



Yealink Meeting Server Administrator Guide

Version 10.23.0.55
Apr.2018

Copyright

Copyright © 2018 YEALINK (XIAMEN) NETWORK TECHNOLOGY

Copyright © 2018 Yealink (Xiamen) Network Technology CO., LTD. All rights reserved. No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Yealink (Xiamen) Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

When this publication is made available on media, Yealink (Xiamen) Network Technology CO., LTD. gives its consent to downloading and printing copies of the content provided in this file only for private use but not for redistribution. No parts of this publication may be subject to alteration, modification or commercial use. Yealink (Xiamen) Network Technology CO., LTD. will not be liable for any damages arising from use of an illegally modified or altered publication.

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

This guide provides daily operations and maintenance for enterprise administrators to use YMS.

Introduction to Yealink Meeting Server

The Yealink Meeting Server (YMS) is a distributed cloud-based video conferencing infrastructure tailored for HD video conferencing collaboration in the modern workplace. A powerful all-in-one meeting server, YMS brings MCU, registrar server, directory server, traversal server, meeting and device management server, SIP Trunk, WebRTC server and GK & H.460 server together. Seamlessly working with Yealink VC devices, the Yealink Meeting Server brings people together at any time from any location with the touch of a button.

Intended Audience

This guide is mainly intended for:

- Distributor
- Network administrator

Conventions

The topic describes the conventions in the document.

General Conventions

Convention	Description
Bold	Highlights the user interface items such as menus or menu selections when they are involved in a procedure or user action (for example, click Log In). Also used to emphasize text.
Colored Text	Used for cross references to other sections within this documentation (for example, refer to SMTP Mailbox).
<i>Blue Text in Italics</i>	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (for example, for more information, refer to Yealink Meeting Server User Guide).

GUI Conventions

Convention	Description
->	Indicates the menu path. For example, Status->System information indicates the path of entering system information page.

Basic Concepts

As you read this guide, you'll notice that the same concepts are used repeatedly. Make sure you familiarize yourself with these concepts.

Enterprise directory: This concept mainly refers to the directory which includes user accounts, room system accounts and third party devices.

Yealink VC devices: This concept refers to the endpoints that support YMS, including VC800/VC500/VC400/VC120/VC110 video conferencing endpoint, SIP VP-T49G IP phone, SIP-T58V IP phone, VC Desktop and VC Mobile.

Interactive parties: This concept mainly refers to the participants who send video or audio in the broadcasting interactive conference.

Broadcasting parties This concept mainly refers to the participants who only receive video or audio and do not send video or audio in the broadcasting interactive conference.

Setup Files

You can obtain the setup file of YMS from the Yealink distributor or Yealink technical support engineer.

Hardware and Software Recommendations

The following table lists the hardware and software recommendation of YMS.

Feature	Description
CPU	Intel Xeon E5-2600 series (Haswell architecture) or similar Xeon processors from 2012 or later, 2.3 GHz or faster. A CPU should match 4 RAM.
RAM	4GB/DDR3/2133MHz/ECC or higher 8GB/DDR4/2400MHz/ECC or higher
Hard Drive Space	300GB or higher
Network	<ul style="list-style-type: none"> Gigabit Ethernet connectivity is strongly recommended. In general, you can expect 1 Mbps in a one-way 720P video call. And you can expect 2 Mbps in a one-way 1080P video call.

Feature	Description
Capacity	Capacity is dependent on server specifications. As a general indication, using our recommended hardware (Intel Haswell, 10 cores, 2.3 GHz) YMS can connect: <ul style="list-style-type: none"> The maximum concurrent calls=total CPU cores*frequency. Up to extra 10 audio-only calls at 64 kbps. Servers that are older, have slower processors, or have fewer CPUs, will have a lower overall capacity.
Linux	CentOS 7.0 and later

For example, if you want to initiate 20-way 1080P concurrent calls or 40-way 720P concurrent calls, the following hardware is recommended.

CPU	2 Intel Xeon Processor E5-2620V4, eight cores and sixteen threads, 2.1GHz 20M 8.0GT/s 85W or higher
Memory	8 8GB/DDR4/2400MHz/ECC or higher

If you want to initiate 40-way 1080P concurrent calls or 80-way 720P concurrent calls, the following hardware is recommended.

CPU	2 Intel Xeon Processor E5-2680V4, fourteen cores and twenty-eight threads, 2.4GHz 35M 9.6GT/s 120W or higher
Memory	8 8GB/DDR4/2400MHz/ECC or higher

Browser Requirements

The following browsers are supported:

Browser	Version
Firefox	50 and later
Chrome	50 and later
Internet Explorer	10 and later

Port Forwarding Requirements

If the following ports are restricted in your network environment, please open these ports.













If the YMS is deployed in an Intranet, you should solve the interconnection problem between private and public network by port forwarding. You must forward the following ports to the public network on the router.

Field	Port	UDP/TCP	Effect
System	22	TCP	SSH port
	80	TCP	HTTP port
	443	TCP	HTTPS port
	514	UDP	SYSLOG port
	514	TCP	SYSLOG port
SIP	5060	TCP	SIP port
	5060	UDP	SIP port
	5061	TCP	SIP port
Turn server	3478	UDP	STUN port
	3479	UDP	STUN port
MCU broadcast service	3688	TCP	Broadcasting server listening port
WebRTC	442	TCP	WebRTC listening port
H.323 gateway	1720	TCP	H.225 listening port (TCP)
H.323 gatekeeper	1718	UDP	RAS broadcasting listening port
	1719	UDP	RAS listening port
	1722	TCP	H.225 listening port
	2776	UDP	H.460.19 RTP Multiplex port
	2777	UDP	H.460.19 RTCP Multiplex port
Media/Signaling port	30000-37999	UDP	IVR+BFCP port
	38000-49999	UDP	TURN Relay port Media Proxy port
	50000-60000	UDP	MCU conference port
	30000-39999	TCP	H.245/Q931 port (H.323 gateway)
	20000~24999	TCP	H.245 port (H.323 gatekeeper)

Field	Port	UDP/TCP	Effect
	25000~29999	TCP	Q931 port (H.323 gatekeeper)
	15000~19999	UDP	Media forwarding port (H.323 gatekeeper)

Icon Instructions

Icons appearing on the YMS are described in the following table:

Icons	Description
	Download backups
	Restore backups
	Update device firmware now
	Exporting device logs
	The room system accounts are not registered
	The room system accounts are registered
	Move up the department or the user account in Organizational Structure list
	Move down the department or the user account in Organizational Structure list
	Scheduled conferences or meet now conferences (initiated by Yealink VC devices registered the YMS account)
	Conferences which are enabled RTMP live feature
	Periodic conferences
	Meet now conferences (initiated by joining the permanent VMR)

In This Guide

Topics provided in this guide include:

- Chapter 1 [Yealink Meeting Server Installation](#)
- Chapter 2 [Basic Operation](#)
- Chapter 3 [System Status](#)
- Chapter 4 [System Management](#)
- Chapter 5 [Account Management](#)
- Chapter 6 [Meeting Room Management](#)
- Chapter 7 [Conference Control](#)
- Chapter 8 [Conference Statistics](#)
- Chapter 9 [Troubleshooting](#)
- Chapter 10 [Appendix: Time Zones](#)

Summary of Changes

This section describes the changes to this guide for each release and guide version.

Changes for Release 23, Guide Version 10.23.0.55

The following sections are new for this version:

- [Displaying Participant Name](#) on page 12
- [Sending Content Only](#) on page 16
- [Enabling RTMP Live](#) on page 16
- [Enabling Broadcasting Interactive Video Conferences](#) on page 17
- [LDAP](#) on page 21
- [SIP Trunk IVR](#) on page 29
- [GK](#) on page 36
- [Security Management](#) on page 44
- [Licenses Management](#) on page 53
- [Conference Control](#) on page 79

Major updates have occurred to the following sections:

- [H.323](#) on page 22
- [Port Settings](#) on page 37
- [Adding User Accounts](#) on page 63

- [Adding Room System Accounts](#) on page 66
- [Adding Permanent Virtual Meeting Rooms](#) on page 76

Changes for Release 23, Guide Version 10.23.0.40

The following sections are new for this version:

- [Configuring the Default Layout](#) on page 12
- [Third Party Registration](#) on page 15
- [Redialing Devices Automatically](#) on page 15
- [Record](#) on page 16
- [SIP Trunk ACL](#) on page 28
- [WebRTC](#) on page 36

Major updates have occurred to the following sections:

- [Yealink Meeting Server Installation](#) on page 1
- [Dialing Devices Automatically](#) on page 15
- [SMTP Mailbox](#) on page 41
- [Account Management](#) on page 61
- [Meeting Room Management](#) on page 73

Changes for Release 23, Guide Version 10.23.10.20

The following sections are new for this version:

- [Dialing Devices Automatically](#) on page 15
- [Call Routing](#) on page 18
- [Gateway Configuration](#) on page 21
- [H.323](#) on page 36
- [Meeting Time Zone Configuration](#) on page 40
- [Adding Permanent Virtual Meeting Rooms](#) on page 76

Major updates have occurred to the following sections:

- [Logging into Yealink Meeting Server](#) on page 3
- [Layout](#) on page 12
- [IVR Service](#) on page 15
- [Web](#) on page 33
- [Call Bandwidth](#) on page 12
- [Port Settings](#) on page 36

- [Time Access](#) on page 38
- [SMTP Mailbox](#) on page 41
- [Conference Statistics](#) on page 79

Table of Contents

About This Guide	V
Introduction to Yealink Meeting Server	v
Intended Audience	v
Conventions	v
General Conventions	v
GUI Conventions.....	vi
Basic Concepts	vi
Setup Files	vi
Hardware and Software Recommendations	vi
Browser Requirements	vii
Port Forwarding Requirements	vii
Icon Instructions	ix
In This Guide	x
Summary of Changes	x
Changes for Release 23, Guide Version 10.23.0.55	x
Changes for Release 23, Guide Version 10.23.0.40	xi
Changes for Release 23, Guide Version 10.23.10.20	xi
Table of Contents	xiii
Yealink Meeting Server Installation	1
Basic Operation	3
Logging into Yealink Meeting Server	3
Introduction to the Home Page	4
Managing Enterprise Administrator Account	5
Editing Login Password	5
Editing the Registered Emails	5
Quick Settings.....	5
Logging out of Yealink Meeting Server	8
System Status	9
Viewing System Information	9
Viewing Online Users	9
System Management	11

Call Settings	11
Global Settings	11
Call Routing.....	18
LDAP	21
Gateway Configuration	22
H.323.....	22
SIP Trunk	24
SIP Trunk ACL	28
SIP Trunk IVR.....	29
System Settings	29
Network Settings.....	29
Time/Time Zone Settings	38
SMTP Mailbox	41
Disk Space Settings	43
Security Management.....	44
Registration Blacklist.....	44
Conference Blacklist	45
IP Call Blacklist	45
System Maintenance.....	46
Device Upgrade	46
Backup/Restore	48
System Upgrade.....	51
Reboot/Reset to Factory	52
Licenses Management.....	53
Video Port Licenses	53
Broadcasting Port Licenses	54
Importing Trusted CA Certificates	55
System Logs	56
Server Logs	56
Device Logs	59
Account Management.....	61
Department Management.....	61
Adding Departments.....	62
Editing Department Information	62
Editing Upper Departments Quickly.....	62
Deleting Departments	63
Adding User Accounts.....	63
User Accounts Parameters.....	63
Adding User Accounts Manually	64
Importing User Accounts.....	65
Adding Room System Accounts	66
Adding Third Party Devices.....	68
Third Party Devices Parameters.....	68

Adding Third Party Devices Manually	68
Importing Third Party Devices.....	69
Viewing Accounts.....	69
Viewing User Accounts.....	69
Viewing Third Party Devices	70
Sending Emails to YMS Accounts.....	70
Editing Accounts.....	71
Deleting Accounts	71
Meeting Room Management	73
Adding Meeting Rooms	73
Adding General Meeting Rooms.....	73
Adding Video Meeting Rooms	74
Discussion Mode and Training Mode.....	74
Adding Permanent Virtual Meeting Rooms	76
Editing or Deleting Meeting Rooms	77
Conference Control	79
Viewing Conferences.....	79
Deleting Conferences	79
Controlling Conferences.....	80
Conference Statistics	81
Viewing Conference Statistics	81
Viewing Records.....	81
Troubleshooting.....	83
Troubleshooting Solutions	83
General Issues.....	83
Appendix: Time Zones	85

Yealink Meeting Server Installation

You can install YMS in virtual machine or physical machine. After you install YMS successfully, you need enter the setup wizard to configure the basic settings.

For more information, please refer to [Yealink Meeting Server Installation Guide](#).

Basic Operation

This chapter provides basic operating instructions for YMS.

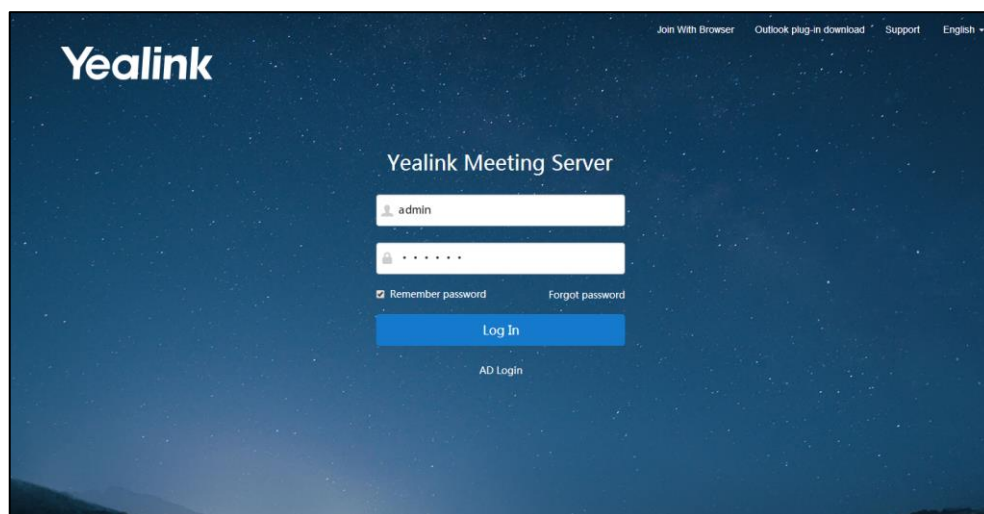
Topic includes:

- [Logging into Yealink Meeting Server](#)
- [Introduction to the Home Page](#)
- [Managing Enterprise Administrator Account](#)
- [Quick Settings](#)
- [Logging out of Yealink Meeting Server](#)

Logging into Yealink Meeting Server

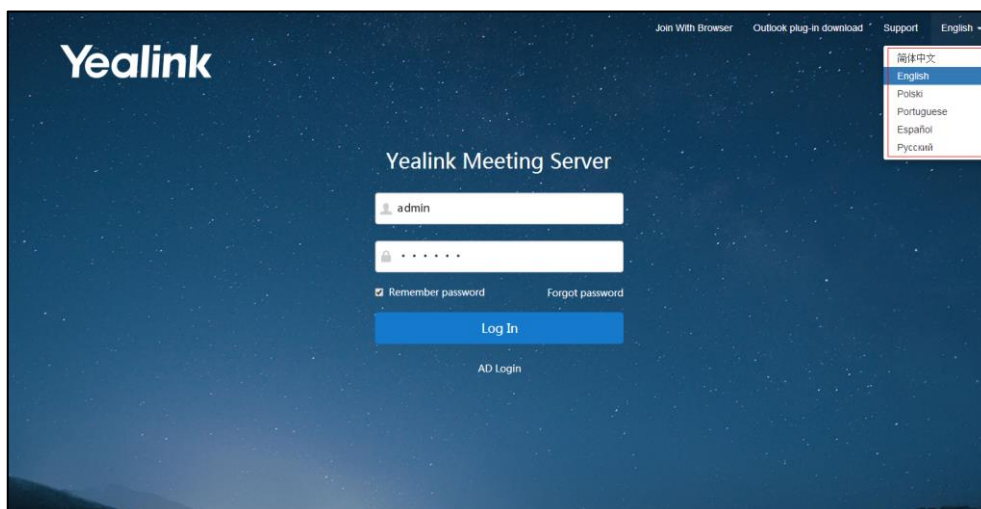
To log into YMS:

1. Open a web browser.
2. Enter the IP address or domain name of YMS in the address bar, and then press the **Enter** key to enter the YMS.
3. Enter the username and password of enterprise administrator you set in setup wizard.



4. (Optional.) To remember password, check the **Remember password** checkbox.
To ensure the security of your account, this action is not recommended on public computer.

- (Optional.) On the top-right of the page, select the desired display language from the pull-down list.



- Click **Log In**.

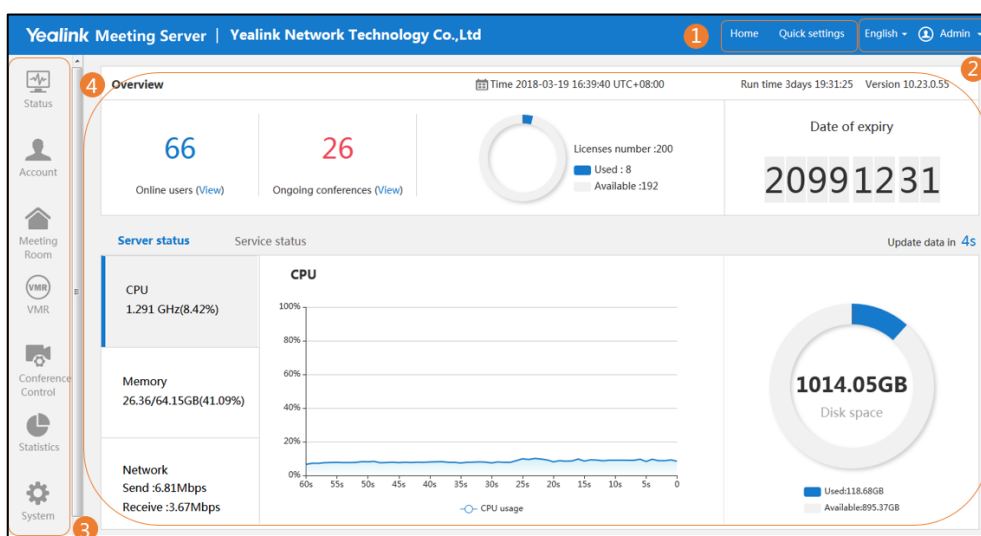
Note

If you enter the wrong password 5 times, this account will be locked for 3 minutes. Please wait 3 minutes and then try again.

If you forget password, you can click **Forgot password**, and then follow the prompts to reset the password.

Introduction to the Home Page

After you log into the YMS successfully, the home page displays as below. You should be familiar with the layout of the home page to help you quickly learn operation entries and system information.



No.	Description
1	Main entry of the home page and setup wizard.
2	The name of the account currently logged into the YMS and system language.
3	Main entry of the status, account, meeting room, VMR, call statistics and settings.
4	Overview of system status, server status and service status.

Managing Enterprise Administrator Account

Editing Login Password

To improve system security, change the password periodically.

