Yealink

Yealink Device Management Platform Administrator Guide

Version 2.0.0.14
May.2018

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 *DocsFeedback@yealink.com*.

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.

Yealink device management platform supports the management of the following devices:

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. XX represents a fixed number for each phone model.
Skype for Business HD T4XS IP phones	SIP-T41S/T42S/T46S/T48S	66.9.0.45 or later.
Video Conference Systems	VC200/VC500/VC800/VC880	XX.32.0.3 or later. XX represents a fixed number for each phone model.

Related Documentations

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

- Quick Start Guides, which describe how to assemble devices and configure the most basic features available on devices.
- User Guides, which describe the basic and advanced features available on devices.
- Administrator Guide, which describe 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/*.

Typographic and writing Conventions

Yealink documentations contain a few typographic conventions.

You need to know the following basic typographic conventions to distinguish types of in-text information:

Convention	Description
Bold	Highlights the items such as menus or menu selections when they are involved in a procedure or user action (for example: Click on **Site management**).
Blue Text	Used for cross references to other sections within this documentation (for example: refer to Troubleshooting).
Blue Text in Italics	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink Technical Support website (for example: *http://support.yealink.com/*).

You also need to know the following writing conventions to distinguish conditional information:

Convention	Description
<>	Indicates that you must enter specific information. For example, when you see <IP address>, enter Yealink device management platform's IP address.
->	Indicates that you need to select an item from a menu. For example, **Dashboard->Running state analysis** indicates that you need to select **Running state analysis** from the pull-down list of **Dashboard**.

In This Guide

Topics provided in this guide include:

- Chapter 1 Getting Started
- Chapter 2 Administrator Account Management
- Chapter 3 Managing Sites

- Chapter 4 Managing Accounts
- Chapter 5 Managing Devices
- Chapter 6 Managing Device Configuration
- Chapter 7 Managing Tasks
- Chapter 8 Monitoring and Managing the Devices
- Chapter 9 Troubleshooting
- Chapter 10 Appendix: Alarm Types

Table of Contents

Getting Started

This chapter provides basic information for Yealink device management platform.

Topic includes:

- Hardware and Software Recommendations
- Browser Requirements
- Icons Instructions
- Installing Yealink Device Management Platform
- Updating Yealink Device Management Platform
- Uninstalling Yealink Device Management Platform
- Logging into the Yealink Device Management Platform as System Administrator
- Managing Sub-administrators
- Logging into the Yealink Device Management Platform as Sub-administrator
- Home Page
- Running State

Hardware and Software Recommendations

Server system: Linux CentOS 7.0 or later.

Device Quantity	CPU	Memory	Hard Drive
0~3000	Quad-core	8G	200G
3000~6000	8-core	16G	The capacity of the hard drive should be increased by 30G with every 1000 devices added.
6000~10000	12-core	32G	
10000~20000	32-core	64G	

The Device Management Platform Port Requirements

You should open four ports for the device management platform: 443, 28443, 9090, and 80. We do not recommend that you modify these ports.

Browser Requirements

Operating System	Browser
Win7	Internet Explorer 11 or later
Win8	Internet Explorer 11 or later
Win10	Microsoft Edge 14 or later
MAC	Safari 10 or later

Icons Instructions

Icons on the Yealink device management platform are described in the following table:

Icons	Description
🔍	Search for sub-administrators, alarms, sites, devices, user accounts, tasks, resources and so on.
📝	Edit sites, devices, user accounts, tasks, configuration templates, resources and so on.
🗑	Delete alarms, sites, devices, user accounts, timer tasks or immediate tasks, executed tasks, configuration templates, resources and so on.
📥	Download configuration, firmware and resources.
🧰	Enter the Device diagnostic page.
↗	Send the firmware , resource or configuration to devices.
ℹ	View the details of task execution, alarms or call quality.
🔍	View the system log or more device info.
📄	View parameters.
⚙	Set parameters.
📝	Edit parameters in text.

Icons	Description
⬆	Update the group device.
⏸	Pause the timer task.
✓	Enable the timer task.
✕	End the timer task.
⚙	Edit the receivers of the alarm strategy.

Installing Yealink Device Management Platform

Before you begin

1. Review hardware and software recommendations.
2. Obtain the installation package of Yealink device management platform from the Yealink distributor or SE and then save it at the path **/usr/local**.

To install Yealink device management platform (log into CentOS as the root user):

The following takes version 2.0.0.7 and server IP 10.2.62.12 as an example.

1. Open the terminal.
2. Run the command as below:

```
cd /usr/local
tar -zxvf DeviceManagement_2.0.0.7.tar.gz
cd /usr/local/dm_install
./install.sh install 10.2.62.12
```

After you finish the installation, it prompts "Install Success!!!".

Related topics

Hardware and Software Recommendations

Updating Yealink Device Management Platform

If you have installed the Yealink device management platform, you can upgrade the Yealink device management platform to its latest version.

Before you begin

1. 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**.

To update Yealink device management platform application (log into CentOS as the root user):

The following takes version 2.0.0.7 as an example.

1. Open the terminal.
2. Run the command as below:

```
cd /usr/local
rm -rf dm_install
tar -zxvf DeviceManagement_2.0.0.7.tar.gz
cd /usr/local/dm_install
./install.sh upgrade
```

The Yealink device management platform will be updated to the latest version.

Uninstalling Yealink Device Management Platform

To uninstall Yealink device management platform:

1. Open the terminal.
2. Run the command as below:

```
cd /usr/local
./install.sh uninstall
```

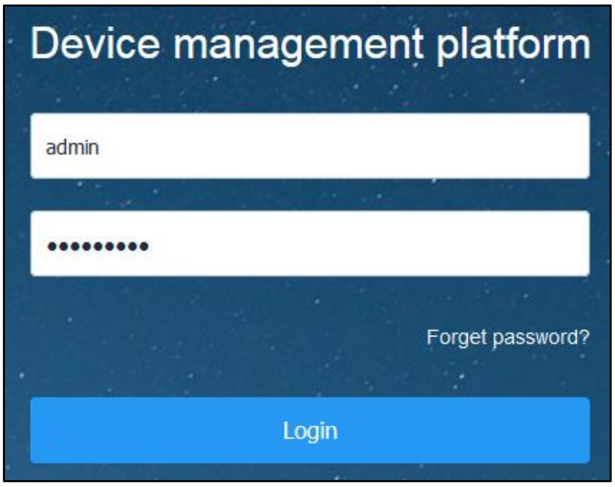
The Yealink device management platform will be uninstalled from the CentOS.

Logging into the Yealink Device Management Platform as System Administrator

To log into Yealink device management platform:

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. (Option.) Select your desired language.

4. Enter your username (admin) and password (admin), and click **Login**.

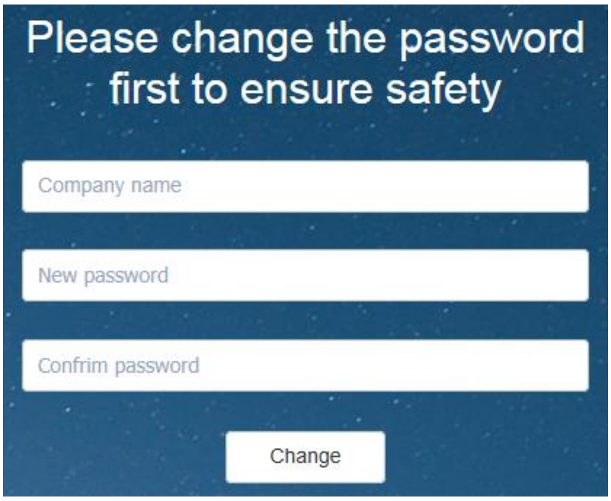


Device management platform

admin

••••••••••

If you log into the platform using the default password for the first time, the system will prompt you to change the password.



Please change the password first to ensure safety

5. Enter the company name, new password and re-enter the new password to change the default password.
6. Click **Change** to enter the homepage of Yealink device management platform directly.

Managing Sub-administrators

The system administrator can add sub-administrators as needed to assign different function permissions to the sub-administrators. So that sub-administrators can manage the devices according to the corresponding functions.

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

Adding Sub-administrators

Before you begin

1. Log into the Yealink device management platform as system administrator.
2. Configure the SMTP mailbox to send the account information to sub-administrators.

To add a sub-administrator:

1. Click **System management**->**User management**.
2. From the top right of the page, click **Add new user**.
3. Configure the user name, password (default password: Yealink@dmp), phone number, email, office address and function list in the corresponding field.
4. Click **Save**.

   You can also click **Save and add** to save the change and continue to add a new sub-administrator.

Related topics

Configuring the SMTP Mailbox

Editing Sub-administrators

Before you begin

1. Log into the Yealink device management platform as system administrator.

To edit a sub-administrator:

1. Click **System management**->**User management**.
2. From the left of the page, select a desired template from the **User name** list.
3. Reset the password (default password: Yealink@dmp) and edit the phone number, email, office address and function list in the corresponding field.
4. Click **Save**.

   You can also click **Save and add** to accept the change and enter the **Add new user** template page.

   The sub-administrator’s mailbox will receive the email which contains the account information if you reset the password.

Related topics

Configuring the SMTP Mailbox

Searching for Sub-administrators

You can search for sub-administrators by the login name.

Before you begin

1. Log into the Yealink device management platform as system administrator.

To search for sub-administrators:

1. Click **System management**->**User management**.
2. Enter a few or all characters of the login name in the search box.
3. Click 🔍 or press **Enter** to perform a search.

   The search result displays in the User name list.

Deleting Sub-administrators

Before you begin

1. Log into the Yealink device management platform as system administrator.

To delete a sub-administrator:

1. Click **System management**->**User management**.
2. From the left of the page, select a desired sub-administrator from the **User name** list.
3. Click **Delete**.

   The page prompts "Sure to deletion? The data cannot be restored after deletion".
4. Click **Confirm**.

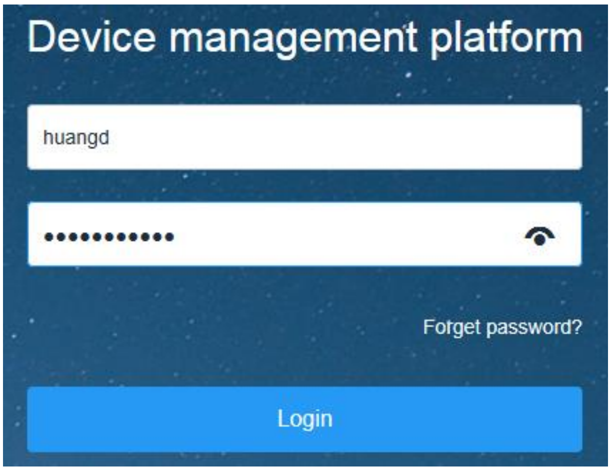
Logging into the Yealink Device Management Platform as Sub-administrator

The sub-administrator can log into the device management platform according to the received email which includes the URL of the device management platform, the user name and password.

To log into Yealink device management platform as sub-administrator:

1. Click the URL of Yealink device management platform in emails.

2. Select your desired language, enter your username and password (Yealink@dmp), and click **Login**.

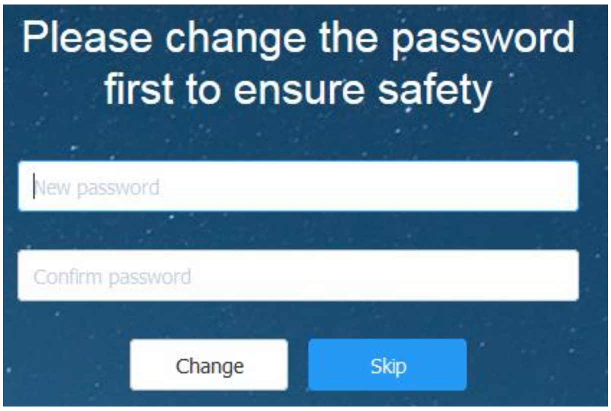


Device management platform

huangd

●●●●●●●●●●●

If you log into the platform for the first time, the system will prompt you to change the password.

