Yealink

Yealink Device Management Platform Administrator Guide

Version 3.1.0.14

Jan.2019

Copyright

Trademarks

Yealink®, the logo and the name and marks is trademark of Yealink (Xiamen) Network Technology CO., LTD, which are registered legally in China, the United States, EU (European Union) and other countries.

All other trademarks belong to their respective owners. Without Yealink's express written permission, recipient shall not reproduce or transmit any portion hereof in any form or by any means, with any purpose other than personal use.

Warranty

(1) **Warranty**

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS GUIDE ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS GUIDE ARE BELIEVED TO BE ACCURATE AND PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF PRODUCTS.

(2) **Disclaimer**

YEALINK (XIAMEN) NETWORK TECHNOLOGY CO., LTD. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS GUIDE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Yealink (Xiamen) Network Technology CO., LTD. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance, or use of this guide.

(3) **Limitation of Liability**

Yealink and/or its respective suppliers are not responsible for the suitability of the information contained in this document for any reason. The information is provided "as is", and Yealink does not provide any warranty and is subject to change without notice. All risks other than risks caused by use of the information are borne by the recipient. In no event, even if Yealink has been suggested the occurrence of damages that are direct, consequential, incidental, special, punitive or whatsoever (Including but not limited to loss of business profit, business interruption or loss of business information), shall not be liable for these damages.

End User License Agreement

This End User License Agreement ("EULA") is a legal agreement between you and Yealink. By installing, copying or otherwise using the Products, you: (1) agree to be bounded by the terms of this EULA, (2) you are the owner or an authorized user of the device, and (3) you represent and warrant that you have the right, authority and capacity to enter into this agreement and to abide by all its terms and conditions, just as if you had signed it. The EULA for this product is available on the Yealink Support page for the product.

Patent Information

China, the United States, EU (European Union) and other countries are protecting one or more patents of accompanying products and/or patents being applied by Yealink.

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to 1.

Technical Support

Visit Yealink WIKI (*http://support.yealink.com/*) for the latest firmware, guides, FAQ, Product documents, and more. For better service, we sincerely recommend you to use Yealink Ticketing system (*https://ticket.yealink.com*) to submit all your technical issues.

About This Guide

Yealink device management platform allows administrators to efficiently realize centralized management for Yealink IP phones, Skype for Business HD T4XS IP phones and VCS Video Conference Systems in the same enterprise.

This guide provides operations for administrators to use the Yealink device management platform. The system administrators can add sub-administrators to use the Yealink device management platform to manage a series of devices.

Related Documentations

For more information about the series of devices Yealink, view the following related documents:

- Quick Start Guides, which describes how to assemble devices and configure the most basic features available on devices.
- User Guides, which describes the basic and advanced features available on devices.
- Administrator Guide, which describes how to properly configure, customize, manage, and troubleshoot the devices
- Auto Provisioning Guide, which describes how to provision devices using the configuration 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.
- Description of Configuration Parameters in CFG Files, which describes all configuration parameters in configuration files.

  Note that Yealink administrator guide contains most parameters. If you want to find out more parameters which are not listed in this guide, please refer to Description of Configuration Parameters in CFG Files guide.

For support or service, please contact your Yealink reseller or go to Yealink Technical Support online: *http://support.yealink.com/*.

In This Guide

Topics provided in this guide include:

- Chapter 4 Managing Administrator Accounts
- Chapter 5 Managing Sites
- Chapter 6 Managing Device Accounts
- Chapter 7 Managing Devices
- Chapter 8 Managing Device Configuration
- Chapter 9 Managing Tasks
- Chapter 10 Monitoring and Managing the Devices
- Chapter 11 Diagnosing Devices
- Chapter 12 Troubleshooting
- Chapter 13 Appendix: Alarm Types

Summary of Changes

Changes for Release 31, Version 3.1.0.14

The following section is new for this version:

- Restoring Yealink Device Management Platform (from V3.1 to V2.0)
- Disk Allocation Plan

Changes for Release 31, Version 3.1.0.13

The following section is new for this version:

- Activating the License

Major updates have occurred to the following section:

- Getting Started
- Deploying Yealink Device Management Platform
- Deploying Devices
- Managing Administrator Accounts
- Managing Device Accounts
- Managing Devices
- Updating the Device Firmware
- Pushing Resource Files to Devices

- Diagnosing Devices

Table of Contents

Getting Started

This chapter introduces the requirements of Yealink device management platform.

Topics include:

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

Hardware and Software Requirements

Server operating system: Linux CentOS 7.0 or later.

Device Quantity	CPU	RAM	Hard Drive
0~6000	8-core	16G	There should be at least 200G partition used for installing the device management platform (for more information about disk allocation, refer to Disk Allocation Plan), 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	

Disk Allocation Plan

You can allocate the disk when you meet the following situations:

- When you fail to upgrade the device management platform to V3.1
- When you restore the device management platform to V2.0
- When you create 3 primary partitions

Procedure

1. Log into CentOS as the root user, open the terminal.
2. Run the command below to close the services that may not be closed:

```
systemctl stop microdm
systemctl stop microtcp
systemctl stop microuser
systemctl stop dbc
systemctl stop redis
systemctl stop rocketmq-broker
systemctl stop rocketmq-namesvr
systemctl stop smserver
```

3. Run the command below to close the corresponding services of version 2.0:

```
systemctl stop tomcat_dm
systemctl stop mariadb
systemctl stop tcp-server
systemctl stop rabbitmq-server
systemctl stop redis
```

4. Run the command (the red font parts) below to create partitions. The example command below is only for reference. The specific data should be based on the real environment. **Do operate with caution, otherwise the data may be lost.**

```
[root@localhost ~]fdisk /dev/sdb              # operate according to the real device name, which can be viewed via lsblk
Command (m for help): n     #create a partition
Partition type:
   p     primary (3 primary, 0 extended, 1 free)
   e     extended
Select (default e): e          #create an extended partition
Selected partition: 4          #the extension number
First sector (125831168-419430399, default 125831168):          # press Enter to select the default value
Last sector, +sectors or +size{K,M,G} (125831168-419430399, default 419430399): +100G
#the size of the extended partition is increased by 100G
Command (m for help): n     #create a logical partition
Partition type:
   p     primary (2 primary, 1 extended, 1 free)
   l     logical (number from 5)
Select (default p): l               #the extension number is 5
First sector (125833216-335546367, default 125833216):        #press Enter to select the default value
Last sector, +sectors or +size{K,M,G} (125833216-335546367, default 335546367):
#press Enter to select allocating all the extended partition space by default
Command (m for help): p     #print the information of the extended partition
Command (m for help): wq      #save and exit
```

5. Format and mount the new partitions, for example, if the new partition name is /dev/sda5, run the command is as below:

```
mkfs.xfs /dev/sda5
mount /dev/sda5 /mnt          #make sure that there is nothing under /mnt
```

6. Migrate the old data.

```
cp -rp /usr/local/yealink/* /mnt
```

7. Run the command *ls /mnt* to check whether the data migration is completed. If the migration is completed, run the command below:

```
rm -rf /usr/local/yealink/*
```

8. Uninstall and mount the new partitions.

```
umount /mnt
mount /dev/sda5 /usr/local/yealink
```

9. Start the device management platform V2.0.

```
systemctl start tomcat_dm
systemctl start mariadb
systemctl start tcp-server
systemctl start rabbitmq-server
systemctl start redis
```

10. If you fail to start the database, it may be caused by the denied permission in the log. If the permission is changed from mysql to root, run the command below:

```
chown mysql.mysql /usr/local/yealink/commom/mariadb/*   -R
```

11. If you still fail to start the database, you can view the database log.

```
tail -f -n 100 /var/log/yealink/common/mariadb/mariadb.log
```

12. If it prompts "Can't init tc log", run the command below:

```
mv ib_logfile* /usr/local/
mv tc.log /usr/local/
systemctl restart mariadb
```

13. If you can start the database, you can upgrade the device management platform from V2 to V3 (refer to Updating Yealink Device Management Platform (from V2.0 to V3.1)).

14. Start and mount the device management platform.

```
blkid   | grep /dev/sda5          #view the UUID of /dev/sda5
/dev/sdb1: UUID="dd1ad555-6d19-4eb5-a210-b5379501a64b" TYPE="xfs"
#the returned UUID
echo "UUID=dd1ad555-6d19-4eb5-a210-b5379501a64b
/usr/local/yealink xfs defaults 0 0" >>/etc/fstab
```

Port Requirements

You should open four ports for the device management platform: 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.
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

Browser	Version
Firebox	50 and later
Chrome	50 and later
360	8.1 and later
Internet Explorer	10 and later

The Supported Device Models

You can manage the following devices via Yealink Device Management Platform.

