

Yealink Device Management Platform Administrator Guide V3.6.0.1

Contents

About This Guide.....	7
Related Documentations.....	7
Summary of Changes.....	7
Changes for Release 36, Guide Version V3.6.0.1.....	7
Changes for Release 35, Guide Version V3.5.0.21.....	8
Changes for Release 35, Guide Version V3.5.0.20.....	8
Changes for Release 35, Guide Version V3.5.0.11.....	8
Changes for Release 35, Guide Version V3.5.0.10.....	8
Changes for Release 35, Guide Version V3.5.0.1.....	9
Changes for Release 34, Guide Version V3.4.0.10.....	9
Introduction of Yealink Device Management Platform.....	9
Browser Requirements.....	9
Supported Device Models.....	10
Port Requirements.....	11
Deploying YDMP.....	11
Hardware and Software Requirements.....	12
Updating YDMP (from V2.0 to V3.1).....	12
Restoring YDMP (from V3.1 to V2.0).....	13
Installing YDMP 3.X (3.5.0.11 or Earlier Versions).....	14
Installing YDMP 3.X (3.5.0.20 or later Versions).....	14
Downloading the Installation Package.....	15
Closing the Firewall Came with the Linux System.....	15
Unzipping the Installation Package.....	15
Installing YDMP.....	15
Importing the HTTPS Certificate.....	17
Updating YDMP (from V3.1 to V3.X).....	18
Installing the Diagnostic Script.....	18
Activating the License.....	19
Importing the Device Certificate.....	19
Activating the License Online.....	20
Activating the License Offline.....	20
Updating the Configuration.....	20
Uninstalling YDMP.....	21
Getting Started.....	21
Logging in to YDMP.....	21
Home Page.....	22
Logging out of YDMP.....	23
Connecting to YDMP.....	23
Connecting SIP Device.....	23

Using Certificates for Mutual TLS Authentication.....	24
Configuring the Common.cfg File.....	24
Deploying Devices on the RPS (Redirection & Provisioning Server) Management Platform...	25
Configuring the Server Address.....	25
Connecting USB Devices.....	26
Connecting Room System.....	26

Managing Devices.....26

Device Status.....	26
Running State Page.....	27
Managing SIP Devices.....	27
Editing the Device Information.....	28
Exporting the Device Information.....	28
Viewing the Information of SIP Device.....	29
Searching for Devices.....	29
Assigning Accounts to Devices.....	30
Setting the Sites.....	30
Pushing Configuration Files to Devices.....	31
Pushing Firmware to Devices.....	31
Pushing Resource Files to Devices.....	32
Diagnosing Devices.....	33
Enabling/Disabling DND.....	33
Sending Messages to Devices.....	34
Rebooting Devices.....	35
Resetting the Devices to Factory.....	35
Deleting Devices.....	36
Managing USB Devices.....	36
Editing the Device Information.....	37
Exporting the Device Information.....	37
Viewing the USB Device.....	37
Searching for Devices.....	37
Setting the Sites.....	38
Deleting Devices.....	38
Managing Room System.....	38
Editing the Device Information.....	39
View the Information of the Room System.....	39
Searching for Devices.....	40
Setting the Sites.....	40
Rebooting Devices.....	40
Pushing Firmware to Devices.....	41
Deleting Devices.....	41
Managing Firmware.....	42
Adding Firmware.....	42
Pushing Firmware to Devices.....	42
Editing the Firmware.....	43
Downloading the Firmware.....	43
Deleting Firmware.....	43
Managing Resources.....	44
Adding Resource Files.....	44
Pushing Resource Files to Devices.....	44
Editing Resource Files.....	45
Downloading the Resource Files.....	45
Deleting Resource Files.....	45

Managing Accounts.....	46
Adding Accounts.....	46
Importing Accounts.....	46
Editing the Account Information.....	47
Exporting Accounts.....	47
Deleting Accounts.....	47
 Managing the Device Configuration.....	 47
Managing Model Configuration.....	48
Adding Configuration Templates.....	48
Setting Parameters.....	48
Pushing Configuration to Devices.....	51
Editing Configuration Templates.....	52
Downloading the Model File.....	52
Viewing Parameters.....	52
Deleting Templates.....	53
Managing the Site Configuration.....	53
Adding Site Configuration Templates.....	53
Setting Parameters.....	53
Pushing the Site Configuration to Devices.....	56
Editing the Site Configuration Template.....	56
Downloading the Site Configuration Template.....	57
Deleting Site Configuration Templates.....	57
Managing the Group Configuration.....	57
Adding the Group Configuration.....	57
Setting Parameters.....	58
Editing Groups.....	61
Pushing the Group Configuration.....	62
Viewing Parameters.....	62
Downloading Configuration File.....	63
Deleting Groups.....	63
Managing the MAC Configuration.....	63
Uploading Backup Files.....	63
Generating Configuration Files.....	64
Setting Parameters.....	64
Pushing Backup Files to Devices.....	65
Downloading the Configuration Files.....	66
Exporting the Configuration Files.....	66
Deleting Backup Files.....	66
Configuring Global Parameters.....	66
 Managing Sites.....	 66
Adding Sites.....	66
Importing Sites.....	67
Editing Sites.....	68
Deleting Sites.....	69
 Managing Tasks.....	 69
Adding Timer Tasks.....	70
Editing Timer Tasks.....	71
Pausing or Resuming Timer Tasks.....	71

Ending Timer Tasks.....	72
Searching for Timer Tasks.....	72
Viewing Timer Tasks.....	72
Viewing Tasks.....	73
Searching for Executed Tasks.....	73

Diagnosing Devices..... 74

Starting Diagnosing.....	74
Exporting the Packets, Logs, and Configuration Files by One Click.....	75
Capturing Packets.....	76
Diagnosing the Network.....	78
Exporting System Logs.....	79
Exporting the Configuration Files.....	79
Viewing the CPU and the Memory Status.....	79
Viewing Recordings.....	80
Capturing the Screenshot of the Device.....	81
Getting the Device Log.....	81
Setting the Log Level.....	82
Download the Device Log.....	82
Diagnostic Assistance.....	82
Ending the Diagnostic.....	82

Managing Alarm..... 82

Alarm Statistics.....	83
Adding Alarm Strategies.....	85
Managing Alarm Strategies.....	87
Viewing Alarms.....	88
Filtering the Alarms.....	90
Customizing Filters.....	90
Filtering the Alarms.....	91
Exporting Alarm Records.....	91

Viewing Call Quality Statistics..... 92

Customizing the Indicators of Call Quality Detail.....	92
Viewing the Call Data.....	92

Managing System..... 94

Viewing Operation Logs.....	94
Exporting the Server Log.....	95
Configuring the SMTP Mailbox.....	95
Uploading DST Rules.....	97
Obtaining the Accesskey.....	97

Managing Administrator Accounts..... 97

Adding/Editing/Deleting a Group.....	97
Adding/Editing/Deleting a Role.....	98
Assigning the Function Permission.....	99
Assigning the Data Permission.....	100
Adding and Managing Sub-Administrator Accounts.....	100
Editing the Account Information.....	101
Viewing the Account Code.....	101

Troubleshooting..... 102

 Forget the Login Password?..... 102

 Why You Cannot Access the Login Page?..... 102

 Why the Browser Prompts That the Security Certificate of the Website Is not Trusted When You
 Access the Login Page?..... 103

About This Guide

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

- [Related Documentations](#)

Related Documentations

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

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

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

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

Summary of Changes

- [Changes for Release 36, Guide Version V3.6.0.1](#)
- [Changes for Release 35, Guide Version V3.5.0.21](#)
- [Changes for Release 35, Guide Version V3.5.0.20](#)
- [Changes for Release 35, Guide Version V3.5.0.11](#)
- [Changes for Release 35, Guide Version V3.5.0.10](#)
- [Changes for Release 35, Guide Version V3.5.0.1](#)
- [Changes for Release 34, Guide Version V3.4.0.10](#)

Changes for Release 36, Guide Version V3.6.0.1

The following sections are new for this version:

- [Getting the Device Log](#)

Major updates have occurred to the following sections:

- [Supported Device Models](#)
- [Viewing the Information of SIP Device](#)
- [Adding 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 sections are new for this version:

- [Installing YDMP 3.X \(3.5.0.20 or later Versions\)](#)

Major updates have occurred to the following sections:

- [Hardware and Software Requirements](#)
- [Supported Device Models](#)
- [Updating YDMP \(from V3.1 to V3.X\)](#)
- [Why the Browser Prompts That the Security Certificate of the Website Is not Trusted When You Access the Login Page?](#)

Changes for Release 35, Guide Version V3.5.0.11

Major updates have occurred to the following sections:

- [Supported Device Models](#)
- [Deploying YDMP](#)
- [Viewing Alarms](#)

Changes for Release 35, Guide Version V3.5.0.10

The following sections are new for this version:

- [Alarm Statistics](#)
- [Filtering the Alarms](#)
- [Exporting Alarm Records](#)

Major updates have occurred to the following sections:

- [Supported Device Models](#)
- [Adding Alarm Strategies](#)
- [Managing Alarm Strategies](#)

Changes for Release 35, Guide Version V3.5.0.1

The following sections are new for this version:

- [Uploading DST Rules](#)

Major updates have occurred to the following sections:

- [Managing Tasks](#)

Changes for Release 34, Guide Version V3.4.0.10

The following sections are new for this version:

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

Major updates have occurred to the following sections:

- [Configuring the Common.cfg File](#)
- [Adding Sites](#)
- [Starting Diagnosing](#)

Introduction of Yealink Device Management Platform

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

- [Browser Requirements](#)
- [Supported Device Models](#)
- [Port Requirements](#)

Browser Requirements

YDMP supports the following browsers:

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

Supported Device Models

You can manage the following devices via YDMP:

Device Types	Supported Device Models	Version Requirements
SIP IP Phones	SIP-T27P/T27G/ T29G/T41P/T41S/T42G/T42S/ T42U/T46G/ T46S/T48G/T48S/T52S/T54S	XX.83.0.30 or later (except for XX.84.0.10). XX represents the fixed number for each device model.
	SIP-T56A/T58	58.83.0.5 or later.
	SIP-T19(P)E2/T21(P)E2/T23P/ T23G/T40P/T40G	XX.83.0.30 or later (XX.84.0.10 is not supported and XX.84.0 or later versions are not supported anymore). XX represents the fixed number for each device model.
	SIP-CP960	73.83.0.10 or later.
	SIP-CP920	78.84.0.15 or later.
	SIP-T53/T53W	95.84.0.10 or later.
	SIP-T54W	96.84.0.10 or later.
	SIP-T57W	97.84.0.30 or later.
	VP59	91.283.0.10 or later.
	SIP-T42U/T43U/T46U/T48U	108.84.0.30 or later.
	SIP-T30/T30P/T31/T31P/T31G/ T33P/T33G	124.85.0.10 or later.
Skype for Business HD IP phones	T41S/T42S/T46S/T48S	66.9.0.45 or later (except for 66.9.0.46).
	T58/T56A/T55A	55.9.0.6 or later.
	CP960	73.8.0.27 or later.
	MP56	122.9.0.1 or later.
Teams phones (It is not available for managing the accounts and viewing the call quality)	CP960	73.15.0.20 or later.
	T56A/T58	58.15.0.20 or later.
	T55A	58.15.0.36 or later.
	VP59	91.15.0.16 or later.
	MP56	122.15.0.9 or later.
	VC210	118.15.0.20 or later.
Video Conferencing Systems	VC200/VC500/VC800/VC880	XX.32.10.25/XX.32.0.25 or later. XX represents the fixed number for each device model.

Device Types	Supported Device Models	Version Requirements
	PVT950/PVT980	1345.32.10.40 or later.
	VP59	91.332.0.10 or later.
	PVT940/PVT960	120.43.0.25 or later.
Zoom phones	CP960	73.30.0.10 or later.
Room System	MVC500/MVC800/MVC300/ CP960-UVC Zoom Rooms Kit/ VP59 Zoom Rooms Kit	XX.11.0.10 or later.
	MVC400	2.2.23.0 or later



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

Port Requirements

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

Port	Description
443	It is used for accessing the device management platform via HTTPS.
9989	It is used for the phone to download the configuration files and calling the API.
9090	TCP persistent connection. It is used for reporting the device information.
8446	It is used for mutual authentication between YDMP and the devices when pushing the configuration, the firmware, and the resource files to the devices.
80	It is used for accessing the platform via HTTP.

Deploying YDMP

This chapter introduces how to install and deploy YDMP.

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

- [Updating the Configuration](#)
- [Uninstalling YDMP](#)

Hardware and Software Requirements

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

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

Requirements for stand-alone installation:

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

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

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



Note:

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

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

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

- 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](#) .
1. Log into CentOS as the root user and open the terminal.
 2. Run the command:

```
cd /usr/local
tar -zxvf DM_3.1.0.13.tar.gz
cd yealink_install&& tar -zxvf 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.

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)

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

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

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

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



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

1. Run the command:

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

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

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

YDMP will be restored to V2.0.

Installing YDMP 3.X (3.5.0.11 or Earlier Versions)

The following is an example of installing V3.5.0.1.

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

```
cd /usr/local
tar -zxf DM_3.5.0.1.tar.gz
cd yealink_install&& tar -zxf install.tar.gz
./install --host the internal IP or the external IP
##If it is the deployment of a single NIC (the internal network or the external network), run this
command. ##
./install --host the internal IP -e nat_ip=the external IP behind NAT
##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this
command.## This command is only applicable to 3.3.0.0 or later versions.
Make sure that the default gateway is the gateway of the external NIC.
Run the command "ip route" to request the default gateway.
Run the command "ip route add default via gateway IP dev external NIC name" to edit the
default gateway. ##
./install --host the internal IP -e nat_ip=the external IP behind NAT
##If it is the deployment of dual NIC (the internal and the external network), run this command. This
command is only applicable to 3.3.0.0 or later versions. ##
```

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

```
./conf/roles/tasks/l1configure.yml
./conf/roles/tasks/l2logrotate.yml
./conf/roles/tasks/l3service.yml
./conf/roles/tasks/main.yml
./conf/roles/templates
./conf/roles/templates/l1.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 all
[B] - deploy ydmp for cluster
Please Input your choice: A
```

The installation starts and takes some time to finish.

Installing YDMP 3.X (3.5.0.20 or later Versions)

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

- [Downloading the Installation Package](#)
- [Closing the Firewall Came with the Linux System](#)
- [Unzipping the Installation Package](#)
- [Installing YDMP](#)
- [Importing the HTTPS Certificate](#)

Downloading the Installation Package

- The server can access the external network

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

```
cd /usr/local
```

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

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

- The server cannot access the external network

1. Manually download the installation package, which you obtain from Yealink technical support engineers.
2. Use SecureCRT to go to the command interface of the root account via SSH.
3. Run the following command to go to the directory (/usr/local).

```
cd /usr/local
```

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

Closing the Firewall Came with the Linux System

Run the following command to close the firewall:

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

Unzipping the Installation Package

Run the following command:

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

Installing YDMP

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

- 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.

1. Run the command:

```
cd /usr/local/yealink_install/
./install
##If it is the single NIC deployment (internal or external), run this command.##
./install -e nat_ip=the external IP behind NAT IP
##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this
command.
Make sure that the default gateway is the gateway of the external NIC.
```

Run the command “`ip route`” to request the default gateway.
 Run the command “`ip route add default via gateway IP dev external NIC name`” to edit the default gateway. ##
`./install -e nat_ip=the external IP`
 ##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this command.##

```

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: _

```

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.