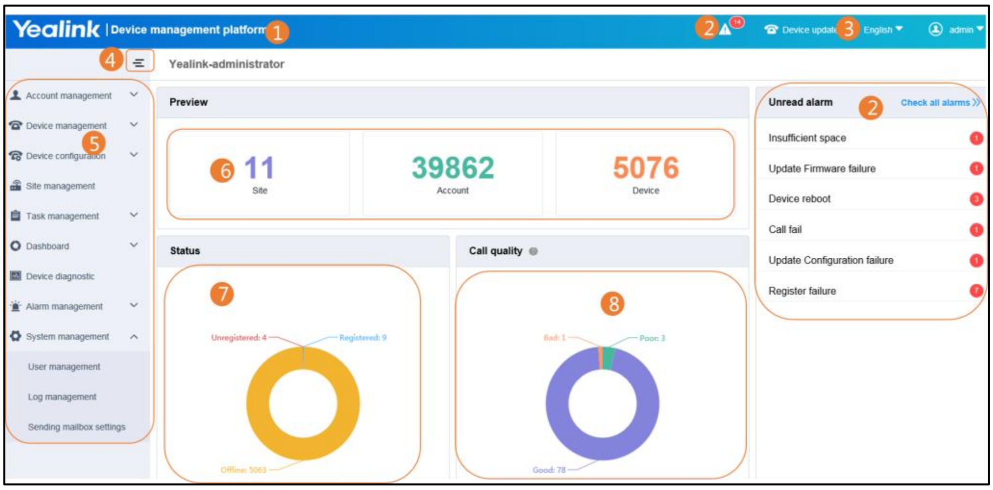


Please change the password first to ensure safety

3. Enter the new password and re-enter the new password to change the default password.
4. Click **Change** to enter the home page of Yealink device management platform directly.

Home Page

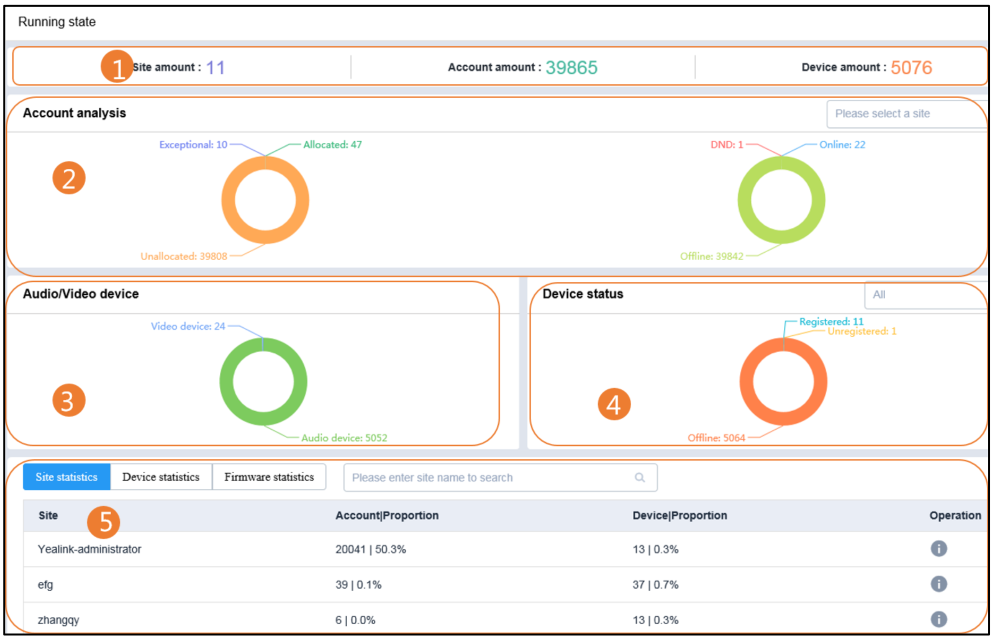
After you log into the Yealink device management platform successfully, the home page is shown as below:



No.	Description
1	Goes to the home page quickly when you are in other pages.
2	Displays the number of unread alarms and the type of alarms.
3	Click to go to the Timer task management page quickly.
4	Folds or unfolds the navigation pane.
5	Navigation pane.
6	**Data preview:** ● Displays the number of sites, accounts and devices. ● You can click the corresponding module to enter the module management page.
7	**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.
8	**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.

Running State Page

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



Running state

Site amount : 11 | Account amount : 39865 | Device amount : 5076

Site	Account|Proportion	Device|Proportion	Operation
Yealink-administrator	20041 | 50.3%	13 | 0.3%	ⓘ
efg	39 | 0.1%	37 | 0.7%	ⓘ
zhangqy	6 | 0.0%	13 | 0.3%	ⓘ

No.	Description
1	Displays the number of sites, accounts and devices.
2	**Account analysis:** ● Displays the number of allocated, unallocated and exceptional devices. ● Displays the number of devices who are online, offline and DND.
3	**Audio/Video analysis:** Displays the number of video devices and audio devices.
4	**Device status:** Displays the number of unregistered, registered and offline devices.
5	**Site statistics:** Displays the site name, the number of accounts and proportion and the number of devices and proportion. **Device statistics:** Displays the model, device and the number of devices and proportion. **Firmware statistics:** Displays the firmware, model and the number of devices and proportion.

Deploying the Devices

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

To deploy the devices:

1. Connect the devices into the network.
2. The devices perform mutual TLS authentication using default certificates.
3. If there is a provisioning server you are using in your environment, you need to configure the Common.cfg file (for example, <y0000000000xx>.cfg) of the corresponding devices.
4. Else, you need to configure the devices to obtain the provisioning server address in the following ways:

   - **DHCP option 66, 43, 160** or **161**.

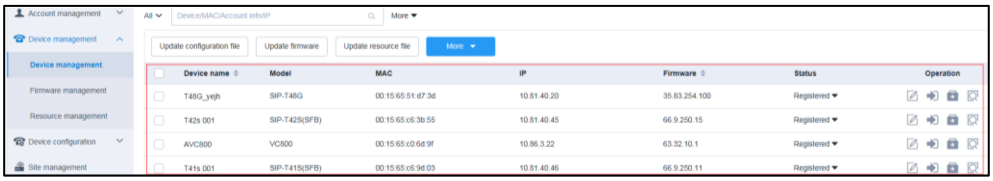
     The DHCP option must meet the following format:

     https://<IP address>:28443/dm.cfg (for example: https://10.2.62.12:28443/dm.cfg)

   - **Configure server address on the RPS platform**.
   - **Phone flash**

   Note that the device should support the device management platform. If not, please upgrade the firmware first. Refer to About This Guide to check the required firmware version of the device.

After the devices connect to the platform, the devices' information will display in the device list.



□	Device name	Model	MAC	IP	Firmware	Status	Operation
□	T48G_yejh	SIP-T48G	00:15:65:51:d7:3d	10.81.40.20	35.83.254.100	Registered	
□	T42s 001	SIP-T42S(SFB)	00:15:65:c6:3b:55	10.81.40.45	66.9.250.15	Registered	
□	AVC800	VC800	00:15:65:c0:6d:9f	10.86.3.22	63.32.10.1	Registered	
□	T41s 001	SIP-T41S(SFB)	00:15:65:c6:9d:03	10.81.40.46	66.9.250.11	Registered	

Related topics

Using Certificates for Mutual TLS Authentication

Configuring Common CFG File

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

Obtaining the Provisioning Server Address from Phone Flash

Using Certificates for Mutual TLS Authentication

To allow the Yealink device management platform and device to authenticate 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.

To configure trusted certificates via the web user interface of devices:

1. Log into the web user interface of the device.
2. Click on **Security**->**Trusted Certificates**.
3. Select **Enabled** from the pull-down list 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.

To configure device certificates via the web user interface:

1. Log into the web user interface of the device.
2. Click on **Security**->**Server Certificates**.
3. Select **Default Certificates** from the pull-down list 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

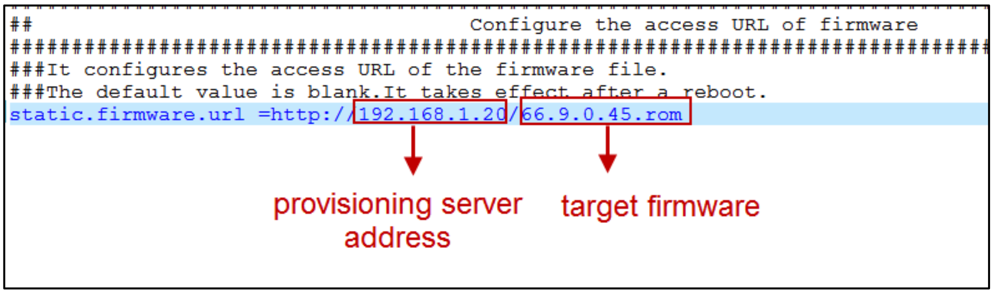
If the device does not support the device management platform, you need to upgrade the firmware before you connect the device to the device management platform. For ease deployment, you can configure the parameters of upgrading the firmware and the access URL of the device management platform in the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

To configure the Common.cfg file:

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.

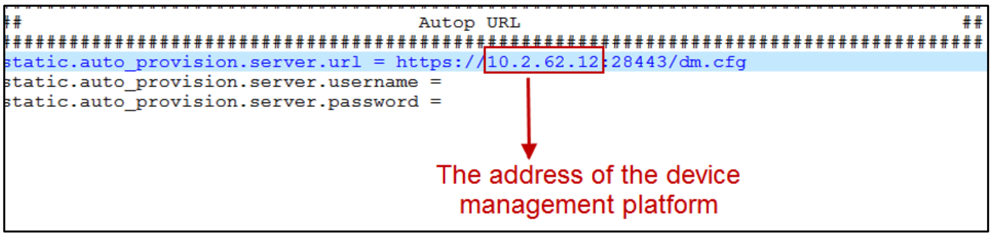
   Place the target firmware on your provisioning server, and then specify the access URL of the firmware.