Device Type	Device Model	Version Requirements
SIP IP Phones	SIP-T19(P)E2/T21(P)E2/T23P/T23G/T27P/T27G/T29G/T40P/T40G/T41P/T41S/T42G/T42S/T46G/T46S/T48G/T48S/T52S/T54S	XX.83.0.30 or later (except XX.84.0.10) XX represents the fixed number for each device model.
	SIP-T56A/T58	58.83.0.5 or later
	SIP-CP960	73.83.0.10 or later
	SIP-CP920	78.84.0.15 or later
Skype for Business phones	SFB-T41S/T42S/T46S/T48S	66.9.0.45 or later(except 66.9.0.46).
	SFB-T58(T56)	55.9.0.2 or later

Device Type	Device Model	Version Requirements
	SFB-CP960	73.8.0.27 or later
Video Conference Systems	VC200/VC500/VC800/VC880	XX.32.0.25 or later. XX represents a fixed number for each device model.

Deploying Yealink Device Management Platform

This chapter provides instructions on how to install and deployment Yealink Device Management Platform, and introduces its interface.

Topics include:

Updating Yealink Device Management Platform (from V2.0 to V3.1)

The following is an example of updating the device management platform from V2.0.0.14 to V3.1.0.13.

Before you begin

- Obtain the latest installation package of Yealink device management platform from the Yealink distributor or SE and then save it at the path **/usr/local**.
- Your hardware, software and ports meet the hardware and software requirements and port requirement.

Procedure

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

```
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.

The device management platform will be updated to the corresponding version if it is updated successfully.

Note Updating the version has no influence on the devices connected to the device management platform.

Restoring Yealink Device Management Platform (from V3.1 to V2.0)

Procedure

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

   ```
   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, the device management platform will be restored to version 2.0.

Note that if you enter the wrong password, do not restore the device management platform again, because it will cause all the data on device management platform be deleted. However, you can follow the steps below:

1. Run the command below:

   ```
   cd /usr/local/
   mv yealink yealink_bak          #it means making a data backup for version 2.0
   cd yealink_install/
   ./uninstall                    #it means uninstalling version 3.0
   ```

2. According to the prompts, enter the password “*Yealink1105*”.
3. According to the prompts, enter the “*Y*”to confirm to uninstall.
4. According to the prompts, enter the “*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 version 2.0
   ```

6. If the contents of the device management platform do not exist, run the command below:

```
cd /var/log/yealink/
mkdir dm
cd dm/
mkdir tomcat_dm
cd tomcat_dm/
touch catalina.out
```

7. Run the command below to start the corresponding services of version 2.0:

```
systemctl restart mariadb
systemctl restart redis
systemctl restart rabbitmq-server
systemctl restart tcp-server
systemctl restart tomcat_dm
```

The device management platform will be restored to version 2.0.

Installing Yealink Device Management Platform

Before you begin

- Your hardware, software and ports meet the hardware and software requirements and port requirements.
- One device running CentOS.
- Obtain the installation package of Yealink device management platform from the Yealink distributor or SE and then save it at the path **/usr/local**.

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

Procedure

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

```
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 prompts "Install Success!!!", the installation succeeds.

Logging into the Yealink Device Management Platform

Procedure

1. Open your web browser.

2. Enter https://<IP address>/ (for example: https://10.2.62.12/) in the address box, and then press the **Enter**.
3. Optional: select your desired language.
4. Enter your username (default: admin) and the password (default: v123456789), and click **Login**.
5. If you log into the platform for the first time, the system will remind you to change the password. After that, you can go to the homepage of the device management platform.

Logging out of the Yealink Device Management Platform

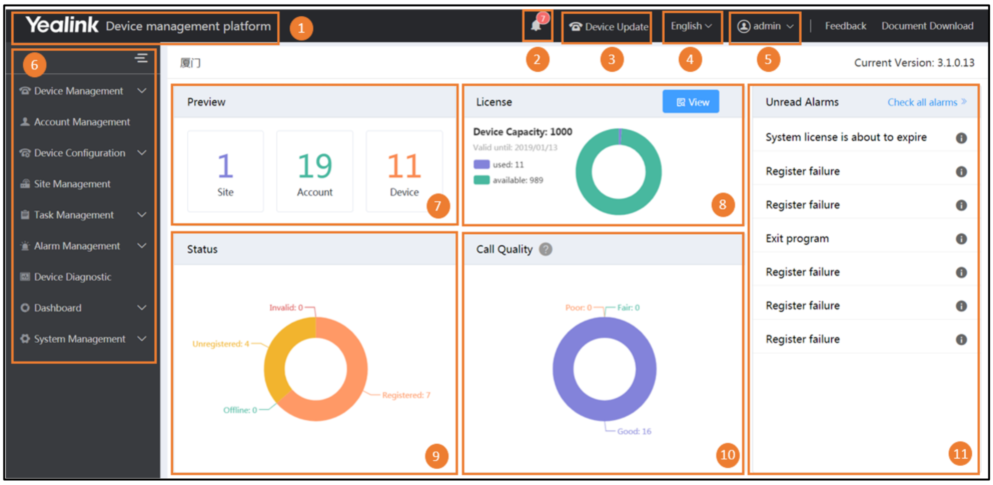
Procedure

1. 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.

The Home Page of Yealink Device Management Platform

After you log into the Yealink device management platform successfully, the home page is shown as below:

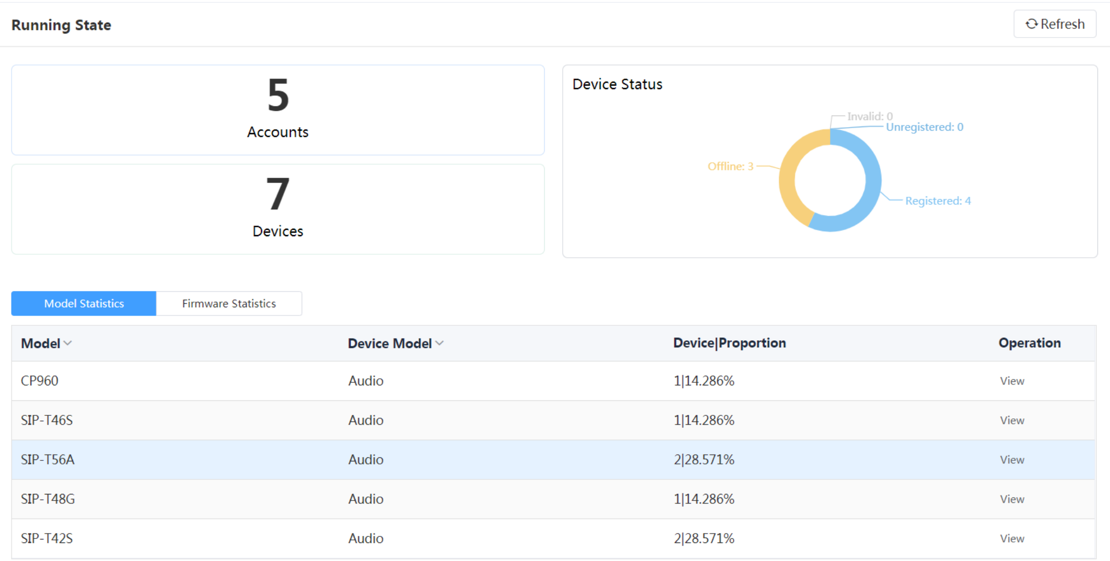


No.	Description
1	Go to the home page quickly when you are on other pages.
2	Display the number of unread alarms and the type of alarms.
3	Go to the Device list page quickly.
4	Change the display language.

No.	Description
5	Go to the page of setting administrator account.
6	Navigation pane.
7	**Data preview:** ● Displays the number of sites, accounts and devices. ● You can click the corresponding module to enter the module management page.
8	**License:** Display the current number of manageable devices.
9	**Device status:** ● Displays the number of unregistered, registered and offline devices. ● You can click the corresponding device status to enter all the device list page of this status.
10	**Call quality:** ● Displays the number of devices whose call quality are good, bad or poor. ● You can click the corresponding call quality module to view the call statistics page.
11	**Unread alarm:** ● Click **ALL>>** to go to Alarm List page. ● Hover your mouse on the icon ⓘ to view the detailed information of the alarm.

The Page of Running State

Click **Dashboard**->**Running State** to go to the running state page, and you can view the number of sites, accounts, devices and detailed analysis and statistics:



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, and you can manage the account directly.
- Click **Devices** to go to the Device List page, and you can manage the 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** on the right side of the corresponding device to go to the Device List page, and you can view the device information or update this device.
- Click **Firmware Statistics** to view all the running firmware.
- Click **View** on the right side of the corresponding firmware to go to the Device List page, and you can view the or update this firmware.