```

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

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]
#The settings of global variable
ansible_ssh_user = root #The default value is root user. It is used to log into the back-end server.
ansible_ssh_pass = xxxxxxxxxx #The login password of the user. We recommend that you set the same password for all
# ansible_become = true #nodes to edit them together in the global settings.
# ansible_become_pass = xxxxxx
nginx_http_listen_port = 80 #The non-root user should configure these two items. The
nginx_https_listen_port = 443 #password is same with the above one.
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 #Master node
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

#Sub-master node

[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
```

Annotations in the image:

- `microdm_mail_web_domain`: The same as microdm_mail_web_domain. Remove https://
- `microdm_domain`: Edit it as the domain name for accessing YDMP.
- `microdm_tcp_server_address`: Edit it as the domain name for phones to connect to YDMP through TCP connection.
- `microdm_service_default_domain`: You do not need to edit this. It is used for interactive use among cluster servers.

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.

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).

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)

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

1. Log into CentOS as the root user and open the terminal.

2. Do one of the following:

- If you want to upgrade YDMP to the version earlier than 3.4.0.10 (not including 3.4.0.10), run the following command:

```
cd /usr/local
rm -rf yealink_install
tar -xvzf DM_3.3.0.0.tar.gz
cd yealink_install&& tar -xvzf install.tar.gz
./upgrade --host internal IP or the external IP
##If it is the deployment of a single NIC (the internal or the external network), run this
command.##
./upgrade --host the internal IP -e nat_ip=the external IP behind NAT
##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this
command. This command is only applicable to 3.3.0.0 or later versions. ##
./upgrade --host the internal IP -e nat_ip=the external IP behind NAT
##If it is the deployment of dual NIC (the internal and the external network) and NAT, run this
command. This command is only applicable to 3.3.0.0 or later versions. ##
```

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

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

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

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 *ydmpt_diag_time.tar.gz*. And then, you can provide the developers or operation and maintenance engineers with the file.

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

Unzip and run the script.

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

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 core dump 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 again
,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 on YDMP, you need purchase the license from your supplier and activate it.

1. [Importing the Device Certificate](#) .
 2. [Activating the License Online](#) or [Activating the License Offline](#) .
- [Importing the Device Certificate](#)
 - [Activating the License Online](#)
 - [Activating the License Offline](#)

Importing the Device Certificate

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

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

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



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

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

License Device ID : A63A4F480DF2F5C

Unbind License

Refresh

Activate offline license

Activating the License Online

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

- 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.

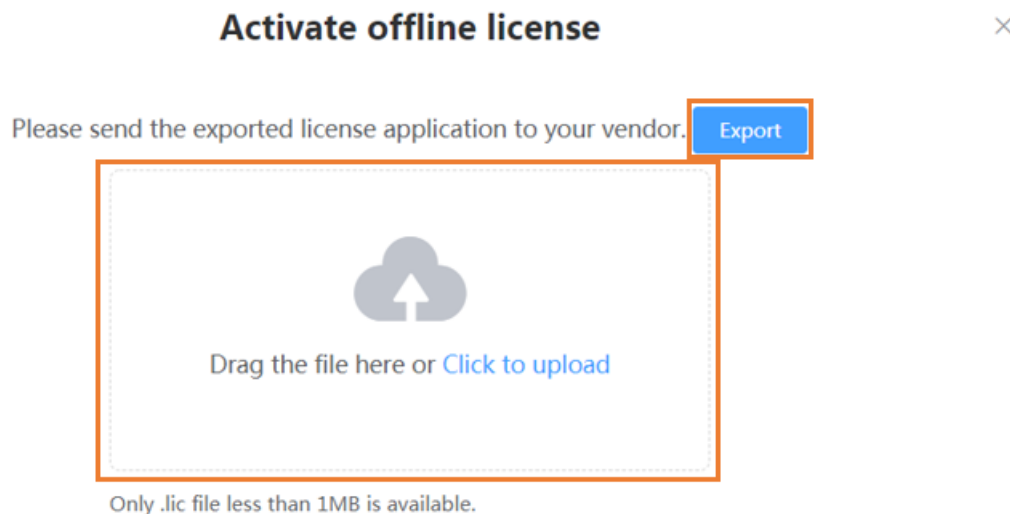
Click **System Management > License > Refresh**.

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.

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



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

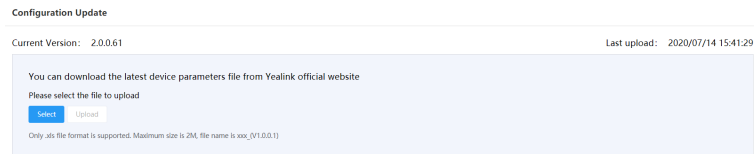
The authorized license is displayed on the page.

Updating the Configuration

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

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

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



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

3. Click **Upload**.

Uninstalling YDMP

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

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

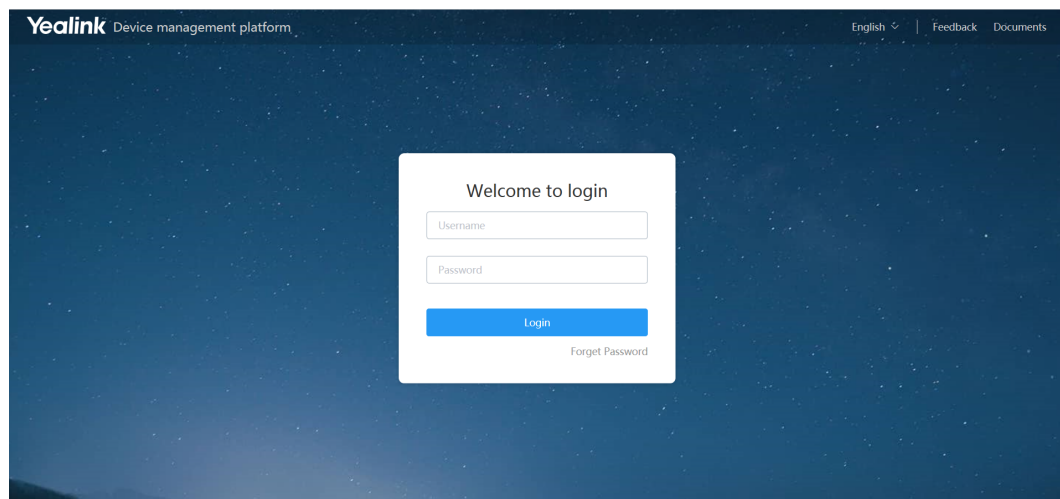
3. According to the prompts, enter the password *Yealink1105*.
YDMP will be uninstalled from the CentOS.

Getting Started

- [Logging in to YDMP](#)
- [Home Page](#)
- [Logging out of YDMP](#)

Logging in to YDMP

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

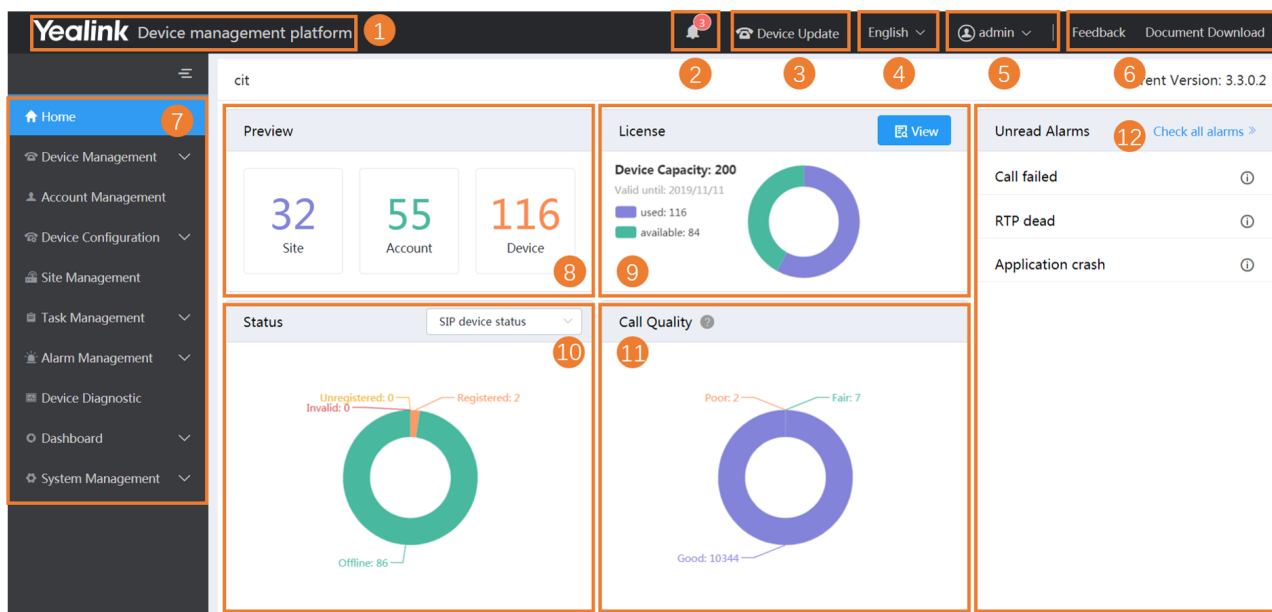


2. Select the desired language from the drop-down menu of **Language** in the top-right corner.
3. Enter your username (default: admin) and the password (default: v123456789).


4. Click **Login**.
5. When the first time you use the default password to log in, the system will remind you to change the password, click **Change** to go to the home page of YDMP .

Home Page

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



Number	Description
1	Go to the home page quickly when you are browsing other pages.
2	Display the number of unread alarms and the type of alarms.
3	Go to the Device List page quickly.
4	Change the display language.
5	Go to the page of setting the administrator account.
6	Go to the page of sending feedback or downloading a document.
7	Navigation pane.
8	Data preview: <ul style="list-style-type: none"> Display the number of sites, accounts and devices. Click the desired module to go to the corresponding module.
9	License: <p>Display the current number of manageable devices.</p>

Number	Description
10	Device status: <ul style="list-style-type: none"> • Select a device type. • Display the number of the unregistered, the registered, the invalid and the offline devices. • Click the corresponding device status to go to the page that lists all the devices of this status.
11	Call quality: <ul style="list-style-type: none"> • Display the number of the good, the bad or the poor call quality. • You can click the desired module to view the call statistics.
12	Unread Alarms: <ul style="list-style-type: none"> • Click Check all alarms to go to the Alarm List page. • Hover the mouse over the icon  to view the alarm details.

Logging out of YDMP

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

Connecting to YDMP

- [Connecting SIP Device](#)
- [Connecting USB Devices](#)
- [Connecting Room System](#)

Connecting SIP Device



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.

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.

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

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

Related concepts

[Supported Device Models](#)

Using Certificates for Mutual TLS Authentication

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

• Configuring Server Certificates

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

Procedure

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

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

• Configuring Trusted Certificates

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

Procedure

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

Only when the authentication succeeds will the device trust YDMP.

Configuring the Common.cfg File

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

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
```

provisioning server address target firmware

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

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

```
dm.site_id = baylplwe
```

The site ID



Note:

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

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

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

- Save the file.

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.

- Log in to YMCS for RPS Enterprise.

The address of the RPS management platform is <https://dm.yealink.com/manager/login>.

- On the **Server Management** page, add the server URL.

- 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`)

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.

- Log into the web user interface of the device.
- 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

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

For more information about the configuration of USB Device Manager client, refer to [Yealink USB Device Manager Client User Guide](#).

Open USB Device Manager client, go to **Config DM Server**, and complete the correspond configuration.

The device will be connected to YDMP automatically.

Connecting Room System

For more information about deploying Room System, refer to [Yealink RoomConnect User Guide](#).

On your MTouch, open Yealink RoomConnect, go to **Remote Management**, and configure the related parameters.

The device will be connected to YDMP automatically.

Managing Devices

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



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

- [Device Status](#)
- [Running State Page](#)
- [Managing SIP Devices](#)
- [Managing USB Devices](#)
- [Managing Room System](#)
- [Managing Firmware](#)
- [Managing Resources](#)

Device Status

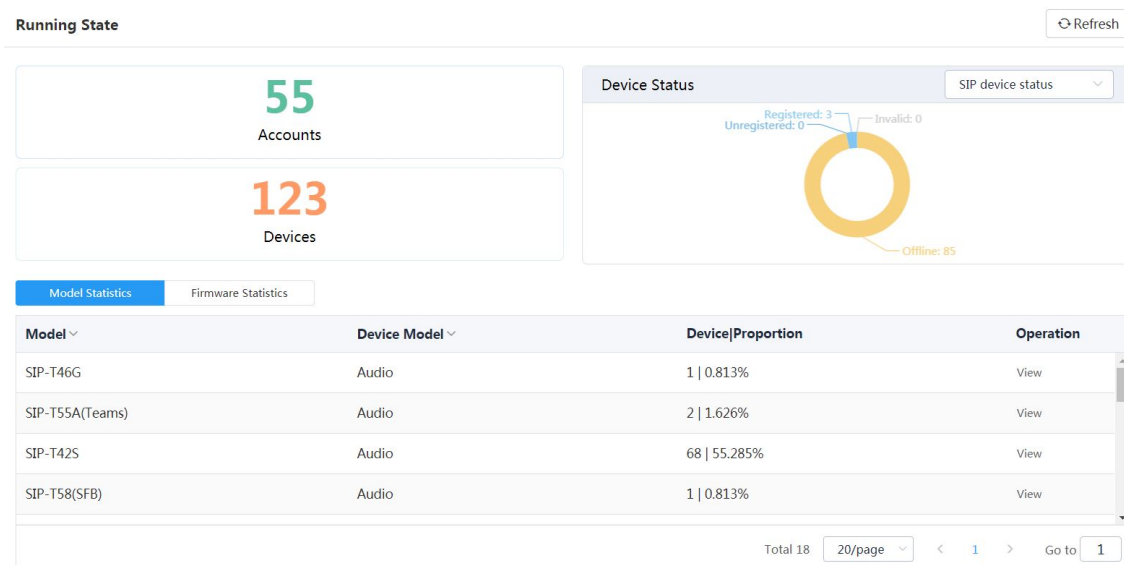
Before managing devices, you can familiarize yourself with the device status.

- Device status of the SIP device

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

Running State Page

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




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

Managing SIP Devices


- [Editing the Device Information](#)
- [Exporting the Device Information](#)
- [Viewing the Information of SIP Device](#)
- [Searching for Devices](#)
- [Assigning Accounts to Devices](#)
- [Setting the Sites](#)
- [Pushing Configuration Files to Devices](#)
- [Pushing Firmware to Devices](#)
- [Pushing Resource Files to Devices](#)
- [Diagnosing Devices](#)
- [Enabling/Disabling DND](#)
- [Sending Messages to Devices](#)
- [Rebooting Devices](#)
- [Resetting the Devices to Factory](#)
- [Deleting Devices](#)

Editing the Device Information

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

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

Edit Device



MAC Address : 000000000033
Device Model : SIP-T58

Please edit :

Device Name
1056

* Site
Yealink

Bind Account
(Maximum 16)
+ Add

Save

Cancel

Related tasks

[Adding Accounts](#)

[Setting the Sites](#)

Exporting the Device Information

You can export the basic information of all devices.

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

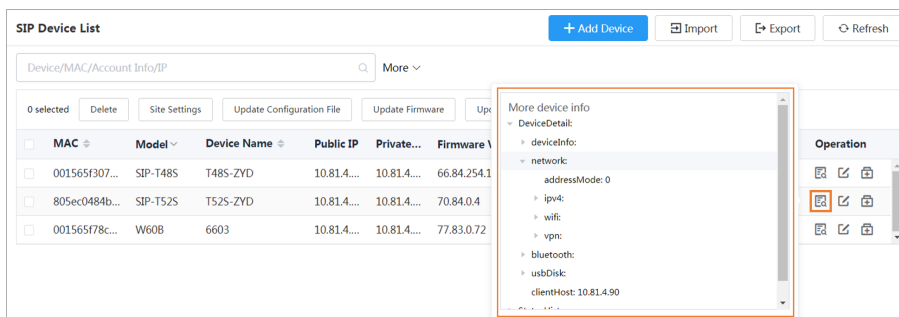
Viewing the Information of SIP Device

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

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

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

2. Click beside the desired device.

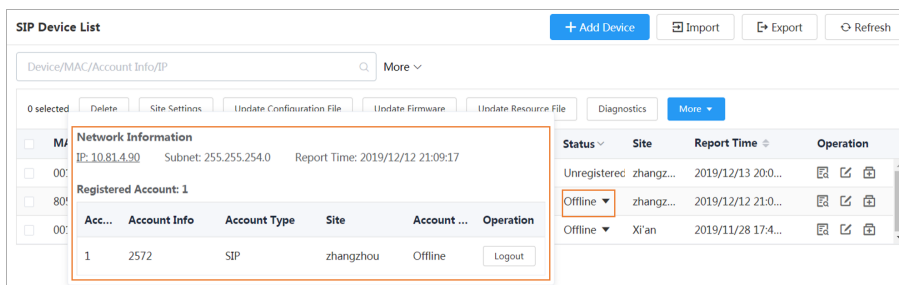


The screenshot shows the 'SIP Device List' interface. A table lists devices with columns: MAC, Model, Device Name, Public IP, Private IP, and Firmware Version. The first device is selected. To its right, a 'More device info' panel is expanded, showing details like deviceInfo, network (addressMode: 0, ipv4, wifi, vpn), bluetooth, and usbDisk (clientHost: 10.81.4.90). On the far right, an 'Operation' panel contains icons for edit, delete, and refresh.



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

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



The screenshot shows the 'SIP Device List' interface. A table lists devices with columns: MAC, Model, Device Name, Public IP, Private IP, Firmware Version, Status, Site, Report Time, and Operation. The first device is selected. To its right, a 'Network Information' panel is expanded, showing IP: 10.81.4.90, Subnet: 255.255.254.0, Report Time: 2019/12/12 21:09:17, and Registered Account: 1. Below this, an 'Account Info' table is shown with columns: Acc..., Account Info, Account Type, Site, Account..., Operation. The first row shows account 1, 2572, SIP, zhangzhou, Offline, and a Logout button.



Note: This feature is not applicable to invalid devices.

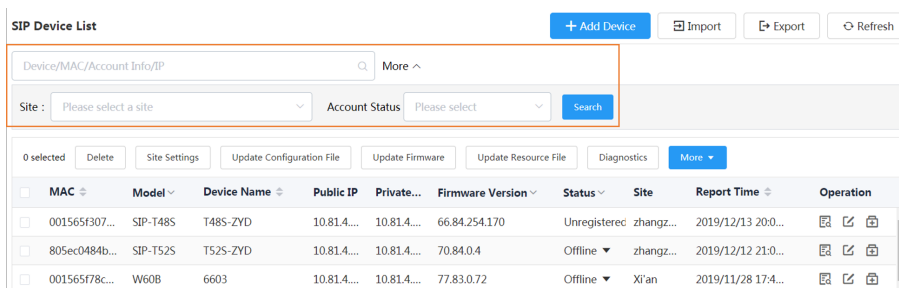
Related concepts

[Device Status](#)

Searching for Devices

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

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



The screenshot shows the 'SIP Device List' interface. At the top, there is a search bar with the placeholder 'Device/MAC/Account Info/IP' and a 'More' dropdown. Below the search bar, there are two filter dropdowns: 'Site : Please select a site' and 'Account Status : Please select'. A 'Search' button is located to the right of these filters. Below the filters, the same table of devices is shown as in the previous screenshots.


The search results are displayed in the list.

Assigning Accounts to Devices

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

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

Edit Device



MAC Address : 001565f460d4
 Device Model : SIP-T48S(SFB)

Please edit :

Device Name

* Site

Bind Account 1

2

SFB

yl553@yealinksfb.com

✖

3

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.

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

SIP Device List

3 selected

MAC	Model	Device Name	Public IP	Private...	Firmware Version	Status	Site	Report Time	Operation
<input checked="" type="checkbox"/> 001565f307...	SIP-T48S	T48S-ZYD...	10.81.4...	10.81.4...	66.84.254.170	Unregistered	zhangzhou	2019/12/13 20:0...	
<input checked="" type="checkbox"/> 805ec0484b...	SIP-T52S	T52S...						2019/12/12 21:0...	
<input checked="" type="checkbox"/> 001565f78c...	W60B	66...						2019/11/28 17:4...	