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://10.2.62.12:28443/dm.cfg
static.auto_provision.server.username =
static.auto_provision.server.password =
```

4. Save the file.

   After perform auto provisioning, the devices will connect to the device management platform.

Related topics

About This Guide

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

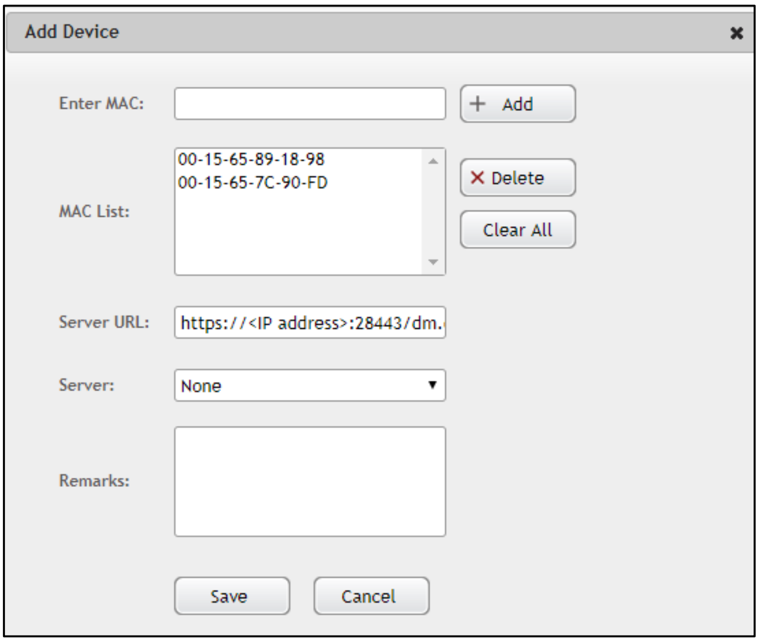
If you deploy the device through the RPS platform for the first time, after the devices are powered on and connected into the network, the RPS platform pushes the device management platform address to the devices so that they can connect to the platform.

To deploy devices on the RPS platform:

1. Log into the RPS platform.
2. Click on **Add Device**.
3. Enter the MAC address and server URL in the corresponding field.

   The server URL must meet the following format:

https://<IP address>:28443/dm.cfg (for example: https://10.2.62.12:28443/dm.cfg)



Add Device

Enter MAC:

MAC List:
00-15-65-89-18-98
00-15-65-7C-90-FD

Server URL: https://<IP address>:28443/dm.

Server: None

Remarks:

You can click **Add** to add more devices and all added devices are displayed in the MAC list.

4. Click **Save**.

   The device will connect to the platform.

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.

To obtain the provision server address from phone flash:

1. Log into the web user interface of the device.
2. Click on **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>:28443/dm.cfg (for example: https://10.2.62.12:28443/dm.cfg).
4. Click **Auto Provision Now** to trigger the device to connect to the platform immediately.

Administrator Account Management

This chapter provides basic instructions for Yealink device management platform.

Topic includes:

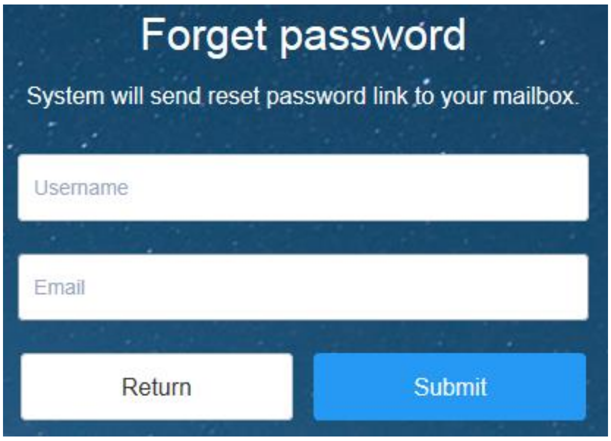
- Resetting Password
- Changing Login Password
- Editing the Administrator Account
- Log out of the Administrator Account

Resetting Password

If you forget password, you can click **Forget password?** to reset password.

To reset password:

1. On the device management platform login page, click **Forget password?**.



Forget password

System will send reset password link to your mailbox.

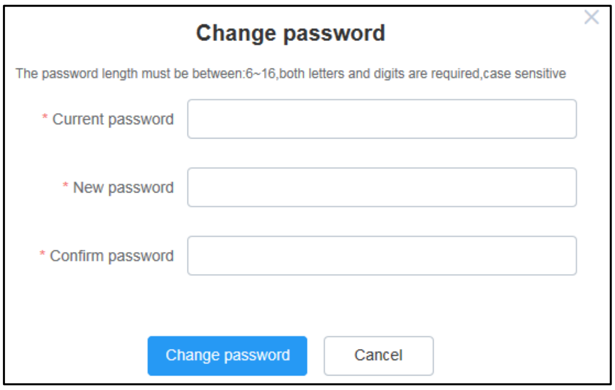
2. Enter your username and registered email in the corresponding field.
3. Click **Submit**.
4. Log into your registered email and click the link to set a new password in 24 hours.
5. Enter the new password and the re-enter the new password.
6. Click **Change** to reset the password.

Changing Login Password

To edit login password:

1. Click the user name on the top-right of the page, and then click **Account settings**.

2. Click **Change password**.
3. Enter the current password, new password and re-enter the new password.



Change password

The password length must be between:6~16,both letters and digits are required,case sensitive

* Current password

* New password

* Confirm password

4. Click **Change password**.

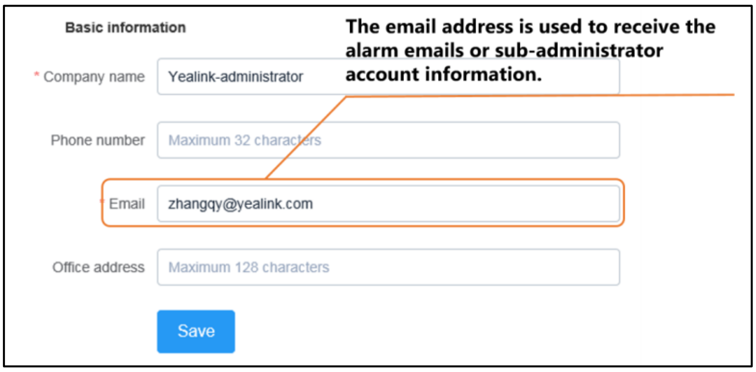
Editing the Administrator Account

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

If you are system administrator, the email is used to receive alarm emails. If you are sub-administrator, the email is used to receive alarm emails and account information.

To edit the administrator account:

1. Click the user name on the top-right of the page, and then click **Account settings**.
2. Configure the administrator account in the corresponding field you want to edit.



Basic information

* Company name: Yealink-administrator

Phone number: Maximum 32 characters

Email: zhangqy@yealink.com

Office address: Maximum 128 characters

The email address is used to receive the alarm emails or sub-administrator account information.

3. Click **Save** to accept the change.

Related topics

Managing Alarm Strategies

Adding Sub-administrators

Editing Sub-administrators

Log out of the Administrator Account

To log out of the administrator account:

1. Click the user name on the top-right of the page.
2. Click **Exit** to log out of the current administrator account and return to login page.

Managing Sites

You can set up the site according to different user requirements, and the default site named after your company name is added when the system is initialized. You can add, edit, search and delete sites.

Adding Sites

Adding Sites Manually

To add a site manually:

1. Click **Site management**.
2. From the top right 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 add sites.

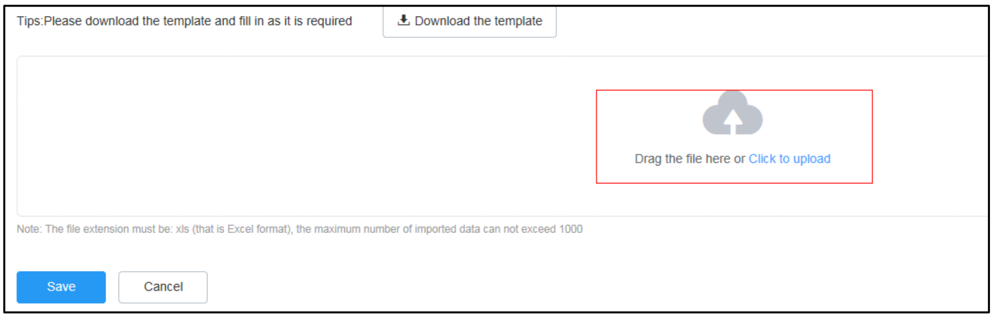
Importing Sites

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

To import sites:

1. Click **Site management**.
2. From the top right 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 local system.

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



Tips:Please download the template and fill in as it is required

Drag the file here or Click to upload

Note: The file extension must be: xls (that is Excel format), the maximum number of imported data can not exceed 1000

6. Click **Save** to import sites.

Note Read the note in the template before editing.

Editing Sites

To edit a site:

1. Click **Site management**.
2. Select a desired site in the Site name list.
3. Edit the site name and description in the corresponding field.
4. Click **Save**.

Searching for Sites

You can search for sites by site name.

To search for a site:

1. Click **Site management**.
2. Enter a few or all characters of site name in the search box.
3. Click 🔍 or press **Enter** to perform a search.

   The search result displays 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.

To delete a site:

1. Click **Site management**.
2. Select a desired site in the Site name list.
3. Click **Delete**.

If there are no accounts under this site, it prompt "Sure to delete? The data cannot be restored after deletion?"

4. Click **Confirm** to delete the site.

Related topics

Adding Accounts

Setting site for Accounts

Note

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

Managing Accounts

You can manage different types of 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.

Topic includes:

- Adding Accounts
- Editing Accounts
- Configuring Server Advanced Settings
- Searching for Accounts
- Allocating Devices to Accounts
- Setting site for Accounts
- Exporting Accounts
- Deleting Accounts

Adding Accounts

You can add accounts and then allocate devices to these accounts. If a device is allocated to the account, the server will push the account information to the device. When the terminal devices log in or log out of the account, the server automatically adds the account or updates the device account status.

The following table shows the information when you add different types of accounts:

Account	Required information	Optional information
SFB account	Login info(Account info or Pin info), Site	Device
SIP account	Login info(User name and Password), Site, Server1	Resister, Label, Display name, Server2, Device
YMS account	Login info(ID and Password), Site, Server address and Port	Device
Cloud account	Login info(User name and Password), Site, Server address	Device
H.323 account	Login info(Extension), Site, Gatekeeper type.	User name, Gatekeeper server address1 and Port, Gatekeeper server address2 and Port, Device

Adding Accounts Manually

You can add accounts manually, edit accounts or allocate devices to the account. Before allocating devices, ensure that the device has been added to the device management platform.

To add accounts manually:

1. Click **Account management**->**SFB account/SIP account/YMS account/Cloud account/H.323 account**.

2. From the top right of the page, click **Add account**.

3. Configure the account information.

4. Click **Save**.

Related topics

Adding Devices

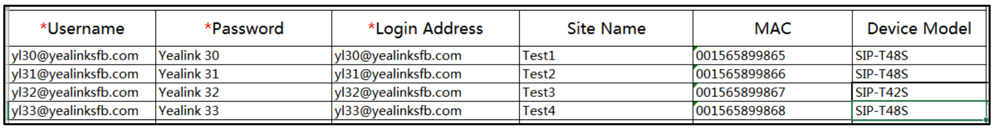
Importing Accounts

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

To import accounts:

1. Click **Account management**->**SFB account/SIP account/YMS account/Cloud account/H.323 account**.
2. From the top right of the page, click **Import**.
3. Click **Download the template** to download an empty .xls file.
4. Edit the template and save it to your local system.

   Before editing the information, you need to read the note and then fill in the template as required. For example, the template for the SFB account is shown as follows:



*Username	*Password	*Login Address	Site Name	MAC	Device Model
yl30@yealinksfb.com	Yealink 30	yl30@yealinksfb.com	Test1	001565899865	SIP-T48S
yl31@yealinksfb.com	Yealink 31	yl31@yealinksfb.com	Test2	001565899866	SIP-T48S
yl32@yealinksfb.com	Yealink 32	yl32@yealinksfb.com	Test3	001565899867	SIP-T42S
yl33@yealinksfb.com	Yealink 33	yl33@yealinksfb.com	Test4	001565899868	SIP-T48S

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

Editing Accounts

You can modify your account's information, re-select sites, or allocate devices. When you deallocate the device, the allocation between the device and the account will release directly.

To edit accounts:

1. Click **Account management->SFB account/SIP account/YMS account/Cloud account/H.323 account**.
2. Click ✎ beside the desired account.
3. Edit the account information.

4. Click **Save**.

Configuring Server Advanced Settings

You can configure server advanced settings for SIP accounts, YMS accounts and Cloud accounts.

If you update the server advanced settings on the server, the corresponding devices will update automatically. Note that when you update the server advanced settings on the terminal device, it will not be synchronized to the server. When you allocate a device to an account, the configuration will be pushed and updated to the device.

The server advanced settings for the SIP account are as follows:

Account	Required information	Optional information
SFB account	Transport: UDP/TCP/TLS/DNS-NAPTR **Default:** TCP	**Outbound server** Outbound proxy server1 and Port (default: 5060), Outbound proxy server2 and Port (default: 5060), Proxy fallback interval (default: 3600)
	Server expires **Default:** 3600	
	Server retry counts **Default:** 3	
	Outbound server: Disabled/Enabled **Default:** Disabled	
	NAT traversal: Disabled/Enabled **Default:** Disabled	

The server advanced settings for the YMS account are as follows:

Account	Required information	Optional information
YMS account	DTMF type: INBAND/RFC2833/SIP INFO/ RFC2833+SIP INFO **Default:** RFC2833	Outbound proxy server
	DTMF info type: DTMF-Relay/DTMF/Telephone-Event **Default:** DTMF-Relay **Note:** It can be selected only when the DTMF type is SIP INFO or RFC2833+SIP INFO.	
	DTMF load (96~127): **Default:** 101	

The server advanced settings for the Cloud account are as follows:

Account	Required information
Cloud account	DTMF type: INBAND/RFC2833/SIP INFO/ RFC2833+SIP INFO **Default:** RFC2833
	DTMF info type: DTMF-Relay/DTMF/Telephone-Event **Default:** DTMF-Relay **Note:** It can be selected only when the DTMF type is SIP INFO or RFC2833+SIP INFO.
	DTMF load (96~127): **Default:** 101

The server advanced settings for the H.323 account are as follows:

Account	Required information
H.323 account	Gatekeeper authentication: Disabled/Enabled **Default:** Disabled
	Gatekeeper username: **Note:** It can be configured only when the Gatekeeper authentication is enabled.
	Gatekeeper password: **Note:** It can be configured only when the Gatekeeper authentication is enabled.
	H.460 active: Disabled/Enabled **Default:** Disabled
	H.323 tunneling: Disabled/Enabled **Default:** Disabled
	H.235: Disabled/Enabled **Default:** Disabled
	Protocol Monitor Port (0~65535) **Default: 1720**
	DTMF type: INBAND/Auto **Default:** Auto
	Local early media: Disabled/Enabled **Default:** Disabled
	H.239: Disabled/Enabled **Default:** Enabled
	FECC (H.239): Disabled/Enabled **Default:** Enabled

To configuring server advanced settings:

1. Click **Account management**->**SFB account/SIP account/YMS account/Cloud account/H.323 account**.

2. Click **Server advanced settings**.
3. Configure the server advanced settings in the corresponding field.
4. Click **Save**.

Searching for Accounts

You can search for the accounts by directly entering the device basic information or using filter conditions on the device management platform.

To search for an account:

1. Click **Account management**->**SFB account/SIP account/YMS account/Cloud account/H.323 account**.
2. Do one of the following:
   - Search for an account directly:
     1) Enter the register name, extension, device name or MAC address in the search box.
     2) Click 🔍 or press **Enter** to perform a search.
   - Search for an account using filter conditions:
     1) Click **All**, and then select a desired allocation status.
     2) Click **More**, and then select a desired site and status.
     3) Click **Search**.

     The search result displays in the account list.

Allocating Devices to Accounts

If you did not allocate a device to your account when you added it, or you want to change the allocated devices, you can allocate devices to the account on the Account management page.

To allocate devices to an account:

1. Click **Account management**->**SFB account/SIP account/YMS account/Cloud account/H.323 account**.
2. Click ✎ beside the desired account.
3. Click **Add**.
4. Select the device model and the available MAC.
5. Click **Save**.

   The account information is updated to the allocated device(s).

Related topics

Adding Accounts

Setting site for Accounts

You can set the site for your account according to the needs of different sites for users. Note that one account can only set one site.

To set site for accounts:

1. Click **Account management**->**SFB account/SIP account/YMS account/Cloud account/H.323 account**.
2. Check the checkbox of the account that you need to set site for.
3. Click **Site settings**.
4. Select a desired site.
5. Click **Sure**.

Related topics

Managing Sites

Exporting Accounts

You can export basic information of all accounts.

To export accounts:

1. Click **Account management**->**SFB account/SIP account/YMS account/Cloud account/H.323 account**.
2. From the top right of the page, click **Export**.
3. Save the file to your local system.

   You can view the basic information of all accounts in the file.

Deleting Accounts

You can delete one account or more at a time whether it is allocated or not.

To delete accounts:

1. Click **Account management**->**SFB account/SIP account/YMS account/Cloud account/H.323 account**.
2. Check the checkboxes of the accounts that you want to delete.

   If the account you checked has allocated the device or the allocation status is **Exceptional**, it prompts “Sure to delete the account? After deletion, the allocating relation will be removed!”.
3. Click **Sure** to delete the accounts.

Managing Devices

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

Topic includes:

- Managing Devices
- Managing Firmware
- Managing Resource

Managing Devices

Adding Devices

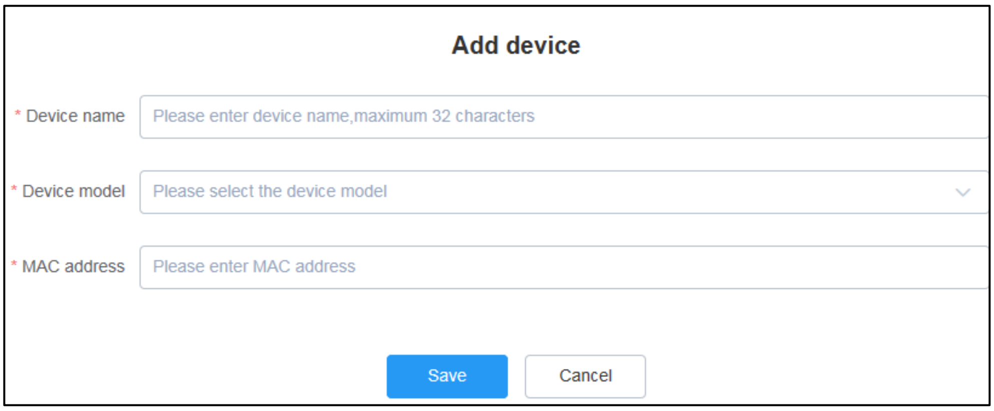
You can preconfigure device information by adding devices.

Note that you need to deploy the device to connect to the device management platform.

Adding Devices Manually

To add devices manually:

1. Click **Device management**->**Device list**.
2. From the top right of the page, click **Add devices**.
3. Configure the device information in the corresponding filed.



Add device

* Device name: Please enter device name,maximum 32 characters

* Device model: Please select the device model

* MAC address: Please enter MAC address

4. Click **Save**.

   The device will display in the device list.

Related topics

Deploying the Devices

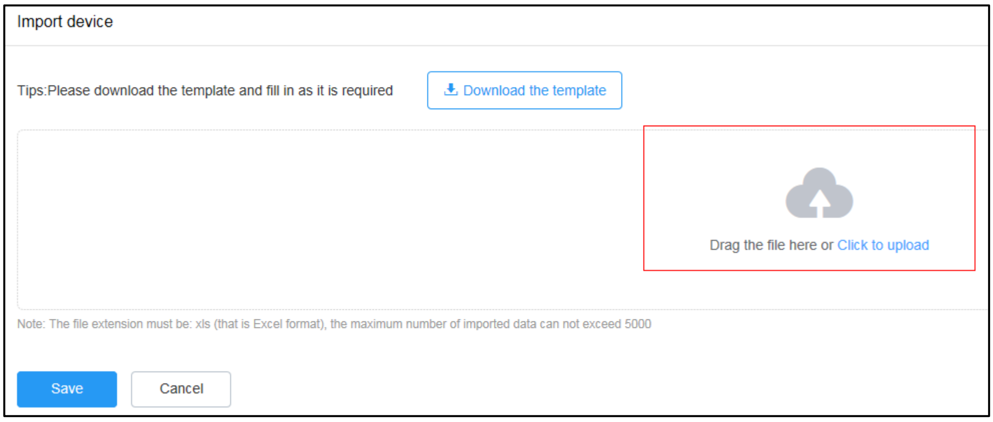
Importing Devices

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

To import devices:

1. Click **Device management**->**Device list**.
2. From the top right of the page, click **Import**.
3. Click **Download the template**.
4. Add the device information to the template and save it to your local system.

   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.



Import device

Tips:Please download the template and fill in as it is required

Drag the file here or Click to upload

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

6. Click **Save** to import devices.

Note Read the note in the template before editing.

Related topics

Deploying the Devices

Editing Devices

You can only edit the device name.

To edit devices:

1. Click **Device management**->**Device list**.