Activating the License

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

Procedures of activating the license: 1. Importing the device certificate; 2. Activating the license online or activating the license offline.

Importing the Device Certificate

You need to import a device certificate which is associated with this server only.

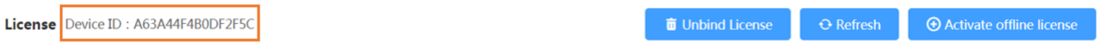
Before you begin

Obtain the device certificate from Yealink by submitting the enterprise name, the distributor name, the applicant and the country.

Procedure

1. Click **System Management**->**License**.
2. Import the corresponding certificate.

   If the association between the device ID and the server succeeds, the page is shown 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

- Import the device certificate.
- You purchase the corresponding service and obtain the authorization for device management.

Procedure

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

   The authorized license is displayed on the page.

Activating the License Offline

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

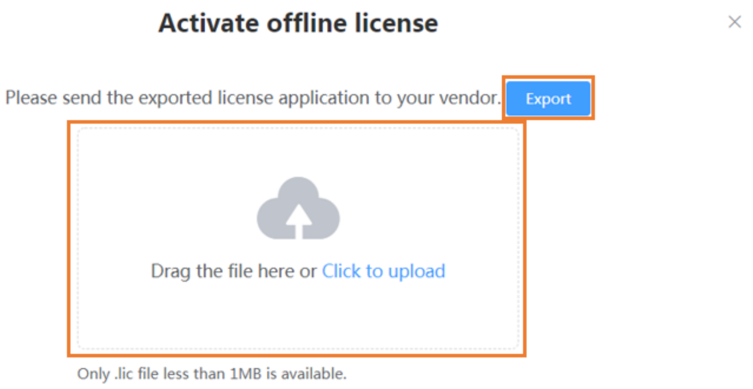
Before you begin

- Import the device certificate.
- You purchase the corresponding service and obtain the authorization for device management.

Procedure

1. Click **System Management**->**License**->**Activate offline license**.
2. Click **Export** and send the exported file to Yealink to get the license.

3. Upload the license.



Activate offline license

Please send the exported license application to your vendor. Export

Drag the file here or Click to upload

Only .lic file less than 1MB is available.

Uninstalling Yealink Device Management Platform

Procedure

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

   cd /usr/local/yealink_install

   ./uninstall

3. Enter the root password (Yealink1105) according to the prompts.

   The Yealink device management platform will be uninstalled from the CentOS.

Deploying Devices

Before you manage the devices via Yealink device management platform, you should deploy the devices.

Procedure

1. Use certificates for mutual TLS authentication.
2. Configuring common cfg file if there is a provisioning server you are using in your environment.
3. If there is not a 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)
   - Deploy devices on the RPS (Redirection & Provisioning Server) platform to configure server address.
   - Obtain the provisioning server address from phone flash to deploy a single phone.

   Note that the device should support the device management platform. If not, please upgrade the firmware first.

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

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 using default certificates.

Configuring Trusted Certificates

When a device requests an SSL connection with the platform, the device should verify that 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**.

   It is enabled by default.

The device will verify the platform certificate based on the trusted certificates list. Only when the authentication succeeds, will the device trust the platform.

Configuring Device Certificates

When the platform requests an SSL connection with a device, the device sends a 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**.

   Default Certificates is selected by default.

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

Configuring Common CFG File

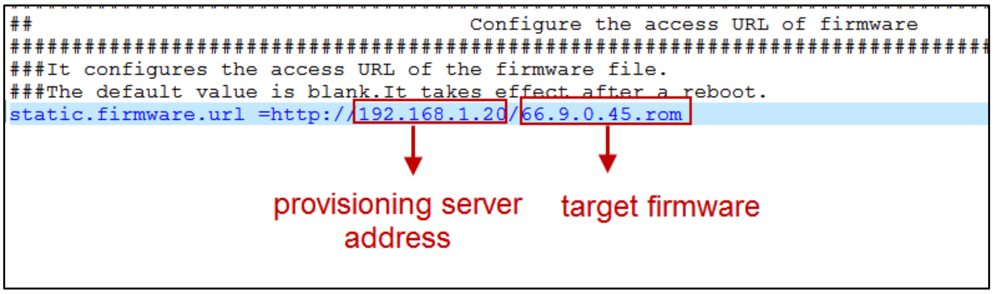
If the device does not support the device management platform, you need to upgrade the firmware before you connect the device to the device management platform. For easy deployment, you can configure the parameters of upgrading the firmware and the access URL of the device management platform in the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

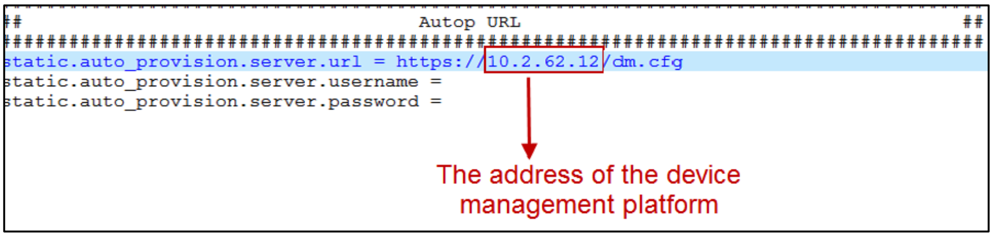
   Place the target firmware on your provisioning server, and then specify the access URL of the firmware.

Refer to About This Guide to check the required firmware version of the device.



