offline, and invalid devices. • Click the corresponding device status to go to the page that lists the devices of this status.
9	**Device Type:** • Select a device type. • Display the number of devices in each model. • Click the corresponding model to go to the page that lists the devices in this model.
10	**Call Quality:** • Display the number of calls with good, bad or poor call quality. • You can click the desired module to view the call statistics.
11	**Unhandled Alarms:** • Display the number of critical, major, and minor alarms. • Click the corresponding alarm level to go to the page that lists the alarm in this level.
12	Display the server version.

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

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

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.

About this task

By default, we support using IPv4 to connect phone devices to YDMP. If your phone devices support IPv6, you can also use the IPv6 network to connect phone devices to YDMP.

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 for authentication.

  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**.

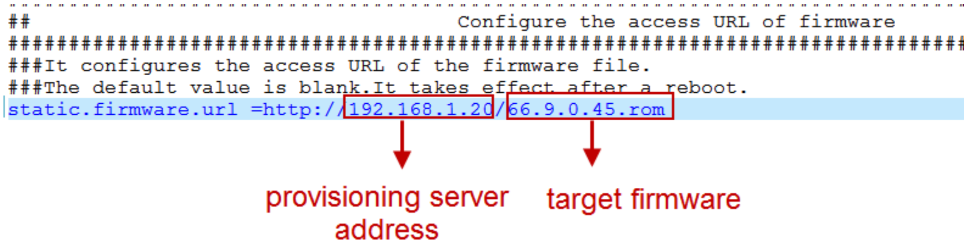
     Only when the authentication succeeds will the device trust YDMP.

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.

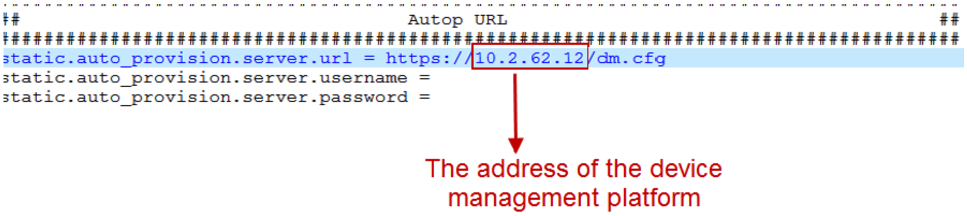
Procedure

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.



```
##                                   Configure the access URL of firmware
###############################################################################
###It configures the access URL of the firmware file.
###The default value is blank.It takes effect after a reboot.
static.firmware.url =http://192.168.1.20/66.9.0.45.rom
```

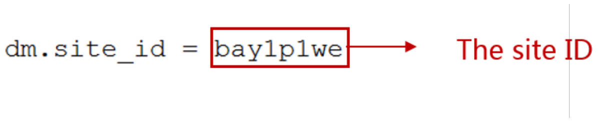
3. Configure the URL of the auto-provisioning server to connect the devices to YDMP.



```
##                                    Autop URL                                   ##
########################################################################################
static.auto_provision.server.url = https://10.2.62.12/dm.cfg
static.auto_provision.server.username =
static.auto_provision.server.password =
```

The address of the device management platform

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



```
dm.site_id = bay1p1we
```

The site ID

Note:

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

  The supported device and firmware version are as below:

Device Type	Model	Version
DECT Phone	W60B	77.85.0.25 or later
	W70B	146.85.0.20 or later
Desk Phone	T27G	69.86.0.5 or later
	T30, T30P, T31, T31P, T31G, T33P, T33G	124.86.0.5 or later
	T41S, T42S, T46S, T48S	66.86.0.5 or later
	T41U, T42U, T46U, T48U	108.86.0.10 or later
	T53, T53C, T53W, T54W, T57W	96.86.0.10 or later
Conference Phone	CP960	73.86.0.5 or later
	CP920	78.86.0.10 or later
Video phones	VP59	91.86.0.5 or later
For Zoom Rooms Collaboration Bars	MeetingBar A20, MeetingBar A30	133.30.0.35 or later

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

5. Save the file.

Results

After auto-provisioning, the devices will be connected to 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 MVC/ZVC Room Systems

About this task

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

Procedure

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

Connecting Workspace Devices

Procedure

1. Do one of the following to perform auto-provision:

Model	Supported Connecting Method
RoomPanel (Teams), RoomPanel (Zoom) and RoomCast	• Configuring the Common.cfg File • Configuring the Server Address

2. Reboot the device.
3. Add the device to the device list on the platform.

Model	Supported Connecting Method
RoomPanel (Teams), RoomPanel (Zoom) and RoomCast	On the YMCS platform, add devices.

Results
You can see the device on the device list and its status is online.

Managing Devices

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

Note:

Phone devices include

The maximum number of devices that you can manage on 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
- Device Managing Features and Their Supported Devices
- Editing the Device Information

- Exporting the Device Information
- Viewing the Detailed Information of Phone Devices
- 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
- Auto Provisioning
- Viewing the Information of Connected Accessories
- Viewing the Devices Statistics
- Updating Software of USB Devices

Device Status

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

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

Device Managing Features and Their Supported Devices

Following is the available features and their supported device type.

Supported Feature	Devices
Exporting the Device Information	Phone device, Room System, USB device,Workspace device
Editing the Device Information	Phone device, Room System, USB device, Workspace Device
Viewing the Detailed Information of Phone Devices	Phone device
Searching for Devices	Phone device, Room System, USB device, Workspace Device
Assigning Accounts to Devices	Phone device, Room System (only applicable to VC Room System and Zoom Rooms Kits)
Setting the Sites	Phone device, Room System, USB device, Workspace Device
Pushing Configuration Files to Devices	Phone device, Room System (only applicable to VC Room System), USB device, Workspace device

Supported Feature	Devices
Pushing Firmware to Devices	Phone device, Room System, USB device, Workspace Device
Pushing Resource Files to Devices	Phone device, Room System (only applicable to VC Room System), USB device, Workspace Device
Diagnosing Devices	Phone device, Room System, Workspace device, USB device
Enabling/Disabling DND	Phone device, Room System (only applicable to VC Room System)
Sending Messages to Devices	Phone device, Room System (only applicable to VC Room System)
Rebooting Devices	Phone device, Room System, Workspace Device
Resetting the Devices to Factory	Phone device, Room System, Workspace Device
Deleting Devices	Phone device, Room System, USB device, Workspace Device
Auto Provisioning	Phone device
Viewing the Information of Connected Accessories	Room System
Updating Software of USB Devices	USB device

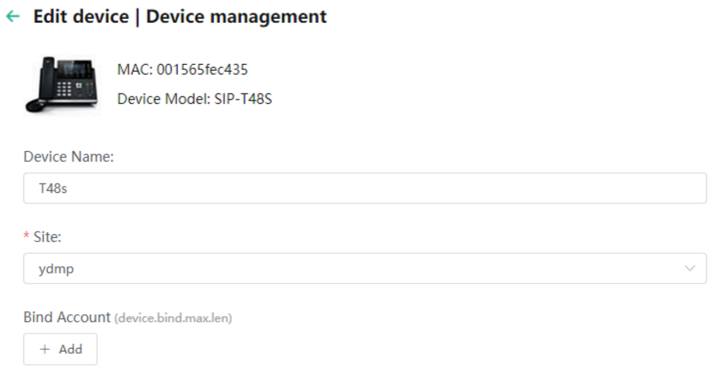
Editing the Device Information

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

Procedure

1. Click **Device Management** > **Phone Device/USB Device/Room System**.
2. Click ✎ beside the desired device.
3. Edit the device information and save it.

   Take the image of phone device as an example.



← Edit device | Device management

MAC: 001565fec435

Device Model: SIP-T48S

Device Name: T48s

* Site: ydmp

Bind Account (device.bind.max.len)

Note: For Teams phones with Hybrid mode enabled, you can assign SIP accounts to them.

Related tasks

Adding Accounts

Setting the Sites

Exporting the Device Information

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

Procedure

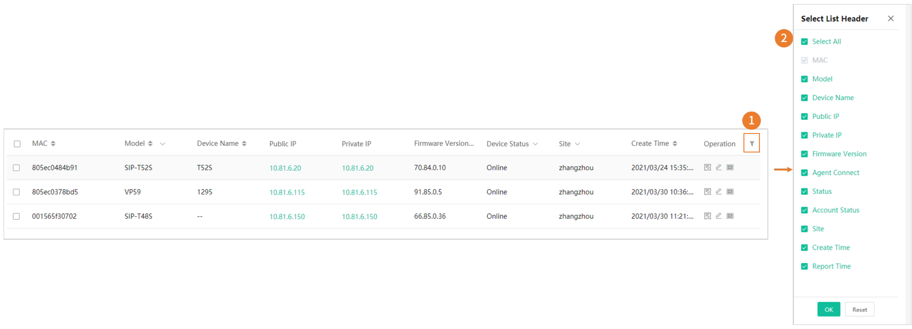
Click **Device Management** > **Phone Device/USB Device/Room System/Worksapce Device** > **Export**.

Viewing the Detailed Information of Phone Devices

You can view the device information, including the MAC address, the model, the name, the IP, the firmware version, the status, the site , the report time and so no. You can customize the desired information.

Procedure

1. Click **Device Management** > **Phone Device**.
2. Click ▼ on the right side of the page and select the desired filter.

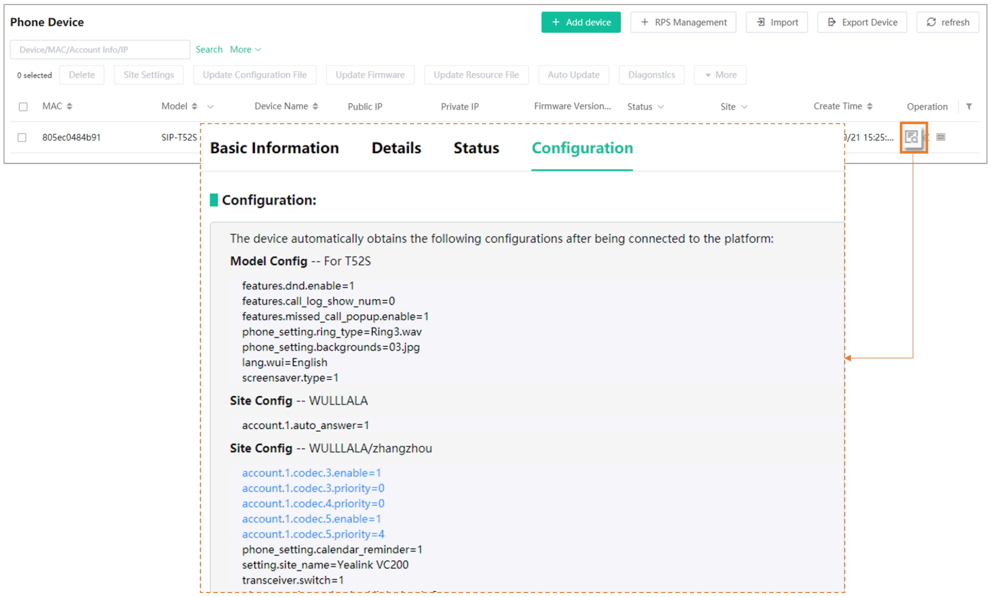


□	MAC	Model	Device Name	Public IP	Private IP	Firmware Version...	Device Status	Site	Create Time	Operation
□	805ec0484b91	SIP-T52S	T52S	10.81.6.20	10.81.6.20	70.84.0.10	Online	zhangzhou	2021/03/24 15:35:...	
□	805ec0378bd5	VP59	1295	10.81.6.115	10.81.6.115	91.85.0.5	Online	zhangzhou	2021/03/30 10:36:...	
□	001565f30702	SIP-T48S	--	10.81.6.150	10.81.6.150	66.85.0.36	Online	zhangzhou	2021/03/30 11:21:...	

Select List Header

☑ Select All
☑ MAC
☑ Model
☑ Device Name
☑ Public IP
☑ Private IP
☑ Firmware Version
☑ Agent Connect
☑ Status
☑ Account Status
☑ Site
☑ Create Time
☑ Report Time

3. Click beside the desired device.



MAC	Model	Device Name	Public IP	Private IP	Firmware Version...	Status	Site	Create Time	Operation
805ec0484b91	SIP-T52S							/21 15:25:...	

Basic Information | Details | Status | Configuration

Configuration:

The device automatically obtains the following configurations after being connected to the platform:

Model Config -- For T52S

```
features.dnd.enable=1
features.call_log_show_num=0
features.missed_call_popup.enable=1
phone_setting.ring_type=Ring3.wav
phone_setting.backgrounds=03.jpg
lang.wui=English
screensaver.type=1
```

Site Config -- WULLLALA

```
account.1.auto_answer=1
```

Site Config -- WULLLALA/zhangzhou

```
account.1.codec.3.enable=1
account.1.codec.3.priority=0
account.1.codec.4.priority=0
account.1.codec.5.enable=1
account.1.codec.5.priority=4
phone_setting.calendar_reminder=1
setting.site_name=Yealink VC200
transceiver.switch=1
```

Note:

- Since the release of V3.6.0.30, YDMP will present the device online time (under the **Status** tab) after the device is connected.
- Click the **Configuration** tab to view the mandatory parameters (blue font) inherited by the device.

Related concepts

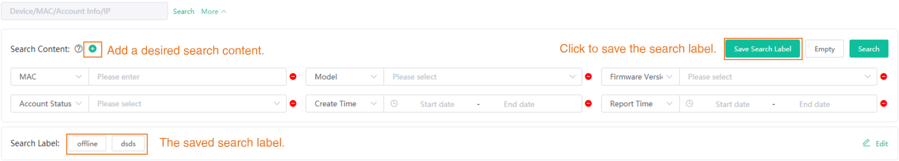
Device Status

Searching for Devices

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

Procedure

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



Add a desired search content.

Click to save the search label.

The saved search label.

The search results are displayed in the device list.

Assigning Accounts to Devices

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

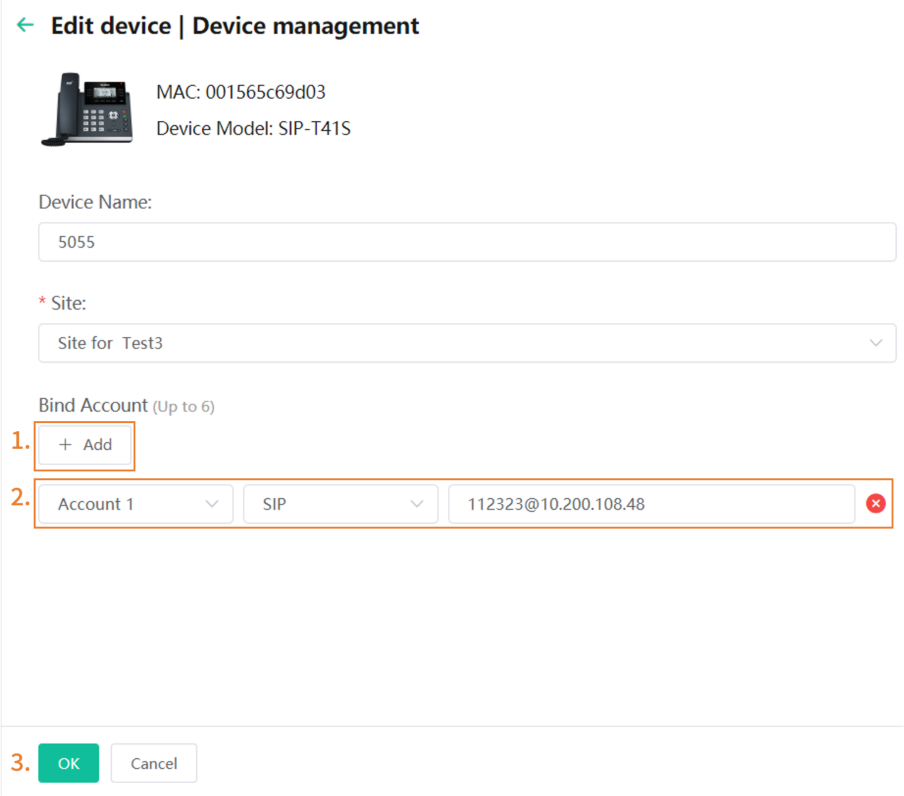
About this task

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

Procedure

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

   Take the image of phone device as an example.



Edit device | Device management

MAC: 001565c69d03

Device Model: SIP-T41S

Device Name: 5055

* Site: Site for Test3

Bind Account (Up to 6)

1. + Add

2. Account 1 | SIP | 112323@10.200.108.48

3. OK Cancel

   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

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

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

Related tasks

Adding Sites

Pushing Configuration Files to Devices

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

Before you begin

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

About this task

Note:

- 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 online, the configuration file will be pushed.

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

Procedure

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

   Note:

   - If you select **Update CFG by model template** and both the current site and the parent site have site configuration, the devices access both the configuration. The priority of the configuration in ascending order is the parent site and the current site.

- If you select **Update CFG by site template**, YDMP will push the configuration of both the parent and the subordinate sites to the selected devices.

  If the devices have the same configuration, the configuration will be overwritten by the pushed configuration.

  The priority of the configuration in ascending order is the parent site and the current site.

  See the following example:

  Table 1: Before pushing configuration:

Configuration of Site A	Configuration of Site A-1	Device in Site A	Device in Site A-1

features.dnd.enable=1
auto_redial.enable=**1**
call_waiting.tone=1
	features.dnd.enable=**0**
	auto_redial.enable=**0**
		features.dnd.enable=**0**	features.key_tone=1

  Table 2: After pushing configuration

Configuration of Site A	Configuration of Site A-1	Device in Site A	Device in Site A-1

features.dnd.enable=**1**
auto_redial.enable=**1**
call_waiting.tone=1
	features.dnd.enable=**0**
	auto_redial.enable=**0**
		features.dnd.enable=**1**
		auto_redial.enable=**1**
		call_waiting.tone=1
			features.key_tone=1
			features.dnd.enable=**0**
			auto_redial.enable=**0**
			call_waiting.tone=1

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

Related concepts

Managing the Device Configuration

Pushing Firmware to Devices

You can push the firmware to one or multiple devices.

Before you begin

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

About this task

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

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

Procedure

1. Click **Device Management** > **Phone Device/USB Device/Room System/Workspace Device**.
2. Select the corresponding devices and click **Update Firmware**.

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

   Note:

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

Related concepts
Managing Firmware

Pushing Resource Files to Devices

You can push resource files to one or multiple devices.

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

About this task

- 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 online, the resource file will be pushed.

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

Procedure

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

   Note:

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

Related concepts
Managing Resources

Diagnosing Devices

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

About this task

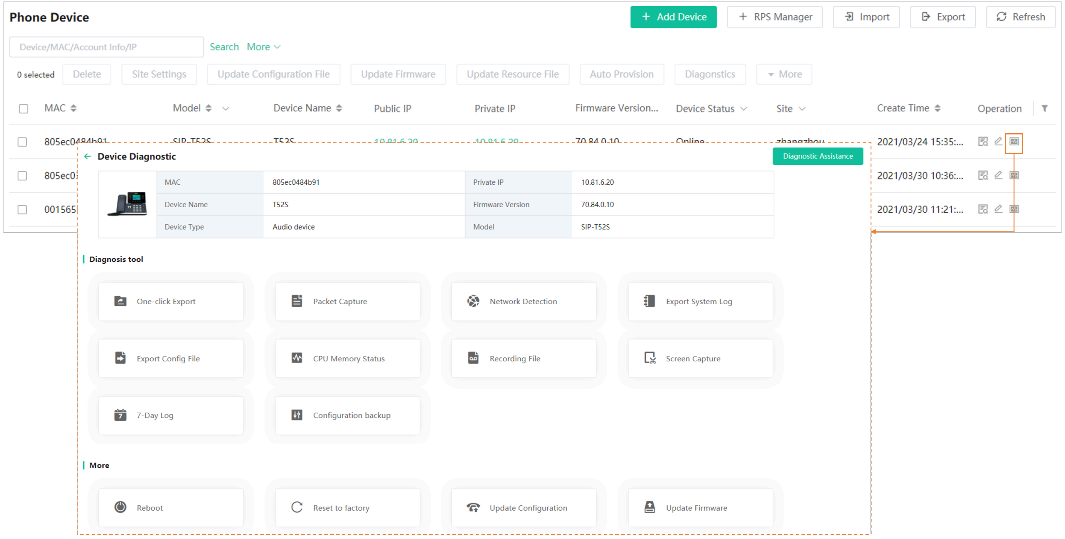
Note:

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

Procedure

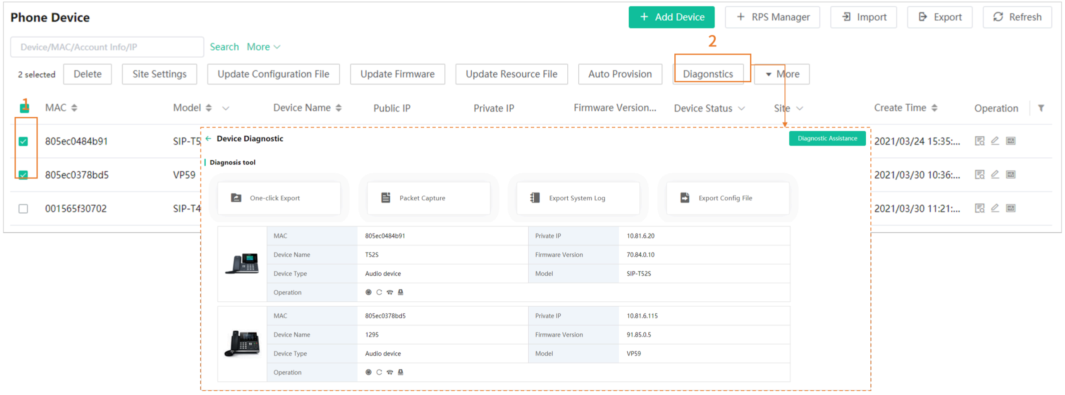
1. Click **Device Management** > **Phone Device/USB Device/Room System**.

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



MAC	805ec0484b91	Private IP	10.81.6.20
Device Name	T52S	Firmware Version	70.84.0.10
Device Type	Audio device	Model	SIP-T52S

    - Diagnose multiple devices



MAC	805ec0484b91	Private IP	10.81.6.20
Device Name	T52S	Firmware Version	70.84.0.10
Device Type	Audio device	Model	SIP-T52S
Operation	● C ☎ 🔒		

MAC	805ec0378bd5	Private IP	10.81.6.115
Device Name	1295	Firmware Version	91.85.0.5
Device Type	Audio device	Model	VP59
Operation	● C ☎ 🔒		

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

Related concepts

Diagnosing Devices

Enabling/Disabling DND

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

About this task

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

Procedure

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

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

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

Sending Messages to Devices

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

About this task

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

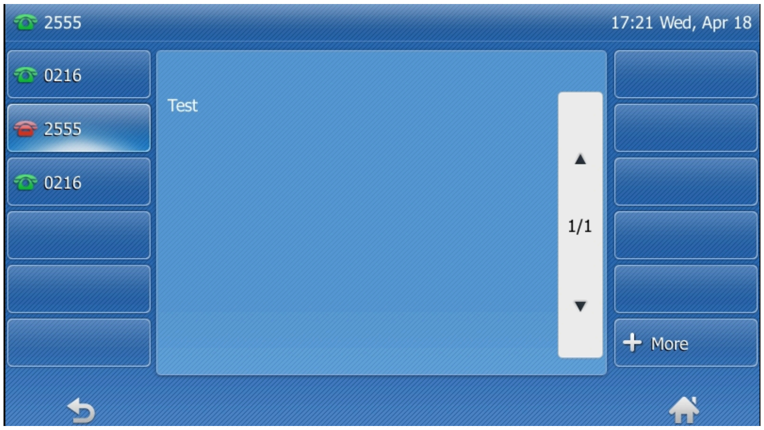
Procedure

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

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

Results

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



Test

Rebooting Devices

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

Procedure

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

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

Resetting the Devices to Factory

About this task

For devices that you have already assigned accounts to, they will automatically obtain the assigned account after reset to factory.