Site Settings

* Select site

3
4



Note: After setting the site, you can see the task details, refer to [Viewing Tasks](#) .

Related tasks

[Adding Sites](#)

Pushing Configuration Files to Devices

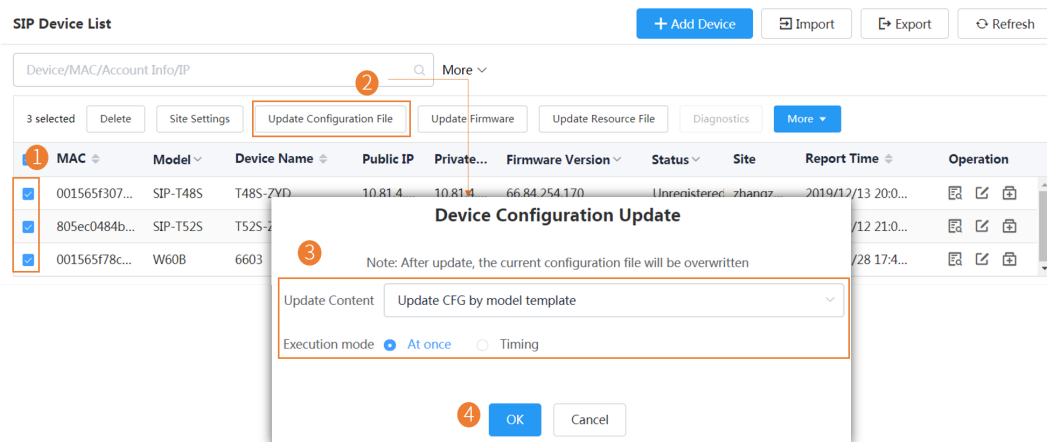
You can push the configuration files to one or multiple devices.

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

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

For more information about the device status, refer to [Device Status](#) .

1. Click **Device Management > SIP Device List**.
2. Push the configuration file to the selected devices.



Note: After updating the configuration file, you can see the task details, refer to [Viewing Tasks](#) .

Related concepts

[Managing the Device Configuration](#)

Pushing Firmware to Devices

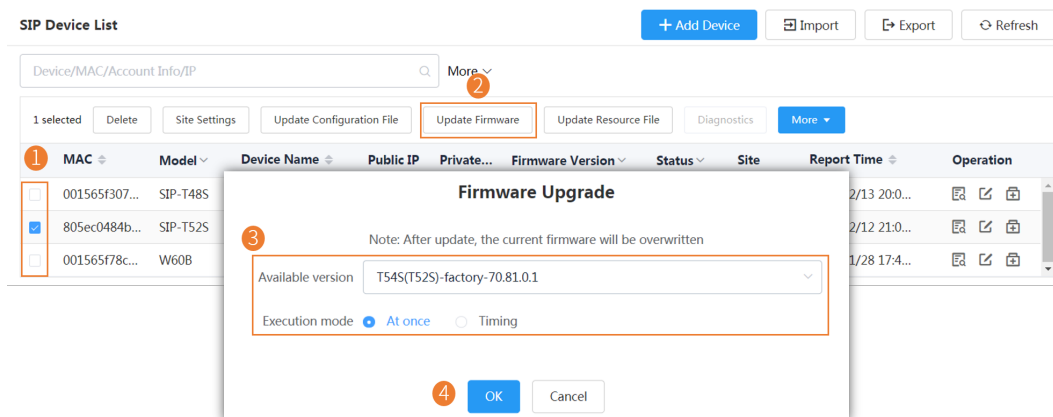
You can push the firmware to one or multiple devices.

If there is no desired firmware, you need to [Adding Firmware](#) .

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

For more information about the device status, refer to [Device Status](#) .

1. Click **Device Management > SIP Device List**.
2. Push the firmware to the selected devices.

**Note:**

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

Related concepts

[Managing Firmware](#)

Pushing Resource Files to Devices

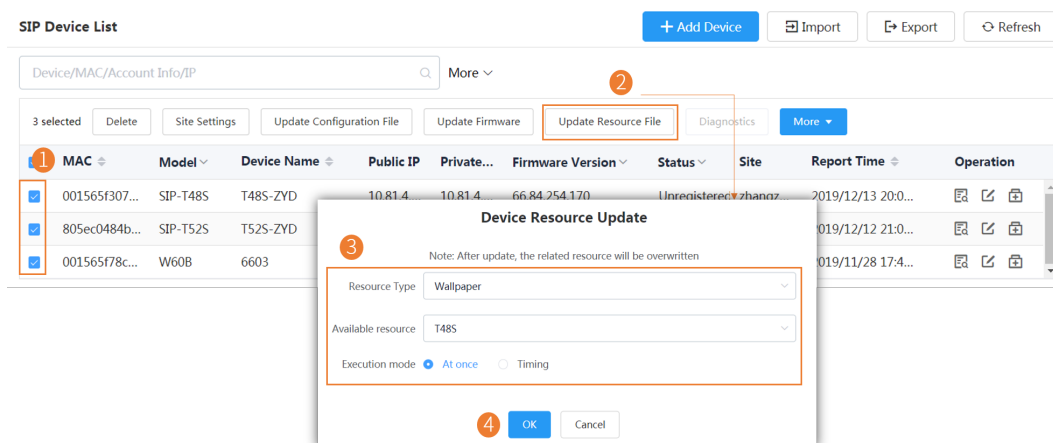
You can push resource files to one or multiple devices.

If there are no desired resource files, you need to [Adding Resource Files](#).

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

For more information about the device status, refer to [Device Status](#).

1. Click **Device Management > SIP Device List**.
2. Push the resource file.

**Note:**

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

Related concepts

[Managing Resources](#)

Diagnosing Devices

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

This feature is not applicable to the offline and invalid devices. For more information about the device status, refer to [Device Status](#).

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

2. Diagnose the device.

- Diagnose a single device

The screenshot shows the 'SIP Device List' interface. At the top, there are buttons for '+ Add Device', 'Import', 'Export', and 'Refresh'. Below these is a search bar labeled 'Device/MAC/Account Info/IP' and a 'More' dropdown. A row of action buttons includes 'Delete', 'Site Settings', 'Update Configuration File', 'Update Firmware', 'Update Resource File', 'Diagnostics', and 'More'. The table below has columns: MAC, Model, Device Name, Public IP, Private IP, Firmware Version, Status, Site, Report Time, and Operation. Two devices are listed: 805ec006d9c (VC200) and 001565c4c6e1 (SIP-T46S). The 'Diagnostics' button for the first device is highlighted with a red box. An arrow points from this box to the 'Device Diagnostic' panel below, which shows login details (VC200, 10.81.6.21) and various diagnostic tools like Packetcapture, Network Detection, etc.

- Diagnose multiple devices.

This screenshot shows the 'SIP Device List' interface with three devices selected in the table. A red box highlights the 'More' button in the top action bar, with an arrow pointing to a 'More' dropdown menu. Another red box highlights the checkboxes for the three selected devices. The 'More' dropdown menu is open, showing a 'Device Diagnostic' option. Below this, a 'Device Diagnostic' panel is shown for the selected devices, displaying their login names, device types, and IP addresses.

3. Select the desired diagnostic tool to diagnose the device.

4. After diagnosing, click **End Diagnostic**.

Related concepts

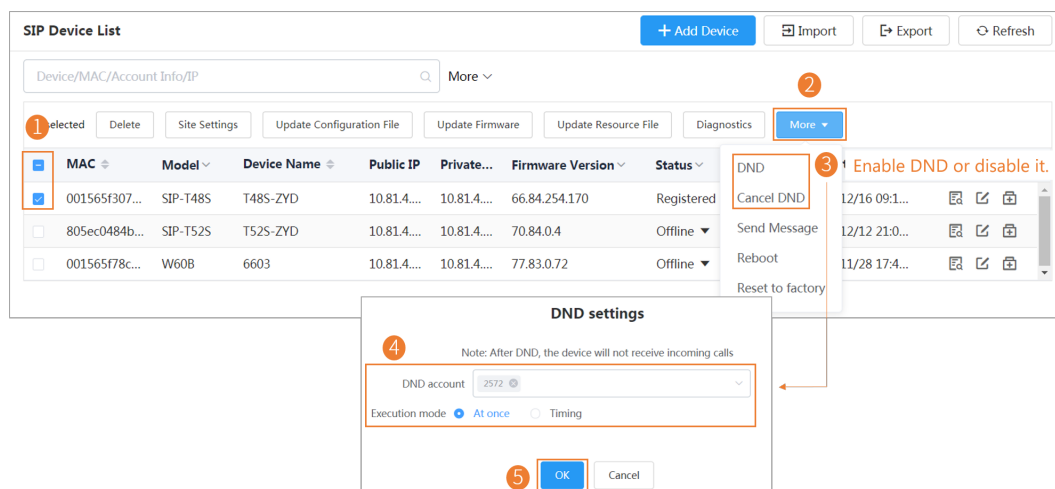
[Diagnosing Devices](#)

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.

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

2. Select the corresponding devices and click **More**→ **DND/Cancel DND**.
3. According to the prompts, select the desired execution mode, and click **OK**.

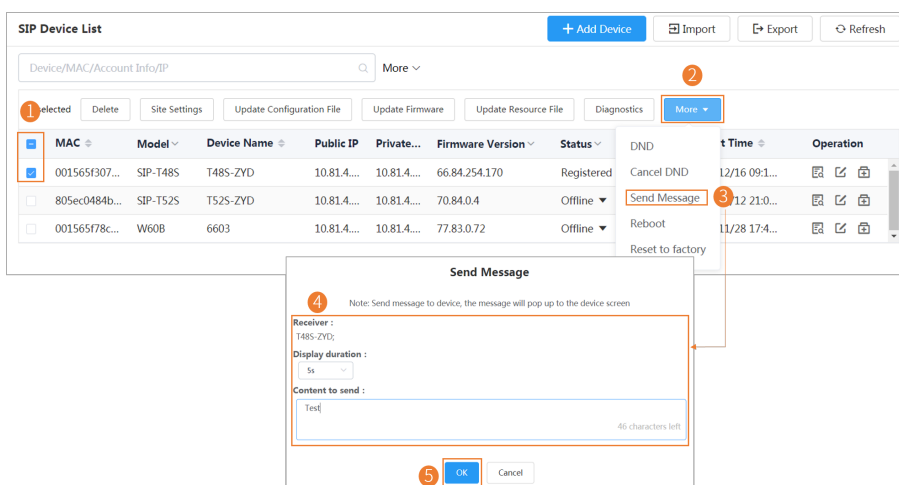


Note: After enabling/disabling DND, you can see the task details, refer to [Viewing Tasks](#).

Sending Messages to Devices

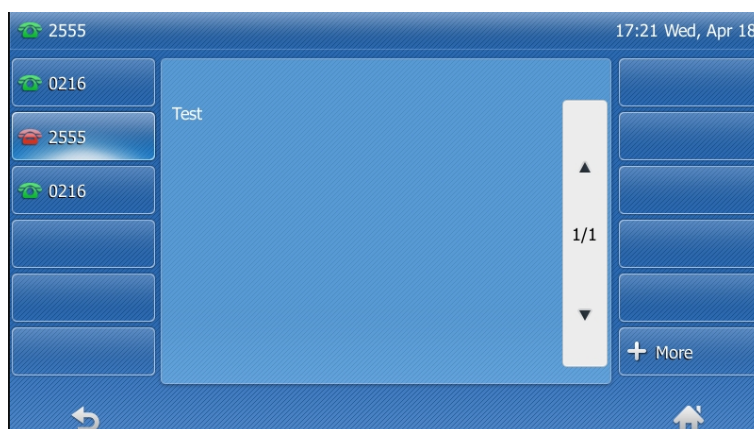
If you need to perform operations, for example, updating the firmware for the device, and you want to notify the device owner in advance, you can send a message to the device through YDMP. YDMP supports sending messages to one or multiple devices.

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



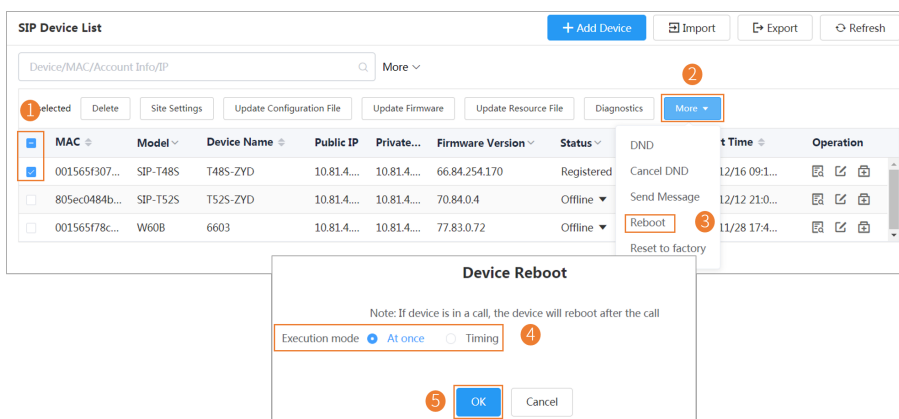
Note: After sending the messages, you can see the task details, refer to [Viewing Tasks](#).


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



Rebooting Devices

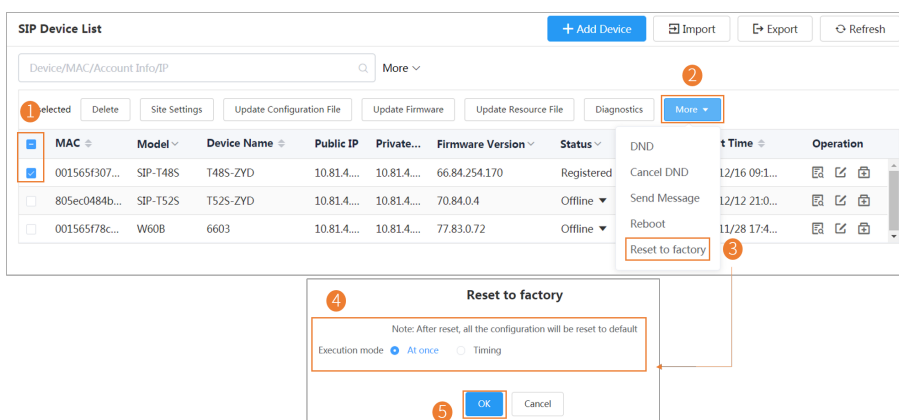
1. Click **Device Management > SIP Device List**.
2. Select the corresponding devices and click **More** → **Reboot**
3. According to the prompts, select the desired execution mode, and click **OK**.




 **Note:** After rebooting the device, you can see the task details, refer to [Viewing Tasks](#) .

Resetting the Devices to Factory

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



 **Note:** After resetting the device, you can see the task details, refer to [Viewing Tasks](#).

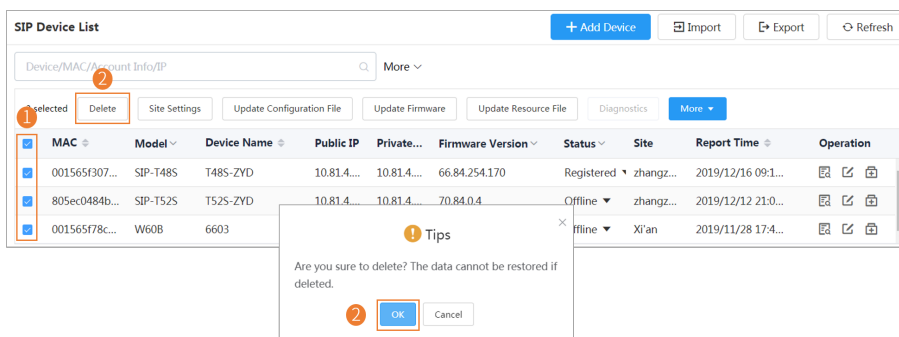
- After you reset the device, the account information, personal settings, or call history on the devices will be deleted.

 **Note:**

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

Deleting Devices

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




Managing USB Devices


- [Editing the Device Information](#)
- [Exporting the Device Information](#)
- [Viewing the USB Device](#)
- [Searching for Devices](#)
- [Setting the Sites](#)
- [Deleting Devices](#)

Editing the Device Information

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

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

Edit Device



Device ID : 8800819099...1271
Device Model : CP900

Please edit :

* Device Name
YL2648-A03971NB

* Site
Yealink

Save

Cancel

Exporting the Device Information

You can export the basic information of all devices.

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

Viewing the USB Device

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

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

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

Searching for Devices

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

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









USB Device List

Export
Refresh

Device name/host IP/ Device ID
More ^

Site : Please select a site
Search

0 selected
Delete
Site Settings

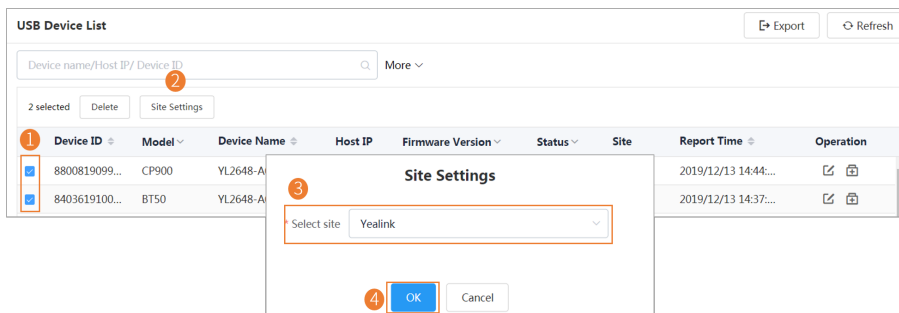
<input type="checkbox"/>	Device ID	Model	Device Name	Host IP	Firmware Version	Status	Site	Report Time	Operation
<input type="checkbox"/>	8800819099...	CP900	YL2648-A03971NB	10.83.4.64	100.420.0.5	Offline	Yealink	2019/12/13 14:44:...	 
<input type="checkbox"/>	8403619100...	BT50	YL2648-A03971NB	10.83.4.64	1.1.0.6	Offline	Yealink	2019/12/13 14:37:...	 
<input type="checkbox"/>	5801219060...	CP700	YL2648-A03971NB	10.83.4.64	115.0.0.10	Offline	Yealink	2019/12/11 19:31:...	 
<input type="checkbox"/>	5800818129...	CP900	YL2648-A03971NB	10.83.4.64	100.420.0.5	Offline	Yealink	2019/12/11 09:57:...	 