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

3. Configure the 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 =
```

4. Save the file.

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

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

If you deploy the device through the RPS platform for the first time, after the devices are powered on and connected into the network, the RPS platform pushes the device management platform address 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.

   The server URL must meet the following format:

   https://<IP address>/dm.cfg (for example: https://10.2.62.12/dm.cfg).

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

Note For more information on how to use the RPS management platform, refer to *Yealink_Device_Management_Cloud_Service_for_RPS_Admin_Guide*.

Obtaining the Provisioning Server Address from Phone Flash

The devices can obtain the provisioning server address from the phone flash. To obtain the provisioning server address by reading the phone flash, make sure the configuration is set properly.

Procedure

1. Log into the web user interface of the device.
2. Click **Settings**->**Auto Provision**.
3. Enter the URL the provisioning server 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** to trigger the device to connect to the platform immediately.

Managing Administrator Accounts

This chapter provides basic instructions on Yealink device management platform.

Topics include:

- Changing Login Password
- Editing the Administrator Account
- Managing Sub-Administrator

Changing Login Password

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**.
3. Enter the current password, and enter the new password twice.
4. Click **Confirm**.

Editing the Administrator Account

You can edit the company name, the phone number, the email address and the office address of your account.

If you are an administrator, the email 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. Configure the account information in the corresponding field.
3. Click **Save**.

Managing Sub-Administrator Accounts

The system administrator can add sub-administrator accounts as needed to assign different function permissions to the sub-administrators. Therefore, the sub-administrators can manage the devices according to their function permissions.

The system administrator can add, edit, search for and delete sub-administrator accounts.

Adding Sub-Administrator Accounts

Procedure

1. Click **System Management**->**Sub account management**.
2. In the top-right corner of the page, click **Add sub account**.
3. Configure the user name, the phone number, and the email.
4. In the **Function List** field, select the corresponding permission for this sub-administrator.
5. Click **Save**.

   If you enable SMTP mailbox, the account information will be sent to the sub-administrator's mailbox automatically.

Related topics

Configuring the SMTP Mailbox

Deleting Sub-Administrator Accounts

Procedure

1. Click **System Management**->**Sub account management**.
2. On the left side of the page, select a desired sub-administrator from the **Username** list.
3. Click **Delete**.

   It prompts whether or not you are sure to delete it.
4. Click **Confirm**.

Resetting the Passwords of the Sub-Administrator Accounts

If a sub-administrator forgets the password, you can reset it.

Procedure

1. Click **System Management**->**Sub account management**.
2. On the left of the page, select a desired sub-administrator from the **Username** list.
3. Click **Reset password**.
4. Click **Save**.

   If you enable SMTP mailbox, the reset password will be sent to the sub-administrator's mailbox.

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. You can add, edit, search and delete sites.

Topics include:

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

Adding Sites

Procedure

1. Click **Site Management**.
2. In the top-right corner of the page, click **Add Site**.
3. Enter name and select a desired parent site.
4. Optional: enter the site description.
5. Click **Save**.

   You can also click **Save and Add** to save the change and continue to add sites.

Importing Sites

You can import a file to add multiple sites quickly. You need to download the template, edit and then import it.

Procedure

1. Click Site Management.
2. In the top-right corner of the page, click **Import**.
3. Click **Download the template** to download a blank .xls file.
4. Edit the template and 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**.

Note Edit the template according to the note in the template.

Editing Sites

Procedure

1. Click **Site Management**.
2. Select a desired site from 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 the search.

   The search result is displayed in the Site Name list.

Deleting Sites

You can delete sites in the Site Name list, but you cannot delete the default site named after your company name.

Procedure

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

   It prompts whether or not you are sure to delete it.
4. Click **OK** to delete the site.

Related topics

Adding Sites

Adding Accounts

Note If there are accounts under the site, you cannot delete it.
If there are child sites under this site and there are no accounts under the child sites, the site and its child sites will be delete simultaneously.

Managing Device Accounts

You can manage different products on Yealink device management platform.

Different products may use different types of login accounts, so we divide the accounts into SFB account, SIP account, YMS account, Cloud account and H.323 account for better management.

Topics include:

- Adding Accounts
- Importing Accounts
- Editing Accounts
- Searching for Accounts
- Exporting Accounts
- Deleting Accounts

Adding Accounts

Procedure

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

Importing Accounts

You can import a file to add multiple accounts quickly. You need to download the template, edit and then import it.

Procedure

1. Click **Account Management**.
2. In the top-right corner of the page, click **Import Account**->**Import SFB account**/**Import SIP account**/**Import YMS account**/**Import CLOUD account**/**Import H.323 account**.
3. Click **Download the template** to download a blank .xls file.
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 Accounts

Procedure

1. Click **Account Management**.
2. Click ✎ on the right side of the desired account.
3. Edit the account information.
4. Click **Save**.

Searching for Accounts

Procedure

1. Click **Account Management**.
2. Enter the account information in the search box, and press Enter:

   The search result is displayed in the account list.

Exporting Accounts

You can export the basic information of all accounts. The exported files are sorted by the account types. You can view the account information you added in the files.

Procedure

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

Deleting Accounts

Procedure

1. Click **Account Management**.
2. Select the checkboxes of the desired accounts.
3. Click **OK** to delete the accounts.

Managing Devices

Yealink device management platform can manage up to 20000 devices. You can manage Yealink products by logging in to the device management platform as a system administrator or as a sub-administrator.

Topics include:

- Managing Devices
- Managing Firmware
- Managing Resource Files

Managing Devices

Adding Devices Manually

You can preconfigure the device information by adding devices.

Note that you need to deploy the device so that the device can be connected to the device management platform.

Procedure

1. Click **Device Management**->**Device List**.
2. In the top-right corner of the page, click **Add Devices**.
3. Configure the device name, the site, the model, and the MAC address in the corresponding filed.
4. Optional: click **Add**, select the desired account, and allocate it to the device.
5. Click **Save**.

   The device is displayed in the device list.

Related topics

Deploying Devices

Importing Devices

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

Note that you can import only the device without registered accounts, and you need to deploy the device so that the device can be connected to the device management platform.

Procedure

1. Click **Device Management**->**Device List**.
2. In the top-right corner of the page, click **Import**.
3. Click **Download the template** to download the template.
4. Edit the device information in the template and save the template to your computer.
5. Click **Click to upload** to import the file or drag the file to the specified field directly.
6. Click **Import** to import devices.

Note Edit the template according to the note in the template.

Related topics

Deploying Devices

Editing Devices Information

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

Procedure

1. Click **Device Management**->**Device List**.
2. Click ✎ on the right side of the desired account.
3. Edit the device name.
4. Click **Save**.

Exporting the Device Information

You can export the basic information of all devices. The device information includes the name, the MAC address, the model, the status, the IP address, the subnet mask, and the firmware version.

Procedure

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

Viewing the Device Information

You can view device name, the model, the MAC address, the status, the IP address, the firmware version, the site, and the report time.