Procedure

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

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

Results

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

  Note:

  - After you reset the device, the device status becomes offline on YDMP. You need to re-deploy the device (Connecting Phone Devices and Room Systems (Except for MVC/ZVC)) 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** > **Phone Device/USB Device/Room System**.
2. Select the corresponding devices and click **Delete**.
3. Click **OK**.

Auto Provisioning

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

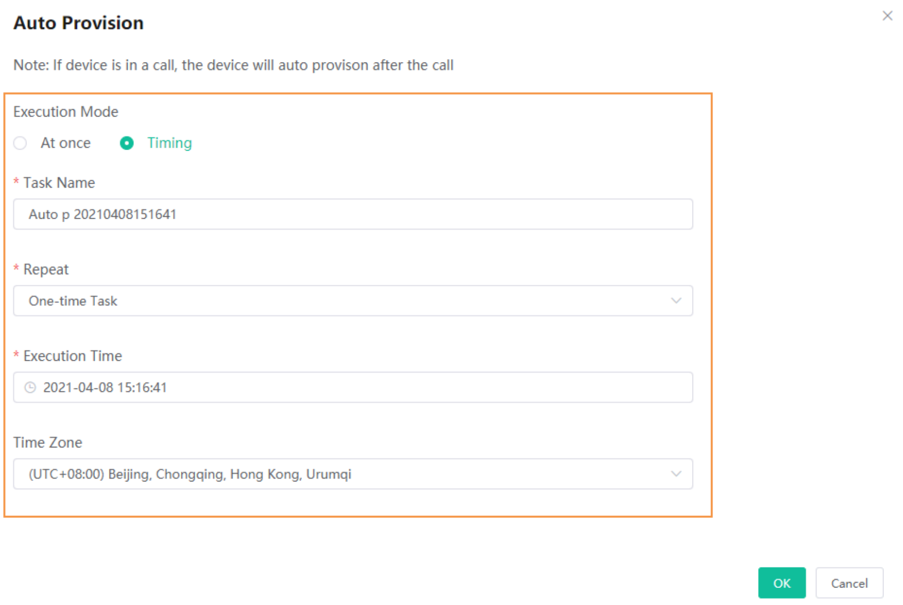
About this task

Note: This feature is only applicable to phone devices.

Procedure

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

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



Auto Provision

Note: If device is in a call, the device will auto provison after the call

Execution Mode

○ At once ● Timing

* Task Name

Auto p 20210408151641

* Repeat

One-time Task

* Execution Time

2021-04-08 15:16:41

Time Zone

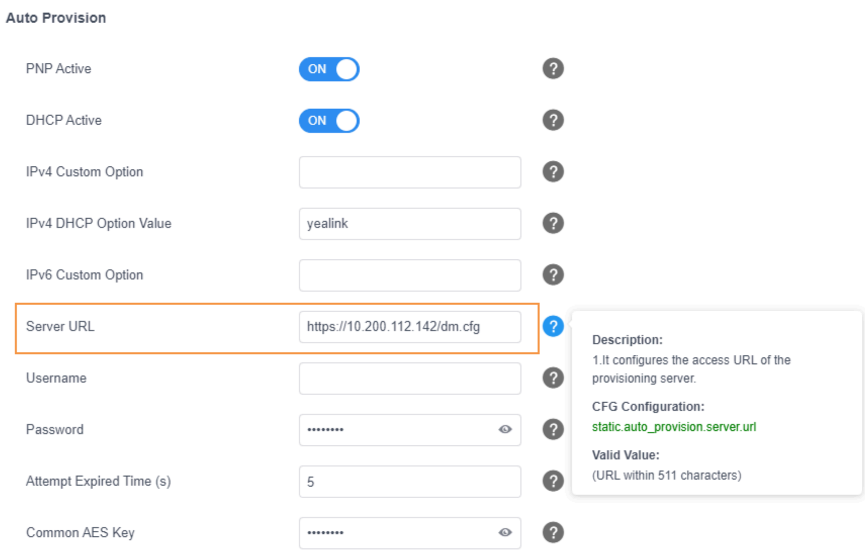
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

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

Results

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

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



Auto Provision

PNP Active: ON

DHCP Active: ON

IPv4 Custom Option:

IPv4 DHCP Option Value: yealink

IPv6 Custom Option:

Server URL: https://10.200.112.142/dm.cfg

Username:

Password: ••••••••

Attempt Expired Time (s): 5

Common AES Key: ••••••••

Description:
1.It configures the access URL of the provisioning server.

CFG Configuration:
static.auto_provision.server.url

Valid Value:
(URL within 511 characters)

Viewing the Information of Connected Accessories

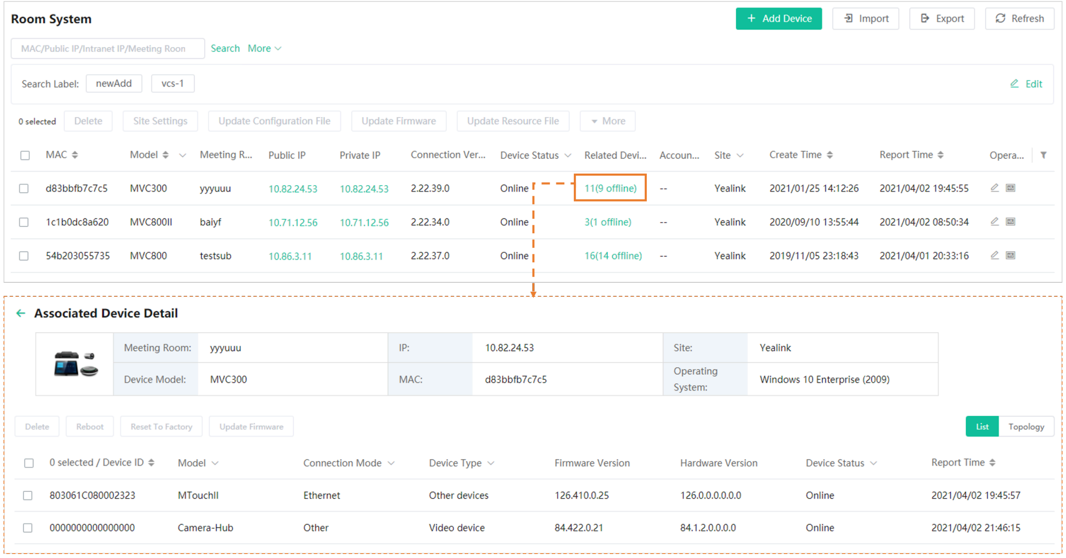
You can view the information of accessories connected to the Room System, including the name, the MAC address, the model, the meeting room name, the IP, the operating system, the status, the site and the report time.

About this task

Note: This feature is only applicable to room system.

Procedure

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



Search Label: newAdd vcs-1

□	MAC	Model	Meeting R...	Public IP	Private IP	Connection Ver...	Device Status	Related Devi...	Accoun...	Site	Create Time	Report Time	Opera...
□	d83bbfb7c7c5	MVC300	yyyuuu	10.82.24.53	10.82.24.53	2.22.39.0	Online	11(9 offline)	--	Yealink	2021/01/25 14:12:26	2021/04/02 19:45:55	
□	1c1b0dc8a620	MVC800II	baiyf	10.71.12.56	10.71.12.56	2.22.34.0	Online	3(1 offline)	--	Yealink	2020/09/10 13:55:44	2021/04/02 08:50:34	
□	54b203055735	MVC800	testsub	10.86.3.11	10.86.3.11	2.22.37.0	Online	16(14 offline)	--	Yealink	2019/11/05 23:18:43	2021/04/01 20:33:16	

Associated Device Detail

Meeting Room:	yyyuuu	IP:	10.82.24.53	Site:	Yealink
Device Model:	MVC300	MAC:	d83bbfb7c7c5	Operating System:	Windows 10 Enterprise (2009)

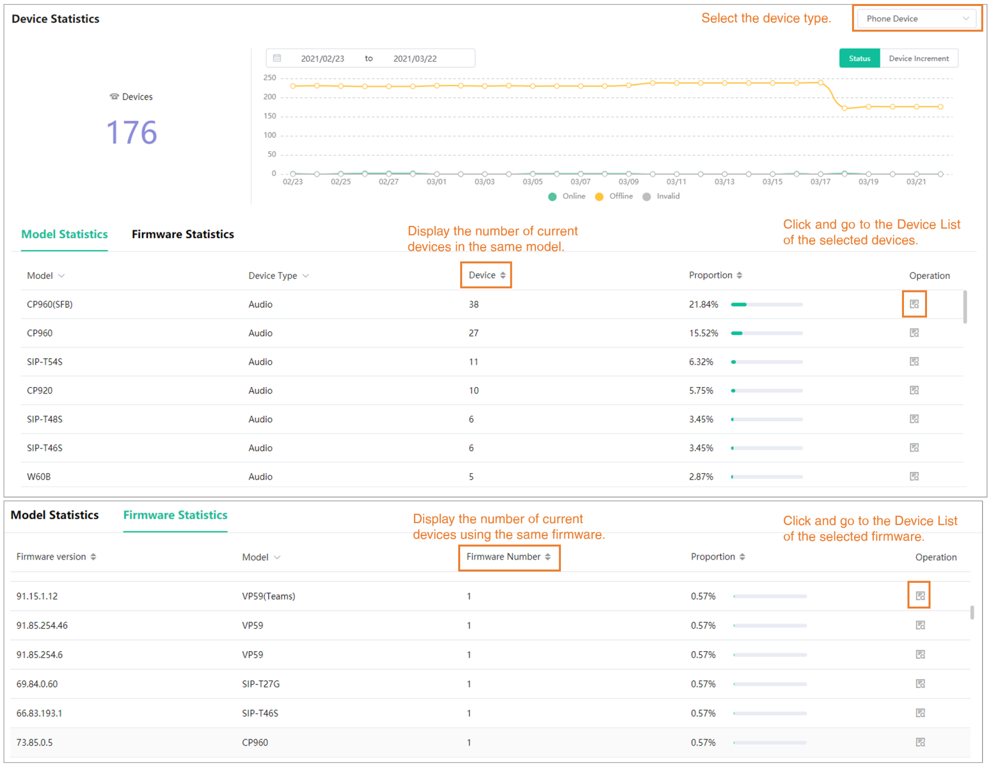
□	0 selected / Device ID	Model	Connection Mode	Device Type	Firmware Version	Hardware Version	Device Status	Report Time
□	803061C080002323	MTouchII	Ethernet	Other devices	126.410.0.25	126.0.0.0.0.0.0	Online	2021/04/02 19:45:57
□	0000000000000000	Camera-Hub	Other	Video device	84.422.0.21	84.1.2.0.0.0.0	Online	2021/04/02 21:46:15

Viewing the Devices Statistics

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

Procedure

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



Model Statistics | Firmware Statistics

Display the number of current devices in the same model.

Click and go to the Device List of the selected devices.

Model	Device Type	Device	Proportion	Operation
CP960(SFB)	Audio	38	21.84%	🔍
CP960	Audio	27	15.52%	🔍
SIP-T54S	Audio	11	6.32%	🔍
CP920	Audio	10	5.75%	🔍
SIP-T48S	Audio	6	3.45%	🔍
SIP-T46S	Audio	6	3.45%	🔍
W60B	Audio	5	2.87%	🔍

Model Statistics | Firmware Statistics

Display the number of current devices using the same firmware.

Click and go to the Device List of the selected firmware.

Firmware version	Model	Firmware Number	Proportion	Operation
91.15.1.12	VP59(Teams)	1	0.57%	🔍
91.85.254.46	VP59	1	0.57%	🔍
91.85.254.6	VP59	1	0.57%	🔍
69.84.0.60	SIP-T27G	1	0.57%	🔍
66.83.193.1	SIP-T46S	1	0.57%	🔍
73.85.0.5	CP960	1	0.57%	🔍

Updating Software of USB Devices

About this task

- When the device is in a call, the software will not be updated until the call is finished.
- When the device is offline or invalid, the software cannot be updated.
- When the device is online, the software will be updated.

Procedure

1. Click **Device Management** > **USB Device**.
2. Select the corresponding devices and click **Update Software**.
3. In the pop-up window, select the desired version resource, software version, and the execution mode, then click **OK**.

   Note:

   - After updating the software, you can see the task details, refer to Viewing Executed Tasks.
   - If you select **Official Version**, the software is provided by Yealink. You can also select **Custom Version** to select the software uploaded by your enterprise.

Managing Firmware

You can manage all the device firmware on YDMP.

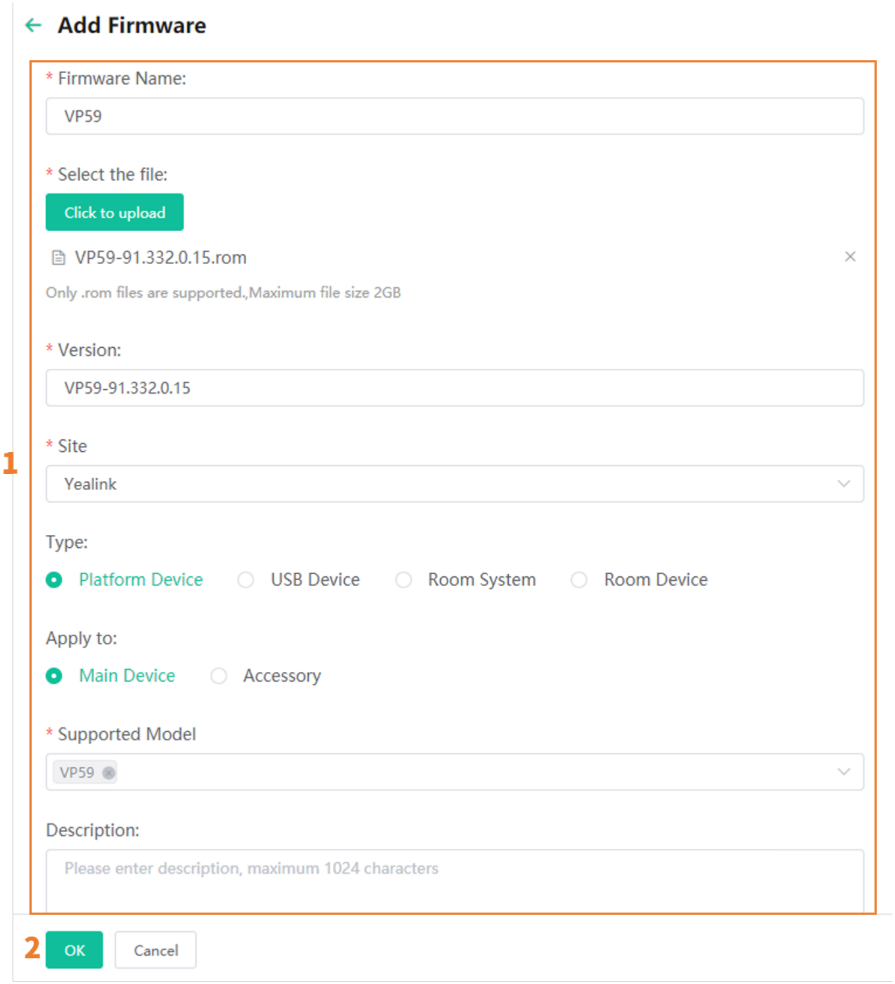
- Adding Firmware
- Sharing Firmware

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

Adding Firmware

Procedure

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



Add Firmware

* Firmware Name:
VP59

* Select the file:
Click to upload
VP59-91.332.0.15.rom
Only .rom files are supported.,Maximum file size 2GB

* Version:
VP59-91.332.0.15

* Site
Yealink

Type:
● Platform Device ○ USB Device ○ Room System ○ Room Device

Apply to:
● Main Device ○ Accessory

* Supported Model
VP59

Description:
Please enter description, maximum 1024 characters

OK Cancel

Sharing Firmware

You can share the desired firmware to others by sending the firmware address. Also, you can get devices to access this address to obtain the firmware by pushing M7 configuration lines.

Procedure

1. Click **Firmware Management**.

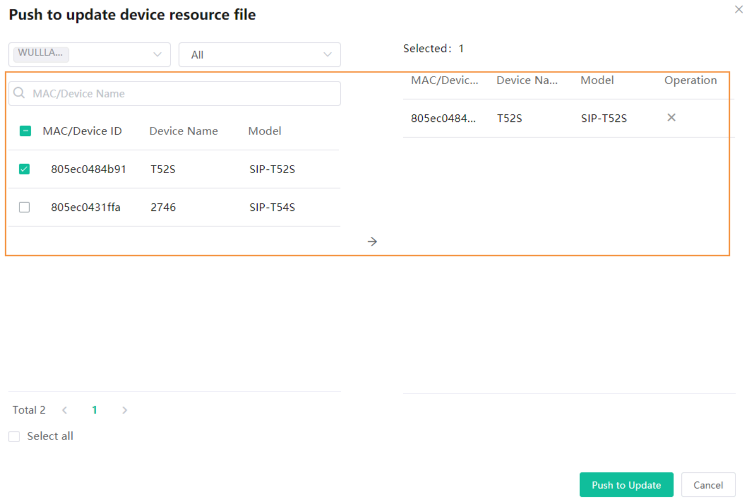
2. Click beside the desired software.
3. Paste and share the address to the desired person.

Pushing Firmware to Devices

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

Procedure

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



Push to update device resource file

WULLLA... | All

Selected: 1

MAC/Device Name

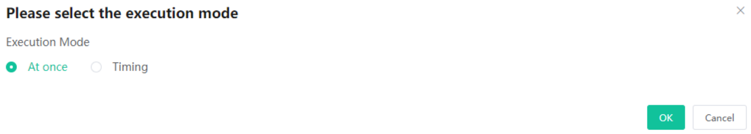
☑	MAC/Device ID	Device Name	Model
☑	805ec0484b91	T52S	SIP-T52S
□	805ec0431ffa	2746	SIP-T54S

MAC/Devic...	Device Na...	Model	Operation
805ec0484...	T52S	SIP-T52S	×

Total 2 < 1 >

□ Select all

4. Select the desired execution mode.



Please select the execution mode

Execution Mode

● At once ○ Timing

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

Note:

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

Editing the Firmware

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

About this task

If you edit the firmware or upload a new firmware, the firmware address would not be changed.

Procedure

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

Downloading the Firmware

Procedure

1. Click **Firmware Management**.
2. Click ⤓ beside the desired firmware.

Deleting Firmware

Procedure

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

Results

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

Managing Resources

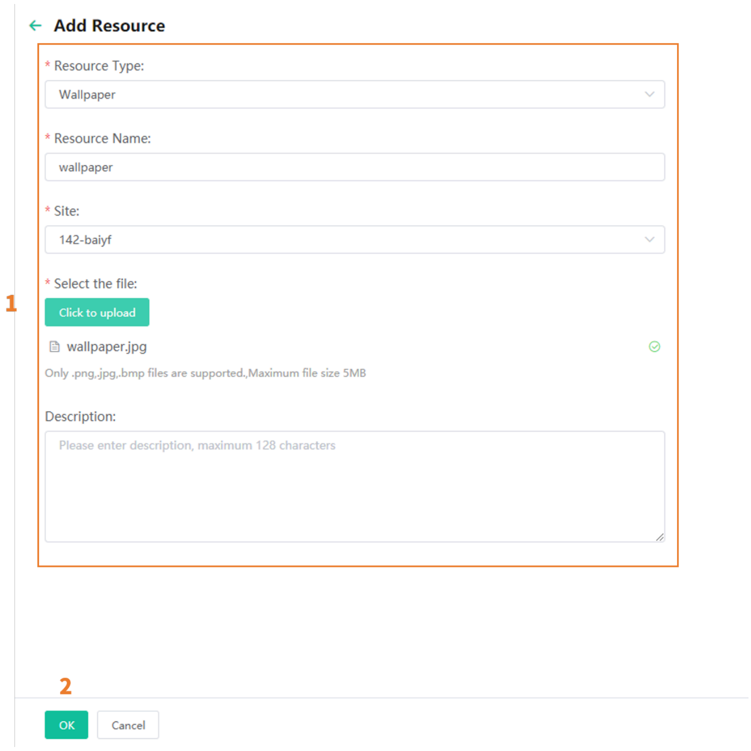
You can add and edit resource files, push resource files to devices or download them to your local system.

- Adding Resource Files
- Sharing Resource
- Pushing Resource Files to Devices
- Editing Resource Files
- Downloading the Resource Files
- Deleting Resource Files
- Pushing SkypeSettings Files to Microsoft Teams Rooms

Adding Resource Files

Procedure

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



← Add Resource

* Resource Type: Wallpaper

* Resource Name: wallpaper

* Site: 142-baiyf

* Select the file:

wallpaper.jpg

Only .png,.jpg,.bmp files are supported.,Maximum file size 5MB

Description: Please enter description, maximum 128 characters

Sharing Resource

You can share the desired resource to others by sending the resource address. Also, you can get devices to access this address to obtain the resource by pushing M7 configuration lines.

Procedure

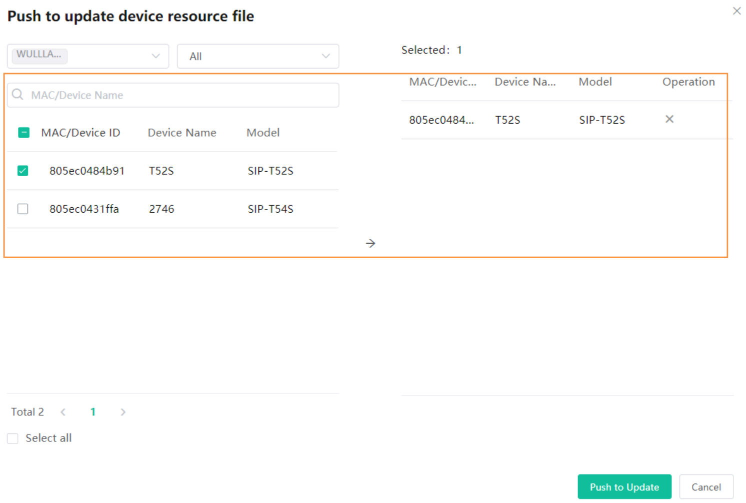
1. Click **Resource Management**.
2. Click ≋ beside the desired software.
3. Paste and share the address to the desired person

Pushing Resource Files to Devices

Procedure

1. Click **Resource Management**.
2. Click ⇗ beside the desired resource.

3. Select the desired devices in the pop-up window.



Push to update device resource file

WULLLA... All

Selected: 1

MAC/Device Name

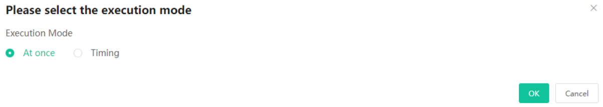
☑	MAC/Device ID	Device Name	Model
☑	805ec0484b91	T52S	SIP-T52S
□	805ec0431ffa	2746	SIP-T54S

MAC/Devic...	Device Na...	Model	Operation
805ec0484...	T52S	SIP-T52S	×

Total 2 < 1 >

□ Select all

4. Click **Push to Update**.
5. Select the desired execution mode.



Please select the execution mode

Execution Mode

● At once ○ Timing

6. Click **OK**.

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

Note:

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

Editing Resource Files

About this task

If you edit the resource or upload a new firmware, the resource address would not be changed.

Procedure

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

Downloading the Resource Files

Procedure

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

Deleting Resource Files

Procedure

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

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

Pushing SkypeSettings Files to Microsoft Teams Rooms

You can upload one or multiple SkypeSettings files to customize the console settings of your Microsoft Teams Rooms.

