Yealink Device Management Platform Administrator Guide V3.3.0.0

Contents

About This Guide

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 realize the centralized management for Yealink devices used in an enterprise.

This guide provides operations for enterprise administrators to use the YDMP.

- *Related Documentations*
- *In This Guide*

Related Documentations

Except for this guide, we also provide the following document of the corresponding device:

- 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 a basic guidance for provisioning Yealink phones in a provisioning server. If you are new to this, it is helpful to read this guide.

You can download the above documents from Yealink's official website or the web page of YDMP.
The address of Yealink's official website is as below: *http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage*.

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

In This Guide

Topics include:

Getting Started

This chapter introduces some basic requirements and information about YDMP.

- *Hardware and Software Requirements*
- *Port Requirements*
- *Browser Requirements*
- *Supported Device Models*

Hardware and Software Requirements

The requirements of the hardware and software are different based on different server requirements. Linux operating system: CentOS 7.0 or later. The detailed requirements are as below:

Device Quantity	CPU	RAM	Hard Drive
0~6000	8-core	16G	It should be at least 200G , 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	

Port Requirements

You should open four ports: 443, 9989, 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, is used for reporting the device information.
80	It is used for accessing the device management platform via HTTP.

Browser Requirements

YDMP supports the following browsers:

Browser	Version
Firebox	55 or later

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

Supported Device Models

You can manage the following devices via the device management platform:

Device Types	Supported Device Models	Version Requirements
SIP IP Phones	SIP-T27P/T27G/ T29G/T41P/T41S/T42G/T42S/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.84.0.70 or later versions are not supported any more). 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.
	W60B	77.83.0.10 or later.
	VP59	91.283.0.10 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.
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.
Video Conferencing Systems	VC200/VC500/VC800/VC880	XX.32.10.25/XX.32.0.25 or later. XX represents the fixed number for each device model.
	PVT950/PVT980	1345.32.10.40 or later.
	VP59	91.332.0.10 or later.

Device Types	Supported Device Models	Version Requirements
Zoom phones	CP960	73.30.0.10 or later.
Room System	MVC500/MVC800	92.11.0.10 or later

Deploying YDMP

This chapter provides instructions on how to install and deploy YDMP, and introduces its interface.

- *Updating YDMP (from V2.0 to V3.1)*
- *Restoring YDMP (from V3.1 to V2.0)*
- *Installing YDMP (3.X)*
- *Updating YDMP (from V3.1 to V3.X)*
- *Logging into YDMP*
- *Home Page*
- *Running State Page*
- *Logging out of YDMP*
- *Activating the License*
- *Uninstalling YDMP*

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

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

Before you begin

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

Procedure

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

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

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

Results

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

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

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

Procedure

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

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

3. According to the prompts, enter *2* which means restoring.
4. According to the prompts, enter the password *Yealink1105*.
5. According to the prompts, enter the*Y* to confirm to restore.
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)

The following is an example of installing V3.1.0.13, with the server IP address 10.2.62.12.

Before you begin

- Obtain the installation package of YDMP from the Yealink distributor or SE and then save it at the path /usr/local.

- Meet the following requirements: *Hardware and Software Requirements* and *Port Requirements* .

Procedure

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

```
cd /usr/local
tar -zxf DM_3.1.0.13.tar.gz
cd yealink_install&& tar -zxf install.tar.gz
./install --host 10.2.62.12 ##If it is the internal deployment or the
 external deployment, run this command. ##
./install --host internal IP -e nat_ip=external IP ##If it is the NAT
 deployment, run this command. Only 3.3.0.0 or later versions can be
 supported. ##
```

Results

Note: 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.

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

The following is an example of updating YDMP from V3.1.0.13 to V3.3.0.0, with the server IP address as 10.2.62.12.

Before you begin

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

Procedure

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

```
cd /usr/local
rm -rf yealink_install
tar -xvzf DM_3.3.0.0.tar.gz
cd yealink_install&& tar -xvzf install.tar.gz
./upgrade --host 10.2.62.12
```

Results

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

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

Logging into YDMP

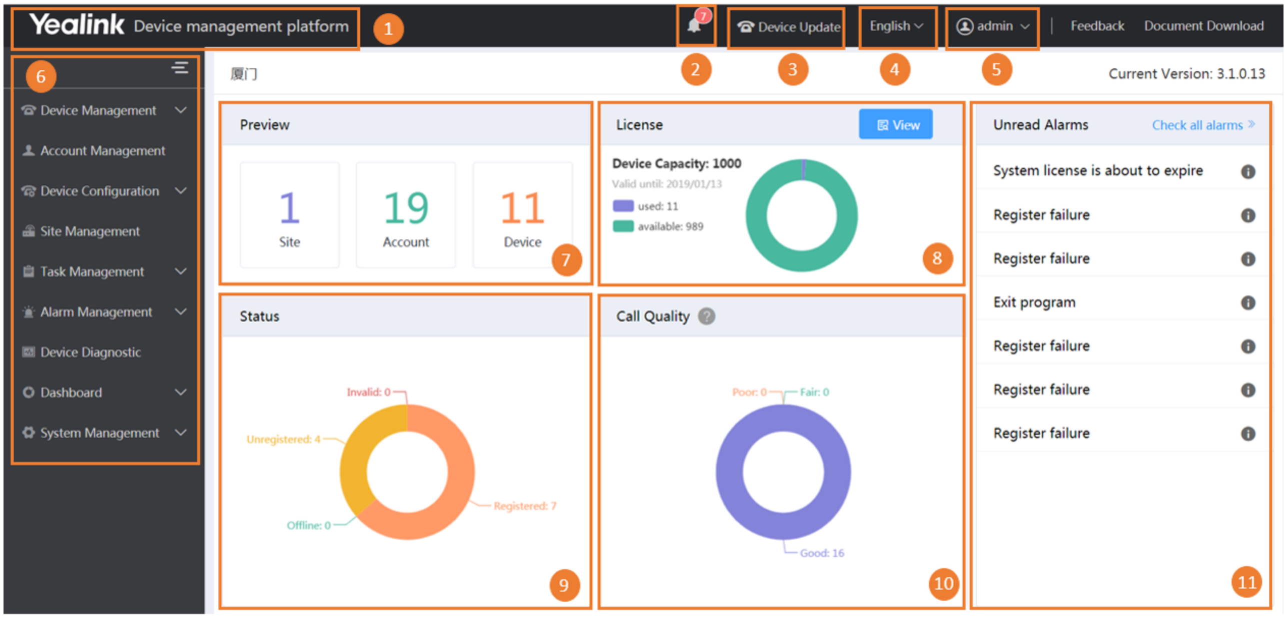
Procedure

1. Enter https://<IP address>/(for example: https: //10.2.62.12/) in the browser address box, and then press Enter.
2. Select the desired language from the drop-down menu of **Language** in the top-right corner.

3. Enter your username (default: admin) and the password (default: v123456789), and click **Login**.
4. If you log in for the first time, the system will remind you to change the password, click **Change** to go to the homepage.

Home Page

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

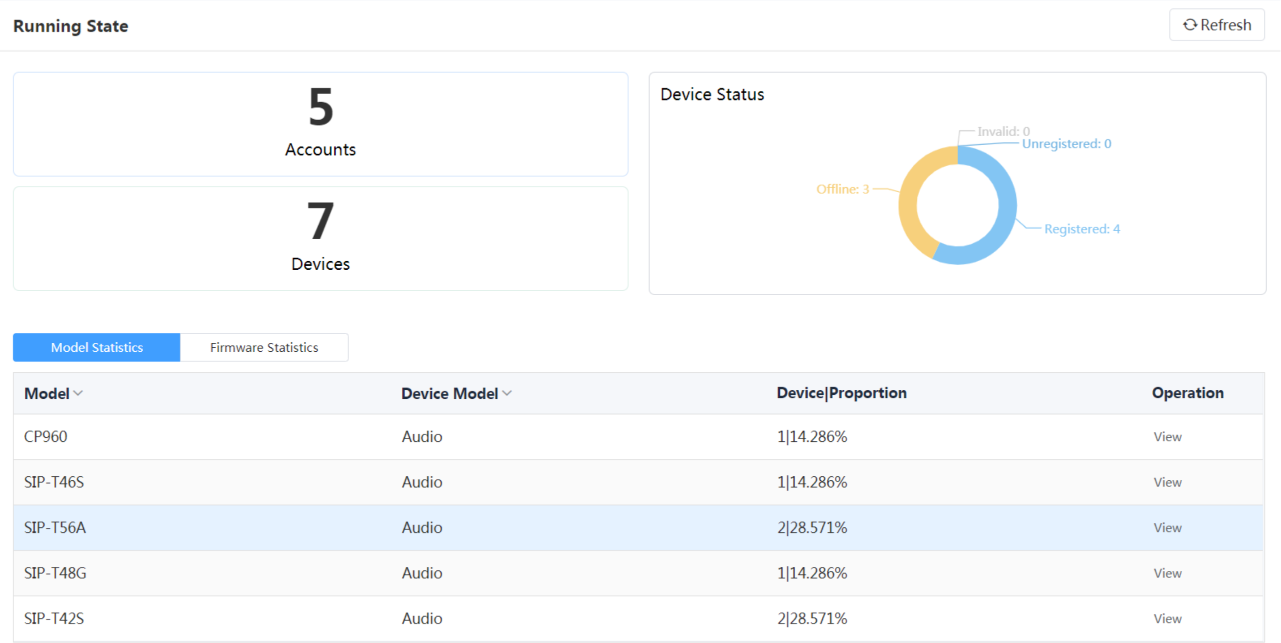


Number	Description
1	Go to the home page quickly when you are browsing other pages.
2	Display the number of unread alarms and the type of alarms.
3	Go to the Device List page quickly.
4	Change the display language.
5	Go to the page of setting administrator account.
6	Go to sending a feedback or downloading a document.
7	Navigation pane.
8	**Data preview:** • Displays the number of sites, accounts and devices. • Click the desired module to go to the corresponding module.
9	**License:** Displays the current number of manageable devices.
10	**Device status:** • Displays 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 device of this status.