To edit login password:

1. Click **Admin** on the top-right of the page.
2. Click **Change password**.
3. Enter the current password, new password and re-enter the new password to confirm.
4. Click **Confirm**.

Editing the Registered Emails

You can edit the email. The email is used to receive the information of resetting password and receive a warning from your system.

To edit the registered email:

1. Click **Admin** on the top-right of the page.
2. Click **Edit email** to edit the registered emails.
3. Enter the new email.
4. Click **Confirm**.

Quick Settings

You can configure network settings, time/time zone settings, username/password, license and SMTP settings quickly.

To configure settings quickly:

1. Click **Quick settings** on the top-right of the page.
2. Configure network settings.

For more information, please refer to [Network Settings](#) on page 28.

Setup wizard

[Network settings](#)
Time/Time zone settings
Edit username/password
Activate the license
SMTP mailbox settings

Native domain name :

Internal network settings

Network adapter settings :

Ethernet port type : Static IP address

IP address :

Subnet mask :

Gateway :

Preferred DNS :

Alternate DNS :

Network settings

Network adapter settings :

Ethernet port type : Static IP address

IP address :

Subnet mask :

Gateway :

Preferred DNS :

Alternate DNS :

NAT : Enabled

IP address :

Routing Rules Routing rules specify network adapter when access to the destination IP address. When using two network adapters, configure one of them first.

	Destination IP address	Subnet mask	Gateway	Network adapter	Operation
1	0.0.0.0	0.0.0.0	59.57.242.65	enp3s0f1	
2	192.168.0.0	255.255.0.0	10.2.62.254	enp3s0f0	
3	10.0.0.0	255.0.0.0	10.2.62.254	enp3s0f0	

[+](#) Add routing rules

3. Click **Next** to continue.
4. Set the time and time zone.

For more information, please refer to [Time/Time Zone Settings](#) on page 38.

The screenshot shows the 'Time/Time zone settings' page. At the top, there is a progress bar with five steps: Network settings, Time/Time zone settings (highlighted), Edit username/password, Activate the license, and SMTP mailbox settings. Below the progress bar, the 'Current server time' is displayed as '2017-07-14 09:58:21'. Under the 'Time access' section, the 'SNTP' radio button is selected. The 'Server domain name' is 'pool.ntp.org' and the 'Time zone' is '(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi'. Under the 'Date & time configuration' section, the 'Meeting time zone configuration' radio button is selected. The 'Default time zone' is '(UTC+05:30) Sri Jayawardenepura' and 'Enable DST automatically' is set to 'Disable'. At the bottom, there are three buttons: 'Back', 'Next', and 'Skip'.

5. Click **Next** to continue.

6. Enter login password and re-enter the password to confirm.

Enter the enterprise administrator's email. The email is used to reset password and receive a warning from your system.

Check **Agree Improvement Plan** checkbox to allow continual monitoring and improvement of YMS, the incidents that occur in your product will be given a feedback to technician.

The **Agree Improvement Plan** checkbox is checked by default.

The screenshot shows the 'Edit username/password' page. At the top, there is a progress bar with five steps: Network settings, Time/Time zone settings, Edit username/password (highlighted), Activate the license, and SMTP mailbox settings. Below the progress bar, the 'Username' is 'admin', 'Password' is masked with dots, 'Confirm Password' is also masked with dots, and 'Email' is 'vccloud@yealink.com'. The 'Agree Improvement Plan' checkbox is checked. At the bottom, there are three buttons: 'Back', 'Next', and 'Skip'.

7. Click **Next** to continue.

8. Enter the number of video port license to activate the video port license.

The screenshot shows the 'Activate the license' page. At the top, there is a progress bar with five steps: Network settings, Time/Time zone settings, Edit username/password, Activate the license (highlighted), and SMTP mailbox settings. Below the progress bar, the 'License' is 'blUeIpV0/BtlYf8lwwCCQ+2/V9ChEt/uvdal9F+pDvitXMYzxa4nS5TzvkBJZ'. At the bottom, there are three buttons: 'Back', 'Next', and 'Skip'.

9. Click **Next** to continue.

10. Set SMTP mailbox.

For more information, please refer to [SMTP Mailbox](#) on page 41.

The screenshot shows the 'SMTP mailbox settings' configuration page. At the top, there is a navigation bar with five steps: 'Network settings', 'Time/Time zone settings', 'Edit username/password', 'Activate the license', and 'SMTP mailbox settings' (which is highlighted). The main content area contains the following fields and options:

- SMTP server :
- Mail address :
- Username :
- Password :
- Mail signature:
- Port :
- This server requires a secure connection.
- Certification:
- Imported mail certificate: Null
- The imported mail certification will take affect after Web service restarted.
-

At the bottom of the form, there are three buttons: 'Back', 'OK', and 'Skip'.

11. Click **OK**.

Logging out of Yealink Meeting Server

If you want to log into YMS using other accounts, you can log out of the enterprise administrator account first.

To log out of YMS:

1. Click **Admin** on the top-right of the page.
2. Click **Log out**.

Note

If the page is idle more than 30 minutes, you will log out of the current enterprise administrator account and return to login page.

System Status

This chapter provides the basic instructions for viewing YMS status, Topics include:

- [Viewing System Information](#)
- [Viewing Online Users](#)

Viewing System Information

To view system information:

1. Click **Status**->**System information**.
You can view version information, server information and license information.
2. (Optional.) If YMS uses two adapters, select the desired adapter from the pull-down list to view the network adapter information.

Server information

Hardware information

CPU : Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz

Memory : 64.15GB

Disk : 1014.05GB

Network adapter

MAC address : 0C:C4:7A:28:3D:00

Interface type : Static IP

IP address : 10.2.62.202

Subnet mask : 255.255.255.0

Gateway : 10.2.62.254

Preferred DNS server : 192.168.1.20

Alternate DNS server :

Viewing Online Users

To view online users' information:

1. Click **Status**->**Online users**.
2. Select the desired online users, and then click **View**.

You can view the details of the device, including the device model registered the YMS account, software version, IP address, protocol and status.

Name	Account	Status	Device model				
1	0101	Idle	View				
2	1002	Busy	Device model	Software version	IP address	Protocol	Status
3	1003	Busy	VP-T49G	51.24.0.2	10.81.43.4	SIP	Idle

System Management

This chapter provides information on how to manage the YMS.

Topics include:

- [Call Settings](#)
- [Gateway Configuration](#)
- [System Settings](#)
- [Security Management](#)
- [System Maintenance](#)
- [Licenses Management](#)
- [System Logs](#)

Call Settings

Global Settings

Video Resolution

If you want to limit the resolutions of video calls, you can configure maximum video resolution and maximum content sharing resolution.

To configure the video resolution:

1. Click **System->Call Settings->Global settings**.
2. Configure the video resolution.

Parameters are described below:

Parameter	Description
Max video resolution	Configure the maximum video resolution. <ul style="list-style-type: none"> • 1080P/30FPS • 720P/30FPS • 360P/30FPS • 4CIF • CIF Default: 720P/30FPS.
Max content sharing resolution	Configure the maximum content sharing resolution.

Parameter	Description
	<ul style="list-style-type: none"> • 1080P/30FPS • 1080P/15FPS • 1080P/5FPS • 720P/30FPS • 720P/15FPS • 720P/5FPS <p>Default: 1080P/5FPS</p> <p>If you select 1080P/30FPS or 1080P/15FPS as the maximum content sharing resolution, it will bring the problem of high computing performance.</p>

3. Click **Confirm**.

Call Bandwidth

You can limit the uplink bandwidth of sending media stream to conference participants via YMS.

To configure the call bandwidth:

1. Click **System->Call Settings->Global settings**.
2. Select the desired bandwidth from the pull-down list of **Call bandwidth**.
3. Click **Confirm**.

Layout

Displaying Participant Name

To display the name of participant in the conference, you can enable the **Display participant name** feature.

To display the name of participant in the conference:

1. Click **System->Call Settings->Global settings**.
2. Enable **Display participant name**.
It is enabled by default.
3. Click **Confirm**.

Configuring the Default Layout

You can configure the default layout of conference participants.

The conference participants refer to the persons who are in meet now conferences, the persons who are in **Discussion mode** scheduled conferences or the moderators who are in **Training mode** scheduled conferences.

The following layouts are YMS supported:

- **Equal N × N**: All participants are displayed in the same size.
- **OnePlusN**: The first participant is given prominence with the largest pane. Other participants will be displayed in a strip around the first participant.

To configure the default layout:

1. Click **System->Call Settings->Global settings**.
2. Select **Equal N × N** or **onePlusN**.
The **onePlusN** is selected by default.
3. Click **Confirm**.

Configuring the Layout Parameter

You can configure the Equal N×N and OnePlusN layout.

In the **Equal N×N** and **OnePlusN** layout, if the number of current conference participants is more than the maximum, the video image will switch between conference participants every time interval. You can configure the time interval and switching rules.

In the **OnePlusN** layout, you can use voice-activated feature to switch layout between conference participants, the system will automatically identify the conference speaker. When the conference speaker speaks for the certain time, it is given prominence with the largest pane, other participants will be displayed in a strip around the first participant. The certain time is configurable.

To configure equal N×N:

1. Click **System->Call Settings->Global settings**.
2. Configure equal N×N.

Parameters are described below:

Parameter	Description
Equal N×N	Configure the maximum number of videos. <ul style="list-style-type: none"> • 2*2 • 3*3 • 4*4 • 5*5 • 6*6 • 7*7 Default: 4*4
	Configure the time interval of cycle.
	Configure the way of cycle: <ul style="list-style-type: none"> • One video switches per cycle: One video is replaced with the

Parameter	Description
	extra one per cycle. <ul style="list-style-type: none"> • All videos switch per cycle: All videos are replaced with extra videos per cycle.

3. Click **Confirm**.

To configure OnePlusN:

1. Click **System->Call Settings->Global settings**.
2. Configure OnePlusN.

Parameters are described below:

Parameter	Description
OnePlusN	Configure the maximum number of videos. <ul style="list-style-type: none"> • 1+0 • 1+4 • 1+7 • 1+9 • 1+12 • 1+20 Default: 1+7
	Configure the time interval of cycle.
	Configure the way of cycle: <ul style="list-style-type: none"> • X video switches per cycle: X video is replaced with the extra one per cycle. • All videos switch per cycle: All videos are replaced with extra videos per cycle.
	Configure the time of voice-activated feature.

3. Click **Confirm**.

Conference Settings

Joining Conference Beforehand

You can specify the time that allows users to join the scheduled conferences in advance.

To configure the time that allows devices to join the scheduled conferences beforehand:

1. Click **System->Call Settings->Global settings**.
2. Select the desired time from the pull-down list of **Join conference beforehand**.
3. Click **Confirm**.

Third Party Registration

If you want to register YMS accounts by devices which are not Yealink devices, you need enable the **Third party registration** feature.

To enable the third party registration:

1. Click **System->Call Settings->Global settings**.
2. Enable **Third party registration**.
3. Click **Confirm**.

Dialing Devices Automatically

You can enable **Auto dialing** feature. When the scheduled conference begins, the devices registered the YMS accounts and the third party devices in enterprise directory will receive a call to invite to join the conference. You can answer or reject the call by devices manually. If the devices enable the auto answer feature, they will join the scheduled conference automatically.

The VC800/VC500/VC400/VC120/VC110 video conferencing endpoint, SIP VP-T49G IP phone, SIP-T58V IP phone and third party devices are supported.

To configure auto dialing feature:

1. Click **System->Call Settings->Global settings**.
2. Enable **Auto dialing**.
It is enabled by default.
3. Check the desired checkboxes of devices.
4. Click **Confirm**.

Note

If the third party devices register the YMS accounts by H.323 protocol, they do not apply to the **Auto dialing** feature.

Redialing Devices Automatically

If the **Auto dialing** feature is enabled, while the devices you invited disconnect with the YMS in conference. To invite them to join the conference again after they connect to YMS, you can enable the **Auto redialing** feature.

To enable the auto redialing feature:

1. Click **System->Call Settings->Global settings**.
2. Enable **Auto redialing**.
It is enabled by default.
3. Click **Confirm**.

Note

If the third party devices register the YMS accounts by H.323 protocol, they do not apply to the **Auto redialing** feature.

Sending Content Only

If the device does not support dual-stream protocol, you can enable **Content only** feature. When other devices share content in a call, the device only receives content and audio.

To enable the content only feature:

1. Click **System->Call Settings->Global settings**.
2. Enable **Content only**.
3. Click **Confirm**.

Configuring Roll Call

During the roll call, the participant who is called is unmuted by default. If other participants do not want to hear the participant who is called, you can disable **Roll call setting** feature.

To disable the roll call setting feature:

1. Click **System->Call Settings->Global settings**.
2. Disable **Roll call setting**.
3. Click **Confirm**.

Record

If the **Record** feature is enabled, you can add studios to the YMS to record conferences.

Note

Before you add the studio, make sure Yealink technical support engineer have deployed the recording server. If the recording server is deployed, you need obtain the studio URI, username and password from the Yealink technical support engineer.

To enable the record feature:

1. Click **System->Call Settings->Global settings**.
2. Enable **Record**.
3. Enter the studio name, studio URI, username and password in the corresponding field.
4. According to the network of the recording server, select the desired adapter from the pull-down list of **Network adapter**.
5. Click **Confirm**.

Note

You can add 20 studios at most.
When a studio is in use, it takes up a video port.

Enabling RTMP Live

You can enable the **RTMP live** feature, it allows users to watch the live conference.

Before you enable the RTMP live feature, you need obtain the information of AliCloud service,

including domain, APP name, live domain and authentication key.

To enable the RTMP live feature:

1. Click **System->Call Settings->Global settings**.
2. Enable **RTMP live**.
3. Configure the live server to generate the streaming address.

Parameters are described below:

Parameter	Description
Domain	Specify the domain name.
APP name	Specify the application name.
Live domain	Specify the live video domain name.
Authentication	Enable or disable the H.323 protocol. Default: Disabled
Authentication key	Specify the authentication password.

4. Click **Confirm**.

Note

When a conference enables RTMP live feature, it takes up a video port.

Enabling Broadcasting Interactive Video Conferences

If the **Broadcasting interactive** feature is disabled, you can initiate a 20-way 1080P conference or 40-way 720P conference. After you enable the feature, you can enable a broadcasting interactive video conference which contains more than 200-way.

Before you enable the feature, you need import the broadcasting port license ([Activating the Broadcasting Port License](#) on page 54), and make sure the Yealink technical support engineer deploys the broadcasting server.

To enable broadcasting interactive video conferences:

1. Click **System->Call Settings->Global settings**.
2. Enable **Broadcasting interactive**.
3. Click **Confirm**.

Note

When a broadcasting interactive conference is initiated, it takes up two video ports. And broadcasting parties take up the resource of master server.

When the broadcasting interactive conference needs more interactive parties, contact with Yealink technical support engineer. Yealink technical support engineer will increase the number of interactive parties by stacking several MCUs together.

IVR Service

You can configure the voice prompt language for IVR service or the display language on devices while waiting for lecturer. The languages supported are Chinese Simplified, English, Russian, Polish, Spanish and Portuguese.

To configure the IVR language:

1. Click **System->Call Settings->Global settings**.
2. Select the desired language from the pull-down list of **IVR language**.
3. Click **Confirm**.

Call Routing

If you want to place a PSTN call, you should configure the call routing rules. Call routing rules determine how calls are routed.

When you place a PSTN call, the server will select the desired gateway based on your call routing rules, and send the SIP request message. The gateway will call the PSTN telephone through the PSTN network.

Before you configure the call routing rules, please ensure you have added the SIP trunk which can be set as the destination gateway of the call routing rules. For more information, please refer to [SIP Trunk](#) on page 24.

Adding Call Routing Rules

To add call routing rules:

1. Click **System->Call Settings->Call routing**.
2. On the top-right of page, click **Add Call Routing Rule**.

3. Configure the call routing rules.

Add Call Routing Rule

Routing information

Name*

Priority*
1~200

Check each rule by priority ascending order until you find the first matching rule, then apply the rule.

Enable

Any disabled rules are still displayed in the rule list, but will be ignored.

Rule setting

Destination regex match*
A regular expression for checking the target to see if this rule applies to this call.

Call target*

Outgoing location*

Call routing rules parameters are described below:

Parameter	Description
Name	Specify the name of the call routing rule.
Priority 1~200	Configure the priority of the call routing rule. The lower the number is, the higher the priority is. The range of ports is 1-200 by default. When you place a PSTN call, the server will check each rules by priority ascending order until you find the first matching rule, then apply the rule.
Enable	Enable or disable the call routing rule. Default: Enabled Any disabled rules are still displayed in the rule list, but will be ignored.
Destination regex match	Configure the Perl Compatible Regular Expressions (PCRE) to check the target to see if this rule applies to this call.
Call target	Default: PSTN. Note: It is not configurable.
Outgoing location	Configure the gateway when access to the destination.



Common Perl Compatible Regular Expressions (PCRE) are described below:

PCRE	Description
^(1\d{10})\$	Matches the number which begins with 1 followed by 10 digits. For example: 12345678912
^0(\d+)\$	Matches the number which begins with 0 followed by one or more digits. For example: 02, 0157
^(13[0-9] 14[57] 15[0 1 2 3 5 6 7 8 9] 18[0 1 2 3 5 6 7 8 9])\d{8}\$	Matches 11-digit mobile phone number, the first 3-digit mobile phone number includes the following types, the rest digit is optional: <ul style="list-style-type: none"> • Begins with 13 and the third number is a 0-9 character • Begins with 14 and the third number is a 5/7 character • Begins with 15 and the third number is a 0/1/2/3/5/6/7/8/9 character • Begins with 18 and the third number is a 0/1/2/3/5/6/7/8/9 character For example: 13012345678, 14512345678, 15987654321 or 18243218765
^\d{3,4}-?\d{7,8}\$	Matches the number in the following format: <ul style="list-style-type: none"> • XXX-XXXXXXX, 10-digit number • XXX-XXXXXXX, 11-digit number • XXXX-XXXXXXX, 11-digit number • XXXX-XXXXXXX, 12-digit number • XXXXXXX, 7-digit number • XXXXXXX, 8-digit number For example: XXXXXXXX represents 1234567 or other 7 digits numbers
\d{3}-\d{8} \d{4}-\d{7}	Matches the number in the following format: <ul style="list-style-type: none"> • XXX-XXXXXXX, 11-digit number • XXXX-XXXXXXX, 11-digit number For example: XXX-XXXXXXX represents 012-12345678 or other 11 digits number, XXXX-XXXXXXX represents 0123-1234567 or other 11 digits number
(\d{11}) ((\d{3,4}-?)\d{7,8})-(\d{1,4})?	Matches the number in the following format: <ul style="list-style-type: none"> • 11-digit mobile phone number • XXXXXXX, 8-digit number • XXXXXXX, 7-digit number

PCRE	Description
	<ul style="list-style-type: none"> • XXX/XXXX-XXXXXXXX/XXXXXXXX, 4 formats in total • XXX/XXXX-XXXXXXXX/XXXXXXXX-X/XX/XXX/XX XX, 16 formats in total • XXXXXXXX/XXXXXXXX-X/XX/XXX/XXXX, 8 formats in total <p>For example: XXXX-XXXXXXX represents 0731-8784888 or other 11 digits number</p>

4. Click **Save**.

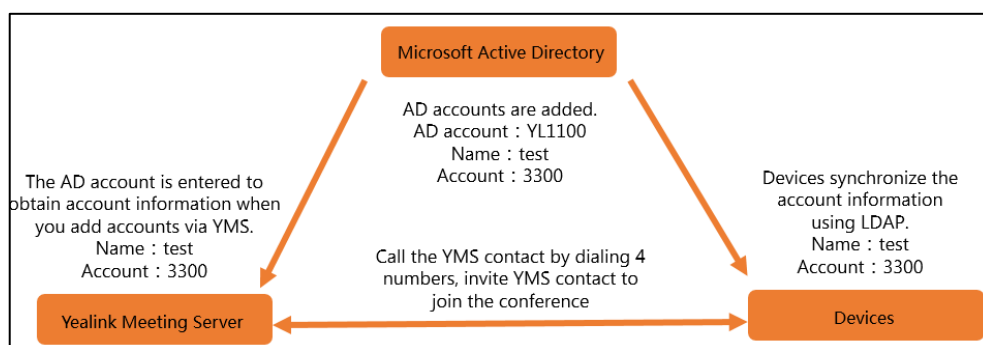
Adding or Editing Call Routing Rules

You can click **System->Call Settings->Call routing**, and then click  on the right of page to edit call routing rules, or click  on the right of page to delete the call routing rule.