Procedure

1. Configure the XML configuration file. See https://docs.microsoft.com/en-us/microsoftteams/rooms/xml-config-file for more details.
2. Upload the XML configuration file.

   Note:

   - The file should be XML or ZIP format and less than 50M.
   - Each file in the SkypeSettings ZIP file should be named as *SkypeSettings_MAC*, for example, SkypeSettings_001565FA0856. The ZIP file name has no limit.
3. Push the XML configuration file to the desired devices.

   Note: When creating a scheduled task or selecting a batch of devices to push the SkypeSettings file, the system will search all SkypeSettings files and push them to the corresponding devices.

   If the selected devices do not have the corresponding SkypeSettings files, it will prompt update failure. Otherwise, the update will succeed.

Managing USB Software

YDMP allows you add Yealink USB Connect software to the platform and push the software to a batch of USB devices for update. After adding the software, you can add, download, and share the software.

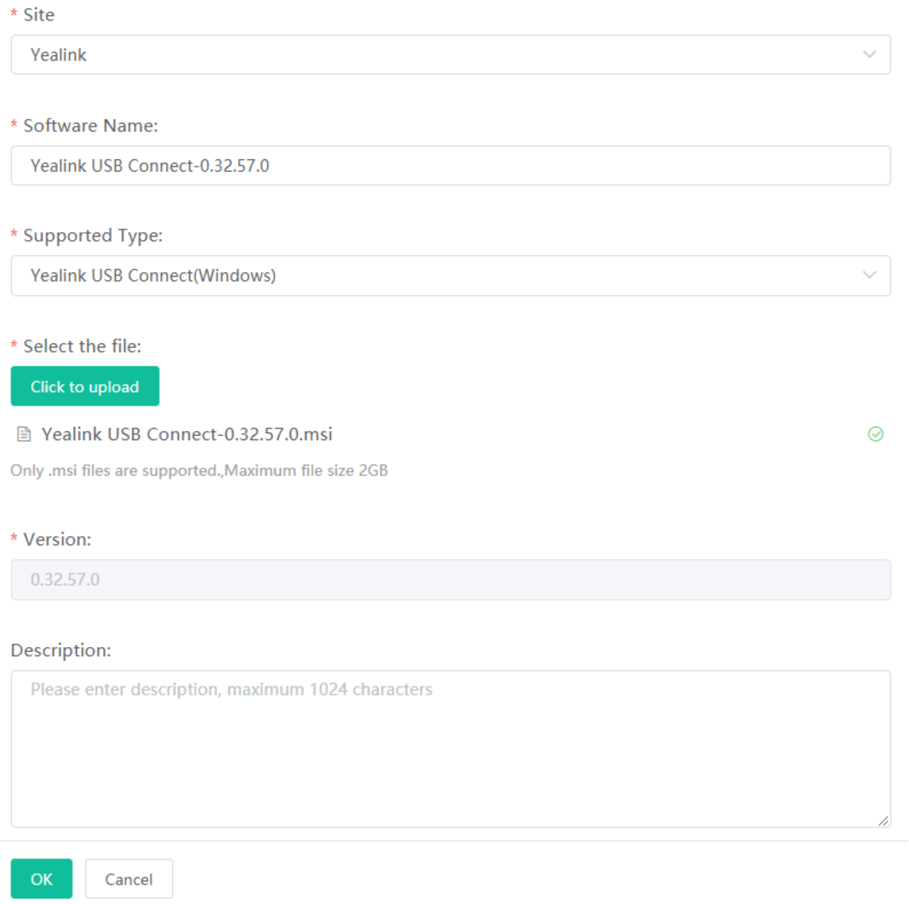
- Adding USB Software
- Sharing USB Software
- Pushing Software to USB Devices
- Editing USB Software
- Downloading the USB Software
- Deleting USB Software

Adding USB Software

You can add USB software for Windows or macOS.

Procedure

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



* Site
Yealink

* Software Name:
Yealink USB Connect-0.32.57.0

* Supported Type:
Yealink USB Connect(Windows)

* Select the file:
Yealink USB Connect-0.32.57.0.msi
Only .msi files are supported.,Maximum file size 2GB

* Version:
0.32.57.0

Description:
Please enter description, maximum 1024 characters

Sharing USB Software

You can share the desired USB software to others by sending the USB software address. Also, you can get devices to access this address to obtain the USB software by pushing M7 configuration lines.

Procedure

1. Click **Software Management**.
2. Click ≋ beside the desired software.
3. Paste and share the address to the desired person.

Pushing Software to USB Devices

About this task

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

Procedure

1. Click **Software Management**
2. Click ↗ beside the desired software.
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 Software**, and select the corresponding software type to update. See Updating Software of USB Devices.

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

Editing USB Software

Procedure

1. Click **Software Management**.
2. Click ✎ beside the desired software.
3. Edit the related information of the software in the corresponding field.
4. Click **Confirm**.

Downloading the USB Software

Procedure

1. Click **Software Management**.
2. Click ⤓ beside the desired software.
3. The file will be downloaded to your computer.

Deleting USB Software

Procedure

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

Results
After the software is deleted, the scheduled task associated with this software fails 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 H323 account**.
3. Configure the account information.
4. Click **Confirm**.

Related tasks

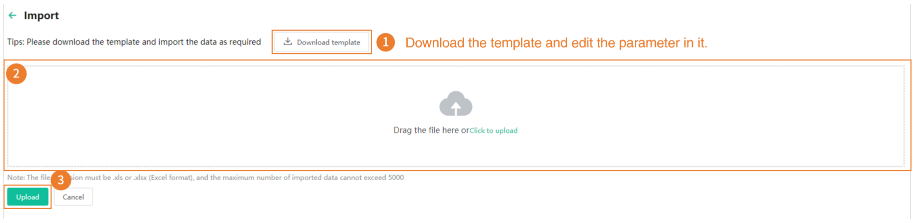
Assigning Accounts to Devices

Importing Accounts

You can import the template to add multiple accounts quickly. You need to download the template, add a batch of accounts, and then import the template to 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 H323 account**.



Import

Tips: Please download the template and import the data as required

Download the template and edit the parameter in it.

Drag the file here or Click to upload

Note: The file sion must be .xls or .xlsx (Excel format), and the maximum number of imported data cannot exceed 5000

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.

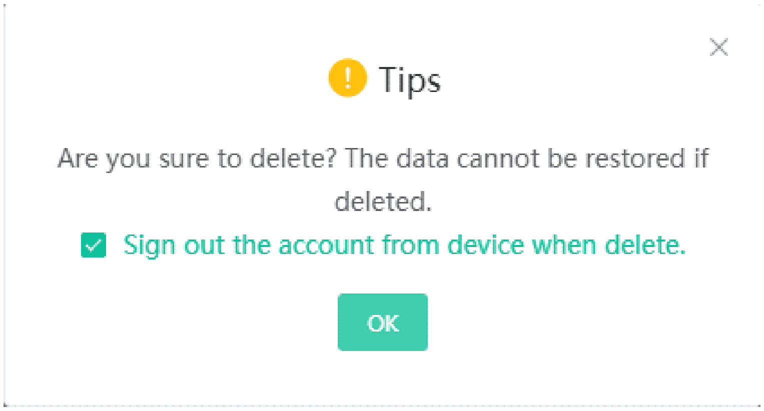
Deleting Accounts

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.



Tips

Are you sure to delete? The data cannot be restored if deleted.

☑ Sign out the account from device when delete.

Managing the Device Configuration

You can manage the configuration file by model, by site, by group, or by MAC (device ID) on YDMP, for example, creating or pushing the configuration file.

Introduction of obtaining the configuration:

Method	Description	Priority
Automatic	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. • When you reboot the device(this should be enabled on the configuration strategy)	global < model < parent site < sub-site < MAC (device ID) The group configuration can only be updated manually. **Note:** If you enable the mandatory parameters feature, the priority order is reversed.
Manual	For the devices existing on YDMP, they would not automatically obtain the updated configuration. Therefore, you need to push the configuration to them.	The configuration you push later has higher priority.

- Managing Model Configuration
- Managing the Site Configuration
- Managing the Group Configuration
- Managing the Single Device Configuration
- Configuring Global Parameters
- Updating the Configuration
- Making Parameters Mandatory and Pushing Them to Devices

- Setting the Configuration Policy

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.

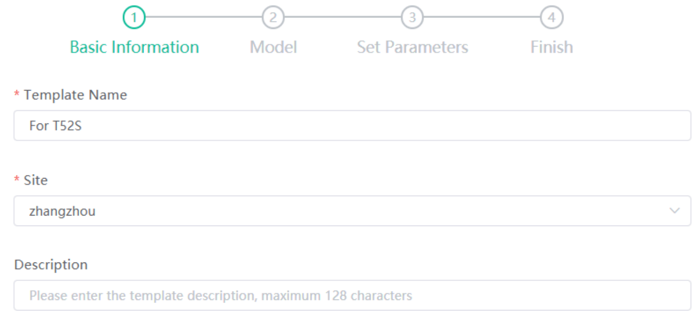
- Adding Configuration Templates
- Setting Parameters
- Pushing Configuration to Devices
- Editing Template Information
- Downloading the Model File
- Deleting Templates

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



* Template Name

For T52S

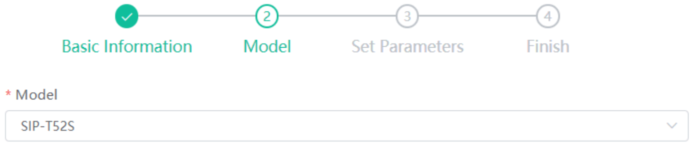
* Site

zhangzhou

Description

Please enter the template description, maximum 128 characters

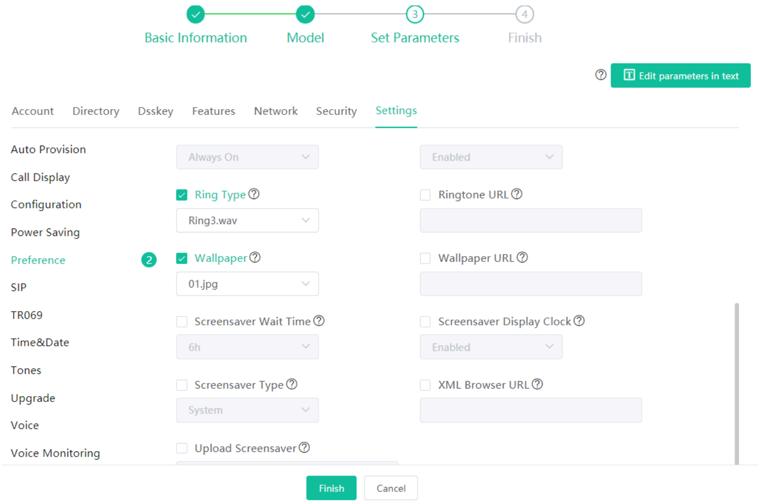
3. Select the device model and click **Next step**.



* Model

SIP-T52S

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



Always On | Enabled

☑ Ring Type: Ring3.wav | □ Ringtone URL

☑ Wallpaper: 01.jpg | □ Wallpaper URL

□ Screensaver Wait Time: 6h | □ Screensaver Display Clock: Enabled

□ Screensaver Type: System | □ XML Browser URL

□ Upload Screensaver

Setting Parameters

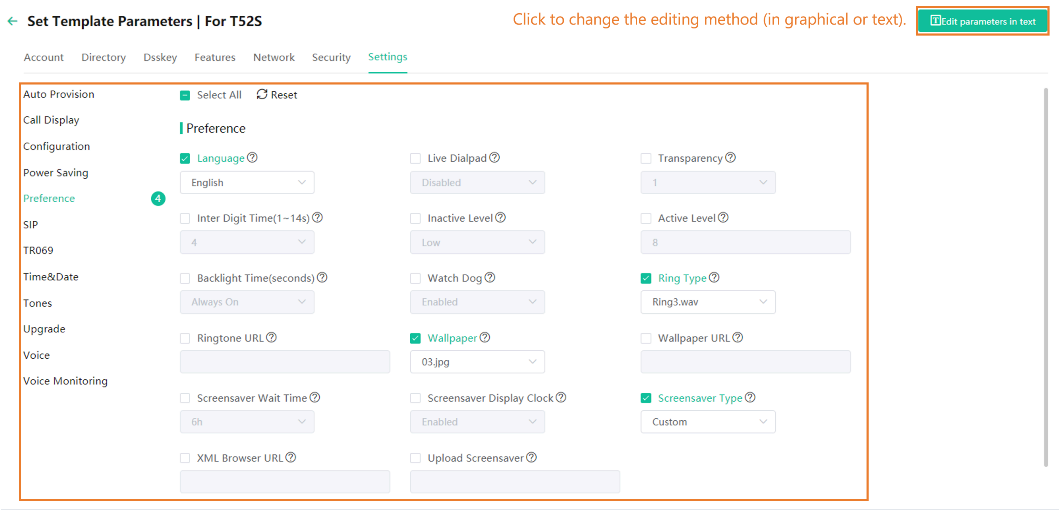
About this task

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

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

Procedure

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



☑ Language: English | □ Live Dialpad: Disabled | □ Transparency: 1

□ Inter Digit Time(1~14s): 4 | □ Inactive Level: Low | □ Active Level: 8

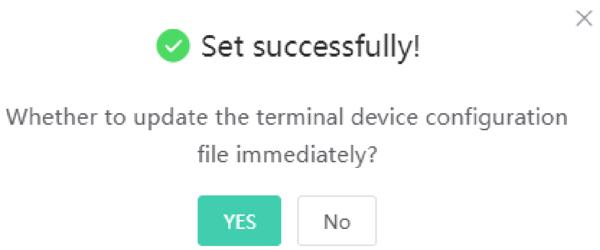
□ Backlight Time(seconds): Always On | □ Watch Dog: Enabled | ☑ Ring Type: Ring3.wav

□ Ringtone URL | ☑ Wallpaper: 03.jpg | □ Wallpaper URL

□ Screensaver Wait Time: 6h | □ Screensaver Display Clock: Enabled | ☑ Screensaver Type: Custom

□ XML Browser URL | □ Upload Screensaver

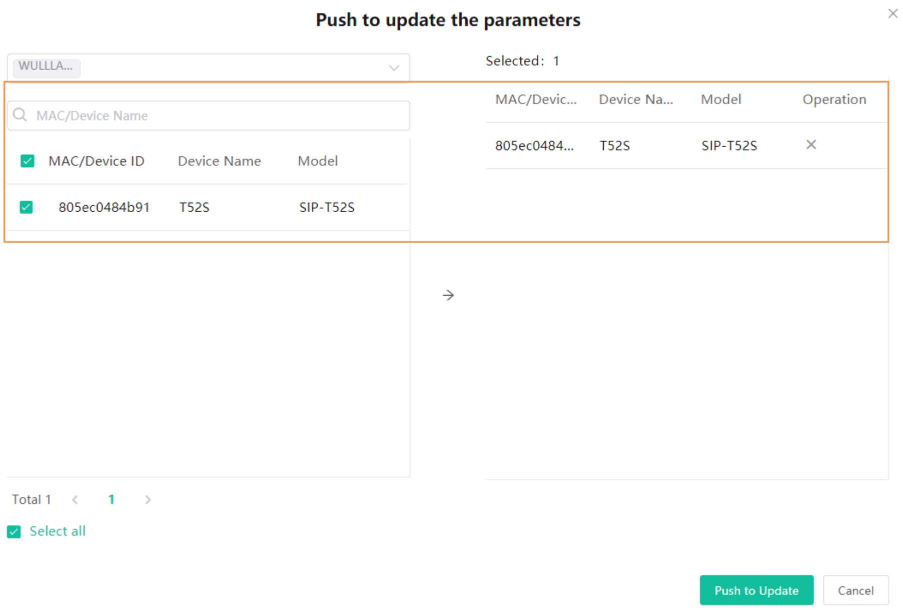
4. On the pop-up window, select **Yes** to push the edited configuration immediately, or **No** to save the edited configuration.



Set successfully!

Whether to update the terminal device configuration file immediately?

5. Push the selected configuration.



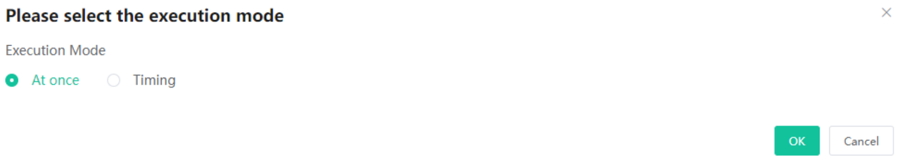
Push to update the parameters

Selected: 1

☑	MAC/Device ID	Device Name	Model
☑	805ec0484b91	T52S	SIP-T52S

MAC/Devic...	Device Na...	Model	Operation
805ec0484...	T52S	SIP-T52S	×

6. Select the desired execution mode.



Please select the execution mode

Execution Mode

● At once ○ Timing

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.

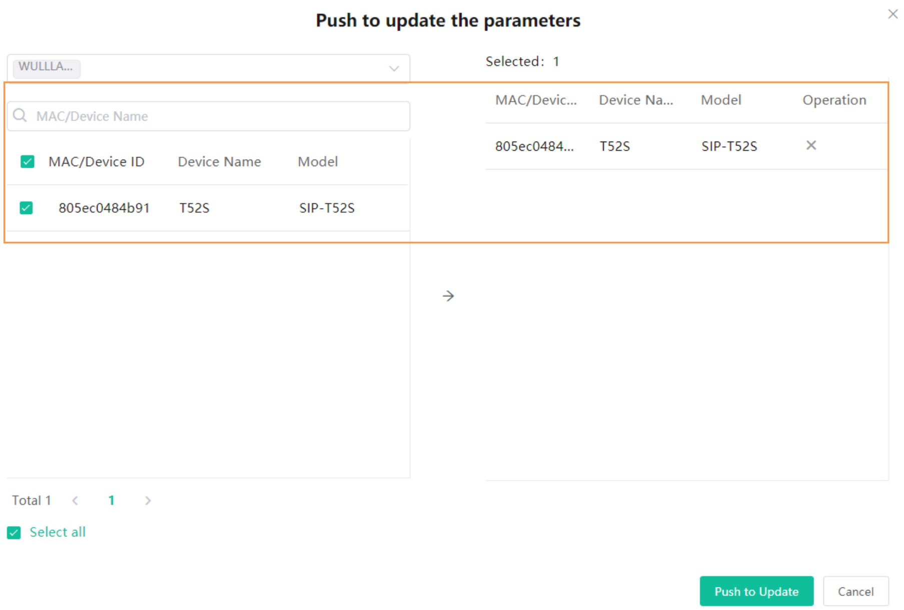
Pushing Configuration to Devices

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 on the right side of the desired template.
3. Push the selected configuration.



Push to update the parameters

WULLLA...

MAC/Device Name

☑	MAC/Device ID	Device Name	Model
☑	805ec0484b91	T52S	SIP-T52S

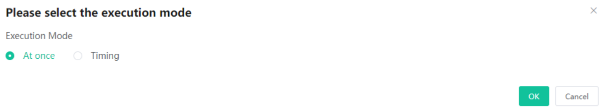
Total 1 < 1 >

☑ Select all

Selected: 1

MAC/Devic...	Device Na...	Model	Operation
805ec0484...	T52S	SIP-T52S	×

4. Select the desired execution mode.



Please select the execution mode

Execution Mode

● At once ○ Timing

Note:

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

Editing Template Information

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

Procedure

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

Downloading the Model File

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

Procedure

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

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

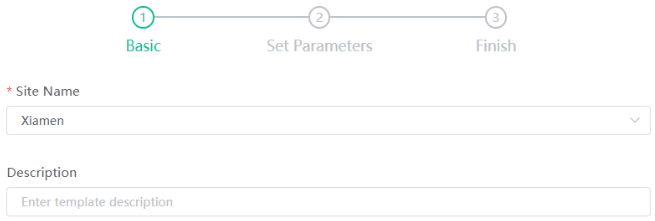
You can customize and manage the configuration according to the site to which the devices belong. Site configuration applies to all the online devices in the site and its sub-sites.

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

Adding Site Configuration Templates

Procedure

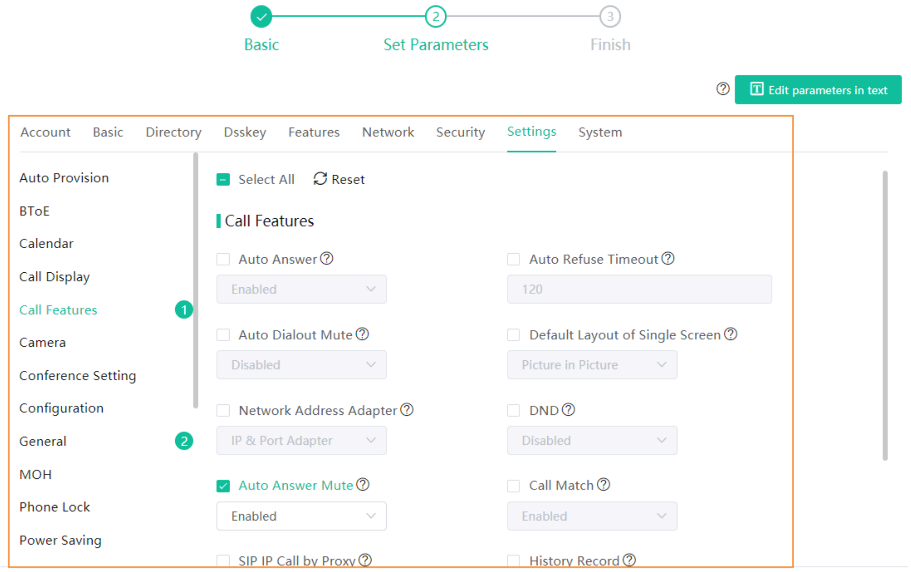
1. Click **Device Configuration** > **Site Configuration** > **Add Template**.
2. Set the site name and click **Next**.



* Site Name
Xiamen

Description
Enter template description

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



Call Features

☐ Auto Answer: Enabled

☐ Auto Refuse Timeout: 120

☐ Auto Dialout Mute: Disabled

☐ Default Layout of Single Screen: Picture in Picture

☐ Network Address Adapter: IP & Port Adapter

☐ DND: Disabled

☑ Auto Answer Mute: Enabled

☐ Call Match: Enabled

☐ SIP IP Call by Proxy

☐ History Record

Setting Parameters

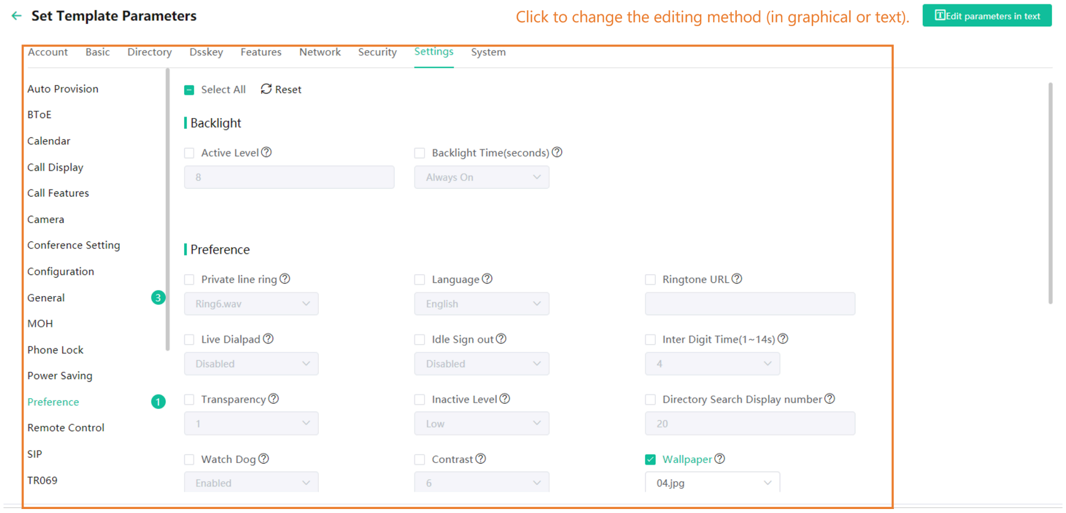
About this task

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

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

Procedure

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



Click to change the editing method (in graphical or text).