Number	Description
11	**Call quality:** • Displays the number of the good, the bad or the poor call quality. • You can click the desired module to view the call statistics.
12	**Unread Alarms:** • Click **Check all alarms** to go to the Alarm List page. • Hover the mouse over the icon ⓘ to view the alarm details.

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:



Model	Device Model	Device|Proportion	Operation
CP960	Audio	1|14.286%	View
SIP-T46S	Audio	1|14.286%	View
SIP-T56A	Audio	2|28.571%	View
SIP-T48G	Audio	1|14.286%	View
SIP-T42S	Audio	2|28.571%	View

- 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, click the corresponding status (offline, registered, invalid, and unregistered) to go to the Device List page, and 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.

Logging out of YDMP

Procedure

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

Activating the License

Before managing your devices via the device management platform, you need purchase the license from your supplier and activate it.

Procedure

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

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

Importing the Device Certificate

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

Before you begin

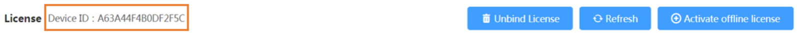
You provide the enterprise name, the distributor and the country for Yealink. Yealink will generate a device certificate according to the information you provide.

Procedure

1. Click **System Management** > **License**.
2. Select the 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 : A63A44F4B0DF2F5C

Activating the License Online

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

Before you begin

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

Procedure

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

After Yealink authorizes the license, you can see the license in the list.

Activating the License Offline

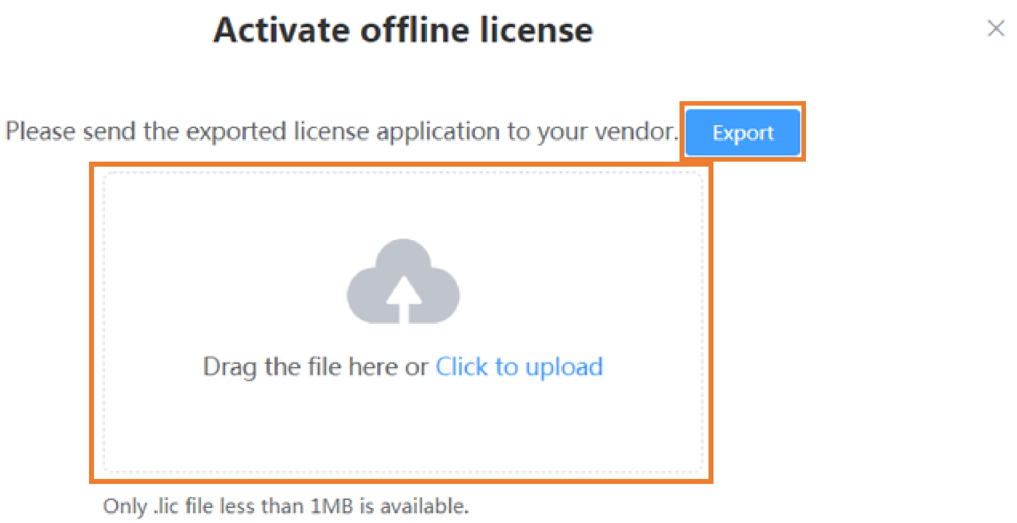
If your server cannot access the public network, you can activate the license offline.

Before you begin

- *Importing the Device Certificate* is finished.
- You provide the device ID, the license type, the concurrent number and the validity for Yealink. Yealink will authenticate based on the above information.

Procedure

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



Activate offline license

Please send the exported license application to your vendor.

Drag the file here or Click to upload

Only .lic file less than 1MB is available.

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

Results

The license is displayed in the list.

Uninstalling YDMP

Procedure

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

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

3. According to the prompts, enter the password *Yealink1105*.

YDMP will be uninstalled from the CentOS.

Deploying the Room System

Before you manage the Room System via the device management platform, you should deploy to the Room System to make it connect to the device management platform.

About this task

For more information about deploying Room System, refer to *Yealink MVC800&MVC500 for Microsoft Teams Rooms System Deployment Guide*.

Procedure

On your MTouch, open Yealink Room Connect, go to **Remote Management**, and configure the related parameters.
The Room System will be connected to the device management platform automatically.

Deploying Other Devices

Before you manage the devices via the device management platform, you should deploy the devices to make them connect to the device management platform.

Before you begin

Note: Note that the device firmware version should support the device management platform. Otherwise, you should upgrade the device firmware first.

Procedure

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

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

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

Results

After the device is connected to the platform, the device information will be displayed in the device list.

- *Using Certificates for Mutual TLS Authentication*
- *Configuring 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 the Yealink device management platform and the device to authenticate with each other, the platform supports mutual TLS authentication by using default certificates.

- *Configuring Trusted Certificates*
- *Configuring Server Certificates*

Configuring Trusted Certificates

When a device sends an SSL connection request to the platform, the device need verify whether the platform can be trusted. The platform 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**.

Results

Only when the authentication succeeds, will the device trust the platform.

Configuring Server Certificates

When the device management platform sends an TLS connection request to the device, the device management platform need verify whether the device can be trusted. The device will send the default device certificate to the platform for authentication.

Procedure

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

Results

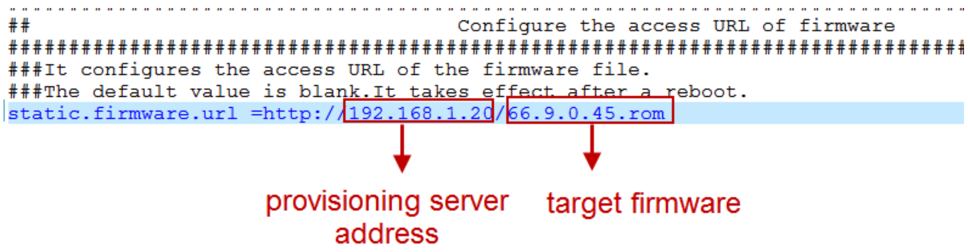
The device will send the default device certificate to the platform for authentication.

Configuring Common CFG File

If the device does not support the device management platform, you need to upgrade the firmware before you connect the device to the device management platform. For easy deployment, you can configure the parameters of upgrading the firmware and the access URL of the device management platform in the Common.cfg file.

Procedure

1. Open the Common CFG file of the corresponding device.
2. If your device does not support the device management platform, upgrade the firmware of the device. Place the target firmware on your provisioning server, and then specify the access URL of the firmware.