LDAP

LDAP (Lightweight Directory Access Protocol) is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. YMS is configurable to interface with an enterprise directory server that supports LDAP version 3. So that the devices which register to YMS by standard SIP/H.323 protocol can obtain YMS contacts and organizational structure. Microsoft Active Directory as LDAP servers is supported.

Because the LDAP server can only be read, the administrator of LDAP server should add accounts via LDAP server and you should add accounts via YMS, and two types of accounts need be associated with each other. Take image below as an example: when the administrator of LDAP server add accounts, the rule of adding accounts via LDAP should be consistent with it via YMS. And when you add accounts via YMS, you can enter a specific AD account to obtain the YMS account. The devices which register to YMS can obtain YMS contacts from LDAP server, call the YMS contact by dialing 4 numbers, invite YMS contact to join the conference and so on.



Note

When the administrator of LDAP server edits the name and account of AD account, the YMS account will update the name synchronously, while the account will not be updated.

The organizational structure of YMS and that of the LDAP server are independent of each other. If you want to edit the organizational structure, the organizational structure viewed by third party devices should be edited via the LDAP server, and the organizational structure viewed by Yealink VC devices should be edited via YMS.

To configure LDAP:

1. Click **System**->**Call Settings**->**LDAP**.
2. Configure LDAP.

LDAP parameters are described below:

Parameter	Description
Enable	Enable or disable the LDAP feature. Default: Disabled
Server address	Configure the domain name or IP address of the LDAP server.
Port	Configure the LDAP server port.
Base DN	Configure the root path of the LDAP search base. Example: OU=test_ymms,DC=ldap,DC=yealink,DC=cn
Username	Configure the user name used to log into the LDAP server. Note: The user name is provided by the LDAP server administrator.
Password	Configure the password to log into the LDAP server. Note: The password is provided by the LDAP server administrator.
Name attribute	Configure the name attributes of each record to be returned by the LDAP server. Example: name
Number attribute	Configure the number attributes of each record to be returned by the LDAP server. Example: telephoneNumber
AD account attribute	Configure the account attributes in the LDAP server. Example: sAMAccountName

3. Click **Connection Test**.

If the configuration is correct, the page prompts "connection successful".

4. Click **Confirm**.

Gateway Configuration

You can configure the H.323, SIP trunk, SIP truck ACL and SIP trunk IVR.

H.323

If H.323 devices want to join conference by direct IP call or invite conference participants by direct IP call, you can enable H.323 gateway. Moreover, YMS supports H.323 devices register to the **embedded GK** and H.323 gateway registers to the **embedded GK** or the **external GK**.

To configure the H.323 gateway:

1. Click **System->Gateway Configuration->H.323**.

2. Check **H.323 Gateway** checkbox.

The checkbox is checked by default.

3. Configure the H.323 gatekeeper.

- To register to the embedded GK, configure the embedded gatekeeper.

Parameters are described below:

Parameter	Description
Embedded GK server	Enable or disable the embedded GK server. Default: Enabled Note: the H.323 gateway is enabled and register to the embedded GK server by default
Display name	Specify the name to identify this embedded GK server.
TTL timeout duration (10~600s)	Configure the registration expires time. After the registration expires time, YMS will send the request for registering with the embedded GK server again. Default: 60s
IRR timeout duration (10~600s)	Configure expires time that H.323 gateway sends status response message to the embedded GK server according to ACF command and IRO request. Default: 120s

- To register to the external GK, configure the external gatekeeper.

Parameters are described below:

Parameter	Description
Display name	Specify the name to identify this external GK server.
GK address	Configure the IP address and domain name of the external GK server.
GK authentication	Enable or disable support for external GK authentication. Default: Disabled Note: When GK Authentication is enabled, the gatekeeper ensures that only trusted H.323 device are allowed to access the gatekeeper.
GK account	Specify the account for authentication with external GK.
GK code	Specify the password for authentication with external GK.

4. Specify the H.235 type during an H.323 call.

Parameters are described below:

Parameter	Description
-----------	-------------

Parameter	Description
H.235 encryption	<p>Specify the H.235 type during an H.323 call.</p> <ul style="list-style-type: none"> • Optional—negotiate with the far site whether to use H.235 for media encryption in H.323 calls. • Compulsory—compulsory use H.235 for media encryption in H.323 calls. • Disable—do not use H.235 in H.323 calls. <p>Default: Disabled</p>

5. Check the **Enable** checkbox in the **H.239** field.

When H.323 devices which register to YMS join a video conference, they receive and send contents by H.239 protocol.

6. Click **Confirm**.

If the registration is successful, the status shows "Registered".

Embedded GK Server

Display name :

TTL timeout duration : s
(10~600s)

IRR timeout duration : s
(10~600s)

H.323 Gateway (Status: Registered)

Display name :

GK address :

GK authentication : Enable

H.235 encryption : Optional Compulsory Disable

H.239 : Enable

SIP Trunk

To place a PSTN call, you should configure the SIP trunk which can be set as the destination gateway of the call routing rules. Note that if you add, edit or delete the SIP trunk, YMS will reboot to make the change take effect.

Adding SIP Trunks

To add SIP trunks:

1. Click **System->Gateway Configuration->SIP trunk**.
2. On the top-right of page, click **Add SIP Trunk**.
3. Configure the SIP trunk.

Gateway information

Gateway name*

Gateway type*

Outgoing network* Intranet Extranet

Enable

Support video

Registration information

Server address* Port*

Transport protocol*

Session expires (30s~3600s)

Server retry counts (1~16)

Outbound proxy server

SIP trunk parameters are described below:

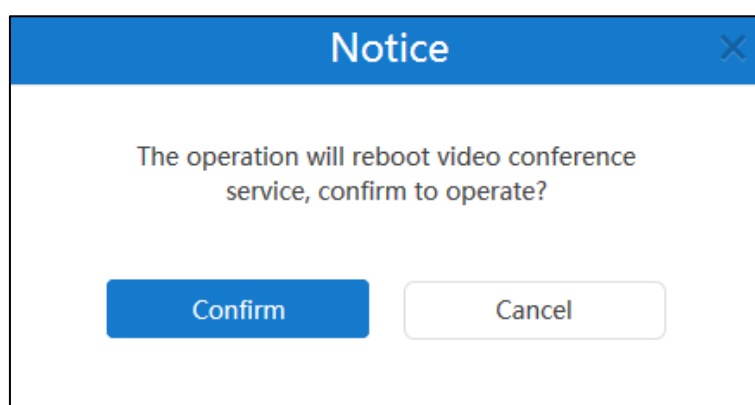
Parameter	Description
Gateway name	Specify the name of SIP voice gateway.
Gateway type	Configure the SIP voice gateway type. <ul style="list-style-type: none"> • New Rock • Audiocodes You can also select General to specify the other SIP voice gateway type. Default: New Rock. The SIP voice gateway is configured by IT administrator.
Outgoing network	Configure the outgoing network. <ul style="list-style-type: none"> • Intranet: SIP voice gateway is deployed in internal network. • Extranet: SIP voice gateway is deployed in external network.

Parameter	Description
Enable	Enable or disable the SIP voice gateway. Default: Enabled
Support video	If the SIP voice gateway supports video, enable Support video .
Connection	If you select General , enable or disable the server to register with the SIP voice gateway. When the SIP voice gateway needs the server to register with it, you should enable Registered to the gateway . On the contrary, you should disable it. Default: Registered to the gateway checkbox is checked by default. Note that New Rock or Audiocodes do not need the server to register with it.
Username	When you select General and check the Registered to the gateway checkbox, configure the user name for authentication.
Realm	When you select General and check the Registered to the gateway checkbox, configure the IP address or domain name of SIP voice gateway for authentication.
Password	When you select General and check the Registered to the gateway checkbox, configure the password for authentication.
Number	When you select General and check the Registered to the gateway checkbox, configure the number which is assigned by SIP voice gateway to identify the server.
Server address	Configure the IP address or domain name of SIP voice gateway.
Port	Configure the port of the SIP voice gateway. Valid values: Integer from 0 to 65535. Default: 5060
Transport protocol	Configure the type of transport protocol for the SIP account. <ul style="list-style-type: none"> • UDP—provides best-effort transport via UDP for SIP signaling. • TCP—provides reliable transport via TCP for SIP signaling. • TLS—provides secure communication of SIP signaling. • DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. Default: UDP
Session expires (30s~3600)	Configure the session expires time. After the session expires time, the server will send the request for registering with the SIP voice gateway again.

Parameter	Description
	Default: 3600s
Server retry counts (1~16)	When the registration is unsuccessful, configure the number of time which the server retries to send the request for registering with the SIP voice gateway. Default: 3
Outbound proxy server	Enable or disable the server to send requests to the outbound proxy server. Default: Disabled
Outbound proxy server	Configure the IP address or domain name of the outbound proxy server. Default: it is configurable only when the Outbound Proxy Server is enabled.
Port	Configure the port of the outbound proxy server. Valid values: Integer from 0 to 65535. Default: 5060. It is configurable only when the Outbound Proxy Server is enabled.
Proxy fallback interval (30s~3600s)	Configure the proxy fallback interval of outbound proxy server. After the proxy fallback interval, the server will send the request for registering with outbound proxy server again. Default: 3600s. It is configurable only when the Outbound Proxy Server is enabled.

- Click **Save**.


The notice is displayed as shown next:



- Click **Confirm** to reboot video conference service.

Adding or Editing SIP Trunks

You can click **System->Gateway Configuration->SIP trunk**, and then click  on the right

of page to edit SIP trunks, or click  on the right of page to delete SIP trunks.

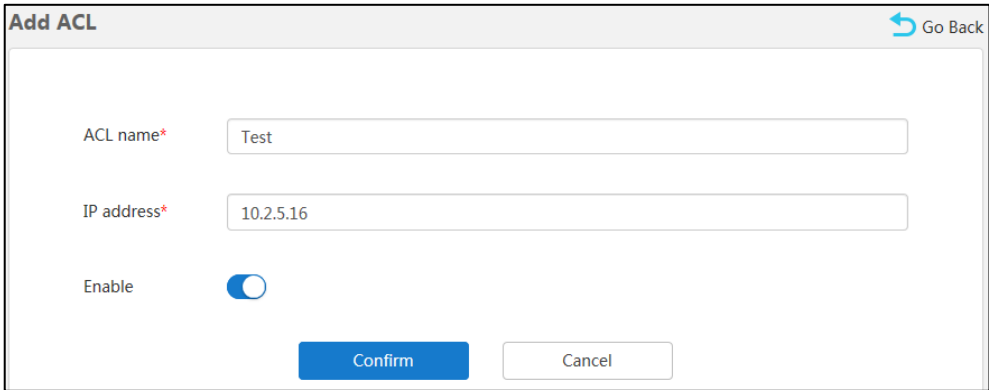
SIP Trunk ACL

Adding SIP Trunk ACL

If devices are not registered YMS account, the devices cannot place a call to YMS account directly. To solve this problem, you need add the SIP trunk ACL (Access Control List). The format of calling information must meet: YMS account@ domain name of YMS, and the domain name of YMS must be resolvable.

To add SIP trunk ACL:

1. Click **System->Gateway Configuration->SIP trunk ACL**.
2. On the top-right of page, click **Add ACL**.
3. Configure the SIP trunk ACL.





Parameters are described below:

Parameter	Description
ACL name	Specify the name of the SIP trunk ACL.
IP address	Configure the IP address or network segment (for example: 192.168.1.0/24) of server on which the devices register accounts. Note: If the devices are not registered accounts, configure the IP address of device.
Enable	Enable or disable the SIP trunk ACL. Default: Enabled

4. Click **Confirm**.

Adding or Editing SIP Trunk ACL

You can click **System->Gateway Configuration->SIP trunk ACL**, and then click  on the right of page to edit SIP trunk ACL, or click  on the right of page to delete SIP trunk ACL.

SIP Trunk IVR

After you configure the SIP trunk and call routing, users will listen to the voice prompt when they enter YMS via SIP trunk. You can configure the voice prompt and key functions.

Note To make sure devices can send DTMF tones normally according to voice prompt, it is recommended that the DTMF type of devices is RFC2833.

To configure SIP trunk IVR:

1. Click **System->Gateway Configuration->SIP trunk IVR**.
2. Configure voice prompt, do one of the following:
 - Select **Default Greeting**. The language depends on your IVR language. For more information, please refer to [IVR Service](#) on page 18.
 - Select **Personal Greeting**.
Click **Browse** to select the desired .wav file.
Click **Upload** to upload the desired file.
3. (Optional.) To enable users can dial extension or conference ID directly, check the **Enable first-level extension dialing** checkbox to enable
4. If **Personal Greeting** is selected, select the desired key, and then enter the description and select options, available options contain transfer to extension, transfer to conference, extension dialing, conference dialing, repeat and exit.
5. Click **Confirm**.

System Settings

Network Settings

Basic Settings

The server supports two adapters, you can configure the network based on the actual enterprise network condition.

Native Domain Name

You can configure the domain name of YMS. The domain name is used to authentication when devices register YMS accounts.

To configure the domain name of YMS:

1. Click **System->System Settings->Network**.
2. Select **Basic settings** to enter the page of basic settings.
3. Configure the domain name of YMS in in the **Native domain name** field.

Configuring IP Addresses of Internal Network or External Network

You can configure static IP addresses of internal network or external network manually.

Note that if you configure the static IP addresses, YMS will reboot to make the change take effect.

To configure IP address of internal network or external network:

1. Click **System**->**System Settings**->**Network**.
2. Select **Basic settings** to enter the page of basic settings.
3. Check the **Internal network settings** or **Network settings** checkbox.
4. Select the desired adapter from the pull-down list of **Network adapter settings**.
5. Configure the static IP address.

Internal network settings

Network adapter settings : enp3s0f0

Ethernet port type : Static IP address

IP address : 10.2.62.202

Subnet mask : 255.255.255.0

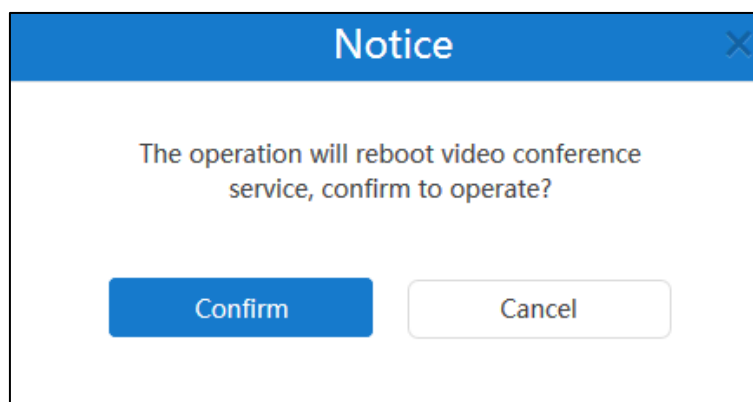
Gateway : 10.2.62.254

Preferred DNS : 192.168.1.20

Alternate DNS : Alternate DNS

6. Click **Confirm**.

The notice is displayed as shown next:



7. Click **Confirm** to reboot video conference service.

Static NAT

NAT enables communication between devices on your LAN that have private IP addresses and devices that are accessed through a public IP network. Static NAT ensures that the same public IP address always maps to a system's private IP address so that data from the public network intended for the private system can be routed to the system reliably.

To ensure the YMS security and maintain internal network, you can deploy the YMS in internal network. And you should configure static NAT by address forwarding on the router to accomplish the effect that users in external network can access to the YMS.

Note that if you configure static NAT, YMS will reboot to make the change take effect.

To configure static NAT:

1. Click **System->System Settings->Network**.
2. Select **Basic settings** to enter the page of basic settings.
3. Check the **Network settings** checkbox.
4. Configure the static NAT.

Network settings

Network adapter settings :

Ethernet port type : Static IP address

IP address :

Subnet mask :

Gateway :

Preferred DNS :

Alternate DNS :

NAT : Enabled

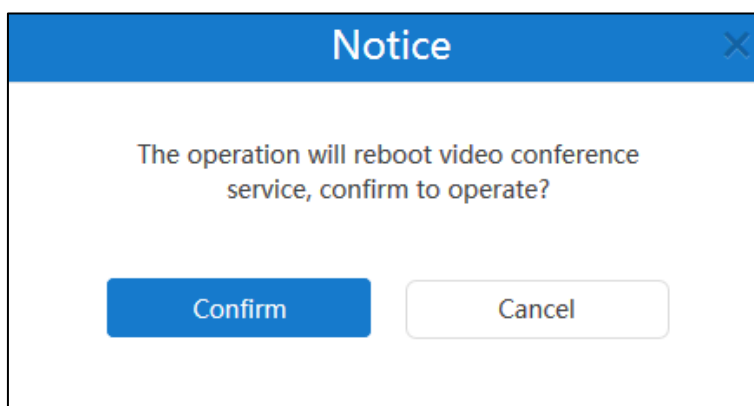
IP address

Static NAT feature parameters are described below:

Parameter	Description
NAT	Enable or disable the static NAT feature. Default: Disabled
IP address	Configure the NAT public address for YMS.

5. Click **Confirm**.

The notice is displayed as shown next:



6. Click **Confirm** to reboot video conference service.

Routing Rules

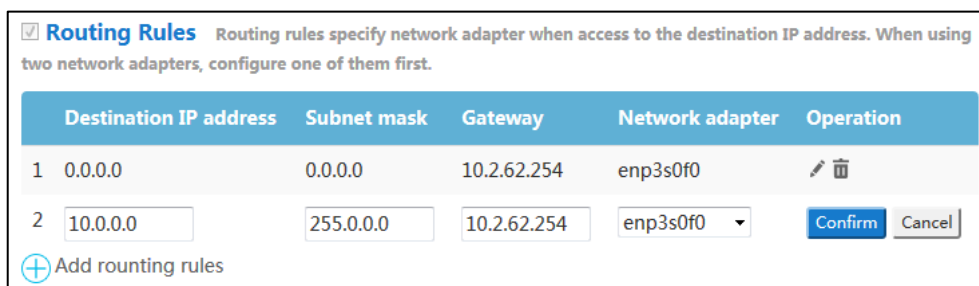
When YMS uses two adapters, you can configure routing rules based on the actual enterprise network condition. To reach the destination, you can specify the network adapters to use

It is recommended that external network and all network segments in your enterprise must be specified routing rules. Note that If you add, edit or delete the contents of routing rules, YMS will reboot to make the change take effect.