Procedure

1. Click **Device management**->**Device list**.
2. Click the corresponding device status, and you can view the network information (the IP address, the subnet and the report time).

If the device is registered with an account, you can also view the registered account information.

3. Click 🔍 on the right side of the desired device to view more information.

Searching for Devices

You can search for devices by entering the basic device information, or you can filter the device site or the account status to perform the search.

Procedure

1. Click **Device Management**->**Device List**.
2. Do one of the following:
   - Search for a device directly:
     1) Enter the device name, the MAC address, the account information or the IP address in the search box.
     2) Press Enter to perform the search.
   - Search for a device by filtering:
     1) Click **More**, and then select the account status and the site.
     2) Click **Search**.

     The search result is displayed in the device list.

Allocating Accounts to Devices

You can allocate an account to the device, and the platform will push this account to the device.

Procedure

1. Click **Device Management**->**Device List**.
2. Click ✎ on the right side of the desired device.
3. Click **Add**, select the desired account, and allocate it to the device
4. Click **Save**.

   The allocated account information is pushed the devices.

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. Select the corresponding device.

3. Click **Site settings**.
4. Select the corresponding site and click **OK**.

Enabling/Disabling DND

If you do not want to be disturbed when having a break, you can enable DND, and disable DND during office hours. You can also enable the timing DND if you often need this kind of setting.

Procedure

1. Click **Device management**->**Device list**.
2. Select the checkboxes of the desired devices.
3. Click **More**, and then select **DND/Cancel DND** from the drop-down menu.
4. If you select a single device in step 2, select the corresponding account.
5. 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.
6. Click **OK**.

Sending Message to Devices

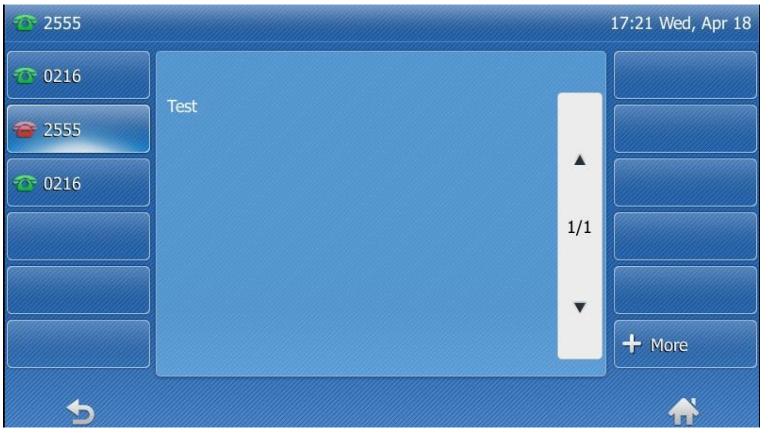
If you want to perform operations such as upgrading the device firmware and you want to inform the device user in advance, you can send the message to the device.

The device management platform supports sending messages to single or multiple devices.

Procedure

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

The message will be popped up on the device screen.



Test

(Take the T48S IP phone as an example)

Rebooting Devices

Procedure

1. Click **Device Management**->**Device List**.
2. Select the checkboxes of the desired devices.
3. Click **More**, and then select **Reboot** from the drop-down menu.
4. Select a desired execution mode:
   - If you select **At once**, the devices will reboot at once.
   - If you select **Timing**, configure the task name, the repeat type and the execution time.
5. Click **OK**.

Resetting the Devices to Factory

Procedure

1. Click **Device Management**->**Device List**.
2. Select the checkboxes of the desired devices.
3. Click **More**, and then select **Reset to factory** from the drop-down menu.
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,
5. Click **Confirm**.

   After reset to the factory, the device becomes offline. You need deploy the device again to connect the device to the device platform.

Related tasks

Deploying Devices

Deleting Devices

Procedure

1. Click **Device Management**->**Device List**.
2. Select the checkboxes of the desired devices.
3. Click **Delete**.

   It prompts whether or not you are sure to delete it.
4. Click **OK.**

Managing Firmware

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

Adding Firmware

Procedure

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

Search for Firmware

Procedure

1. Click **Device Management**->**Firmware Management**.
2. Enter the firmware name, the version or the description in the search box.
3. Press **Enter** to perform the search.

Updating the Device Firmware

When you need update the device firmware, you can push the new firmware to the device. When the enterprise is not convenient to update the firmware, you can set timing update.

Procedure

1. Click **Device Management**->**Firmware Management**.
2. Click ➦ on the right side of the desired firmware.
3. Select the checkboxes of the desired devices.
4. Click **Push to update**.
5. Select a desired execution mode:

   - If you select **At once**, the device firmware will be updated at once.

   - If you select **Timing**, configure the task name, the repeat type and the execution time.
6. Click **OK**.

   The new firmware will be applied to the device.

Note

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

Editing the Firmware Information

You can modify the firmware information such as the name, the version, the supported model and the description, or upload a new firmware to replace the old one.

Procedure

1. Click **Device Management**->**Firmware Management**.
2. Click ✎ on the right side of the desired firmware.
3. Edit the corresponding information.
4. Click **Save**.

Downloading the Firmware

Procedure

1. Click **Device Management**->**Firmware Management**.
2. Click ⬇ on the right side of the desired firmware to download it to your computer.

Deleting Firmware

Procedure

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

   It prompts whether or not you are sure to delete it.
4. Click **Confirm**.

Managing Resource Files

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

Adding Resource Files

Procedure

1. Click **Device Management**->**Resource Management**.
2. In the top-right corner of the page, click **Add resource**.
3. Configure the resource information in the corresponding filed.
4. Click **Click to upload** to upload the resource file.
5. 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. Press **Enter** to perform the search.

Pushing Resource Files to Devices

Procedure

1. Click **Device Management**->**Resource Management** to go to the Resource Management page.
2. Click ↗ on the right side of the desired resource.
3. Select the checkboxes of the desired devices.
4. Click **Push to Update**.
5. Select a desired execution mode:
   - If you select **At once**, the resource file will be updated at once.
   - If you select **Timing**, configure the task name, the repeat type and the execution time, and the resource file will be updated at a specified time.
6. Click **OK**.

   The current resource files of the devices will be updated.

Note 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. If a selected device does not support this resource file, the update will fail.

Editing Resource Files

You can modify the resource information or upload a new resource file.

Procedure

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

Downloading Resource Files

Procedure

1. Click **Device Management**->**Resource Management**.
2. Click ⬇ on the right side of the desired resource to download it to your computer.

Deleting Resource Files

Procedure

1. Click **Device Management**->**Resource Management**.
2. Select the checkboxes of the desired resource.
3. Click **Delete**.

   It prompts whether or not you are sure to delete it.
4. Click **OK**.

Managing Device Configuration

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

Topics include:

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

Managing Model Configuration

You can customize the configuration template according to the device model, that is, one template for one device model configuration. When you push the configuration, online devices (registered or unregistered) are updated in real time when they receive updates. Offline devices will be automatically updated them when they are connected to the platform.

Note that when the device of this model is connected to the management platform for the first time, its configuration template will be automatically updated.

Adding Configuration Templates

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

Procedure

1. Click **Device Configuration**->**Model Configuration**.
2. In the top-right corner of the page, click **Add Template**.
3. Enter the template name, select the device model, and add 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 parameters 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)

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 ••• on the right side of the desired template.
3. Select **Edit Parameters in text** from the drop-down menu.
4. Configure the parameters in the text.

   The parameter you enter can take effect only when they meet the format requirements.
5. Click **Save**.

   It prompts whether or not you want to update the configuration file immediately.
6. Click **Yes**, and push the updated parameters to the devices.

Setting Parameters in the Template (Model Configuration)

You can configure parameters supported by the device in the template.

Procedure

1. Click **Device Configuration**->**Model Configuration**.
2. Click ⚙ on the right side of the desired template.
3. Configure the corresponding parameters on the template.
4. Click **Save**.

   It prompts whether or not you want to update the configuration file immediately.
5. Click **No**, the parameter will be saved.