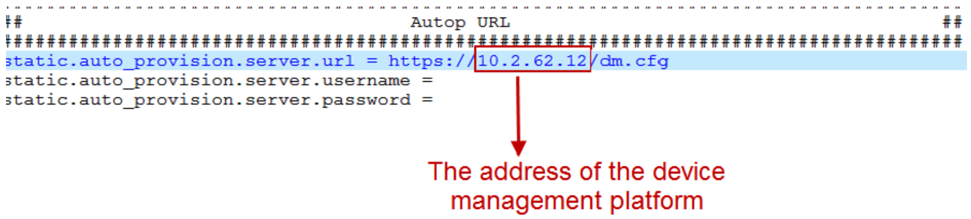


```
##                                   Configure the access URL of firmware
#####################################################################################
###It configures the access URL of the firmware file.
###The default value is blank.It takes effect after a reboot.
static.firmware.url =http://192.168.1.20/66.9.0.45.rom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

provisioning server address

target firmware

3. Configure the provisioning URL to connect the devices to the device management platform.



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

The address of the device management platform

4. Save the file.

Results

After auto provisioning, the devices will be connected to the device management platform.

Related concepts

Supported Device Models

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 the device management platform to the devices so that they can be connected to the platform.

Procedure

1. Log into the RPS management platform.

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

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

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

Results

After you trigger the device to send an RPS request, the device will be connected to the device management platform.

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

Configuring the Server Address

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

Procedure

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

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

   (for example: https://10.2.62.12/dm.cfg).
4. Click **Auto Provision Now**.
   The device will be connected to the device management platform successfully.

Managing Administrator Accounts

This chapter provides the basic operations for the administrator account.

- *Changing the Login Password*
- *Editing the Information of the Administrator Account*
- *Managing Sub-Administrator Accounts*

Changing the Login Password

In order to ensure the account security, we recommended that you change the password regularly.

Procedure

1. Hover your mouse over the account avatar in the top-right corner of the page, and then click **Account Settings**.
2. Click **Edit** beside the password.
3. Enter the current password and enter the new password twice.
4. Click **Confirm**.

Editing the Information of the Administrator Account

You can edit the information, for example the contact, the phone number and the country, so that the superior distributor or reseller can contact you. The administrator mailbox is used to receive the alarm and the account information.

Procedure

1. Hover your mouse over the account avatar in the top-right corner of the page, and then click **Account Settings**.
2. Edit the administrator account in the corresponding field.
3. Click **Save**.

Managing Sub-Administrator Accounts

You can add sub-administrator accounts, and assign different data permissions or function permissions to different sub-administrator accounts.

- *Adding/Editing/Deleting a Group*
- *Adding/Editing/Deleting a Role*
- *Assigning Roles to Sub-Administrator Accounts*
- *Assigning the Function Permission*
- *Assigning the Data Permission*
- *Adding and Managing Sub-Administrator Accounts*

Adding/Editing/Deleting a Group

You can manage the roles by the group.

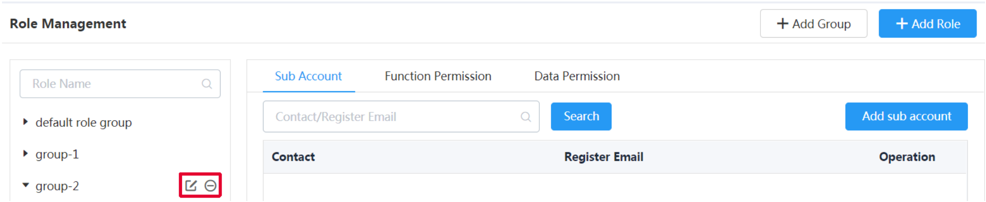
About this task

You cannot edit or delete the default group.

Procedure

1. Click **System Management** > **Role Management**.
2. In the top-right corner, click **Add Group**.
3. Enter the group name.
4. Click **OK**.

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



Adding/Editing/Deleting a Role

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

About this task

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

Table 1: Default role

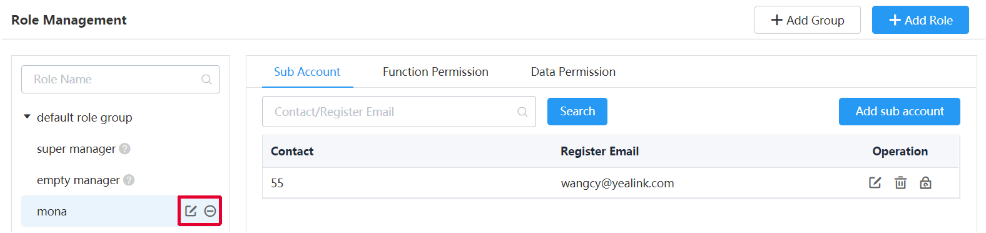
Name	Department	Function and data permission
Super manager	Default role group	All function and data permission
Empty manager	Default role group	Only the login permission

Procedure

1. Click **System Management** > **Role Management**.
2. In the top-right corner, click **Add Role**.

3. Specify the role name.
4. Select the desired group.
5. Click **OK**.

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



Contact	Register Email	Operation
55	wangcy@yealink.com	

Assigning Roles to Sub-Administrator Accounts

After adding the roles, you can add sub-administrator accounts for them. You can also assign roles to sub-administrator accounts when adding the sub-administrator accounts (for more information, see *Adding and Managing Sub-Administrator Accounts*).

Before you begin

You has added roles.

Procedure

1. Go to Role Management, select the corresponding role, and click **Add sub account**.
2. Configure the phone number and the email.
3. Click **Confirm**.

Related tasks

Adding/Editing/Deleting a Role

Assigning the Function Permission

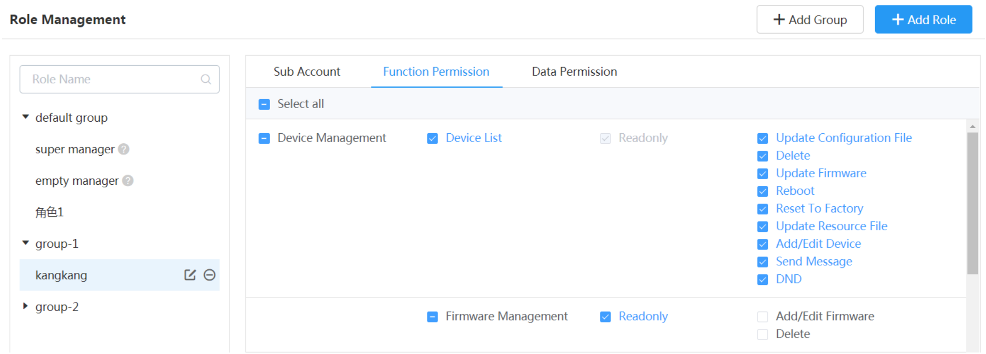
If you want to allow non-managers to use the sub-administrator account, for example, checking the call quality of the phone and diagnosing the devices, but you do not want them to add or delete devices, you can assign the limited function permission to them.

Before you begin

You has added roles.

Procedure

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



Role Management

+ Add Group   + Add Role

Role Name

- default group
  - super manager
  - empty manager
  - 角色1
- group-1
  - kangkang
- group-2

Sub Account   Function Permission   Data Permission

▣ Select all

▣ Device Management   ☑ Device List   ☑ Readonly   ☑ Update Configuration File
☑ Delete
☑ Update Firmware
☑ Reboot
☑ Reset To Factory
☑ Update Resource File
☑ Add/Edit Device
☑ Send Message
☑ DND

▣ Firmware Management   ☑ Readonly   ☐ Add/Edit Firmware
☐ Delete

Related tasks

Adding/Editing/Deleting a Role

Assigning the Data Permission

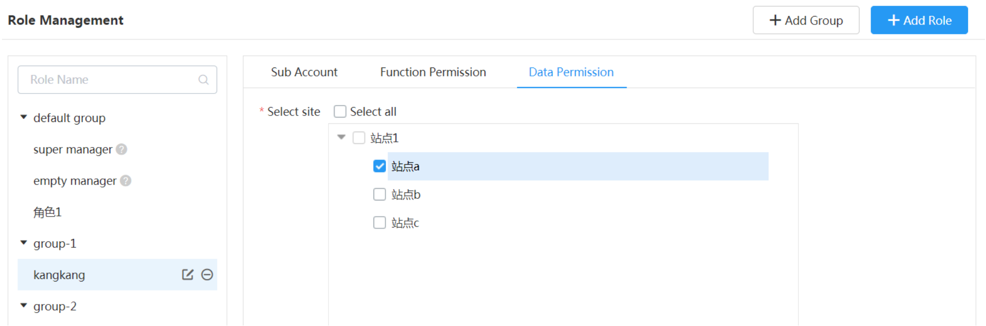
If you want to manage the device of your own site or of a certain amount sites, you can assign the data permission.

Before you begin

You has added roles.

Procedure

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



Role Management

+ Add Group   + Add Role

Role Name

- default group
  - super manager
  - empty manager
  - 角色1
- group-1
  - kangkang
- group-2

Sub Account   Function Permission   Data Permission

* Select site   ☐ Select all

- ☐ 站点1
  - ☑ 站点a
  - ☐ 站点b
  - ☐ 站点c

Related tasks

Adding/Editing/Deleting a Role

Adding and Managing Sub-Administrator Accounts

Before you begin

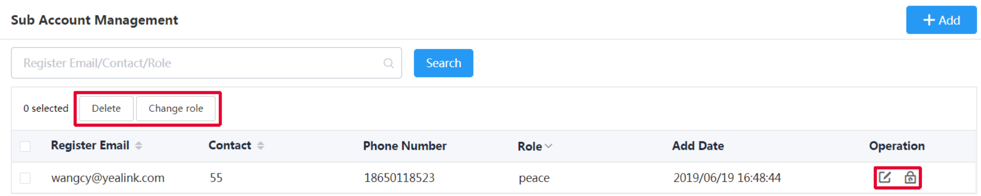
You has added roles.

Procedure

1. Click **System Settings** > **Sub Account Management**.
2. In the top-right corner, click **Add**.
3. Configure the phone number, and the email.
4. Select a desired role from the drop-down menu of **Role**.
5. Click **Confirm**.

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

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



□	Register Email	Contact	Phone Number	Role	Add Date	Operation
□	wangcy@yealink.com	55	18650118523	peace	2019/06/19 16:48:44	

Related tasks

Adding/Editing/Deleting a Role

Managing Sites

You can set up the site according to the organizational structure of your company. For example, you can set up different sites according to different departments, and divide all the accounts in the same department into the same site.

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

- *Adding Sites*
- *Importing Sites*
- *Editing Sites*
- *Searching for Sites*
- *Deleting Sites*

Adding Sites

Procedure

1. Click **Site Management**.
2. In the top-right corner, click **Add Site**.
3. Enter the site name and select the parent site.
4. Enter the description.
5. Click **Save**.

   If you want to add several sites continuously, you can also click **Save and add** to save the change and continue adding sites.

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 the device management platform.

Procedure

1. Click **Site Management**.
2. In the top-right corner, click **Import**.
3. Click **Download the template**.
4. Edit the template and save it to your computer.

Before editing the information, you need to read the note and then fill in the template as required.

5. Click **Click to upload** to import the file or drag the file to the specified field directly.
6. Click **Upload**.

Editing Sites

Procedure

1. Click **Site Management**.
2. Select a desired site in the Site Name list.
3. Edit the site name, select the parent site, and add description in the corresponding field.
4. Click **Save**.

Searching for Sites

Procedure

1. Click **Site Management**.
2. Enter the site name or the site description in the search box.
3. Press **Enter** to perform a search.
   The search result is displayed in the Site Name list.

Deleting Sites

You can delete sites created by your own, but you cannot delete the default site named after your company name. 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.

About this task

The site cannot be deleted if there are devices under it.

Procedure

1. Click **Site Management**.
2. Select a desired site in the Site Name list.
3. Click **Delete**.
4. Click **OK** according to the prompts.

Managing Accounts

You can manage different products on the device management platform. Different products 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: Managing accounts is not applicable to Teams phone.

Adding Accounts

Procedure

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

Importing Accounts

You can import the template to add multiple accounts quickly. You need to download the template, edit the information in the template and then import the template to the device management platform.

Procedure

1. Click **Account Management**.
2. In the top-right corner, click **Import** > **Import SFB account/Import SIP account/Import YMS account/Import CLOUD account/Import H.323 account**.
3. Click **Download the template**.
4. Read the note, enter the corresponding information in the template and then save it to your computer.
5. Click **Click to upload** to import the file or drag the file to the specified field directly.
6. Click **Upload**.

Editing the Account Information

Procedure

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