Backlight

☐ Active Level: 8

☐ Backlight Time(seconds): Always On

Preference

☐ Private line ring: Ring6.wav

☐ Language: English

☐ Ringtone URL:

☐ Live Dialpad: Disabled

☐ Idle Sign out: Disabled

☐ Inter Digit Time(1~14s): 4

☐ Transparency: 1

☐ Inactive Level: Low

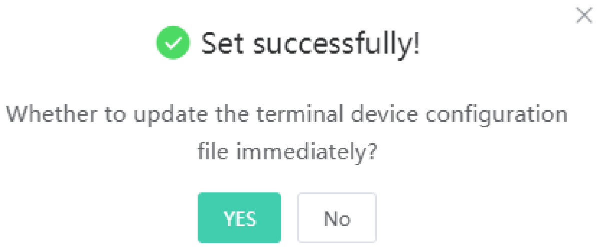
☐ Directory Search Display number: 20

☐ Watch Dog: Enabled

☐ Contrast: 6

☑ Wallpaper: 04.jpg

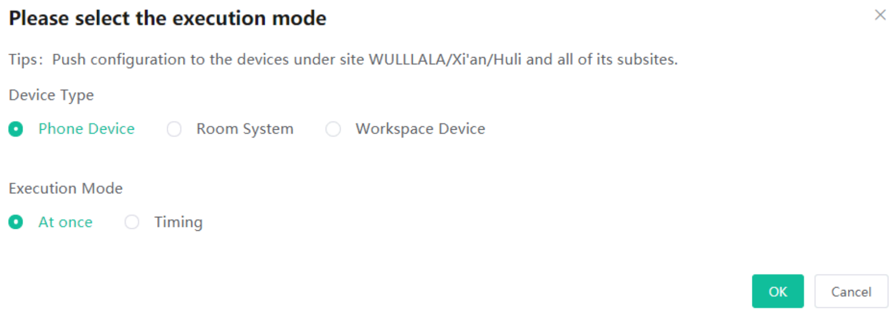
4. On the pop-up window, select **Yes** to push the edited configuration immediately, or **No** to save the edited configuration.



Set successfully!

Whether to update the terminal device configuration file immediately?

5. Select the desired device type and executing mode.



Please select the execution mode

Tips: Push configuration to the devices under site WULLLALA/Xi'an/Huli and all of its subsites.

Device Type

● Phone Device ○ Room System ○ Workspace Device

Execution Mode

● At once ○ Timing

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 the Site Configuration to Devices

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

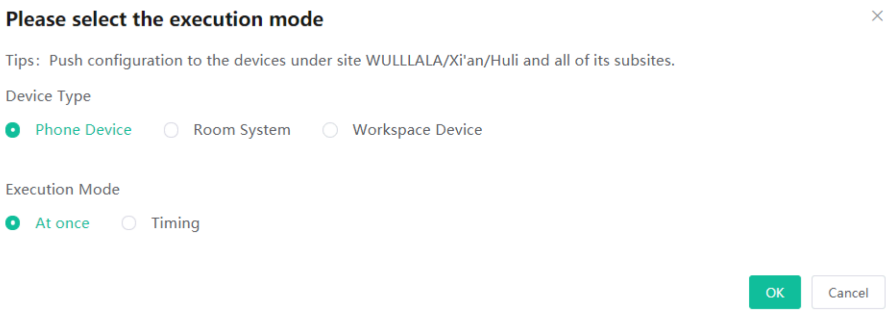
About this task

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

Procedure

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

3. Select the desired device type and executing mode.



Please select the execution mode

Tips：Push configuration to the devices under site WULLLALA/Xi'an/Huli and all of its subsites.

Device Type

● Phone Device ○ Room System ○ Workspace Device

Execution Mode

● At once ○ Timing

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

Editing the Site Configuration Template

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

Procedure

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

Downloading the Site Configuration Template

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

About this task

Procedure

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

Deleting Site Configuration Templates

Procedure

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

Results

After you delete the template, the 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.

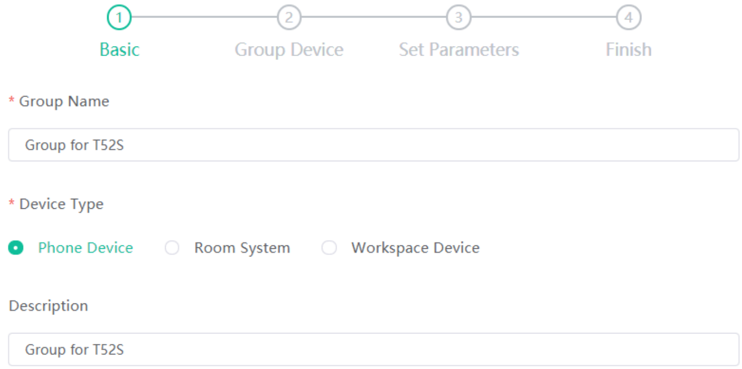
- Adding the Group Configuration
- Setting Parameters
- Editing the Group Configuration Template
- Pushing the Group Configuration
- Downloading Configuration File
- Deleting Groups

Adding the Group Configuration

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

Procedure

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

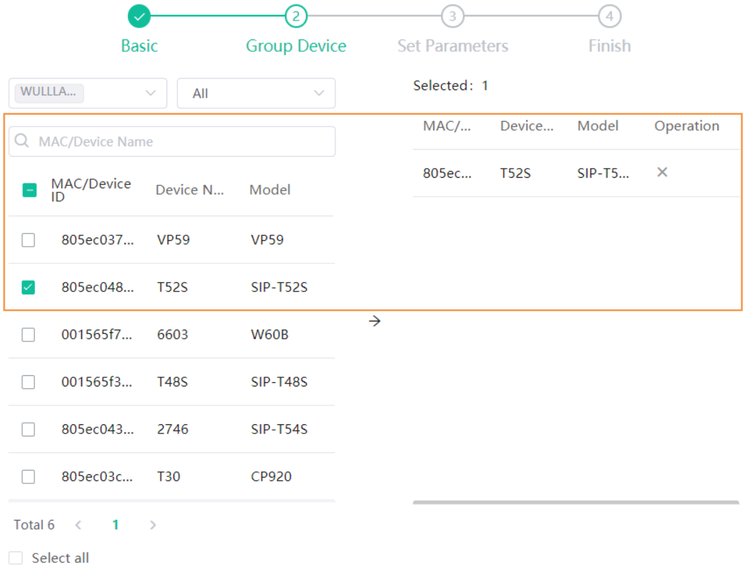


* Group Name: Group for T52S

* Device Type: ● Phone Device ○ Room System ○ Workspace Device

Description: Group for T52S

3. Select the desired device to the group.



Selected: 1

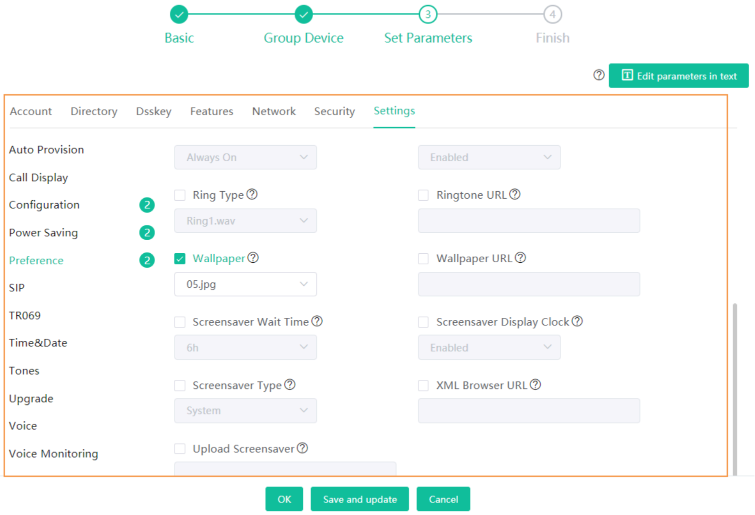
☑	MAC/Device ID	Device N...	Model
□	805ec037...	VP59	VP59
☑	805ec048...	T52S	SIP-T52S
□	001565f7...	6603	W60B
□	001565f3...	T48S	SIP-T48S
□	805ec043...	2746	SIP-T54S
□	805ec03c...	T30	CP920

Total 6 ‹ 1 ›

□ Select all

MAC/...	Device...	Model	Operation
805ec...	T52S	SIP-T5...	×

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



Always On | Enabled

□ Ring Type: Ring1.wav

□ Ringtone URL

☑ Wallpaper: 05.jpg

□ Wallpaper URL

□ Screensaver Wait Time: 6h

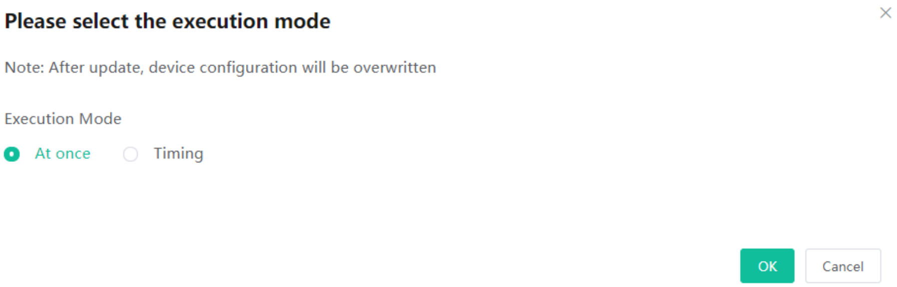
□ Screensaver Display Clock: Enabled

□ Screensaver Type: System

□ XML Browser URL

□ Upload Screensaver

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


Please select the execution mode

Note: After update, device configuration will be overwritten

Execution Mode

● At once ○ Timing

Note:

- If you select **At once**, the configuration will be pushed to the selected devices immediately.
- If you select **Timing**, the configuration will be pushed to the selected devices at the time you set.
- After updating the configuration file, you can see the task details, refer to Viewing Executed Tasks.

Setting Parameters

About this task

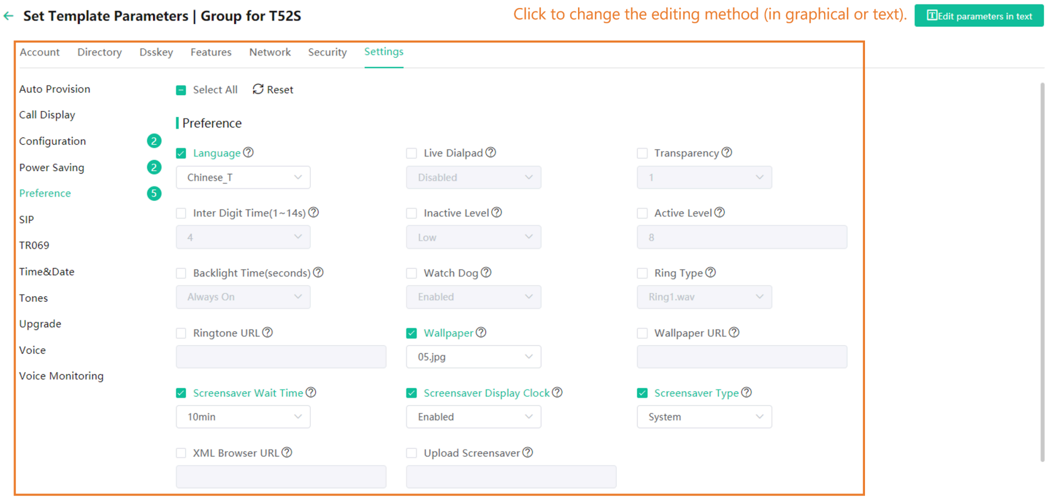
You can choose one of the following methods to configure the parameters:

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

Procedure

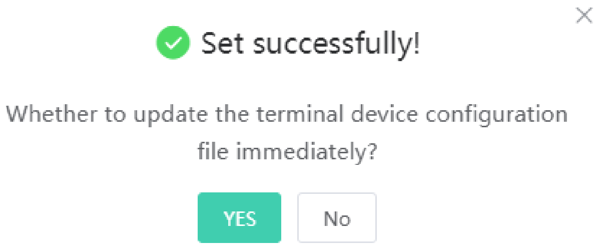
1. Click **Device Configuration** > **Group Configuration**.
2. Click ▤ / 🅃 on the right side of the desired template.

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



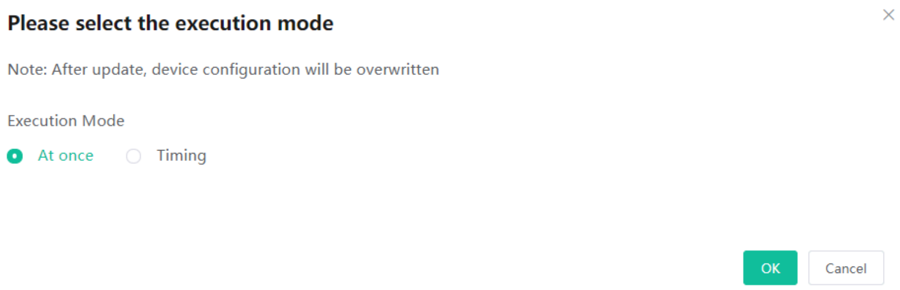
☑ Language: Chinese_T
□ Live Dialpad: Disabled
□ Transparency: 1
□ Inter Digit Time(1~14s): 4
□ Inactive Level: Low
□ Active Level: 8
□ Backlight Time(seconds): Always On
□ Watch Dog: Enabled
□ Ring Type: Ring1.wav
□ Ringtone URL
☑ Wallpaper: 05.jpg
□ Wallpaper URL
☑ Screensaver Wait Time: 10min
☑ Screensaver Display Clock: Enabled
☑ Screensaver Type: System
□ XML Browser URL
□ Upload Screensaver

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


Set successfully!

Whether to update the terminal device configuration file immediately?

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


Please select the execution mode

Note: After update, device configuration will be overwritten

Execution Mode

● At once ○ Timing

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.

Editing the Group Configuration Template

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

Procedure

1. Click **Device Configuration** > **Group Configuration**.

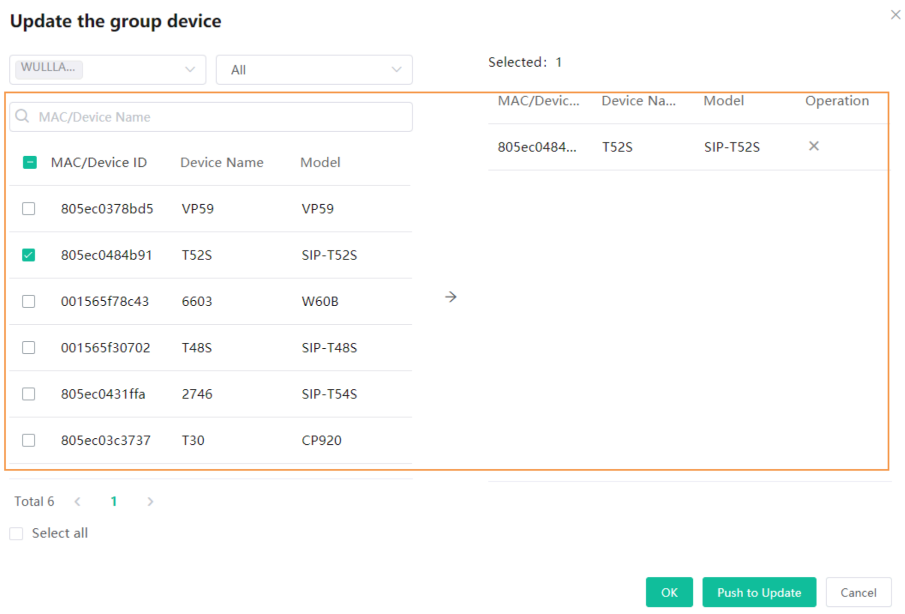
2. Click ✎ on the right side of the desired template.
3. Edit and save the parameters.

Pushing the Group Configuration

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

Procedure

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



Update the group device

WULLLA... | All

MAC/Device Name

☑	MAC/Device ID	Device Name	Model
□	805ec0378bd5	VP59	VP59
☑	805ec0484b91	T52S	SIP-T52S
□	001565f78c43	6603	W60B
□	001565f30702	T48S	SIP-T48S
□	805ec0431ffa	2746	SIP-T54S
□	805ec03c3737	T30	CP920

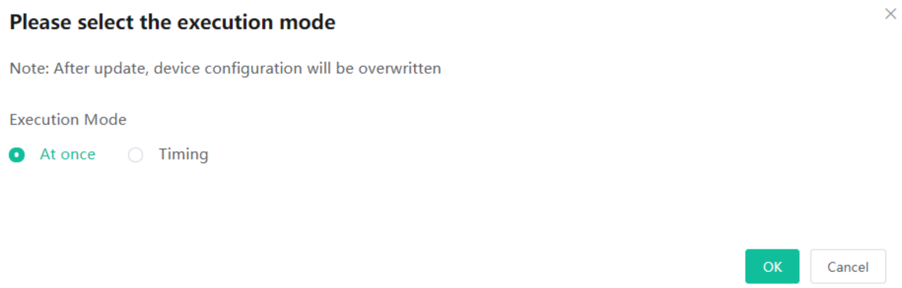
Total 6 < 1 >

□ Select all

Selected: 1

MAC/Devic...	Device Na...	Model	Operation
805ec0484...	T52S	SIP-T52S	×

4. Select the desired execution mode.



Please select the execution mode

Note: After update, device configuration will be overwritten

Execution Mode

● At once ○ Timing

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

Downloading Configuration File

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

Procedure

1. Click **Device Configuration** > **Group Configuration**.

2. Click ⤓ on the right side of the desired template.

Deleting Groups

Procedure

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

Results

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

Managing the Single Device Configuration

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

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

Uploading Configuration Files

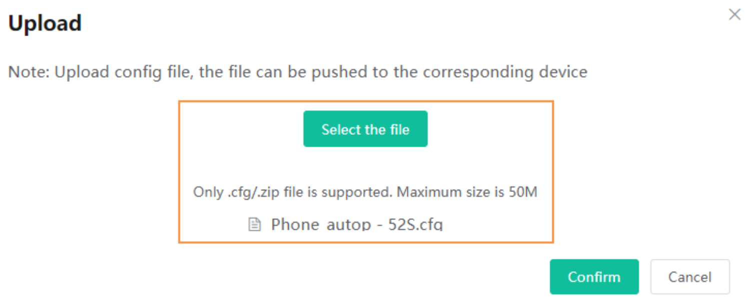
You can update the configuration for one or more devices by uploading the configuration file.

About this task

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

Procedure

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



Upload

Note: Upload config file, the file can be pushed to the corresponding device

Only .cfg/.zip file is supported. Maximum size is 50M

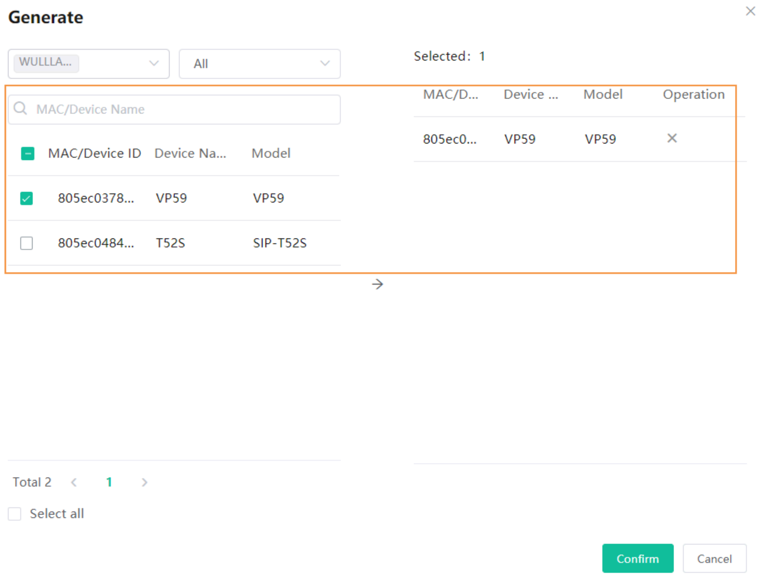
Phone autop - 52S.cfg

Generating Configuration Files

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

Procedure

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



Generate

WULLLA... | All

MAC/Device Name

☐	MAC/Device ID	Device Na...	Model
☑	805ec0378...	VP59	VP59
☐	805ec0484...	T52S	SIP-T52S

Total 2 < 1 >

☐ Select all

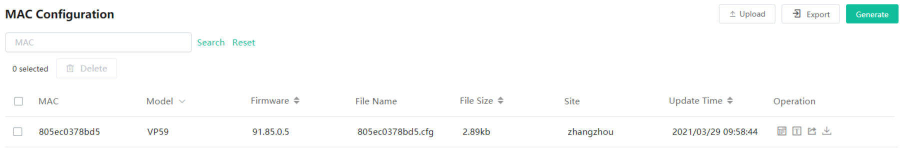
Selected: 1

MAC/D...	Device ...	Model	Operation
805ec0...	VP59	VP59	×

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:



MAC Configuration

0 selected Delete

☐	MAC	Model	Firmware	File Name	File Size	Site	Update Time	Operation
☐	805ec0378bd5	VP59	91.85.0.5	805ec0378bd5.cfg	2.89kb	zhangzhou	2021/03/29 09:58:44	

Pushing Backup Files to Devices

Procedure

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

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

Downloading the Configuration Files

You can download the backup files to your local system.

Procedure

1. Click **Device Configuration** > **Single Device Configuration**.

2. Click ⤓ beside the desired MAC configuration to download the backup to your local system.

Exporting the Configuration Files

You can export all device configuration files by one click.

Procedure

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

   This will export all MAC configuration files.

Deleting Backup Files

Procedure

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

   Note:

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

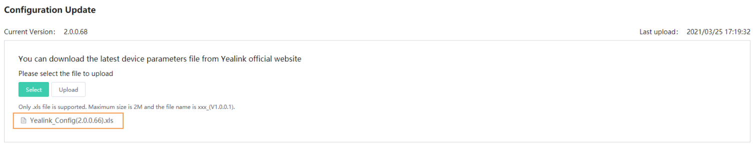
Updating the Configuration

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 Yealink Support.

Procedure

1. Click **Device Configuration** > **Configuration Update**.

2. Click **Select** and select the desired file to upload.



Configuration Update

Current Version: 2.0.0.68

Last upload: 2021/03/25 17:19:32

You can download the latest device parameters file from Yealink official website

Please select the file to upload

Only .xls file is supported. Maximum size is 2M and the file name is xxx_(V1.0.0.1).