2. Click ✎ beside the desired account.
3. Edit the device name.
4. Click **Save**.

Exporting Devices

You can export basic information of all devices.

To export devices:

1. Click **Device management**->**Device list**.
2. From the top right of the page, click **Export**.
3. Save the file to your local system.

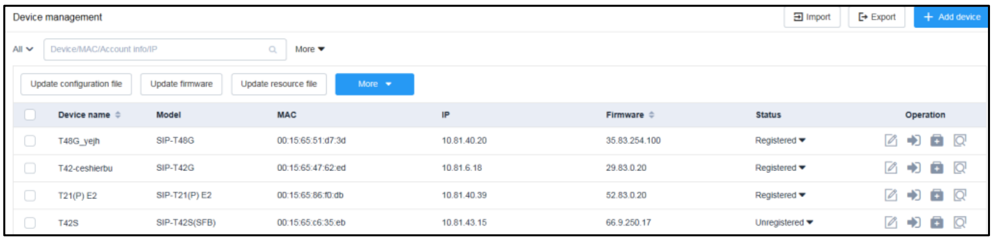
   You can view the basic information of all devices in the file.

Viewing Devices

To view devices:

1. Click **Device management**->**Device list**.

   The page will display device name, model, MAC, IP, firmware, status and view more devices info.



□	Device name	Model	MAC	IP	Firmware	Status	Operation
□	T48G_yejh	SIP-T48G	00:15:65:51:d7:3d	10.81.40.20	35.83.254.100	Registered	
□	T42-ceshierbu	SIP-T42G	00:15:65:47:62:ed	10.81.6.18	29.83.0.20	Registered	
□	T21(P) E2	SIP-T21(P) E2	00:15:65:86:f0:db	10.81.40.39	52.83.0.20	Registered	
□	T42S	SIP-T42S(SFB)	00:15:65:c6:35:eb	10.81.43.15	66.9.250.17	Unregistered	

2. Click the status of the desired device, you can view the network information (IP, subnet and report time).

   If the device has registered with an account, you can also view the registered account information of the device.
3. Click beside the desired device to view more information.

Searching for Devices

You can search for devices by directly entering the device basic information or using filter conditions on the device management platform.

To search for a device:

1. Click **Device management**->**Device list**.
2. Do one of the following:
   - Search for a device directly:

     3) Enter the device name, MAC, account info or IP in the search box.

     4) Click or press **Enter** to perform a search.
   - Search for a device using filter conditions:

4) Click **All**, and then select a desired device status.

5) Click **More**, and then select a desired device type, model, firmware, DND status and site.

6) Click **Search**.

The search result displays in the device list.

Allocating Accounts to Devices

If you did not allocate an account to your device when you added the account, you can allocate accounts for the device in the device list.

To allocate accounts for devices:

1. Click **Device management**->**Device list**.
2. Clic ➡ beside the desired device.
3. Check the checkboxes of the desired accounts to log in.

   The right side of the page displays the selected accounts and registered amounts.
4. Click **Confirm**.

   The allocated account information is pushed the devices.

Related topics

Allocating Devices to Accounts

Enabling/Disabling DND

The device management platform supports enabling/disabling the DND feature for single or multiple devices.

To enable/disable DND:

1. Click **Device management**->**Device list**.
2. Check the checkboxes of the desired device.
3. Click **More**, and then select **DND/Cancel DND** from the pull down list.
4. If you select a single device, you need to select the DND/Cancel DND accounts for the device.
5. Select a desired execution mode:
   - If you mark the radio box of **At once**, it will be executed immediately after you click **Confirm**.
   - If you mark the radio box of **Timing**, configure the task name, repeat type and the execution time, it will be executed at specified time.

6. Click **Confirm**.

Note

Only when all devices allocated to the account have enabled DND will the account display the status icon ⛔ .

Sending Message to Devices

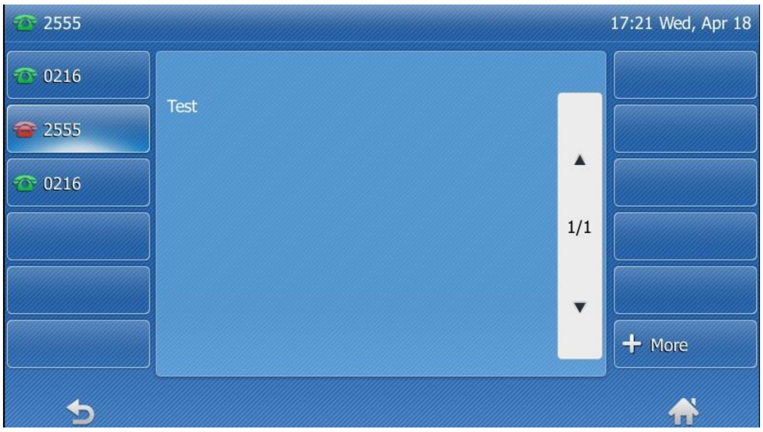
You can send the message to the devices and configure the duration that the message displays on the devices' screen.

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

To send Message to devices:

1. Click **Device management**->**Device list**.
2. Check the checkboxes of the desired devices.
3. Click **More**, and then select **Send message** from the pull down list.
4. Select a desired value from the pull-down list of **Display duration**.
5. Enter the content in the corresponding field.
6. Click **Confirm**.

   The message will pop up on the device screen.



Test

(Take the T48S IP phone as an example)

Managing Firmware

Adding Firmware

To add firmware:

1. Click **Device management**->**Firmware management**.
2. From the right top of the page, click **Add firmware**.

3. Configure the firmware information in the corresponding filed.
4. Click **Click to upload** to upload the firmware file.
5. Click **Save**.

   The firmware will display in the firmware list.

Search for Firmware

To search for firmware:

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

   You can also click **All**, and then select a desired device model to use the filter condition.
3. Click 🔍 or press **Enter** to perform a search.

   The search result displays in the firmware list.

Pushing Firmware to Devices

You can choose one of the following to push firmware to devices:

- Push the specified firmware to devices
- Update the firmware of the specified devices

Pushing the Specified Firmware to Devices

To push the specified firmware to devices:

1. Click **Device management**->**Firmware management** to enter the Firmware management page.
2. Click ➦ beside the desired firmware.
3. Check the checkboxes of the desired devices you want to push.

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

   The right side of the page displays the selected devices.
4. Click **Push to update**.
5. Select a desired execution mode:
   - If you mark the radio box of **At once**, the device firmware will be updated at once.
   - If you mark the radio box of **Timing**, configure the task name, repeat type and the execution time, the device firmware will be updated in the specified time.
6. Click **Confirm**.

   The current firmware of the devices will be updated.

Updating the Firmware of the Specified Devices

To update the firmware of the specified devices:

1. Click **Device management**->**Device list** to enter the Device list page.
2. Check the checkboxes of the desired devices.

   You can only select devices which are used the same firmware for centralized firmware updates.
3. Click **Update firmware**.
4. Select the available version to update.
5. Select a desired execution mode:
   - If you mark the radio box of **At once**, the device firmware will be updated at once.
   - If you mark the radio box of **Timing**, configure the task name, repeat type and the execution time, the device firmware will be updated at specified time.
6. Click **Confirm**.

   The current firmware of the devices will be update.

Editing Firmware

You can modify the firmware information or upload new firmware.

To edit firmware:

1. Click **Device management**->**Firmware management**.
2. Click ✎ beside the desired firmware.
3. Edit the related information of the firmware in the corresponding field.
4. Click **Save**.

Downloading Firmware

To download firmware:

1. Click **Device management**->**Firmware management**.
2. Click ⬇ beside the desired firmware to download it to your local system.

Deleting Firmware

To delete firmware:

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

   It prompts “Sure to delete the firmware? After deletion, the data can not be restored.”

4. Click **Confirm**.

Managing Resources

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

Adding Resource Files

To add a resource file:

1. Click **Device management**->**Resource management**.
2. From the right top 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**.

   The resource will display in the all resource list.

Search for Resources

To search for resources:

1. Click **Device management**->**Resource management**.
2. Enter the resource name, file name or description of the resource in the search box.

   You can also click **All**, and then select a desired resource type to use the filter condition.
3. Click 🔍 or press **Enter** to perform a search.

   The search result displays in the resource list.

Pushing Resource Files to Devices

You can choose one of the following to push resource file to devices:

- Push the specified resource file to devices
- Update the resource file of the specified devices

Pushing the Specified Resource File to Devices

To push the specified resource files to devices:

1. Click **Device management**->**Resource management** to enter the Resource management page.
2. Click ➦ beside the desired resource.
3. Check the checkboxes of the desired devices you want to push.

You can select a site, device model 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 mark the radio box of **At once**, the resource will be updated at once.
   - If you mark the radio box of **Timing**, configure the task name, repeat type and the execution time, the resource will be updated at specified time.
6. Click **Confirm**.

   The current resource of the devices will be updated.

Updating Resource Files of the Specified Devices

To update resource files of the specified devices:

1. Click **Device management**->**Device list** to enter the Device list page.
2. Check the checkboxes of the desired devices.
3. Click **Update resource file**.
4. Select the desire resource type and available resource.
5. Select a desired execution mode:
   - If you mark the radio box of **At once**, the resource file will be updated at once.
   - If you mark the radio box of **Timing**, configure the task name, repeat type and the execution time, the resource file will be updated at specified time.
6. Click **Confirm**.

   The current resource file of the devices will be updated. The devices will fail to update if not support this type of resource file.

Editing Resource Files

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

To edit resource files:

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

Downloading Resources

To download a resource:

1. Click **Device management**->**Resource management**.

2. Click ⬇ beside the desired resource to download it to your local system.

Deleting Resources

To delete resources:

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

   It prompts "Sure to delete the resource? After deletion, the data can not be restored."
4. Click **Confirm**.

Managing Device Configuration

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

Topic includes:

- 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 (registered or unregistered) devices are updated in real time when they receive updates. Offline devices will automatically update them when they connect to the platform.

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

You can add configuration templates to manage the corresponding models of devices.

To add a configuration template:

1. Click **Device configuration**->**Model configuration**.
2. From the top right of the page, click **Add template**.
3. Enter the template name, select the device model, and edit the description.
4. Click **Save**.

Setting Parameters

You can choose one of the method to configure parameters:

- Set parameters in text
- Set the template parameters.

Setting Parameters in Text

You can configure any parameter supported by the devices in text. You should edit the parameters in the required format.

To set parameters in text:

1. Click **Device configuration**->**Model configuration**.
2. Click ⋯ beside the desired template.
3. Select **Editing parameters in text** from the pull-down list.
4. Configure the parameters in the text.
5. Click **Save**.

Setting Template Parameters

You can configure parameters on the Set template parameters page.

To set template parameters:

1. Click **Device configuration**->**Model configuration**.
2. Click ⚙ beside the desired template.
3. Configure the parameters on the Set template parameters page.
4. Click **Save**.

   It prompts "Set successfully! Update the device configuration now?".
5. Click **No**, the parameter configuration will be saved.

   You can also click **Yes** to update the device configuration.

Pushing Parameters to Devices

You can push the parameters to devices if you have set parameters for the configuration template.

Before you begin:

1. Add the configuration template.
2. Set parameters.

To push parameters to devices:

3. Click **Device management**->**Model configuration**.
4. Click ↗ beside the desired template.
5. Check the checkboxes of the desired devices you want to push.

   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.
6. Click **Push to update**.

7. Select a desired execution mode:

   - If you mark the radio box of **At once**, the parameters will be updated at once.
   - If you mark the radio box of **Timing**, configure the task name, repeat type and the execution time, the parameters will be updated at specified time.

8. Click **Confirm**.

   The current parameters of the devices will be updated.

Related topics

Adding Configuration Templates

Setting Parameters

Editing Configuration Templates

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

To edit a configuration template:

1. Click **Device configuration**->**Model configuration**.
2. Click ⋯ beside the desired template.
3. Select **Edit template** from the pull-down list.
4. Edit the template information.
5. Click **Save**.

Viewing Parameters

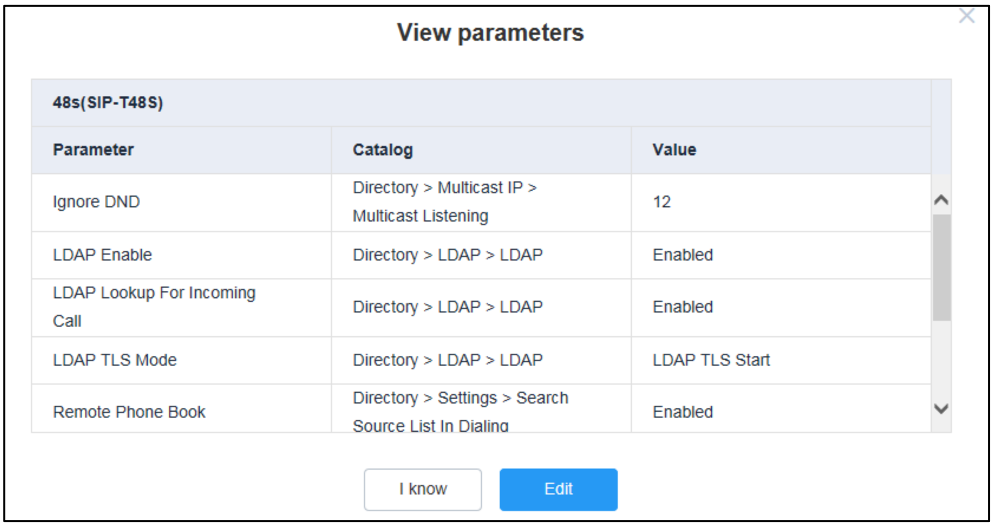
You can quickly view the parameter information to check them.

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

To view parameters:

1. Click **Device management**->**Model configuration**.

2. Click 🔍 beside the desired template.



View parameters

48s(SIP-T48S)

Parameter	Catalog	Value
Ignore DND	Directory > Multicast IP > Multicast Listening	12
LDAP Enable	Directory > LDAP > LDAP	Enabled
LDAP Lookup For Incoming Call	Directory > LDAP > LDAP	Enabled
LDAP TLS Mode	Directory > LDAP > LDAP	LDAP TLS Start
Remote Phone Book	Directory > Settings > Search Source List In Dialing	Enabled

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

Deleting Templates

To delete templates:

1. Click **Device management**->**Model configuration**.
2. Check the checkboxes of the desired templates.
3. Click **Delete**.

   It prompts “Sure to delete? After the deletion, the timer task using this template will fail.”
4. Click **Confirm**.

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. while the offline devices will automatically update them once they connect to the platform.

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

Adding Groups

You can add groups to manage the corresponding devices of this group.

To add a group:

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

2. From the top right of the page, click **Add group**.
3. Enter the group name and description.
4. Click **Next step** to enter the group device setting page.
5. Check the checkboxes of the desired devices.

   You can select a desired site, a device model or the device related information to search the device.

   The right side of the page displays the selected devices.
6. Click **Next step** to enter the setting the device 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 of this group.

Setting Parameters

You can choose one of the method to configure parameters for the group:

- Set parameters in text
- Set the template parameters.

Editing Parameters in Text

You can configure any parameter supported by the devices in each group in text. You should edit the parameters in the required format.

You can also update the configuration after setting the parameters.

To edit parameters in text:

1. Click **Device configuration**->**Group configuration**.
2. Click ··· beside the desired group.
3. Select **Editing parameters in text** from the pull-down list.
4. Configure the parameters in the text.
5. Click **Save**.

   It prompts “Set successfully! Update the device configuration now?”.
6. Click **No**, the parameters will be saved.

   You can also click **Yes** to update the parameter configuration.

Setting Template Parameters

You can configure parameters for each group on the Set template parameters page. You can also update the configuration after setting the parameters.

To set template parameters:

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

2. Click ⚙ beside the desired group.
3. Configure the parameters on the Set template parameters page.
4. Click **Save**.

   It prompts "Set successfully! Update the device configuration now?".
5. Click **No**, the parameter configuration will be saved.

   You can also click **Yes** to update the device configuration.

Editing Groups

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

To edit groups:

1. Click **Device configuration**->**Group configuration**.
2. Click --- beside the desired group.
3. Select **Edit group** from the pull-down list.
4. Follow the steps to edit the information of the group configuration.
5. Click **Save**.

Related topics

Adding Group

Updating the Group Device

You can add or delete devices for groups.

To update the group device:

1. Click **Device configuration**->**Group configuration**.
2. Click ⬆ beside the desired group.
3. Check the checkboxes of the desired devices.

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

   The right side of the page displays the selected devices.
4. Click **Save**.

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

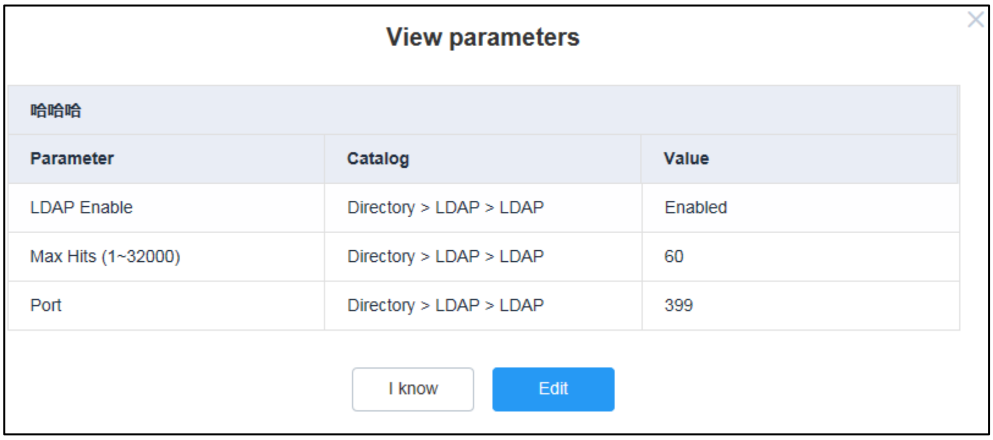
Viewing Parameters

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

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

To view parameters:

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



View parameters

哈哈哈

Parameter	Catalog	Value
LDAP Enable	Directory > LDAP > LDAP	Enabled
Max Hits (1~32000)	Directory > LDAP > LDAP	60
Port	Directory > LDAP > LDAP	399

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

Related topics

Adding Group

Downloading Configuration Files

To download configuration files:

1. Click **Device configuration**->**Group configuration**.
2. Click ⋯ beside the desired group.
3. Click ⬇ from the pull-down list to download the configuration file to your local system

Deleting Groups

To delete groups:

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

   It prompts “Delete the configuration?”.
4. Click **Confirm**.

Managing MAC Configuration

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

Uploading backup Files

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

To upload a backup file:

1. Click **Device configuration**->**MAC configuration**.
2. Click **Upload backup file**.
3. Click **Please select the file** to select the backup from the local system.
4. Click **Confirm**.

Generating Configuration Files

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

To generate configuration files:

1. Click **Device configuration**->**MAC configuration**.
2. From the top right of the page, click **Generate config file**.
3. Check the checkboxes of the desired devices.

   You can select a desired site, a device model or the device related information to search the device.

   The right side of the page displays the selected 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

To push backup files to devices:

1. Click **Device configuration**->**MAC configuration**.
2. Click ➦ beside the desired MAC address to send the backup file and restore backup.

Note

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.

Downloading Backup Files

You can download the backup files locally.

To download backup Files:

1. Click **Device configuration**->**MAC configuration**.
2. Click ⬇ beside the desired MAC to download the backup to your local system.

Exporting Backup Files

To export backup files:

1. Click **Device configuration**->**MAC configuration**.
2. From the top right of the page, click **Export**.
3. Save the file to your local system.

   You can view all backups in the file.

Deleting Backup Files

To delete a backup file:

1. Click **Device configuration**->**MAC configuration**.
2. Check the checkboxes beside the desired MAC address.
3. Click **Delete**.

   It prompts "Sure to delete? The data can not be restored after deletion?".
4. Click **Confirm**.

Configuring Global Parameters

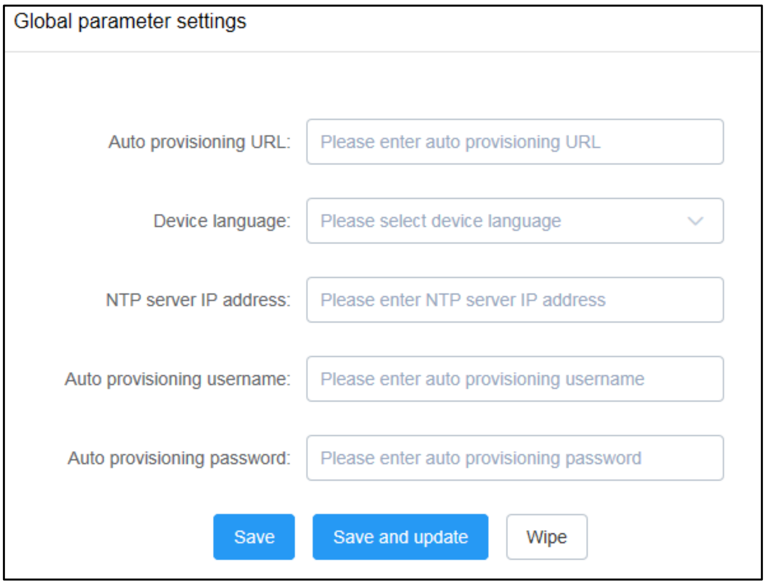
The global parameter applies to all devices connected to the device management platform.

Note that when the device connects to the management platform for the first time, they will automatically update the parameters.

To configure global parameters:

1. Click **Device configuration**->**Global parameters**.

2. Configure the global parameters in the corresponding field.



Global parameter settings

Auto provisioning URL: Please enter auto provisioning URL

Device language: Please select device language

NTP server IP address: Please enter NTP server IP address

Auto provisioning username: Please enter auto provisioning username

Auto provisioning password: Please enter auto provisioning password

3. Click **Save**.

   You can also click **Save and update** 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.

To update configuration:

1. Click **Device configuration**->**Configuration update**.
2. Click **Select** to upload the file.
3. Click **Upload**.

Managing Tasks

Topic includes:

- Managing Timer Tasks
- Executed Tasks

Managing Timer Tasks

Adding Timer Tasks

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. The platform will not push the file to the devices which is not supported by this device.
Update firmware	If you select the devices in different models, only the firmware that applies to all the devices can be updated.
DND/Cancel DND	DND/Cancel DND is enabled for all registered accounts on the device.

To add a timer task:

1. Click **Task management**->**Timer task management**.
2. From the top right of the page, click **Add timer task**.
3. Check the checkboxes of the desired devices.

   You can select a site, device model or enter the device information to search the devices.

   The right side of the page displays the selected devices.
4. Configure the task name, content and 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**.

To edit timer task:

1. Click **Task management**->**Timer task management**.
2. Check the desired checkbox.
3. Click ✎ beside the desired task name.

4. Edit the timer task information in the corresponding field.
5. Click **Save**.

Pausing or Enabling Timer Tasks

To pause or enable timer tasks:

1. Click **Task management**->**Timer task management**.
2. Click ⏸ beside the desired task name to pause the timer task.

   If you want to enable the timer task, click ✓ .

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 to be executed until it ends. Once you end the task, they will no longer be executed.

To end timer tasks:

1. Click **Task management**->**Timer task management**.
2. Click ✕ beside the desired task name.

Searching for Timer Tasks

You can search for timer tasks by directly entering the related information or using filter conditions on the device management platform.

To search for timer tasks:

1. Click **Task management**->**Timer task management**.
3. Do one of the following:
   - Search for a timer task directly:

     1) Enter a few or all characters of task name in the search box.

     2) Click 🔍 or press **Enter** to perform a search.
   - Search for a device using filter conditions:

     1) Click **All**, and then select a desired execution status.

     2) Click **All result**, and then select a desired execution result.

     3) Click **More**, and then select a desired task content, repeat interval or enter the MAC address.

     4) Click **Search**.

   The search result displays in the timer task list.

Viewing Timer Tasks

To view timer tasks:

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

   It goes to the Executed task page. You can view the execution info when the task is executed successfully or exceptionally.

Related topics

Executed Tasks

Executed Tasks

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

Viewing the Execution Info

To view the execution Info:

1. Click **Task management**->**Executed task**.
2. Click ⓘ beside the desired task to enter the Execution detail page.

   If the task is executed exceptionally, you can check the execution exception or failure in the status field.

Retry Exceptional Tasks

If the task is exceptional, you can retry to execute it.

To retry exceptional tasks:

1. Click **Task management**->**Executed task**.
2. Click ⓘ beside the desired task to enter the Execution detail page.
3. Check the exceptional devices checkboxes, 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 using filter conditions on the device management platform.

To search for executed tasks:

1. Click **Task management**->**Executed task**.
2. Do one of the following:
   - Search for an executed task directly:
     1) Enter a few or all characters of task name in the search box.
     2) Click 🔍 or press **Enter** to perform a search.
   - Search for an executed task using filter conditions:
     1) Click **All**, and then select a desired execution status.
     2) Click **More**, and then select a desired execution mode, task content, execution time or enter the MAC address.
     3) Click **Search**.

   The search result displays in the executed task list.

Monitoring and Managing the Devices

After you log into the Yealink device management platform, you can monitor and manage the devices in the enterprise. You can view the call quality of the devices for QoE analysis and solve the problems by viewing alarms.

Topic includes:

- Viewing Call Quality Statistics
- Monitoring Alarms

Viewing Call Quality Statistics

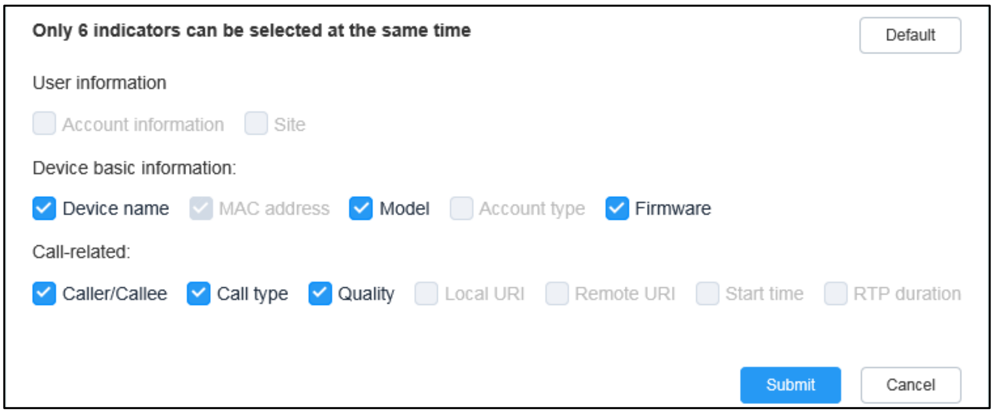
You can view the call quality and session conversation on the Call statistics page under the **Dashboard**. You can also view the details of call quality, including the user information, device basic information and call-related.

Customizing the Indicators of Call Quality Detail

You can customize the indicators displayed in the field of call quality detail, but only 6 indicators can be selected at the same time.

To customize the indicators of the call quality detail:

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:

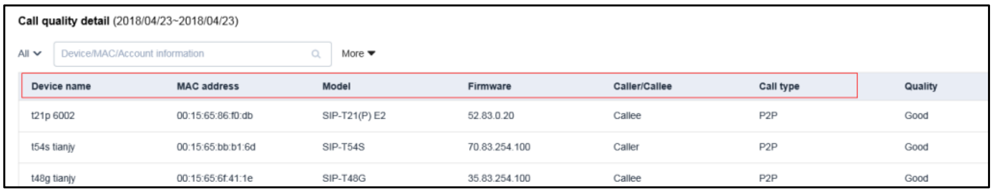
☑ Caller/Callee ☑ Call type ☑ Quality □ Local URI □ Remote URI □ Start time □ RTP duration

3. Check the checkboxes of the desired indicators.

   The MAC address is selected by default

4. Click **Submit**.

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



Call quality detail (2018/04/23~2018/04/23)

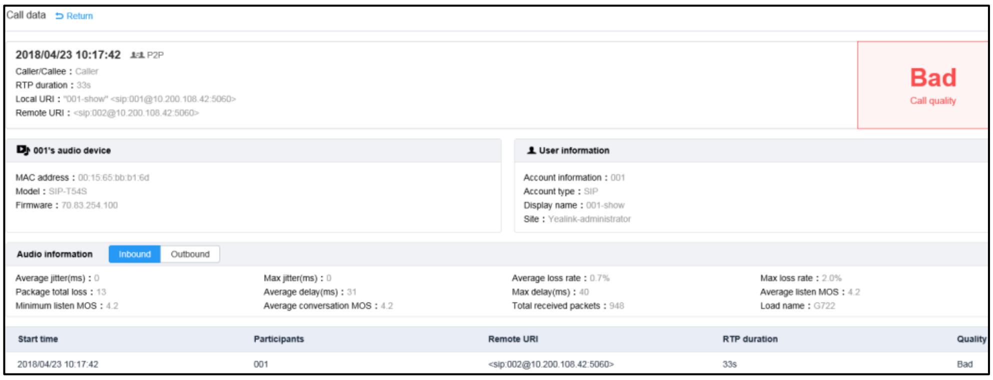
Device name	MAC address	Model	Firmware	Caller/Callee	Call type	Quality
t21p 6002	00:15:65:86:f0:db	SIP-T21(P) E2	52.83.0.20	Callee	P2P	Good
t54s tianjy	00:15:65:bb:b1:6d	SIP-T54S	70.83.254.100	Caller	P2P	Good
t48g tianjy	00:15:65:6f:41:1e	SIP-T48G	35.83.254.100	Callee	P2P	Good

Viewing the Call Data of Call Quality

To view the call data of call quality:

1. Click **Dashboard->Call statistics**.
2. Click ⓘ beside the desired call.

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



2018/04/23 10:17:42 P2P

Caller/Callee : Caller
RTP duration : 33s
Local URI : "001-show" <sip:001@10.200.108.42:5060>
Remote URI : <sip:002@10.200.108.42:5060>

Bad
Call quality

001's audio device

MAC address : 00:15:65:bb:b1:6d
Model : SIP-T54S
Firmware : 70.83.254.100

User information

Account information : 001
Account type : SIP
Display name : 001-show
Site : Yealink-administrator

Audio information

Average jitter(ms) : 0
Package total loss : 13
Minimum listen MOS : 4.2
Max jitter(ms) : 0
Average delay(ms) : 31
Average conversation MOS : 4.2
Average loss rate : 0.7%
Max delay(ms) : 40
Total received packets : 948
Max loss rate : 2.0%
Average listen MOS : 4.2
Load name : G722

Start time	Participants	Remote URI	RTP duration	Quality
2018/04/23 10:17:42	001	<sip:002@10.200.108.42:5060>	33s	Bad

Monitoring Alarms

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

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:

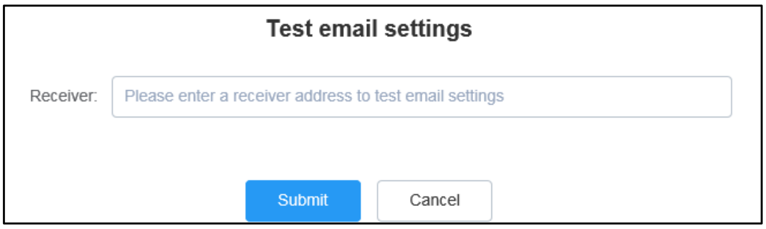
Parameter	Description
SMTP	Specifies the address of the SMTP server.
Sender	Configures the email address of the sender.
Username	Specifies the email username of the sender.

Parameter	Description
Password	Specifies the email password of the sender.
Port	Specifies the connection port.
This server requires secure connection to the	Enables or disables connection security. If connection security is enabled, you should specify the protocol to be used when it connect to the SMTP server. ● **SSL** ● **TLS**
Enable the mailbox	Enables or disables the mailbox. **Default:** Disabled

To configure the SMTP mailbox:

1. Click **System management->Sending mailbox settings**.
2. Configure the sending mailbox settings.
3. (Optional.) Check the **This server requires secure connections to the** checkbox, and then select **SSL** or **TSL** from the pull-down list.
4. Check the **Enable the mailbox** checkbox.
5. (Optional.) **Test email settings**.

   Enter the email address of the receiver.



Test email settings

Receiver: Please enter a receiver address 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 password.

6. Click **Save**.

Managing Alarm Strategies

Adding Alarm Strategies

You can add alarm strategies so that 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_defalut alarm strategy added when the system was initialized, but you can edit the receivers.

To add an alarm strategy:

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, do the following:

   1) Check the desired receiver checkboxes.

      The right side of the page displays the selected receivers.

   2) Click **Confirm**.
5. Drag the slider to enable the alarm strategy.

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

Editing Alarm Strategies

To edit alarm strategies:

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

Related topics

Adding Alarm Strategies

Deleting Alarm Strategies

To delete alarm strategies:

1. Click **Alarm management->Alarm Strategy**.
2. Click 🗑 beside the desired alarm strategy.

   It prompts "This operation will delete this alarm strategy, continue?".
3. Click **Confirm**.

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 details of the alarm.

To view alarms via the Yealink device management platform:

1. Click **Alarm management**->**Alarm list**.
2. Click ⓘ beside the desired alarm.

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

Related topics

Managing Alarm

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

To delete alarms:

1. Click **Alarm management**->**Alarm list**.
2. Check the checkboxes of the desired alarms.
3. Click **Delete**.

   It prompts "Sure to delete? The data can not be restored after deletion?".
4. Click **Confirm**.

Viewing Recordings

To view recordings:

1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Strat diagnostic**.
3. Click **Recording file** under the diagnostic tools.

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

   You can also click ⬇ to download the recording.

Capturing the Current Screen of the Device

To capturing the current screen of the device:

1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Strat diagnostic**.
3. Click **Screencapture** in the diagnostic tools.

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

Troubleshooting

This chapter helps you solve the problems you might encounter when using Yealink device management platform.

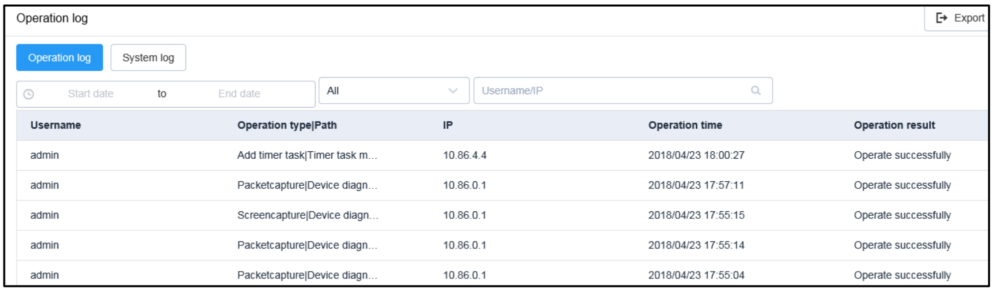
System Diagnostics

Viewing Operation Log Files

Operation logs record the operation that the administrator manages the Yealink device management.

To view operation log files:

1. Click **System management->Log management**.
2. Select **Operation log**.
3. (Optional.) Select time, operation type and path or enter the username or IP in the search box to search for the desired operation file.



Username	Operation type|Path	IP	Operation time	Operation result
admin	Add timer task|Timer task m...	10.86.4.4	2018/04/23 18:00:27	Operate successfully
admin	Packetcapture|Device diagn...	10.86.0.1	2018/04/23 17:57:11	Operate successfully
admin	Screencapture|Device diagn...	10.86.0.1	2018/04/23 17:55:15	Operate successfully
admin	Packetcapture|Device diagn...	10.86.0.1	2018/04/23 17:55:14	Operate successfully
admin	Packetcapture|Device diagn...	10.86.0.1	2018/04/23 17:55:04	Operate successfully

You can also click **Export** on the top right of the page to export all operation log files.

Viewing System Log Files

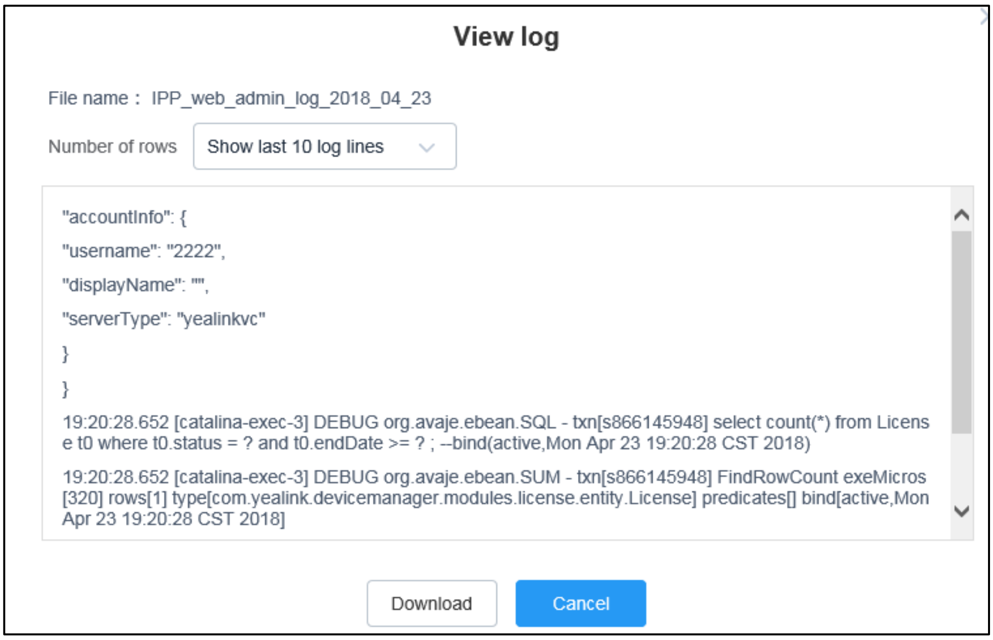
System logs record the key process or abnormal status about the Yealink device management platform in recent 7 days, such as whether the parameters reported by devices are correct or the process of sending configuration files to devices by the platform.

You can view the system logs online or download the log files to your local system to view logs.

To view system log files online:

1. Click **System management->Log management**.
2. Select **System log**.

3. Click 🔍 beside the desired system log.



File name： IPP_web_admin_log_2018_04_23

Number of rows: Show last 10 log lines