Searching for Accounts

Procedure

1. Click **Account Management**.
2. Enter the account information and click **Search**.
   The search result is displayed in the account list.

Exporting Accounts

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

Procedure

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

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

Deleting Accounts

Procedure

1. Click **Account Management**.
2. Select the desired accounts.
3. Click **Delete**.
4. Click **OK** Deleting Accounts.

   If the account is linked to a device, it prompts whether or not you want to unlink the account.

   Click **OK** to delete the account.

Managing Devices

- *Managing Devices*
- *Managing Firmware*
- *Managing Resources*

Managing Devices

The number of devices that you can manage on the device management platform depends on the license you purchased from the reseller or the distributor. You are not able to add new devices once the upper limit is reached. When a part 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.

- *Adding Devices*
- *Importing Devices*
- *Editing the Device Information*

- *Exporting the Device Information*
- *Viewing the Information of SIP Device*
- *View the Information of the Room System*
- *Searching for Devices*
- *Assigning Accounts to Devices*
- *Setting the Site*
- *Enabling/Disabling DND*
- *Sending Messages to Devices*
- *Rebooting Devices*
- *Resetting the Devices to Factory*
- *Deleting Devices*

Adding Devices

About this task

Note: Note that you need to deploy the device (refer to *Deploying Other Devices*) so that the device can be connected to the device management platform.

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device**.
3. In the top-right corner, click **Add Device**.
4. Configure the device name, the site, the model, the MAC address and the Machine ID in the corresponding filed.
5. Optional: On the right side of the **Bind Account** field, click **Add** and select an account and the account type to assign the account to the device.
6. Click **Save**.

Related tasks

Adding Accounts

Importing Devices

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

About this task

Note: You need to deploy the device (refer to *Deploying Other Devices*)so that the device can be connected to the device management platform.

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device**.
3. In the top-right corner, click **Import**.
4. Click **Download the template**.
5. Add the device information to the template and save it to your local system.
6. Click **Click to upload** to import the file or drag the file to the specified field directly.
7. Click **Upload**.

Editing the Device Information

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

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device** or **Room System**.
3. Click ✎ beside the desired device.
4. Editing the device information.
5. Click **Save**.

Exporting the Device Information

You can export the basic information of all devices.

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device**.
3. In the top-right corner, click **Export**.

Viewing the Information of SIP Device

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

Procedure

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

   You can click **Refresh** in the top-right corner to obtain the latest device information,
2. Click **SIP Device**.
3. Click one desired status entry under the **Status** tab and you can view the network information of the device, including the IP address, the subnet and the report time.

   The device status: unregistered, registered, offline, and invalid.

   - 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 service license expires, or the number of the devices reported to the platform exceeds the number allowed in the license.
4. Click 🔍 beside the desired device to view more information.

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.

Procedure

1. Click **Device Management** > **Device List**.
2. Click **Room System**.

   You can click **Refresh** in the top-right corner to obtain the latest device information, The device status: online, offline, and invalid.

- Online: the applications connected to the MVC devices are connected to the platform.
- Offline: the MVC devices are disconnected, or the applications connected to the MVC devices are disconnected to the platform.
- Invalid: the service license expires, or the number of the devices reported to the platform exceeds the number allowed in the license.

3. Click the blue font under the **Associated Device** tab and you can view the detailed information of the associated device of the room system.

Searching for Devices

You can search for devices by directly entering the basic information or selecting the site, which the devices belong to.

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device** or **Room System**.
3. For SIP devices, do one of the following:
   - Enter the device name, the MAC address, the account information or the IP address in the search box and press Enter.
   - Click **More**, select a desired site or the account status, and click **Search**.
4. For the Room System, do one of the following:
   - Enter the name, the MAC address or the IP address in the search box and press Enter.
   - Click **More**, select a desired site, and click **Search**.

   The search results are displayed in the list.

Assigning Accounts to Devices

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

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device**.
3. Click ✎ beside the desired device.
4. On the right side of the **Bind Account** field, click **Add** and select an account and the account type to assign the account to the device.
5. Click **Save**.
   The account information is sent to the device.

Related tasks

Adding Accounts

Setting the Site

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

Procedure

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

2. Click **SIP Device** or **Room System**.
3. Select the desired device.
4. Click **Site settings**.
5. Select the corresponding site and click **OK**.

Enabling/Disabling DND

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

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device**.
3. Select the desired device.
4. Click **More**, and then select **DND/Cancel DND** from the drop-down menu.
5. If you select a single device in step 2, you need to select a desired account.
6. Select a desired execution mode:
   - If you select **At once**, it will be executed immediately after you click OK.
   - If you select **Timing**, configure the task name, the repeat type and the execution time, the resource will be updated at a specific time.
7. Click **OK**.

Sending Messages to Devices

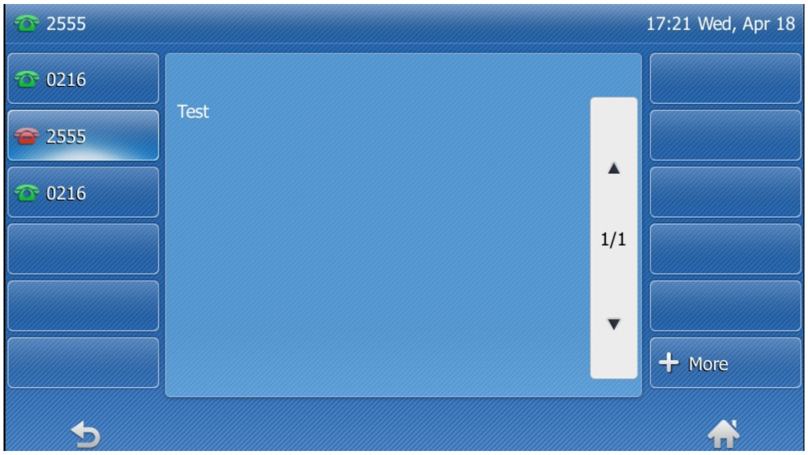
If you need to perform operations, for example, updating the firmware for the device, and want to notify the user in advance, you can send a message to the device through the platform. The device management platform supports sending messages to single or multiple devices.

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device**.
3. Select the desired devices.
4. Click **More**, and then select **Send message** from the drop-down menu.
5. Select a desired value from the drop-down menu of **Display duration**.
6. Enter the content in the corresponding field.
7. Click **OK**.

Results

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



Rebooting Devices

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device** or **Room System**.
3. For SIP devices, select the desired devices, click **More**, and select **Reboot**. For the Room System, select the desired system and click **Reboot**; or click its associated devices, select the devices that you want reboot and click **Reboot**.
4. Select a desired execution mode:
   - If you select **At once**, the devices will be reset at once.
   - If you select **Timing**, configure the task name, the repeat type and the execution time, the resource will be updated at a specific time.
5. Click **OK**.

Resetting the Devices to Factory

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device** or **Room System**.
3. For SIP devices, select the desired devices and click **More**. For the Room System, click its associated devices, and select the desired devices.
4. Select **Reset to factory** from drop-down menu.
5. Select a desired execution mode:
   - If you select **At once**, the devices will be reset at once.
   - If you select **Timing**, configure the task name, the repeat type and the execution time, the resource will be updated at a specific time.
6. Click **OK**.

Results

After the device is reset to the factory, its status becomes offline. You need re-deploy the device (*Deploying Other Devices*), to make the device connect to the device management platform.

Deleting Devices

Procedure

1. Click **Device Management** > **Device List**.
2. Click **SIP Device** or **Room System**.
3. For SIP devices, select the desired devices; for the Room System, select the desired system or click its associated devices, and select the device you want to delete.
4. Click **Delete**.
5. Click **OK** according to the prompts.

Managing Firmware

You can manage all the device firmware via the device management platform.

- *Adding Firmware*
- *Searching for Firmware*
- *Updating the Device Firmware*
- *Editing the Firmware*
- *Downloading the Firmware*
- *Deleting Firmware*

Adding Firmware

Procedure

1. Click **Device Management** > **Firmware Management**.
2. In the top-right corner, click **Add Firmware**.
3. Configure the firmware information in the corresponding filed and upload the firmware file.
4. Click **Save**.

Searching for Firmware

Procedure

1. Click **Device Management** > **Firmware Management**.
2. Enter the firmware name, the version or the description of the firmware in the search box.
3. Click **Search**.

Updating the Device Firmware

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

Procedure

1. Click **Device Management** > **Firmware Management**.
2. Click ↗ beside the desired firmware.
3. Select the desired devices.
4. Click **Push to Update**.

5. Select a desired execution mode:
   - If you select **At once**, the firmware will be updated at once.
   - If you select **Timing**, configure the task name, the repeat type and the execution time, the firmware will be updated at a specific time.
6. Click **OK**.

   Tip: You can also select the desired device in the Device List, click **Update Firmware**, and select the corresponding firmware version to update. Note that the firmware must be applicable to all selected devices.

Editing the Firmware

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

Procedure

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

Downloading the Firmware

Procedure

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

Deleting Firmware

Procedure

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

Managing Resources

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

- *Adding Resource Files*
- *Search for Resources*
- *Pushing Resource Files to Devices*
- *Editing Resource Files*
- *Downloading Backup Files*
- *Deleting Resource Files*

Adding Resource Files

Procedure

1. Click **Device Management** > **Resource Management**.
2. In the top-right corner, click **Add Resource**.
3. Configure the resource information in the corresponding filed and click **Upload** to upload the resource file.
4. Click **Save**.

Search for Resources

Procedure

1. Click **Device Management** > **Resource Management**.
2. Enter the resource name, the file name or the description in the search box.
3. Click **Search**.

Pushing Resource Files to Devices

Procedure

1. Click **Device Management** > **Resource Management**.
2. Click ↗ beside the desired resource.
3. Select the desired devices.
4. Click **Push to Update**.
5. Select a desired execution mode:
   - If you select **At once**, the resource will be updated at once.
   - If you select **Timing**, configure the task name, the repeat type and the execution time, the firmware will be updated at a specific time.
6. Click **OK**.

   ℹ **Tip:** You can also select the desired devices in the Device List, click **Update Resource File**, and select the corresponding resource type to update. The resource file must be applicable to all the selected devices.

Editing Resource Files

Procedure

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

Downloading Backup Files

Procedure

1. Click **Device Management** > **Resource Management**.

2. Click ⤓ beside the desired resource.
3. The file will be downloaded to your computer.

Deleting Resource Files

Procedure

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

Managing Device Configuration

You can manage device configuration by logging into the device management platform as a system administrator.

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

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 configuration to the device through setting the parameters in the template or editing the model configuration in the text.

Note that when the device of this model connects to the management platform for the first time, it will automatically update the configuration.

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

Adding Configuration Templates

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

Procedure

1. Click **Device Configuration** > **Model Configuration**.
2. In the top-right corner, click **Add Template**.
3. Enter the template name, select the device model, and edit the description.
4. Click **Save**.

Setting Parameters (Model Configuration)

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 in the template: you can edit the corresponding parameters in the template.

- *Setting Parameters in the Text (Model Configuration)*
- *Setting Template Parameters (Model Configuration)*

Setting Parameters in the Text (Model Configuration)

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

Procedure

1. Click **Device Configuration** > **Model Configuration**.
2. Click ⋯ beside the desired template.
3. Select **Editing Parameters in text** from the drop-down menu.
4. Configure the parameters in the text.
5. Click **Save**.
6. Click **No**, the parameters will only be saved.

   You can also click **Yes** to push the updated parameters to the device in this group.

Setting Template Parameters (Model Configuration)

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

Procedure

1. Click **Device Configuration** > **Model Configuration**.
2. Click ⚙ beside the desired template.
3. Configure the parameters.
4. Click **Save**.
5. Click **No**, the parameters will only be saved.

   You can also click **Yes** to push the updated parameters to the device in this group.

Pushing Configuration to Devices

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

Procedure

1. Click **Device Configuration** > **Model Configuration**.
2. Click ↗ beside the desired template.
3. Select the desired devices.
4. Click **Push to Update**.
5. Select a desired execution mode:

   - If you select **At once**, the parameters will be updated at once.
   - If you select **Timing**, configure the task name, the repeat type and the execution time, the firmware will be updated at a specific time.
6. Click **OK**.

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

Editing Configuration Templates

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

Procedure

1. Click **Device Configuration** > **Model Configuration**.
2. Click ••• beside the desired template.
3. Select **Edit Template** from the drop-down menu.
4. Edit the template information.
5. Click **Save**.

Downloading the Model File

You can download the model file to your computer to view the updated configuration parameters of the corresponding model.

Procedure

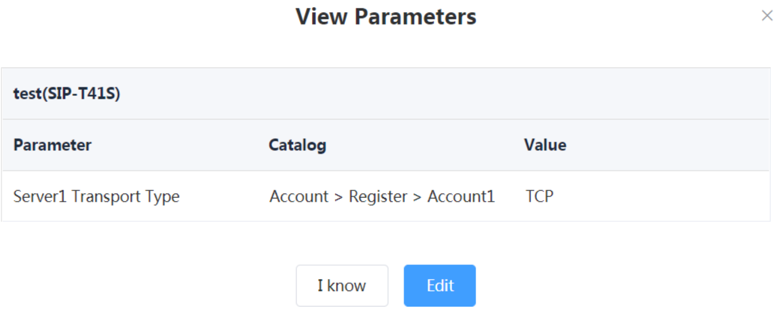
1. Click **Device Configuration** > **Model Configuration**.
2. Click ••• beside the desired template.
3. Select **Download config file** from the drop-down menu to download the configuration file to your local system.

Viewing Parameters

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

Procedure

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



test(SIP-T41S)

Parameter	Catalog	Value
Server1 Transport Type	Account > Register > Account1	TCP

You can click **Edit** to view the parameters in the template.

Deleting Templates

Procedure

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

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 Groups*
- *Setting Parameters (Group Configuration)*
- *Editing Groups*
- *Updating the Group Device*
- *Viewing Parameters*
- *Downloading Configuration File*
- *Deleting Groups*

Adding Groups

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

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. In the top-right corner, click **Add**.
3. Enter the group name and the description.
4. Click **Next step** to go to the Group Device page.
5. Select the desired devices.
6. Click **Next step** to go to the Set Parameters page.
7. Configure the desired parameters.
8. Click **Save**.

   You can also click **Save and update** to push the updated parameters to all the devices in this group.

Setting Parameters (Group Configuration)

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 in the template: you can edit the corresponding parameters in the template.

- *Editing Parameters in Text (Group Configuration)*
- *Setting Template Parameters (Group Configuration)*

Editing Parameters in Text (Group Configuration)

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

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Click ⋯ beside the desired group.
3. Select **Editing Parameters in text** from the drop-down menu.
4. Configure the parameters in the text.
5. Click **Save**.
6. Click **No**, the parameters will only be saved.

   You can also click **Yes** to update the parameters to all the device in this group.

Setting Template Parameters (Group Configuration)

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

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Click ⚙ beside the desired group.
3. Configure the parameters.
4. Click **Save**.
5. Click **No**, the parameters will only be saved.

   You can also click **Yes** to update the parameters to all the device in this group.

Editing Groups

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

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Click ⋯ beside the desired group.
3. Select **Edit Group** from the drop-down menu.
4. Edit the corresponding information.
5. Click **Save**.

Updating the Group Device

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 all devices in your group immediately.

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Click ⬆ beside the desired group.
3. Select the desired devices.
4. Click **Save**.

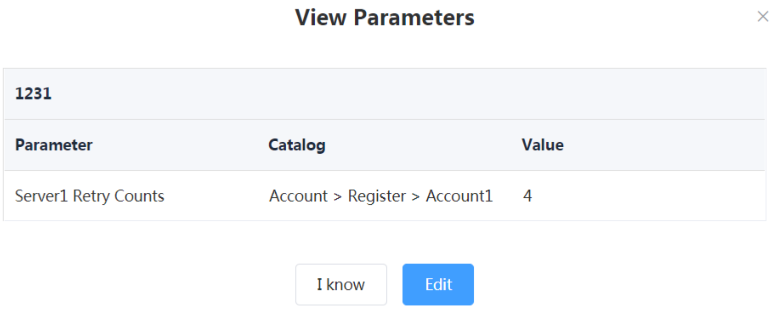
   You can click **Push to Update** to update the parameter configuration to all the devices in this group.

Viewing Parameters

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

Procedure

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



1231

Parameter	Catalog	Value
Server1 Retry Counts	Account > Register > Account1	4

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

Downloading Configuration File

You can download the configuration file to your computer to view the updated configuration parameters of the corresponding group.

Procedure

1. Click **Device Configuration** > **Group Configuration**.
2. Click ⋯ beside the desired group.
3. Select **Download config file** from the drop-down menu to download the configuration file to your local system.

Deleting Groups

Procedure

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

Managing the MAC Configuration

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

Not that when the device is connected to the management platform for the first time, and if there is a MAC backup file, it will be pushed to the device automatically.

- *Uploading backup Files*
- *Generating Configuration Files*
- *Pushing Backup Files to Devices*
- *Downloading Backup Files*

- *Exporting Backup Files*
- *Deleting Backup Files*

Uploading backup Files

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

Procedure

1. Click **Device Configuration** > **MAC Configuration**.
2. In the top-right corner, click **Upload backup file**.
3. Click **Select the file**, then select the desired file from your computer.