   You can also click **Yes** to push the updated parameters to the devices.

Pushing Configuration Parameters to Devices

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

Procedure

1. Click **Device Management**->**Model Configuration**.
2. Click ↗ on the right side of the desired template.
3. Select the checkboxes of the desired devices.

   You can select a desired site or enter the device information to search the device.

   The right side of the page displays the selected 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 parameters will be updated at a specified time.
6. Click **OK**.

   The current parameters of the devices will be updated.

Note 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 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 Configuration file

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

Procedure

1. Click **Device Configuration**->**Model Configuration**.
2. Click ••• on the right side of the desired template.
3. Select **Download config file** from the drop-down menu to save the file to your computer.

Viewing Parameters

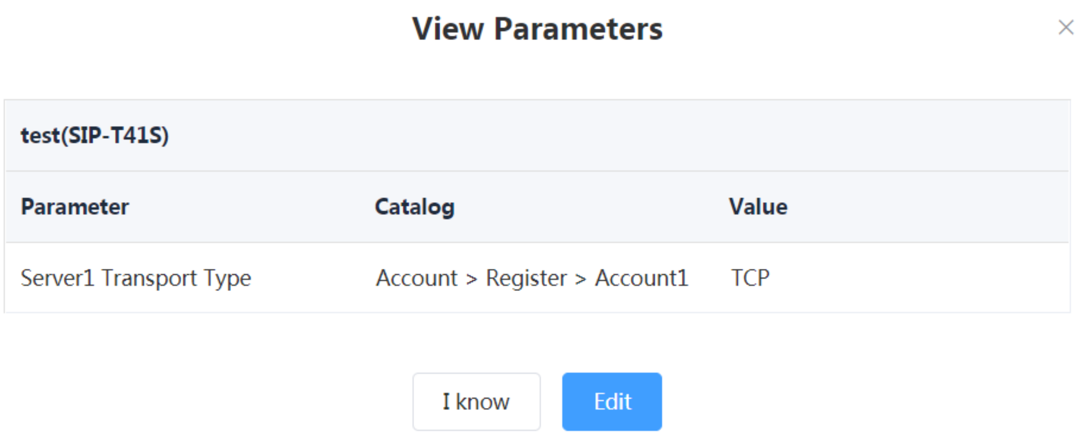
You can quickly view the parameter information to check them.

Note that you can only view the parameters in the configuration template.

Procedure

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

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



View Parameters

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

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

Related tasks

Setting Parameters

Deleting Templates

Procedure

1. Click **Device Management**->**Model Configuration**.
2. Select the checkboxes of the desired templates.
3. Click **Delete**.

   It prompts whether or not you are sure to delete it.
4. Click **OK**.

Managing Group Configuration

You can customize the group configuration to manage all the devices of this group. When you push the configuration, online (registered or unregistered) devices are updated in real time when they receive updates.

Adding Groups

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

Procedure

1. Click **Device configuration**->**Group configuration**.

2. In the top-right corner of the page, click **Add Group**.
3. Enter the group name and description.
4. Click **Next step** to go to the Group Device setting page.
5. Select the checkboxes of the desired devices.
6. Click **Next step** to go to the Set Parameters page.
7. Configure the desired parameters.
8. Click **Save and update** to push the updated parameters to all the devices of 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 parameters supported by the device in the text.
- Edit parameters in the template: you can edit the corresponding parameters in the template.

Editing Parameters in the Text (Group Configuration)

You can configure any parameter supported by the devices in each group via text.

You can also update the configuration after setting the parameters.

Procedure

1. Click **Device Configuration**->**Group Configuration**.
2. Click ••• on the right side of the desired group.
3. Select **Editing Parameters in text** from the drop-down menu.
4. Configure the parameters in the text.

   The parameter you enter can take effect only when they meet the format requirements
5. Click **Save**.

   It prompts whether or not you want to update the configuration file immediately.
6. Click **No**, the parameters will be saved.

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

Setting Parameters in the Template (Group Configuration)

You can configure parameters for each group in the Set Template Parameters page. You can also update the configuration after setting the parameters.

Procedure

1. Click **Device Configuration**->**Group Configuration**.
2. Click ⚙ on the right side of the desired group.
3. Configure the parameters.

4. Click **Save**.

   It prompts whether or not you want to update the configuration file immediately.

5. Click **No**, the parameter configuration will be saved.

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

Editing Groups

You can edit the name and description of the groups, reselect the device in the groups and reset the parameters.

Procedure

1. Click **Device Configuration**->**Group Configuration**.
2. Click ••• on the right side of the desired group.
3. Select **Edit Group** from the drop-down menu.
4. Edit the corresponding information.
5. Click **Save**.

Updating the Group Devices

When adding or deleting devices in a group, you can update the group devices and select to save this group or push the parameters to the devices in this group.

Procedure

1. Click **Device configuration**->**Group configuration**.
2. Click ⬆ on the right side of the desired group.
3. Select the checkboxes of 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

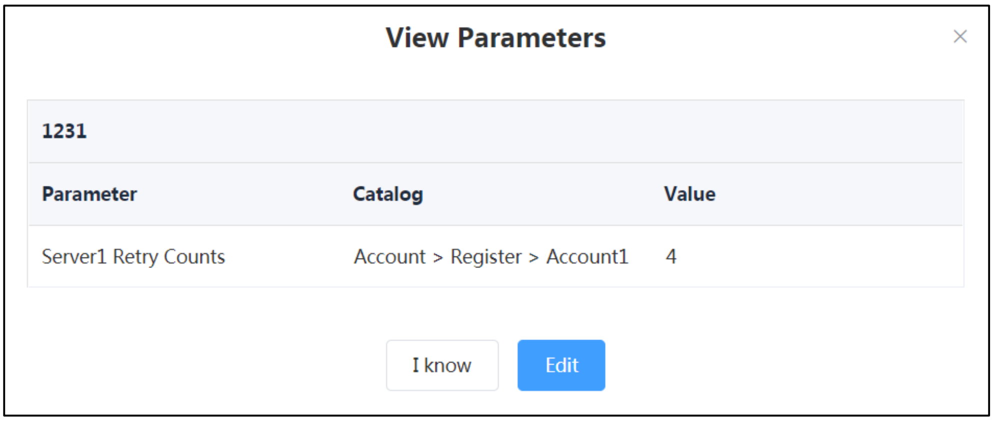
You can quickly view the parameter information edited for the group.

Note that you can only view the parameters in the configuration template.

Procedure

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

2. Click on the right side of the desired group.



View Parameters

1231		
Parameter	**Catalog**	**Value**
Server1 Retry Counts	Account > Register > Account1	4

You can click **Edit** to set the parameters in the Edit Group page.

Related topics

Setting Parameters in the Template (Group Configuration)

Downloading Configuration Files (Group)

Procedure

1. Click **Device Configuration**->**Group Configuration**.
2. Click ••• on the right side of the desired group.
3. Select **Download config file** from the drop-down menu to download the configuration file to your computer.

Deleting Groups

Procedure

1. Click **Device Configuration**->**Group Configuration**.
2. Select the checkboxes of the desired groups.
3. Click **Delete**.

   It prompts whether or not you are sure to delete it.

4. Click **OK**.

Managing MAC Configuration

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

When the device is connected to the management platform for the first time, and if there is a backup file, the template configuration of the model is pushed first, and then the MAC backup file is pushed. If there is no backup file, the template configuration of the model is pushed only.

Related topics

Managing Model Configuration

Uploading backup Files

You can upload a backup file to update the configuration for a single device, but the file format must be .cfg named after MAC address.

Procedure

1. Click **Device Configuration**->**MAC Configuration**.
2. Click **Upload backup file** in the top-right corner of the page.
3. Click **Select the file** to select the desired file from your computer.
4. Click **Confirm**.

Generating Configuration Files

You can back up the corresponding device configuration in the device management platform through generating a configuration file.

Procedure

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

   If the device has 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 ➦ on the right side of the desired MAC address to push the backup file to the corresponding device.

Downloading Backup Files

You can download the backup files to your computer.

Procedure

1. Click **Device Configuration**->**MAC Configuration**.
2. Click ⬇ on the right side of the desired MAC to download the backup to your computer.

Exporting Backup Files

Procedure

1. Click **Device Configuration**->**MAC Configuration**.
2. In the top-right corner of the page, click **Export** to save the file to your computer.

Deleting Backup Files

Procedure

1. Click **Device Configuration**->**MAC Configuration**.
2. Select the checkboxes of the desired MAC addresses.
3. Click **Delete**.

   It prompts whether or not you are sure to delete it.
4. Click **OK**.

Configuring Global Parameters

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

Note that when a device is connected to the management platform for the first time, the global parameters will be updated automatically.

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 Configuration

You can download the latest configuration parameter file from the Yealink official website to update the template parameters. Once you upload the configuration parameter file, the template parameters will be updated synchronously.

You can download the latest firmware(Yealink_Config(2.0.0.11).rar) online: http://support.yealink.com/documentFront/forwardToDocumentDetailPage?documentId=242.

Procedure

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

   Only .xls file format is supported and the size should not greater than 2M.
3. Click **Upload**.

Managing Tasks

You can create and manage timing task, you can also view all the task execution records for troubleshooting or re-execute the task.

Topics include:

- Managing Timer Tasks
- Managing Executed Tasks Records

Managing Timer Tasks

Timer Tasks and Pushing Rules

You can select the task type and the repeat time when creating timer tasks. For example, you do not want to update the firmware or the configuration during the office hour, because it will reboot the devices and the staff cannot use the devices. Therefore, you can set the timer tasks that are executed during non-office hour.

The rules for pushing timer tasks are as follows:

Task	Rules
Push resource file	You can choose only one resource item to push in a task. The resource type unsupported by the devices will not be pushed.