Yealink_Config(2.0.0.66).xls

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

3. Click **Upload**.

Making Parameters Mandatory and Pushing Them to Devices

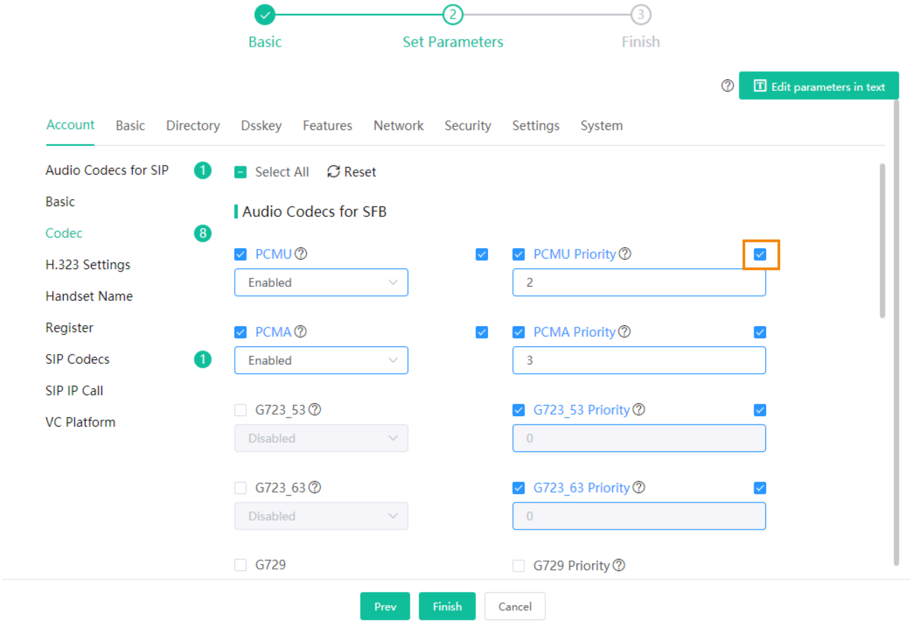
If you want to make some parameters unaffected by the configuration update rule, you can make those parameters mandatory. Therefore, devices using those configuration templates will inherit those mandatory parameters.

About this task

Parameters	Update priority
General parameters	MAC (device ID) configuration < parent site configuration < sub-site configuration
Mandatory parameters	MAC (device ID) configuration > parent site configuration > sub-site configuration

Procedure

1. Click **Device Configuration** > **Model Configuration/Site Configuration**.
2. Add or edit a site configuration (add or edit a model configuration).
3. In the graphical editing page, select the check box in the right side beside the selected parameter and click **Finish**.



Audio Codecs for SFB

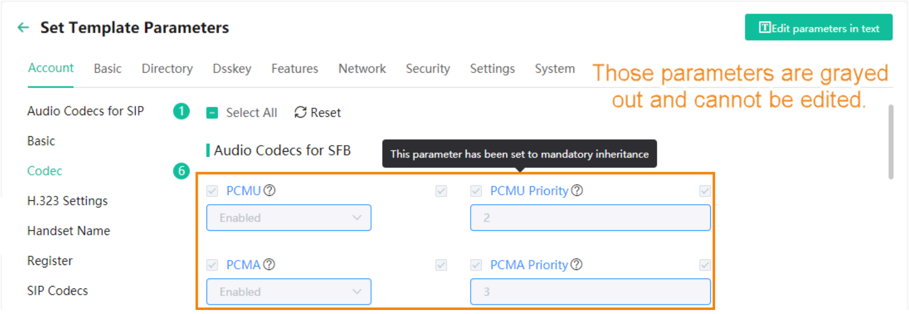
☑ PCMU: Enabled	☑	☑ PCMU Priority: 2	☑
☑ PCMA: Enabled	☑	☑ PCMA Priority: 3	☑
□ G723_53: Disabled		☑ G723_53 Priority: 0	☑
□ G723_63: Disabled		☑ G723_63 Priority: 0	☑
□ G729		□ G729 Priority	

4. Click to push the mandatory parameters to the desired devices.

   Tip: If you want to see whether the device inherits the mandatory parameters or not, see device details.

Results

1. Devices using those configuration templates will inherit those mandatory parameters.
2. If you set some parameters in the parent site configuration templates, the sub-site configuration templates will inherit those mandatory parameters. Moreover, those mandatory parameters in the sub-site templates cannot be edited, as shown as below.



Those parameters are grayed out and cannot be edited.

This parameter has been set to mandatory inheritance

PCMU: Enabled

PCMU Priority: 2

PCMA: Enabled

PCMA Priority: 3

Setting the Configuration Policy

You can set preferred situations for the device to automatically obtain the device configuration file.

About this task

For the configuration obtaining priority, see Managing the Device Configuration.

Procedure

1. Click **System Management** > **Configuration Strategy**.
2. Select or clear the check box of **Reboot**.
3. Click **Save**.

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
- Exporting Sites
- Managing Sites

Adding Sites

You can add site according to the specific IP range or your enterprise organization or location.

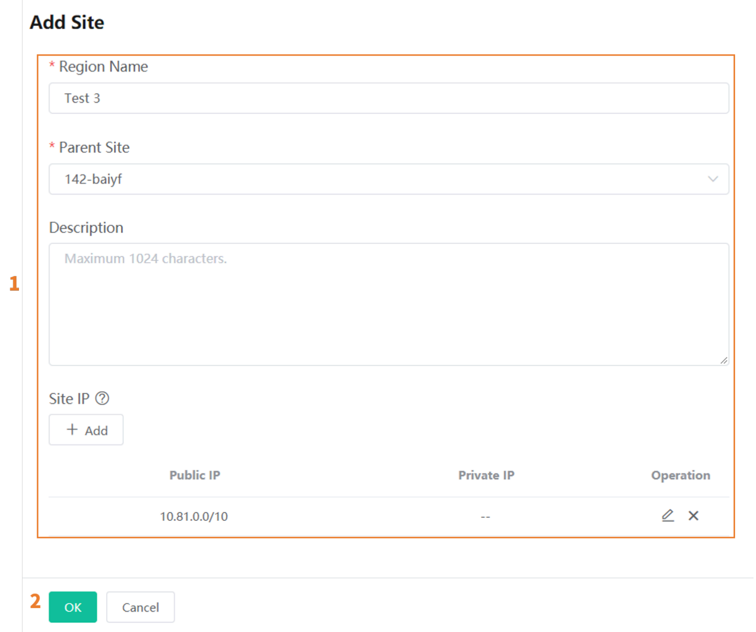
About this task

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.

Procedure

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



Add Site

* Region Name: Test 3

* Parent Site: 142-baiyf

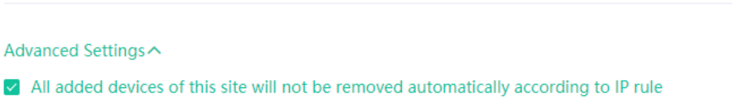
Description: Maximum 1024 characters.

Site IP

Public IP	Private IP	Operation
10.81.0.0/10	--	

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

3. Optional: If you want to make the devices under this site not affected by the IP rules set by other sites, click **Advanced Settings** and select the check box of **All added devices of this site will not be removed automatically according to IP rule**.



Advanced Settings

☑ All added devices of this site will not be removed automatically according to IP rule

Results

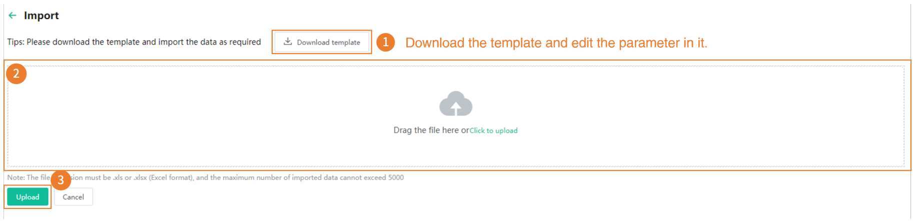
After adding sites, you can move devices to the site and manage the devices. Setting site IP makes the devices automatically assigned to the corresponding site if the device IP addresses are in the site IP range.

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 Management** > **Import**.



Tips: Please download the template and import the data as required

Download the template and edit the parameter in it.

Note: The file sion must be .xls or .xlsx (Excel format), and the maximum number of imported data cannot exceed 5000

Exporting Sites

You can export the site information to edit them, and import the edited information to the platform to manage multiple sites quickly.

About this task

If you are a sub-administrator, the site range you can export depends on the data permission the enterprise administrator assigns to you.

Procedure

Click **Site Management** > **Export**.

Managing Sites

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

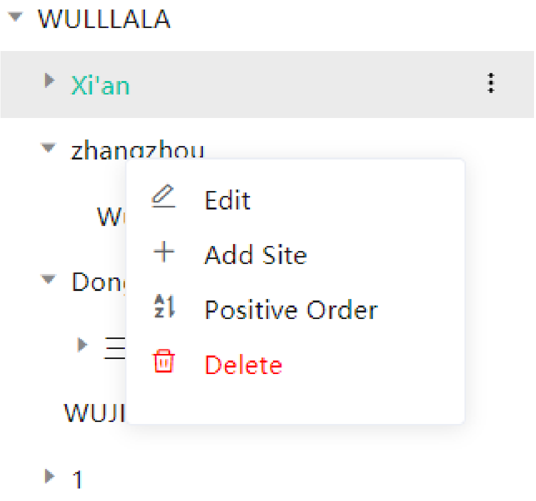
Procedure

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

     Note:

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

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



Managing Tasks

The Scheduled Task page displays the added scheduled 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.

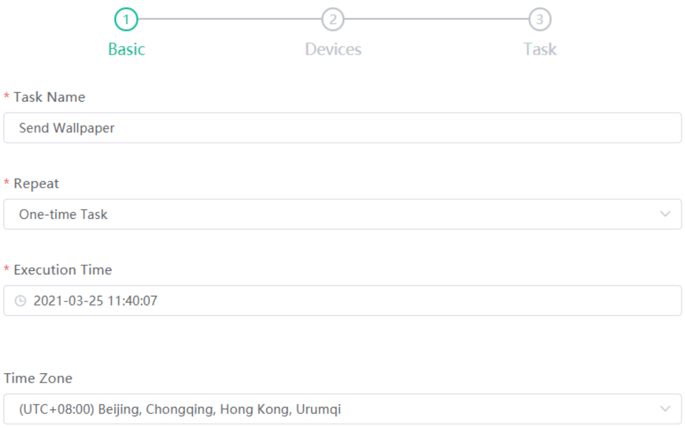
Execution mode	• At once: the task is executed immediately. • Timing: the task is executed at the time you set.
Tasks and Rules	• Update resource file: you can only push one file of the same resource type at a time. Only the resource file supported by the selected device can be pushed. • Upgrade firmware: 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 Timer Tasks

Procedure

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



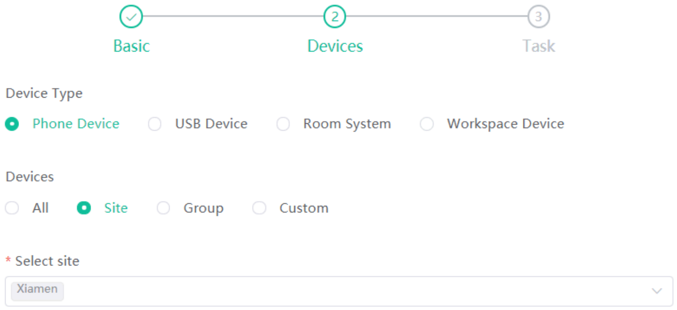
* Task Name
Send Wallpaper

* Repeat
One-time Task

* Execution Time
2021-03-25 11:40:07

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

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



Device Type

● Phone Device ○ USB Device ○ Room System ○ Workspace Device

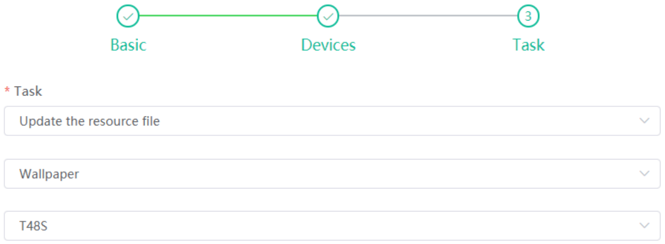
Devices

○ All ● Site ○ Group ○ Custom

* Select site

Xiamen

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



* Task

Update the resource file

Wallpaper

T48S

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 Timer Tasks

Viewing Executed 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 executing scheduled task, the task can still be executed until it is finished. If you end the periodic scheduled task, they will no longer be executed.

Procedure

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

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

Related tasks

Viewing Timer Tasks

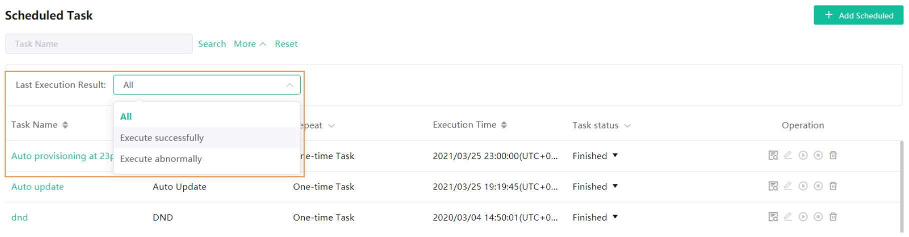
Viewing Executed Tasks

Searching for Scheduled Tasks

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

Procedure

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



Last Execution Result: All

Task Name		epeat	Execution Time	Task status	Operation
Auto provisioning at 23p		e-time Task	2021/03/25 23:00:00(UTC+0...	Finished ▼	
Auto update	Auto Update	One-time Task	2021/03/25 19:19:45(UTC+0...	Finished ▼	
dnd	DND	One-time Task	2020/03/04 14:50:01(UTC+0...	Finished ▼	

Results

The search results are displayed in the list.

Viewing Timer Tasks

Procedure

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

Results

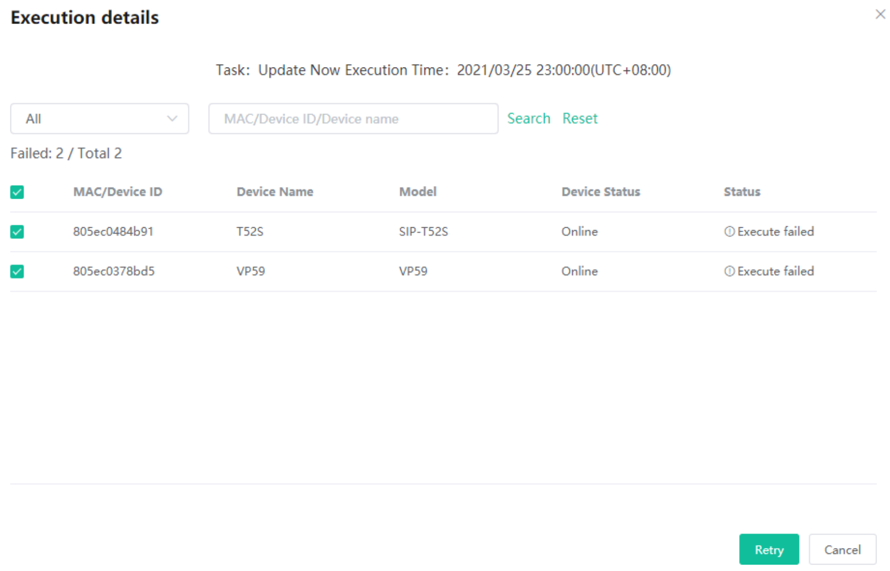
It goes to the Executed task page and you can view the execution details.

Viewing Executed Tasks

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

Procedure

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



Execution details

Task: Update Now Execution Time: 2021/03/25 23:00:00(UTC+08:00)

Failed: 2 / Total 2

☑	MAC/Device ID	Device Name	Model	Device Status	Status
☑	805ec0484b91	T52S	SIP-T52S	Online	ⓘ Execute failed
☑	805ec0378bd5	VP59	VP59	Online	ⓘ Execute failed

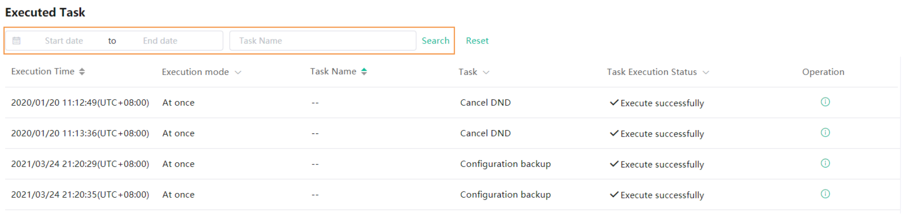
3. Optional: Select the exceptional devices, and then click **Retry** to re-execute the task.

Searching for Executed Tasks

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

Procedure

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


Executed Task

Execution Time	Execution mode	Task Name	Task	Task Execution Status	Operation
2020/01/20 11:12:49(UTC+08:00)	At once	--	Cancel DND	✓ Execute successfully	ⓘ
2020/01/20 11:13:36(UTC+08:00)	At once	--	Cancel DND	✓ Execute successfully	ⓘ
2021/03/24 21:20:29(UTC+08:00)	At once	--	Configuration backup	✓ Execute successfully	ⓘ
2021/03/24 21:20:35(UTC+08:00)	At once	--	Configuration backup	✓ Execute successfully	ⓘ

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.

- Start 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 Recordings
- Taking the Screenshot of the Device
- Setting the Log Level
- Download the Device Log
- Backing up Configuration Files

Start Diagnosing

About this task

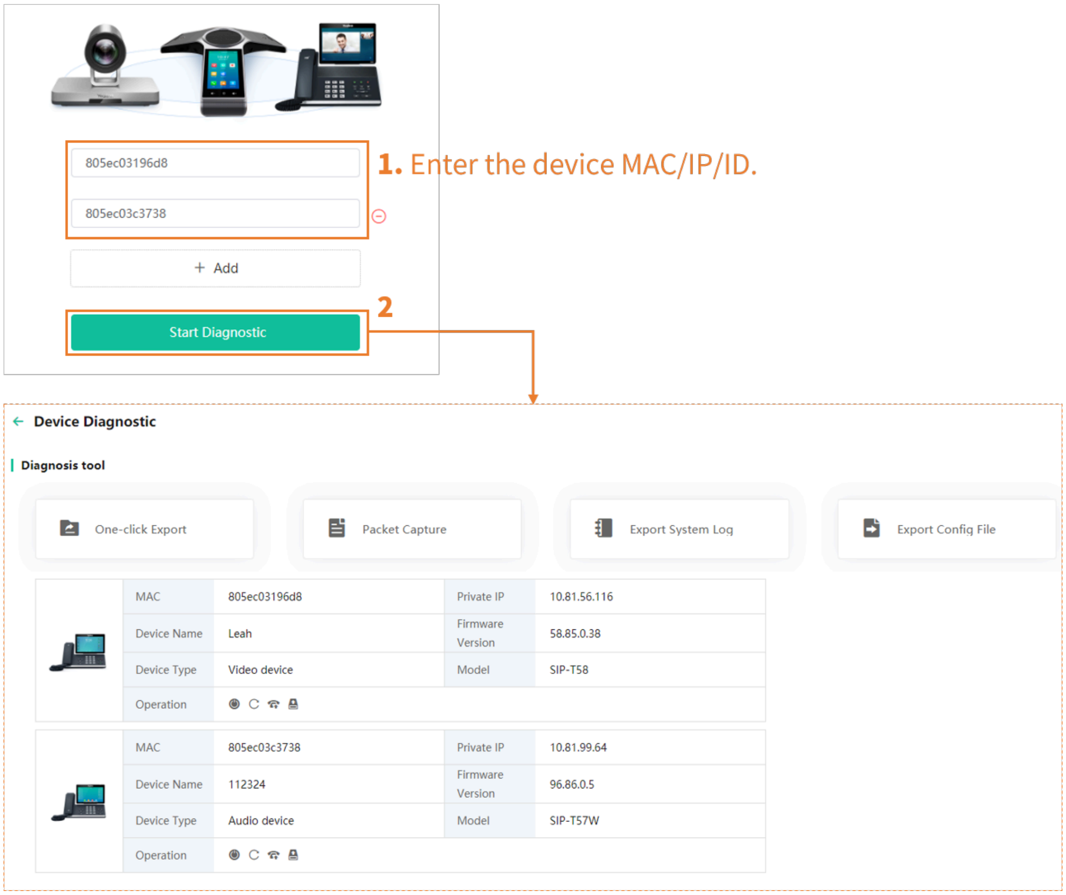
Note:

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

Procedure

Diagnose a single/multiple devices.

Take the image of phone device as an example.



805ec03196d8

805ec03c3738

1. Enter the device MAC/IP/ID.

MAC	805ec03196d8	Private IP	10.81.56.116
Device Name	Leah	Firmware Version	58.85.0.38
Device Type	Video device	Model	SIP-T58
Operation	◉ C ☎ 🔒		

MAC	805ec03c3738	Private IP	10.81.99.64
Device Name	112324	Firmware Version	96.86.0.5
Device Type	Audio device	Model	SIP-T57W
Operation	◉ C ☎ 🔒		

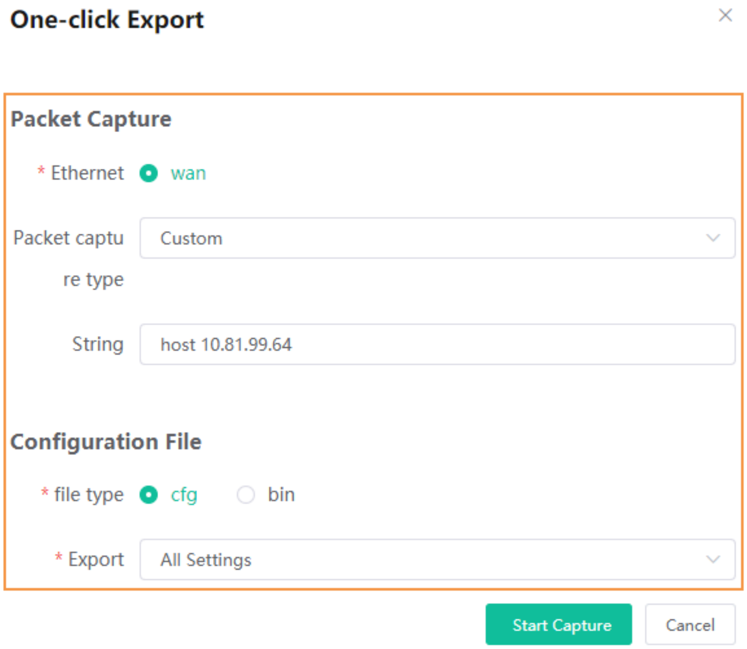
Exporting the Packets, Logs, and Configuration Files by One Click

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**.



One-click Export

Packet Capture

* Ethernet ● wan

Packet capture type: Custom

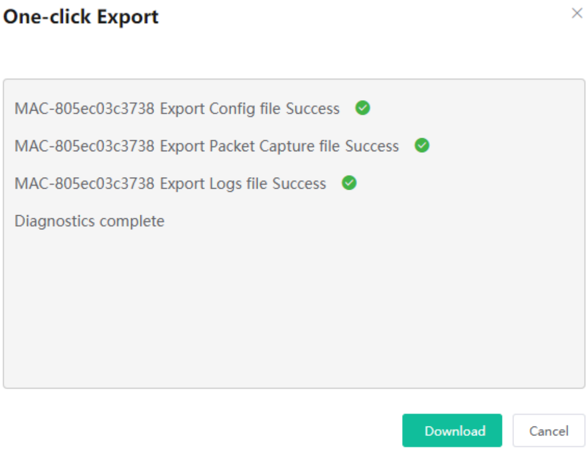
String: host 10.81.99.64

Configuration File

* file type ● cfg ○ bin

* Export: All Settings

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



One-click Export

MAC-805ec03c3738 Export Config file Success ✓
MAC-805ec03c3738 Export Packet Capture file Success ✓
MAC-805ec03c3738 Export Logs file Success ✓
Diagnostics complete

5. 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.