4. Click **Confirm**.

Generating Configuration Files

You can generate configuration files to back up the configuration on the device management platform directly.

Procedure

1. Click **Device Configuration** > **MAC Configuration**.
2. In the top-right corner, click **Generate config file**.
3. Select the desired devices.
4. Click **Confirm**.

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

Pushing Backup Files to Devices

Procedure

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

Downloading Backup Files

You can download the backup files to your local system.

Procedure

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

Exporting Backup Files

You can export the basic information of all devices.

Procedure

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

Deleting Backup Files

Procedure

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

Configuring Global Parameters

The global parameter applies to all devices connected to the device management platform. Note that when the device is connected to the management platform for the first time, they will automatically update the parameters.

Procedure

1. Click **Device Configuration** > **Global Parameters**.
2. Configure the global parameters in the corresponding field.
3. Click **Save**.

   You can also click **Save and update,** and click **OK** to update the global parameters to all devices.

Updating the Configuration

You can update the configuration by downloading the latest configuration file from Yealink official website. If the configuration is updated, the parameters in the template will be updated synchronously. You can download the latest configuration file from: *http://support.yealink.com/documentFront/forwardToDocumentDetailPage?documentId=242*.

Procedure

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

   Only the .xls file format is supported and the size should be no more than 2M.
3. Click **Upload**.

Managing Tasks

You can create timer tasks and manage them. You can also view the task operational log, and if an exceptional situation occurs, you can troubleshoot or retry the task.

- *Timer Tasks and Task Rules*
- *Adding Timer Tasks*
- *Editing Timer Tasks*
- *Pausing or Resuming Timer Tasks*
- *Ending Timer Tasks*
- *Searching for Timer Tasks*
- *Viewing Timer Tasks*
- *Viewing Tasks*
- *Retrying Tasks*

- *Searching for Executed Tasks*

Timer Tasks and Task Rules

When creating a timer task, you can choose the task type and the execution period. For example, you don't want to update the firmware or the configuration during the office hour, because the firmware or the configuration update process will cause the device to reboot, making it unable for users to use the device normally. Therefore, you can set up a timer task to control the device to perform the one-time task during non-office hour.

The rules of pushing timer tasks are as follows:

Task	Rules
Push resource file	You can only push one file of the same resource type at a time. Only the resource file supported by the device can be pushed.
Update firmware	If you select the devices of different models, only the firmware applicable to all the devices can be updated.
Update config File	If you select Update CFG by the model template, the device will update the configuration of the corresponding model template. If the corresponding model temple does not exist, no push is performed. If you select Update CFG by factory defaults, the device will update the system default configuration.
DND/cancel DND	DND/Cancel DND is enabled for all registered accounts on the device.
Push global parameters	/
Send message	/
Reboot/Reset to factory	/

Adding Timer Tasks

Procedure

1. Click **Task Management** > **Timer Task**.
2. In the top-right corner, click **Add Timer Task**.
3. Select the desired devices.
4. Configure the name, select the content, the period and the executive time in the corresponding field.
5. Click **Save**.

Editing Timer Tasks

You can only edit the timer tasks which is to be executed or suspending.

Procedure

1. Click **Task Management** > **Timer Task**.

2. Click ✎ beside the desired task.
3. Select the desired devices in the list.
4. Edit the timer task information in the corresponding field.
5. Click **Save**.

Pausing or Resuming Timer Tasks

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

Procedure

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

Ending Timer Tasks

You can end timer tasks in the status of to be Executed, Suspending or Executing. If you end the Executing timer task, the task can still be executed until it is finished. If you end the periodic timer task, they will no longer be executed.

Procedure

1. Click **Task Management** > **Timer Task**.
2. Click ⏹ beside the desired task.

Searching for Timer Tasks

You can search for timer tasks by directly entering the related information or according to the execution result.

Procedure

1. Click **Task Management** > **Timer Task**.
2. Do one of the following:
    - Enter the task name in the search box, and press Enter to perform the search.
    - Click **More**, select a desired execution result, and click **Search**.

    The search results are displayed in the timer task list.

Viewing Timer Tasks

Procedure

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

Viewing Tasks

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

Procedure

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

Retrying Tasks

Procedure

1. Click **Task Management** > **Executed Task**.
2. Click ⓘ beside the desired resource.
3. Select the exceptional devices, and then click **Retry** to re-execute the task.

Searching for Executed Tasks

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

Procedure

1. Click **Task Management** > **Executed Task**.
2. Enter the task name in the search box, and press Enter to perform the search.

   You can also search for an executed task by selecting the start time and the end time.

   The search results are displayed in the executed task list.

Monitoring Devices

You can view the call quality of the devices for QoE analysis and solve the problems by viewing the alarm.

Note: The call quality and the device alarm are advanced features, not supported by the basic package. If you want to use the advanced features, you can *Trying Advanced Features* or contact your distributor/reseller to subscribe to the advanced package. You can view the details of the subscribed package on the page of *Managing Orders*.

- *Viewing Call Quality Statistics*
- *Managing Alarm*

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: Uploading the call statistics to the device management platform is not supported by the Teams phone, so you are not available to view the call quality of the Teams phone.

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

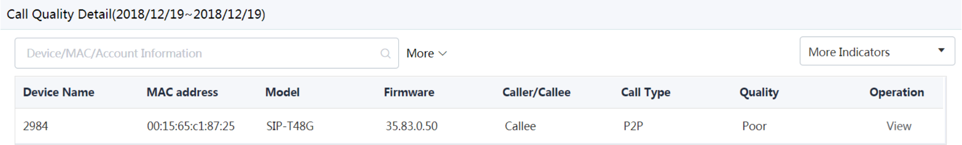
Customizing the Indicators of Call Quality Detail

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

Procedure

1. Click **Dashboard** > **Call Statistics**.
2. Click **More indicators**.
3. Select the desired indicators.
4. Click **Submit**.

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



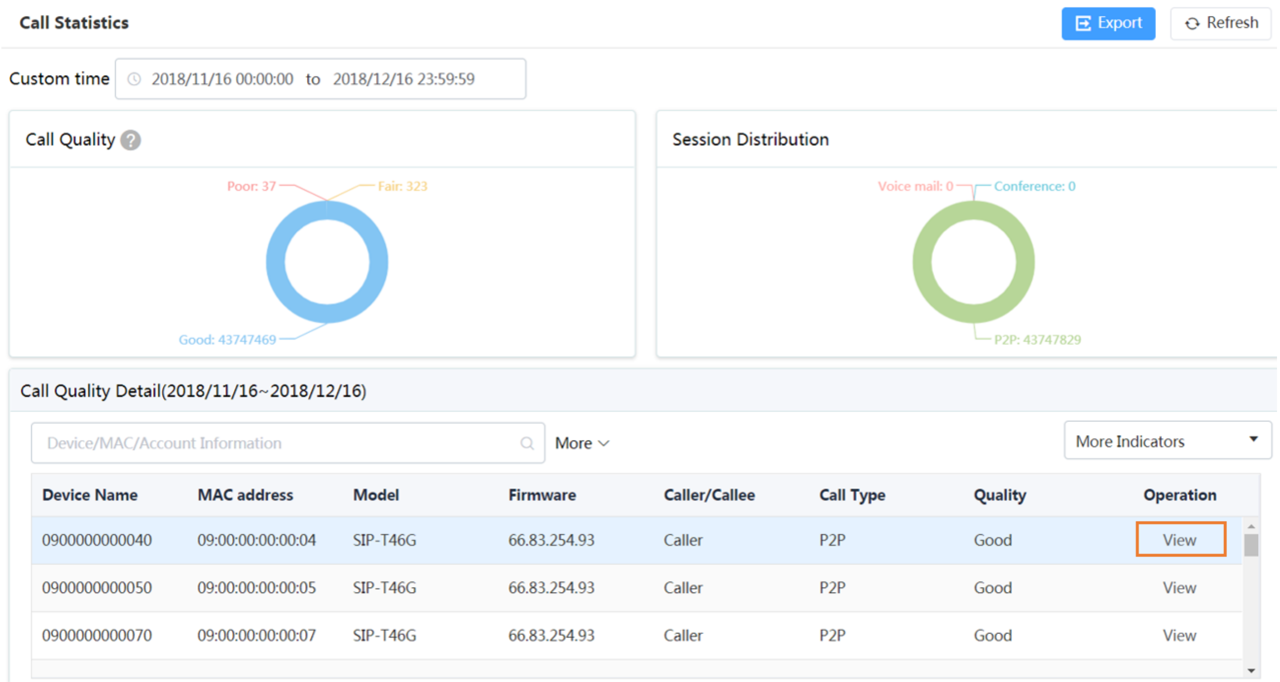
Call Quality Detail(2018/12/19~2018/12/19)

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

Procedure

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



Call Statistics

Custom time 2018/11/16 00:00:00 to 2018/12/16 23:59:59

Call Quality

Session Distribution

Call Quality Detail(2018/11/16~2018/12/16)

Device Name	MAC address	Model	Firmware	Caller/Callee	Call Type	Quality	Operation
0900000000040	09:00:00:00:00:04	SIP-T46G	66.83.254.93	Caller	P2P	Good	View
0900000000050	09:00:00:00:00:05	SIP-T46G	66.83.254.93	Caller	P2P	Good	View
0900000000070	09:00:00:00:00:07	SIP-T46G	66.83.254.93	Caller	P2P	Good	View

Managing Alarm

When the devices are abnormal, they will send alarm to the platform so that you can detect and solve problems such as network or server problems in time. You can manage the alarm strategies and choose to view the alarm via email or on the management platform.

- *Adding Alarm Strategies*
- *Editing Alarm Strategies*
- *Deleting Alarm Strategies*
- *Viewing Alarms*
- *Deleting Alarm*

Adding Alarm Strategies

Procedure

1. Click **Alarm Management** > **Alarm Strategy**.
2. Click **Add Strategy**.
3. Enter the strategy name.
4. Select the desired alarm severity.
5. Click ⚙ to add the alarm receiver, and click **OK**.
6. Enable the alarm strategy.
7. Click **Save**.

Related concepts

Appendix: Alarm Types

Editing Alarm Strategies

Procedure

1. Click **Alarm Management** > **Alarm Strategy**.
2. Click ✎ beside the desired alarm.
3. Edit the related information of the alarm strategy.
4. Click **Save**.

Deleting Alarm Strategies

Procedure

1. Click **Alarm Management** > **Alarm Strategy**.
2. Click 🗑 beside the desired alarm strategy.
3. Click **OK** according to the prompts.

Viewing Alarms

When a problem 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.

Before you begin

The in-site alarm reminder is enabled, and the alarm recipient is the login account.

Procedure

1. Click **Alarm Management** > **Alarm List**.
2. Click ⓘ beside the desired alarm.

   You can view the alarm information, including the latest reporting time, the times and the detailed information.

Related concepts

Appendix: Alarm Types

Managing Alarm

Deleting Alarm

Procedure

1. Click **Alarm Management** > **Alarm List**.
2. Select the desired alarm.
3. Click **Delete**.
4. Click **OK** according to the prompts.

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 the device management platform before being diagnosed.

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

- *Going to the Device Diagnostics Page*
- *Setting the Device Logs*
- *Capturing Packets*
- *Diagnosing the Network*
- *Exporting Syslogs*
- *Exporting Backup Files*
- *Viewing the CPU and the Memory Status*
- *Viewing Recordings*
- *Capturing the Screenshot of the Device*

Going to the Device Diagnostics Page

Do one of the following:

- Click **Device Management**->**Device list**, and then click ⊞ beside the desired device.
- Click **Device Diagnostic**, enter the MAC address or the IP address of the desired device, and then click **Start Diagnostic**.