Update firmware	If you select devices of different models, only the firmware that is supported by all devices can be updated.
Update config file	When pushing the configuration by template, the configuration of the corresponding device model will be pushed. If a device does not have the template of the corresponding model, the configuration will not be pushed to this device. When pushing the configuration by default, the default configuration will be pushed.
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 of the page, click **Add Timer Task**.
3. Select the checkboxes of the desired devices.
4. Configure the task name, the content 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 ✎ on the right side of the desired task.
3. Select the desired devices in the list.
4. Edit the corresponding information.
5. Click **Save**.

Related tasks

Adding Timer Tasks

Pausing or Enabling Timer Tasks

Procedure

1. Click **Task Management**->**Timer Task**.
2. On the right side of the desired task, click ⏸ / ✓ to pause/execute the task.

Ending Timer Tasks

You can end timer tasks that are in the status of **to be executed**, **Suspending** or **Executing**. If you end the **Executing** timer task, the task will continue until it is finished. For recurrence task, they will no longer be executed once you end them.

Procedure

1. Click **Task Management**->**Timer Task**.
2. Click ✖ , on the right side of the desired task name.

Searching for Timer Tasks

You can search for timer tasks by directly entering the related information by filtering.

Procedure

1. Click **Task Management**->**Timer Task**.
3. Do one of the following:
   - Search for a timer task directly:
     1) Enter a few or all characters of the task name in the search box.
     2) Press **Enter** to perform a search.
   - Search for a timer task based on the execution result:
     1) Click **More**.
     2) Select the corresponding execution result.
     3) Click **Search**.

     The search result is displayed in the timer task list.

Viewing Timer Tasks

Procedure

1. Click **Task Management**->**Timer Task**.
2. Click the desired task or click ⓘ on the right side of the desired task name.

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

Related topics

Managing Executed Tasks Records

Managing Executed Tasks Records

You can view the detailed records of the timer tasks and one-time tasks, the details include the execution time, the execution mode, the task name, the task content, and the execution status. When the task is executed successfully or exceptionally, you can view the execution details.

Viewing the Execution Information

Procedure

1. Click **Task Management**->**Executed Task**.
2. Click ⓘ on the right side of the desired task to go to the Execution detail page.

Retrying Exceptional Tasks

If the task is exceptional, you can execute it again.

Procedure

1. Click **Task Management**->**Executed Task**.
2. Click ⓘ on the right side of the desired task to enter the Execution detail page.
3. Select the checkboxes of 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 by filtering.

Procedure

1. Click **Task Management**->**Executed Task**.
2. Enter a few or all characters of the task name in the search box, and press Enter to perform the search.

   You can also search the task by filtering the execution time.

   The search result displays in the Executed Task list.

Monitoring and Managing the Devices

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

Topics include:

- Viewing Call Quality Statistics
- Monitoring Alarms

Viewing Call Quality Statistics

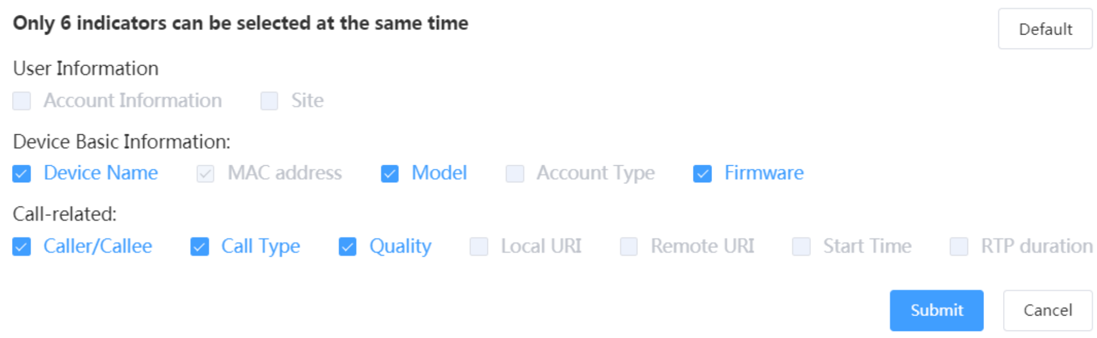
You can view the call quality and the session distribution on the Call statistics page. You can also view the details of call quality, including the user information, the basic device information and the call-related information.

Customizing the Indicators of Call Quality Detail

You can customize the indicators displayed in the Call Quality Detail list, but you can select only 6 indicators and the MAC address is default.

Procedure

1. Click **Dashboard**->**Call Statistics**.
2. Click **More Indicators**.



Only 6 indicators can be selected at the same time

User Information

☐ Account Information ☐ Site

Device Basic Information:

☑ Device Name ☑ MAC address ☑ Model ☐ Account Type ☑ Firmware

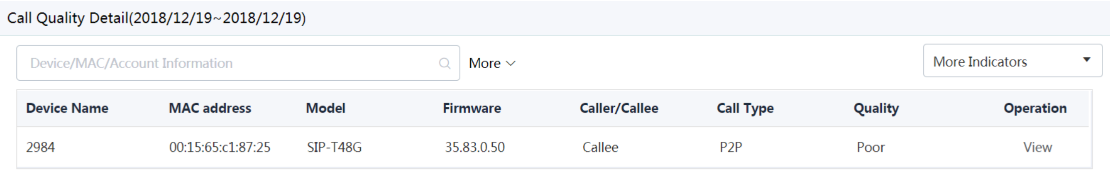
Call-related:

☑ Caller/Callee ☑ Call Type ☑ Quality ☐ Local URI ☐ Remote URI ☐ Start Time ☐ RTP duration

3. Select the checkboxes of the desired indicators.

4. Click **Submit**.

   The selected indicators are displayed in the list.



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

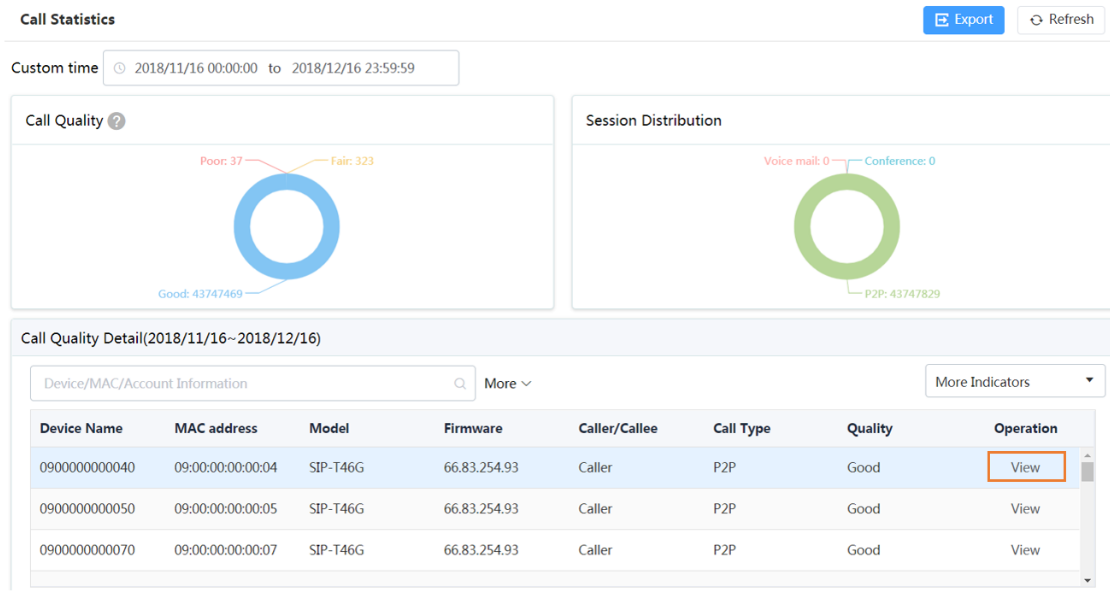
Device Name	MAC address	Model	Firmware	Caller/Callee	Call Type	Quality	Operation
2984	00:15:65:c1:87:25	SIP-T48G	35.83.0.50	Callee	P2P	Poor	View

Viewing the Call Data of Call Quality

Procedure

1. Click **Dashboard**->**Call Statistics**.
2. Click **View** on the right side of the desired call to go to the Call Data page.

   You can view more detailed information about the call quality on the Call data page.



Call Statistics

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

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

Monitoring Alarms

When the devices are abnormal, they will send alarms to the platform and the administrator can monitor the alarm to troubleshoot problems.

Managing Alarm Strategies

Adding Alarm Strategies

You can add alarm strategies. Therefore, the alarm receivers can receive alarms of the corresponding severity in the email or the Alarm list page, and then monitor the alarms to troubleshoot problems, such as network or server problems.

You cannot delete the system default alarm strategy added when the system was initialized, but you can edit the receivers.

Procedure

1. Click **Alarm Management**->**Alarm Strategy**.
2. Click **Add Strategy**.
3. Enter the name of the strategy, select a desired alarm severity and alarm strategy.

   You can choose to receive alarms by email or via the platform.
4. Click ⚙ to add the receivers, and do the following:
   1) Select the checkboxes of the desired receivers.

      The selected receivers are displayed on the right side of the page.
   2) Click **OK**.
5. Enable the alarm strategy.

   It is enabled by default.
6. Click **Save**.

Editing Alarm Strategies

Procedure

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

Deleting Alarm Strategies

Procedure

1. Click **Alarm Management**->**Alarm Strategy**.
2. Click 🗑 on the right side of the desired alarm strategy.

   It prompts whether or not you are sure to delete it.
3. Click **OK**.

Viewing Alarms

When there is a problem such as call failure or register failure, the problem will be uploaded to the server. You can quickly locate the problem by viewing the alarm details.

Procedure

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

2. Click ⓘ on the right side of the desired alarm.

   You can view last alarm time, the counts and the description.

Related topics

Managing Alarm Strategies

Note If you have configured to receive the alarm via email, please refer to Appendix: Alarm Type for more information on the alarm type.

Deleting Alarms

Procedure

1. Click **Alarm Management**->**Alarm List**.
2. Select the checkboxes of the desired alarms.
3. Click **Delete**.

   It prompts whether or not you are sure to delete it.
4. Click **OK**.

Diagnosing Devices

You can use the diagnostic tools, such as the log files, the captured packet, and the network detection, to find out the cause of the problem and to troubleshoot the problem.

Make sure that the device is connected to the device management platform before diagnosing.

Topics include:

- Going to the Device Diagnostics Page
- Setting the Device Logs
- Capturing Packets
- Network Diagnostics
- Exporting Syslogs
- Exporting Configuration Files
- Viewing the CPU and Memory Status
- Viewing Recordings
- Capturing the Current Screen of the Device

Going to the Device Diagnostics Page

Do one of the following:

- Click **Device Management**->**Device list**, and then click + on the right side of the desired device.
- Click **Device Diagnostic**, enter the MAC address or the IP address of the desired device, and then click **Start Diagnostic**.

Related tasks

- Setting the Log Level
- Capturing Packets
- Network Diagnostics
- Exporting Syslogs
- Exporting Configuration Files
- Viewing the CPU and Memory Status
- Viewing Recordings

- Capturing the Current Screen of the Device

Setting the Device Logs

You can enable the Log Data Backup feature, and the device will send 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 videoconferencing system, version XX.32.0.35 or later (XX represents the fixed number of each device model).

Setting the Log Level

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **Log Level**.
2. Enter the desired value.
3. Click **Confirm**.

Related tasks

Going to the Device Diagnostics Page

Setting the Module Log

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

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **Log Settings**.
2. In the **Module Log** field, select the log type and the level.
3. Click **Save**.

Related tasks

Going to the Device Diagnostics Page

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

Go to the Device Diagnostic page.

Procedure

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