The search results are displayed in the list.

Setting the Sites

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

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



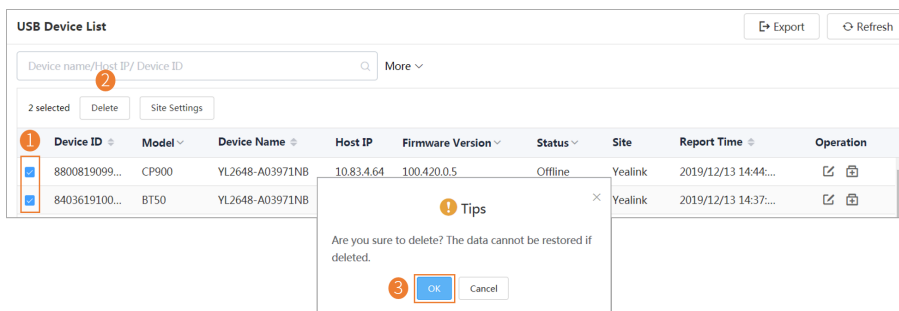
Note: After setting the site, you can see the task details, refer to [Viewing Tasks](#).

Related tasks

[Adding Sites](#)

Deleting Devices

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





Managing Room System

- [Editing the Device Information](#)
- [View the Information of the Room System](#)
- [Searching for Devices](#)
- [Setting the Sites](#)
- [Rebooting Devices](#)
- [Pushing Firmware to Devices](#)
- [Deleting Devices](#)

Editing the Device Information

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

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



MAC Address : 54b203055a8c
Device Model : MVC800

Please edit :

* Meeting Room

zehuittest

* Site

Yealink

Save

Cancel

View the Information of the Room System

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

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

Room System

Refresh

MAC/IP/Meeting Room

More

0 selected

Delete

Site Settings

Reboot

Update Firmware

MAC	Model	Meeting Room	IP	Connector	Version	Status	Associa...	Site	Report Time	Operation
54b203055...	MVC800	zehuittest	10.82.2...	2.0.14.0	Online	11(4 offli...	Yealink	2019/12/16 09:1...		
1c697a004...	ZVC Zoom Room	zehuittest	10.82.2...	2.0.14.0	Online	2(0 offli...	Yealink	2019/12/14 04:0...		

Associated Device Detail

Return

Meeting Room : zehuittest

Device Model : MVC800

IP : 10.82.2.135

MAC : 54b203055a8c

Site : Yealink

Operating System : Windows 10 Enterprise (1903)

Sub-device list

0 selected

Delete

Reboot

Reset to Factory

Update Firmware

Device ID	Model	Connection Mode	Device Type	Firmware Ver...	Hardware Ver...	Status	Report Time
...	UVC30	USB	Video device	105.420.254.10	105.1.0.0.0.0	Offline	2019/12/13 17:48:54
...	CPW90	USB	Audio device	100.420.0.5	100.0.7.0.0.0	Offline	2019/12/16 08:55:40
...	CPW90	Det1	Audio device	Offline	2019/12/16 09:15:36
...	CPW90	Det1	Audio device	Offline	2019/12/16 09:15:36
...	CPW90	USB	Audio device	73.20.254.55	73.0.0.0.0.0	Online	2019/12/16 09:15:36
...	M5404	USB	Other	94.420.0.5	94.0.0.0.0.0	Online	2019/12/16 09:15:36
...	VCM04	Ethernet	Audio device	92.0.0.13	...	Online	2019/12/16 09:15:36
...	VCM04	Ethernet	Audio device	92.0.0.13	...	Online	2019/12/16 09:15:36
...	UVC30	USB	Video device	92.420.0.15	92.0.0.0.0.1	Online	2019/12/16 09:15:36
...	M5404	USB	Other	1.0.1.2	...	Online	2019/12/16 09:15:36
...	CPW90	Det1	Audio device	55.80.0.20	55.0.0.0	Online	2019/12/16 09:15:34

Searching for Devices

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

Click **Device Management > Room System**.

The search results are displayed in the list.

Setting the Sites

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

Click **Device Management > Room System**.



Note: After setting the site, you can see the task details, refer to [Viewing Tasks](#) .

Related tasks

[Adding Sites](#)

Rebooting Devices

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



Note: After rebooting the device, you can see the task details, refer to [Viewing Tasks](#) .

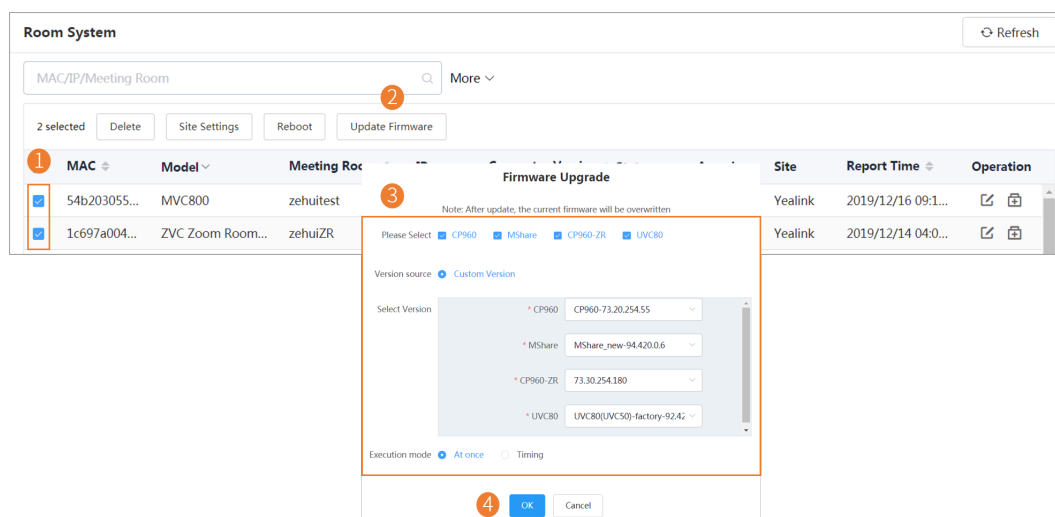
Pushing Firmware to Devices

If there is no desired firmware, you need to [Adding Firmware](#).

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

For more information about the device status, refer to [Device Status](#).

1. Click **Device Management > Room System**.
2. Push the firmware to the selected devices.



Note:

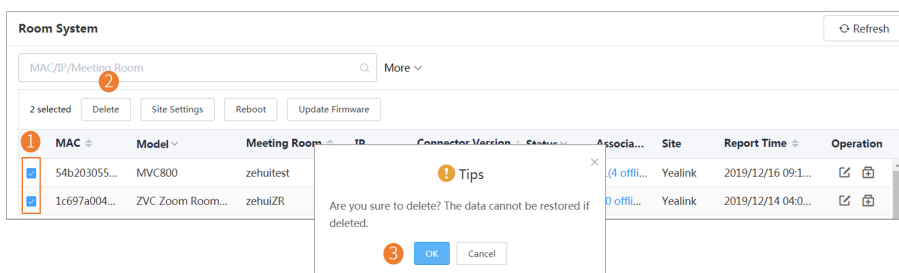
- Note that the firmware must be applicable to all selected devices.
- After updating the firmware, you can see the task details, refer to [Viewing Tasks](#).

Related concepts

[Managing Firmware](#)

Deleting Devices

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



Managing Firmware

You can manage all the device firmware on YDMP.

- [Adding Firmware](#)
- [Pushing Firmware to Devices](#)
- [Editing the Firmware](#)
- [Downloading the Firmware](#)
- [Deleting Firmware](#)

Adding Firmware

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

Add Firmware

* Firmware Name

* Select File:

Only .rom file is supported. Maximum size is 1G

T54S(T52S)-factory-70.81.0.10.rom

* Version

Type ☒ SIP Device List ☐ Room System

Apply to ☒ Main Device ☐ Accessory

* Supported Model

Description

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.

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

Push to upgrade firmware ×

Please select a site SIP-T52S

MAC/Device Name/Account Info Q

MAC	Device Name	Account Info
<input checked="" type="checkbox"/>	805ec0484b2f	baiyf-T52S 5066
<input type="checkbox"/>	001565c50cca	40030 40030
<input type="checkbox"/>	001565c128f6	8635 8635

Selected: 1

MAC	Device Name	Account Info
805ec0484b2f	baiyf-T52S	5066

Push to Update
Cancel

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

Please select the execution mode ×

Note: After update, device Current Firmware will be overwritten

Execution mode ☒ At once ☐ Timing

OK
Cancel



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



Note:

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

Editing the Firmware

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

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

Downloading the Firmware

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

Deleting Firmware

1. Click **Device Management > Firmware Management**.
2. Select the desired firmware.
3. Click **Delete**.

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

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

Managing Resources

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

- [Adding Resource Files](#)
- [Pushing Resource Files to Devices](#)
- [Editing Resource Files](#)
- [Downloading the Resource Files](#)
- [Deleting Resource Files](#)

Adding Resource Files

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

Add Resource

* Resource Type: Wallpaper

* Resource Name: WP-T52S

* Select File: [Click to upload](#)


Only .png/.jpg/.bmp file is supported file, maximum size for each file is 5M

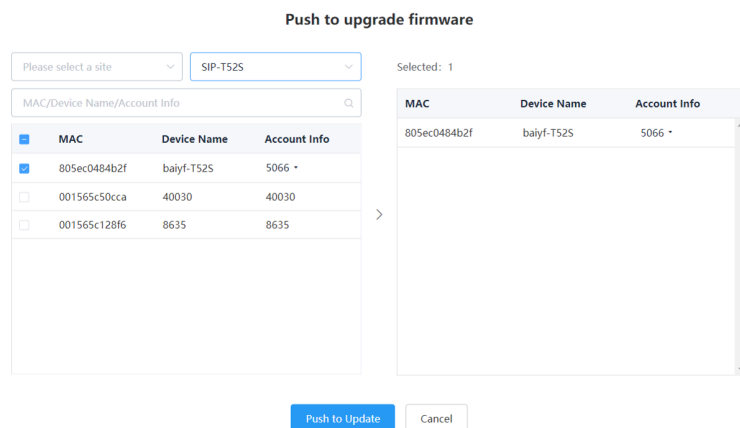
v2-4ae759dfcfc69d7d71fe9ff020726693_r.jpg

Description: Please enter description, maximum 128 characters

2 [Save](#) [Cancel](#)

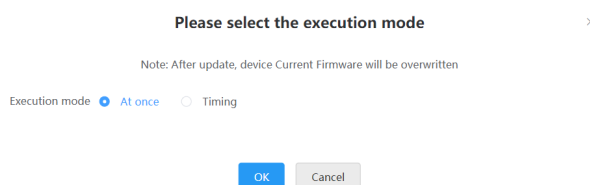
Pushing Resource Files to Devices

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



4. Click **Push to Update**.

5. Select the desired execution mode.



6. Click **OK**.



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



Note:

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

Editing Resource Files

- Click **Device Management > Resource Management**.
- Click beside the desired resource.
- Edit the related information of the resource file in the corresponding field.
- Click **Confirm**.

Downloading the Resource Files

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

Deleting Resource Files

- Click **Device Management > Resource Management**.
- Select the desired resource.
- Click **Delete**.

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

After the resource is deleted, the timer task associated with this resource file 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

1. Click **Account Management**.
2. In the top-right corner of the page, click **Add Account > Add SFB account/Add SIP account/Add YMS account/Add CLOUD account/Add H.323 account**.
3. Configure the account information.
4. Click **Confirm**.

Related tasks

[Assigning Accounts to Devices](#)

Importing Accounts

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

1. Click **Account Management**.
2. In the top-right corner, click **Import > Import SFB account/Import SIP account/Import YMS account/Import CLOUD account/Import H.323 account**.

Import

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


1 [Download the template](#) Download the template and edit the parameter in it.

2 Drag the file here or [Click to upload](#)

Note: The file format must be .xls or .xlsx(that is an Excel file), the maximum number of imported data can not exceed 5000

3 [Upload](#) [Cancel](#)

Editing the Account Information

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.

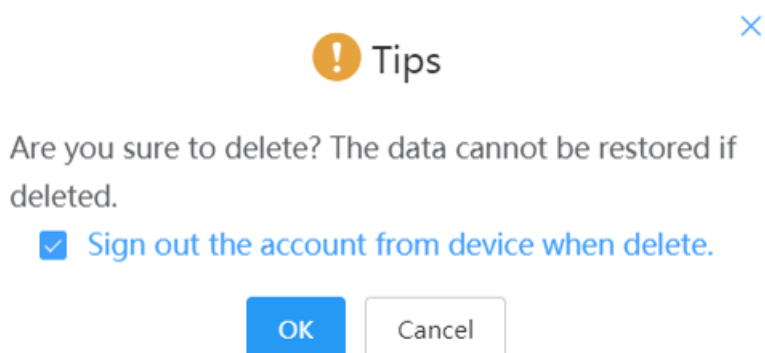
1. Click **Account Management**.
2. In the top-right corner, click **Export**.

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

Deleting Accounts

1. Click **Account Management**.
2. Select the desired accounts.
3. Click **Delete** and confirm the action.

If you select **Sign out the account from device when delete**, the account will be deleted from YDMP and signed out from the device. If you select **Sign out the account from device when delete**, the account will only be deleted from YDMP but not signed out from the device.



Managing the Device Configuration

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

Introduction of obtaining the configuration:

- **Automatically obtaining the configuration:**

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

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

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

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

- **Manually obtaining the configuration:**

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

- [Managing Model Configuration](#)
- [Managing the Site Configuration](#)
- [Managing the Group Configuration](#)
- [Managing the MAC Configuration](#)
- [Configuring Global Parameters](#)

Managing Model Configuration

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

- [Adding Configuration Templates](#)
- [Setting Parameters](#)
- [Pushing Configuration to Devices](#)
- [Editing Configuration Templates](#)
- [Downloading the Model File](#)
- [Viewing Parameters](#)
- [Deleting Templates](#)

Adding Configuration Templates

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

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

Template Name	Model	Description	Operation
<input type="text" value="T54S"/>	<input type="text" value="SIP-T54S"/>	<input type="text" value="T54S"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Setting Parameters

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

- Edit parameters in the text: you can edit any parameter supported by the device in the text.
- Edit parameters on the graphical editing page: you can edit the corresponding template parameters on the graphical editing page.
- [Setting Parameters in the Text](#)

- [Setting Parameters on the Graphical Editing Page](#)

Setting Parameters in the Text

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

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

Set Template Parameters | T48S 1 [Edit the parameter on the Graphical editing page.](#)

You can edit template parameters in text, the format is: key=value, every parameter must be in different line. Here are the examples:

```
static.lang.gui=Chinese_S
features.hotline_delay=8
linekey.1.line=1
phone_setting.phone_lock.lock_time_out=20
dm.enterprise_id=leynhkqe
linekey.1.type=15
phone_setting.phone_lock.unlock_pin=1234
features.dnd.emergency_enable=1
lang.wui=Chinese_T
dm.site_id=bay1p1we
phone_setting.backgrounds=04.jpg
phone_setting.phone_lock.enable=1
features.dnd_mode=0
features.key_tone=1
```

2 Save Cancel

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



Set successfully!



Update the device configuration now?

Yes

No

5. Push the selected configuration.

Push to update the parameters

Please select a site

MAC/Device Name/Account Info

MAC	Device Name	Account Info
001565f30702	T48S-ZYD	2572

Selected : 1

1 Push to Update Cancel

6. Select the desired execution mode.

Please select the execution mode



Note: After update, device Current Firmware will be overwritten

Execution mode ☒ At once ☐ Timing

OK


Cancel

**Note:**

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

Setting Parameters on the Graphical Editing Page

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

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

3. Set and save the parameters.

**Tip:**

- You can select the edited configuration, and push it to the desired devices.
 - You can click **Reset** to reset the configuration on this page to the value before modification.
4. On the pop-up window, select **Yes** to push the edited configuration immediately, or **No** to save the edited configuration.

✓ Set successfully!



Update the device configuration now?