Adding Routing Rules

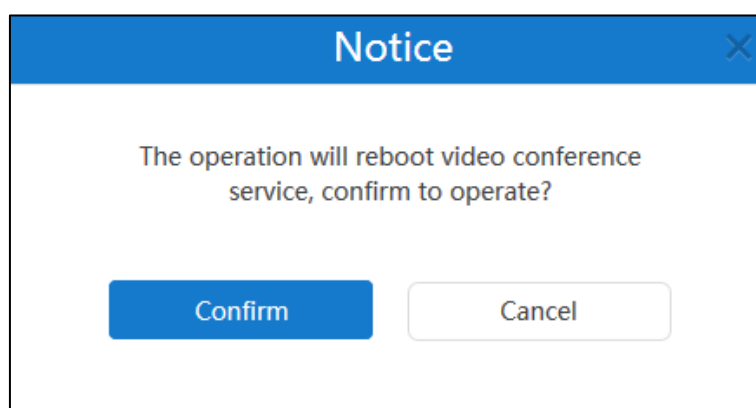
To add the contents of routing rules:

1. Click **System**->**System Settings**->**Network**.
2. Select **Basic settings** to enter the page of basic settings.
3. Click **Add routing rules** to add the contents of routing rules.
4. Configure the routing rules.





5. Click **Confirm** to save the change.
6. Click **Confirm**.

The notice is displayed as shown next:



7. Click **Confirm** to reboot video conference service.

Editing or Deleting Routing Rules

You can click **System->System Settings->Network**, and then click  on the right of page to edit routing rules, or click  on the right of page to delete routing rules.

Service Settings

Web

You can configure HTTP protocol and HTTPS protocol. If you enable HTTP protocol and HTTPS protocol, the system priority of selection is as follows: HTTPS protocol>HTTP protocol.

Note that if you configure HTTP protocol and HTTPS protocol, YMS will reboot to make the change take effect.

To configure the Web page:

1. Click **System->System Settings->Network**.
2. Select **Service settings** to enter the page of service settings.
3. Configure the Web page.

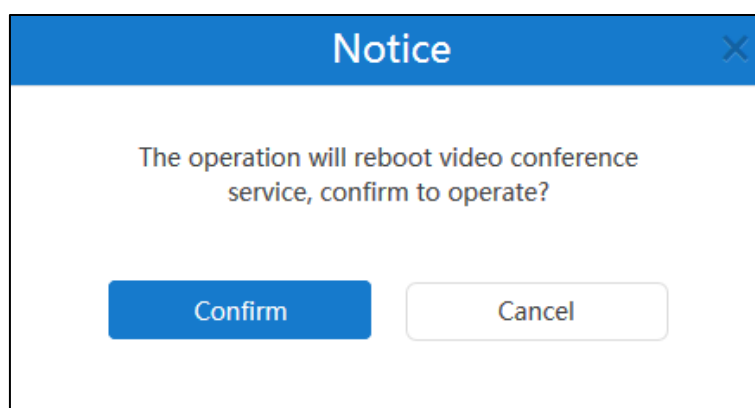
Web page parameters are described below:

Parameter	Description
Enable HTTP	Enable the HTTP protocol. Default: It is not configurable.
HTTP listener	Specify the HTTP listener port of HTTP protocol. Valid values: 1-65535 Default: 80
HTTP NAT	If you enabled static NAT in external network settings, configure the HTTP NAT port of HTTP protocol is used to access to the external network. Default: 80. The port should be the same as it configured on the

Parameter	Description
	router.
Enable HTTPS	Enable or disable the HTTPS protocol. Default: Enabled
HTTPS listener	Specify the HTTPS listener port of HTTPS protocol. Valid values: 1-65535 Default: 443
HTTPS NAT	If you enabled static NAT in external network settings, configure the HTTPS NAT port of HTTPS protocol is used to access to the external network. Default: 443. The port should be the same as it configured on the router.

4. Click **Confirm**.

The notice is displayed as shown next:



5. Click **Confirm** to reboot video conference service.

SSH

SSH (Secure Shell) is a cryptographic network protocol for operating network services securely over an unsecured network. It provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login and remote command execution, but any network service can be secured with SSH. Note that if you configure SSH, YMS will reboot to make the change take effect.

To configure SSH:

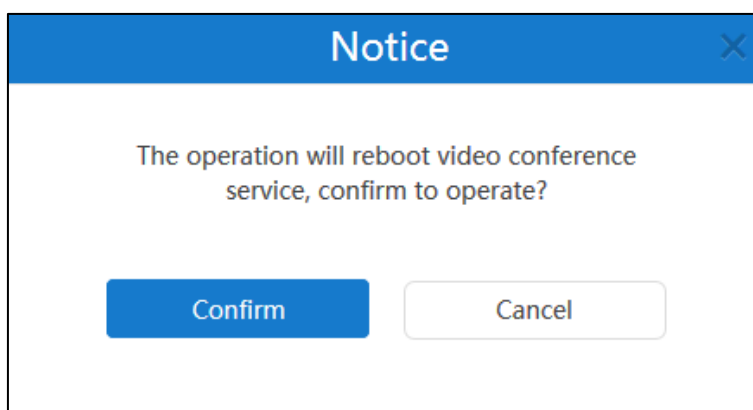
1. Click **System->System Settings->Network**.
2. Select **Service settings** to enter the page of service settings.
3. Configure SSH.

SSH parameters are described below:

Parameter	Description
Enable SSH	Enable or disable the SSH protocol. Default: Enabled
Port	Specify the port of SSH protocol. Valid values: 1-65535 Default: 22

- Click **Confirm**.

The notice is displayed as shown next:



- Click **Confirm** to reboot video conference service.

SIP

YMS supports SIP protocol and UDP, TCP and TLS protocol to transport SIP (Session Initiation Protocol) signaling. You can specify the ports of these protocols. Note that if you configure the port parameters to transport SIP signaling, YMS will reboot to make the change take effect.

To configure the port parameters to transport SIP signaling:

- Click **System->System Settings->Network**.
- Select **Service settings** to enter the page of service settings.
- Configure the port parameters to transport SIP signaling.

SIP :

UDP/TCP port :

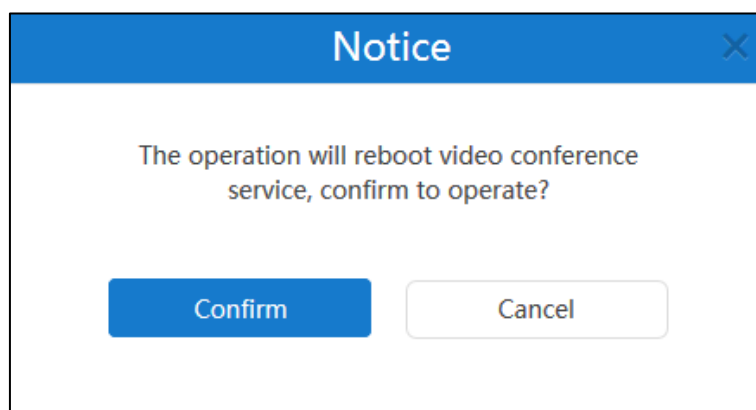
Note : used for IVR

TLS port :

Note : must be different from the TCP/UDP port

- Click **Confirm**.

The notice is displayed as shown next:



5. Click **Confirm** to reboot video conference service.

H.323 Gateway

H.225 is part of the H.323 family of telecommunication protocols. If the H.323 gateway has registered, H.225 was used to establish the H.323 call. For more information, please refer to [H.323](#) on page 22.

H.225 listener port is not configurable.

To view H.323 gateway parameters:

1. Click **System->System Settings->Network**.
2. Select **Service settings** to enter the page of service settings.

GK

If the embedded GK server is enabled, H.323 GK ports are enabled by default to make sure the H.323 gateway can register to embedded GK server. For more information, please refer to [H.323](#) on page 22.

H.323 gatekeeper parameters are not configurable.

To view H.323 gatekeeper parameters:

1. Click **System->System Settings->Network**.
2. Select **Service settings** to enter the page of service settings.

WebRTC

Joining conferences from a Web browser are supported by YMS.

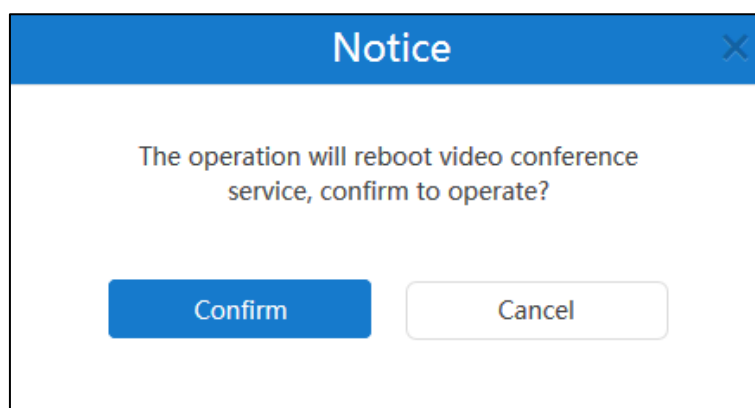
You can configure the WebRTC listener port. Note that if you configure the WebRTC listener port, YMS will reboot to make the change take effect.

To configure the WebRTC listener port:

1. Click **System->System Settings->Network**.
2. Select **Service settings** to enter the page of service settings.

3. Enter the listener port in the **webRTC listener** field.
4. Click **Confirm**.

The notice is displayed as shown next:



5. Click **Confirm** to reboot video conference service.

Port Settings

You can configure UDP ports and TCP ports. After you configure it, YMS will reboot to make the change take effect.

To configure port settings:

1. Click **System->System Settings->Network**.
2. Select **Port settings** to enter the page of port settings.
3. Configure the ports in the corresponding field.

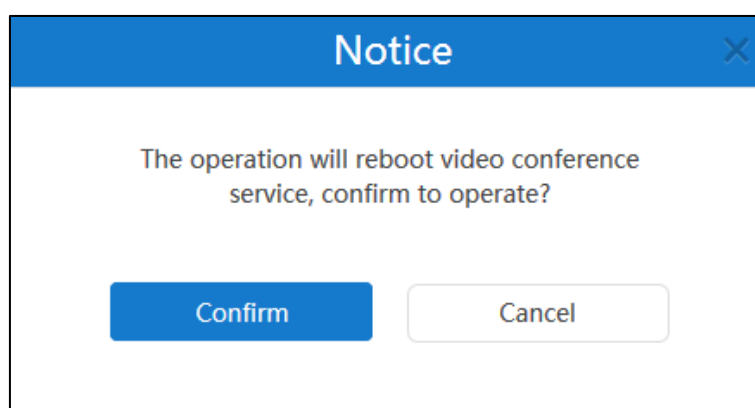
Port settings parameters are described below:

Parameter	Description
IVR port	Specify the range of IVR ports. Default: A call occupies 6 ports. If you initiate presentation in the call, the call occupies additional 2 ports. The range of ports is 30000-37999 by default. And the difference between the maximum signaling port and the minimum port should be not less than 1000 to avoid the port conflict. For example, you set 30000 as the minimum port, the maximum port should be not less than 31000.
TURN service port	Specify the range of TURN service ports. Default: 38000-49999. And the difference between the maximum port and the minimum port should be not less than 1000 to avoid the port conflict. For example, you set 38000 as the minimum port, the maximum port should be not less than 39000.
MCU port	Specify the range of MCU ports. Default: 50000-59999. And the difference between the maximum port and the minimum port should be not less than 1000 to avoid the port conflict. For example, you set 50000 as the minimum port, the

Parameter	Description
	maximum port should be not less than 51000.
GK media forwarding port	Specify the range of GK media forwarding ports. Default: 15000-19999. And the difference between the maximum port and the minimum port should be not less than 1000 to avoid the port conflict. For example, you set 15000 as the minimum port, the maximum port should be not less than 16000.
H.245/Q.931	Specify the range of H.245/Q.931 ports. Default: 30000-39999. And the difference between the maximum port and the minimum port should be not less than 1000 to avoid the port conflict. For example, you set 30000 as the minimum port, the maximum port should be not less than 31000.
H.245	Specify the range of H.245 ports. Default: 20000-24999. And the difference between the maximum port and the minimum port should be not less than 1000 to avoid the port conflict. For example, you set 20000 as the minimum port, the maximum port should be not less than 21000.
Q.931	Specify the range of Q.931 ports. Default: 25000-29999. And the difference between the maximum port and the minimum port should be not less than 1000 to avoid the port conflict. For example, you set 25000 as the minimum port, the maximum port should be not less than 26000.

- Click **Confirm**.

The notice is displayed as shown next:



- Click **Confirm** to reboot video conference service.

Time/Time Zone Settings

Time Access

Time and date are synced automatically from the SNTP server by default. If YMS cannot obtain the time and date from the SNTP server, you need to manually configure them.

When configuring YMS to obtain the time and date from the SNTP server, you must set the time zone.

To configure the time access:

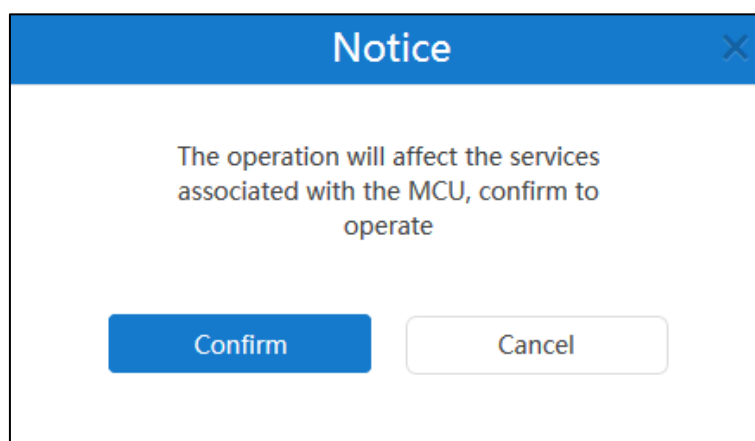
1. Click **System->System Settings->Time/Time zone**.
2. Configure the time access.

Time access parameters are described below:

Parameter	Description
Current server time	The current time of YMS.
Time access	Configure the Daylight Saving Time (DST) type. <ul style="list-style-type: none"> • SNTP: obtain the time and date from the SNTP server automatically. • Date & time configuration: configure the time and date manually. Default: SNTP
Server domain name	Configure the SNTP server. Default: pool.ntp.org
Time zone	Configure the time zone.

3. Click **Confirm**.

The notice is displayed as shown next:



- Click **Confirm**.

Note

Please refer to [Appendix: Time Zones](#) for the list of available time zones on YMS.

Meeting Time Zone Configuration

You can configure the meeting time zone. When users schedule the conference, the default zone and enabled state of Daylight Saving Time (DST) is determined by the meeting time zone configuration.

To configure the meeting time zone:

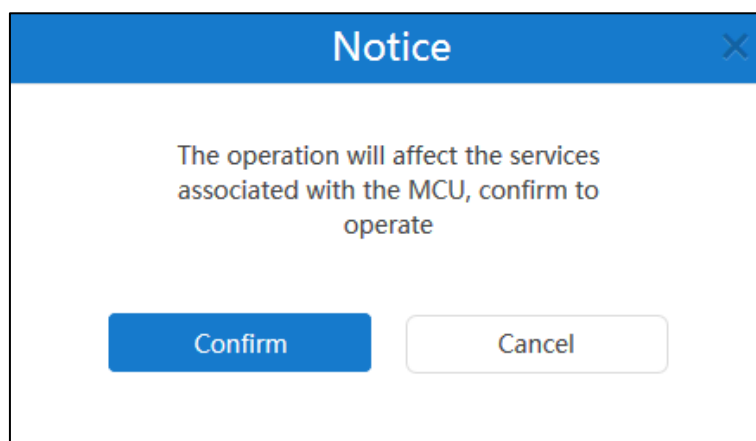
- Click **System->System Settings->Time/Time zone**.
- Configure the meeting time zone.

Meeting time zone parameters are described below:

Parameter	Description
Default time zone	<p>When users schedule the conference, configure the default time zone.</p> <p>Default: The default time zone interacts with the time zone of server.</p>
Enable DST automatically	<p>When users schedule the conference, configure the DST type.</p> <p>The available types for YMS are:</p> <ul style="list-style-type: none"> Auto: DST will be configured automatically. When users schedule the conference in the countries which use DST, the DST is enabled automatically. Disable: do not use DST. <p>Default: Auto</p>

- Click **Confirm**.

The notice is displayed as shown next:



4. Click **Confirm**.

SMTP Mailbox

You can use the SMTP mailbox to send emails to users. For example, you can send account information to users by emails.

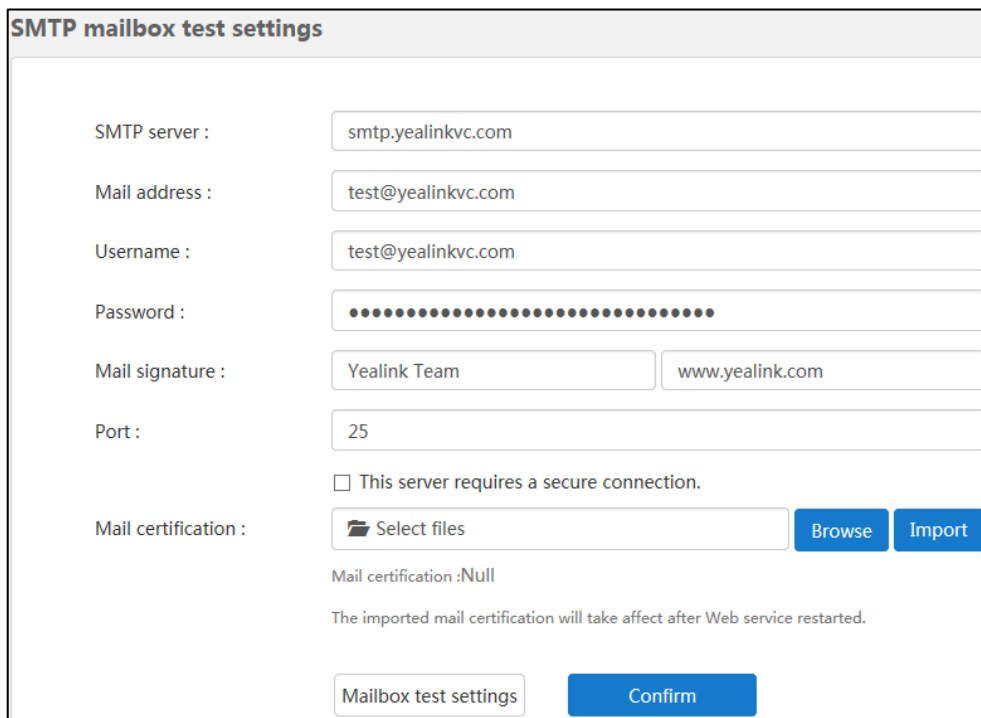
When the SMTP server you configured meets all of the following conditions, before you configure SMTP mailbox, you should obtain the mail certification from your enterprise IT.