Note The module log level is less 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.

Related tasks

Going to the Device Diagnostics Page

Setting the Syslog

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

Before you begin

Go to the Device Diagnostic page.

Procedure

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

Note The module log level is less 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.

Related tasks

Going to the Device Diagnostics Page

Putting the Log Backups to a Specified Server

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

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **Log Settings**.
2. In the **Other Log Settings** field, enable **Log File Backup**.
3. Enter the address, the user name and the password of the specified server.
4. Select the desired method in the **Http Method** and the **Http Post Mode** fields.
5. Click **Save**.

Related tasks

Going to the Device Diagnostics Page

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 of the past 7 days.

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **Log Settings**.
2. In the **Other Log Settings** field, enable **Log Data Backup**.
3. Click **Save**.

Related tasks

Going to the Device Diagnostics Page

Downloading the Backup Log

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

Before you begin

Go to the Device Diagnostic page.

Procedure

1. On the right side of the corresponding log, click ⬇ to download it to your computer.

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

Related tasks

Going to the Device Diagnostics Page

Enabling the Log Data Backup

Capturing Packets

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **Packetcapture** in the Diagnostic Tools.
2. Select the desired Ethernet and type, and then enter the string.

   You can enter the string only when you select **Custom** from the drop-down menu of the **Type**.
3. Click **Start** to begin capturing the signal traffic.
4. Click **Finish** to stop capturing, and the file is generated automatically.
5. Click Download to save the file to your computer.

Note If the devices are offline, you cannot capture packets. If it takes more than 1 hour to capture packets, the packet capturing will be automatically ended.

Related tasks

Going to the Device Diagnostics Page

Network Diagnostics

Network diagnostics include: Ping (ICMP Echo) and Trace Route.

About this task:

- **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.

Before you begin

Go to the Device Diagnostic page.

Procedure

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

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

Related tasks

Going to the Device Diagnostics Page

Exporting Syslogs

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

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **Export System Log** in the **Diagnostic Tools** filed.
2. Save the file to your local computer.

Related tasks

Going to the Device Diagnostics Page

Exporting 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.

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **Export Config File** in the **Diagnostic Tools** filed.

2. Select a desired file type.

   If you select **cfg**, you can choose to export static settings, non-static settings or all settings.

3. Click **Export**, and then save the file to your local computer.

Related tasks

Going to the Device Diagnostics Page

Viewing the CPU and Memory Status

The device will report its CPU and memory information to the device management platform at a regular time. You can update the information and view the latest information. You can also copy the information to view the detailed memory information.

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **CPU Memory Status** in the **Diagnostic Tools** filed.
2. Do one of the following:

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

Related tasks

Going to the Device Diagnostics Page

Viewing Recordings

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **Recording file** in the Diagnostic Tools.

   You can select the **Automatic upload recording file**, so that the recording file will be uploaded to the platform when the recording finished.

   You can also click ⬇ to download the recording.

Related tasks

Going to the Device Diagnostics Page

Capturing the Current Screen of the Device

Before you begin

Go to the Device Diagnostic page.

Procedure

1. Click **Screencapture** in the Diagnostic Tools.

   You can click **Reacquire** to get the current screenshot.

Related tasks

Going to the Device Diagnostics Page

Managing the System

Topics include:

- Viewing Operation Log Files
- Configuring the SMTP Mailbox

Viewing Operation Log Files

Any operations on the device management platform will be recorded in the operation logs. You can view the operation history.

Procedure

1. Click **System management**->**Log management**.
2. Optional: you can view or filter the operation log by selecting the time, the operation type, the path, the username or the IP address in the search.

   You can also view the username, the type, the path, the IP address, the time, and the result of the corresponding operation log.

Configuring the SMTP Mailbox

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

The parameters for SMTP mailbox setting are described below:

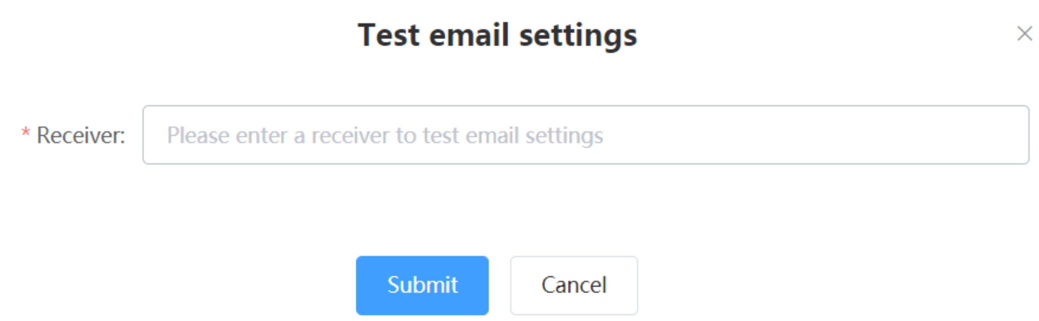
Parameter	Description
SMTP	Specifies the address of the SMTP server.
Sender	Configures the email address of the sender.
Username	Specifies the email username of the sender.
Password	Specifies the email password of the sender.
Port	Specifies the connection port.
This server requires secure connection	Enables or disables the secure connection. If connection security is enabled, you should select the protocol used to connect to the SMTP server. ● SSL ● TLS **Default:** TLS

Parameter	Description
Enable the mailbox	Enables or disables the mailbox. **Default:** Disabled

Procedure

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

   Enter the email address of a receiver.



Test email settings

* Receiver: Please enter a receiver to test email settings

   Click **Submit** to test whether the email address you set is available.

   If the Email sending failed, please check the account and the password.

4. Click **Save**.

Troubleshooting

This chapter provides you with general information for troubleshooting some common problems while using the Yealink device management platform. Upon encountering a case not listed in this section, contact your Yealink reseller for further support.

Topics include:

- General Issues

General Issues

Forget the Password?

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

Procedure

1. Click **Forget Password** on the Login page of the device management platform.
2. Enter the email and the captcha in the corresponding field.
3. Optional: click **OK**.

   Click **OK** according to the prompts.
4. Log into your mailbox, click the link for resetting the password, and then reset the password according to the prompts.

Why You Cannot Access the Login Page of Yealink Device Management Platform

Server:

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

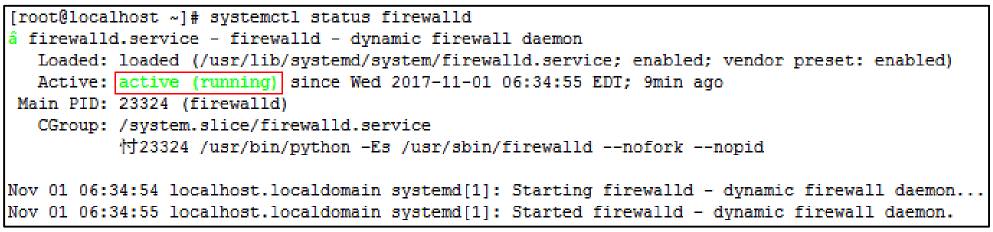
Windows:

- Run Network Diagnostics of Window.

Procedure

1. Log into CentOS as the root 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, reflesh 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 of Yealink Device Management Platform?

The Yealink server has built-in application certificates. For security considerations, the browser only trusts certificates issued by the professional certificate issuing authorities. Therefore, by default, they do not trust our certificates.

- When you access login page for the first time, it will prompt you an insecure connection (certificate security issue). You can continue to access the browser.
- If you have purchased your own certificate, you can also replace our certificate.

Procedure

In the following, “serverdm” is the certificate file name you want to replace.

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 serverdm.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

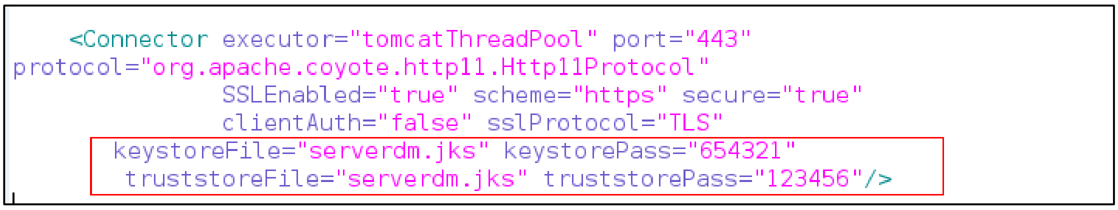
   It will prompt you to enter the target key, and then enter the export password you set in step 2.

Note that you the target key should be the same as the key you set in step 2.

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.



```
    <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"/>
```

Reboot the server and the certificate will take effect.

Appendix: Alarm Types

Alarm type	Severity
Bad quality call	Critical
Register failure	Critical
DNS server discovery failure	Critical
Network traversal failure	Critical
Update Configuration failure	Critical
Update Firmware failure	Critical
Play visual voicemail failure	Minor
Hold failure	Minor
Resume failure	Minor
Visual voicemail retrieve failure	Minor
RTP violate	Minor
RTP address change	Minor
RTP SSRC change	Minor
RTP dead	Minor
SRTP failure	Minor
Calendar synchronization failure	Minor
Calllog retrieve failure	Minor
Call failure	Minor
Outlook contact retrieve failure	Minor
Time synchronization failure	Major
Transfer failure	Major
Bluetooth pairing fail	Major
Meeting join failure	Major
Meet now failure	Major

Alarm type	Severity
BToE pairing failure	Major
Exchange discovery failure	Major
Device reboot	Major
Program exit	Major
Insufficient memory	Major
Insufficient space	Major