Setting the Device Logs

You can enable the Log Data Backup feature, and the device will send the system log to the device management platform. You can set the log level, view or download the current backup file. You can also set the module log, save the log to the local computer, export the log to the USB flash drive, upload the log to a log server, or put the log backup to a specified server.

Note that this section is only available for the video conferencing system, version XX.32.0.35 or later (XX represents the fixed number of each device model).

- *Setting the Log Level*
- *Setting the Module Log*
- *Setting the Local Log*
- *Setting the Syslog*
- *Putting the Log Backups to a Specified Server*
- *Enabling the Log Data Backup*
- *Downloading the Backup Log*

Setting the Log Level

Procedure

1. Go to the device diagnostics page.
2. Click **Log Level**.

3. Enter the desired value.
4. Click **Confirm**.

Setting the Module Log

You can set module log type and the log level for the device. The module log includes all, the driver, the system, the service, the connectivity, the audio & video, the protocol, the deploy, the web, the app and the talk.

Procedure

1. Go to the device diagnostics page.
2. Click **Log Settings**.
3. In the **Module Log** field, select the log type and the level.
4. Click **Save**.

Setting the Local Log

You can enable the Local Log feature, configure the local log level and the maximum size of the log file, and enable the USB Auto Exporting Syslog feature to export the local log to the USB flash drive connected to the device.

Before you begin

Note: The module log level is smaller than the local log level. For example, if you set the log level of the hardware drive as 6 and the local log level as 3, the exported log level of the hardware drive is 3.

Procedure

1. Go to the device diagnostics page.
2. Click **Log Settings**.
3. In the **Local Log** field, enable **Local Log**.
4. Enable **USB Auto Exporting Syslog**.
5. Select the local log level and the log file size.
6. Click **Save**.

Setting the Syslog

You can upload the log generated by the device to a log server.

Before you begin

Note: The module log level is smaller than the syslog level. For example, if you set the log level of the hardware drive as 6 and the syslog level as 3, the exported log level of the hardware driver is 3.

Procedure

1. Go to the device diagnostics page.
2. Click **Log Settings**.
3. In the **Syslog** field, enable **Syslog**.
4. Configure the syslog server and the port.
5. Select the syslog transport type and the syslog level.
6. Select the syslog facility, which is the application module that generates the log.
7. Enable **Syslog Prepend MAC**, and configure the MAC address come with the device in the uploaded log file.
8. Click **Save**.

Putting the Log Backups to a Specified Server

You can make backups for the device log and put the backups to a specified server.

Procedure

1. Go to the device diagnostics page.
2. Click **Log Settings**.
3. In the **Other Log Settings** field, enable **Log File Backup**.
4. Enter the address, the user name and the password of the specified server.
5. Select the desired HTTP method and the POST mode.
6. Click **Save**.

Enabling the Log Data Backup

After you enable this feature, the device management platform will make a log backup every day, and only save the log generated in the past 7 days.

Procedure

1. Go to the device diagnostics page.
2. Click **Log Settings**.
3. In the **Other Log Settings** field, enable **Log Data Backup**.
4. Click **Save**.

Downloading the Backup Log

If you enable the Log Data Backup feature, you can download the log saved by the device management platform.

Procedure

1. Go to the device diagnostics page.
2. On the right side of the corresponding log, click **Download Log**.

   You can select multiple logs, and click **Batch Download**.

Related tasks

Enabling the Log Data Backup

Capturing Packets

Procedure

1. Go to the device diagnostics page.
2. Click **Packetcapture**.
3. Select the desired Ethernet and type, and then enter the string.
4. Click **Start** to begin capturing the signal traffic.
5. Click **Finish** to stop capturing, and the file is generated automatically.
6. 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.

Procedure

1. Go to the device diagnostics page.
2. Click **Network detection** in the **Diagnostic Tools** filed.
3. Select Ping (ICMP Echo) or Trace route.
4. Enter the IP address.

   The IP address of the device management platform is default.
5. Select the desired value from the drop-down menu of Request times.
6. Click **OK** to start.

Exporting Syslogs

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

Procedure

1. Go to the device diagnostics page.
2. Click **Export System Log** in the **Diagnostic Tools** filed.
3. Save the file to your local computer.

Exporting Backup Files

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

Procedure

1. Go to the device diagnostics page.
2. Click **Export Config File** in the **Diagnostic Tools** filed.
3. Select the file type.

   If you select cfg, you can choose to export static settings, non-static settings or all settings.
4. Click **Export**, and then save the file to your local computer.

Viewing the CPU and the Memory Status

The device will report its CPU and memory information to the device management platform at a regular time, so you can update the information and view the latest information. You can also view the memory information by copying it to Microsoft Word.

Procedure

1. Go to the device diagnostics page.
2. Click **CPU Memory Status** in the **Diagnostic Tools** filed.
3. Do one of the following:
   - Click **CPU** to view the CPU usage.
   - Click **Memory** to view the memory usage.

Viewing Recordings

Procedure

1. Go to the device diagnostics page.
2. Click **Recording file**.

   You can select the **Automatic upload recording file** checkbox to enable the automatic uploading, so that the recording file will be uploaded to the platform automatically.

   You can also click 📥 to download the recording.

Capturing the Screenshot of the Device

Procedure

1. Go to the device diagnostics page.
2. Click **Screencapture**.

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

Managing System

- *Obtaining the Accesskey*
- *Viewing Operation Logs*
- *Configuring the SMTP Mailbox*

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 more information, refer to *API for Yealink Device Management Platform*.

Procedure

1. Click **System Management** > **AccessKey**.
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.

Viewing Operation Logs

Operation logs record the operation performed by the administrator or the authorized superior on the device management. You can view the operation log.

Procedure

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

Tip: You can search for the operation log by selecting the start time, the end time, the username, the IP address, the operation type or the path.

Configuring the SMTP Mailbox

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

About this task

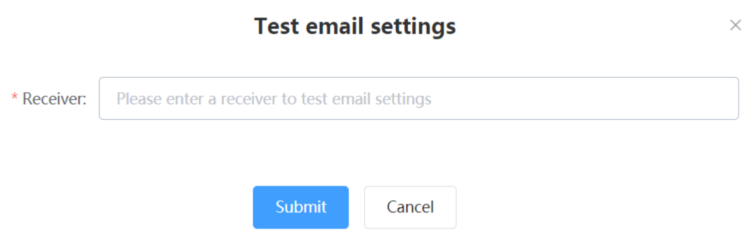
The SMTP mailbox is used to send the alarm emails and the account information to administrators.

The parameters for SMTP mailbox setting are described below:

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 the secure connection.	Enables or disables the secure connection: SSL or TLS (default)
Enable the mailbox	Enables or disables the mailbox.

Procedure

1. Click **System Management** > **Mailbox Settings**.
2. Configure the parameters.
3. Optional: click **Test email settings**.



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

4. Click **Save**.

Troubleshooting

This chapter helps you solve the problems you might encounter when using YDMP.

- *General Issues*

General Issues

This chapter lists the general issues and its solution. If the case you encounter is not listed in this section, contact your Yealink reseller or technical support engineer for further support.

- *Forgetting the Login Password*
- *Why You Cannot Access the Login Page*
- *Why It Prompts There Is an Insecure Connection (Certificate Security Issue) When Accessing the Login Page?*

Forgetting the Login Password

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

Procedure

1. On the Login page, click **Forget Password**.
2. Enter your email and the captcha in the corresponding field.
3. Click **OK**.
4. Click **OK** according to the prompts.
5. After you receive the email for resetting the password, click the resetting link in 10 minutes to reset the password.

Why You Cannot Access the Login Page

Server:

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

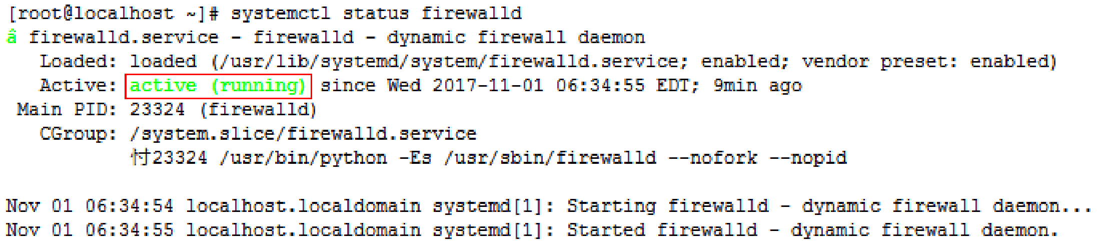
Windows:

- Run Network Diagnostics of Window.

Check your server and the firewall.

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

- systemctl status firewalld



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

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

- If the firewall is active, 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, refresh the login page, you can access the login page successfully.

Why It Prompts There Is an Insecure Connection (Certificate Security Issue) When Accessing 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 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.
4. In the following, “serverdm” is the certificate file name you want to replace.

Solution:

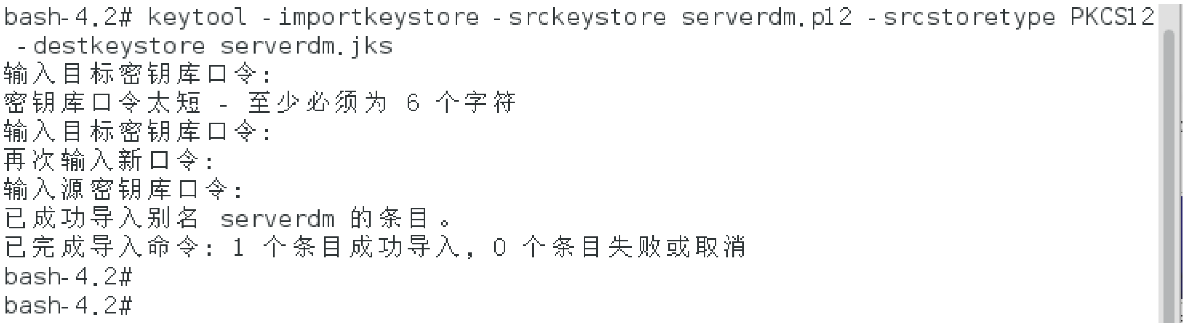
1. Open the terminal and enter the directory where you put the certificate file.
2. Generate dm.12 file, run the command:

   openssl pkcs12 -export -in serverdm.crt -inkey dm.key -out serverdm.p12 -name serverdm

   It will prompt you to enter and verify the export password. You need to remember this password.
3. Generate Keystore file (jks file), run the command:

   keytool -importkeystore -srckeystore serverdm.p12 -srcstoretype PKCS12 -destkeystore serverdm.jks

   It will prompt you to enter the target key, and then enter the export password you set in step 2. Note that you the target key should be the same as the key you set in step 2.

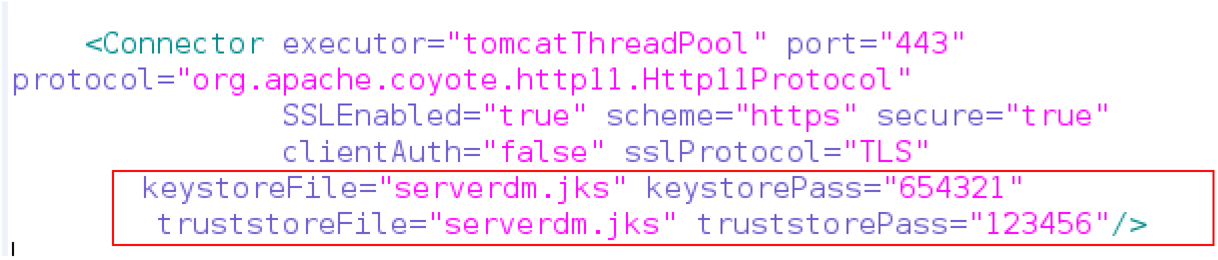