Yes

No

5. Push the selected configuration.

Push to update the parameters

Please select a site

MAC/Device Name/Account Info

MAC	Device Name	Account Info
001565f30702	T48S-ZYD	2572

Selected : 1

MAC Device Name Account Info

001565f30702 T48S-ZYD 2572

Push to Update Cancel

6. Select the desired execution mode.

Please select the execution mode



Note: After update, device Current Firmware will be overwritten

Execution mode ☒ At once ☐ Timing

OK

Cancel




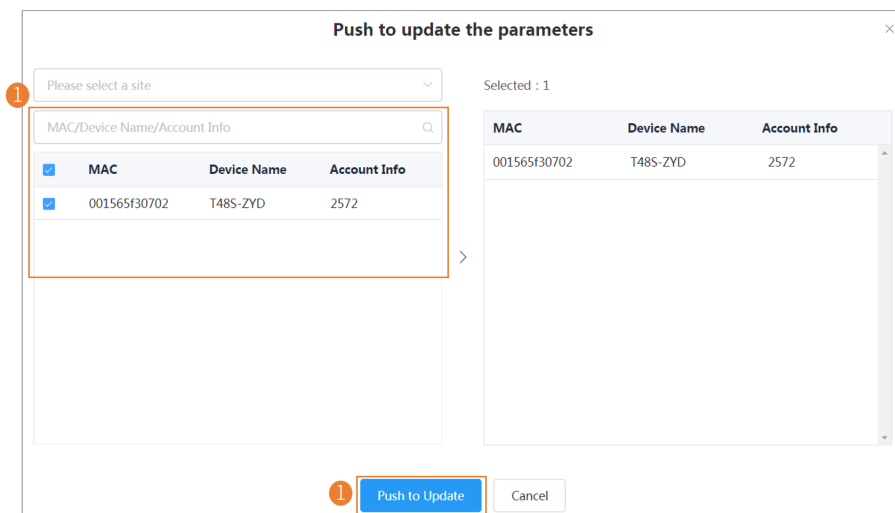
Note:

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

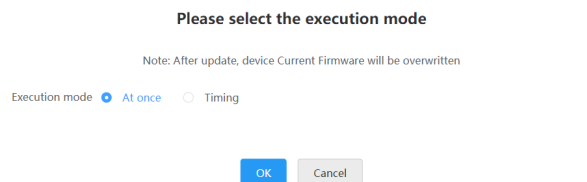
Pushing Configuration to Devices

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

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



4. Select the desired execution mode.



Note:

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

Editing Configuration Templates

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

- Click **Device Configuration > Model Configuration**.
- Click ******* on the right side of the desired template, and select **Edit Template** from the drop-down menu.
- Edit and save the parameters.



Downloading the Model File


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

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

Viewing Parameters

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

- Click **Device Configuration > Model Configuration**.

- Click  beside the desired template to view the parameters.

×

View Parameters

test(SIP-T41S)		
Parameter	Catalog	Value
Server1 Transport Type	Account > Register > Account1	TCP

I know
Edit

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

Deleting Templates

- Click **Device Configuration > Model Configuration**.
- Select the desired templates.
- Click **Delete**.
- Click **OK** according to the prompts.

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

Managing the Site Configuration

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

- [Adding Site Configuration Templates](#)
- [Setting Parameters](#)
- [Pushing the Site Configuration to Devices](#)
- [Editing the Site Configuration Template](#)
- [Downloading the Site Configuration Template](#)
- [Deleting Site Configuration Templates](#)

Adding Site Configuration Templates

- Click **Device Configuration > Site Configuration > Add Template**.
- Set and save the parameters.

+ Add Template

Site Configuration

Site Name/Description Q Search

0 selected Delete

<input type="checkbox"/>	Site Name	Description	Modification Time	Operation
<input type="checkbox"/>	DongNan	Please enter description, maximum 255	--	2 Save Cancel

Setting Parameters

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

- Edit parameters in the text: you can edit any parameter supported by the device in the text.

- Edit parameters on the graphical editing page: you can edit the corresponding template parameters on the graphical editing page.
- [Setting Parameters in the Text](#)
- [Setting Parameters on the Graphical Editing Page](#)

Setting Parameters in the Text

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

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

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

Set successfully!

Update the device configuration now?

Yes

No

5. Select the desired execution mode.

Please select the execution mode

Note: After update, device Current Firmware will be overwritten

Execution mode ☒ At once ☐ Timing

OK

Cancel




Note:

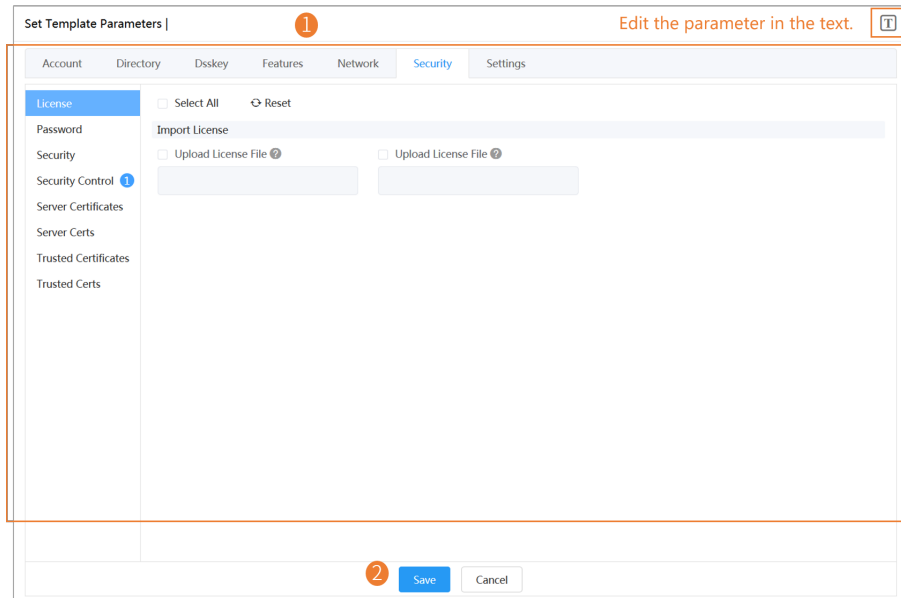
- If you select **At once**, the configuration will be pushed to all the devices in this site immediately.

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

Setting Parameters on the Graphical Editing Page

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

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




Tip:

- You can select the edited configuration, and push it to the desired devices.
 - You can click **Reset** to reset the configuration on this page to the value before modification.
4. On the pop-up window, select **Yes** to push the edited configuration immediately, or **No** to save the edited configuration.



Set successfully!



Update the device configuration now?

Yes

No

5. Select the desired execution mode.

×

Please select the execution mode

Note: After update, device Current Firmware will be overwritten

Execution mode ☒ At once ☐ Timing




Note:

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

Pushing the Site Configuration to Devices

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

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

1. Click **Device Configuration > Site Configuration**.
2. Click  beside the desired template.
3. Select a desired execution mode on the pop-up window.

×

Please select the execution mode

1 Tips : Push configuration to the devices under site and all of its subsites.

Execution mode ☐ At once ☒ Timing

Task Name

* Repeat

* Execution Time

2




Note: After updating the configuration file, you can see the task details, refer to [Viewing Tasks](#) .

Editing the Site Configuration Template

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

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

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

Site Configuration + Add Template


Site Name/Description Search

0 selected Delete

<input type="checkbox"/> Site Name	Description	Modification Time	Operation
<input type="checkbox"/> WULLALA/zhangzhou	<input type="text" value="Please enter description, maximum 25"/>	2019/12/16 17:09:07	Save Cancel

Downloading the Site Configuration Template

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

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

Deleting Site Configuration Templates

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

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

Managing the Group Configuration

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

- [Adding the Group Configuration](#)
- [Setting Parameters](#)
- [Editing Groups](#)
- [Pushing the Group Configuration](#)
- [Viewing Parameters](#)
- [Downloading Configuration File](#)
- [Deleting Groups](#)

Adding the Group Configuration

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

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

3. Select the desired device to the group.

MAC	Device Name	Account Info
<input checked="" type="checkbox"/> 805ec0484b2f	balyf-TS25	5066 *
<input checked="" type="checkbox"/> 001565c50cca	40030	40030
<input checked="" type="checkbox"/> 001565c128b6	8635	8635

4. Set the parameters.

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

Setting Parameters

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

- Edit parameters in the text: you can edit any parameter supported by the device in the text.
- Edit parameters on the graphical editing page: you can edit the corresponding template parameters on the graphical editing page.
- [Setting Parameters in the Text](#)
- [Setting Parameters on the Graphical Editing Page](#)

Setting Parameters in the Text

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

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

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

Set successfully!

Update the device configuration now?

Yes

No

5. Select the desired execution mode.

Please select the execution mode

Note: After update, device Current Firmware will be overwritten

Execution mode ☒ At once ☐ Timing

OK

Cancel




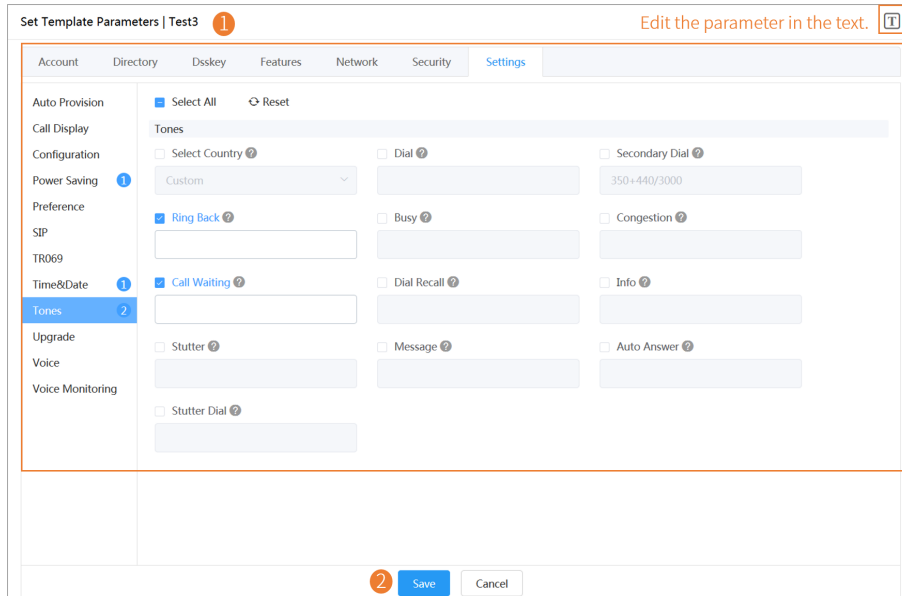
Note:

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

Setting Parameters on the Graphical Editing Page

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

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




Tip:

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

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



Set successfully!



Update the device configuration now?

Yes

No

5. Select the desired execution mode.

Please select the execution mode



Note: After update, device Current Firmware will be overwritten

Execution mode ☒ At once ☐ Timing

OK

Cancel



Note:

- If you select **At once**, the configuration will be pushed to all the devices in this group immediately.

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

Editing Groups

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

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

4. Select the desired device to the group.

MAC	Device Name	Account Info
<input checked="" type="checkbox"/> 805ec0484b2f	balyf-TS25	5066
<input checked="" type="checkbox"/> 001565c50cca	40030	40030
<input checked="" type="checkbox"/> 001565c128f6	8635	8635


MAC	Device Name
805ec0484b2f	balyf-TS25
001565c50cca	40030
001565c128f6	8635

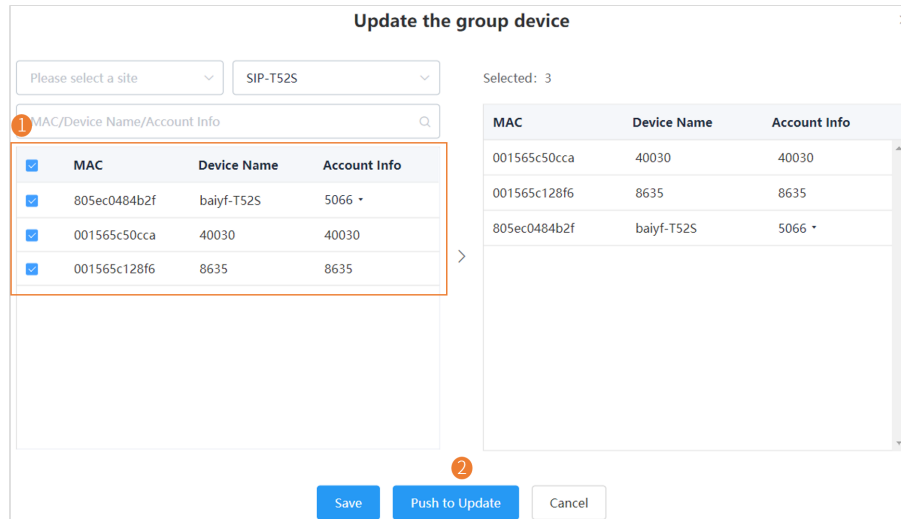
5. Edit the device parameters.

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

Pushing the Group Configuration

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

- Click **Device Configuration > Group Configuration**.
- Click  beside the desired group.
- Select the desired device.



Update the group device

Please select a site SIP-T52S

MAC/Device Name/Account Info

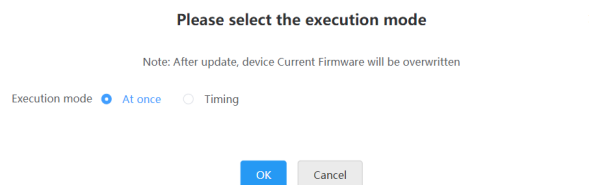
MAC	Device Name	Account Info
805ec0484b2f	baiyf-T52S	5066
001565c50cca	40030	40030
001565c128f6	8635	8635

Selected: 3

MAC	Device Name	Account Info
001565c50cca	40030	40030
001565c128f6	8635	8635
805ec0484b2f	baiyf-T52S	5066

Save Push to Update Cancel

- Select the desired execution mode.




Please select the execution mode

Note: After update, device Current Firmware will be overwritten


Execution mode ☒ At once ☐ Timing

OK Cancel

 **Note:** After updating the configuration file, you can see the task details, refer to [Viewing Tasks](#).

Viewing Parameters

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

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

View Parameters ×		
1231		
Parameter	Catalog	Value
Server1 Retry Counts	Account > Register > Account1	4
<div> I know Edit </div>		

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

Downloading Configuration File

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

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

Deleting Groups

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

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

Managing the MAC Configuration

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

- [Uploading Backup Files](#)
- [Generating Configuration Files](#)
- [Setting Parameters](#)
- [Pushing Backup Files to Devices](#)
- [Downloading the Configuration Files](#)
- [Exporting the Configuration Files](#)
- [Deleting Backup Files](#)

Uploading Backup Files

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

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

Upload backup file

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

1

Select the file

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

📄 001565c50cca_all.cfg

2

Confirm

Cancel

Generating Configuration Files

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

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

Generate config file

Please select a site: ▼ All ▼

MyDevice

MAC	Device Name	Account Info
805ec04bdbaf	MyDevice	1233

Selected Device: 1

MAC	Device Name	Account Info
805ec04bdbaf	MyDevice	1233

2

Confirm Cancel

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

The generated files are in the list as below:

MAC	Model	Firmware	File Name	File Size	Update Time	Operation
805ec04f3c89	--	--	805ec04f3c89.cfg	0.21kb	2020/03/24 11:22:19	🔍 ⬇ ⬆ ⬇
805ec04bdbaf	SIP-T545	70.84.0.70	805ec04bdbaf.cfg	1.62kb	2020/03/17 10:56:45	🔍 ⬇ ⬆ ⬇

Setting Parameters


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


- Edit parameters in the text: you can edit any parameter supported by the device in the text.
- Edit parameters on the graphical editing page: you can edit the corresponding template parameters on the graphical editing page.
- [Setting Parameters in the Text](#)
- [Setting Parameters on the Graphical Editing Page](#)

Setting Parameters in the Text

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


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

2. Click  beside the desired template.
3. Set and save the parameters.

Set Template Parameters | 001565f30702
Edit the parameter on the Graphical editing page. 


You can edit template parameters in text, the format is: key=value, every parameter must be in different line. Here are the examples:


```
static.lang.gui=Chinese_S
features.hotline_delay=8
local_time.time_zone=+8
{"sessionId":"U48aqZscjw7fuyafLuimXp2ITGExuPDv/vQRHbbp1A8dkZmwTnTw9yg0W3M1qTeaTS41GWYyMST11ZsnAlgQeoYkxMAC8viXl2GDacY=","ret":-1,"error":{"errorCode":20302,"msg":"Generate config file failed.,"fieldErrors":""}}
```
















 Save
Cancel


Setting Parameters on the Graphical Editing Page

You can edit the parameter supported in the template.

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

Set Template Parameters | 001565f30702
Edit the parameter in the text. 

Account	Directory	Deskey	Features	Network	Security	Settings
Auto Provision	Time&Date	<input checked="" type="checkbox"/> DHCP Time  <input type="checkbox"/> Manual Time  <input checked="" type="checkbox"/> Time Zone  <input type="checkbox"/> Daylight Saving Time  <input type="checkbox"/> Location  <input type="checkbox"/> Fixed Type  <input type="checkbox"/> DST Start Time  <input type="checkbox"/> DST End Time  <input type="checkbox"/> Offset(minutes)  <input type="checkbox"/> NTP By DHCP Priority  <input type="checkbox"/> Primary Server  <input type="checkbox"/> Secondary Server  <input type="checkbox"/> Update Interval (15-86400s)  <input type="checkbox"/> Time Format  <input type="checkbox"/> Date Format 	Disabled Disabled +8 Australia(Perth), China(Beijing), Disabled China(Beijing) DST by Date 1000 Hour 24 WWW MMM DD			


 Save
Cancel



Tip:

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

Pushing Backup Files to Devices

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



Note: After updating the configuration file, you can see the task details, refer to [Viewing Tasks](#) .

Downloading the Configuration Files

You can download the backup files to your local system.

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

2.



Click beside the desired MAC address to download the backup to your local system.

Exporting the Configuration Files

You can export all device configuration files by one click.

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

2. In the top-right corner, click **Export**.

Deleting Backup Files

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

2. Select the desired backup file.

3. Click **Delete**.

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

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

Configuring Global Parameters

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

1. Click **Device Configuration > Global Parameters**.

2. Set and save the parameters.



Note:

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

Managing Sites

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



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

- [Adding Sites](#)
- [Importing Sites](#)
- [Editing Sites](#)
- [Deleting Sites](#)

Adding Sites

1. Click **Site ManagementAdd Site**.

2. Set and save the parameters.

Add Site

1

* Site Name

WUJI

* Parent Site

WULLLALA

Description

Maximum 1024 characters.

Site IP

+ Add

Public IP	Private IP	Operation
10.152.123.56/9	10.12.12.49/12	

2

Save

Cancel



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

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



Note:

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

Importing Sites


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

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

Import

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

1 [Download the template](#) Download the template and edit the parameter in it.