- The SMTP server is built by the enterprise.
- The certification which the SMTP server uses is not the certification issued by CA formally.
- The SMTP server sends emails by a secure connection.

To configure the mailbox parameter:

1. Click **System->System Settings->SMTP mailbox**.

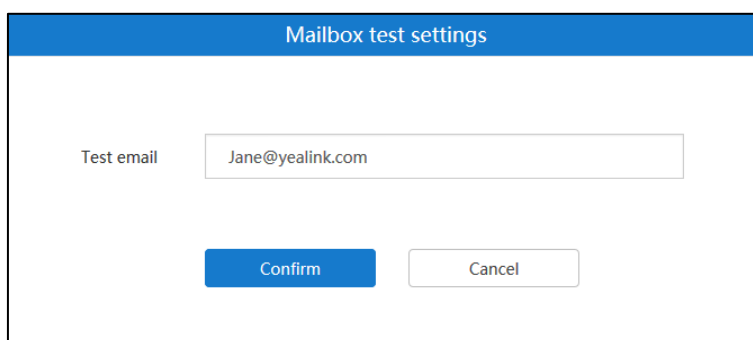
2. Configure the SMTP server address, mailbox address, username, password, signature and port.



The screenshot shows the 'SMTP mailbox test settings' configuration page. It includes the following fields and options:

- SMTP server : smtp.yealinkvc.com
- Mail address : test@yealinkvc.com
- Username : test@yealinkvc.com
- Password : [masked with dots]
- Mail signature : Yealink Team | www.yealink.com
- Port : 25
- This server requires a secure connection.
- Mail certification : [Select files] [Browse] [Import]
- Mail certification :Null
- The imported mail certification will take affect after Web service restarted.
- [Mailbox test settings] [Confirm]

3. (Optional.) Click **Browse** in the **Mail certification** field, and then select the desired certification in your computer.
Click **Import**.
YMS will reboot to make the change take effect.
4. Click **Mailbox test settings**.
Enter the email address of the recipient in the **Test email** field.



The screenshot shows a dialog box titled 'Mailbox test settings'. It contains a 'Test email' field with the value 'Jane@yealink.com' and two buttons: 'Confirm' and 'Cancel'.

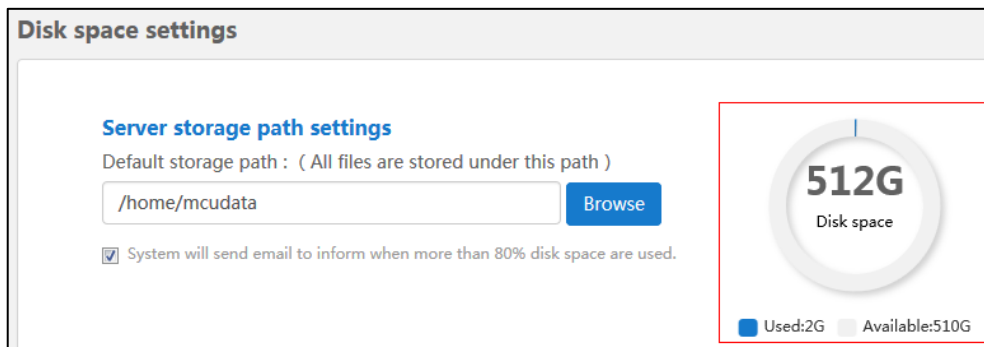
5. Click **Confirm** to test to test whether the email address you set is available.
If the mailbox has connected successfully, the page prompts "Operation success".
6. Click **Confirm**.

Disk Space Settings

Configuring the Default Storage Path

This setting specifies the default storage path, and it is used for storing all files.

You can view the used space and the available space of specified storage path by the doughnut chart on the right of page.



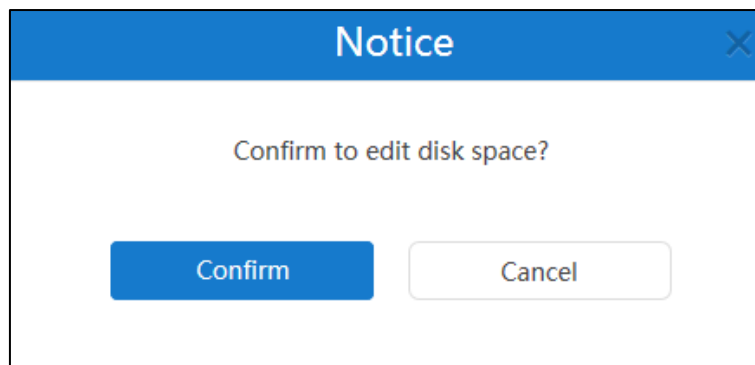
To configure the storage path:

1. Click **System**->**System Settings**->**Disk space**.
2. Click **Browse** and then select the desired path in the **Default storage path** field.
3. (Optional.) Check **System will send email to inform when more than 80% disk space are used** checkbox.

The checkbox is checked by default.

4. Click **Confirm**.

The notice is displayed as shown next:



5. Click **Confirm**.

Allocating the Space Quota

You can allocate **Call history**, **Syslog**, **Device log**, **Backup space** and **Device firmware** quota manually.

Note that the quotas should be integers. Moreover, the minimum actual quota is the maximum of the default quota and used quota. For example, the default quota of call history is 10G and

the used quota of call history is 0G, the minimum quota is 10G. If the used quota of call history is 12G, the minimum quota is 12G. And the total of call history, syslog, device log, backup space and device firmware quota should not be more than the available space of specified storage path.

To allocate the space quota:

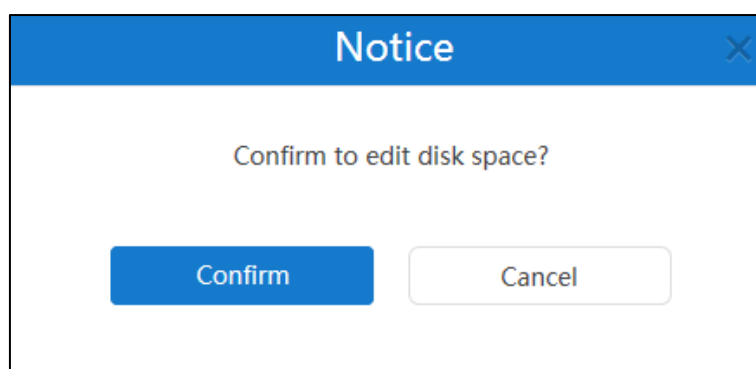
1. Click **System**->**System Settings**->**Disk space**.
2. Enter **Call history**, **Syslog**, **Device log**, **Backup space** and **Device firmware** quota in the corresponding field.

In the **Syslog** field, click **Details**, enter **Web**, **FreeSwitch**, **MCU**, **Turn Server** and **WebRTC** percentage in the corresponding field.

You can view the usage by histogram on the right of page.

3. Click **Confirm**.

The notice is displayed as shown next:



4. Click **Confirm**.

Note

After the storage quota is fulfilled, the old files will be covered automatically. If you want to release the storage, you can click **Clean up**.

Security Management

To prevent YMS from a malicious attack, YMS supports blacklist. You can view the blacklist or delete blacklist.

Registration Blacklist

When users fail to register the same YMS account 5 times in a minute using the same IP address, the users will be recorded in the blacklist and cannot register YMS accounts in the certain time.

Viewing Registration Blacklist


To view the registration blacklist:

1. Click **System->Security->Registration blacklist**.

Deleting Registration Blacklist

To allow users to register YMS accounts, you can delete the record in the blacklist.

To delete the registration blacklist:

1. Click **System->Security->Registration blacklist**.
2. Click  on the right of the desired record.

Conference Blacklist

When users fail to join conferences 30 times in a minute by dialing the same conference ID, the users will be recorded in the blacklist and cannot join conferences in the certain time.

Viewing Conference Blacklist


To view the conference blacklist:

1. Click **System->Security->Conference blacklist**.

Deleting Conference Blacklist

To allow users to join conferences, you can delete the record in the blacklist.

To delete the conference blacklist:

1. Click **System->Security->Conference blacklist**.
2. Click  on the right of the desired record.

IP Call Blacklist

When users make IP calls 100 times in a minute (including place a call to YMS directly or join conferences by URI), the users will be recorded in the blacklist and cannot make IP calls in the certain time.

Viewing IP Call Blacklist


To view the IP call blacklist:

1. Click **System->Security->IP call blacklist**.

Deleting IP Call Blacklist

To allow users to make IP calls, you can delete the record in the blacklist.

To delete the IP call blacklist:

1. Click **System->Security->IP call blacklist**.
2. Click  on the right of the desired record.

System Maintenance

Device Upgrade

You can update VC800/VC500/VC400/VC120/VC110 video conferencing endpoint, SIP VP-T49G IP phone and SIP-T58V IP phone registered the YMS account remotely. Note that only *.rom format file is available.

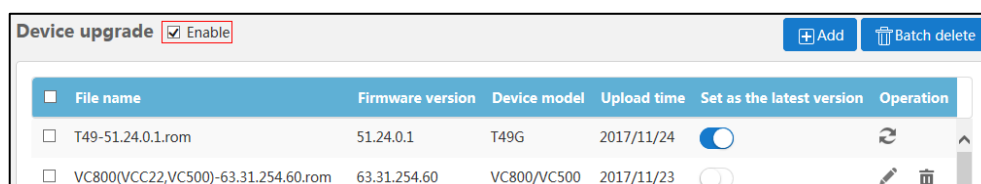
Enabling Device Upgrade Feature

Before you use device upgrade feature, you need enable **Device upgrade** feature for YMS.





To enable device upgrade feature:

1. Click **System->System Maintenance->Device upgrade**.
2. Check the **Enable** checkbox.

The checkbox is checked by default.



The screenshot shows the 'Device upgrade' page with an 'Enable' checkbox checked. Below the checkbox is a table with the following data:

File name	Firmware version	Device model	Upload time	Set as the latest version	Operation
<input type="checkbox"/> T49-51.24.0.1.rom	51.24.0.1	T49G	2017/11/24	<input checked="" type="checkbox"/>	 
<input type="checkbox"/> VC800(VCC22,VC500)-63.31.254.60.rom	63.31.254.60	VC800/VC500	2017/11/23	<input type="checkbox"/>	 

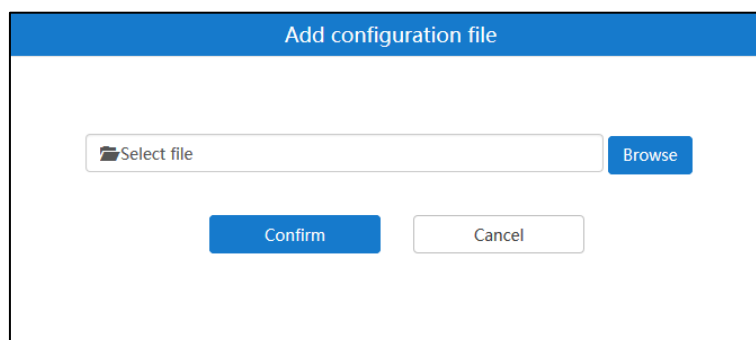
Adding Configuration Files

The configuration file is the firmware of device. You can add configuration files to update them.

To add configuration files:

1. Click **System->System Maintenance->Device upgrade**.
2. On the top-right of page, click **Add**.

3. Click **Browse** to add configuration files.



4. Click **Confirm**.


The page will display the progress bar, the configuration file is not added successfully until the progress bar reaches 100% and it is displayed in the list.

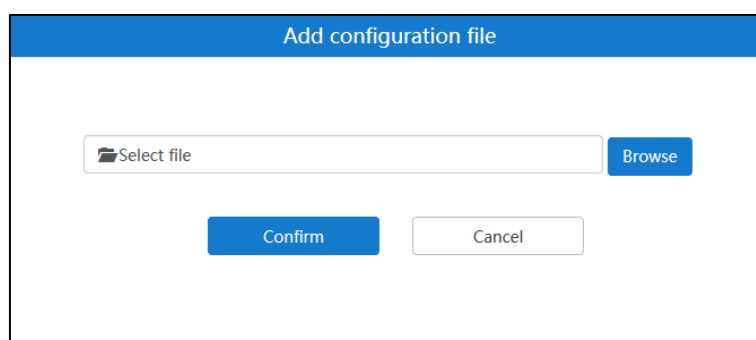
The configuration file will be set as the latest version automatically.

Updating Configuration Files

If the configuration file does not set as the latest version, you can upload a file to update the configuration file.

To update configuration files:

1. Click **System->System Maintenance->Device upgrade**.
2. Check the desired checkbox of configuration file.
3. Click  on the right of page, the dialog box of **Add configuration file** pops up.
4. Click **Browse** to update configuration file.



5. Click **Confirm**.


The page will display the progress bar, the configuration file is not added successfully until the progress bar reaches 100% and it is displayed in the list.

Updating Device Firmware

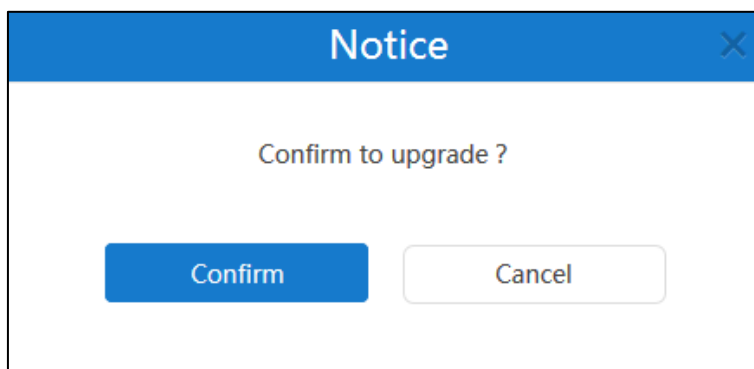
Before you update the device registered YMS account, you need set a configuration file as the latest version. When the version of the device firmware is not the same as the latest version, it

will be updated.

To update device firmware:

1. Click **System->System Maintenance->Device upgrade.**
2. Select the desired configuration file and click the switch to On in **Set as the latest version** field.
3. Click  on the right of page.

The notice is displayed as shown next:




4. Click **Confirm** to update the same type of devices.







Deleting Configuration Files

You can delete configuration files which do not set as the latest version.

To delete configuration files:

1. Click **System->System Maintenance->Device upgrade.**
2. In configuration file list, you can do the following:
 - Check the desired checkbox of configuration file, click  on the right of page to delete the configuration file.
 - Check the multiple checkboxes of configuration files.

If you want to check all checkboxes, you can check the checkboxes as following:

<input checked="" type="checkbox"/>	File name	Firmware version	Device model	Upload time	Set as the latest version	Operation
<input checked="" type="checkbox"/>	VC110-50.23.0.15.rom	50.23.0.15	VC110	2017/07/03	<input type="checkbox"/>	 
<input checked="" type="checkbox"/>	VC400-30.23.0.15.rom	30.23.0.15	VC400	2017/07/03	<input type="checkbox"/>	 
<input checked="" type="checkbox"/>	T49-51.23.0.15.rom	51.23.0.15	T49G	2017/07/03	<input type="checkbox"/>	 

On the top-right of page, click **Batch delete** to delete configuration files.

Backup/Restore

The configuration file except for license and logs of YMS can be exported and saved as a backup to disk. When the server fails, you can restore the backup.

Auto Backup Settings

You can take regular backups of the configuration data. Auto backup settings contain cycle, date and maximum backup number.

To configure the auto backup settings:

1. Click **System->System Maintenance->Backup/Restore**.
2. On the top-right of page, click **Auto backup settings**.
3. Configure the auto backup settings.
4. Click **Confirm**.

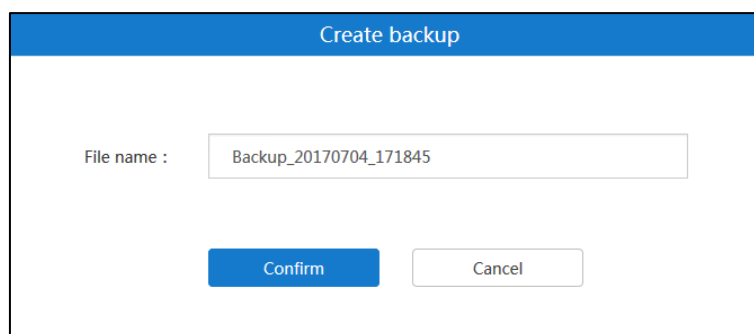
Creating a Backup Manually

You can create a backup of YMS manually.

To create a backup:

1. Click **System->System Maintenance->Backup/Restore**.
2. On the top-right of page, click **Create backup**.
3. Enter the file name in the **File name** field.

The **File name** field is filled in the format of Backup_date_time automatically.




4. Click **Confirm**.

Downloading a Backup

You can download the desired backup of YMS.

To download a backup:


1. Click **System->System Maintenance->Backup/Restore**.
2. Check the desired checkbox of backup.
3. Click  on the right of page to download the backup, and then save it to the local system.

Restoring a Backup

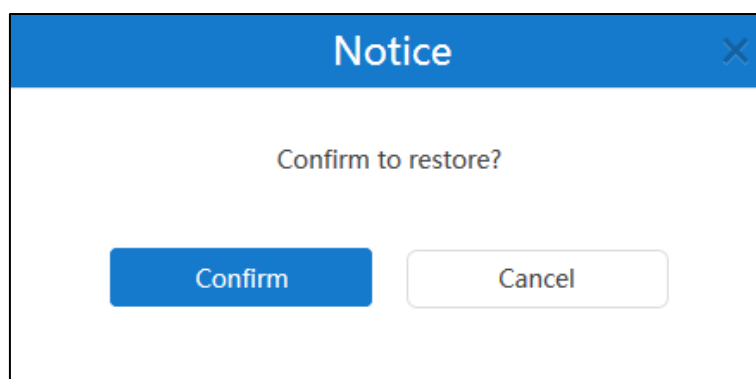
Restoring a backup by Selecting a Backup Directly

In backup list, you can select the desired backup to restore.

To restore a backup:

1. Click **System->System Maintenance->Backup/Restore**.
2. Check the desired checkbox of backup.
3. Click  on the right of page.

The notice is displayed as shown next:



4. Click **Confirm**, YMS will reboot to make the change take effect.

Restoring a backup by Uploading a Backup

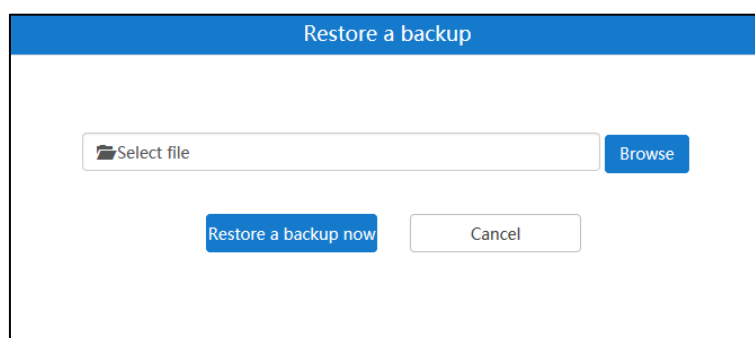
You can upload the backup saved in your computer to restore. You can upload a backup in the following scenarios:

- If the current backup was saved in your computer and the YMS is reset to factory, you need upload the backup to restore settings.
- If the backup of other YMS was saved in your computer, you can upload the backup to apply to the current YMS.