```
"accountInfo": {
"username": "2222",
"displayName": "",
"serverType": "yealinkvc"
}
}
19:20:28.652 [catalina-exec-3] DEBUG org.avaje.ebean.SQL - txn[s866145948] select count(*) from License t0 where t0.status = ? and t0.endDate >= ? ; --bind(active,Mon Apr 23 19:20:28 CST 2018)
19:20:28.652 [catalina-exec-3] DEBUG org.avaje.ebean.SUM - txn[s866145948] FindRowCount exeMicros[320] rows[1] type[com.yealink.devicemanager.modules.license.entity.License] predicates[] bind[active,Mon Apr 23 19:20:28 CST 2018]
```

4. Select a desired value from the pull down list of **Number of rows**.

Downloading System Log Files

To download the log files:

1. Click **System management**->**Log management**.
2. Select **System log**.
3. Click ⬇ beside the desired system log to download the log file and save it to your local system.

   You can also click **Download all** from the top right of the page to download all system log files.

Device Diagnostics

On the Device diagnostics page, you can use the diagnostic tools such as log files, packet capture, and network detection and recent logs to quickly find the root cause of the problem and troubleshoot the problem.

You can enter the Device diagnostic page in the following ways:

- On the Device list page, click ➕ beside the device.
- On the Device diagnostic page, enter the MAC address of the device, and then click **Start diagnostic**.

Viewing the Syslog of Devices

The devices will send syslog message to the device management platform in real time. You can specify the severity level of the syslog to be sent to the platform.

You can preview the backup logs or download the syslog files. The platform backs up the syslog files once a day and only saves them for last seven days.

Setting the Log Level

To set the log level:

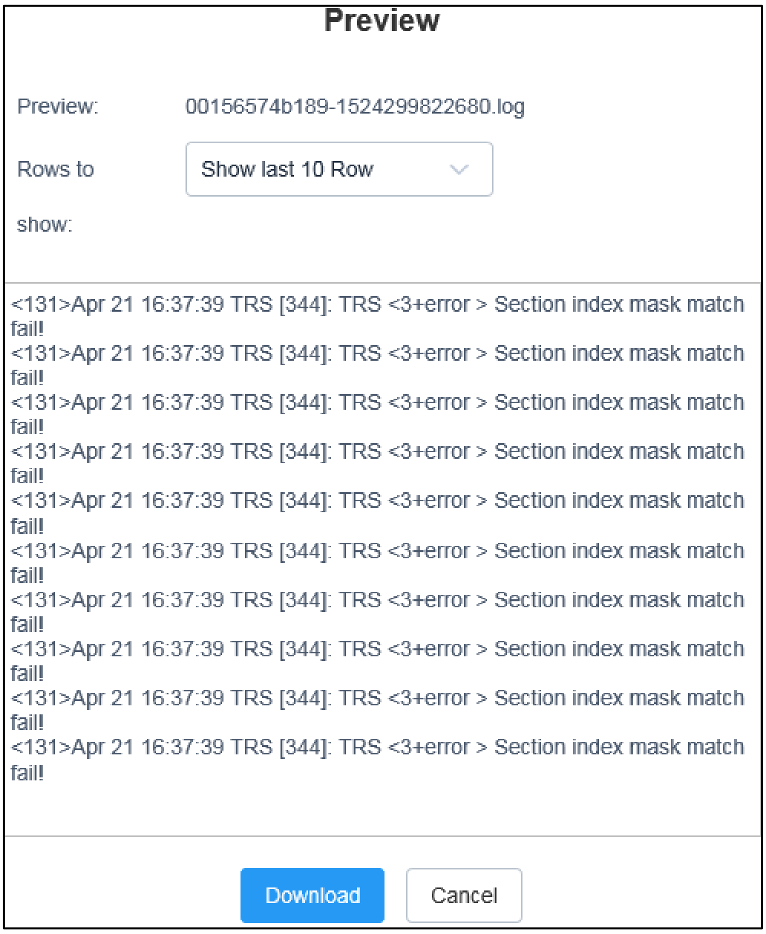
1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Start diagnostic**.
3. Click ✎ on the left of log level.
4. Set a desired log level.
5. Click **Confirm**.

Previewing the Backup Syslog

To preview the backup syslog online:

1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Start diagnostic**.
3. Click 🔍 beside the desired log in the recent logs list.

4. Select a desired number of rows in the pull down list of **Rows to**.



Preview

Preview: 00156574b189-1524299822680.log

Rows to show: Show last 10 Row