```
bash-4.2# keytool -importkeystore -srckeystore serverdm.p12 -srcstoretype PKCS12
 -destkeystore serverdm.jks
输入目标密钥库口令：
密钥库口令太短 - 至少必须为 6 个字符
输入目标密钥库口令：
再次输入新口令：
输入源密钥库口令：
已成功导入别名 serverdm 的条目。
已完成导入命令：1 个条目成功导入，0 个条目失败或取消
bash-4.2#
bash-4.2#
```

4. Replace /usr/local/yealink/dm/tomcat_dm/dm.jks with the serverdm.jsk.
5. Change the keystore password you set at the path of /usr/loca/yealink/dm/tomcat_dm/conf/server.xml.

Suppose that 654321 is your keystore password.

Reboot the server and the certificate will take effect.



```
    <Connector executor="tomcatThreadPool" port="443"
protocol="org.apache.coyote.http11.Http11Protocol"
                SSLEnabled="true" scheme="https" secure="true"
                clientAuth="false" sslProtocol="TLS"
        keystoreFile="serverdm.jks" keystorePass="654321"
         truststoreFile="serverdm.jks" truststorePass="123456"/>
```

Appendix: Alarm Types

Alarm type	Severity
Poor quality call	Critical
Registration failure	Critical
Upgrade firmware failure	Critical
Update configuration failure	Critical
Application crash	Critical
Application no response	Critical
Kernel panic	Critical
Visual voicemail retrieve failure	Minor
Hold failure	Minor
Resume failure	Minor
Play visual voicemail failure	Minor
RTP violate	Minor
RTP address change	Minor
RTP dead	Minor
SRTP failure	Minor
Calendar synchronization failure	Minor
Calllog retrieve failure	Minor
Outlook contact retrieve failure	Minor
Call failed	Minor
Bluetooth paired failed	Major
BToE pairing failure	Major
Exchange discovery failure	Major
Exit program	Major