To restore a backup:

1. Click **System->System Maintenance->Backup/Restore**.


- Click **Upload backup file**, the dialog box of **Restore a backup** pops up.












- Click **Browse** to select a backup.
- Click **Restore a backup now**, YMS will reboot to make the change take effect.

Deleting a Backup

To delete a backup:

- Click **System->System Maintenance->Backup/Restore**.
- Check the desired checkbox of backup.
- In the backup list, you can do the following:
 - Check the desired checkbox of backup, click  on the right of page to delete the backup.
 - Check the multiple checkboxes of backup.

If you want to check all checkboxes, you can check the checkboxes as following:

<input checked="" type="checkbox"/>	File name	File size(MB)	Build time	Operation
<input checked="" type="checkbox"/>	AutoBackup_20170704_040000.tar.gz	5.78	2017/07/04 16:00:00	  
<input checked="" type="checkbox"/>	AutoBackup_20170703_040000.tar.gz	5.05	2017/07/03 16:00:00	  
<input checked="" type="checkbox"/>	AutoBackup_20170702_040000.tar.gz	4.83	2017/07/02 16:00:00	  

Click **Batch delete** to delete backups.

System Upgrade

Viewing System Information

You can view the current version and package time of YMS.

To view the system information:

- Click **System->System Maintenance->System upgrade**.

Upgrading System

When a new version is available, you can upgrade YMS. The latest version can be obtained from

Yealink.

To upgrade system:

1. Click **System->System Maintenance->System upgrade.**
2. Click **Browse** to upload the latest version.
3. Click **Upgrade**, YMS will reboot to finish update automatically.

Note The YMS supports the files in the format of .tar.gz.

Reboot/Reset to Factory

Resetting to Factory

You can reset to factory when you encounter problems using YMS.

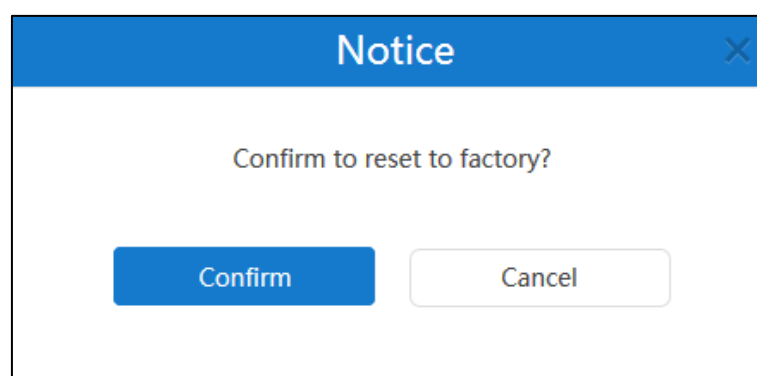
Do one of the following to reset to factory:

- **Only clear configuration information under system settings module:** Only server configurations information will be cleared. The user information (meeting rooms, account information, conference information will be saved. But conference histories, call history, log files and so on will not be saved.
- **Clear all user data:** All user data will be cleared.

To reset to factory:

1. Click **System->System Maintenance->Reboot/Factory reset.**
2. Select **Only clear configuration information under system settings module.**
3. Click **Reset.**

The notice is displayed as shown next:



4. Click **Confirm** to reset to factory.

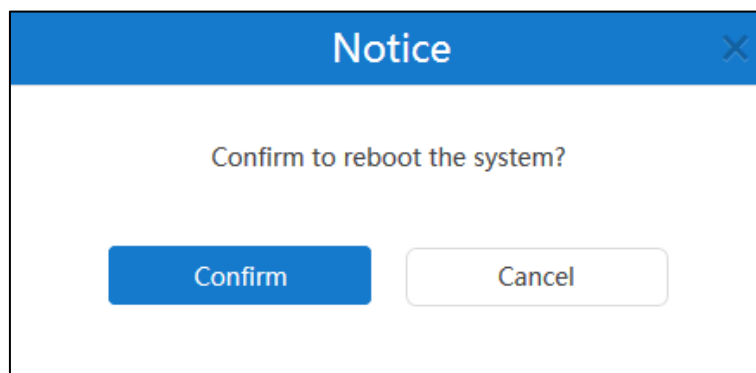
Reboot

When YMS fails to upgrade, for example if it remains on the Account Management page, you can reboot system.

To reboot system:

1. Click **System->System Maintenance->Reboot/Factory reset.**
2. Select **Reboot system.**
3. Click **Reboot.**

The notice is displayed as shown next:



4. Click **Confirm** to reboot the system.

Licenses Management

Video Port Licenses

If interactive parties want MCU to process video image or users want to register accounts, you can activate a video port license. You need purchase the license from Yealink.

When the video port is insufficient, interactive parties can only join conference by audio call. YMS supports extra 40 audio ports.

Activating the Video Port License

You can activate the video port license to enable video ports.

To activate the video port license:

1. Click **System->Licenses->Video port.**
2. Enter the license number in the **License** field.
3. Click **Activate the license.**

License information are displayed as below:

Licenses

License :	bIUeIpV0/BtIYf8IwwCCQ+2/V9ChEt/uvdaI9F+pDvitXMYzxa4nS5TzvkJZ+h
Activation type :	Offline
Status :	Activation
Current ports :	100
Valid time :	3 month(s)
Expired date :	2017/10/04

[Renew license](#)

Renewing the Video Port License

To renew the video port license:

1. Click **System->Licenses->Video port**.
2. Click **Renew license**.
3. Enter the license number in the **License** field.
4. Click **Confirm** to renew the license.

Broadcasting Port Licenses

If the video port license is activated, you can activate a broadcasting (only receive video and audio, and do not send video and audio) port license to use the broadcasting interactive feature. You need purchase the license from Yealink.

Activating the Broadcasting Port License

You can activate the broadcasting port license to enable broadcasting ports.

To activate the broadcasting port license:

1. Click **System->Licenses->Broadcast port**.
2. Enter the license number in the **License** field.
3. Click **Activate the license**.

License information are displayed as below:

Licenses

License :	bIUeIpV0/BtIYf8IwwCCQ+2/V9ChEt/uvdaI9F+pDvitXMYzxa4nS5TzvkJZ+h
Activation type :	Offline
Status :	Activation
Current ports :	100
Valid time :	3 month(s)
Expired date :	2017/10/04

[Renew license](#)

Renewing the Broadcasting Port License

To renew the broadcasting port license:

1. Click **System->Licenses->Broadcast port**.
2. Click **Renew license**.
3. Enter the license number in the **License** field.
4. Click **Confirm** to renew the license.

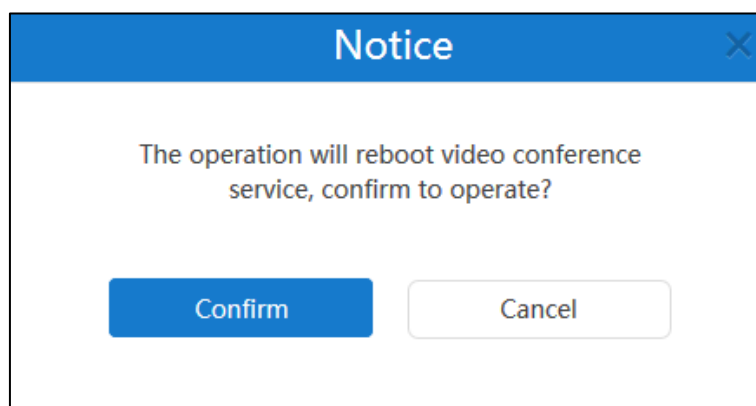
Importing Trusted CA Certificates

When you access YMS by domain name, the browser will prompt you that it is insecure. To solve this, you need import trusted CA certificates related to domain name.

To import trusted CA certificates:

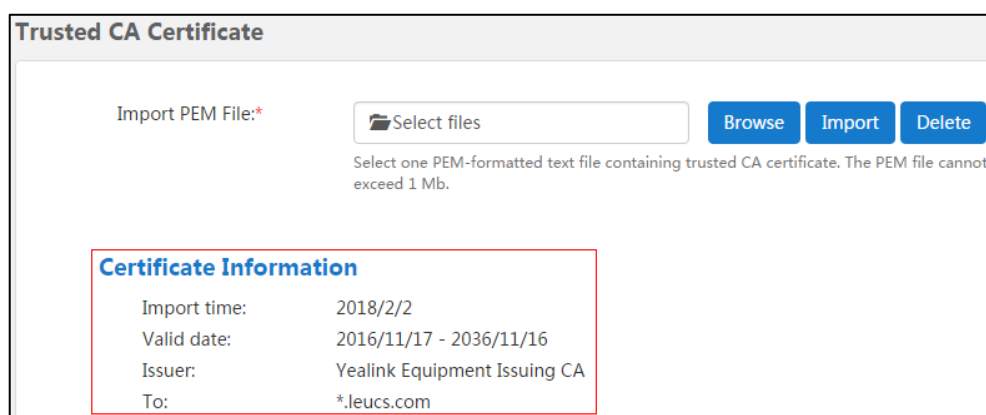
1. Click **System->Licenses->Trusted CA Certificate**.
2. Click **Browse**, and then select trusted CA certificates.
3. Click **Import**.

The notice is displayed as shown next:



4. Click **Confirm**.

Certificate information are displayed as below:



System Logs

System logs record the information of devices and YMS problem, and it can also monitor the event that occurs in the YMS. Enterprise administrator can check the reason of problems or look for the trace of attacks.

Server Logs

Syslog Server Settings

You can configure remote syslog server to collect operation logs and system logs.

To configure the syslog server settings:

1. Click **System->System Log->Server log**.
2. On the top-right of page, click **Syslog server settings**.

3. Configure the syslog server.

Syslog server settings

Server address
The IP address of the remote syslog server.

Port(1~65535)*
The port on the remote syslog server.

Transport protocol*
The transport protocol used to connect to the remote syslog server.

Parameters are described below:

Parameter	Description
Server address	Specify the IP address of the remote syslog server.
Port (1~65535)	Specify the port on the remote syslog server. Default: 514
Transport protocol	Configure the type of transport protocol used to communicate with the remote syslog server. <ul style="list-style-type: none"> • UDP—provides best-effort transport via UDP. • TCP—provides reliable transport via TCP. • TLS—provides secure communication. Default: UDP

4. Click **Confirm**.

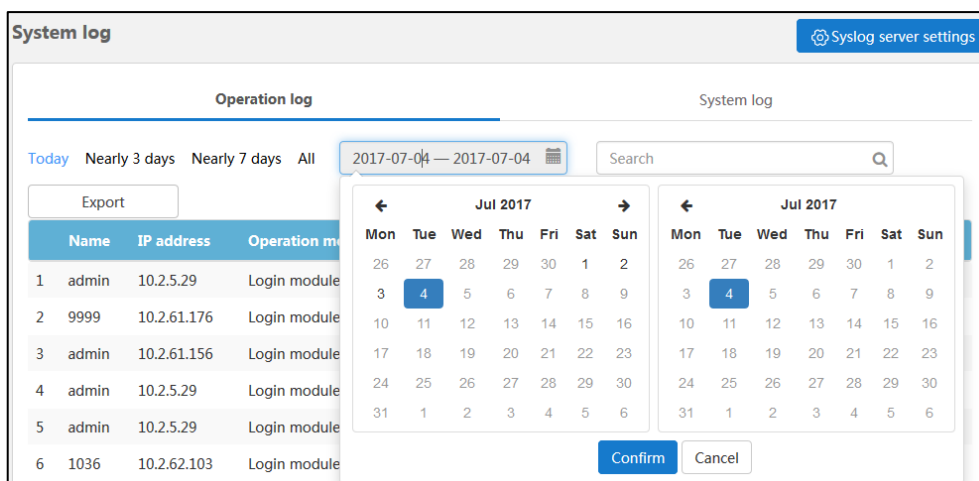
Operation Logs

Operation logs record the change logs, including access logs or configuration changes.

To view the operation log:

1. Click **System->System Log->Server log**.
2. Select **Operation log** to enter the page of operation log.
3. Click **Today**, **Nearly 3 days**, **Nearly 7 days** or **All**, the page will display the operation log during the selected time.

You can also select the start time and end time in the date selection box.



4. Click **Export** to export the operation logs.

The following is an example of operation logs:

No.	UserName	Module/Menu	Operation/Time	Remark
1	admin	SystemManager(Configuration backup/restore)	2016-12-07T16:02:41Z	Download the backup successful!
2	admin	Login/Login	2016-12-07T16:01:05Z	Account admin login success!
3	admin	Login/Login	2016-12-07T15:57:10Z	Account admin login success!
4	2221	Login/Login	2016-12-07T15:56:45Z	Account 2221 login success!
5	admin	Login/Login	2016-12-07T15:42:32Z	Account admin login success!
6	admin	SystemManager(Configuration backup/restore)	2016-12-07T15:36:05Z	Download the backup successful!
7	admin	SystemManager(Configuration backup/restore)	2016-12-07T15:36:01Z	Download the backup successful!
8	admin	SystemManager(Terminal/AutoUpgrade)	2016-12-07T15:21:53Z	Delete terminal config successful!
9	admin	登录模块登录模块	2016-12-07T15:19:28Z	账号admin登录成功!
10	4201	Login/Login	2016-12-07T15:18:53Z	Account 4201 login success!
11	4201	Login/Login	2016-12-07T15:17:31Z	Account 4201 login success!
12	admin	登录模块登录模块	2016-12-07T15:16:34Z	账号admin登录成功!
13	2221	Login/Login	2016-12-07T15:14:44Z	Account 2221 login success!
14	admin	Login/Login	2016-12-07T15:14:31Z	Logout success!
15	1222	Login/Login	2016-12-07T15:13:08Z	Account 1222 login success!
16	admin	登录模块登录模块	2016-12-07T15:10:39Z	账号admin登录成功!
17	1256	登录模块登录模块	2016-12-07T15:08:35Z	账号1256登录成功!
18	admin	Login/Login	2016-12-07T15:02:09Z	Account admin login success!
19	admin	SystemManager(Terminal/AutoUpgrade)	2016-12-07T15:00:53Z	Add terminal config success!
20	4004	Login/Login	2016-12-07T14:57:18Z	Account 4004 login success!
21	4004	Login/Login	2016-12-07T14:57:16Z	Account 4004 login success!
22	admin	Login/Login	2016-12-07T14:57:02Z	Logout success!
23	4004	Login/Login	2016-12-07T14:56:44Z	Account 4004 login success!
24	4004	Login/Login	2016-12-07T14:56:39Z	Account 4004 login success!
25	admin	Login/Login	2016-12-07T14:56:34Z	Logout success!
26	4002	Login/Login	2016-12-07T14:55:41Z	Account 4002 login success!
27	admin	Login/Login	2016-12-07T14:55:33Z	Logout success!

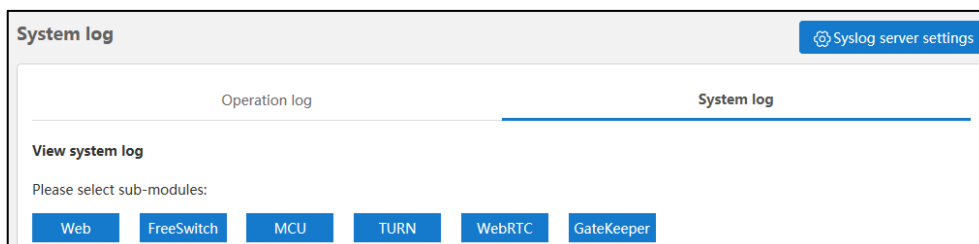
System Logs

System logs record conference logs.

You can export **Web**, **FreeSwitch**, **MCU**, **TURN**, **WebRTC** or **GateKeeper** logs and save these in your computer to view logs.

To view the system log:

1. Click **System->System Log->Server log**.
2. Select **System log** to enter the page of system log.
3. Select the desired type of system logs, and then click **Web**, **FreeSwitch**, **MCU**, **TURN**, **WebRTC** or **GateKeeper**, the selected type is blue.



- Click **Today**, **Nearly 3 days**, **Nearly 7 days** or **All**.

You can also select the start time and end time in the date selection box.

Please select the desired time to export syslog :

Today Nearly 3 days Nearly 7 days All

2017-07-04 — 2017-07-04

Export

Jul 2017							Jul 2017						
Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun
26	27	28	29	30	1	2	26	27	28	29	30	1	2
3	4	5	6	7	8	9	3	4	5	6	7	8	9
10	11	12	13	14	15	16	10	11	12	13	14	15	16
17	18	19	20	21	22	23	17	18	19	20	21	22	23
24	25	26	27	28	29	30	24	25	26	27	28	29	30
31	1	2	3	4	5	6	31	1	2	3	4	5	6

Confirm Cancel

- Click **Export** to export the system logs and save in your computer to view system logs.

Device Logs

You can enable the **Device log** feature. After you enable it, the device logs will occupy a certain amount of bandwidth. System's actual performance may vary based on the number of devices. Device logs contain SIP information, when devices interact with YMS, the information are generated.

To view the device log:

- Click **System->System Log->Device log**.
- Check the **Enable** checkbox to enable the Device log feature.

Device log Enable

All types All status Search

Name	Account	Device model	IP adress	Status	Operation
------	---------	--------------	-----------	--------	-----------

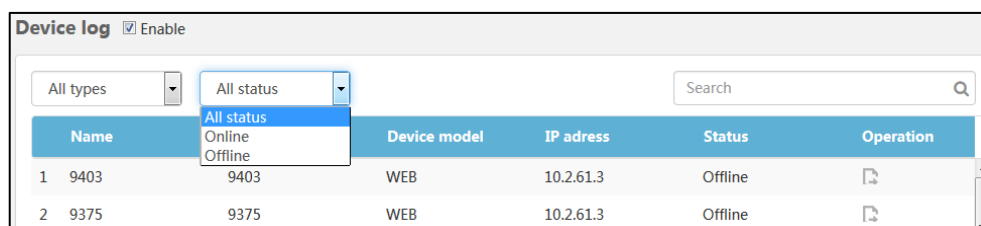
- Select the desired device type from the pull-down list, the page will display devices of the selected type.