2  Drag the file here or [Click to upload](#)

Note: The file format must be .xls or .xlsx(that is an Excel file), the maximum number of imported data can not exceed 5000

3 [Upload](#) [Cancel](#)

Editing Sites

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

Site Management [Import](#) [+ Add Site](#)

Site Name/Description


Site Name

- WULLLALA
 - X'an
 - zhangzhou
 - DongNan
 - WUII
 - 1

* Site Name: zhangzhou

* Parent Site: WULLLALA

Description

Site IP 

Public IP	Private IP
0.0.0.0	--

[Edit](#) [Delete](#)


3. Set and save the parameters.

Edit Site

* Site Name: zhangzhou

* Parent Site: WULLLALA

Description: Maximum 1024 characters.


Site IP  [+ Add](#)

Public IP	Private IP	Operation
0.0.0.0/30	--	Edit Delete

[Save](#) [Cancel](#)

Deleting Sites

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

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

Site Management

Site Name/Description

Site Name

- Yealink
 - SITE1
 - SITE2
 - SITE3
 - SITE5
 - 1212
 - SITE-TEST
 - SITE6
 - SITE7
 - 12312312
 - baiyf-site1
 - baiyf-site2
 - huangxiaoyi
 - API添加站点
 - Site for Test3

* Site Name
Site for Test3

* Parent Site
Yealink

Description
Site for Test3

Site IP

Public IP	Private IP
10.81.6.9/10	10.81.0.2/5

Edit Delete

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

Managing Tasks

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

Execution mode	<ul style="list-style-type: none"> At once: the task is executed immediately. Timing: the task is executed at the time you set.
Tasks and Rules	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Update CFG by model template: the system will push the configuration of the corresponding model template to the selected device. If the corresponding model template 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](#)
- [Editing Timer Tasks](#)
- [Pausing or Resuming Timer Tasks](#)
- [Ending Timer Tasks](#)
- [Searching for Timer Tasks](#)
- [Viewing Timer Tasks](#)
- [Viewing Tasks](#)
- [Searching for Executed Tasks](#)

Adding Timer Tasks

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

The screenshot shows the 'Add Timer Task' form. It has a title bar 'Add Timer Task'. Below it, there's a section for device selection with radio buttons: 'Devices' (selected), 'All', 'Site', 'Group', and 'Custom devices'. This is marked with a red circle '1'. Below that, there's a section for task configuration with fields: '* Task Name' (text input with 'Enable DND'), '* Task' (dropdown menu with 'DND'), '* Repeat' (dropdown menu with 'One-time Task'), '* Execution Time' (datetime picker with '2020-08-04 14:22:51'), and 'Time Zone' (dropdown menu with '(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi'). This entire section is marked with a red circle '2'. At the bottom, there are 'Save' and 'Cancel' buttons, marked with a red circle '3'.



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 Timer Tasks](#)

[Pausing or Resuming Timer Tasks](#)


[Ending Timer Tasks](#)

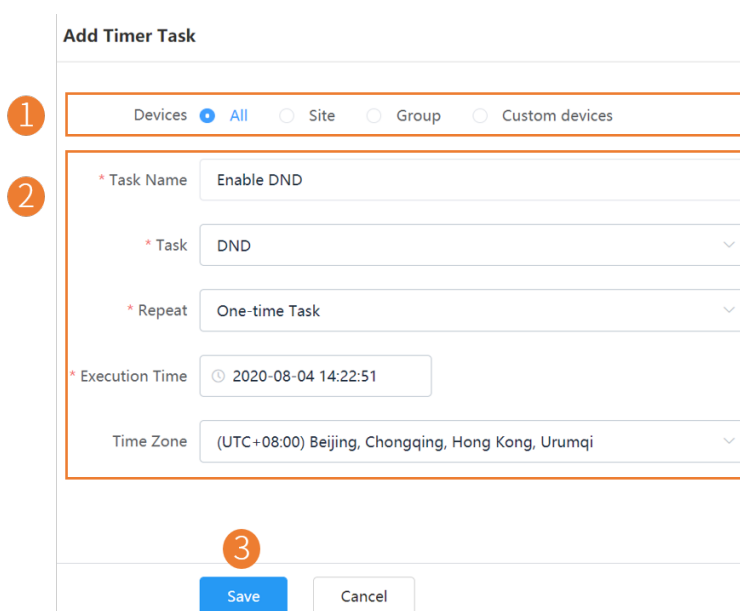
[Viewing Timer Tasks](#)

[Viewing Tasks](#)

Editing Timer Tasks

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

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





The screenshot shows the 'Add Timer Task' dialog box. It has a title bar 'Add Timer Task'. Below the title bar, there are four radio buttons: 'Devices' (selected), 'All', 'Site', 'Group', and 'Custom devices'. Below this, there are five fields: '* Task Name' (text input with 'Enable DND'), '* Task' (dropdown menu with 'DND'), '* Repeat' (dropdown menu with 'One-time Task'), '* Execution Time' (datetime picker with '2020-08-04 14:22:51'), and 'Time Zone' (dropdown menu with '(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi'). At the bottom, there are two buttons: 'Save' and 'Cancel'. Three orange circles with numbers 1, 2, and 3 are overlaid on the image. Circle 1 points to the 'Devices' radio button. Circle 2 points to the '* Task Name' field. Circle 3 points to the 'Save' button.



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

Pausing or Resuming Timer Tasks


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

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

Ending Timer Tasks

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

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

2. Click  on the right side of the desired task to end the task.



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

Related tasks

[Viewing Timer Tasks](#)

[Viewing Tasks](#)

Searching for Timer Tasks

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

Click **Task Management > Scheduled Task**.

Scheduled Task + Add Timer Task					
<div> <input type="text" value="Task Name"/> <input type="button" value="More ^"/> </div> <div> Last Execution Result : All <input type="button" value="Search"/> </div>					
Task Name	Task	Repeat	Execution Time	Task Status	Operation
测试	Send Message	Daily	14:08:06(UTC+08:00)	Pending	
重启-1529	Reboot	One-time Task	2020/03/02 15:29:32(UT...	Finished	
配置更新-1526	Update Config File	One-time Task	2020/03/02 15:26:55(UT...	Finished	
发送消息-测试	Send Message	Daily	14:07:08(UTC+08:00)	Finished	
型号更新配置	Update Config File	One-time Task	2020/03/02 11:45:51(UT...	Finished	
站点配置更新	Update site Configuration	One-time Task	2020/03/02 12:01:34(UT...	Finished	

The search results are displayed in the list.

Viewing Timer Tasks

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

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

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

Executed Task					
<div> <input type="text" value="Start date"/> to <input type="text" value="End date"/> <input type="text" value="789"/> <input type="button" value="Search"/> </div>					
Execution Time	Execution Mode	Task Name	Task	Execution Status	Operation
2020/01/21 14:45:35 (UTC+...	Timing	789	Update site Configuration	✓ Execute successfully	



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


Executed Task

Start date to End date
 提前取消发送消息

Execution Time	Execution Mode	Task Name	Task	Execution Status	Operation
No data, add first					

Viewing Tasks

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

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

Execution Details ×

Task : Send message Execution Time : 2020/02/27 20:54:26 (UTC+08:00)

All
 MAC/Device Name/Account Info

Failed: 2 / Total 2

<input type="checkbox"/>	MAC	Device Name	Model	Status	Status
<input type="checkbox"/>	Device has been de...	--	--	--	ⓘ Execute failed,T...
<input type="checkbox"/>	805ec0431ffa	2746	SIP-T54S	Unregistered ▼	ⓘ Execute failed,T...

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.

Click **Task Management > Scheduled Task**.

Executed Task

Start date to End date
 Task Name

Execution Time	Execution Mode	Task Name	Task	Execution Status	Operation
2020/03/02 09:28:46 (UTC+...)	At once	--	Update Config File	ⓘ Execute abnormally	ⓘ
2020/03/02 09:21:27 (UTC+...)	At once	--	Update Config File	ⓘ Execute abnormally	ⓘ
2020/03/02 09:14:44 (UTC+...)	At once	--	Send Message	ⓘ Execute abnormally	ⓘ
2020/03/02 09:14:21 (UTC+...)	At once	--	Upgrade Firmware	ⓘ Execute abnormally	ⓘ
2020/03/02 09:13:53 (UTC+...)	At once	--	Update Config File	✓ Execute successfully	ⓘ
2020/03/02 08:49:26 (UTC+...)	At once	--	Update Resource File	ⓘ Execute abnormally	ⓘ
2020/03/02 15:29:32 (UTC+...)	Timing	重启-1529	Reboot	✓ Execute successfully	ⓘ
2020/03/02 15:26:55 (UTC+...)	Timing	配置更新-1526	Update Config File	✓ Execute successfully	ⓘ
2020/03/02 06:26:20 (UTC+...)	At once	--	Send Message	✓ Execute successfully	ⓘ
2020/03/02 14:08:06 (UTC+...)	Timing	测试	Send Message	✓ Execute successfully	ⓘ
2020/03/02 12:01:34 (UTC+...)	Timing	站点配置更新	Update site Configuration	✓ Execute successfully	ⓘ

The search results are displayed in the executed task list.

Diagnosing Devices

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

- [Starting Diagnosing](#)
- [Exporting the Packets, Logs, and Configuration Files by One Click](#)
- [Capturing Packets](#)
- [Diagnosing the Network](#)
- [Exporting System Logs](#)
- [Exporting the Configuration Files](#)
- [Viewing the CPU and the Memory Status](#)
- [Viewing Recordings](#)
- [Capturing the Screenshot of the Device](#)
- [Getting the Device Log](#)
- [Setting the Log Level](#)
- [Download the Device Log](#)
- [Diagnostic Assistance](#)
- [Ending the Diagnostic](#)

Starting Diagnosing

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

The screenshot illustrates the 'Device Diagnostic' interface. At the top, there are icons for a speakerphone, a smartphone, and a laptop. Below these, a text input field is labeled '1 Enter the device MAC\IP\ID.' and contains the value '805ec0066d9c'. A '+ Add' button is located below the input field. A blue button labeled '2 Start Diagnostic' is positioned below the '+ Add' button. An orange arrow points from the 'Start Diagnostic' button to the main diagnostic panel below.

The main diagnostic panel, titled 'Device Diagnostic', displays the following information:

- Login Name:** VC200
- Device Type:** Video Device
- IP:** 10.81.6.21
- Model:** VC200

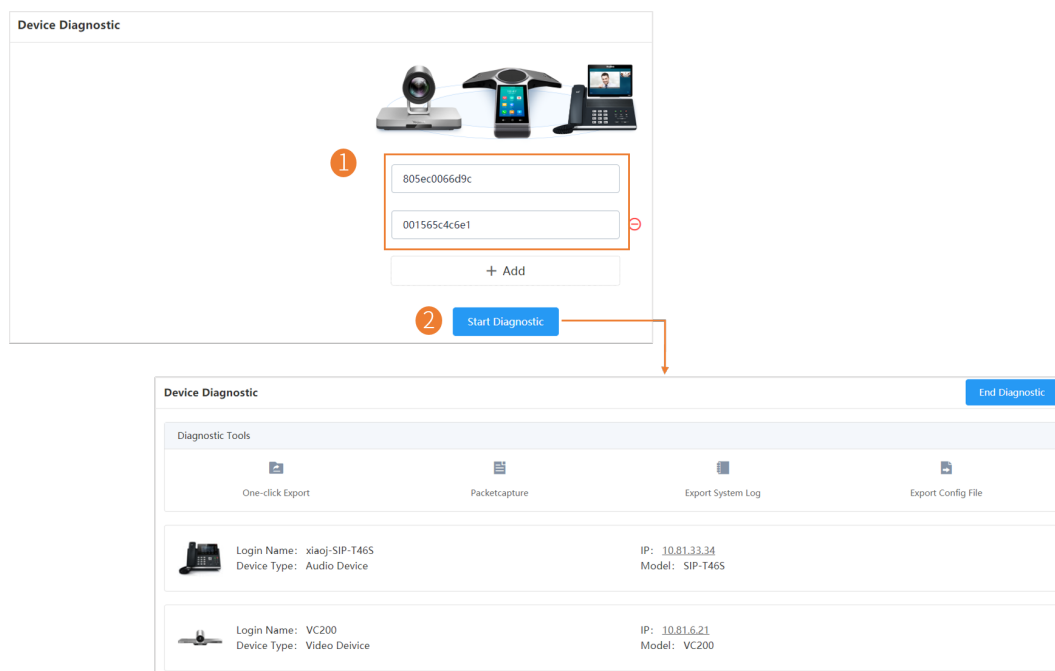
On the right side of this panel, there are two buttons: 'End Diagnostic' and 'Diagnostic Assistance'.

Below this information is a section titled 'Diagnostic Tools' with several icons representing different diagnostic actions: One-click Export, Packetcapture, Network Detection, Export System Log, Export Config File, CPU Memory Status, Recording File, and Screenshot.

At the bottom, there is a '7-Day Log' section. It includes a date range selector (Start date to End date) and a 'Search' button. Below the search bar, there is a table with the following columns: File Name, Time, Size, Description, Storage Space, and Operation. The table contains three rows of log entries.

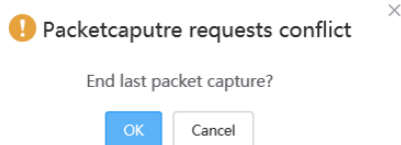
File Name	Time	Size	Description	Storage Space	Operation
805ec0066d9c-2020-08-07...	2020-08-07	1663.66KB	--	server	Download
805ec0066d9c-2020-08-06...	2020-08-06	2434.25KB	--	server	Download
805ec0066d9c-2020-08-05...	2020-08-05	292.81KB	--	server	Download

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



Note:

- This feature is not applicable to the offline and invalid devices.
- Users can diagnose the same devices at the same time except for capturing packets. The later request of capturing packets will automatically disable the former one.



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

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

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

One-click Export

×

Packetcapture

* Ethernet

wan

▼

Type

Custom

▼

String

Please enter packetcapture string

Configuration File

* File Type

cfg

▼

* Export

All Settings

▼

Start Capture

Cancel

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

One-click Export

×

Diagnostics start. .

MAC-001565f30702 Export Config file Success ✓

MAC-001565f30702 Export Config file Success ✓

MAC-001565f30702 Export Log file Success ✓

MAC-001565f30702 Export Packetcapture file Success ✓

Diagnostics complete

Download

Cancel

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

Capturing Packets

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 <i>and</i> . 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 <i>or</i> . 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.

1. On the Device Diagnostics page, click **Packetcapture**.



Note:

- Customize the time for capturing.
 - You can enter the string only when you select **Custom** from the drop-down menu of the **Type**.
2. Click **Finish** to stop capturing, and the file is generated automatically.
 3. Click **Download** to save the file to your computer.
If it takes more than 1 hour to capture packets, the packet capturing will be automatically ended.

Diagnosing the Network

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.

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

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

- If you select Ping, the example result is below

```
PING 10.200.112.72 (10.200.112.72) 56(84) bytes of data.
64 bytes from 10.200.112.72: icmp_seq=1 ttl=62 time=0.641 ms
64 bytes from 10.200.112.72: icmp_seq=2 ttl=62 time=0.588 ms
64 bytes from 10.200.112.72: icmp_seq=3 ttl=62 time=0.619 ms
64 bytes from 10.200.112.72: icmp_seq=4 ttl=62 time=0.832 ms
64 bytes from 10.200.112.72: icmp_seq=5 ttl=62 time=0.625 ms

--- 10.200.112.72 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 0.588/0.661/0.832/0.087 ms
```

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

```
traceroute to 10.200.112.72 (10.200.112.72), 5 hops max, 46 byte packets
 1 10.81.7.254 (10.81.7.254) 3.278 ms 2.472 ms 1.396 ms
 2 10.0.254.253 (10.0.254.253) 2.313 ms 0.984 ms 0.838 ms
 3 10.200.112.72 (10.200.112.72) 0.716 ms 0.568 ms 0.567 ms
```

Exporting System Logs

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

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

Exporting the Configuration Files

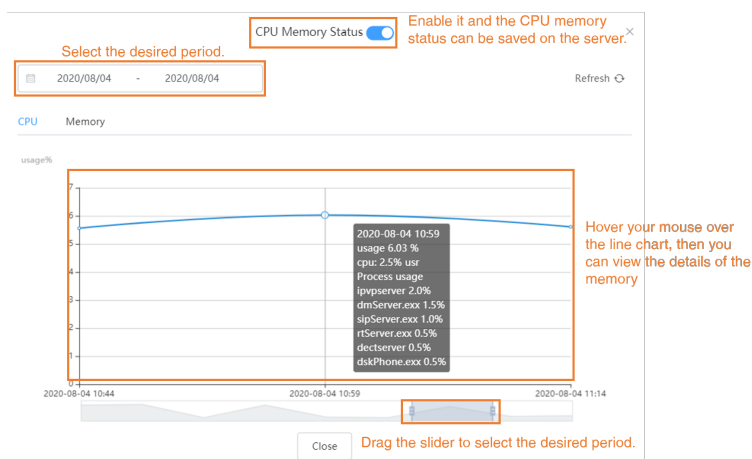
You can export the cfg files or the bin files. For cfg files, you can choose to export static setting files, non-static setting files or all setting files. You cannot export configuration files of the offline devices.

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

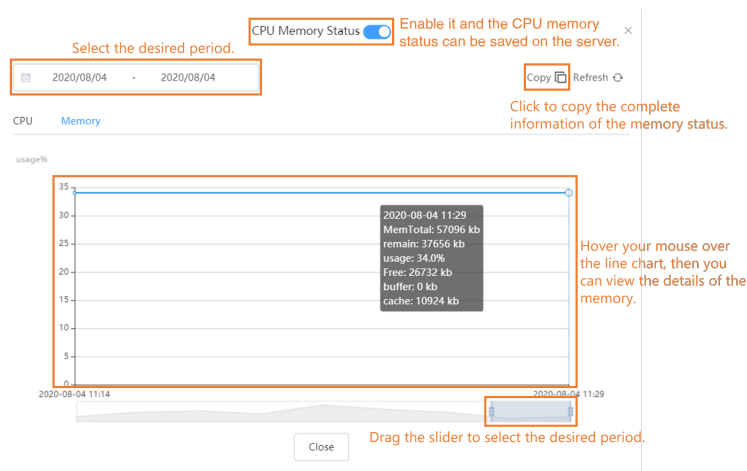
Viewing the CPU and the Memory Status

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.