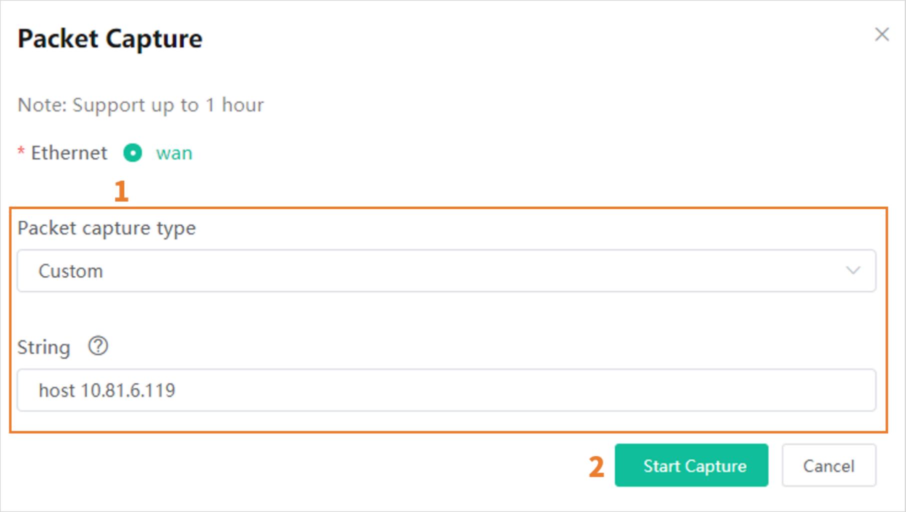
String	Example	Introduction
host IP	host 10.81.36.16	Only see the incoming and outgoing traffic of a specific IP.

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

Procedure

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

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



Packet Capture

Note: Support up to 1 hour

* Ethernet ● wan

Packet capture type: Custom

String: host 10.81.6.119

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

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

Diagnosing the Network

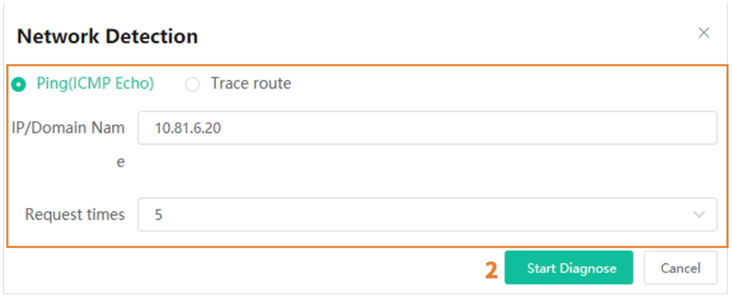
About this task

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**.



Network Detection

● Ping(ICMP Echo) ○ Trace route

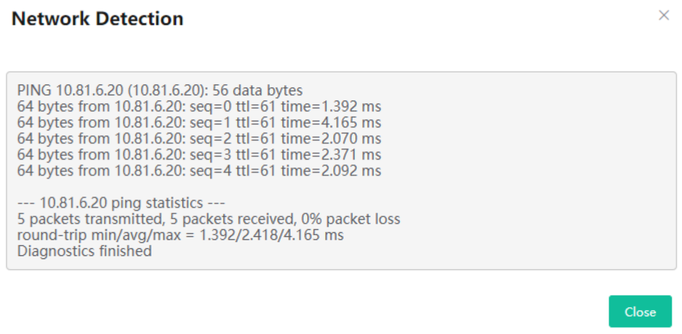
IP/Domain Nam e: 10.81.6.20

Request times: 5

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

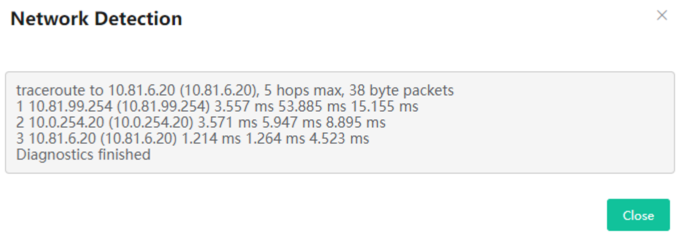
Results

- If you select Ping, following is the example result



```
PING 10.81.6.20 (10.81.6.20): 56 data bytes
64 bytes from 10.81.6.20: seq=0 ttl=61 time=1.392 ms
64 bytes from 10.81.6.20: seq=1 ttl=61 time=4.165 ms
64 bytes from 10.81.6.20: seq=2 ttl=61 time=2.070 ms
64 bytes from 10.81.6.20: seq=3 ttl=61 time=2.371 ms
64 bytes from 10.81.6.20: seq=4 ttl=61 time=2.092 ms

--- 10.81.6.20 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.392/2.418/4.165 ms
Diagnostics finished
```

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



```
traceroute to 10.81.6.20 (10.81.6.20), 5 hops max, 38 byte packets
1 10.81.99.254 (10.81.99.254) 3.557 ms 53.885 ms 15.155 ms
2 10.0.254.20 (10.0.254.20) 3.571 ms 5.947 ms 8.895 ms
3 10.81.6.20 (10.81.6.20) 1.214 ms 1.264 ms 4.523 ms
Diagnostics finished
```

Exporting System Logs

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

Procedure

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

Exporting the Configuration Files

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

About this task

Procedure

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

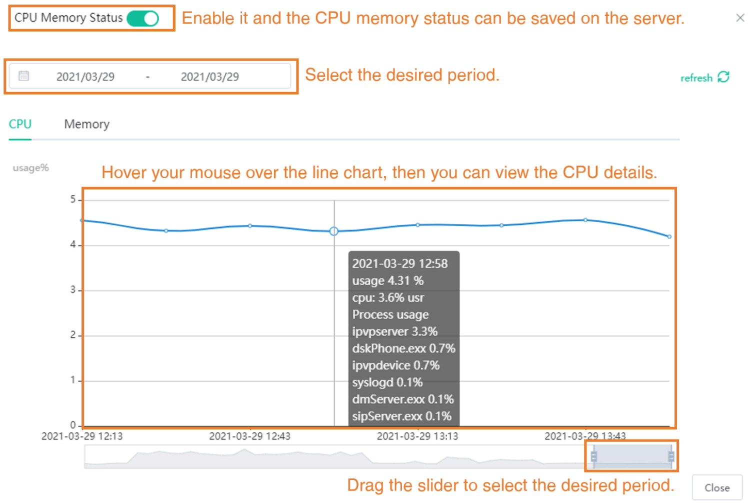
Viewing the CPU and the Memory Status

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.

About this task

Procedure

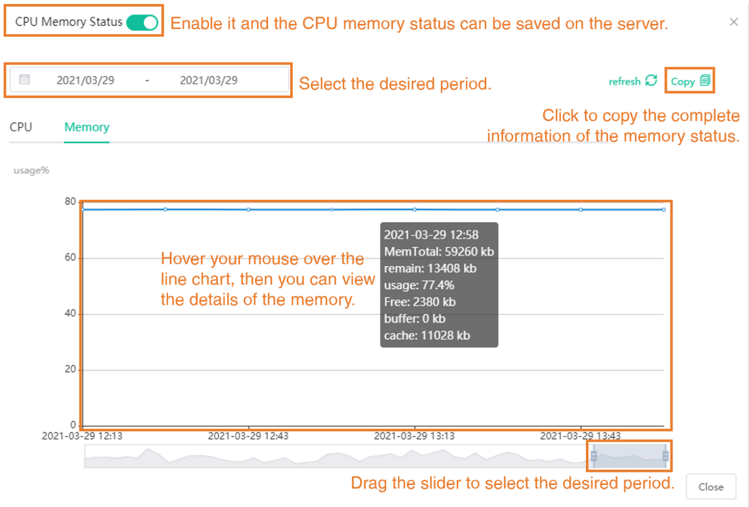
1. On the Device Diagnostics page, click **CPU Memory Status**.
2. Do one of the following:
   - Click **CPU** to view the CPU usage.



CPU Memory Status
Enable it and the CPU memory status can be saved on the server.
2021/03/29 - 2021/03/29
Select the desired period.
refresh
CPU
Memory
usage%
Hover your mouse over the line chart, then you can view the CPU details.
5
4
3
2
1
0
2021-03-29 12:13
2021-03-29 12:43
2021-03-29 13:13
2021-03-29 13:43
Drag the slider to select the desired period.
Close

2021-03-29 12:58
usage 4.31 %
cpu: 3.6% usr
Process usage
ipvpserver 3.3%
dskPhone.exx 0.7%
ipvpdevice 0.7%
syslogd 0.1%
dmServer.exx 0.1%
sipServer.exx 0.1%

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



CPU Memory Status
Enable it and the CPU memory status can be saved on the server.
2021/03/29 - 2021/03/29
Select the desired period.
refresh
Copy
Click to copy the complete information of the memory status.
CPU
Memory
usage%
80
60
40
20
0
Hover your mouse over the line chart, then you can view the details of the memory.
2021-03-29 12:13
2021-03-29 12:43
2021-03-29 13:13
2021-03-29 13:43
Drag the slider to select the desired period.
Close

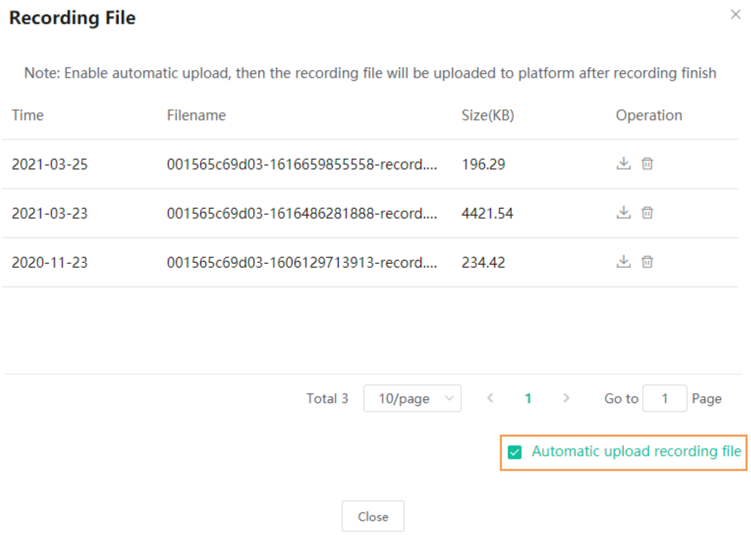
2021-03-29 12:58
MemTotal: 59260 kb
remain: 13408 kb
usage: 77.4%
Free: 2380 kb
buffer: 0 kb
cache: 11028 kb

Viewing Recordings

Before you begin

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

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

  Recording File

  Note: Enable automatic upload, then the recording file will be uploaded to platform after recording finish

Time	Filename	Size(KB)	Operation
2021-03-25	001565c69d03-1616659855558-record....	196.29	⤓ 🗑
2021-03-23	001565c69d03-1616486281888-record....	4421.54	⤓ 🗑
2020-11-23	001565c69d03-1606129713913-record....	234.42	⤓ 🗑

  Total 3 10/page < 1 > Go to 1 Page

  ☑ Automatic upload recording file

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

Procedure

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

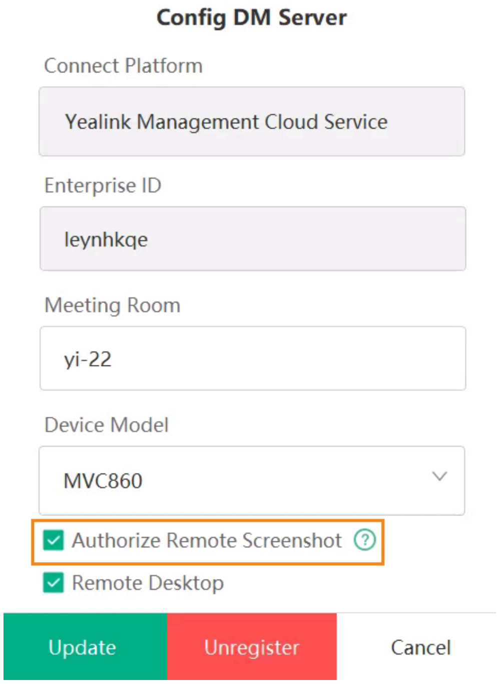
Note: You can click ⤓ to download the recording file or click 🗑 to delete the recording file.

Taking the Screenshot of the Device

About this task

For Microsoft Teams Rooms System, you should meet the following conditions. Otherwise, you cannot take screenshoot.

- Yealink RoomConnect in version 2.23.XX.0 (soon to be released) or higher.
- Enable the **Authorize Remote Screenshot** feature (on Yealink Room Connect software, go to ⚙ > **Config DM Server**).



Config DM Server

Connect Platform: Yealink Management Cloud Service

Enterprise ID: leynhkqe

Meeting Room: yi-22

Device Model: MVC860

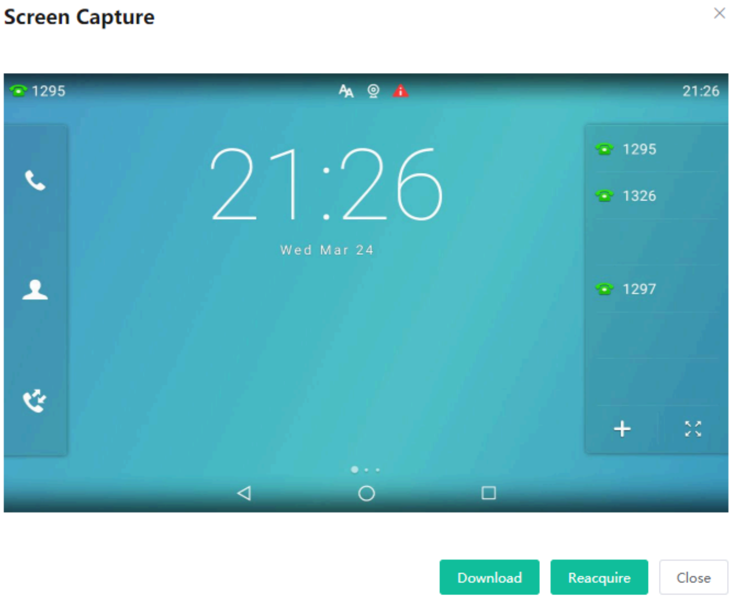
☑ Authorize Remote Screenshot

☑ Remote Desktop

For other devices, a dialog might pop up on the device screen when the first time you take screenshot. If the device owner does not allow your request for taking screenshots, you cannot take the screenshot. If the owner allow your request, the dialog will not pop up again and you can take screenshots.

Procedure

1. On the Device Diagnostics page, click **Screen Capture**.
2. Click **Download** to download the screenshoot.

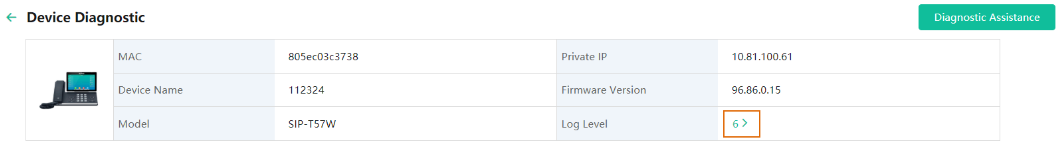


Tip: You can click **Reacquire** to acquire the latest screenshot.

Setting the Log Level

Procedure

1. On the Device Diagnostics page, click the value of **Log Level**.



← Device Diagnostic

MAC	805ec03c3738	Private IP	10.81.100.61
Device Name	112324	Firmware Version	96.86.0.15
Model	SIP-T57W	Log Level	6 >

2. Enter the desired value.
3. Click **OK**.

Download the Device Log

If you configure devices to report device logs to YDMP, you can download the 7-day logs saved on YDMP.

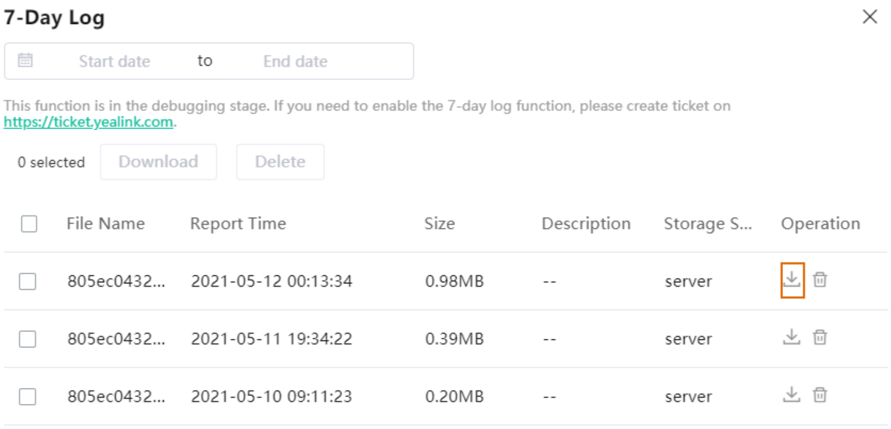
About this task

Note: Contact Yealink technical support to enable the feature of 7-day log.

Procedure

On the Device Diagnostics page, click **7-Day Log**, and do one of the following:

- Download a single log

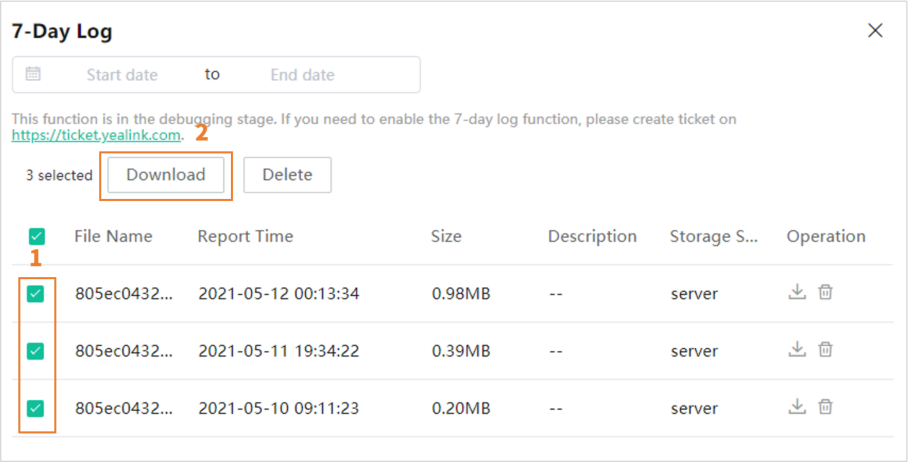


7-Day Log

This function is in the debugging stage. If you need to enable the 7-day log function, please create ticket on https://ticket.yealink.com.

□	File Name	Report Time	Size	Description	Storage S...	Operation
□	805ec0432...	2021-05-12 00:13:34	0.98MB	--	server	
□	805ec0432...	2021-05-11 19:34:22	0.39MB	--	server	
□	805ec0432...	2021-05-10 09:11:23	0.20MB	--	server	

- Download a batch of logs



7-Day Log

Start date to End date

This function is in the debugging stage. If you need to enable the 7-day log function, please create ticket on https://ticket.yealink.com.

3 selected

☑	File Name	Report Time	Size	Description	Storage S...	Operation
☑	805ec0432...	2021-05-12 00:13:34	0.98MB	--	server	
☑	805ec0432...	2021-05-11 19:34:22	0.39MB	--	server	
☑	805ec0432...	2021-05-10 09:11:23	0.20MB	--	server	

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

Backing up Configuration Files

You can back up 5 historical configuration files at most.

About this task

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 Timer Tasks.

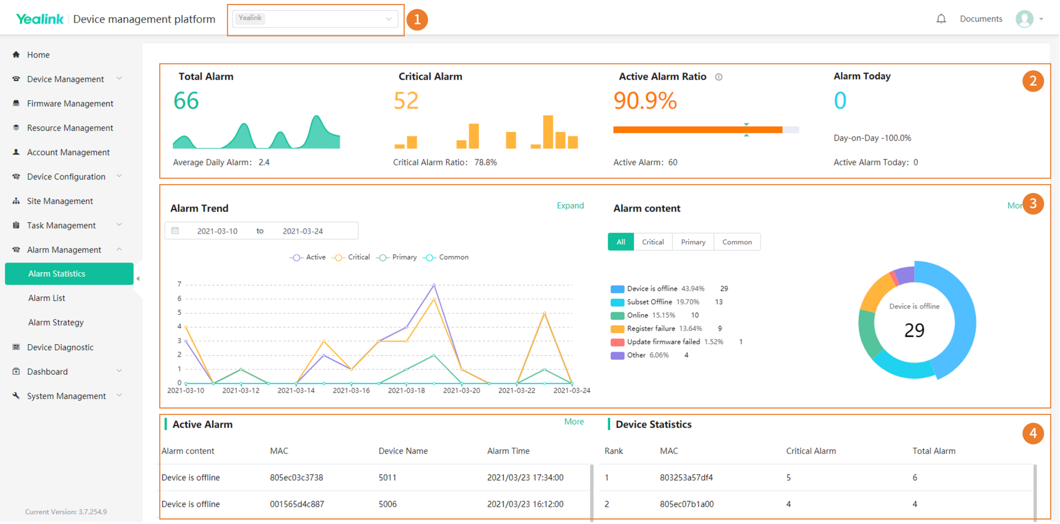
Managing Alarm

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.



Total Alarm
66
Average Daily Alarm: 2.4

Critical Alarm
52
Critical Alarm Ratio: 78.8%

Active Alarm Ratio
90.9%
Active Alarm: 60

Alarm Today
0
Day-on-Day -100.0%
Active Alarm Today: 0

Alarm Trend
2021-03-10 to 2021-03-24

Alarm content

Device is offline	43.94%	29
Subset Offline	19.70%	13
Online	15.15%	10
Register failure	13.64%	9
Update firmware failed	1.52%	1
Other	6.06%	4

Active Alarm

Alarm content	MAC	Device Name	Alarm Time
Device is offline	805ec03c3738	5011	2021/03/23 17:34:00
Device is offline	001565d4c887	5006	2021/03/23 16:12:00

Device Statistics

Rank	MAC	Critical Alarm	Total Alarm
1	803253a57df4	5	6
2	805ec07b1a00	4	4

Table 3:

No.	Feature	Description
1	Select the sites.	After you select the sites, the chart displays the statistics of the selected sites. The default value is all sites. **Note:** You can only select the sites which your account has the permission to.
2	Total Alarm	This chart displays the trend of the alarms in the recent 15 days.
	Critical Alarm	This chart displays the distribution of the critical alarms in the recent 15 days.
	Active Alarm Ratio	1. When the ratio is below 30%, the color of the scale bar is green. 2. When the ratio is between 30% ~ 70%, the color of the scale bar is yellow. 3. When the ratio is above 70%, the color of the scale bar is red.
	Alarm Today	The number of alarms today, the ratio of the alarms compared between today and yesterday, the number of active alarms today.
3	Alarm Trend	1. The statistics of the chart can select any rage within a half year. The default value is the statistics in the recent 15 days. 2. Click ⛶ to view in a larger screen. You can use this feature to view the statistics within a longer time scale. 3. Display or hide the trend of the statistics. The default value is displaying the trend of all statistics. 4. Move your mouse to the corresponding date to display the detailed data.
	Alarm Content	This chart displays the ratio and the number of each alarm content.