Device log Enable

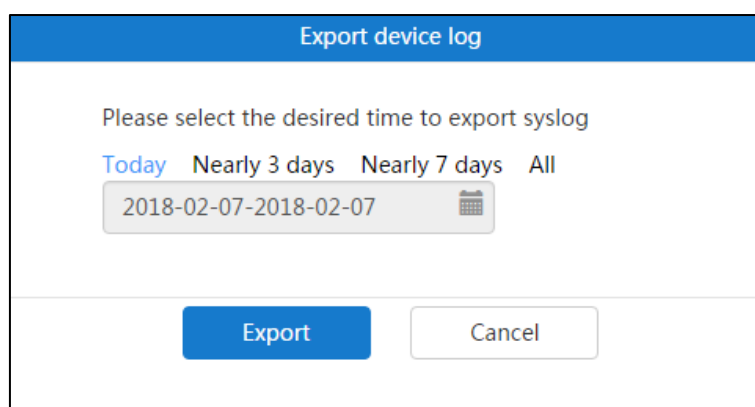
All types All status Search

All types	Account	Device model	IP adress	Status	Operation
All types					
=					
AutoTest					
SIPp	9403	WEB	10.2.61.3	Offline	🔄
T23P					
VC110	9375	WEB	10.2.61.3	Offline	🔄
VC120					
VC400	9023	WEB	10.2.61.3	Offline	🔄
VC800					
VCDesktop	1017	VP-T49G	10.15.84.18	Offline	🔄
VP-T49G					
WEB	9410	WEB	10.2.61.3	Offline	🔄

4. Select the desired status from the pull-down list, the page will display the device logs of the selected status.



5. Click on the right of desired device log.



6. Select the desired time to export syslog, and then click **Export** to export the device log.

Account Management

YMS allows you to manage user accounts in a hierarchical manner, and you can also manage room system accounts and the third party devices.

The differences between user accounts, room system accounts and third party devices are listed below:

Type	Description	Note
User accounts	Users can log into devices using the account. An account can be used to log into five devices at most simultaneously.	They are called as YMS accounts.
Room system accounts	The account is used to log into YMS by devices in the video meeting room. An account can be used to log into five devices at most simultaneously.	YMS can store up to 10000 accounts at most.
Third party devices	The devices without YMS accounts.	No

This chapter provides the account management, Topics include:

- [Department Management](#)
- [Adding User Accounts](#)
- [Adding Room System Accounts](#)
- [Adding Third Party Devices](#)
- [Viewing Accounts](#)
- [Sending Emails to YMS Accounts](#)
- [Editing Accounts](#)
- [Deleting Accounts](#)

Department Management

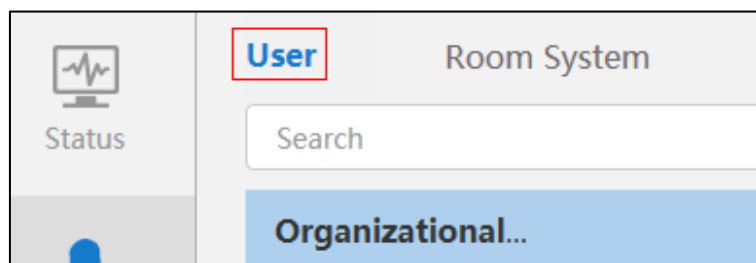
You can add departments based on the enterprise organization to manage user accounts in a hierarchical manner.

The default name in root node is the name of your enterprise. It depends on license. You can manage the department's accounts and children department's accounts.

Adding Departments

To add departments:

1. Click **Account->User**.




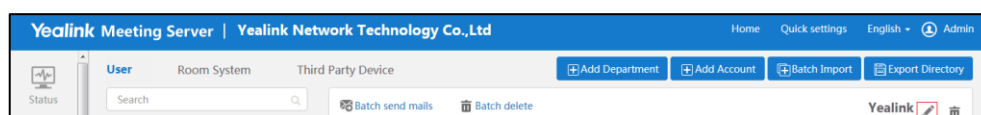
2. On the top-right of page, click **Add Department**.
3. Enter the name of department in the **Name** field.
4. Click **Select** in the **Upper department** field, and then select the desired department.
5. Click **Confirm**.

Editing Department Information

If the department information has changed, you can edit the name and upper department.

To edit department information:

1. Click **Account->User**.
2. In the Organizational Structure list, select the desired department, and then click  on the right of page.



3. Edit the corresponding parameters.
4. Click **Confirm**.

Editing Upper Departments Quickly

If the upper department has changed, you can edit upper departments quickly.


To edit upper departments quickly:

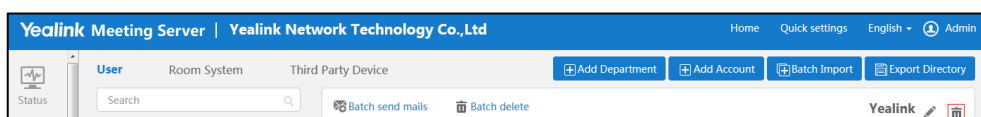
1. Click **Account->User**.
2. In the Organizational Structure list, drag the department under your desired upper departments.

Deleting Departments

If the enterprise organization has been simplified, you can delete the department. Note that if there are children departments or user accounts in the department, you cannot delete the department.

To delete departments:

1. Click **Account->User**.
2. In the Organizational Structure list, select the desired department, and then click  on the right of page to delete the department.



Adding User Accounts

User Accounts Parameters

When you add user accounts, you should know user accounts parameters.

Parameters are described below:

Parameter	Description
Manner	If the LDAP feature is enabled, specify the way of adding accounts. The available ways are: <ul style="list-style-type: none"> • Manual: you should add names and accounts manually. • Obtain from AD server: according to the account you specified, you can obtain names and accounts from AD server.
Name	If Manual is selected, specify the user's full name.
Account	If Manual is selected, specify the account which is used to log into the YMS.
Password	If you import user accounts, you can specify the passwords of YMS accounts.
AD Account	If Obtain from AD server is selected, specify the account which is used to obtain the name and account of AD account from AD server. The specified account should be obtained from AD administrators.
Obtain	Obtain the name and account of AD account from the specified account.
Enable GK registration	If the YMS registers to the embedded GK, enable or disable the account to be registered by H.323 protocol. Default: Disabled

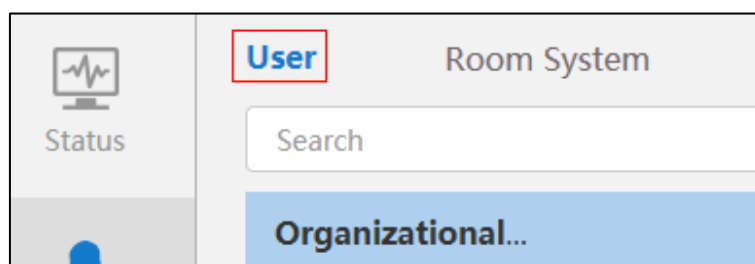
Parameter	Description
Enable authentication	Enable or disable the account to be registered with any password or without entering the password. Default: Disabled. The account can be registered with any password or without entering the password.
Email	Email address of the user. This email address is used to receive the initial password of the user and conference notification emails.
Department	Name of the department to which the user is added.
Authority	<p>The rights you want to assign to the user.</p> <p>The available rights for YMS are:</p> <ul style="list-style-type: none"> • A: All users, room system accounts, the permanent VMRs which are added to enterprise directory and the third party devices within the enterprise are visible. • B: The users, room system accounts and the permanent VMRs which are added to enterprise directory within the enterprise within the same level and subordinate deployments are visible. If the user is in root node, the third party devices are also visible. • C: The users, room system accounts and the permanent VMRs which are added to enterprise directory within the department are visible. • D: Only you are visible. When the user schedule conferences, all meeting rooms are not visible. • E: Customize the users, room system accounts, the permanent VMRs which are added to enterprise directory and the third party devices which are visible.

Note You cannot import the users with the custom right.

Adding User Accounts Manually

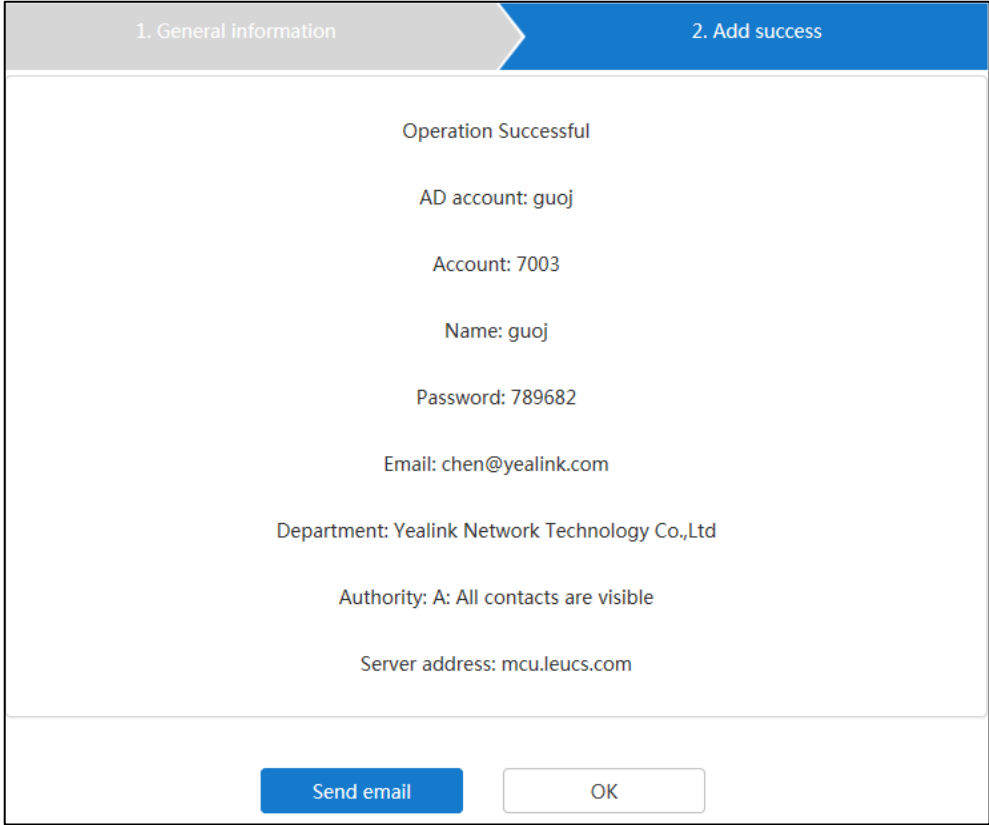
To add user accounts manually:

1. Click **Account->User**.



2. In the Organizational Structure list, select the desired department, and then click **Add Account** on the top-right of page.
3. Configure the user accounts parameters.
4. Click **Confirm**.

The account details are displayed as below:



The screenshot shows a dialog box with two tabs: '1. General information' (grey) and '2. Add success' (blue). The 'Add success' tab is active and displays the following account details:

- Operation Successful
- AD account: guoj
- Account: 7003
- Name: guoj
- Password: 789682
- Email: chen@yealink.com
- Department: Yealink Network Technology Co.,Ltd
- Authority: A: All contacts are visible
- Server address: mcu.leucs.com

At the bottom of the dialog, there are two buttons: 'Send email' (blue) and 'OK' (white).

5. If you entered the email address parameter, click **Send email** to send an email which contains the account information to users.
6. Click **Ok** to finish.

Note

If you do not set a new user's email parameters, send the user's initial password to the user and remind the user to change the password promptly.

Importing User Accounts

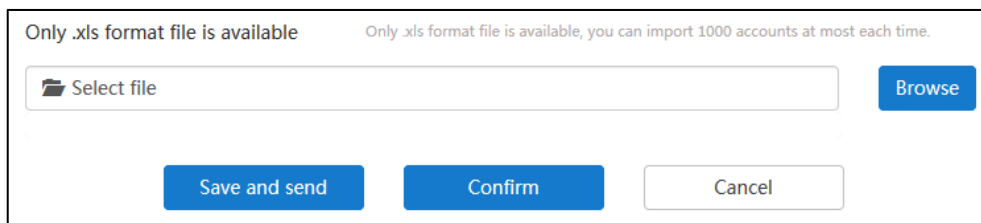
If you want to add multiple accounts quickly, you can import accounts by .xls files. Note that you cannot customize template, you need download a blank template first.

To import user accounts:

1. Click **Account->User**.
2. On the top-right of page, click **Batch Import**.
3. If the LDAP feature is enabled, click **Template download** or **Template download (AD)** to

download a blank .xls file.

4. Add the user account parameters to the template and save it in your computer.
5. According to the type of template, select **Ordinary** or **AD**.
6. Click **Browse** to import the file saved in your computer.



7. If you entered the email address parameter, click **Save and send** to send an email which contains the account information to users.
8. Click **Confirm** to finish importing accounts.

Note

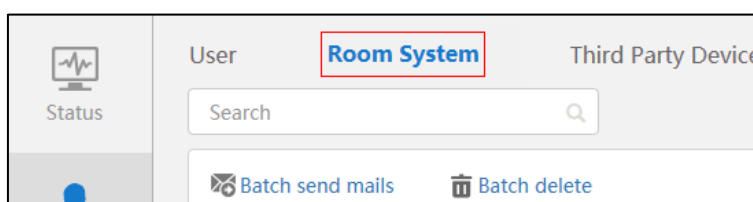
If you add user accounts by importing a .xls file, those accounts cannot be registered by H.323 protocol. If you want to allow those to be registered by H.323 protocol, contact Yealink technical support engineer.

Adding Room System Accounts

You can add room system accounts. The account is used to be associated with the device in the video meeting room.

To add room system accounts:

1. Click **Account->Room System**.



2. On the top-right of page, click **Add Account**.
3. Enter the corresponding parameters.

Parameters are described below:

Parameter	Description
Manner	<p>If the LDAP feature is enabled, specify the way of adding accounts.</p> <p>The available ways are:</p> <ul style="list-style-type: none"> • Manual: you should add names and accounts manually. • Obtain from AD server: according to the account you

Parameter	Description
	specified, you can obtain names and accounts from AD server.
Name	If Manual is selected, specify the user's full name.
Account	If Manual is selected, specify the account which is used to log into the YMS.
AD Account	If Obtain from AD server is selected, specify the account which is used to obtain the name and account of AD account from AD server. The specified account should be obtained from AD administrators.
Obtain	Obtain the name and account of AD account from the specified account.
Enable GK registration	If the YMS registers to the embedded GK, enable or disable the account to be registered by H.323 protocol. Default: Disabled
Enable authentication	Enable or disable the account to be registered with any password or without entering the password. Default: Disabled
Email	Email address of the user. This email address is used to receive the initial password of the user and conference notification emails.
Visible department	The range of the users is visible.

4. Click **Confirm**.

The account details are displayed as below:

1. General information
2. Add success

Operation Successful

AD account: guoj

Account: 7003

Name: guoj

Password: 457197

Email: chen@yealink.com

Authority: E: Custom

Server address: mcu.leucs.com

Send email
OK

5. If you entered the email address parameter, click **Send email** to send an email which contains the account information to device owner.
6. Click **Ok** to finish.

Note If you do not set a new room system account's email parameters, send the room system account's initial password to the user and remind the user to change the password promptly.

Adding Third Party Devices

If you want to invite the third party devices to join the conference, you can add them to the enterprise directory.

Third Party Devices Parameters

When you add third party devices, you should know third party devices parameters.

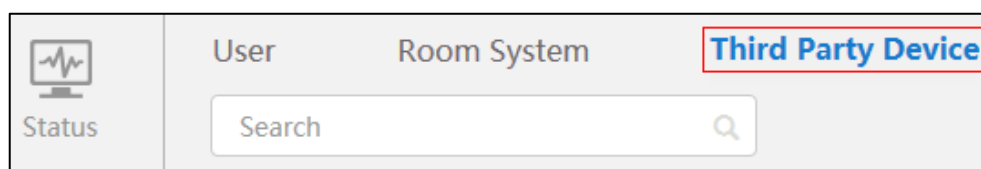
Parameters are described below:

Parameter	Description
Name	The device's full name.
Protocol	The device's call protocol.
Number	The device's URI.
Device IP	The device's IP address.
Email	The device's email address. This email address is used to receive the initial password of the device and conference notification emails.

Adding Third Party Devices Manually

To add the third party devices manually:

1. Click **Account->Third Party Device**.



2. On the top-right of page, click **Add Third Party Device**.

- Configure the third party devices parameters.

A screenshot of a web form for configuring third party devices parameters. The form contains the following fields and values:

- Name***: Jack
- Number***: SIP (dropdown menu) and 2210@sip.com
- Device IP***: 192.168.1.15
- Email**: chen@yealink.com

At the bottom of the form, there are two buttons: a blue **Confirm** button and a white **Cancel** button with a grey border.

- Click **Confirm**.

Importing Third Party Devices

If you want to add multiple accounts quickly, you can import accounts by .xls files. Note that you cannot customize template, you need download a blank template first.

To import third party devices:

- Click **Account->Third Party Device**.
- On the top-right of page, click **Batch Import**.
- Click **Template download** to download a blank .xls file.
- Add the third party devices parameters to the template and save it in your computer.
- Click **Browse** to import the file saved in your computer.

A screenshot of a file selection dialog box. The dialog contains the following elements:

- Message: "Only .xls format file is available. Only .xls format file is available, you can import 1000 unionAccounts at most each time."
- Input field: "Select file" with a folder icon on the left.
- Button: A blue **Browse** button.
- Buttons: A blue **Confirm** button and a white **Cancel** button with a grey border at the bottom.

- Click **Confirm**.

Viewing Accounts

Viewing User Accounts

To view the user accounts details:

- Click **Account->User**.

2. On the top-right of page, click **Export Directory** to export the file, and then save it in the local system.

Viewing Third Party Devices

To view the third party devices:

1. Click **Account->Third Party Device**.
2. On the top-right of page, click **Export** to export the file, and then save it in the local system.

The following is an example of file:

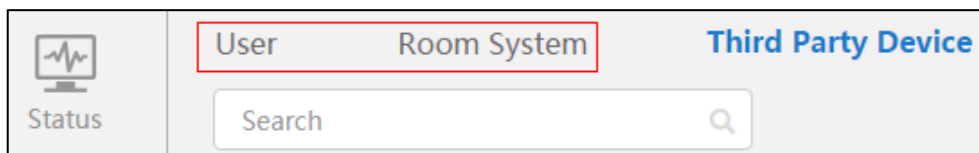
Name *	Protocol *	Number *	Device IP *	E-mail
Test	H323	90000	10.2.5.61	
Test 2	SIP	1008	10.2.61.6	


Sending Emails to YMS Accounts

If the YMS accounts are associated with emails, you can send emails to tell their users about the account information.







To send emails to YMS accounts:

1. Click **Account->User** or **Account->Room System**.



2. In the account list, you can do the following:
 - Check a checkbox, click  on the right of page to send an email.
 - Check the multiple checkboxes.

If you want to check all checkboxes, you can check the checkbox as following:

<input checked="" type="checkbox"/>	Name ^	Account ↕	Department	Email	Build tim... ↕	Operation	
<input checked="" type="checkbox"/>	1	2078	2078	Yealink Network Techn...	chensw@yealink.c...	2017-09-04	  
<input checked="" type="checkbox"/>	2	2081-Portugues	2081	Yealink Network Techn...		2017-09-04	  

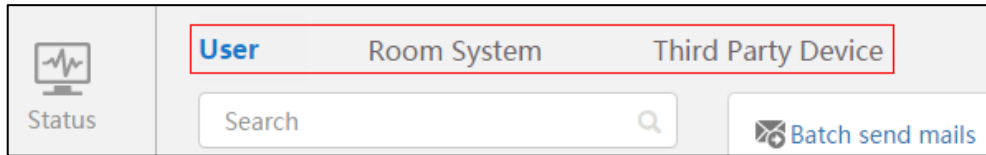
(Take the user account list for example)


Click **Batch send mails** to send emails in the batch.