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



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



Viewing Recordings

- There are recording files on the devices.
- You already select **Automatic upload recording file** check box to enable the automatic uploading, so the recording file will be uploaded to the platform automatically.

Recording File

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

Time	File Name	Size(KB)	Operation
2019-12-30	001565262635-1577673...	107621.55	
2019-12-30	001565262635-1577673...	960.05	
2019-12-30	001565262635-1577673...	885.34	

☒ Automatic upload recording file

Close

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

Recording File



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

Time	File Name	Size(KB)	Operation
2019-12-30	001565262635-1577673...	107621.55	
2019-12-30	001565262635-1577673...	960.05	
2019-12-30	001565262635-1577673...	885.34	

☒ Automatic upload recording file

Close

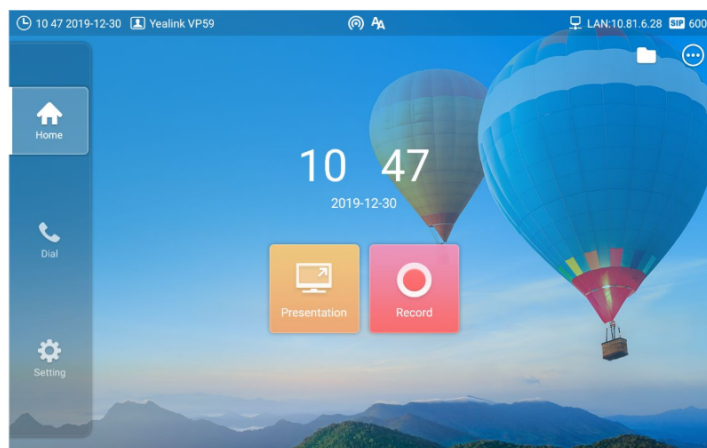


Note: Click to download the recording file or click to delete the recording file.

Capturing the Screenshot of the Device

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

Screencapture



Re-acquire

Close



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

Getting the Device Log



Note:

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

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

Setting the Log Level

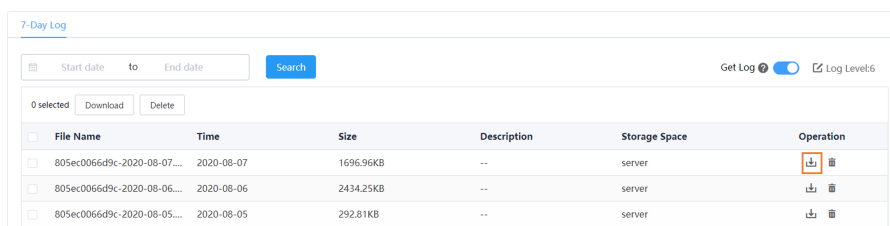
1. On the Device Diagnostics page, click **Log Level**.
2. Enter the desired value.
3. Click **Confirm**.

Download the Device Log

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

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

- Download a single device log:









7-Day Log

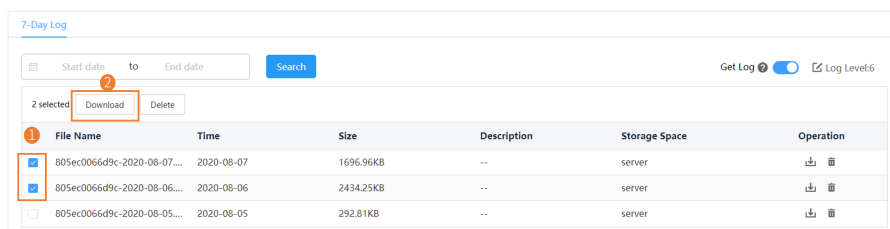
Start date to End date Search

Get Log ☒ Log Level: 6

0 selected Download Delete

File Name	Time	Size	Description	Storage Space	Operation
805ec0066d9c-2020-08-07...	2020-08-07	1696.96KB	--	server	 
805ec0066d9c-2020-08-06...	2020-08-06	2434.25KB	--	server	 
805ec0066d9c-2020-08-05...	2020-08-05	292.81KB	--	server	 

- Download a batch of device logs:









7-Day Log

Start date to End date Search

Get Log ☒ Log Level: 6

2 selected Download Delete

File Name	Time	Size	Description	Storage Space	Operation
<input checked="" type="checkbox"/> 805ec0066d9c-2020-08-07...	2020-08-07	1696.96KB	--	server	 
<input checked="" type="checkbox"/> 805ec0066d9c-2020-08-06...	2020-08-06	2434.25KB	--	server	 
<input type="checkbox"/> 805ec0066d9c-2020-08-05...	2020-08-05	292.81KB	--	server	 

Diagnostic Assistance

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

Ending the Diagnostic

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

Managing Alarm

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

- [Alarm Statistics](#)
- [Adding Alarm Strategies](#)
- [Managing Alarm Strategies](#)

- [Viewing Alarms](#)
- [Filtering the Alarms](#)
- [Exporting Alarm Records](#)

Alarm Statistics

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

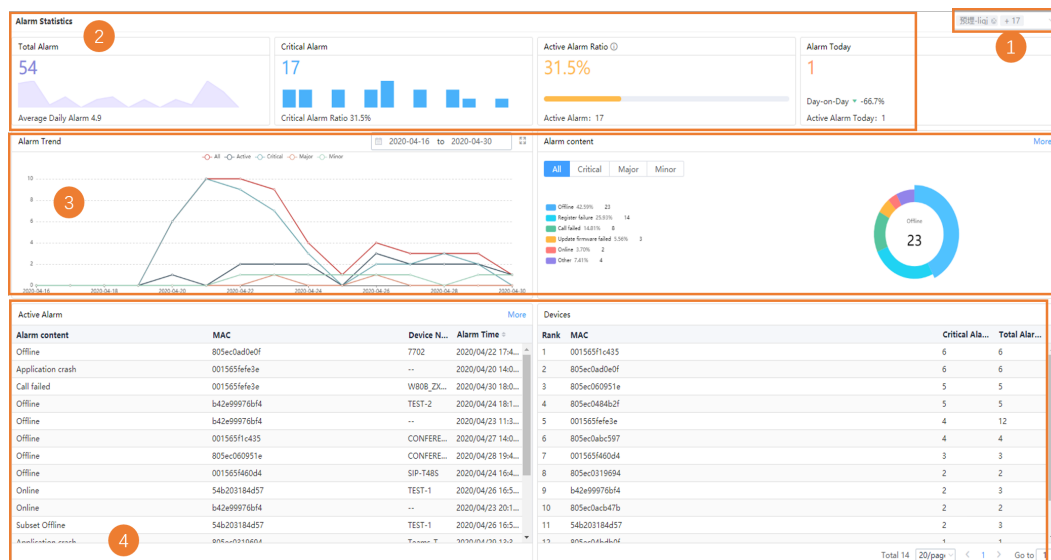



Table 1:

Number	Feature	Description
1	Select the sites.	After you select the sites, the chart displays the statistics of the selected sites. The default value is all sites. Note: You can only select the sites which your account has the permission to.
2	The total alarms of the enterprises.	This chart displays the trend of the alarms in the recent 15 days.
	The critical alarms of the enterprises.	This chart displays the distribution of the critical alarms in the recent 15 days.

Number	Feature	Description
	The active alarm ratio and the total number of active alarms.	<p>1. When the ratio is below 30%, the color of the scale bar is green.</p> <p>2. When the ratio is between 30% ~ 70%, the color of the scale bar is yellow.</p> <p>3. When the ratio is above 70%, the color of the scale bar is red.</p>
	The number of alarms today, the ratio of the alarms compared between today and yesterday, the number of active alarms today.	
3	The chart of the alarm trends.	<p>1. The statistics of the chart can select any range within a half year. The default value is the statistics in the recent 15 days.</p> <p>2. Click  to view in a larger screen. You can use this feature to view the statistics within a longer time scale.</p> <p>3. Display or hide the trend of the statistics. The default value is displaying the trend of all statistics.</p> <p>4. Move your mouse to the corresponding date to display the detailed data.</p>
	The alarm content.	This chart displays the ratio and the number of each alarm content.
4	The active alarm.	Display the content of the active alarms of devices.
	The devices.	<p>1. The devices ranks based on the number of critical alarms and the total number of alarms.</p> <p>2. Click Critical Alarm. The devices ranks based on the number of the critical alarms in positive or negative sequence.</p> <p>3. Click Total Alarm. The devices ranks based on the number of the total alarms in positive or negative sequence.</p>

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).

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

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



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

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

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

Add strategy

1 Set basic information 2 Alarm Receiver 3 Alarm content 4 Devices 5 Finish

<input type="checkbox"/> Critical	<input type="checkbox"/> Bad call quality <input type="checkbox"/> Register failure <input type="checkbox"/> Update firmware failed <input type="checkbox"/> Update configuration failed <input type="checkbox"/> Offline <input type="checkbox"/> Application crash <input type="checkbox"/> Application no response <input type="checkbox"/> Kernel panic <input type="checkbox"/> Subset Offline <input type="checkbox"/> Low power <input type="checkbox"/> Power off or Disconnect
<input type="checkbox"/> Major	<input type="checkbox"/> Meet now failure <input type="checkbox"/> BToE pairing failure <input type="checkbox"/> Exchange discovery failure <input type="checkbox"/> Time synchronization failure <input type="checkbox"/> Exit program <input type="checkbox"/> DNS server discovery failure <input type="checkbox"/> Online <input type="checkbox"/> Calendar synchronization failure
<input type="checkbox"/> Minor	<input type="checkbox"/> Call failed <input type="checkbox"/> Hold failed <input type="checkbox"/> Resume failed <input type="checkbox"/> Play visual voicemail failed <input type="checkbox"/> Visual voicemail retrieve failure <input type="checkbox"/> Calllog retrieve failure <input type="checkbox"/> Outlook contact retrieve failure <input type="checkbox"/> RTP violate <input type="checkbox"/> RTP address change <input type="checkbox"/> RTP SSRC change <input type="checkbox"/> RTP dead <input type="checkbox"/> SRTP failure <input type="checkbox"/> Bluetooth paired failed

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

8. On the page of Devices, do one of the following:

- Select All to display all alarms.
- Select Site and select the desired sites from the top-down menu.

Devices ☐ All ☒ Site ☐ Group ☐ Custom devices

Please select a site ^

- ▶ ☐ D
 - ☐ hahahaha
 - ☐ hahahhahahah2
- ▶ ☐ A
 - ☐ 21
 - ☐ xinde
 - ☐ A11

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

Devices ☐ All ☐ Site ☒ Group ☐ Custom devices

Please select group

Group name

- ☐ GROUP1
- ☐ test3
- ☐ GROUP3
- ☐ GROUP2
- ☐ TEST2

- Select Custom devices and enter the corresponding information.

Select the sites from the top-down menu. Select the devices from the top-down menu.

Devices ☐ All ☐ Site ☐ Group ☒ Custom devices

Please select a site: All

MAC/Device Name/Account info


MAC	Device Name	Account Info
<input type="checkbox"/> 001565fefe3e	W808_ZXL_1	13473
<input type="checkbox"/> 805ec0319694	Teams_T38A_pcy	--
<input type="checkbox"/> 805ec0484b2f	T525	5005
<input type="checkbox"/> 000000002b01	Teams_MP56_pcy	--
<input type="checkbox"/> 001565c19083	YL_SIP-T38	7008

Total 17 < 1 2 3 > Go to 1

Selected: 0

MAC	Device Name	Account Info
-----	-------------	--------------

Select MAC/Device Name/Account Information from the top-down menu.

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

Devices ☐ All ☐ Site ☐ Group ☒ Custom devices

Please select a site: All

MAC/Device Name/Account info

MAC	Device Name	Account Info
<input checked="" type="checkbox"/> 805ec03c3738	5002	5002
<input checked="" type="checkbox"/> 001565c99d03	BYP-T415	5055
<input checked="" type="checkbox"/> 001565f460d4	yf554@yealinkftb.com	yf554@yealinkftb.com
<input type="checkbox"/> 805ec07b1a00	BAIYF-W608	8503
<input type="checkbox"/> 001565c2d8f1	4639	--


Total 130 < 1 2 3 4 ... 17 > Go to 1

Selected: 3

MAC	Device Name	Account Info
805ec03c3738	5002	5002
001565c99d03	BYP-T415	5055
001565f460d4	yf554@yealinkftb.com	yf554@yealinkftb.com

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

Managing Alarm Strategies

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

Alarm Strategy + Add Strategy

0 selected Delete

<input type="checkbox"/>	Strategy	Alarm Str...	Notificati...	Status	Alarm Receiver	Alarm content	Devices	Operation
<input type="checkbox"/>	每日everyDay	Email,In-st...	Daily	On	chencany@yealink.com	Call failed, Hold failed, Resume faile...	All	
<input type="checkbox"/>	111	Email	Real-time	Off	923085715@qq.com,hongy@yeal...	Call failed, Hold failed, Resume faile...	All	

- Select the corresponding strategy and click **Delete**.

报警策略管理 + 新增策略

已选 1 项 删除

<input type="checkbox"/>	名称	报警策略	报警周期	状态	报警接收人	报警内容	设备范围	操作
<input type="checkbox"/>	baby子账号	邮箱,站内	实时	启用	babychild@yealink.com	通话质量差, 注册失败, 固件升级失败, 配置文件更新失败, 设备离线	站点	
<input type="checkbox"/>	system_default	邮箱,站内	实时	启用	liq@yealink.com	通话建立失败, 通话保持错误, 通话质量差, 通话质量异常错误, ...	全部	

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.

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

Alarm List Export

Device name/MAC/IP/Model More all

0 selected Delete Resolved Ignore Active

<input type="checkbox"/>	Status	MAC	Device Name	Model	Site	IP	Alarm Severity	Alarm Time	Alarm Type	Module	Operation
<input type="checkbox"/>	Resolved	e0d55efda9be	99999	MVC400	Yealink	10.86.3.13	Critical	2020/04/30 09:31:00	Offline	Connectivity	
<input type="checkbox"/>	Resolved	803253c2de9e	testZjq	MVC400	Yealink	10.82.22.132	Critical	2020/04/29 21:25:00	Offline	Connectivity	
<input type="checkbox"/>	Resolved	e0d55efda9be	99999	MVC400	Yealink	10.86.3.13	Critical	2020/04/29 18:40:00	Offline	Connectivity	
<input type="checkbox"/>	Active	001565c69d03	BYF-T41S	SIP-T41S	balyf	10.81.88.65	Critical	2020/04/28 18:05:00	Offline	Connectivity	
<input type="checkbox"/>	Resolved	001565c69d03	BYF-T41S	SIP-T41S	1212	10.81.88.65	Critical	2020/04/28 17:15:10	Register failure	Protocol	
<input type="checkbox"/>	Ignore	001565f460d4	yf554@yealinksfb.c...	SIP-T485S...	Yealink	10.81.88.50	Critical	2020/04/28 16:14:00	Offline	Connectivity	
<input type="checkbox"/>	Resolved	001565f460d4	yf554@yealinksfb.c...	SIP-T485S...	Yealink	10.81.88.50	Critical	2020/04/27 16:27:41	Register failure	--	
<input type="checkbox"/>	Resolved	805ec07b1a00	BAIYF-W60B	W60B	Yealink	10.81.88.28	Critical	2020/04/27 15:38:00	Offline	Connectivity	
<input type="checkbox"/>	Resolved	805ec07b1a00	BAIYF-W60B	W60B	Yealink	10.81.88.28	Critical	2020/04/27 14:57:47	Register failure	Protocol	
<input type="checkbox"/>	Active	805ec03c3738	5002	SIP-T57W	Yealink	10.71.1.25	Critical	2020/04/27 11:17:06	Register failure	Protocol	
<input type="checkbox"/>	Resolved	e0d55efda9be	99999	MVC900	Yealink	10.86.3.13	Critical	2020/04/26 18:01:00	Offline	Connectivity	

2. Optional: Do one of the following:

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

Alarm Information



MAC: e0d55efda9be

Last Alarm Time: 2020/04/30 09:31:00

Count: 1

Description: This alarm occurs when the connection status of the Mini-PC changes from online to offline for 15 minutes.

Reason: This alarm occurs when the connection status of the Mini-PC changes from online to offline for 15 minutes.

Detail: 2020/04/30 13:42:40 online
 2020/04/30 13:42:40 offline (The device close the connection)
 2020/04/30 10:12:01 online

Close

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

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

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

Alarm List Export

Device name/MAC/IP/Model More all

1 selected Delete Resolved Ignore Active

Status	MAC	Device Name	Model	Site	IP	Alarm Severity	Alarm Time	Alarm Type	Module	Operation
Active	e0d55efda9be	99999	MVC400	Yealink	10.86.3.13	Critical	2020/04/30 09:31:00	Offline	Connectivity	
Resolved	803253c2de9e	testZjq	MVC400	Yealink	10.82.22.132	Critical	2020/04/29 21:25:00	Offline	Connectivity	

- Click to diagnose the device and troubleshoot the reason.
- Click **Delete** to delete the alarm.