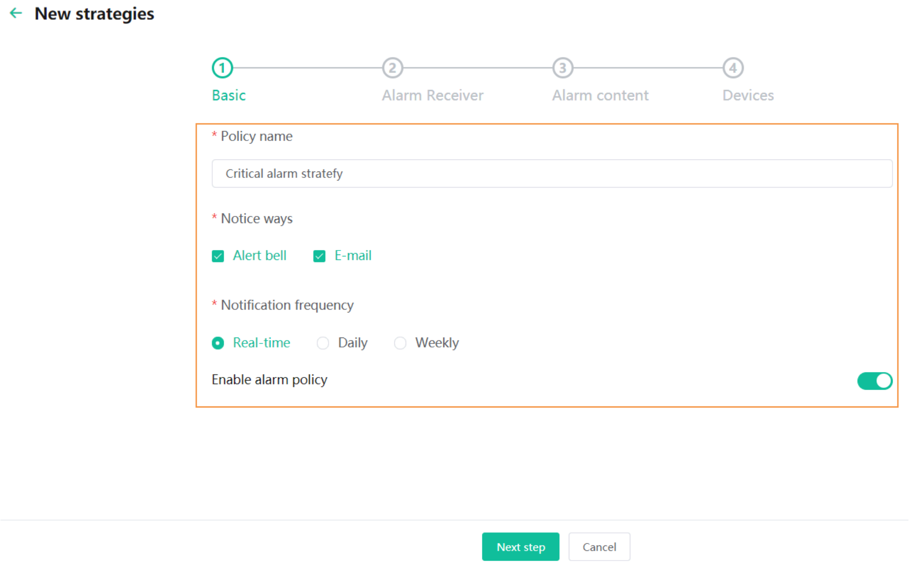
No.	Feature	Description
4	Active Alarm	Display the content of the active alarms of devices.
	Device Statistics	1. The devices ranks based on the number of critical alarms and the total number of alarms. 2. Click Critical Alarm. The devices ranks based on the number of the critical alarms in positive or negative sequence. 3. Click Total Alarm. The devices ranks based on the number of the total alarms in positive or negative sequence.

Adding Alarm Strategies

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

Procedure

1. Click **Alarm Management** > **Alarm Strategy** > **New strategies**.
2. Enter the corresponding information and click **Next step**.



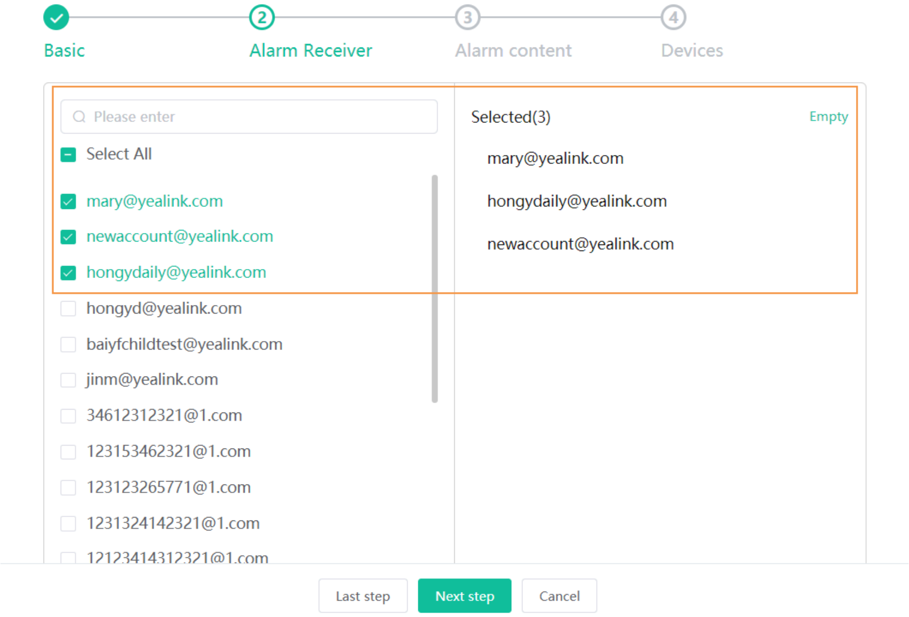
* Policy name: Critical alarm stratefy

* Notice ways: ☑ Alert bell ☑ E-mail

* Notification frequency: ● Real-time ○ Daily ○ Weekly

Enable alarm policy: On

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



☐ Select All

☑ mary@yealink.com

☑ newaccount@yealink.com

☑ hongydaily@yealink.com

☐ hongyd@yealink.com

☐ baiyfchildtest@yealink.com

☐ jinm@yealink.com

☐ 34612312321@1.com

☐ 123153462321@1.com

☐ 123123265771@1.com

☐ 1231324142321@1.com

☐ 12123414312321@1.com

Selected(3)

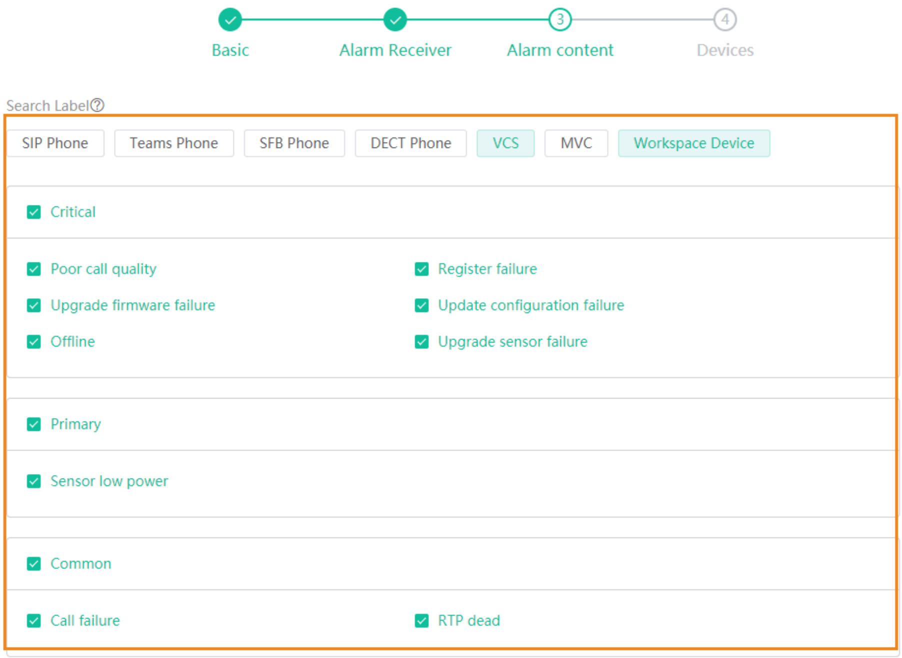
mary@yealink.com

hongydaily@yealink.com

newaccount@yealink.com

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

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



☑ Critical

☑ Poor call quality ☑ Register failure

☑ Upgrade firmware failure ☑ Update configuration failure

☑ Offline ☑ Upgrade sensor failure

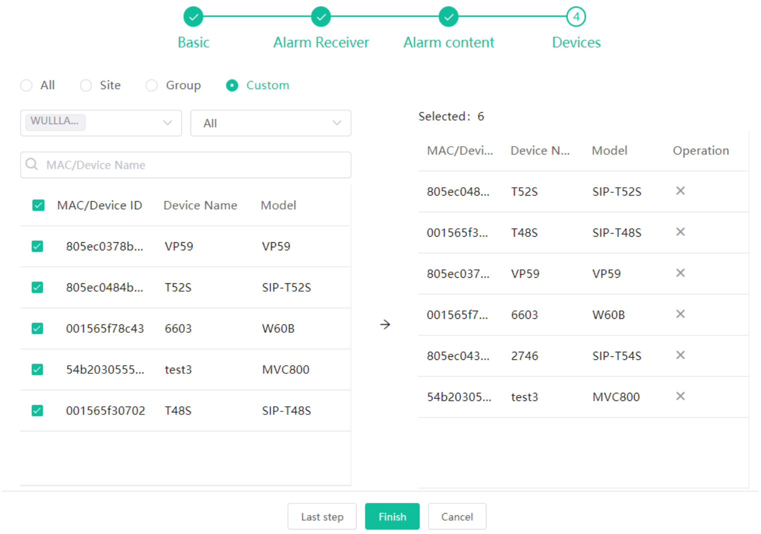
☑ Primary

☑ Sensor low power

☑ Common

☑ Call failure ☑ RTP dead

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



☑	MAC/Device ID	Device Name	Model
☑	805ec0378b...	VP59	VP59
☑	805ec0484b...	T52S	SIP-T52S
☑	001565f78c43	6603	W60B
☑	54b2030555...	test3	MVC800
☑	001565f30702	T48S	SIP-T48S

Selected: 6

MAC/Devi...	Device N...	Model	Operation
805ec048...	T52S	SIP-T52S	×
001565f3...	T48S	SIP-T48S	×
805ec037...	VP59	VP59	×
001565f7...	6603	W60B	×
805ec043...	2746	SIP-T54S	×
54b20305...	test3	MVC800	×

6. Click **Finish**.

Managing Alarm Strategies

Procedure

1. Click **Alarm Management** > **Alarm Strategy**.
2. Do one of the following:

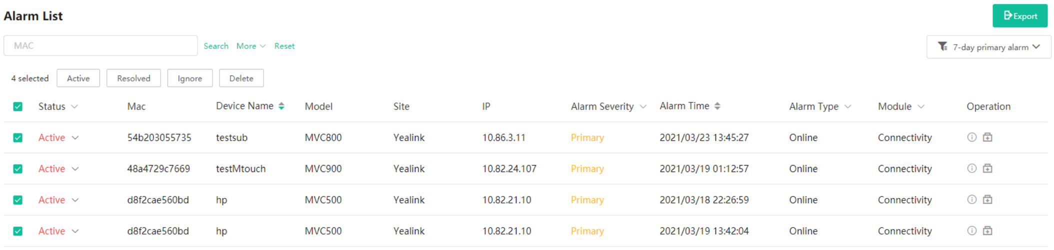
- Click ✎ beside the desired strategy, edit the parameter and save it.
- Select the corresponding strategy and click **Delete**.

Viewing Alarms

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

Procedure

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



☑	Status	Mac	Device Name	Model	Site	IP	Alarm Severity	Alarm Time	Alarm Type	Module	Operation
☑	Active	54b203055735	testsub	MVC800	Yealink	10.86.3.11	Primary	2021/03/23 13:45:27	Online	Connectivity	ⓘ
☑	Active	48a4729c7669	testMtouch	MVC900	Yealink	10.82.24.107	Primary	2021/03/19 01:12:57	Online	Connectivity	ⓘ
☑	Active	d8f2cae560bd	hp	MVC500	Yealink	10.82.21.10	Primary	2021/03/18 22:26:59	Online	Connectivity	ⓘ
☑	Active	d8f2cae560bd	hp	MVC500	Yealink	10.82.21.10	Primary	2021/03/19 13:42:04	Online	Connectivity	ⓘ

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

    The common alarm types are as below:

Device Model	Alarm Type	Severity
SIP Phones	Poor call quality	Critical
	Register failure	Critical
	Upgrade firmware failure	Critical
	Update configuration failure	Critical
	Offline	Critical
	Hold failure	Common
	Resume failure	Common
	RTP violate	Common
	RTP address change	Common
	RTP dead	Common
	SRTP failure	Common
	Call failure	Common
	Contact download failed	Common
SfB Phones	Poor call quality	Critical
	Register failure	Critical
	Upgrade firmware failure	Critical
	Update configuration failure	Critical
	Offline	Critical
	Visual voicemail retrieve failure	Common
	Hold failure	Common
	Resume failure	Common
	RTP violate	Common
	RTP address change	Common
	RTP dead	Common
	SRTP failure	Common
	Call log retrieve failure	Common
	Outlook contact retrieve failure	Common

Device Model	Alarm Type	Severity
	Call failure	Common
	Calendar synchronization failure	Primary
	Exchange discovery failure	Primary
VC Room Systems	Poor call quality	Critical
	Register failure	Critical
	Upgrade firmware failure	Critical
	Update configuration failure	Critical
	Offline	Critical
	Subset Offline	Critical
	Visual voicemail retrieve failure	Common
	RTP dead	Common
	SRTP failure	Common
	Call failure	Common
MVC Room Systems	Offline	Critical
	Associated device offline	Critical
	Wireless mic low power	Critical
	Wireless mic power off or disconnect	Critical
	Offline associated device back online	Primary
Teams Phones	Upgrade firmware failure	Critical
	Update configuration failure	Critical
	Offline	Critical
DECT Phones	Dect Manager backup	Critical
	Base backup	Critical
	Base upgrade failed	Critical
	Base status abnormal	Critical
	Handset upgrade failed	Critical
	Handset offline (only available to W70B)	Critical
	Handset low power (only available to W70B)	Critical
	Handset abnormal status (only available to W70B)	Critical
	Handset call failure	Common
YDMP	System license is about to expire	Critical
	Device capacity of license is insufficient	Critical

Related concepts

Managing Alarm

Filtering the Alarms

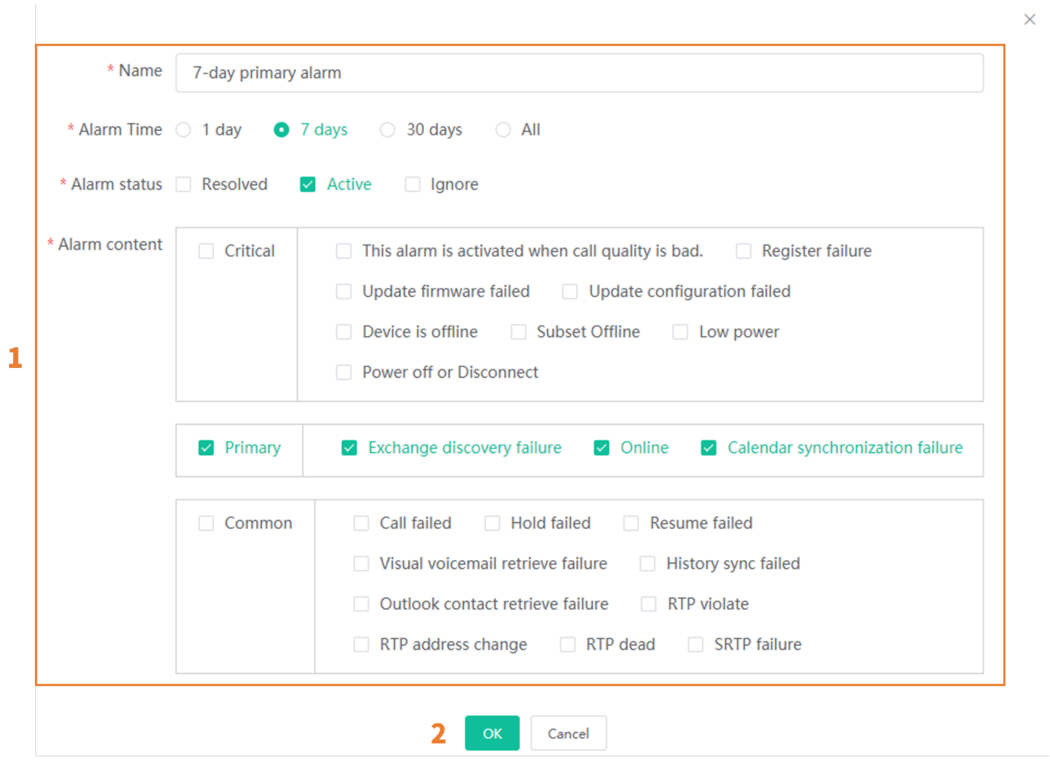
You can use the system built-in filter or customize the filters for filtering alarms.

- 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**.



* Name: 7-day primary alarm

* Alarm Time: ○ 1 day ● 7 days ○ 30 days ○ All

* Alarm status: □ Resolved ☑ Active □ Ignore

* Alarm content:

□ Critical: □ This alarm is activated when call quality is bad. □ Register failure □ Update firmware failed □ Update configuration failed □ Device is offline □ Subset Offline □ Low power □ Power off or Disconnect

☑ Primary: ☑ Exchange discovery failure ☑ Online ☑ Calendar synchronization failure

□ Common: □ Call failed □ Hold failed □ Resume failed □ Visual voicemail retrieve failure □ History sync failed □ Outlook contact retrieve failure □ RTP violate □ RTP address change □ RTP dead □ SRTP failure

OK Cancel

Filtering the Alarms

Procedure

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

Exporting Alarm Records

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

Procedure

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

Viewing Call Quality Statistics

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

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

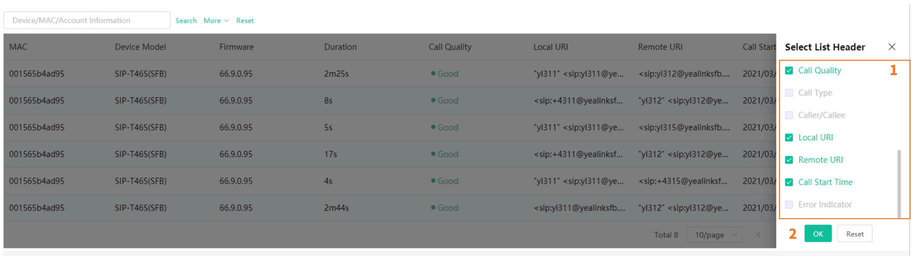
- Customizing the Indicators of Call Quality Detail
- Viewing the Call Data

Customizing the Indicators of Call Quality Detail

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

Procedure

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



MAC	Device Model	Firmware	Duration	Call Quality	Local URI	Remote URI	Call Start
001565b4ad95	SIP-T46S(SFB)	66.9.0.95	2m25s	● Good	"yl311" <sip:yl311@ye...	<sip:yl312@yealinksfb....	2021/03/
001565b4ad95	SIP-T46S(SFB)	66.9.0.95	8s	● Good	<sip:+4311@yealinksf...	"yl312" <sip:yl312@ye...	2021/03/
001565b4ad95	SIP-T46S(SFB)	66.9.0.95	5s	● Good	"yl311" <sip:yl311@ye...	<sip:yl315@yealinksfb....	2021/03/
001565b4ad95	SIP-T46S(SFB)	66.9.0.95	17s	● Good	<sip:+4311@yealinksf...	"yl312" <sip:yl312@ye...	2021/03/
001565b4ad95	SIP-T46S(SFB)	66.9.0.95	4s	● Good	"yl311" <sip:yl311@ye...	<sip:+4315@yealinksf...	2021/03/
001565b4ad95	SIP-T46S(SFB)	66.9.0.95	2m44s	● Good	<sip:yl311@yealinksfb....	"yl312" <sip:yl312@ye...	2021/03/

Total 8 10/page

Select List Header

☑ Call Quality
□ Call Type
□ Caller/Callee
☑ Local URI
☑ Remote URI
☑ Call Start Time
□ Error Indicator

OK Reset

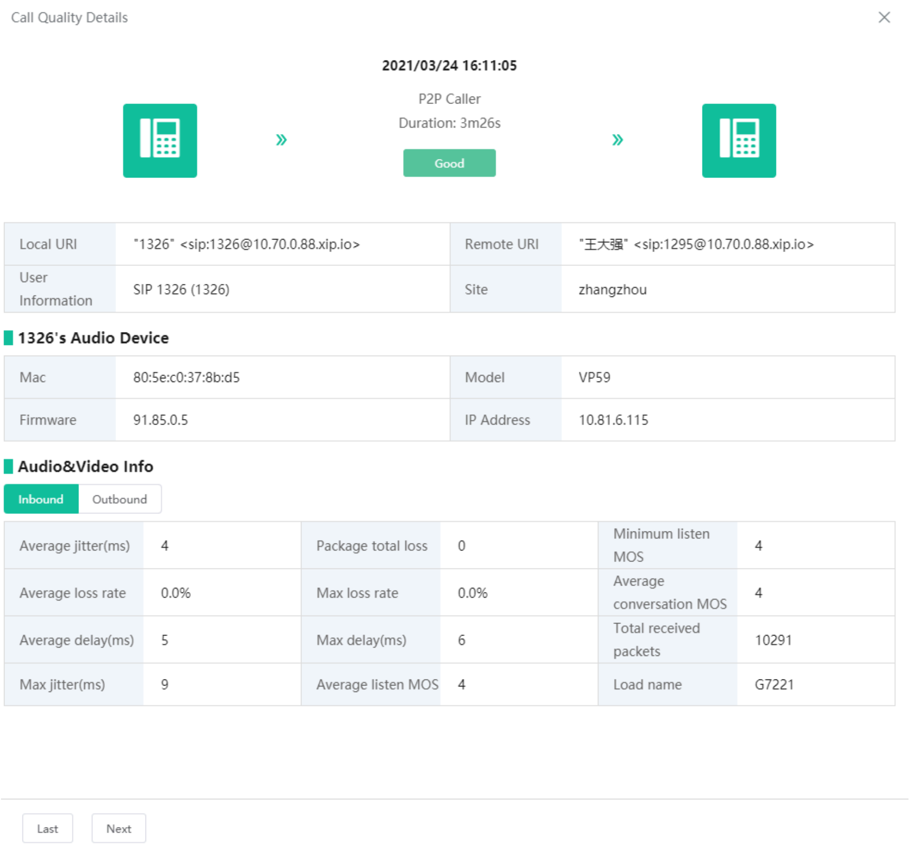
Results
The selected indicators are shown in the list of call quality detail.

Viewing the Call Data

Procedure

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

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



Call Quality Details ×

2021/03/24 16:11:05

P2P Caller

Duration: 3m26s

Good

Local URI	"1326" <sip:1326@10.70.0.88.xip.io>	Remote URI	"王大强" <sip:1295@10.70.0.88.xip.io>
User Information	SIP 1326 (1326)	Site	zhangzhou

1326's Audio Device

Mac	80:5e:c0:37:8b:d5	Model	VP59
Firmware	91.85.0.5	IP Address	10.81.6.115

Audio&Video Info

Inbound | Outbound

Average jitter(ms)	4	Package total loss	0	Minimum listen MOS	4
Average loss rate	0.0%	Max loss rate	0.0%	Average conversation MOS	4
Average delay(ms)	5	Max delay(ms)	6	Total received packets	10291
Max jitter(ms)	9	Average listen MOS	4	Load name	G7221

Last | Next

Table 4: Metrics of Call Data

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

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

Table 5: Evaluation Metrics of Call quality

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

System Management

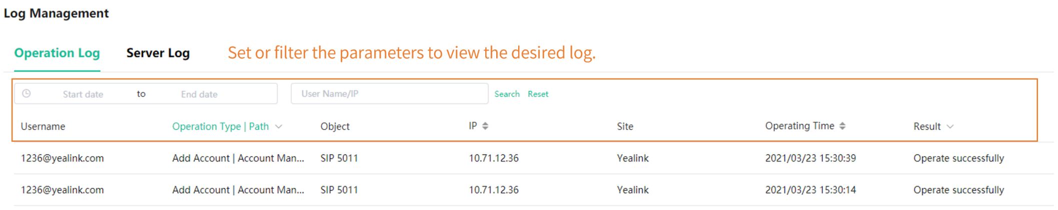
- Viewing Operation Logs
- Exporting the Server Log
- Configuring the SMTP Mailbox
- Uploading DST Rules
- Obtaining the Accesskey
- Uploading Multilingual Template for Importing Devices

Viewing Operation Logs

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

Procedure

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



Set or filter the parameters to view the desired log.

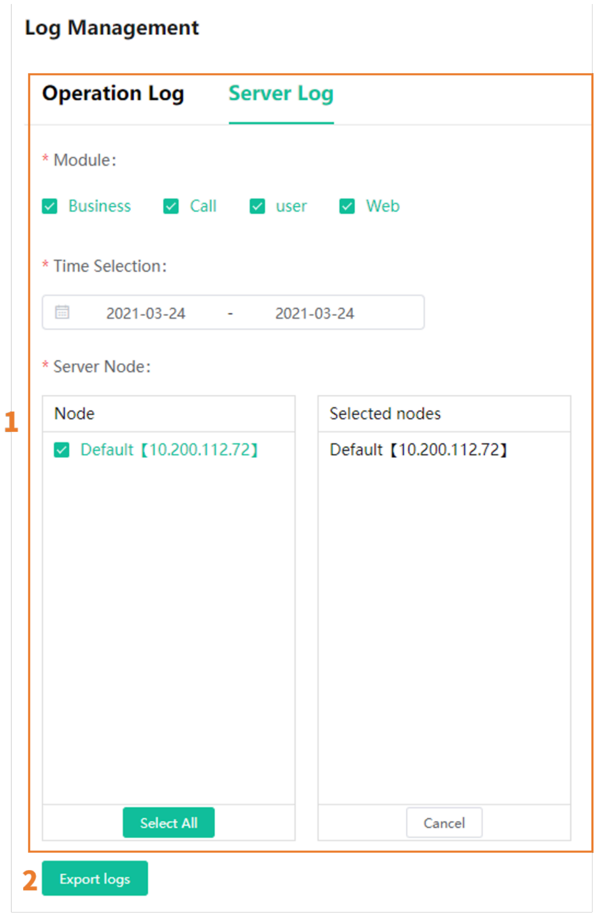
Username	Operation Type | Path	Object	IP	Site	Operating Time	Result
1236@yealink.com	Add Account | Account Man...	SIP 5011	10.71.12.36	Yealink	2021/03/23 15:30:39	Operate successfully
1236@yealink.com	Add Account | Account Man...	SIP 5011	10.71.12.36	Yealink	2021/03/23 15:30:14	Operate successfully

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.