```
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
<131>Apr 21 16:37:39 TRS [344]: TRS <3+error > Section index mask match
fail!
```

Downloading the Backup Syslog Files

To download the backup syslog files:

1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Start diagnostic**.
3. Click ⬇ beside the log in the recent logs list to download the syslog files and save it to your local system.

   If you want to download syslog files in batch, you can check the checkboxes of the desired syslog files and then click **Batch download**.

Capturing Packets

To capture packets:

1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Start diagnostic**.
3. Click **Packetcapture** in the diagnostic tools.
4. Select a desired Ethernet and type and enter the packetcapture string.

You can enter the packetcapture string only when you select custom for the packetcapture type.

5. Click **Start** to begin capturing signal traffic.

   You can click **Finish** to manually stop the capture or just wait until it stops automatically.

6. Save the file to your local system.

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

Network Diagnostics

Network diagnostics includes:

- **Ping**: Check whether the network between the local and the remote system is connected.
- **Trace Route**: Display the route (path) and measure transit delays of packets across an Internet Protocol (IP) network.

To diagnose network:

1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Start diagnostic**.
3. Click **Network detection**.
4. Select **Ping(ICMP Echo)** or **Trace route**.
5. Enter the IP address (for example, the IP address of the remote system) or domain name in the **IP/Domain name** field.

   Ping: It measures the round-trip time from transmission to reception and reports errors and packet loss. The results of the test include a statistical summary of the response packets received, including the minimum, the maximum, and the mean round-trip times.

   Trace route: If the test is successful, the platform lists the hops between the system and the IP address you entered. You can check whether congestion happens via the time cost between hops.

6. Select the request time from the pull-down list of **Request times**.
7. Click **Confirm** to start.

Exporting System logs

You can export the current system logs to diagnose the device. It is only available for online devices.

To export system logs:

1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Start diagnostic**.

3. Click **Export system log** under the diagnostic tools.
4. Save the file to your local system.

Exporting Configuration Files

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

To export configuration files:

1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Start diagnostic**.
3. Click **Export configuration file** under the diagnostic tools.
4. Select a desired file type.

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

Viewing the CPU and Memory Status

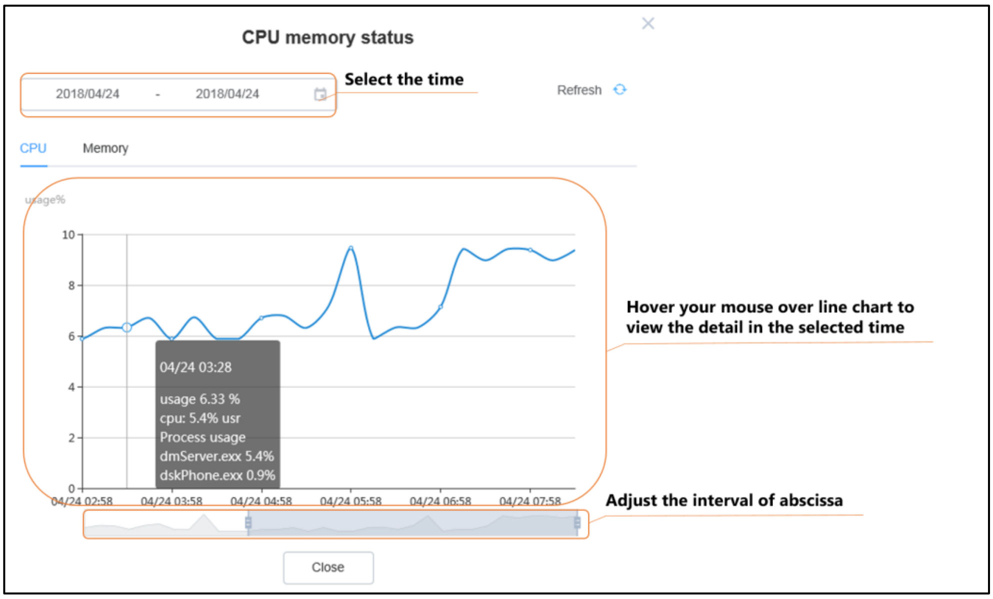
When the call quality is bad, you can view the CPU and memory status of devices. The devices will report the CPU and memory information to the platform every 15 minutes.

To view the CPU and memory status:

1. Click **Device diagnostic**.
2. Enter the MAC address of the device, and then click **Start diagnostic**.
3. Select **CPU memory status**.

4. You can do one of the following:

   − Click **CPU** to view the CPU usage in the specified time.



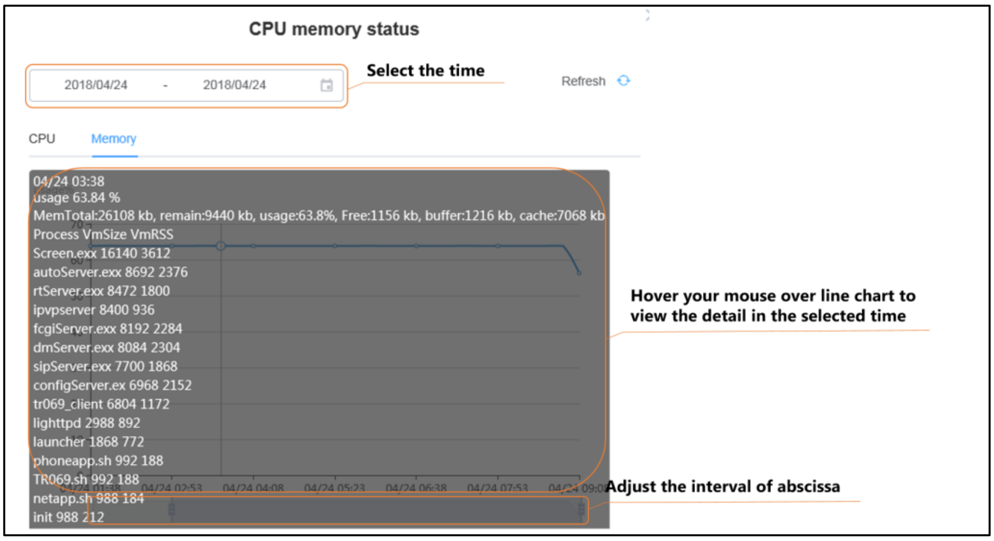
```
04/24 03:28