The common alarm types are as below:

Alarm type	Severity
Poor call quality	Critical
Register failure	Critical
Upgrade firmware failure	Critical
Update configuration failure	Critical
Offline	Critical
System license is about to expire	Critical
Device capacity of license is insufficient	Critical
Subset Offline	Critical
Low power	Critical
Power off or Disconnect	Critical
Visual voicemail retrieve failure	Minor
Hold failure	Minor

Alarm type	Severity
Resume failure	Minor
RTP violate	Minor
RTP address change	Minor
RTP dead	Minor
SRTP failure	Minor
Call log retrieve failure	Minor
Outlook contact retrieve failure	Minor
Call failed	Minor
Calendar synchronization failure	Major
Exchange discovery failure	Major
Online	Major

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

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

Alarm List

Device name/MAC/IP/Model More ▾

1 selected

Status ▾	MAC	Device Name	Model	Site	IP	Alarm Severity ▾	Alarm Time	Alarm Type ▾	Module ▾
<input checked="" type="checkbox"/> Active ▾	e0d55efda9be	99999	MVC400	Yealink	10.86.3.13	Critical	2020/04/30 09:31:00	Offline	Connectivity
<input type="checkbox"/> Resolved ▾	803253c2de9e	testZjq	MVC400	Yealink	10.82.22.132	Critical	2020/04/29 21:25:00	Offline	Connectivity
<input type="checkbox"/> Resolved ▾	e0d55efda9be	99999	MVC400	Yealink	10.86.3.13	Critical	2020/04/29 18:40:00	Offline	Connectivity
<input type="checkbox"/> Active ▾	001565c69d03	BYF-T41S	SIP-T41S	baiyifeng	10.81.88.65	Critical	2020/04/28 18:05:00	Offline	Connectivity
<input type="checkbox"/> Resolved ▾	001565c69d03	BYF-T41S	SIP-T41S	1212	10.81.88.65	Critical	2020/04/28 17:15:10	Register failure	Protocol
<input type="checkbox"/> Ignore ▾	001565f460d4	yl554@yealinksfb.c...	SIP-T485C...	Yealink	10.81.88.50	Critical	2020/04/28 16:14:00	Offline	Connectivity

all
7 Days Active Alarm
7 Days Critical Alarm
test
test-Major
test-Minor
test-Critical
Filter management >

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

Add filter



* Alarm content

* Alarm Time ☒ All ☐ 1 day ☐ 7 days ☐ 30 days

* Alarm status ☒ Active ☒ Resolved ☒ Ignore

* Alarm content


☐ Critical
 ☐ Bad call quality
 ☐ Register failure
 ☐ Update firmware failed
 ☐ Update configuration failed
 ☐ Offline
 ☐ Application crash
 ☐ Application no response
 ☐ Kernel panic
 ☐ Subset Offline
 ☐ Low power
 ☐ Power off or Disconnect

☐ Major
 ☐ Meet now failure
 ☐ BToE pairing failure
 ☐ Exchange discovery failure
 ☐ Time synchronization failure
 ☐ Exit program
 ☐ DNS server discovery failure
 ☐ Online
 ☐ Calendar synchronization failure

☐ Minor
 ☐ Call failed
 ☐ Hold failed
 ☐ Resume failed
 ☐ Play device response failed

OK Cancel

Filtering the Alarms

Click  to filter the alarms, and select the desired filter to view the corresponding alarms.

Alarm List Export

Device name/MAC/IP/Model More

0 selected Delete Resolved Ignore Active

<input type="checkbox"/>	Status	MAC	Device Name	Model	Site	IP	Alarm Severity	Alarm Time	Alarm Type	Module
<input type="checkbox"/>	Active	e0d55efda9be	99999	MVC400	Yealink	10.86.3.13	Critical	2020/04/30 09:31:00	Offline	Connectivity
<input type="checkbox"/>	Active	001565c69003	BYF-T415	SIP-T415	balye测试站...	10.81.88.65	Critical	2020/04/28 18:05:00	Offline	Connectivity
<input type="checkbox"/>	Active	805ec03c3738	5002	SIP-T57W	Yealink	10.71.1.25	Critical	2020/04/27 11:17:06	Register failure	Protocol

all

7 Days Active Alarm

7 Days Critical Alarm

test

test-Major

test-Minor


test-Critical

Filter management >

Exporting Alarm Records

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

1. Click **Alarm Management** → **Alarm List**.

2. Optional: Click  in the top-right corner of the page to filter the desired alarm records.

3. Click **Export** to export the alarm records.

Viewing Call Quality Statistics

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



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

- [Customizing the Indicators of Call Quality Detail](#)
- [Viewing the Call Data](#)

Customizing the Indicators of Call Quality Detail

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

Click **Dashboard > Call Statistics**.

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

Call Quality Detail(2018/12/19~2018/12/19)							
Device/MAC/Account Information				More ▾		More Indicators ▾	
Device Name	MAC address	Model	Firmware	Caller/Callee	Call Type	Quality	Operation
2984	00:15:65:c1:87:25	SIP-T48G	35.83.0.50	Callee	P2P	Poor	View

Viewing the Call Data

1. Click **Dashboard > Call Statistics**.
2. Click **View** beside the desired call to go to the Call Data page.

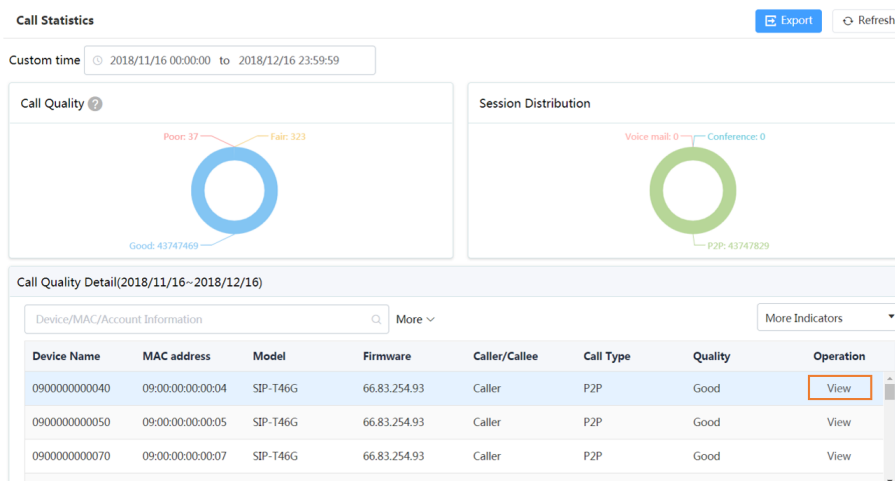


Table 2: Metrics of Call Data

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

Table 3: Evaluation Metrics of Call quality

Call quality	Metrics
Excellent (all metrics should be satisfied)	Delay: the average call delay should be less than or equal to 200ms

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

Managing System

- [Viewing Operation Logs](#)
- [Exporting the Server Log](#)
- [Configuring the SMTP Mailbox](#)
- [Uploading DST Rules](#)
- [Obtaining the Accesskey](#)

Viewing Operation Logs

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

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

Operation Log		Server Log		Set or filter the parameters to view the desired log.	
Start date to End date		User Name/IP		Search	
User name	Operation Type Path	Operation Object	IP	Operation Time	Results
88888@qq.com	Login Login	88888@qq.com	10.70.4.11	2019/11/14 11:34:22	Operate successfully
88888@qq.com	Login Login	88888@qq.com	10.70.4.11	2019/11/14 11:41:19	Operate successfully
88888@qq.com	Login Login	88888@qq.com	10.70.4.11	2019/11/14 12:21:52	Operate successfully
88888@qq.com	Login Login	88888@qq.com	10.70.4.11	2019/11/15 11:28:30	Operate successfully
99@qq.com	Login Login	99@qq.com	10.70.4.11	2019/11/15 11:11:56	Operate successfully
99@qq.com	Login Login	99@qq.com	10.70.4.11	2019/11/15 11:34:20	Operate successfully
admin	Login Login	admin	10.82.23.32	2019/09/16 19:58:09	Operate successfully
admin	Login Login	admin	10.83.2.17	2019/09/16 20:34:20	Operate successfully
admin	Login Login	admin	10.83.2.17	2019/09/16 21:07:14	Operate successfully
admin	Login Login	admin	10.82.23.32	2019/09/16 21:16:53	Operate successfully
admin	Login Login	admin	10.82.24.132	2019/09/17 09:13:01	Operate successfully
admin	Login Login	admin	10.83.2.17	2019/09/17 10:00:45	Operate successfully
Total 1047		20/page		1 2 3 4 5 6 ... 53 > Go to 1	

Exporting the Server Log

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

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

The screenshot shows the 'Server Log' export configuration window. It includes the following elements:

- Module Selection:** Checkboxes for Business, Connection, User, and Web.
- Time Range:** A date range selector set to 2019-12-16.
- Server Node Selection:** A list of nodes with 'Default [10.200.112.72]' selected. A 'Selecte Node' column is also present.
- Action Buttons:** 'Select all' and 'Cancel' buttons are located at the bottom of the configuration area.
- Export Button:** A blue 'Export Log' button is located at the bottom of the window.

Configuring the SMTP Mailbox

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

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

Mailbox Settings

* SMTP:

* Sender:

* Username:

* Password:

* Port:

☒ This server requires secure connections to the

☒ Enable the mailbox

Save

Test email settings

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

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

Test email settings ×

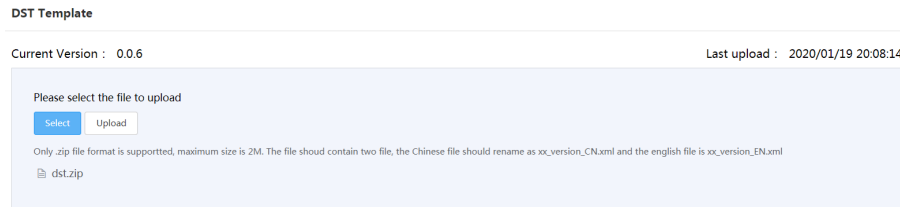
* Receiver:

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

4. Click **Confirm**.

Uploading DST Rules

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](#).

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

Managing Administrator Accounts

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

- [Adding/Editing/Deleting a Group](#)
- [Adding/Editing/Deleting a Role](#)
- [Assigning the Function Permission](#)
- [Assigning the Data Permission](#)
- [Adding and Managing Sub-Administrator Accounts](#)
- [Editing the Account Information](#)
- [Viewing the Account Code](#)

Adding/Editing/Deleting a Group

You can manage the roles by the group.

You cannot edit or delete the default group.

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

Add Group

* Group Name

Test-3

OK

Cancel

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

Devices ☐ All ☐ Site ☒ Group ☐ Custom devices

Please select group

Group name

☐ GROUP1☐ test3☐ GROUP3☐ GROUP2☐ TEST2

Adding/Editing/Deleting a Role

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

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

Table 4: Default role

Name	Group	Function and data permission
Super manager	Default role group	All function and data permission
Empty manager	Default role group	No function permission except for the permission to log in.

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

Add Role

* Role Name

* Group

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

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

Role Management + Add Group + Add Role

- default group
 - super manager
 - empty manager
 - role for mary

Sub Account Function Permission Data Permission

Username	Email	Operation
houwq	houwq@yealink.com	Edit Delete Add
hulq1	hulq@yealink.com	Edit Delete Add

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.

You have added roles, refer to [Adding/Editing/Deleting a Role](#).

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

Role Management + Add Group + Add Role

- default group
 - super manager
 - empty manager
 - role for mary

Sub Account Function Permission Data Permission

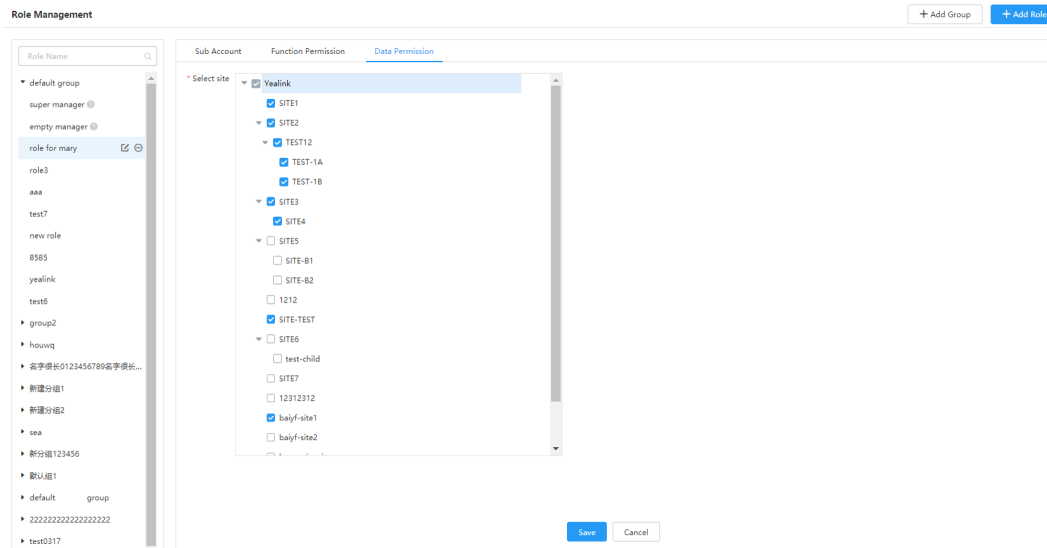
Room System	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Edit Device <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Reboot <input checked="" type="checkbox"/> Reset To Factory <input checked="" type="checkbox"/> Update Firmware
Firmware Management	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Add/Edit Firmware <input checked="" type="checkbox"/> Delete
Resource Management	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Add/Edit Resource <input checked="" type="checkbox"/> Delete
Account Management	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Add/Edit Account <input checked="" type="checkbox"/> Delete
Device Configuration	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Model Configuration <input checked="" type="checkbox"/> Add/Edit Config <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Download
Site Configuration	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Add/Edit Config <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Download
Group Configuration	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Add/Edit Config <input checked="" type="checkbox"/> Download <input checked="" type="checkbox"/> Delete
MAC Configuration	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Export <input checked="" type="checkbox"/> Upload <input checked="" type="checkbox"/> Generate <input checked="" type="checkbox"/> Set Parameters <input checked="" type="checkbox"/> Download <input checked="" type="checkbox"/> Delete
Global Parameter Setting	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Edit/Push
Configuration Update		
Site Management	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Add/Edit Site <input checked="" type="checkbox"/> Delete
Task Management	<input checked="" type="checkbox"/> Scheduled Task <input checked="" type="checkbox"/> Readonly <input checked="" type="checkbox"/> Add/Edit Task <input checked="" type="checkbox"/> Pause/Stop Task	
Executed Task		
Alarm Management	<input checked="" type="checkbox"/> Alarm Statistics <input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Status Management
Alarm List		
Alarm Strategy		
Device Diagnostic	<input checked="" type="checkbox"/> Readonly	<input checked="" type="checkbox"/> One-click Export <input checked="" type="checkbox"/> Packet Capture <input checked="" type="checkbox"/> Network Detection <input checked="" type="checkbox"/> Export System Log <input checked="" type="checkbox"/> Export Config File <input checked="" type="checkbox"/> CPU
Recording File		
Dashboard	<input checked="" type="checkbox"/> Call Statistics <input checked="" type="checkbox"/> Running State	
System Management	<input checked="" type="checkbox"/> Log Management <input checked="" type="checkbox"/> Mailbox Settings <input checked="" type="checkbox"/> License <input checked="" type="checkbox"/> API Service	

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.

You have added roles, refer to [Adding/Editing/Deleting a Role](#).

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



Related tasks

[Adding Sites](#)

Adding and Managing Sub-Administrator Accounts

You have added roles, refer to [Adding/Editing/Deleting a Role](#).

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

Add sub account

1

* Username mary

* Email mary@yealink.com

Phone Number Please enter the phone number, maximum 32 characters

Office Address Please enter office address, maximum 128 characters

* Role role for mary

2
Confirm
Cancel



Note:

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

Sub Account Management + Add

Register Email/Contact/Role Search

0 selected Delete Change role

<input type="checkbox"/>	Register Email	Contact	Phone Number	Role	Add Date	Operation
<input type="checkbox"/>	wangcy@yealink.com	55	18650118523	peace	2019/06/19 16:48:44	✎ 🔒


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.

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

[Account Settings](#) [Account Code](#)



Username: admin

Password: ***** [Edit](#)

Basic Settings

* Company name

Phone number

* Email

Office address

Country/Area

Parameter	Introduction
Password	The password of this account. Click Edit to change the password according to the prompt. For account security, we recommend that you change the password regularly.
Email	The mailbox is used to receive alarms and the account information.
Country/Area	You can change your current country/area to other countries/ areas under the same site, for example in the international site. However, changing countries over two different site are not allowed.

Viewing the Account Code

The account code is the site ID. You can put the account code into the Common.cfg file and push the file to the device, to make the device automatically connected to the corresponding site of YDMP. For more information, refer to [Configuring the Common.cfg File](#).

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**.

Account Settings Account code

SiteID

Site Name/Site ID

Site Name	Site ID	
Yealink	m1lej3me	Copy
Yealink/1212	eqvwncc	Copy

Troubleshooting

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

- [Forget the Login Password?](#)
- [Why You Cannot Access the Login Page?](#)
- [Why the Browser Prompts That the Security Certificate of the Website Is not Trusted When You Access the Login Page?](#)

Forget the Login Password?

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

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 reset 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
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2017-11-01 06:34:55 EDT; 9min ago
     Main PID: 23324 (firewalld)
       CGroup: /system.slice/firewalld.service
              └─23324 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

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

- If you enable the firewall, you should run the following commands to enable the related ports in the firewall configuration:
- `firewall-cmd --permanent --zone=public --add-port=80/tcp`
- `firewall-cmd --permanent --zone=public --add-port=443/tcp`
- `firewall-cmd --permanent --zone=public --add-port=9989/tcp`
- `firewall-cmd --permanent --zone=public --add-port=9090/tcp`
- `firewall-cmd --reload`
- `firewall-cmd --list-ports`
- After you finish the configuration and refresh the page, you can access the login page of YDMP successfully.

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

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

Solution:

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

```
microdm_tcp_server_address = tcp.yealinkops.com
microdm_mail_web_domain = https://dm.yealinkops.com
microdm_domain = dm.yealinkops.com
```

2. Run the command as below:

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

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