Editing Accounts

To edit accounts:

1. Click **Account->User**, **Account->Room System** or **Account->Third Party Device**.



2. Check the desired checkbox of account, and then click  on the right of page to edit accounts.
3. Edit the corresponding parameters, and then save the change.

If the user account or room system account is associated with an email address, it will receive an email which informs you the account information is edited.

Note

If the user accounts or third party devices are created by importing accounts, you can edit accounts information in the original .xls file which is used to be imported to YMS.

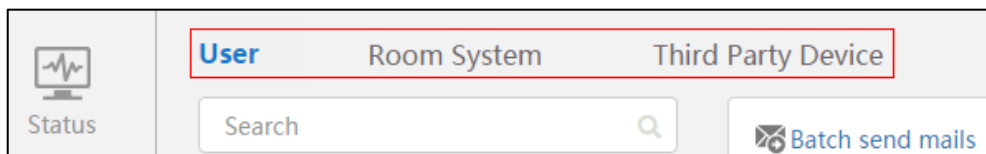
If you want to edit the department to which the user is added quickly, you can drag the user account under your desired departments in the Organizational Structure list.


If the conference which is scheduled by the user account or room system account is ongoing, you cannot edit the account.

Deleting Accounts











To delete accounts:

1. Click **Account->User**, **Account->Room System** or **Account->Third Party Device**.



2. In the account list, you can do the following:
 - Check the desired checkbox of account., click  on the right of page to delete the account.
 - Check the multiple checkboxes.

If you want to check all checkboxes, you can check the checkbox as following:

 Batch send mails		 Batch delete					Test  
<input checked="" type="checkbox"/>	Name ^	Account v	Department	Email	Build tim... v	Operation	
<input checked="" type="checkbox"/>	1	2078	2078	Yealink Network Techn...	chensw@yealink.c...	2017-09-04	  
<input checked="" type="checkbox"/>	2	2081-Portugues	2081	Yealink Network Techn...		2017-09-04	  

(Take the user account list for example)

Click **Batch delete** to delete accounts in the batch.

If the user account or room system account is associated with an email address, it will receive an email which informs you the account and relate data are deleted.

Note

If the conference which is scheduled by the user account or room system account is ongoing, you cannot delete the account.

Meeting Room Management

You can view, edit and delete entity meeting rooms and permanent Virtual Meeting Rooms (VMRs).

Meeting rooms include entity meeting rooms and permanent VMRs. The differences between these are listed below:

Difference	Mode	Description	
Definition	Entity meeting rooms	YMS integrates with OA, users can use the meeting room to schedule conferences. For more information, please refer to Yealink Meeting Server User Guide .	
	Permanent VMRs	Users can join the permanent VMR at any time. But permanent VMRs cannot be used to schedule conferences.	
Category	Entity meeting rooms	General meeting rooms	The general meeting rooms do not have devices.
		Video meeting rooms	The video meeting rooms have devices.
	Permanent VMRs	No	

This chapter provides the meeting room management, Topics include:

- [Adding Meeting Rooms](#)
- [Editing or Deleting Meeting Rooms](#)

Adding Meeting Rooms

Adding General Meeting Rooms

To add general meeting rooms:

1. Click **Meeting Room**.

2. On the top-right of page, click **Add Meeting Room**.

The screenshot shows a dialog box titled "Add Meeting Room". It contains a "Type" field with two radio buttons: "Meeting" (which is selected) and "Video". Below this is a "Room name" field with a text input box containing the placeholder "Please enter meeting room name". At the bottom of the dialog are two buttons: "Confirm" and "Cancel".

3. Select **Meeting** in the **Type** field.
4. Enter the name of meeting room in the **Room name** field.
5. Click **Confirm**.

Adding Video Meeting Rooms

To add video meeting rooms:

1. Click **Meeting Room**.
2. On the top-right of page, click **Add Meeting Room**.
3. Select **Video** in the **Type** field.

The screenshot shows a dialog box titled "Add Meeting Room". It contains a "Type" field with two radio buttons: "Meeting" and "Video" (which is selected). Below this are two text input fields: "Room name" with the placeholder "Please enter meeting room name" and "Account bound" with the placeholder "Please select an account registered on device" and a dropdown arrow. At the bottom of the dialog are two buttons: "Confirm" and "Cancel".

4. Enter the name of meeting room in the **Room name** field.
5. Select the desired account from the pull-down list of **Account bound**.
The account is used to log into YMS by the Yealink VC device in the video meeting room.
6. Click **Confirm**.

Discussion Mode and Training Mode

There are two modes of permanent VMRs: **Discussion mode** and **Training mode**. The differences between these two modes are listed below:

Difference	Mode	Description
------------	------	-------------

Difference	Mode	Description	
Role	Discussion	Moderator	Enterprise administrator can specify contacts in enterprise directory to be moderators.
		Guest	The participants of the permanent VMR without moderator privileges.
	Training	Moderator	Enterprise administrator can specify contacts in enterprise directory to be moderators. If broadcasting interactive feature is enabled, moderators are interactive parties by default.
		Lecturer	Moderator can promote any moderator and guest to be lecturers. Lecturers can speak in the conference.
Guest	The participants of the permanent VMR without moderator privileges. If broadcasting interactive feature is enabled, guests are broadcasting parties by default.		
Feature Privilege	Discussion	When moderators log into the YMS, moderators can view conferences information, they can also configure messages, call participants, invite participants, search for participants, remove participants, mute or unmute participants, turn on or off video, block or unblock audio, switch the roles between the moderators and guests, control far-end camera, lock or unlock conferences, record conferences, exit conferences and end conferences.	When moderators log into the YMS, moderators can configure the conference layout.
	Training	When guests log into the YMS, guests can only view conferences information.	When moderators log into the YMS, moderators can configure the personal layout, allowing/rejecting/ignoring participants to speak, , call the roll and switch the roles between the lecturers and moderators/guests.
Layout	Discussion	Moderators and guests can view all participants. The default layout depends on the default layout configuration which you set. For more information, please refer to Configuring the Default Layout on page 12.	
	Training	<ul style="list-style-type: none"> For moderator, they can view all participants by default. The default layout depends on the default layout configuration which you set. For more information, please refer to Configuring the Default Layout on page 12. If broadcasting interactive feature is enabled, moderators can view all interactive parties by default. For guest, the layout gives equal prominence to every lecturer by default. If no lecturer exists in the conference, all guests can only view the reminder of waiting for the lecturer. 	

Difference	Mode	Description
		If broadcasting interactive feature is enabled, for broadcasting party, the layout gives equal prominence to every lecturer by default. If no lecturer exists in the conference, the broadcasting party can only view the reminder of waiting for the lecturer.
Speaking	Discussion	Free speech.
	Training	By default, all moderators and guests are muted automatically. If they want to speak, moderators should be unmuted, guests should apply for speaking, and then wait for the moderator to allow the application.
Sharing content	Discussion	By default, both moderators and guests can share content.
	Training	By default, only moderators and lecturers can share content, guests cannot.

Adding Permanent Virtual Meeting Rooms

To add permanent VMRs:

1. Click **VMR**.
2. On the top-right of page, click **Add Virtual Meeting Room**.
3. Enter the corresponding parameters.



Parameters are described below:

Parameter	Description
ID	ID required to join the conference. Default: The range of ID is 20000-89999
Require password	Enable or disable the password required to join the conference. Default: Enabled
Password	Password required to join the conference.
Moderators	They can control the permanent VMRs at any time. For more information, please refer to Yealink Meeting Server User Guide .
Favorites	In conference, you can select the favorites to invite them to join the permanent VMR.
Max participants	If the participates are more than the number, the participant cannot join the permanent VMR.
Add to directory	The permanent VMR will be added to the enterprise directory of devices. Default: Enabled
Video resolution	Max video resolution Configure the maximum video resolution.

Parameter	Description
	<ul style="list-style-type: none"> • 1080P/30FPS • 720P/30FPS • 360P/30FPS • 4CIF • CIF <p>Default: 720P/30FPS.</p>
	<p>Configure the maximum content sharing resolution.</p> <ul style="list-style-type: none"> • 1080P/30FPS • 1080P/15FPS • 1080P/5FPS • 720P/30FPS • 720P/15FPS • 720P/5FPS <p>Default: 1080P/5FPS</p> <p>If you select 1080P/30FPS or 1080P/15FPS as the maximum content sharing resolution, it will bring the problem of high computing performance.</p>
Call bandwidth	limit the bandwidth of media which is received by YMS from individual participants.
Layout	Configure the default layout of conference participants. The conference participants refer to the persons who are in Discussion mode permanent VMRs or the moderators who are in Training mode permanent VMRs.
Broadcasting interactive	If the permanent VMRs are in Training mode and Broadcasting interactive feature is enabled (Enabling Broadcasting Interactive Video Conferences on page 17, enable Broadcasting interactive feature. By default, moderators are interactive parties, others are broadcasting parties.

4. Click **Confirm**.

Editing or Deleting Meeting Rooms

You can click **Meeting Room/VMR**, and then click  on the right of page to edit meeting rooms, or click  on the right of page to delete meeting rooms.

Conference Control

You can view, delete and control video conferences.

The video conferences include scheduled conferences, meet now conferences and permanent

This chapter provides the meeting room management, Topics include:

- [Viewing Conferences](#)
- [Deleting Conferences](#)
- [Controlling Conferences](#)

Viewing Conferences

You can view ongoing conferences, upcoming conferences in nearly a month. Conference information contains subject, start time, organizers, type, ID and duration.

To view conferences:

1. Click **Conference Control**.
2. Do the following:
 - Click **All** to view all upcoming conferences and ongoing conferences
 - Click **Ongoing Conference** to view ongoing scheduled conferences, ongoing meet now conferences and permanent VMRs in use.
 - Click **Upcoming Conference** to view upcoming video conferences and permanent VMRs in idle.

Deleting Conferences

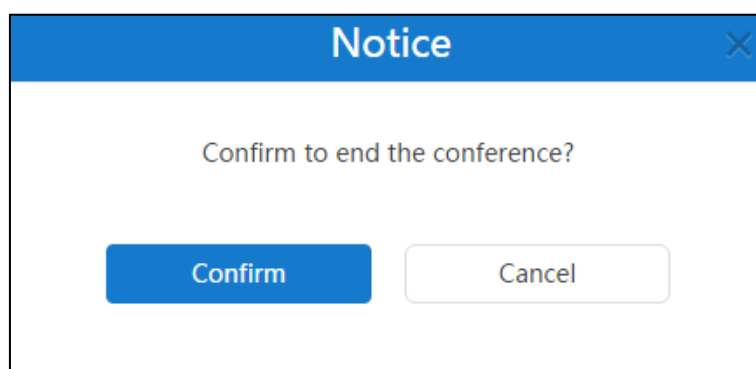
You can delete ongoing conferences, upcoming conferences in nearly a month.

If you want to delete ongoing scheduled conferences, ongoing meet now conferences and permanent VMRs in use, conferences will end.

To delete conferences:

1. Click **Conference Control**.
2. Click **Ongoing Conference/Upcoming Conference**, and then click  on the right of the desired conference.

The notice is displayed as shown next:





3. Click **Confirm**.

Controlling Conferences

You can control ongoing scheduled video conferences, ongoing meet now conferences and permanent VMRs in use, and you can also configure permanent VMRs in idle. The options of controlling conferences are configuring the conference layout, configuring the personal layout, configuring messages, manage conference participants and so on.

To control conferences:

1. Click **Conference Control**.
2. Do the following to enter conference control page:
 - To control ongoing scheduled video conferences, ongoing meet now conferences and permanent VMRs in use, click **Ongoing Conference**.
Click  on the right of the desired conference.
 - To control permanent VMRs in idle, click **Upcoming Conference**.
Click  on the right of the desired conference.
3. Control the conference. For more information, refer to [Yealink Meeting Server User Guide](#).

Conference Statistics

You can view the call statistics of YMS, and you can also view the records of different call types.

Topics include:

- [Viewing Conference Statistics](#)
- [Viewing Records](#)

Viewing Conference Statistics

You can click **Statistics** to view the conference statistics of YMS.

The page shows as below:

Statistics (2017/03/11 ~ 2017/04/11) → Displays the selected time, the page shows the conference details and ports details during the selected time.

Conference details			Ports details		
Type	Conference times	Duration	Rank	Concurrent ports	Frequency
Total conferences 459 Total duration 410:19:42			Total ports 100 Max concurrent ports 12		
P2P	116 (25.27%)	09:07:30	1	1	53.33%
Meet Now	228 (49.67%)	66:48:05	2	3	20.35%
Scheduled	115 (25.05%)	334:24:07	3	2	11.93%
			4	4	6.67%
			5	Others	7.72%

Total conferences and duration. Times and duration of different conference types.

Total ports and maximum concurrent ports. The concurrent ports and frequency of top five.

Name	Description
P2P	The call between two devices.
Meet Now	They are initiated by the device or They are initiated by joining the permanent VMRs, without reservation.
Scheduled conferences	They are scheduled in advance.
Max concurrent ports	They show the maximum concurrent ports during the whole time.
Concurrent ports	They show the maximum concurrent ports during the selected time.

Viewing Records

You can view all calls records, P2P calls records, meet now records and scheduled conference records.

To view records:

1. Click **Statistics**.
2. Select **All**, **P2P**, **Meet Now** and **Scheduled**, the page will display the selected type of conferences.
3. Click the desired call subject or click **View** on the right of page.

Subject	Type	ID	Time	Duration	Detail
1 Call from 2550 to Jannie	P2P	--	2017/07/04 14:28:05 - 14:28:23	00:00:18	View
2 Jannie's video conference	Scheduled	73967	2017/07/04 13:55:00 - 14:30:00	00:35:00	View

4. Click **Export** to export records and save it in your computer.

The following is an example of call records:

Subject	Type	ID	Start	End	Duration
test4's video conference	Meet Now	65665	2018/02/28 10:39:11	2018/02/28 10:39:12	00:00:01
test5's video conference	Meet Now	79855	2018/02/28 10:38:58	2018/02/28 10:39:02	00:00:04

Troubleshooting

This chapter provides general troubleshooting information to help you solve problems you might encounter when using YMS.

Troubleshooting Solutions

This chapter provides general troubleshooting solutions to help you solve the problems you might encounter when using YMS

If problems you encounter are not mentioned in this chapter, you can contact Yealink distributor or Yealink technical support engineer.

General Issues

Why does web page prompt error message when you enter data?

- Check whether the data follow the rules.

The rules are as following:

Type	Character Limit	Range
Login password	No	[6,16]
Email's password	No	[1,128]
Email address	<, >, ", ', & are illegal characters, the correct format of email address is <user>@<domain.com/IP address>.	No
Accounts	Digits.	4
The name of account	Digits or characters	[1,64]
The domain name of server	No	[1,128]
The name of backup	Digits, characters or _	[1,128]

Why do you fail to send emails to accounts?

- Check SMTP mailbox parameters are correct.

Why does the user place an audio-only call?

- Check whether the used license ports reach the limit.
- Check whether the license has not been activated or has expired.

Why does not the user receive emails?

- Ask users to check spam folders to check intercepted emails.
- Contact the enterprise staff in IT department to check the back-end server, the back-end server may intercept emails.

Appendix: Time Zones

Time Zone Name
(UTC-11:00) Coordinated Universal Time-11
(UTC-11:00) Samoa
(UTC-10:00) Hawaii
(UTC-09:00) Alaska
(UTC-08:00) Baja California
(UTC-08:00) Pacific Time (US & Canada)
(UTC-07:00) Arizona
(UTC-07:00) Chihuahua, La Paz, Mazatlan
(UTC-07:00) Mountain Time (US & Canada)
(UTC-06:00) Central America
(UTC-06:00) Central Time (US & Canada)
(UTC-06:00) Guadalajara, Mexico City, Monterrey
(UTC-06:00) Saskatchewan
(UTC-05:00) Bogota, Lima, Quito
(UTC-05:00) Eastern Time (US & Canada)
(UTC-05:00) Indiana (East)
(UTC-04:00) Asuncion
(UTC-04:00) Atlantic Time (Canada)
(UTC-04:00) Cuiaba
(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
(UTC-04:00) Santiago
(UTC-03:30) Newfoundland
(UTC-03:00) Brasilia
(UTC-03:00) Buenos Aires
(UTC-03:00) Cayenne, Fortaleza
(UTC-03:00) Greenland
(UTC-03:00) Montevideo
(UTC-02:00) Coordinated Universal Time-02
(UTC-02:00) Mid-Atlantic
(UTC-01:00) Azores
(UTC-01:00) Cape Verde Is.
(UTC) Casablanca
(UTC) Coordinated Universal Time
(UTC) Dublin, Edinburgh, Lisbon, London
(UTC) Monrovia, Reykjavik
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Time Zone Name
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb
(UTC+01:00) West Central Africa
(UTC+01:00) Windhoek
(UTC+02:00) Amman
(UTC+02:00) Athens, Bucharest, Istanbul
(UTC+02:00) Beirut
(UTC+02:00) Cairo
(UTC+02:00) Damascus
(UTC+02:00) Harare, Pretoria
(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(UTC+02:00) Jerusalem
(UTC+02:00) Minsk
(UTC+03:00) Baghdad
(UTC+03:00) Kuwait, Riyadh
(UTC+03:00) Moscow, St. Petersburg, Volgograd
(UTC+03:00) Nairobi
(UTC+03:30) Tehran
(UTC+04:00) Abu Dhabi, Muscat
(UTC+04:00) Baku
(UTC+04:00) Port Louis
(UTC+04:00) Tbilisi
(UTC+04:00) Yerevan
(UTC+04:30) Kabul
(UTC+05:00) Ekaterinburg
(UTC+05:00) Islamabad, Karachi
(UTC+05:00) Tashkent
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
(UTC+05:30) Sri Jayawardenepura
(UTC+05:45) Kathmandu
(UTC+06:00) Astana
(UTC+06:00) Dhaka
(UTC+06:00) Novosibirsk
(UTC+06:30) Yangon (Rangoon)
(UTC+07:00) Bangkok, Hanoi, Jakarta
(UTC+07:00) Krasnoyarsk
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
(UTC+08:00) Irkutsk
(UTC+08:00) Kuala Lumpur, Singapore
(UTC+08:00) Perth
(UTC+08:00) Taipei
(UTC+08:00) Ulaanbaatar

Time Zone Name
(UTC+09:00) Osaka, Sapporo, Tokyo
(UTC+09:00) Seoul
(UTC+09:00) Yakutsk
(UTC+09:30) Adelaide
(UTC+09:30) Darwin
(UTC+10:00) Brisbane
(UTC+10:00) Canberra, Melbourne, Sydney
(UTC+10:00) Guam, Port Moresby
(UTC+10:00) Hobart
(UTC+10:00) Vladivostok
(UTC+11:00) Magadan
(UTC+11:00) Solomon Is., New Caledonia
(UTC+12:00) Auckland, Wellington
(UTC+12:00) Coordinated Universal Time+12
(UTC+12:00) Fiji
(UTC+13:00) Nuku'alofa