usage 6.33 %
cpu: 5.4% usr
Process usage
dmServer.exx 5.4%
dskPhone.exx 0.9%
```

Select the time

Hover your mouse over line chart to view the detail in the selected time

Adjust the interval of abscissa

   − Click **Memory** to view the memory usage at specified time.



```
04/24 03:38
usage 63.84 %
MemTotal:26108 kb, remain:9440 kb, usage:63.8%, Free:1156 kb, buffer:1216 kb, cache:7068 kb
Process VmSize VmRSS
Screen.exx 16140 3612
autoServer.exx 8692 2376
rtServer.exx 8472 1800
ipvpserver 8400 936
fcgiServer.exx 8192 2284
dmServer.exx 8084 2304
sipServer.exx 7700 1868
configServer.ex 6968 2152
tr069_client 6804 1172
lighttpd 2988 892
launcher 1868 772
phoneapp.sh 992 188
TR069.sh 992 188
netapp.sh 988 184
init 988 212
```

Select the time

Hover your mouse over line chart to view the detail in the selected time

Adjust the interval of abscissa

Troubleshooting Solutions

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.

Rebooting Devices

To reboot devices:

1. Click **Device management**->**Device list**.
2. Check the checkboxes of the desired devices.
3. Click **More**, and then select **Reboot** from the pull down list.
4. Select a desired execution mode:
   - If you mark the radio box of **At once**, the devices will reboot at once.
   - If you mark the radio box of **Timing**, configure the task name, repeat type and the execution time, the devices will reboot at specified time.
5. Click **Confirm**.

Resetting the Devices to Factory

Reset the devices to factory defaults after you have tried almost all troubleshooting suggestions but do not solve the problem.

To reset the devices to factory:

1. Click **Device management**->**Device list**.
2. Check the checkboxes of the desired devices.
3. Click **More**, and then select **Reset to factory** from the pull down list.
4. Select a desired execution mode:
   - If you mark the radio box of **At once**, the devices will be reset at once.
   - If you mark the radio box of **Timing**, configure the task name, repeat type and the execution time, the devices will be reset at specified time.
5. Click **Confirm**.

   All configurations and user data on the devices will be reset.

General Issues

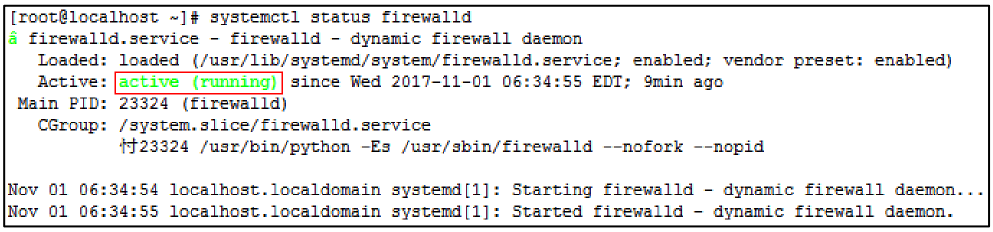
Why cannot you access the login page of Yealink device management platform

- Check the network connection of the devices.
- Whether the firewall of your server is active.
- Run Network Diagnostics of Windows

To check the status of firewalls (log into CentOS as the root user):

1. Enter 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=28443/tcp

firewall-cmd --permanent --zone=public --add-port=9090/tcp

firewall-cmd --reload

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 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 professional certificate issuing authorities. So, 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.

To replace our certificate:

1. Enter terminal.
2. Generate dm.12 file, run the command:

   Openssl pkcs12 -export -in dm.drt -inkey dm.key -out dm.p12 -name dm

   It will prompt you to create your own password and re-enter the password. You need to remember this password.
3. Generate Keystore file (jks file), run the command:

   Keytool -importkeystore dm.pl12 -srcstoretype PKCS12 -destkeystore dm.jks

   It will prompt you to enter the password you set in step 2, and then enter a new keystore password.
4. (Optional.) Generate public key, run the command:

   Openssl rsa -in dm.key -out dm_public.key
5. (Optional.) Merge the root certificate, run the command:

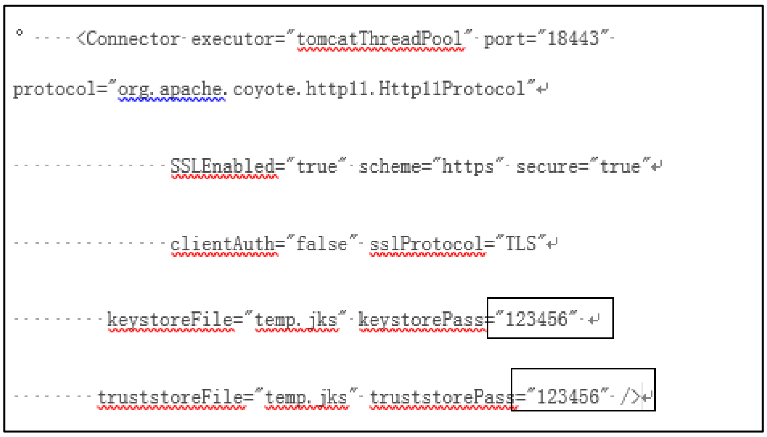
Keytool -keystore dm.jks -import -trustcacerts -alias alias -file ca.crt

The certificate is converted to the dm.jks file.

6. Replace /usr/local/yealink/dm/tomcat_dm/dm.jks with the dm.jsk generated in step 5.

7. Change the keystore and truststore passwords you set at the path of /usr/loca/yealink/dm/tomcat_dm/conf/server.xml.

Suppose that 123456 is your keystore and truststore password.



```
°    <Connector executor="tomcatThreadPool" port="18443"
protocol="org.apache.coyote.http11.Http11Protocol"
               SSLEnabled="true" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
         keystoreFile="temp.jks" keystorePass="123456"
        truststoreFile="temp.jks" truststorePass="123456" />
```

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