Log Management

Operation Log | Server Log

* Module:

☑ Business ☑ Call ☑ user ☑ Web

* Time Selection:

2021-03-24 - 2021-03-24

* Server Node:

Node	Selected nodes
☑ Default【10.200.112.72】	Default【10.200.112.72】

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.

Parameter	Description
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 **Save and 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 **OK**.

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.

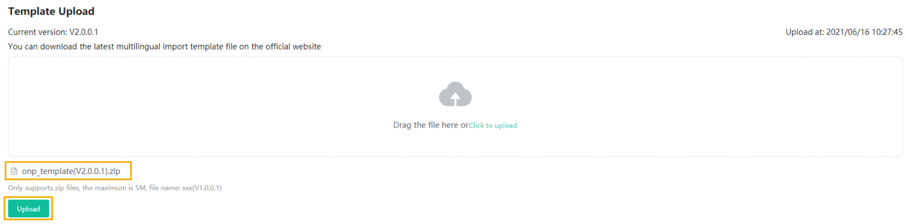
Uploading Multilingual Template for Importing Devices

The multilingual template for importing devices can help you import a batch of devices supported by YDMP. However, the template might not include the device newly supported by YDMP of the latest version if you upgrade YDMP from a lower version. Therefore, you need to download the template from Yealink official website and upload it to your YDMP. After that, the device model in the template will be updated synchronously.

Procedure

1. Click **System Management** > **Template Upload**.

2. Upload the zip file downloaded from Yealink website and click **Upload**.



Template Upload

Current version: V2.0.0.1

Upload at: 2021/06/16 10:27:45

You can download the latest multilingual import template file on the official website

Drag the file here orClick to upload

onp_template(V2.0.0.1).zip

Only supports zip files, the maximum is 5M, file name: xxx(V1.0.0.1)

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
- Enabling Login Protection
- Viewing the Account Code

Adding and Managing Groups

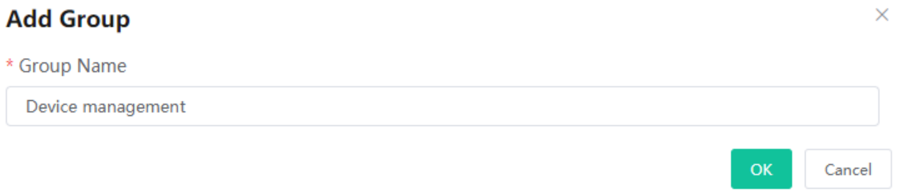
You can manage the roles by the group.

About this task

You cannot edit or delete the default group.

Procedure

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

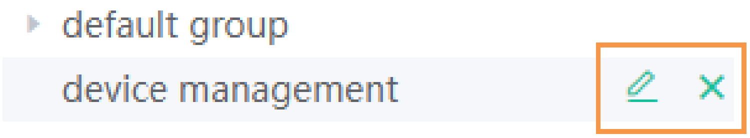


Add Group

* Group Name

Device management

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



Adding and Managing Roles

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

About this task

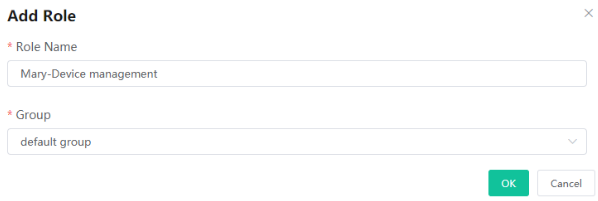
The default roles are as below, you cannot edit or delete them.

Table 6: Default role

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

Procedure

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



Add Role

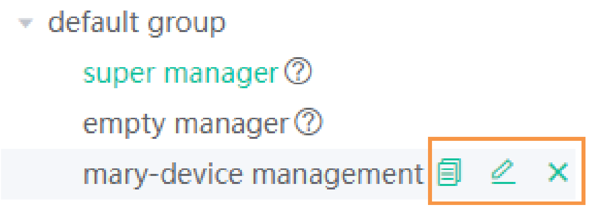
* Role Name

Mary-Device management

* Group

default group

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



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

Assigning the Function Permission

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

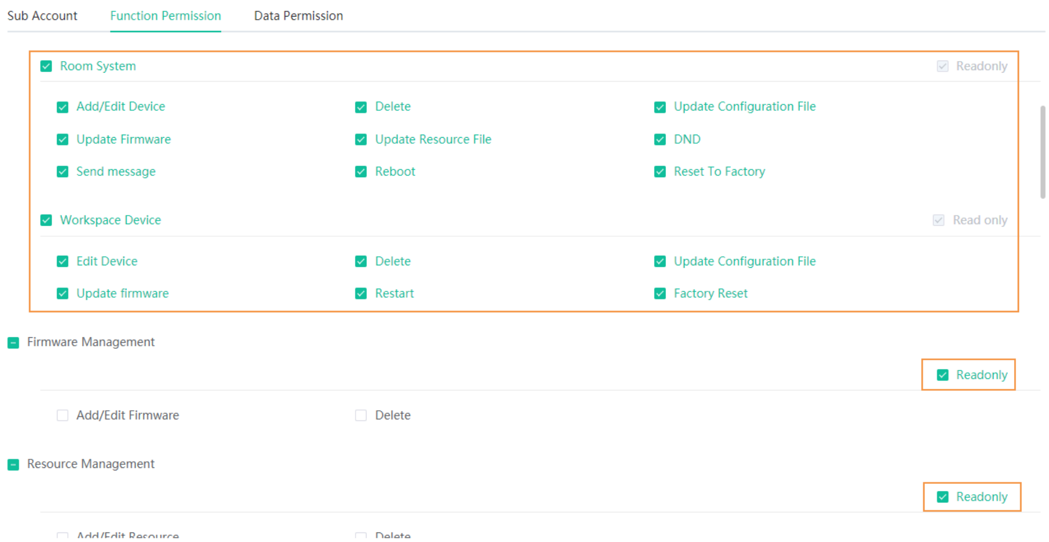
Before you begin

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

Procedure

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

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



Sub Account | Function Permission | Data Permission

☑ Room System — ☑ Readonly

☑ Add/Edit Device ☑ Delete ☑ Update Configuration File
☑ Update Firmware ☑ Update Resource File ☑ DND
☑ Send message ☑ Reboot ☑ Reset To Factory

☑ Workspace Device — ☑ Read only

☑ Edit Device ☑ Delete ☑ Update Configuration File
☑ Update firmware ☑ Restart ☑ Factory Reset

▣ Firmware Management — ☑ Readonly

□ Add/Edit Firmware □ Delete

▣ Resource Management — ☑ Readonly

□ Add/Edit Resource □ Delete

Assigning the Data Permission

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

Before you begin

Add roles, refer to Adding and Managing Roles.

Procedure

1. Click **System Management** > **Role Management**.
2. Select the corresponding role and click **Data Permission**.
3. Select the check box of the site you want to manage.

- □ If you have assigned the function permission to the sub-administrator (Assigning the Function Permission), the sub-administrator can only view/use the firmware, resources, accounts, and configuration of this site, but cannot modify/delete them.
- ☑ If you have assigned the function permission to the sub-administrator (Assigning the Function Permission), the sub-administrator can view/use/modify/delete the firmware, resources, accounts, and configuration of this site.

Related tasks

Adding Sites

Adding Accounts

Adding Firmware

Adding Resource Files

Adding Configuration Templates

Adding and Managing Sub-Administrator Accounts

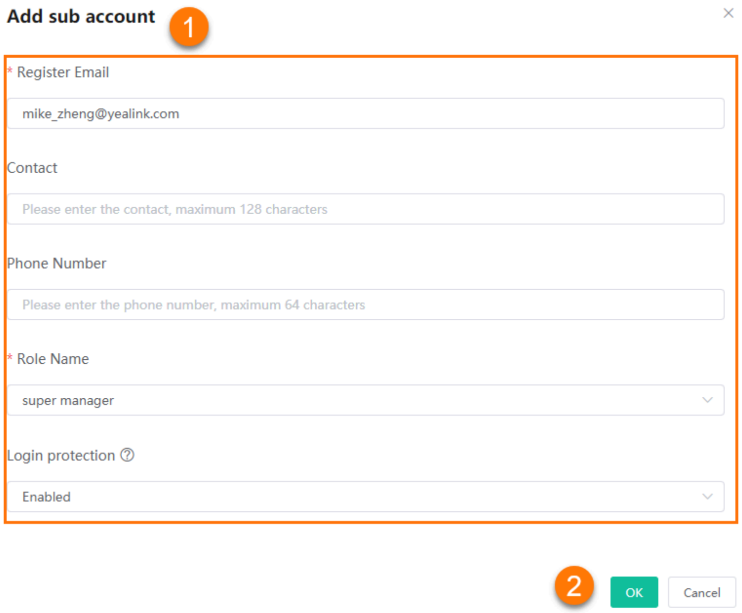
Before you begin

You have added roles.

If you want to enable the login protection feature for a sub-administrator account, see Enabling Login Protection.

Procedure

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



Add sub account

* Register Email: mike_zheng@yealink.com

Contact: Please enter the contact, maximum 128 characters

Phone Number: Please enter the phone number, maximum 64 characters

* Role Name: super manager

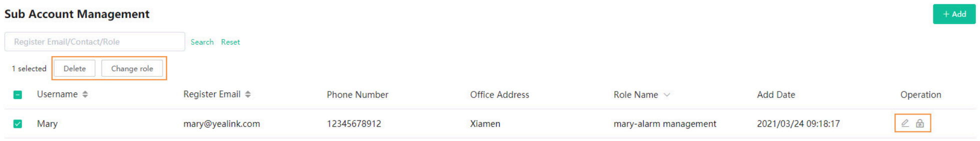
Login protection ⓘ: Enabled

2. Confirm the account information and click **OK**.

Note:

After adding the sub-administrator account, you can change the role, assign function permission or data permission, or reset the password.

If you change the account information, YDMP will email the corresponding sub-administrators automatically.



Sub Account Management

1 selected | Delete | Change role

☐	Username	Register Email	Phone Number	Office Address	Role Name	Add Date	Operation
☑	Mary	mary@yealink.com	12345678912	Xiamen	mary-alarm management	2021/03/24 09:18:17	✎ 🔒

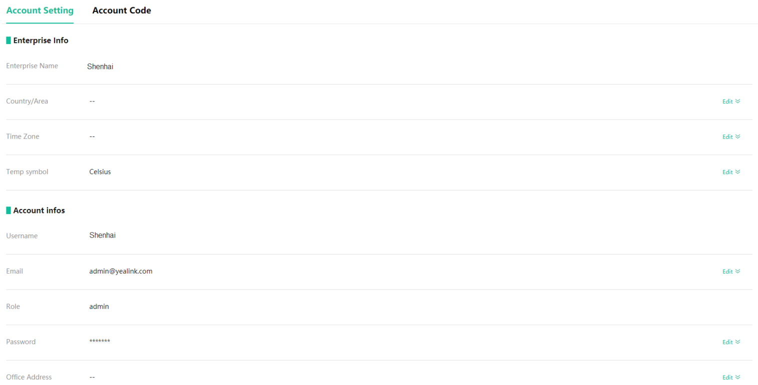
If you enable SMTP mailbox (refer to Configuring the SMTP Mailbox), the account information will be sent to the mailbox of the sub-administrator automatically.

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 and save the related information.



Account Setting Account Code

Enterprise Info

Enterprise Name Shenhai

Country/Area -- Edit

Time Zone -- Edit

Temp symbol Celsius Edit

Account infos

Username Shenhai

Email admin@yealink.com Edit

Role admin

Password ******* Edit

Office Address -- Edit

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.

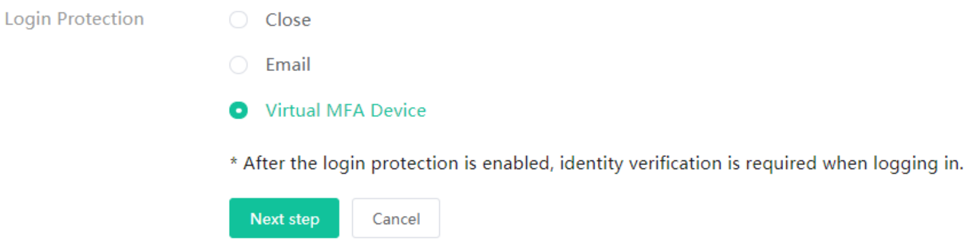
Enabling Login Protection

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

Procedure

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

2. In the **Login Protection** field, click **Edit**.



Login Protection

○ Close

○ Email

● Virtual MFA Device

* After the login protection is enabled, identity verification is required when logging in.

Note: The enterprise administrator controls the login protection feature. Therefore, the sub-administrators cannot disable this feature on their own.

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

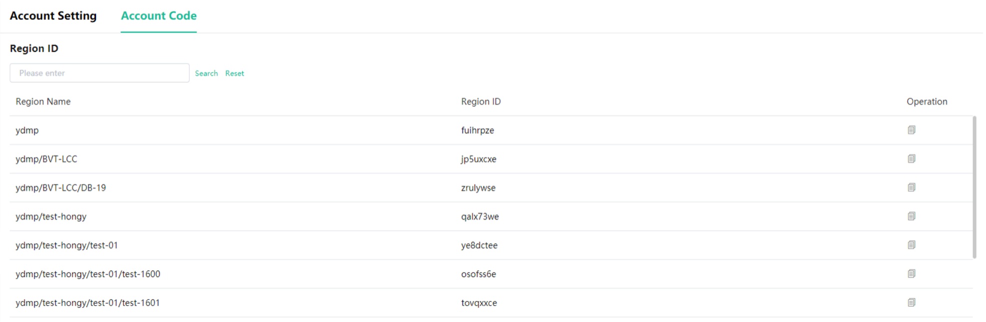
   If the page prompts “Login expired, please log in again", you need to use the new verification method to complete the login.

Viewing the Account Code

The account code is the 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**.



Region Name	Region ID	Operation
ydmp	fuihrpze	▤
ydmp/BVT-LCC	jp5uxcxe	▤
ydmp/BVT-LCC/DB-19	zrulywse	▤
ydmp/test-hongy	qalx73we	▤
ydmp/test-hongy/test-01	ye8dctee	▤
ydmp/test-hongy/test-01/test-1600	osofss6e	▤
ydmp/test-hongy/test-01/test-1601	tovqxxce	▤

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?
- How to Change/Customize Port 443 If It Is Occupied

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.

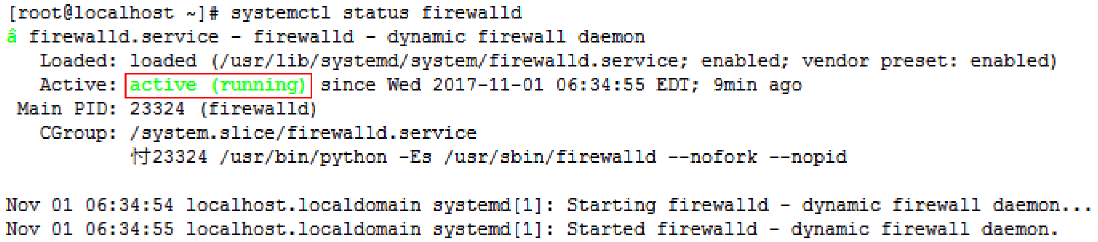
Windows:

- 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
           忖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:

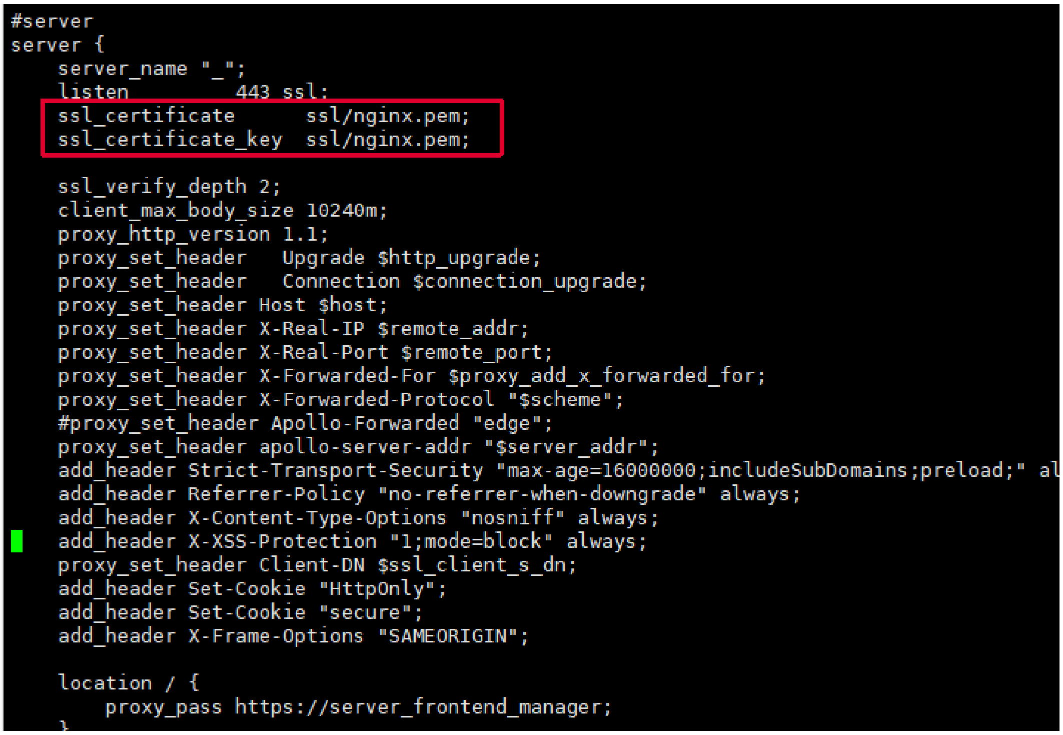
1. Edit the install.conf file under the directory of /usr/local/yealink/data/. Add the domain name of tcp and web in the [global] configuration field, see the following example

   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*.

How to Change/Customize Port 443 If It Is Occupied

When using HTTPS certificate to access the YDMP web page, you also need to upload the corresponding certificate to the devices, which might cause the device unavailable to obtain the *dm.cfg* file. To solve this problem, you can assign two port, with one for accessing YDMP web page and another one for the phone to access *dm.cfg*.

About this task

Note:

If it is the first time you deploy YDMP and want to change the port 443, you can press Ctrl + C after running the command *./install*. This will generate an *install.conf* file. After that, you can follow the step below.

Procedure

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

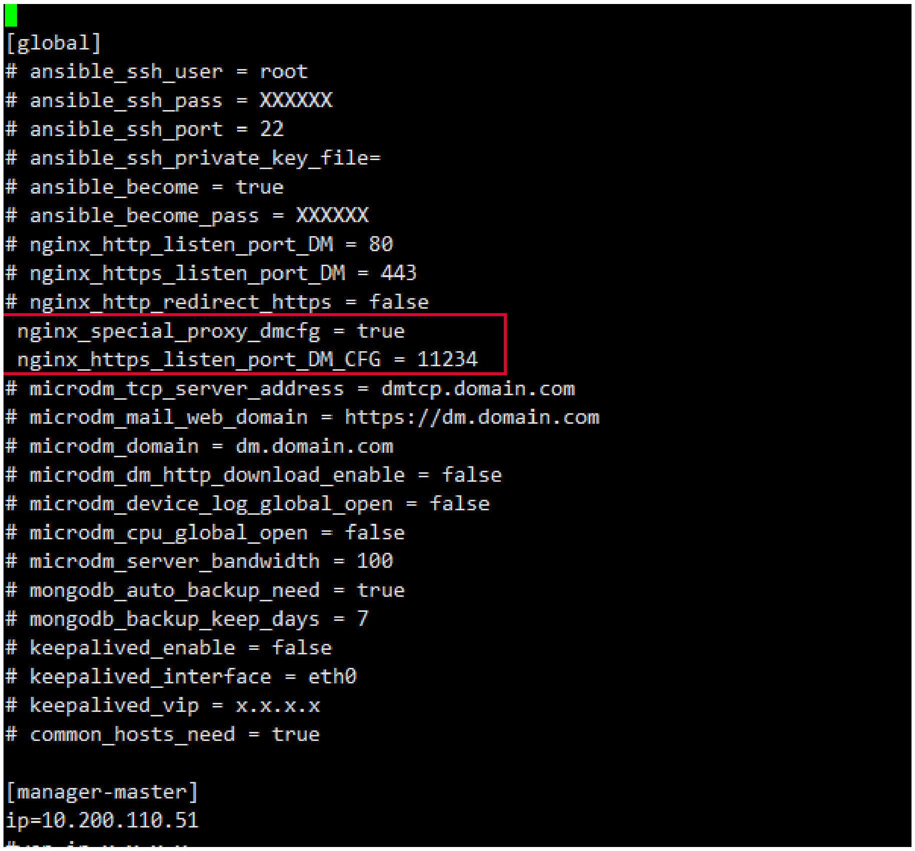
   ```
   vi /usr/local/yealink/data/install.conf
   ```

3. Run the command below:

   ```
   nginx_special_proxy_dmcfg = true ## Remove the # symbol.##
   ```

```
nginx_https_listen_port_DM_CFG = XXX ## Change XXX
 in nginx_https_listen_port_DM_CFG = XXX to the desired port (range: 0-65535) and remove
 the # symbol.##
```

Note: For versions lower than 3.7.0.1 (not including 3.7.0.1), this parameter may be different or wrong. Please change it to *nginx_https_listen_port_DM_CFG = XXX*.



```
[global]
# ansible_ssh_user = root
# ansible_ssh_pass = XXXXXX
# ansible_ssh_port = 22
# ansible_ssh_private_key_file=
# ansible_become = true
# ansible_become_pass = XXXXXX
# nginx_http_listen_port_DM = 80
# nginx_https_listen_port_DM = 443
# nginx_http_redirect_https = false
 nginx_special_proxy_dmcfg = true
 nginx_https_listen_port_DM_CFG = 11234
# microdm_tcp_server_address = dmtcp.domain.com
# microdm_mail_web_domain = https://dm.domain.com
# microdm_domain = dm.domain.com
# microdm_dm_http_download_enable = false
# microdm_device_log_global_open = false
# microdm_cpu_global_open = false
# microdm_server_bandwidth = 100
# mongodb_auto_backup_need = true
# mongodb_backup_keep_days = 7
# keepalived_enable = false
# keepalived_interface = eth0
# keepalived_vip = x.x.x.x
# common_hosts_need = true

[manager-master]
ip=10.200.110.51
```

4. Save the change and run the following command to apply the change to all services.

```
./install
```

If it prompts "nginx failure", the port you choose might be occupied by other services.

Repeat step 2, 3 and 4 to change the port to another one and rerun command *./install*.

Results

When the installation finishes, you can use the new port to access YDMP.